DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiWeb

Study Guide

for FortiWeb 6.4

Vouchers & Dumps are Available | WhatsApp

FORTINET NSE Training Institute

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Fortinet Training

https://training.fortinet.com

Fortinet Document Library

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://training.fortinet.com/local/staticpage/view.php?page=certifications

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Feedback

Email: askcourseware@fortinet.com

FORTINET

1/5/2022

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

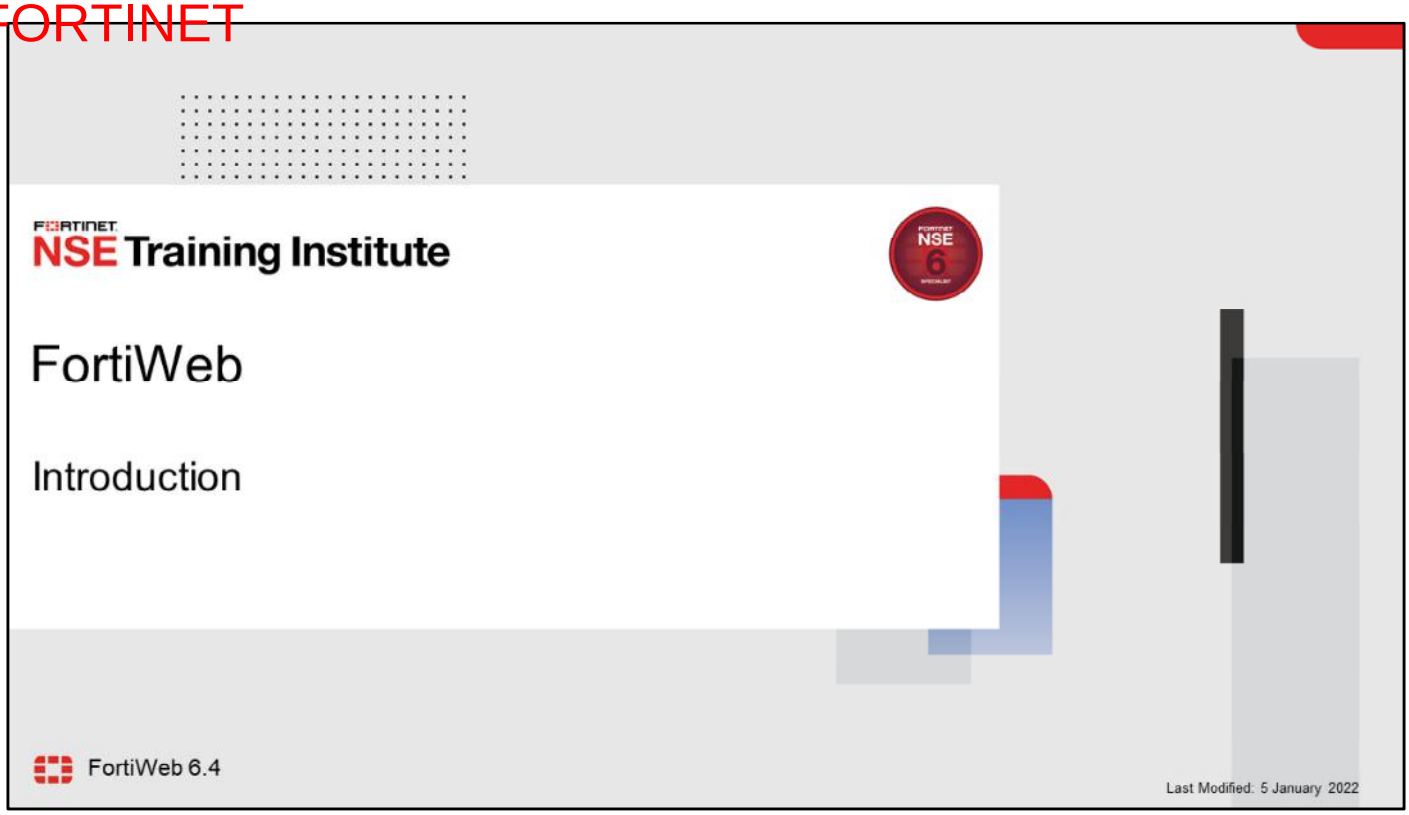
Brave-dumps.com

TABLE OF CONTENTS

01 Introduction 4
02 Basic Setup 49
03 Compliance 103
04 Authentication and Access Control 145
05 Web Application Security 202
06 DoS and Defacement 254
07 Machine Learning and Bot Detection 289
08 SSL and TLS 344
09 Application Delivery 397
10 API Protection and Bot Mitigation 426
11 Additional Configuration 466
12 Troubleshooting 505

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

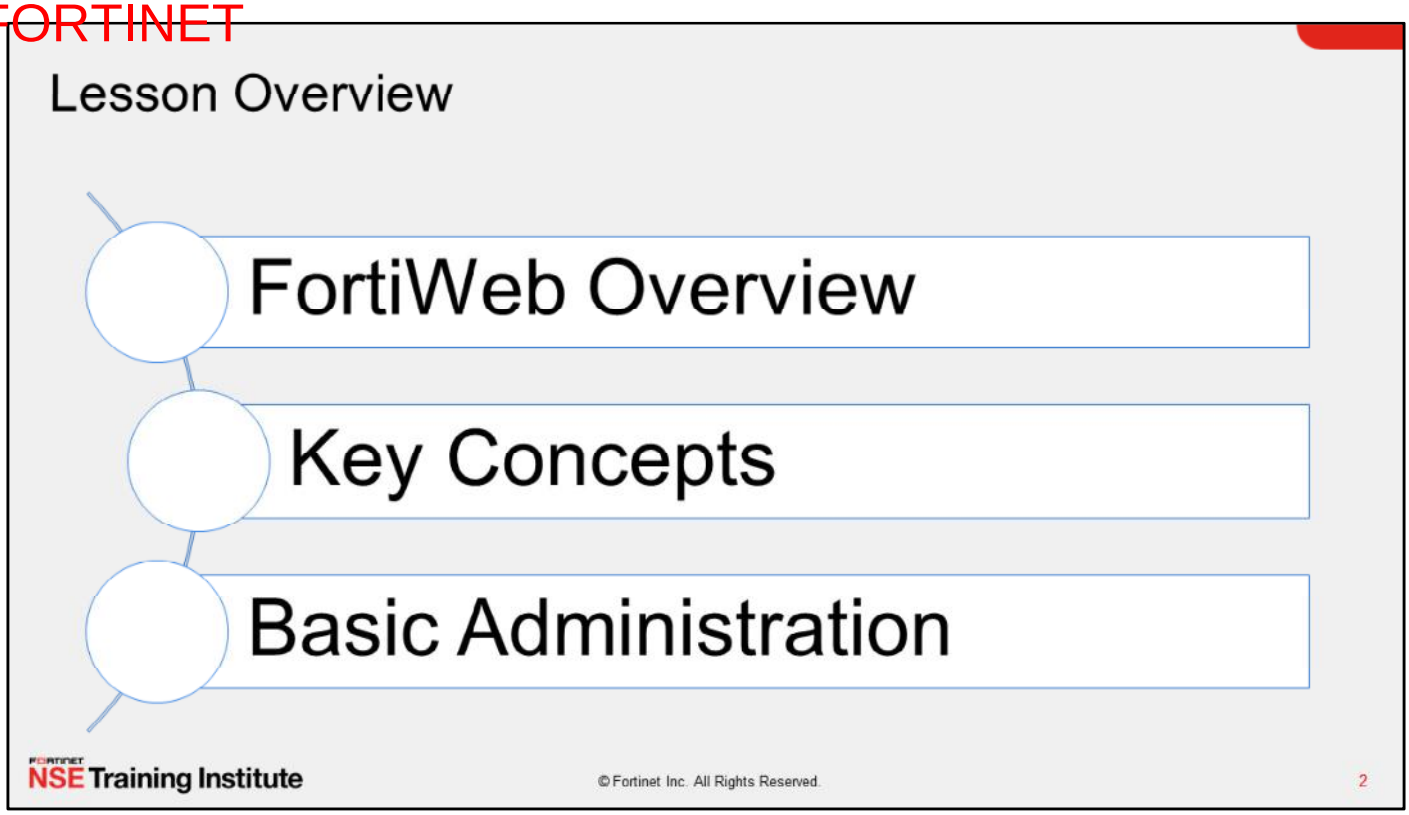


In this lesson, you will learn the basics of FortiWeb. This includes how to perform some basic initial configuration and how FortiWeb fits into existing network architectures.

While products such as FortiGate protect your client systems from network threats, FortiWeb is specifically designed to protect your web servers from specific threats unique to web content delivery.

Vouchers & Dumps are Available | WhatsApp +201224560923

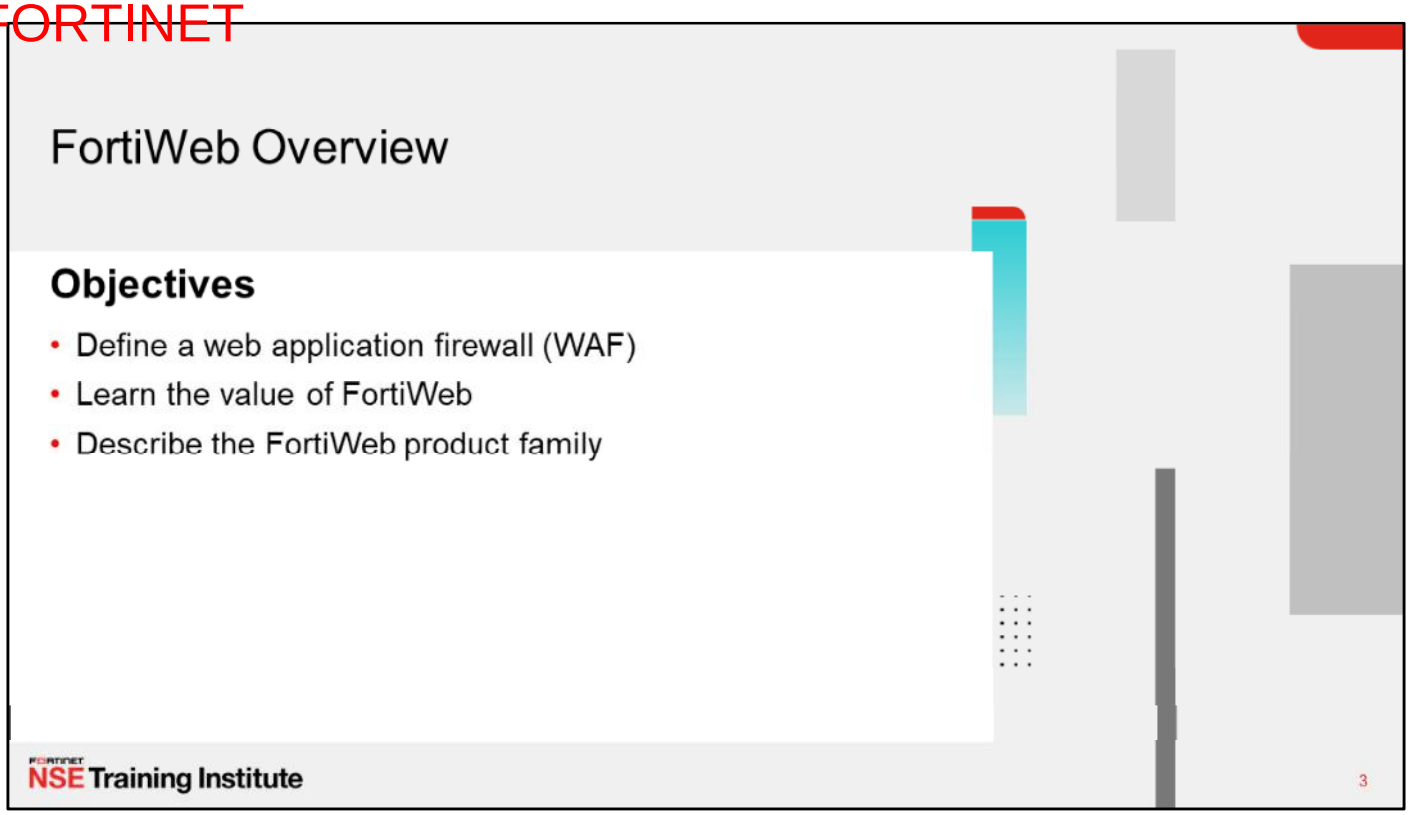
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

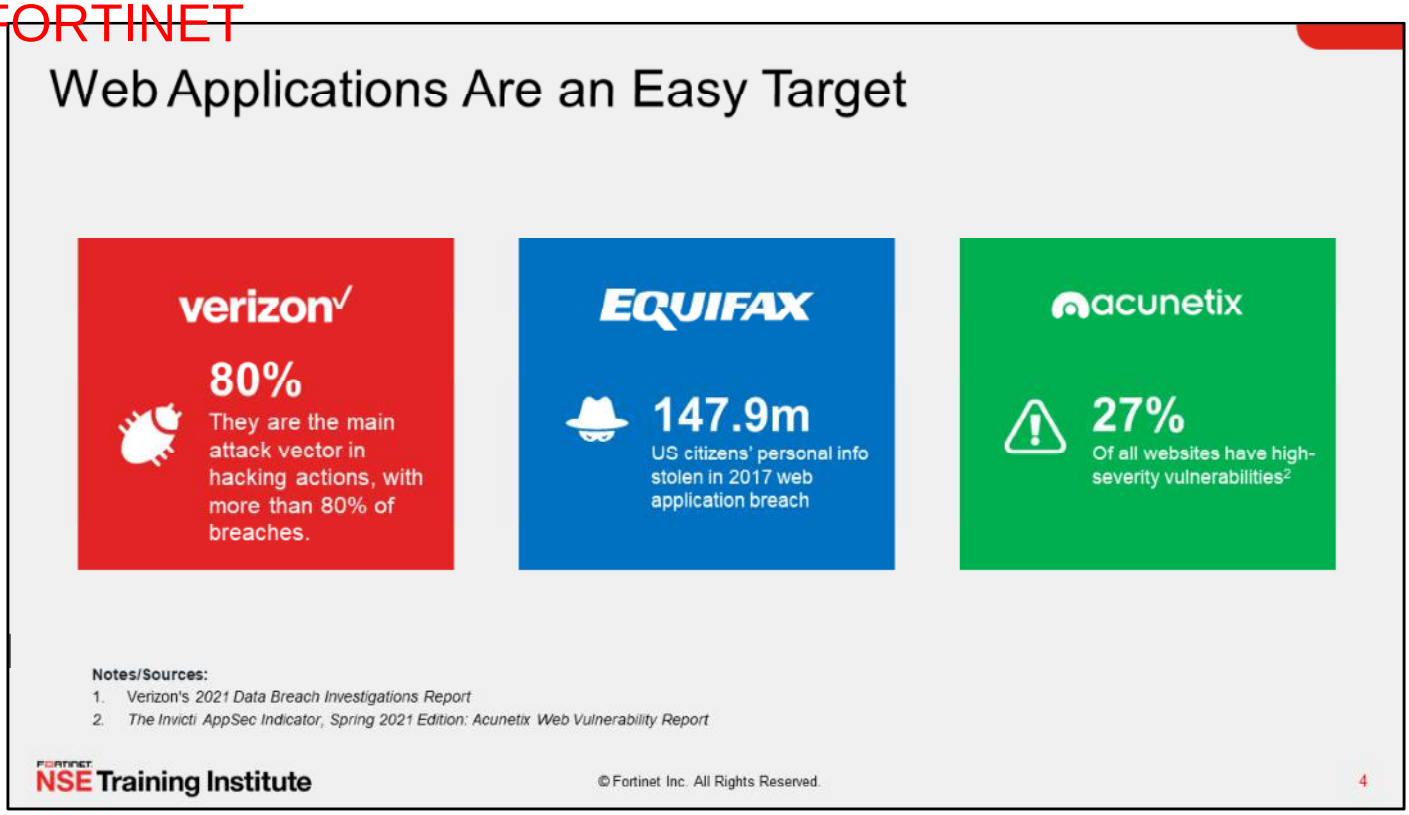


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the basics of FortiWeb, you will be able to effectively integrate FortiWeb into your network to protect web resources.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

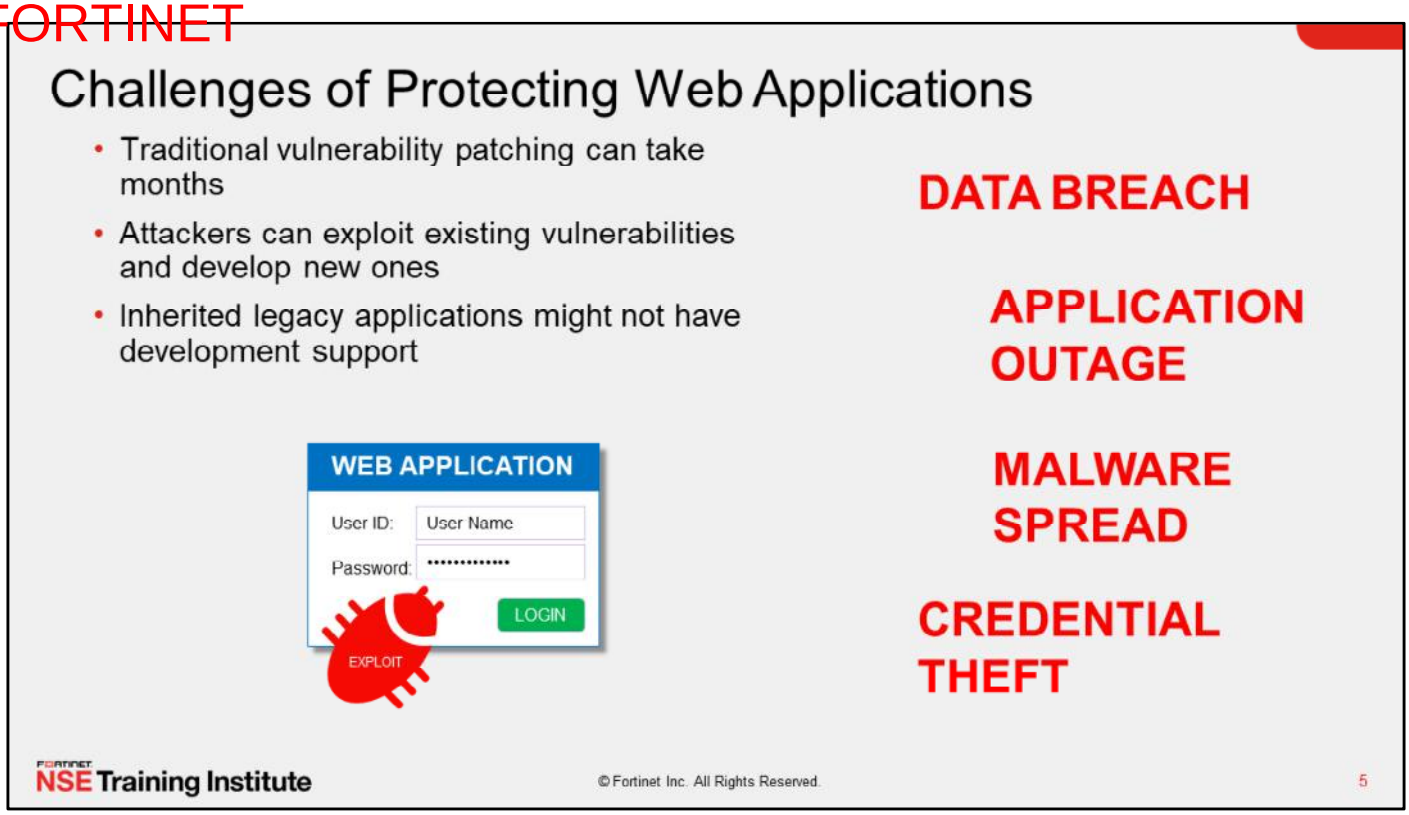


Web applications are attractive targets to hackers because they are often public-facing applications that must be open to the internet to provide major e-commerce and business tools for organizations. Connected to back-end databases, web applications are perfect for hackers because these databases are the primary repository for cardholder data, company data, and other sensitive information. Web application vulnerabilities such as SQL injection and cross-site scripting flaws in custom-built applications account for more than 80% of the vulnerabilities that are discovered.

According to Verizon, "Attacks on web apps were a part of 43% of breaches, more than double the results from last year. As workflows move to cloud services, it makes sense for attackers to follow. The most common methods of attacking web apps are using stolen or brute-forced credentials (over 80%) or exploiting vulnerabilities (less than 20%) in the web application to gain access to sensitive information."

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



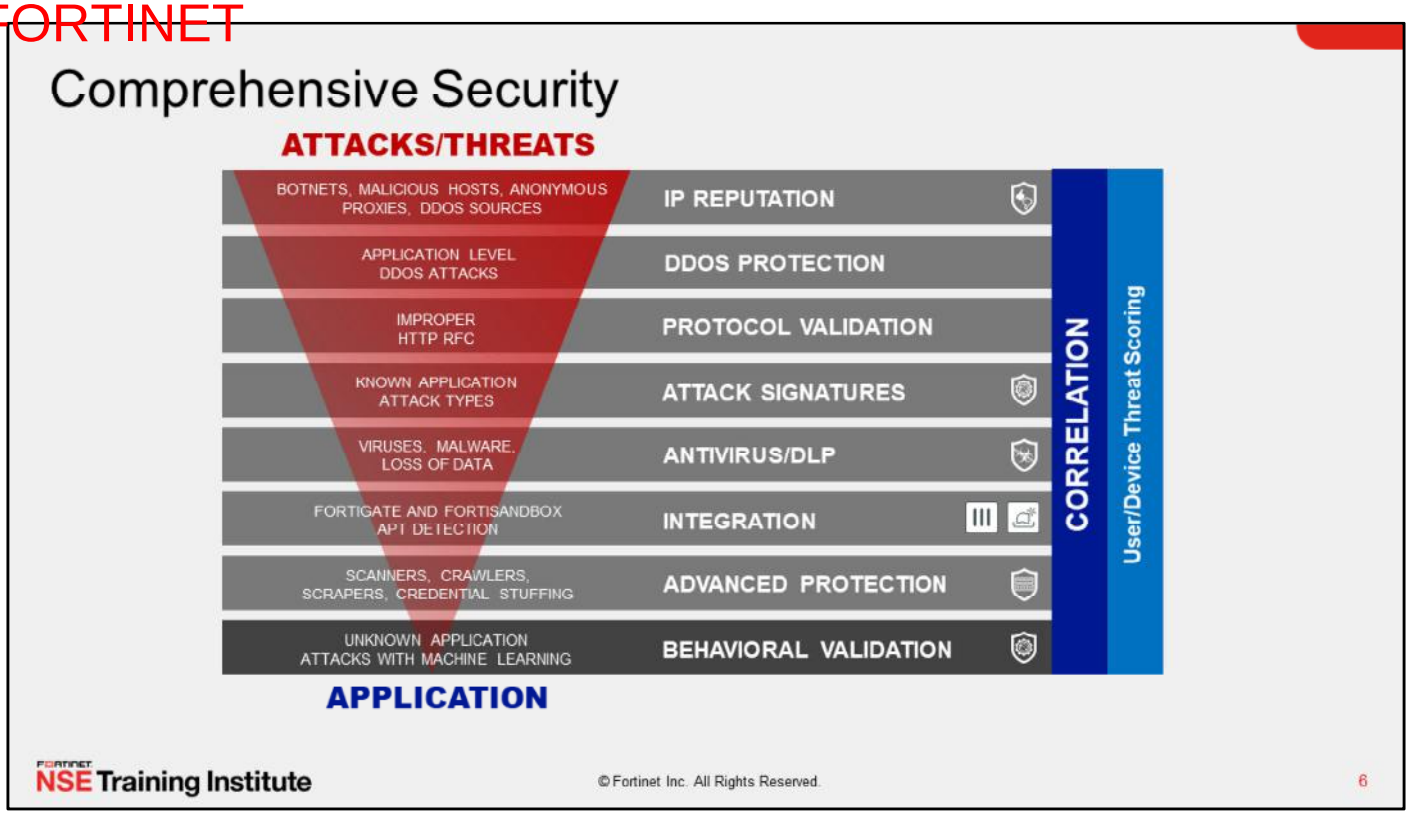
Traditional vulnerability patching can take months and relies on third-party vendors to supply updates. Attackers can exploit these vulnerabilities while you wait for a security patch. Inherited legacy applications might not have development support.

Identified threats need to be remediated quickly. Lengthy manual investigations allow threats more than enough time to do damage to your applications. It is also important to minimize the number of false positives, to prevent legitimate traffic from being blocked.

Failing to meet these challenges may cause data leaks, credential theft, application outages, and malware propagation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



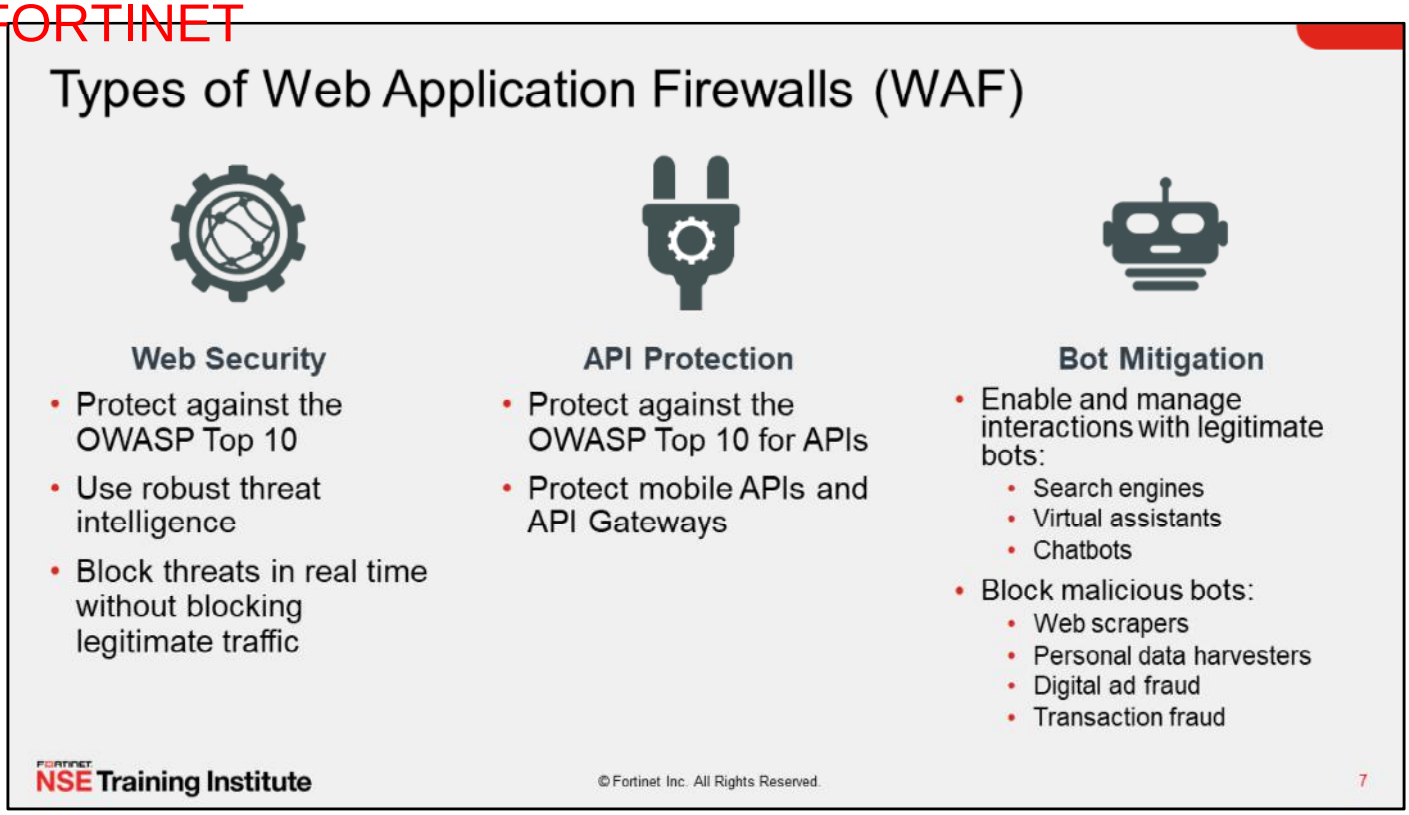
FortiWeb provides multiple layers of protection to safeguard web applications from external threats. As shown on this slide, various FortiWeb features leverage FortiGuard threat intelligence such as:

- IP reputation, which detects known botnets, malicious hosts, anonymous proxies, and much more
- Attack signatures that detect known application layer attacks
- Antivirus and data leak prevention (DLP) that protect against known malware and loss of data
- Advanced protection that detects scanners, crawlers, scrapers, and more

Using a multilayered and correlated approach, FortiWeb provides complete security from threats for web-based applications. At the core of FortiWeb threat protection is the machine learning-based detection engine that identifies requests that don't fit normal patterns and takes action to protect applications from known and unknown zero-day threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Web applications are one of the most vulnerable parts of your network. Attackers adapt and evolve quickly to circumvent defenses against the most vulnerable parts of your network.

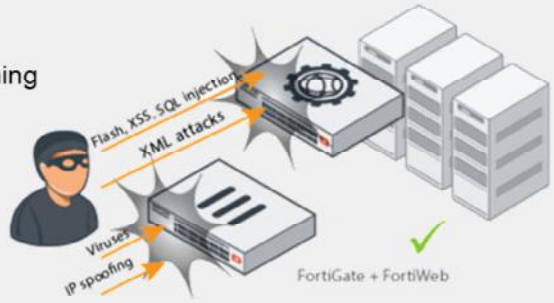
The CVE Program identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities. It is critically important to fix the vulnerabilities in your infrastructure that the CVE Program publishes. You can be sure attackers know about these vulnerabilities and will try to take advantage of affected websites and applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Why FortiWeb WAF?

- FortiGate can scan HTTP/HTTPS, so why FortiWeb?
- While FortiGate protects client endpoints, FortiWeb optimizes and protects web servers
- FortiWeb provides specialized application-layer threat detection and protection for HTTP or HTTPS
- The FortiWeb application-aware firewalling and load balancing engine can:
  - Secure HTTP applications that are often gateways into valuable databases
  - Prevent and reverse defacement of websites
  - Improve application stability
  - Monitor servers for downtime and connection load
  - Prevent unknown and zero-day attacks using machine learning



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

What is a web application firewall (WAF), and why does your security infrastructure need one?

The FortiGate HTTP proxy and FortiClient protect endpoint clients, not servers. For example, FortiGuard web filtering URL ratings block requests based on the category of the server web pages. Antivirus protection prevents clients from accidentally downloading spyware and worms. Neither feature protects servers from threats such as malicious scripts or ransomware.

Protecting servers requires a different approach than protecting clients because servers are subject to different types of attacks. Protecting web servers that handle popular websites, and enterprise web applications like IBM Lotus Notes or Microsoft SharePoint, also require high performance. Most web applications are supported by a database, which also requires protection.

FortiWeb uses multi-layered and correlated detection methods to defend applications from known vulnerabilities and zero-day threats. FortiWeb also offers a machine-learning function that enables it to automatically detect malicious web traffic. In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate and FortiWeb

- Working together with FortiGate, FortiWeb can:
  - Maximize website performance and maintain security
  - Reduce response times
  - Accelerate SSL/TLS with dedicated ASIC chips or through software
  - Accelerate websites through compression
  - Perform real-time content rewriting
  - Customizable redirection rules to tailor incoming web traffic

NSE Training Institute

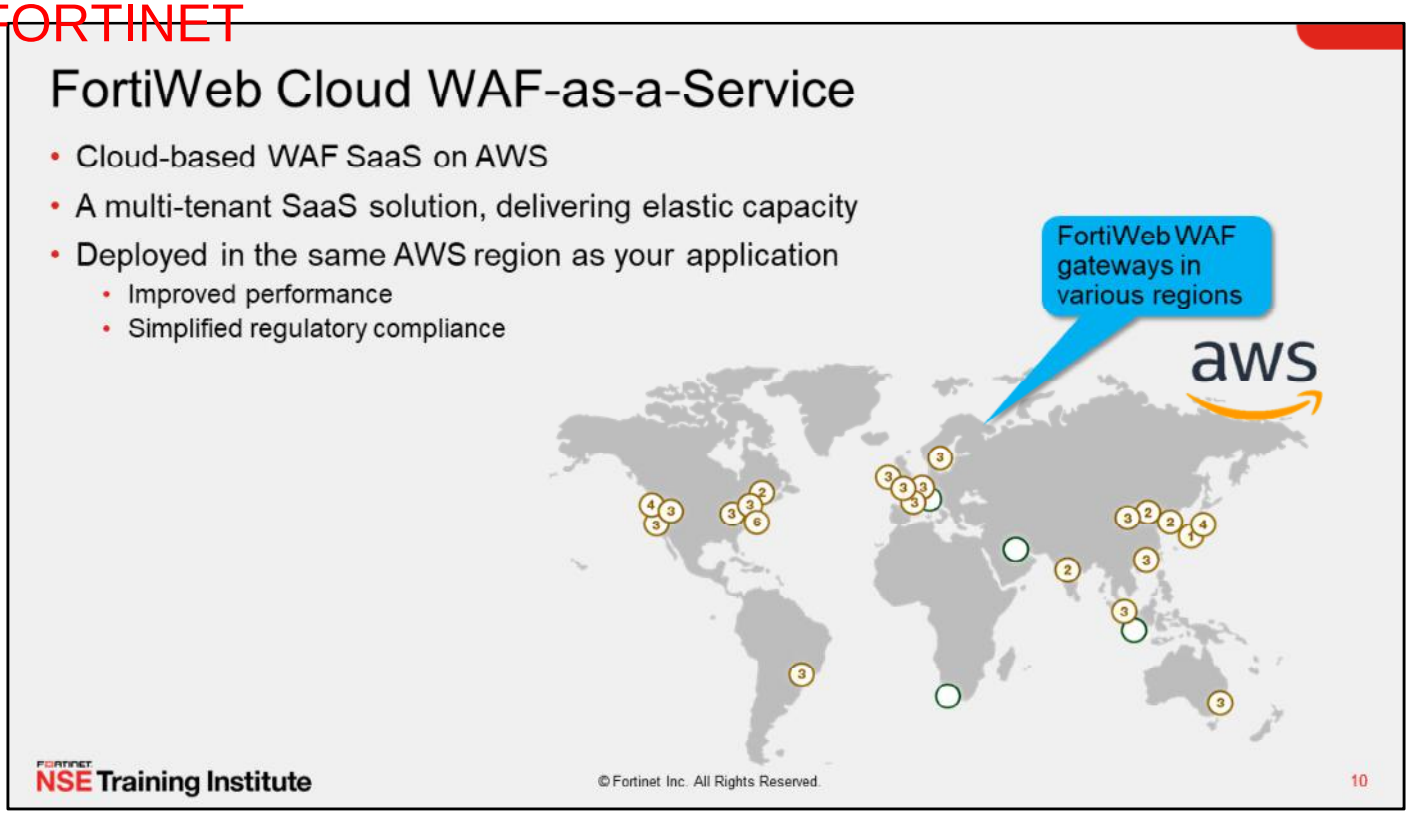
© Fortinet Inc. All Rights Reserved.

9

Because FortiWeb is a separate device or virtual machine, some functions of web content delivery can be offloaded. FortiWeb can perform SSL/TLS decryption to help reduce response times, protect the server because traffic can now be inspected, and reduce web server load because the web server no longer must perform the CPU-intensive cryptography.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb Cloud WAF-as-a-Service is a new SaaS cloud-based web application firewall that protects public cloud-hosted web applications. Currently supported on Amazon AWS it will be supported on other public cloud infrastructures in the future.

FortiWeb has a colony of WAF gateways in almost every AWS region. When you onboard an application to FortiWeb Cloud, you can choose which region the application resides in. FortiWeb Cloud then knows which WAF colony to use to protect your application. By deploying in the same region, FortiWeb Cloud offers a simplified regulatory environment where using the solution keeps the data in the same region with the same regulatory environment.

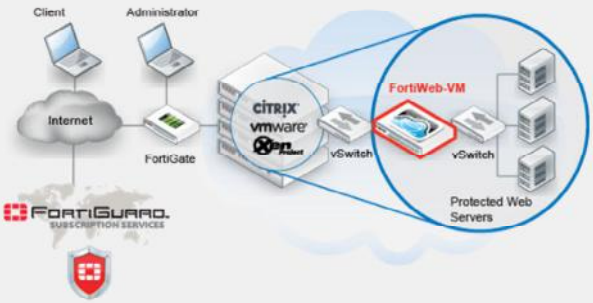
FortiWeb Cloud WAF is available on the AWS marketplace. For FortiGuard services, you will still have to contact Fortinet Customer Support.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb in the Cloud

- Deploy FortiWeb in a virtualized environment
- VMware, Hyper-V, Citrix Xen Server, Open Source Xen, or Amazon AWS
- Protects web applications, regardless of connection origin
- Visibility to internal connections
- Same functionality as physical device



	System Requirements
Licenses	1 vCPU, 2 vCPU, 4 vCPU, 8 vCPU
Hypervisor	VMware ESX/ESXi, Hyper-V, Citrix Xen, Open Source Xen, AWS
Memory	4GB (Recommended)
CPU	1+ virtual CPU
10/100/1000 Interfaces	2-4 virtual NICs
Storage Capacity	40+ GB

amazon web services
Microsoft Hyper-V
CITRIX XenServer
vmware

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

FortiWeb can be deployed in multiple types of virtualization solutions. Virtualized FortiWeb devices have almost identical functionality to a physical device except for the dedicated ASIC chips for accelerating features like SSL offloading.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Availability

Appliances	Virtual Machines	Public Cloud	SaaS	Container
7 models 50 Mbps to 20 Gbps 4 SFP GE	4 models 25 Mbps to 3 Gbps Perpetual licenses Supports: • VMware • Hyper-V • Xen • Citrix Xenserver • KVM • VirtualBox	4 models BYOL and on-demand licenses Supports: • Amazon • Azure • Google Cloud • Oracle Cloud	Subscription-based Hosted by Fortinet	4 virtual appliances 24 Mbps to 3 Gbps Docker support Amazon Elastic Container Service

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

The FortiWeb product family comprises multiple models, designed to suit specific needs. The FortiWeb models range from those suited to SMB applications to models suited to an enterprise data center. FortiWeb product family includes both dedicated hardware and VM appliances.

FortiWeb provides maximum flexibility in supporting virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as the hardware-based devices and can be deployed in multiple private and public cloud infrastructures.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which systems does FortiWeb protect?
   - ✓ A. HTTP and HTTPS-based servers
   - B. SIP-based telephony servers

2. Which characteristic best describes a web application firewall?
   - ✓ A. Provides specialized application-layer threat detection
   - B. Protects clients and servers

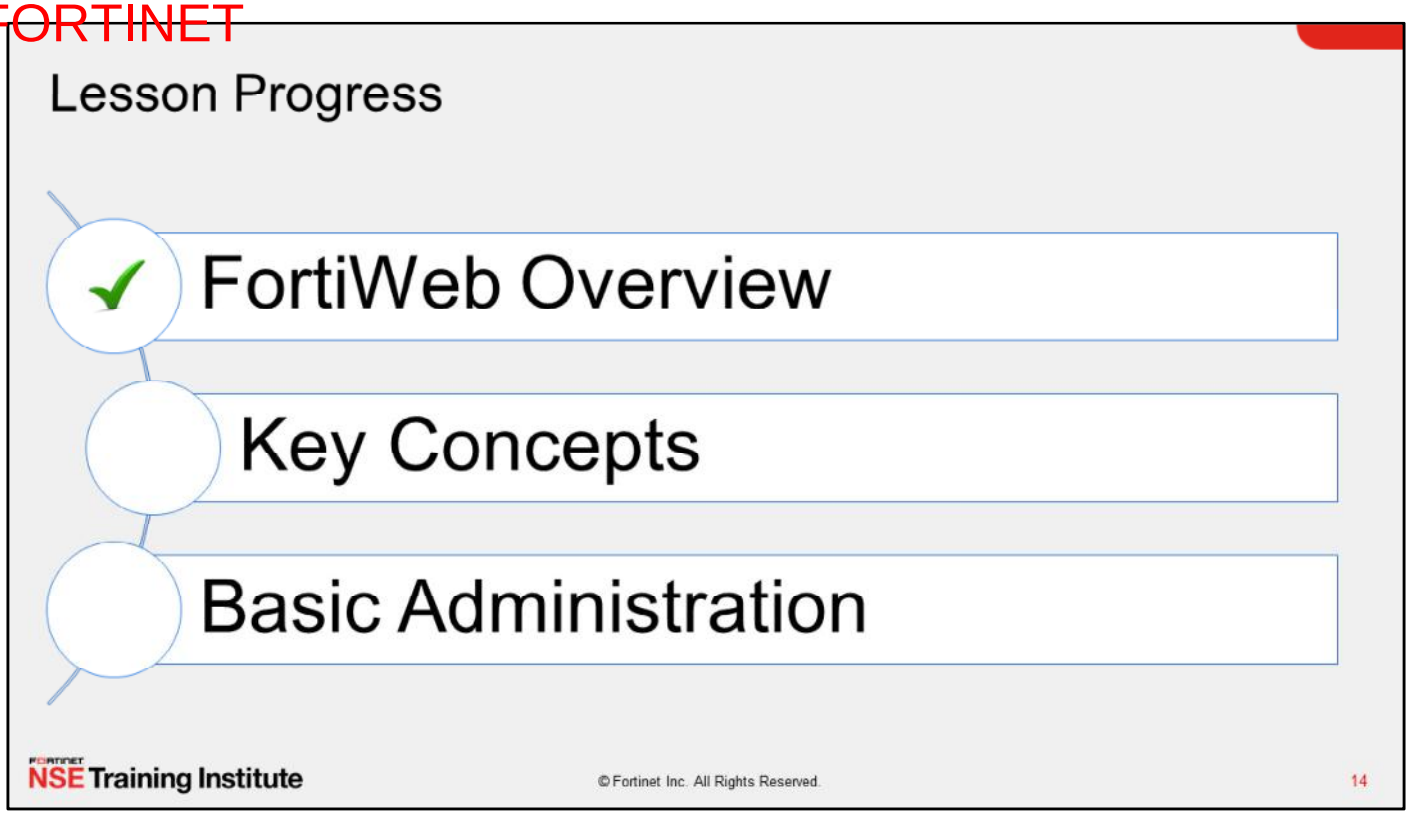
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



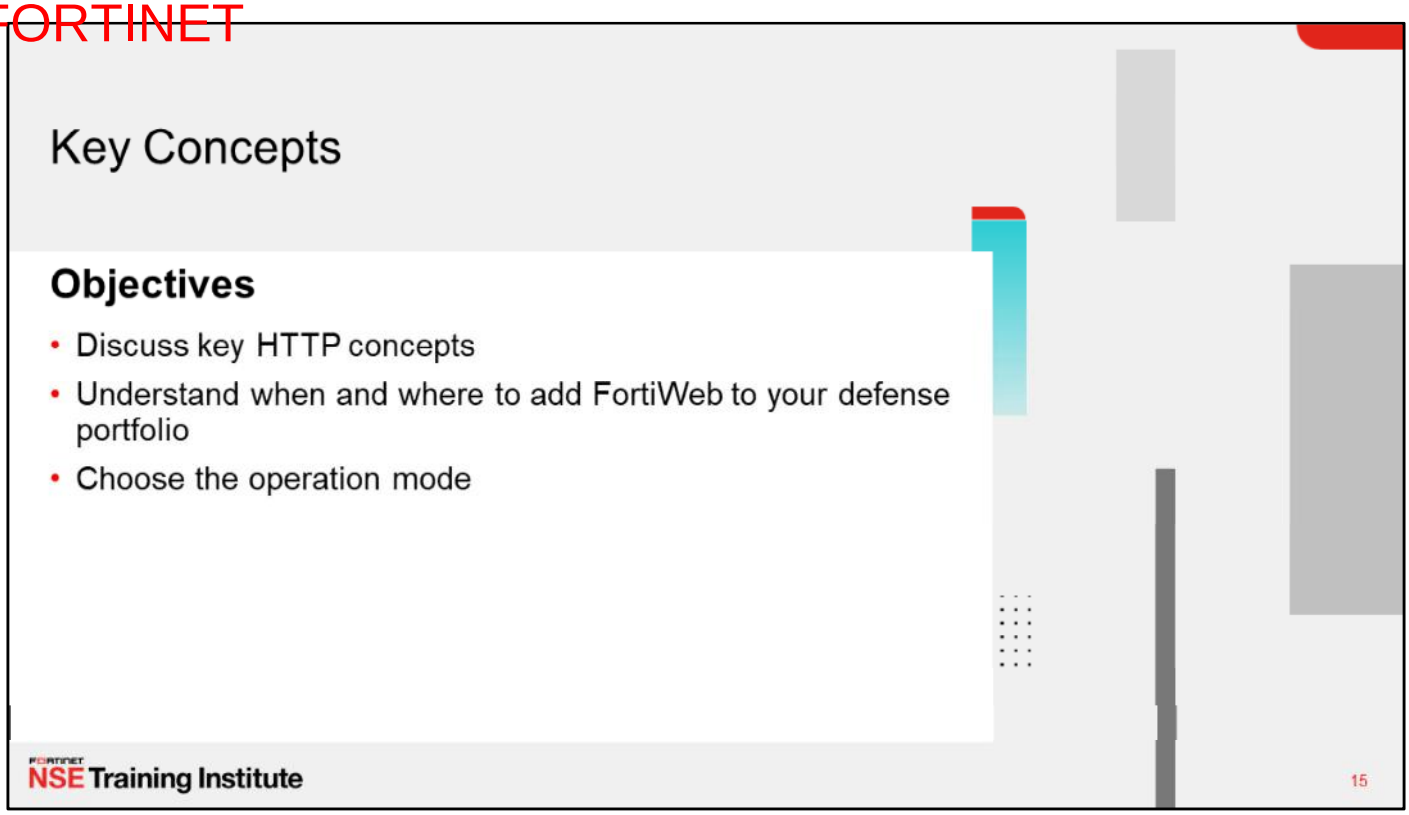
Good job! You now understand the key features of FortiWeb.

Now, you will learn about the ways that you can deploy FortiWeb to protect against these threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in key concepts, you will be able to make more informed decisions on how best to implement FortiWeb in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Web Server Attacks

- There are a large number of types of web server attacks
- Comprehensive list is in the FortiWeb documentation:
  - https://help.fortinet.com/fweb/571/Content/FortiWeb/fortiweb-admin/solutions_for_specific.htm

Key concepts > Solutions for specific web attacks

Solutions for specific web attacks

The types of attacks that web servers are vulnerable to are varied, and evolve as attackers try new strategies.

FortiWeb appliances offer numerous configurable features for preventing web-related attacks, including denial-of-service (DoS) assaults, brute-force logins, data theft, and more.

Early in your deployment of FortiWeb, configure and run web vulnerability scans to detect the most common attack vulnerabilities. You can use this to discover attacks that you may be vulnerable to. For more information, see Vulnerability scans.

HTTP/HTTPS threats

Servers are increasingly being targeted by exploits at the application layer or higher. These attacks use HTTP/HTTPS and aim to compromise the target web server, either to steal information, deface it, or to post malicious files on a trusted site to further exploit visitors to the site, using the web server to create botnets.

Among its many threat management features, FortiWeb's fends off attacks that use cross-site scripting, state-based, and various injection attacks. This helps you comply with protection standards for:

- credit-card data, such as PCI DSS 6.6
- personally identifiable information, such as HIPAA

Web-related threats lists several HTTP-related threats and describes how FortiWeb appliances protect servers from them. FortiWeb can also protect against threats at higher layers (HTML, Flash or XML applications).

Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
Adobe Flash binary (AMF) protocol attacks	Attackers attempt XSS, SQL injection or other common exploits through an Adobe Flash client.	Decode and scan Flash action message format (AMF) binary data for matches with attack signatures.	Enable AMF3 Protocol Detection
Botnet	Utilizes zombies previously exploited or infected (or willingly participating), distributed usually globally, to simultaneously overwhelm the target when directed by the command and control server(s).	Decode and scan Flash action message format (AMF) binary data for matches with attack signatures.	IP Reputation

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

FortiWeb solutions vary by the type of attack that they are meant to combat. Many of the FortiWeb solutions combat the (OWASP) top 10 attacks.

A large list of types of web attacks can be found in the *FortiWeb Administration Guide*. These will cover the attack techniques, a brief description, and steps that can be taken to prevent the attack from happening, including specific FortiWeb configuration options.

It is highly recommended that you review this list because it prioritizes attacks that your web applications may be vulnerable to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Do Attacks Have in Common?

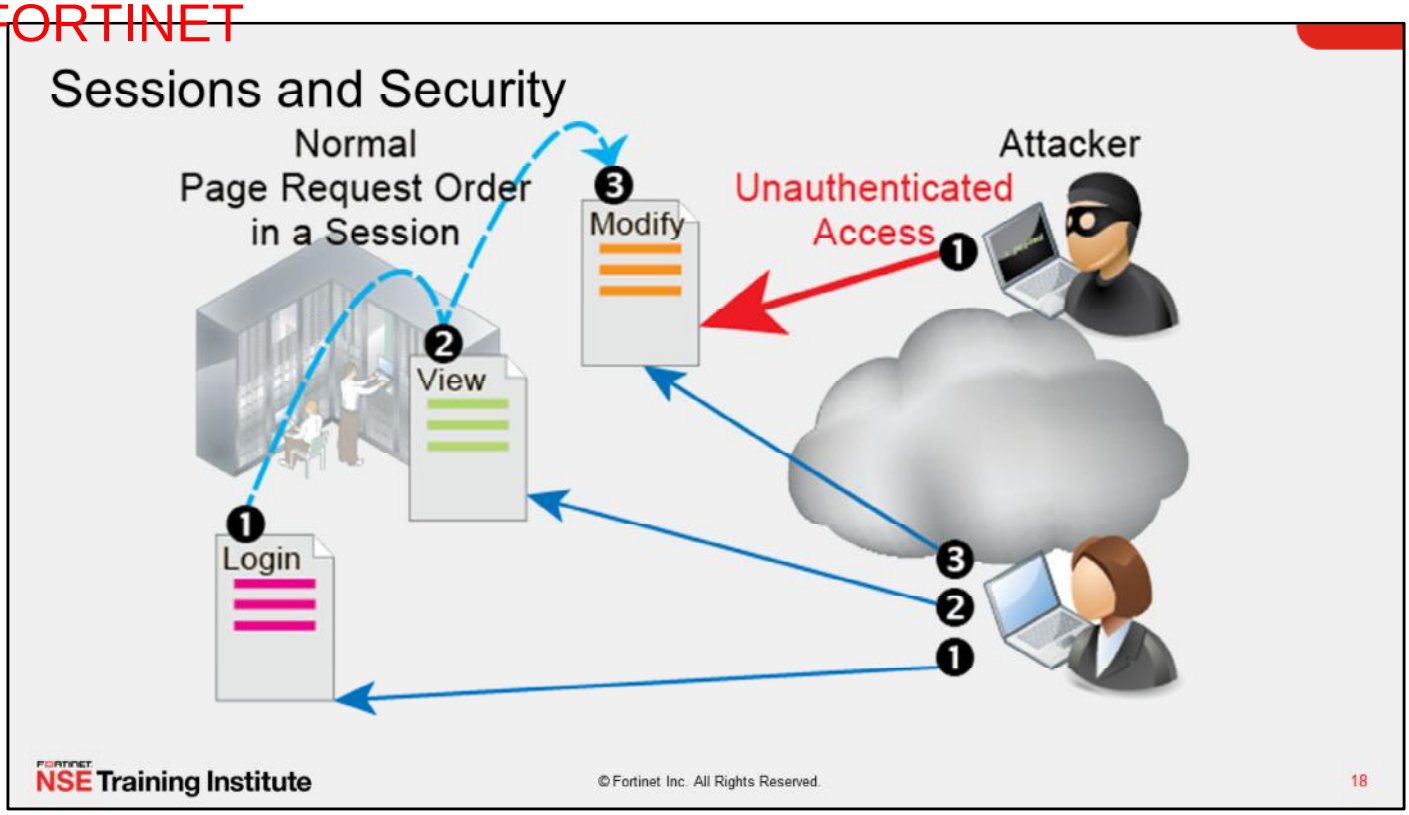
- Aim for the weakest link
  - Weak passwords
  - Unencrypted passwords
- Exhaust finite connection and session capacity
- Exploit incorrect assumptions about input
  - Overflow buffers
  - Input invalid data type
    - Example: parser wants numbers, but attacker sends SQL query
- Test limits of poor design and server defaults
  - Unlimited and long timeouts
  - Unlimited inputs and length
- Create an illogical flow between app URLs if app doesn't enforce prerequisites

NSE Training Institute © Fortinet Inc. All Rights Reserved. 17

The previous slides covered some of the more common types of attacks, but there are many more. Attacks can use many strategies in HTTP, and they don't always appear in the usual web server logs. How can you tell when your infrastructure is under attack? How can you block an attack?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Although HTTP 1.1 is *stateless*, meaning that it does not automatically support persistent sessions, many web applications require *stateful* sessions.

Sessions occur when a set of hits (correlated requests for individual web pages or data) forms the impression of an overall client visit for a particular time span. Sessions typically consist of a session ID and data indicating the current state of the connection. Some memory of these requests is retained between visits. Examples of a session include logins, shopping carts, and lists of previously viewed items.
Web applications also use next page requests, or transitions from one state to another state, to ensure that a client's requested operations make sense.

Attackers can take advantage of unprotected sessions. Next page requests must be restricted to valid ones, or the client's next page request in the session could break the web application logic.
If session IDs and cookies aren't guarded, and valid state transitions aren't enforced, attackers have multiple avenues to gain access to sensitive information:

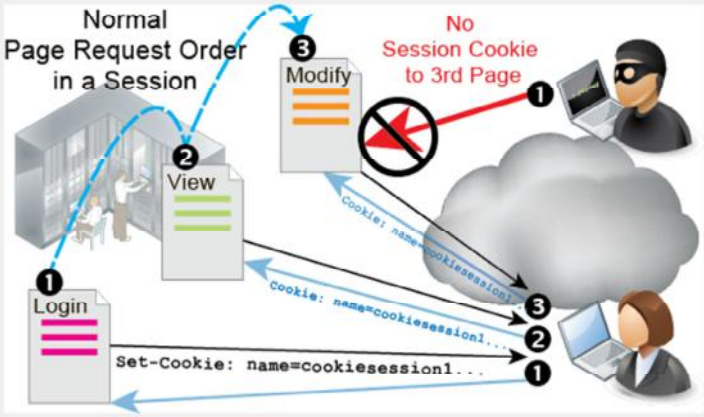
- Sessions can be stolen and used in the side jacking attacks made famous by Firesheep.
- Session tracking cookies can be poisoned and grant access to someone other than the intended user.
- Web applications can become vulnerable to state transition-based attacks, where pages are requested out of the expected order, by a different client.
- Inputs can be used out of order to glean information from the web application.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Web Access Flow

- Page flow and access must make sense
  - Logic
    - Example: HTTP session cookie presented from the USA but the initial client connected from Germany (session hijack)
  - Business requirements
    - Example: Ordering laptops without submitting a valid payment
  - Illogical flows can break the normal data flow of the application engine
- Protocol design must gracefully handle finite resources



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

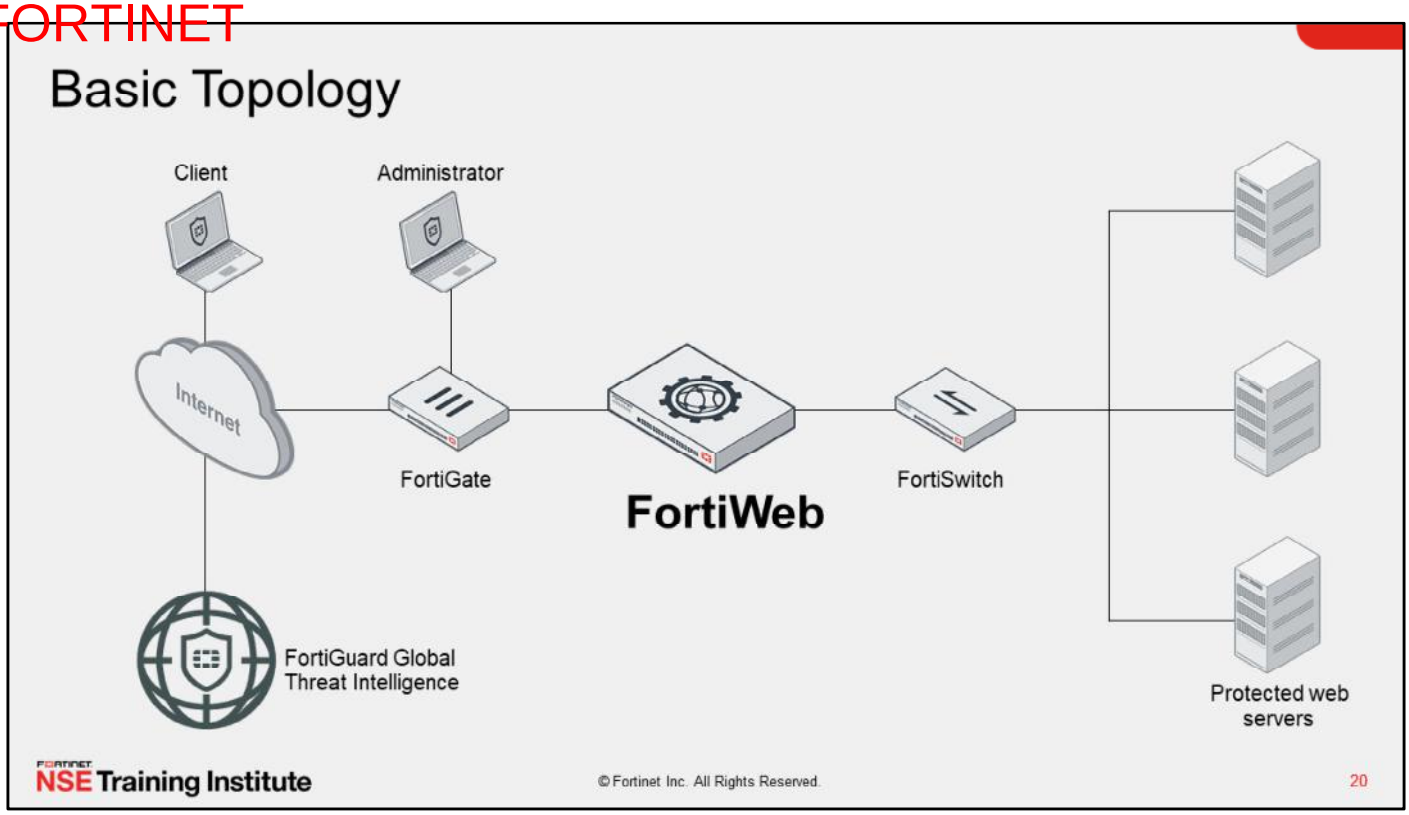
Principles of design that will help prevent most HTTP attacks are as follows:

- The order of page requests in a web application session must make sense. The page has prerequisites that should be enforced, but HTTP has no built-in session logic mechanism.
- Protocol and application design must flow gracefully and successfully contain itself within finite resources and access (principle of least privilege).

Don't assume that increasing the web server maximum number of allowed simultaneous connections, or enabling threading, will solve the problem of access and performance. The Slowloris DDoS attack, for example, can have more severe effects on servers where threading is enabled. Ideally, only expected and validated sessions should be allowed to reach the web server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb can be deployed in a one-arm topology or positioned inline to intercept all incoming client connections and redistribute them to your servers. FortiWeb has TCP-specific and HTTP-specific firewalling capabilities. Because FortiWeb provides security only to HTTP/HTTPS applications, you should deploy it behind a firewall such as FortiGate, that focuses on security for other protocols that may be forwarded to your backend servers, such as FTP and SSH.

After you deploy FortiWeb, you can configure it from a web browser on your management computer, using its web GUI and CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Blocking Methods

- Varies by operation mode
  - Reverse proxy
  - Offline protection
  - True transparent proxy
  - Transparent inspection
  - Web Cache Coordination Protocol (WCCP)
- Reverse proxy and true transparent proxy
  - Establishes a separate connection with both the client and the server
  - Has full control over the data
  - Closes the connection when suspicious activity is detected
- Offline and transparent inspection mode
  - Function physically out-of-band, or forward packets before scanning
  - Sends a packet reset (RST) to interrupt the connection
  - Work well in most cases, but may be too late to block some attacks
  - Use TCP resets, but these are not 100% reliable because of:
    - Race condition—interruption of the attack depends on the CPU load and the speed of the inline route
    - Inability to sanitize or rewrite because the packets have already egressed to the server

NSE Training Institute © Fortinet Inc. All Rights Reserved. 21

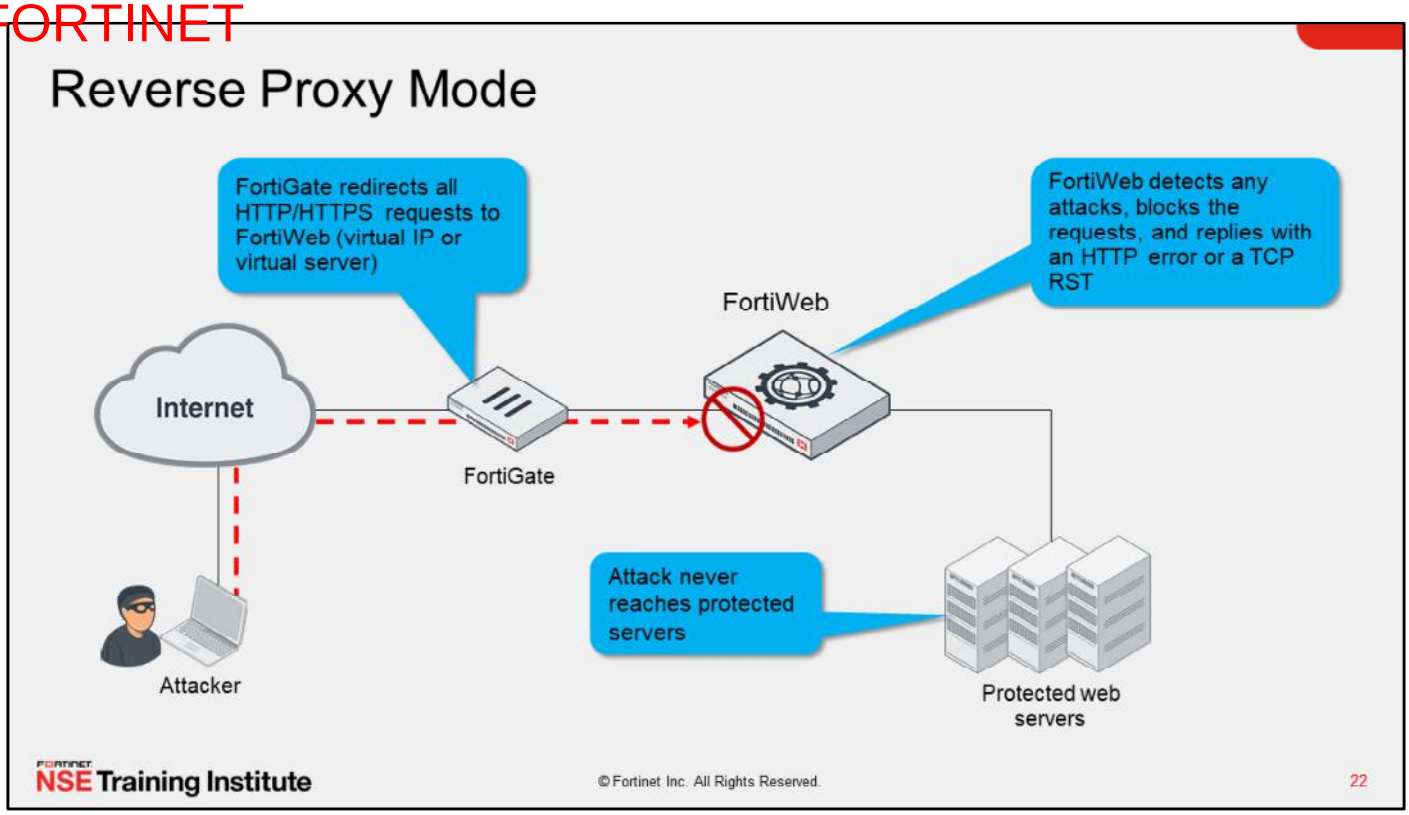
Consider your choice of operation mode carefully, because it can be time-consuming to reconfigure your network if you switch modes later. If you are not sure which operation mode is best for your network, you can temporarily deploy FortiWeb in the offline protection mode. Using offline protection, you can learn about the vulnerabilities of your web servers and then switch FortiWeb to an inline operation mode.

All operation modes support many of the same features, but some features are specific to certain operation modes. For example, rewriting content and URLs requires an inline topology. If you are streaming media, where high performance and zero latency is more critical than absolute security, you can choose offline or transparent inspection mode.

For the broadest feature support, choose reverse proxy mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

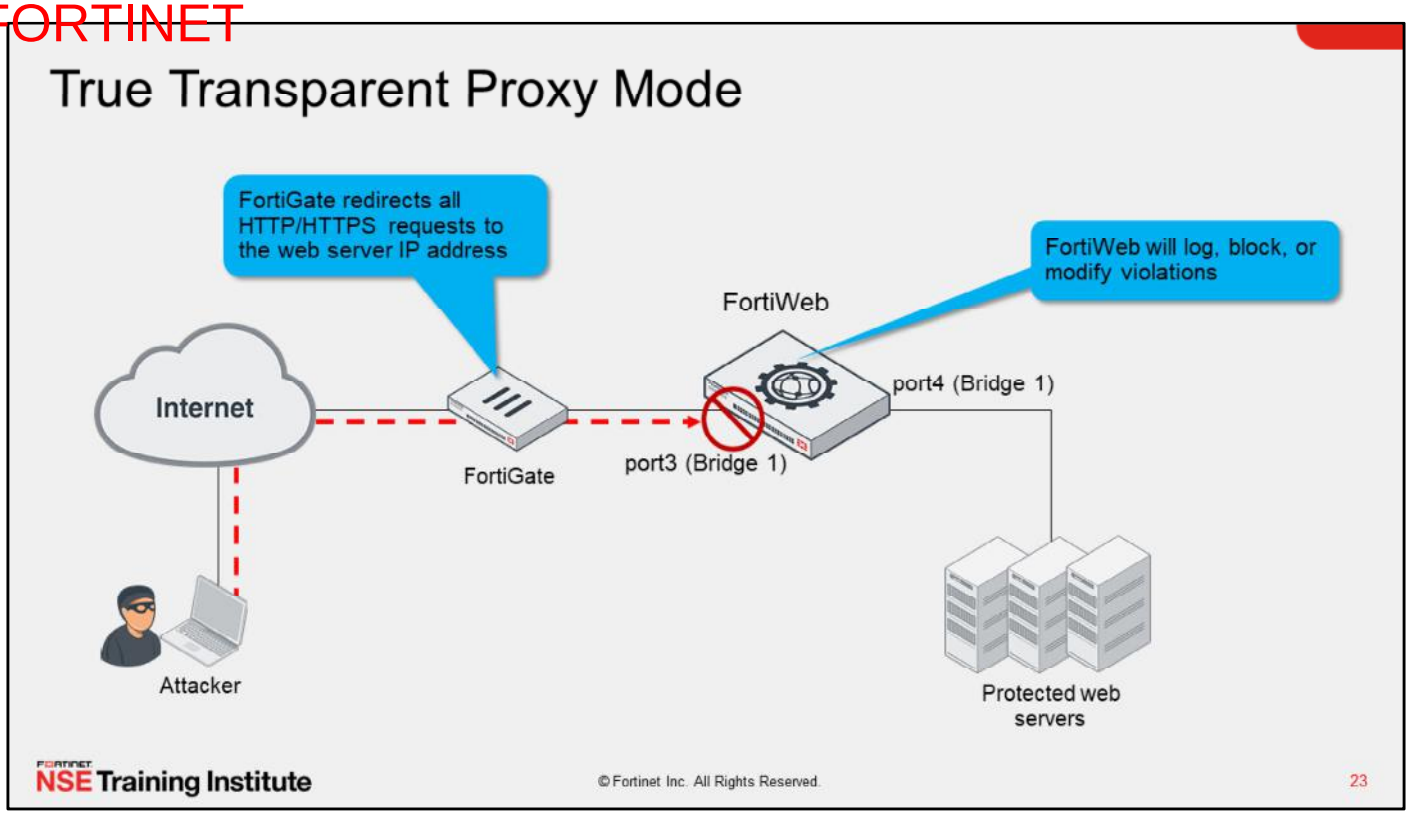
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now you will learn about how attacks are blocked when FortiWeb is operating in reverse proxy mode. Because FortiWeb is acting as a proxy for your servers, it is a termination point at the IP layer. When FortiWeb detects an attack, it doesn't forward the traffic to your protected servers, so a connection is never made. Depending on the OSI layer of the client attack, FortiWeb replies with either a TCP reset or an HTTP error code, whichever is appropriate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

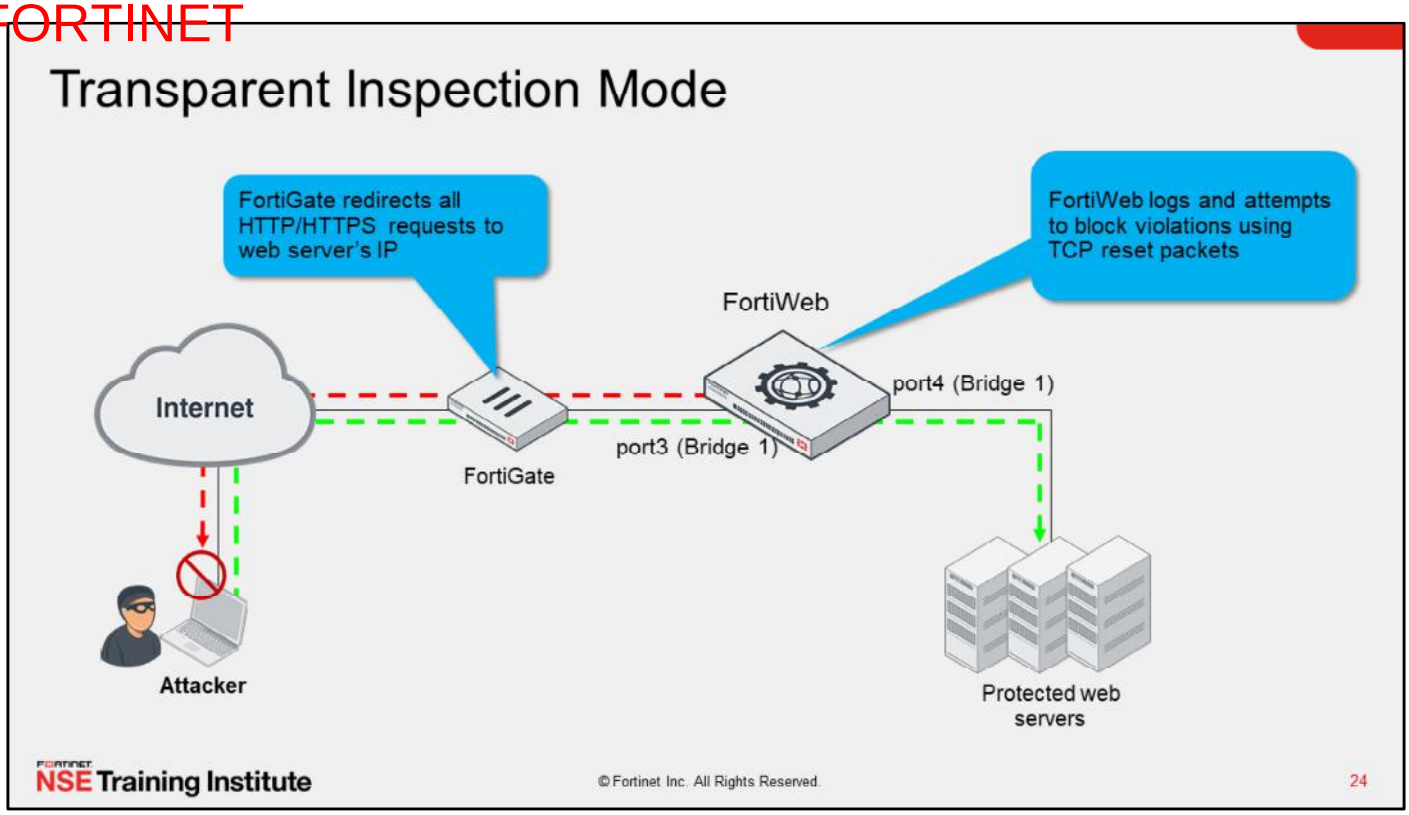


Take a look at how FortiWeb operates in true transparent proxy and transparent inspection modes. Both modes are useful if you want to transparently inspect traffic and retain the IP address scheme of your network. Requests are sent to the IP address of the web server, not to the IP address of FortiWeb. Both modes have the same topology but have some important differences because of how they intercept traffic.

In true transparent proxy mode, FortiWeb transparently proxies the traffic arriving on a network port that is in the v-zone (a Layer 2 bridge). Depending on the traffic, FortiWeb logs, blocks, or modifies violations according to the matching policy and protection profile before passing the traffic on to the destination server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



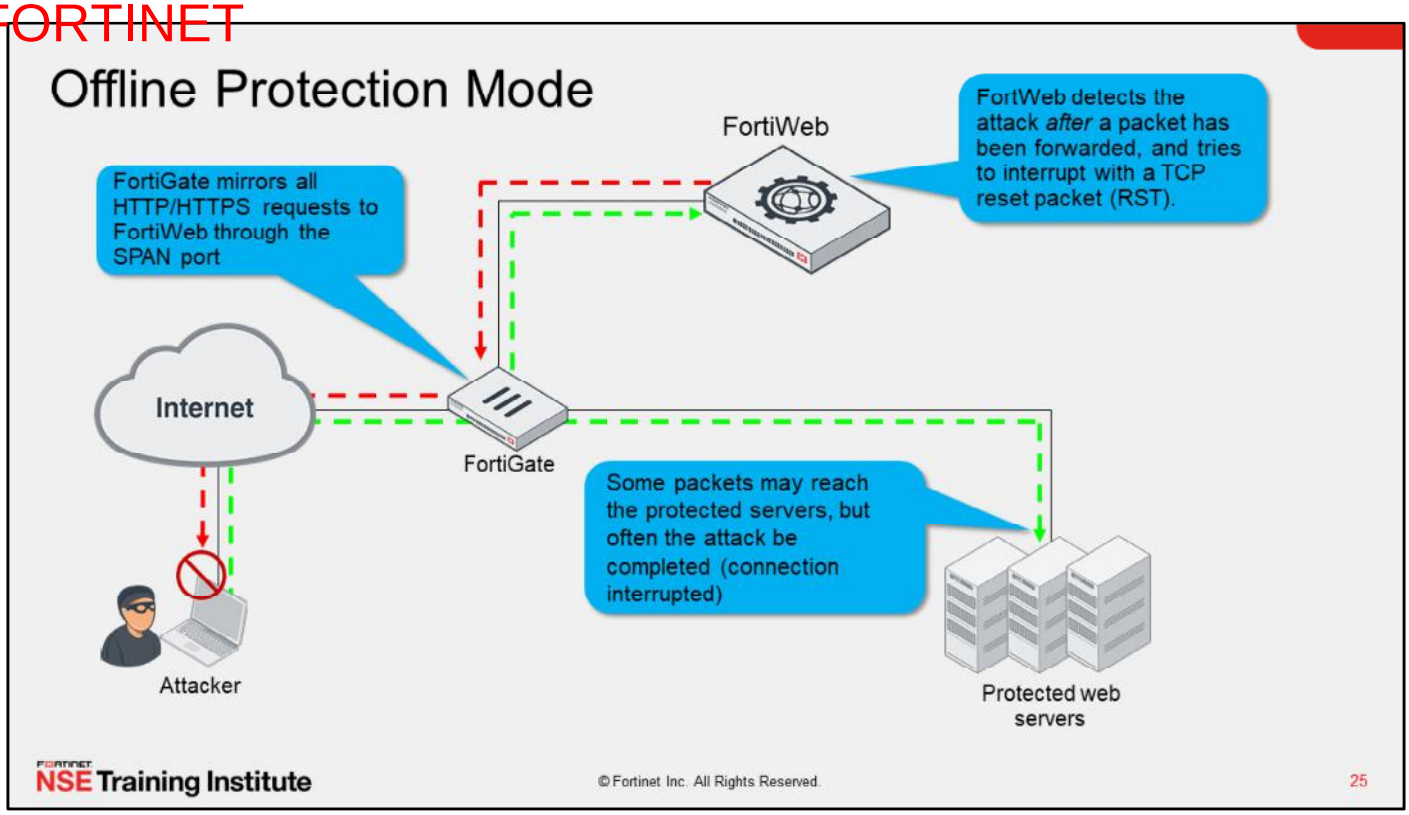
In transparent inspection mode, FortiWeb asynchronously inspects traffic arriving on a network port that is in the v-zone (Layer 2 bridge). Depending on the traffic, FortiWeb logs or blocks violations according to the matching policy and protection profile, but does not otherwise modify it. In this mode, FortiWeb attempts to block traffic that violates the policy.

Because of the nature of asynchronous inspection, the client or server may have already received the traffic that violates the FortiWeb policy. FortiWeb then reactively attempts to block connections when it detects an attack. If the TCP reset packet is not successful in stopping the attack, remediation may be required.

In contrast, when FortiWeb is operating in reverse proxy or true transparent proxy mode, blocking is more reliable because suspicious information is blocked immediately and not passed to the web server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Out-of-band is an appropriate descriptor for the offline protection mode deployment. Deploying this mode requires minimal changes and it does not introduce any latency. However, many FortiWeb features are not supported.

Requests are destined for a web server, not the FortiWeb device. Traffic is duplicated from the flow and sent on an out-of-line link to FortiWeb through a switched port analyzer (SPAN or mirroring) port. Unless there is a policy violation, FortiWeb does not send reply traffic. If upstream firewalls or routers apply source NAT (SNAT), the web servers can use the source IP addresses of clients.

FortiWeb monitors traffic received on the data capture port network interface (regardless of the IP address), and applies the first applicable policy. Because FortiWeb is not inline with the destination, it does not forward permitted traffic. FortiWeb logs or blocks violations according to the matching policy and its protection profile. If FortiWeb detects a malicious request, it sends a TCP reset (RST) packet through the blocking port to the web server and client to attempt to terminate the connection. It does not otherwise modify traffic. FortiWeb cannot, for example, offload SSL, load balance connections, or support user authentication. FortiWeb provides detection, but does not load balance, block, or otherwise modify traffic to or from the two web servers.

Most organizations do *not* permanently deploy their FortiWeb in offline protection mode. Instead, they use offline protection mode as a way to learn about the vulnerabilities of their web servers and to configure some of the FortiWeb features. After this transition period, they switch to an operation mode that places the appliance inline (between clients and web servers). Switching out of offline protection mode when the transition is complete can prevent bypass problems that can arise as a result of misconfigured routing. It also gives you the ability to offer protection features that cannot be supported in an out-of-band mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Policy Behavior by Operation Mode

	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection	WCCP
Matches by	• Server port • Virtual server	• Data capture port • Server pool	• V-zone (bridge) • Server pool	• V-zone (bridge) • Server pool	• Server port • Virtual server
Violations	• Block • Modify	• Attempt to block by sending TCP reset	• Block • Modify	• Attempt to block by sending TCP reset	• Block • Modify
SSL	• Offloading • Optional re-encryption	• Inspection only	• Inspection only	• Inspection only	• Inspection only
Forwarding	• Forwarding to a single server • Load balancing to server pool	• Pass-through to server pool member	• Pass-through to server pool member	• Pass-through to server pool member	• Forwarding to a single server • Load balancing to server pool
Machine Learning	• Supported		• Supported		• Supported

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

The blocking method and attack protection used varies by operation mode, but so does traffic forwarding and SSL offloading or inspection. The table shown on this slide provides a summary only. If you need a specific feature, check the documentation to determine if the feature is supported.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Choosing Your Operation Mode

- Not all operation modes can stop all attacks!
- Features (ADC, authentication, rewriting) also vary by operation mode
  - Check docs.fortinet.com for feature support by operation mode
- Reverse proxy mode is the default and most popular operation mode
- Offline protection mode is best for a trial period and proof of concepts

System > Status > Status

System Information

HA Status:	Standalone [Configure]
Host Name:	FortiWeb-VM [Change]
Serial Number:	FVVM020000011103
Operation Mode:	Reverse Proxy [Change]
System Time:	Thu Oct 4 12:18:34 2018 [Change]
Firmware Version:	FortiWeb-KVM 6.01,build0036,180822 [Update]
System Uptime:	[1 day(s) 1 hour(s) 4 min(s)]
Administrative Domain:	Disabled [Enable]
FIPS-CC Mode:	Disabled
Log Disk:	Available

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Because blocking is not guaranteed to succeed in offline mode, this mode is best used during the evaluation and planning phase, early in implementation.

Reverse proxy is the most popular operation mode. It can rewrite URLs, offload TLS, load balance, and apply NAT.

For very large managed security services providers (MSSPs), true transparent mode has a significant advantage. You can drop it in without changing any schemes of limited IPv4 space–in transparent mode, you don't need to send IP addresses to the network interfaces on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which operation mode provides the most flexibility and highest degree of protection?
   A. True transparent proxy
   ✓ B. Reverse proxy
   C. Transparent inspection

2. In which operation mode can FortiWeb modify HTTP packets?
   ✓ A. True transparent proxy
   B. Transparent inspection

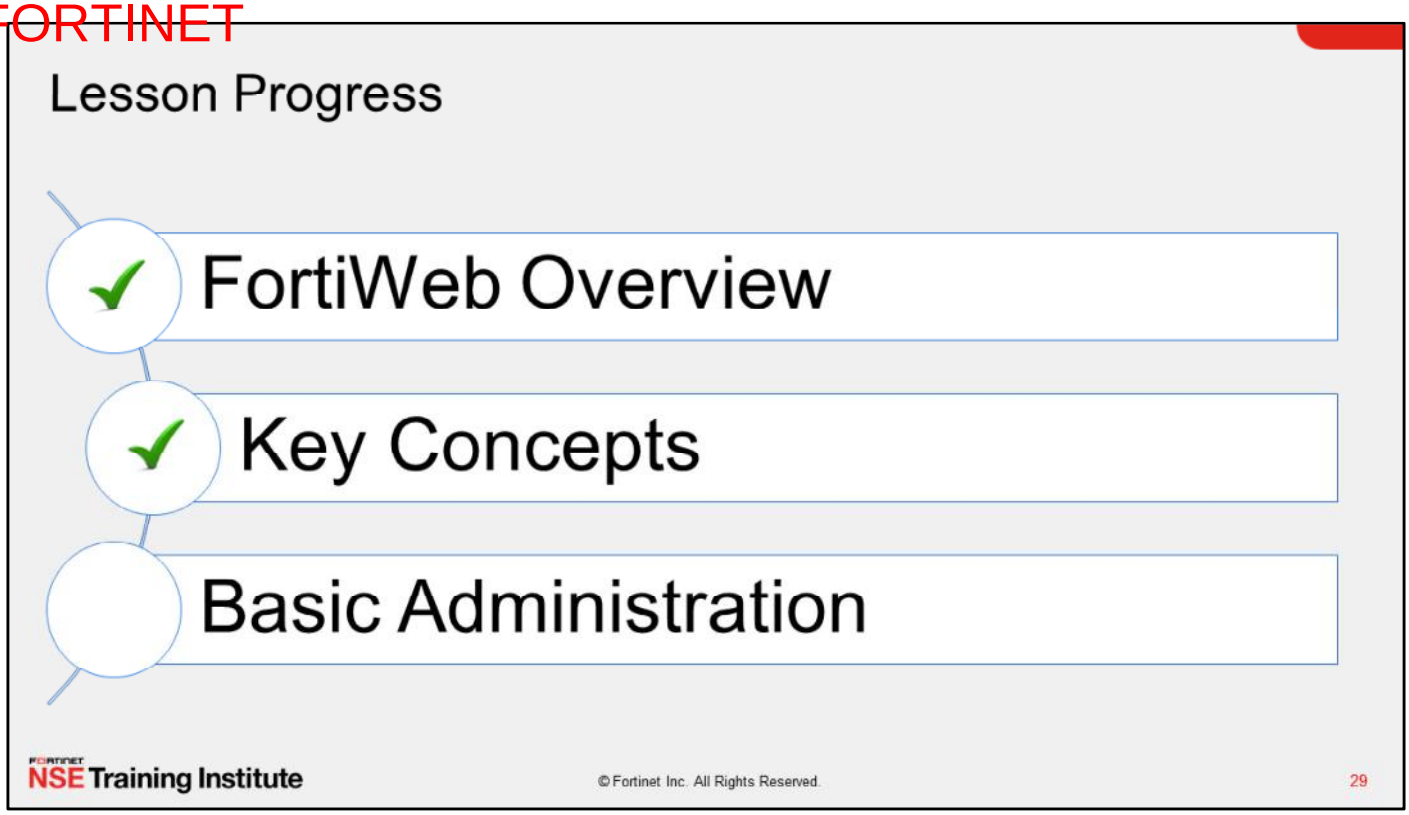
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

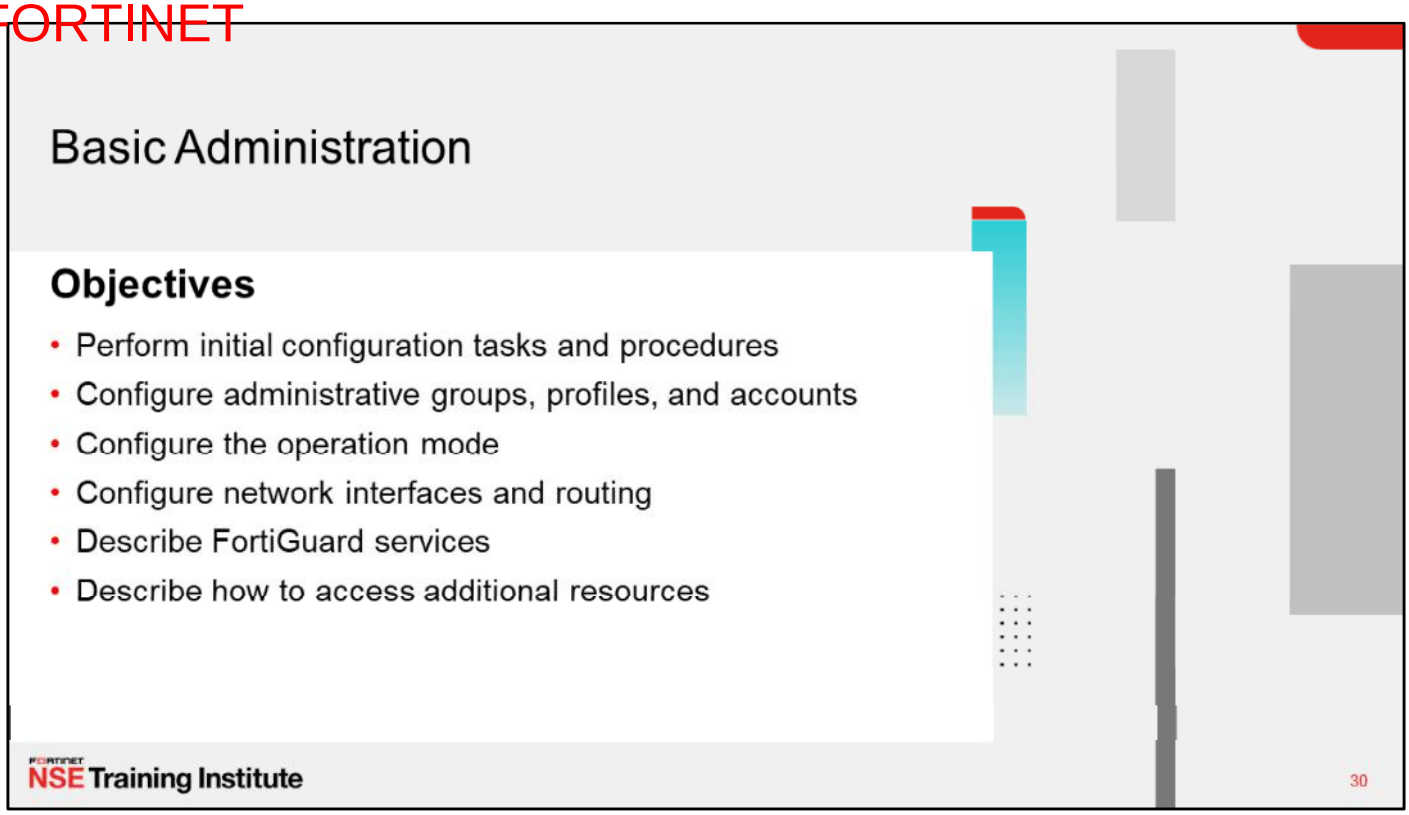


Good job! You now know the key concepts and how to best deploy FortiWeb to protect your web servers.

Now, you will learn about basic administration on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic administration, you will be able to set up and manage FortiWeb devices and services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Setting up FortiWeb

1. Administrative domains and administrator accounts
2. Operation mode
3. Network settings
   a. Management IP
   b. Static routes
4. FortiGuard
5. Server pools and persistence
6. Policies
7. X-Forwarded-For and IP-based forwarding

NSE Training Institute

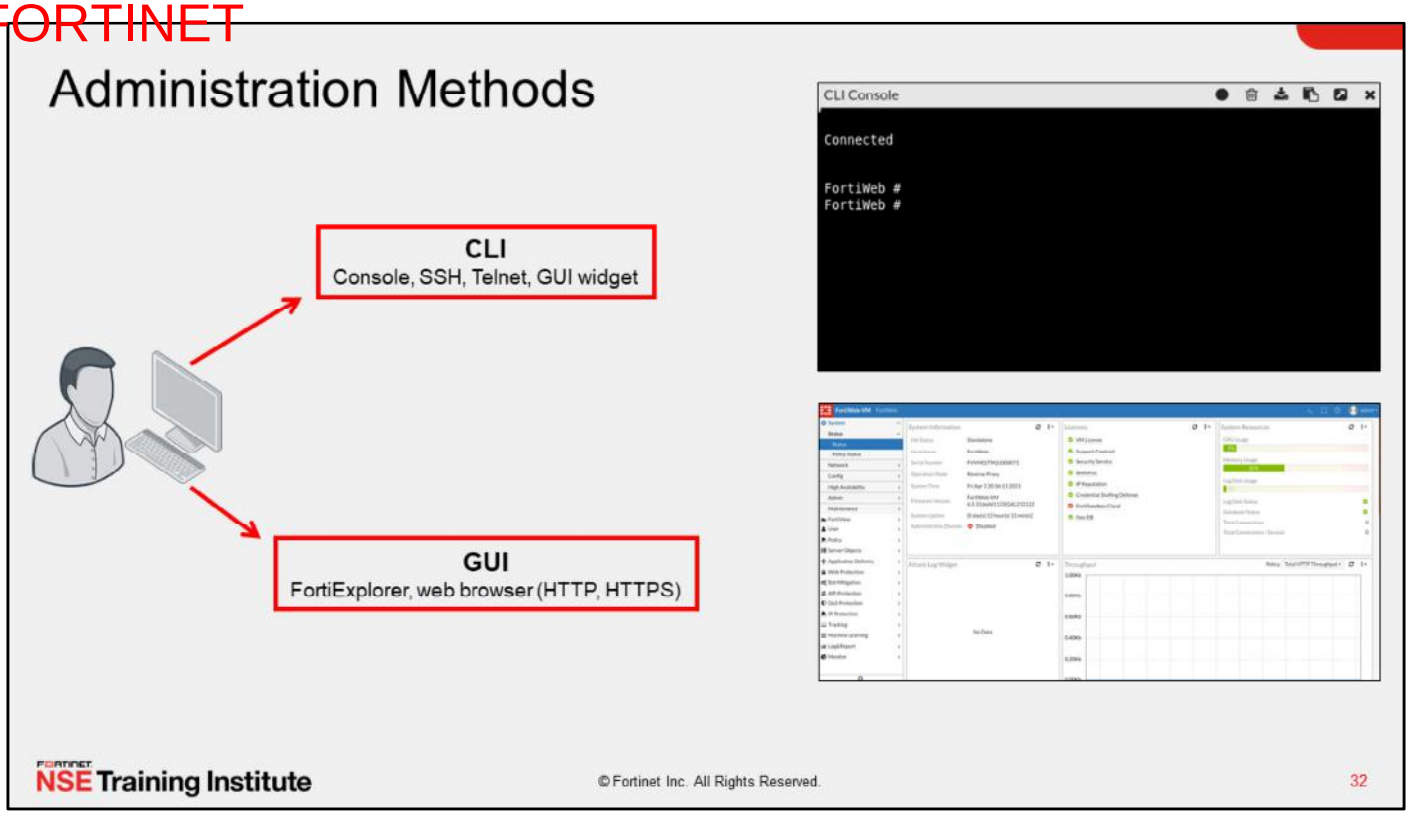
© Fortinet Inc. All Rights Reserved.

31

Setting up FortiWeb for the first time has a few required initial steps. After setting up new administrator accounts and changing default passwords, you must select the correct operation mode. Based on the operation mode selected, IP address, routes and other network configuration should be performed. Server IP addresses, persistence cookies and other session management settings should be set. Finally policies, rules, and forwarding information can be configured to properly start inspecting and enforcing traffic policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are familiar with how to access FortiGate, you will also be familiar with how to access FortiWeb.

Use either a console connection or a peer network connection to configure FortiWeb with an IP address and gateway. Then you can link FortiWeb to your network and access the GUI and CLI through the network. You can set the operation mode using either the dashboard or the CLI.

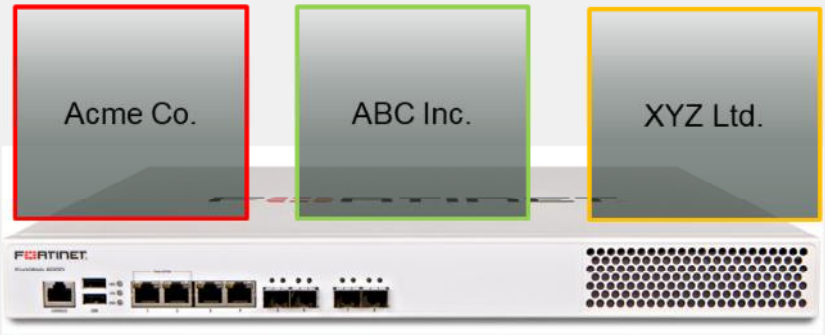
Tip: If you plan to use one of the transparent modes, do not configure the FortiWeb network settings right away. Changing the operation mode from reverse proxy mode to a transparent mode, or the opposite, resets FortiWeb network settings, and only port1 can be the management port. What does this mean? If you are connected through the network, you might lose GUI or CLI connectivity. So, during setup for transparent mode, do not place FortiWeb in your network immediately. Use a local console or peer network connection to the GUI or CLI after you've switched the operation mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

ADOMs on FortiWeb

- Logically separate each of your protected web apps
  - Domains share physical resources, but behave logically like separate FortiWebs
  - Ideal for hosting providers and enterprises—multi-tenant
- Similar to VDOMs on FortiGate
  - Separate policies, protection settings, and administrators for each domain
  - Restructures GUI and CLI



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

You can use administrative domains (ADOMs) to divide the workloads among administrators. Everything from certificates to policies can be separated by ADOMs; therefore, they can be used for multi-tenant deployments. However, ADOMs do not have virtualized networking and although they may look and act mostly like FortiGate VDOMs, they are not true VDOMs.

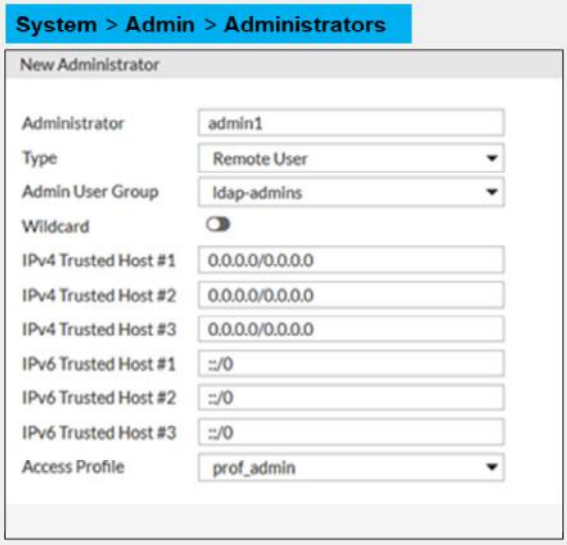
ADOMs on FortiWeb subdivide the configuration. You can allocate separate access by web applications, customers, or other logical divisions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Administrator Accounts

- By default, FortiWeb has one administrator account: **admin**
  - Uses the profile **prof_admin**, which grants full permissions
  - Cannot be renamed or deleted
- Must define all IPv4 trusted hosts to lock down access
  - If any remain `0.0.0.0/0.0.0.0`, FortiWeb is vulnerable to login brute forcing from any accessible IP
  - Only IPv6 can remain empty
- Use administrator groups to group queries while creating new administrator accounts



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

Don't allow multiple users to log in as administrators. Administrator accounts must be separate. Also, specify the access profile and, if applicable, the query to the authentication server.

Scripts from attackers are constantly scanning IP addresses on the internet for open ports, especially for brute forcing. It's a good idea to provide an extra layer of security by preventing your routers from allowing login attempts from the internet to FortiWeb. Because the FortiWeb GUI and CLI respond only to trusted IP addresses, define all allowed IPv4 management IP addresses for every administrator account. If only one host or subnet is allowed, use it in all three fields.

When using LDAP, RADIUS queries, or certificates to authenticate FortiWeb administrators, you must group queries and certificates for administrator accounts into a single set so that you can use it when configuring an administrator account.

If you leave any **IPv4 Trusted Host** field set to 0.0.0.0/0.0.0.0, FortiWeb will allow login attempts from any IP address. Attackers who want to brute force your network security can take advantage of this.

You can leave IPv6 fields empty, because FortiWeb respods only if you define a trusted host or subnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring the Operation Mode

- Topology must be correct for operation mode
- Many FortiWeb features vary by operation mode:
  - Features (SSL Offloading, Authentication, Rewriting, and so on)
  - Blocking style
  - Policy and load balancing behavior
  - Proxy pickup style
  - IP-based forwarding of non-HTTP traffic

```
config system settings
      set opmode <offline-protection|reverse-proxy|transparent|transparent-
inspection|wccp>
end
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

You can configure FortiWeb operation mode using the GUI or CLI. Reverse proxy operation mode, the most popular mode, is the default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring Network Interfaces

```
config system settings
      set opmode transparent
      set gateway 10.0.0.1
end

Switching the system operation mode, the configuration of Policy, Virtual Server,
Virtual IP, V-Zone, and static routes will be lost. Do you want to continue?
(y/n) y

config system interface
      edit port1
            set ip 10.0.0.7/24
            set allowaccess https ssh ping
      next
end
```

Port1 has to be the management interface in transparent mode

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

If you switch to transparent mode through the CLI, do not forget to set the gateway IP. FortiWeb will keep the port1 management IP, but, since the routes are lost, you must specify the gateway when you switch operation modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring Network Interfaces (Contd)

- FortiWeb supports:
  - DHCP (for AWS On-Demand), 802.11q VLANs, and 802.11ad link aggregation
  - Native IPv6 or IPv6-to-IPv4 mixed networks
  - Administrator access on VLAN interfaces
- Don't configure interfaces that will be a bridge or high availability (HA) link
- HTTPS to FortiWeb GUI uses the factory default certificate

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

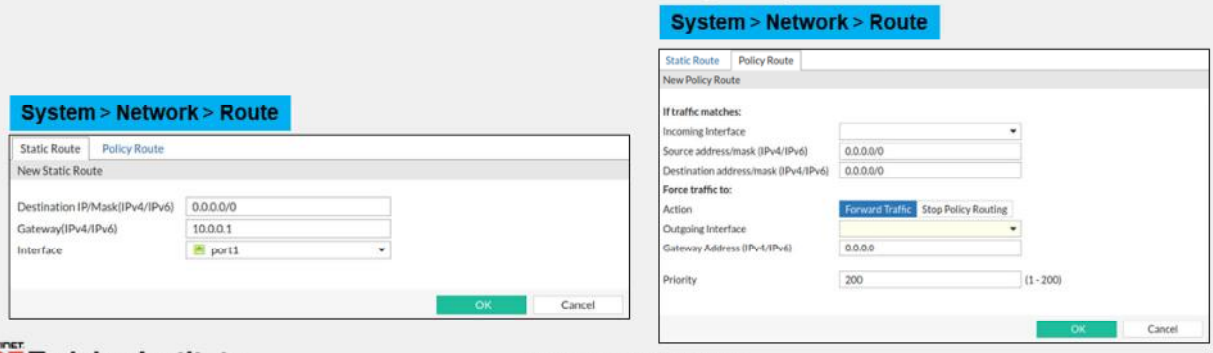
37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Routing

- Look up by destination IP address, most specific route is selected
  - Default route is most generic: destination IP/mask `0.0.0.0/0` matches all
  - If multiple equally specific routes exist, FortiWeb chooses the route with the smallest index number
- FortiWeb supports policy-based routes, lookup by ingress port, source IP, or destination IP address
- Route by port, gateway, or both
  - Useful for cloud solutions where DHCP determines the gateway



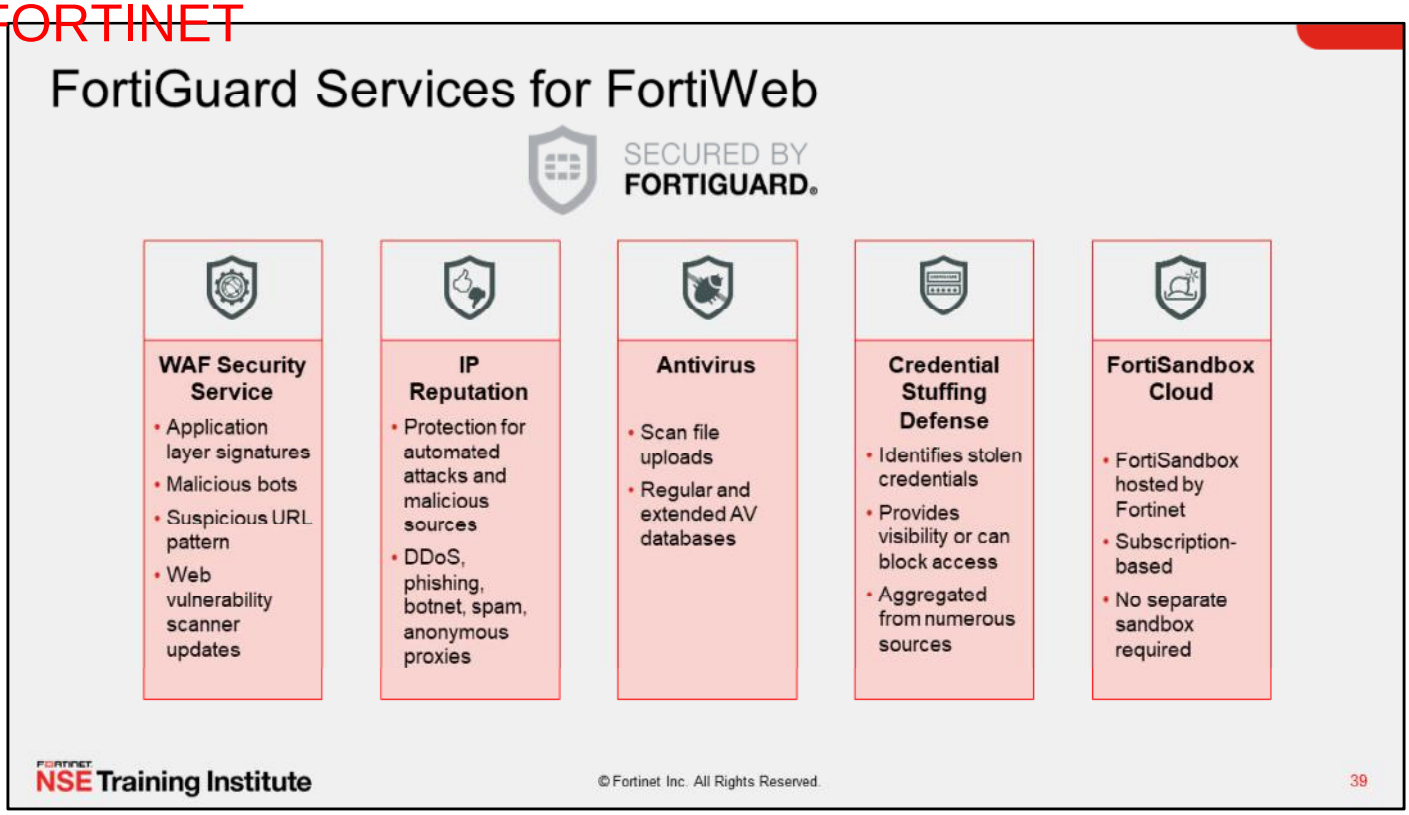
NSE Training Institute © Fortinet Inc. All Rights Reserved. 38

You should specify at least one route to the default gateway. This route is where FortiWeb sends traffic if an IP isn't directly connected. Usually, this is the upstream FortiGate or (if FortiGate is in transparent mode) the internet router. If you have a large internal network, and your protected web servers are not on the same subnet, you must add a route for those destinations as well.

If your network interfaces use DHCP, especially if you have dual gateways, then static routes are not enough. You may need to route traffic based upon the ingress port, the source, or both. To do this, you can configure policy-based routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Most exploits and virus exposures occur within the first two months of a known vulnerability. Most botnets consist of thousands of zombie computers whose IP addresses are continuously changing. Every day, spilled account credentials are used to launch credential stuffing attacks. FortiWeb uses signatures, IP lists, and data type definitions for many features. FortiWeb can also use virus definitions to block trojan uploads, IP reputation definitions to allow search engines but block botnets and anonymize proxies preferred by hackers, and the spilled account credential database to prevent credential stuffing attacks. FortiGuard services ensure that your FortiWeb is using the most advanced attack protections. Timely updates are crucial to defending your network.

The best practice is to enable FortiWeb to periodically check for FortiGuard updates from the FortiGuard Distribution Network (FDN), and automatically download and apply updates if they exist.

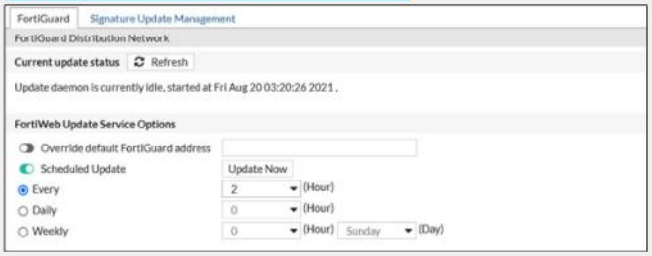
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

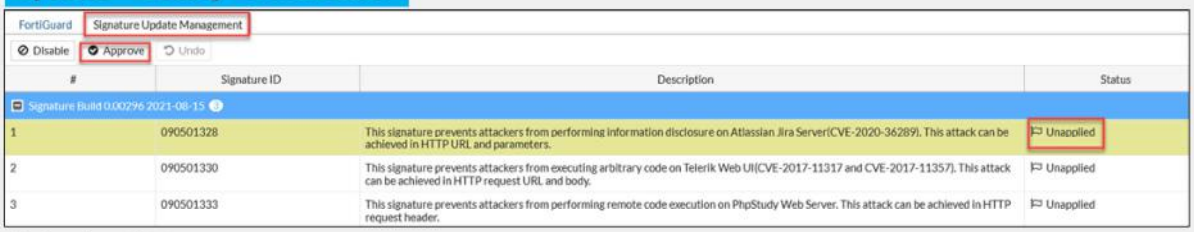
Updating FortiGuard Signatures

- FortiGuard
  - Update signatures
  - Verify signature versions
- Signature Update Management
  - New signatures in the update, if any, are listed here. You can see the signature ID, description, and status (Applied, Unapplied) of each signature.
  - Provides the ability to apply new signatures in Alert mode for testing before implementing

System > Config > FortiGuard



System > Config > FortiGuard



NSE Training Institute © Fortinet Inc. All Rights Reserved. 40

FortiWeb allows you to deploy new signature updates in alert mode so that you can test new signatures in your environment before setting them to block mode.

When you update the FDS, new signatures in the update are listed on the **Signature Update Management** pane, where you can view the new signatures. From here, you can select and right-click a signature and perform any of the following three actions:

- **Disable**: Disable the signature across all the web protection policies. If this signature-related rule brings multiple blocks, you can confirm the false positive and enable this option.
- **Approve**: Change the alert mode of the signature to normal status, with the action as configured in the signature protection policy.
- **Undo**: Use this option to cancel the Disable and Approve operations for a signature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Need More Details?

- Fortinet Tech Docs http://docs.fortinet.com/ and **Help** button
- FortiGuard Threat Research https://www.fortiguard.com/
- Forums http://support.fortinet.com/forums and Support

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

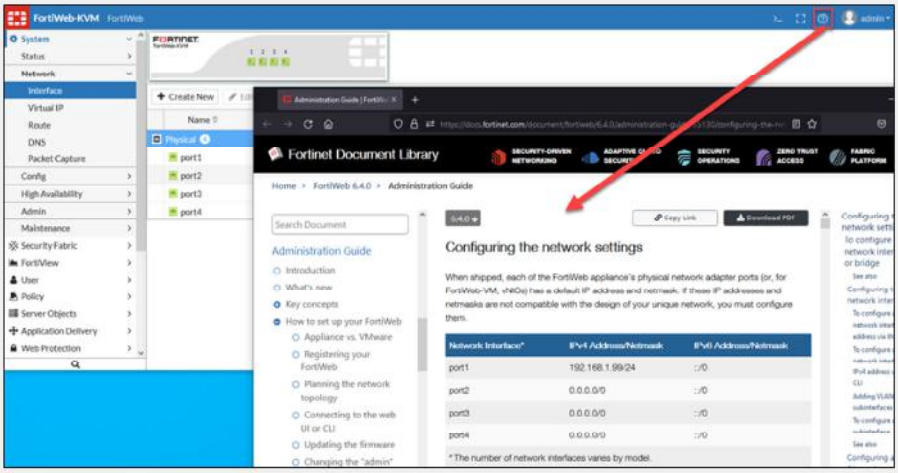
FortiWeb is a full-featured product and continues to evolve to meet the challenges presented by the HTTP threat landscape. This slide shows the main sources of information that can help you with your implementation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Help

- Help jumps to the corresponding page
- Table of contents
- Can't find it? Search!
  - Expand window to show magnifier icon, search **this doc**
  - Google, Yahoo!, MSN, Baidu search all on `docs.fortinet.com`



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

42

As on other Fortinet products, click the help button in FortiWeb to view the relevant content in the documentation. The help information gives how-to examples, feature overviews, and detailed references about specific options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the command to change or create an IP address on FortiOS?
   A. `set system interface`
   B. `edit system interface`
   ✓ C. `config system interface`
   D. `show system interface`

2. Which port is used by default for management in transparent mode?
   ✓ A. port1
   B. port2
   C. port3
   D. port4

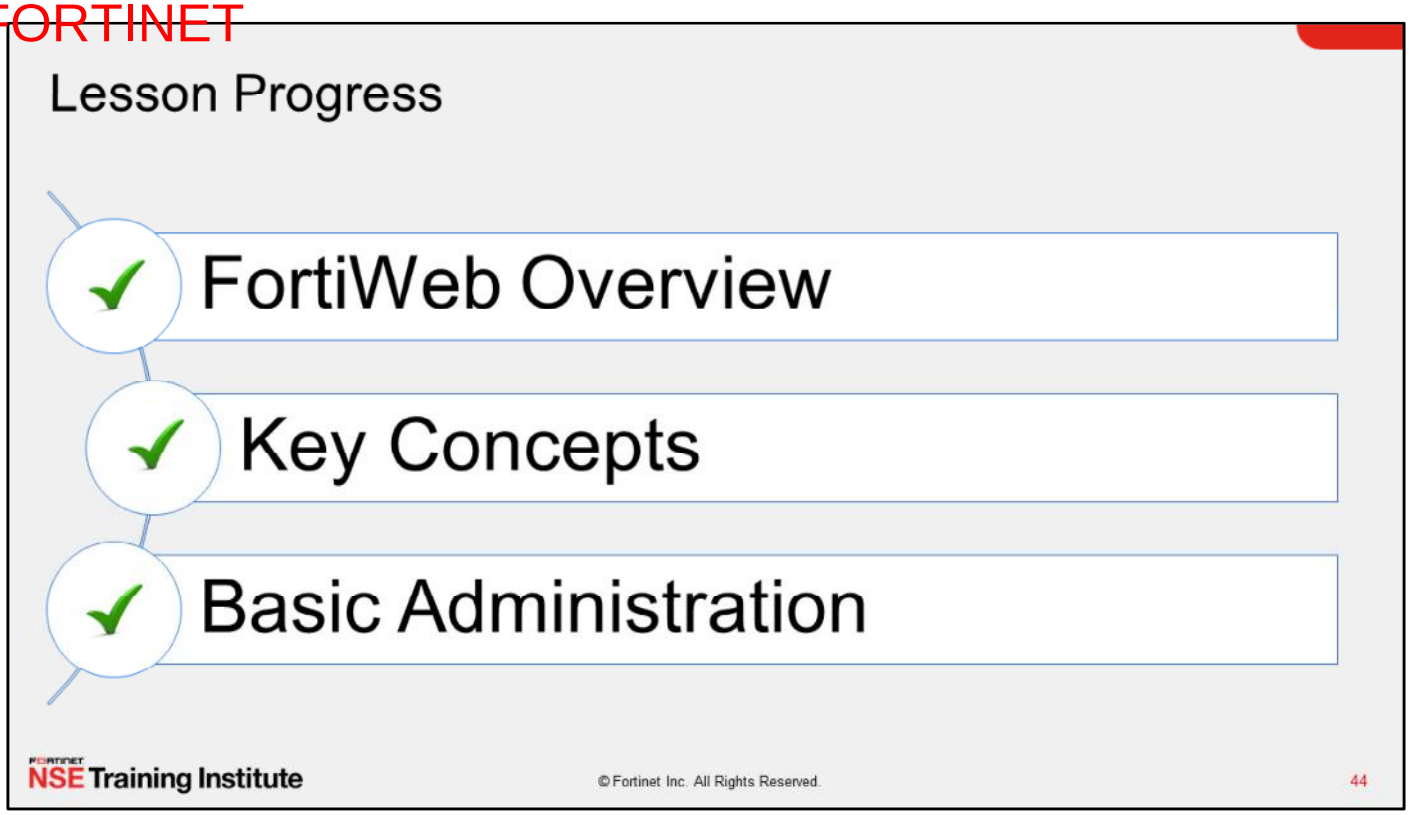
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

43

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ What is a web application firewall?
- ✓ Why FortiWeb?
- ✓ FortiWeb product family overview
- ✓ Understand when and where to add FortiWeb to your defense portfolio
- ✓ Choose the right operation mode
- ✓ Management access methods
- ✓ Support resources

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

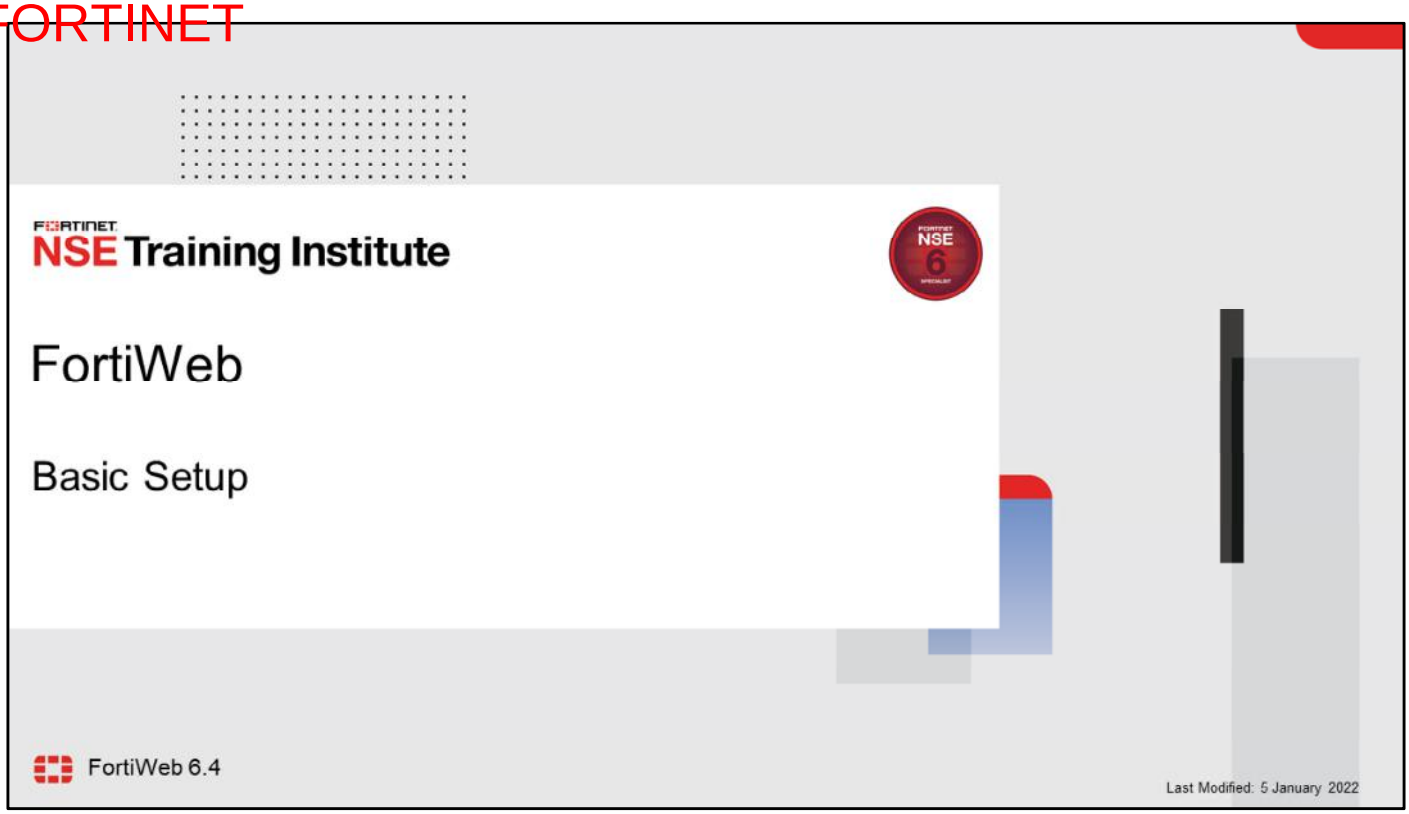
45

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiWeb features to protect your network from security threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you'll learn how to physically deploy FortiWeb and complete basic settings so that you can begin to integrate FortiWeb into your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Setup Scenarios
- Configuration Components and Initial Configuration
- Server Pools, Policies, and Protected Host Names
- Policy Overview
- HTTP Content Routing and Rewriting

NSE Training Institute

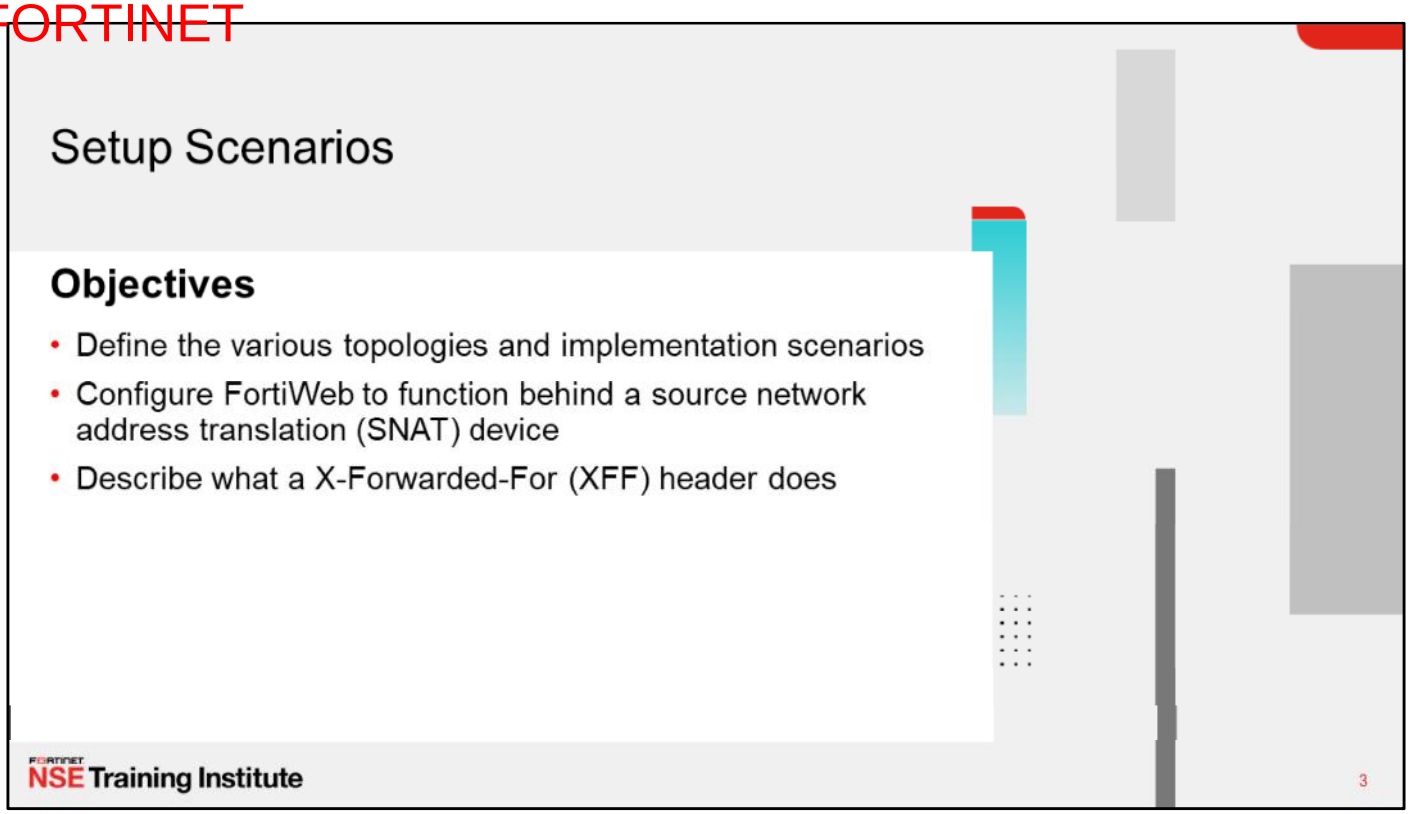
© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

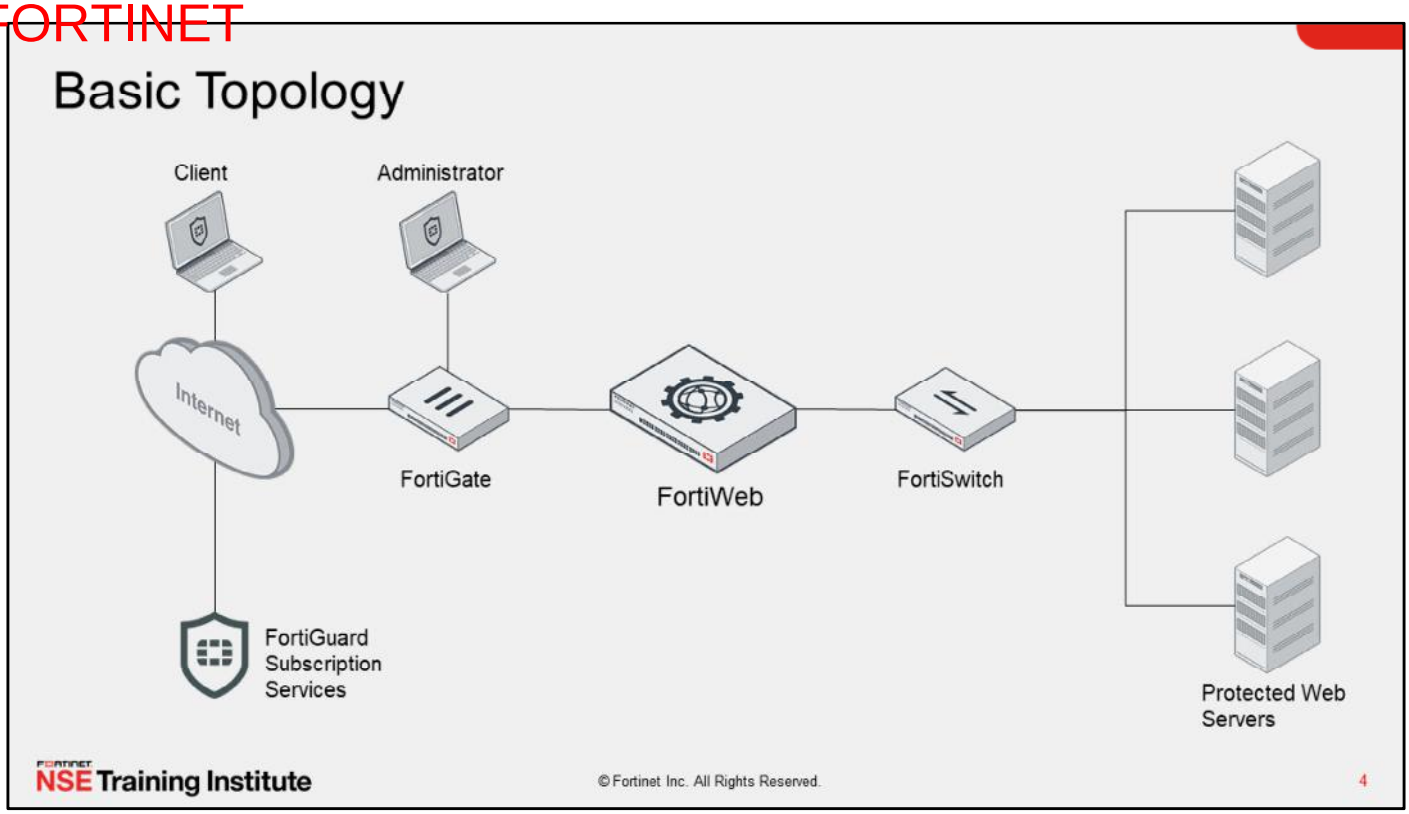


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of setup scenarios, you will know the various ways you can integrate FortiWeb into a network environment, even behind NAT devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

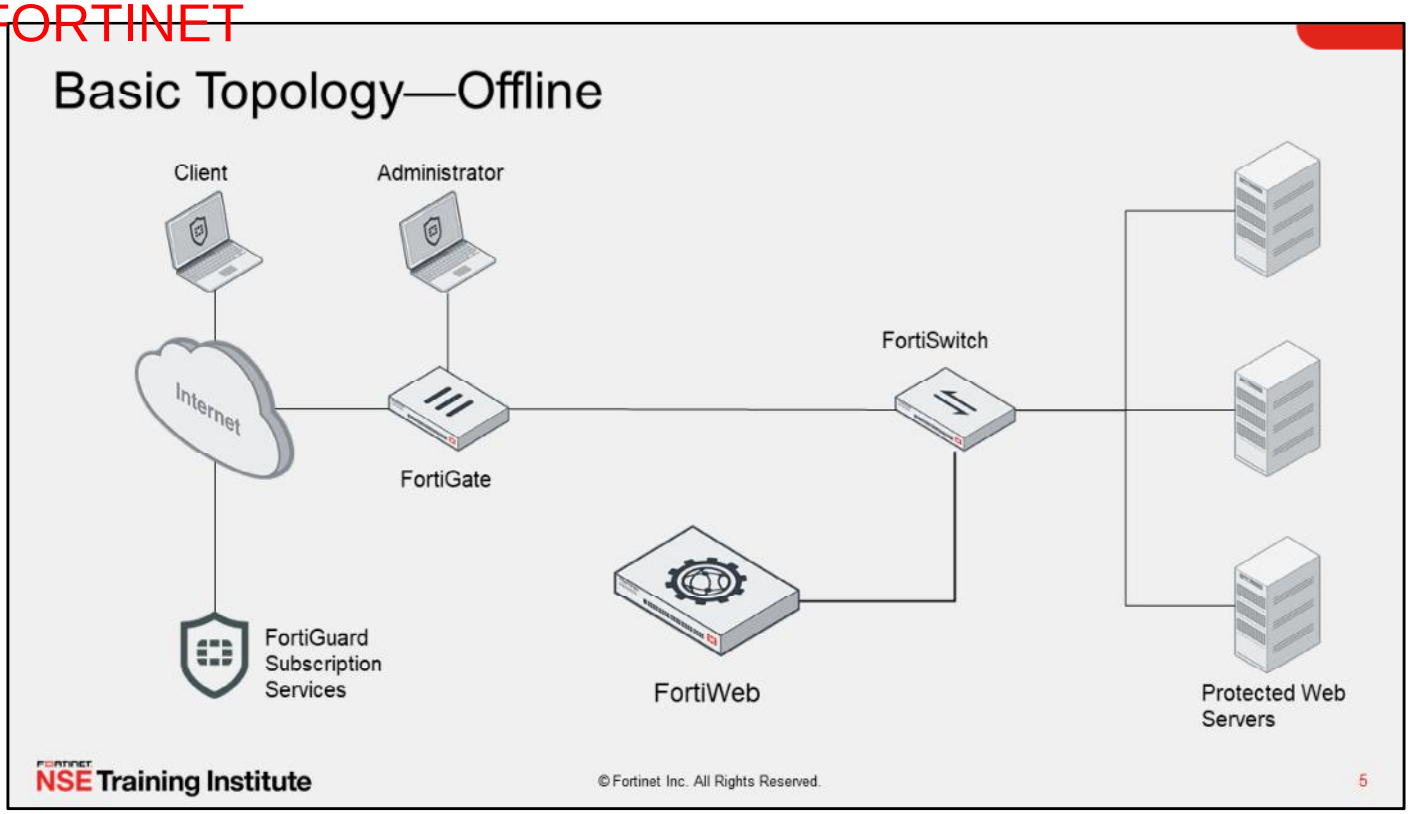
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb can be deployed in a one-arm topology, but is more commonly positioned inline, to intercept all incoming client web connections and redistribute them to your servers. FortiWeb has TCP and HTTP-specific firewalling capabilities. Because FortiWeb is not designed to provide security to non-HTTP applications, you should almost always deploy it behind a firewall, such as FortiGate, that focuses on security for other protocols that may be forwarded to your back-end servers, such as FTP and SSH. After you deploy FortiWeb, you can configure it from a web browser and terminal on your management computer, using its web GUI and CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Offline or out-of-band is a common descriptor for this mode. Minimal changes to an existing network environment are required. It does not introduce any additional hops or network latency to communications to the protected web servers. However, many features are not supported.

Web requests continue to be sent to a web server, and not forwarded through the FortiWeb appliance. Traffic is duplicated from a switch or router and sent on an out-of-line link to FortiWeb through a switched port analyzer (SPAN or mirroring) port. Unless there is a policy violation in the traffic, there is no reply traffic or communication from FortiWeb. Depending on whether the upstream firewalls or routers apply source NAT (SNAT), the FortiWeb and web servers might be able to see and use the source IP addresses of clients.

FortiWeb monitors traffic received on the data capture port's network interface (regardless of the IP address) and applies the first applicable policy. Because it is not inline with the destination, it does not forward permitted traffic. FortiWeb logs or blocks violations according to the matching policy and its protection profile. If FortiWeb detects a malicious request, it sends a TCP RST (reset) packet through the blocking port to the web server and client to attempt to terminate the connection. FortiWeb does not attempt modify the traffic, just interrupt and block it if something is detected. FortiWeb cannot offload SSL services, load balance connections, or support user authentication in Offline mode. FortiWeb can provide detection, but does not directly block or modify traffic to or from the two web servers.

Most organizations do *not* permanently deploy FortiWeb in offline protection mode. Instead, they will use it as a way to learn about web servers vulnerabilities. They can also use it as an opportunity to do some FortiWeb configuration during a transition period, after which they switch to an operation mode that places FortiWeb inline (between clients and web servers). Switching out of offline protection mode when the transition is complete can prevent bypass problems that can arise as a result of misconfigured routing. It also offers you the ability to offer protection features that cannot be supported in a SPAN port topology.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Traffic Mirror from FortiWeb

- Configure FortiWeb to send traffic to third-party IPS/IDS devices through network interfaces for traffic monitoring
  - Reverse proxy - traffic mirror on both a virtual and physical FortiWeb are supported
  - True transparent proxy - only supported by a virtual FortiWeb
- Traffic mirror supports three types of connections to an IPS/IDS:
  - To a physical port of FortiWeb
  - To FortiWeb by the switch (destination MAC address is required)
  - To FortiWeb through the network (IPS/IDS operates in server mode)
- The corresponding three modes for traffic mirroring:
  - Direct mode
  - Switch mode
  - Server mode

NSE Training Institute © Fortinet Inc. All Rights Reserved. 6

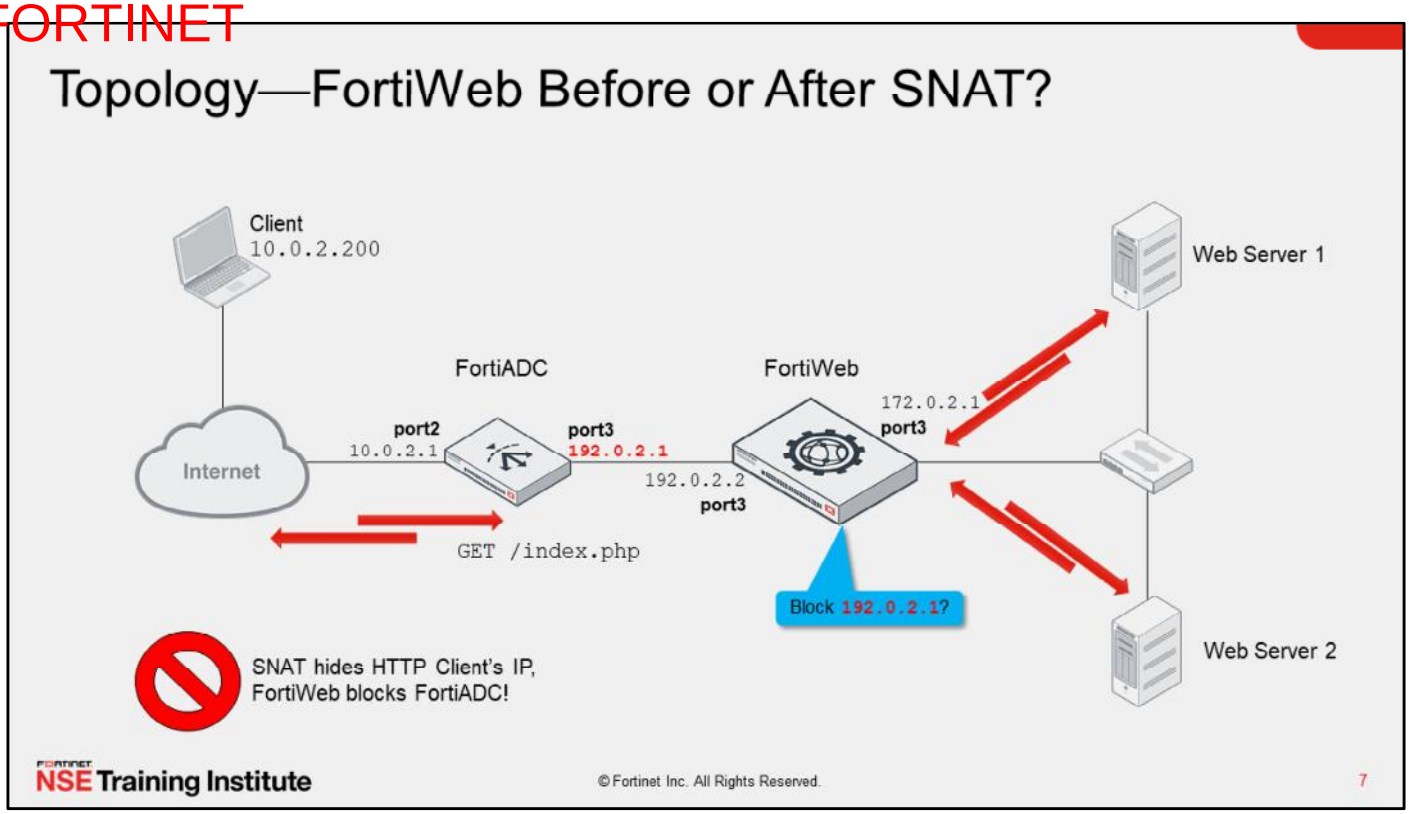
In reverse proxy and true transparent proxy modes, you can configure FortiWeb to send traffic to third-party IPS/IDS devices through its network interfaces for traffic monitoring. In reverse proxy mode, traffic mirror on both a virtual server and real server are supported, while in true transparent proxy mode, only traffic mirror of the virtual server is supported.

Traffic mirror supports three topologies of IPS/IDS:
- To a physical port of FortiWeb
- To FortiWeb by the switch (destination MAC address is required)
- To FortiWeb through the network (IPS/IDS operating in server mode).

Accordingly, three modes for traffic mirror are available:
- Direct mode
- Switch mode
- Server mode

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



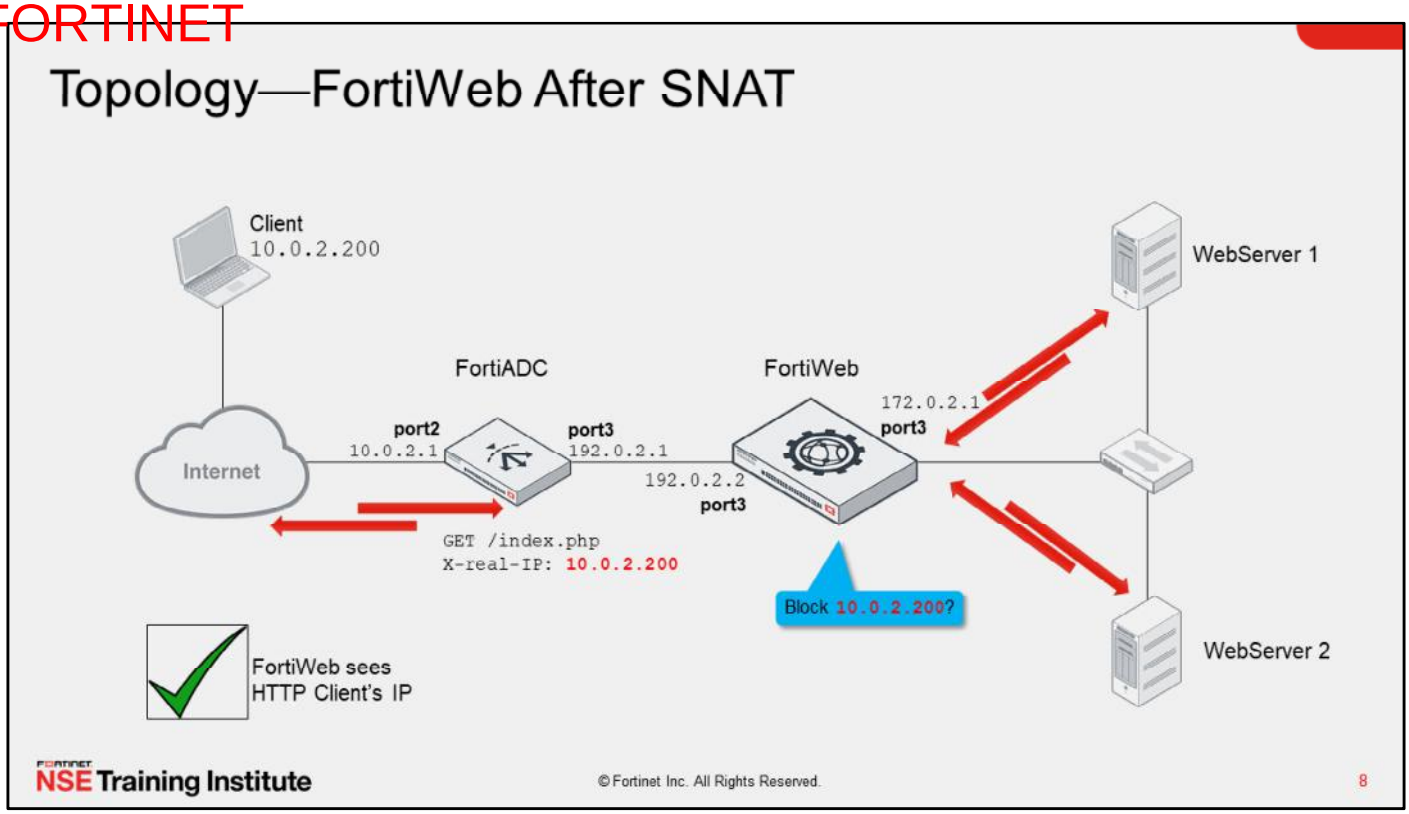
Regardless of whether you deploy real or virtual hardware, you need to know if source NAT (SNAT) is being used. If you have a FortiGate operating in transparent mode and placed in front of your network or your upstream router is not perming source NAT, this scenario is not relevant.

But if you are using a gateway device in NAT/route mode, or a load balancer such as FortiADC or Citrix NetScaler, you should check its configuration. By default, FortiWeb blocks many attacks based upon source IP address. So, if FortiGate hides the real source address from FortiWeb, FortiWeb may not behave as intended and accidentally block traffic from your upstream gateway.

In the example shown on this slide, an upstream load balancer is applying SNAT, but FortiWeb is configured to handle this. As a result of the misconfiguration, whenever an attack occurs, FortiWeb blocks sessions from FortiADC, breaking all connectivity from all users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are two solutions you can use if you have upstream SNAT. This slide shows one solution.

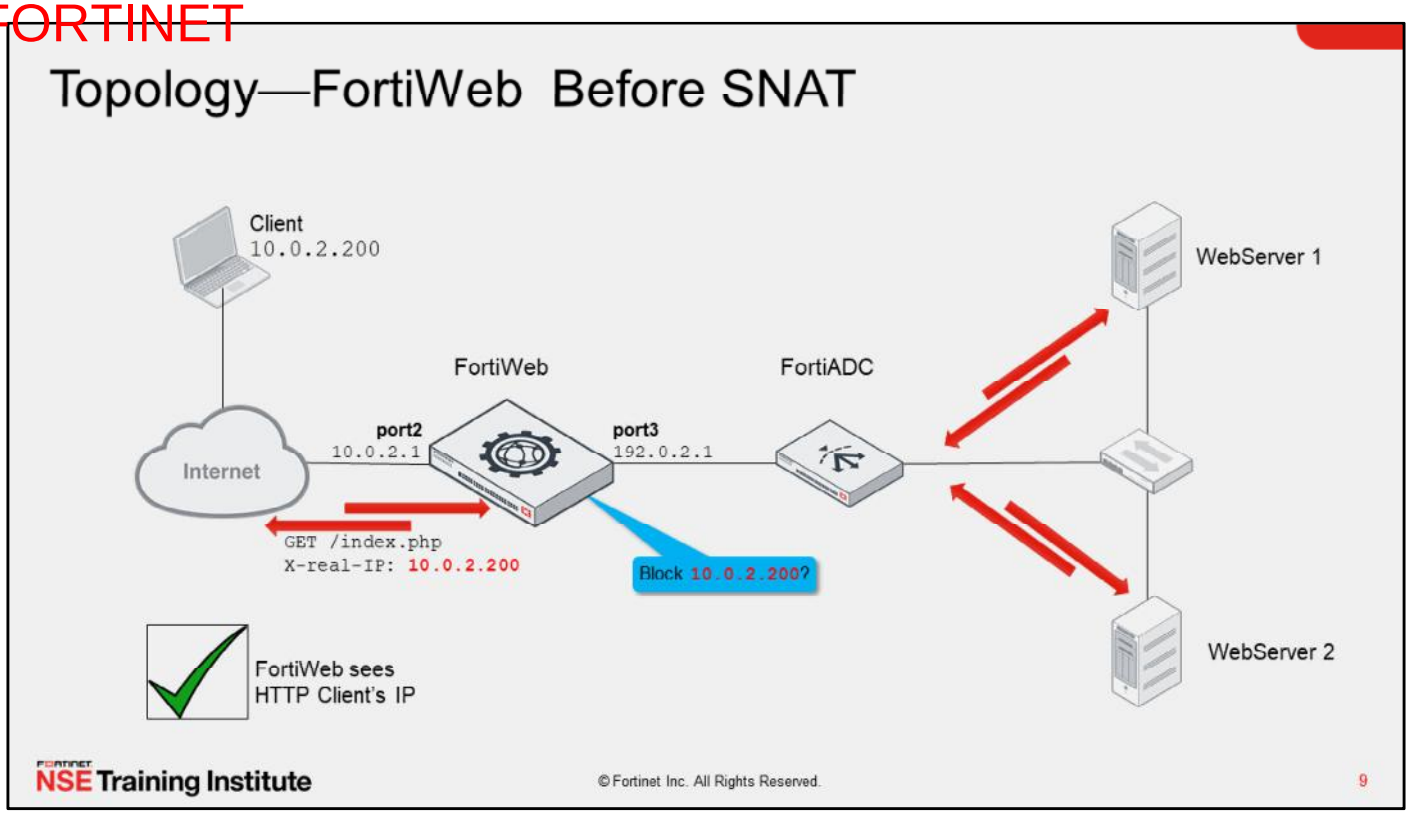
Configure the upstream NAT device to put the original client's IP address in an HTTP header such as X-Forwarded-For. The name format can vary. Some CDNs, like Akamai use X-True-IP or X-Real-IP. If you're not sure what name format to use, run a packet capture or use browser developer tools to observe the HTTP transactions.

Configure FortiWeb to find the IP in the HTTP header, not the IP header.

This solution works in many cases, including when FortiGate is used. Be careful, because not all NAT devices support the use of this solution and can add a header to a connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

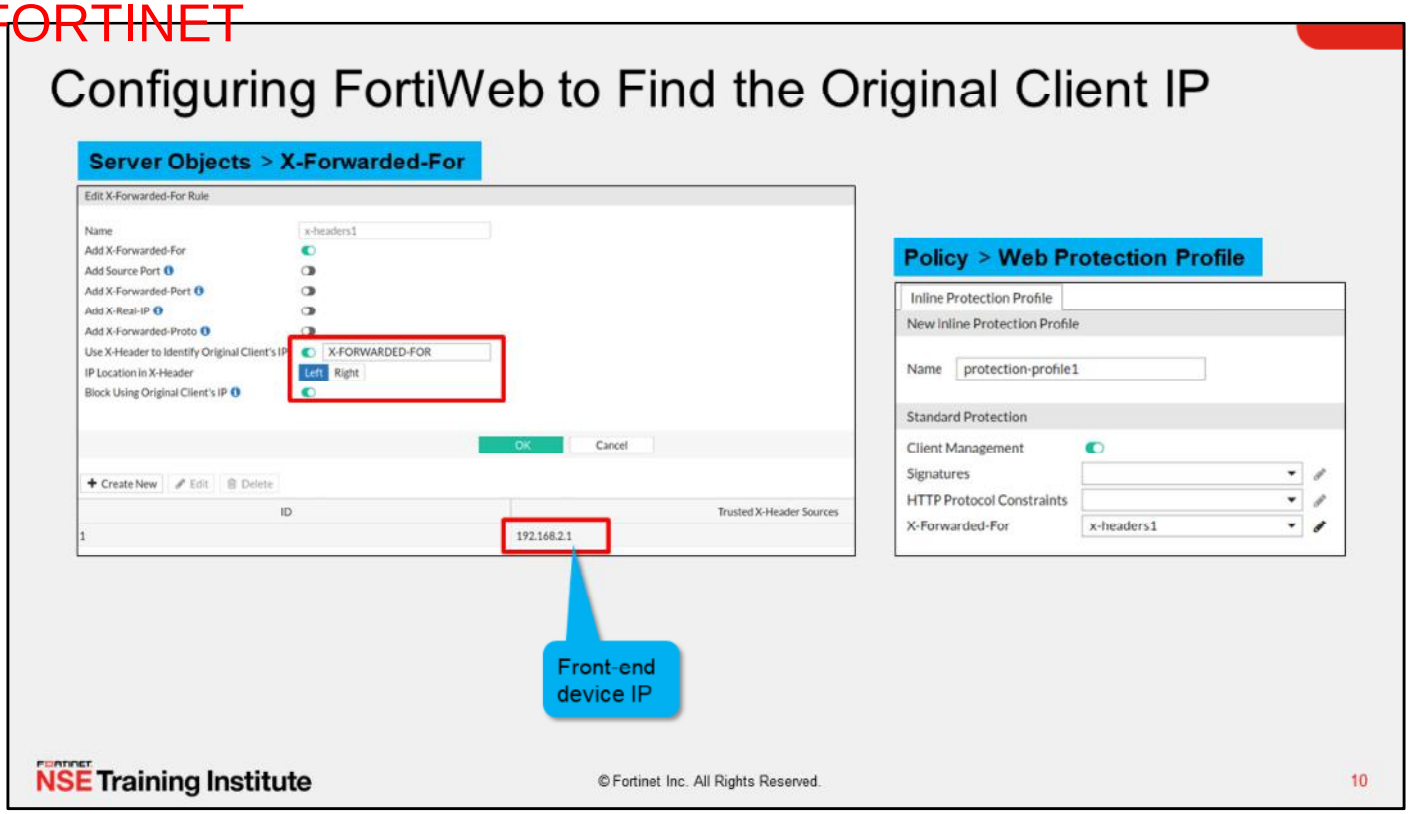


The easier of the two solutions is to place FortiWeb in front of the load balancer or routing device. Some other positive side effects of this topology are that the load balancer only receives legitimate traffic, so it's protected, and the load balancer resources are used efficiently. It a very common setup to have FortiWeb between the internet device (like FortiGate) and the load balancers protecting a server farm (like FortiADC). XFF headers are used to ensure the proper connections are allowed and blocked.

Remember that load balancers sometimes use the source IP address for session persistence or client-based load balancing. If this is the case, also configure FortiWeb to transmit the original client IP address in X-Forwarded-For in the HTTP header and configure your load balancer to use that address instead of the source address in the IP header.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

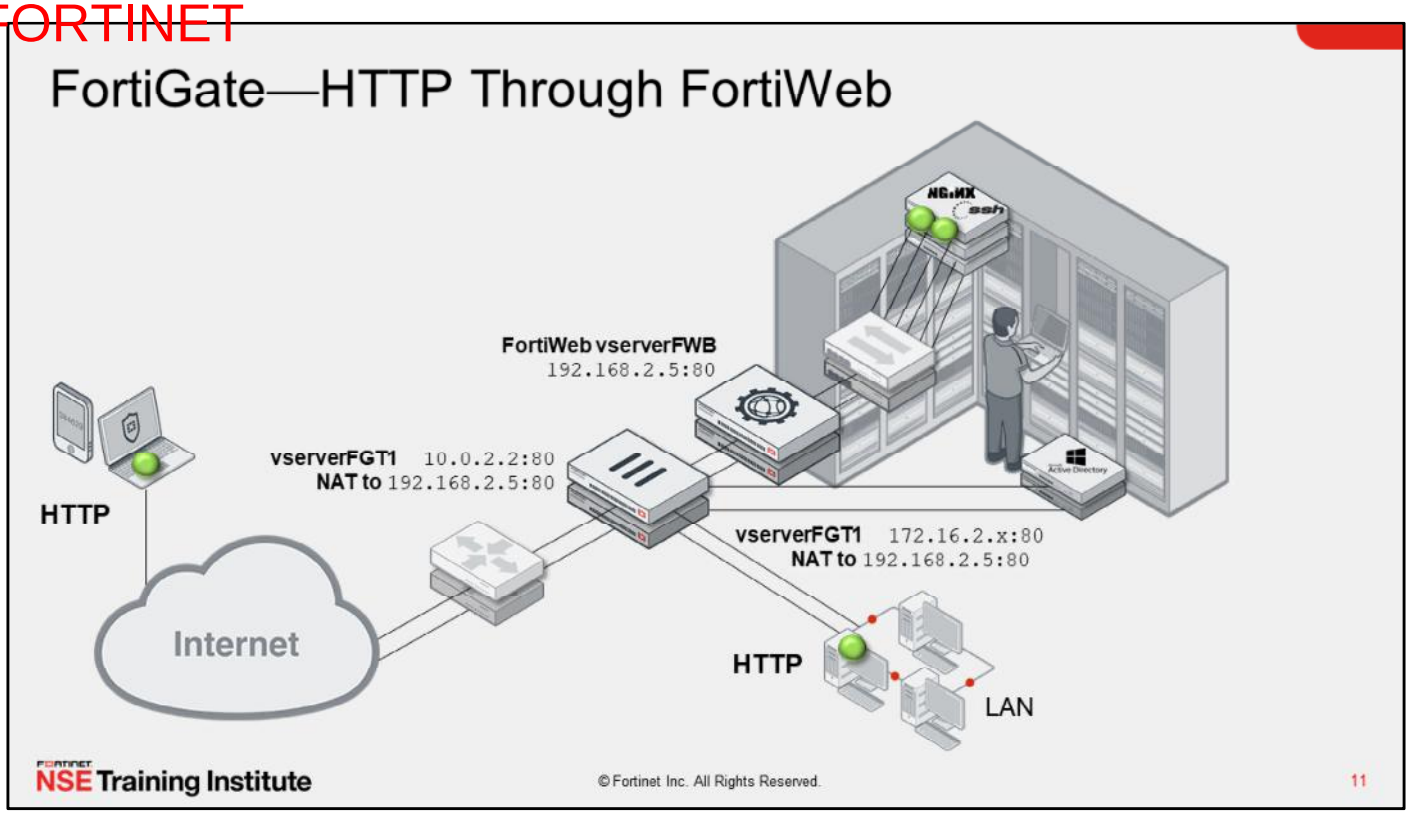


After you configure the upstream or downstream NAT device to read or send X-headers, configure your FortiWeb to use them. The settings you need to configure if your load balancer is positioned upstream are highlighted on this slide. If your load balancer is positioned downstream, the settings you configure are different. Enable **Add X-Forwarded-For** or **Add X-Real-IP** instead. Since HTTP headers aren't authenticated and are easy to spoof, be sure to define which IP addresses—for example, your upstream FortiGate—are the trusted providers of this header.

When FortiWeb is configured to use the X-Forwarded-For (XFF) header, you can apply the header by selecting it in a protection profile that is used by a server policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This diagram shows a network topology that you might see in an enterprise-sized business. It's slightly simplified, but it would probably involve an authentication server, full mesh topology, a management LAN on FortiWeb port1, and, possibly, HA for redundancy. Because FortiGate in this topology is operating in NAT/route mode, and applying SNAT, the administrator has enabled load balancing and configured two virtual servers. FortiGate applies X-headers: one for road warriors connecting from the internet, and another for employees on the headquarters office LAN.

Can you find the misconfiguration?

That's right: it's the FortiGate virtual server for the office LAN. Because FortiGate would be using private network IP addresses, many LANs could have clients using those same private IP addresses; that is, the addresses are not globally unique. So, FortiWeb wouldn't use the X-header for those private IP addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How does a SNAT device usually communicate a client source IP to FortiWeb?
   A. TCP ID number
   ✓ B. HTTP header
   C. Cookie
   D. A SNAT device cannot send an additional IP address

2. Which feature is available in inline modes (like reverse proxy mode) and not in offline modes (like transparent mode)?
   A. Logging traffic
   B. Blocking malicious connections
   ✓ C. Authentication
   D. Web Filtering

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Progress

- ✓ Setup Scenarios
- Configuration Components and Initial Configuration
- Server Pools, Policies, and Protected Host Names
- Policy Overview
- HTTP Content Routing and Rewriting

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

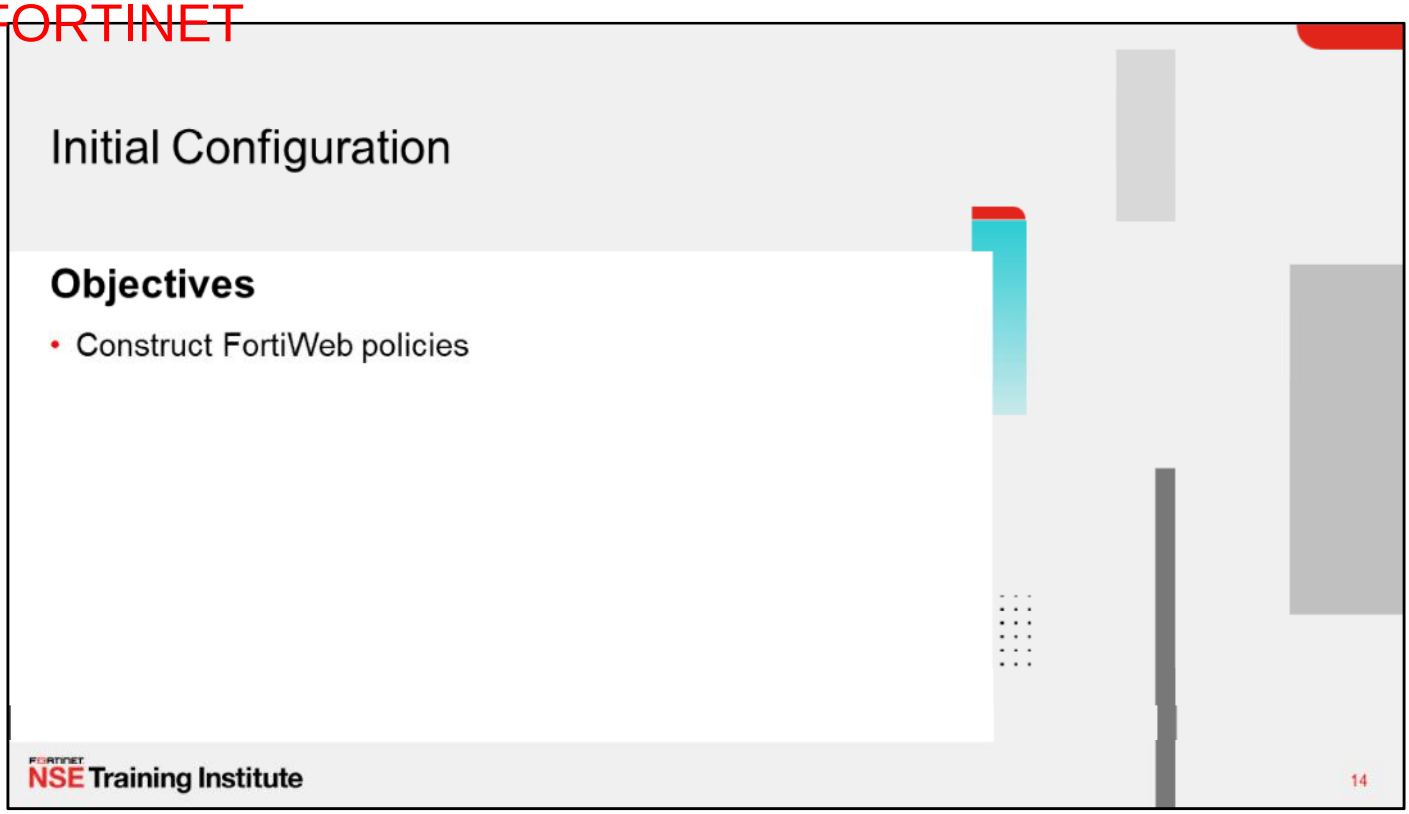
13

Good job! You now understand the various network topologies possible with FortiWeb.

Now, you will learn about the nesting of configuration components and initial configuration, which is the logic of configuring FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding which configuration objects are used and how these objects link together, you will be able to start to configure FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Policy Objects

- A FortiWeb server policy consists of many different components, but generally must include:
  - A virtual server (where clients connect to)
  - A server pool
  - A web protection profile (contents vary depending on if running inline or offline modes)
- Web protection profiles (inline or offline modes) consist of multiple leaf objects and policies:
  - XFF header rules
  - URL access policies
  - Geolocation IP policy
  - Web shell detection policy
- These leaf policies are not all required, but are configured depending on the requirements of the administrator

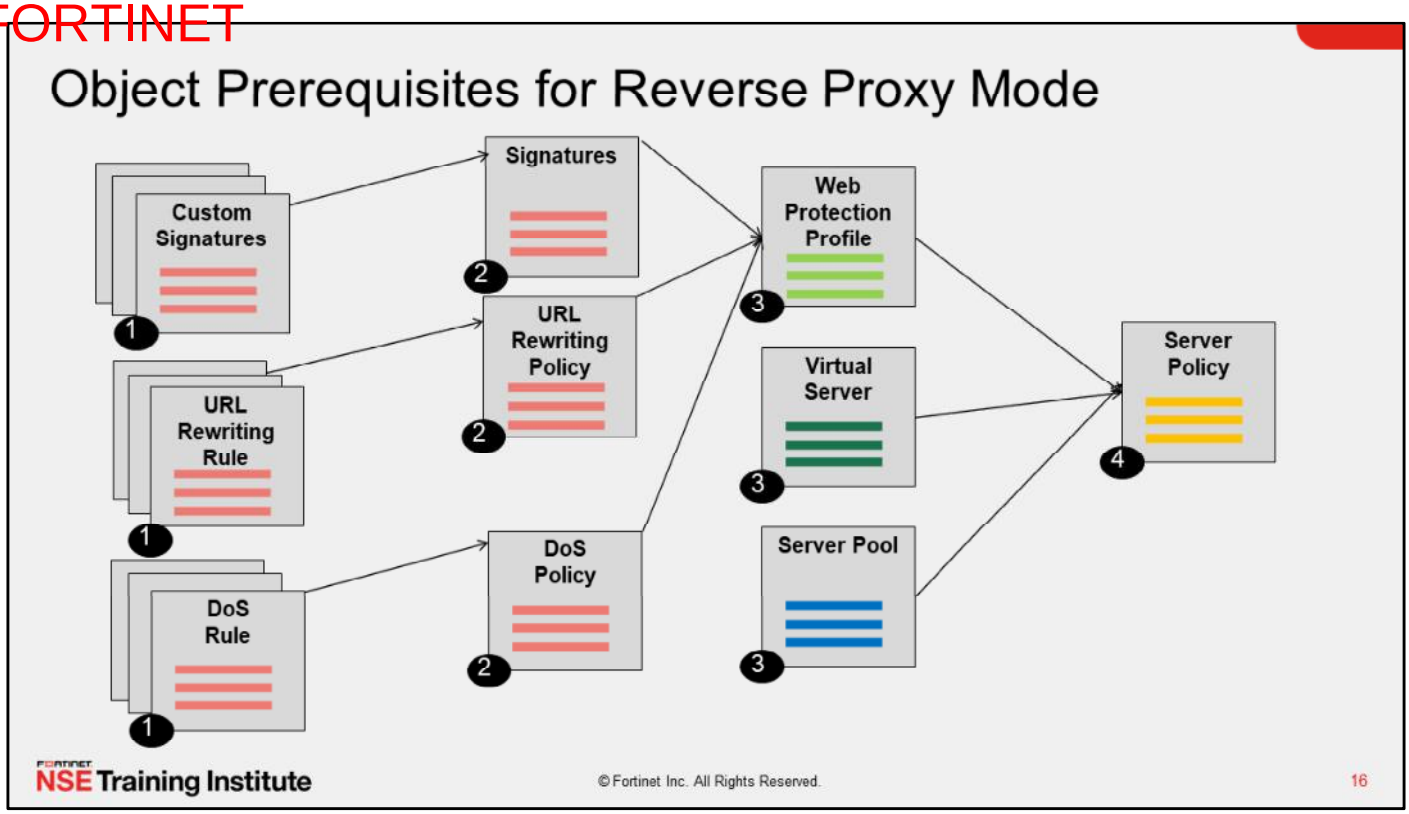
NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

FortiWeb ties policies to an associated virtual server and server pool. Once defined, these three components make up a server policy. FortiWeb can have multiple server policies and protect multiple web servers and server farms. The server policies contain a web protection profile which is a consolidation of the settings the FortiWeb can apply to web traffic. Each profile consists of multiple leaf objects configuring a specific FortiWeb feature, like authentication or IP reputation blocking.

Depending on the policy, multiple leaf policies will be configured if a specific feature is required for a particular web server. The policy configuration is extremely granular.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You usually start by configuring the leaf node objects—not the server policy or web protection profile. Server policies group objects together and apply settings to matching traffic. But, to use server policies, you must configure the objects first.

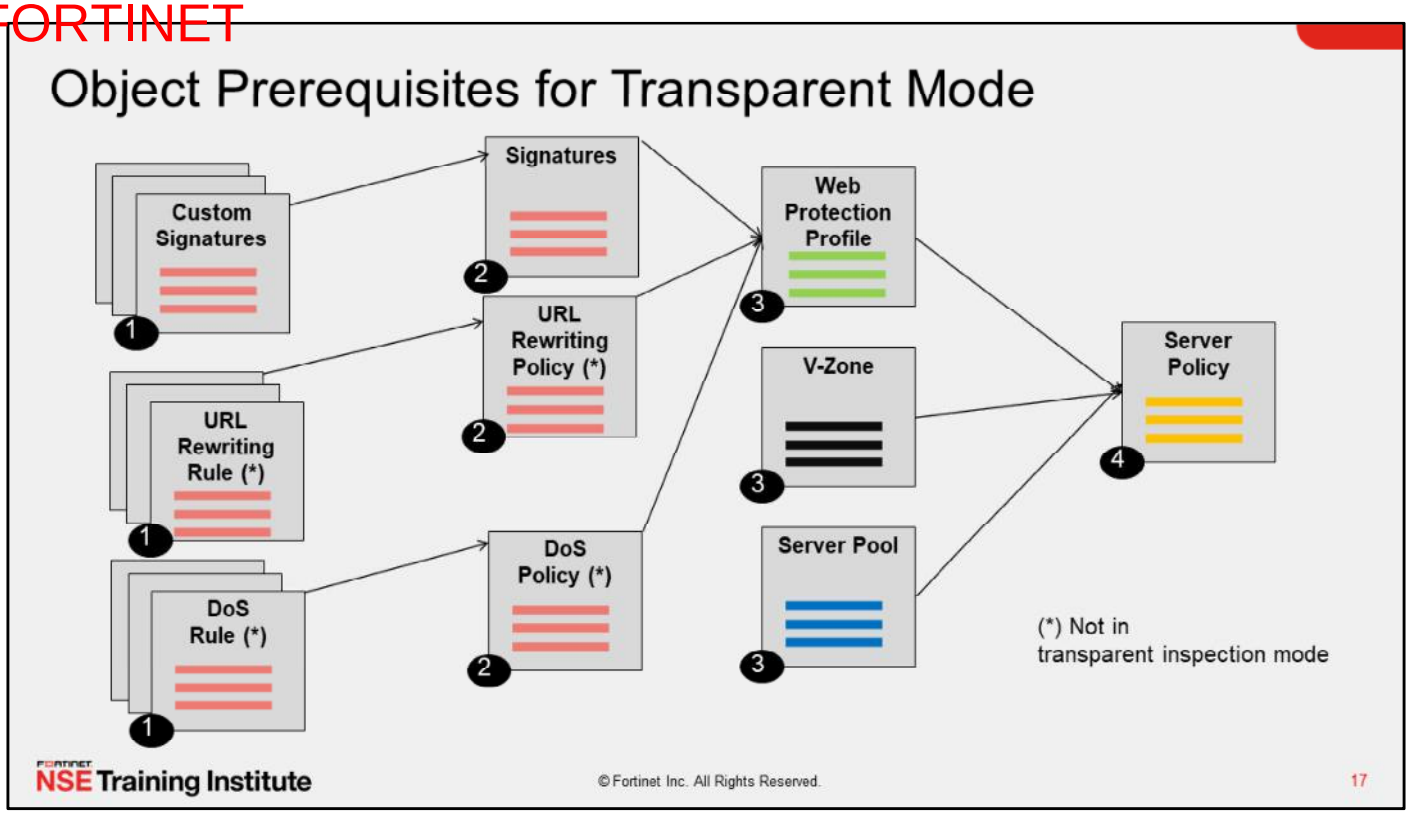
In reverse proxy mode, start by configuring fine-grained objects, such as:

- A virtual server
- A certificate for HTTPS
- Persistence settings that will be used by the server pool
- Custom signatures
- TCP flood rate limits
- Authentication rules
- Rewrite rules
- Input rules

Then, select these objects in DoS policies, server pools, and other intermediate objects, before binding them all together in a server policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

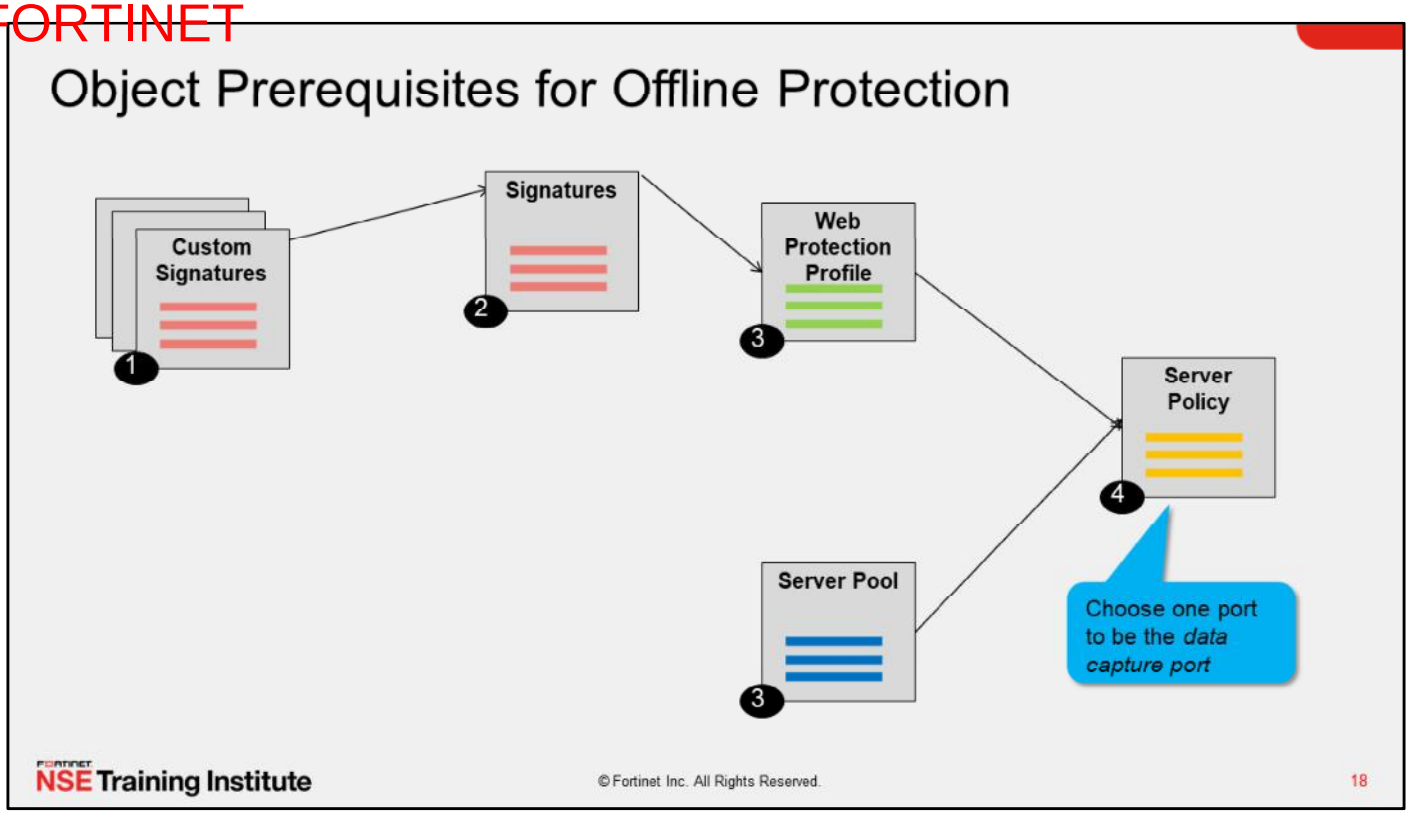


Transparent inspection mode or true transparent proxy mode are configured similarly to reverse proxy mode. The significant exception is the virtual server. Virtual servers don't exist in these operation modes, because they don't forward traffic at the IP layer. Instead, virtual servers use an OSI Layer 2 bridge, together with the IP-layer port number. This is called a V-zone.

Also, because of differences in how the two modes work, some features that are supported in reverse proxy mode aren't supported in transparent mode. For example, when operating in transparent mode, FortiWeb forwards traffic while inspection is being completed. Therefore, FortiWeb can't rewrite URLs in packets that have already egressed; it can only interrupt connections it detects when an attack is in progress, so transparent and offline protection modes have far fewer leaf objects available for policy configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In offline protection mode, most features are not supported. You would use offline protection mode primarily in the preparation phase, with auto learning to discover applicable signatures and input constraints. When operating in offline protection mode, FortiWeb doesn't pick up traffic on the proxy or bridge. It accepts all traffic on a data capture port, one of the network interfaces, and listens for attacks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Policies

- Usually only one policy is applied to each HTTP/S request
  - Policies can be chained to apply multiple rule sets in sequence
- Determine which connections are allowed or blocked
- Specify which protection policies are applied: how traffic is inspected
- SSL inspection and offloading, if applicable
- If no matching policy exists, behavior is mode dependent:
  - Reverse proxy: non-matching traffic is **denied**
    - Like NAT/route mode FortiGate
  - Other modes: non-matching traffic is **allowed**
    - Easy drop-in solution for transparent modes like MSSP and data centers
    - Less disruptive

NSE Training Institute © Fortinet Inc. All Rights Reserved. 19

When all objects are ready, create a server policy that combines all the leaf objects into one comprehensive group.

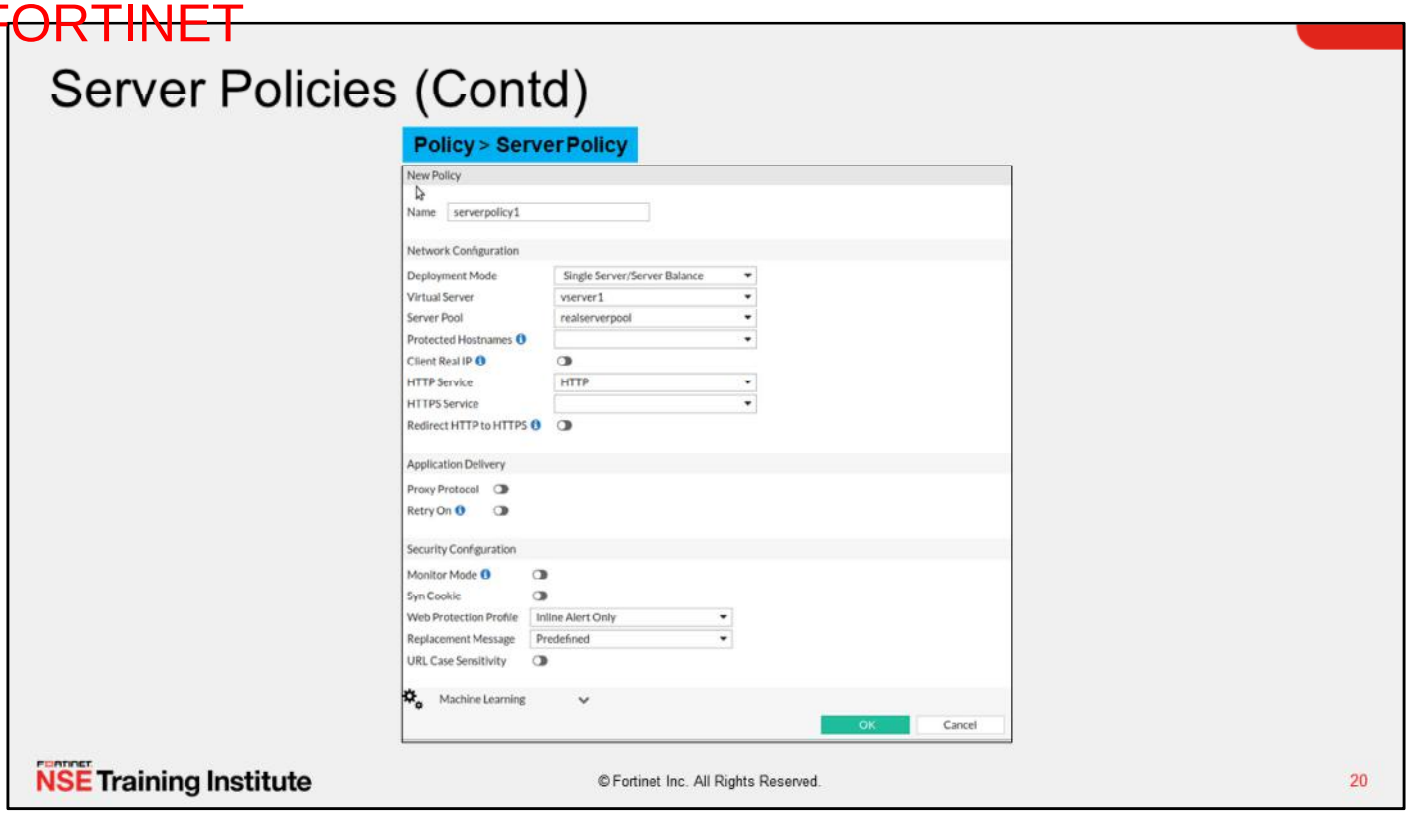
You must use a web protection profile in order to save the policy, regardless of the operating mode.

To test traffic flow in reverse proxy mode, it is recommended that you configure and use the **Alert Only** profile or enable **Monitor Mode**. This will match traffic, and log any attacks that the protection profile detects, but it will not block any traffic. After security and connectivity has been verified, clone and modify the protection profile to begin blocking attacks. Be sure to disable **Monitor Mode** when you are ready to begin blocking.

In transparent mode, remember that just because traffic is allowed, it does not mean it was picked up by the proxy. Transparent mode allows non-matching traffic, by default. To be sure that traffic is matched by a policy, enable and check your traffic logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure server policy for HTTP, HTTPS, and load balancing. If you are configuring policy for HTTPS, to be able to scan secure traffic, you must also configure FortiWeb to decrypt it, and therefore must provide it with the server's certificate and private key.

After you configure the server policy, traffic should pass through FortiWeb to your server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which is not used in a FortiWeb server policy in reverse proxy mode?
   A. Virtual server
   ✓ B. Security policy
   C. Web protection profile
   D. Server pool

2. Which is not used in a FortiWeb server policy in transparent inspection mode?
   A. V-Zone
   B. Web protection profile
   ✓ C. URL rewriting policy
   D. Server pool

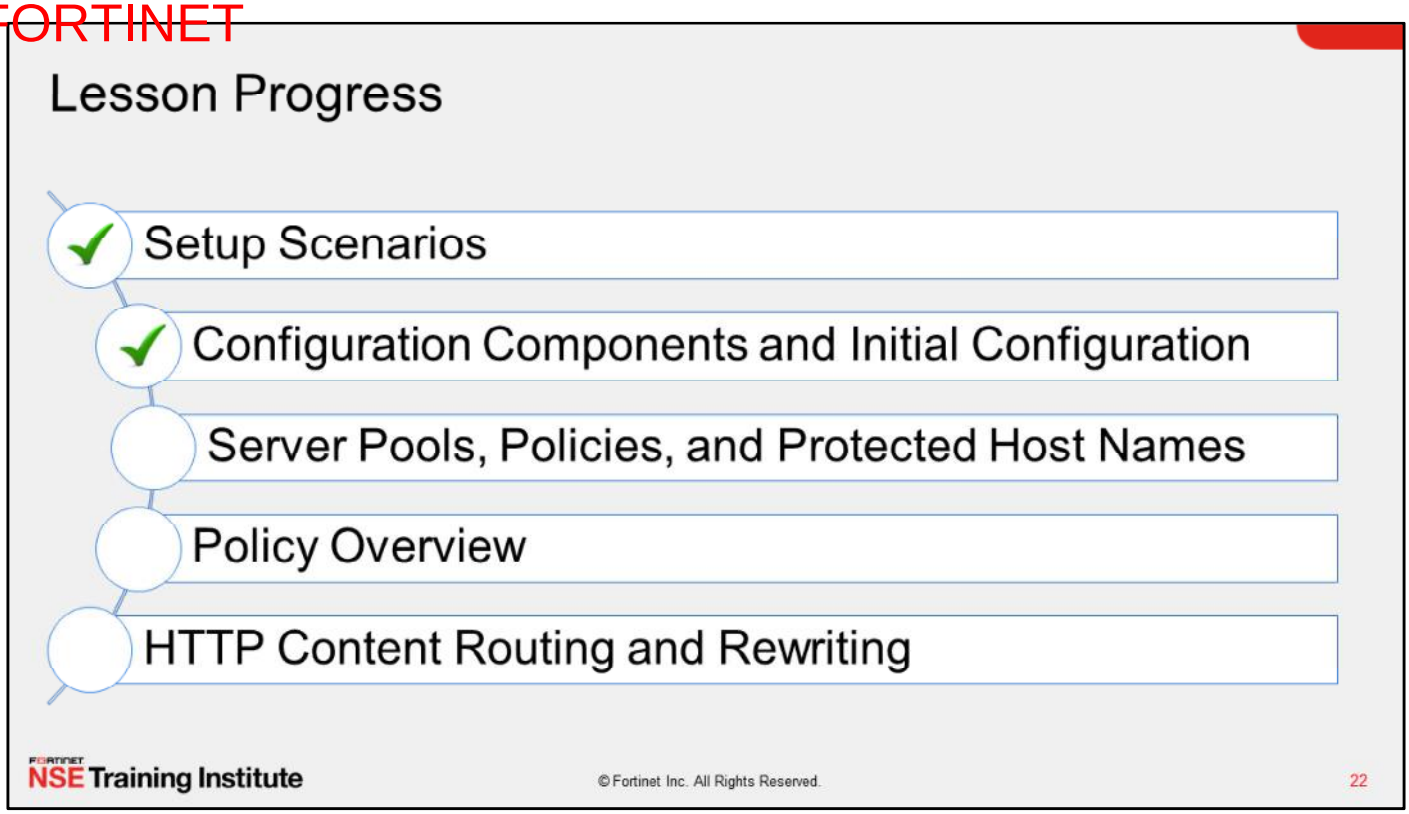
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

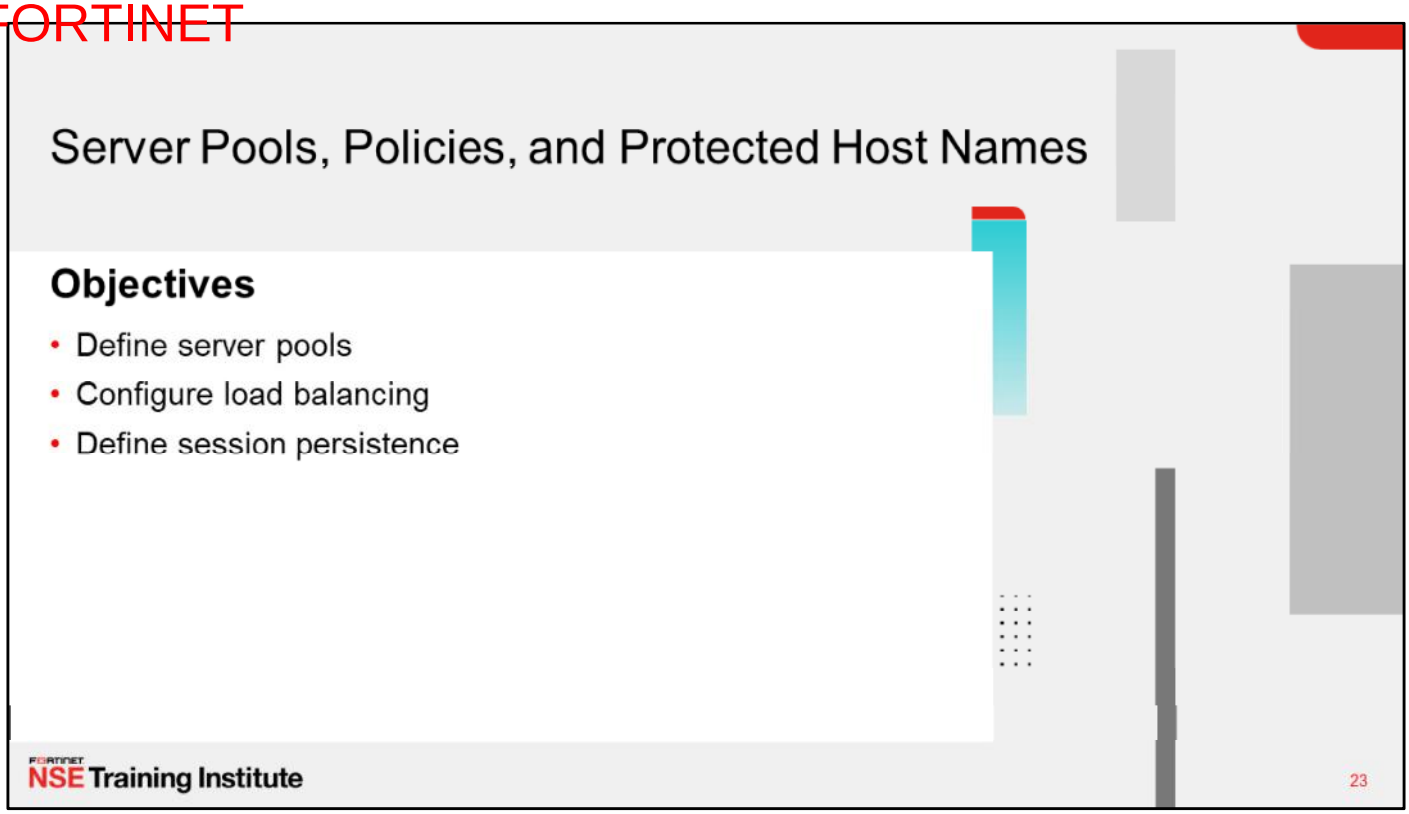


Good job! You now know how to configure FortiWeb for high availability.

Now, you will learn about defining server pools and policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in describing and discussing server pools, load balancing, and session persistence, you will be able to define where FortiWeb directs traffic in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Define Web Server—Server Pools

- In a server pool, define web servers by IP (physical) or DNS
  - **Reverse Proxy Mode**: Traffic is load balanced (forwarded) among the members of the server pool
  - **Offline Protection/Transparent Inspection**: Traffic is passed through to the members of the server pool
- In reverse proxy mode, FortiWeb replies to ARP requests looking for the MAC address of the virtual server IP addresses

Server Objects > Server > Server Pool

NSE Training Institute © Fortinet Inc. All Rights Reserved. 24

One of the first step should be to configure objects representing webservers on the FortiWeb. They can be defined using either a domain name or an IP address.

Server pools define a group of one or more physical or domain servers (web servers) that FortiWeb distributes connections among, or where the connections pass through to, depending on the operating mode.

You define your destination backend web servers by specifying their IP addresses in server pools. Depending on the FortiWeb operation mode, it will either:

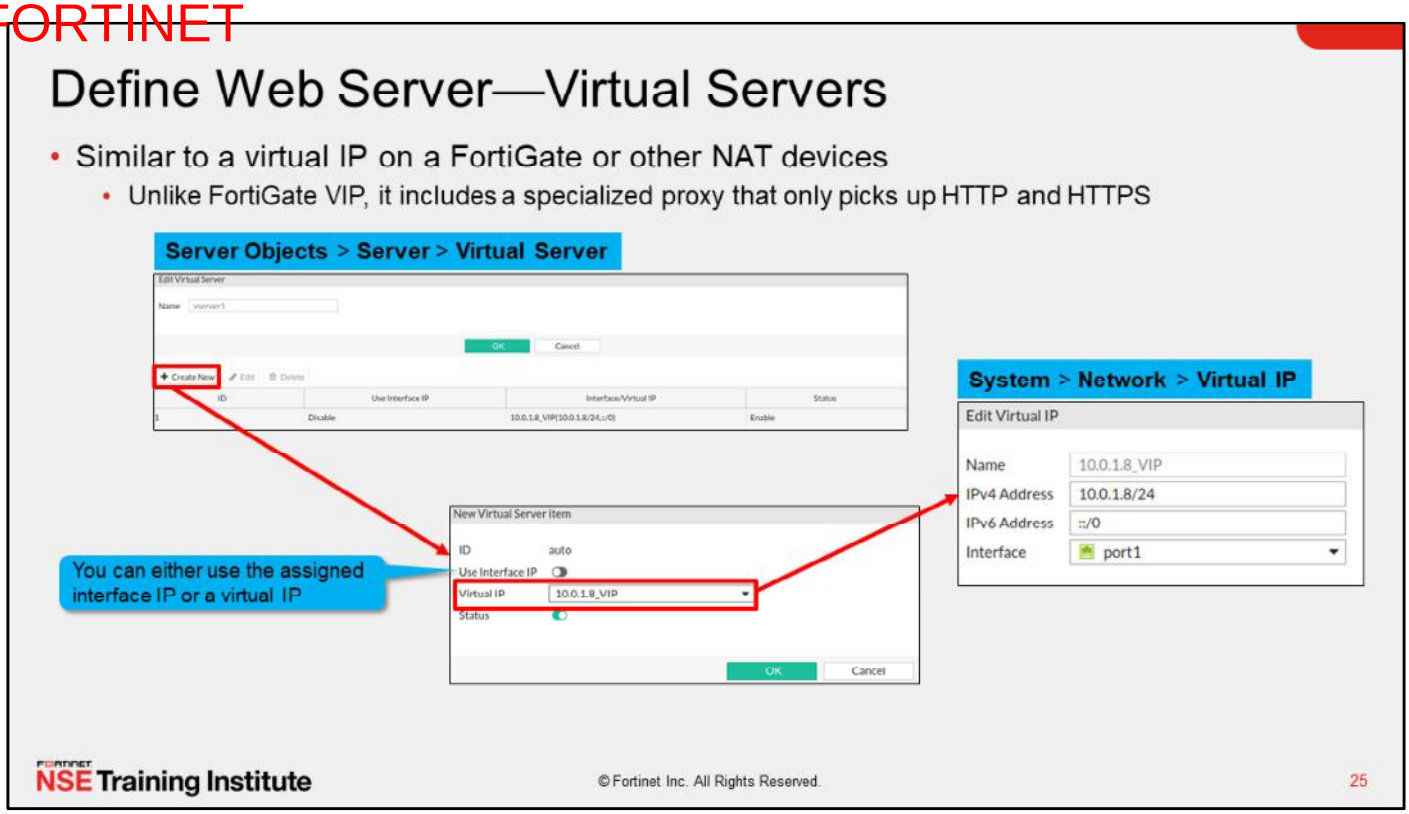
- Forward the frames, if it's operating as a Layer 2, transparent device
- Rewrite the destination IP and distribute it according to your load balancing algorithm, if it's operating in reverse proxy mode

Before configuring an HTTP server pool, you should do the following:

- If clients connect through HTTPS and FortiWeb is operating in a mode that performs SSL inspection, upload the website's server certificate.
- If you want to use the pool for load balancing and want to monitor its members for responsiveness, configure one or more server health checks to use with it.
- If client connections require persistent sessions, create a persistence configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



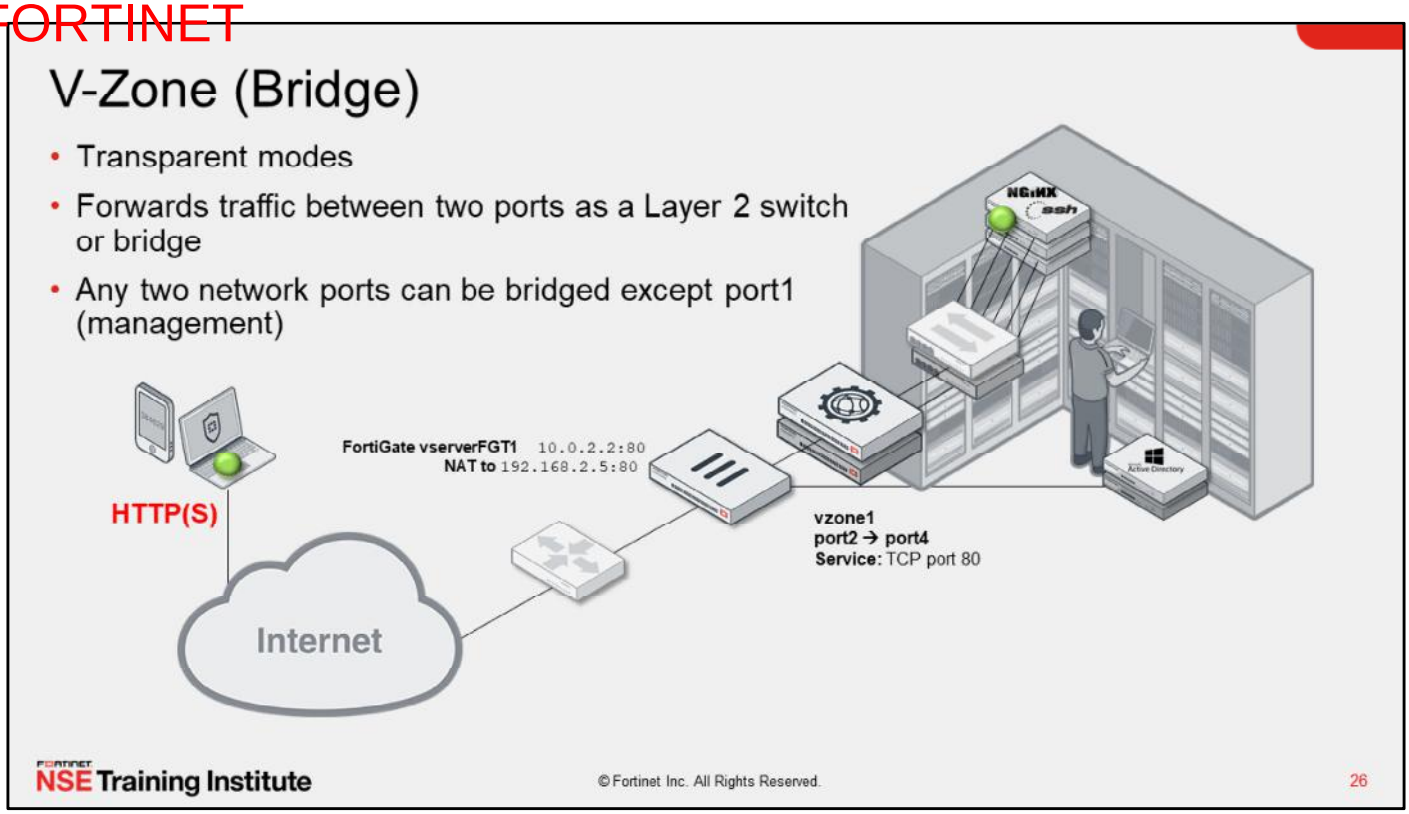
Before configuring a server policy, you must configure a virtual server that defines the network interface or bridge and the IP address where traffic destined for a server pool will be directed to. When the FortiWeb receives traffic destined for a virtual server, it then forwards the traffic to a single web server or distribute sessions among servers in a server pool.

FortiWeb identifies traffic as being destined for a specific virtual server if:

- The traffic arrives on the network interface or bridge associated with the virtual server.
- For reverse proxy mode, the destination address is the IP address of a defined virtual server. (The destination IP address is ignored in other operation modes; however, it must not be identical to the web server's IP address.)

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In transparent mode, FortiWeb acts as a Layer 2 device. So, by default, web traffic passes through. If you want web traffic to be inspected, you must define where FortiWeb should pick up traffic: which bridge and TCP port number. This is a key difference from operating in reverse proxy mode.

In reverse proxy mode, FortiWeb forwards as a Layer 3 device. So, by default, traffic that is not destined for a management IP or virtual server IP is dropped. Web traffic won't flow until you define a virtual server IP and listening port number, as well as the destination server IP. Other, non-web traffic isn't picked up by a virtual server, nor is it destined for FortiWeb itself, so traffic won't flow unless you enable IP-based forwarding (that is, routing).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IP-Based Forwarding

- In transparent mode, non-HTTP traffic passes through automatically
  - Not a Layer 3 router in these modes, simply a bridge or switch
  - FortiWeb does not inspect other protocols, so any traffic should be limited by the upstream gateway
    - SSH brute force and root kits are very common attacks and will NOT be blocked by FortiWeb in transparent mode
- In reverse proxy mode, SSH, RDP, and others are not forwarded to the protected physical servers unless you enable it
  - To enable routing of non-web traffic to your servers:

```
config router setting
  set ip-forward enable
  set ip6-forward enable
end
```

  - FortiGate must forward to web server's IP, not FortiWeb virtual server
    - Only HTTP/HTTPS is picked up by proxy (Virtual Server IP)

NSE Training Institute

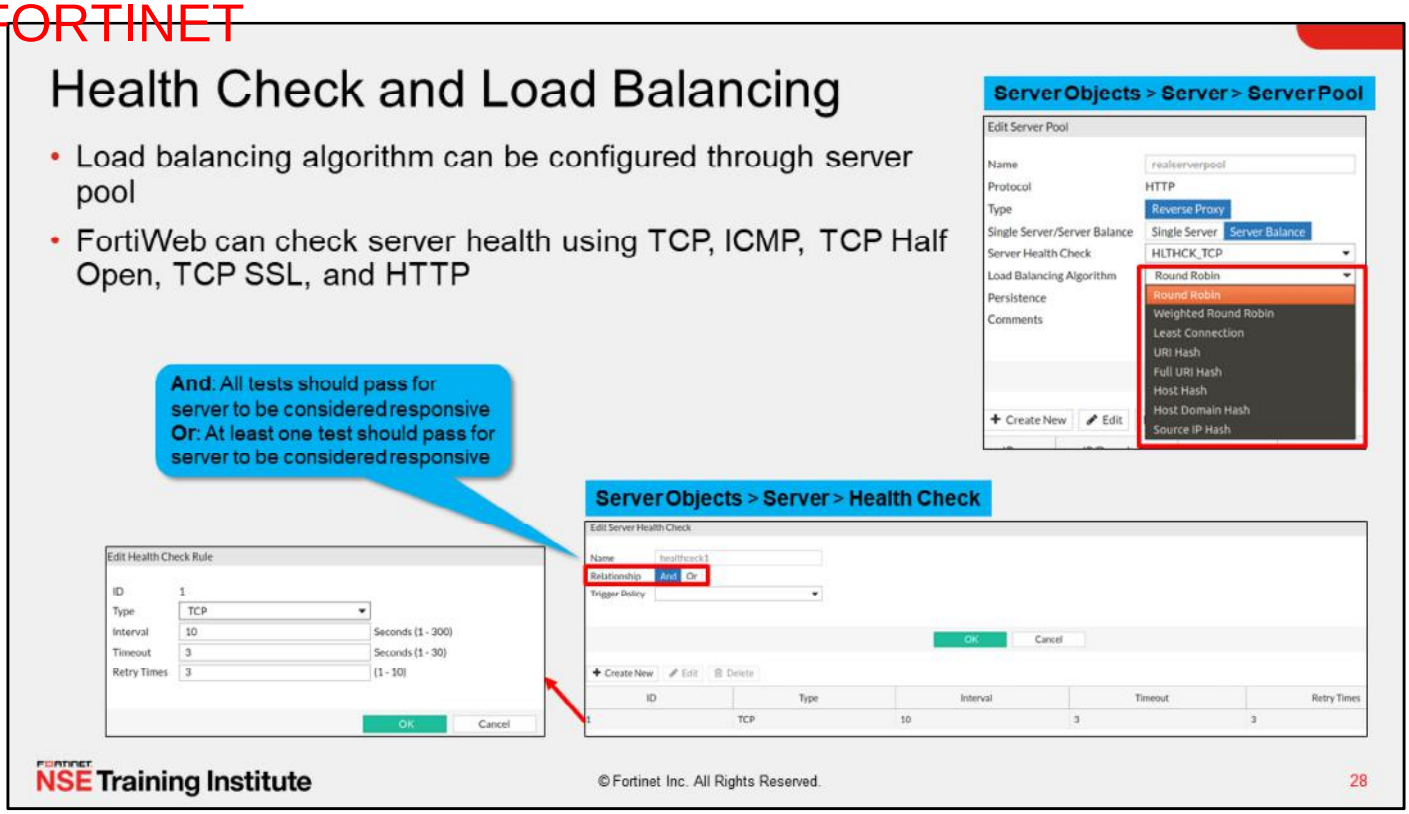
© Fortinet Inc. All Rights Reserved.

27

If you are using transparent mode, no configuration is required. FortiWeb allows all other protocols to pass through. However, if you are using FortiWeb in reverse proxy mode, then you must enable IP-based forwarding (routing) if you want it to transmit other protocols. It is very common for web servers to have secondary services such as RDP or SSH. This allows web developers to update their applications and upload new files. Remember that as a Web Application Firewall, FortiWeb specializes in web protocols. FortiGate and other specialized network routing devices have session helpers for SIP and other dynamic port protocols, but FortiWeb does not. In that case, you may need to adjust your topology so that FortiWeb is not a router hop.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Load balancing on FortiWeb is like load balancing on FortiGate, but with the addition of web-specific methods. This is useful since HTTP has its own sessions, and sometimes different web servers are dedicated to hosting specific web apps.

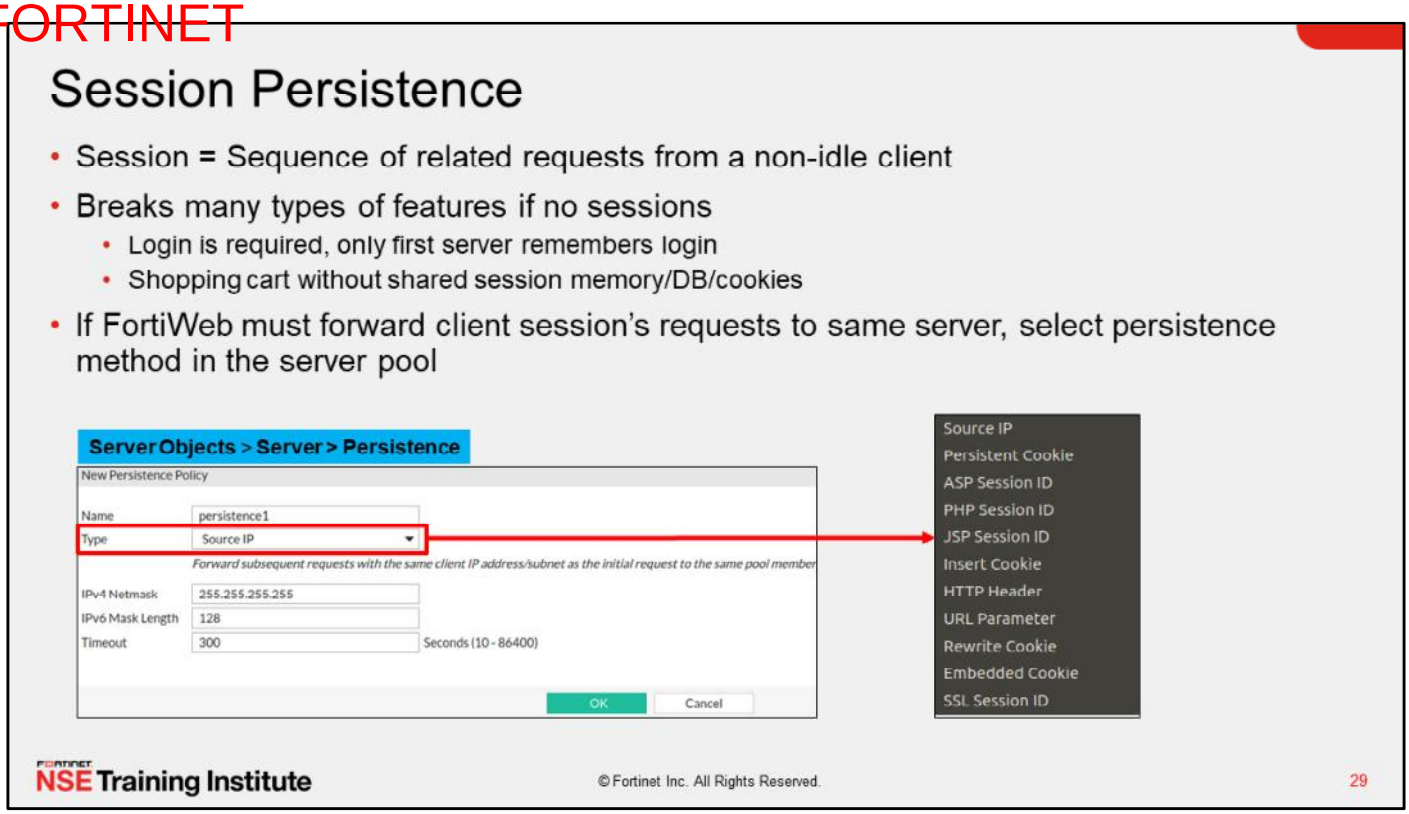
When the status of a physical server in a server pool is disabled, a health check indicates it is down, or it is manually removed from the server pool, FortiWeb will transfer any remaining HTTP transactions in the TCP stream to an active physical server in the server pool according to the load balancing algorithm. If you specify a persistence method for the server pool, after an initial client request, FortiWeb routes any subsequent requests according to that method.

Tests for server availability poll web servers that are members of a server pool to determine their responsiveness before forwarding traffic. FortiWeb reacts to unresponsive servers by disabling traffic to that server until it becomes responsive.

To simplify health check creation, FortiWeb provides predefined health checks for each of the available protocols.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you make the initial load balancing decision, by default, each subsequent request could be sent to a different web server, according to the algorithm. If you don't want this to happen—for example, if your users log in and only that server can associate the next request with that login—then you must configure session persistence.

You can define session persistence in several ways, using either the IP or HTTP layer. This is similar to FortiGate. If you want to use a session cookie-based method, the most efficient way is to use one of your app's own session cookies. If your session doesn't have a cookie, FortiWeb can inject its own load balancing session cookie, and use it to track the sessions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Protected Hostnames

- IP addresses and FQDNs
- Defines virtual and real web hosts according to the `Host` field inside HTTP header
  - For example, Apache virtual host

```
GET /index.php HTTP/1.1
Host: www.example.com
```

- Should contain *all* virtual IPs and domain names that clients should be able to enter in their browser's URL bar
  - In a server pool, a domain name is often a private DNS and is *not* resolvable or routable on the internet
  - Protected hostnames usually *are* resolvable on the Internet

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

Protected host names can be domain names, but they can also be IP addresses. You should add all host names that clients use, or that DNS could resolve to.

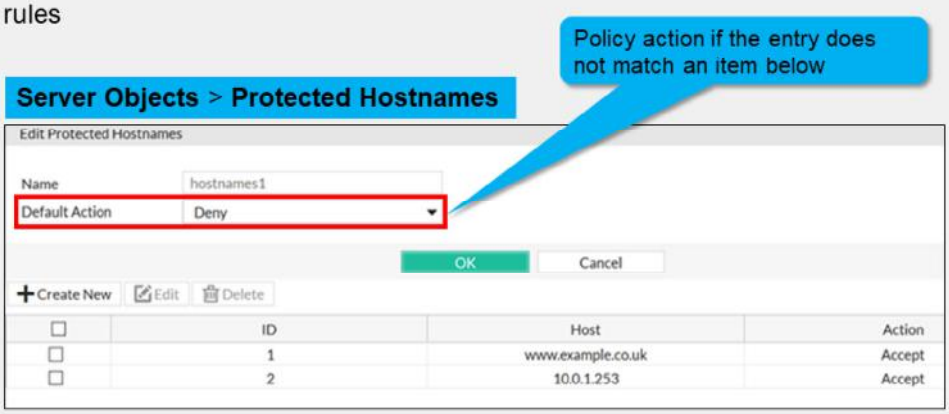
Protected host names can be used in the server policy to filter which traffic matches. They can also be used to restrict matching in component objects, such as URL rewrites, and for HTTP content routing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Protected Hostnames (Contd)

- Also used by rules to apply to specific requests:
  - Input validation rules
  - Start page rules
  - Page order rules
  - IP lists
  - HTTP authentication rules
  - Hidden fields rules



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

Here's an example of how you can use a protected host names definition to deny all requests that are not for either `www.example.co.uk` or `10.0.1.253`.

When applied in a server policy, a reverse proxy FortiWeb would block a request to `http://example.co.uk` because it is not an exact match. If you want to accept that variant and forward it to your web servers, then you would add that host name to the list and select **Accept** in the **Default Action** drop-down list. The request could still be blocked by a later scan—antivirus, for example—but it would not be because of the host name.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which one can be used to define a protected host?
   A. NETBIOS name
   ✓ B. Domain name

2. Why is session persistence important for web traffic?
   ✓ A. To ensure that all connections from the same client go to the same server
   B. To ensure that WAF knows which connections to block
   C. To ensure that web servers get a balanced number of connections

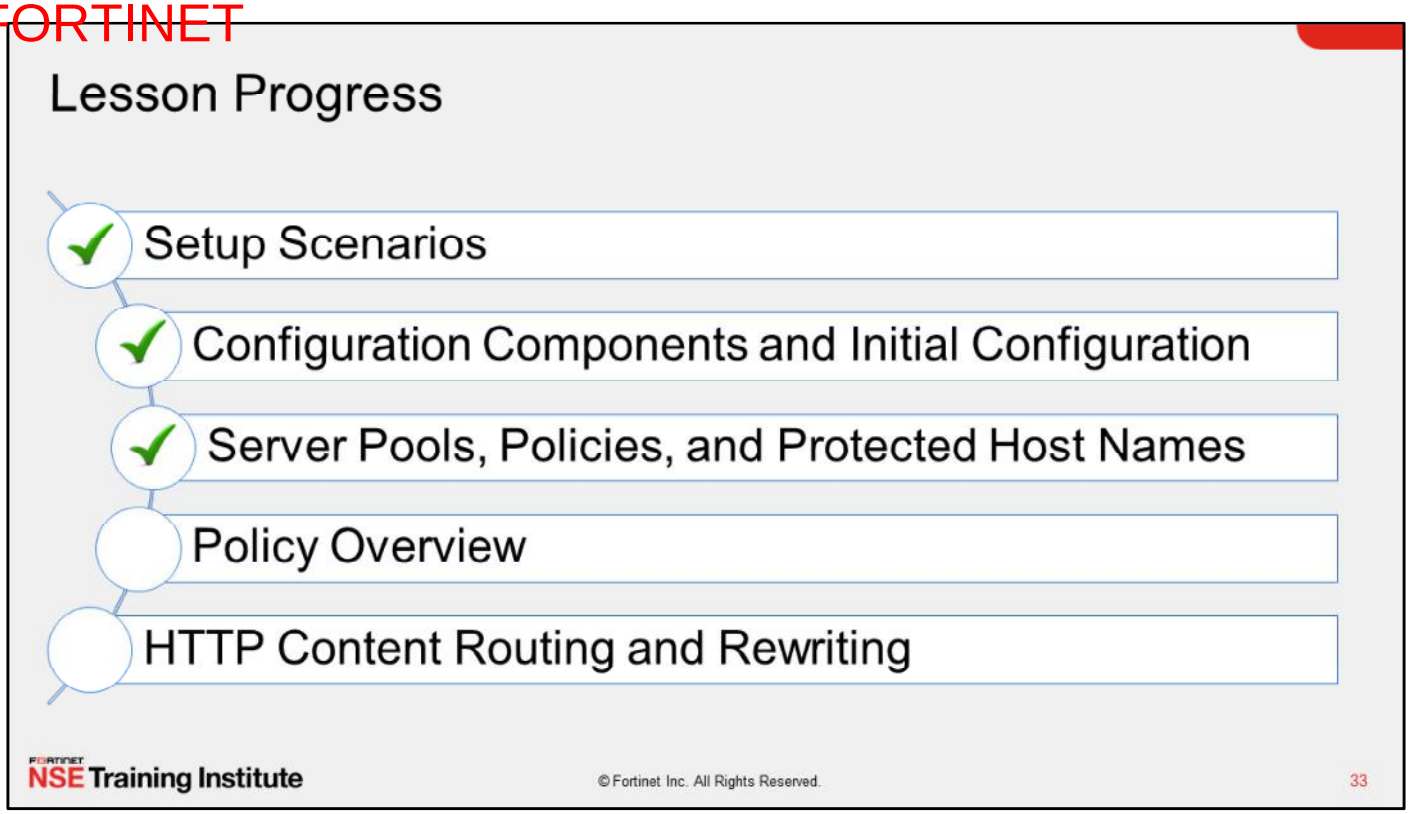
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

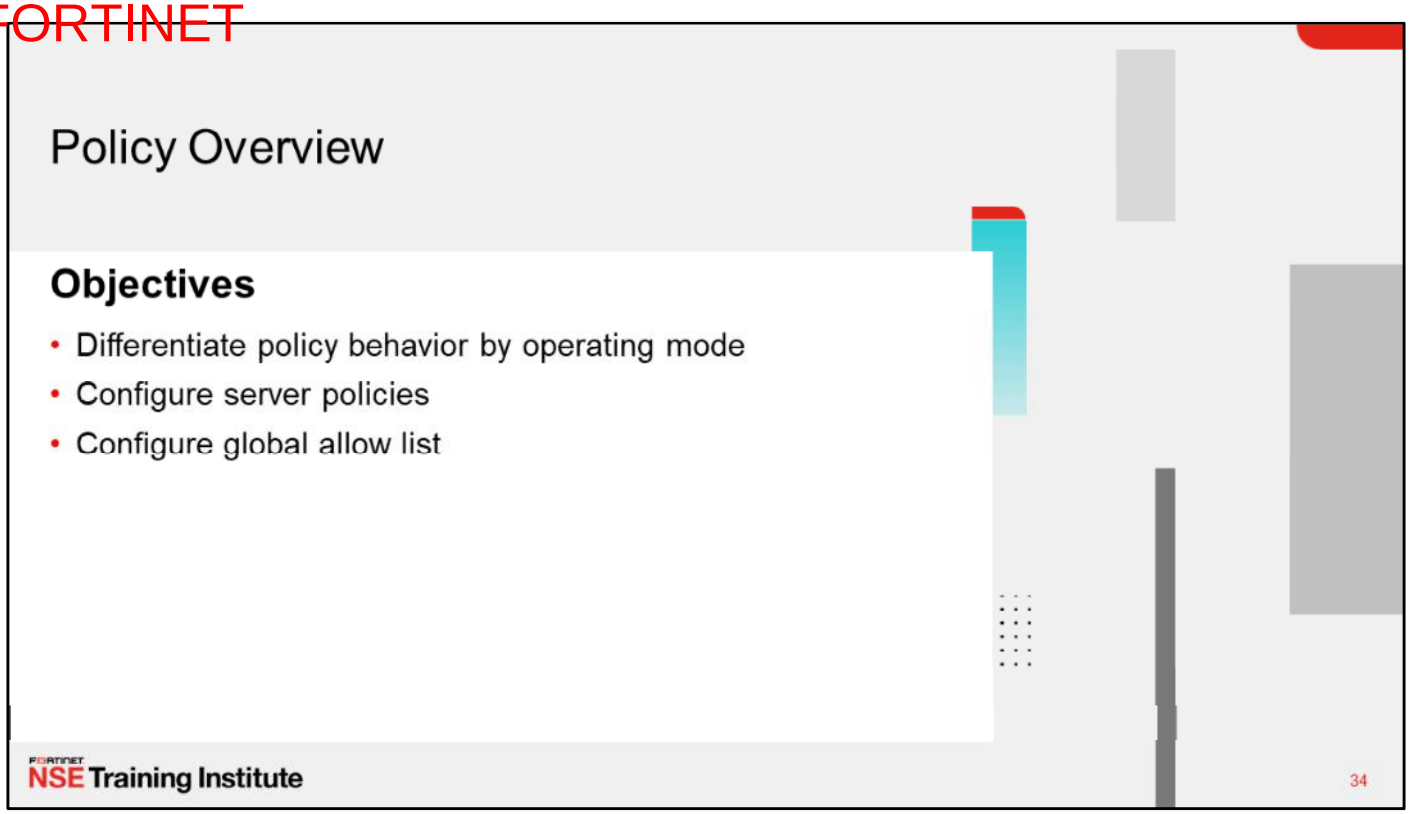


Good job! You now understand how to configure a server pool and policies, as well as how to define protected host names.

Now, you will learn how to configure server policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding policy overview, you should be able to configure server policies and pass monitored and secured traffic to your servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Policy Behavior by Operating Mode

	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection	WCCP
Matches by	• Service • Virtual server	• Data capture port • Server pool	• V-zone (bridge) • Server pool	• V-zone (bridge) • Server pool	• Server port • Virtual server
Violations	• Block • Modify	• Attempt to block by sending TCP reset	• Block • Modify	• Attempt to block by sending TCP reset	• Block • Modify
Profile support	• Inline protection profiles	• Offline protection profiles	• Inline protection profiles	• Offline protection profiles	• Inline protection profiles
SSL	• Offloading • Optional re-encryption	• Inspection only	• Inspection only	• Inspection only	• Inspection only
Forwarding	• Forwarding to a single server • Load balancing to server pool	• Pass-through to server pool member	• Pass-through to server pool member	• Pass-through to server pool member	• Pass-through to server pool member

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

The blocking method and attack protection used varies by operation mode, but so does traffic forwarding and SSL offloading or inspection. This table provides a summary; but if you need a specific feature, check the documentation to make sure that the required feature is supported.

If a TCP connection does not match any of the policies, FortiWeb either refuses the connection (if it is operating in reverse proxy mode) or denies the connection (if it is operating in other operation modes). Even if the TCP connection has a matching policy and is allowed, subsequently, if the HTTP/HTTPS request is not allowed by the policy's profiles, it is considered to be in violation of the policy, and the client may be blocked at the application (request) level or connection level, depending on the action that you configure.

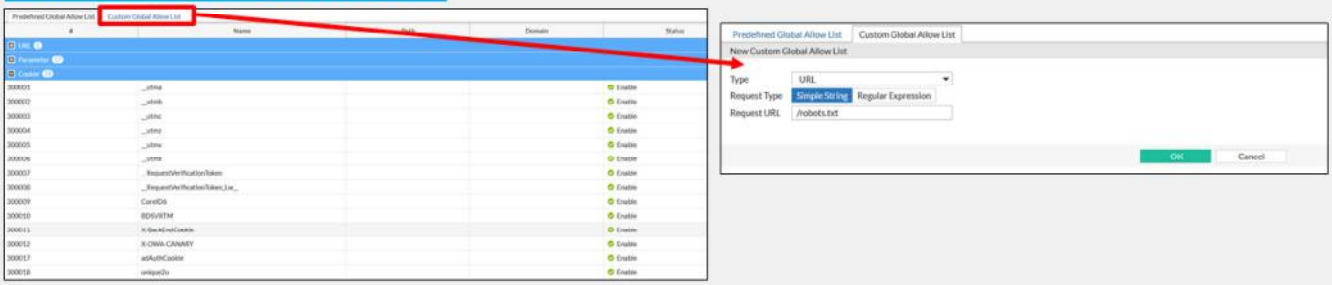
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Global Allow List

- Predefined global allow lists includes list of common internet entities:
  - Google analytics cookies such as `_utma`
  - AJAX parameter such as `_LASTFOCUS`
- Items included in global allow list will be ignored when FortiWeb enforces policies
- FortiGuard updates the predefined global allow list
- Reduces false positives and improves performance

Server Objects > Global > Global Allow List



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

When enabled, items on the allow list will skip the subsequent scans after the global allow list is processed, improving performance. You can also allow list your own custom URLs, header field, cookies, and parameters on the **Custom Global Allow List** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Client Management

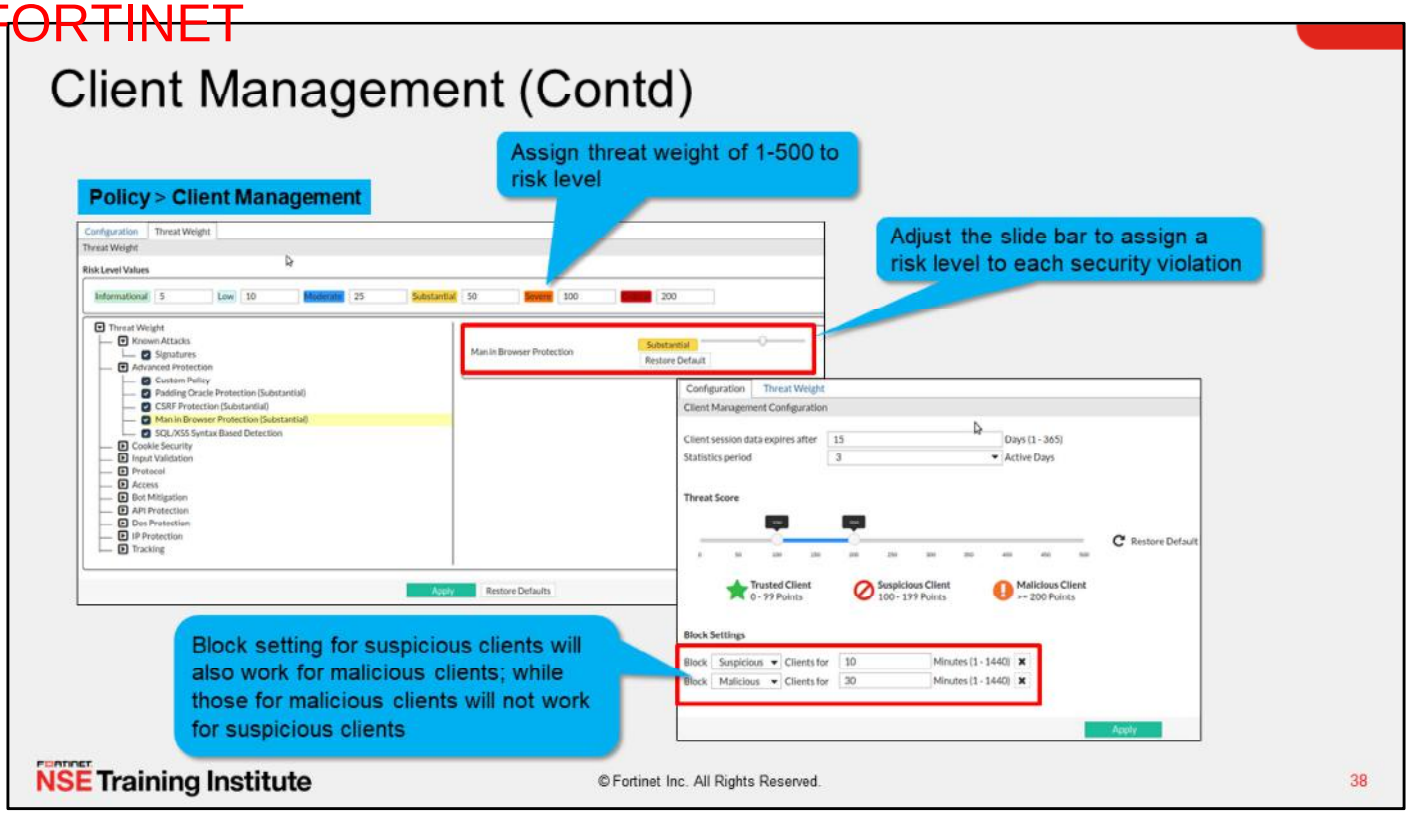
- Identifies suspected attacks based on the clients
- Track client by either the recognized cookie or the source IP
- Client management considers following factors:
  - Threat weight of security violations
  - Threat score of a client
  - Risk level of a client
  - Blocking action based on risk level
- View each client that FortiWeb tracks under **Monitor > Client Management**

NSE Training Institute © Fortinet Inc. All Rights Reserved. 37

When a client triggers a threat, FortiWeb accumulates the threat score based on the configured threat weight value. When the client's threat score reaches a certain threshold, a corresponding blocking action is performed. To identify a visiting client, FortiWeb generates a unique client ID according to the cookie value or source IP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Under the **Threat Weight** tab, configure risk level values, depending on how serious a security violation is. You can use the default values and later adjust them according to specific security concerns.

To define the threat score and violation actions, configure the settings under the **Configuration** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. In which operating mode does FortiWeb offer both the ability to offload SSL as well as the ability to re-encrypt SSL?
   A. True transparent proxy
   ✓ B. Reverse proxy

2. Which operating mode allows the blocking of connections directly (not using a TCP reset packet)?
   A. Offline protection proxy
   ✓ B. True transparent proxy
   C. Transparent inspection mode
   D. Transparent blocking mode

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Progress

- ✓ Setup Scenarios
- ✓ Configuration Components and Initial Configuration
- ✓ Server Pools, Policies, and Protected Host Names
- ✓ Policy Overview
- HTTP Content Routing and Rewriting

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

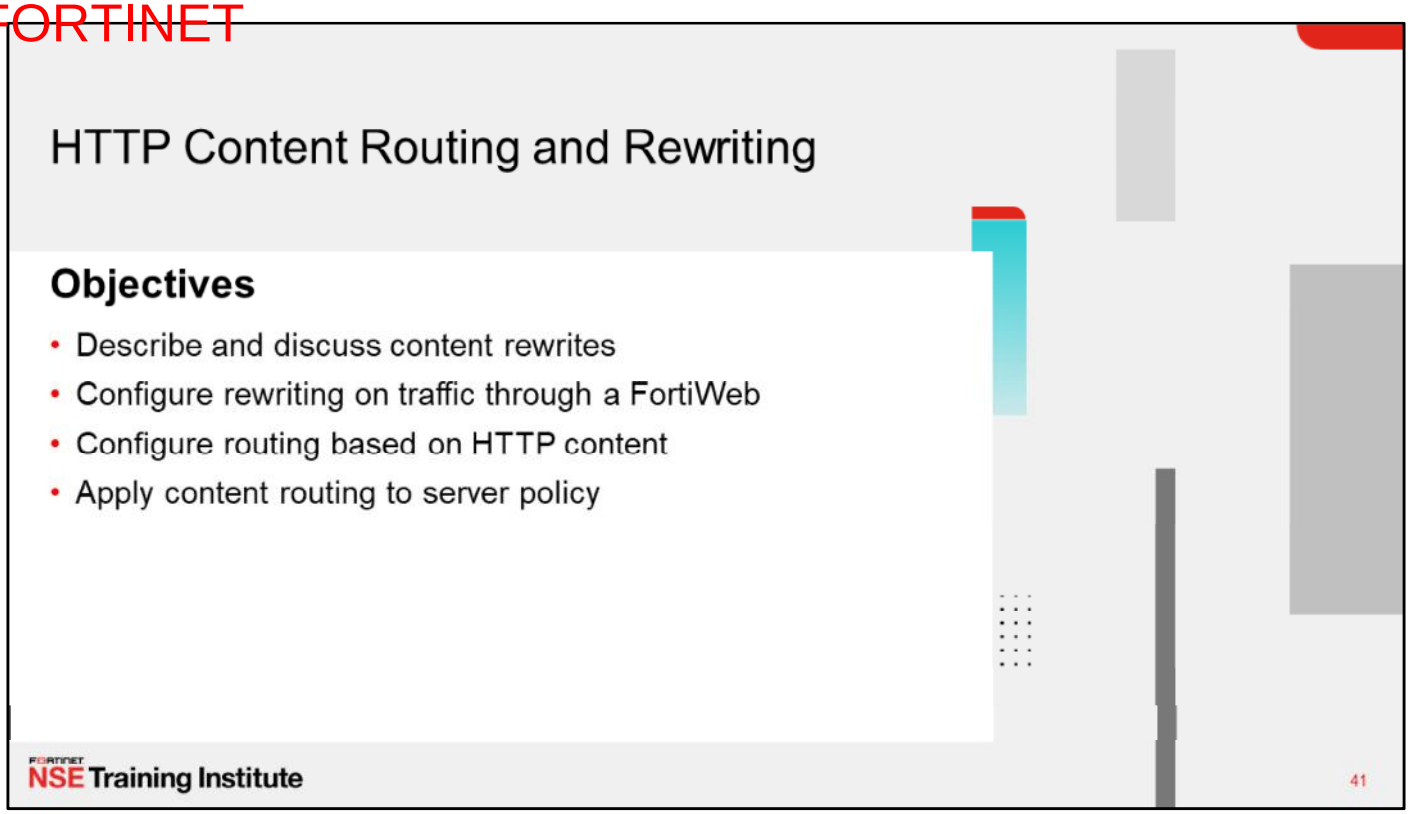
Good job! You now understand how FortiWeb can handle non-HTTP traffic.

Now, you will learn about HTTP content routing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in HTTP content routing, you should be able to route traffic based on HTTP contents.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Why Rewrite?

- Caches often don't work if the URL has parameters
- Human-readable URLs are easier to remember
  - Search engines give these a better rank
- Translate public Internet DNS names to private network hosts
  - `store.example.com` to `nginx1.example.com`, and so on
- Access control
  - Return copyright notice if other sites are hot linking
  - Return `403 Forbidden`
- Cloak information disclosure
  - Don't show .asp, or similar file names
  - Don't show `/drupal`, or similar folder names
- Replace vulnerable functions
- Sanitize responses during post-compromise cleanup
  - Protect your clients from DB-stored XSS attacks

NSE Training Institute © Fortinet Inc. All Rights Reserved. 42

When FortiWeb is inline, it can do more than intercept. It can modify HTTP traffic. If FortiWeb rewrites absolute links to use the HTTPS address, then the client will only be redirected the first time, when they begin a browsing session.

Rewriting HTTP is a common option on Apache, IIS, and other web servers, so rewrites may be familiar to you. But if the regular expressions being used for the rewrites are complex, they can require significant processing time. So, if your server is spending most of its processing time on rewrites, instead of querying the database and building the web page, you may be able to improve performance by offloading the rewrites to FortiWeb.

There are many more reasons why administrators might rewrite traffic. Rewriting is sometimes required for the web app to work. For example, your internet DNS records might refer to public host names that don't match the web servers host names on your private network, such as www1 or www2. Rewriting can also be used to improve security.

For example, FortiWeb can return 403 error codes to URLs that should not be publicly available instead of forwarding the web page from the server. It can also cloak server information disclosure in headers and in the body. If your web servers have already been compromised, FortiWeb can proactively sanitize responses to safeguard your users while your incident response team makes a retroactive intrusion analysis. But even better, FortiWeb can patch security holes in your applications on the fly, replacing vulnerable functions with safe ones.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Finding More Regex for Rewrites

- *FortiWeb Administration Guide: Appendix E*

Appendix E: Regular expressions 880

Popular FortiWeb regular expression syntax

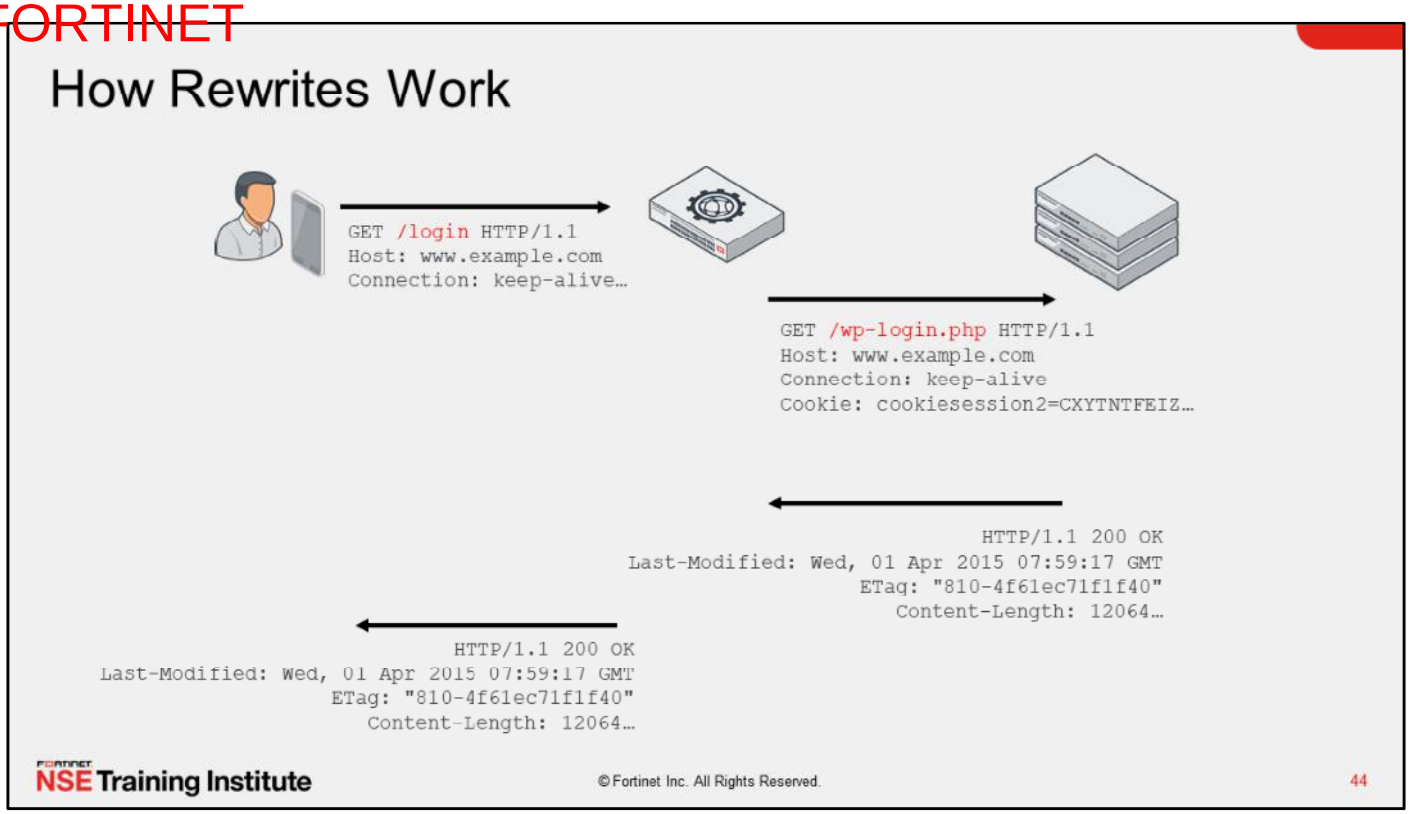
Notation	Function	Sample Matches
Anything **except** *.|^$?+\(){}[]	Literal match, **except** if the character is part of a: • Capture group • Back-reference (e.g. $0 or \1) • Other regular expression token (e.g. \w)	**Text:** My cat catches things. **Regular expression:** cat **Matches:** cat Depending on whether the feature looks for all instances, it may also match "cat" in the beginning of "catches".
\	Escape character. If it is followed by: • An alphanumeric character, the alphanumeric character is **not** matched literally as usual. Instead, it is interpreted as a regular expression token. For example, \w matches a word, as defined by the locale. • Any regular expression special character: *.|^$?+\(){}[]\ this escapes interpretation as a regular expression token, and instead treats it as a normal letter. For example, \\ matches: \	**Text:** /url?parameter=value **Regular expression:** \?param **Matches:** ?param

NSE Training Institute © Fortinet Inc. All Rights Reserved. 43

If you need to rewrite HTML tags or UTF-8 encoded domain names, there are specific regular expression examples that you can copy or modify from the *FortiWeb Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you configure a rewrite, you first indicate the direction of the traffic:

- HTTP request?
- HTTP reply?

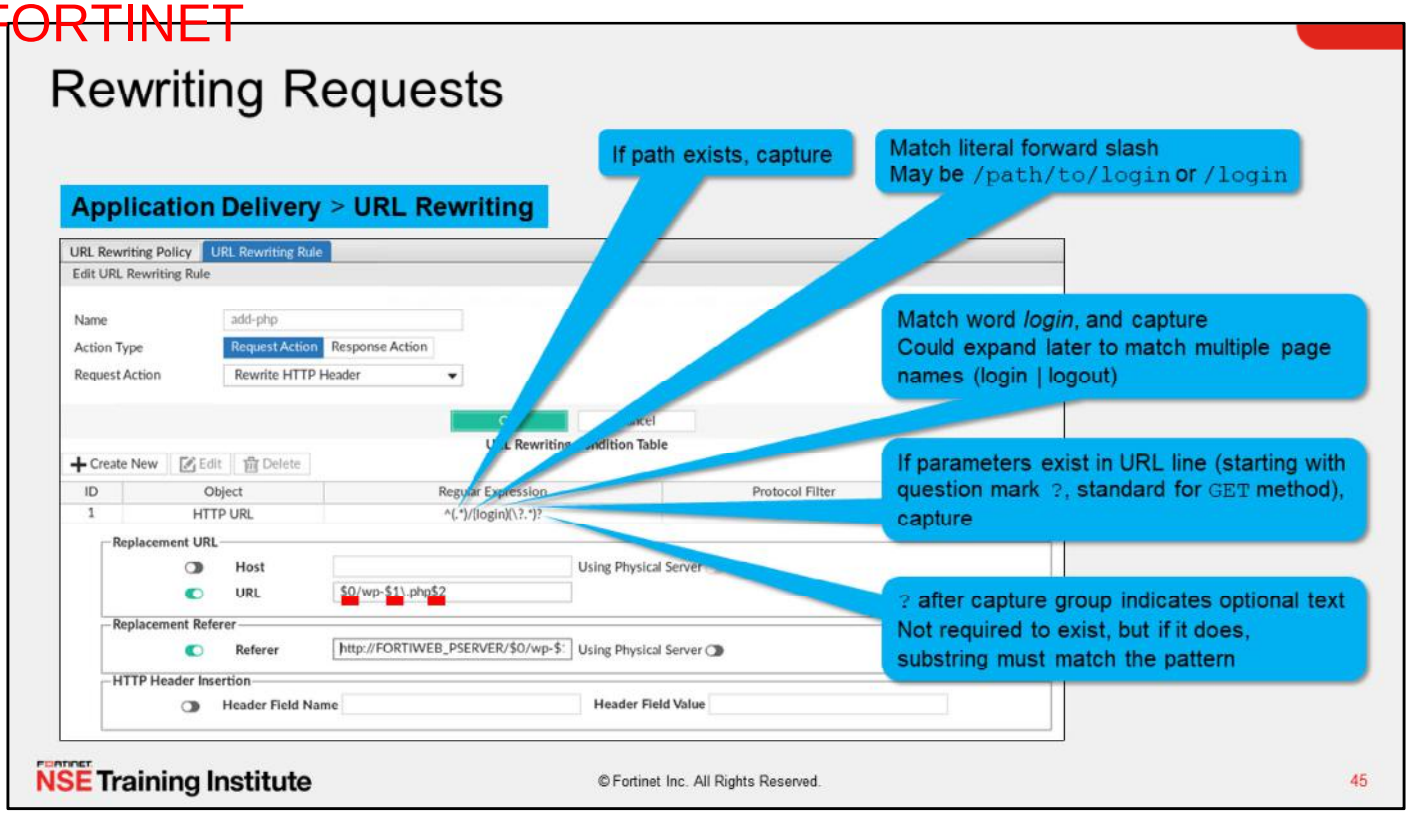
Requests and replies have different HTTP headers and content, so the options are different, too.

When evaluating traffic for a match with your rewrite policy, FortiWeb doesn't necessarily test for incoming or outgoing, relative to the packet's source IP and your defined server pools. Unlike FortiMail, FortiWeb doesn't need to. That's because the headers and content of requests and replies are different.

So, regardless of direction, FortiWeb HTTP parser dissects the traffic. It splits it into its header fields and body. It stores each part in a buffer. Then, depending on your rules, FortiWeb rewrite engine looks for the corresponding buffer, and evaluates it for a match. If the traffic meets all match conditions, then FortiWeb rewrites the specified parts of the HTTP layer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Look at the match conditions in this slide. Can you guess which URLs will match? What are the capture groups? What is the output?

This example is attempting to hide the `.php` file extension and WordPress-specific login URL from clients. This helps to prevent attackers from fingerprinting your server's software stack. It also means that, if you change your application to movable type or Drupal, the following will be true:

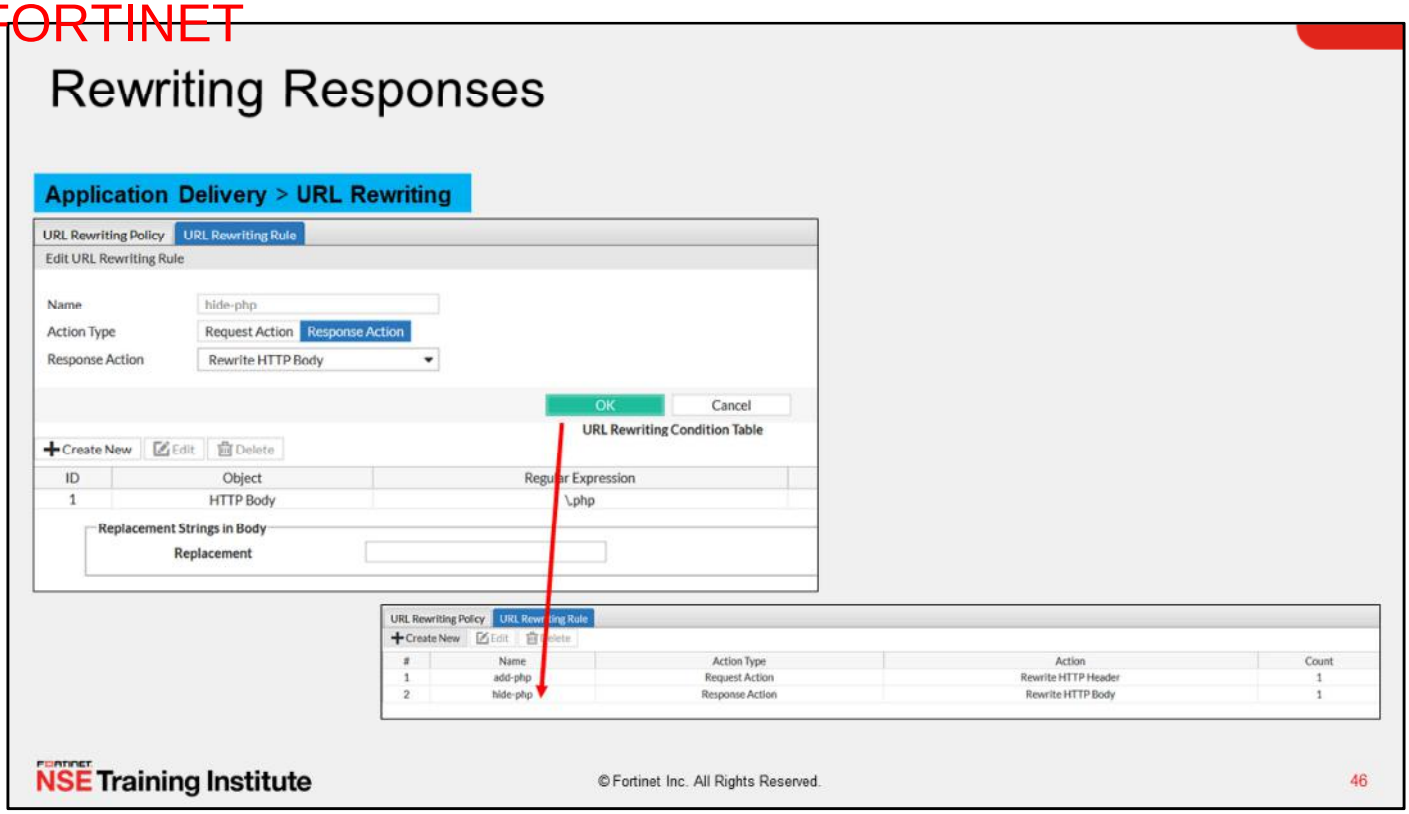
- People won't need to fix their browser bookmarks.
- You won't have to configure any redirects to avoid 404 errors.

To make this work, you need two rules:

- One to translate the incoming request's URL to its real, server-side URL (which is shown here)
- One to translate hyperlinks in the reply to platform-agnostic URLs

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On the left side, you can see the second rule. It scans the reply body—which could be HTML or JavaScript—and removes all instances of .php before FortiWeb forwards it to the client.

To apply your rules, you group them in a URL rewriting policy, then select them in the protection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HTTP Content Routing

- Also known as Layer 7 Routing
- Based on HTTP, not MAC address
- One or multiple match conditions
  - `Host:` header
  - URL (HTTP request)
  - Previous URL per header (HTTP referer)
  - Cookie
  - Source IP
    - Like PBR, but with extra HTTP-based match features
- Forwards requests to a specific server or server pool that each host different web apps, virtual hosts, sessions, localizations, and so on
  - Each server pool has a logical function
    - Could be a cloud or CDN
  - More fine-grained delivery control *without* chaining policies

NSE Training Institute © Fortinet Inc. All Rights Reserved. 47

FortiWeb has static and policy-based Layer 3 routes, like many network devices. They match traffic based on the IP layer's source and destination. But FortiWeb can also route based on HTTP content (Layer 7).

Like other load balancing methods, HTTP content routing can avoid servers that are down for maintenance. It can also distribute TCP connections among servers in the pool. But unlike the other load balancing methods, with HTTP content routing, you may have multiple server pools. Each one has a logical function.

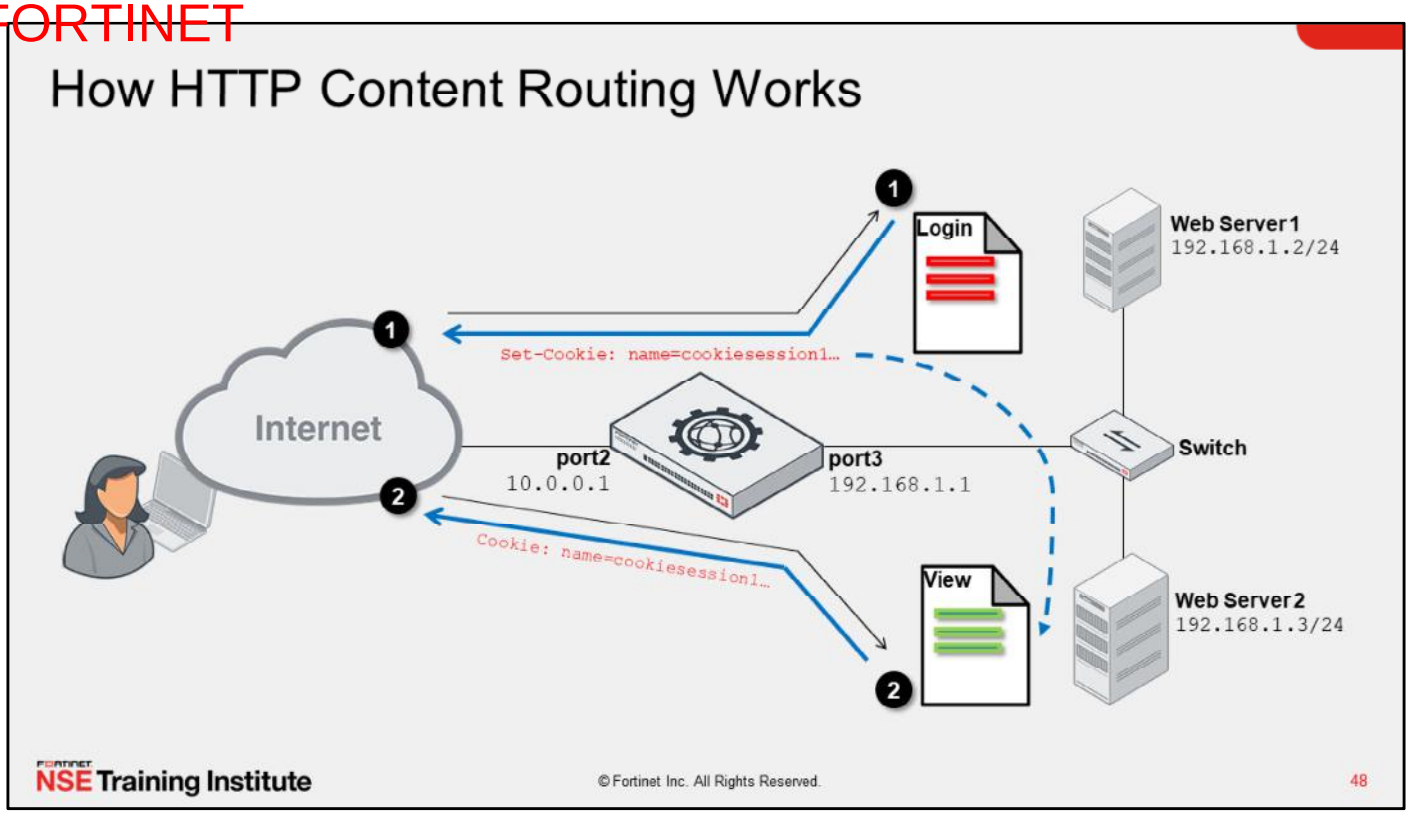
For example, some servers might host only SharePoint, and others might host only Outlook Web App, while a third server pool hosts both your e-commerce storefront and CRM portal. Depending on which web app the client asks for, FortiWeb would route the request to the appropriate server pool.

HTTP content routing can match based on criteria that are also rewritable:
- Host
- URL
- Referer

If both HTTP rewriting and contenting routing is being used, be very careful of your match conditions. Do your match criteria look for the initial URL, or the rewritten one? If the interactions are complex, it can help to look at the sequence of scans section of the *FortiWeb Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows an example of HTTP content routing based on the `Cookie` HTTP header.

When a user goes to the website, at first, they don't have any session ID. You must configure a rule on FortiWeb that directs the first page request to a login server, which assigns a session ID.

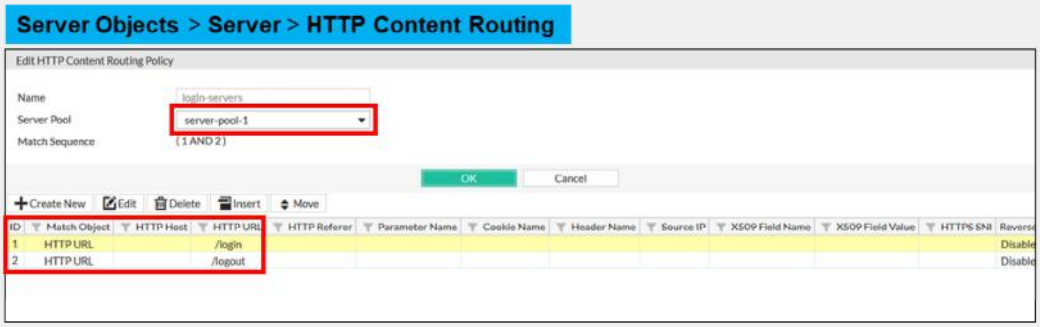
By directing a user to a login server, you can use the login server as a logical controller. The login server inserts a session ID with a number in a range that always belongs to Web Server2, or Web Server3, and so on. On FortiWeb, you must configure an HTTP content routing rule that routes requests with each range of session IDs to their assigned servers. FortiWeb forwards the next request and all subsequent requests to the same backend server. This provides HTTP session persistence, and it can do the same for a logical group—a server pool—not just for a single server.

Because each server can host different web applications, FortiWeb allows you to select a separate protection profile for each one. So, in the case of HTTP content routing, a policy may use multiple protection profiles.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Defining Route Matches and Destinations



NSE Training Institute

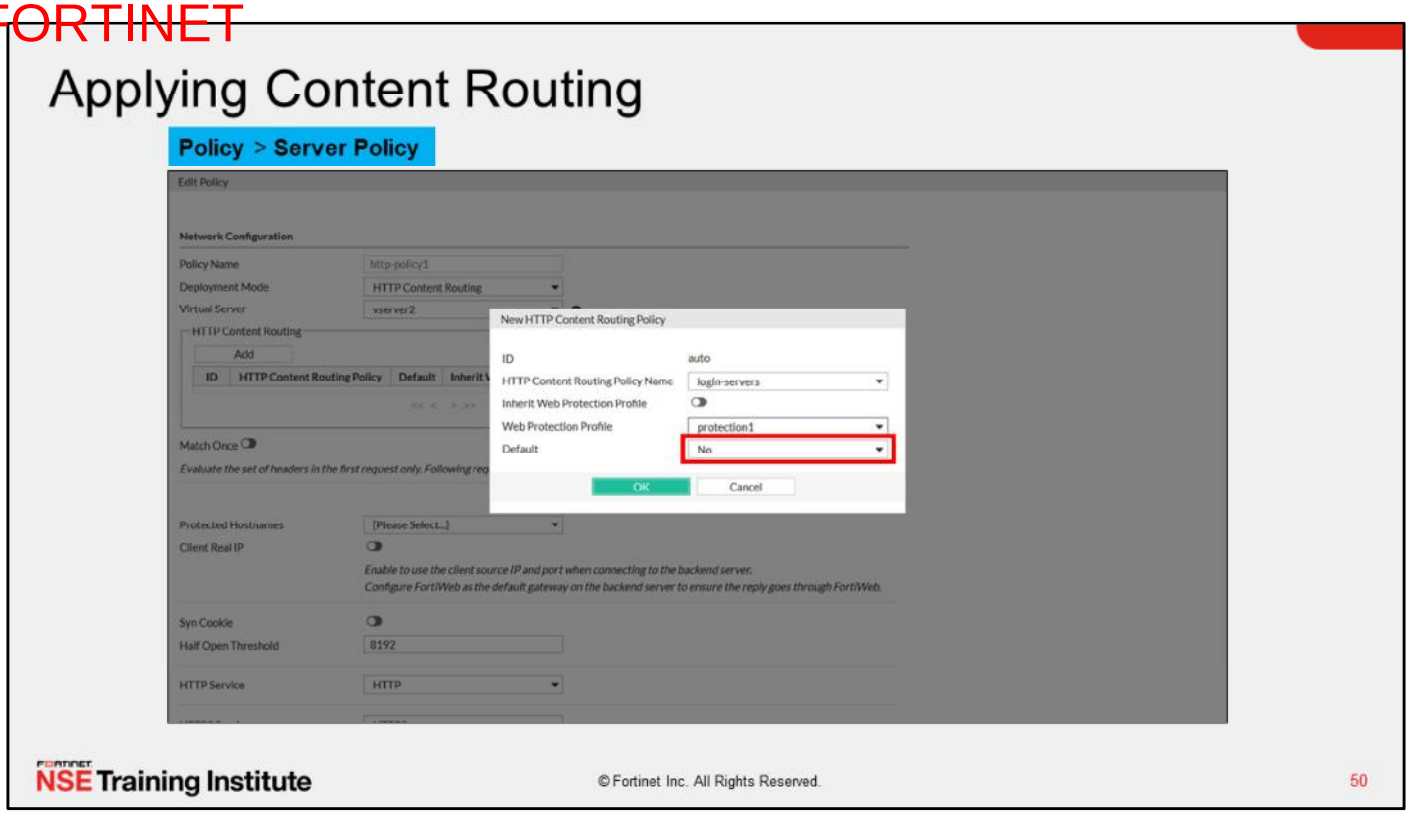
© Fortinet Inc. All Rights Reserved.

49

Now you will learn how to configure content routing. Begin by configuring your server pools. Each server pool will be a separate target of traffic that matches the HTTP content route. The next step is to configure the content routes themselves.

Vouchers & Dumps are Available | WhatsApp +201224560923

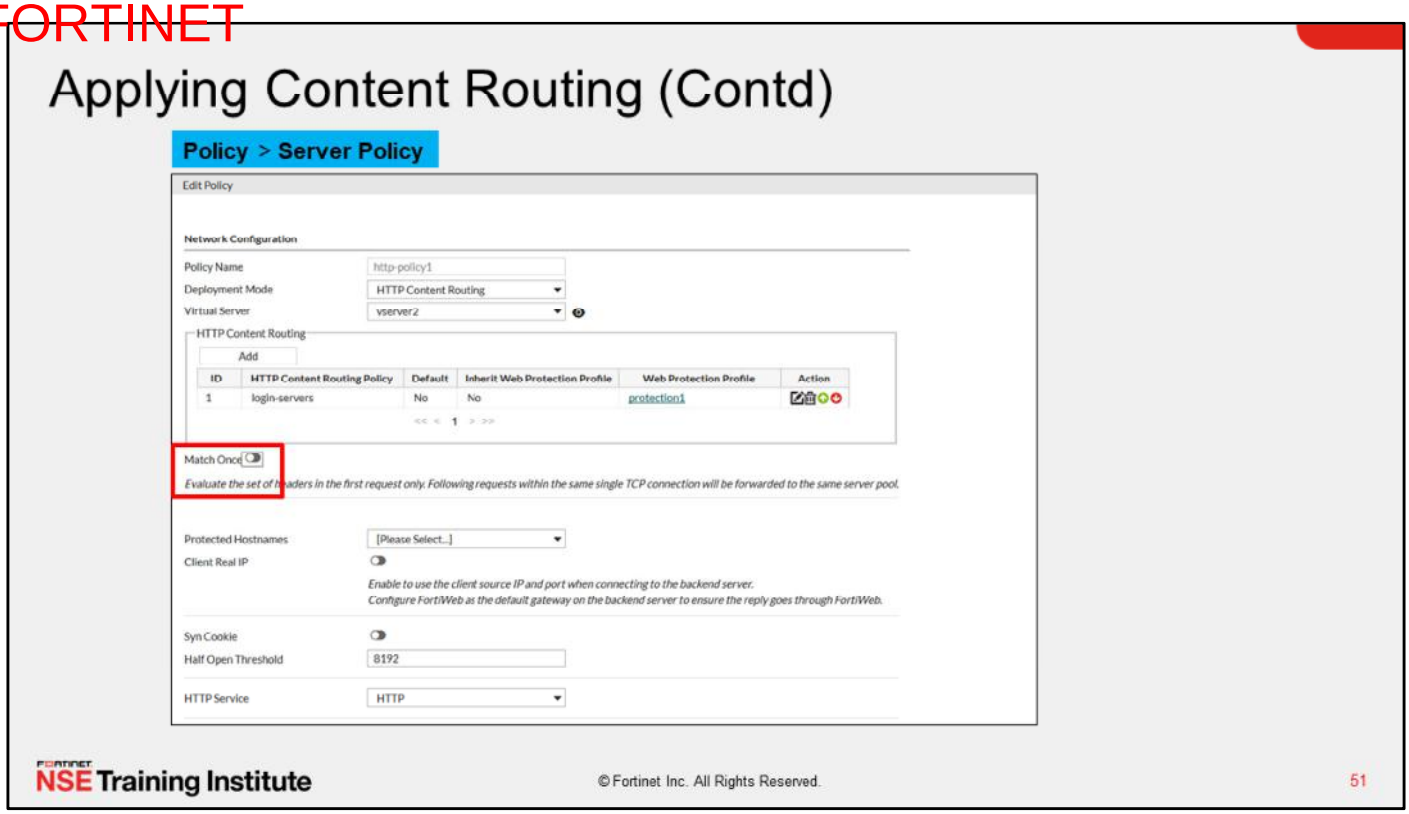
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To apply your routes, in your server policy, select **HTTP Content Routing** in the **Deployment Mode** drop-down list. Then, add each route to the table that appears. Similar to how you configure a default gateway at the IP layer, you can also configure a default content route at the HTTP content routing layer that applies to all traffic that does not match any other defined HTTP content routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If a multiplexing device is in front of FortiWeb, and if it is intelligent enough to pipeline requests from the same client, for the same web app, together in the same TCP connection, then you can enable the **Match Once** setting.

Enabling **Match Once** improves performance. For routing, FortiWeb will only evaluate the first request in the connection. It won't repeatedly evaluate content routes for the related requests. However, don't enable the setting otherwise. If the connection multiplexes unrelated requests from multiple clients, many requests could be routed to the wrong server pool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which one cannot be used to make a decision in policy-based routing?
   - ✓ A. MAC address
   - B. IP address
   - C. Cookie
   - D. URL

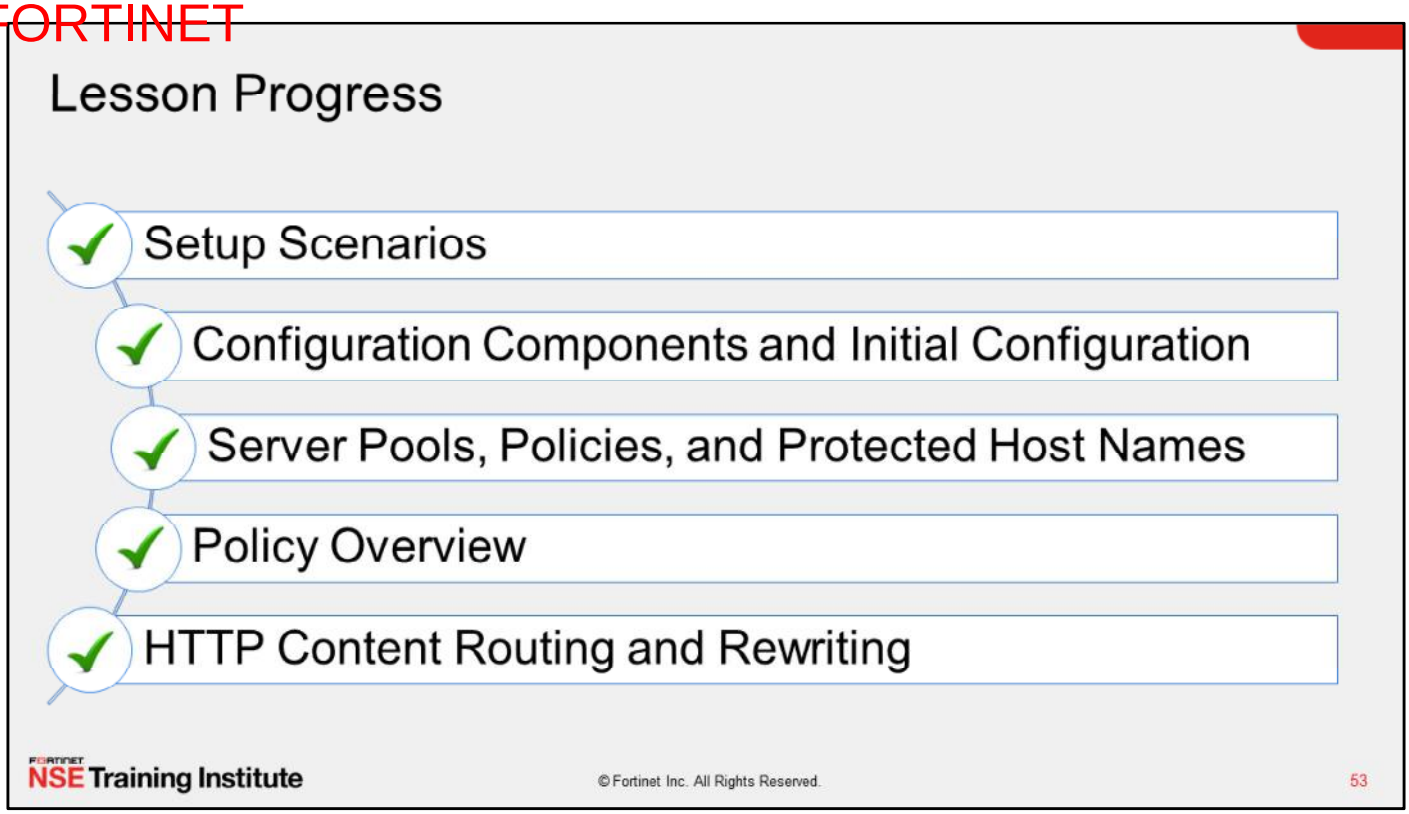
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

52

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Define and discuss possible topologies and implementation scenarios
- ✓ Understand configuration objects and basic configuration logic
- ✓ Route FTP and other non-HTTP protocols through FortiWeb
- ✓ Describe and discuss forwarding HTTP through FortiWeb
- ✓ Describe and discuss server pools
- ✓ Describe and discuss load balancing
- ✓ Describe and discuss session persistence
- ✓ Describe and discuss protected hostnames
- ✓ Configure server policies
- ✓ Configure routing based on HTTP content

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

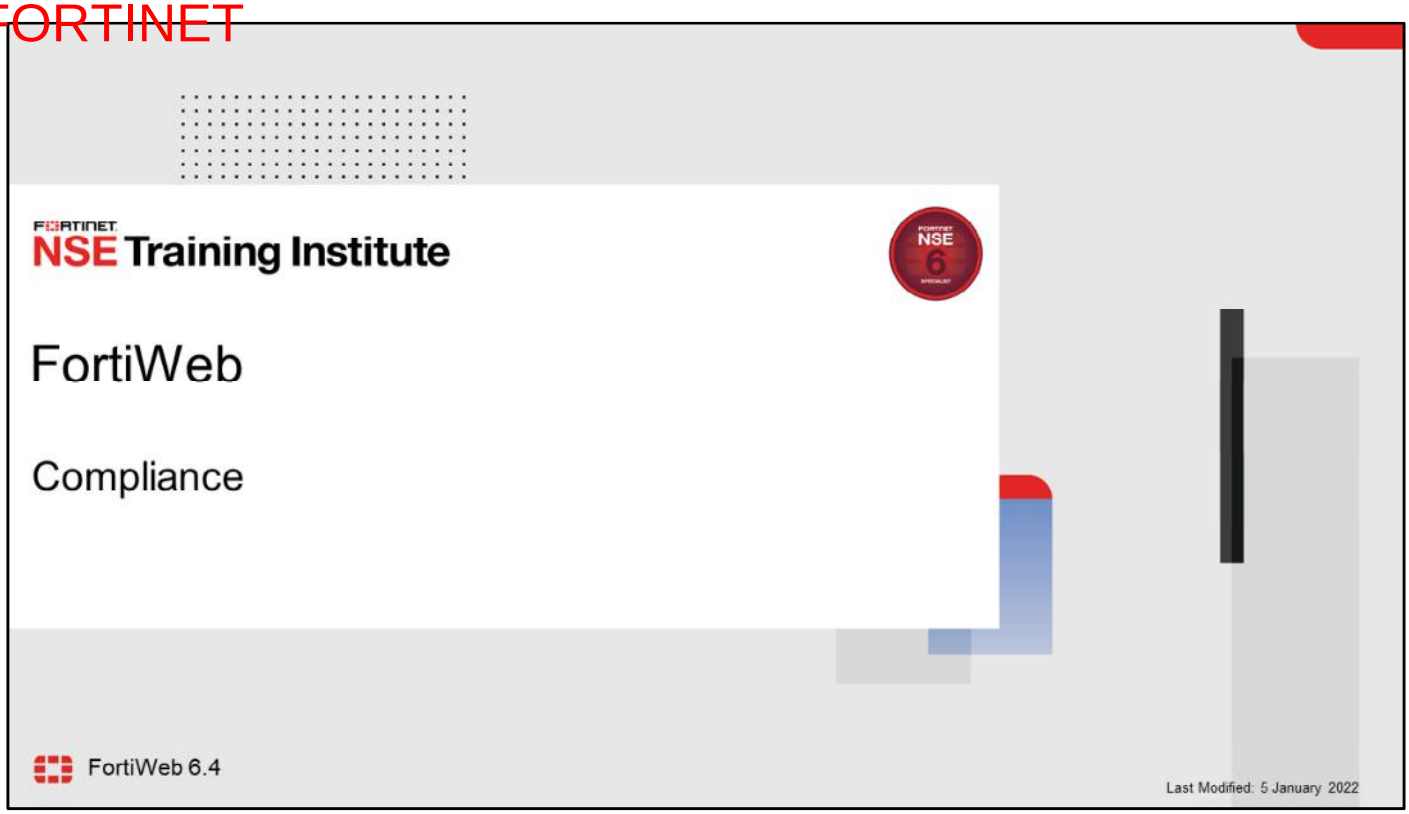
54

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to complete tasks involved in the basic set up of FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to apply FortiWeb features to help you meet the requirements of the payment card industry data security standard (PCI DSS). This includes applying industry best practices from the Open Web Security Application Project (OWASP) Top 10.

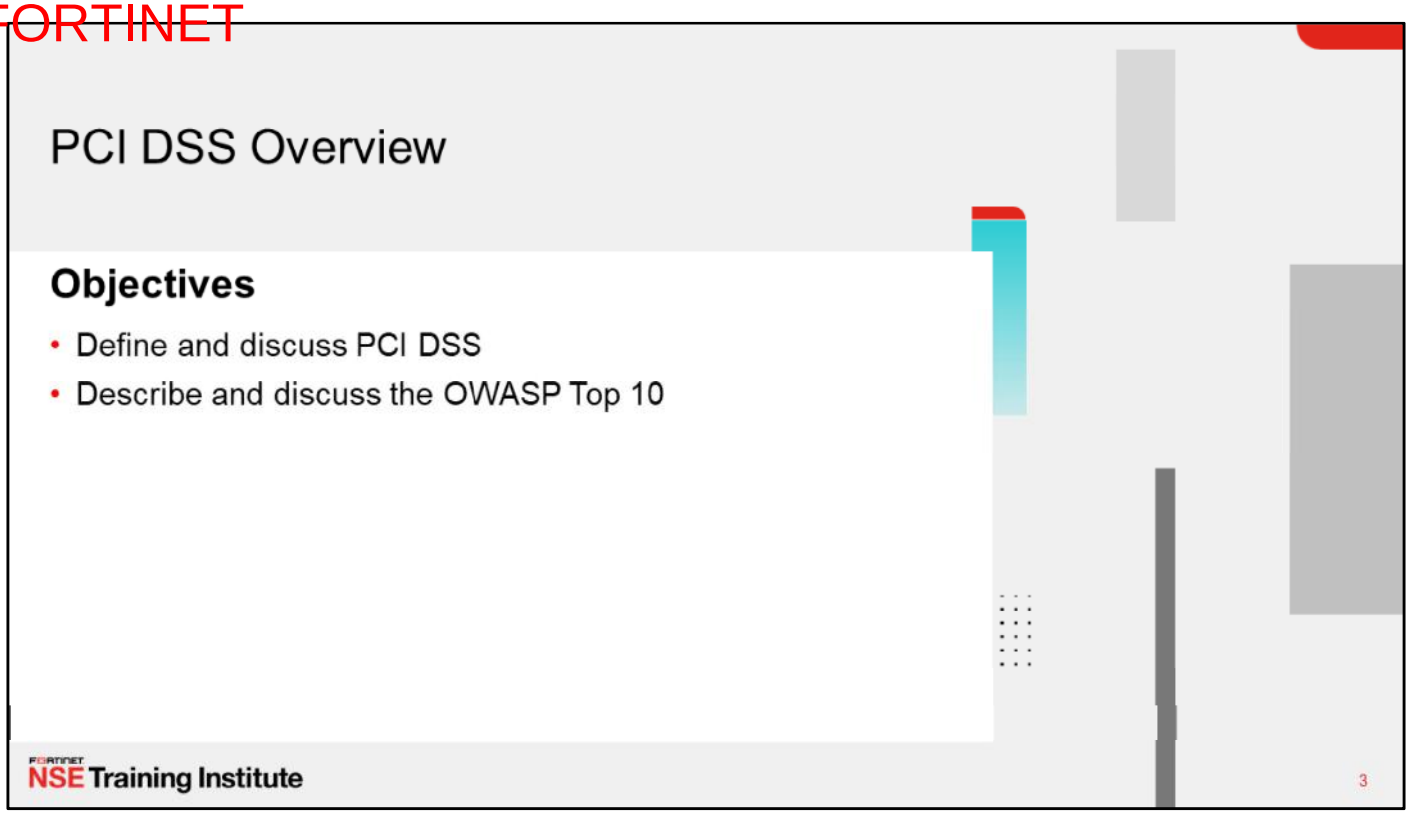
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding PCI DSS and the OWASP Top 10, you will be able to better identify and protect your network from web application security threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

The Threat

"Only 27.9% of global organizations maintained full compliance with PCI DSS."

– 2020 Verizon *Payment Security Report*

"Payment data is the most-sought commodity by threat actors."

– 2020 Verizon *Data Breach Investigations Report*

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

Compliance regimes, whether required by law or business organizations, typically require companies and organizations to demonstrate effective security policies and practices.

Requirements can very wildly by business type and country. The Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) emphasize the need for database security, authorization, and the prevention of data leaks. The Heath Information Technology for Economic and Clinical Heath Act (HITECH) requires disclosure of security breaches. The Payment Card Industry Data Security Standard (PCI DSS) concerns the prevention of information disclosure but also requires periodic scans.

The objective of professional attackers is usually to acquire sensitive, personal information that they can sell on the black market. For online retail companies, this can include addresses, personal ID numbers, and passwords, but most often, it is bank debit and credit card numbers.

According to Verizon *2020 Data Breach Investigations Report*, financial gain remains a primary motivator for cybercrime and accounts for nearly 9 in 10 (86%) breaches. Within the retail industry, 99% of incidents were financially motivated, with payment data remaining the most-sought-after and lucrative commodity by threat actors.

Because of constricted budgets, short-term thinking, and applying quick fixes rather than developing strategic plans for long-term solutions, there is a steady multiyear decrease in PCI DSS compliance. Although fines are not published for the public, they can be steep for PCI compliance violations. This holds true for both on-premises and cloud systems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

No Cost?

KrebsonSecurity
In-depth security news and investigation

06 The Target Breach, By the Numbers

News that **Target's CEO Gregg Steinhafle** is stepping down has prompted a flurry of reports from media outlets trying to recap events since the company announced a data breach on Dec. 19, 2013. Sprinkled throughout those reports were lots of numbers, which got me to thinking about synthesizing them with some of the less-reported numbers associated with this epic breach.

40 million – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.

46 – The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.

200 million – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards – about half of the total stolen in the Target breach.

100 million – The number of dollars Target says it will spend upgrading their payment terminals to support Chip-and-PIN enabled cards.

- Breaches cost millions of dollars, not counting fines
- Recent breaches:
  - HSBC
  - Target
  - Neiman Marcus
  - Home Depot
  - Staples
  - Adobe
  - Sony
  - Charge Anywhere
  - Citigroup

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

Because retailers and payment service providers often do not directly bear the cost of fraud, many assume that it does not hurt their business. Many executives assume that security costs more than the risk itself.

This is false.

This article highlights one breach in 2014 against the Target Corporation. Because their point-of-sale systems were not correctly secured, 40,000,000 debit cards were compromised. Target had a huge 46% drop in 4th quarter 2013 profits. Customers became nervous about using their cards to pay for purchases at Target in the USA. Currently there is no legislation that requires vendors like this to pay for identity theft monitoring after a compromise, so for each individual customer, the risk is huge. Target was forced to immediately spend $100,000,000 to improve security. Banks that did business with Target were affected, too. They spent $200,000,000 to reissue compromised cards, and this was for only one breach.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is PCI DSS?

- Payment Card Industry Data Security Standard (PCI DSS)
- Formed in December 2004
  - Top five credit card companies
  - Fortinet has been a member of PCI Security Standard Council since Oct 6th, 2009
- Developed to combat cost of fraud with consistent security
- Merchants must meet minimum levels of security when they store, process, and transmit cardholder data
- https://www.pcisecuritystandards.org/

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

The payment card network—including banks—absorbs most of the losses due to credit card fraud and online compromise of billing information. As a result, it has a clear financial interest in securing these assets. Security directly affects the profitability of payment card companies. They pass these costs on to businesses and, ultimately, on to customers. This is the hidden cost of crime.

It is now required by law in most countries that payment service providers and retailers must demonstrate basic responsibility when transmitting or storing payment card data. In the United States, these standards are known as PCI DSS. A similar system of standards in the EU is the General Data Protection Regulation (GDPR).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PCI DSS Requirements

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

PCI Security Standards Council

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

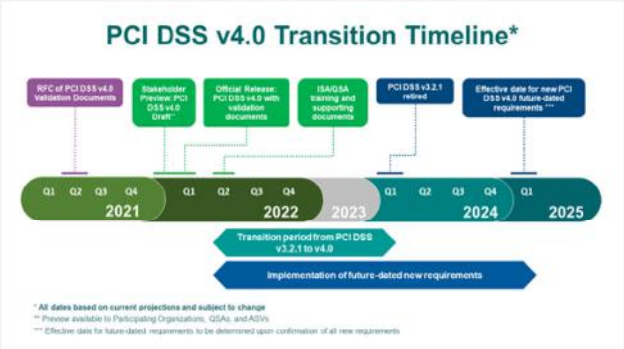
If you are new to PCI compliance, here is a brief overview. As you can see, it has been enforcing many of security's best practices for more than a decade. So, you may already be mostly compliant.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PCI DSS 3.2.1

- PCI DSS 3.2 retired on January 1, 2019 and PCI DSS 3.2.1 is the current standard
- PCI DSS 4.0 has finished RFC and is set for draft publication in Q1 2022
- 12 core areas are the same
- Sub-requirements
  - Clarifications
  - Stricter evaluation, but more flexible in implementation
  - Updates for most prominent threats today
    - OWASP
    - NIST
    - NSS



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

The current PCI security standard, version 3.2.1, came into effect in May 2018.

The core areas of security remain the same as previous versions. However, the standards development is now three years long, and there are new subrequirements to deal with the most current threats—specifically, web application firewalls.

The next version of PCI standards, version 4.0, is due to be released in 2022, with full implementation required by 2024. Major changes include stricter password and authentication module checks, and new guidelines on mandatory periodic testing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Requirements for WAF

- Section 6.5
  - Develop web applications securely based on the OWASP Top 10 guidelines
- Section 6.6
  - Ensure that all web-facing applications are protected against known attacks and address new threats and vulnerabilities by applying any of the following methods:
    - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
    - Having all applications reviewed manually or with automated application vulnerability assessment tools or methods
    - Installing a web application firewall (WAF) in front of web-facing applications

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediation against the top 10 vulnerabilities according to OWASP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is OWASP?

- Open Web Application Security Project (OWASP)
- 501(c)(3) non-profit worldwide charity
- Vendor-neutral security analysis and education

"Our mission is to make software security visible, so that people and organizations can make informed decisions about true software security risks."

https://www.owasp.org/

OWASP
Open Web Application Security Project

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

OWASP is a global non-profit security group. Its goal is to promote secure application coding and hardening.

OWASP has been growing steadily since 2004 and maintains a list of the top evolving web threats that companies and developers should be aware of.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP Top 10

- https://owasp.org/Top10/
- Broad consensus about what the most critical web application security flaws (based on real, public data) are
- Strongly recommended as defense best practice by:
  - U.S. Federal Trade Commission
  - U.S. Defense Information Systems Agency
  - PCI DSS
- This is the latest list of the top 10 threats as of Q3 2021

OWASP Top 10
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

The OWASP top 10 is a list of vulnerabilities that are considered by security experts to be the most serious web security threats. OWASP periodically updates them, based on its available attack data.

Many large organizations, including PCI, recommend that you scan for these vulnerabilities and fix or defend against them.

OWASP's last update to the top 10 was in 2017. It will be updated again in Q4 2021. It is available in many languages, including Arabic, Chinese, Spanish, and Ukrainian. Take a look at how FortiWeb can help you to find these vulnerabilities in your web applications and defend against them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP

- A2. Cryptographic Failures
  - Improperly configured TLS/SSL certificates
  - Accidentally exposing sensitive information that should be encrypted
  - Using self signed, old or weak certificates
- A3. Injection (includes cross-site scripting (XSS))
  - SQL, LDAP, OS commands like `passwd` or `dir`
  - Occurs if app sends unvalidated input with command or query to interpreter
  - Interpreter executes attacker's commands or accesses unauthorized data
    - Example: SQL dump of customers' stored credit card data
- A5. Security Misconfiguration
  - Example: If XML document includes hostile content to exploit vulnerable code, dependencies or integration, and information is not successfully scrubbed
    - Example: An attempt at a denial-of-service attack by including a potentially endless file:

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Injection and XSS remain the most common threats every year. This could be because they are the easiest to exploit, even for inexperienced attackers. All you need to do is insert a line of code into any input. If the input does not reject it, you might be able to exploit it.

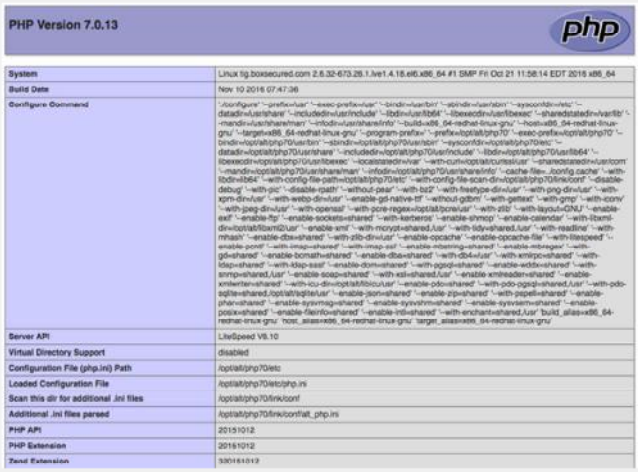
If a web application does not sanitize its inputs to make sure that they do not contain scripts, queries, or shell commands, and if the web app passes that input to an unsuspecting database engine, command line, or browser, it could accidentally run the attack.

Numerous public XML External Entity (XXE) issues have been discovered, including attacking embedded devices. XXE occurs in a lot of unexpected places, including deeply nested dependencies. The easiest way is to upload a malicious XML file, if accepted

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Does Your Server Talk Too Much?



- Fingerprinting info:
  - OS kernel and build date
  - Web server version
  - PHP module version
  - Supported directives
  - All configuration files
  - Location of all configurations
  - Settings such as IPv6 and thread safety
- In HTTP header:
  - X-Powered-By: PHP/5.4.4-7.1~www
  - server: gws
  - Server: Apache/2.2.29 (Unix) DAV/2

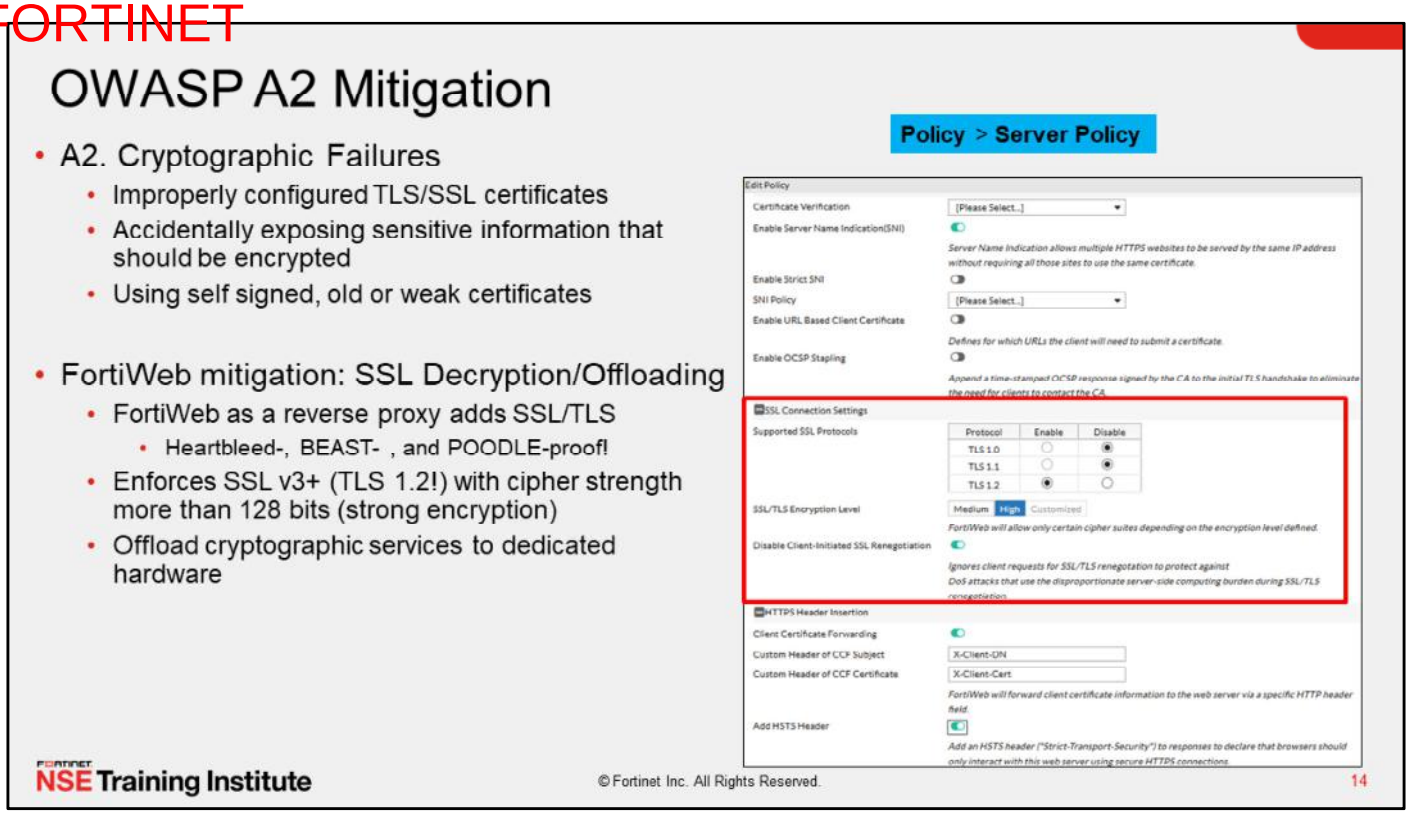
NSE Training Institute © Fortinet Inc. All Rights Reserved. 13

The file `phpinfo.php` usually has a simple function that displays all PHP settings. Each application could have its own `php.ini` and `.htaccess` file. IIS, Apache, and many other web servers, may insert an `X-Powered-By: or Server:` header that indicates which server and patch versions are installed. Software stack fingerprints are useful for crafting attacks or even buying prebuilt ones.

If any configuration files can be read, written, or executed by users on the internet, then attackers can gain information on how to exploit unpatched servers, rewrite the configuration, and more.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A2 covers sensitive data exposure.

This objective is at the heart of PCI DSS compliance and website security in general. The other OWASP Top 10 threats can impact the safety of stored sensitive information—yet another reason to remove such a feature from your web application, if possible—but this threat is specifically about the data while it is in transit, on the wires.

Like FortiGate, FortiWeb has data leak protection to detect credit card leaks on server replies. Ideally, servers should accept card numbers, but never increase risk by repeating them to the client. FortiWeb goes further, though. As an SSL or TLS terminator, FortiWeb can offer only the most secure protocol versions and cipher suites to your clients. This helps to keep your servers—and clients—more secure. If attacks are logged, you can easily mask passwords and credit card numbers so that they don't appear in your unencrypted logs.

In addition, FortiWeb appliances can have specialized ASIC chips that can be dedicated to cryptographic services, improving performance of all HTTPS transactions and improving web server performance.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A2 Mitigation—Credit Card Detection

Web Protection > Known Attacks > Signatures

New Signature Policy

Name
Custom Signature Group
Comments

Name	Status	False Positive Mitigation	Action	Block Period	Severity	Trigger Policy
Cross Site Scripting	On		Alert & Deny	600	High	
Cross Site Scripting (Extended)	Off		Alert	600	Medium	
SQL Injection	On	On	Alert & Deny	600	High	
SQL Injection (Extended)	Off	Off	Alert	600	Medium	
Generic Attacks	On		Alert & Deny	600	High	
Generic Attacks(Extended)	Off		Alert	600	Medium	
Known Exploits	On		Alert & Deny	600	High	
Trojans	On		Alert	600	Medium	
Information Disclosure	On		Alert	600	Low	
Personally Identifiable Information	On		Alert & Deny	600	High	
Detection Threshold	1					

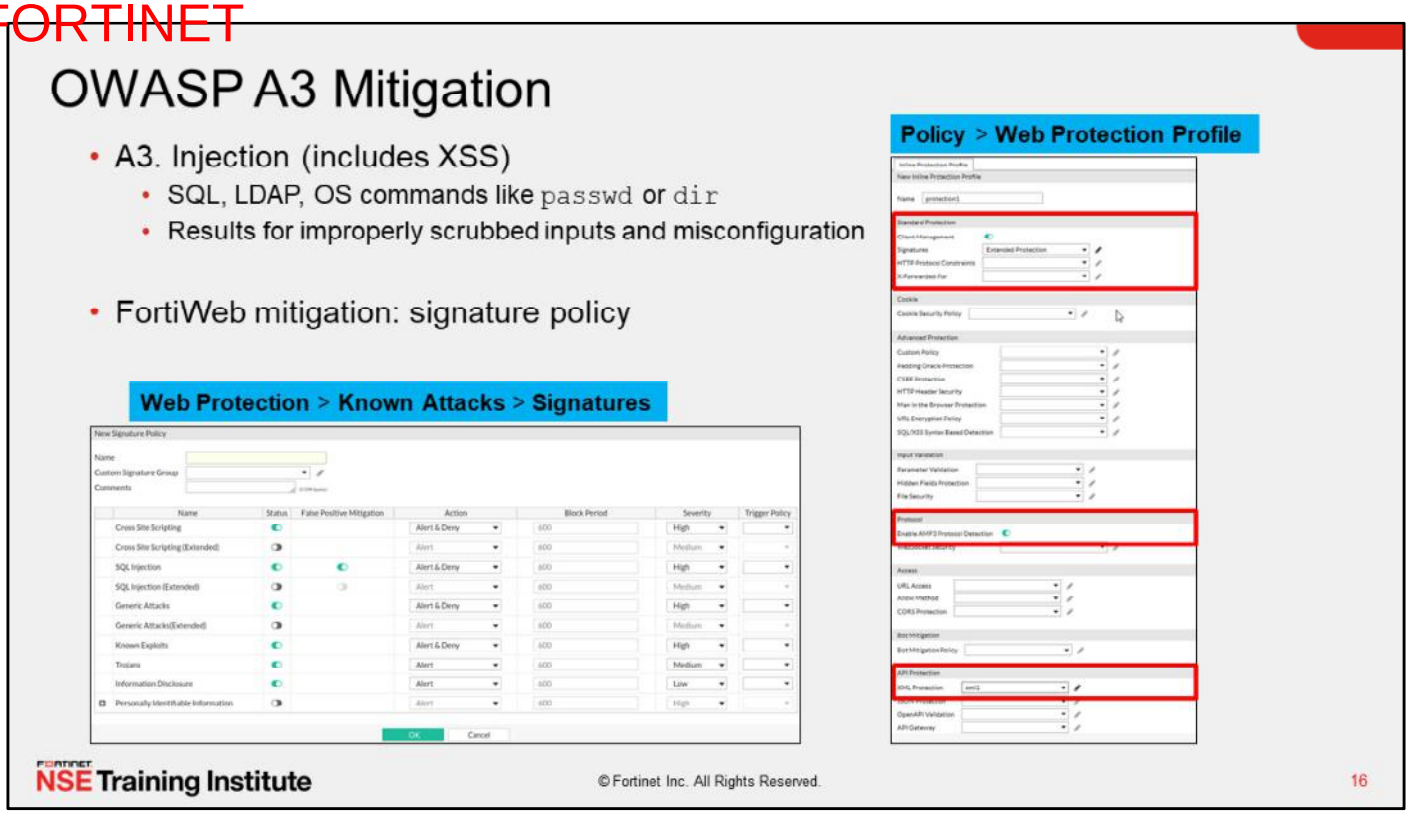
OK Cancel

NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

FortiWeb can identify if sensitive information appears on a protected web page. For example, you can configure FortiWeb to detect a violation based on a specific number of payment card numbers or other PII values, and alert or block the page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The good news is that FortiWeb can easily prevent injection and XSS attacks. In signature policies, enable their signature categories, then select that signature policy in the protection profile that you are using.

Plain ASCII inputs are not the only type that HTTP can transport. If your web application uses Flash or AJAX, you can enable FortiWeb to scan binary AMF and XML inputs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A5 Mitigation

- Security misconfiguration:
  - App is still configured for development and staging
  - Attacker leverages insecure settings
    - Back doors
    - Incorrect file permissions (`chmod 777 php.ini` etc.)
- FortiWeb mitigations: vulnerability scanning and machine learning
  - Web vulnerability scanner
  - Machine learning detects each server's sensitive URLs

Web Vulnerability Scan > Scan Profile > Scan Template

Scan Profile | Scan Template

+ Create New | Edit | Delete | View

#	Name
1	Full Audit
2	Fast Scan
3	Brute Force
4	OWASP Top 10

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Most web servers have default pages. When you're configuring the web server for the first time, this helps to quickly confirm that the software is running. However, these files should never be exposed on live production servers. This is essentially the message of A5. These files provide information that can be useful to attackers. Web servers that are setup incorrectly can leak lots of sensitive information to web crawlers and vulnerability scanners. Proper testing and machine learning of website usage patterns can ensure websites are used for their intended purposes and not exploited.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the purpose of the PCI DSS?
   A. To provide guidance on how to process cash transactions
   ✓ B. To set minimum security requirements for merchants based on best practices
   C. To ensure governments can access all online transactions performed online

2. What is the significance of the OWASP Top 10 list?
   A. It lists the top 10 political influences.
   ✓ B. It lists the 10 most serious threats.
   C. It identifies the top 10 web hacking groups active in a given year.

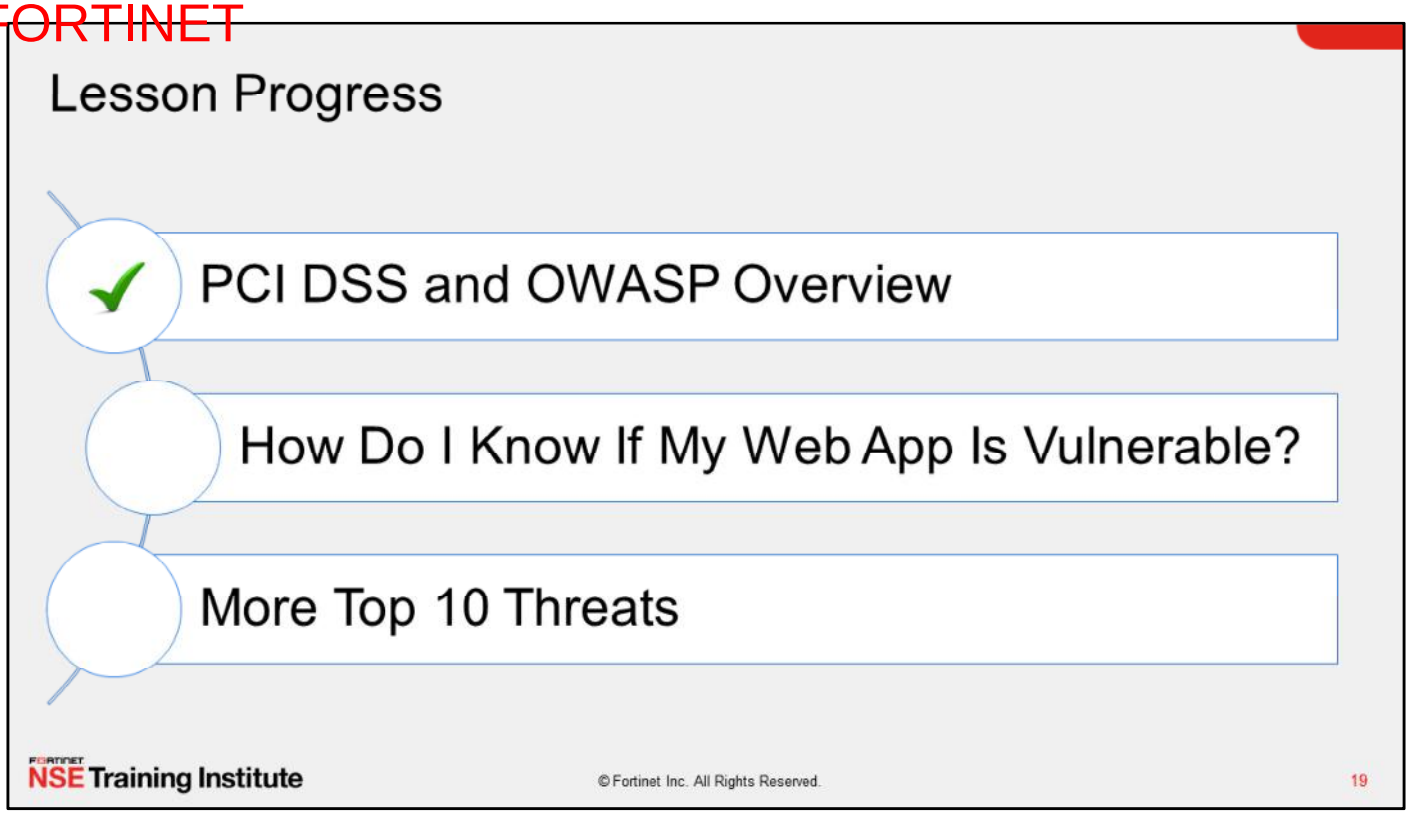
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

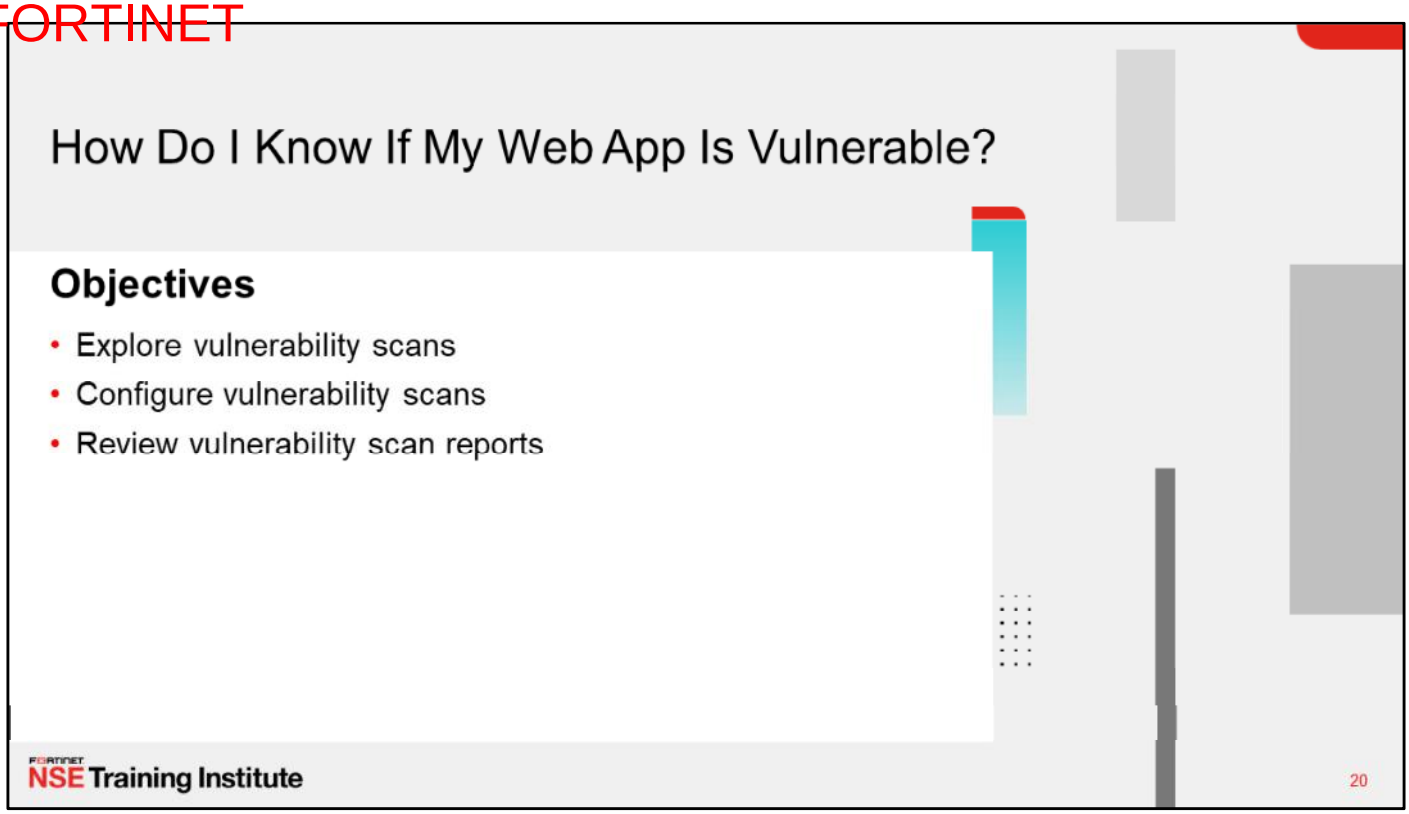


Good job! You are now familiar with PCI DSS and the OWASP Top 10 list.

Next, you will learn how to identify if your web app is vulnerable.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring and reviewing vulnerability scans, you will be able to use them to protect your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Web Vulnerability Scan

- Required at least one time each quarter for compliance, such as PCI DSS
  - More emphasis on periodic scanning and testing in PCI DSS 4.0
- The FortiWeb vulnerability scan is HTTP-specific
  - *Doesn't* require an OS login
  - More than a simple port scan
  - Accesses using HTTP, like users, and simulates input
- Detects four major types of vulnerabilities:
  - SQL injection (SQLi)
  - XSS
  - OS command line injections
    - `dir, passwd, sudo, tail, echo, source.cfm`
  - Source code disclosure

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

For performance reasons, FortiWeb should not actively scan for attacks that your web apps are not vulnerable to. It's a waste of resources. Manual penetration tests are slow and costly. How can you speed up some of your PCI compliance audits? How can you quickly discover the correct FortiWeb settings for your web apps?

FortiWeb has a vulnerability scan engine that is tailored to web applications. Quarterly vulnerability scans by an approved vendor are part of the requirements for PCI DSS compliance. The FortiWeb vulnerability scan gives you a quick start so that you are better prepared and will have fewer required remediations.

The web vulnerability scanner does not test for every possible vulnerability—some things are better investigated by creative human penetration testers—but it does scan for these top OWASP vulnerabilities:

- SQLi
- XSS
- Operating system command line injection
- Source code disclosure, which tricks the preprocessor into echoing the PHP, ASP, Ruby, or other page source code

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Prepare for a Vulnerability Scan

1. Copy the website and database into a test environment
   - Do not scan live websites
     - Performance hit possible
     - Enhanced mode uses HTTP POST method, tries to inject the database
     - Database changes less likely in basic mode, but still possible because many apps put parameters in URL of HTTP GET method
2. Schedule an appropriate time
   - Lower load = faster scan
3. Disable rate limiting of connections from the FortiWeb IP
4. Start scan
   - WVS schedule (optional)
   - WVS profile
   - WVS policy

Caution: Do not scan live websites, especially through the internet!

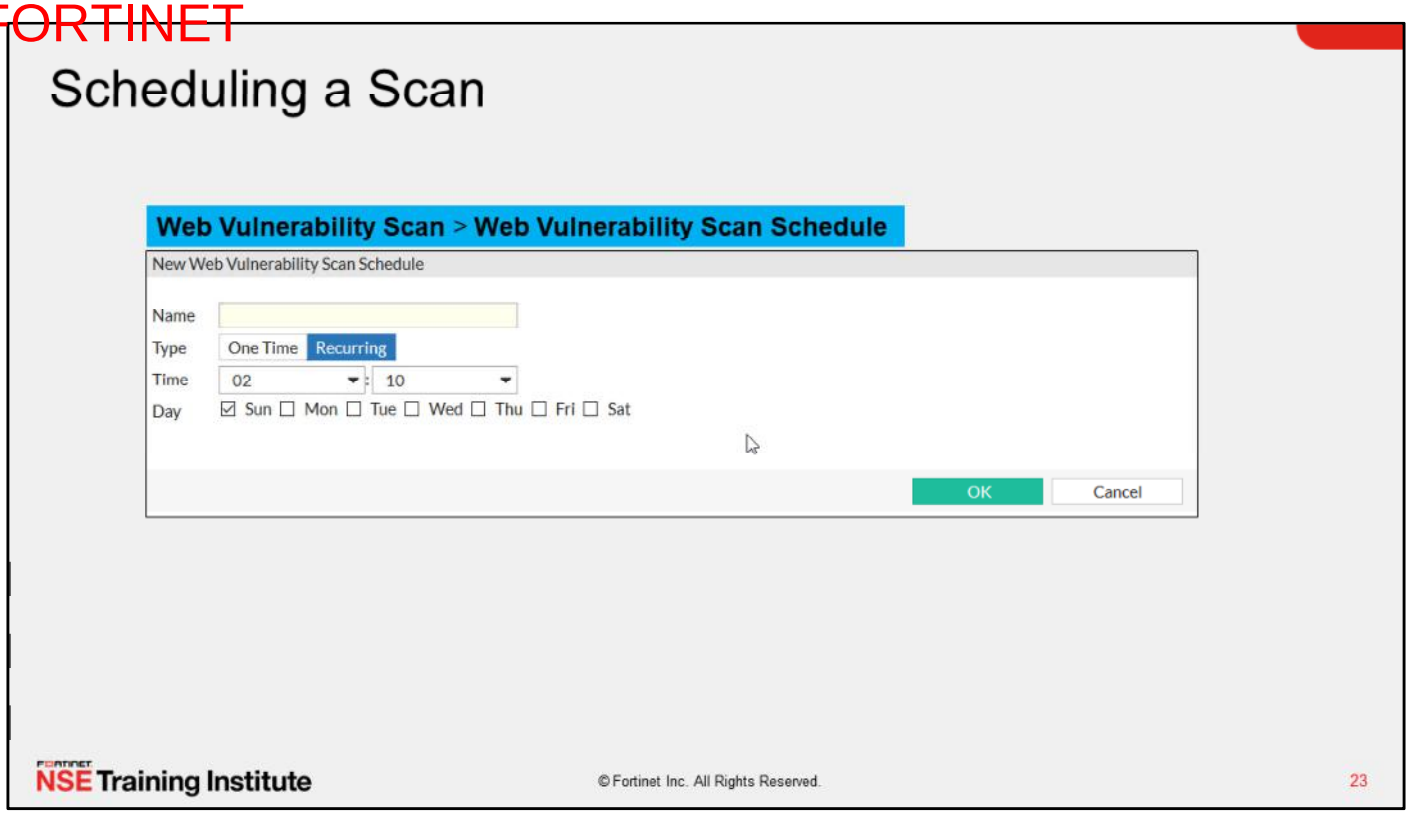
NSE Training Institute © Fortinet Inc. All Rights Reserved. 22

To prepare for a vulnerability scan, always begin by copying the web app and its database to a test environment. *Do not scan live websites, especially over the internet*. If your public IP is a known source of potential attacks, your ISP could ban you and reputation-based services could also blacklist you. Additionally, depending on the web app, the scan could inject data into the database, requiring you to restore from backup, potentially causing some data loss and downtime. Also, if your FortiWeb is directly attached to the test servers, no other network devices rate limit or interfere with the accuracy of the scan, so the scan is faster and more accurate. For all of these reasons, you should scan a test copy of the web app—not the live production network.

To configure a vulnerability scan, define the schedule, then the profile. Optionally, if you want FortiWeb to email the finished report to you, also configure a connection to an email server. Finally, bind them together in a scan policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will learn how to configure a web vulnerability scan on FortiWeb.

First, determine the schedule. When a web app is updated, or different plugins installed, its vulnerabilities can change. While a recurring vulnerability scan may be part of your PCI compliance routine, it is a best practice to run the scan manually, whenever new software is introduced or changes are made.

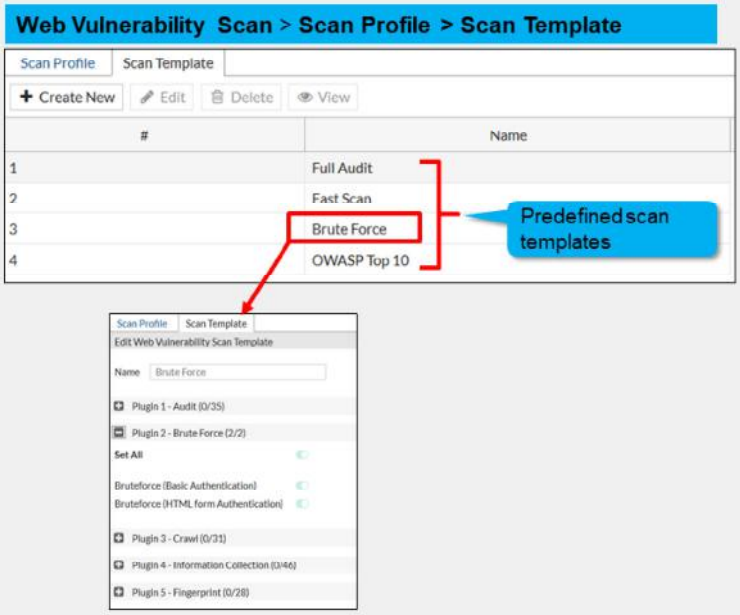
Any recurring scan can also be started on demand, whenever you need it, so it does not prevent you from manually forcing a scan. But if you want FortiWeb to scan the website one time at a specific time, in the **Edit Web Vulnerability Scan Schedule** window, to the right of **Type**, select **One Time**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scan Template

- Scan template that is used in scan profile
- By default, four scan templates are predefined
  - Full Audit
  - Fast Scan
  - Brute Force
  - OWASP Top 10
- Customize your own template by configuring different plugins



NSE Training Institute © Fortinet Inc. All Rights Reserved. 24

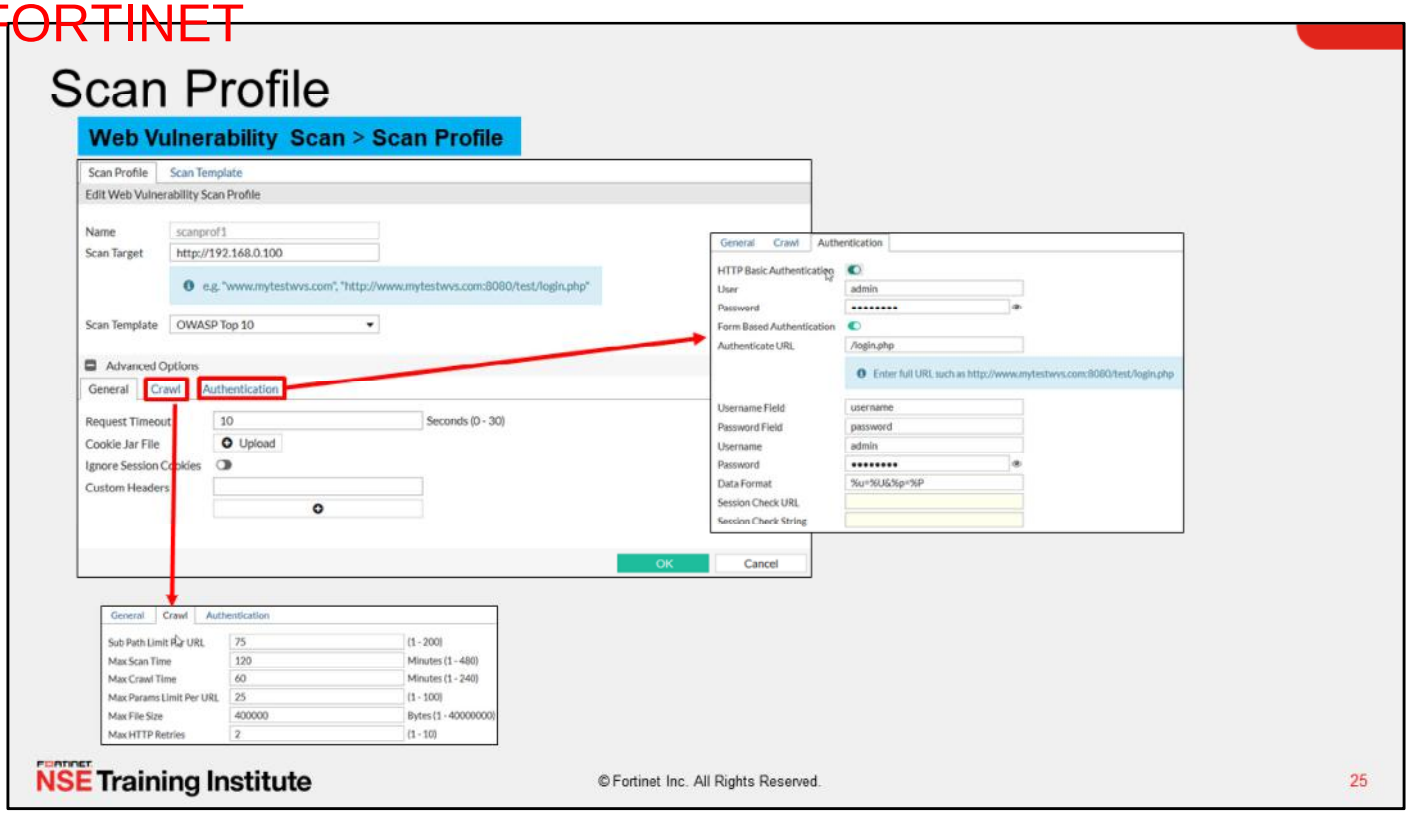
To configure a scan profile, you should have a scan template ready. Four scan templates are introduced by default, which can not be edited or deleted. You can create your own scan templates by configuring plugins for each different plugin category.

Here are the four predefined templates:

- **Full Audit**: Perform a full audit of the target website, using only the web spider plugin for discovery.
- **Fast Scan**: Perform a fast scan of the target the site, using only a few discovery plugins and the fastest audit plugins.
- **Brute Force**: Brute force form or basic authentication access controls using default credentials. Set the target URL to the resource where the access control is.
- **OWASP Top 10**: As a worldwide free and open community focused on improving the security of application software, OWASP searches for and publishes the ten most common security flaws.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A vulnerability scan profile defines a web server that you want to scan, as well as the specific vulnerabilities to scan for. In turn, scan profiles are used by vulnerability scan policies, which determines when to perform the scan and how to publish the results of the scan defined by the profile.

If your web application has a login page, remember to provide FortiWeb with a username and password. That way, FortiWeb can test all the pages in your web app and its authentication procedures. Otherwise, the report could be incomplete. Depending on your application, logins could be HTML form-based, HTTP dialog only, or both. Remember, with a form based login, when you click **Log In**, your browser could be sending credentials to a different URL than the one that you're currently viewing. To find the URL, view the source code for the page. Search for the `<form>` tag. Its action attribute shows the URL where your app receives login attempts—the authentication URL of the scan.

FortiWeb logs in and then crawls the links in the app, trying injection and echo vulnerability probes in each input that FortiWeb finds on each page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Starting a Vulnerability Scan

Web Vulnerability Scan > Web Vulnerability Scan Policy

New Web Vulnerability Scan Policy

Name	scanpolicy1
Type	Run Now / Schedule
Schedule	scanschedule1
Profile	scanprof1
Report Format	☑ HTML ☐ XML ☐ PDF
Email Policy	

OK Cancel

Web Vulnerability Scan > Scan History

Delete View Download

#	Name	Target Server	Request Count	Requests per Minute	Scan Time	End Time	Alerts Found
1	fast-scan	http://10.0.1.21	1177	1088	2021-10-06 12:45:45	2021-10-06 12:47:08	16
2	id-scan	http://www.example.com	0	0	2021-10-06 13:33:04	2021-10-06 13:33:51	0
3	id-scan	http://10.0.1.8	27	46	2021-10-06 13:26:06	2021-10-06 13:26:53	3
4	id-scan	http://10.0.1.8	27	45	2021-10-06 13:21:13	2021-10-06 13:22:03	3
5	id-scan	http://10.0.1.21	27	46	2021-10-06 13:11:41	2021-10-06 13:12:28	3

NSE Training Institute

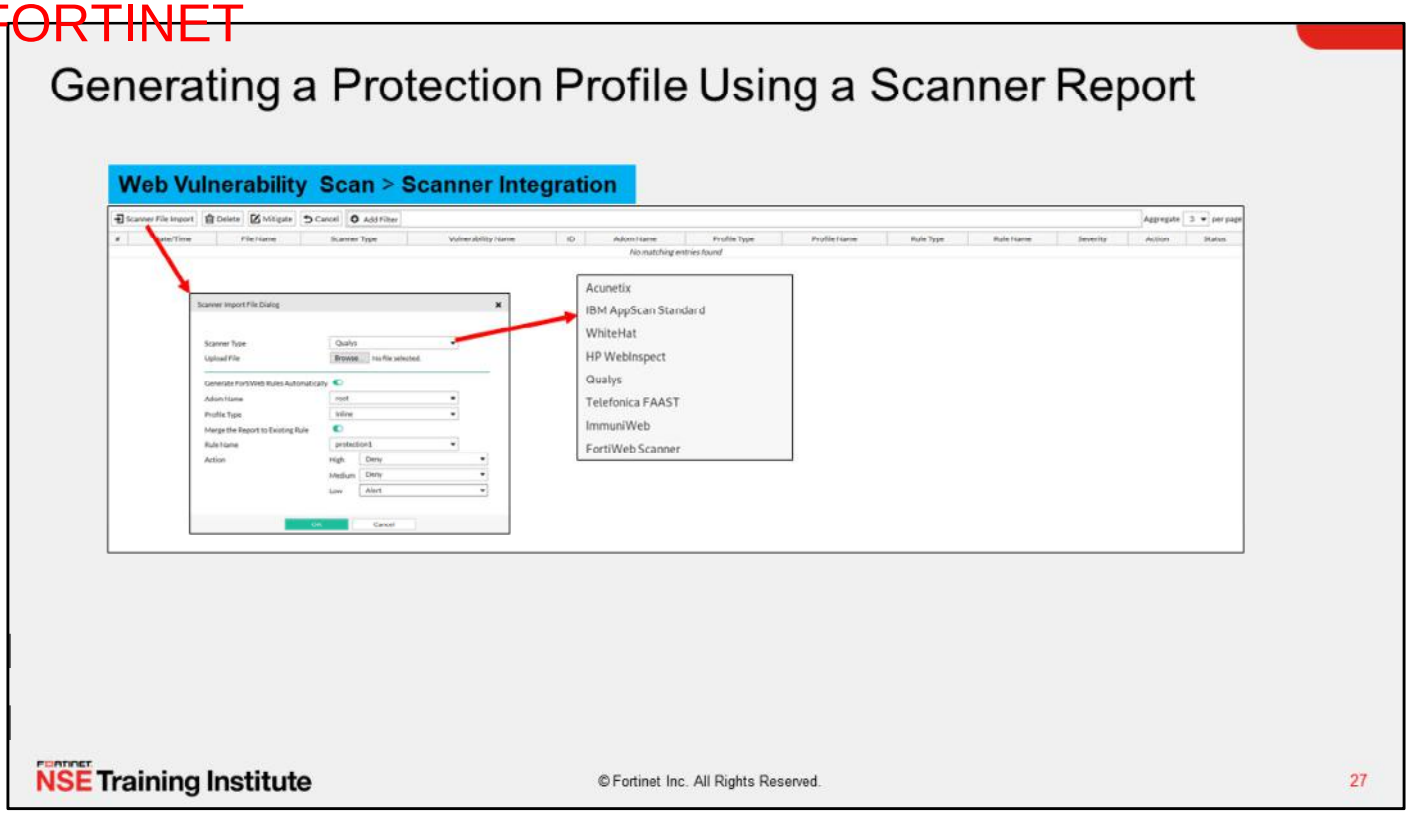
© Fortinet Inc. All Rights Reserved.

26

After you configure the scan, you can immediately run it by selecting **Run Now**, and then clicking **OK**, or waiting for the appropriately scheduled time. For extended scans, you can either periodically return to the **Scan History** page to see the scan status or configure the scan to email the results. Results are also available to view and download through the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also use XML-format reports from third-party web vulnerability scanners to automatically generate FortiWeb protection profiles that contain rules and policies that are appropriate for your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Why is it critical to avoid scanning live websites when performing a vulnerability scan?
   A. You could accidentally purchase an item from the website.
   B. It could flag your public IP as a threat. ✓
   C. Concurrent traffic could interfere with the scan.

2. Which type of vulnerability does FortiWeb not scan for?
   A. Unvalidated redirects ✓
   B. SQL injection
   C. robots.txt file
   D. Server information pages

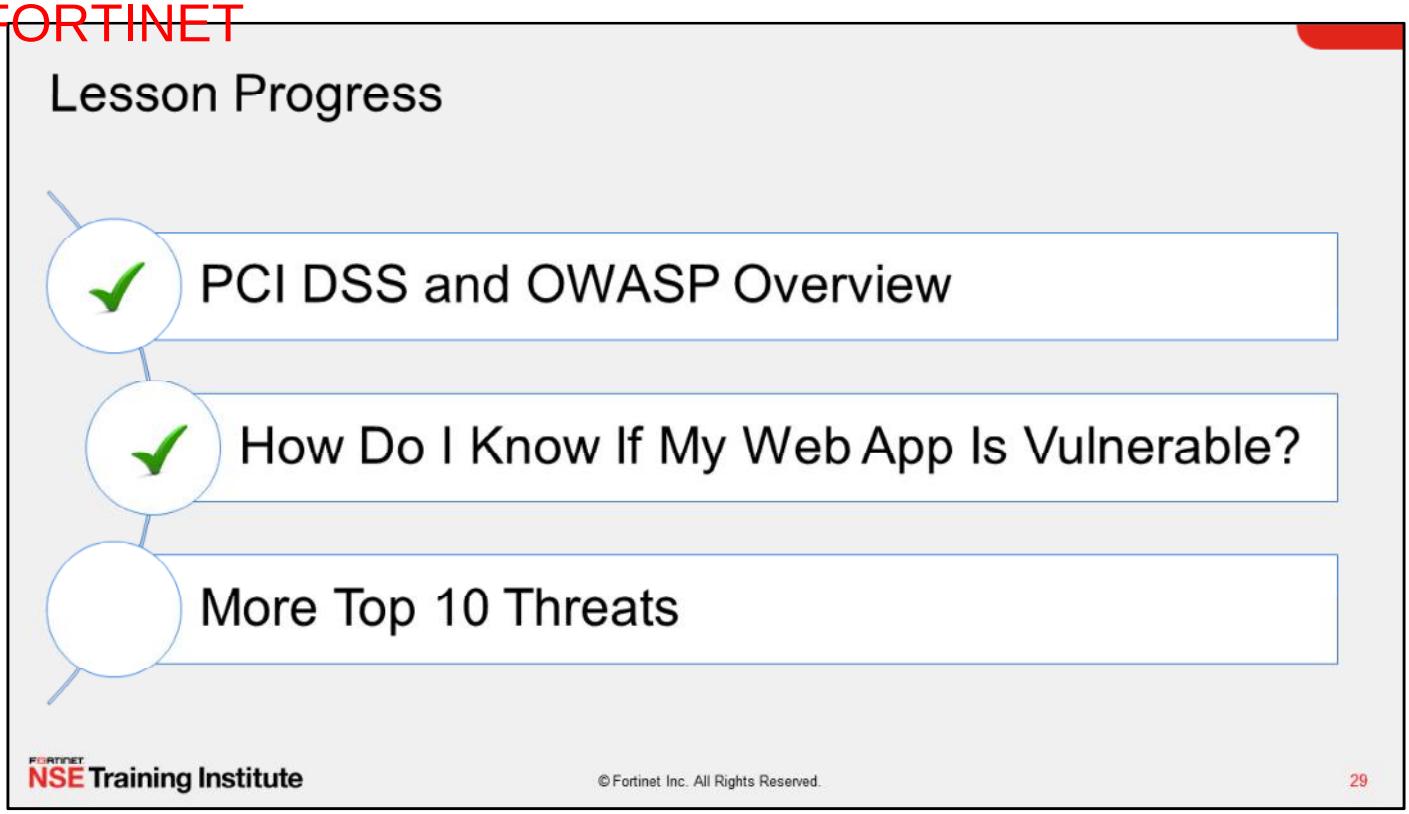
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

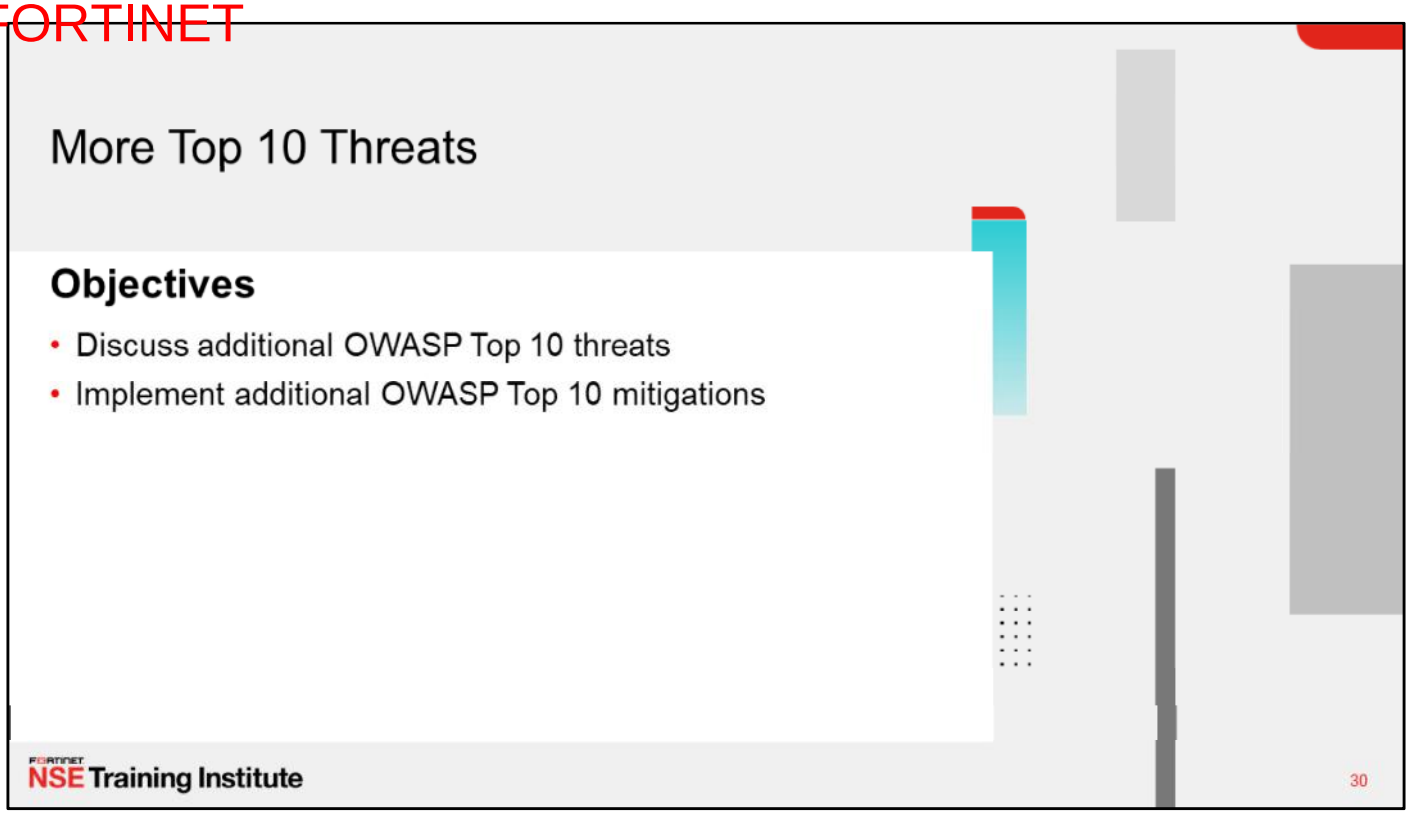


Good job! You now know how to perform a vulnerability scan on FortiWeb.

Now, you will learn more about additional top 10 threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the additional top 10 threats, you will be able to better protect your network through effective threat mitigation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A6

- A6. Vulnerable and Outdated Components:
  - Libraries, frameworks and other software components may run with full root or administrator privileges
  - Attackers exploit components with known vulnerabilities and can gain root access
- FortiWeb mitigation:
  - Signatures for known exploits
  - FortiGuard antivirus (Trojans)
  - SSL/TLS offload instead of vulnerable, old OpenSSL installations on every server

NSE Training Institute

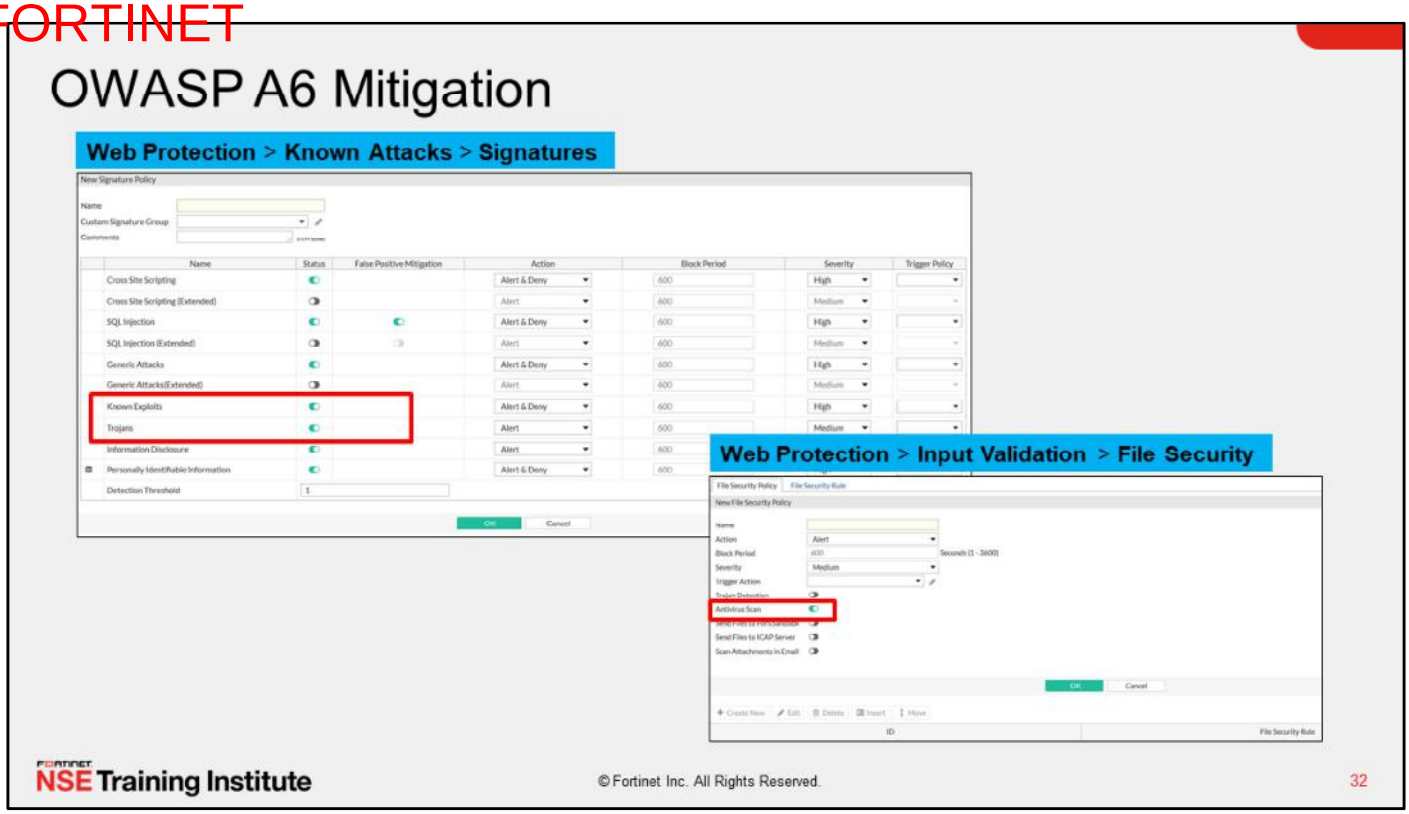
© Fortinet Inc. All Rights Reserved.

31

It may surprise you to know that unpatched software is not considered by OWASP to be the most serious threat, but awareness is increasing. In 2021, vulnerable components were upgraded from ninth to sixth on the list of its 10 most serious security threats, even though it is one of the most common. This ranking is partly this is because it is one of the easiest to defend against. If FortiWeb is scanning for known exploits and Trojans, and blocking Heartbleed HTTPS leaks, then this allows you some time to patch your servers. Automatic updates on many server software components also make this threat easy to fight.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb can mitigate old, outdated components by enforcing a consistent SSL/TLS version across all protected servers and performing spontaneous antivirus, trojan, and known exploit scanning. So, regardless of the actual version of your web server, FortiWeb can enforce a base level of protection. It is always recommended to use both a WAF and to keep your end servers correctly patched and updated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A7

- A7. Identification and Authentication Failures
  - Authentication and session management are not implemented correctly
  - Attackers compromise passwords, keys, and session tokens to assume users identities
    - Example: Session hijacking, session logic bypass, or fraud
- FortiWeb mitigations:
  - Authentication (site publishing with HTTPS, two-factor, and Kerberos support)
  - Brute force of authentication is blocked
  - Session management
  - Cookie checksums
  - Start pages and page order enforcement
  - Padding oracle protection
  - Sensitive info masking in logs

NSE Training Institute © Fortinet Inc. All Rights Reserved. 33

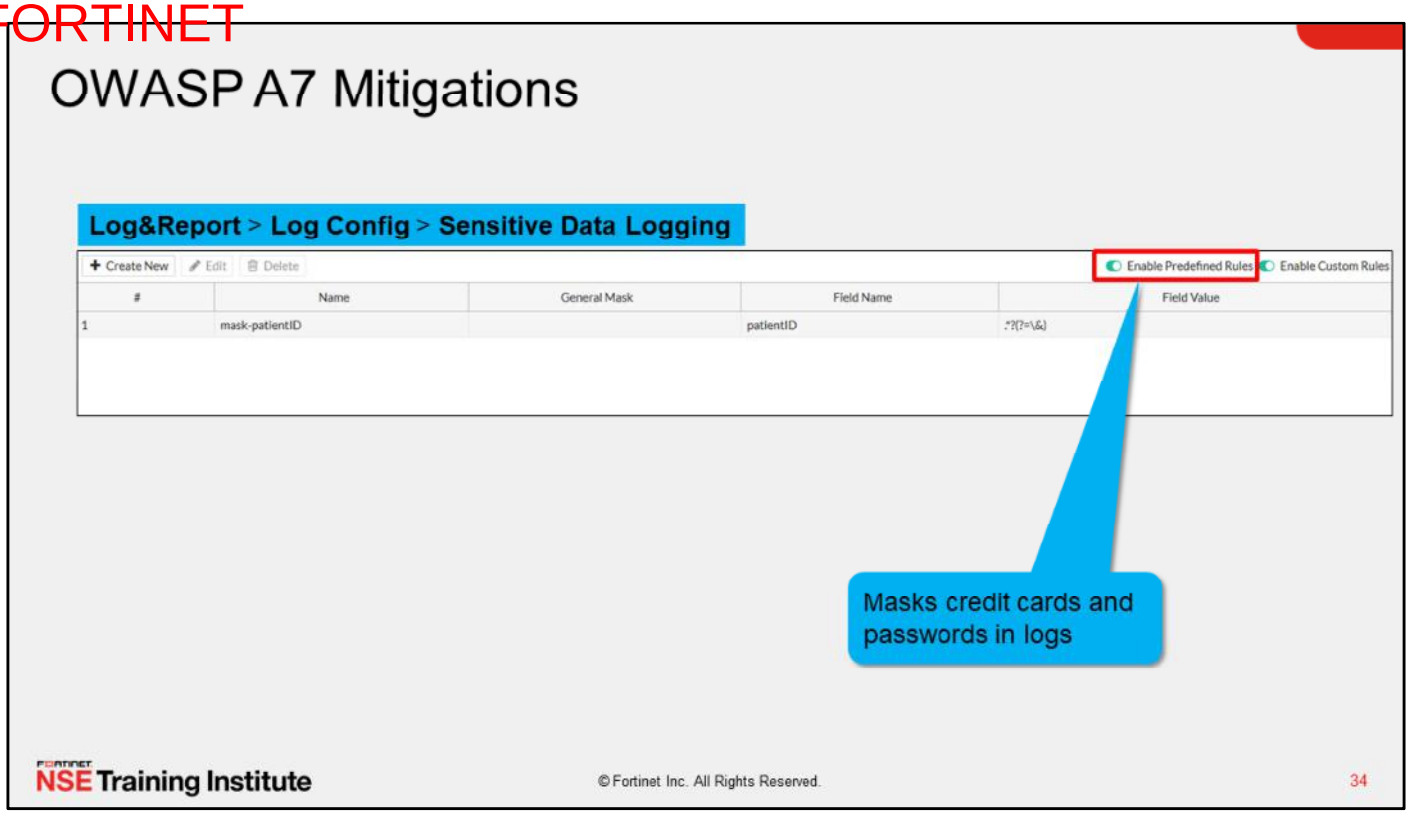
OWASP's A7 threat is one of the most complex to protect against.

Because authentication and sessions can be attacked in many ways, you want to make sure that every step is secure by ensuring the following:

- Sessions are cryptographically hard to predict.
- Sessions are bound to the client IP (if possible, to the individual browser).
- Session cookies, if used, are checksummed. This ensures that a client is not trying to masquerade as another client and hijack a session.
- HTTPS protects both user names and passwords (and, if applicable, two-factor authentication passcodes) during transit.
- Authentication doesn't allow brute force attempts to guess valid user names and passwords.
- Subsequent page accesses use the bound session correctly, and don't allow nonsense page transitions.
- Log messages don't contain passwords or credit card numbers.

Vouchers & Dumps are Available | WhatsApp +201224560923

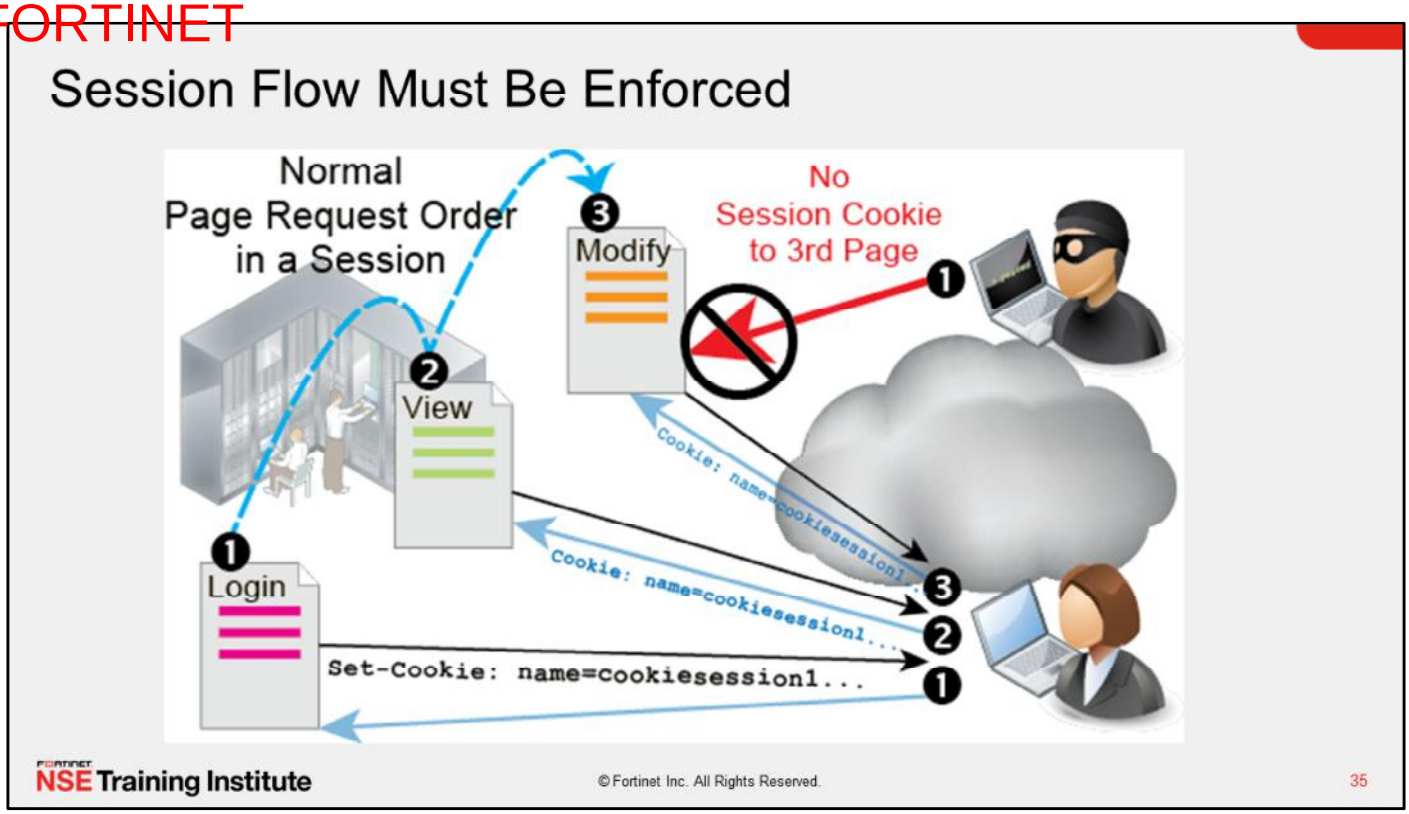
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Remember, if you have enabled logging (especially with the packet payload), credit cards and passwords could be in the log messages—not just the HTTP traffic. To prevent this, and ensure PCI DSS compliance, enable masking of sensitive data in the logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

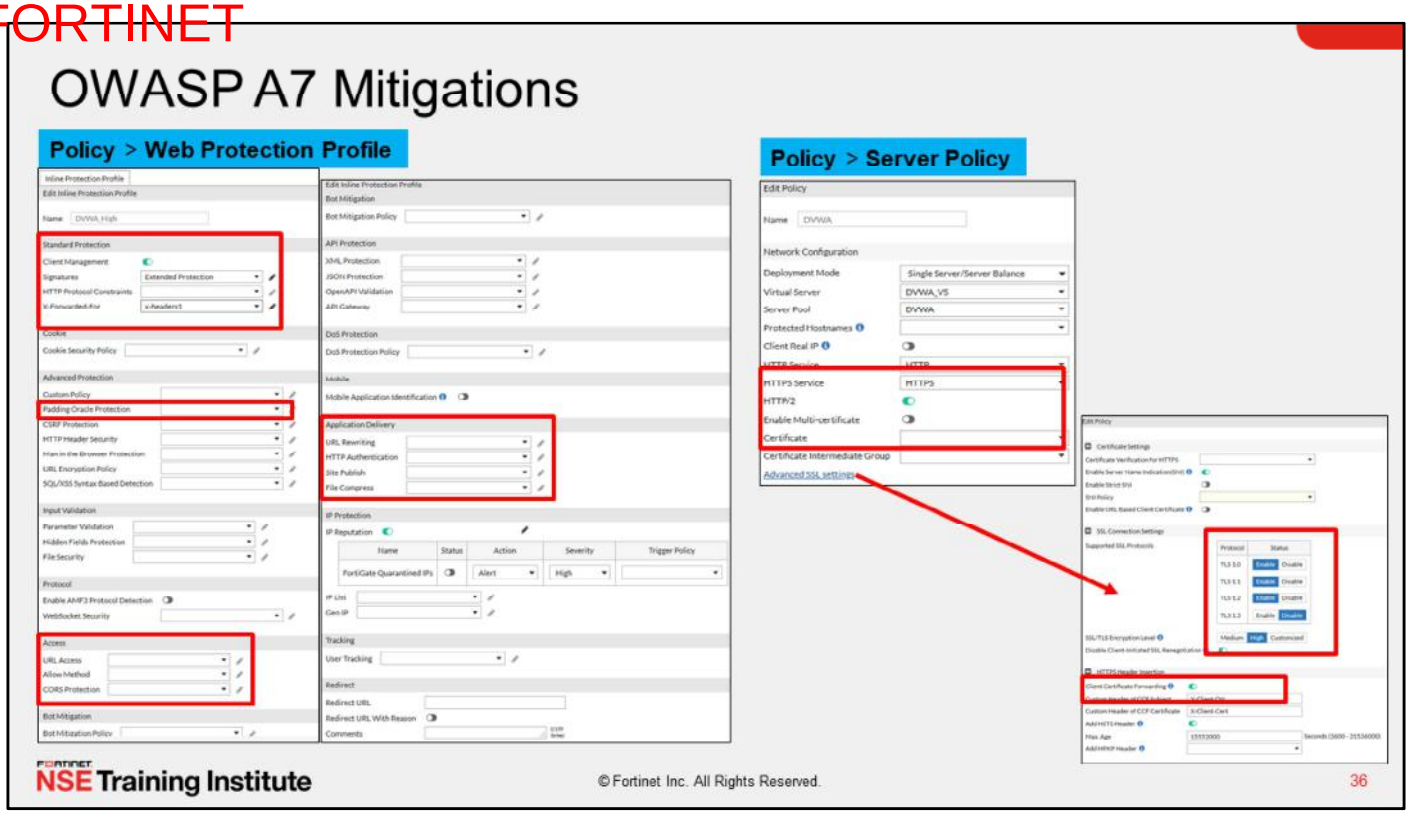
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the example shown on the slide, a normal user begins at the login page and receives a session ID in a cookie. However, if the app does not require a session for access to the other pages, then the page order within the session can't be enforced because the web app has no other way to remember the client's previous page request and associate it with a session. This kind of broken session management can be exploited.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You select most A7 mitigations in the protection profile, but you enable some in the policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A8

- A8. Software and Data Integrity Failures (formerly Insecure Deserialization):
  - Apps are vulnerable if it deserialized hostile or tampered objects supplied by attacker
  - Attacker modifies application logic or achieves arbitrary remote code execution
  - Apps can use serialization for:
    - Remote and inter-process communication
    - Wire protocols, web services, message brokers
    - Caching persistence
    - Databases, cache servers, file systems
    - HTTP cookies, HTML from parameters, API authentication tokens
- FortiWeb mitigations:
  - Attack signatures

  Example: https://fortiguard.com/encyclopedia/ips/44975/red-hat-jboss-as-dofilter-insecure-deserialization

NSE Training Institute © Fortinet Inc. All Rights Reserved. 37

A deserialization exploit is difficult to detect and perform. Some automated tools can help discover deserialization flaws, but human intervention is usually required for problem validation. Therefore, this is included in the top 10 based on industry survey and not on quantifiable data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A9

- A9. Security Logging and Monitoring Failures:
  - Insufficient logging and monitoring is the bedrock of nearly every major incident
  - Lack of monitoring helps attackers to achieve their goals without being detected
- Insufficient logging occurs any time:
  - Auditable events, such as logins, failed logins, and high-value transactions are not logged
  - Warnings and errors generate no, inadequate, or unclear log messages
  - Logs of applications and APIs are not monitored for suspicious activity
  - Logs are only stored locally
  - Logs are not kept for an appropriate length of time
    - PCI DSS requires at least one year of logs to be maintained

NSE Training Institute © Fortinet Inc. All Rights Reserved. 38

Exploitation of insufficient logging and monitoring is core to nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals, without being detected and to have more time to properly exploit a target.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OWASP A9 (Contd)

- FortiWeb mitigation:
  - Full and enhanced attack logs
  - Event correlation and aggregation
  - Violation based alerts and emails
  - FortiAnalyzer integration
  - SIEM Integration

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploits.

One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The testers' actions should be recorded sufficiently to understand what damages they may have inflicted.

You should consider following while configuring logging and monitoring:

- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Establish effective monitoring and alerting so that suspicious activities are detected and responded to in a timely fashion.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which threat type does OWASP A5 (Security Misconfigurations) cover?
   A. Unpatched software
   ✓ B. Incorrect file permissions
   C. SQL injections
   D. Denial of service attacks

2. What should you do with your FortiWeb logs to ensure PCI DSS compliance?
   A. Store logged data in a safe
   B. Enable masking of all PII in the logs
   C. Perform constant real-time penetration scans against your servers to test logging
   ✓ D. Ensure all relevant data is logged and stored for at least a year

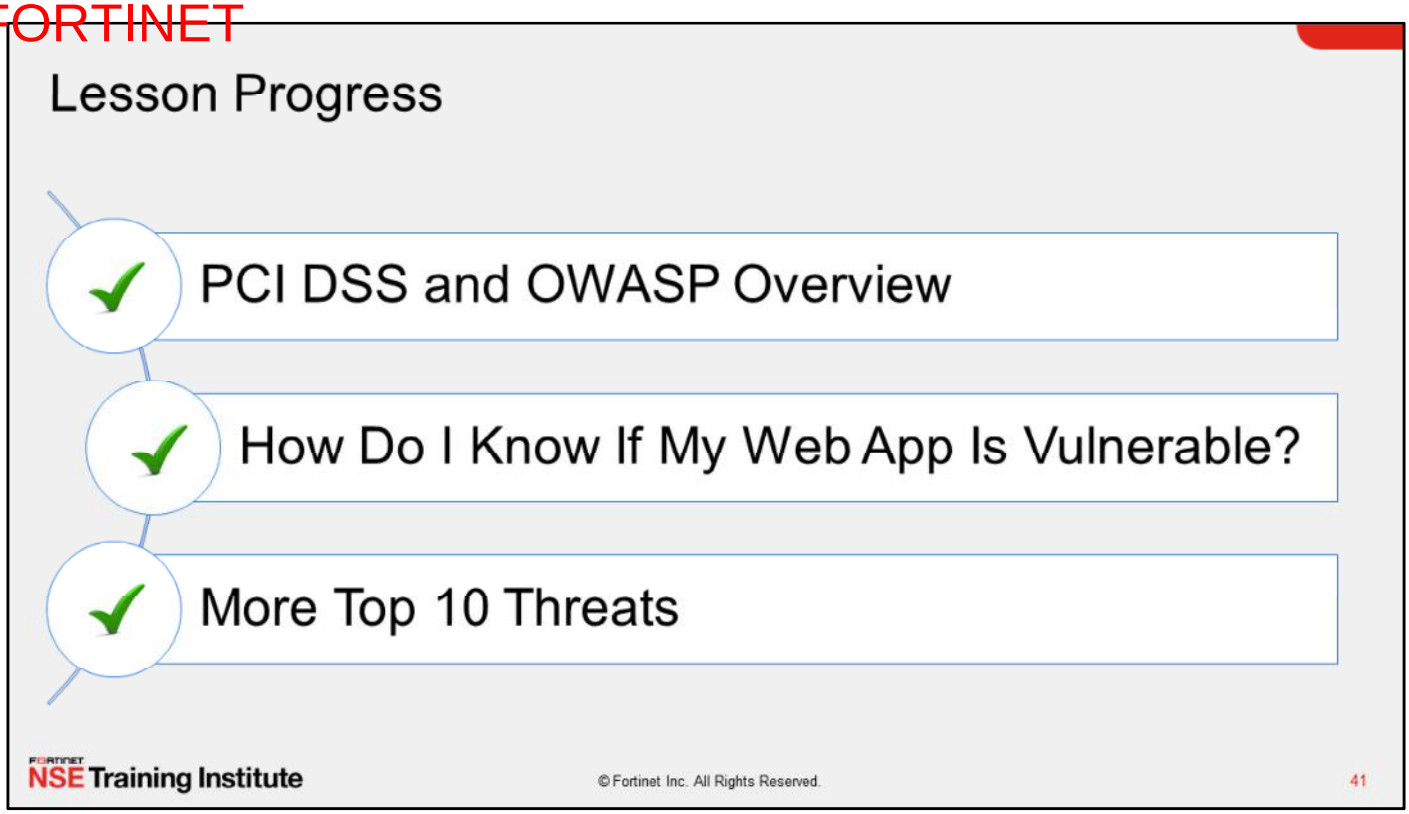
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have successfully completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Define and discuss PCI DSS
- ✓ Describe and discuss the OWASP Top 10
- ✓ Explore vulnerability scans
- ✓ Configure vulnerability scans
- ✓ Review vulnerability scan reports
- ✓ Discuss additional OWASP Top 10 threats
- ✓ Implement additional OWASP Top 10 mitigations

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

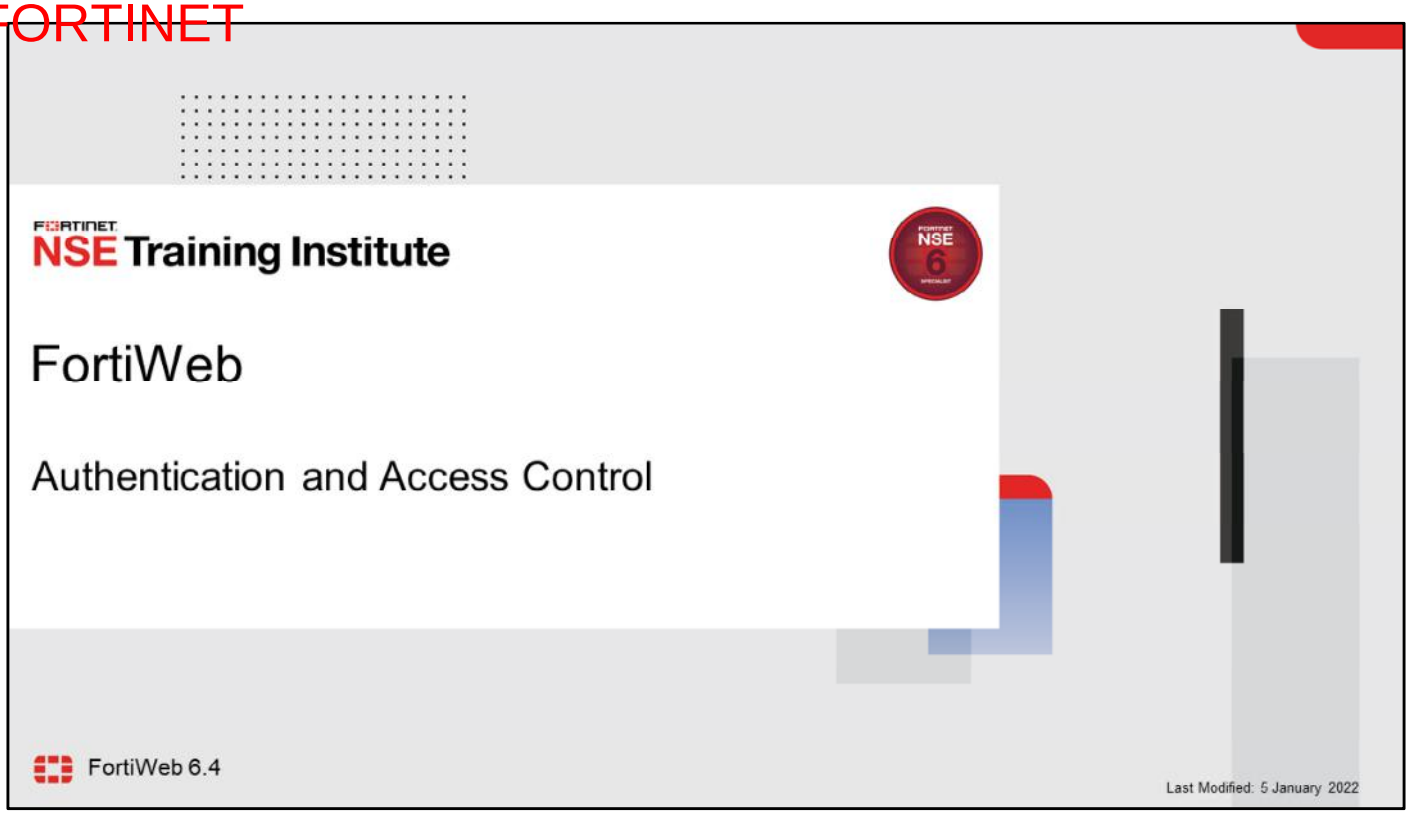
42

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to identify and avoid web application security threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

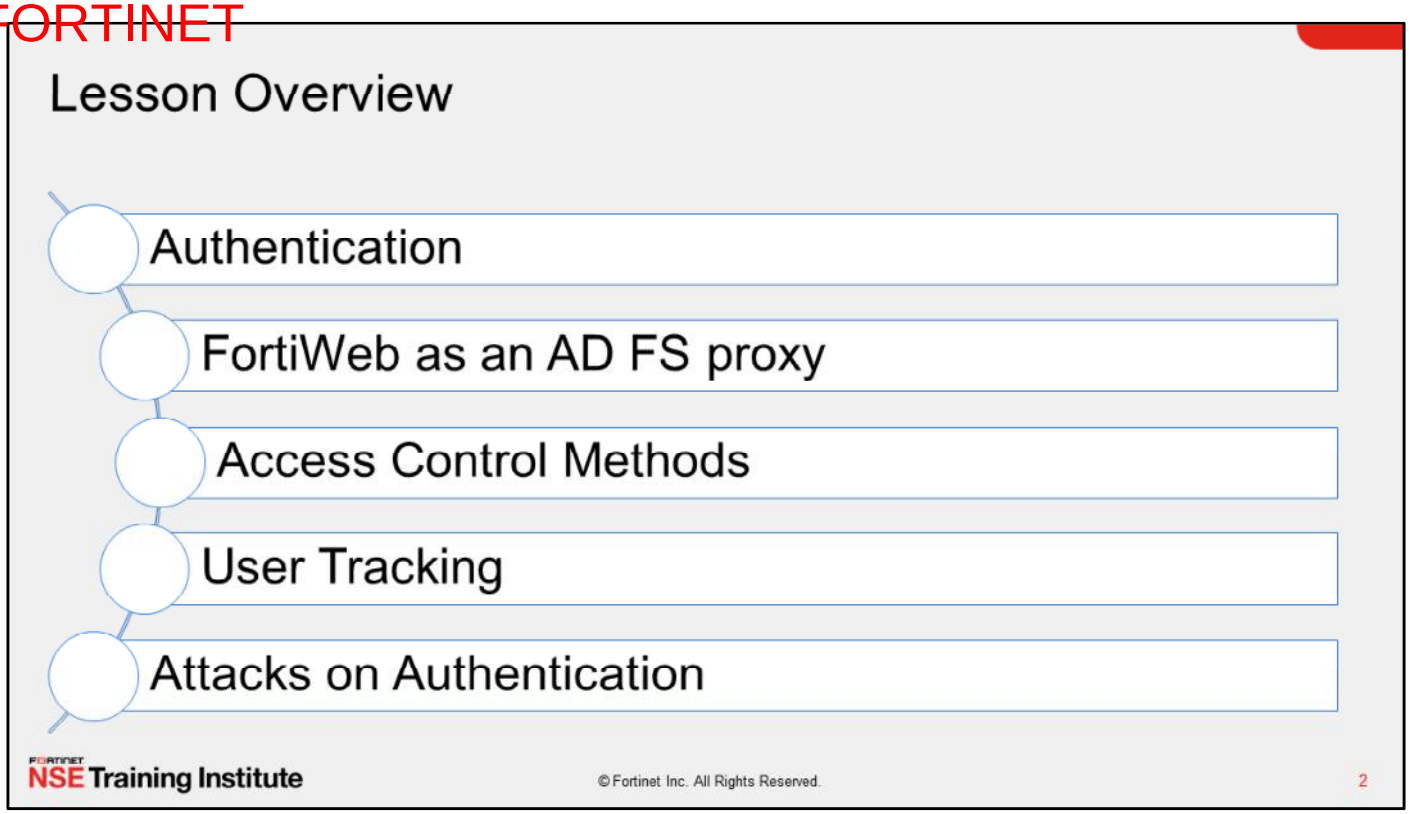
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to add authentication for web applications that don't have it—or where you want to unify the login across multiple applications. You will also learn how to secure the HTTP transactions so that your users' login credentials aren't compromised.

Vouchers & Dumps are Available | WhatsApp +201224560923

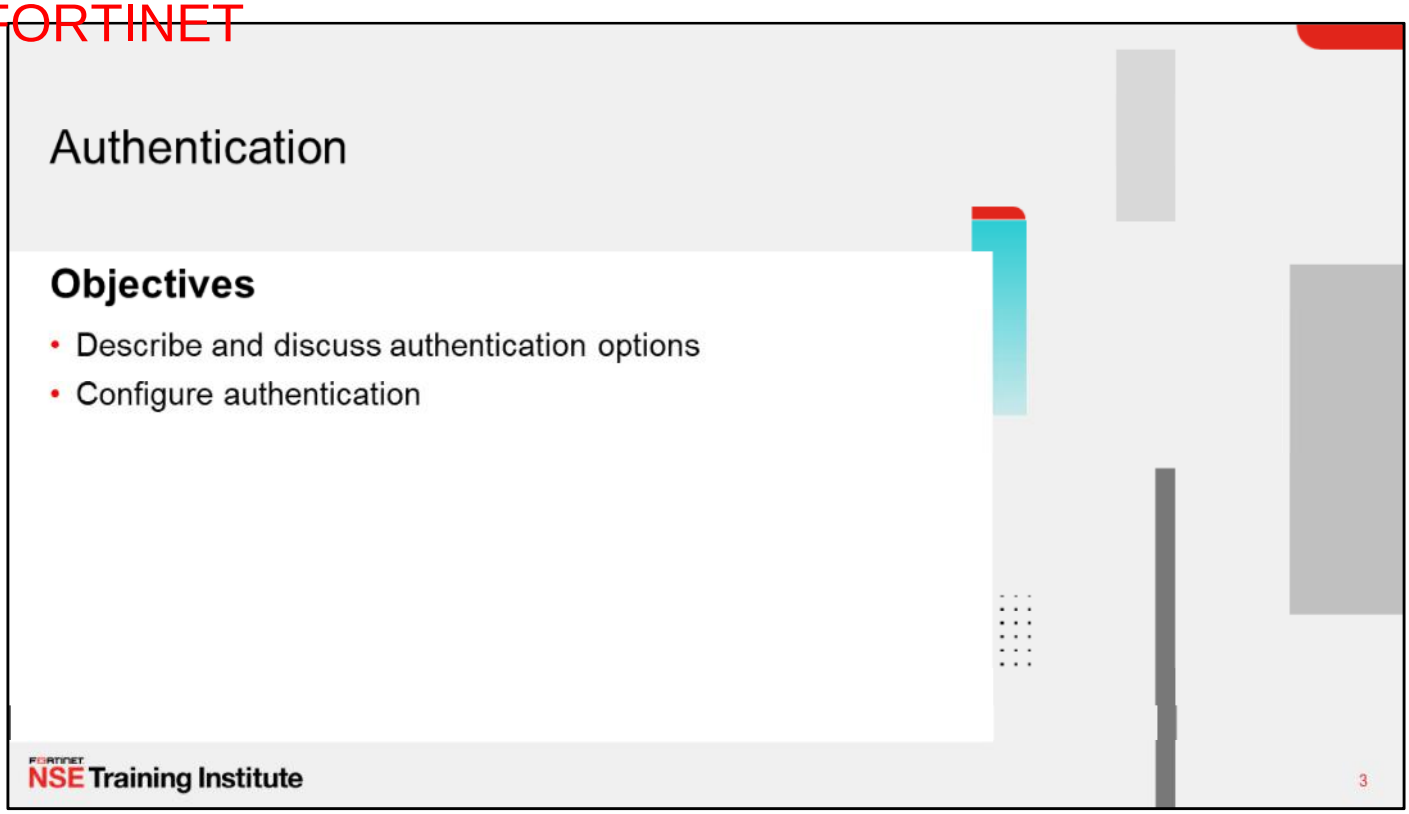
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding and configuring authentication, you will be able to protect your web servers with secure authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Applying HTTP/HTML Form Authentication

- You can configure FortiWeb to prompt users to authenticate before allowing requests
- Supported methods:
  - Accounts on FortiWeb (local)
    - Not supported for site publishing
  - LDAP (Active Directory and more)
  - NTLM
  - RADIUS (FortiAuthenticator and more)

- Steps:
  1. Define user accounts on FortiWeb or remote authentication servers
  2. Define groups and queries to access proper users
  3. Do one of the following:
     - Define authentication rules with authorized realms and user groups, and group rules into an authentication policy
     - Define a site publishing rule with user groups and group rules into a site publishing policy
  4. Apply policy to an inline protection profile
  5. Select a protection profile in a server policy

NSE Training Institute © Fortinet Inc. All Rights Reserved. 4

After you've determined which clients should be allowed to attempt to log in, you need to handle the details of the login itself. If your web application doesn't offer authentication natively, FortiWeb can add authentication before passing the connection to the destination server.

FortiWeb can also strengthen your application's existing authentication. Configure FortiWeb input rules on password strength for URLs that change passwords to prevent users from setting weak passwords that hackers can easily guess or brute force.

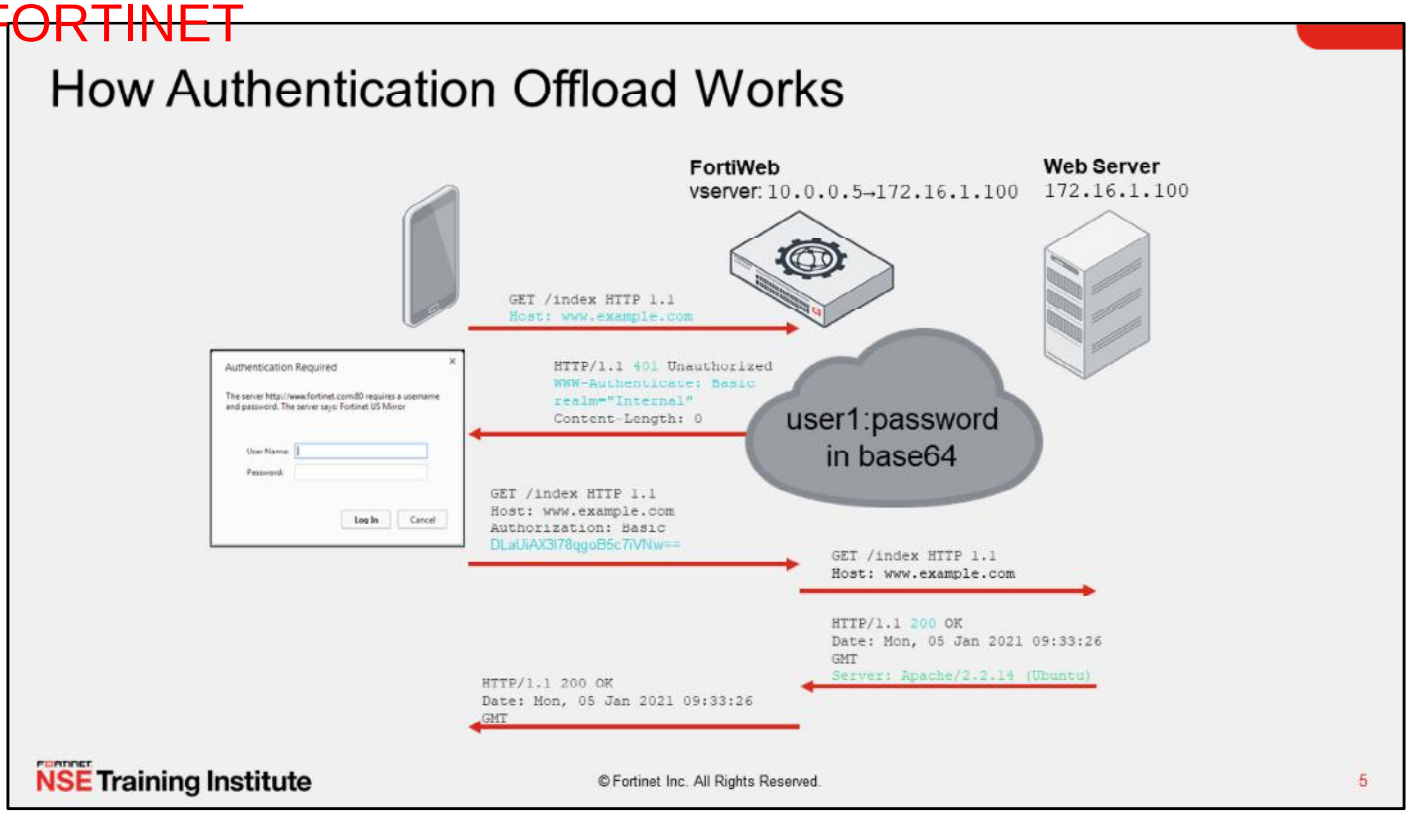
If your web application doesn't have its own native authentication features, FortiWeb authentication rules are a simple way to add them.

Usually, deployments have an existing database of user accounts, such as a Microsoft Active Directory tree. If so, instead of defining all user accounts locally, configure FortiWeb to query the authentication server.

Even if your web application does have authentication, you may still want to use FortiWeb. FortiWeb can delegate the credentials to the back-end web application, yet still cache authenticated sessions locally so that you can apply single sign-on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you add an authentication or site publishing rule, this is what the HTTP transaction looks like.

Notice that the first reply is a 401 error code, with the header that indicates which authentication the client should submit. This triggers the browser's HTTP authentication dialog. When the user submits their username and password, the browser resends the initial request, this time with their authentication details in an HTTP header. Next, FortiWeb forwards the request (with the HTTP authentication header removed) to the backend web server. Since the web server is misconfigured, its reply includes an information disclosure: the associated OS and Apache version. Before it forwards the reply to the client, the FortiWeb information disclosure signature removes the header.

The `Authorization:` header may look encrypted, but it's not. It's only encoded in base64. Use Caution: Use only basic or digest authentication if the passwords are also protected by SSL/TLS!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication Policy vs. Site Publishing

- Site publishing
  - SSO
    - Unlike FortiGate, no FSSO agent
    - FortiGate accepts reused authentication for protected websites in the same SSO domain
  - Logoff URL support
  - HTTP authentication support
  - HTML authentication form support
  - Delegation to back-end server
  - Kerberos, NTLM, 2FA, and more
- Authentication policy
  - Realms
  - HTTP authentication support only
  - Supports local user accounts

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

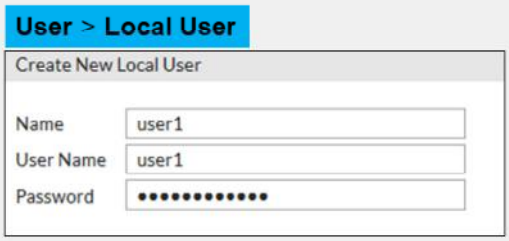
Authentication rules are very simple. If you need more complex features, such as support for single sign-on, logoff URLs, two-factor authentication, and Kerberos delegation, use site publishing rules instead. Site publishing allows access to a web server after the user authenticates to the FortiWeb. FortiWeb can then treat additional sessions and connections from the client as authenticated and allow access to the protected web servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Local User Accounts

- Accounts and passwords are stored on the FortiWeb flash disk
- Cannot be used for site publishing
- Not practical if you have many users
  - Query a RADIUS or directory server instead!



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

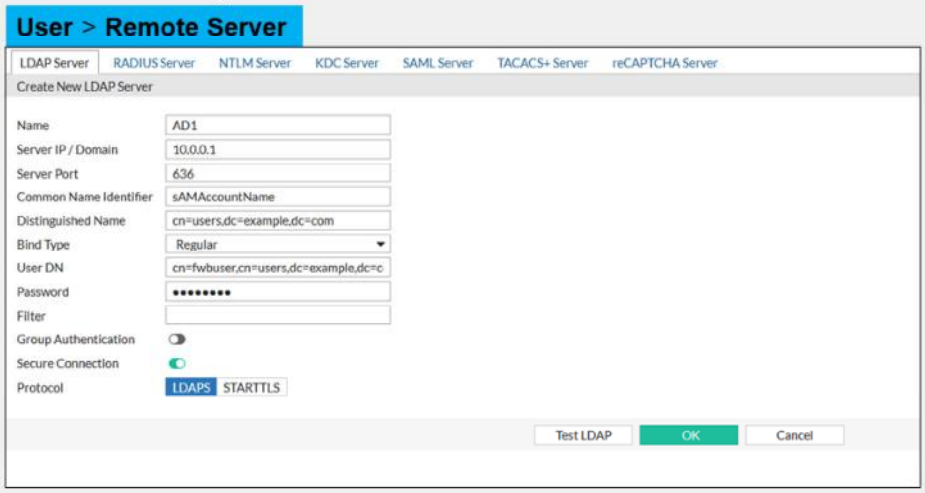
When configuring any kind of authentication the first thing to do is configure or access user accounts. With FortiWeb, you can configure them locally. But, if you have many users, local configuration is not the most practical way to define accounts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Queries for Remote User Accounts

- Accounts and passwords stored in a remote authentication server
- Currently supports LDAP, RADIUS, NTLM, KDC, SAML, and TACACS+
- Upon HTTP request, FortiWeb queries the server



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

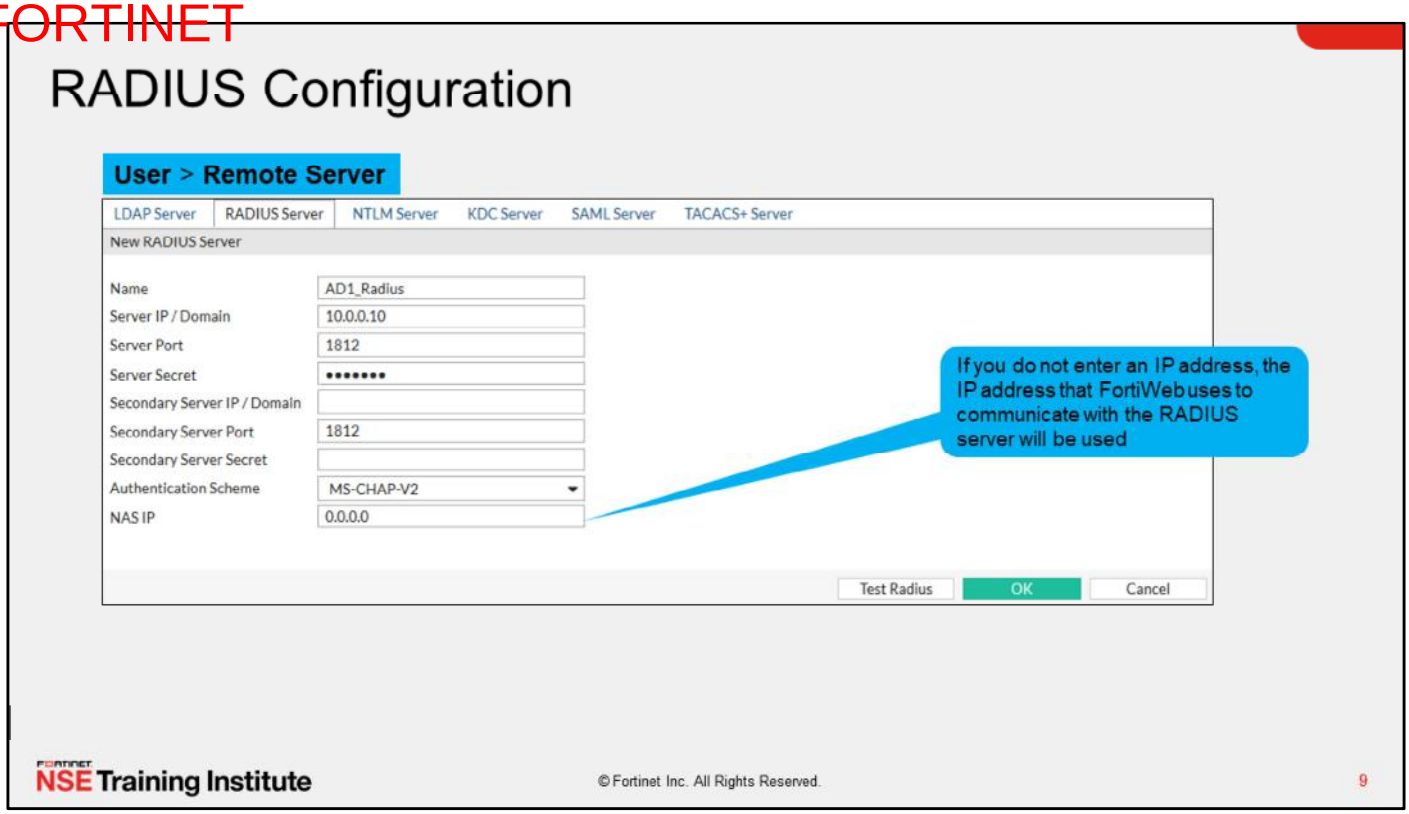
8

If you have many users, you should configure a query. Whenever someone tries to log in, FortiWeb contacts the query server to check whether the credentials are valid.

In this example, FortiWeb is querying a Microsoft Active Directory server using the Lightweight Directory Access Protocol over SSL (LDAPS) protocol. Directory tree structures vary according to the schema, so in IBM Lotus Notes or another application, the common name identifier, distinguished names, and query strings are different.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb can use RADIUS queries to authenticate and authorize end-users' HTTP requests.

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. The FortiWeb authentication feature uses RADIUS user queries to authenticate and authorize HTTP requests. FortiWeb does not fully support RADIUS accounting because the HTTP protocol does not support active logouts and can only passively log users when their connection times out. FortiWeb does support RADIUS authentication with realms (accounts such as admin@example.com).

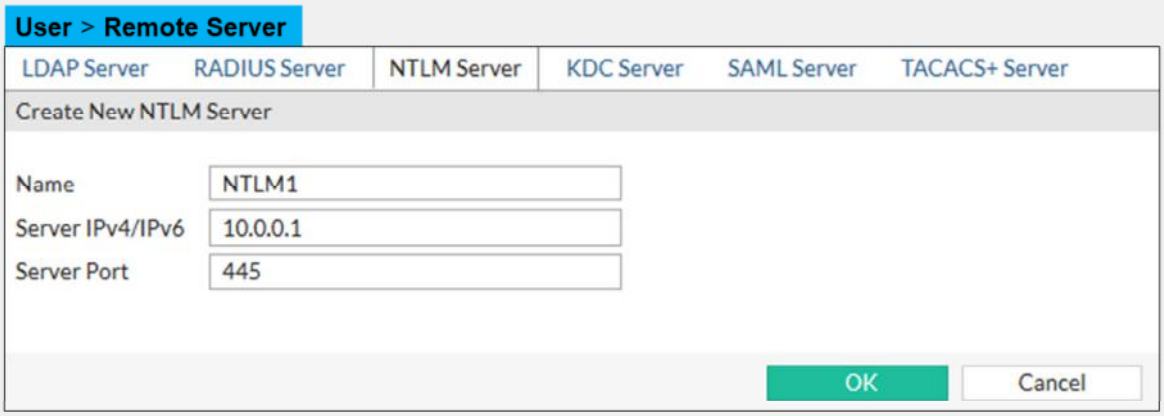
To authenticate a user or administrator, FortiWeb sends the user's credentials to RADIUS for authentication. If the RADIUS server replies to the query with a signal of successful authentication, FortiWeb authenticates the client. If RADIUS authentication fails or the query returns a negative result, FortiWeb refuses the connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

NT LAN Manager (NTLM)

- FortiWeb supports NTLM v1 and NTLM v2



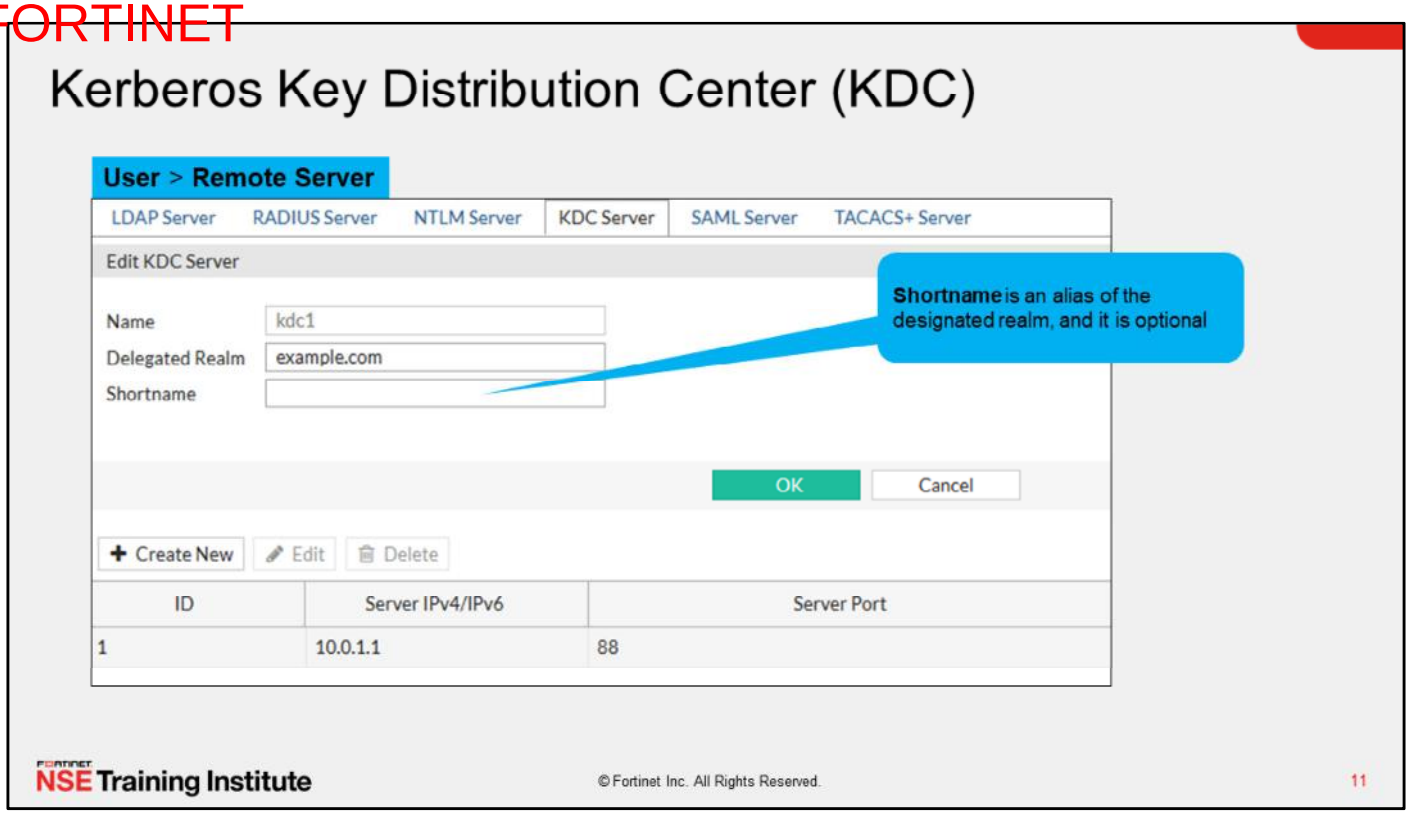
NSE Training Institute © Fortinet Inc. All Rights Reserved. 10

You can make NT LAN Manager (NTLM) queries to a Microsoft Windows or Active Directory server that is configured for NTLM authentication. FortiWeb supports both NTLM v1 and NTLM v2.

FortiWeb can use NTLM queries to authenticate and authorize HTTP requests.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

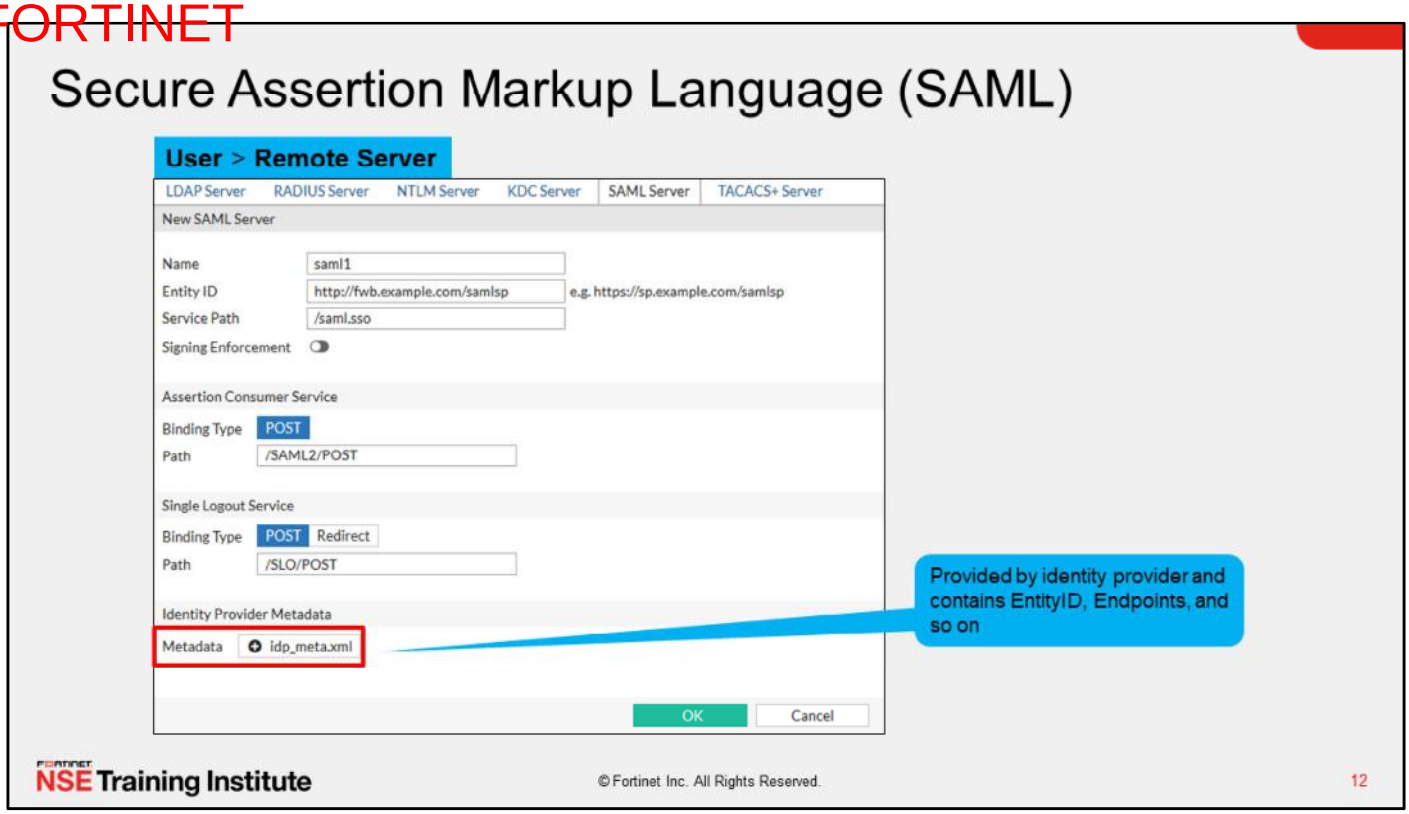


You can specify a Kerberos Key Distribution Center (KDC) that FortiWeb can use to obtain a Kerberos service ticket for web applications on behalf of clients.

Because FortiWeb determines the KDC to use based on the realm of the web application, you do not have to specify the KDC in the site publish rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

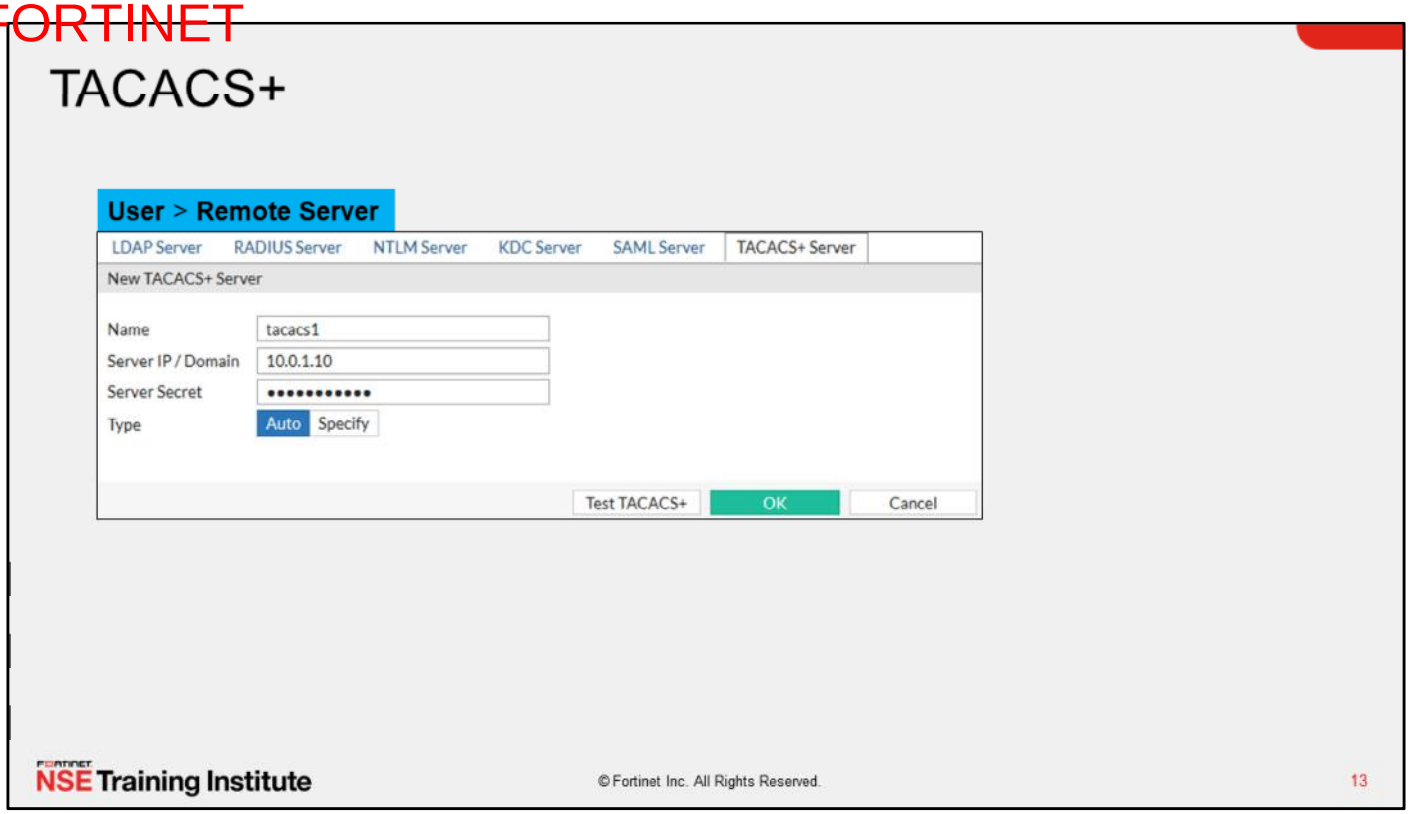


You can use a SAML server in a site publish rule to handle client authentication for web browser single sign-on (SSO).

SAML is an open standard for exchanging authentication and authorization data between parties and is often used for exchanging such data between an identity provider and a service provider.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb supports TACACS+ authentication for FortiWeb administrator users. FortiWeb can also use TACACS+ queries to authenticate administrator access to the web GUI or CLI.

FortiWeb sends the administrator's credentials to the TACACS+ server for authentication. If the TACACS+ server replies to the query with a signal of successful authentication, FortiWeb authenticates the client. If TACACS+ authentication fails or the query returns a negative result, FortiWeb refuses the connection.

If the TACACS+ server is slow to respond, you may need to adjust the authentication timeout setting to prevent the query from failing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Grouping Users and Queries

- Cannot put users in authentication rules directly
- Must put at least one local user or query in a group, then reference it in an authentication rule

User > User Group > User Group

Edit User Group

Name: usergroup1

Auth Type: Basic | Digest | NTLM

OK | Cancel

+ Create New | Edit | Delete | Insert | Move

ID	User Type	Name
1	Local User	user1
2	LDAP User	AD1
3	RADIUS User	AD1_Radius

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

To denote a set of users authorized to request specific URLs when configuring HTTP authentication offloading, you must create user groups.

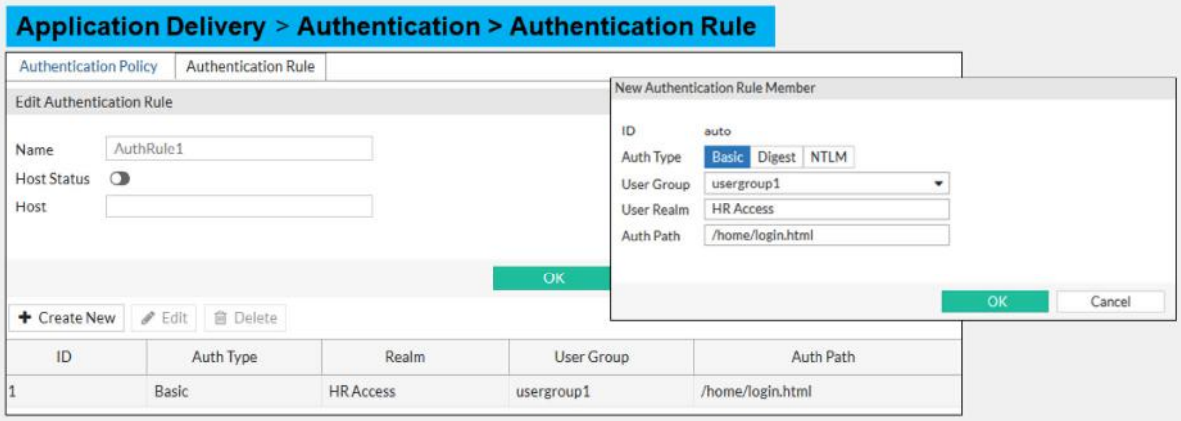
A user group can include a mixture of local end-user accounts, LDAP queries, RADIUS queries, and NTLM queries. Therefore, a user group can consist of accounts or a set of queries.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication Rule

- Authorize user groups for a realm or URL in authentication rules



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

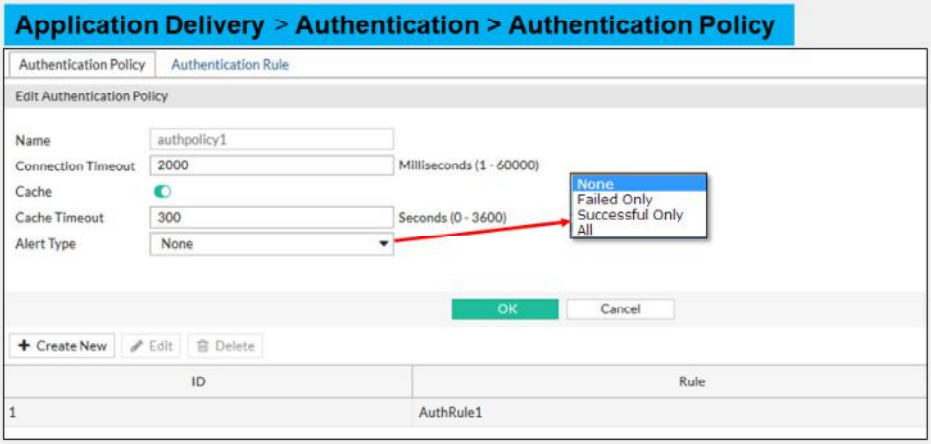
Reference the user group when you define an authentication rule. Authentication rules define who has access to each URL. Note that some HTTP authentication styles like NTLM are not supported by all query types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication Policy

- Apply authentication rules using an authentication policy
- Policy includes connection and cache timeout and what to log (**Alert Type**)
- To apply, select the policy in an inline protection profile



NSE Training Institute © Fortinet Inc. All Rights Reserved. 16

Next, group your authentication rules in an authentication policy. This creates a set of authentication rules, and specifies whether FortiWeb tracks login failures, the connection timeout, and any authenticated HTTP sessions in the cache.

Using faster cache timeouts can improve both security and performance by helping to prevent unattended computers from becoming possible attack vectors and by reducing RAM usage. Fast cache timeouts must be long enough for web applications where users must fill out long forms, such as contact information or tax data, so that the authentication session does not time out between each page submission.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSO/Site Publishing on FortiWeb

1. Client visits application A
2. FortiWeb requests client authentication
3. Client submits correct credentials
4. FortiWeb queries authentication server, receives OK signal:
   a. No FSSO agent installed—*not* like FortiAuthenticator
   b. FortiWeb stores verified HTTP sessions and authorized websites (SSO domain) in RAM
5. FortiWeb forwards HTTP request to back-end web servers
6. Application A replies to client
7. Client visits application B and so on:
   a. FortiWeb does not request client for reauthentication until the session times out
   b. If delegation is enabled, FortiWeb forwards either Kerberos service token or credentials cache to next backend web application

NSE Training Institute © Fortinet Inc. All Rights Reserved. 17

Universities, enterprises, and other large organizations may protect multiple web applications and want to reduce the number of times that a user must log in. If you don't have administrative privileges on the web servers, Fortinet SSO is not an option. In this case, you can enable the agentless SSO feature on FortiWeb, also known as site publishing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Pool

- Contains one or more servers that use either LDAP or RADIUS
- References the site publishing rule

Application Delivery > Site Publish > Authentication Server Pool

Edit Authentication Server Pool

Name serverpool1

OK Cancel

Create New | Edit | Delete | Insert | Move

ID	Authentication Validation Method	LDAP Server	RADIUS Server	RSA SecurID
1	LDAP	AD1	-	-
2	RADIUS	-	AD1_Radius	Disable

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

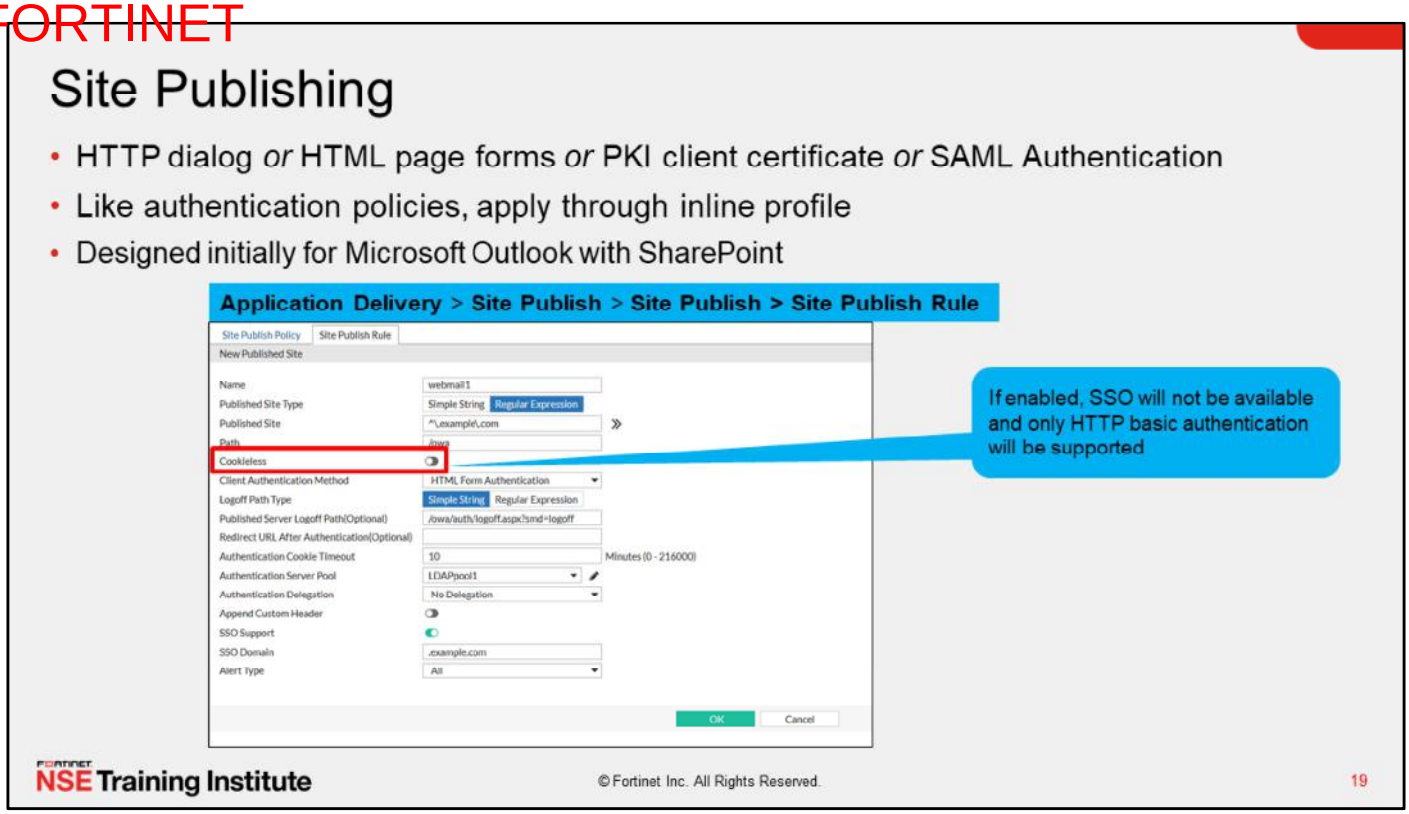
18

When you configure a site publishing rule that offloads authentication for a web application to FortiWeb, you use an authentication server pool to specify the method and server that FortiWeb uses to authenticate clients.

FortiWeb attempts to authenticate clients using the server at the top of the list of pool members, and then continues to the next member in the list if the authentication is unsuccessful, and so on. You can use the list options to adjust the position of each item in the list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Site publishing is a new, more sophisticated gateway authentication method. You can use it to replace applications like Microsoft Forefront Threat Management Gateway (TMG).

Site publishing supports client certificates and HTML form-based authentication as well as HTTP authentication. It also supports delegation, agentless SSO, and two-factor authentication.

If you are using a RADIUS authentication query, site publishing also supports RSA SecurID in addition to, or instead of, a password.

Both LDAP and RADIUS queries support plain HTTP and Kerberos delegation. Kerberos delegation can be integrated with PKI client certificates. The certificate delivers a user name and public key, but also is a selector for the key tab. To use it, select **Client Certificate Authentication** and **Kerberos Constrained Delegation**, then specify:

- Which previously uploaded key tab file to use to create and validate service tickets
- The location in the certificate of the field that contains the user name

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Site Publishing (Contd)

- No Delegation: Web server *not* configured to authenticate with FortiWeb
- Delegation: FortiWeb keeps `Authorization:` header in request, forwards to web server—necessary if web applications have native authentication
  - HTTP Basic: Keep username and password in base64
  - Kerberos: Verifies username and password, but forwards service ticket instead
    - Service ticket: Token that is encrypted by FortiWeb, decrypted by web application *not* username and password
    - Requires key tab set up on server
  - NTLM: Challenge/response protocol to verify identity of clients
    - If the POST method request triggers NTLM authentication, the request body cannot exceed 100M.

NSE Training Institute © Fortinet Inc. All Rights Reserved. 20

One important advantage of site publishing over simple authentication rules is the ability of FortiWeb to forward credentials to the web application after it verifies the login. Many modern web applications have their own authentication dialogs, so if you want to use agentless SSO, then FortiWeb needs the credentials, but so do the protected web applications.

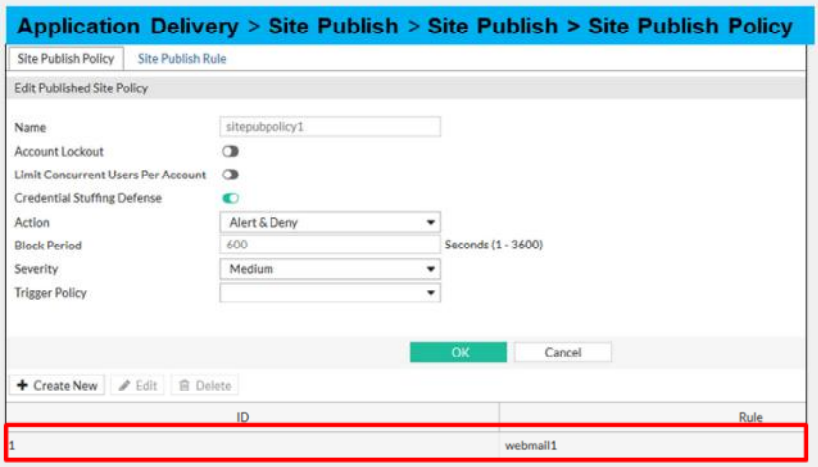
Kerberos does not use the same credentials that the user submitted. Instead, Kerberos uses tokens encrypted with a private key that you designate on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Site Publishing (Contd)

- Link site publish rule with site publish policy
- Select site publish policy in an inline web protection profile

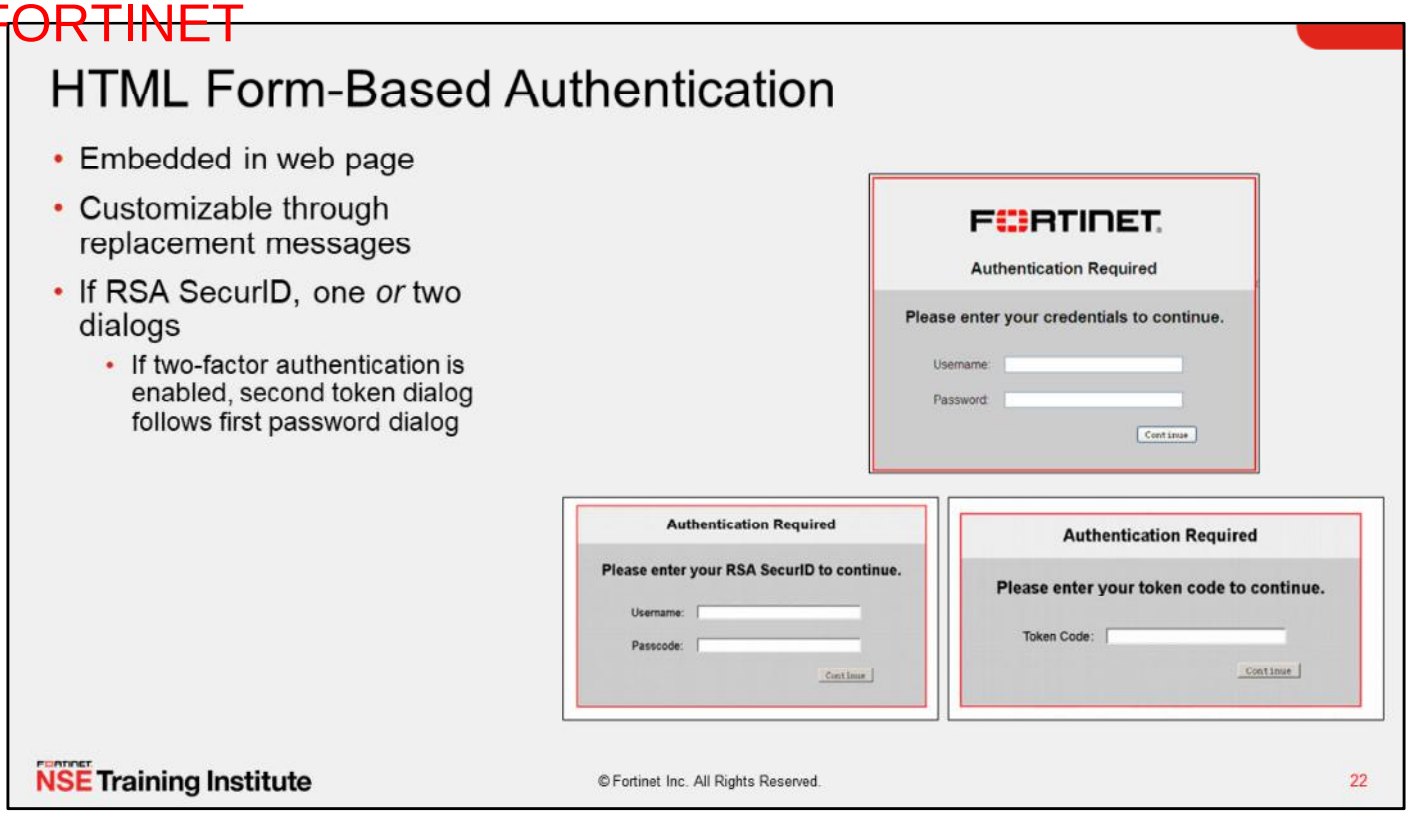


NSE Training Institute © Fortinet Inc. All Rights Reserved. 21

You can configure the account lockout feature if you want to prevent users from making further attempts to login after a specified number of failed login attempts. You can limit the number of concurrent logins per account.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



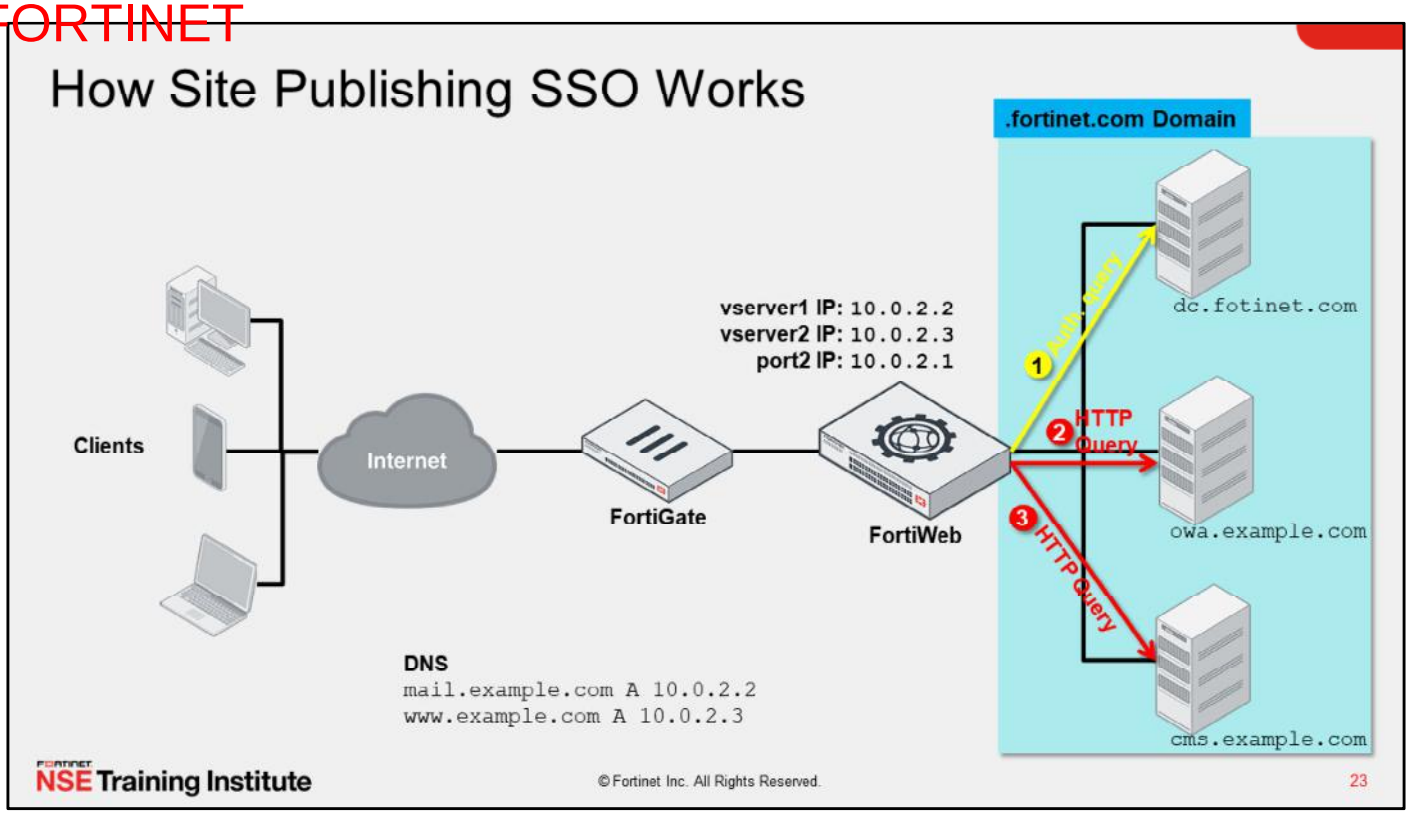
When configuration is complete, the dialog that FortiWeb site publishing opens in users' browsers can be either the HTTP browser pane that you saw previously, or an HTML web page with a form, like the one shown on this slide. Alternatively, FortiWeb invisibly authenticates the user by validating a personal certificate.

If FortiWeb presents a dialog, its appearance varies by the type of authentication tokens that users must enter:

- Username and password
- Username and RSA SecurID passcode
- Username and password then two-factor authentication token, such as RSA SecurID

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When the client authenticates with any website in the SSO domain, FortiWeb caches the credentials in an authentication session. If the user continues to use web applications in that domain, FortiWeb silently allows the user to continue accessing them, forwarding (that is, *delegating*) credentials to each web application, if necessary.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which of the following features is a site publishing-only feature?
   A. Basic HTML (401) authentication
   ✓ B. Single sign-on (SSO)
   C. Local User Authentication

2. Which of the following authentication methods is not supported by FortiWeb?
   ✓ A. PAP
   B. LDAP
   C. TACACS+
   D. Kerberos

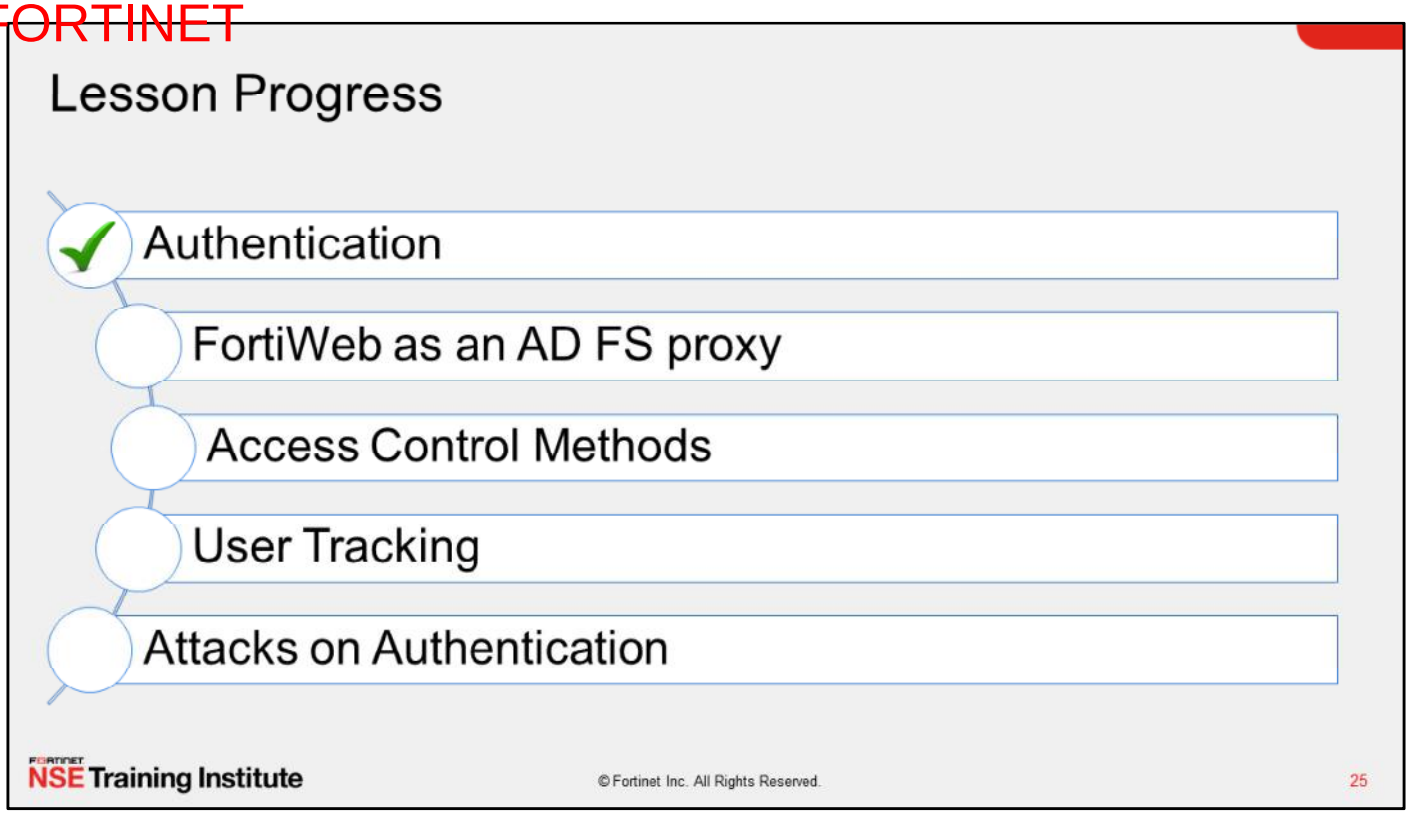
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

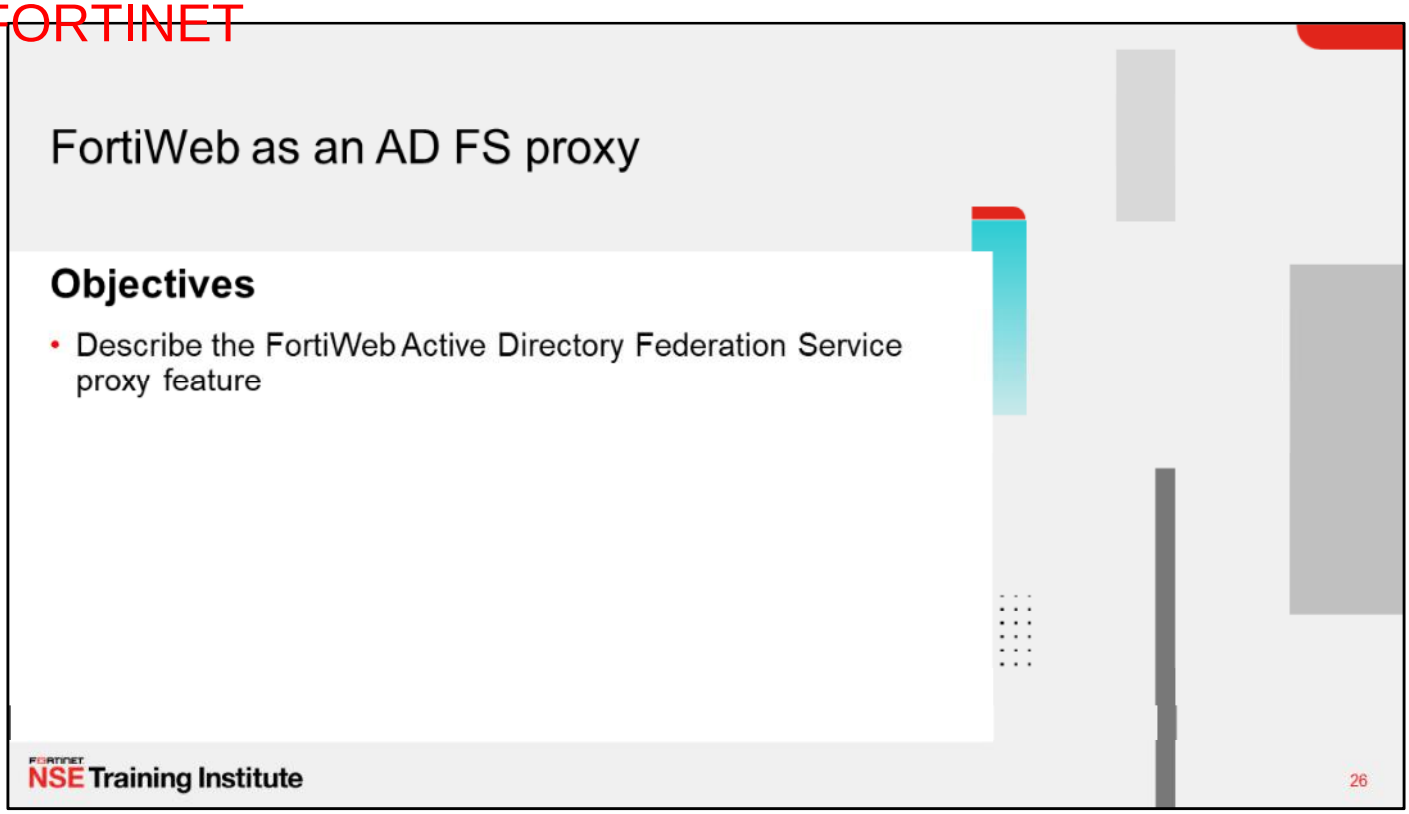


Good job! You now know how to implement authentication features on FortiWeb.

Now, you will learn about how to configure FortiWeb as an AD FS proxy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiWeb as an AD FS proxy, you will be able to configure the AD FS Proxy feature on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb as an AD FS Proxy

- AD FS is a Microsoft SSO solution
- AD FS server usually deployed on internal network
- Potential issues with internet-facing applications
  - External user must authenticate with the web application
  - Web application attempts to redirect to AD FS server
  - External user doesn't have access to the AD FS server and authentication fails
- FortiWeb solves issue by acting as AD FS proxy
- FortiWeb supports AD FS 3.0, 4.0, and 5.0 and Microsoft Server API versions 1 and 2

NSE Training Institute © Fortinet Inc. All Rights Reserved. 27

Active Directory Federation Services (AD FS) is a single sign-on (SSO) solution created by Microsoft. It provides users with authenticated access to applications located across organizational boundaries. Developed to provide flexibility, AD FS gives organizations the ability to simplify the user experience: users need to remember only a single set of credentials to access multiple applications through SSO.

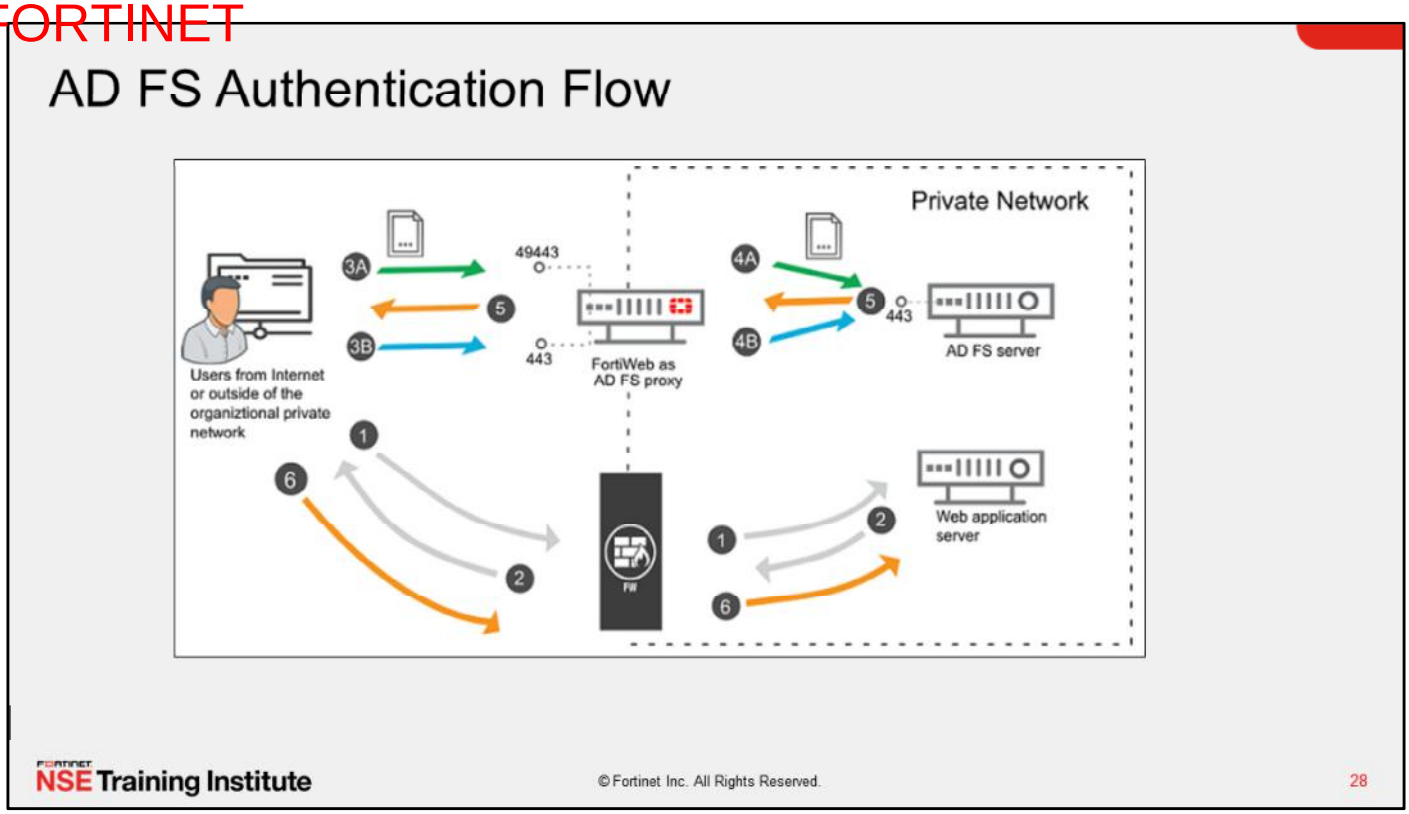
Usually, the AD FS server is deployed inside your organization's internal network. However, in some circumstances, you can deploy FortiWeb as an AD FS proxy in your organization's perimeter network. For example, an external user cannot access a web application that redirects the user to the internal AD FS server for identity authentication. However, if you deploy FortiWeb as an AD FS proxy, the web application requests a security token from FortiWeb, which then forwards the request to the internal AD FS server. This sequence is not apparent to the user, because the proxy and the AD FS use the same URL.

Aside from playing the role of AD FS proxy, FortiWeb can also act as a web application firewall for your AD FS servers. You can leverage the powerful threat protection features on FortiWeb to keep your AD FS servers safe from vulnerability exploits, bots, malware uploads, DoS attacks, APTs, and zero-day attacks.

FortiWeb supports AD FS version 3.0 (on Windows Server 2012 R2), AD FS version 4.0 (on Windows Server 2016), and AD FS version 5.0 (on Windows Server 2019). From 6.3.0, FortiWeb has added support for Microsoft Server API version 2. In versions earlier than 6.3.0, FortiWeb supports only Microsoft Server API version 1.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

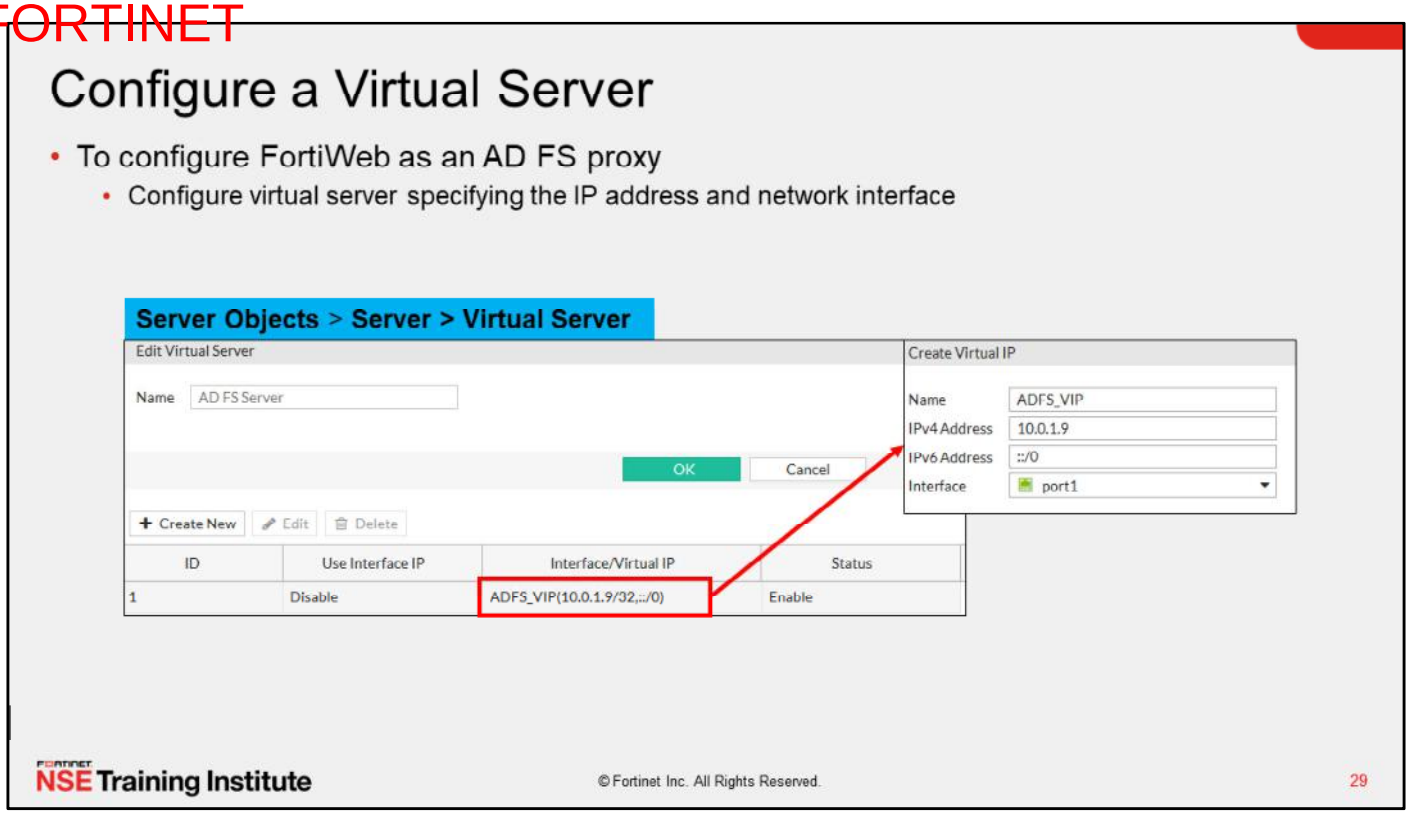


Here you can see the workflow of the AD FS authentication process when using FortiWeb as an AD FS proxy. The process is as follows:

- Step 1 – An external user accesses a web application that requires authentication.
- Step 2 – The web application responds with a URL that redirects the user to the AD FS server for identity authentication.
- Step 3a – The user sends a certificate authentication request to FortiWeb over port 49443.
- Step 4a – FortiWeb uses the locally installed CA to verify the user certificate. If verified, FortiWeb forwards the authentication certificate to the AD FS server.
- Step 3b – The user provides a user name and password to FortiWeb over port 443.
- Step 4b – FortiWeb forwards the user name and password to the AD FS server.
- Step 5 – Once authenticated, the AD FS server provides the user with an authentication claim.
- Step 6 – The user's browser forwards the authentication claim to the web application, confirming that the user has been authenticated by the AD FS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

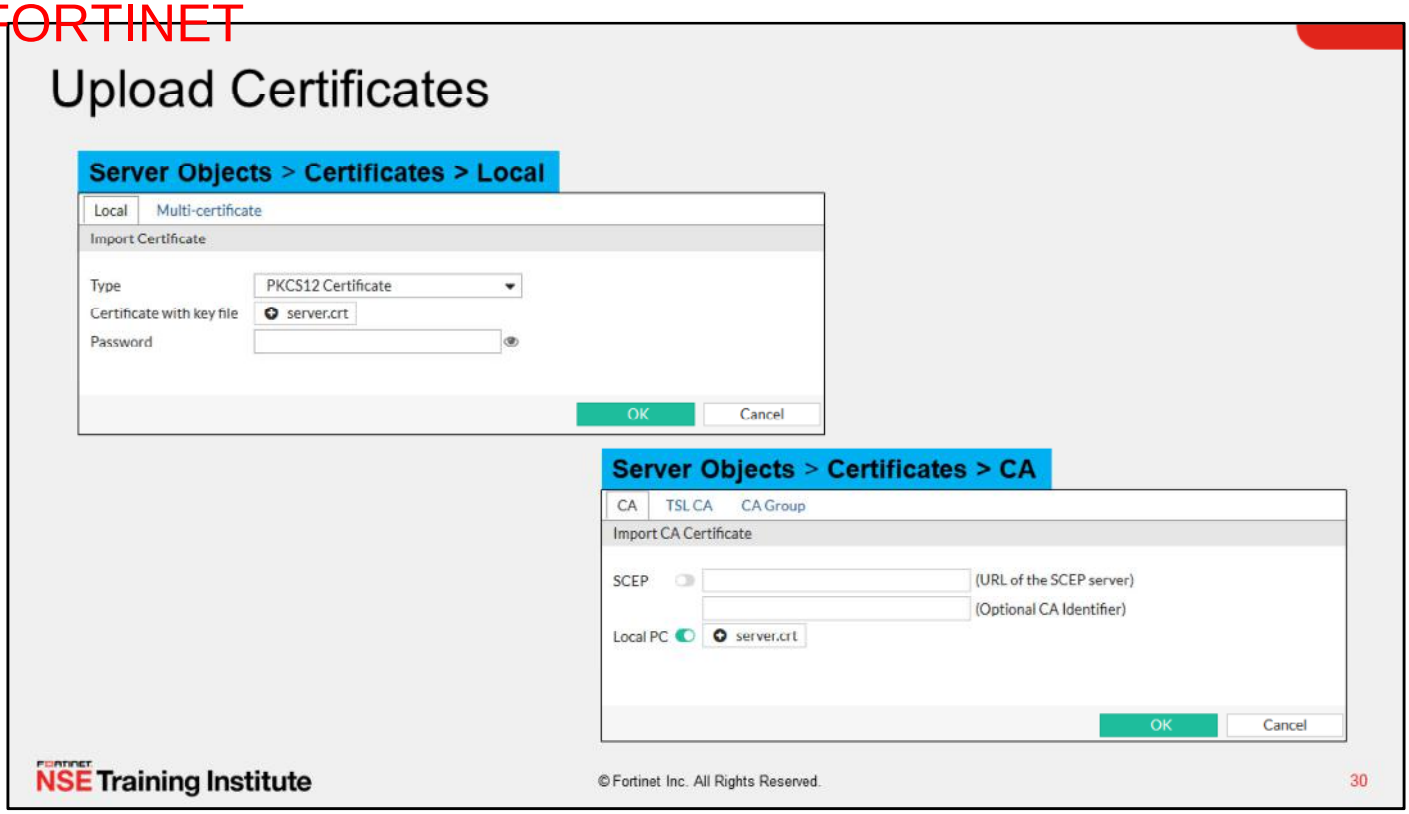
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The virtual server configuration defines the network interface and IP address where traffic destined for a server pool arrives. This is the public-facing address that external traffic is destined for. When FortiWeb receives traffic destined for a virtual server, it can then forward the traffic to an AD FS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

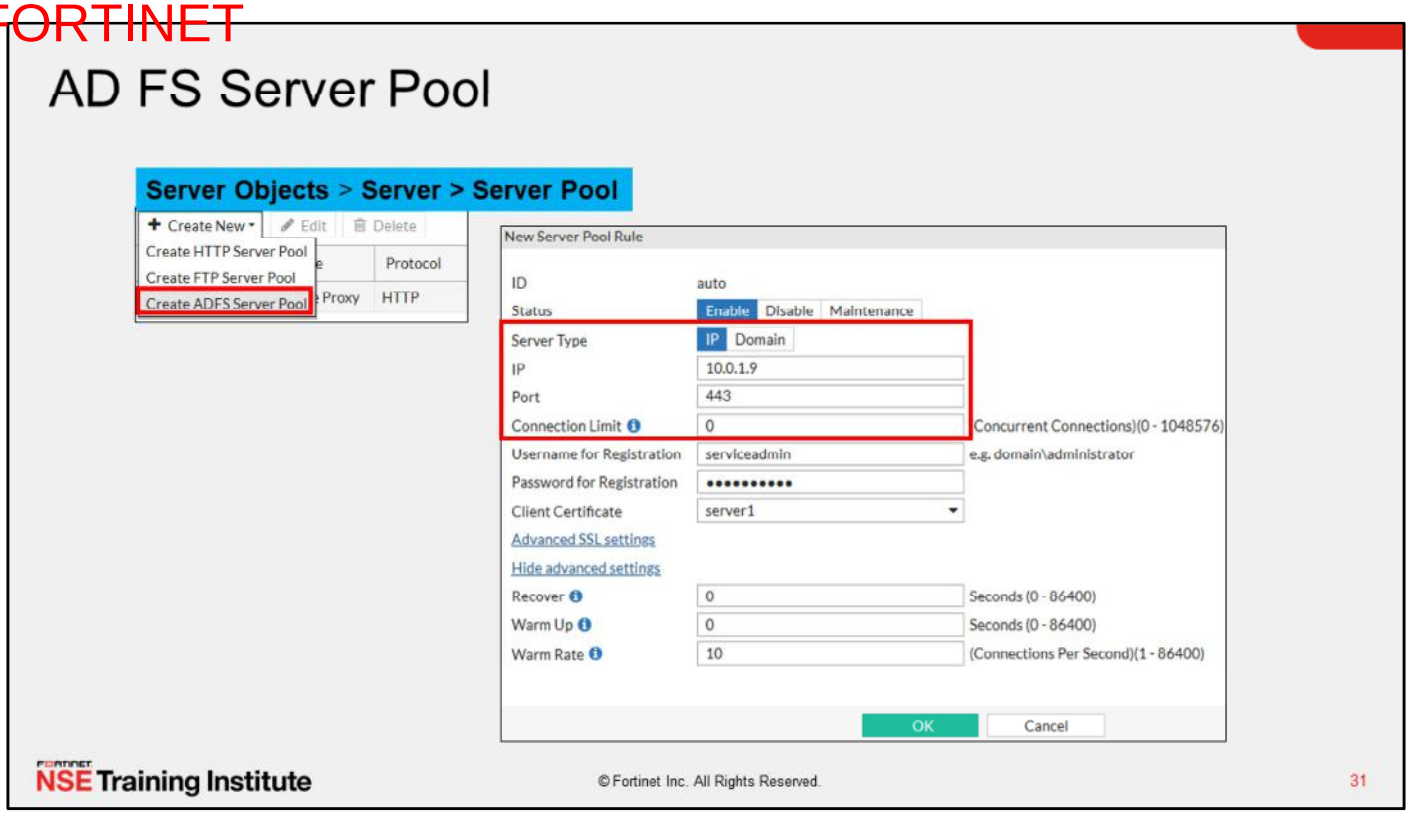


The AD FS servers require a valid client certificate to secure the connections. You need to upload the client certificate for FortiWeb, then reference this certificate in the server pool settings. For FortiWeb to authenticate client certificates, you must upload trusted CA certificates to FortiWeb. Certificate validation rules tell FortiWeb which set of CA certificates to use when it validates personal certificates. They also specify a CRL, if any, if the client's certificate must be checked for revocation.

To use CA certificates in a certificate verification rule for PKI authentication, you will need to create a CA group for the CA certificate(s) that you want to include.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



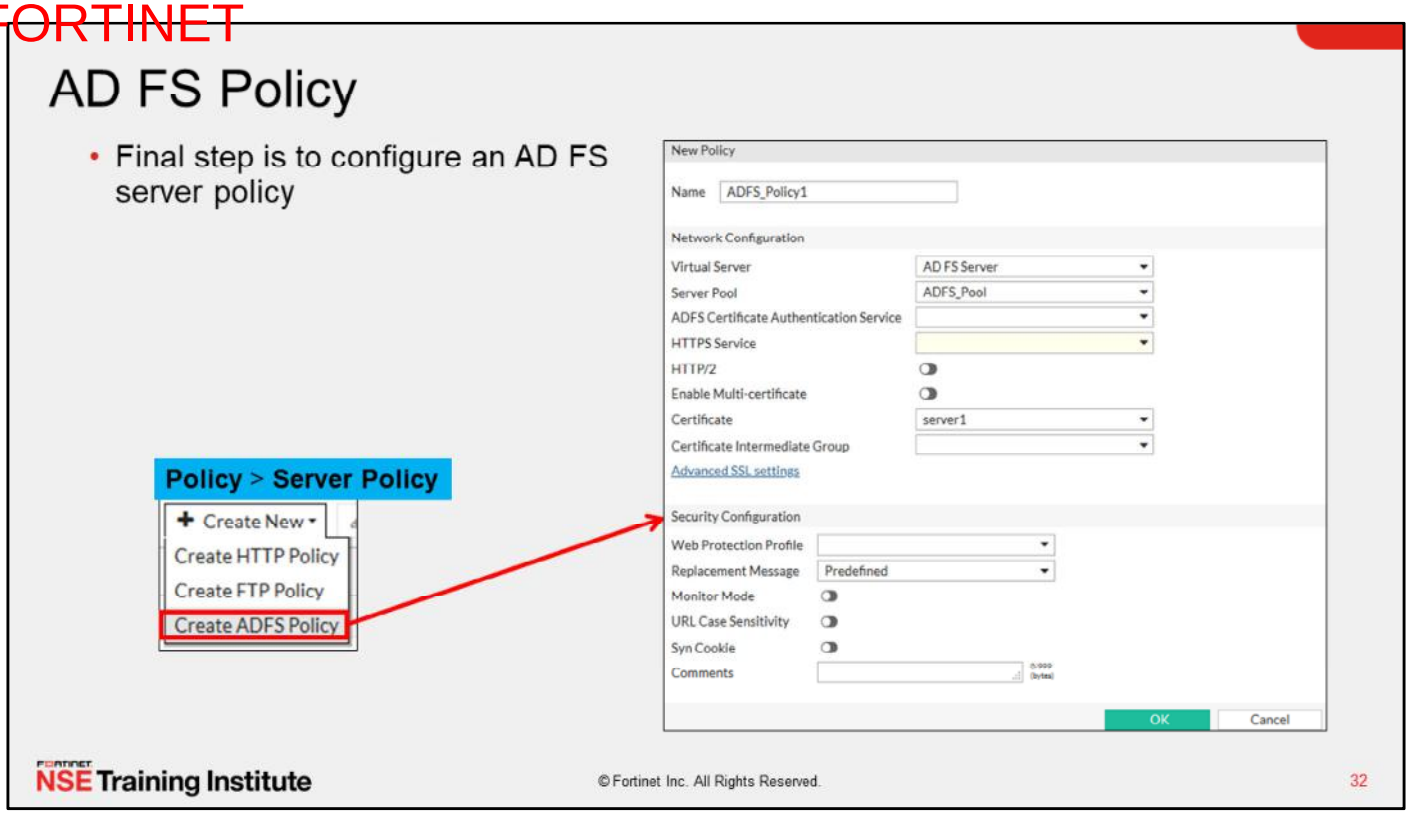
After configuring a virtual server and importing the required certificates, you need to create a server pool that contains the AD FS server.

When FortiWeb receives traffic destined for the virtual server, it forwards the traffic to the server pool containing the AD FS servers.

Note that ADFS server pools are a hidden feature and need to be unlocked under **System > Config > Feature Visibility**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The AD FS policy is what ties all the previously discussed elements together. Here you identify which virtual server, server pool, and certificates will be applied to allow communication to the AD FS servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which scenario needs FortiWeb to act as a proxy for AD FS?
   - ✓ A. Internet-facing applications redirecting to an internal AD FS server
   - B. Internal-facing applications redirecting to an internal AD FS server

2. Which certificate needs to be imported into FortiWeb to allow it to authenticate AD FS?
   - A. External User Certificate
   - ✓ B. Certificate Authority Certificate
   - C. Webserver Certificate
   - D. AD Signing Certificate

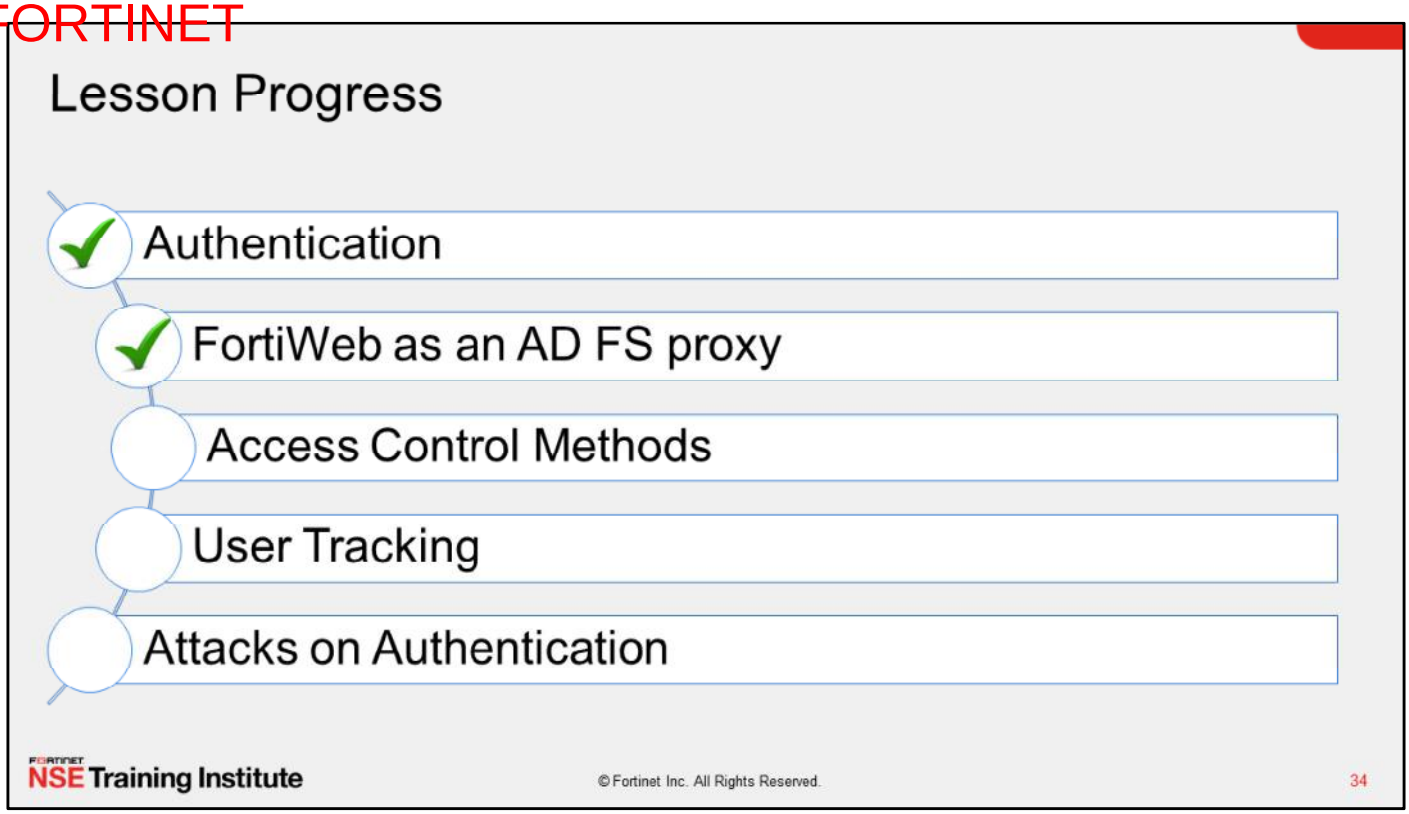
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now know how to use the FortiWeb as an AD FS Proxy.

Now, you will learn about different access control methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

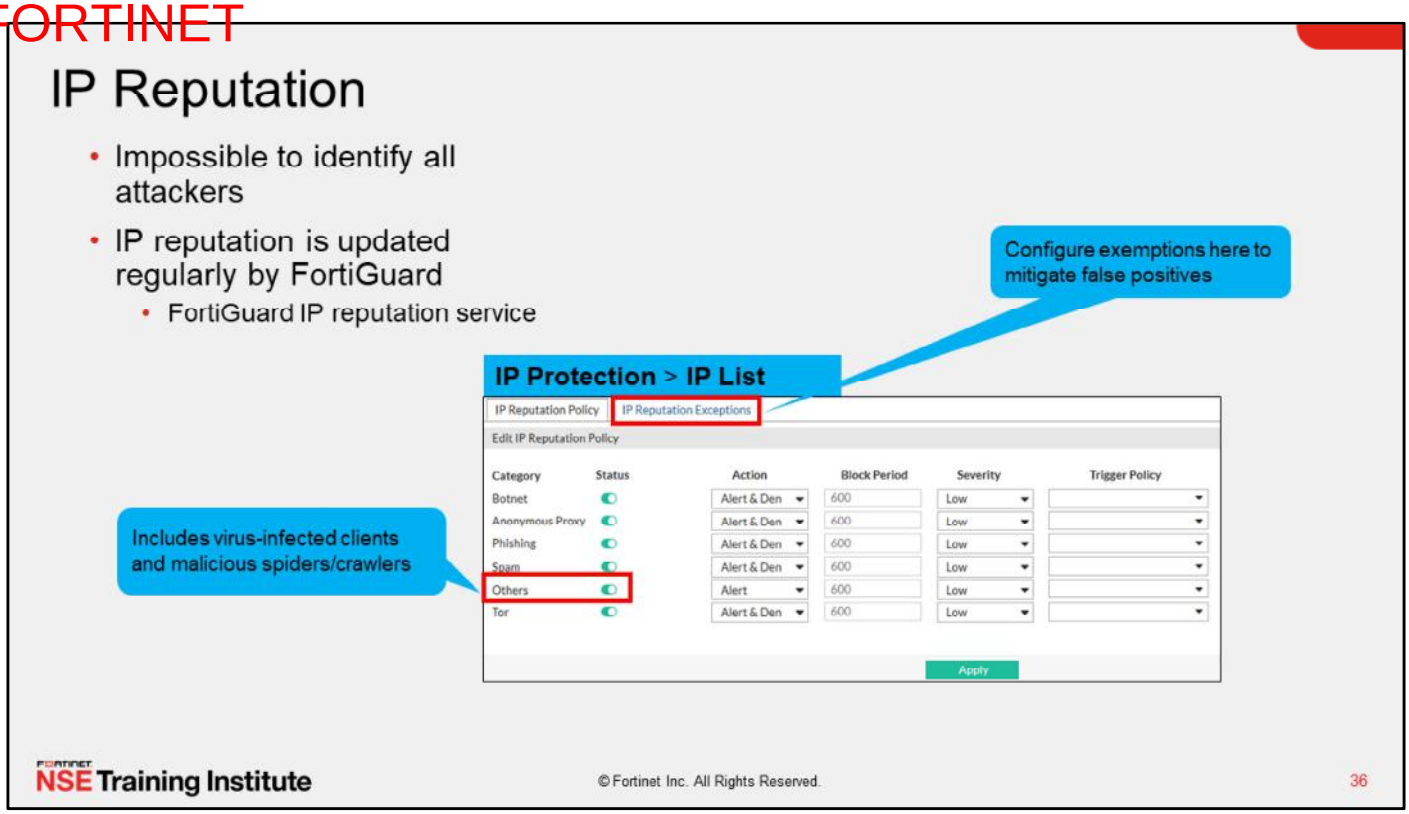
DO NOT REPRINT
© FORTINET
Brave-dumps.com

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding access control methods, you will be able to ensure that user information is protected during authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can block requests from clients based on their source IP address, their current reputation known to FortiGuard, or on their geolocation.

It is an impossible task to manually identify and block all known attackers such as botnets, spammers, DDoS, and so on.

However, you can configure FortiWeb to use the FortiGuard IP Reputation service, which leverages many techniques to identify compromised and malicious clients so you can block attackers before they target your servers. IP Reputation is accurate and frequently updated.

Advanced Persistent Threats (APTs) often mask their source IP address using anonymizing proxies. While casual attackers will move on to easier potential targets if their initial attempts fail, APTs persist until they achieve a successful breach. Early warning is critical. Therefore, even if some innocent anonymous clients use your web servers and you do not want to block them, you still may want to log proxied anonymous requests.

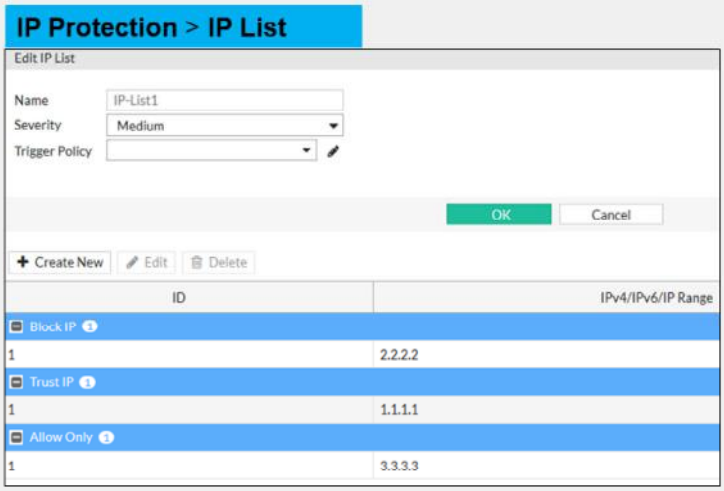
Filtering your other attack logs by these anonymous IP addresses can help you to locate and focus on dangerous requests from these IP addresses, whether you want to use them to configure a defense, for law enforcement, or for forensic analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IP List

- Blocklisted IP addresses
- Trusted IP addresses
  - Exempted from *most* (not all) protection scans
- Unlisted? Then FortiWeb will scan



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

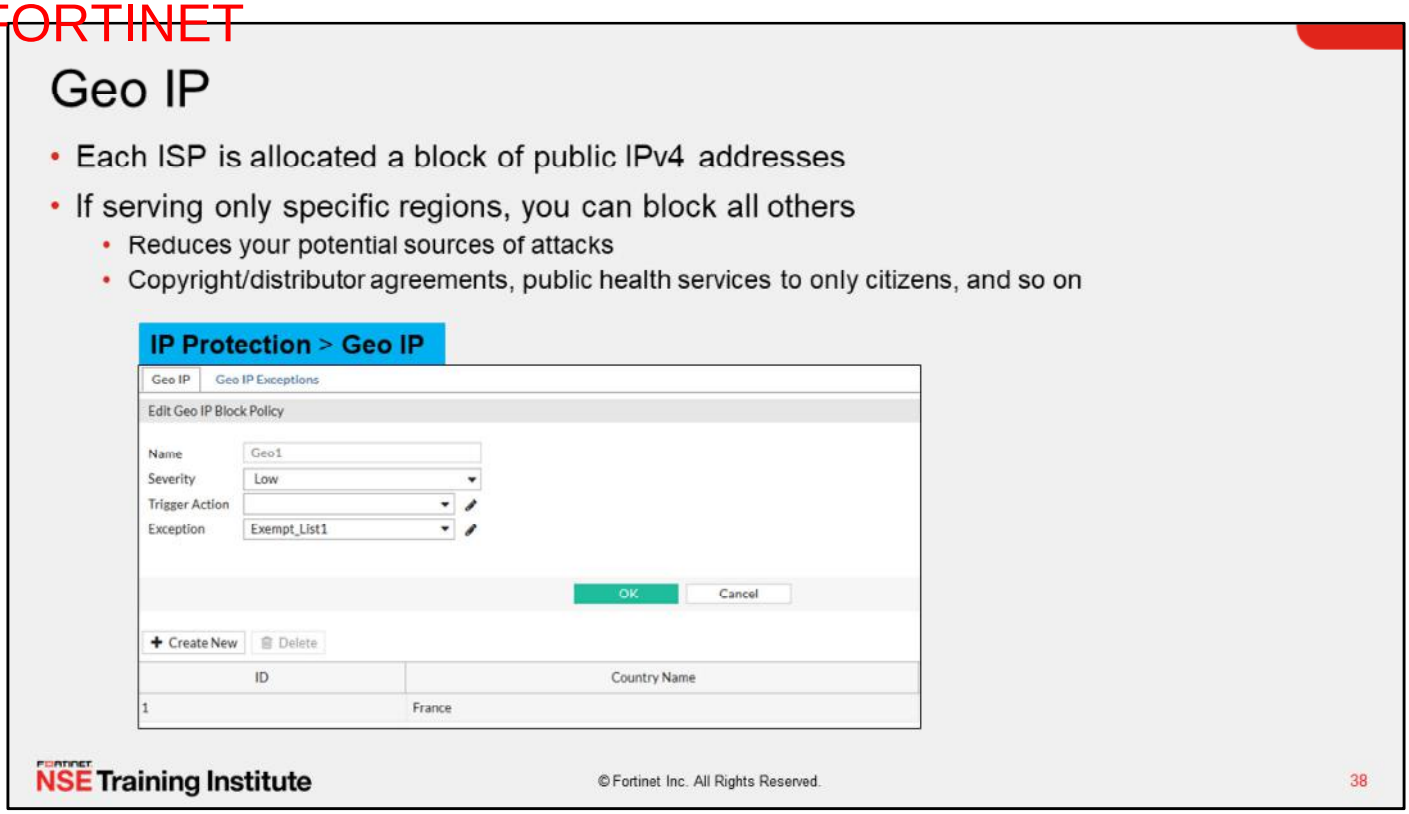
In addition to the FortiGuard IP Reputation lists, you can create you own lists of Trusted and Blocked IP addresses.

Unlisted IP addresses are in a grey zone: they are neither allowed nor denied by this feature. Instead, they are subject to all the other scans that you have configured.

By default, if the IP address of a request is neither in the Block IP nor Trust IP list, FortiWeb sends the request to other scans to determine whether it is allowed to access your web servers. However, you can define the Allow Only IP addresses so that such requests can be screened against the Allow Only IP addresses before they are passed to other scans.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



It is often impractical to manually maintain source IP addresses in blocklists if you have a publicly available site on the internet. So which other FortiWeb features automatically restrict client IP addresses?

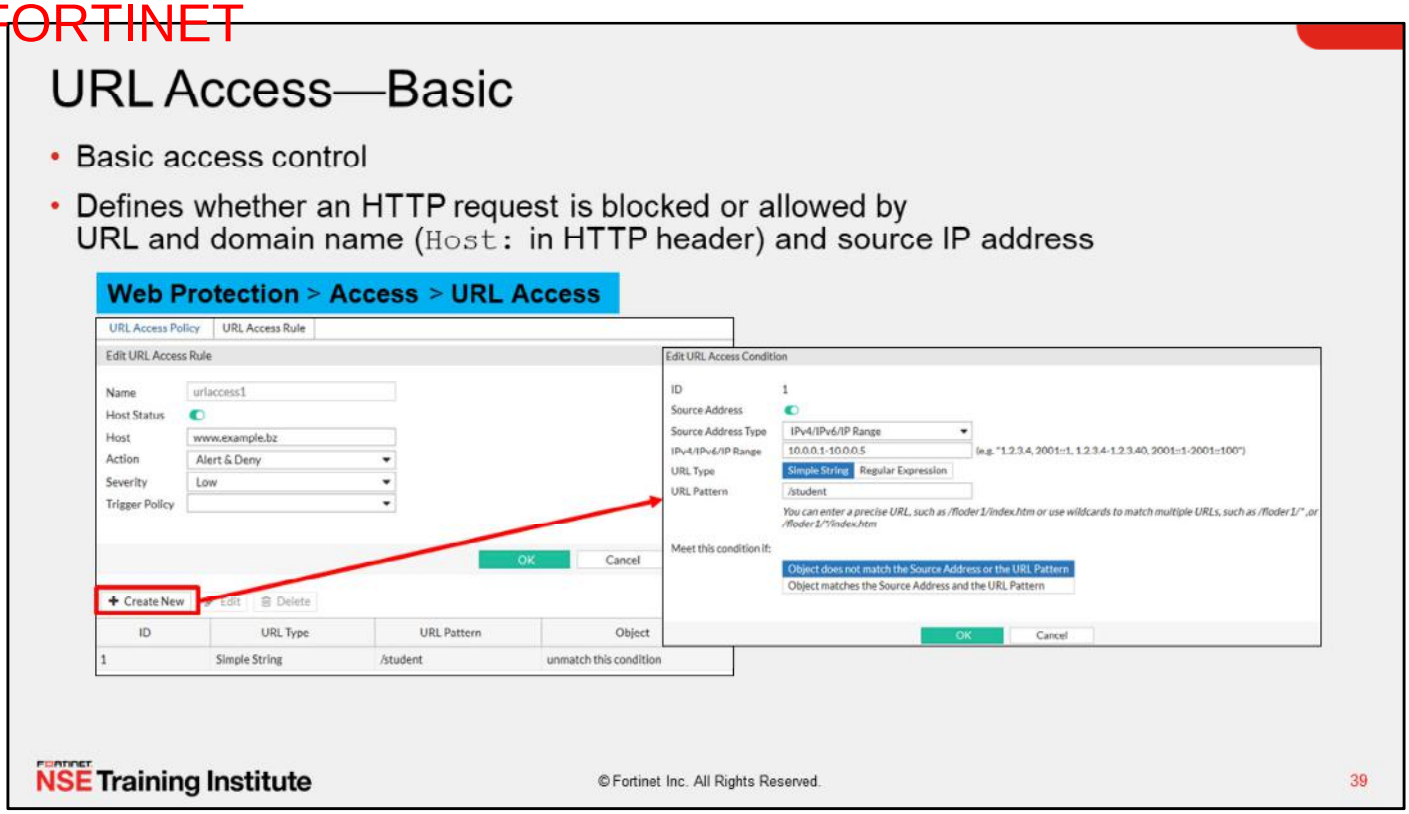
A much more powerful way of blocking IP addresses is the Geo IP feature. With it, you can blocklist IP addresses in all regions that shouldn't be accessing your website. For example, if you sell e-books with a copyright agreement that allows publishing only in France, you can ignore traffic from everywhere else.

The FortiGuard IP Reputation service can help you to effortlessly deny access to IP addresses of unknown reputation due to anonymous proxies, and to block the IP addresses of known botnets and hackers.

If you need to exempt some client public IP addresses to always be allowed, configure Geo IP reputation exemptions first.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

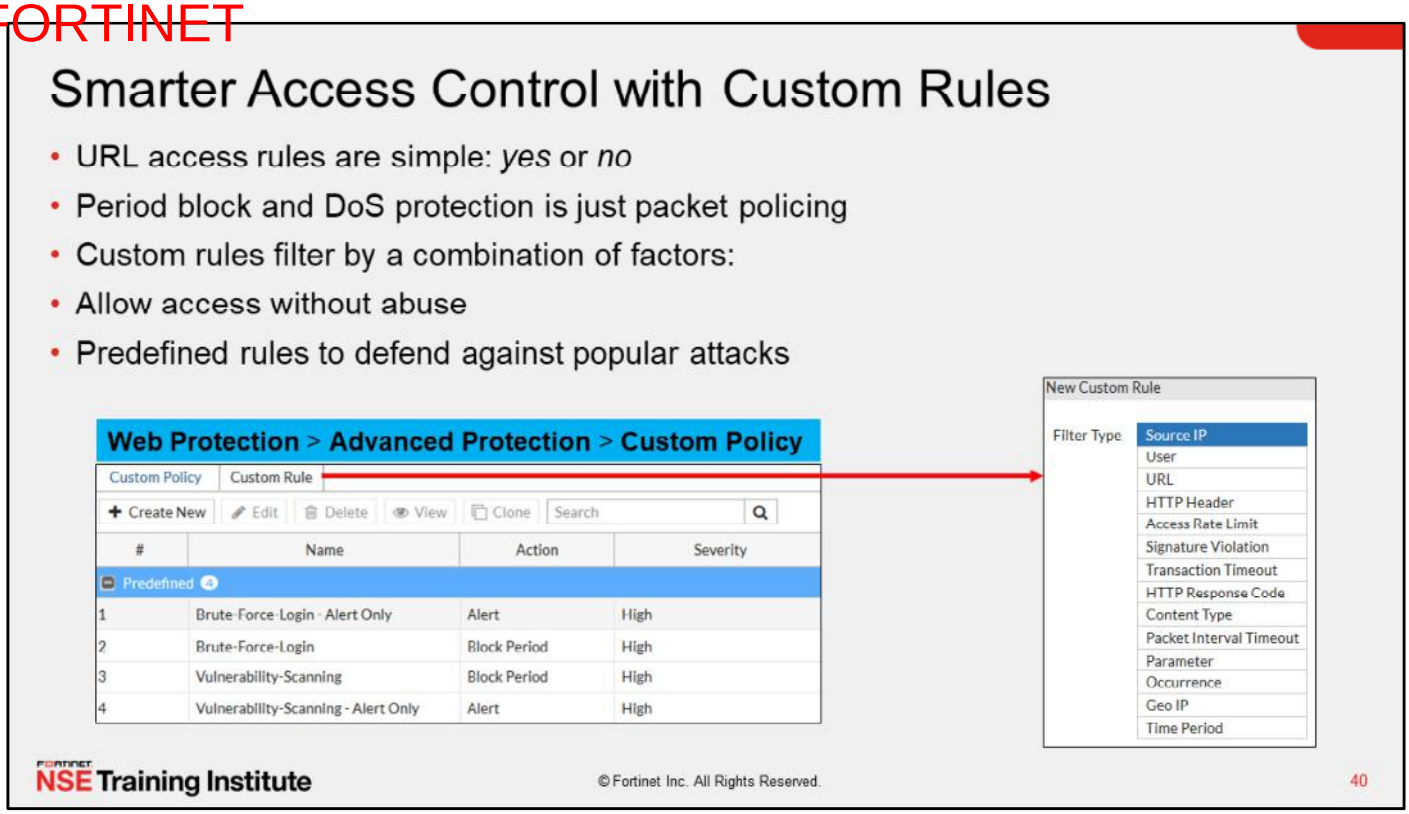


FortiWeb can control access based on the request at the HTTP layer like URL and host. In earlier FortiWeb versions, URL access rules could match only the domain name and URL, but now FortiWeb can also match by the client's source IP address.

For example, you might want to restrict your phpMyAdmin management GUI to only website administrators on the private network. To do this, create a URL access rule that blocks access to all phpMyAdmin URLs, unless they are accessed from a management subnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb also supports a sophisticated HTTP-layer control of URL access rules using **Custom Access Rules**. These rules have extensive additional HTTP-layer criteria that you can use to create fine-grained access control.

FortiWeb includes predefined rules that defend against some popular attacks. You cannot edit these predefined rules, but you can view their settings or create duplicates of them that you can edit by cloning the rule and modifying for your needs.

The filters apply to request traffic only, with the following exceptions:

- **HTTP Response Code** and **Content Type** also apply to responses.
- **Signature Violation** applies to either requests or responses, depending on which signatures you enable.
- **Occurrence** applies to either requests or responses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

URL Access—Advanced

Web Protection > Advanced Protection > Custom Policy > Custom Rule

Custom Policy | Custom Rule

Edit Custom Rule

Name: customrule1
Action: Alert
Block Period: 600 Seconds (1 - 3600)
Severity: Medium
Trigger Policy:
Bot Confirmation:

OK | Cancel

+ Add Filter | Edit | Delete

ID	Filter Type	Value
1	URL	^/admin
2	Source IP	172.16.2.10
3	HTTP Header	User-Agent
4	Access Rate Limit	2

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

On this slide, you can see a rule that restricts URL access to one source IP address and checks the rate limit and self-reported `User-Agent:` string. This rule allows access by only that specific client software.

Bot Confirmation is used to confirm if the client is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check whether it is a bot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which features provide a form of automatic blocklisting IP addresses?
   - ✓ A. Geo IP and FortiGuard
   - B. Private IP addresses
   - C. IP Block list

2. Which IP address type does FortiWeb automatically scan?
   - ✓ A. Unlisted IP addresses
   - B. Blocklisted IP addresses
   - C. Class D IP addresses

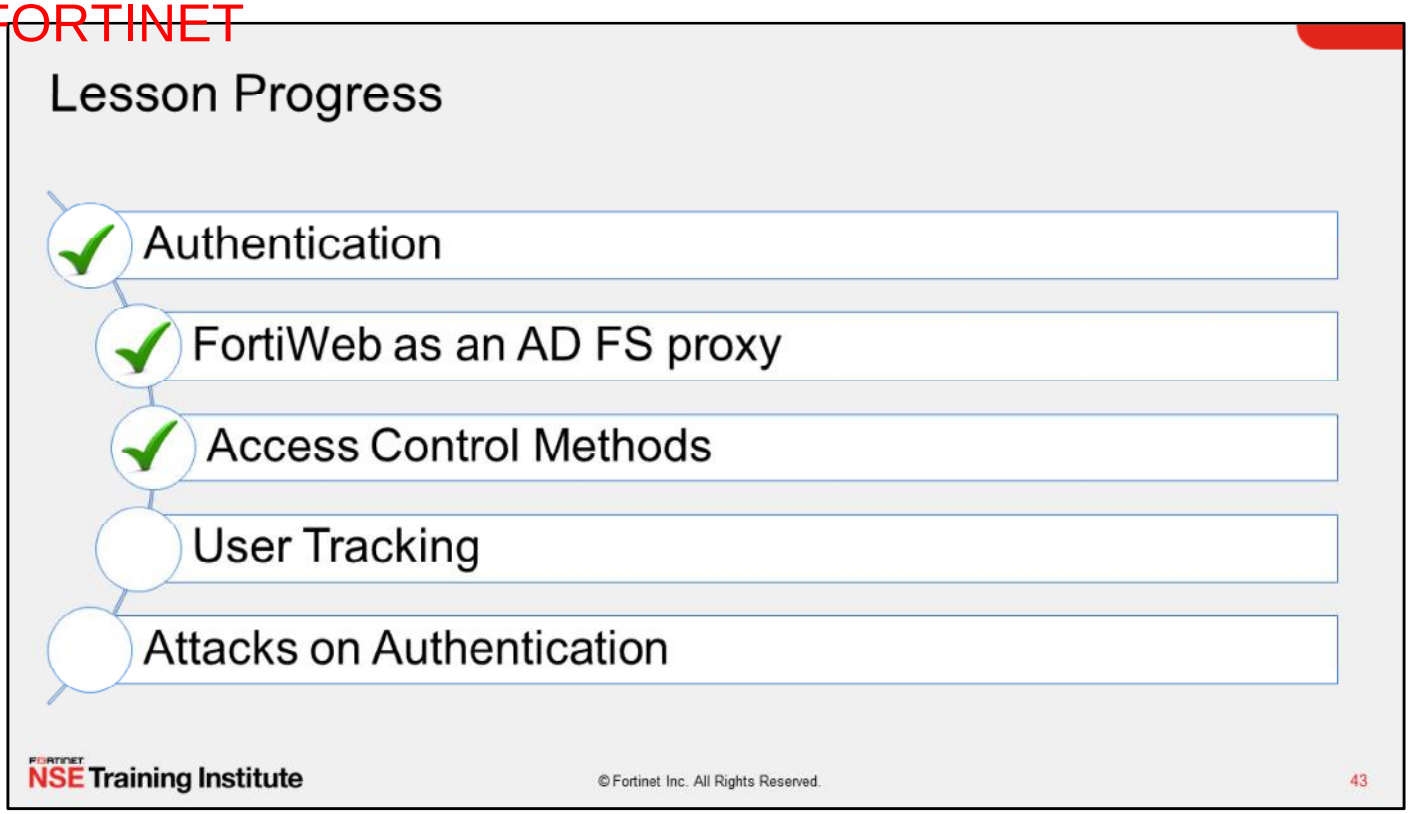
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

42

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now know how to use different access control methods.

Now you will learn about user tracking.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using the user session tracking and username capture features, you will be able to prevent session fixation attacks and instruct FortiWeb to block requests from timed out session IDs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Determining Which Users to Track

- Tracked users are identified in both the attack logs and in the traffic logs
- FortiWeb only tracks users who have logged in successfully. It uses one of the following methods to determine whether a log in is successful:
  - The response matches a condition you specify in the user tracking rule, such as a return code or a string in the response body. These conditions are created in the rule's Authentication Result Condition Table
  - If the response does not match a condition in the table, FortiWeb uses the default result selected for the rule
- When either of the following two events occurs, FortiWeb stops user tracking:
  - The client request contains the log off URL that you specify in the user tracking rule (The log off URL setting is optional)
  - The session is idle for longer than the session timeout value you specify in the rule

NSE Training Institute © Fortinet Inc. All Rights Reserved. 45

FortiWeb tracks only users that have logged in to a resource successfully. It stops tracking the user either when the user logs off normally, or when the user's session times out due to inactivity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Creating a User Tracking Policy

Tracking > User Tracking > User Tracking Rule

User Tracking Policy | User Tracking Rule

Edit User Tracking Rule

Name	usertracknule1
Host Status	
Host	www.example.com
Authentication URL	/login
Username Field	user
Password Field	pass
Session ID Name	JSESSIONID (e.g. "sid", "PHPSESSID", "JSESSIONID")
Default Authentication Result	Failed
Logoff Path	/logout
Session Fixation Protection	
Limit Concurrent Users Per Account	
Session Timeout	
Timeout	10 Minutes(1 - 60)
Session Timeout Enforcement	
Session Freeze Time	30 Minutes(1 - 3600)
Credential Stuffing Defense	
Action	Alert
Block Period	600 Seconds (1 - 3600)
Severity	Low
Trigger Policy	

OK | Cancel

Authentication Result Condition Table

+ Create New | Edit | Delete

ID	Authentication Result Type	HTTP Match Target	Value Type	Value
1	Successful	Return Code	Simple String	200
2	Failed	Response Body	Regular Expression	deny

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

The **User Tracking Rule** tab is shown on this slide.

When you create a user tracking policy, you need to define an **Authentication URL**, a **Logoff Path**, and a **Default Authentication Result**.

When you enable **Session Timeout Enforcement** in a user tracking rule, you can also configure a **Session Freeze Time**. After a session has been idle for longer than the timeout value, if a request has the session ID of the timed-out session, FortiWeb takes the action you specify in the rule. FortiWeb continues to take this action against requests with the session ID for the length of time specified by **Session Freeze Time**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What benefit does user tracking provide?
   A. Provides user GPS location
   ✓ B. Creates log entries with the associated username
   C. Blocks all traffic associated with a username

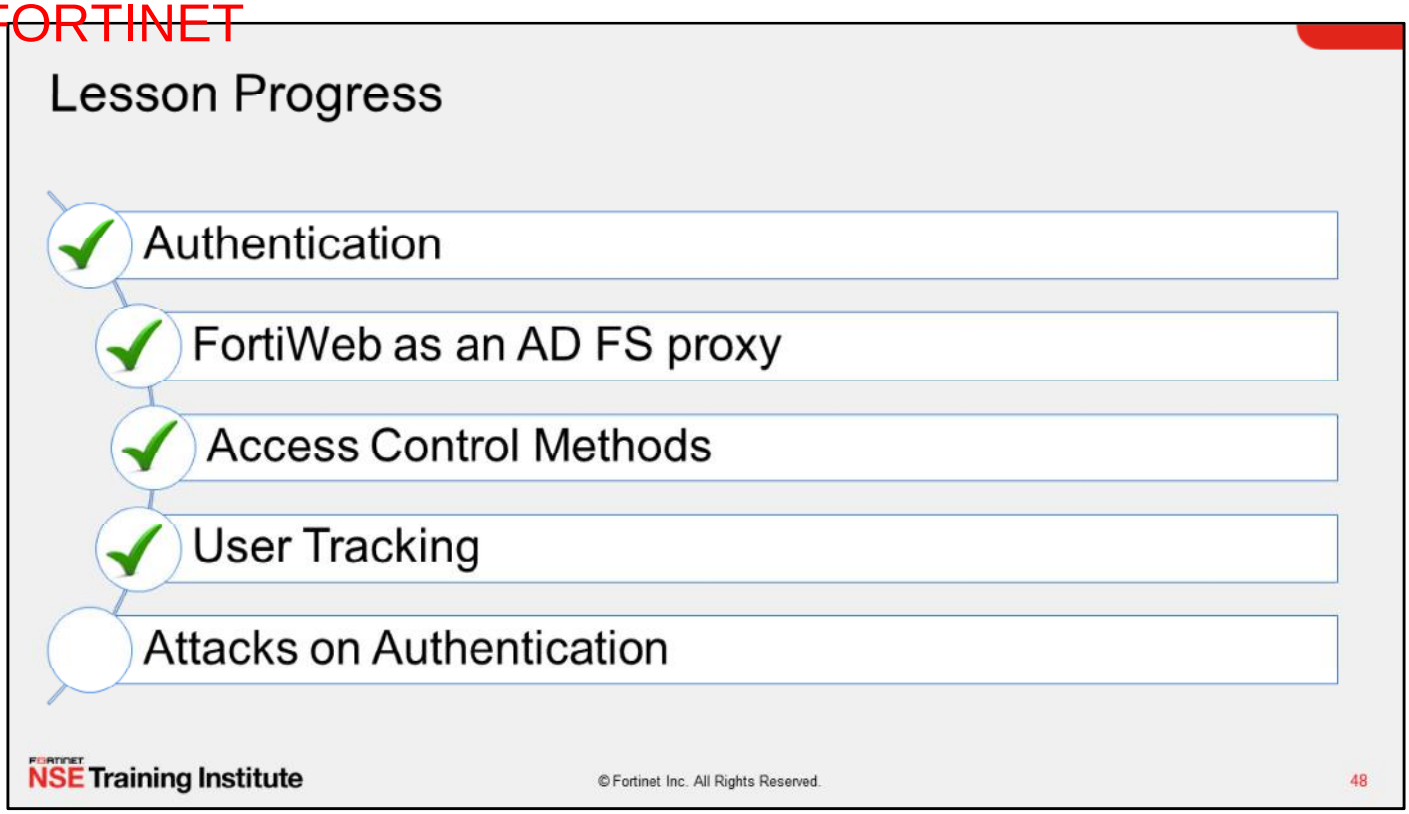
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

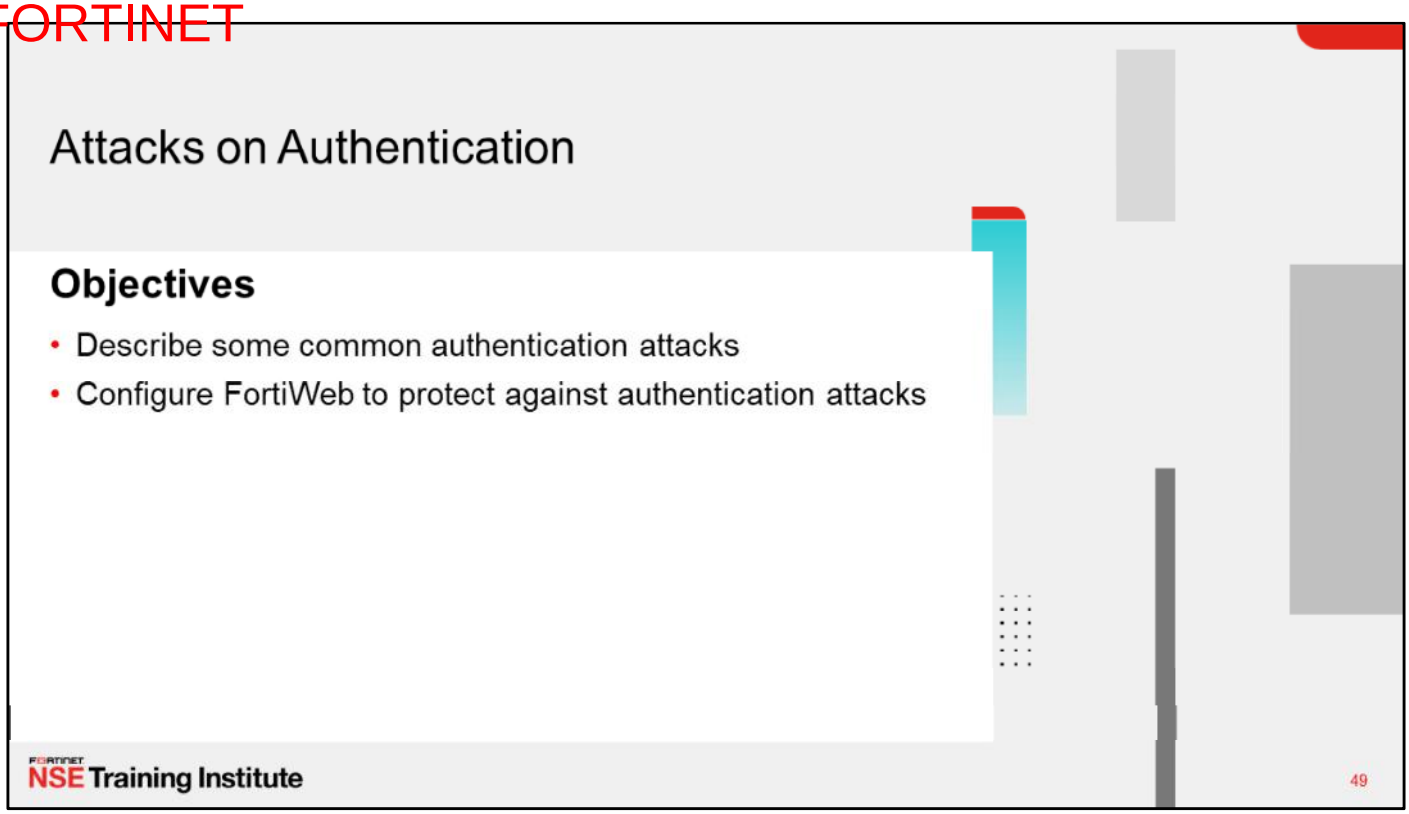


Good job! You now know how to use the user tracking feature on FortiWeb.

Now, you will learn about attacks on authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding how authentication attacks occur, you will be able to take measures to protect your network from attacks that are specific to authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Brute Force Logins

- Tries to guess combinations of usernames and passwords
- Looks for:
  - Names
  - Dates
  - Dictionary words
    - Example: In English, *z* is never followed by *f*, so it can skip that guess to speed up the brute force
  - Simple substitutions of letters with numbers
- Brute force login sensors track rate of each source IP address's requests for login URLs
- If rate exceeds threshold, subsequent requests are blocked for a configurable period

NSE Training Institute © Fortinet Inc. All Rights Reserved. 50

The most obvious protection may be brute force protection. When a client's smart phone, tablet, or laptop becomes infected and subsequently becomes part of a botnet, web applications may receive many requests from what appear to be legitimate sources. However, your attack logs may be full of log messages about authentication failures. This is because the malware (or, in the case of attackers that aren't cautious, a script on their own computer) is trying to guess passwords.

After the attacker successfully guesses a password, they can log in as that user. If the user associated with the guessed password has administrator privileges on your network, this can be a serious security breach for more than just the compromised account.

Brute force detection monitors login URLs for suspicious request rates from each client IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Your Weakest Link

Top Worst Passwords (2020)

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

https://nordpass.com/most-common-passwords-list/

Test your password strength before attackers do!

Popular tools:

- THC Hydra
- L0phtCrack
- John the Ripper

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

51

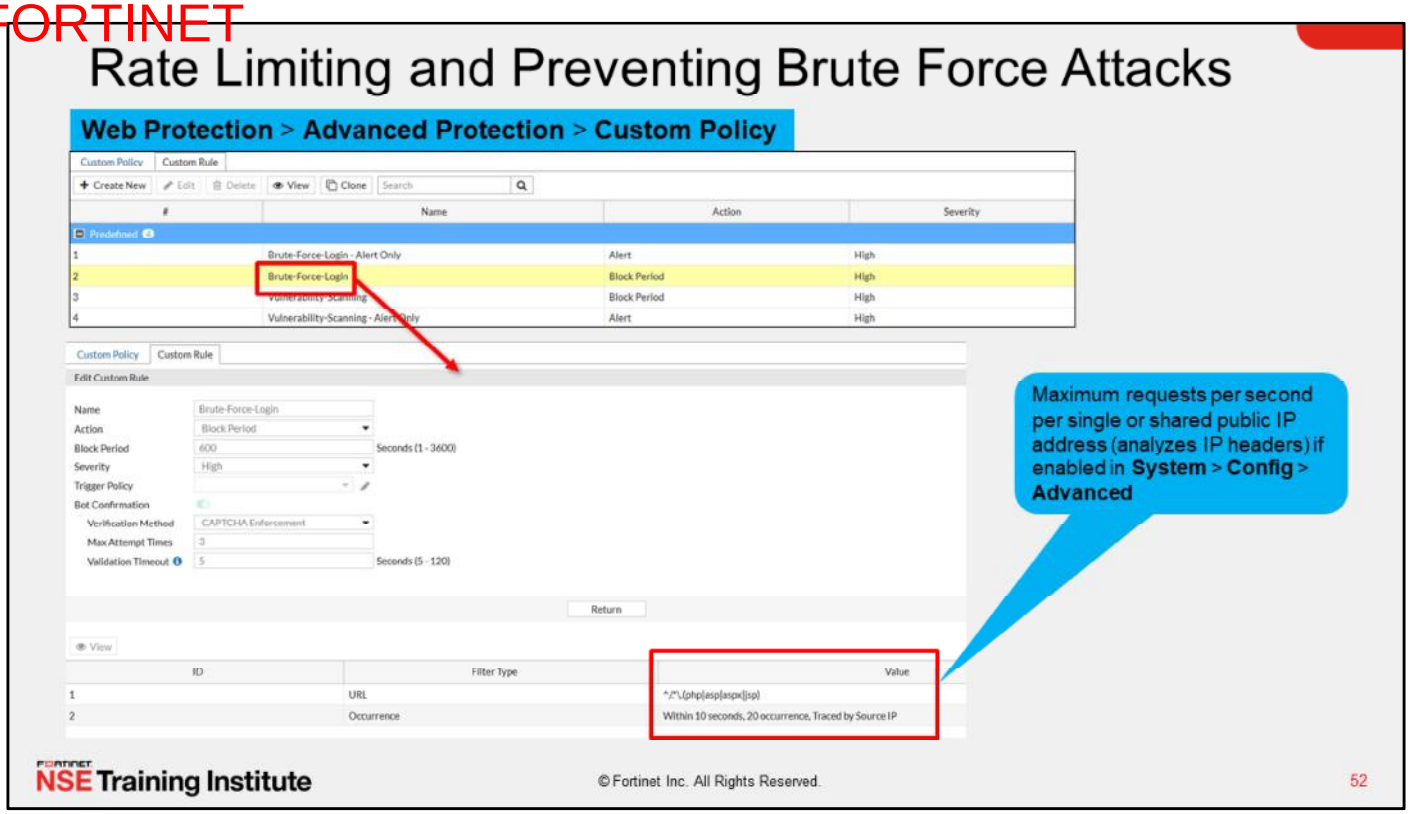
Hands up! How many of you admit to using these passwords?

The widespread use of weak passwords is one of many reasons why using PKI and two-factor authentication is important: They provide stronger authentication.

The use of weak passwords is also a good reason to limit each account to the minimum required permissions for that person's job, and why you should enable brute force protection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The brute force login rule tracks the rate at which each source IP address makes requests for specific URLs during a specific time period. If the source IP address exceeds the threshold, FortiWeb blocks requests from the source IP address for the time period that you specify in the profile.

You can use the predefined **Brute-Force-Login** rule. You can customize this rule by cloning it.

Remember, if multiple clients share a single internet connection behind NAT, then you should allow multiple requests. Otherwise, for example, if 25 people begin their work day at 9 AM and try to log in at about the same time, they will all be locked out!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Padding Oracle Attacks

- When ASP .NET or another application (instead of HTTPS) individually encrypts session ID or login
  - Affected anything encrypted by ASP .NET API
- Often adds padding:
  - Length doesn't give attackers hints about password length
  - If padding is not random each time, crypto-analysis attack is possible
  - Attacker can repeatedly send same input to analyze patterns in output and reduce the number of guesses required to find the key, resulting in faster cracking
  - Reused padding results in identical hashes, predictable length
  - Compression encodes files by patterns, making crypto-analysis faster after each pattern is solved

NSE Training Institute © Fortinet Inc. All Rights Reserved. 53

Padding Oracle attacks are another attack type aimed at authentication and session IDs. In this type of attack, the attacker analyzes the padding in order to find a predictable pattern. Once they find a pattern, they use it to understand the encryption and undo it.

It's the same idea as the SSL/TLS attacks named CRIME & Lucky 13. CRIME requires only six requests to decrypt one cookie byte, due to compression. A TLS MAC calculation always includes 13 bytes of header information. The predictable length, in part, is what makes Lucky 13 attacks possible.

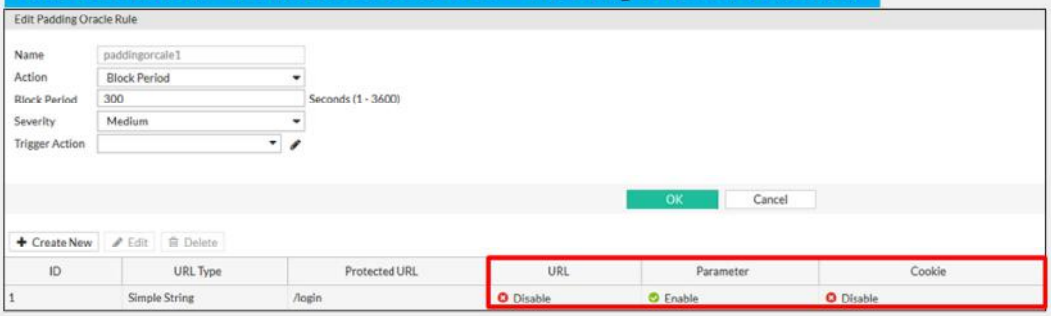
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Padding Oracle Attacks (Contd)

- Which inputs should FortiWeb observe during each session, looking for repeated padding that give crypto hints:
  - Cookie
  - URL: Parameters in the URL, such as /user/0000012FE03BC2)
  - Parameter: Parameters appended to a traditional GET URL parameter, such as /index.php?user=0000012FE03BC2 or POST body

Web Protection > Advanced Protection > Padding Oracle Protection



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

Padding can be found in any individually encrypted HTTP input: the URL line, including parameters at the end of it; a cookie header; or (in the case of POST method requests) parameters in the body.

So, when you configure FortiWeb, indicate which inputs have padding that you want to protect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is one key factor that you must consider when setting brute force rate limiting and blocking?
   - ✓ A. Multiple clients sharing a single internet connection
   - B. Multiple clients connecting to multiple resources

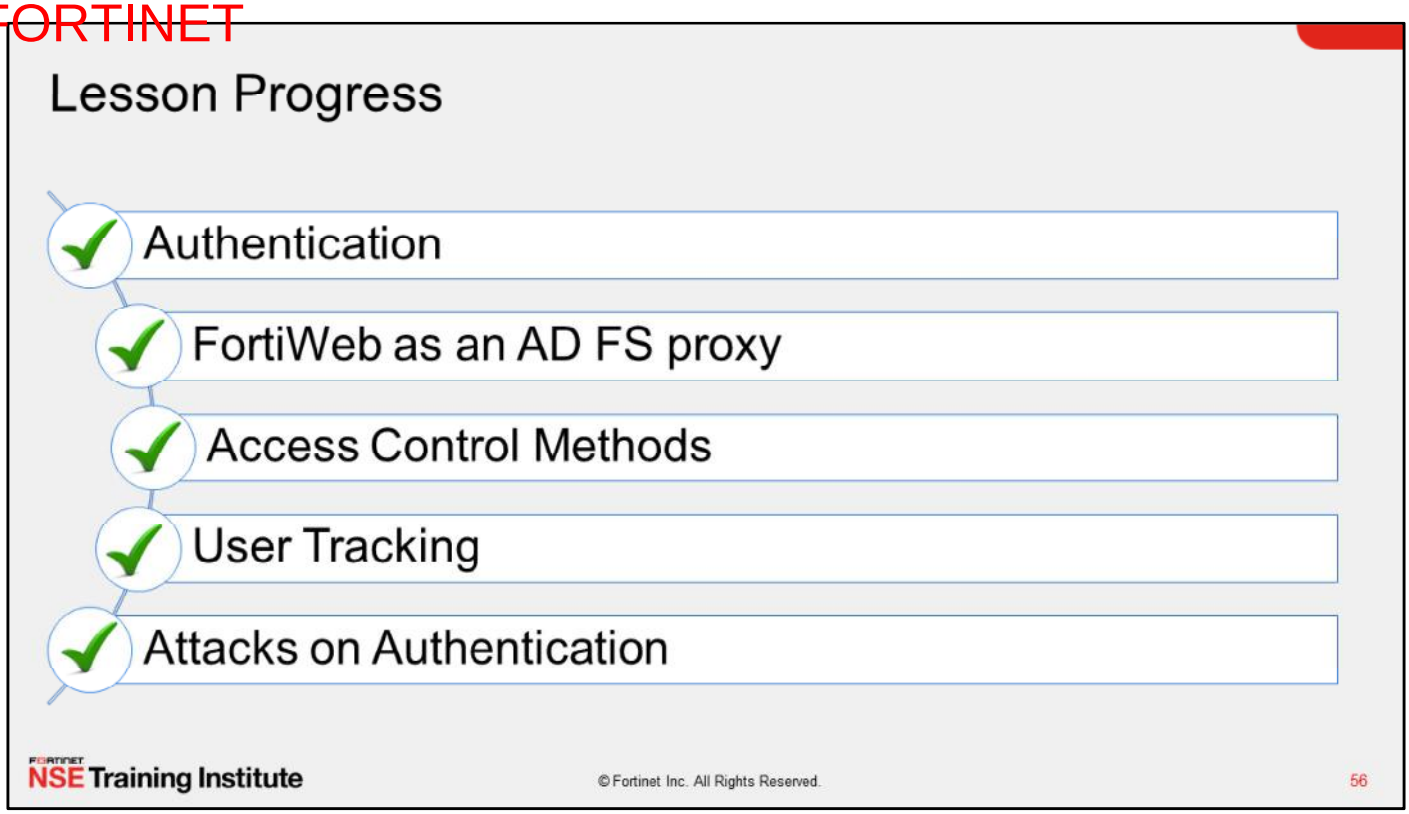
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

55

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have successfully completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe and discuss authentication options
- ✓ Configure authentication
- ✓ Describe the FortiWeb Active Directory Federation Service proxy feature
- ✓ Describe and discuss access control methods
- ✓ Track sessions by user
- ✓ Capture username in traffic and attack logs
- ✓ Store session ID and username when users match specified criteria
- ✓ Describe some common authentication attacks
- ✓ Configure FortiWeb to protect against authentication attacks

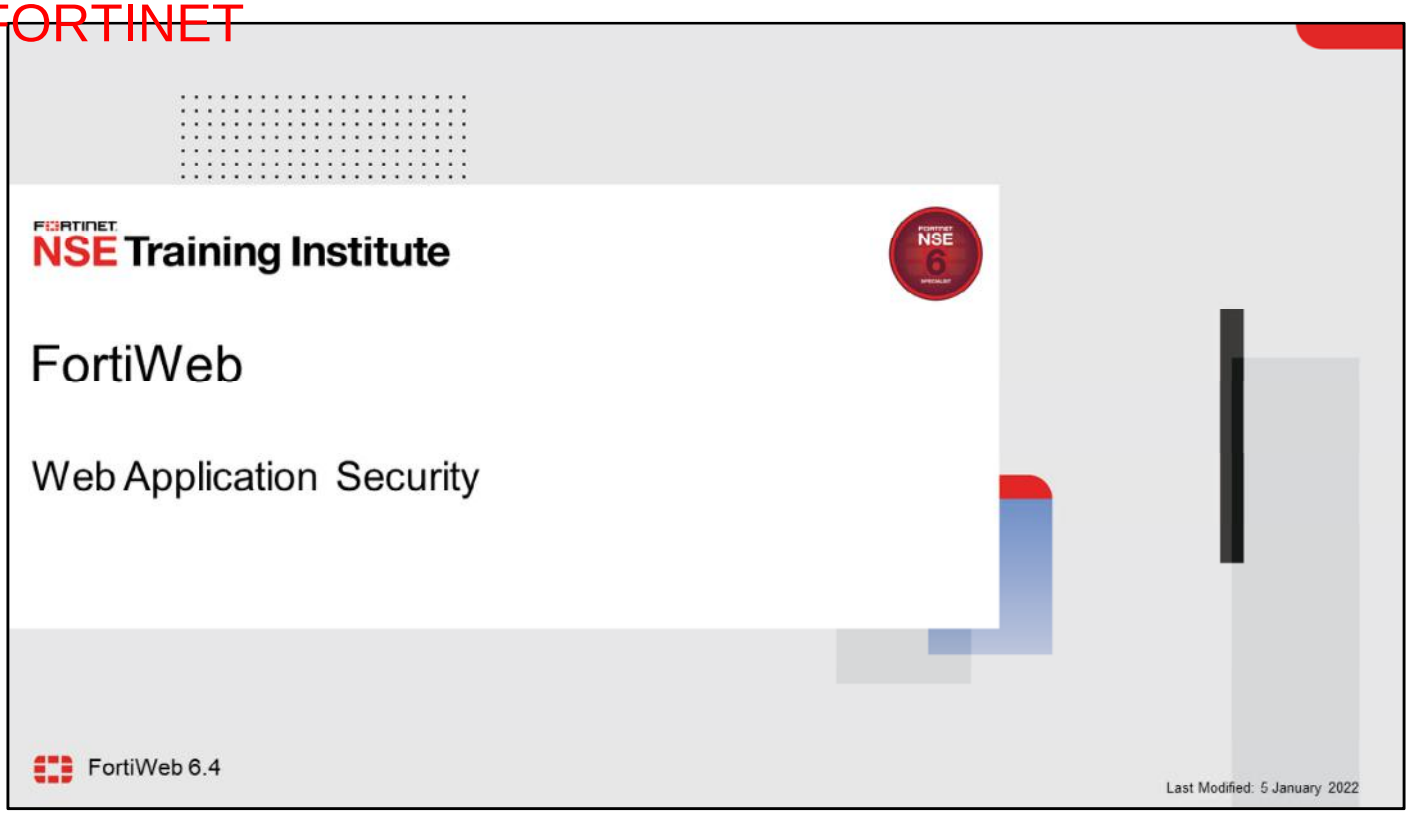
NSE Training Institute © Fortinet Inc. All Rights Reserved. 57

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiWeb to control access at the IP and HTTP layer authentication, credential and SSO capabilities to protect web applications, and defeat some specific authentication attacks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to use signatures from FortiGuard subscription services, and how to create your own custom signatures to address the security needs of your web applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Web Application Security Quick Start
- Generating Signatures and Rules
- Blocking Known Attacks and Data Leaks
- Zero-Day Attacks and Input Validation

NSE Training Institute

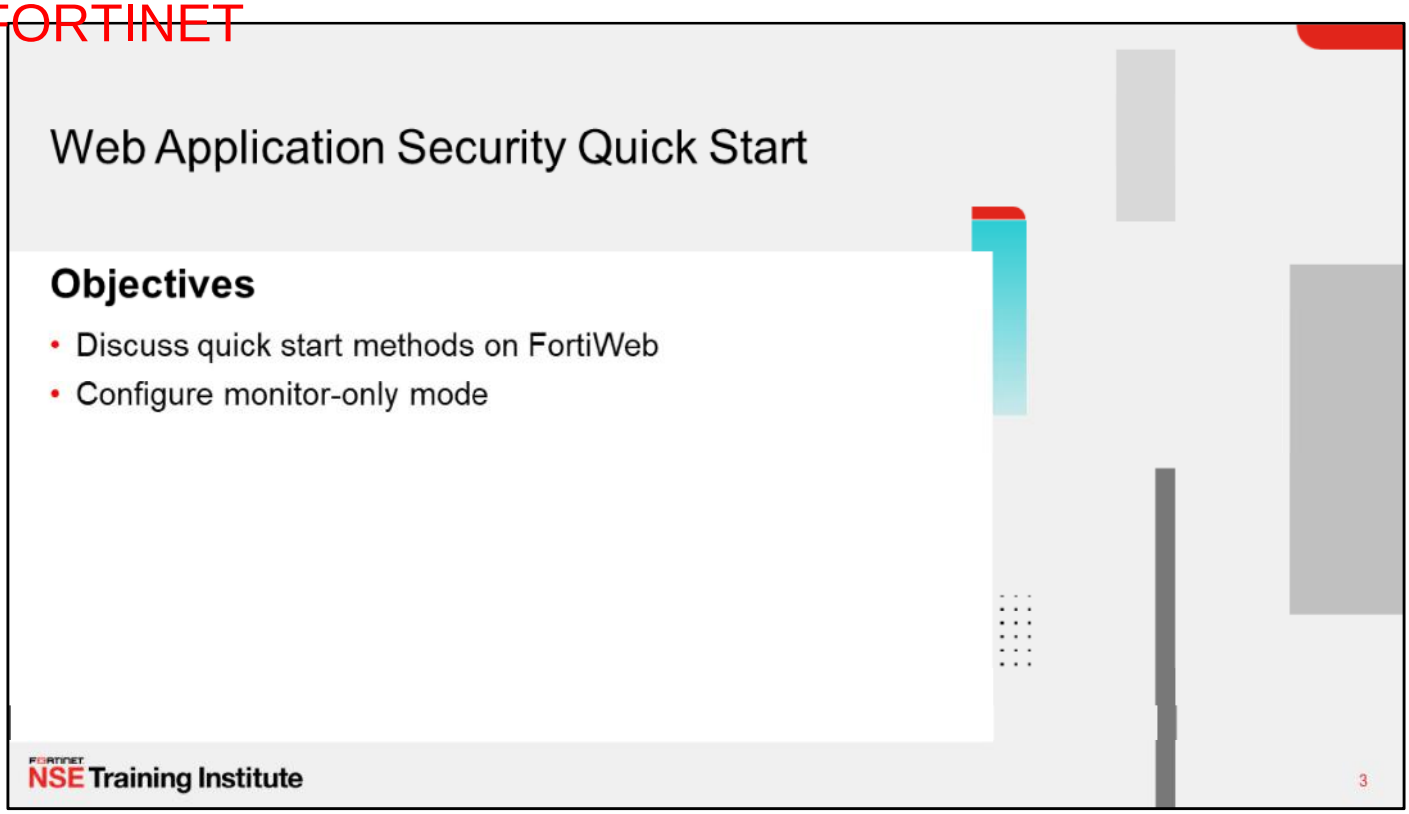
© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in knowing and using quick start methods, you will be able to quickly configure FortiWeb and get it set up in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Attack Protection Methods

- Signatures
- Anomaly analysis
- IP reputation
- Access control
- Rate limits
- Authentication
- Page order and other stateful app analyses
- Input sanitization
- Anti-defacement

Many strategies. Some need configuration. How do you begin protecting apps quickly?

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

When an attack is detected, FortiWeb can send TCP reset signals and depending on the violation and your FortiWeb's operation mode, may also be able to send HTTP return codes and error pages.

What methods does FortiWeb use to determine whether a client's request is an attack?

FortiWeb uses many strategies to detect attacks. In many cases you can use the default FortiWeb settings and adjust as necessary. However, if an administrator updates a web server or web application, you may need to update the FortiWeb settings as well.

How can you configure FortiWeb quickly?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Quick Start Methods

- Start with default settings or predefined profiles
- Gradually enable and start using policies in monitor-only mode
- Take a phased-in approach to using each signature. Possible options to a phased-in approach include:
  - Start using custom signatures individually, one week per application, and monitor results and impact
  - If possible, attach to SPAN or mirror port, and start in offline mode. After verification period, create an inline protection profile and continue in reverse proxy mode.
    - No latency added in offline mode
- Don't enable everything at once!
  - False positives possible
  - Troubleshooting is more difficult
  - Some signatures or settings are not appropriate for all apps
  - Some regular expressions are computationally intensive
  - Some features require more RAM

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

This slide shows an overview of methods that you can use to configure FortiWeb quickly. Now you will take a look at each of them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Start With Defaults

- Find a default profile that is closest to your needs
- Copy and modify as needed
- This method is faster than configuring from scratch

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

Default settings and predefined settings are the easiest to use. If they do not quite fit the situation, you can clone them and adjust them to fit the needs of many different security profiles.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Monitor Mode

- Overrides all profile actions
  - Won't block any traffic
  - Alert (log) only
- Alternatively, select **Alert** in each component
- Logs reveal potential effects of the profile before applying it
- Does not affect any rewriting or redirection actions in the protection profiles, including the action to remove poisoned cookies

© Fortinet Inc. All Rights Reserved.

For a dry run to see if a feature unintentionally blocks normal traffic, you can either enable the **Monitor Mode** option for a policy-wide effect, or you can select the **Alert** action instead of the **Block** action for for a specific feature that you want to test.

If you test your FortiWeb configuration with typical traffic for one week and it doesn't generate any unintentional attack logs, it's unlikely that the feature will interfere with normal traffic, and you can enable it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which of the following methods allows you to observe the actions FortiWeb takes without impacting traffic performance?
   - ✓ A. Monitor mode
   - B. Machine learning
   - C. Reverse proxy mode
   - D. Transparent proxy mode

2. Why should you not enable every FortiWeb feature at once for maximum security?
   - A. Slows down the configuration process
   - ✓ B. Complicates troubleshooting
   - C. Each feature must be configured individually before enabling

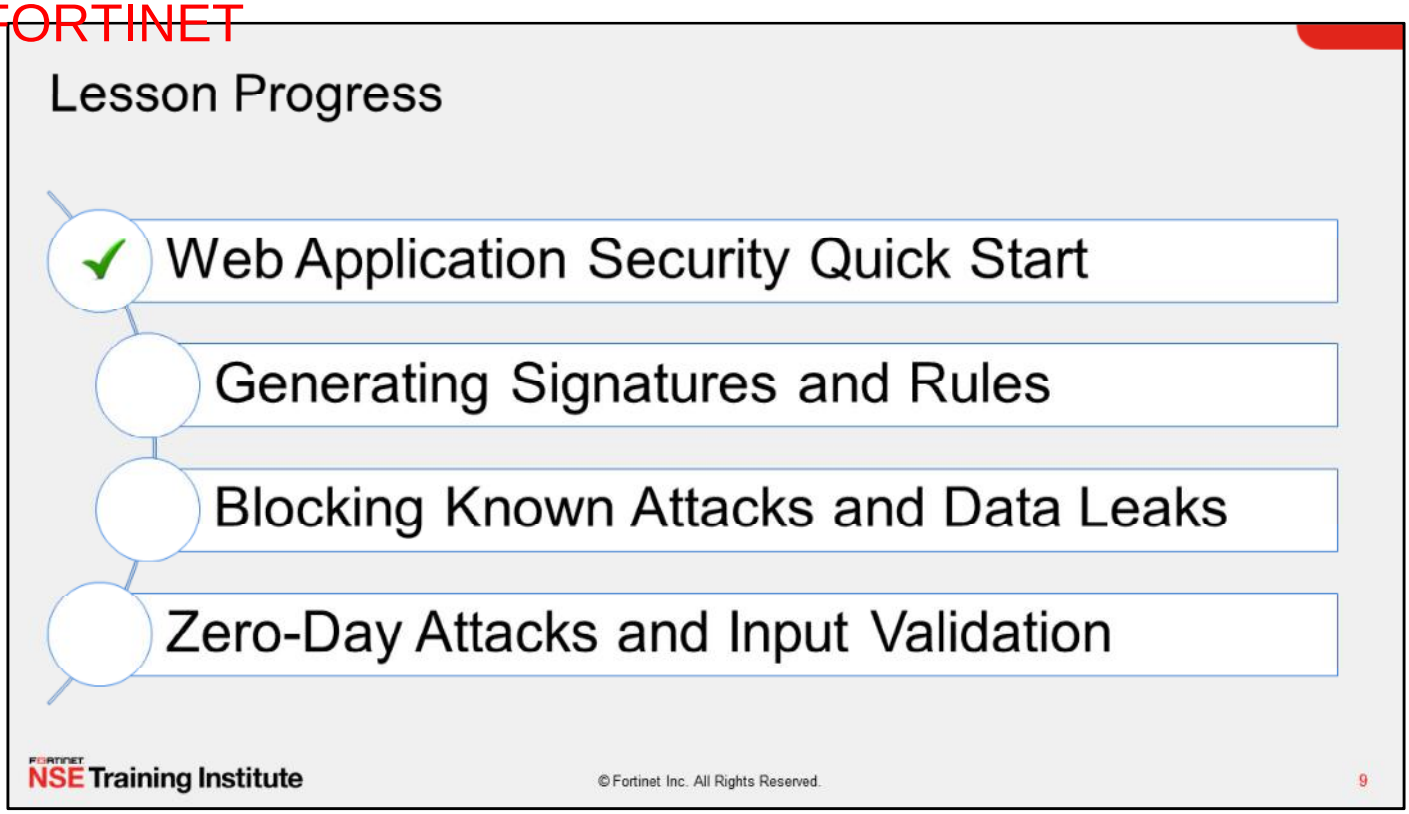
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

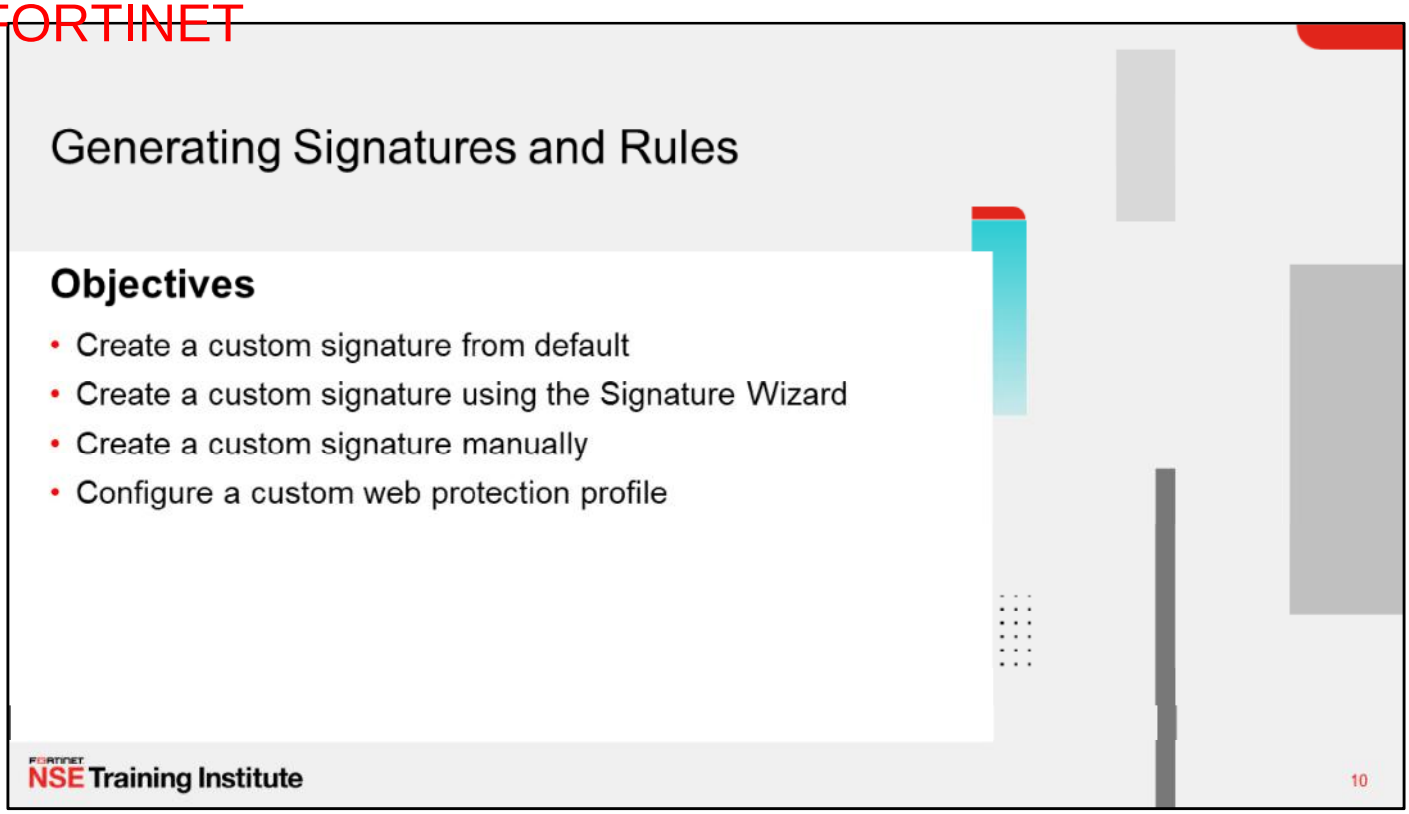


Good job! You now know how to deploy and configure FortiWeb using quick start methods.

Now, you will learn ways to fine-tune FortiWeb to your specific environment by generating signatures and rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

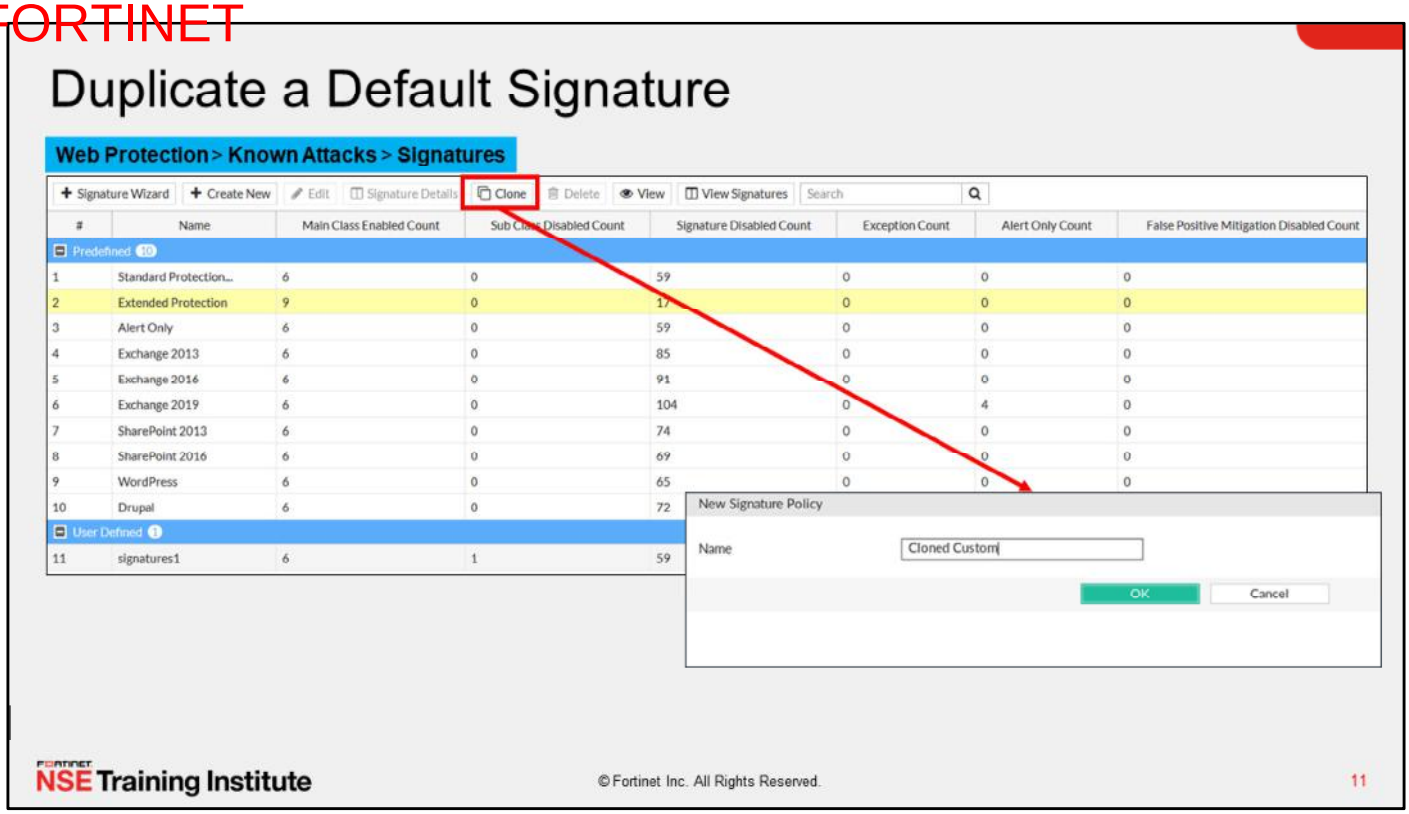


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in creating custom signatures, you will be able to create a configuration that is tailored to your web apps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The easiest way to create a custom signature for your web application is to begin with one of the default signatures that are included on FortiWeb. Review the signature details to locate the one that is the closest match to what you are trying to achieve. Clone this default signature and customize it according to your needs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Edit Cloned Signature

Web Protection > Known Attacks > Signatures

+ Signature Wizard | + Create New | Edit | Signature Details | Clone | Delete | View | View Signatures | Search

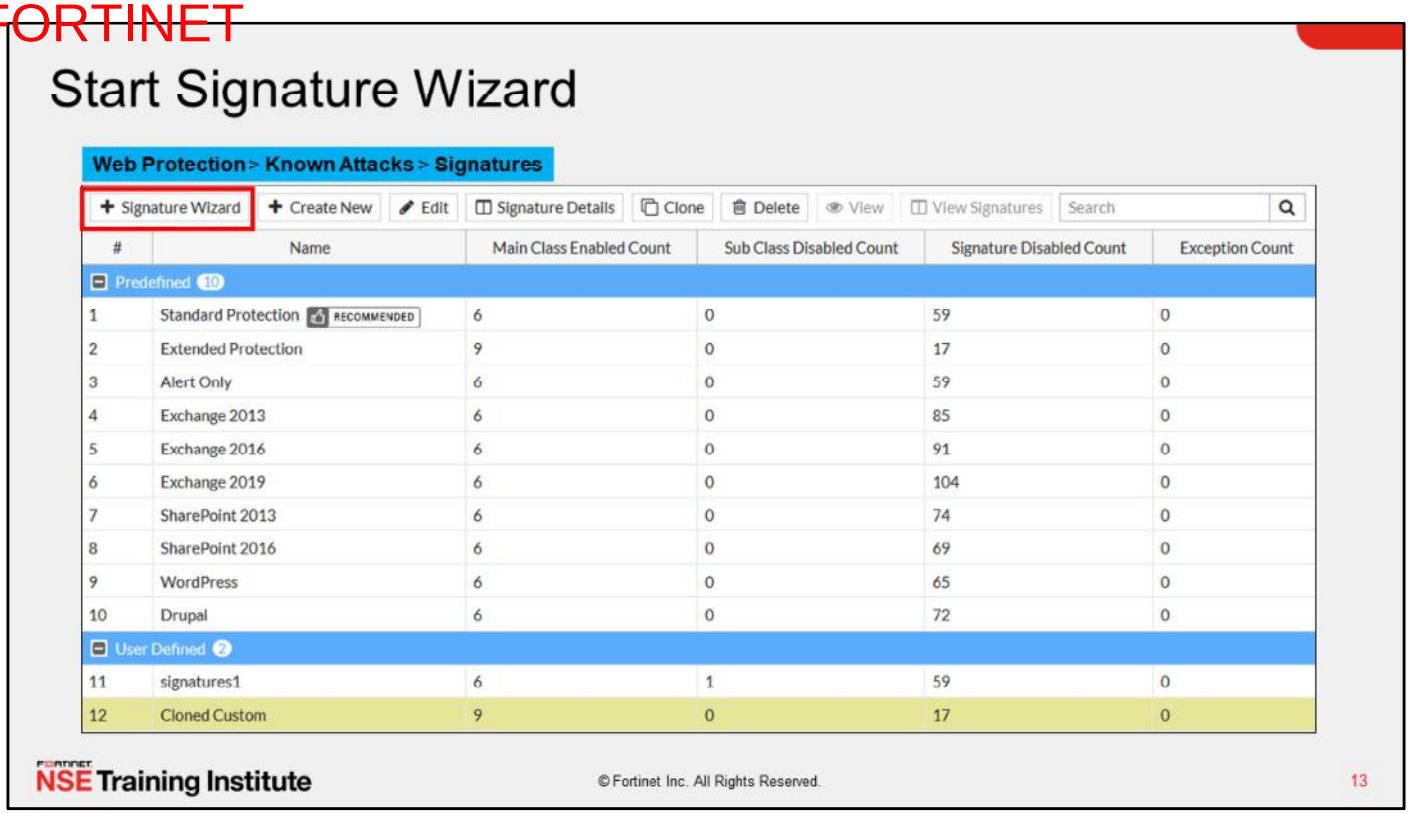
#	Name	Main Class Enabled Count	Sub Class Disabled Count	Signature Disabled Count	Exception Count
Predefined 10					
1	Standard Protection RECOMMENDED	6	0	59	0
2	Extended Protection	9	0	17	0
3	Alert Only	6	0	59	0
4	Exchange 2013	6	0	85	0
5	Exchange 2016	6	0	91	0
6	Exchange 2019	6	0	104	0
7	SharePoint 2013	6	0	74	0
8	SharePoint 2016	6	0	69	0
9	WordPress	6	0	65	0
10	Drupal	6	0	72	0
User Defined 2					
11	signatures1	6	1	59	0
12	Cloned Custom	9	0	17	0

NSE Training Institute © Fortinet Inc. All Rights Reserved. 12

Using both the **Edit** and **Edit Signatures** functions, you can make changes to achieve your web application protection goals.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



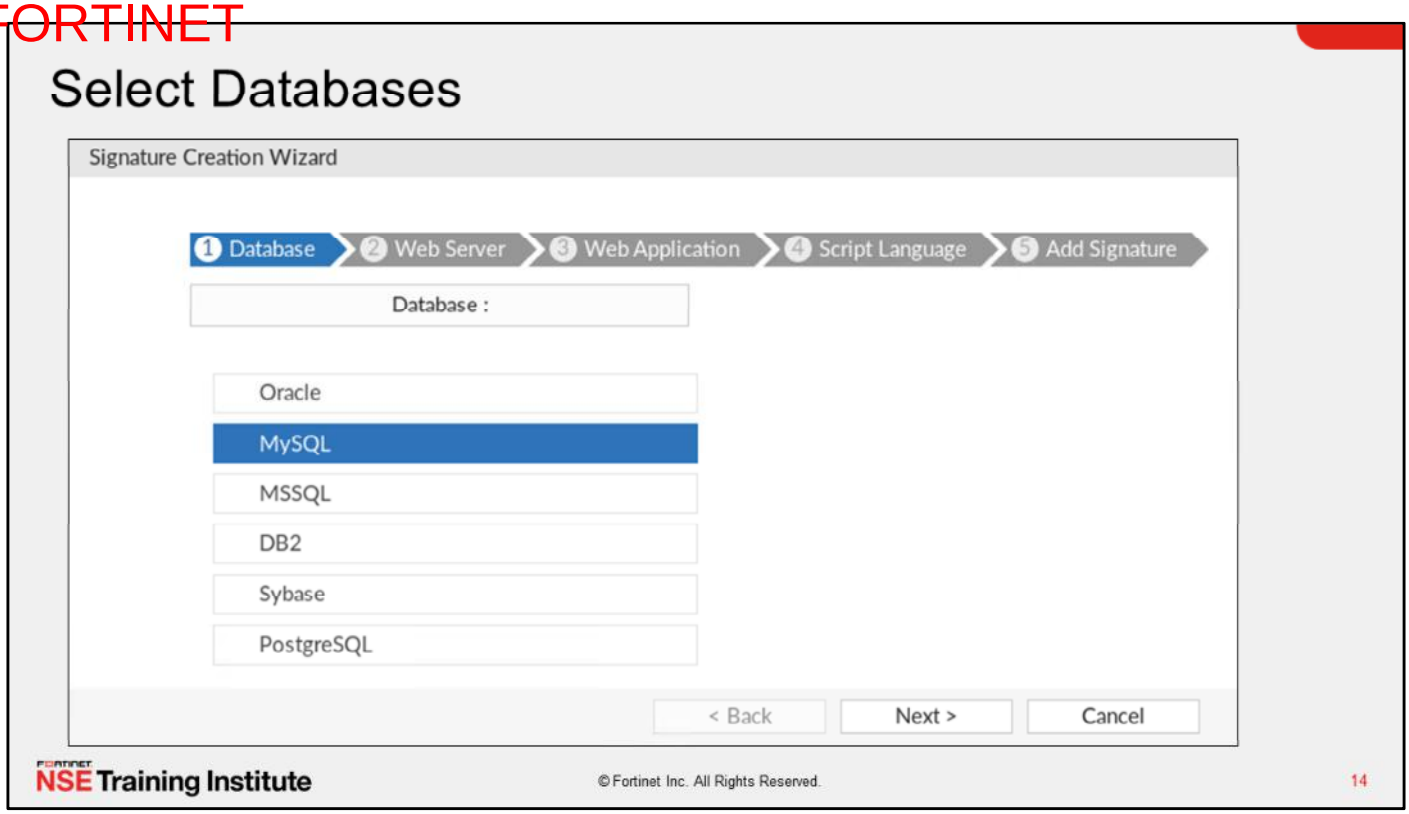
#	Name	Main Class Enabled Count	Sub Class Disabled Count	Signature Disabled Count	Exception Count
Predefined 10					
1	Standard Protection RECOMMENDED	6	0	59	0
2	Extended Protection	9	0	17	0
3	Alert Only	6	0	59	0
4	Exchange 2013	6	0	85	0
5	Exchange 2016	6	0	91	0
6	Exchange 2019	6	0	104	0
7	SharePoint 2013	6	0	74	0
8	SharePoint 2016	6	0	69	0
9	WordPress	6	0	65	0
10	Drupal	6	0	72	0
User Defined 2					
11	signatures1	6	1	59	0
12	Cloned Custom	9	0	17	0

Another option available for creating custom signatures is the **Signature Wizard**.

This wizard guides you through the steps of creating a basic custom signature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



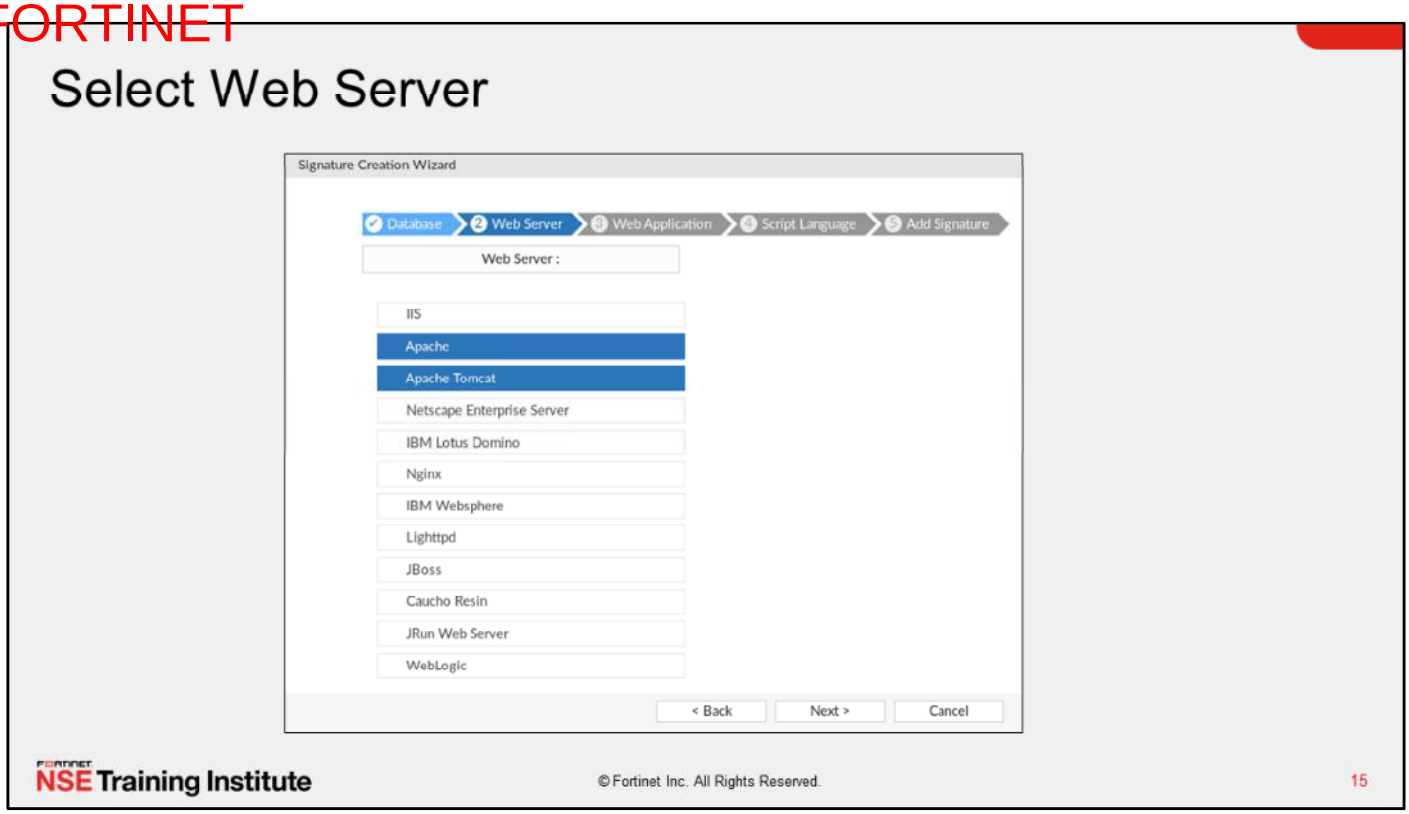
The first step in the **Signature Creation Wizard** is to identify the types of databases your web application uses. The options include:

- Oracle
- MySQL
- MSSQL
- DB2
- Sybase
- PostgreSQL

You can select multiple options if applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

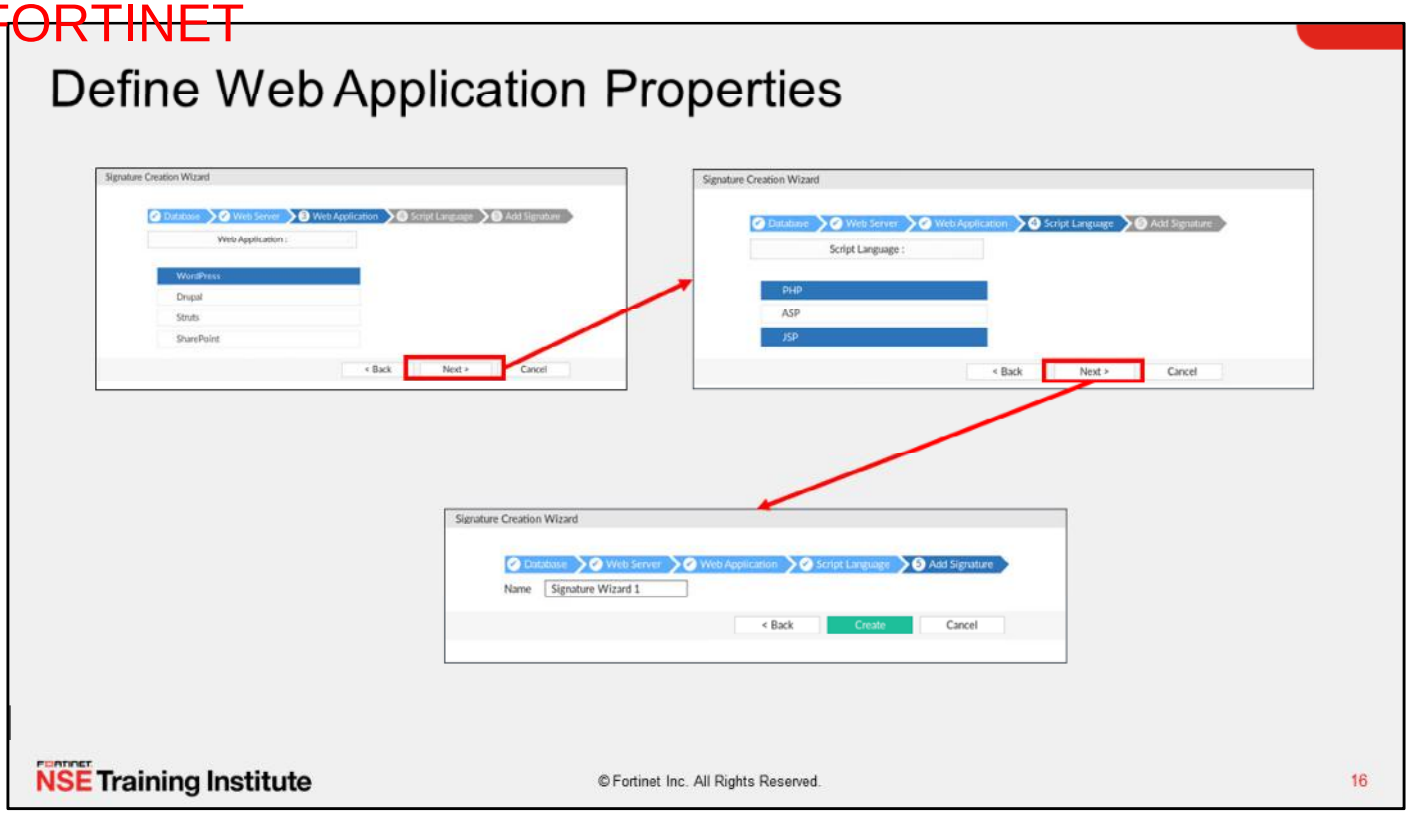


The second step in the **Signature Creation Wizard** is to identify the type of back-end web server that your web application is running on. The supported web server types are:

- IIS
- Apache
- Apache Tomcat
- Netscape Enterprise Server
- IBM Lotus Domino
- Nginx
- IBM WebSphere
- Lighthttpd
- Jboss
- Caucho Resin
- JRun Web Server
- WebLogic

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



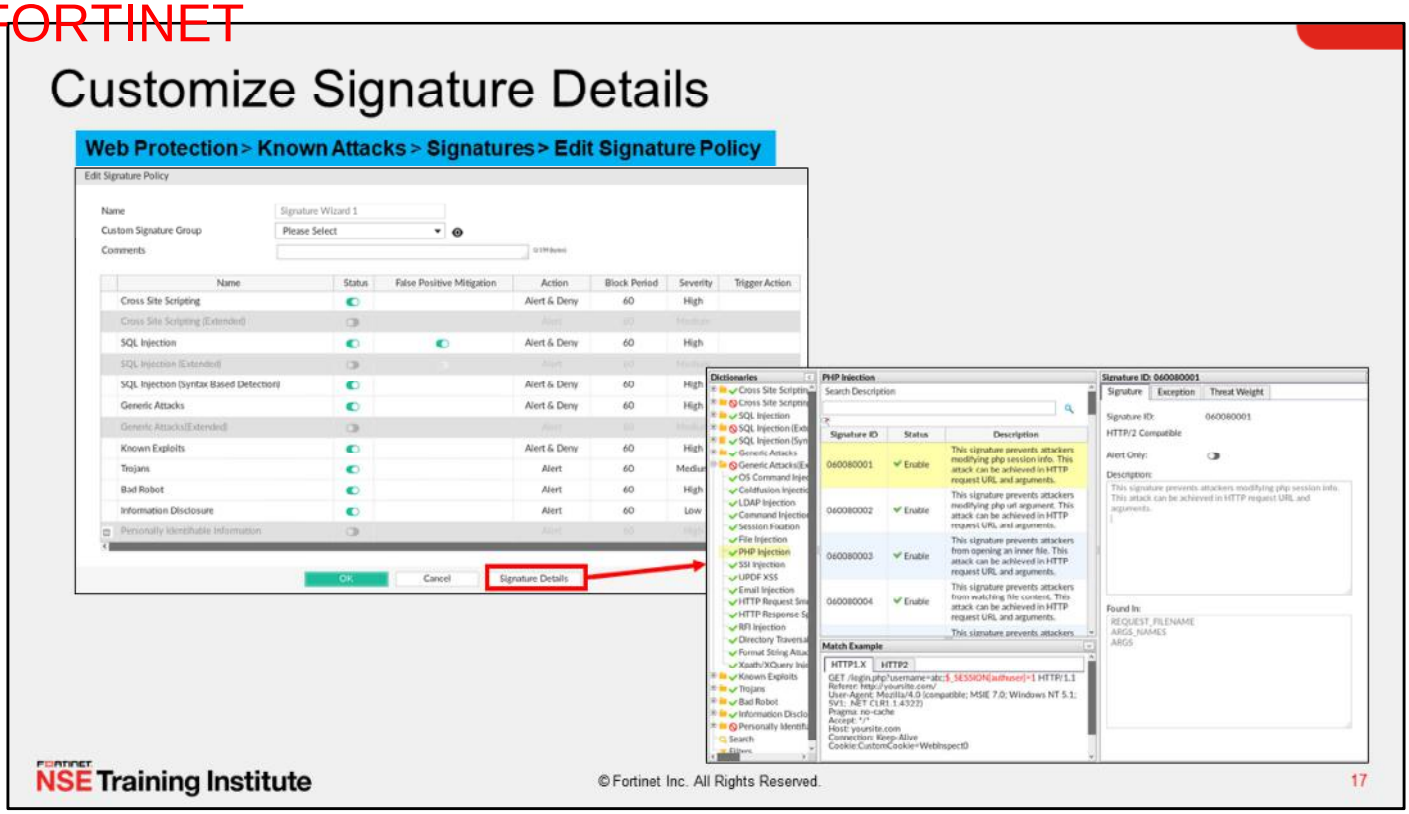
The next three steps define the properties, or characteristics of the web application. First, you define the type of web application, such as WordPress, Drupal, SharePoint, and so on.

Next, you define any script languages used by the web application, such as PHP, ASP, or JSP.

Finally, you give your signature definition a name in order to distinguish it from any other signatures you may already have, including the default ones provided by Fortinet.

Vouchers & Dumps are Available | WhatsApp +201224560923

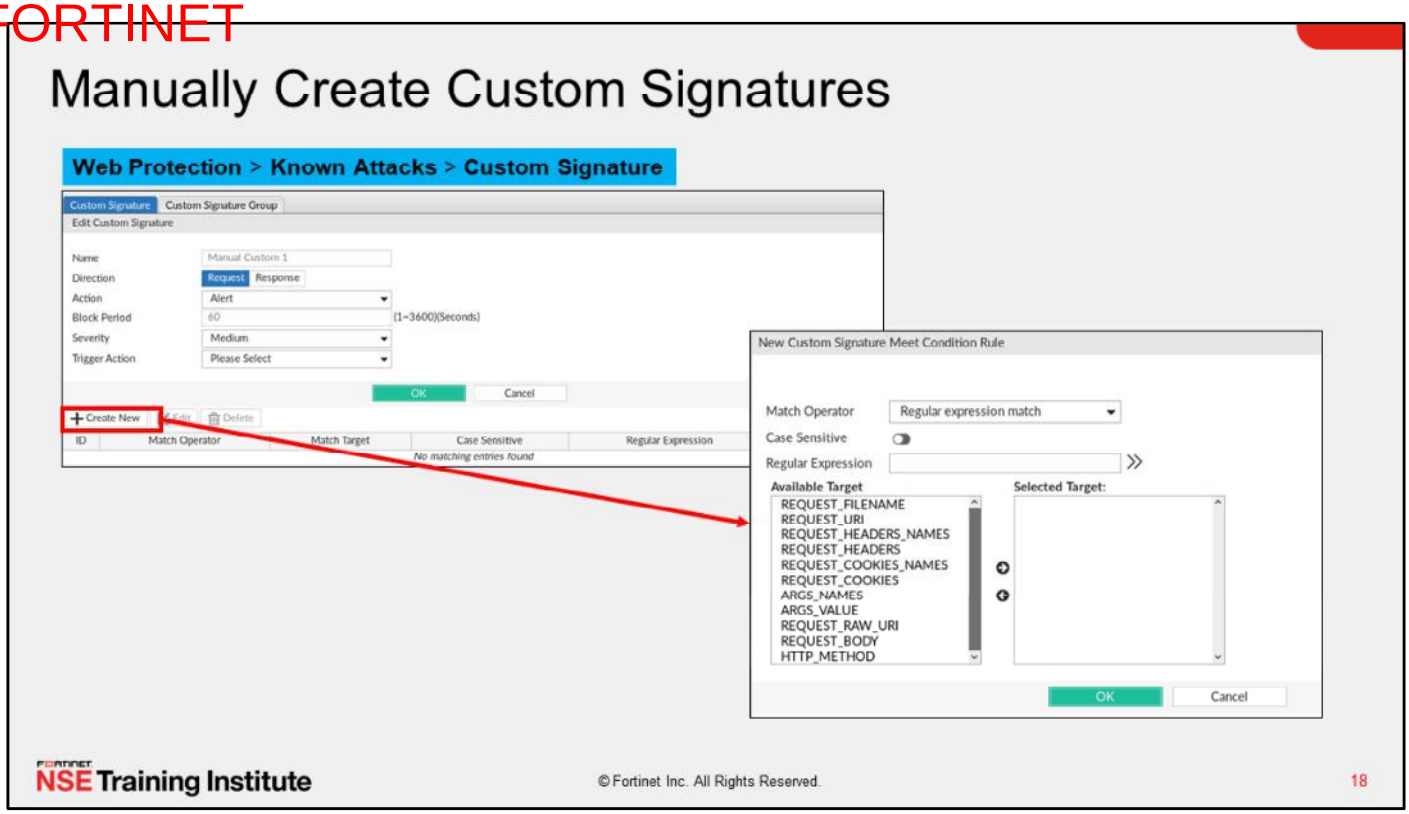
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Whether you have created a custom signature using the **Signature Creation Wizard**, or by cloning one of the default supplied signatures, the final step in customizing the signature is to modify the signature definitions and details.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The third option for creating custom signatures is a full manual creation of a custom signature. This is the most flexible method but is also the most complex. First you manually add a custom signature and then you define each of the condition rules that the signature must match in order to best protect the web application.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Protection Profiles

- Determines which scans and transforms the policy will apply
- Some non-protection actions too:
  - Response cache
  - Redirects
  - Compression
  - Upload limits
- Session management usually required
  - FortiWeb inserts cookie and uses RAM to remember all requests until timeout
  - Required to determine allowed page order, rate limit, and so on

Policy > Web Protection Profile > Inline Protection Profile

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

You select a protection profile in a server policy to indicate which scans FortiWeb performs. The protection profile ties together many component scans. Signatures detect many types of known attacks—like IPS on FortiGate—but FortiWeb analyzes much more than just malformed data. For example, FortiWeb can analyze whether cookies are returned intact and whether sessions are initiated from the correct URL and pages accessed in a logical order. This means that FortiWeb can detect known attacks with signatures and also prevent many zero-day attacks because it has a deeper knowledge of what a proper web connection looks like.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the easiest way to make a custom signature?
   - ✓ A. Clone of a default signature
   - B. Type in regular expression strings individually
   - C. Import signature information from an .xml file

2. Which method of signature creation offers the most flexibility?
   - A. Signature cloning
   - B. Signature wizard
   - ✓ C. Manual signature creation
   - D. FortiGuard default signatures

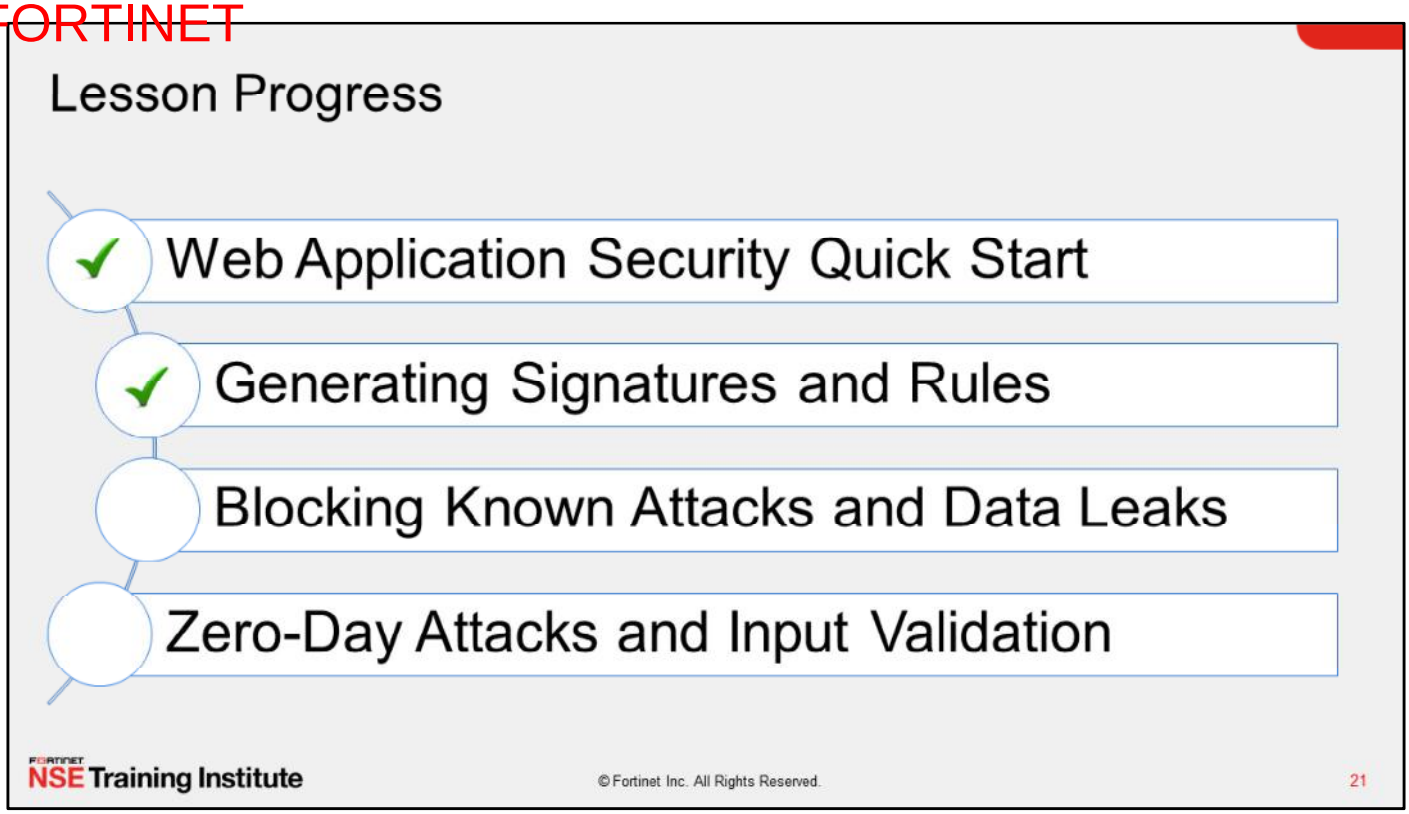
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

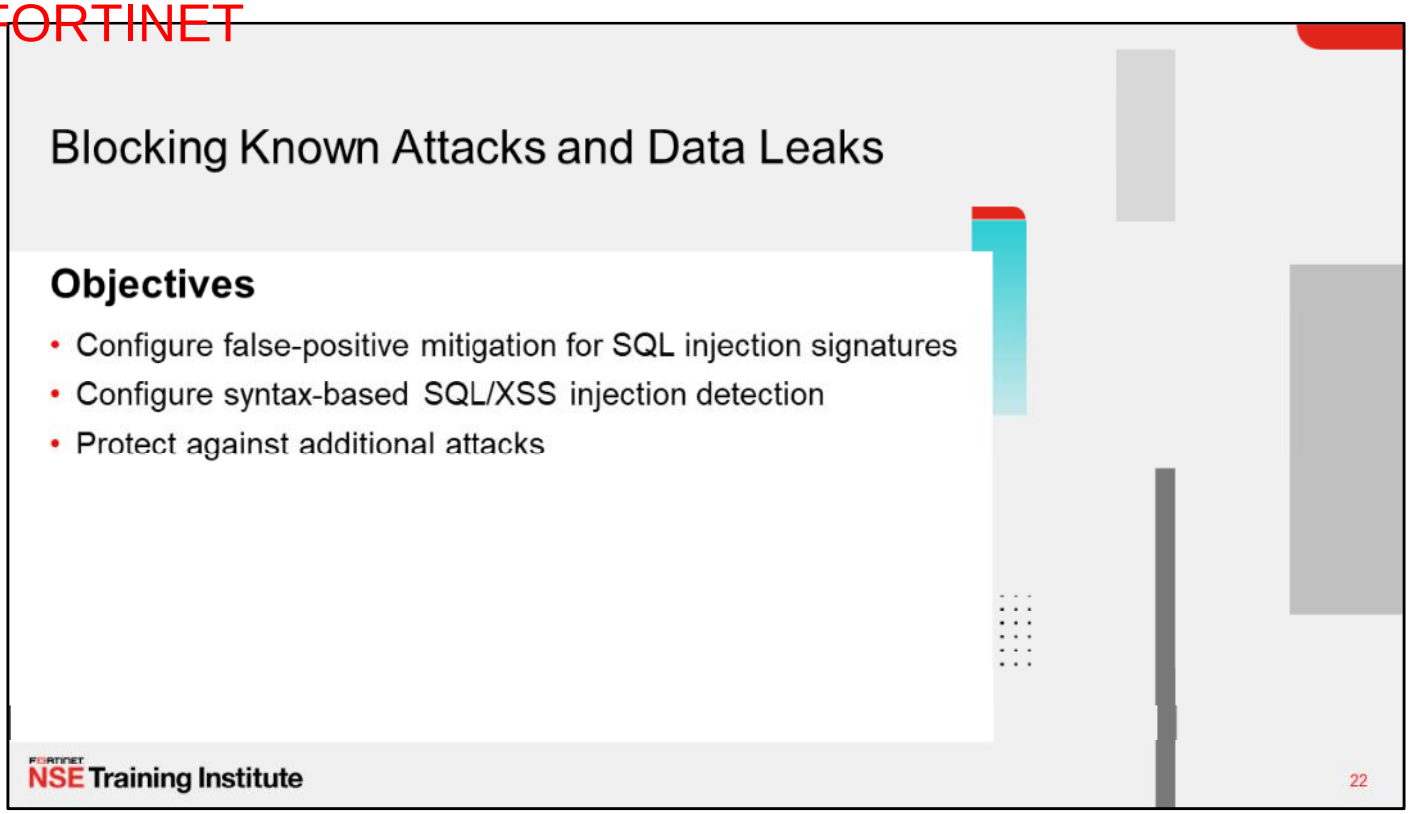


Good job! You now understand ways to fine-tune FortiWeb to your specific environment by generating signatures and rules.

Now, you will learn how to use input validation based on session cookies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in input validation and inspection for SQL injection signatures you will be able to configure FortiWeb to block these types of attacks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Signature Policies

- Signature policies protect web servers from:
  - Cross-site scripting (XSS) attacks
  - SQL injection
  - Common exploits
  - Generic attacks such as OS commands
  - Bad robots, spiders, and scripts
  - Trojans
  - Server information disclosure (`X-Powered-By:`)
  - Credit card data leaks
- Extended signatures are more likely to cause false positives, but may be required in high-security environments
- Use signatures from FortiGuard services or your own custom signatures

NSE Training Institute © Fortinet Inc. All Rights Reserved. 23

FortiGate-style FortiGuard Antivirus signatures are not the only type of signatures that FortiWeb uses.

FortiGuard antivirus is an engine for analyzing binary file uploads; it's enabled by the **Trojans** option in **Signatures**. For non-binary web application exploits, FortiGuard security provides an extensive set of regular expressions that match attack string patterns.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Custom Signatures

- If FortiGuard doesn't have a signature
  - Custom or in-house web applications can be used
- Uses Perl Compatible Regular Expressions (PCRE) syntax
  - Inverse match now widely supported
- Choose which part of the HTTP request FortiWeb evaluates for match

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

Because they are regular expressions, you can also customize or write your own attack signatures. If you do this, use PCRE syntax.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring a Signature Policy

- The **Period Block** setting slows attackers
  - Must wait to try again
- Gives you time to analyze source of attack
- Saves FortiWeb system resources—better performance

Selecting the **Period Block** instead of **Erase & Alert** settings gives you time to respond to hack attempts

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

When configuring which signatures to use, choosing the **Period Block** setting instead of the **Alert & Deny** or **Erase & Alert** setting is an important performance tweak. Select for DoS or persistent attacks to reduce FortiWeb CPU usage and to buy time for forensic analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Known Attacks: Cross-Site Scripting (XSS)

1. Attacker inputs JavaScript in an HTML form or parameter
2. Web application does not reject illegal input
3. Usually, web application saves input to database
4. Innocent client requests page that retrieves from database
   - Now includes malicious script
   - Can cause client's browser to transmit to third-party, malicious server

The variety of attacks based on XSS is limitless, but they commonly include transmitting private data like authentication cookies or other session information to the attacker

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

Signatures detect many types of attacks. Many correspond to the OWASP top 10, which PCI specifically requires that you block.

One type of attack is called cross-site scripting (XSS). The root cause of an XSS attack is that the web application does not sanitize its inputs, rejecting JavaScript. As a result, it stores the XSS attack in its database and, whenever other clients request the page that reuses that data, the JavaScript is embedded in the page.

JavaScript can do many things with a page, including rewriting the whole page and making its own requests. This is the basic mechanism of AJAX applications. In this case, XSS causes innocent clients to transmit to a different server that is controlled by the attacker. This could, for example, transmit credit card information or passwords from a form to the attacker.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Known Attacks: SQL Injection

- Like XSS, but SQL is input
- Web application does not reject illegal input
- When web application connects to database to add input, it can:
  - Download sensitive data from the database (`select * from USERS` and so on)
  - Modify the database (insert, update, or delete)
  - Perform administrative operations (shut down management interface and so on)

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Another very common type of attack is SQL injection. Similar to an XSS attack, its root cause is that the web application does not sanitize input. If the attacker enters a SQL query into an input such as an HTML form, the web application simply accepts it, and passes it along to the database engine, which accidentally runs the query.

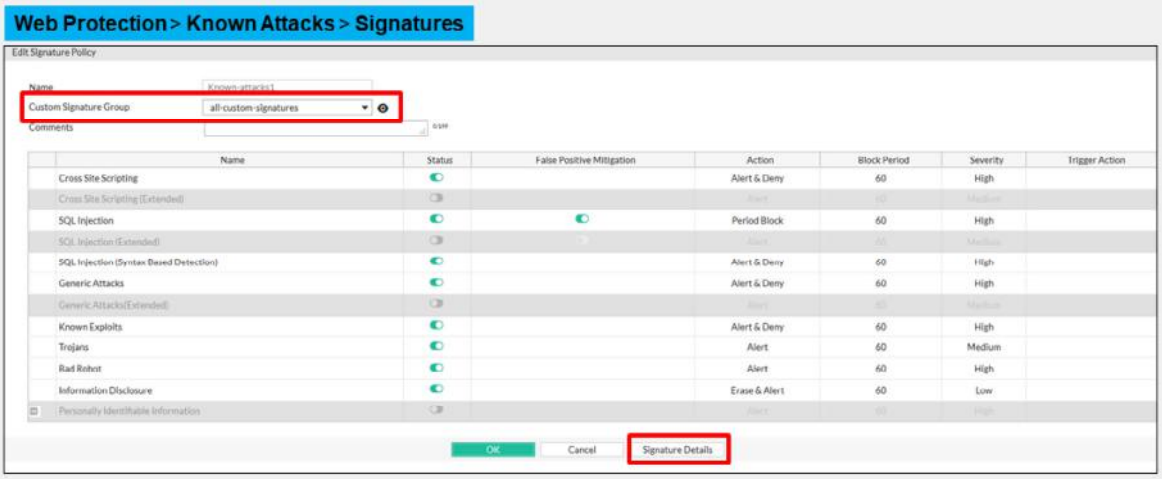
The SQL language can do anything to the data. For example, it can download the table of users so that the attacker can run a password cracker. A query could add new entries for new administrator logins, or modify logins, blocking administrators from logging in to your CMS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fine-Tuning the Signature Selection

- Create, then click **OK**
- Click **Edit**. The **Signature Details** button appears



© Fortinet Inc. All Rights Reserved.

Some signatures apply to most web applications—they are not app-specific. XSS and SQL injection signatures belong in this category.

Popular web applications, such as Drupal and WordPress, are well known. FortiWeb has predefined signatures for their known vulnerabilities, and FortiGuard can provide ongoing updates as new vulnerabilities are discovered. But if you need to protect an in-house, custom web application, you can write your own app-specific custom signatures.

If a predefined signature causes a false positive, edit the signature policy. Click **Signature Details**, and create exceptions, or disable those individual signatures. You don't need to disable the entire category.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Advanced Mode—Signature Policy

- Exceptions by domain name, or URL, or both
- Enable or disable individual signatures to reduce false positives

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

The advanced mode for editing the signature policy offers full flexibility. You can disable a signature in the current policy only, or in all policies. You can also disable it for only a specific domain name, or URL, or both (that is, make an exception to the rule). The exceptions also support PCRE regular expressions so you can match an entire group of URLs if you need to.

Enabling or disabling individual signatures is your primary tool for eliminating false positives.

Alternatively, if you're viewing the attack log and it looks like an innocent request accidentally matched the attack signature, you can also create exceptions or disable signatures while viewing the log.

1. Click a log entry to view its details.
2. In the log entry, click the link to make an exception or disable the signature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which of the following attack type allows an attacker to redirect a client to a malicious website?
   A. Cache poisoning
   B. SQL injection
   ✓ C. XSS

2. What is an example of an HTTP protocol constraint that FortiWeb can enforce?
   A. CSS format
   B. HTTP encryption version
   ✓ C. HTTP body length
   D. HTTP language

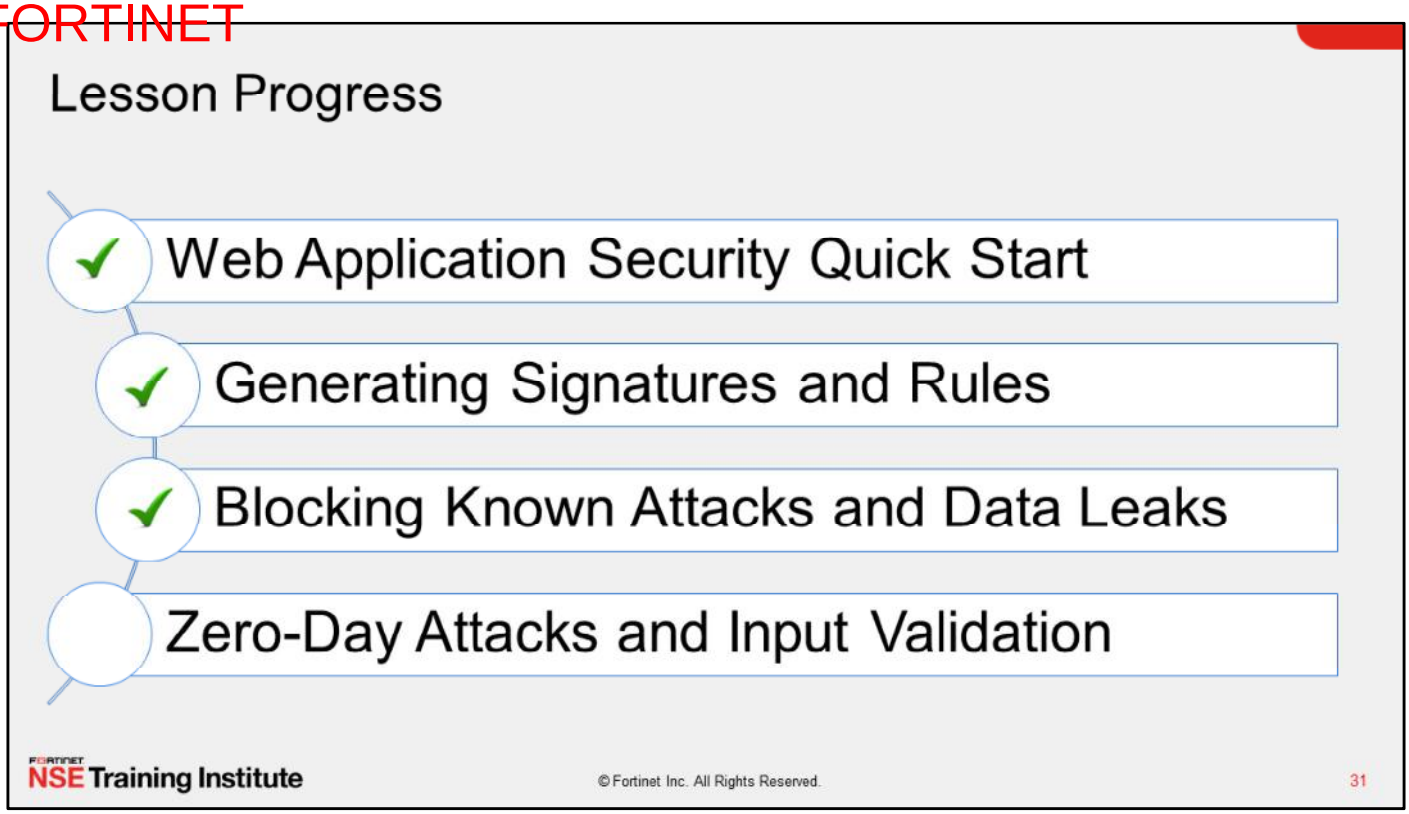
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

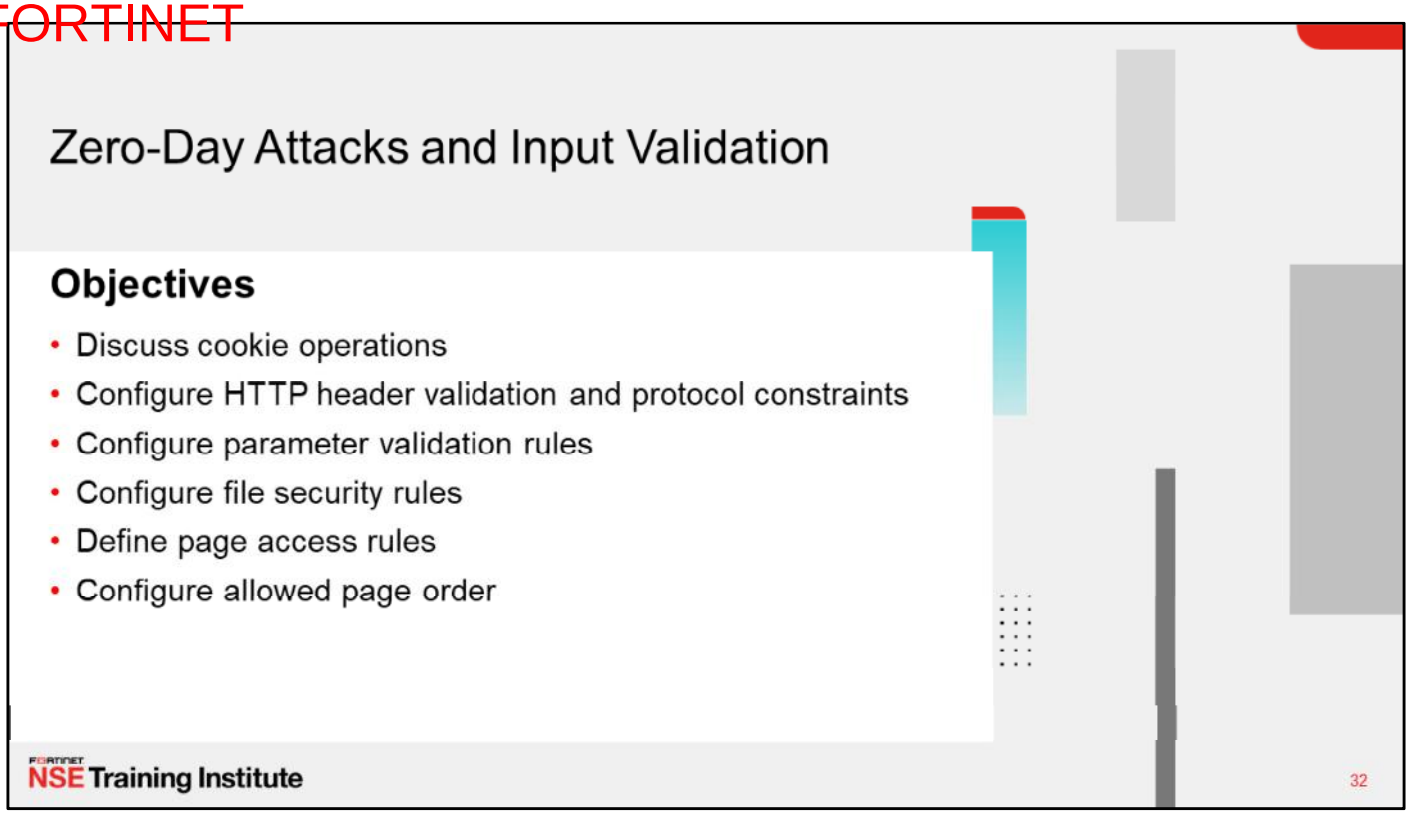


Good job! You now know how to implement input validation based on session cookies.

Now, you will learn how to implement input validation based on headers and body.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

Now, you will learn input validation in reference to the HTTP header and body and how to enforce proper file security practices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How Applications Add Sessions to HTTP

- HTTP protocol is *stateless*
  - Does not store previous page requests, so cannot correlate them
  - Correlation is required for logins, shopping carts, and more
- Most apps or devices add sessions through one of the following:
  - Server-side RAM
  - Client-side cookies stored by browser
- FortiWeb tracks its own security sessions through a cookie
  - When you enable **Client Management**

NSE Training Institute © Fortinet Inc. All Rights Reserved. 33

HTTP is stateless. This means that each request is not correlated to any request before or after.

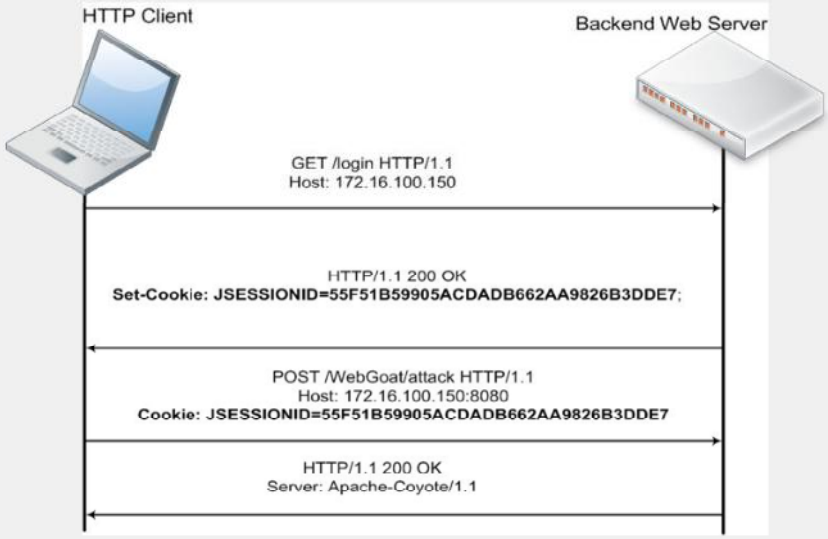
For *simple* web page views, this was enough. However, as web pages became dynamic and eventually became software in their own right—that is, web applications—programmers needed some way for servers to remember variables between each request.

For example, in a page that gradually loads more items as you scroll down, the web application must know which items you have already viewed. If you like a Facebook post, Facebook must know which account you used to log in, so that the like status is applied only when your account is accessing the page—not for everyone. web applications usually remember variables using server-side sessions, session cookies that are stored client-side, or both.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Cookies Sequence



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

This slide shows an example HTTP transaction, showing how cookies are used in a JSP application.

1. First, the client initiates a session by requesting a page: `/login`
2. The server replies. In the reply, the header contains `Set-Cookie:`; the name of a session cookie, `JSESSIONID`; and the session cookie value. The value is a unique ID for this client's session, and allows the server to identify the client and correlate the next request with the first.
3. The client returns the unchanged cookie in its second request.
4. The server uses this ID to remember the settings that it may need to generate the next page in this client's session. Then, it replies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Cookie Poisoning

- Normally, the client should store the cookie and return it unchanged when making the next page request
- Attackers modify the cookie
  - Add code injections
  - Try to overflow buffers
  - Try to access unauthorized state
  - Identity theft

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

Because the server is effectively storing some of its application data on an untrusted client, session cookies are a huge security risk if not protected. A malicious client could change the value of the session cookie. For example, it could replace the session ID with a SQL query. In the next request that the client sends, the poisoned cookie is sent with the request to the server. If the web application does not check the cookie's value for SQL commands before passing the cookie's value into a database query, then the attacker could potentially run any database commands that they want.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Cookie Security

- FortiWeb has two cookie security modes: Signed and Encrypted
- Signed
  - FortiWeb assigns its own session cookie to the connection
  - Hashes session cookie to detect tampering
  - Requires client management to set FortiWeb session cookie to properly track sessions
- Encrypted
  - Encrypts cookie as it is being sent from server to client
  - Only client has access to encrypted cookie
  - FortiWeb decrypts its response to server

NSE Training Institute © Fortinet Inc. All Rights Reserved. 36

FortiWeb has two main cookie security modes.

In Signed mode, FortiWeb sets its own session management cookie. This allows it to track every web session and verify if the session cookies have been tampered with. For every session, FortiWeb hashes the cookies and verifies that it has not been modified since the last time that session was used.

In Encrypted mode, FortiWeb encrypts the cookie as it is being passed to the client. When the client responds to the server with the encrypted cookie, FortiWeb verifies the cookie and decrypts it before passing the connection back to the server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Detecting Cookie Poisoning

- FortiWeb caches the response's cookies
- If the attacker sends a request with an altered cookie, it will not match
- FortiWeb can then do the following:
  - Alert and deny
  - Remove cookie (Erase)
  - Alert (log)
  - Period block
    - FortiWeb won't waste resources scanning requests from a malicious client during this period

NSE Training Institute

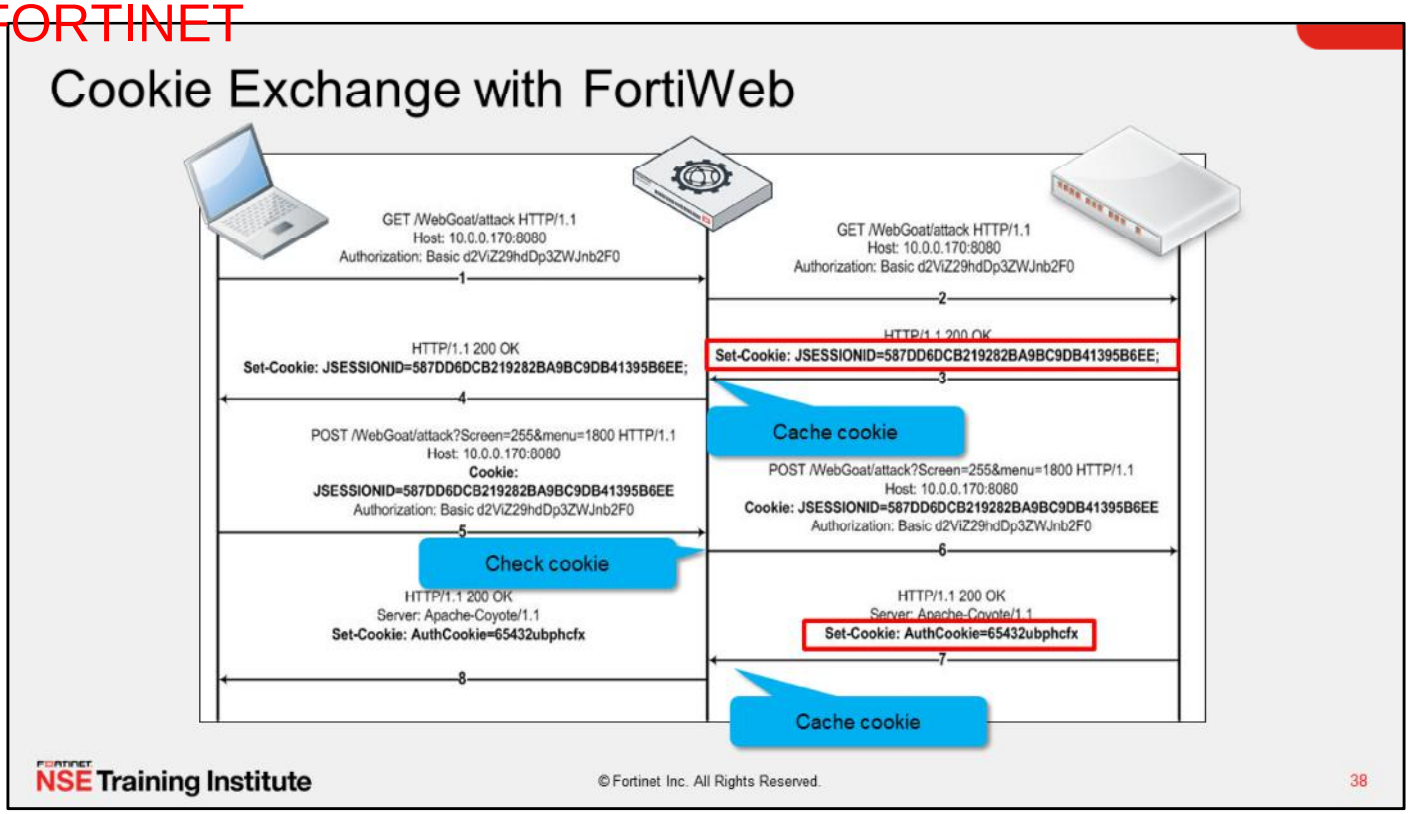
© Fortinet Inc. All Rights Reserved.

37

FortiWeb's cookie poisoning detection blocks this kind of abuse. When cookie poisoning detection is enabled, FortiWeb remembers each cookie, and associates it with FortiWeb's session management cookie. If the next request's cookies don't match the original cookie sent by the server, then FortiWeb knows that the client has changed the cookie. It is very rare for a client to modify its cookies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



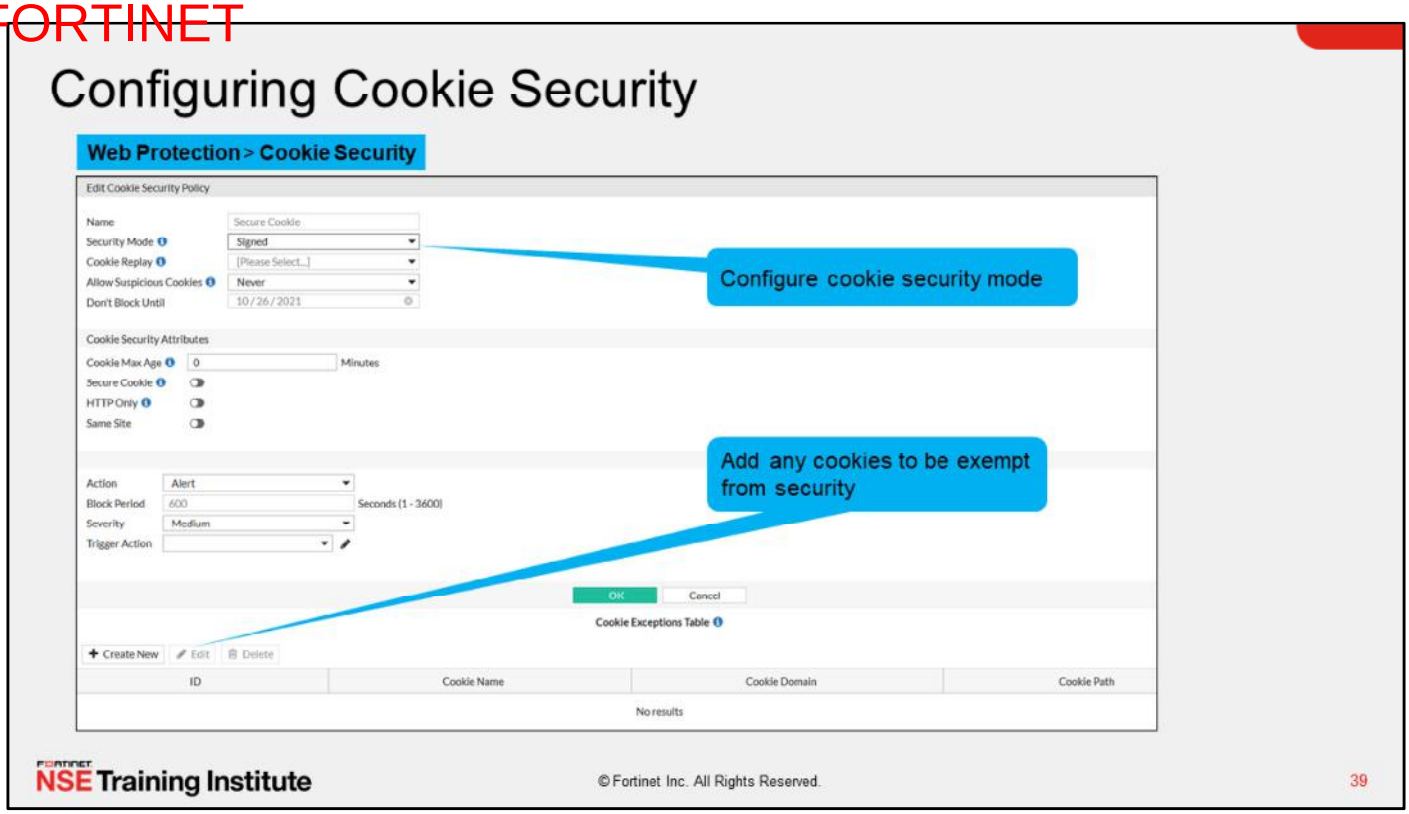
On this slide, you can see an example of a session cookie being present and FortiWeb, inline, scanning for cookie poisoning.

After the client logs in with HTTP authentication, the web application creates a session ID. Then, as the client continues to use the web application, the web application sets a new cookie to indicate that the client has previously authenticated and binds the authentication status to the session ID.

Before the client receives the reply from the server, FortiWeb reads and stores the values of all cookies. If the server changes the cookie's value, FortiWeb updates its cache. After the first request and every time after, FortiWeb validates that the client hasn't changed the cookies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can define a cookie security policy on the **Web Protection** section of the GUI. Here you can define a new security policy, the mode, and what actions FortiWeb should take when cookie tampering is detected. You can also define additional parameters like cookie age and exceptions.

After you define cookie security policies, you can select them in the web protection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HTTP Protocol Constraints

- Protection against buffer overflow attacks and DoS
  - Some HTTP parsers don't restrict the maximum number or length of elements of the HTTP protocol
  - Attackers send requests with large bodies, many headers, and so on
  - Parser loads pieces into buffers, overflowing or exhausting RAM
- Examples:
  - Illegal host names
  - Non-existent HTTP versions
  - Unhandled HTTP request methods
- Required buffer size varies by app

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

HTTP constraints allow you to control the number, type, and length of many HTTP headers. This prevents unexpected inputs from a malicious client that could compromise your server.

The limits can vary according to server software and hardware. For example, if a server has limited RAM, then it's potentially easier to overload or crash with an excessive number of headers, since parsing the headers and storing them in buffers requires RAM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HTTP Protocol Constraints

Web Protection > Protocol > HTTP Protocol Constraints

Edit HTTP Protocol Constraints

Name: SharePoint 2013 Sales

Exceptions Name: [Please Select...]

Status	Name	Length	Action	Period Block	Severity	Threat Weight	Trigger Action	HTTP Protocol Support
Content Length (2)								
	Content Length	16384 (KB)	Alert	60	Low			
	Illegal Content Length		Alert	60	Low			
HTTP Header (6)								
HTTP Parameter (10)								
HTTP Request (9)								
HTTP/2 Frame (5)								
Others (13)								
	Illegal Content Type		Alert	60	Low			
	Illegal Response Code		Alert	60	Low			
	Illegal Host Name		Alert & Deny	60	Medium			
	Illegal HTTP Version		Alert	60	Medium			HTTP/1.X Only
	Body Length	16384 (KB)	Alert	60	Low			
	Number of Cookies in Request	128	Alert	60	Low			
	Number of Ranges in Range Header	5	Alert	60	Low			
	Malformed Request		Alert & Deny	60	Medium			
	WebSocket Protocol		Alert	60	Low			HTTP/1.X Only
	Illegal Connection Preface		Alert & Deny	60	Medium			HTTP/2 Only
	Illegal Frame Type		Alert & Deny	60	Medium			HTTP/2 Only
	Illegal Frame Flags		Alert & Deny	60	Medium			HTTP/2 Only
	Illegal Chunk Size		Alert	60	Low			HTTP/1.x Only

OK Cancel

NSE Training Institute © Fortinet Inc. All Rights Reserved. 41

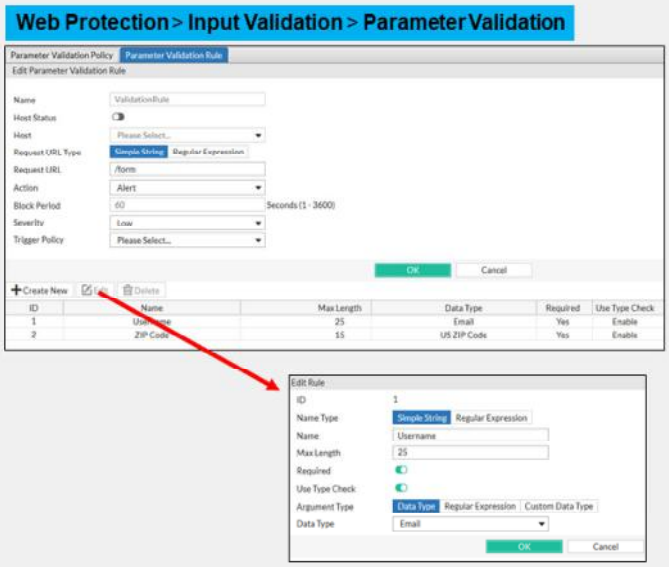
Since requests that use the POST method can have very large bodies, if your web application does not accept movie or music uploads for example, then it can be useful and more secure to reduce the maximum length of the HTTP body.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Parameter Validation Rules

- Defines which parameters in a form are mandatory
- Defines the mandatory format, length, data type for each
- Used for visible inputs usually, but can work for HTML forms where type="hidden"



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

42

FortiWeb can apply reasonable limits to inputs from HTML forms, such as requiring that usernames contain email addresses.

Technically, you can use parameter validation rules regardless of the HTML input type: both visible, user-completed HTML forms, and hidden inputs. HTTP transmits both in the same way. Since hidden inputs are not rendered by the browser as buttons or fields, you may not realize they exist. FortiWeb has rules for hidden inputs. The GUI helps you to quickly configure this specific type of parameter by scanning the URL's HTML page for any hidden inputs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

File Security Rules

- Limits the file size and type

Web Protection > Input Validation > File Security

Edit File Security Rule

Name	File upload limit
Type	Allow File Types / Block File Types
Host Status	
Host	Please Select
Request URL Type	Simple String / Regular Expression
Request URL	/upload$
File Upload Limit	1024 (0-102400)(KBytes)

OK Cancel

+ Create New Delete

	ID	File Types
	1	PDF

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

43

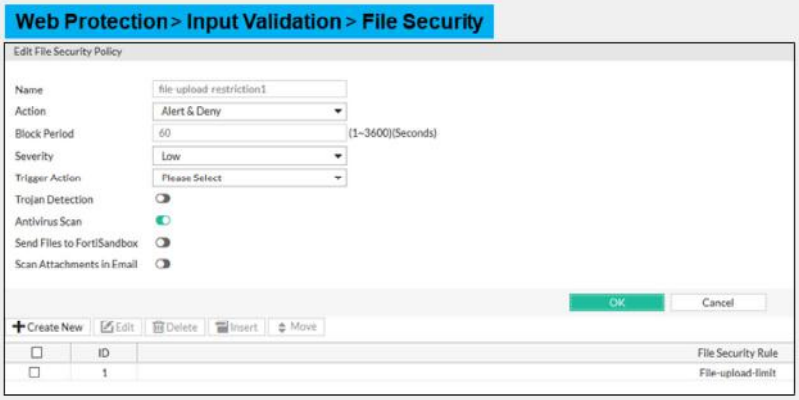
With FortiWeb, you can also specify that excessively large files of a specific type can't be uploaded.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

File Security Policy

- Defines actions if violation
- For antivirus scanning, also enable the signature's trojans in the signature policy



© Fortinet Inc. All Rights Reserved.

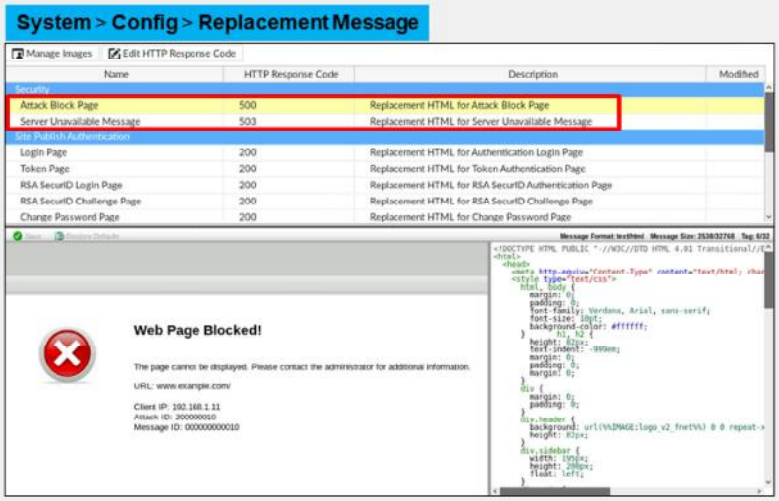
When restricting uploads, you can also engage FortiGuard antivirus.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Replacement Messages

- Customizable on FortiWeb
- Response codes can also be modified



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

Regardless of the reason why a request is detected as an attack, you can usually customize FortiWeb error messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Start Page

- Not all attacks can be detected by a signature
  - Some exploit lack of authentication, rate limits, sessions, and so on
- Defines the valid starting URL for a web application
- User is required to initiate a session from a specific URL
  - Example: `/login.php`
- FortiWeb blocks or redirects if client starts a session from another URL

NSE Training Institute © Fortinet Inc. All Rights Reserved. 46

Not all attacks can be detected by regular expressions that match an input string. The exploits that are hardest to find and protect against are mechanistic. They exploit how the web application allows transitions from one page to the next, and are not logically valid.

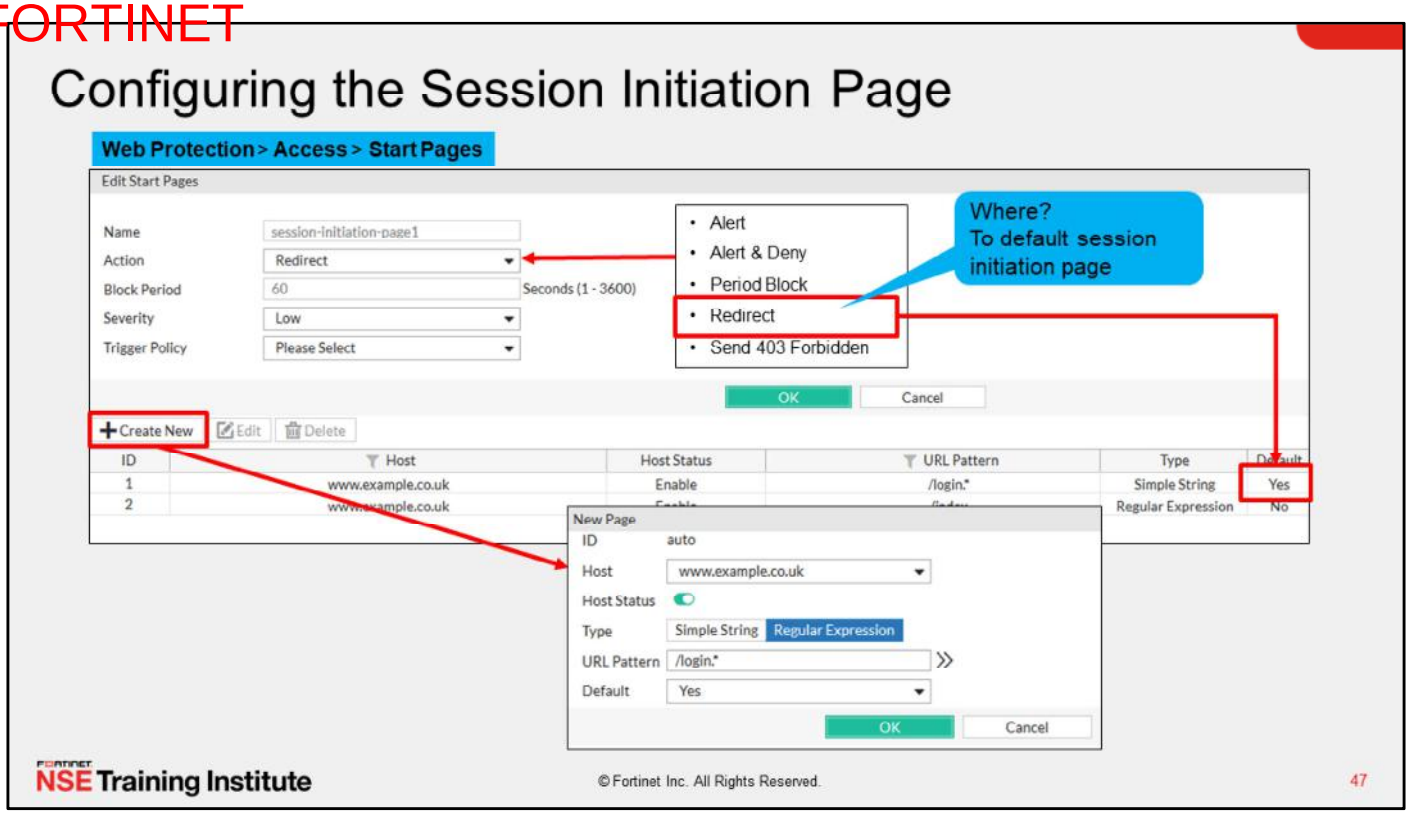
One major category of mechanistic attacks involves how sessions are initiated. If a shopping cart must be associated with an existing session, a file upload must be associated with a previous login. For any other correlation of a page with previous pages, then the web application must validate that:

- The session is not null.
- The session was created by that client IP address or browser.
- The session was created by visiting a URL where sessions normally begin, such as a login page or advertising campaign URL.

Otherwise, the attacker can exploit the app in many ways, including session hijacking.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The session initiation page can be difficult to configure correctly unless you understand the web application well. Instead of selecting **Period Block**, **Send 403 Forbidden**, or **Alert & Deny** from the **Action** drop-down list, select **Redirect**, to redirect the client to the correct page for session initiation. Since a web application can have multiple valid session initiation pages, the default setting indicates the target for the **Redirect** action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Page Access

- Despite the name, order, *not* access control or authentication
- Some URLs must be accessed in a *specific order*
  - Enforces the business logic of a web application
  - Prevents some cross-site request forgery (CSRF) and other state-based attacks

Example: Given the page access rule set shown below:

```
1. /addToCart.do?item=ABC…
2. /checkout.do?login=username1&password=P4sswD
3. /shipment.do
4. /payment.do
5. /confirm.do?id=123456…
```

If a user goes to the page `confirm.do before payment.do`, FortiWeb should block the request

NSE Training Institute © Fortinet Inc. All Rights Reserved. 48

Many other mechanistic attacks exploit page flow after the session is initiated. Page access rules enforce valid page order. You shouldn't, for example, be able to place an order for a TV unless you've submitted payment!

Page access rules can't completely prevent all permutations of CSRF attacks. Some require too much RAM to prevent. A solution could become a potential performance bottleneck or an opportunity for DoS attacks. Vulnerability scans, IP reputation, and other features are still important; however, page order rules can prevent many of these attacks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring the Allowed Page Order

- Either literal URL or regular expression to match multiple URLs
- Enter URLs in expected order
  - FortiWeb allows other pages between

Web Protection > Access > Page Access

Edit Page Access Rule

Name: page-order1
Severity: Medium
Trigger Policy: NotificationSettings

OK | Cancel

Create New | Edit | Delete | Insert | Move

ID	Host	Host Status	URL Pattern	Type
1	www.example.co.uk	Enable	/payment.do	Simple String
2	www.example.co.uk	Enable	/confirm\.do.*	Regular Expression

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

49

This slide shows you how to configure a page order rule. Notice that you don't have to input all pages—only those where the order between two pages must be enforced.

You can specify that the rule applies only to specific virtual hosts and specific URLs. This prevents false positives and wasted resources, improving performance, since FortiWeb needs to store the session page order only for those specific combinations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When do you need to configure a page access rule?
   A. When your application uses dynamic URLs
   ✓ B. When you need to enforce a specific business logic
   C. When you want to deny access to your phpinfo.php file

2. What action can FortiWeb take when cookie poisoning is detected?
   A. Alert & Modify
   ✓ B. Period block
   C. DoS Attack

3. How can FortiWeb protect against cookie poisoning?
   A. FortiWeb issues a new cookie for each packet
   ✓ B. FortiWeb caches each cookie and compares it to each request in the session

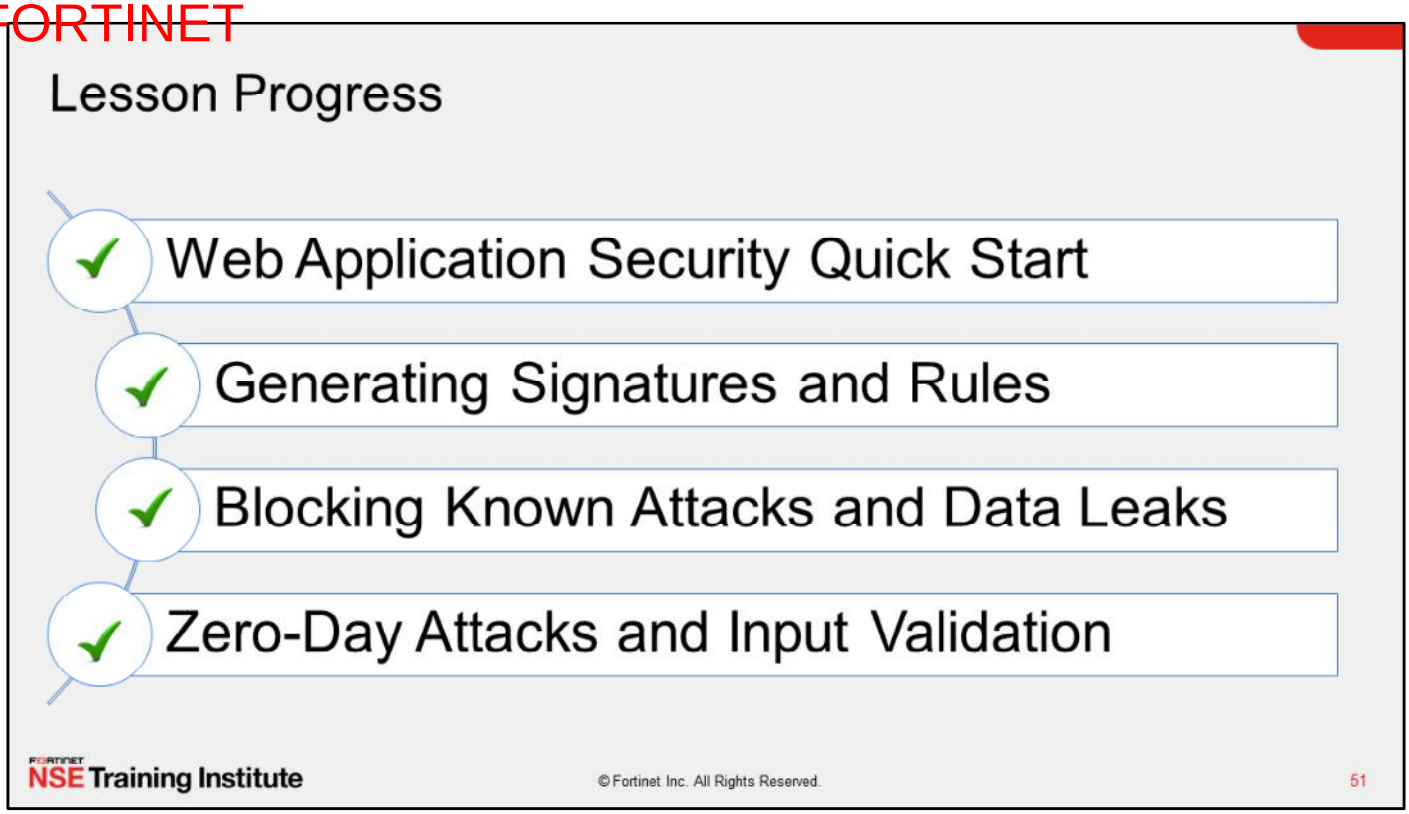
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

50

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now know how to implement input validation based on forms.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Discuss quick start methods on FortiWeb
- ✓ Configure FortiWeb in monitor-only mode
- ✓ Configure a custom web protection profile
- ✓ Configure signature-based attack mitigation
- ✓ Configure custom signatures
- ✓ Configure header validation and protocol constraints
- ✓ Configure input validation rules
- ✓ Configure file security rules
- ✓ Define page access rules

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

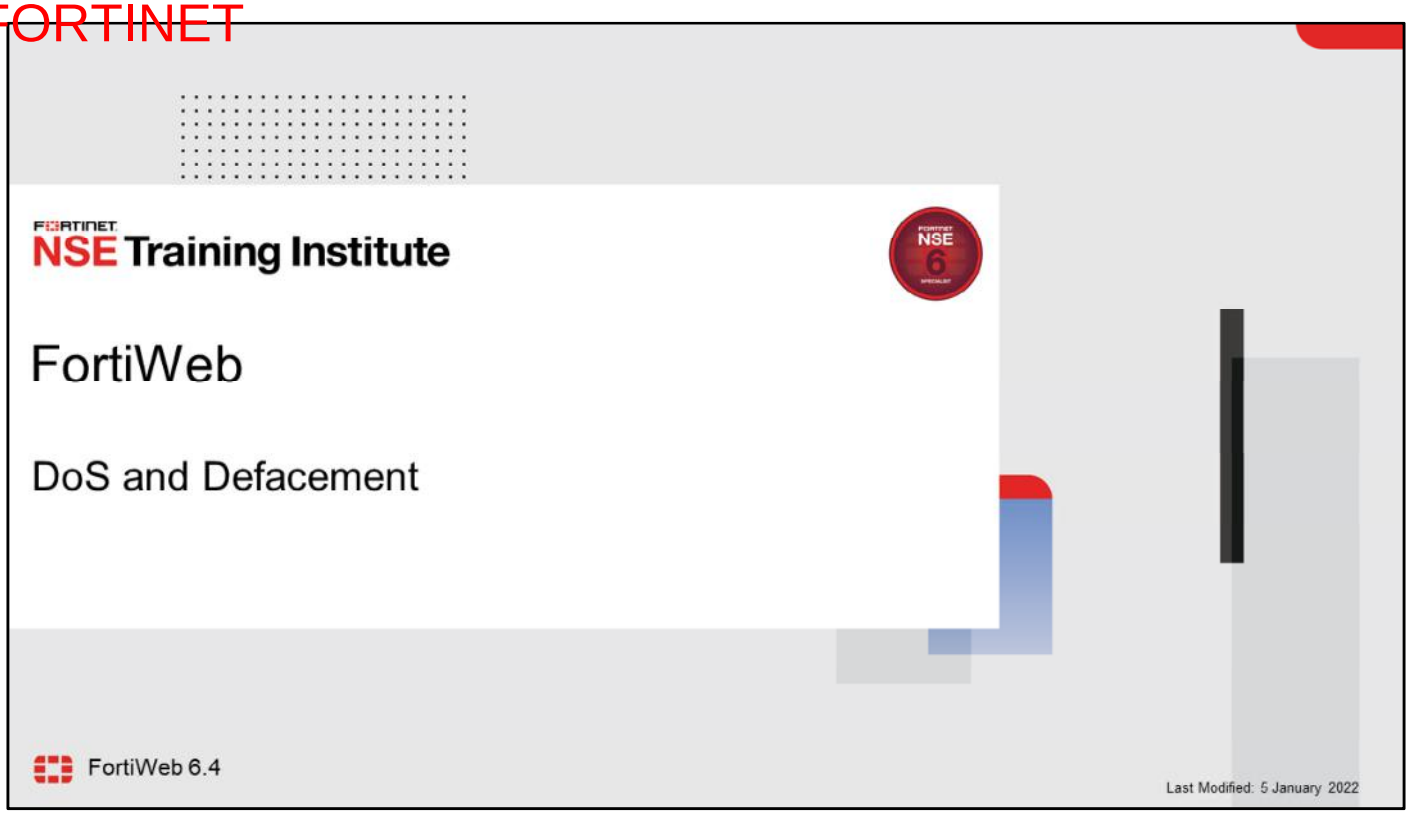
52

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use strategies to quickly deploy FortiWeb and use inputs from various sources to mitigate attacks on your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to mitigate denial of service (DoS) attempts and how to prevent (and rapidly reverse) vandalism to websites protected by FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Threat Overview
- Network and Transport Layer Analysis
- Blended Analysis—Layers 3/4 + 7
- Defacement

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

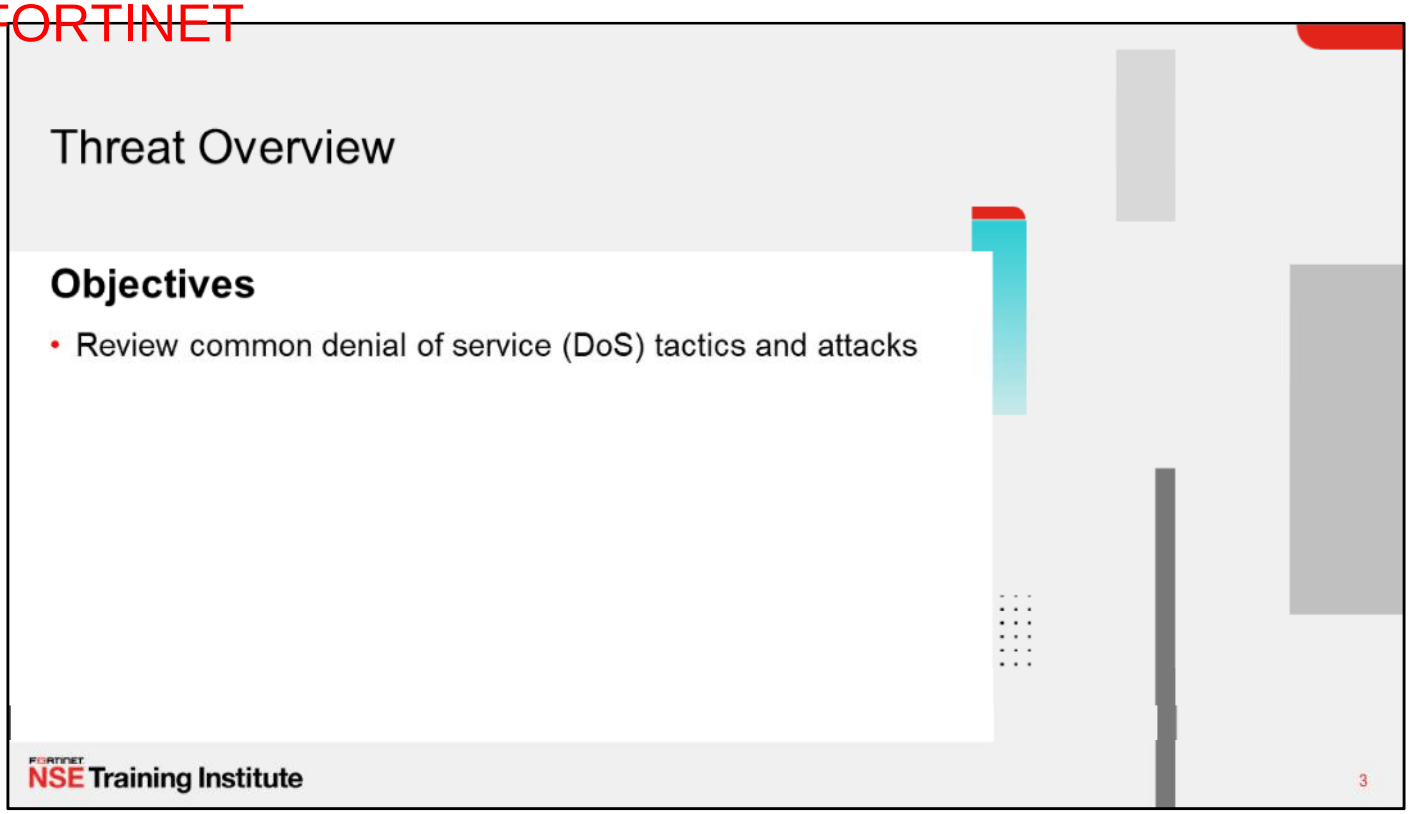
2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

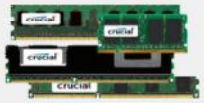
By demonstrating competence in understanding the threats, you will be able to identify how FortiWeb can help protect your network from common DoS attacks.

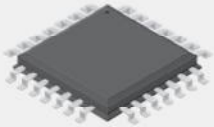
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

DoS Attacks on Web Servers

- A DoS attack is any attack that makes a service unavailable. Multiple mechanisms exist:
  - Using all of the finite memory of the server
  - Asymmetric processing load
    (bigger burden on server side than client side)
  - Tying up all network sockets
- Examples of the impacts that DoS attacks can have include:
  - Server cannot make new sessions (for example out-of-memory errors)
  - Server has too many clients for its resources
    (for example, concurrent connection limit or socket exhaustion)
  - Server CPU uses more cycles to reply than client CPU to send
    (for example, RSA key gen for SSL handshake)
    - SSL/TLS and IPsec VPN are not immune





NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

Denial of service attacks are not harmless, or cheap. Every public web server can be vulnerable to an attack that attempts to make it unreachable and unavailable to users.

What are these types of attacks?

DoS is a broad category of attacks. Protocols like NTP, HTTP, SSL, and DNS have been used to make web servers unreachable. It's any attack that makes a service unresponsive without the need to breach the operating system or process, but simply overwhelms the service's ability to respond and process data. Once a server's bandwidth, CPU, memory, or service-specific sockets or memory buffers are consumed, it cannot respond to legitimate users. To stop a DoS attack, you must prevent those resources from being consumed and ensure only legitimate traffic is reaching the server. Since this lesson is about FortiWeb, you will learn about how to mitigate DoS attacks on the main protocols that affect web traffic: IP, DNS, TCP, HTTP, and SSL or TLS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

DNS and the Web

- DNS is critical to the internet
- FortiWeb doesn't protect DNS, and public DNS is often hosted externally
- Add multiple distributed name servers in your domains' NS records
  - ns1.example.com
  - ns2.example.com
- Use geographically distributed name servers and data centers
  - FortiADC is a worldwide, in-the-cloud, DNS-based load distributor
  - Can monitor for worldwide data center availability
- Load test name servers
- Test for vulnerabilities to DNS poisoning, DNS hijack, and others

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

FortiWeb is not designed to directly defend DNS servers. But it is critical that you don't forget DNS when hardening your defenses.

Without DNS, the internet doesn't work because no one is able to find your website to access and connect to it.

Consider the case of Lenovo. After Lenovo's Superfish vulnerability was disclosed, the hacker group Lizard Squad used a DNS hijack to redirect `lenovo.com` to their own web server. The files on Lenovo's web servers weren't modified or even affected. Only DNS servers were compromised.

There are secure, load-tested DNS solutions. Since many web apps are often hosted in redundant, geographically distributed data centers—some in San Francisco, others in New York, Sao Paulo, Shanghai, Oslo, Frankfurt, or Dubai—it's also worth it to consider a DNS solution, such as FortiADC. It can send clients to the closest data center that is available.

That way, if an individual data center is under a 300 Gbps DoS attack, legitimate clients could still use other sites that aren't affected. In a severe distributed denial of service attack (DDoS), the latency caused by a server being in another country still might be better than a server under heavy attack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Normal Throughput and Baseline

- SNMP polls or SIEM
- HTTP throughput widget
- Data analytics
  - Hit count range
  - Geographic locations – Are they your usual sources of traffic?
- Bot analysis
- External tools
  - Browser development tools
  - Google Analytics
  - FortiADC
  - FortiDDoS

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

To fight DoS attacks, it is very important to know if it is really a DoS attack, or just a regular traffic spike. What's your network's normal behavior including during periods such as holiday shopping seasons? Do you normally have traffic from Brazil or Antarctica?

Some types of DoS attempts are easy to determine. TCP SYN flood and TCP floods using a single HTTP session cookie are almost never caused by normal clients. Unusual spikes of traffic from countries that have no business with your organization can also be a clear sign of a concentrated attack.

But in other cases, traffic anomalies can be part of your normal traffic patterns. How many images, scripts, and videos are loaded for each web page? How many people usually visit your site on Sunday, compared to Monday? If you know your normal ranges, it is easier to recognize a traffic spike, and will help you properly configure the DoS sensors on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Why is it important to have a baseline of your network's normal traffic?
   A. To identify what resources are most frequently accessed
   ✓ B. To determine what is normal so you can better identify when an attack is occurring

2. What is a denial of service attack?
   ✓ A. Any attack that makes a service unavailable
   B. An attempt to deface the site

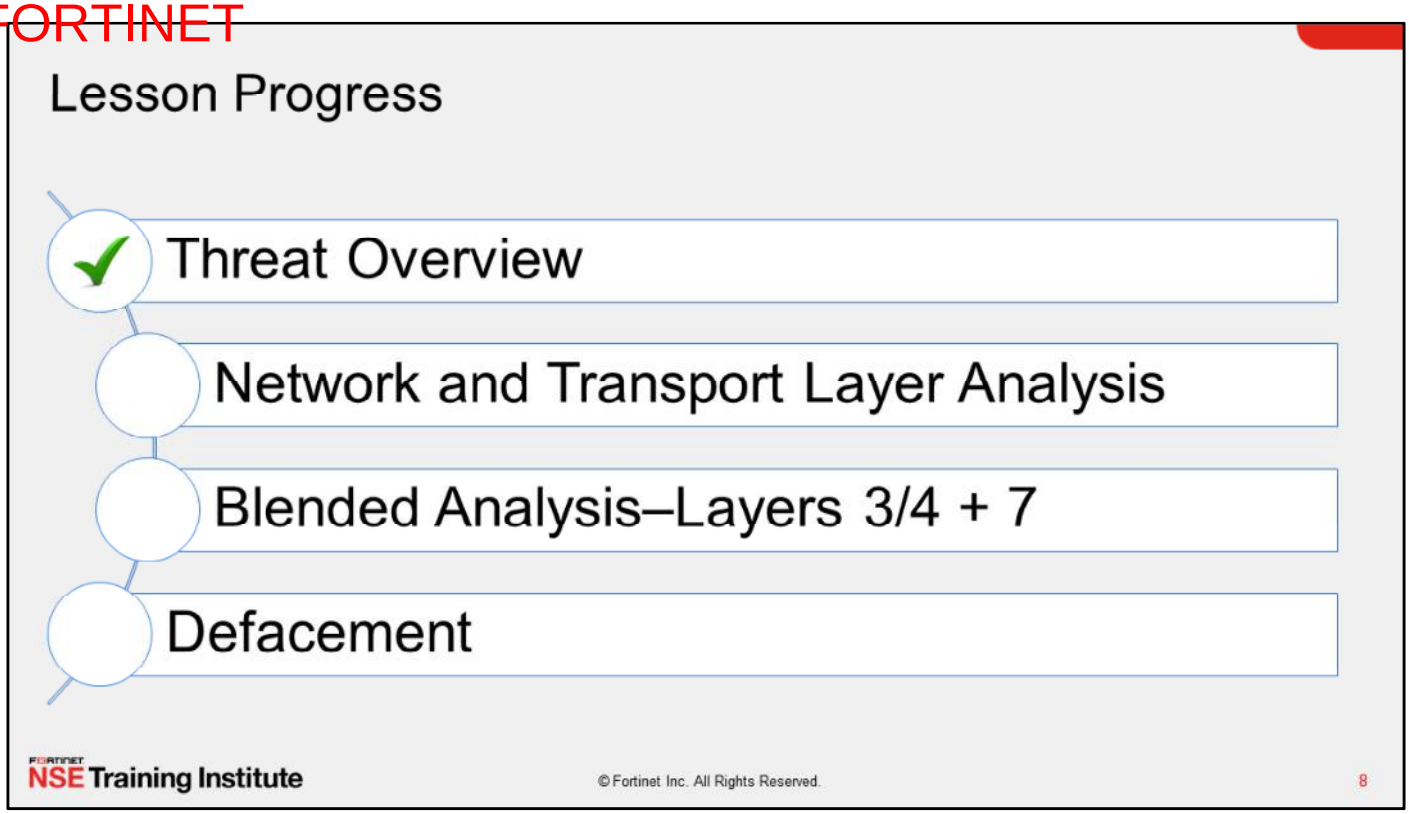
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

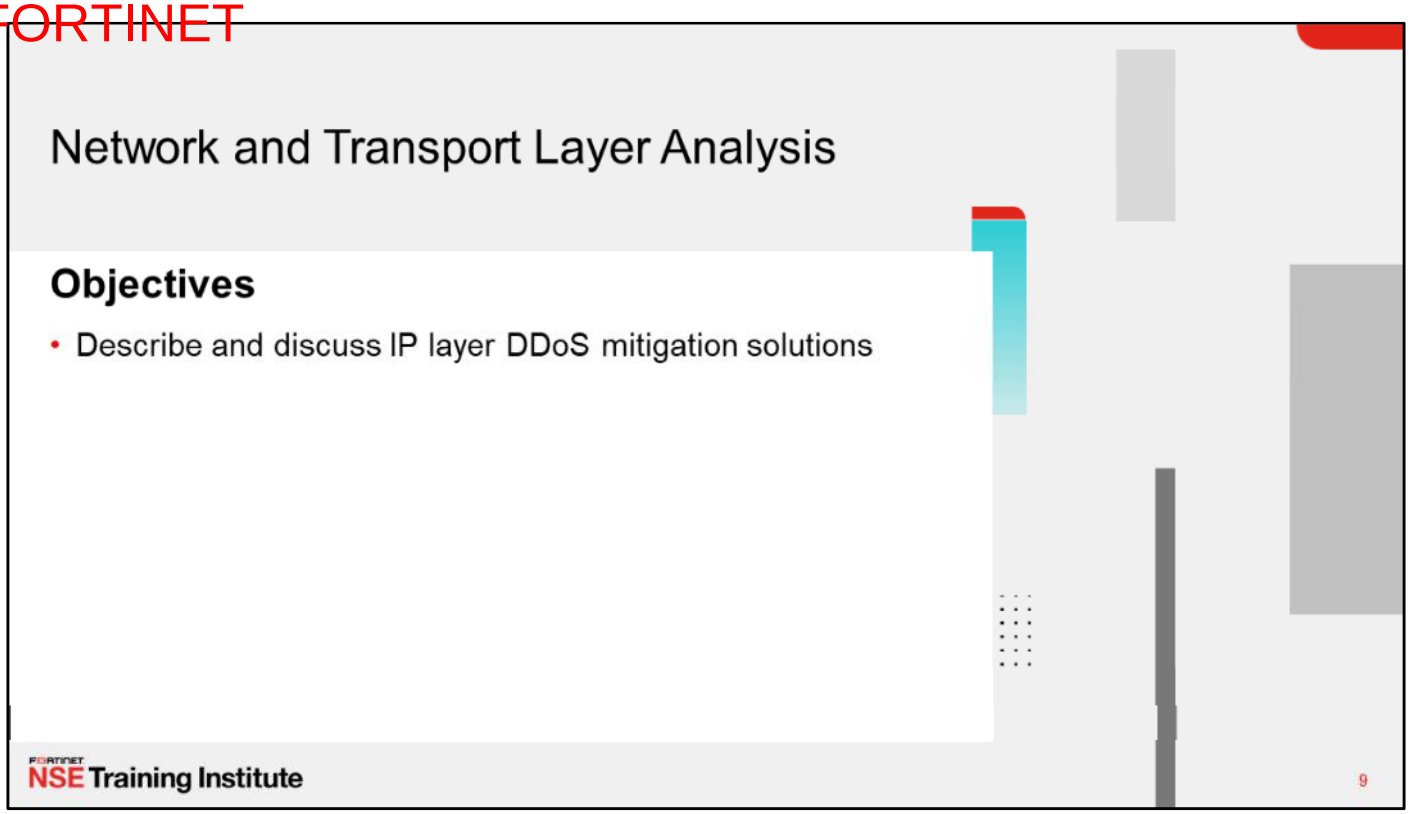


Good job! You now have a better understanding of various threats.

Now, you will learn how to mitigate threats at the network and transport layers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in using FortiWeb against DoS attacks that use web stack protocols, you will be able to mitigate attacks on a couple of different network layers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGuard IP Reputation

- Regularly updated if you have subscribed FortiWeb to FortiGuard IP Reputation service
- FortiGuard maintains a list of public IP addresses
  - Reputation status
  - Why IP is listed
- IP has a bad reputation if it has participated in attacks

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

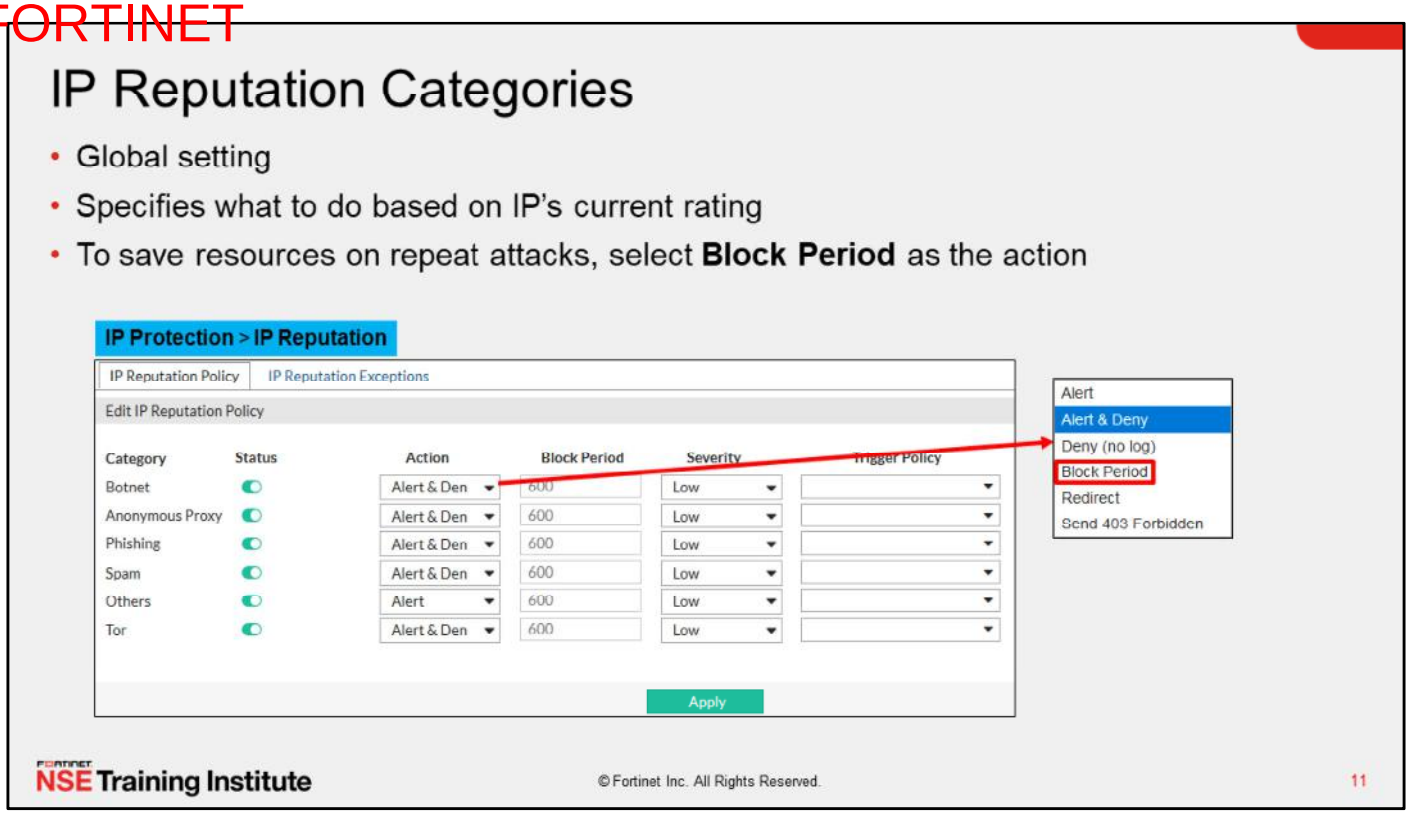
At the IP network layer, FortiWeb can protect you in multiple ways.

When you apply a period block action to a signature or other triggered FortiWeb event, that client's source IP is ignored until the penalty time period is over. But that's not the only way that FortiWeb uses the client's source IP.

One of the best methods of protection is FortiGuard IP reputation. It requires no maintenance, and it's efficient—it blocks quickly, at a low layer, before FortiWeb has wasted CPU time on more intensive actions to determine if the connection should be allowed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



An IP can have a bad reputation for many different reasons. Which of those reasons matter?

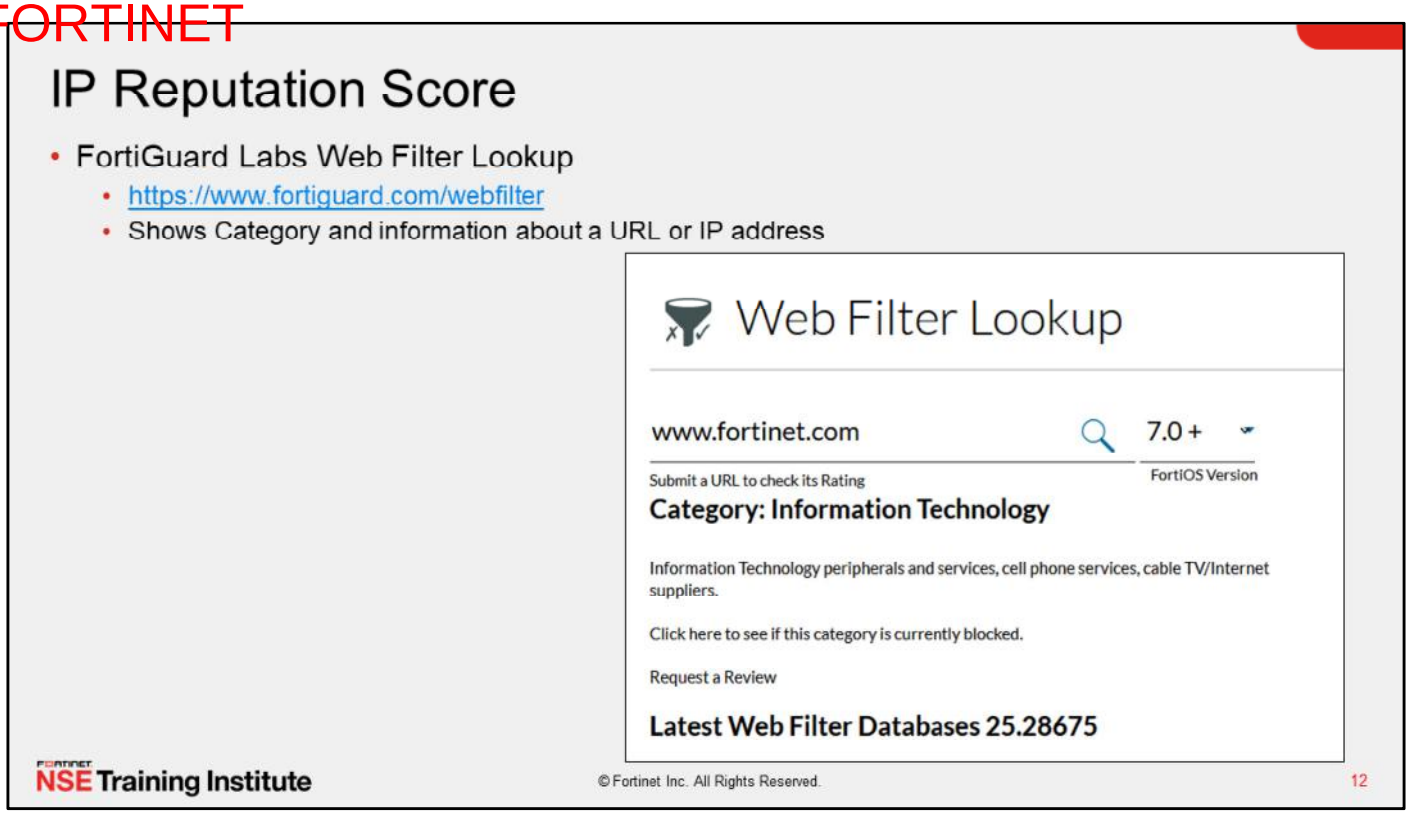
Zombie PCs can send both attacks and innocent traffic—usually the person is using their computer without knowing that it is infected and participating in attacks. Other types of attacks indicate that source IP addresses always should be blocked.

Unless you are protecting webmail servers, you may not need to block IPs that are known spammers; however, you may want to apply a block period action to known botnet participants, since they are often associated with DoS attacks. Proper block periods can improve performance. Like all caching strategies, it uses a little bit of RAM to save CPU and bandwidth resources that are scarce during a DoS attack. FortiWeb will not remove the client's IP from its temporary blacklist cache until the period expires, and it won't waste CPU or bandwidth replying with a 403 error at the HTTP layer.

Specific IP addresses can be exempted from these lists on the **IP Reputations Exceptions** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



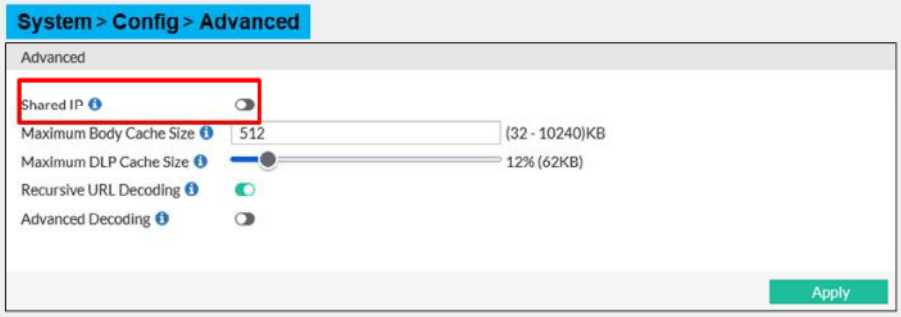
The FortiGuard Web Filter Lookup allows the lookup of IP addresses or URLs in the FortiGuard database. This will show what the category of the host or IP address is categorized as and any additional information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Standalone Compared to Shared IP

- If disabled, FortiWeb gives all source IPs the same rate limit as one client—even if it's an office of 200
- If enabled, brute force, DoS, and others can apply two separate rate limits: standalone or shared internet connections



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

If you are not completely blocking an IP, then the next logical action is to protect your network from rate anomalies. Usually, it doesn't work well to apply the same rate limit to all user types. Request rates that are normal from an airport Wi-Fi network or large office might be very abnormal for a single person at home. You don't want to set too low a limit, effectively blocking all large buildings. But due to IPv4 NAT, it can be hard to tell how many private network clients are behind a single public IP.

On FortiWeb, there are two ways to distinguish shared internet connections and apply different rate limits for them. One way is shared IP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Detecting Shared Internet Connections

- If an IP header's ID field is random or not sequential, it usually means the internet connection is shared
  - One source IP = many clients
- Otherwise, it is standalone
  - One source IP = one client
  - Not all TCP/IP stacks do this, but most do
  - Requires some RAM to remember the previous packet's ID from each source

```
⊞ Frame 3 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Vmware_96:e7:1b (00:0c:29:96:e7:1b)
⊟ Internet Protocol, Src: 10.0.0.200 (10.0.0.200), Dst: 10.0.0.150 (10.0.0.150)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 48
    Identification: 0xa37b (41851)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x41ef [correct]
    Source: 10.0.0.200 (10.0.0.200)
    Destination: 10.0.0.150 (10.0.0.150)
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

The **Shared IP** setting uses a small amount of RAM so FortiWeb can remember the IP ID number in the previous packet's IP header. If your web apps' requests don't have a session cookie, this may be the only way that you can distinguish when multiple clients share the same internet connection.

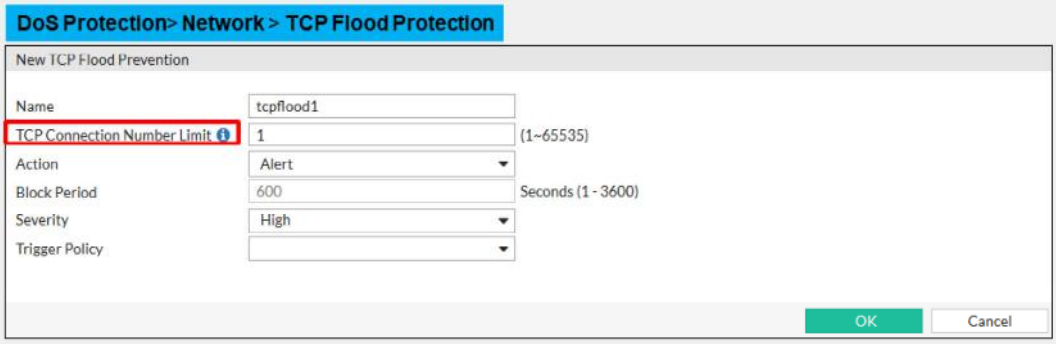
If the numbers are sequential, then that IP usually has only one client behind the public IP. FortiWeb calls this a standalone IP. If the numbers are non-sequential, it usually means that there are multiple clients behind that public IP. FortiWeb calls this a shared IP, and you will usually configure higher rate limits for shared IPs in DoS sensors that use the **Shared IP** setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

TCP Flood Prevention

- Limits fully formed TCP connections for each source IP address
- Only standalone IP addresses (no shared IP) are counted



NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

TCP flood attacks exploit the fact that servers must consume memory to maintain the state of the open connection until either the timeout, or either the client or server closes the connection. This consumes some memory even if the client is not currently sending any HTTP requests. So, a malicious client could attempt to hold as many TCP sessions open as possible without sending data to overwhelm and slow down a web server.

Not all DoS sensors use the **Shared IP** setting. TCP flood prevention, for example, simply specifies one connection rate limit.

This scan is bypassed if you have selected HTTP content routing deployment mode in the server policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How does FortiWeb define a shared internet connection?
   A. A guest Wi-Fi account
   B. Two internet connections bonded together in one pipe
   ✓ C. Multiple computers appearing from a single IP address
   D. Allowing internet access from your phone to a laptop

2. What is one of the key benefits of the FortiGuard IP Reputation feature?
   ✓ A. Maintains a database of public IPs with a reputation for participating in attacks
   B. Maintains a list of private IP addresses

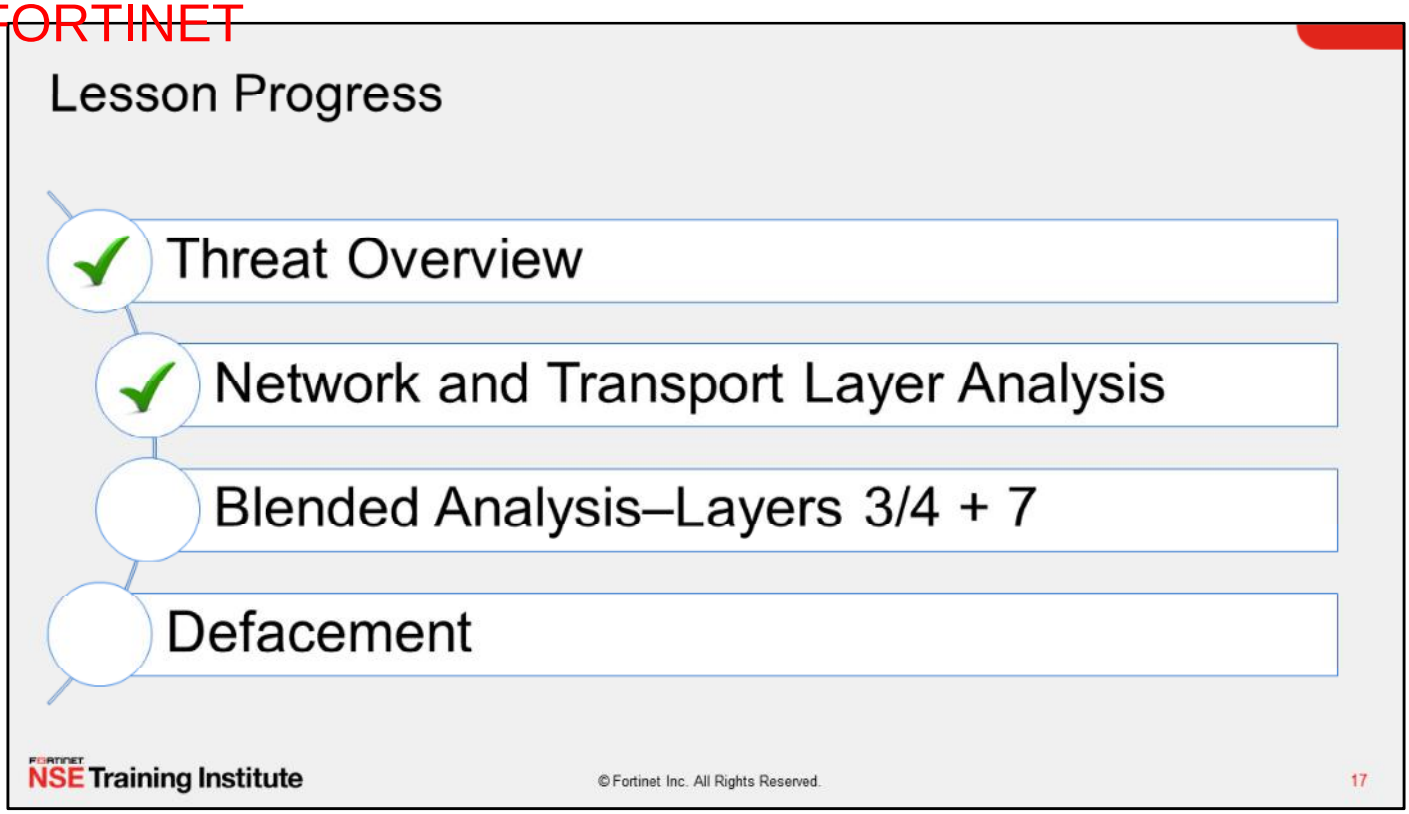
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

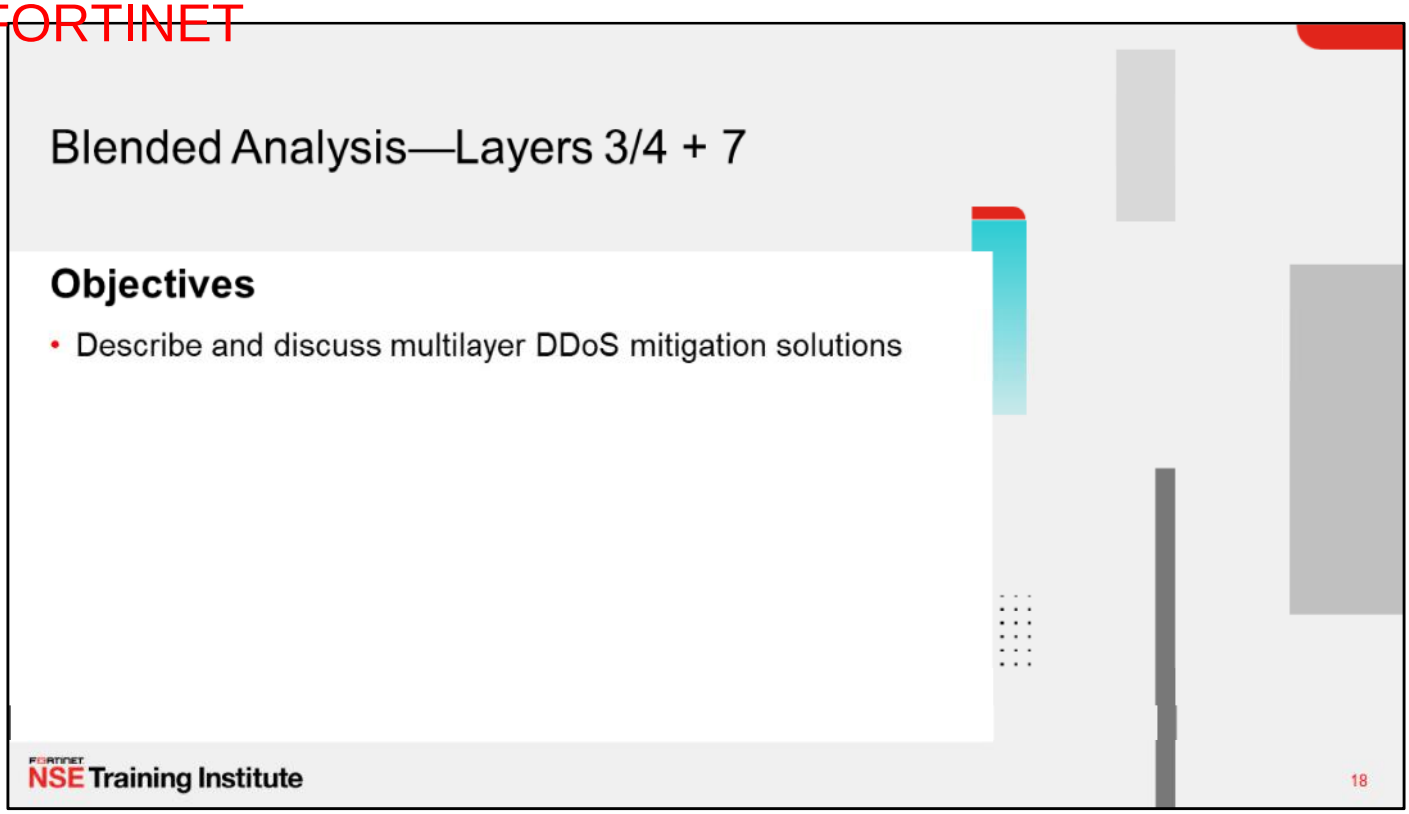


Good job! You now know how to detect and prevent threats at the network and transport layers.

Next, you will learn about blended analysis, where all three layers are involved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

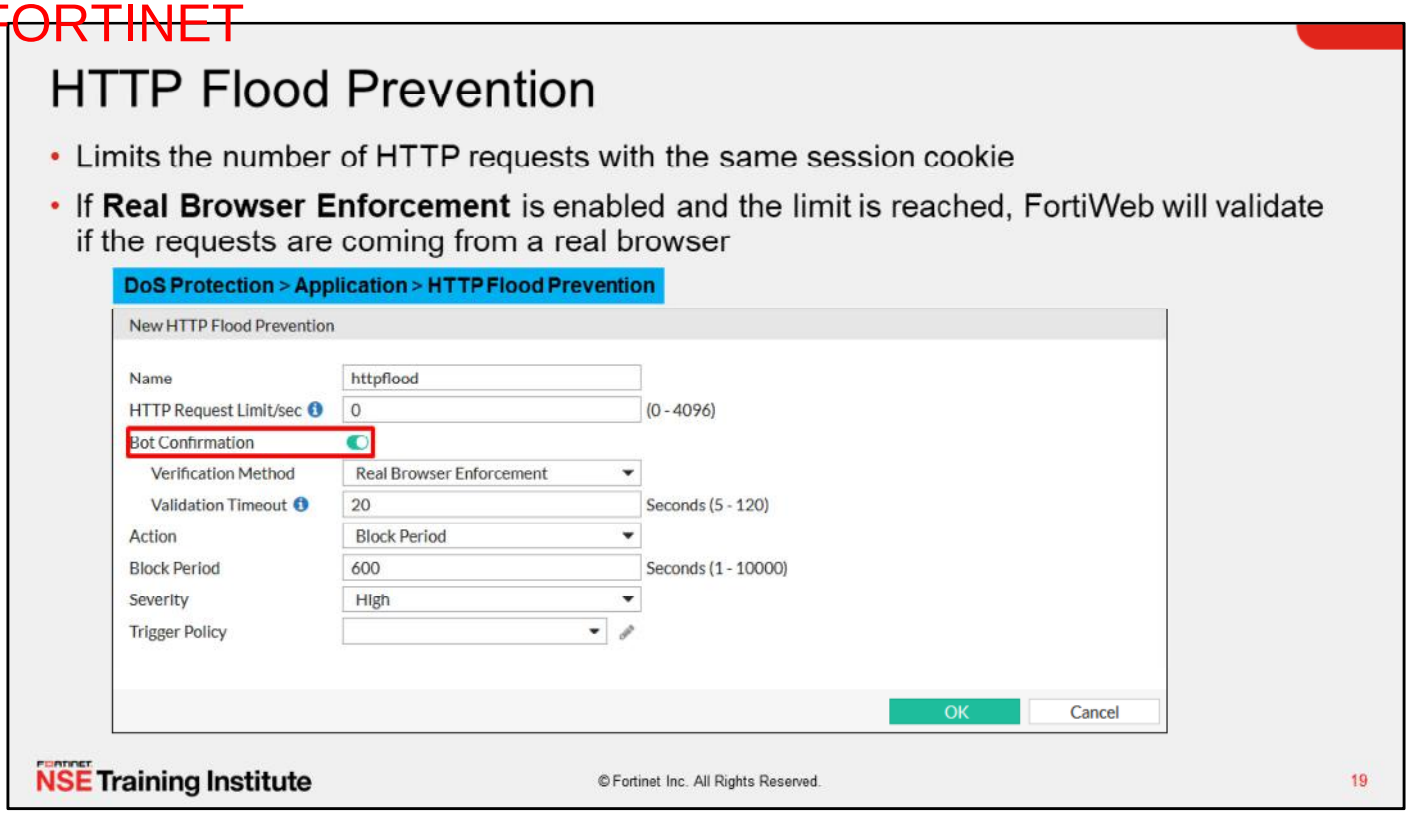


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating a thorough understanding of blended analysis, you will be able to use blended analysis techniques as part of a multilayer DDoS mitigation solution for your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



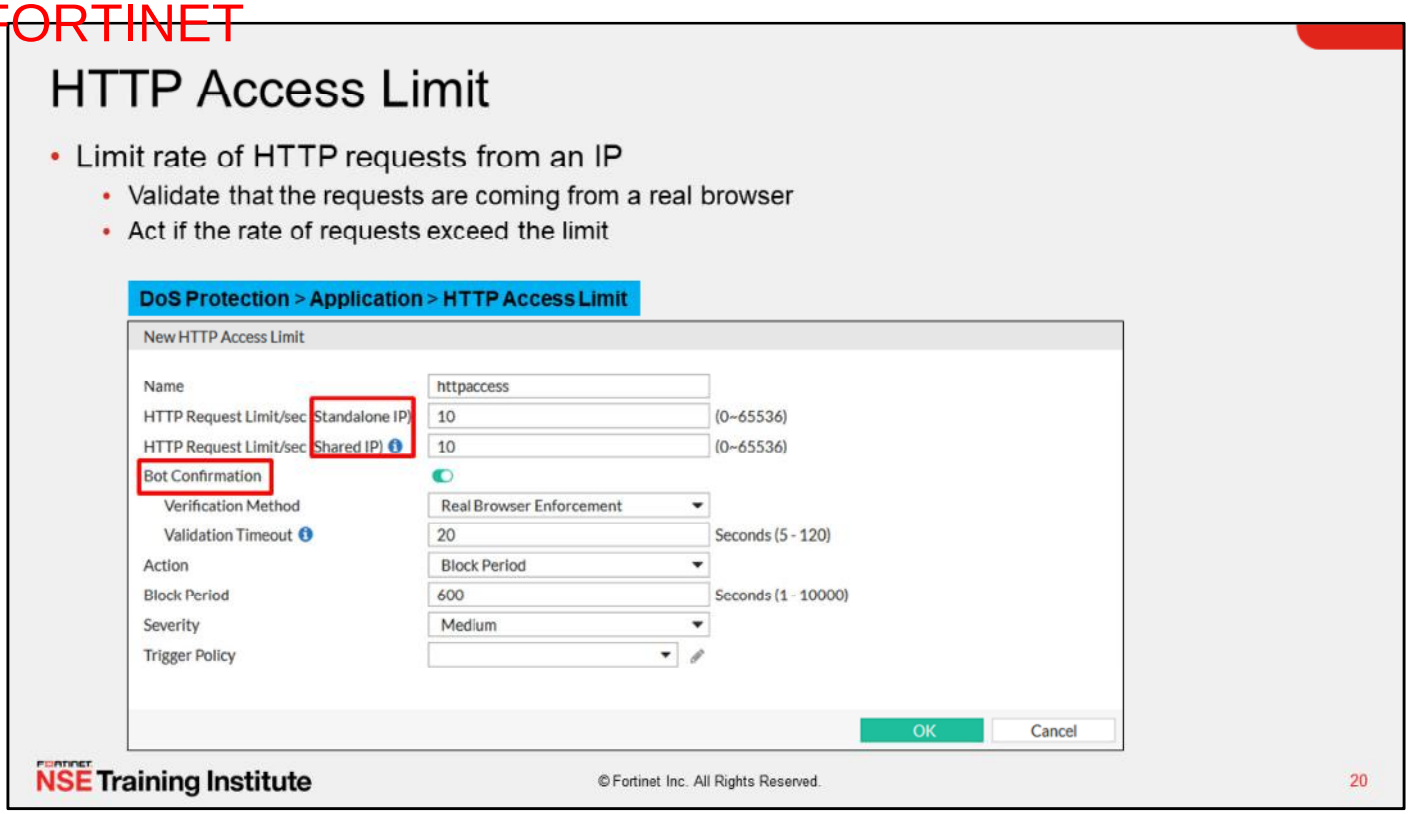
HTTP Flood Prevention also does traffic policing on HTTP requests, but it operates differently from **HTTP Access Limits**. Do you see a separate **Shared IP** rate?

No.

When enforcing **HTTP Flood Prevention**, FortiWeb injects a session cookie into the server's HTTP response. Because clients keep separate session cookie caches, if the client accepts cookies, this will uniquely identify the client. FortiWeb counts the rate of requests from that session cookie value. If the rate is too high, and you've enabled **Real Browser Enforcement**, then FortiWeb uses the real browser enforcement JavaScript to fingerprint the client and determine if it is a person's browser or a bot. If a bot is detected, FortiWeb applies the block action that you've selected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This feature is similar to HTTP Flood Prevention. However, this feature can prevent HTTP request floods that involve many different URLs and connection attempts. It also can detect source IP addresses that are shared by multiple clients, and intelligently enforce a separate request rate limit for those IPs, even if those clients or sessions do not support cookies.

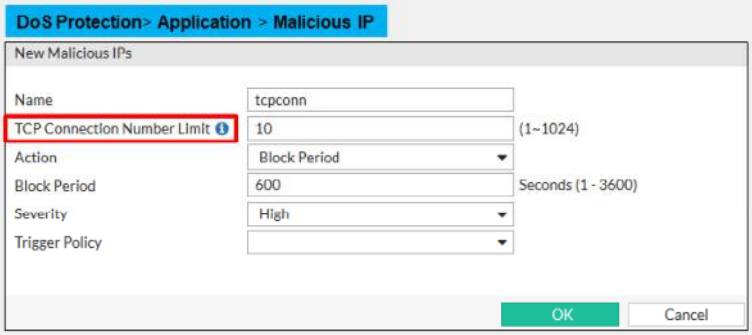
FortiWeb tracks the rate of requests from each source IP address, regardless of their HTTP method. If the rate of requests exceeds the limit, FortiWeb performs the configured action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Malicious IPs

- Limits number of simultaneous TCP connections for each unique HTTP session cookie
  - Protects from TCP socket exhaustion
- If number of connections exceeds limit, FortiWeb applies action



NSE Training Institute

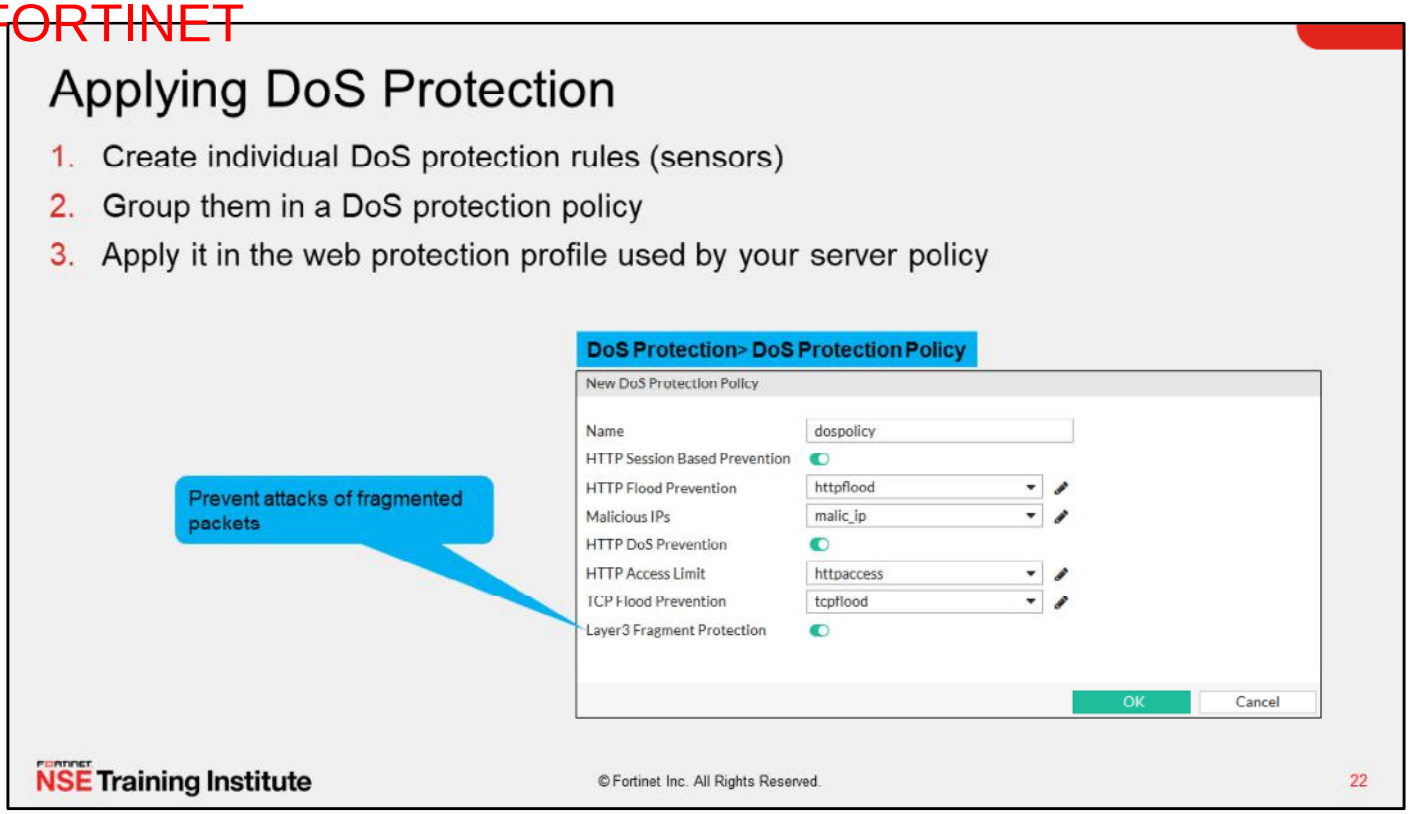
© Fortinet Inc. All Rights Reserved.

21

Malicious IPs is another DoS mitigation technique that you can use with high confidence. Although some download accelerators do use multiple connections, it's very rare that legitimate clients will open many TCP connections simultaneously. Normal browser tabs on Firefox and Chrome are not going to be the source of 1,024 simultaneous TCP connections. So, the **TCP Connection Number Limit** is a good candidate for a period block action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you have configured DoS sensors, group them together into an anti-DoS policy that specifies which sensors and policies to use. You may want to configure multiple DoS policies, tailored to the types of web apps you host. Then, select the sensors in the web protection profile used by a server policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Web App Buffers

- Limit the amount of RAM each client can use
  - When the system exhausts the specified amount of RAM, service can't respond to more clients
- Reasonable limits vary by app
  - Some apps have more variables
  - Some apps allow large uploads
- Use the FortiWeb HTTP constraints
  - Attackers can try large, slow uploads, session keepalive messages, many inputs, and so on, to find app-specific DoS

NSE Training Institute © Fortinet Inc. All Rights Reserved. 23

DoS vulnerabilities can be inherent in the design of some web protocols. You have seen the DoS sensors that involve HTTP session cookies. But your other HTTP headers, individual servlets, and web apps can have their own DoS vulnerabilities too. To prevent attackers from taking advantage of these vulnerabilities, you can use HTTP constraints to limit the HTTP protocol and app-specific input buffers to reasonable amounts on FortiWeb.

Sometimes, web app DoS vulnerabilities can be detected with FortiWeb input rules. You will learn about FortiWeb input rules in another lesson. For example, a login page should usually accept only one password input. If the application accepts many passwords, then it's possible to use that feature to create an app-specific DoS attack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Resources and Buffers

- Like your web servers, FortiWeb has system resources and buffers
- Choose a FortiWeb model with enough processing power and bandwidth. Your FortiWeb should be able to handle:
  - Your average traffic as well as traffic spikes
  - Maximum client-side and server-side connections can vary by RAM
  - FortiWeb OS allocates RAM when you enable a policy
- Buffers too large? Capacity will decrease
  - You can view the antivirus buffer size by clicking **System** > **Config** > **FortiGuard**
  - Response cache
  - Other buffers and cache configurable in CLI
- Use HTTP constraints to control how much of the FortiWeb resources each client can consume

NSE Training Institute © Fortinet Inc. All Rights Reserved. 24

You shouldn't forget your FortiWeb itself when engineering your network to be resilient to attacks. How you configure FortiWeb also affects how successful you will be.

Similar to your web apps, you should consider RAM and other sizing factors. You should also consider your settings for various scan buffers, response cache, and how FortiWeb is configured to handle them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Stronger DDoS Protection?

- Choose the right tool for the job and layer up
- If your apps are high-profile targets and mission critical, think industrial-grade DDoS protection—add a FortiDDoS:
  - Specialized hardware (ASICs) to approach line speed inspection
  - Learns your normal traffic patterns and automatically adapts
  - Defends all downstream devices, not just HTTP
- FortiWeb can block many DDoS attacks, but consider the following:
  - IP/TCP/HTTP only
  - ASICs are for bypass, cryptography, patterns, not network anomaly analysis
  - Performance depends on software and CPU—may not be powerful enough against massive DDoS attacks

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

Most DoS mitigation that FortiWeb does is software based. In other words, scanning and prevention increases CPU usage, RAM load, or both. So, if you have large or high-profile attack targets, it's a best practice to combine FortiWeb with a purpose-built hardware device like FortiDDoS. FortiDDoS is a specialist. Sophisticated anomaly analysis over time, with data aging, ensures that you can intelligently cope with massive throughput. Its specialized chips can help to keep your network working near line speed. Performance like this is simply not possible in software on a general-purpose CPU.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which other Fortinet product should you consider including in your network to enhance the DDoS functions of FortiWeb?
   A. FortiADC
   ✓ B. FortiDDoS
   C. FortiSIEM
   D. FortiWiFi

2. When sizing a FortiWeb for your network, what should you consider?
   ✓ A. Peak traffic
   B. Average traffic
   C. Number of employees

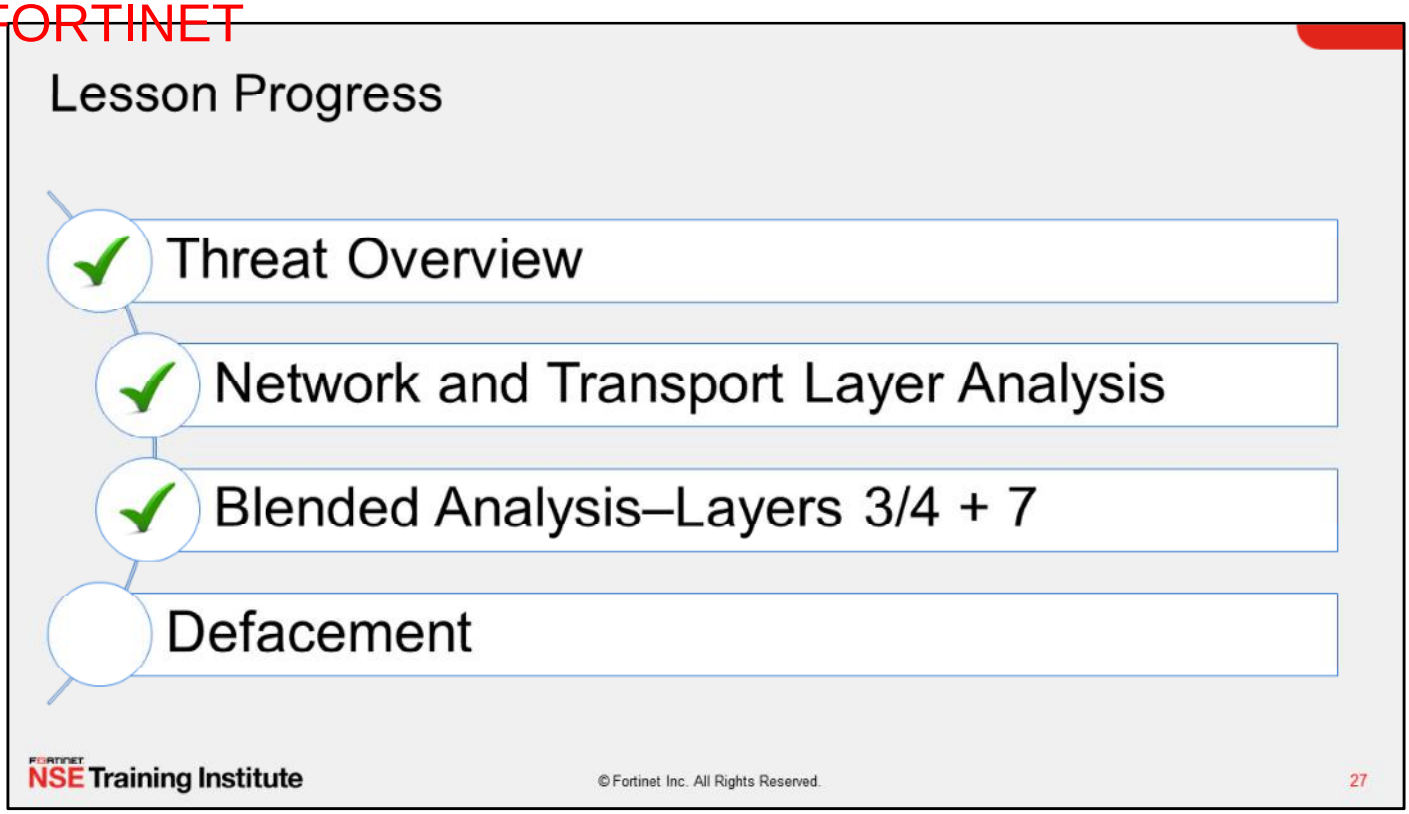
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand how to detect and prevent multilayer threats.

Now, you will learn about breaches in the network and possible recovery options offered by ForitWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating knowledge of well-known security breaches and FortiWeb anti-defacement solutions, you will be able to protect your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Anti-Defacement

- Defacement changes the website:
  - May not be for data theft, just bragging rights or humiliation
  - Hackers tag the page with their group or pseudonym
  - Reason for the attack can be jokes or inappropriate images
- Anti-defacement feature periodically checks for unauthorized changes
- If FortiWeb detects a change, it can notify you or automatically restore your website

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

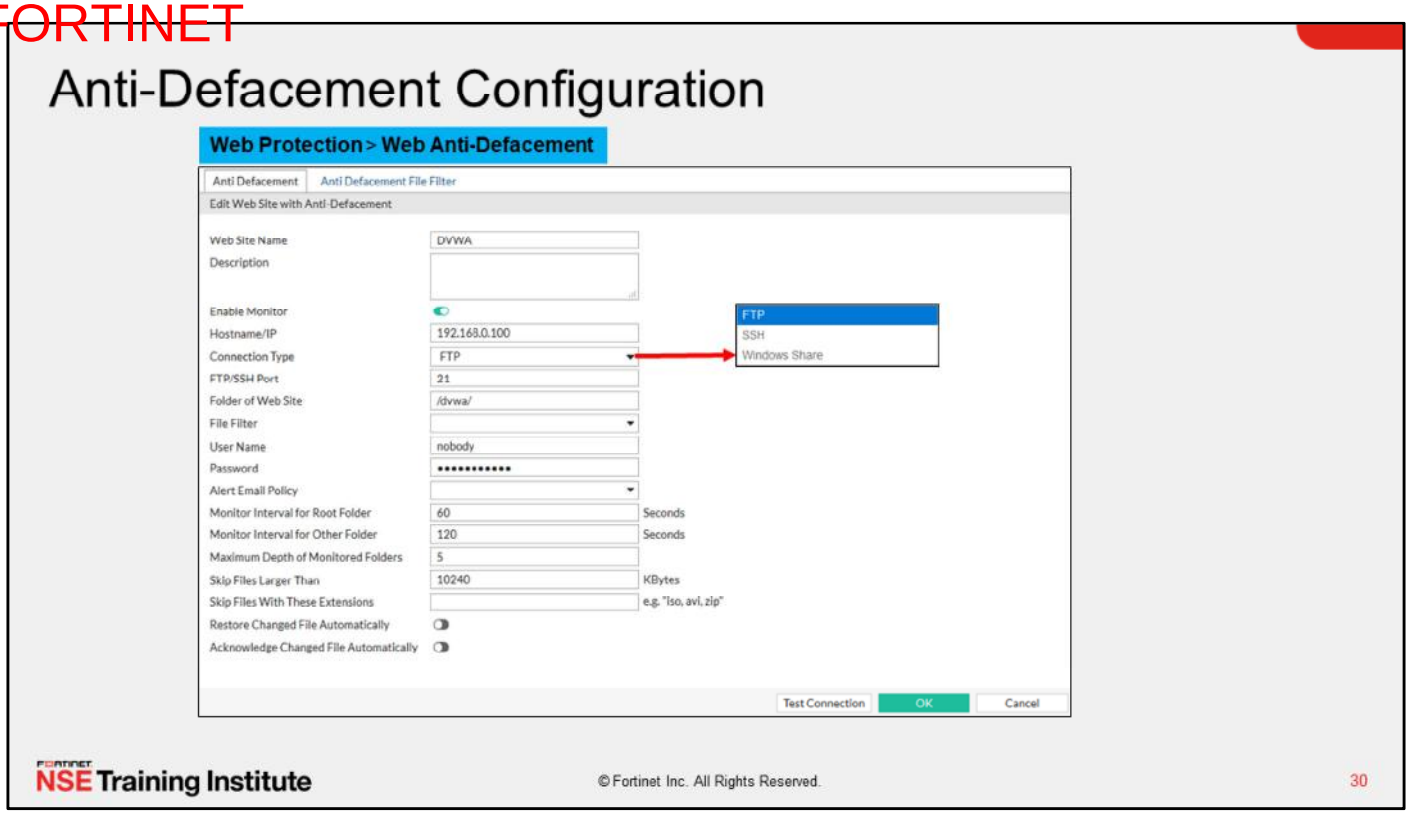
29

Not all security breaches are for extortion or stealing data. Some, like those done by LulzSec and ISIS, are just vandalism. They may spread propaganda or discredit and humiliate the target.

FortiWeb has an anti-defacement feature. It keeps hashes of files in your Apache, IIS, or other website directory. Periodically, FortiWeb connects to the server to see if the files have changed. If it detects a change, and you did not explicitly tell FortiWeb that an authorized change would occur, then FortiWeb can email you or automatically revert the files to a clean copy. This can help minimize the impact of drive-by mass defacements at hosting providers, while you work to discover and analyze the security hole.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you configure anti-defacement, FortiWeb periodically uses FTP, SSH, or the SMB/CIFS protocol to connect to your back-end web servers to look for changes to the files.

The first time it connects, FortiWeb will download copies to its own hard disk. These are the clean copies that it will restore if it detects defacement, and if you have enabled automatic restoration of your websites. Subsequently, FortiWeb will only check to see if the files on the server have changed; it won't download new files each time. So, after the first sync, anti-defacement connections are made quickly.

This is an advanced feature and needs to be enabled in the **Config > Feature Visibility** section of the user interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How Anti-Defacement Works

- FortiWeb makes backups of files (.asp, .jsp, .php, .html)
  - Not a database dump
  - Make sure you are still blocking unauthorized SQL connections
- Makes checksums of those files
- During configurable intervals, FortiWeb compares the checksum to the checksum of files on the server
- If FortiWeb detects a change, you can do one of the following:
  - Revert the file(s) to a backup revision
  - Accept the changes

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

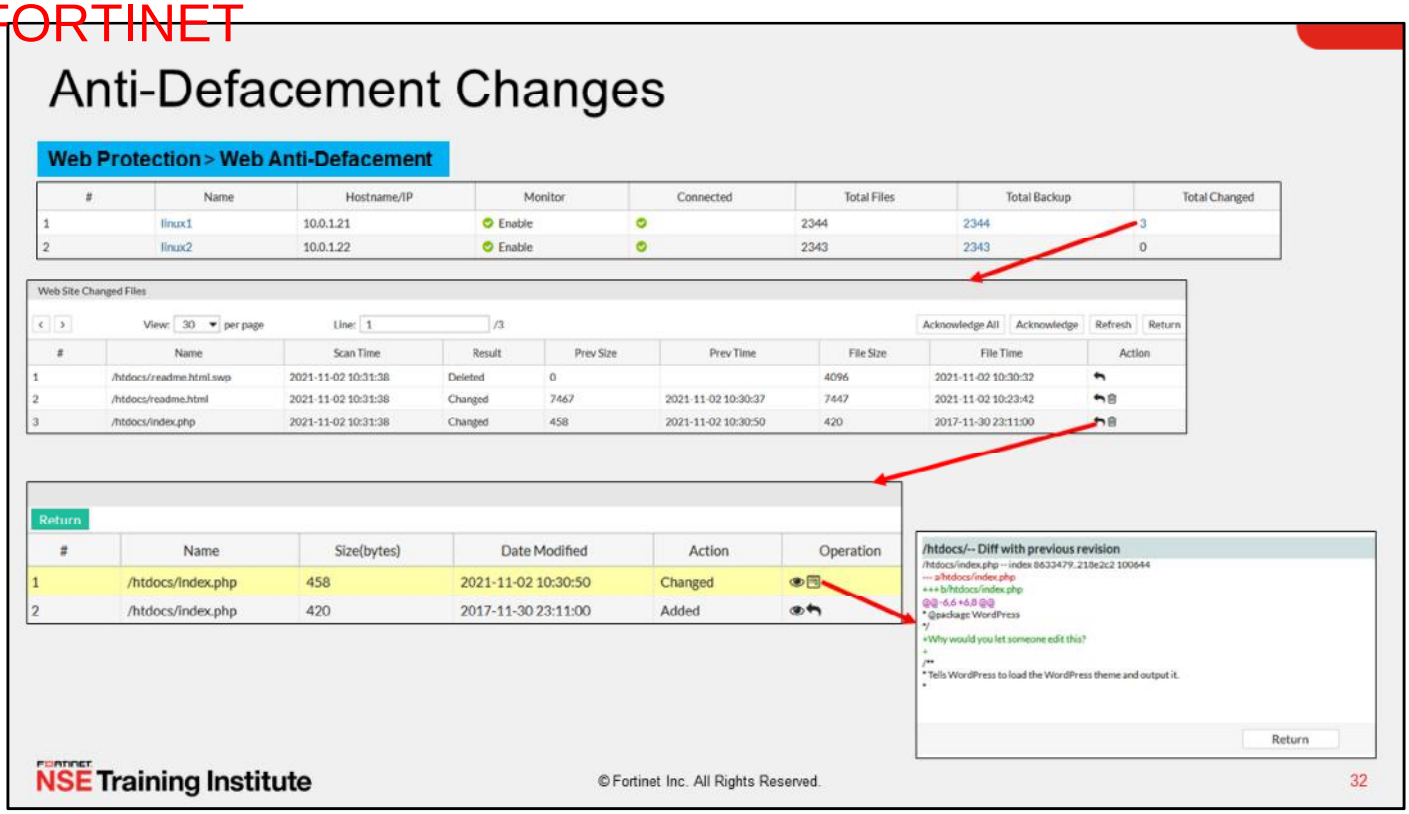
31

Since most modern websites are not static HTML files, but are templates where content is injected from a database, be aware that anti-defacement does not make a full backup copy of your backend databases but only snapshots certain files that are usually static.

Use FortiWeb to block SQL injection attacks and follow best practices. Make sure you back up your database regularly. If your database changes frequently, it can help to log transactions so that you can revert them if necessary. If your web app data is very sensitive, for example, financial information or HR databases, you should also apply database-specific controls. Database security devices such as FortiDB can help.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After Web Anti-Defacement is enabled, FortiWeb will scan and compare the websites to its hashed database. If a change is detected, it will report it on the GUI. There, administrators can review the changes, see a diff comparison, and choose to acknowledge and accept the changes or revert the file to a saved copy.

It is very important to either disable or acknowledge changes after major website updates or regular maintenance changes to make sure FortiWeb has the latest copy saved and ready for reverting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How does FortiWeb protect against defacement attacks?
   A. Keeps a complete backup of all files and the database
   ✓ B. Keeps hashes of files and periodically compares them to the server

2. Which statement is true about anti-defacement on FortiWeb?
   ✓ A. You should disable anti-defacement while updating the web app
   B. If anti-defacement detects a change, it can redirect users to a backup web server

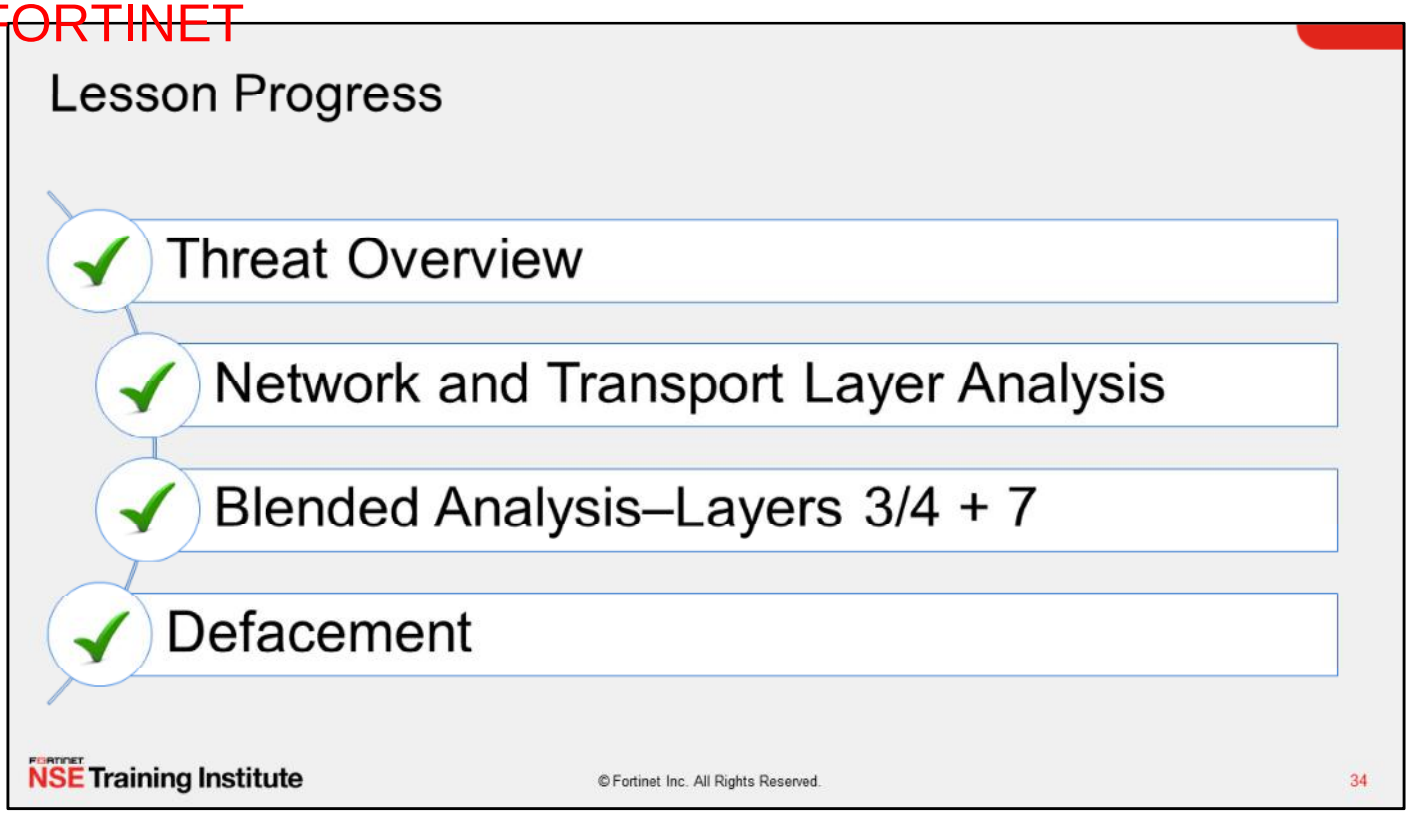
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have successfully completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Review common threats
- ✓ Describe and discuss IP layer DDoS mitigation solutions
- ✓ Describe and discuss application layer DDoS mitigation solutions
- ✓ Describe and discuss multilayer DDoS mitigation solutions
- ✓ Discuss well-known security breaches
- ✓ Discuss and describe anti-defacement solutions

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

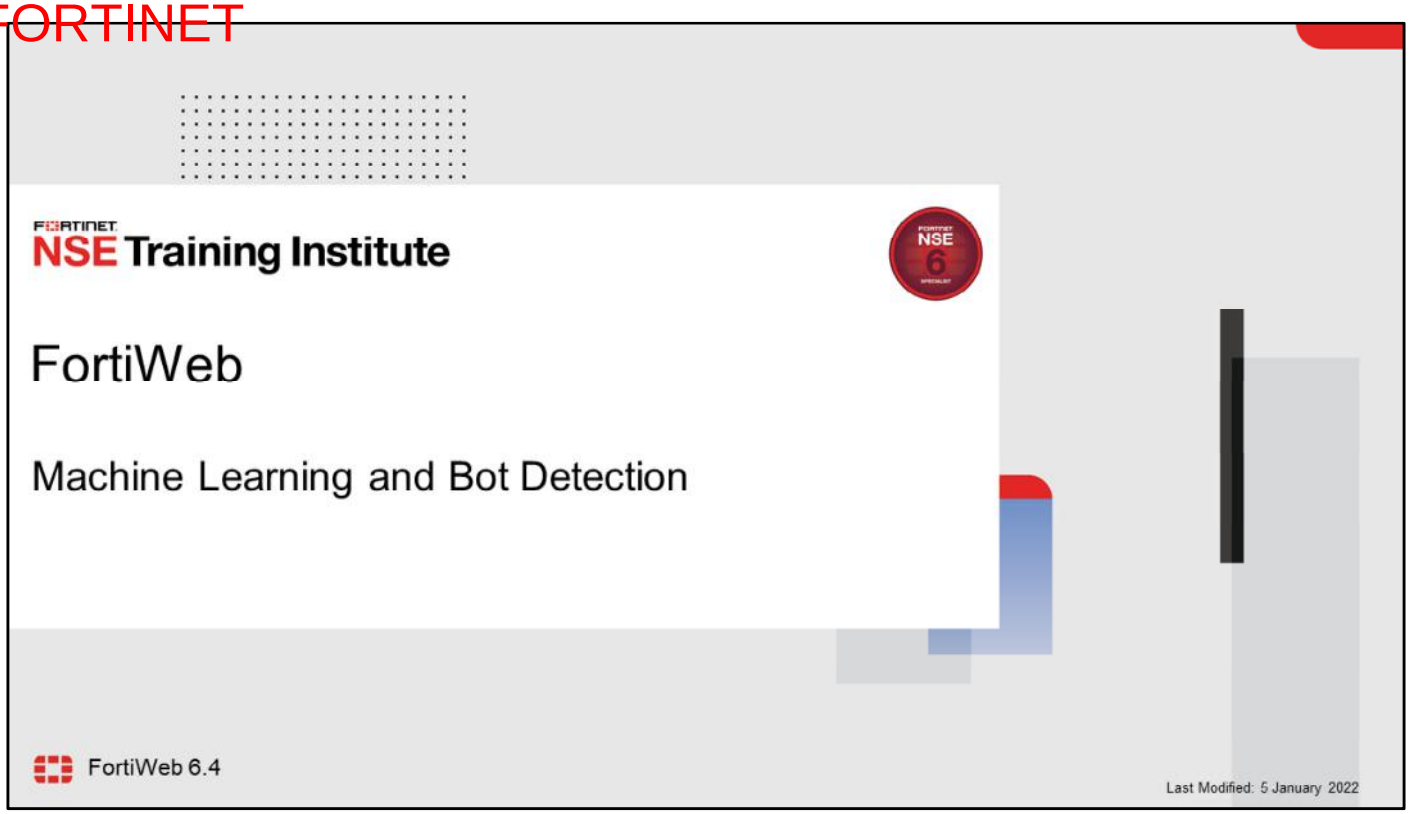
35

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how you can use FortiWeb features to mitigate DoS attacks and prevent vandalism.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the FortiWeb machine learning (ML) capability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Machine Learning Overview
- Hidden Markov Model
- Machine Learning—Anomaly Detection
- Machine Learning—Bot Detection

NSE Training Institute

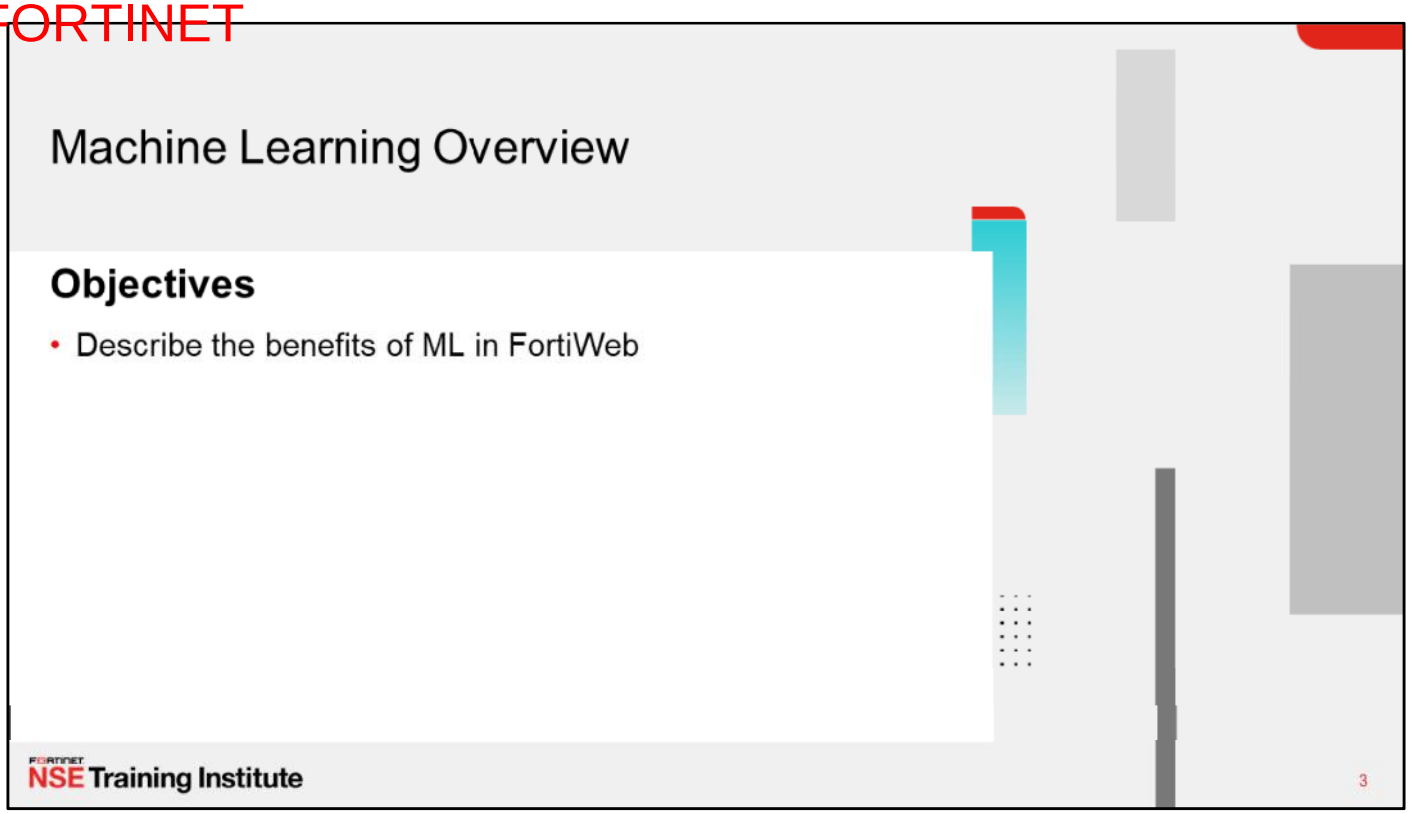
© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

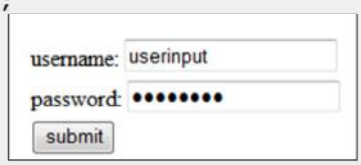
By demonstrating competence in the benefits of ML on FortiWeb, you will be able to explain why FortiWeb is the ideal solution for protecting your web applications because of its ability to use machine learning to detect anomalous behavior.

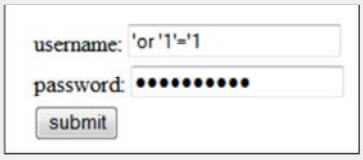
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Why Aren't Signatures Enough? SQL Injection Example

- How does SQL injection work?
- When submitting input to a web application, a query is formed from the application to the database
  - Normal login request
    `select * from user_table where username= ' userinput ' and password=' userinput ';`
- If the app doesn't perform input validation, the attacker can manipulate the input to bypass authentication
  - Injection login request
    `select * from user_table where username= ' ' or ' 1'= ' 1' and password= ' anything ';`





www.example.com/login.asp?username=xxx&password=yyy

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

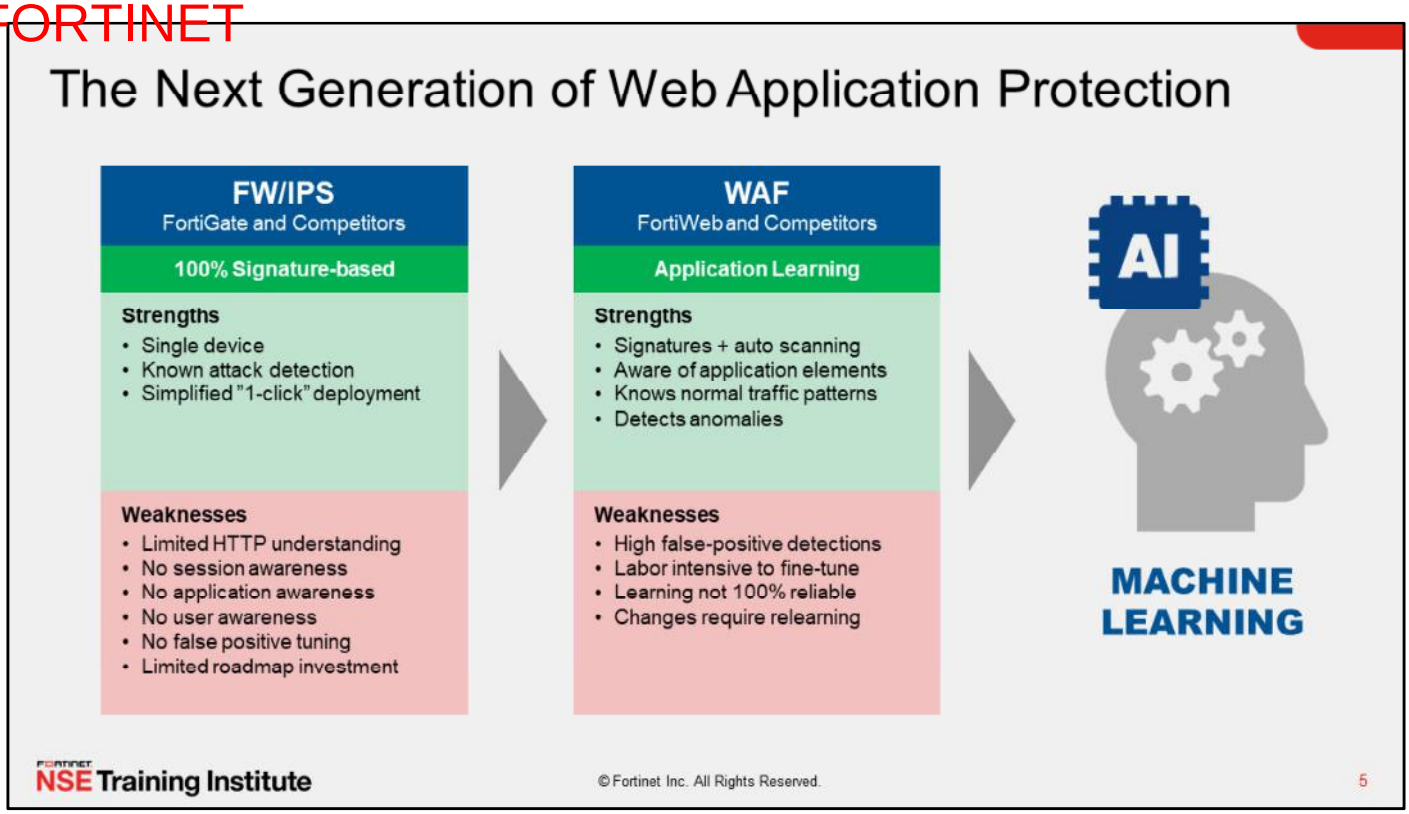
As you learned earlier, FortiWeb provides multiple layers of protection using signatures and traditional detection methods. Why is this not sufficient in some cases? Why is machine learning useful in protecting web applications?

Signatures are attack patterns that are matched against network traffic. Using regular expressions allows for covering a breadth of attack patterns, but not all. Tightening the signatures would likely trigger false positives and there would always be a possibility for signature evasion. Finally, since signatures are based on recognizing known exploits and patterns, there is no way for signatures alone to identify and prevent zero-day exploits.

There must be another layer of protection to validate character input and identify threats!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



WAFs provide many application layer protection mechanisms but, above all, they provide application learning (AL) capability. Once deployed, WAF starts learning normal user behavior, how URLs are accessed, what types of inputs are regularly used, how many characters are typed into certain fields, whether they are required parameters, and so on. By knowing this information on each parameter, WAFs can then restrict any access that doesn't adhere to what has been learned.

While AL is the most important feature of a WAF, it has limitations, primarily requiring manual intervention to review profiles before moving them into blocking mode. This can be resource intensive. Here are the main issues with application learning:

- How can you be sure that the behavior you are seeing is normal?
- What happens if, during the learning phase, only partial data is submitted?
- What happens if all character types are legally added during the learning phase (that is, characters that allow SQLi)? ML then becomes a hindrance to proper security.
- After all the learning, how do I know if a request is really an attack or not? How do you know an anomaly is really a threat, and not just a user error?
- And what happens when the app changes? How is the profile updated without blocking legitimate traffic?

Using AL requires manual review of the profile, and it cannot be relied on to work automatically. Using the FortiWeb ML capability addresses the issues and solves the challenges.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Machine Learning

- With existing application learning solution, once a parameter is learned a new request has either a yes or no answer
  - Blocking action based on answer
- ML is different
  - It's about probability
  - A new request is examined based on the probability of being an anomaly
- FortiWeb uses ML in two layers
  - Identify whether a request is an anomaly
    - Anomaly detection based on HMM processing
  - Identify whether the anomaly is an attack
    - Attack identification based on support vector machine (SVM) processing

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

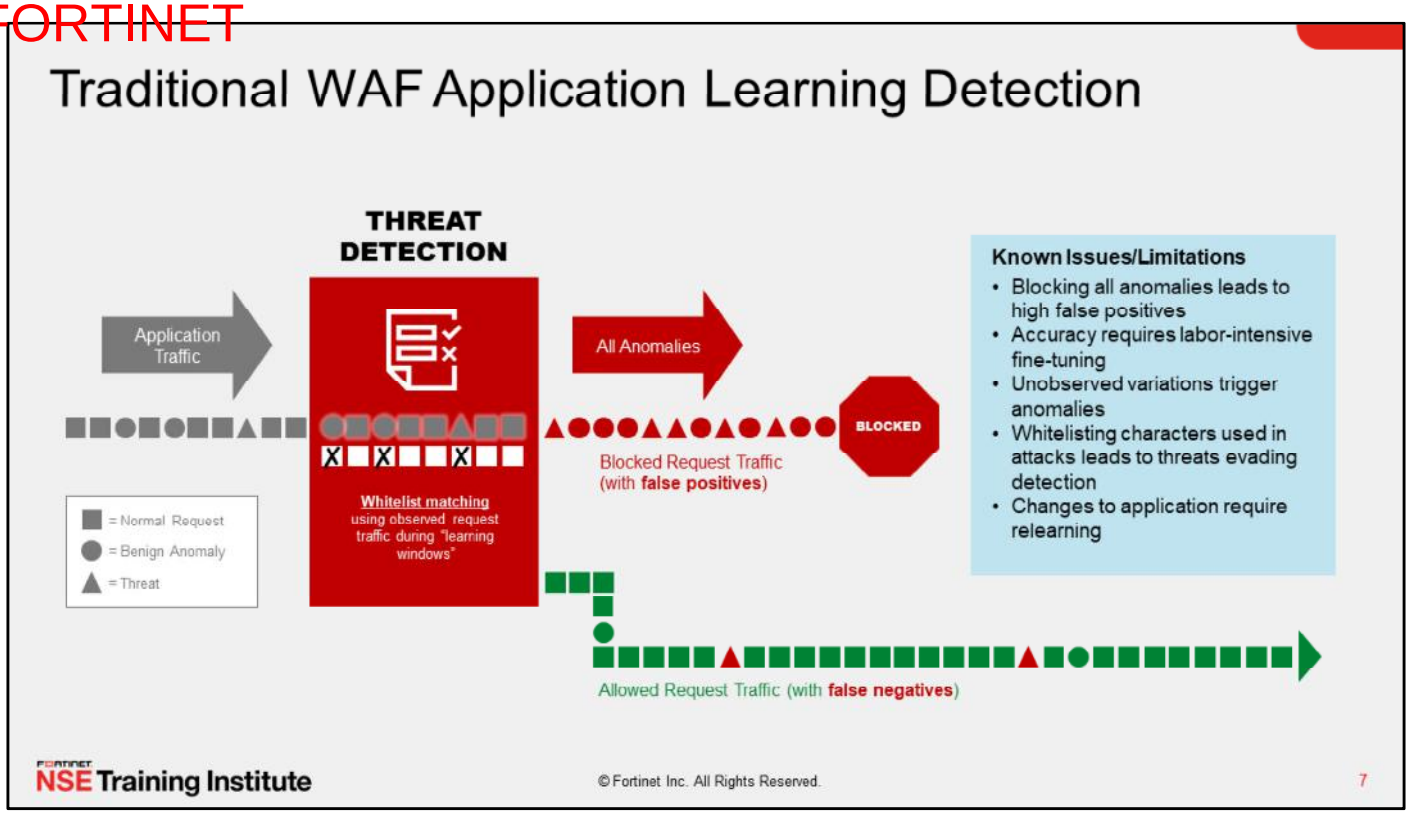
6

FortiWeb uses two ML layers. The first layer checks if the request is an anomaly, and the second layer verifies if the anomaly is an attack. This is very different from today's solutions, which immediately block upon every anomaly, causing false positives and frustration with managing WAFs. Additionally, with ML every request gets a probability value, which is different from a yes or no match to an existing learned profile.

FortiWeb currently uses probability and argument length as two learning dimensions, with the possibility of adding additional dimensions in the future.

Vouchers & Dumps are Available | WhatsApp +201224560923

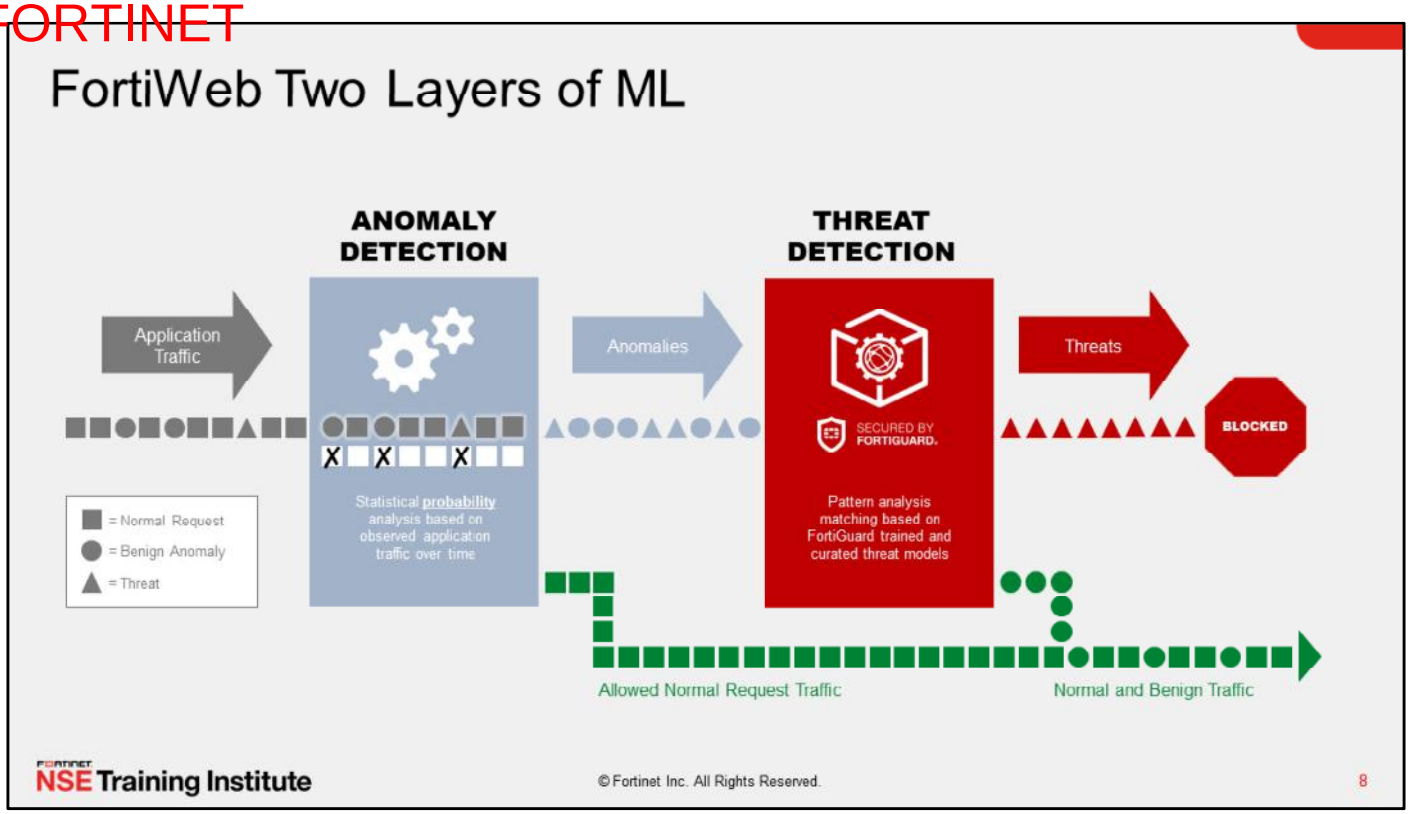
DO NOT REPRINT
© FORTINET
Brave-dumps.com



As mentioned previously, traditional WAF AL detection creates an allowlist based on observed traffic. While this method can be effective, it can often result in a high number of false-positive identifications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiWeb ML approach uses two separate layers.

The first layer is used to identify if traffic is normal, or an anomaly. If the traffic is deemed to be normal, it is allowed to continue unimpeded. If the traffic is deemed an anomaly, it is sent to the second layer of detection.

The second layer of ML is used to decide whether an anomaly detected by the first layer of machine learning is an actual attack or just a mistake entered by the user, or whether the application changed and new types of entries are legitimate.

FortiWeb is loaded with threat models, each for a different attack vector (SQLi, XSS, and so on). These threat models are based on work done by the FortiWeb engineering team, which analyzed thousands of attacks from various sources. FortiWeb arrives with prebuilt threat models that are updated periodically through the FortiGuard Security Service subscription.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Application Learning vs. Machine Learning

	Application Learning	FortiWeb Machine Learning
Methodology	Block on **profile violations**	Block anomalies that are **verified as real attacks**
Profile Building	• **Basic** • Adds traffic elements to profile • No distinction between good and dangerous character groups that are used in attacks	• **Sophisticated** • Learning done using machine learning algorithms • Different threat values for char groups
Attack Detection	Are characters in parameter allowed in profile?	What is the attack probability of the request?
Protect Mode Engagement	**Manual** depending on vendor	**Automatic**
Attack Verification	**No**	**Yes** using second ML layer
False Positives	**High** (every anomaly is blocked that doesn't fit profile)	**Limited** (Anomalies are flagged then inspected by the second ML layer for threat detection)
Tuning Requirements	**High**	**Minimal**
Application Changes	**Limited adaptability** (Legitimate traffic blocked until profile updated)	**Automatic** (Legitimate traffic not blocked because of second layer)
Advantages	• Allows reviewing profile • Easy concept to understand	• Easy to deploy and manage • No manual intervention required • Very few false positives • Addresses both false positives and false negatives

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

This table on this slide shows a comparison between the key elements of AL and ML.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Legitimate traffic that is flagged as a threat is called a:
   A. False Negative
   B. True Negative
   ✓ C. False Positive
   D. True Positive

2. Which layer of FortiWeb machine learning is responsible for confirming a threat?
   A. First layer
   ✓ B. Second layer

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Progress

- ✓ Machine Learning Overview
- Hidden Markov Model
- Machine Learning—Anomaly Detection
- Machine Learning—Bot Detection

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

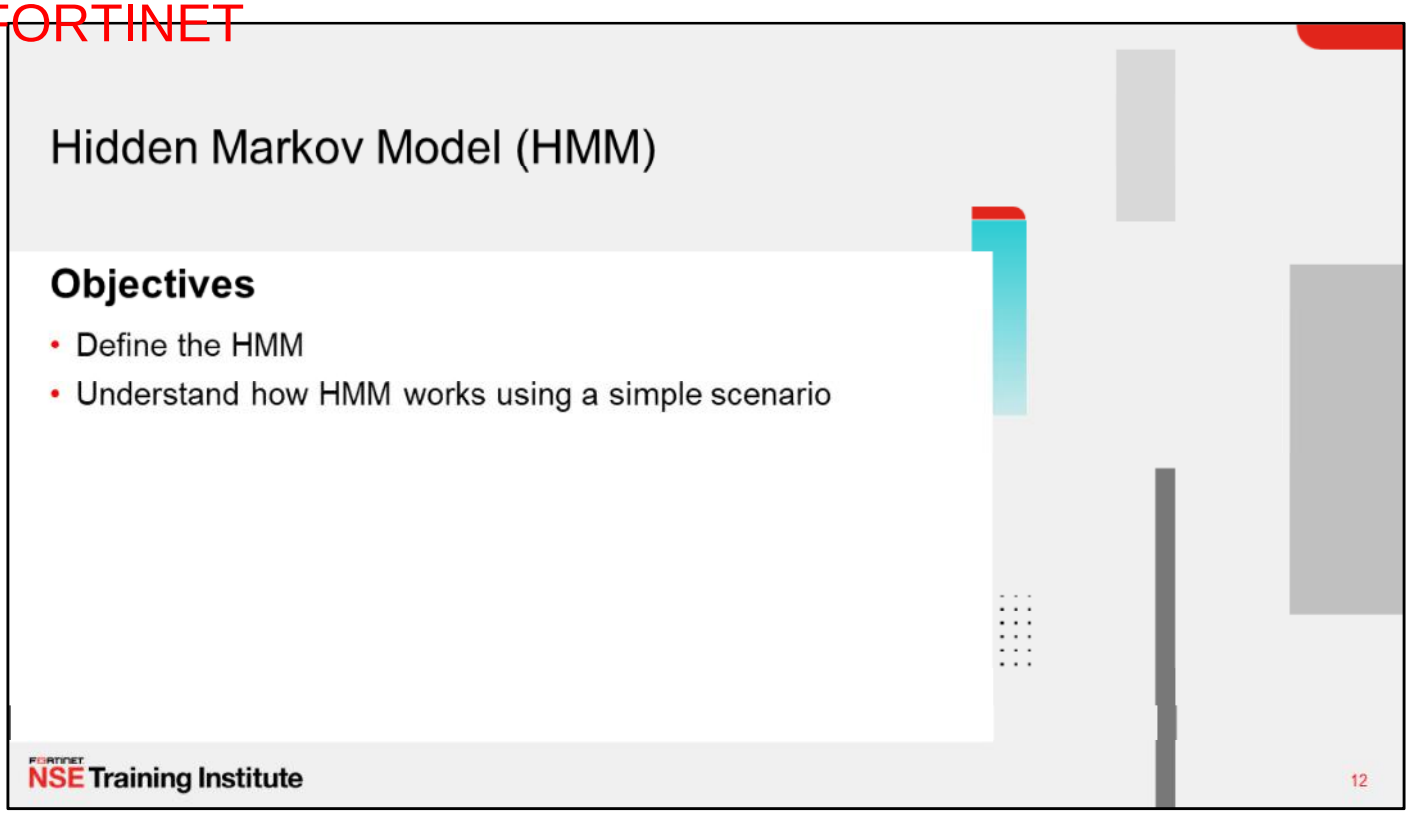
11

Good job! You now know what the key benefits of ML on FortiWeb are.

Now, you will learn about the Hidden Markov model (HMM), which is one of the core elements of the FortiWeb ML capability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the HMM, you will be able to better explain the basic concepts of one of the main mechanisms of ML.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HMM

- ML is based on probability models
- HMMs are the primary probability models used
- Allows us to compute the joint probability of a set of hidden states given a set of observed states

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

In general, ML is based on probabilities. Based on the last received data, what is the probability that the next piece will be an anomaly? The best known, and most commonly used probability models in ML are Hidden Markov Models, or HMMs.

An HMM is a statistical model that allows us to predict a sequence of unknown (hidden) variables from a set of observed variables. The reason it is called a Hidden Markov Model is because we are constructing an inference model based on the assumptions of a Markov process. The Markov process assumption is simply that the future is independent of the past given the present. In other words, assuming we know our present state, we do not need any other historical information to predict the future state.

HMMs allow us to compute the joint probability of a set of hidden states given a set of observed states. The hidden states are also referred to as latent states. Once we know the joint probability of a sequence of hidden states, we determine the best possible sequence, that is, the sequence with the highest probability, and choose that sequence as the best sequence of hidden states.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HMM (Contd)

- The term *states* is used to refer to the hidden states and *observations* is used to refer to the observed states
  - **Transition data**—the probability of transitioning to a new state conditioned on a present state
  - **Emission data**—the probability of transitioning to an observed state conditioned on a hidden state
  - **Initial state information**—the initial probability of transitioning to a hidden state

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

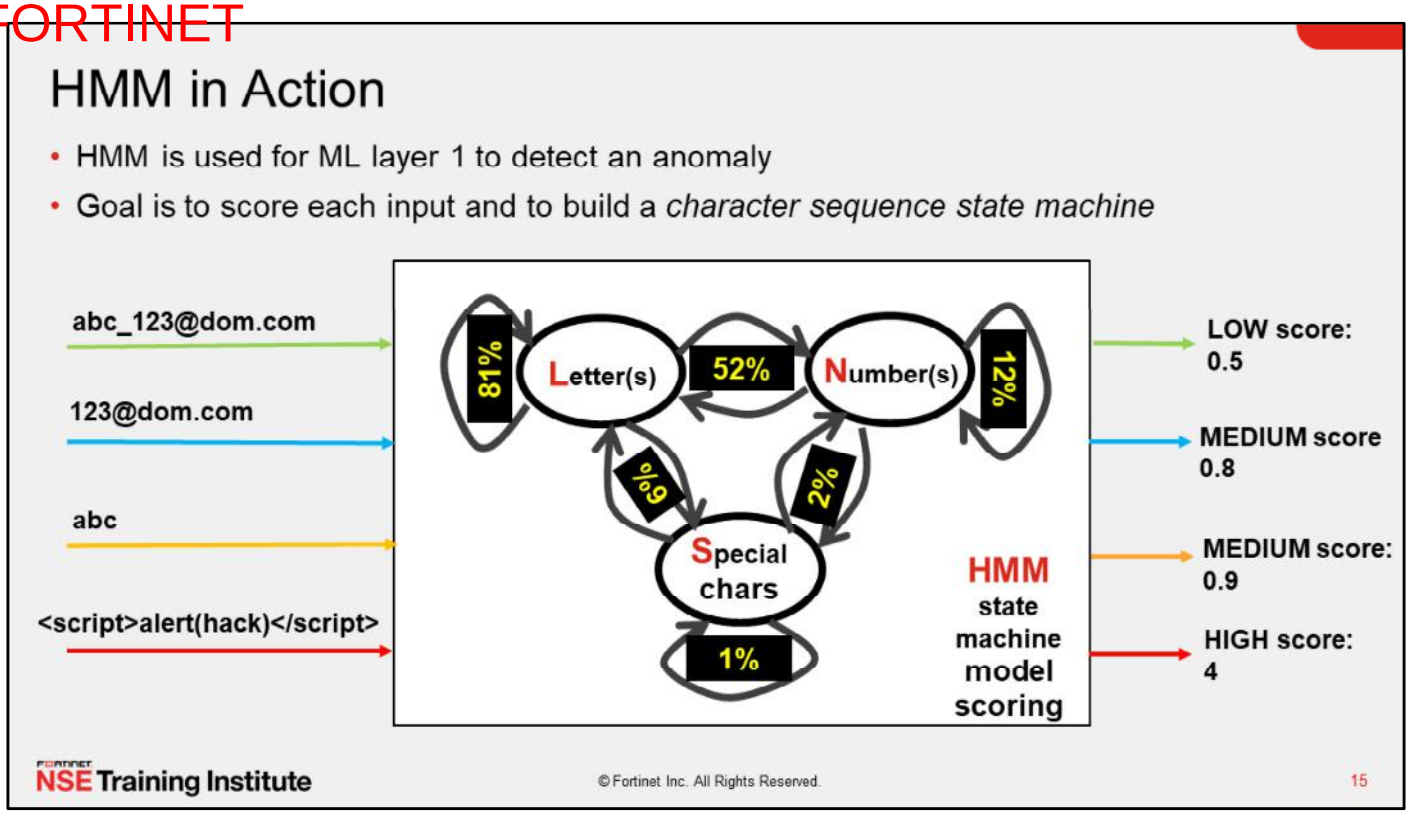
The key idea with HMM is that one or more observations allow us to make an inference about a sequence of hidden states. In order to compute the joint probability of a sequence of hidden states, we must assemble three types of information.

Generally, the term *states* refers to the hidden states, and *observations* refers to the observed states:

- Transition data—the probability of transitioning to a new state conditioned on a present state
- Emission data—the probability of transitioning to an observed state conditioned on a hidden state
- Initial state information—the initial probability of transitioning to a hidden state. This can also be looked at as the prior probability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



First layer of machine learning uses HMM and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method. Once completed, it verifies every request against the model to determine whether it is an anomaly or not.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What does the HMM allow us to do?
   A. Hide complexity of machine learning from external users
   ✓ B. Predict a sequence of unknown variables from a set of observed variables

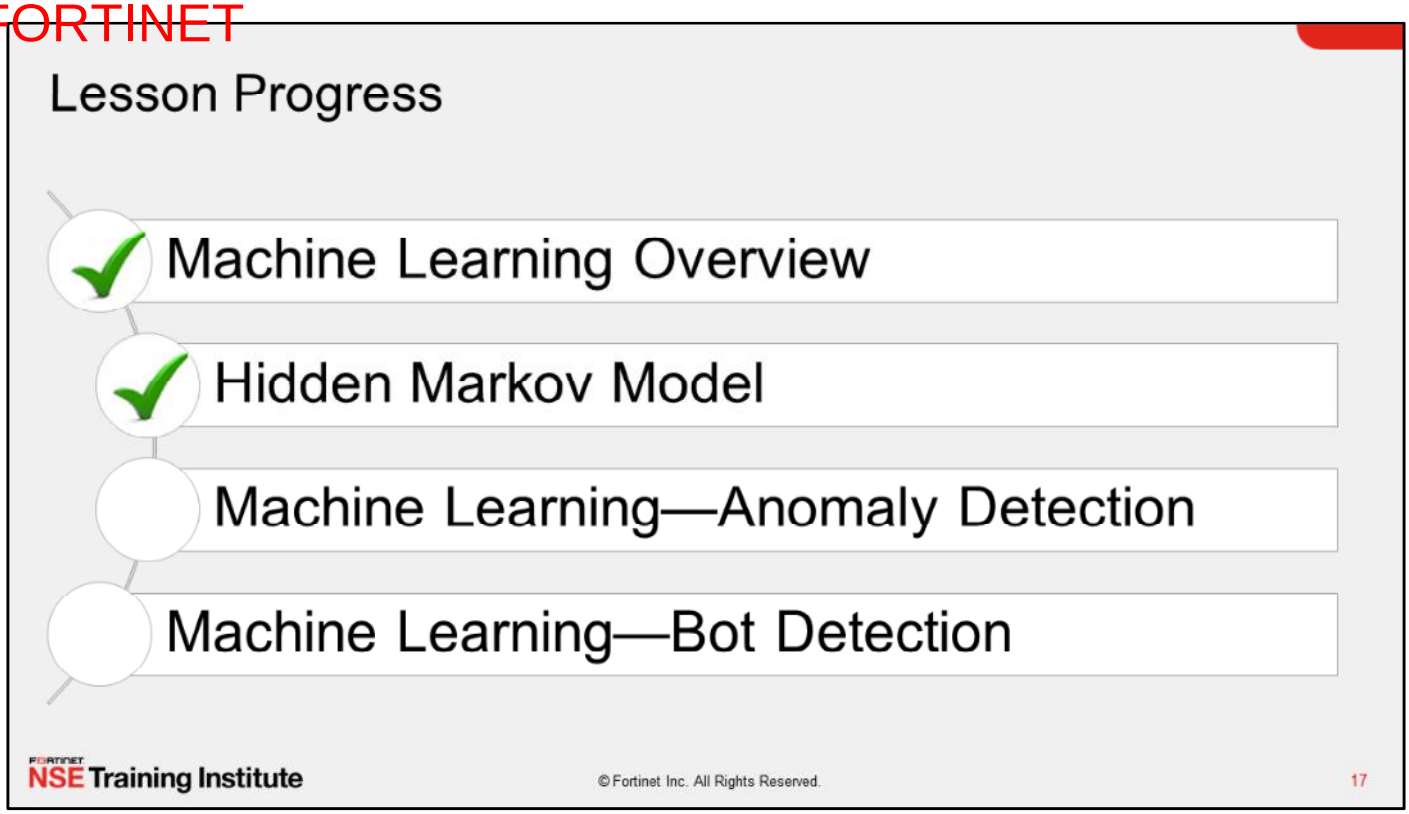
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

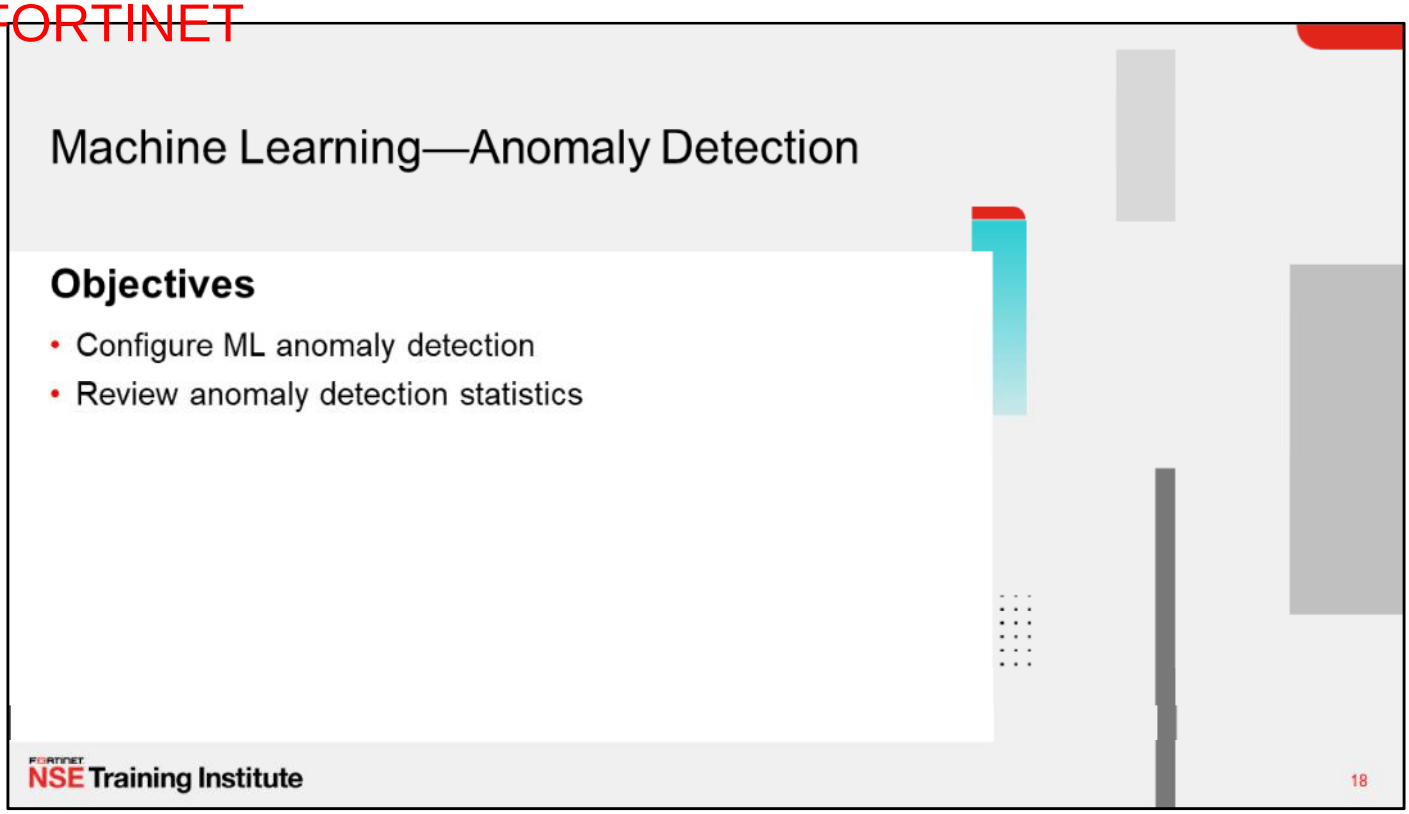


Good job! You now know about the HMM, which is one of the core elements of the FortiWeb ML capability.

Now, you will learn how to configure the FortiWeb ML anomaly detection feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

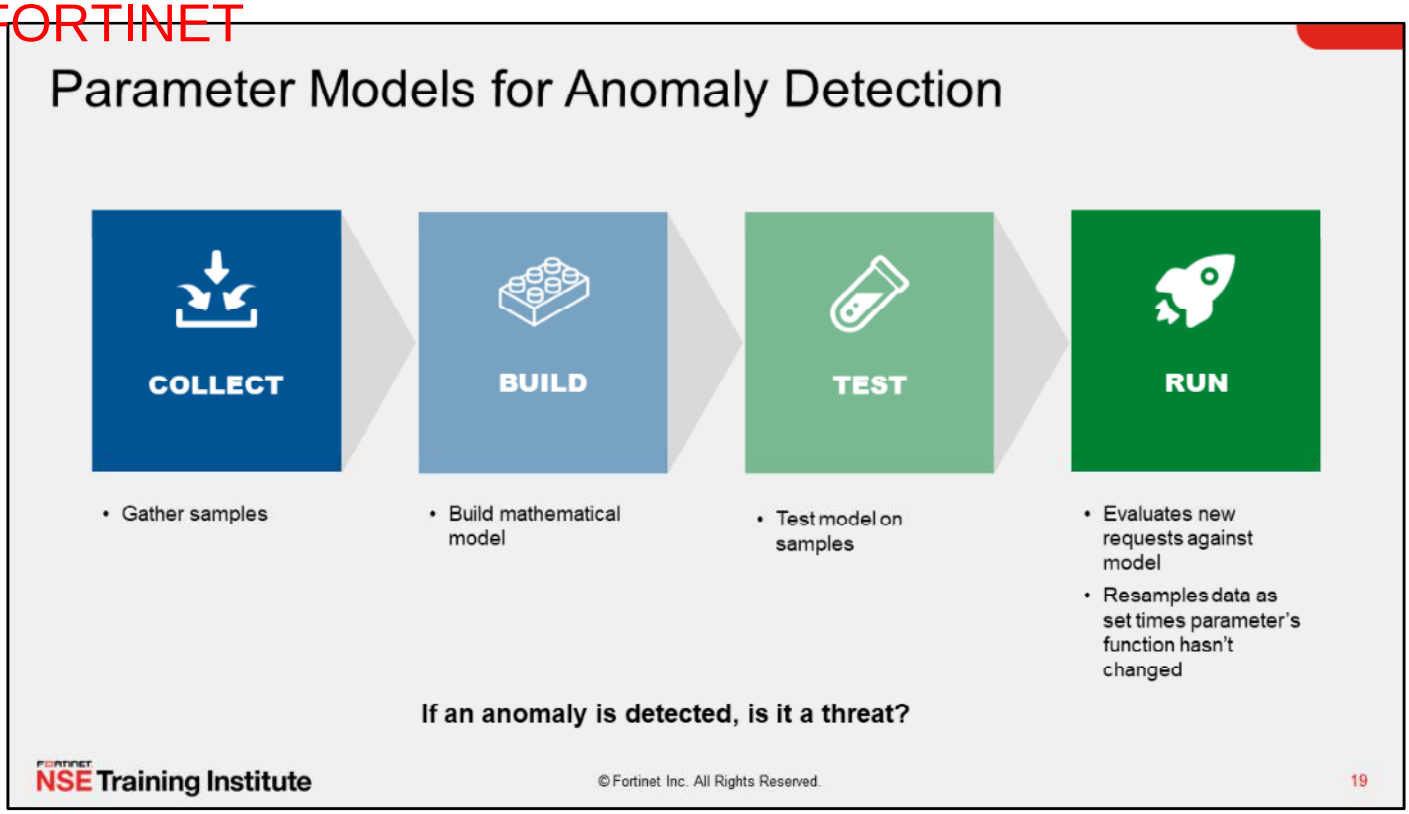


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring ML anomaly detection, you will be able to ensure FortiWeb is offering the highest and most efficient levels of threat detection possible.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how the first layer of ML anomaly detection on FortiWeb works.

First is the collect process. FortiWeb examines up to a maximum of 2500 request parameters in **Extended** mode, stopping if it observes an obvious pattern. If it is configured for **Normal** mode, then the number of samples required is 400.

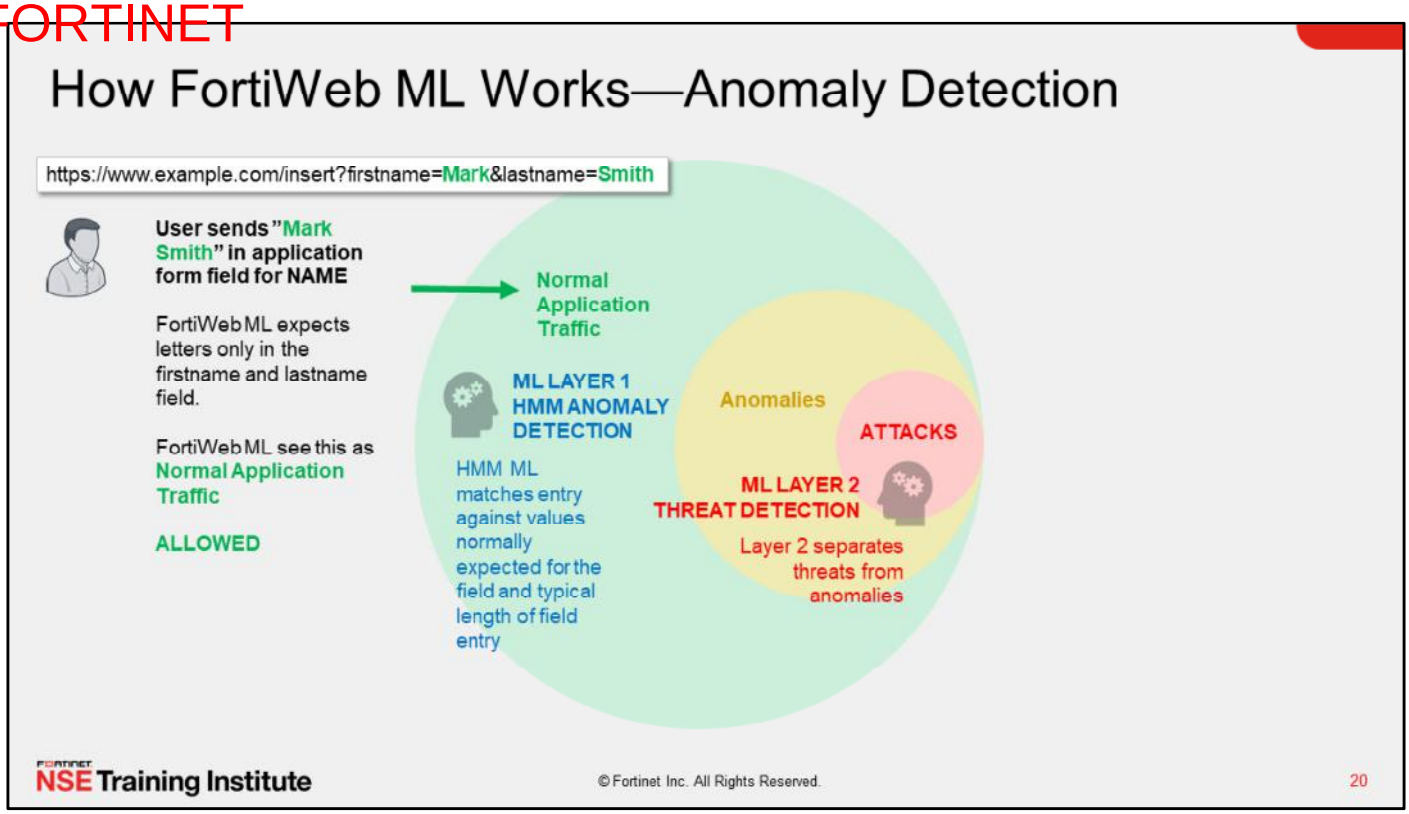
After all the samples are collected, FortiWeb builds the mathematical model for the parameter. A parameter usually corresponds to a specific page or URL.

After building, FortiWeb tests the model against new requests to ensure it is valid and correct.

And finally, the model goes to running mode. In this phase, the mathematical model for the parameter is already built and tested. Every request is evaluated, and anomalies move to the second ML layer (threat detection). Additionally, in this phase FortiWeb uses a sophisticated mechanism to identify whether a parameter has changed. You will learn about this on the next slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

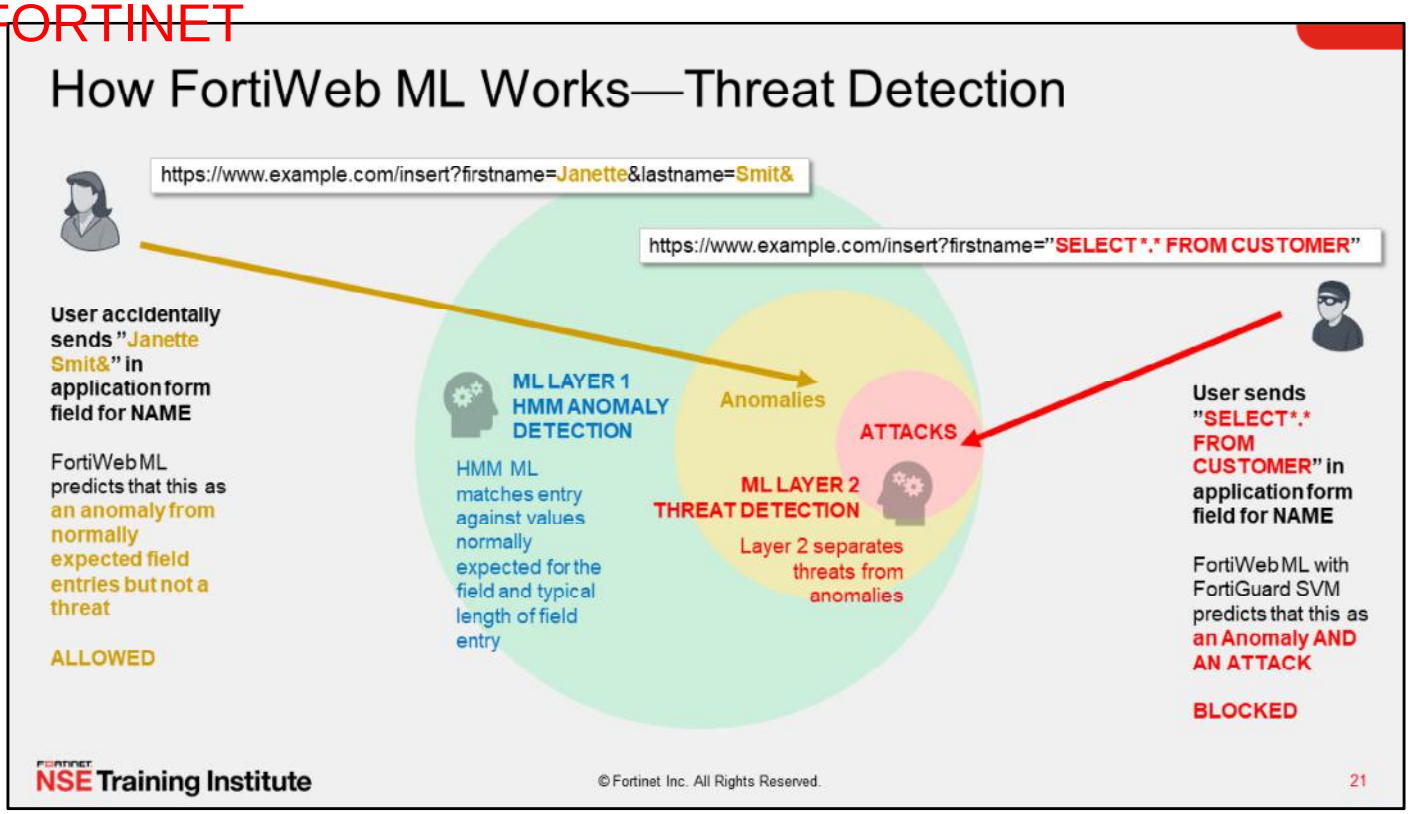


This slide shows a simplified example of a basic client experience:

1. User Mark enters his first and last name correctly in the form field. These entries are inserted in the URL parameters and adhere to the ML profile FortiWeb built. No anomaly is detected and the user is allowed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows two examples of traffic that are flagged as anomalies from normal traffic and are passed on to second ML layer:

1. User Janette mistakenly enters the character '&' which triggers an anomaly by the first layer ML, however, the second layer ML checks it against the threat models and verifies it's not a threat. Note that with existing WAF solutions with standard application learning this would trigger an anomaly that would be blocked, causing a false positive, but with FortiWeb ML the legitimate request passes through.
2. An attacker injects SQL code into a parameter. The first layer ML identifies it as an anomaly and the second layer ML identifies it as an attack and it is blocked.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Detecting Application Changes

- Web applications are not static and change frequently
- New URLs and parameters are added and existing parameters provide new functions
- FortiWeb monitors for these changes
- It samples data for existing parameters and validates if the mathematical model needs updating
- FortiWeb uses anomaly distribution to determine if applications have changed
- FortiWeb updates deviations only after 500 inputs
  - Static number, cannot be changed

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

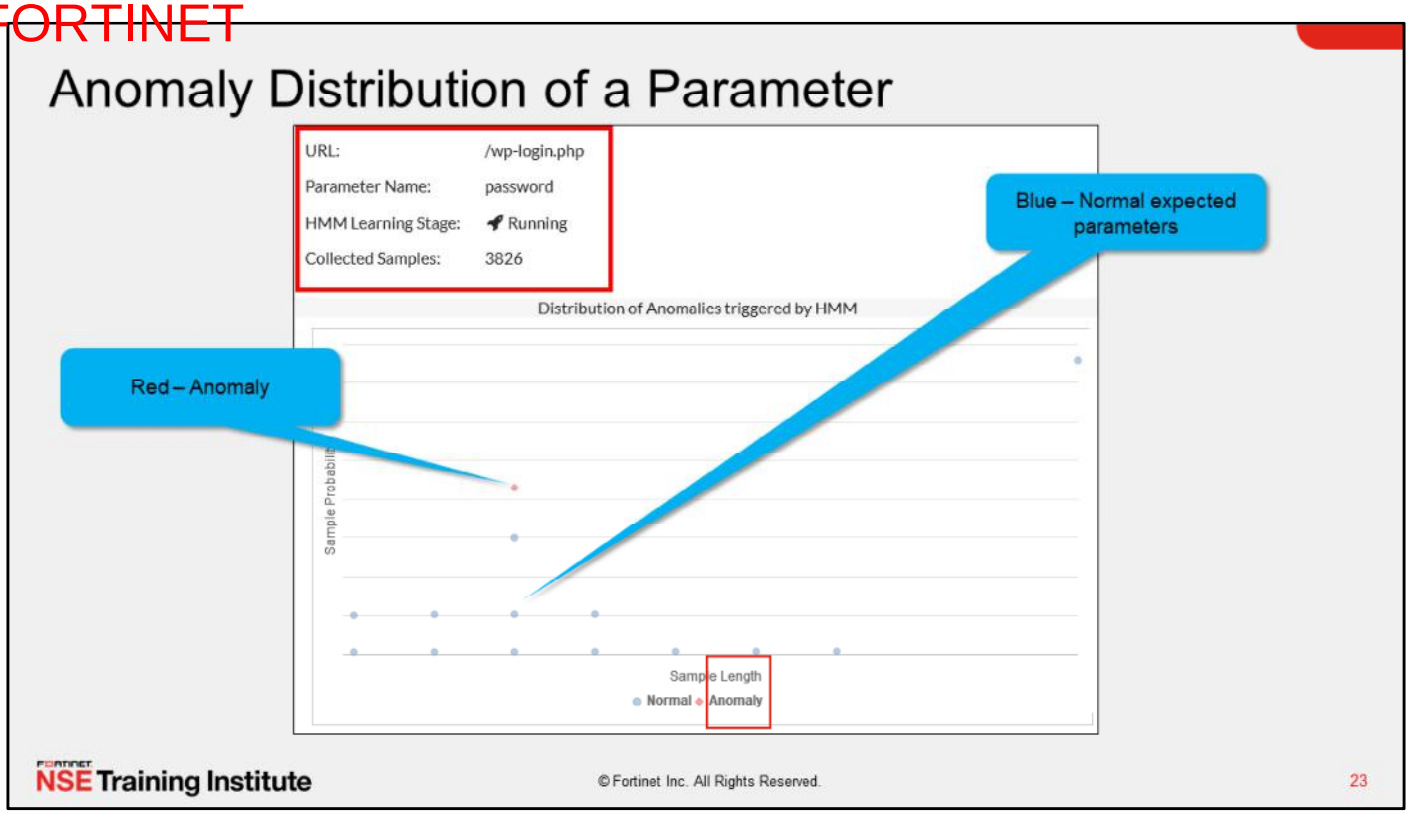
22

Web applications tend to change frequently as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different than what FortiWeb originally observed during the collection phase. In this case, FortiWeb needs to relearn the parameter and then update the mathematical model for it.

FortiWeb uses an anomaly distribution model to determine that the functions of the parameter have changed. Deviation calculation will happen only after 500 inputs. This is a static number and is nonconfigurable.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

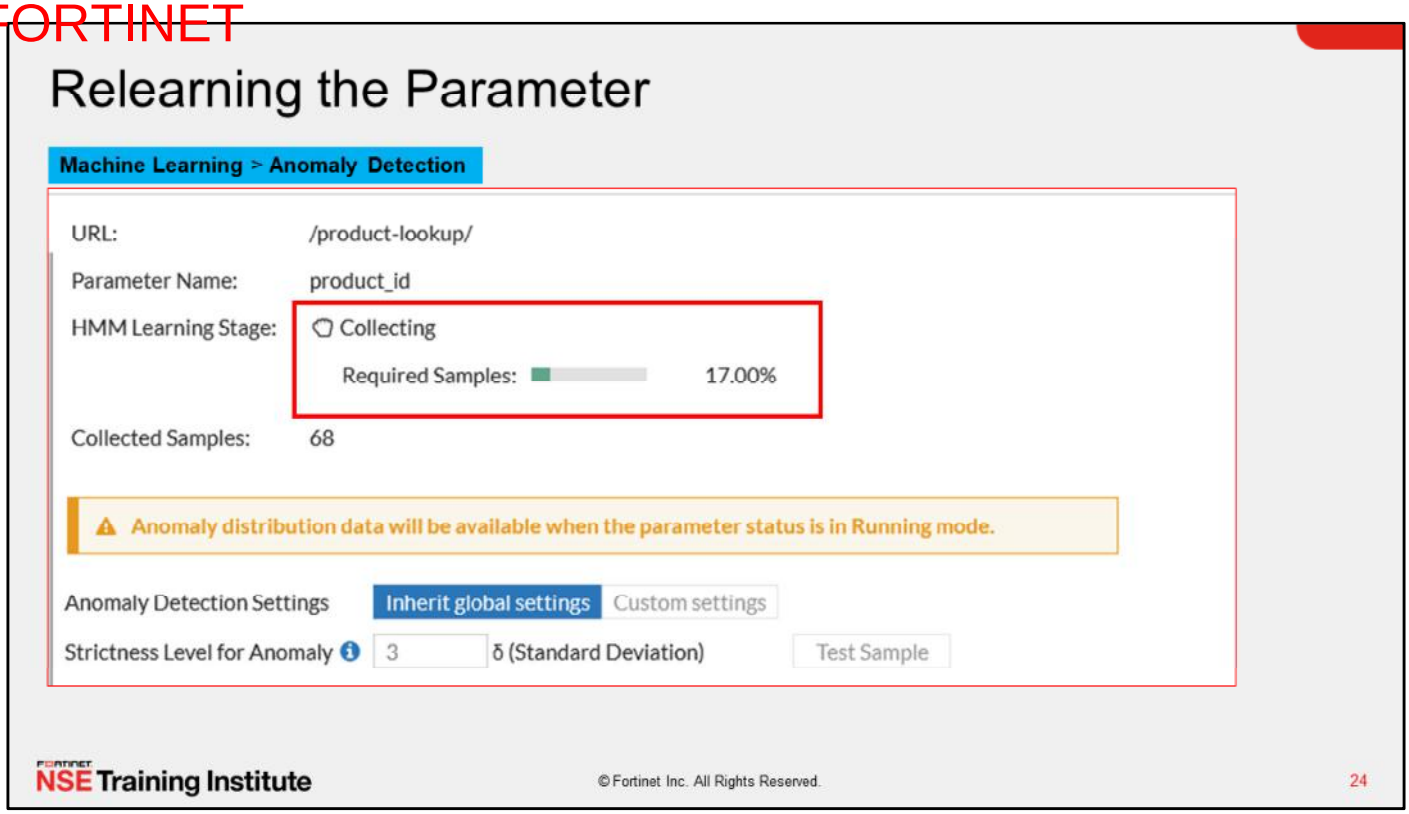


FortiWeb compares previous anomaly plots to newly created ones to see if the parameter has changed and, therefore, if the HMM mathematical model needs to be updated.

This slide shows an example of the anomaly diagram. The acceptable values are in blue and anomalies are in red. When new inputs arrive, and a new anomaly plot is generated, the system regenerates this chart and updates the values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



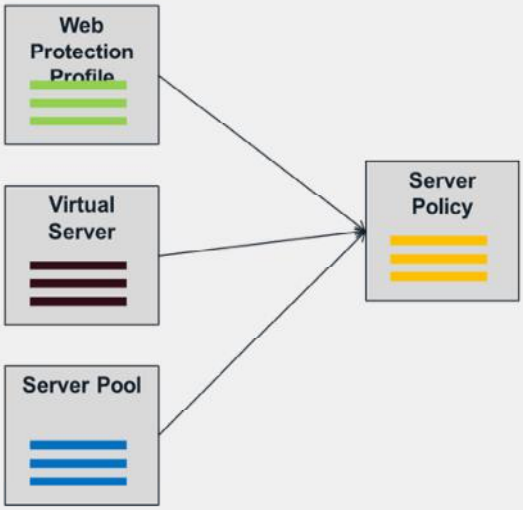
Continuing from the previous slide, you can see that the mathematical learning model for the **product_id** parameter is being rebuilt.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Policy (Reverse Proxy Mode)

- Policy applied to the traffic to protected web applications
- Virtual server defines network interfaces that HTTP/S requests are destined for
- Server pool consists of web application servers that FortiWeb directs requests to
- ML policy is part of the server policy
- ML is supported in reverse proxy and true transparent proxy mode



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

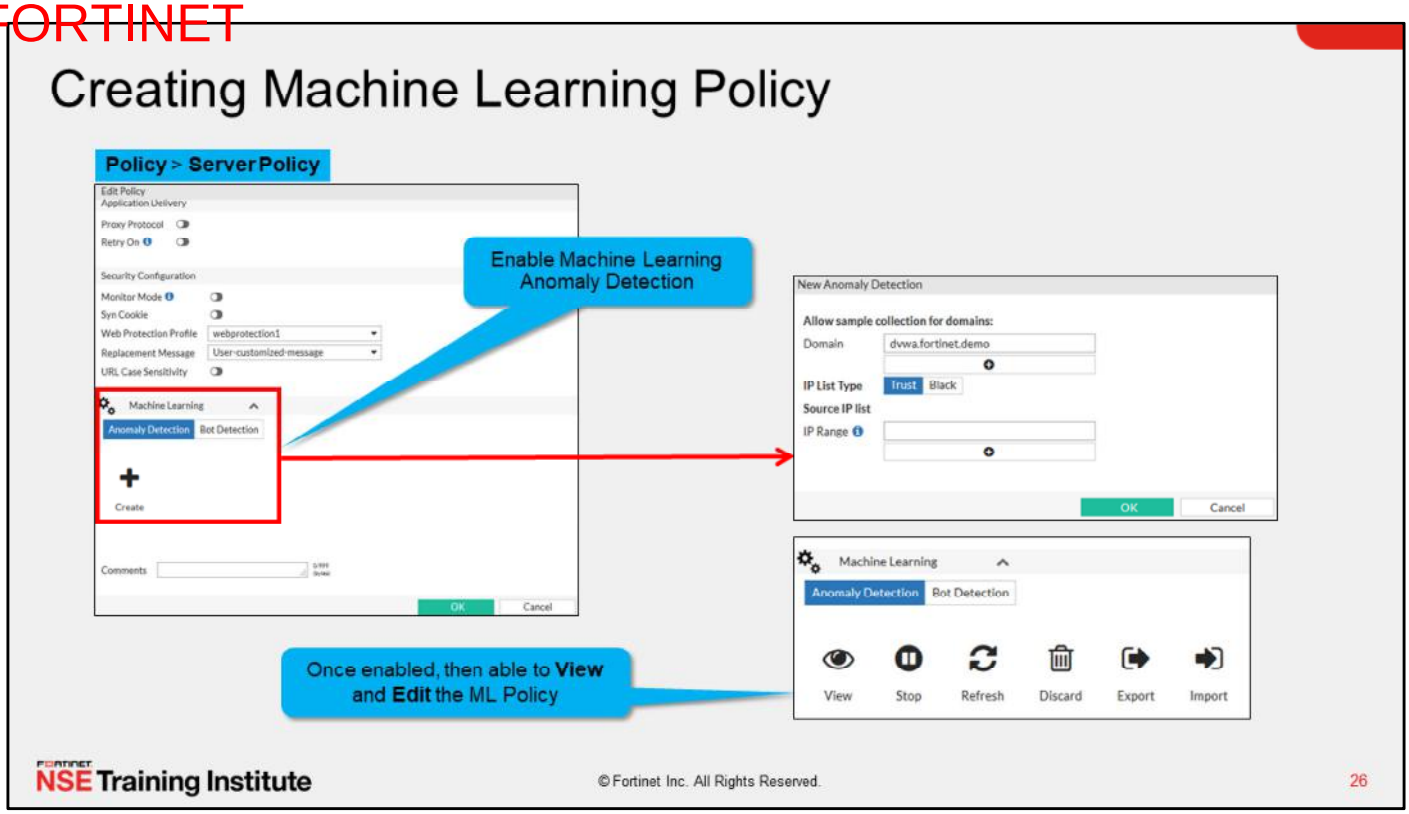
25

To enable ML, at a minimum you must define a server policy, which requires the administrator to define the two server objects: a virtual server and a server pool. While an administrator technically does not have to create a web protection profile, it is through this profile the signatures can be applied to monitor traffic. Although not required when using ML, signatures easily eliminate known attack types before they get to the ML layers. This both reduces strain on system resources and yields cleaner application parameter profiles.

ML is currently only supported in reverse proxy and true transparent proxy modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

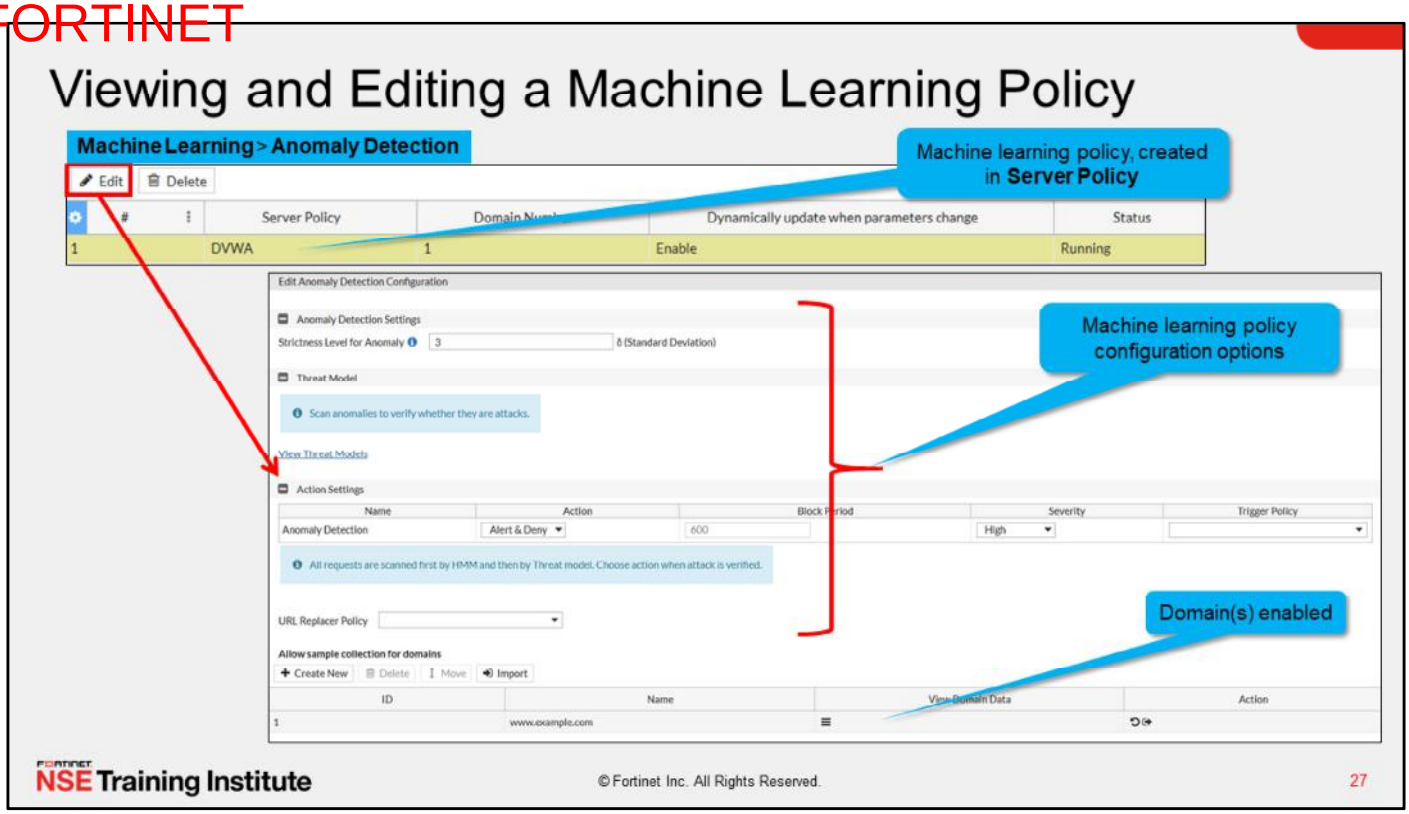


To create an ML policy, click **Policy** > **Server Policy**, and then select **Create New** > **Create HTTP Policy**. This opens the **New Policy** page. After configuring the basic options for the new policy, scroll down to the **Machine Learning** section at the bottom of the page, and then click **Create**.

The **New Machine Learning** dialog opens. Click the **+** (pluss) sign to add the desired domains and IP addresses. Click **Create** to enable ML. Once enabled, the **Machine Learning** section shows six control buttons, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



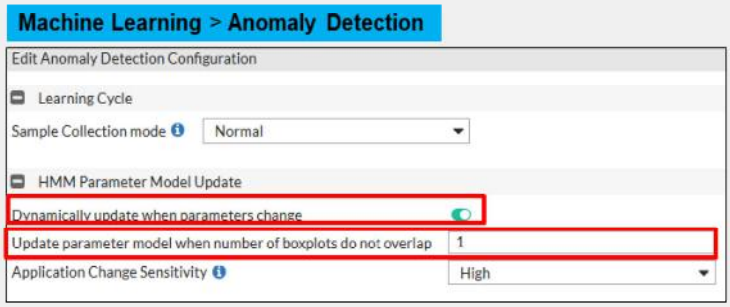
To view or edit the ML policy, click **Machine Learning** > **Anomaly Detection**, select the corresponding server policy, and then click **Edit**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HMM Parameter Model Update Settings

- Dynamically update the parameter
  - Compare results generated in the running stage to those from the collection stage, and if they don't overlap, rebuild the mathematical model
- How many boxplots must not overlap before the parameter model is updated?
  - 2 is the default, can be from 1 to 3



NSE Training Institute © Fortinet Inc. All Rights Reserved. 28

Enabling the **Dynamically update when parameters change** option allows FortiWeb to automatically learn and adjust for changes made to your web application.

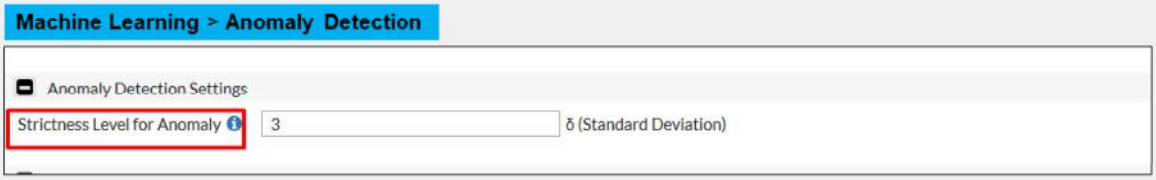
The **Update parameter model when number of boxplots do not overlap** setting allows you to define the threshold for relearning and adjusting the model. This defines how many consecutive boxplots must be outside of the overlap before triggering a relearning process. The options for this setting are 1, 2 (default), and 3.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Anomaly Detection Settings

- The machine learning model judges whether a request is an anomaly or not based on its **HMM probability** and the **length** of the parameter value
- The value for the strictness level can range from 1 to 10
  - Higher the value, the more anomalies are triggered



NSE Training Institute © Fortinet Inc. All Rights Reserved. 29

The ML model judges whether a request is normal or not based on its HMM probability and the length of the parameter value.

You can set the **Strictness Level for Anomaly** for the model to increase or decrease the sensitivity of anomaly detection. The value of the strictness level ranges from 1 to 10.

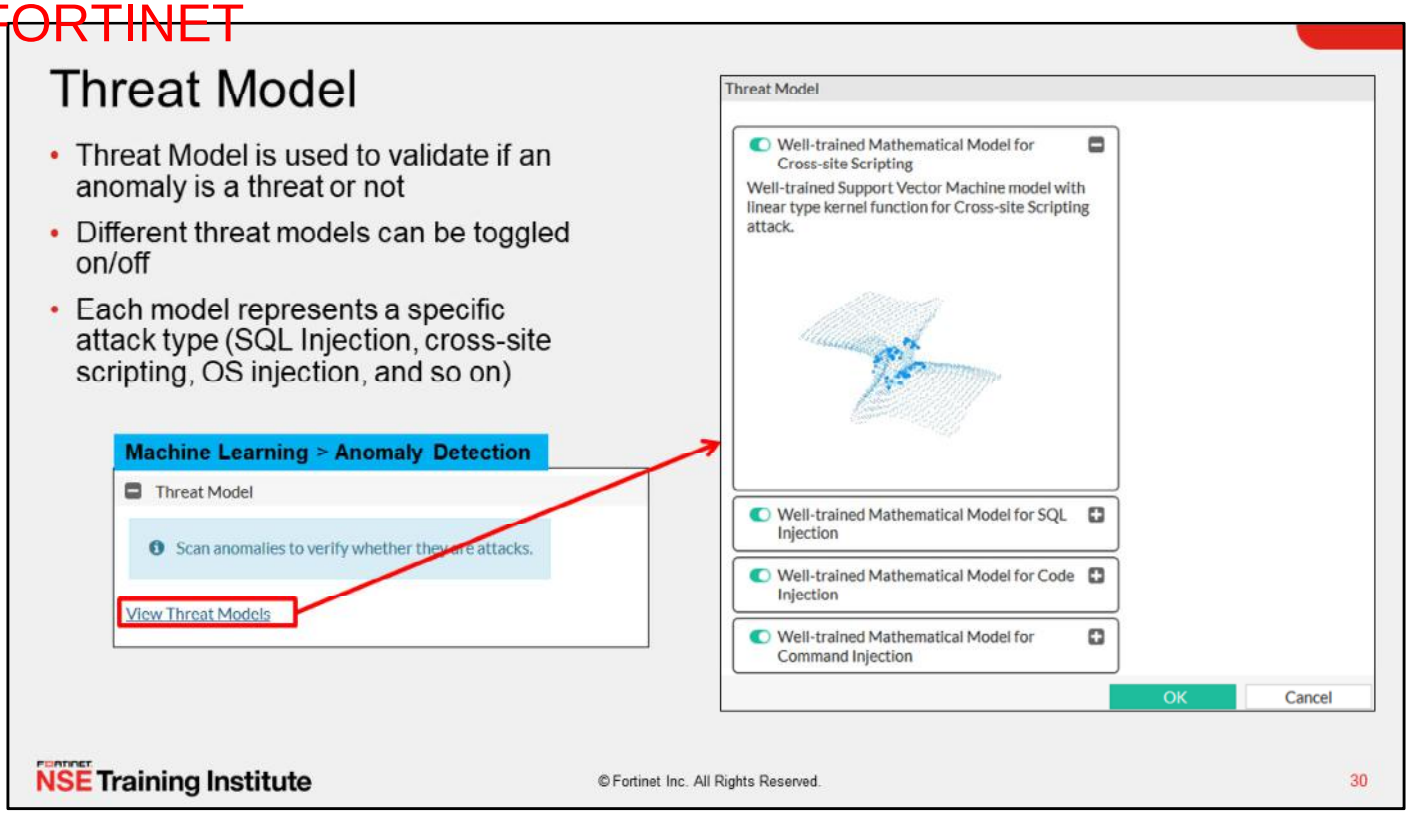
The system uses the following formula to calculate whether a sample is an anomaly: *The probability of the anomaly > μ + the strictness level * σ*

If the probability of the sample is larger than the value of "μ + the strictness level * σ", this sample is identified as anomaly.

μ and σ are calculated based on the probabilities of all the samples collected during the sample collection period, where μ is the average value of all the parameters' probabilities, and σ is the standard deviation. They are fixed values. So, the value of "μ + the strictness level * σ" varies with the strictness level you set. The smaller the value of the strictness level is, the more strict the anomaly detection model will be.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Each model represents a specific attack type (SQL injection, cross-site scripting, OS injection, and so on) and has been extensively trained and tested by the FortiWeb development team. They are created using thousands of real attack samples from various sources. These include well-known, third-party databases, such as CVE and ExploitDB, FortiGuard Labs, and leading third-party vulnerability scanners. Updates to these models are included as part of the FortiGuard WAF Security Service to provide protection from new threats that require model retraining and testing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Action Settings

- Actions to take for parameter anomalies
- **URL Replacer Policy**
  - Used if web applications have dynamic URLs or unusual parameter styles

Machine Learning > Anomaly Detection

Action Settings

Name	Action	Block Period	Severity	Trigger Policy
Anomaly Detection	Alert & Deny	600	High	

All requests are scanned first by HMM and then by Threat model. Choose action when attack is verified.

URL Replacer Policy

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

Here we can set the **Action** to take for parameter **Anomaly Detection**. The options are **Alert**, **Alert & Deny** (default), and **Period Block**.

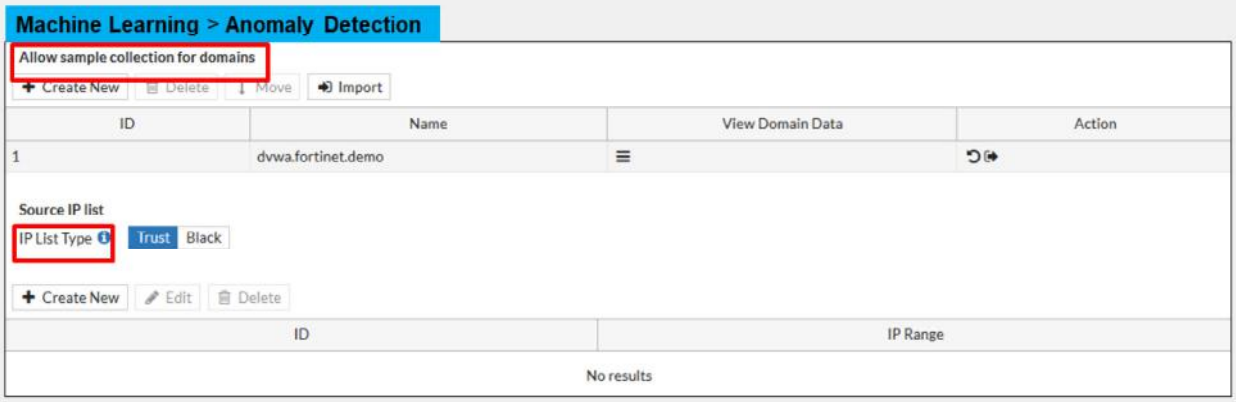
If the web application has dynamic URLs or unusual parameter styles, you must also adapt the **URL Replacer Policy** to recognize them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample Collection Settings

- Allow sample collection for domains
  - FortiWeb collects samples and generates ML models for these domains
- Allow sample collection from IPs
  - System collects traffic data samples only from these IP addresses to build ML models



NSE Training Institute © Fortinet Inc. All Rights Reserved. 32

The **Allow sample collection for Domains** table displays the list of domains that the ML module has automatically generated from information gathered by ML profiles. Here, administrators can view machine learning reports for that specific domain. You will look at this information in the next few slides.

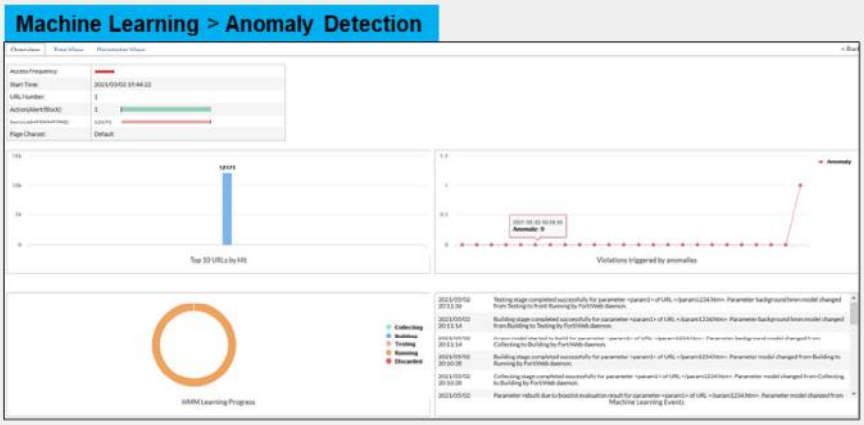
The **Allow sample collection from IPs** table displays the list of IP addresses from which the ML module can gather traffic data samples.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Domain View—Overview

- Summary of data collected for the domain using the machine learning profile
- It reports the
  - Domain overview info
  - Top 10 URLs by Hit
  - HMM Learning Progress
  - Violations Triggered by Anomalies
  - Machine Learning Events



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

The **Overview** tab provides a summary of data collected for the domain through the use of the ML profile. It reports information about the entire domain, including the domain **Overview**, **Top 10 URLs by Hit**, **HMM Learning Progress**, **Violations Triggered by Anomalies**, and **Machine Learning Events** dashboard.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Domain View—Tree View

- Displays the entire URL directory of the domain in a tree view
  - You can click the URL path to view its violation statistics

© Fortinet Inc. All Rights Reserved.

The **Tree View** displays the entire URL directory of the domain in a tree view. You can choose either one of the URLs to view its violation statistics.

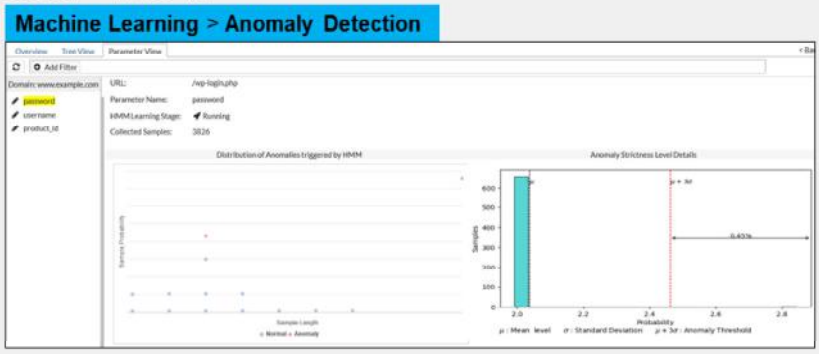
- **Web site directory**—The left panel of the **Tree View** page shows the directory structure of the website. The / (backslash) indicates the root of the site. You can click a URL in the directory tree, then the violation statistics of this URL are displayed on the right side of the **Tree View** page. You can also click a directory, then click **Rebuild Directory** to rebuild machine learning models for all the URLs under the selected directory.
- **Parameters**—**Parameters** tab shows the HMM learning states of all the parameters attached to the URL. For example, if the URL is `http://www.demo.com/1.php?user_name=jack`, then `user_name` is the parameter. A URL can contain multiple parameters.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Domain View—Parameter View

- Display statistics related to parameters
  - HMM learning stages
  - Distribution of anomalies
  - Anomaly strictness level details
- Can rebuild parameters or set the strictness level for anomalies



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

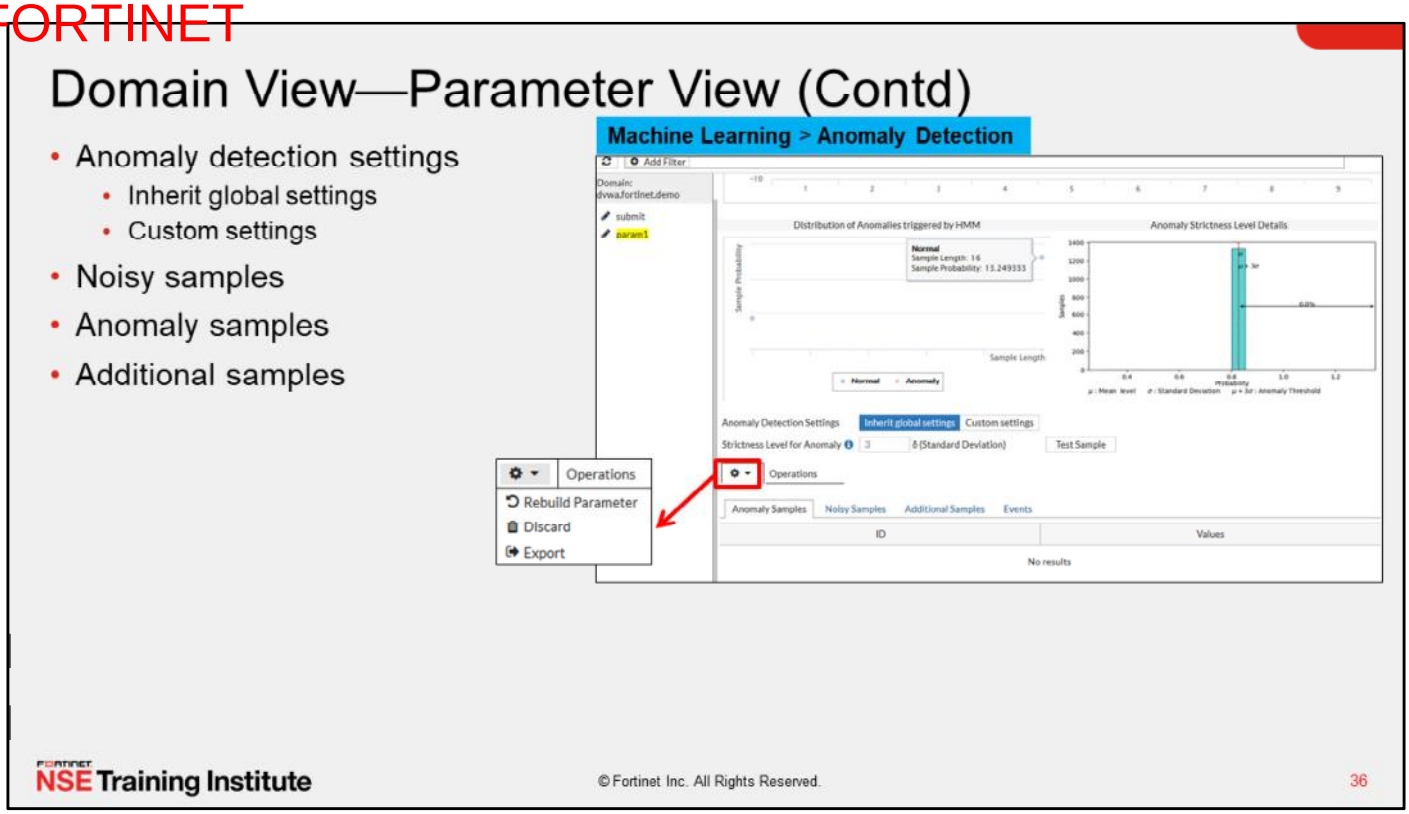
35

Parameter View displays ML statistics for all the parameters. You can click **Add Filter** in the upper-left corner of the page and filter the parameters by name or learning status.

Distribution of Anomalies triggered by HMM displays the potential or definite anomalies in red and the normal requests collected during the sample collection phase in blue. The system judges whether a request is normal or not based on its probability and the length of the parameter value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can customize the strictness level for individual parameters, or inherit the strictness level you have set for the domains, in the anomaly detection policy.

You can also test a sample for a parameter to verify whether it is detected as an anomaly at the current strictness level.

You can take actions like rebuilding, discarding, or exporting on any parameter.

Noisy samples are the abnormal samples detected during the sample collection period. They are excluded from the samples used to build the anomaly detection model. If you believe a sample is falsely detected as a noise, you can click the status icon to exclude it from noisy samples, so that it can be re-admitted to build the anomaly detection model.

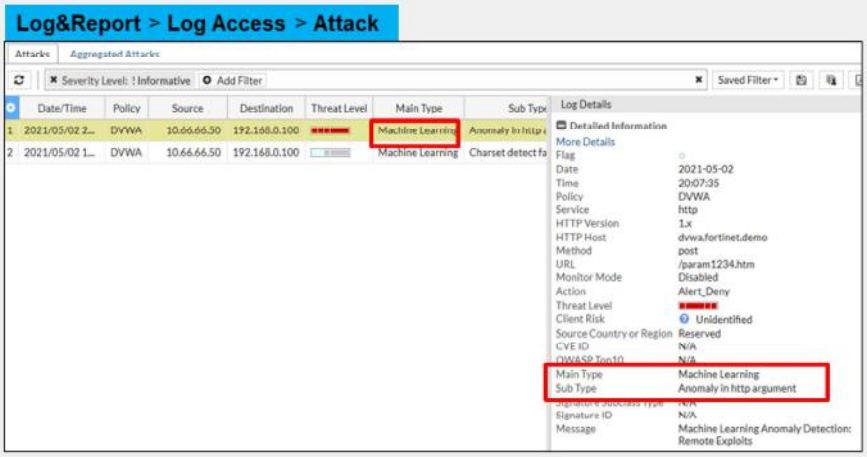
Additional samples are the samples manually added from the attack logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

New Machine Logging Events

- There are new attack logs for ML violations
- The ML log has the following subtypes:
  - Anomaly in http argument
  - HTTP Method violation
  - Charset detect failed



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

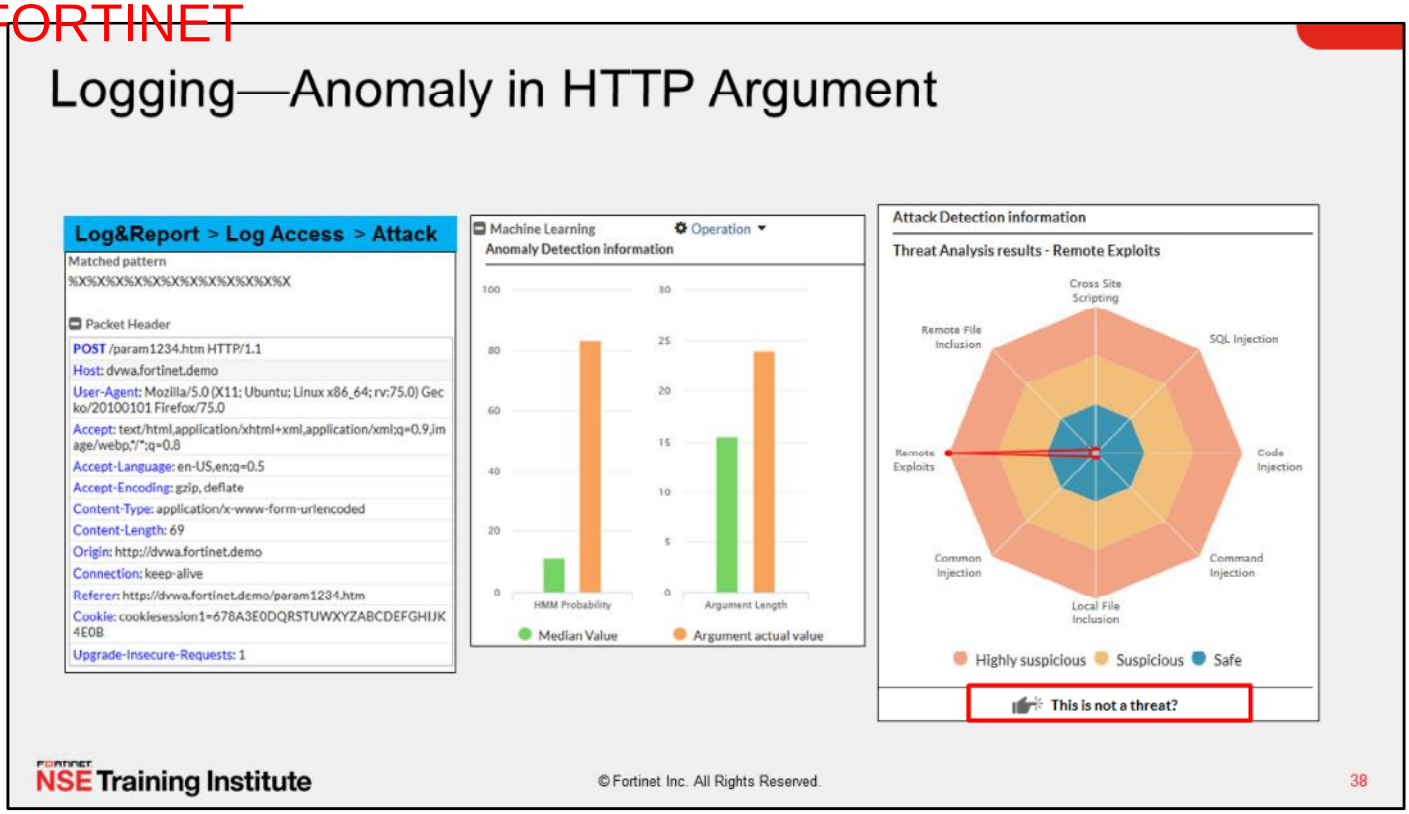
37

There are new attack logs for machine learning violations. The machine learning log has the following subtypes:

- **Anomaly in http argument**
- **HTTP Method violation**
- **Charset detect failed**

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



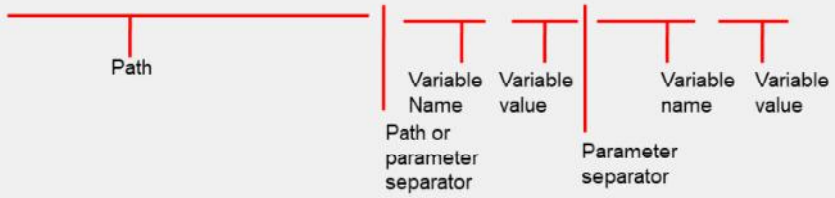
Clicking the log entry shows more detailed information, such the **Matched Pattern**, **Packet Header**, **Anomaly Detection Information**, and **Attack Detection Information**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

URL Structure

/static/path/to/application?username=user1&password=pass WD



- How does FortiWeb find URLs, parameter names, and data types?
- By default, machine learning assumes that your web application uses the most common URL structure
- If your web application uses dynamic URLs or unusual parameter styles, you must use URL replacers in an application policy in the machine learning profile
  - Configures FortiWeb to find the web applications pages and parameters in URL

NSE Training Institute © Fortinet Inc. All Rights Reserved. 39

In an HTTP request that uses the GET method, the URL and parameters are all together on the same line, with no spaces between them. How does ML differentiate each input and its values?

By default, it uses standard cues to find them. A question mark (?) usually separates the URL from the inputs, an equal sign (=) separates the input name from the input value, and an ampersand (&) separates the input's value from the name of the next input.

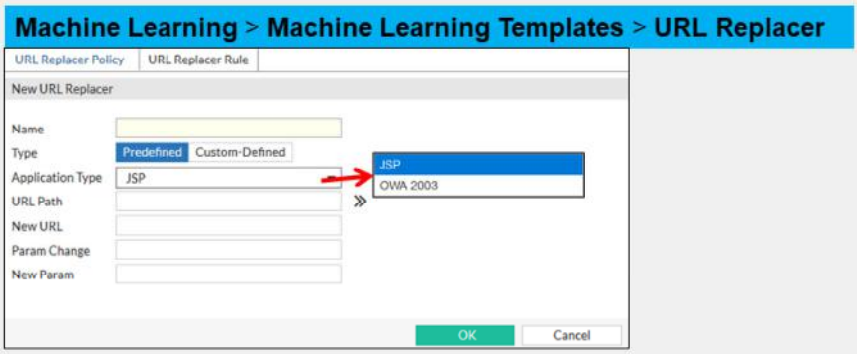
What happens if the URL is dynamically generated, or if the separator characters are different? In that case, you must specify where to find each piece. Otherwise, ML won't function correctly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

URL Replacer

- Interprets dynamic URL or non-standard parameters into standard
  - Despite name, does not replace or rewrite the URL
- Two predefined
  - OWA 2003 for Outlook Web App (formerly called Outlook Web Access)
  - JSP for Java Server Pages
- For custom or in-house apps, you can make your own



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

URL Replacer is what shows auto learning how to interpret the URL line to find the URL and separate each input.

Because Java server pages and Outlook Web App 2003 often don't use the standard URL format, there are predefined objects for them. These can also be configured manually. You can see examples in the documentation. When you've defined a chain of URL replacers to interpret every non-standard part of the URL into the standard format, group them together, in order, in an application policy, then select it in the ML profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How many samples are collected when using the **Extended** collection mode?
   A. At least 5000
   ✓ B. At least 2500

2. What is the default amount of standard deviations a parameter must exceed before being flagged as an anomaly?
   A. 1
   B. 2
   ✓ C. 3
   D. 4

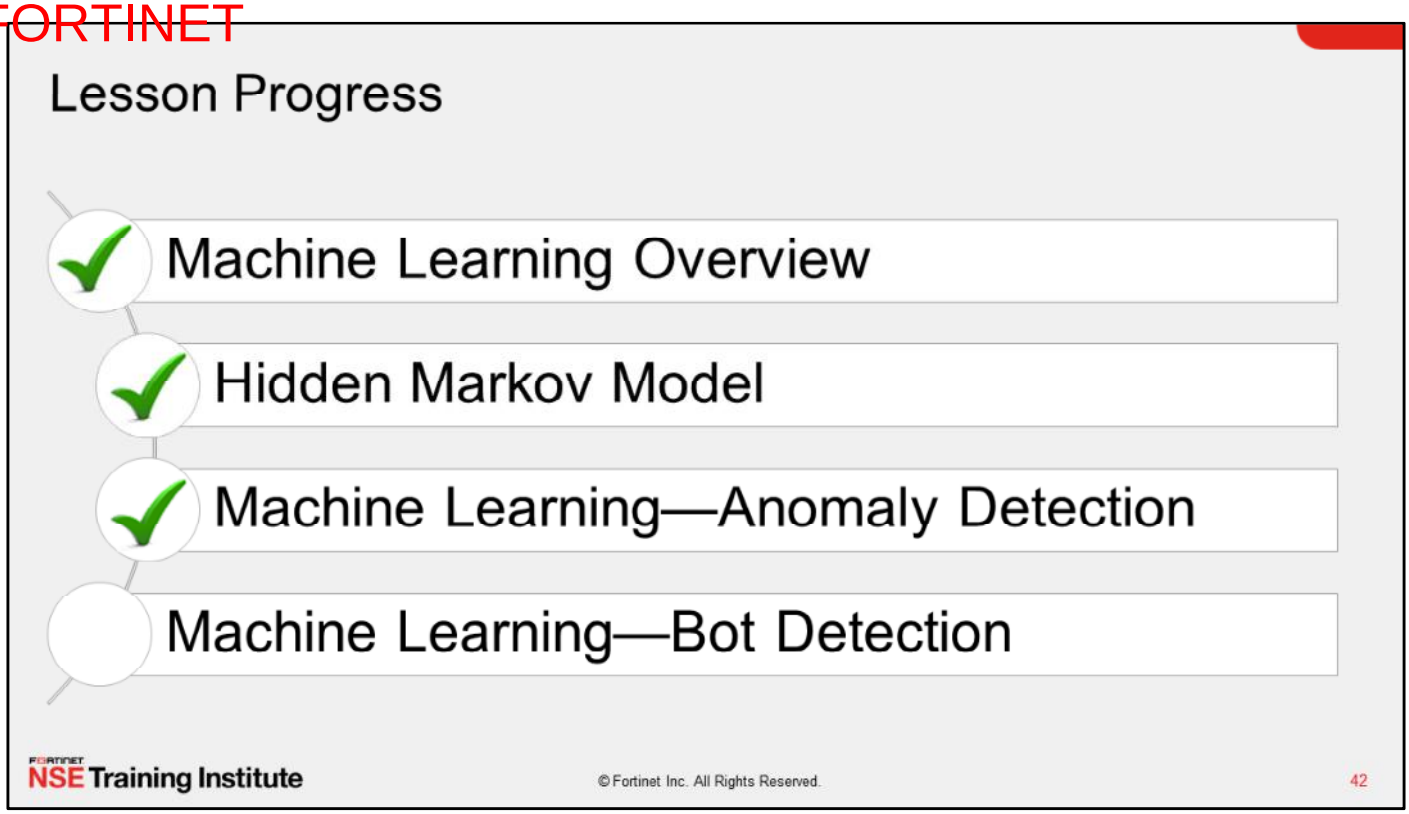
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

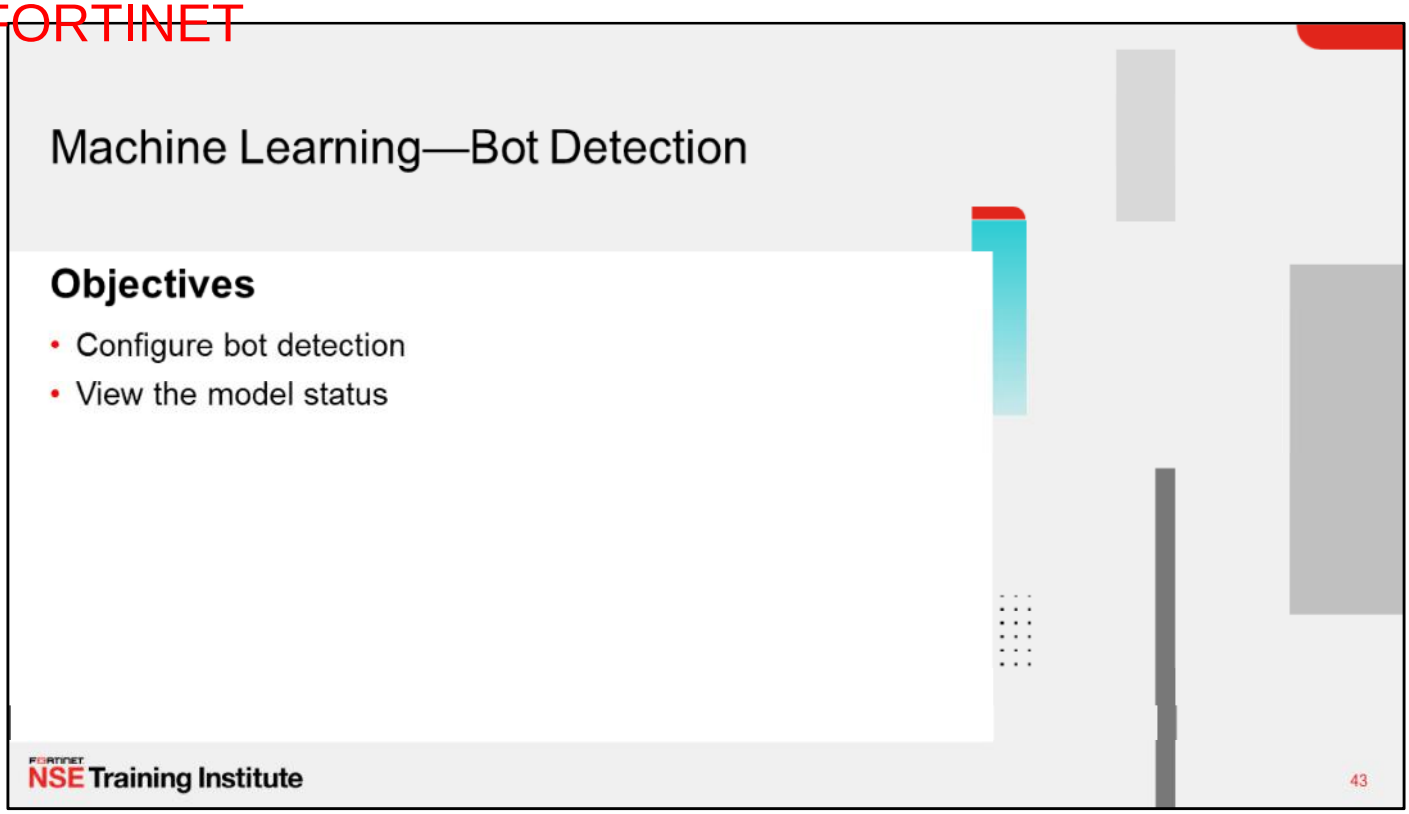


Good job! You now know how to configure the FortiWeb ML anomaly detection capability.

Now, you will learn how to configure the FortiWeb ML bot detection feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in ML bot detection, you will be able to implement bot detection to protect your web applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Detection

- Bot detection tracks and protects based on:
  - Requests per second
  - Connections per second
  - Errors per second
  - Many more stats
- Uses ML based on Support Vector Machine (SVM) algorithm
- Three stages
  - Sample collecting
  - Model building
  - Model running
- Bot confirmation mechanism to confirm if anomaly is a bot or not (false positive detection)
  - Also used to trigger model updates

NSE Training Institute © Fortinet Inc. All Rights Reserved. 44

Bot detection is used to track and protect how legitimate clients access the web app. Bot detection monitors for things such as:
- Requests per second
- Connections per second
- Errors per second
- Many other similar statistics

The bot detection function, although still a form of machine learning, uses a different underlying mechanism. Whereas anomaly detection uses HMM, bot detection is based on the Support Vector Machine (SVM) algorithm. The bot detection model has three stages:
- Sample collecting
- Model building
- Model running

Each of these stages will be discussed on the following slides.

It's possible that sometimes the traffic is falsely detected as an anomaly. The system uses bot confirmation to confirm whether an anomaly is indeed a bot. If the false positive detection occurs so many times that it exceeds a certain threshold, the system considers the current bot detection model invalid, and automatically updates the model.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Detection—Sample Collection

- Collects samples (vectors) of visitor behavior
- Sample records behaviors within a certain timeframe
- Split into two parts: three-quarters are training set, one-quarter are testing set

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

To build up a bot detection model, the system collects samples (also called vectors) of users' behaviors when they are visiting your application. Each sample records a specific user's behaviors in a specific time range. The samples are split into two parts; three-quarters of the samples are divided into the training sample set, one-quarter of the samples are divided into the testing sample set.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Detection—Model Building

- System observes training samples to self-learn
- Builds mathematical model using SVM algorithm
- Multiple models built, based on different parameters
- System narrows the selection down to one model, based on multiple criteria

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

During the model building stage, the system observes the training samples to self-learn user behavior profiles and builds up mathematical models using the SVM algorithm. The system uses the SVM parameters to eliminate rogue training samples and control individual sample influence on the overall result. The system builds multiple models based on different parameter combinations in the SVM algorithm. According to the training accuracy, cross-validation value, testing accuracy, and the model type you have configured, the system narrows down the selection to one model and uses it as the bot detection model.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Detection—Model Running

- System compares users' behaviour against the model
- If traffic doesn't match model, system flags it as an anomaly
- After specific number of anomalies from same user, system takes action

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

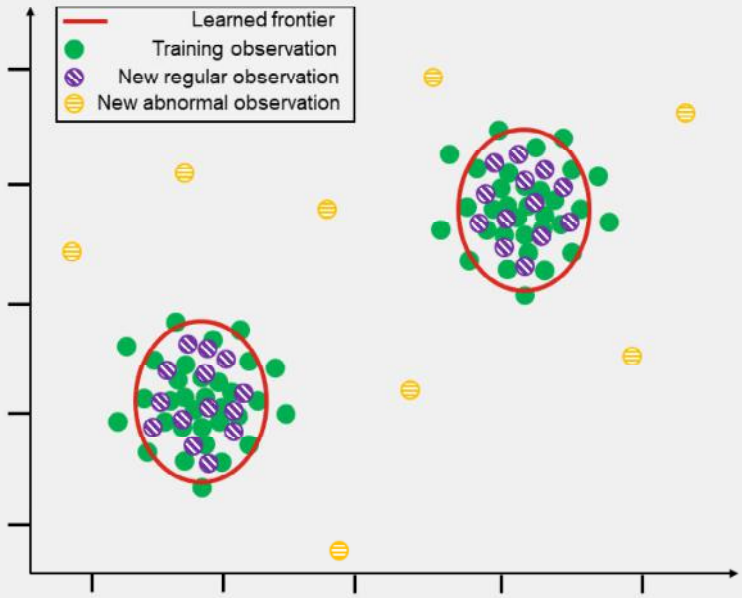
When the bot detection model is in the running state, the system compares users' behaviors against the bot detection model. If the traffic from a certain user doesn't match the model, the system records the traffic as an anomaly. If a certain number of anomalies are recorded for this user, the system acts, such as sending alert emails, or blocking the traffic from this user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Support Vector Machine

- SVMs based on statistical learning
- Frontier created based on observations
- New observations within the frontier considered normal
- New observations outside of frontier considered anomaly



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

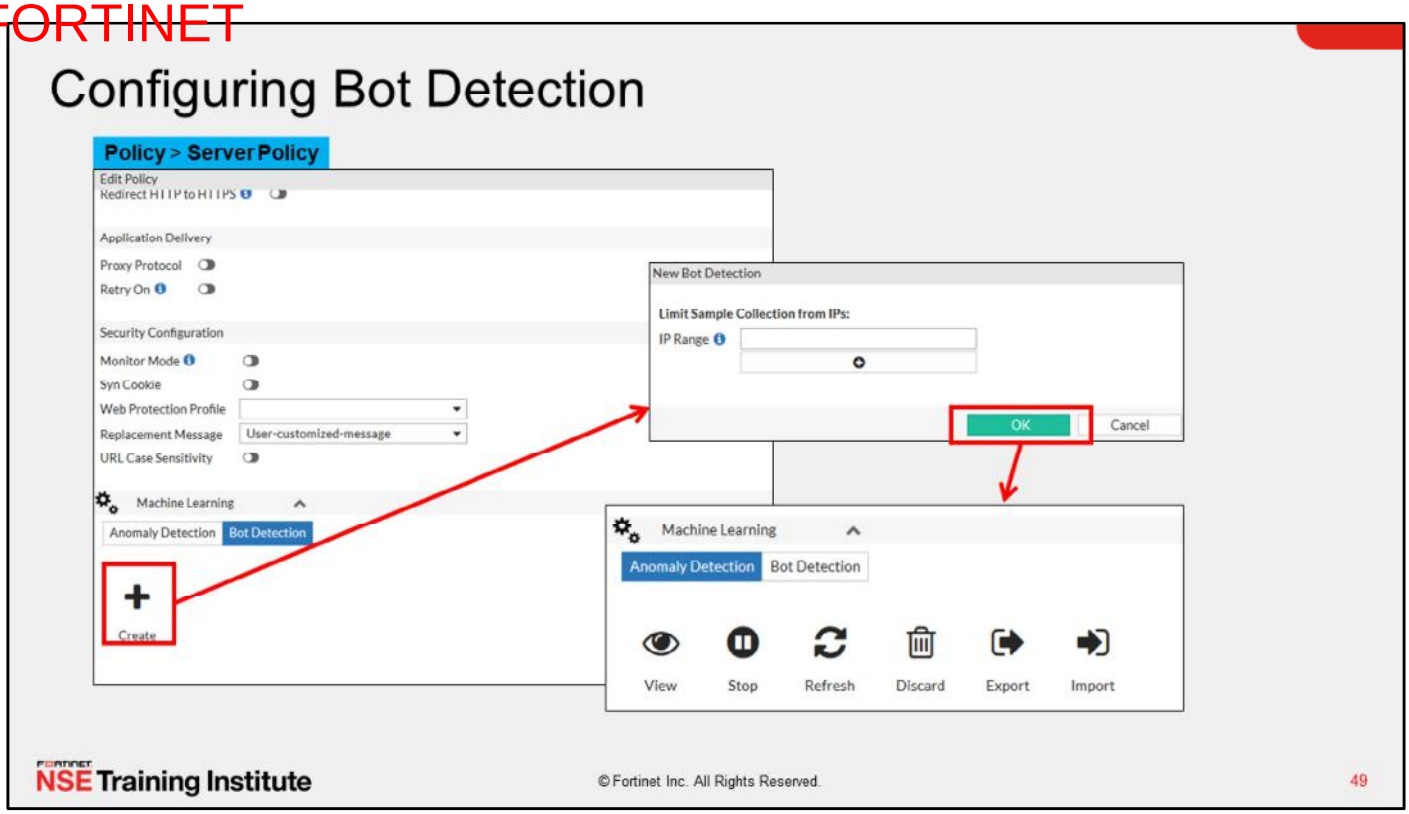
48

An SVM is a statistical ML algorithm that you can use for both classification and regression purposes. SVMs are based on the idea of finding a hyperplane that best divides a dataset into two classes. Support vectors are the data points nearest to the hyperplane, the points of a data set that, if removed, would alter the position of the dividing hyperplane. Simple SVMs based on two dimensions of data points, are referred to as linear SVMs. More complex SVMs, based on three dimensions of data points, are referred to as non-linear. FortiWeb uses non-linear SVMs in the bot detection models.

Data points are collected, and then processed by a complex algorithm to find the hyperplane, or frontier. Once the frontier is calculated, all new observations are plotted against that frontier. Any new observation that falls within the frontier is considered normal, while all new observations plotted outside of the frontier are flagged as anomalies.

Vouchers & Dumps are Available | WhatsApp +201224560923

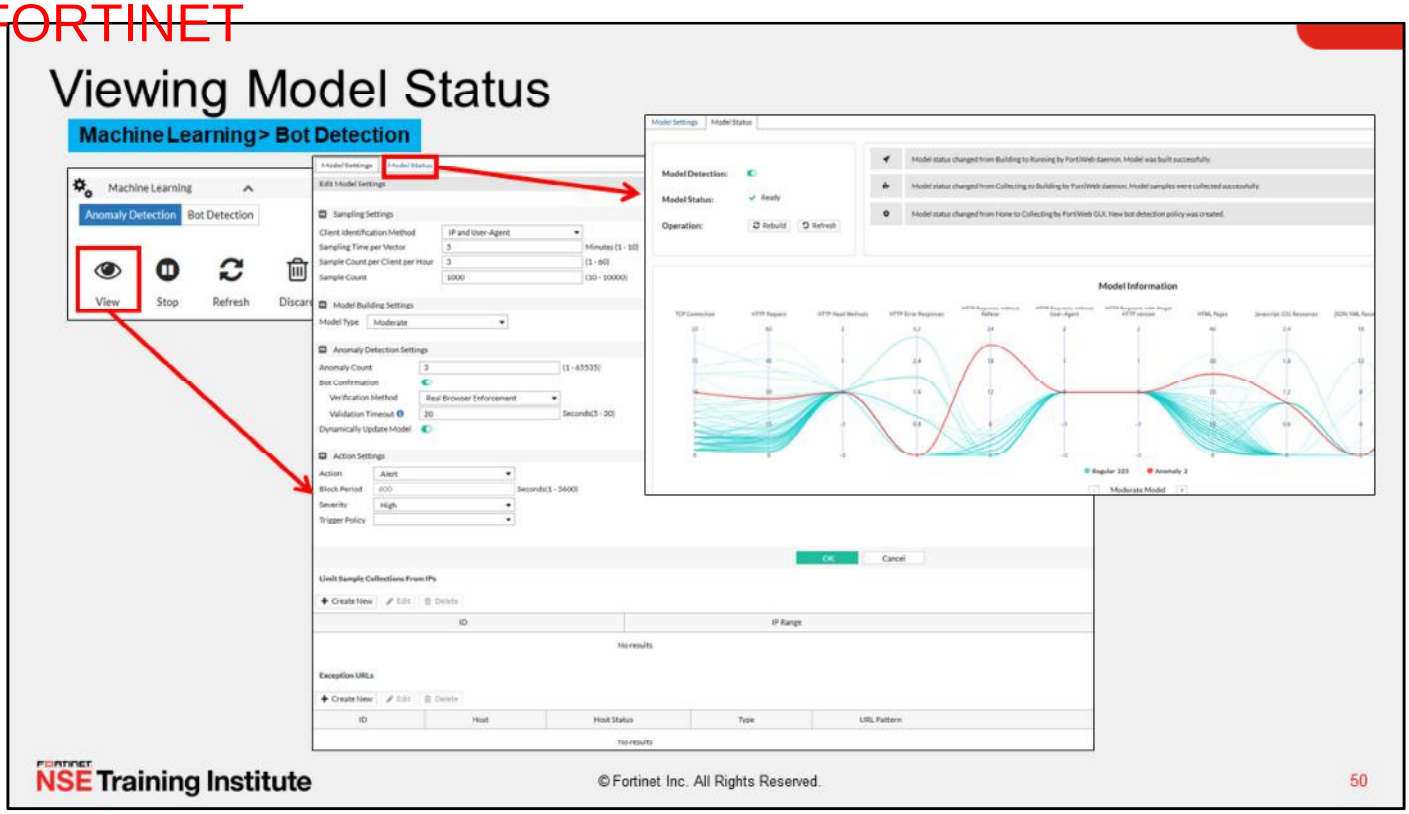
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Bot detection profiles are part of the server policy. They are created on the **Policy** > **Sever Policy** page. All bot detection profiles that you create show up on the **Machine Learning** > **Bot Detection** page, where you can configure or edit them to your preference.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view the bot detection model status in the server policy under **Machine Learning > Bot Detection**, select the specific policy and then click **Edit**.

The model is in one of four statuses:

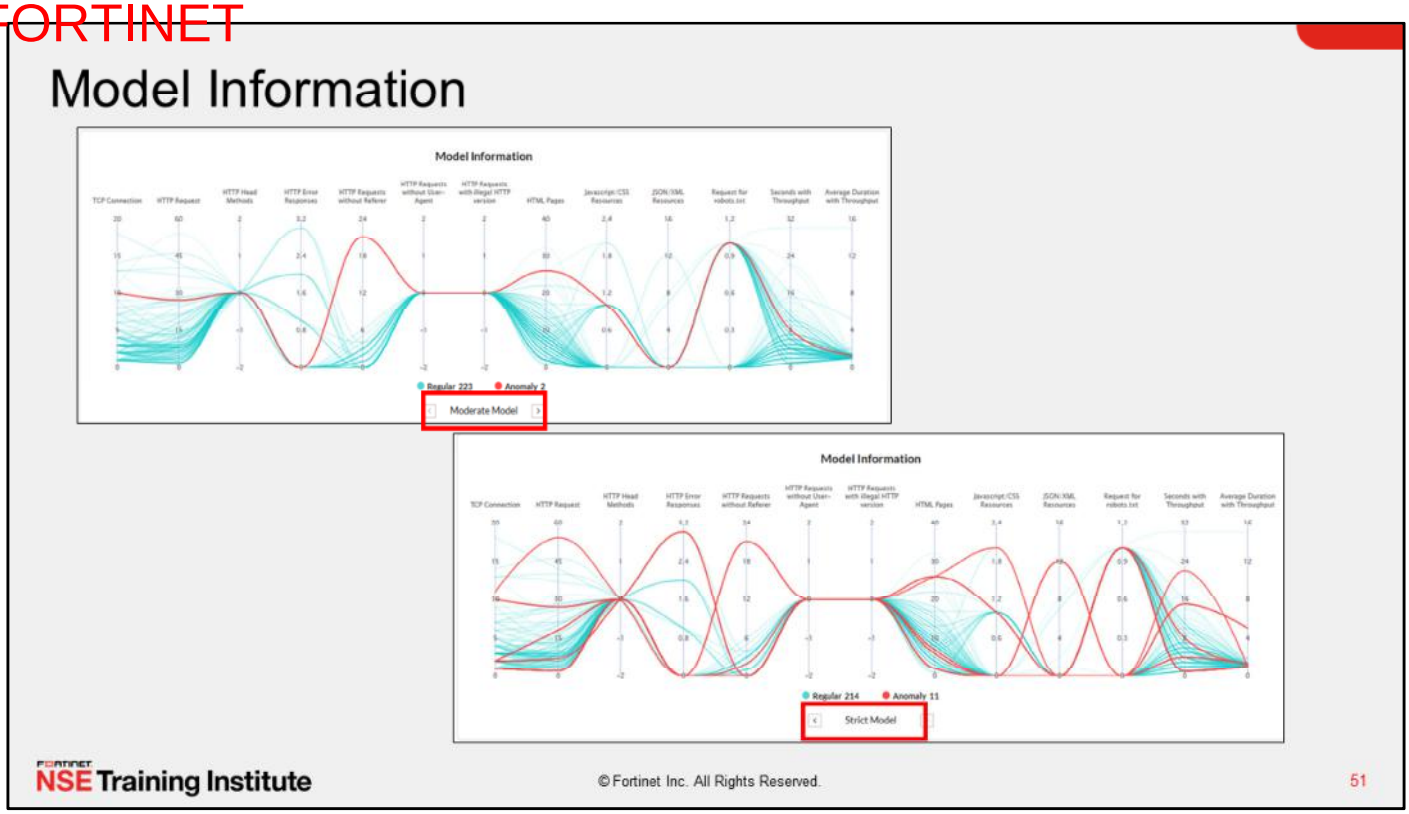
- **Collecting**—The system is collecting samples.
- **Building**—The system is building the bot detection model.
- **Ready**—The model is ready to run. You can use the **Model Detection** option to run or stop the model.
- **Failure**—The model failed to be built. You can check the log messages to get more information on the failure reasons and adjust the settings in the bot detection policy accordingly.

The **Operation** section allows you to manually update the model:

- **Rebuild**—The system rebuilds the model using the existing samples. This option is useful when the policy settings are changed, so that the bot detection model should be rebuilt with the adjusted settings.
- **Refresh**—The system re-collects samples, and then rebuilds the model. This option is useful when you think the model is not accurate, and you want to re-collect samples and rebuild the model. Also, keep in mind to use the **Dynamically Update Model** option in the bot detection policy to automatically refresh the model when too many false positive vectors are detected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Model Information** section displays the anomalies detected in the **Training Set** and **Test Set.** You can switch between the **Moderate Model** and **Strict Model**. The bot detection model evaluates users' behaviors over an extensive number of different dimensions. These include **TCP connection, HTTP request, HTTP HEAD methods, HTTP error responses, TTP requests without Referers, HTTP requests without User-Agent, HTTP requests with illegal HTTP version, HTML pages, JavaScript/CSS resources, JSON/XML resources, Request for robots.txt, Seconds with throughput,** and **Average duration with throughput**.

For specific details of each of these dimensions, see the *FortiWeb Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

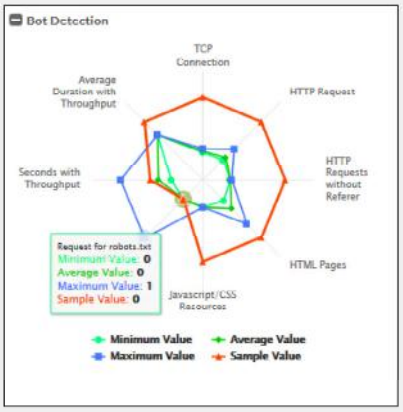
DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Violations

Log&Report > Log Access > Attack

Severity Level: ! Informative | Add Filter

#	Date/Time	Policy	Source	Destination	Threat Level	Main Type	Action	Sub Type
1	2021/05/03 17:53:31	DVWA	10.66.66.112	192.168.0.100		Bot Detection	Period_Block	N/A
2	2021/05/03 17:53:31	DVWA	10.66.66.115	192.168.0.100		Bot Detection	Period_Block	N/A
3	2021/05/03 17:53:31	DVWA	10.66.66.115	192.168.0.100		Bot Detection	Period_Block	N/A
4	2021/05/03 17:53:31	DVWA	10.66.66.114	192.168.0.100		Bot Detection	Period_Block	N/A
5	2021/05/03 17:53:31	DVWA	10.66.66.114	192.168.0.100		Bot Detection	Period_Block	N/A
6	2021/05/03 17:53:31	DVWA	10.66.66.113	192.168.0.100		Bot Detection	Period_Block	N/A



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

52

Bot detection violations can be viewed in **Log&Report** > **Log Access** > **Attack**. Click the item to view its detailed information.

The radar chart is used to compare the current vector with the vectors in the training sample set. The red line represents the values of the current vector, while the other three lines respectively represent the minimum value, average value, and maximum value of the vectors in the training sample set . The example shown on this slide is the radar chart of a violation. You can see the red line is far apart from the other three lines, which means the current vector is quite possibly a bot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. During the sample collection phase, what portion of the samples is used for the training set?
   - ✓ A. 3/4
   - B. 1/4

2. Where is Support Vector Machine not used for detecting threats?
   - A. Bot detection
   - B. Anomaly detection in machine learning
   - ✓ C. Threat detection in machine learning

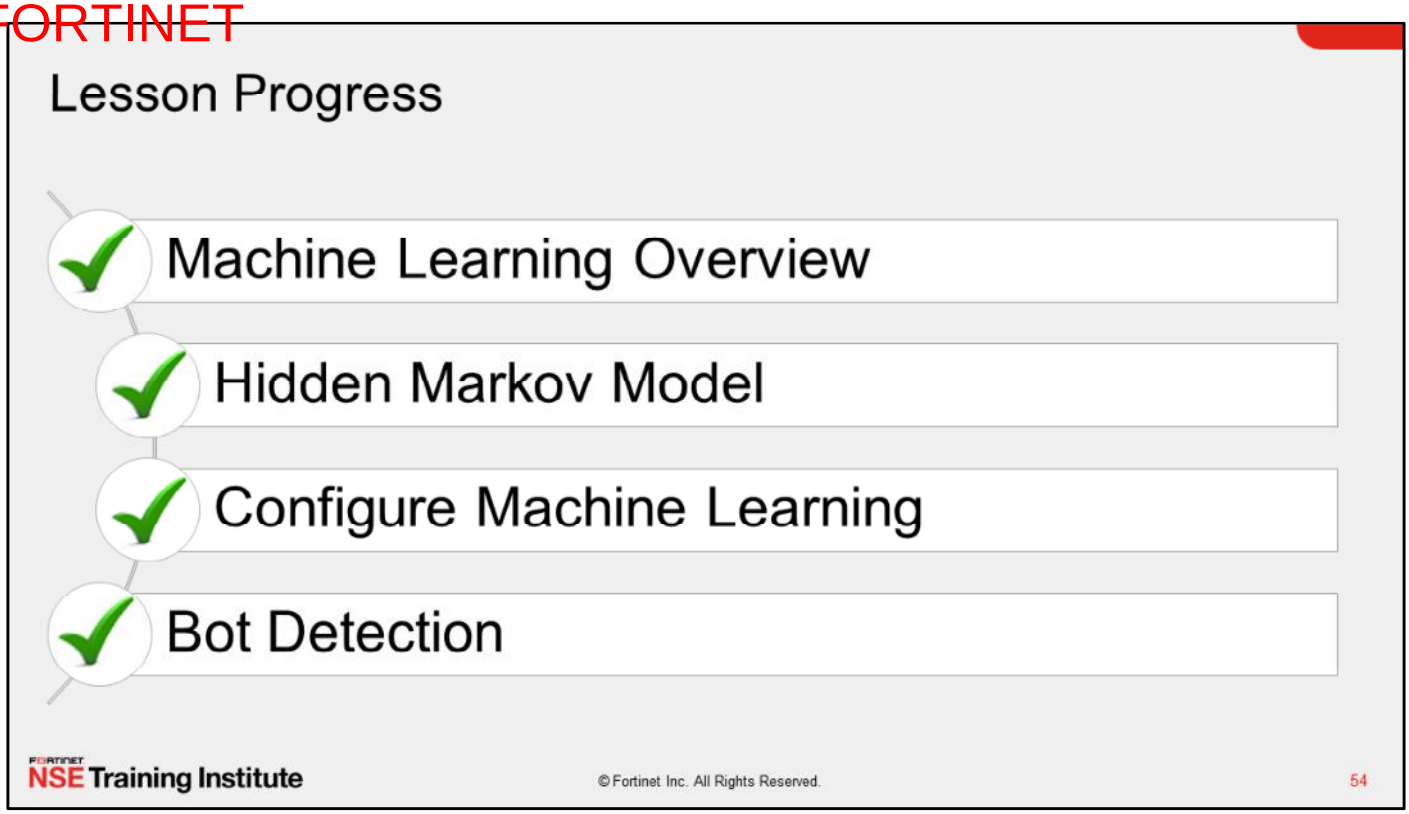
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

53

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe the benefits of machine learning in FortiWeb
- ✓ Define the HMM
- ✓ Understand how the HMM works using a simple scenario
- ✓ Configure machine learning
- ✓ Review machine learning statistics
- ✓ Configure bot detection

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

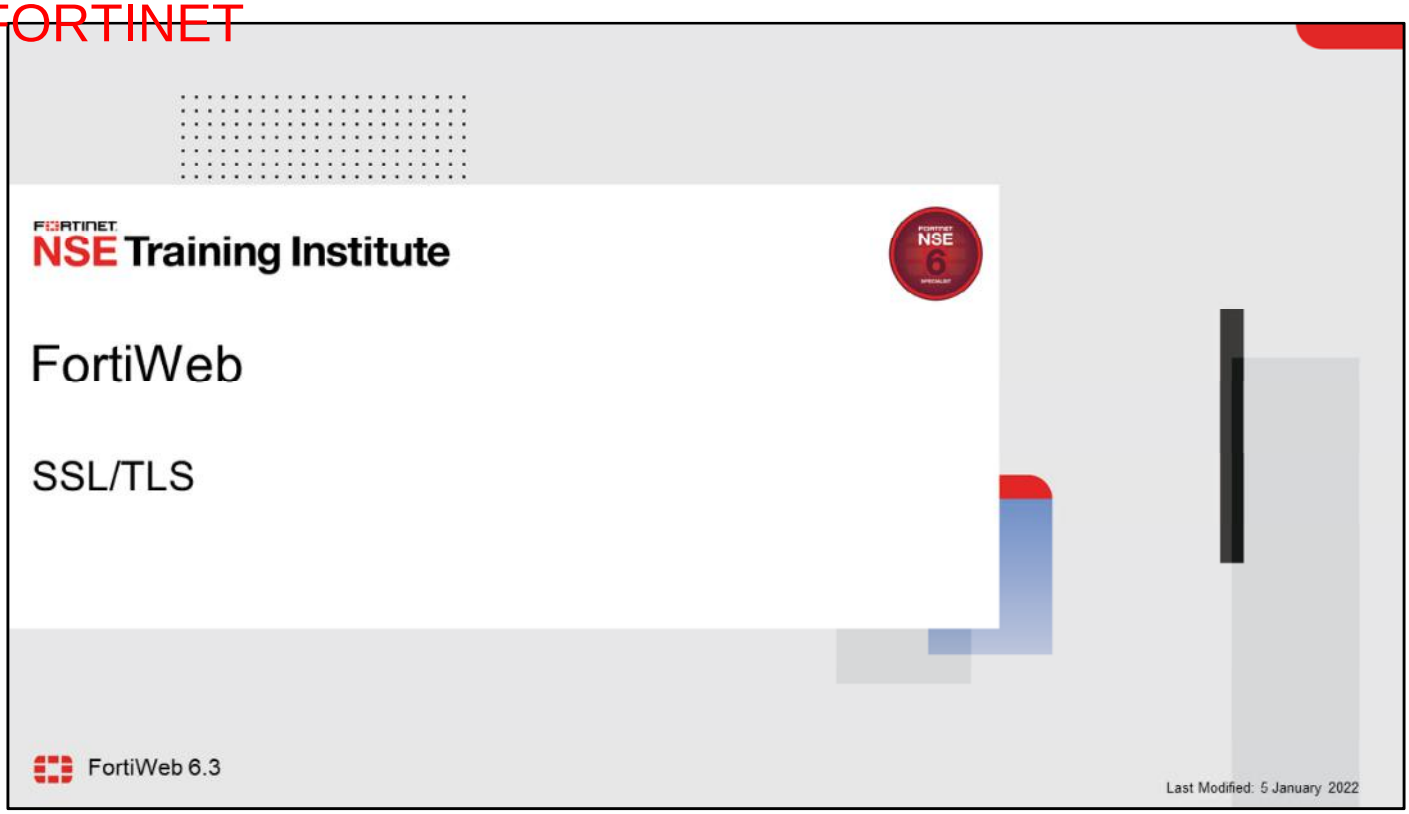
55

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you are able to take advantage of the benefits of the FortiWeb Machine Learning features, and implement them on your FortiWeb, in order to protect your web applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to use encrypted HTTP transactions. With HTTPS, login credentials, and other sensitive data aren't compromised while they're in transit.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- HTTPS Basics
- SSL/TLS Protocols and Ciphers
- X.509 Certificates
- Client PKI Certificates
- Additional Operations

NSE Training Institute

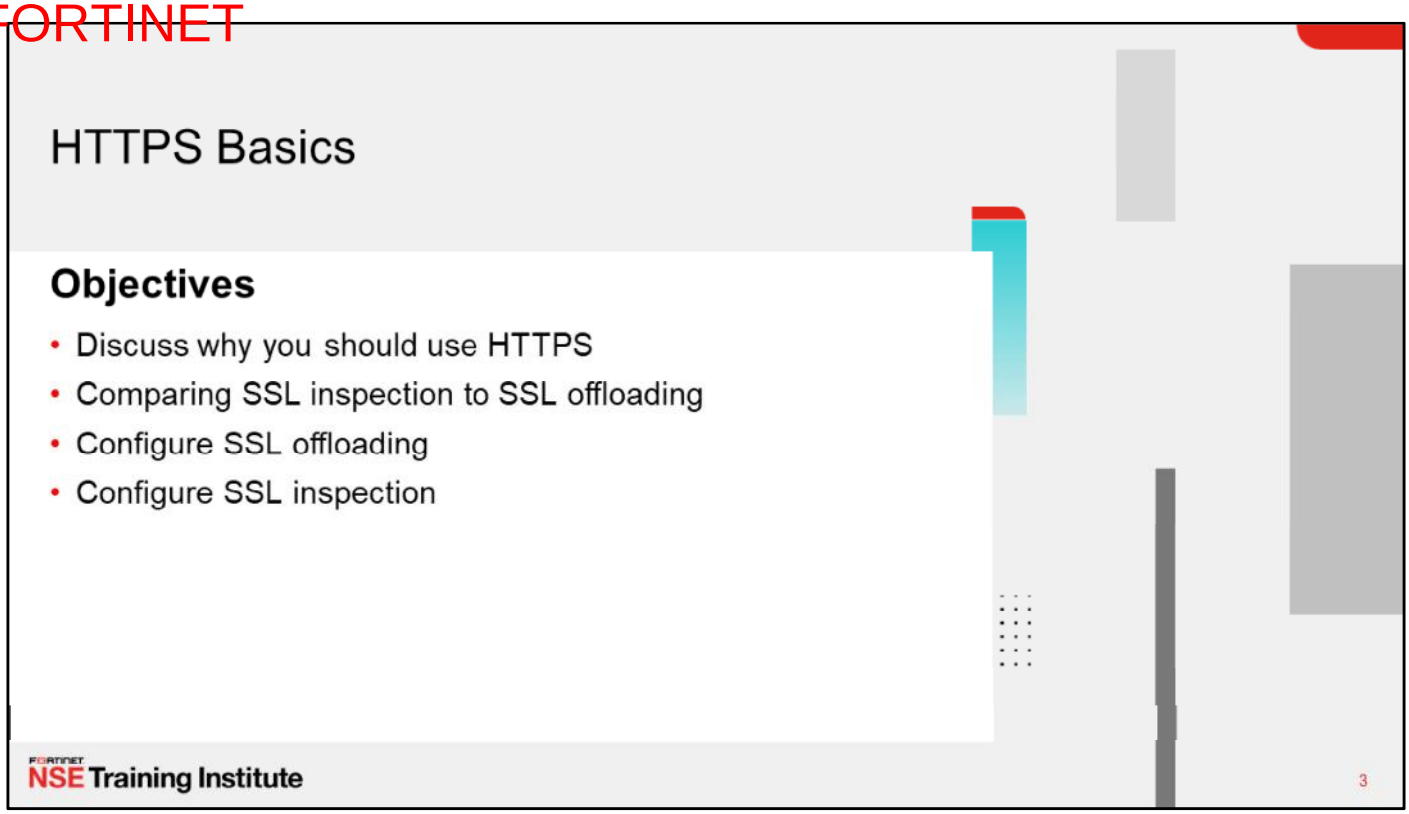
© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in knowing when to use HTTPS and configuring SSL offloading and inspection, you will be able to use them in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Why HTTPS?

- Web is shifting to using HTTPS despite slower performance
  - Google, Facebook, Twitter, and others now automatically redirect to HTTPS
- Search engine optimization (SEO)
  - Google now ranks HTTPS sites slightly higher
  - http://arstechnica.com/security/2014/08/in-major-shift-google-boosts-search-rankings-of-https-protected-sites/
- Consumer confidence
  - https://www.trustworthyinternet.org/ssl-pulse/
  - Certificate shows server (or FortiWeb) identity is genuine
    - Example: browser warning if bank web site or twitter.com is fake
  - Optional client certificate authentication
- Privacy
  - Required by PCI DSS, FIPS-CC, HIPAA, and others
  - Encrypts webmail, search, passwords, credit card numbers, and more, while in transit
    - Only authorized personnel and law enforcement have back-end access
- Brute force attacks are slower
  - Each try is more computationally *expensive* for attacker
  - Handshake plus key generation and exchange before they can try a password

NSE Training Institute © Fortinet Inc. All Rights Reserved. 4

Previously, HTTPS was mostly used for online banking, e-commerce, and government websites. Users needed privacy and confidence in the site's authenticity.

Since the leaks in 2013 and later by Edward Snowden, many of the most popular content websites from Twitter and Facebook, Tumblr and 500px.com, to Gmail, Google's search engine, and YouTube have all switched to HTTPS. Why?

Even seemingly harmless location check-ins and vacation photos can be exploited. If you're on vacation in Bali, obviously you're not home to prevent theft. And privacy laws that govern email have not evolved to cover social media, leaving people vulnerable to unscrupulous employers and free Wi-Fi. People who prefer privacy are shifting to HTTPS. This trustworthiness factor is now reflected in Google search rankings. HTTPS sites have a slightly higher ranking.

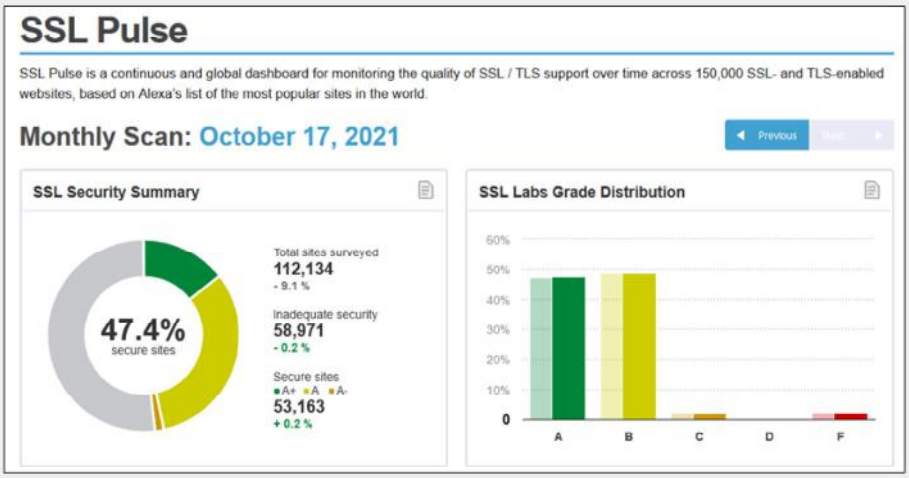
There's a surprising side effect. As a result of the more computationally expensive handshake and encryption, it is also more difficult to brute force the HTTPS site login page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

In-Transit Web Security Still Needs Improvement

- Data as of October 17th, 2021



https://www.ssllabs.com/ssl-pulse/

NSE Training Institute © Fortinet Inc. All Rights Reserved. 5

Many of the top 200 websites have now changed to HTTPS, but what about the millions of other websites on the internet?

This slide shows statistics for approximately 112,000 of the top sites as of October 2021. In this sample, 23 sites were still vulnerable to Heartbleed, an SSL vulnerability more than three years old.

The good news is that FortiWeb has tools that offer HTTPS, and helps you implement it securely for all protected websites.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How FortiWeb Uses HTTPS in Policies

- Server certificates do *not* belong to FortiWeb, but instead belong to the protected web servers
- You upload the servers' certificates to FortiWeb
  - FortiWeb becomes an SSL reverse proxy
- FortiWeb uses the web server's certificate and key because one of the following is true:
  - FortiWeb is acting as an SSL agent for the web server (SSL proxy)
  - FortiWeb is privy to secure connections for scanning purposes (SSL inspection)

NSE Training Institute © Fortinet Inc. All Rights Reserved. 6

When you configure HTTPS on FortiWeb, you are usually configuring policies, not HTTPS connections to the FortiWeb GUI. Policies govern traffic travelling through FortiWeb, not to it.

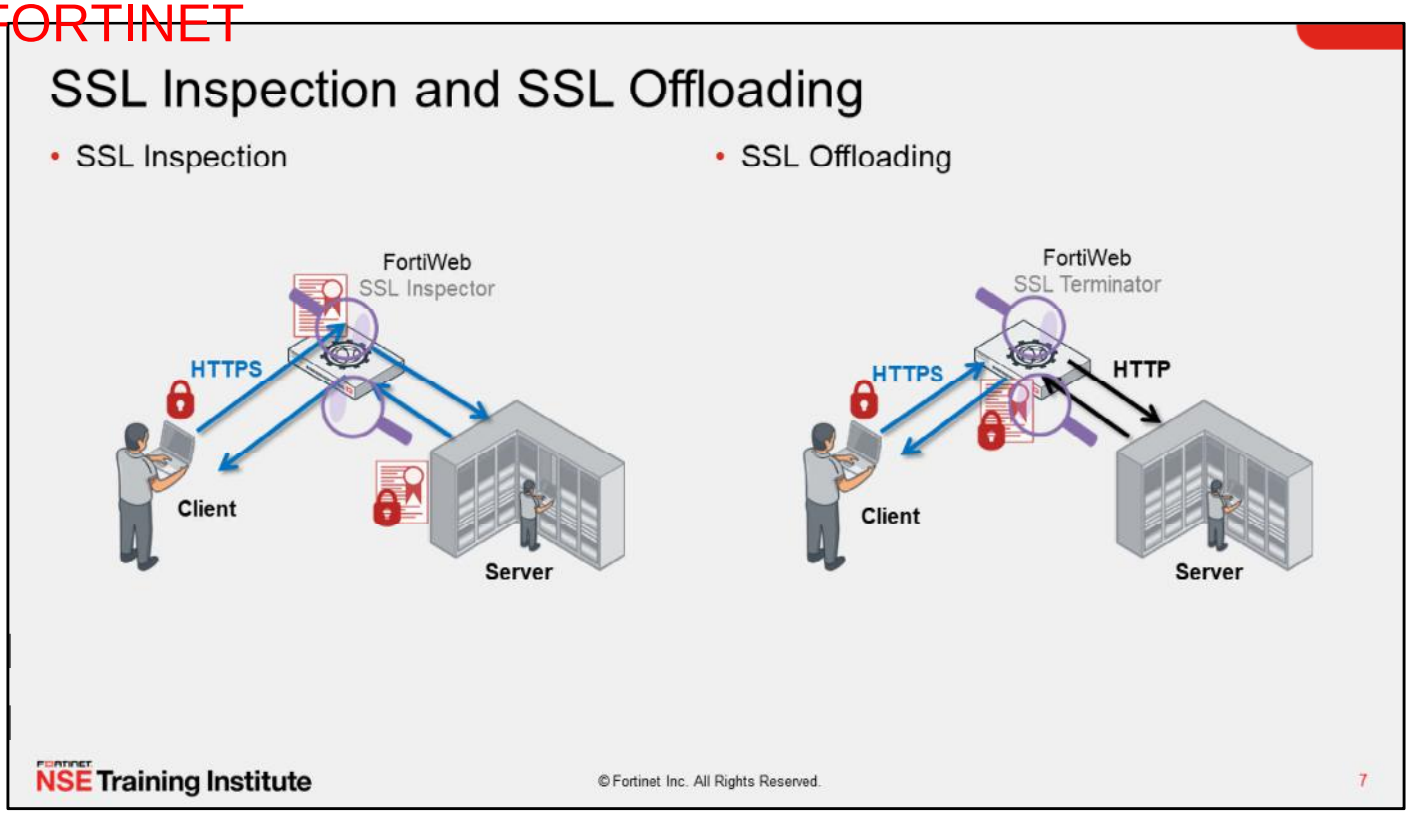
In policies, FortiWeb supports HTTPS. It can be either:

- An SSL reverse proxy, which terminates the SSL session and then (usually) forwards plain HTTP to back-end servers
- An SSL inspector, which does not terminate the SSL session. Instead, it decrypts a copy of the traffic to scan it for viruses and other security violations. It forwards the original, still-encrypted packet to the back-end web servers.

For both, you must upload the website's certificate and private key, and then specify it in the policy. This allows FortiWeb to decrypt the HTTPS traffic and, in the case of SSL offloading, to offer HTTPS service to clients.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The differences between SSL inspection and SSL offloading are explained on this slide.

- SSL inspection puts the certificate and private key on both FortiWeb and the web servers. However, FortiWeb is not an endpoint for the SSL session; it's one continuous session, from the client to the servers. Clients negotiate with the server, not with FortiWeb. If the traffic is not an attack, FortiWeb allows the packets to continue to their destination.
- SSL offloading only puts the certificate and private key on FortiWeb; clients negotiate the SSL session with FortiWeb, not the web servers. This reduces system load on the web servers. Since the traffic is decrypted before FortiWeb forwards it, FortiWeb can also scan traffic in this mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL Inspection and SSL Offloading (Contd)

- SSL Offloading
  - Inline topologies (reverse proxy)
  - Can inspect contents for viruses and more
  - Improves server performance
    - Uses FortiWeb hardware acceleration for cryptography instead
    - Servers don't use HTTPS unless you've enabled a second HTTPS connection to the back end
  - Supports client PKI authentication
- SSL Inspection
  - Out-of-band (offline) topologies
  - Can inspect contents for viruses and more
  - Does not improve server performance
  - Server still applies HTTPS
  - Supported ciphers vary. See documentation.

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

This slide lists some of the main differences between SSL inspection and SSL offloading.

Remember, despite the name, both enable FortiWeb to inspect HTTPS traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Configure SSL/TLS Offloading

1. Buy certificate or generate certificate signing request (CSR)
   - VeriSign, Comodo, Thawte, http://www.cacert.org/, or AD signed
2. If non-root CA signs, do one of the following:
   - Append signing chain to certificate to demonstrate link with mutually trusted root CA
   - Upload intermediate CA certificates
3. Upload signed certificate and private key to FortiWeb
   - Without private key, FortiWeb cannot establish an encrypted HTTPS session with the client
4. If the client shows their certificate to server to authenticate to, upload CRL/OCSP URL and their CA's certificate
   - Define how to verify and revoke client certificates
5. Choose HTTPS and select certificate+key pair in policy

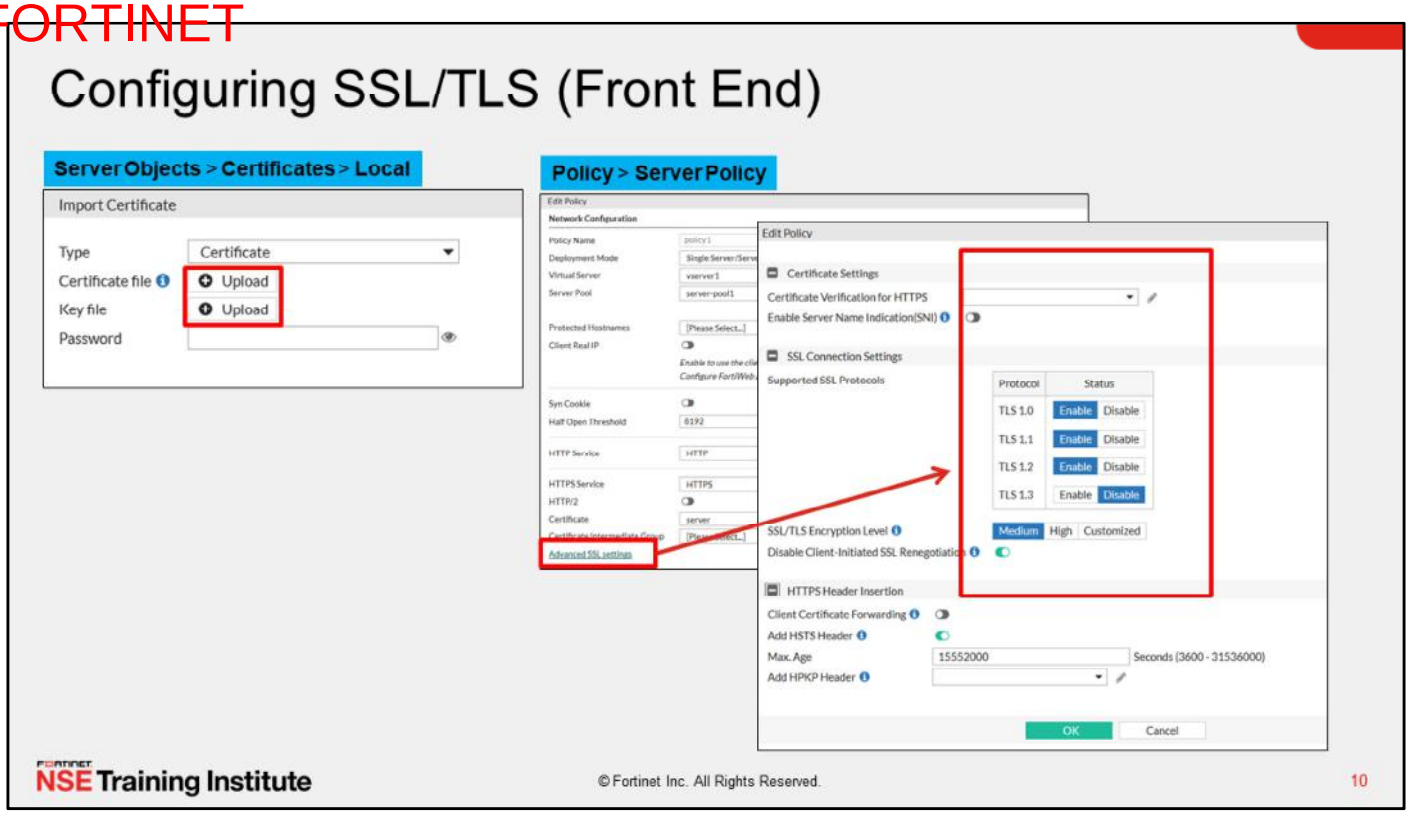
NSE Training Institute © Fortinet Inc. All Rights Reserved. 9

Reverse proxy is the most popular operation mode. In this mode you configure an SSL proxy. These are the configuration steps:

1. Get a signed certificate. If you're an enterprise whose computers all trust your active directory or other CA server, this could be your own private CA. Otherwise, it should be a commercial root CA, so that all browsers will trust your CA-signed certificate.
2. If an intermediate CA signs it, be sure that browsers can link it to a trusted root. Otherwise, include the signing chain in the bottom of the certificate, or as intermediate certificates on FortiWeb.
3. Upload both the signed certificate and its associated private key in the local certificates menu on FortiWeb.
4. PKI authentication is optional. If you want FortiWeb to offer it so that clients, such as iPhones, can log in by showing their personal certificate instead of typing a password, upload those CA certificates and CRL or the address of an OCSP server. This way, FortiWeb will know if any certificates have been revoked.
5. Finally, select your certificate and, if applicable, certificate revocation and validation rules in the policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Let's look at how to configure SSL/TLS offloading on FortiWeb.

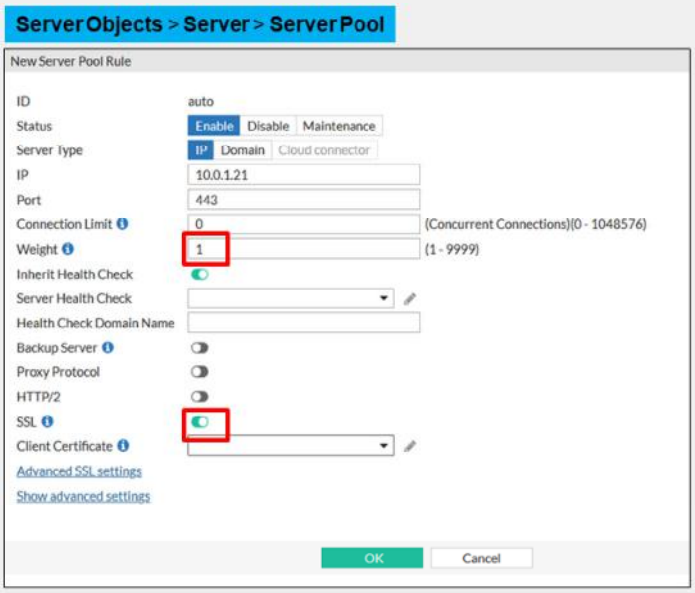
In the simplest case, you need to import the .pem file or a .cert and associated .key file. Then, in the policy, select the predefined HTTPS service, and your certificate. That's it!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Configure SSL/TLS Inspection (TTP/TI/O Mode)

- FortiWeb passes through requests to pool members
- Indicate server's HTTPS listening port
- Enable SSL to trigger inspection
  - True transparent proxy/transparent inspection/offline mode don't support offloading



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

If you're doing SSL inspection in the other operating modes, then, for each server in your server pool, you must also enable the SSL option and define its HTTPS listening port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring SSL/TLS (Back-End and Other Modes)

- In offline and transparent modes, cipher support is determined by back-end web servers, not FortiWeb
- On web servers, disable non-supported ciphers
  - Including ephemeral and anonymous Diffie-Hellman key exchanges
  - Interferes with FortiWeb inspection
- Disable SSL/TLS-level compression
  - BREACH and CRIME vulnerabilities
  - Exploits nature of compression
    - Short codes for repeated blocks of data
    - Repetitive = non-random = can pattern analyze and crack
    - Note: TLS-level compression ≠ GZIP content compression

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

If you're using transparent mode, your back-end web servers must be configured to offer HTTPS. This may be different from reverse proxy—SSL offloading means that the back-end server needs to offer only plain HTTP. So, while transparent mode doesn't require any server-side changes, reverse proxy might.

For better security, you might still want to audit your servers' HTTPS support. Make sure that patches are applied, and that TLS-level compression is disabled. Also, disable any ciphers that FortiWeb doesn't support, and therefore can't inspect.

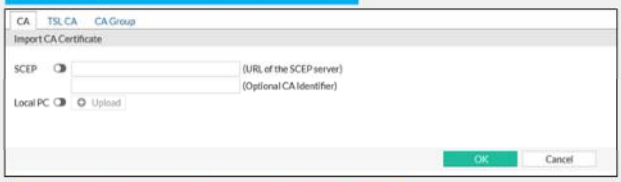
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

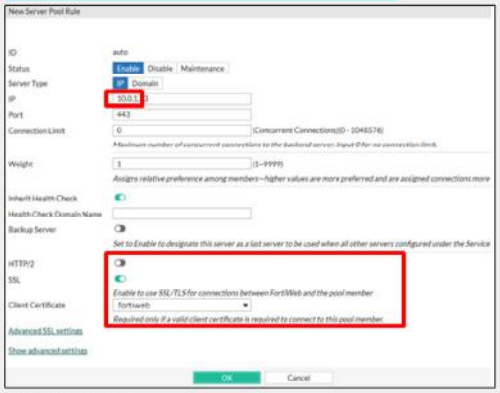
Re-Encryption to Back-End (Reverse Proxy Mode)

- Inspection, not offloading
  - Reverse proxy re-encrypts to back-end servers – FortiWeb must trust server's CA
  - Optionally, as a client to the server, FortiWeb can PKI authenticate itself

Server Objects > Certificates > CA



Server Objects > Server > Server Pool



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

If you want best performance, you should set up FortiWeb for SSL offloading. However, in some cases, such as compliance, where sensitive data must always be encrypted while in transit, you may need FortiWeb to re-encrypt before forwarding data to your web servers. To do this, you'll enable the SSL option for each entry in the server pool.

However, because FortiWeb is acting as a client to your web servers in this second session, you should also upload the certificate of the CA that signed the server certificates. That way, FortiWeb can validate your servers' certificates.

If your web servers require that FortiWeb uses PKI authentication to authenticate itself as a client, this is also where you specify which certificate FortiWeb will present. Again, you'll upload this certificate in the local menu, but this time, its purpose will be different. FortiWeb will present the certificate as a client, not a server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which is a feature of SSL inspection as opposed to SSL offloading?
   - ✓ A. Supports out-of-band (offline) topologies
   - B. Supports client PKI authentication

2. Which device establishes the HTTPS connection to the back-end server in an SSL offloading scenario?
   - A. Client web browser
   - ✓ B. FortiWeb

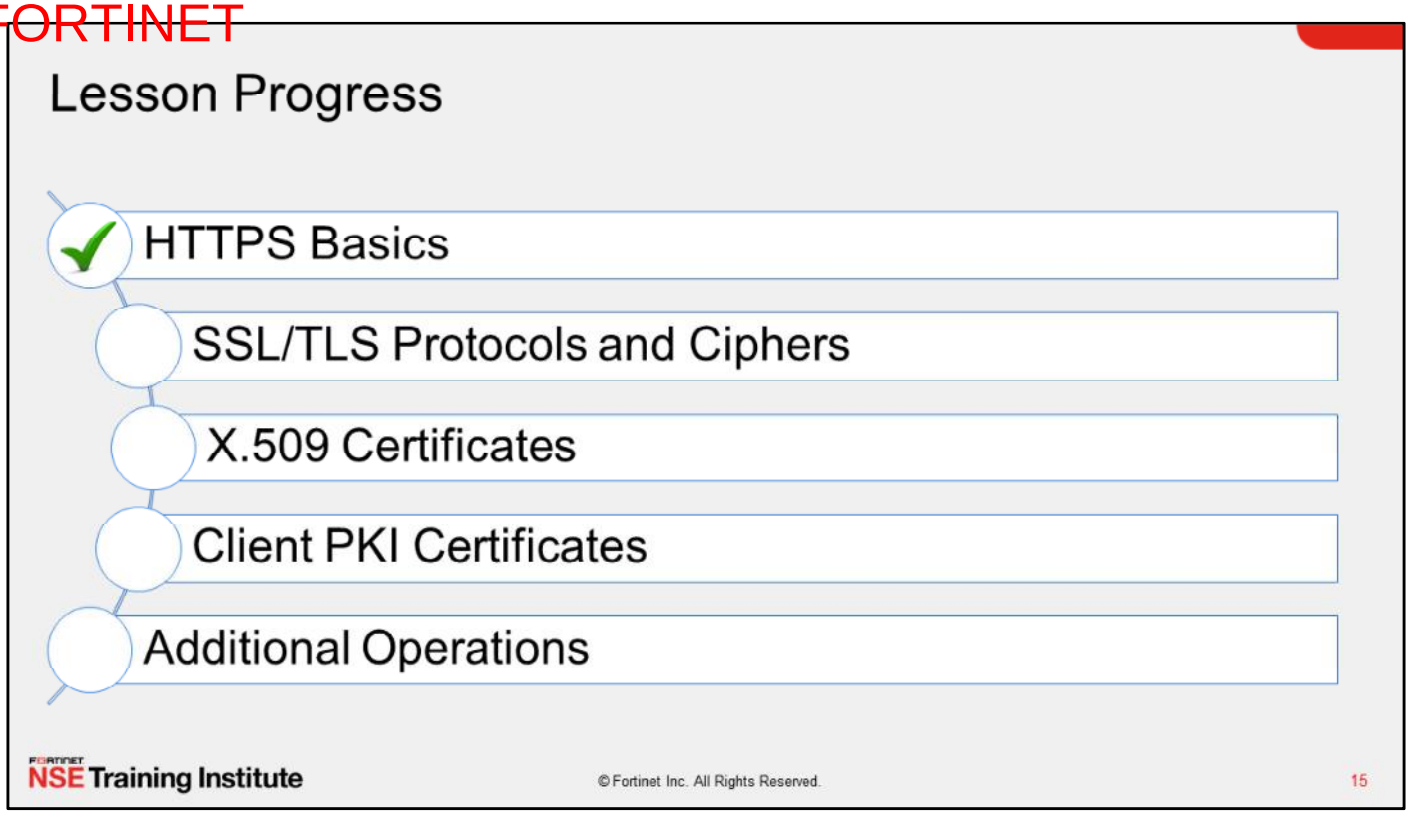
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

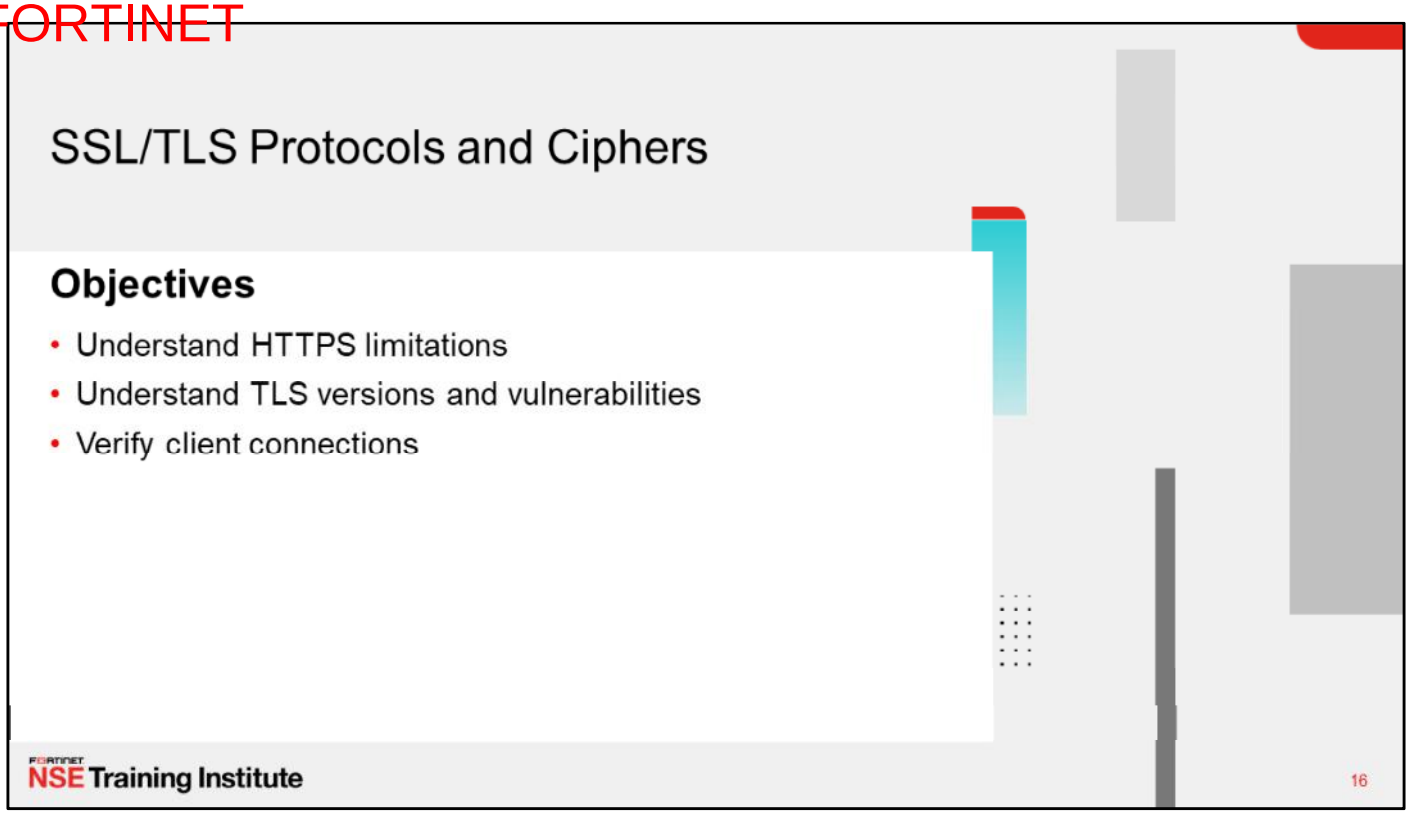


Good job! You are now familiar with HTTPS basics.

Now, you will learn about SSL/TLS protocols and ciphers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



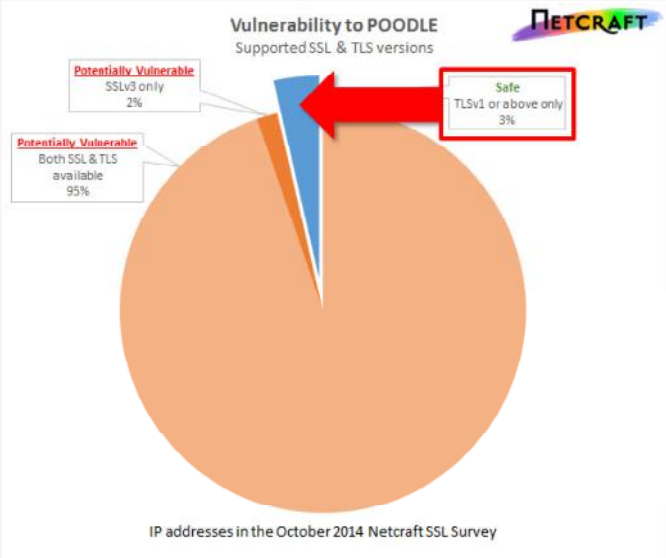
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding SSL/TLS protocols and ciphers, you will be able to use them in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HTTPS Can Have Vulnerabilities



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Enabling HTTPS does not automatically make your website fully secure. Attack signatures and mechanism protections that deal with security once the packet is received are covered in another lesson.

Even in transit, HTTPS is not automatically fully secure. SSL and TLS do have vulnerabilities, so it's important that you configure HTTPS on FortiWeb as securely as you can.

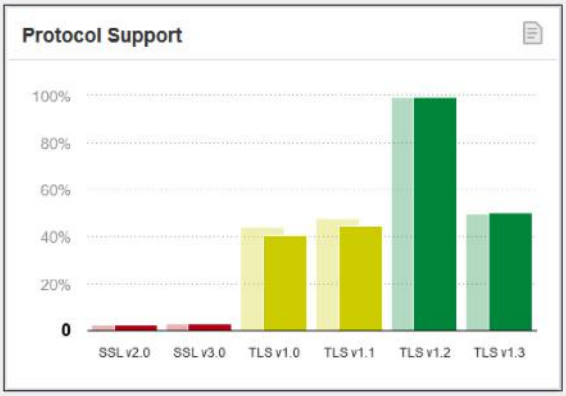
This is a vulnerability, seen in late 2014, that was named POODLE because it exploited padding as an oracle that caused patterns in encrypted packets. These patterns made a crypto-analysis attack possible. Because this was a vulnerability in an implementation of options for older protocols, all servers that supported SSL 2.0 and some that supported SSL 3.0, were vulnerable.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL or TLS?

- FortiWeb Supports TLS 1.0, 1.1, 1.2, and 1.3
- TLS 1.1+ is not backwards compatible with SSL
- Since 2013, many SSL/TLS 1.0 exploits discovered
  - BEAST
  - Lucky 13, CRIME, BREACH
  - Heartbleed, GoToFail
  - POODLE, POODLE for TLS
- NIST now requires USA federal servers to support TLS 1.2, required to support TLS 1.3 by January 2024
  - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/draft
- Many sites still maintain legacy support for TLS 1.0



https://www.ssllabs.com/ssl-pulse/

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

What should these servers have done? First, don't use old SSL protocol versions. Use TLS 1.1 or 1.2, if possible. It is good to support the latest TLS 1.2 and 1.3 protocols but maintaining support for older protocols may leave your webservers at risk.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

TLS 1.2 Support

- TLS 1.2 now supported by all modern browsers
- TLS 1.0/1.1 was be removed from most browsers in 2020 to encourage implementation of TLS 1.2+
- TLS 1.0 is not supported by PCI as of 2018
- After Heartbleed, server adoption of TLS 1.2 was already ≈55%. By August 2014 (up 10% in only one month). By Oct 2016 that was up to 80.7%.
  - https://securityblog.redhat.com/2014/09/10/tls-landscape/
  - https://www.trustworthyinternet.org/ssl-pulse/

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

TLS 1.2 was initially slow to be adopted but is now the standard choice. The Heartbleed SSL vulnerability helped to spur its adoption. Since then, other vulnerabilities in old SSL versions have increased the incentive to upgrade.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Weak Encryption

- Client-side requirement of older protocols now usually less than1%
  - https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/
- SSL 2.0 and MD5 are violations of PCI DSS 3.0 compliance
- Compare with modern strong encryption:
  - TLS 1.1 / 1.2 / 1.3
  - 2,048-bit keys
  - Perfect forward secrecy (PFS)
  - SHA-256 fingerprint
  - AES-256, etc.
  - Secure renegotiation
  - https://wiki.mozilla.org/Security/Server_Side_TLS

NSE Training Institute

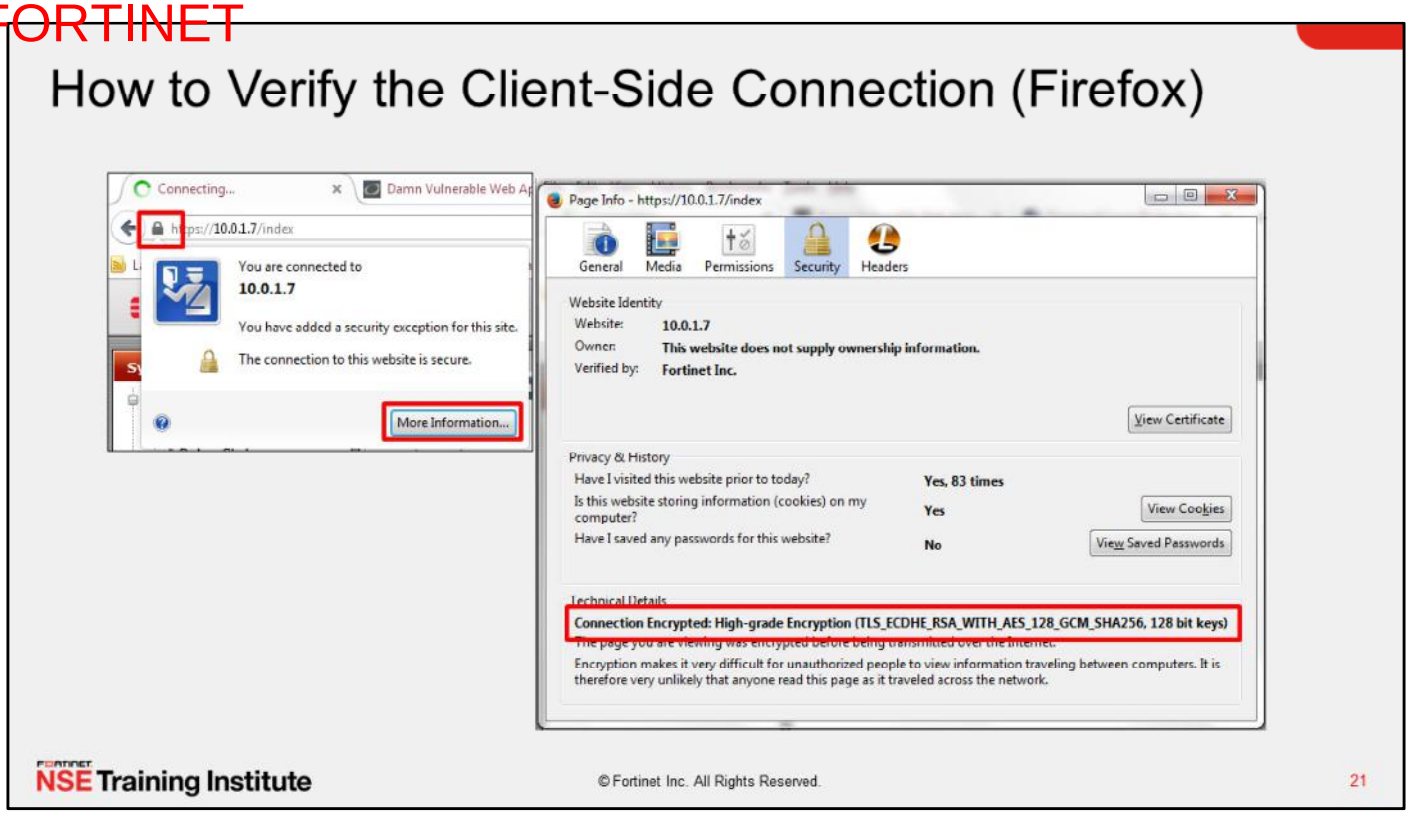
© Fortinet Inc. All Rights Reserved.

20

Weak encryption and checksums, including so-called export-grade encryption are now disabled by default on many browsers. So, reasons to use old, weak encryption are decreasing.

Vouchers & Dumps are Available | WhatsApp +201224560923

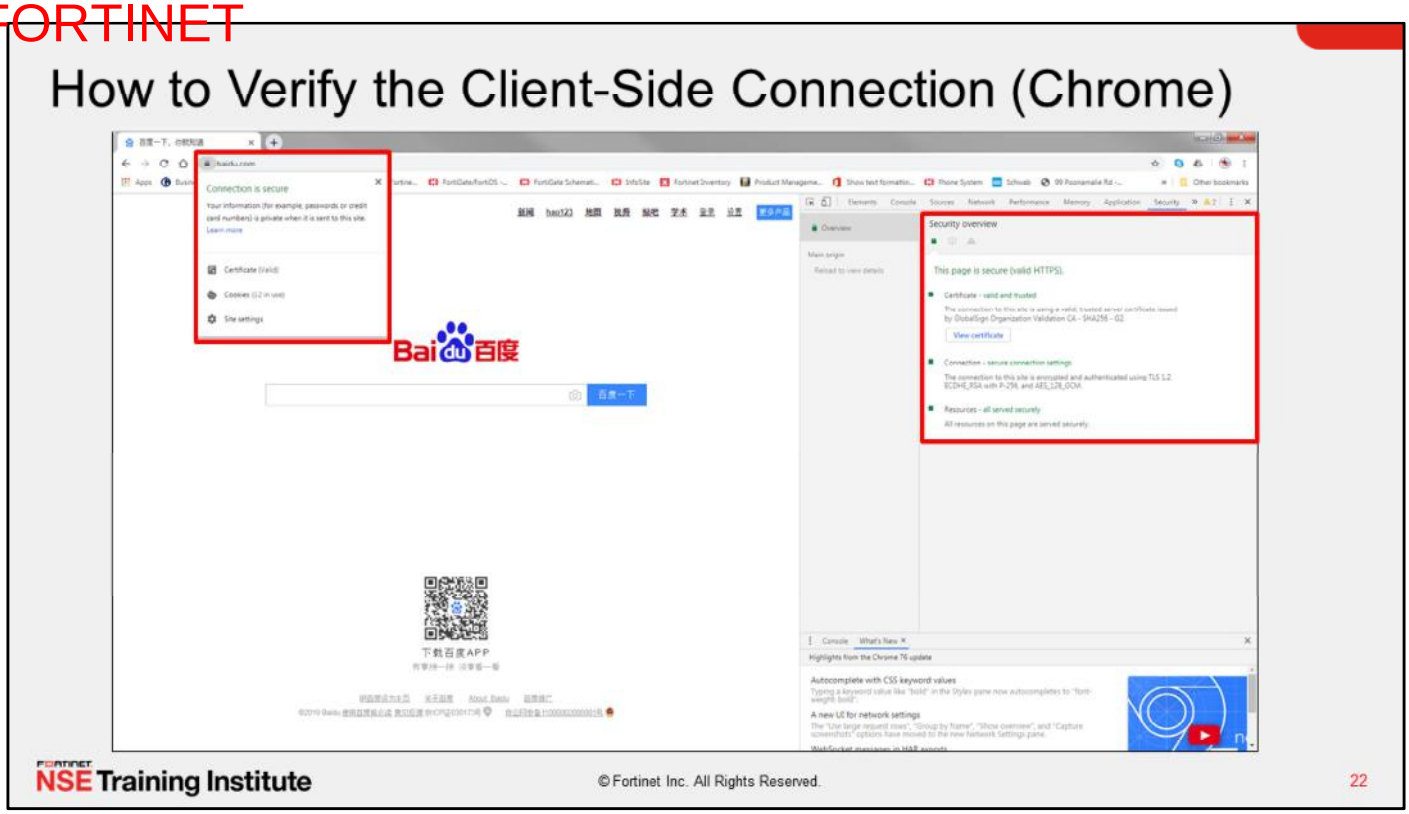
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now that you're aware of some ways to make HTTPS stronger, how can you see what is being used? Client and server (or, for offloading, FortiWeb) will negotiate the protocol and cipher suites that they both support. On the client side, in Firefox and Chrome browsers, you can see the negotiation results. Look for the padlock icon in Firefox's URL bar and click it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In Google Chrome, you also click the padlock to see basic information. For more detailed information, use the `CTRL+SHIFT+I` key combination to open the **Developer Tools** and select the **Security** tab to view the full details.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Verify *Many* Client-Side Connections

```
Air:~ juser$ python sslyze.py --regular www.example.com

 REGISTERING AVAILABLE PLUGINS
 -----------------------------
  PluginHeartbleed
  PluginSessionResumption
  PluginCertInfo
  PluginOpenSSLCipherSuites
  PluginCompression
  PluginHSTS
  PluginSessionRenegotiation
  PluginChromeSha1Deprecation

 CHECKING HOST(S) AVAILABILITY
 -----------------------------
   www.example.com:443                 => 10.0.1.8:443

 SCAN RESULTS FOR WWW.EXAMPLE.COM:443 - 10.0.1.8:443
 ---------------------------------------------------
  * Session Renegotiation:
      Client-initiated Renegotiations:   OK - Rejected
      Secure Renegotiation:              OK - Supported
  * Deflate Compression:
      OK - Compression disabled
Unhandled exception when processing --heartbleed:
utils.SSLyzeSSLConnection.SSLHandshakeRejected - TCP / Received RST
  * Session Resumption:
      With Session IDs:                  OK - Supported (5 successful, 0 failed, 0 errors, 5 total
attempts).
      With TLS Session Tickets:          NOT SUPPORTED - TLS ticket not assigned.
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 23

Unfortunately, there is no easy way to verify client connections to Internet Explorer. However, there are still ways that you can test for robust client support. This is one way to test: a Python script called sslyze. As you can see from the slide, the script checks for several vulnerabilities, such as Heartbleed and insecure renegotiation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Verify *Many* Client-Side Connections (Contd)

```
* Certificate - Trust:
    Hostname Validation:                OK - Common Name matches
    "Mozilla NSS - 08/2014" CA Store:   FAILED - Certificate is NOT Trusted: self signed certificate
    "Microsoft - 08/2014" CA Store:     FAILED - Certificate is NOT Trusted: self signed certificate
    "Apple - OS X 10.9.4" CA Store:     FAILED - Certificate is NOT Trusted: self signed certificate
    "Java 6 - Update 65" CA Store:      FAILED - Certificate is NOT Trusted: self signed certificate
    Certificate Chain Received:         ['www.example.com']

* Certificate - OCSP Stapling:
    NOT SUPPORTED - Server did not send back an OCSP response.

* SSLV2 Cipher Suites:
    Server rejected all cipher suites.

*TLSV1_2 Cipher Suites:
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 200 OK

    Accepted:
              ECDHE-RSA-AES256-SHA384       ECDH-256 bits  256 bits      HTTP 200 OK
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 200 OK
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 200 OK
              DHE-RSA-CAMELLIA256-SHA       DH-1024 bits   256 bits      HTTP 200 OK
              DHE-RSA-AES256-SHA256         DH-1024 bits   256 bits      HTTP 200 OK
              DHE-RSA-AES256-SHA            DH-1024 bits   256 bits      HTTP 200 OK
              DHE-RSA-AES256-GCM-SHA384     DH-1024 bits   256 bits      HTTP 200 OK
              CAMELLIA256-SHA               -              256 bits      HTTP 200 OK
              AES256-SHA256                 -              256 bits      HTTP 200 OK
              AES256-SHA                    -              256 bits      HTTP 200 OK
              AES256-GCM-SHA384             -              256 bits      HTTP 200 OK
              ECDHE-RSA-AES128-SHA256       ECDH-256 bits  128 bits      HTTP 200 OK
              ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 200 OK
              ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits      HTTP 200 OK
              DHE-RSA-CAMELLIA128-SHA       DH-1024 bits   128 bits      HTTP 200 OK
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

The sslyze script also checks for certificate validation errors, and which protocols and cipher suites that the server (or FortiWeb) supports. The example on this slide shows that FortiWeb has been configured for somewhat higher security—it is offering TLS 1.2 with 256-bit AES, RSA keys, and SHA-384 checksums. But its certificate for `www.example.com` is self-signed, so browsers will show error messages. This misconfiguration should be corrected before being used on a production network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Verify *Many* Client-Side Connections (Contd)

```
DHE-RSA-AES128-SHA256          DH-1024 bits   128 bits      HTTP 200 OK
DHE-RSA-AES128-SHA             DH-1024 bits   128 bits      HTTP 200 OK
DHE-RSA-AES128-GCM-SHA256      DH-1024 bits   128 bits      HTTP 200 OK
CAMELLIA128-SHA                -              128 bits      HTTP 200 OK
AES128-SHA256                  -              128 bits      HTTP 200 OK
AES128-SHA                     -              128 bits      HTTP 200 OK
AES128-GCM-SHA256              -              128 bits      HTTP 200 OK
ECDHE-RSA-DES-CBC3-SHA         ECDH-256 bits  112 bits      HTTP 200 OK
EDH-RSA-DES-CBC3-SHA           DH-1024 bits   112 bits      HTTP 200 OK
DES-CBC3-SHA                   -              112 bits      HTTP 200 OK
TLSV1_1 Cipher Suites:
      Preferred:
                 ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 200 OK
      Accepted:
                 ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 200 OK
                 DHE-RSA-CAMELLIA256-SHA       DH-1024 bits   256 bits      HTTP 200 OK
                 DHE-RSA-AES256-SHA            DH-1024 bits   256 bits      HTTP 200 OK
                 CAMELLIA256-SHA               -              256 bits      HTTP 200 OK
                 AES256-SHA                    -              256 bits      HTTP 200 OK
                 ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 200 OK
                 DHE-RSA-CAMELLIA128-SHA       DH-1024 bits   128 bits      HTTP 200 OK
                 DHE-RSA-AES128-SHA            DH-1024 bits   128 bits      HTTP 200 OK
                 CAMELLIA128-SHA               -              128 bits      HTTP 200 OK
                 AES128-SHA                    -              128 bits      HTTP 200 OK
                 ECDHE-RSA-DES-CBC3-SHA        ECDH-256 bits  112 bits      HTTP 200 OK
                 EDH-RSA-DES-CBC3-SHA          DH-1024 bits   112 bits      HTTP 200 OK
                 DES-CBC3-SHA                  -              112 bits      HTTP 200 OK

  * TLSV1 Cipher Suites:
      Server rejected all cipher suites.

  * SSLV3 Cipher Suites:
      Server rejected all cipher suites.

 SCAN COMPLETED IN 7.57 S
 ------------------------
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

SSL scans like this can be very useful to prepare for security audits, as well as when you need to analyze client compatibility, because it can quickly check all of your configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which protocol should not be used because of known security vulnerabilities?
   A. TLS 1.2
   ✓ B. SSL 3.0
   C. TLS 2.0

2. Which HTTPS encryption protocol is the most widely adopted as of 2021?
   A. TLS 1.1
   B. RC4
   ✓ C. TLS 1.2
   D. SSL 3.0

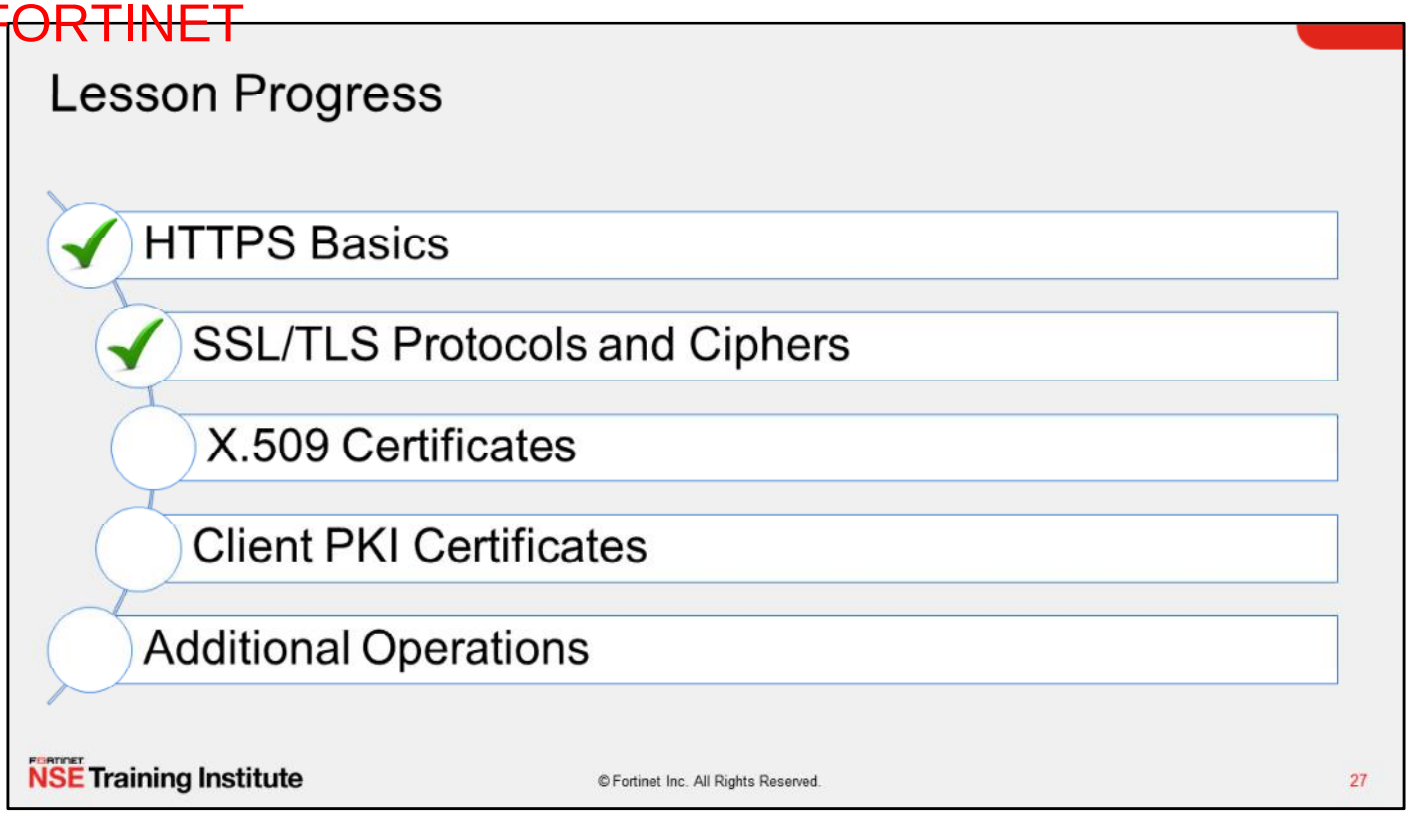
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

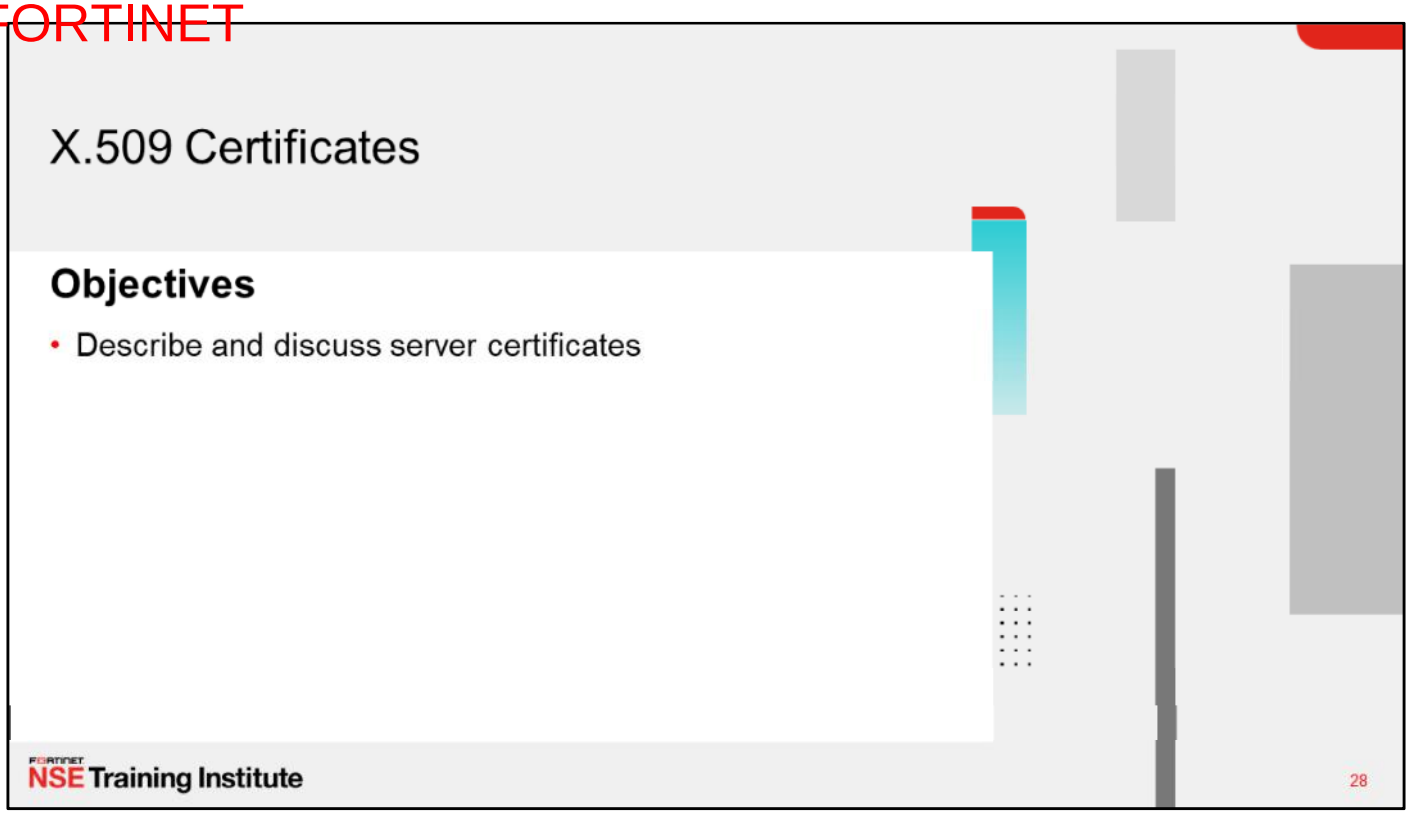


Good job! You now have an understanding of SSL/TLS protocols and ciphers.

Now, you will learn about X.509 certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding certificates, you will be able use them effectively in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

When Does FortiWeb Use Certificates?

- FortiWeb requires its own certificate and private key if:
  - You connect to the GUI through HTTPS
    - FortiWeb presents its server certificate to your browser
    - Built-in factory certificate by default
  - FortiWeb makes a secondary HTTPS connection to back-end servers and you configure it to authenticate as a client (reverse proxy only)
    - FortiWeb presents its client certificate to the back-end server
    - Certificate should have an IP or host name, whichever connects to back-end

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

Aside from protocol versions and cipher suites, the other major component of HTTPS is X.509 certificates.

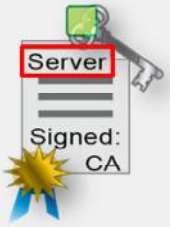
FortiWeb uses several kinds of X.509 certificates. It uses its own, built-in, default, self-signed server certificate when you open your browser and connect to the GUI. FortiWeb may also need its own certificate, if you want it to use PKI authentication as a client to your back-end severs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

When Does FortiWeb Use Certificates? (Contd)

- FortiWeb requires the *websites'* certificates and private keys for:
  - SSL/TLS offloading (reverse proxy only)
    - HTTPS disabled on back-end web server
  - SSL/TLS inspection (reverse proxy, transparent modes, and offline protection)
    - In reverse proxy, can re-encrypt, make second HTTPS connection to back-end
    - HTTPS *not* disabled on server; server must also do encryption
    - Usually required by PCI and other standards that require keeping card data encrypted in transit
- Keep private keys physically secure and encrypted—including in FortiWeb backups! Compromised keys are a serious security risk
  - Base64 encoding is *not* encryption
  - If compromised, CA must immediately revoke certificate
  - Attackers can mimic you until the certificate is revoked
  - You must redeploy all new certificates



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

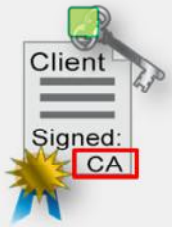
In most cases, since FortiWeb is a proxy, it will be acting as an agent for your websites. So, it will present the websites' certificates when a client connects. Since FortiWeb needs the private key to be able to encrypt and decrypt traffic, be sure to store your FortiWeb backups in a secure location. Like all backups of your private key, physical access to your private key should be tightly restricted to a few authorized individuals, and backups should be password encrypted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

When Does FortiWeb Use Certificates? (Contd)

- CA certificates to verify:
  - CA signature on clients' PKI certificates
  - CA signature on servers' certificates
    - back-end HTTPS servers present their certificate if you configure re-encryption
    - LDAPS queries
    - SMTPS/SMTP over TLS alert email
- FortiWeb uses Online Certificate Status Protocol (OCSP) and revocation lists to verify that certificates are valid



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

What other certificates do you need to upload to FortiWeb?

CA certificates are important for certificate validation. FortiWeb must validate certificates in two cases:
- When a client sends a personal certificate for PKI authentication
- When FortiWeb connects to an OCSP, LDAPS, back-end HTTPS, or secure email server

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How Clients Trust a Certificate

1. Get signed certificate from CA that client trusts
   - VeriSign, Comodo, Thawte, OpenTrust, and so on, in browsers' default stores
2. Upload signed certificate and private key to FortiWeb
3. Select in policy and server pool
4. If host names match and client trusts that CA, they will trust your certificate; otherwise, append chain of CAs showing your link to a trusted CA

- If signed by your own private CA, you must install that CA's certificate in all clients' trust stores
  - Typical in enterprise PKI or development servers
  - Not public internet because of to deployment difficulty
    - Otherwise they can't verify the signature on certificate presented by FortiWeb
    - Causes HTTPS error messages — a cause of *click-through insecurity*
    - People permanently add exceptions just to avoid the security dialog

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

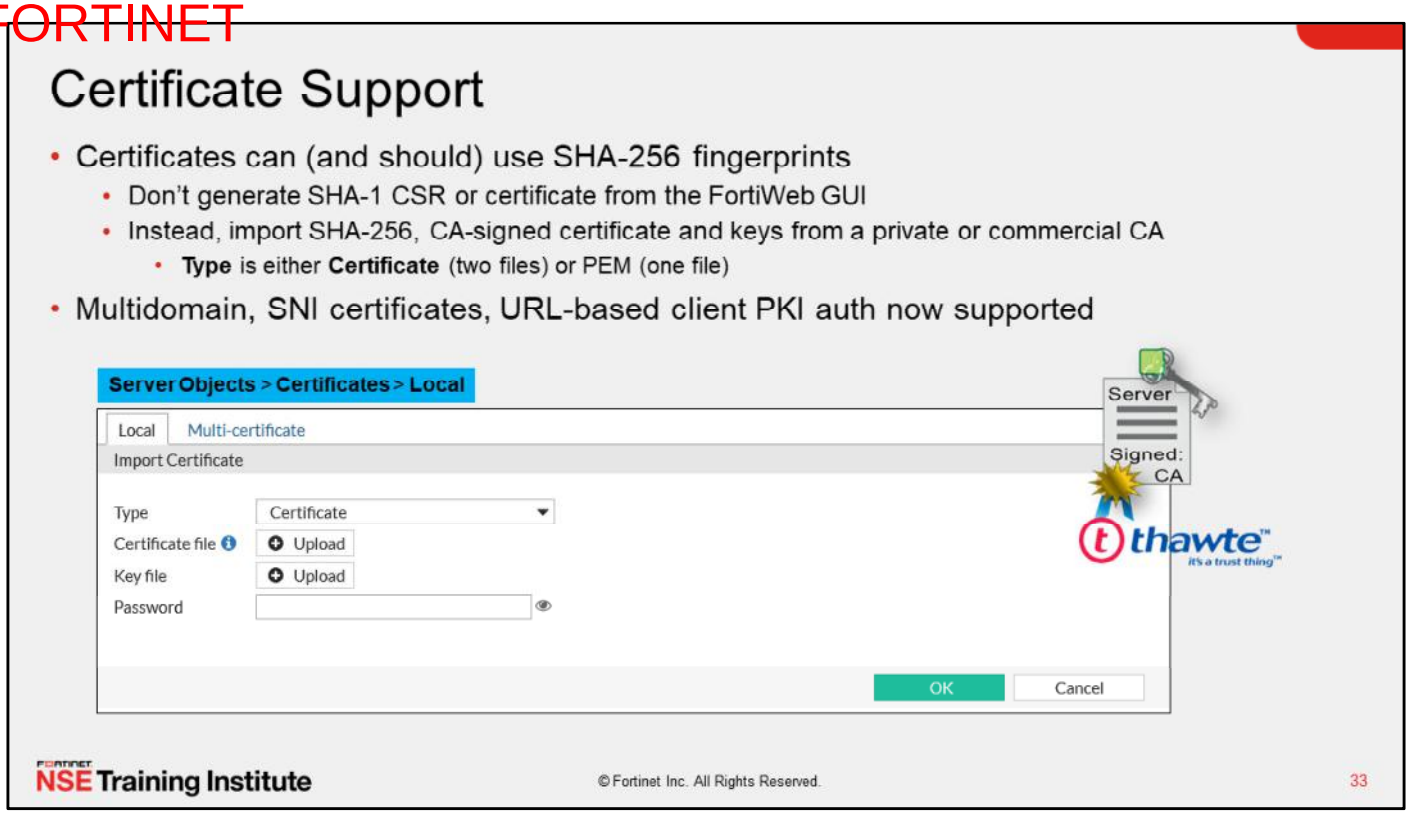
32

Like web browsers, when FortiWeb evaluates a certificate, it will examine the same factors:

- Does the IP address or host name in the certificate match exactly?
- Is it currently valid, not expired, or pending a future time or date?
- Is it signed by a CA that I trust?
- If X.509 extensions exist, such as restricting certificate usage to signing other certificates or as server authentication, is the certificate being used in a valid context?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For CA signatures to be truly trustworthy, it's important that an attacker can't use collision attacks. Collision attacks allow the attackers to mimic the CA's fingerprint, so it's better to use certificates with SHA-256 or greater.

FortiWeb now supports many new certificate-related features, including multi-domain certificates, SNI, and URL-specific contexts for requiring client PKI authentication. Take a look at what this enhanced support allows you to do.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Host Names and Certificates

- Defines virtual and real web hosts according to the `Host:` field inside the HTTP header
  - Example: Apache virtual host

```
GET /index.php HTTP/1.1
Host: www.example.com
```

- Usually must *exactly* match name in SSL/TLS certificate
  - Wildcard certificates (*.example.com) *not* recommended by OWASP
    - Violates principle of least privilege
  - Instead, use a multiple domain certificate, an X.509 certificate extension with list of specific matching domains in the **Subject Alternative Name** field
    - `www.example.com`
    - `store.example.com`
    - `blog.example.com`

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

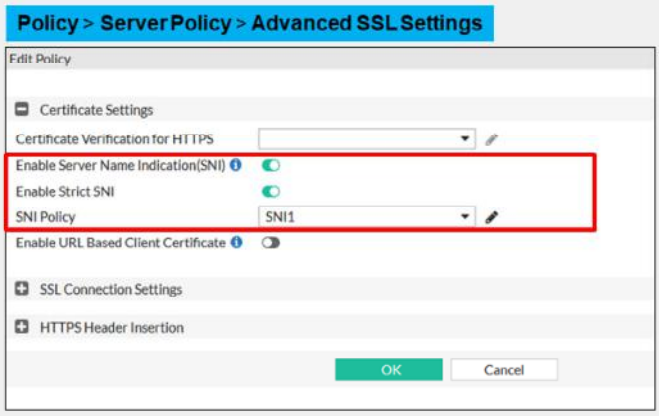
Multidomain certificates mean you don't have to use a wildcard certificate when multiple host names are being protected by the same FortiWeb policy. Wildcard certificates are considered by the Open Web Application Security Project (OWASP) to be less secure. Instead, you can use a SAN certificate extension field to list additional specific host names that are under your control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Name Indication (SNI)

- FortiWeb gives certificate matching host: in client's request
  - Useful for virtual hosts: multiple host names on one public IP
- **Enable Strict SNI** disabled: fall back to certificate if no match exists in SNI list
- **Enable Strict SNI** enabled: use SNI list only



NSE Training Institute

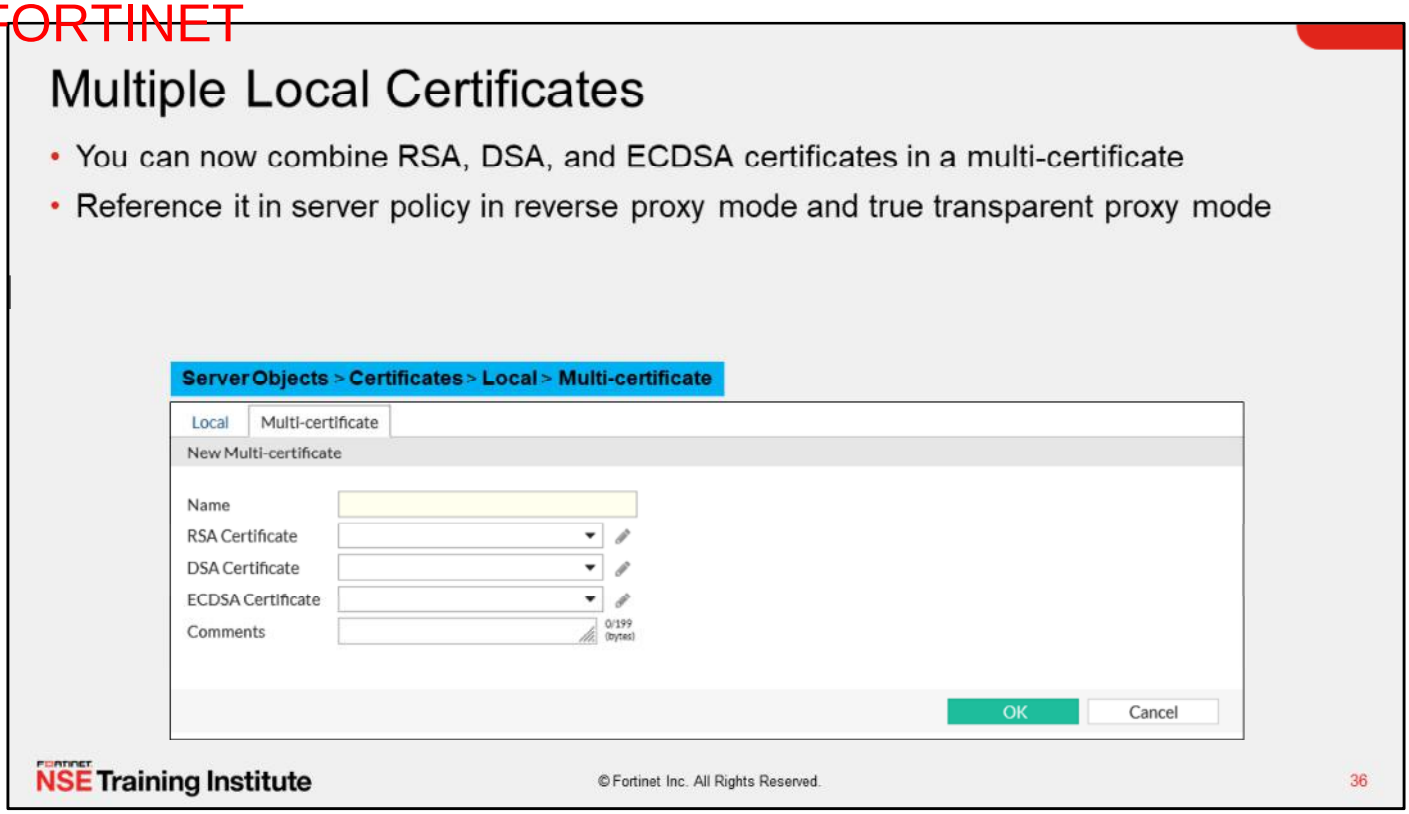
© Fortinet Inc. All Rights Reserved.

35

SNI enables a FortiWeb virtual server to offer different certificates, depending on the host name requested by the client. Like many other objects on FortiWeb, you must configure an SNI list, then select it in the server policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb now supports the use of multiple local certificates for SSL offloading.

After importing or generating individual certificates, you can create a multi-certificate. This multi-certificate can contain up to one of each RSA, DSA, and ECDSA certificates. You can then reference this multi-certificate in the server policy.

This is currently only supported in reverse proxy, and true transparent proxy modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. In which case does FortiWeb use its own local certificate to identify itself?
   A. HTTPS connection to clients when protecting a webserver
   ✓ B. Administrative access to GUI with HTTPS
   C. Connection to the webserver with SSL offloading

2. Which device is identified by the certificate used by FortiWeb in SSL offloading?
   ✓ A. Web server
   B. FortiWeb
   C. CA server

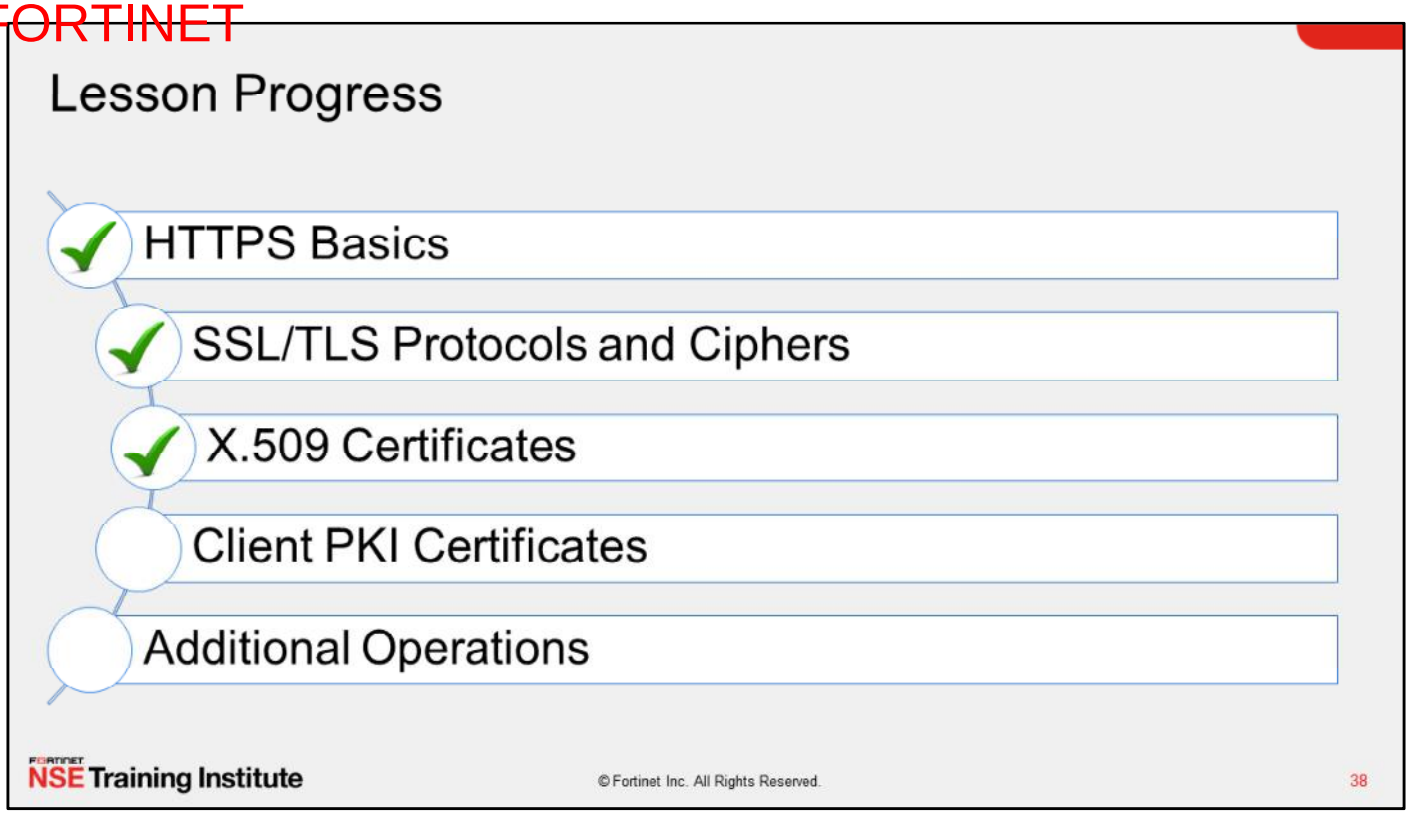
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

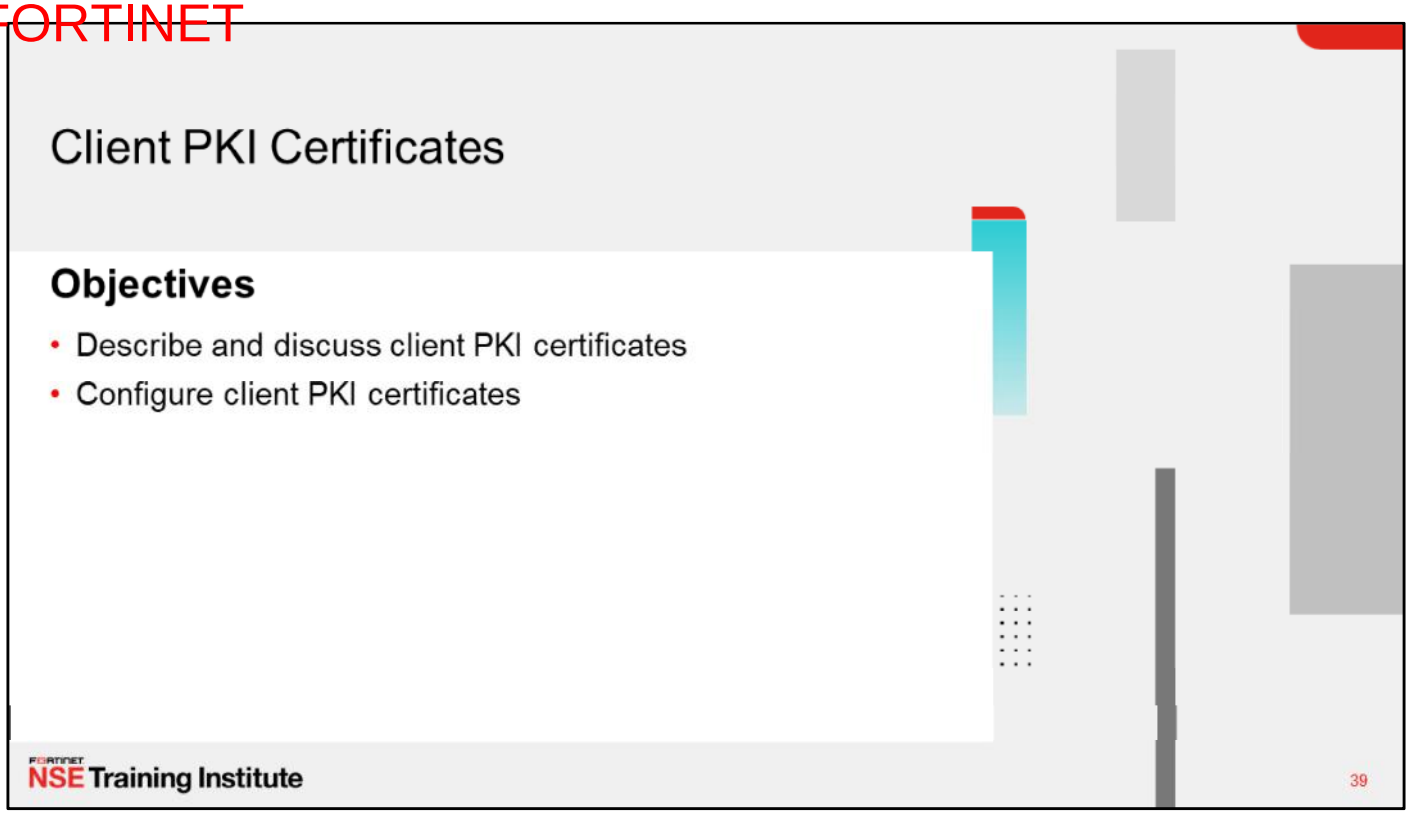


Good job! You now know more about X.509 certificates.

Now, you will learn about client PKI certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

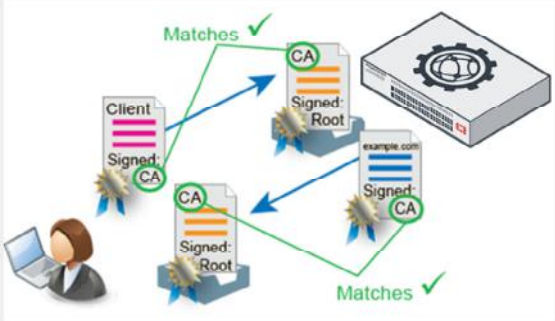
By demonstrating competence in understanding and configuring PKI certificates, you will be able use them effectively in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PKI Authentication

- Common with enterprise smartphone deployments
  - Passwords are hard to type on small keys and touch screens
  - Example: administrator through iPhone profile manager loads certificates and enterprise CA onto employee's phone
- Both client and server show their certificates during HTTPS handshake
  - Mutual or bilateral authentication
- Cryptographic key is stronger than only a simple password
- FortiWeb supports if SSL offloading
- FortiWeb can also be a PKI client to back-end HTTPS servers



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

Passwords have many problems. They are hard to remember, and usually easy to crack. But they are also hard to reliably type on touch-screen devices.

If most of your website's users (or a critical segment of them) use touch screens, and if they are managed by your organization, then it may be both more user-friendly and more secure to authenticate them using personal certificates instead. For example, the administrator could use the Apple iPhone profile manager to install both your enterprise's CA certificate and the personal certificate on the phone. Then, every time that person accessed the website, they would be securely and effortlessly authenticated.

During an HTTPS handshake, the server (or in the case of SSL offloading, FortiWeb) first presents its certificate. The client validates it. However, the client can, optionally, present their own certificate for the server to validate. This is why it's also called *mutual authentication* or *bilateral authentication*.

FortiWeb can also authenticate as a client. If it uses HTTPS to connect to the back-end web servers, it can present its own certificate to authenticate as a client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Uploading CA Certificates

- FortiWeb does not know or trust any CAs *until* you upload at least one CA certificate
  - Until then, FortiWeb can't validate a client's certificate
  - All of those secure connections will fail

NSE Training Institute

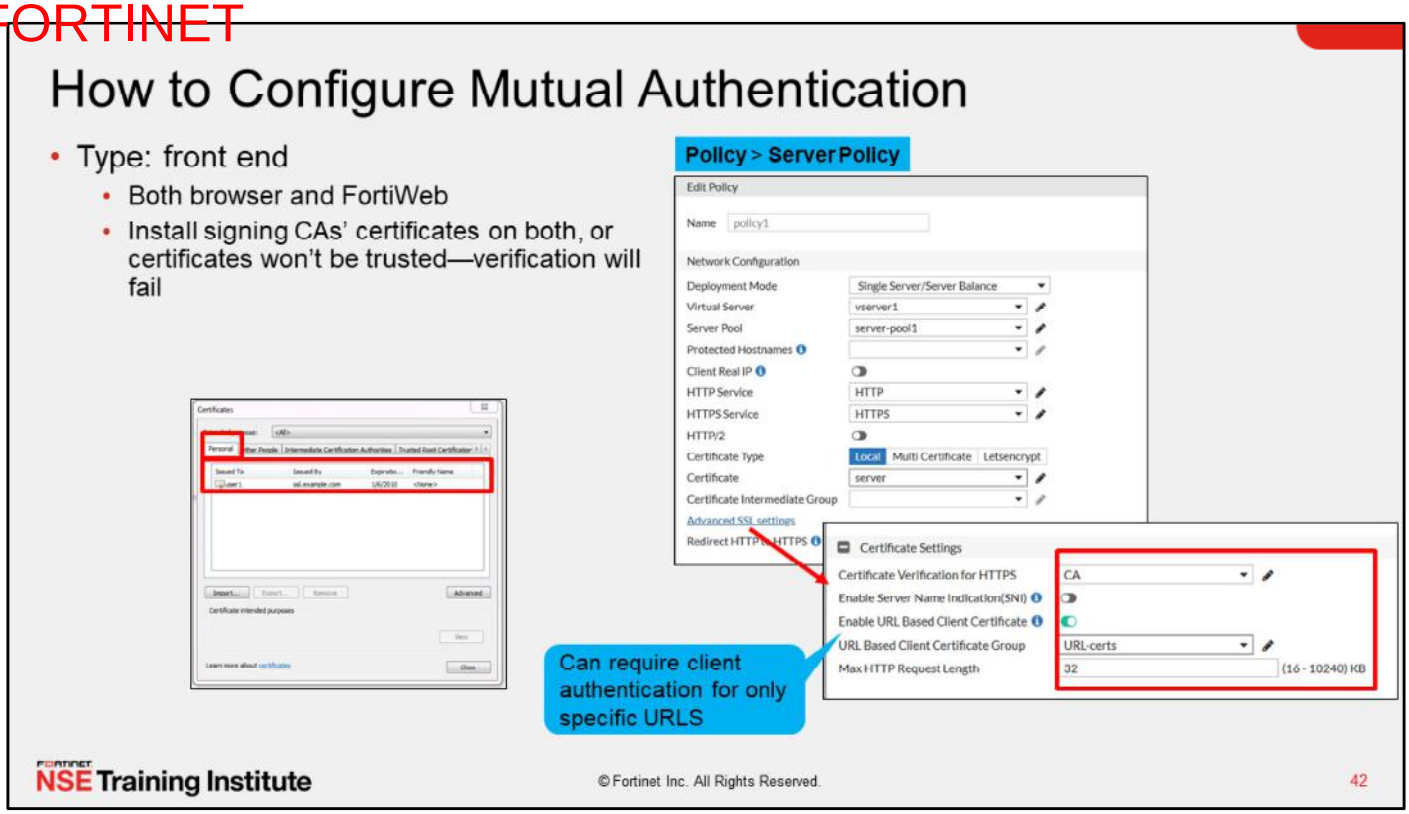
© Fortinet Inc. All Rights Reserved.

41

In order for client PKI authentication to work, you must upload the certificate of the CA that signed the personal certificates. By default, FortiWeb doesn't trust any CAs. So, if you don't upload any, FortiWeb won't validate any clients' certificates. You'll also need to configure a certificate validation rule on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



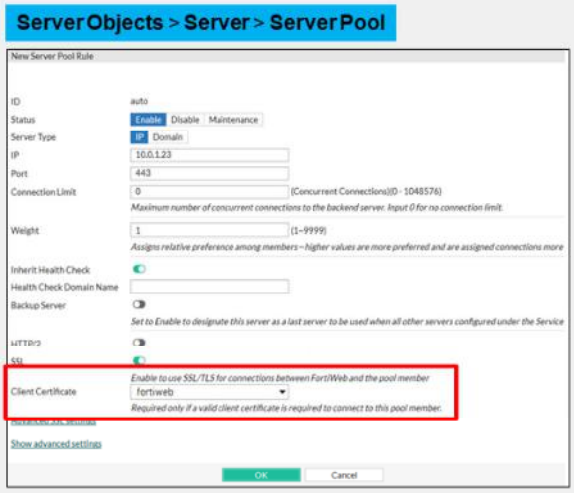
If you're configuring mutual authentication for the SSL session on the front end, you must do it on both the client browser *and* FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Configure Mutual Authentication (Contd)

- Type: back-end
  - Both FortiWeb and server
  - Install signing CAs' certificates on both
  - Otherwise both won't trust each other's certificates — verification will fail



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
43

If you're configuring mutual authentication with the protected web servers behind FortiWeb, they may already be installed with a store of trusted CA certificates. In that case, you'll only need to configure FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When is PKI authentication usually used?
   A. Whenever credit card information is involved
   B. When mobile devices are managed by businesses ✓
   C. When standards require two factor authentication

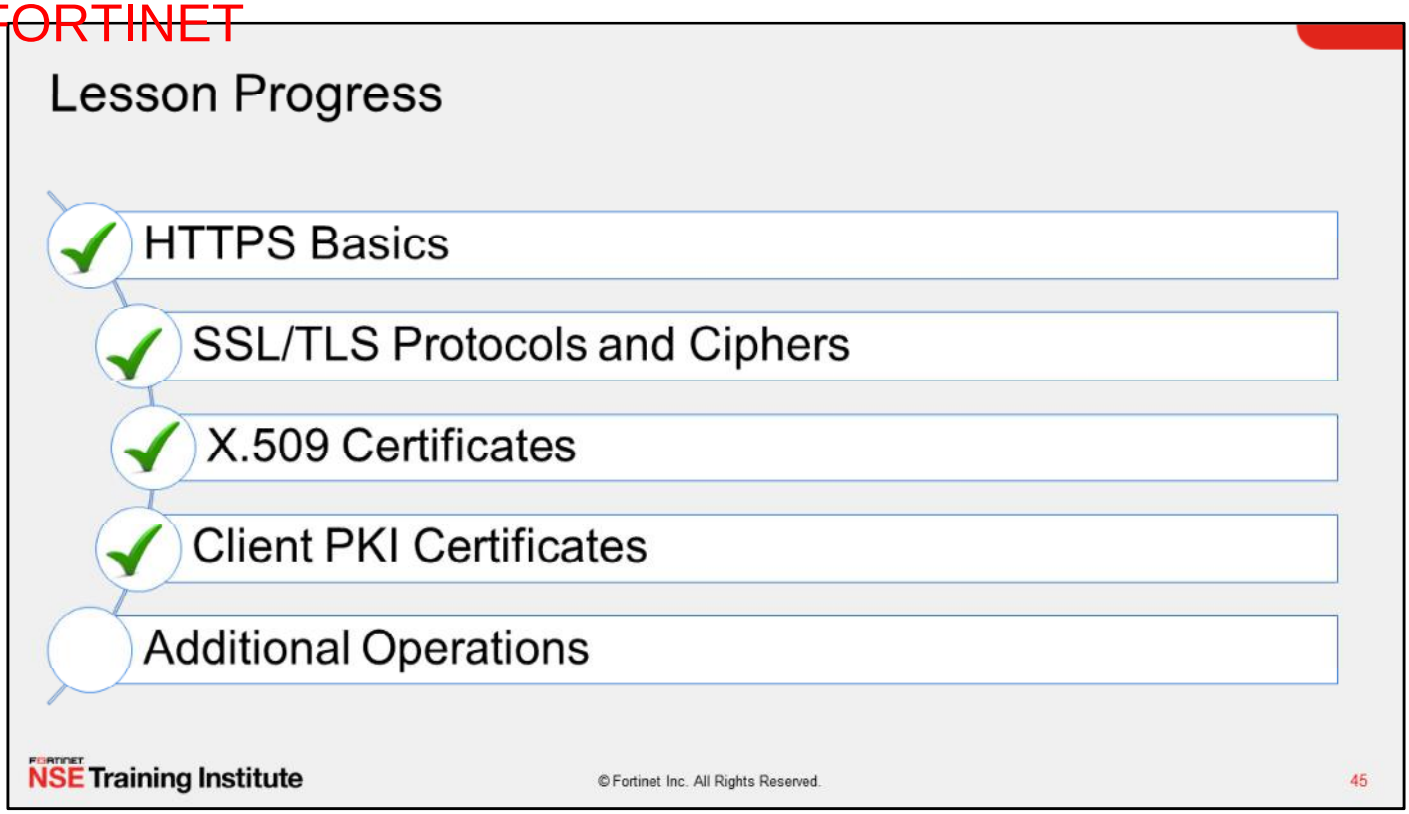
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

44

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

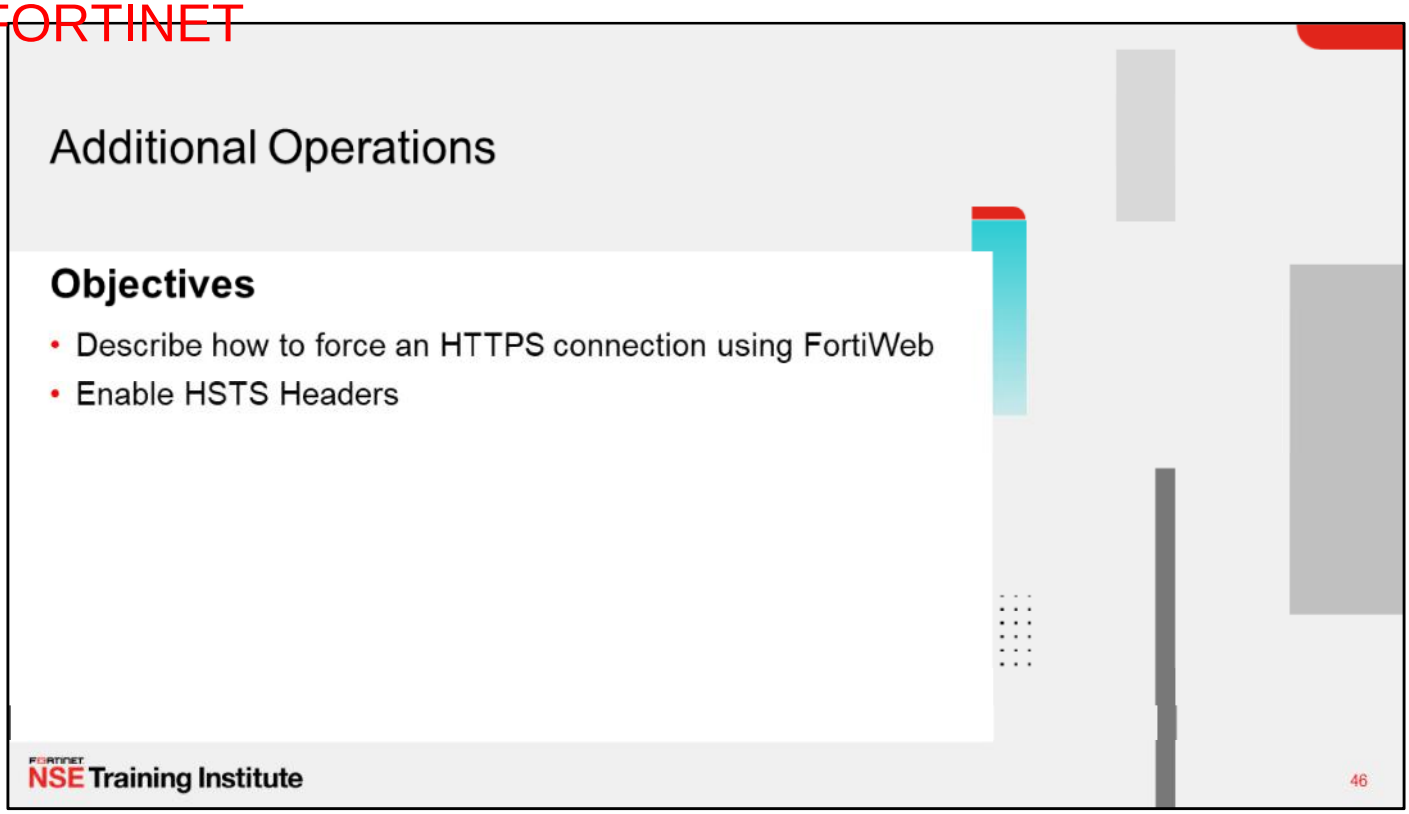


Good job! You now know how to implement and use client PKI certificates on FortiWeb.

Now, you will learn what to do if a user types `HTTP` instead of `HTTPS`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring additional operations, you will be able to direct users who make incorrect entries in their browsers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Redirecting HTTP to HTTPS

- Often used by banks
- If users don't know HTTPS is available and beneficial, server can reply with a 301 HTTP code
  - Says site has moved to HTTPS URL
- Client makes automatic second request to HTTPS site
- MiTM attack (SSL Strip) is possible during HTTP-to-HTTPS redirect

NSE Training Institute © Fortinet Inc. All Rights Reserved. 47

Regardless of whether your servers or FortiWeb offer HTTPS, there is no way that you can prevent a client from typing `http://` into their browser. And, it's a common habit for most people. Unless they're technical, they may not know the difference.

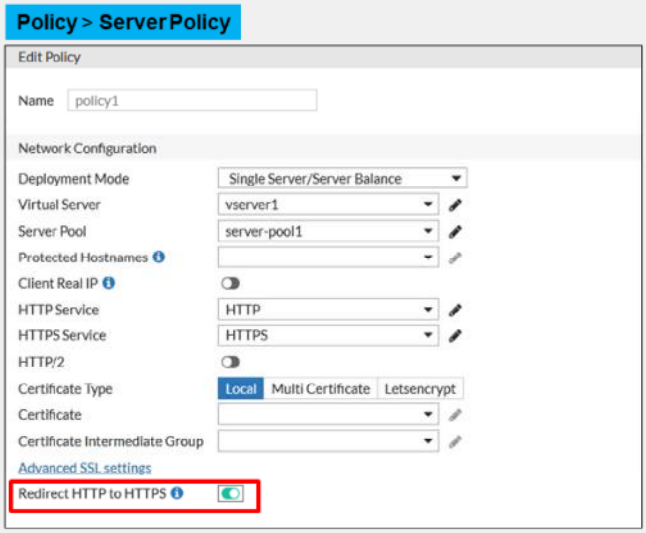
How can you protect these clients?

The most common method is to simply use HTTP's redirect mechanisms to send clients to the secure site. But it's not ideal. SSL stripping attacks are possible.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Redirecting HTTP to HTTPS



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

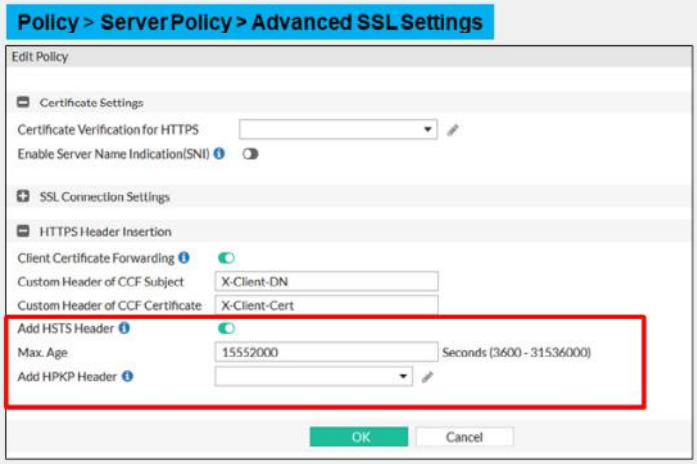
FortiWeb can automatically use HTTP 301 redirects in the server policy. This will respond to any HTTP requests with a redirect to the same site using HTTPS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Enforcing Encryption—HSTS Header

- Browsers except IE have some HTTPS-only domains hard-coded
  - https://www.twitter.com
  - https://google.com/
- But there are strict requirements https://hstspreload.appspot.com/
  - All subdomains, CDN HTTPS-only
  - Difficult for many sites
- Alternative: HSTS header
- An HSTS header forces HTTPS in future
  - Client cache
  - Has Max. Age
  - If client can't validate certificate, also a fatal connection error (RFC 6796)
    - Client's web browser won't show any override dialog that allows the user to ignore mismatch error and continue
    - No click-through insecurity



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

49

It's better to enforce strict transport security. If you enable it, FortiWeb can add an HSTS header so that in the future, the browser will automatically converts HTTP addresses to their HTTPS equivalent, before making the request. It will also suppress dialog boxes that allow users to ignore certificate warnings, a common source of so-called click-through insecurity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Strict Transport Security Header

- Valid for one year
- The client will always automatically use a HTTPS redirect

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 Feb 2015 18:29:36 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: close
Vary: X-Mobile, User-Agent
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

50

This slide shows a reply from a web server where FortiWeb has injected the `Strict-Transport-Security:` header.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

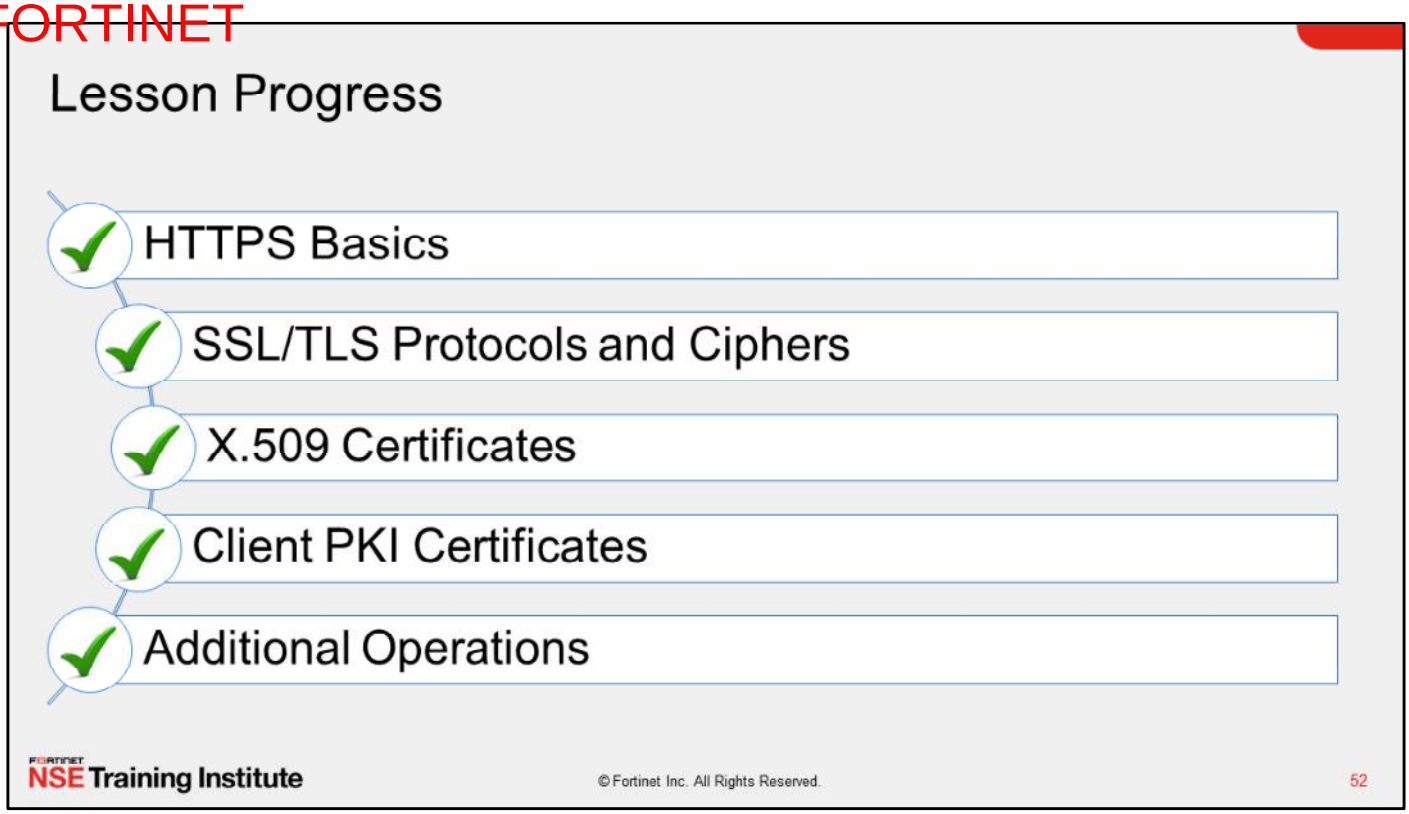
Knowledge Check

1. Which HTTP response code is used to initiate a redirect form HTTP to HTTPS?
   A. 500
   ✓ B. 301

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
51

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have successfully completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Discuss why you should use HTTPS
- ✓ Comparing SSL inspection to SSL offloading
- ✓ Configure SSL offloading
- ✓ Configure SSL inspection
- ✓ Understanding HTTPS limitations
- ✓ Understanding TLS versions and vulnerabilities
- ✓ Describe and discuss server certificates
- ✓ Configure client PKI certificates
- ✓ Configure additional operations

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

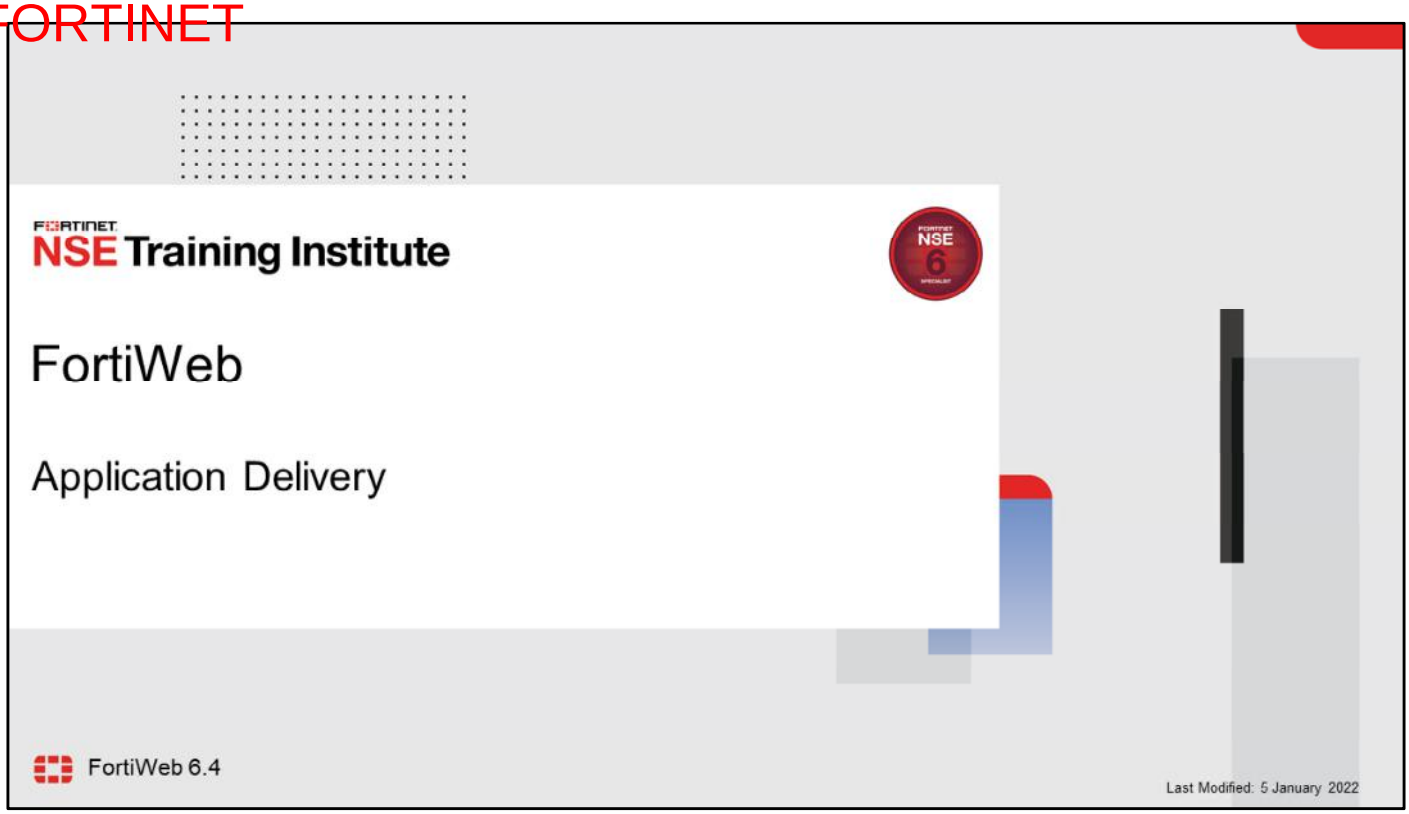
53

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use encrypted HTTP transactions to protect login credentials and other sensitive data that travels through your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

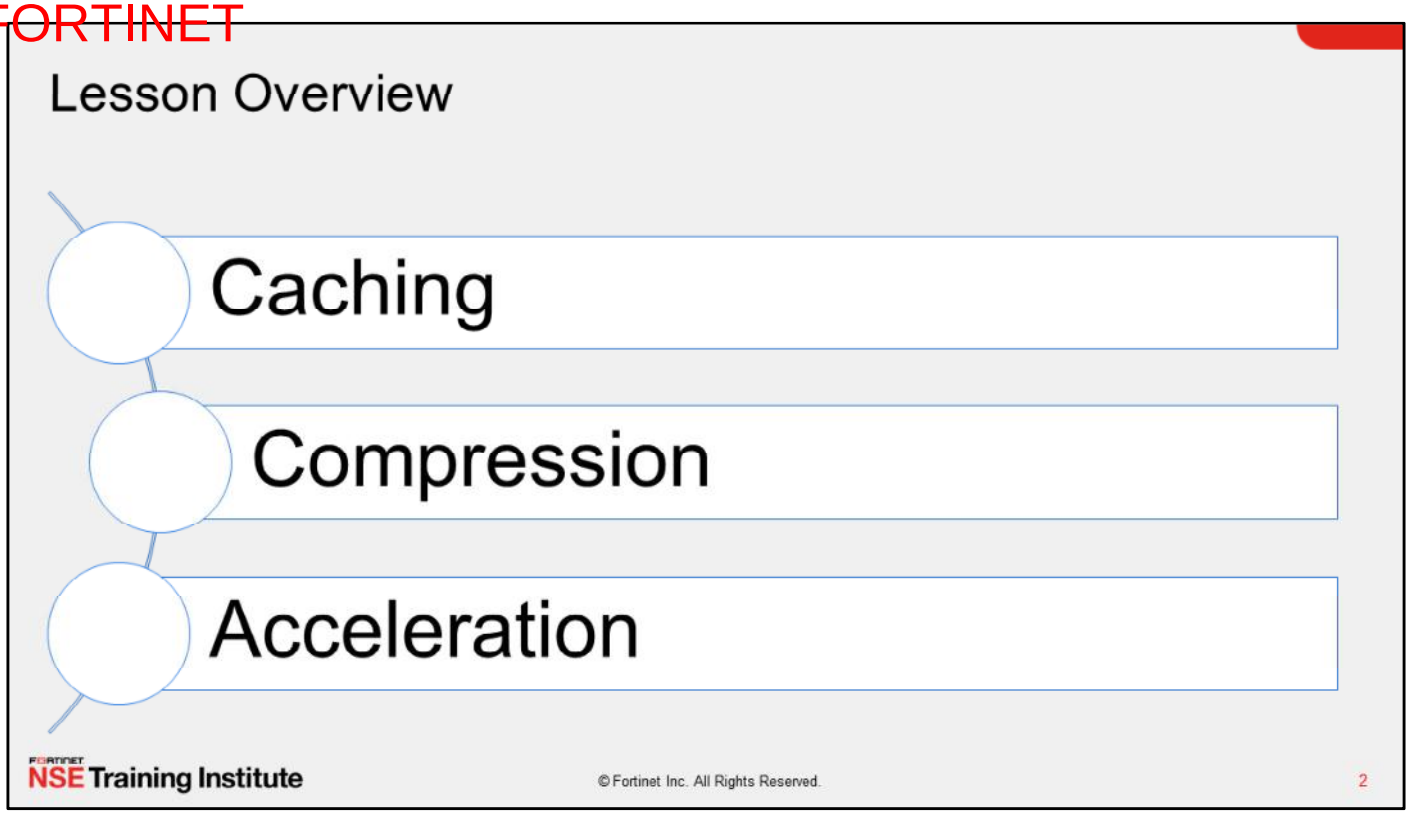
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to cache common responses from the server for improved responsiveness in your web apps, and how to handle response compression.

Vouchers & Dumps are Available | WhatsApp +201224560923

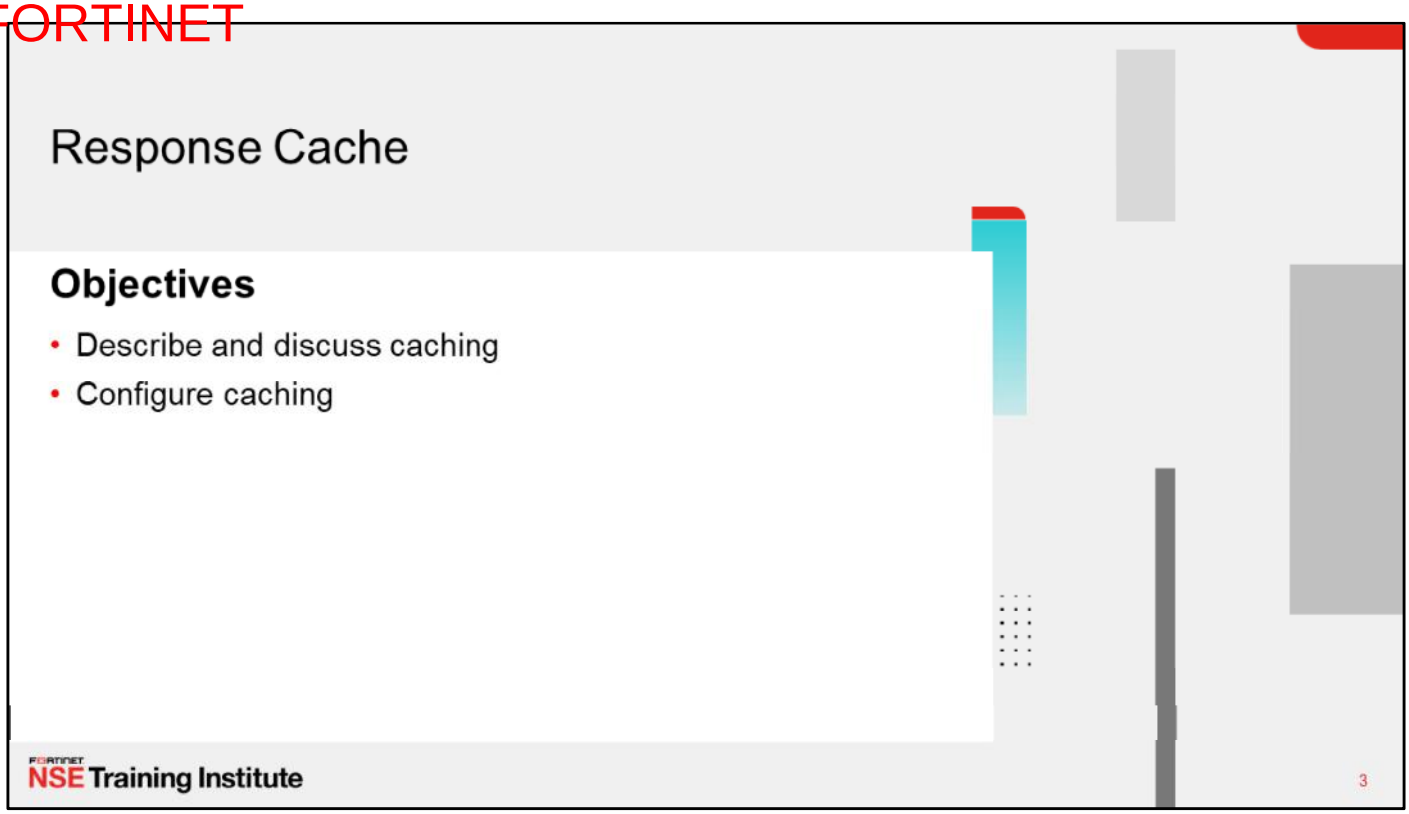
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiWeb response caching, you will be able to secure your web apps, and make them faster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Caching

- Modern web apps can be processor intensive
  - ASP, JSP, PHP, Ruby, SSI
  - All modules are page preprocessors: parse a template, usually query a database, then output HTML
- Cache helps web apps to scale performance for high traffic
  - Reduced server load
  - Faster response from client's perspective
- Not all web applications have native, efficient cache
  - Example: Varnish often added as front end cache to WordPress, despite having a cache plugin

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

Web pages don't usually change every second, or even every hour. Many web pages—even ones generated on-the-fly by a Tomcat servlet or PHP preprocessor for your content management system—are effectively static. Usually, an author writes the web page or uploads a file, and then that file never changes again. Yet every time a client requests the page, the server usually uses CPU and precious time to regenerate the HTML. This increases load and round-trip time and reduces server performance without benefiting the user. When many clients visit your site, this also means that load on your servers and LAN traffic increases proportionately. Many clients can quickly overwhelm your server and adding many more servers is expensive. In other words, these solution don't scale well.

To solve this, a web application could cache responses that haven't changed. However, there is a tradeoff: by sacrificing some RAM to store the response, the server could conserve CPU cycles. If the web application doesn't have a cache of its own, sometimes cache plugins are available.

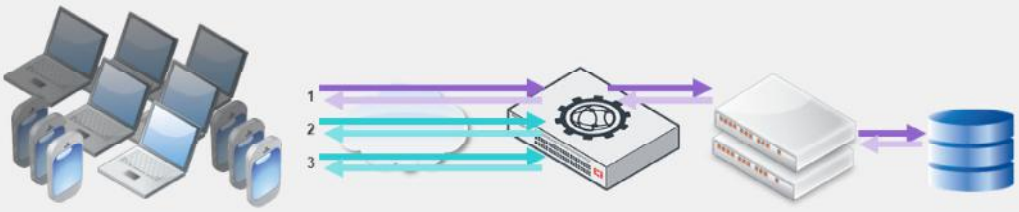
But not all web apps support cache. Plus, if you have a server farm, keeping the same cache on every server can waste additional RAM. So it is usually better to place the cache on a server in front of, or on, your FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Caching (Contd)

- FortiWeb can add front-end cache
  - Reduces LAN usage, *not* WAN usage
  - Keeps a temporary local copy of replies from server
  - Does not forward request to server if content hasn't changed
- Tradeoff: Use some FortiWeb RAM to improve:
  - Round-trip time
  - Server CPU usage
- Maximum cache size varies by FortiWeb model



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

Like the web cache on FortiGate, if the content doesn't appear to be dynamic, FortiWeb can keep a copy of the response. That way, instead of repeatedly forwarding requests for the same content to the server, FortiWeb can reply directly and quickly to the client.

This saves transmission and processing time on the back end. And the user is happier with a faster web application.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What *Can* Be Cached?

- Good for *static* items
  - /about.html
  - /company.css
  - Company logos
  - Banner
  - Sliders
  - Favicons
- FortiWeb caches everything it can *unless* you specify individual URLs, or exceptions, or both
- Does not affect files hosted externally
  - If images, movies, or music have a URL that is a content delivery network (CDN), such as Akamai, Rackspace, CloudFlare, or Amazon Cloud, they have their own cache

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

Cache on FortiWeb uses some of its RAM. So, before you enable cache, make sure it can benefit your web apps.

Cache will only improve the speed if you have many static files that are hosted locally. So, if most of your files are dynamically generated pages based on search results, or personalized pages after a user logs in, or if most files are hosted in a remote CDN such as Akamai, then there may be no net benefit to enabling the FortiWeb cache.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What *Can't* Be Cached?

- No dynamic items–variable, should not be cached
  - Forms that send parameters, `POST` requests
    - Searches
    - Forum posts
  - Contains the header:
    - `Authorization:`
    - `Proxy-Authorization:`
    - `If-Modified-Since`
    - `If-Unmodified-Since`
    - `If-Match`
    - `If-None-Match`
- Also FortiWeb will not cache if response:
  - Has a `Set-Cookie:` field
  - Has a `Vary:` field
  - Forbids caching (for example `Cache-Control: no-cache/no-store/private`)
  - Has no `Content-Length:` field (for example `Connection:close` and `Transfer-Encoding: chunked`)
  - Has no cache expiry tag (for example `Last-Modified/Etag` and `Cache-Control/Expires`)

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

It makes sense that search result pages can't be cached. But you may not be able to guess some of the other things that also can't be cached.

When the server sets a session cookie, even if the page itself is identical to other requests, the `Cookie: HTTP` header *isn't* identical. A session cookie is a unique session ID–different from all other replies on purpose, to identify the client. Remember, if any part of the HTTP request—including that header—is unique, then the page shouldn't be cached.

FortiWeb also won't cache if the response has an unknown content length. (This often occurs with streaming video, such as live news reports.) Cache has a fixed maximum size, and FortiWeb must be able to tell where the content starts and ends, so it can't cache a response if it can't identify the size. Also, by definition, live streams have dynamic content and cannot be cached.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring the Cache

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

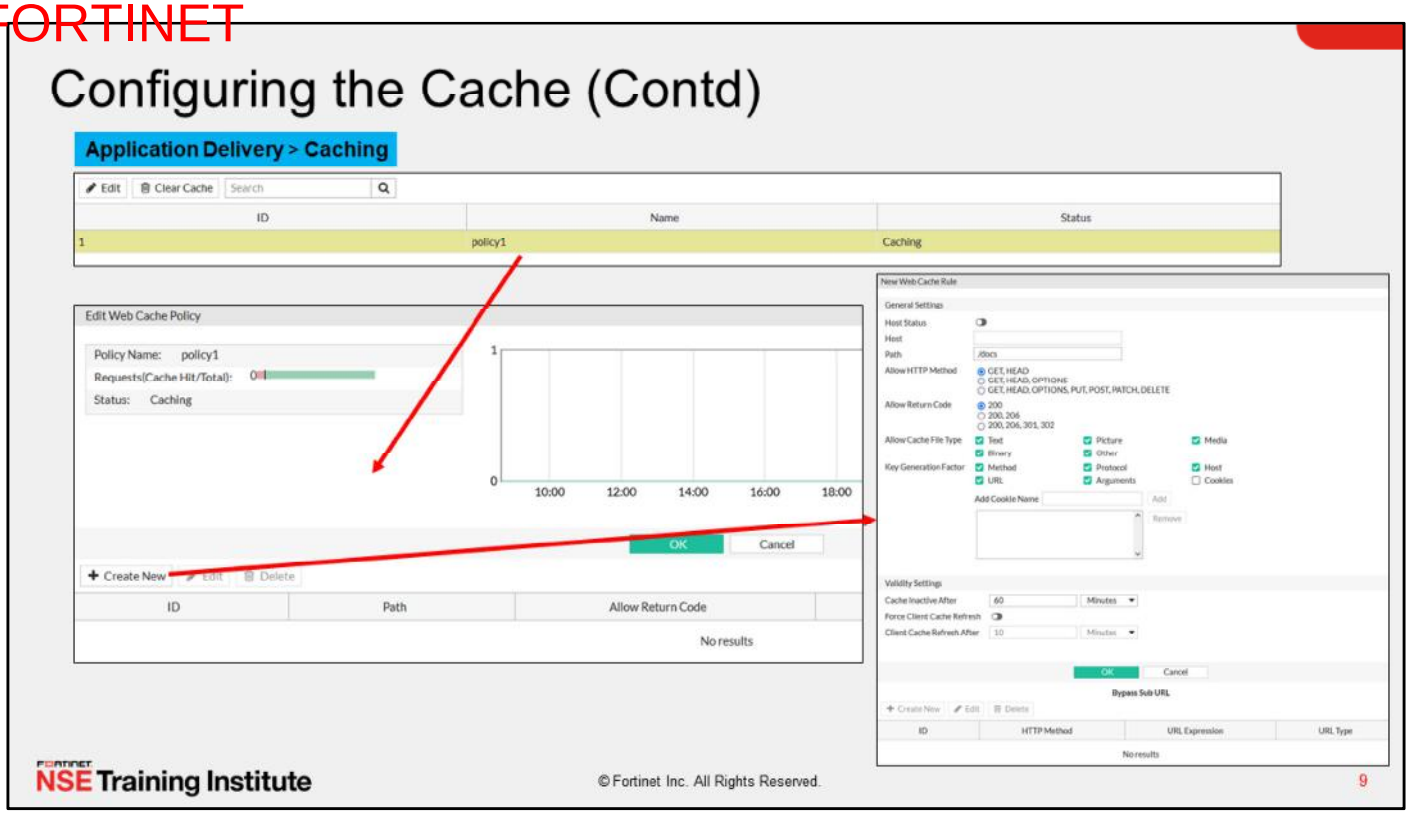
8

Now, take a look at how to enable caching on FortiWeb. It's very easy. You must enable **Web Cache** as a feature under **System** > **Config** > **Feature Visibility** to start using the cache.

Then you must enable in your server policy the **Web Cache** option to enable caching for that policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Next, configure the cache policy. In the simplest case, you just need to specify what methods you want FortiWeb to attempted to cache. FortiWeb automatically tries to cache all static URLs until its cache is full. Alternatively, if you want more fine-grained control, you can manually specify which URLs to cache or bypass. Then, in your protection profile, select the cache policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is a key factor you must consider before deciding to implement caching?
   - ✓ A. The type of data that makes up majority of your traffic
   - B. The most common type of client

2. Which items can be cached using the FortiWeb front-end cache feature?
   - ✓ A. Static items
   - B. Dynamic items

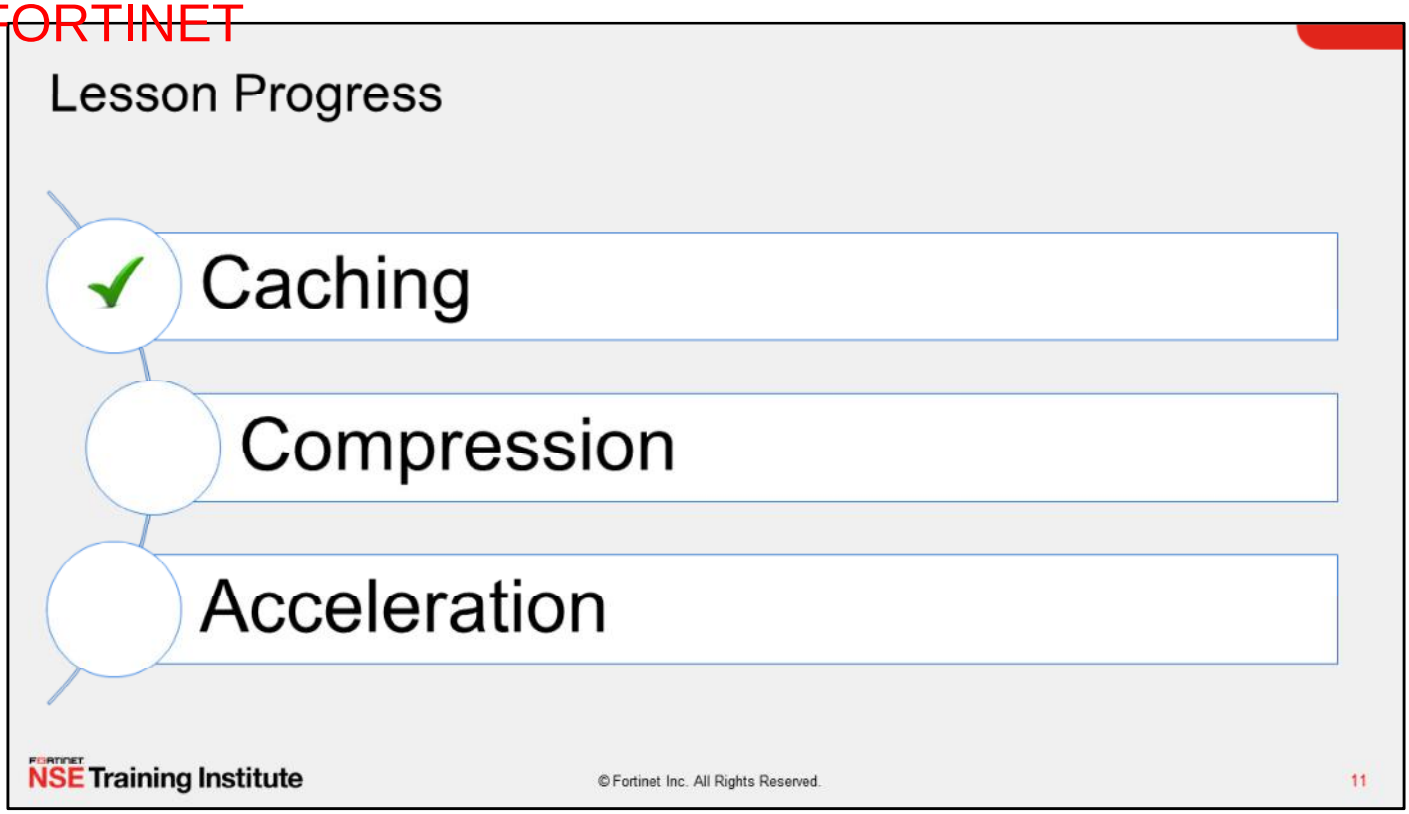
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

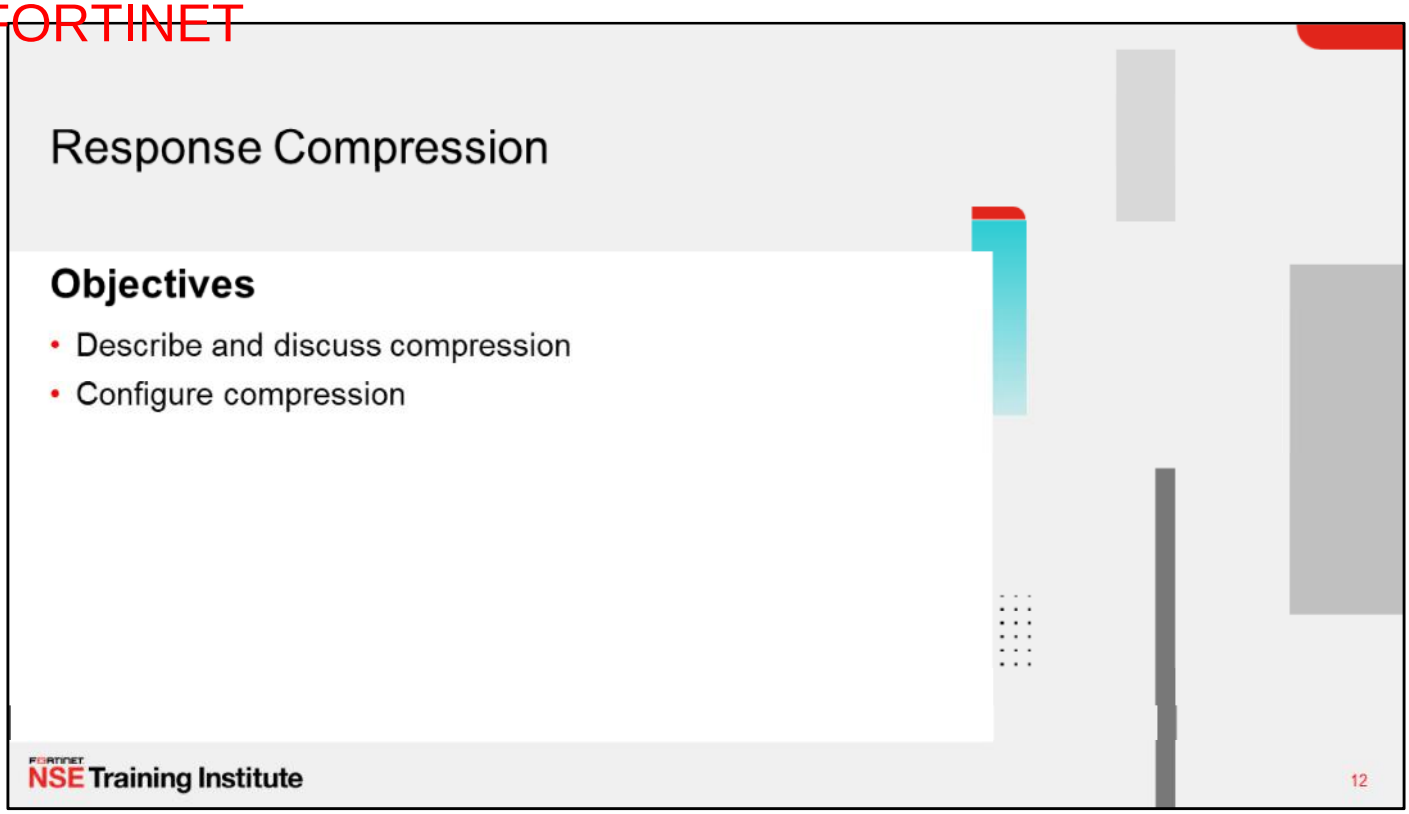


Good job! You now know the purpose of caching and how to implement it on FortiWeb.

Now, you will learn about response compression.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiWeb response compression, you can improve the user experience, and save money.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Offloading Response Compression

- FortiWeb compresses traffic, not servers
  - Client decompresses if this header exists:
    - Content-Encoding: gzip
  - RPC clients often cannot compress and may not be supported
- Reduces total bandwidth for files that comprise a web page
  - Efficient WAN bandwidth use
  - Faster response time to users
  - Tradeoff: takes some CPU time
- Maximum precompressed file size varies by RAM and configuration
  - FortiWeb buffer size: **System** > **Config** > **Advanced**
  - If file is too big for buffer, can't be compressed

NSE Training Institute © Fortinet Inc. All Rights Reserved. 13

FortiWeb can also compress responses. This is another performance feature—something FortiWeb can do to improve your user experience.

Compression can save you money, too. Mobile phone and 4G tablet data plans often have a bandwidth cap, with penalty fees if you download too much. So, if your web applications are used frequently—like webmail at a large company—the savings can be significant.

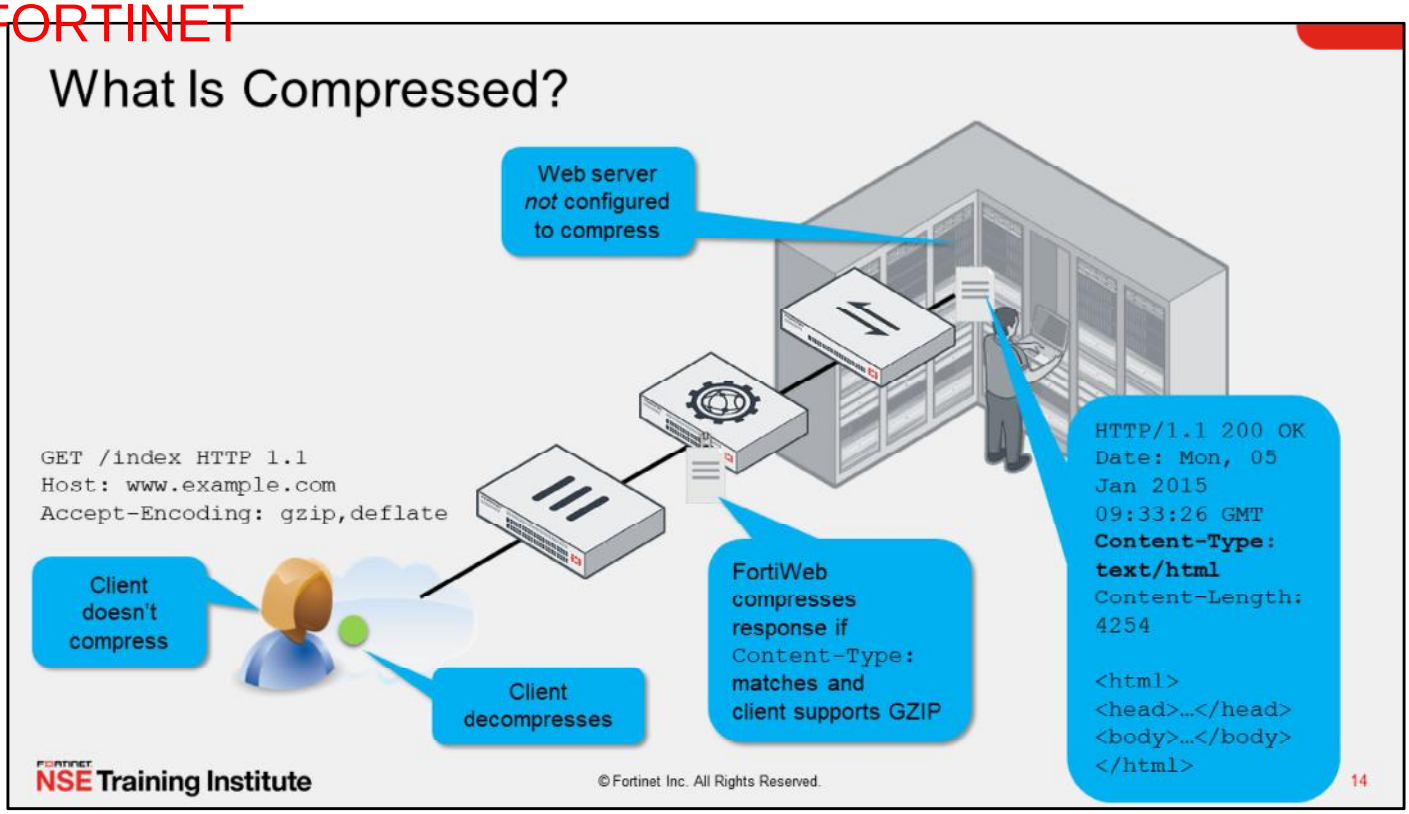
Compression essentially makes a zip file of each request before replying to the client. Clients automatically decompress the received file.

Compression is another feature that web servers sometimes offer, but you may be able to improve performance by having FortiWeb do it instead. This allows your servers to use CPU more efficiently and focus on things such as page preprocessors and queries to the database. It also reduces the total bandwidth you need to deliver each response to the client. This reduces bandwidth usage for Android and iPhone users, but it also uses your WAN or internet link more efficiently.

There are a few cases where you won't want to use compression. If a file is too big to fit in the FortiWeb compression buffer, then FortiWeb won't be able to compress it. Some file types don't compress well. For example, remote procedure call (RPC) clients are essentially using HTTP as a transport for binary. Binary is already somewhat efficient without compression. So, compression rarely improves the file size of a binary enough to be worth the CPU time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Take a look at response compression in action.

Notice that the client's request indicates that it supports GZIP compression. FortiWeb will remember this. Since the client is using the GET method, the request is short and, therefore, uncompressed. But the server replies with a web page, image file, movie, or whatever file was requested, and it's often at least several kilobytes. That's why it's important to compress the response.

Is that always true?

No. GET is the opposite of other HTTP methods. With POST or PUT, the client may be sending a large file–not the server. Uncompressed requests have already been transmitted along most of the network path by the time they reach FortiWeb, so, at that point, compression can't provide much benefit. And the server's reply is a short acknowledgement, so compressing that won't improve performance. But FortiWeb will try to compress the response regardless of the HTTP method.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Offloading Response Compression

- HTML, JavaScript, and CSS compress well
  - Repetitive tags:
    - `<div>`
    - `font-weight:`
- Compressing plaintext and already-compressed files usually *doesn't* improve performance
  - FortiWeb doesn't offer precompressed file types:
    ZIP, DOCX, PPTX, GIF, JPG, PNG, MP3, AVI, SWF
  - Text (TXT) varies by vocabulary, language, formatting, length
    - Compressed FortiGate .conf files can be 13% of original size
    - Compressed Chinese poems can be 98.5% of original size

NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

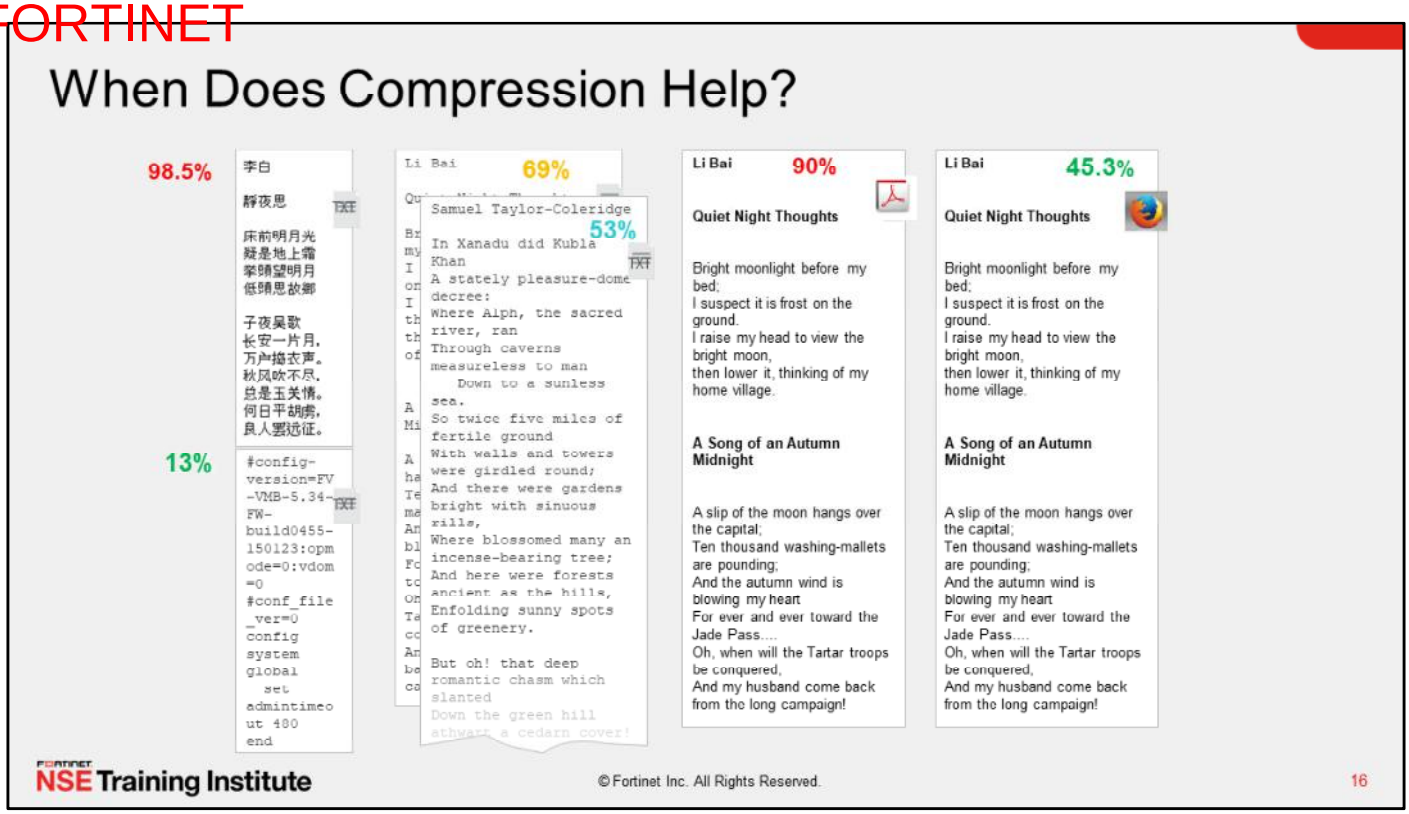
The best compression ratios are achieved when there is repetition in the data, such as HTML tags, JavaScript functions, or CSS attributes that appear many times in the same file. As a result, plain text notes may not compress well.

Some file types have native compression. Zip archives are compressed, but so are MP4 movies, MP3 music, and JPG photos. You might be surprised, but modern Microsoft Office files are compressed, too. In fact, if you temporarily change their file extension from .docx to .zip, you can open the archive and see the XML files inside.

Because it wouldn't be logical to compress file types that are already compressed, FortiWeb won't offer to compress them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When does compression help? When you have long files, with repetitive bytes, GZIP's Huffman coding is good at representing these efficiently. With a Fortinet `.conf` file, the GZIP could be 13% of the original—a good compression ratio.

Written Chinese is already very compact, with almost no repetition. So, compression only reduces the file size of this UTF-8 plain text file by 1.5%. Compression is not worth the CPU time.

An English translation of the same poem is less compact, but compression still doesn't offer much advantage. It reduces the file size by only 31%. Length improves the probability of repetition, though. Look at the second, longer poem. It has a complex vocabulary, but it's about three times as long. Its file size is reduced by 47%. We're finally reaching a 2:1 compression ratio. This still isn't great, but now compression might improve performance.

What about file formats that aren't plain TXT files?

PDF file format is worse; it is a binary format with its own native compression. GZIP compression reduces the file size by only 10%. But HTML gives us a better than 2:1 ratio.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example—Compressed Web Page

- Code is repetitive
- Makes compression effective
- Web page compression ratio typically 4:1 or 5:1

25.2%

NSE Training Institute

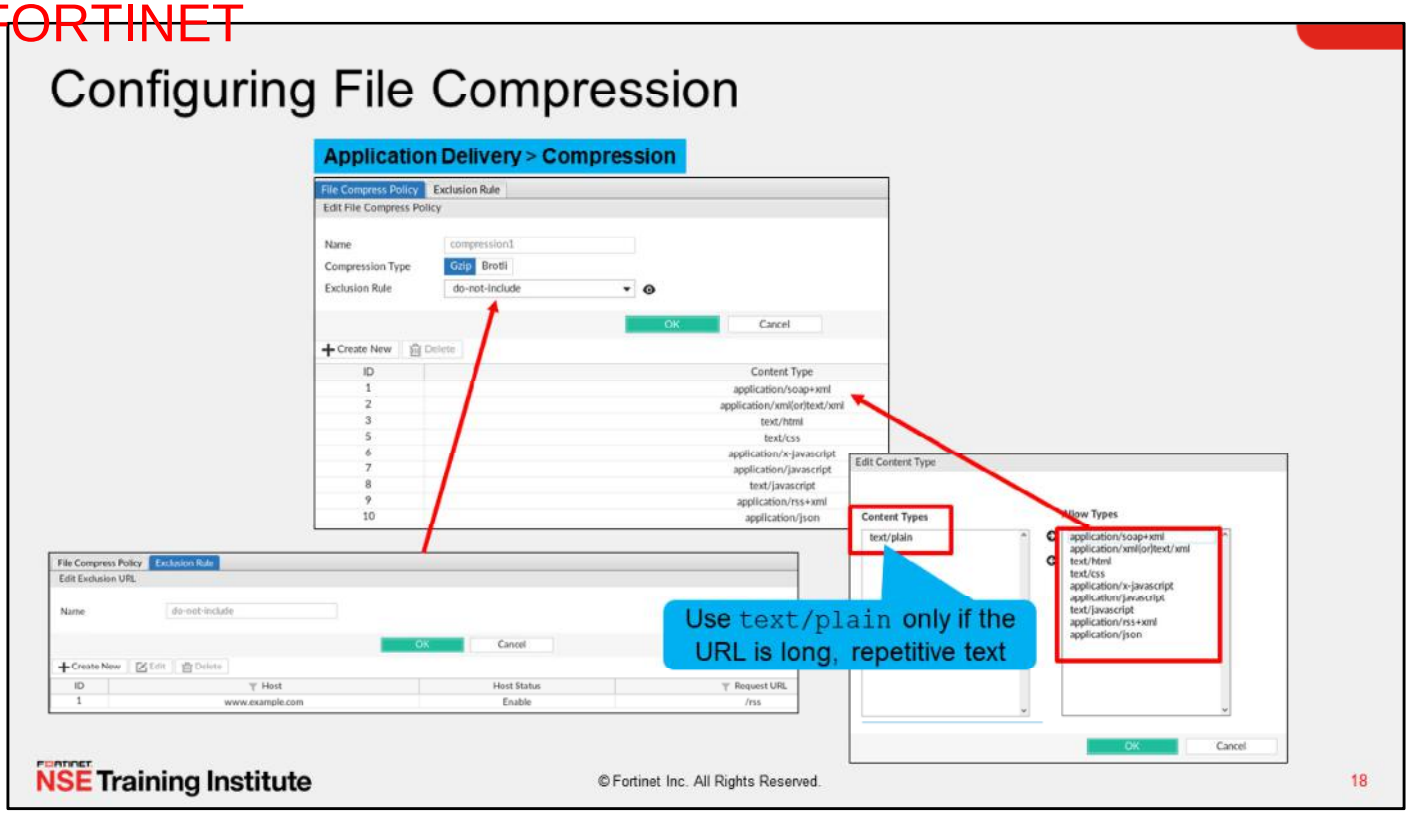
© Fortinet Inc. All Rights Reserved.

17

The example shown on this slide is of a real web page. For the HTML page alone, compression makes the transmitted file four times smaller—a very big speed improvement. When compressing HTML, it's typical to see a 75% to 80% file size reduction.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now take a look at how to configure compression. Like cache, it's simple.

First, configure any URLs that you want to exclude. Next, configure the compression policy. This specifies which internet file types you want FortiWeb to compress before forwarding the response to the client. (Internet file types are the HTTP equivalent of email's MIME types.) In most cases, you should configure FortiWeb to compress all file types except text/plain.

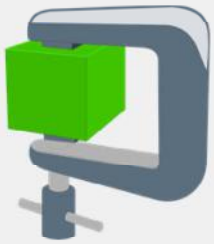
When done, select the compression policy in the protection profile. That's it!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What If the Server Compresses Instead?

- Compression is like weak encryption
  - Can't directly match data leak signatures and so on
  - Can't be modified for rewriting
- Instead of offloading to reverse proxy FortiWeb, server can compress responses
- FortiWeb automatically decompresses to examine contents
  - Data is then recompressed and delivered



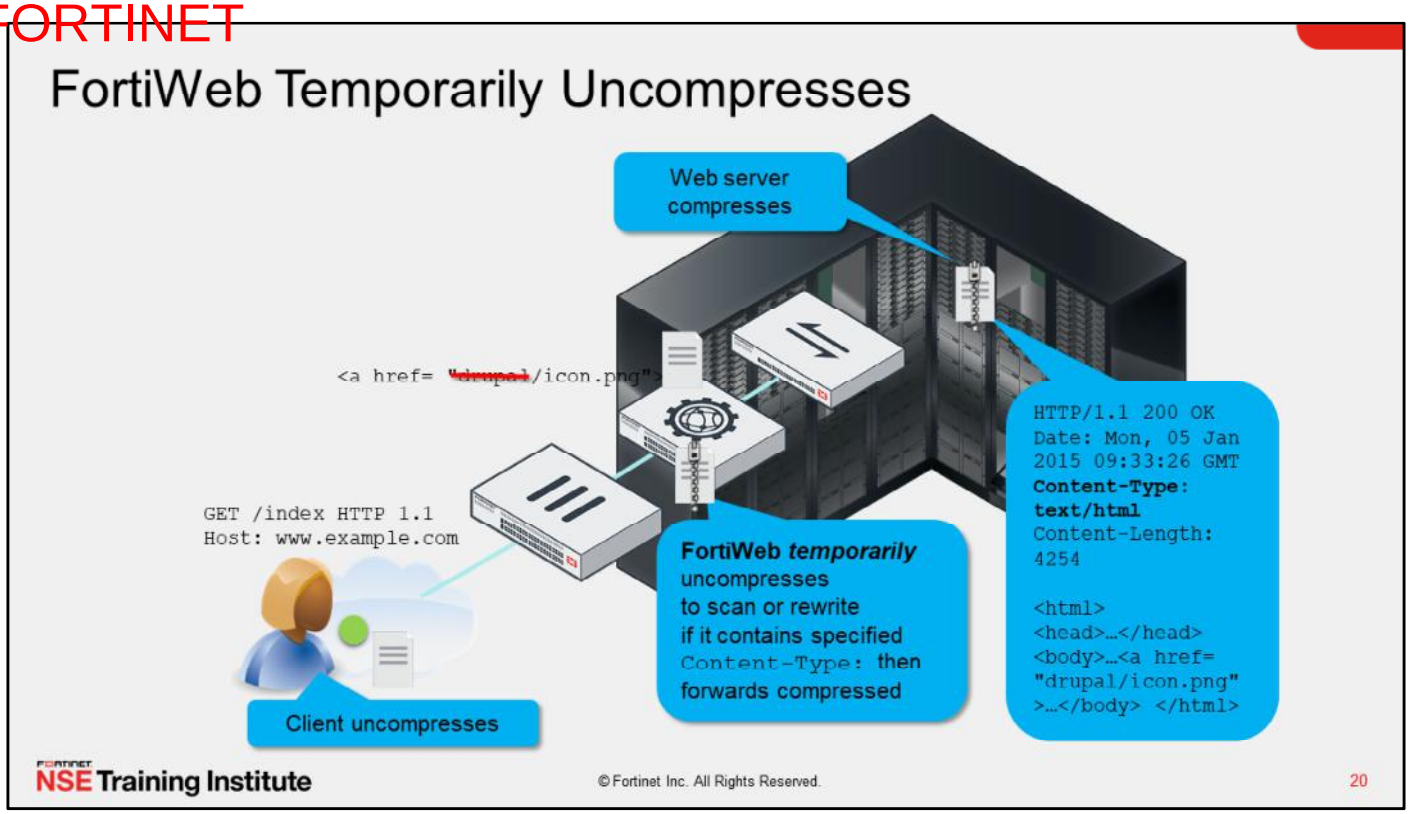
NSE Training Institute © Fortinet Inc. All Rights Reserved. 19

If you decide not to offload compression, as of version 6.1, your FortiWeb will automatically handle the content scan when compressed responses arrive from the web servers.

Compression is, effectively, low-grade encryption. It changes the traffic so that it won't match signatures or rewrite conditions. FortiWeb must undo the compression so that your signature policies, rewrite conditions, and policy scanning work.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Depending on how much load your FortiWeb has, it may be better for your servers to compress files instead.

In that case, FortiWeb receives a precompressed file. Some patterns—such as information leak signatures and HTML body rewrites—won't match unless you undo the compression.

Think of the uncompress process as compression inspection—like SSL inspection. It prevents compression from causing an accidental security bypass. FortiWeb can temporarily undo the compression so that it can scan the data content and type.

However, you don't want to forward an uncompressed file. So, FortiWeb's uncompression is only temporary. After a rewrite or a scan where the erase action is required, FortiWeb automatically applies the compression again. Alternatively, if no patterns match and no change is required, then FortiWeb doesn't need to recompress; it can just reuse the compressed original. Either way, FortiWeb forwards a compressed response to the client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When might you want to use the compression feature on FortiWeb?
   - ✓ A. When you are serving many road warriors who are using 4G tablets and phones
   - B. When you want to reduce buffering of video streams

2. Which file type would not be a good candidate for compression by FortiWeb?
   - ✓ A. .JPG files
   - B. .HTML files
   - C. Test-based configuration files

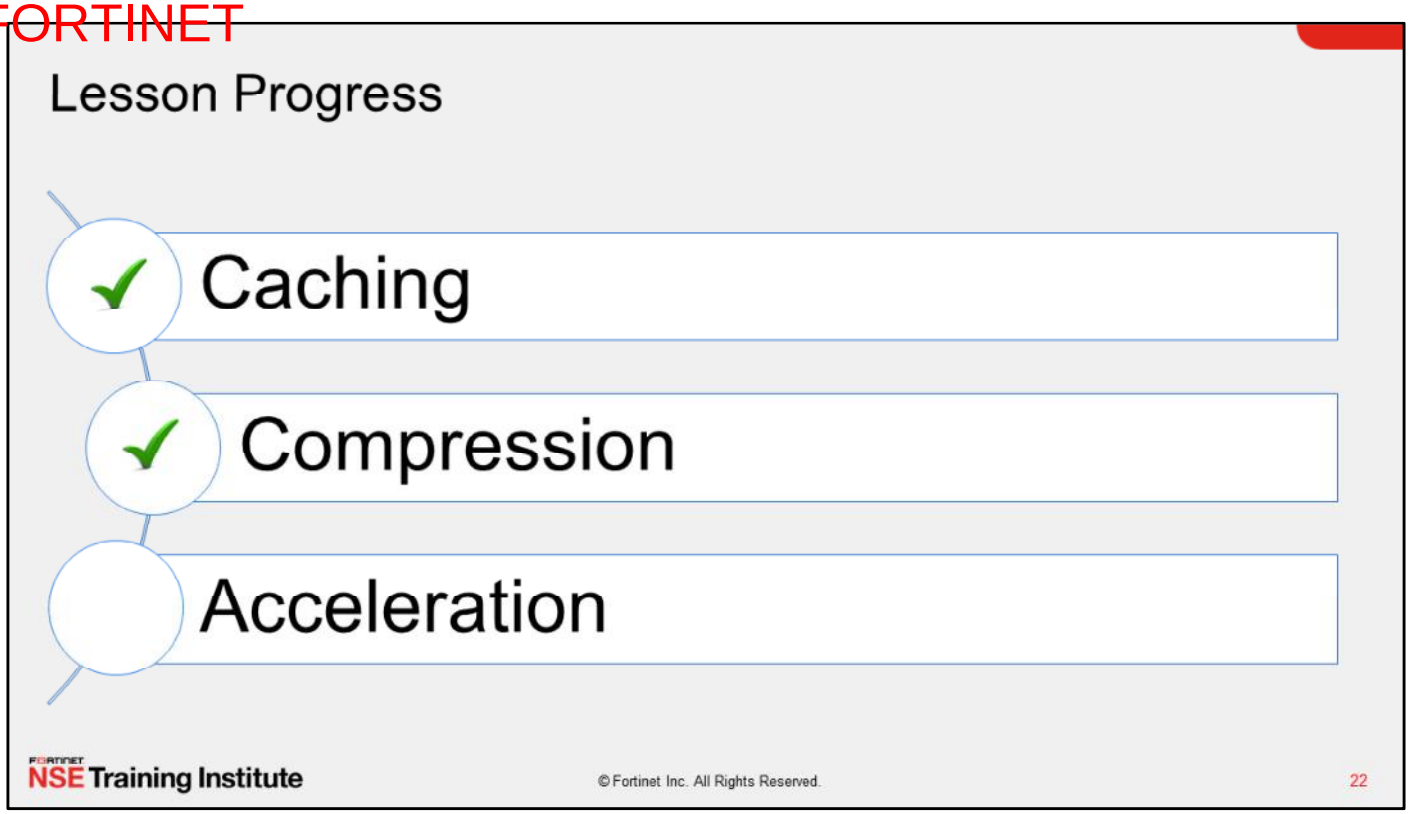
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

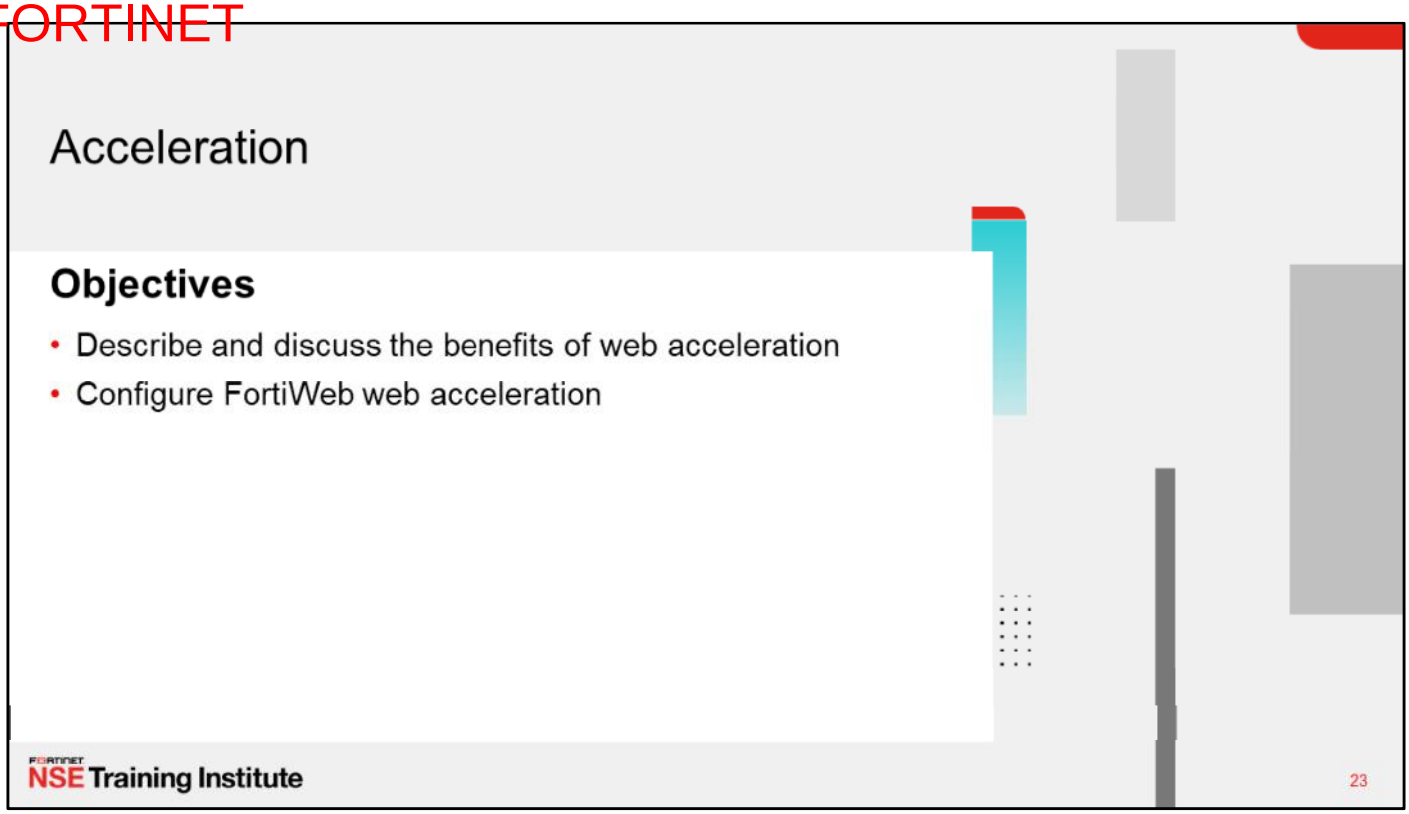


Good job! You now know the purpose of compression in web connections.

Now, you will learn about acceleration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding capture groups and back references, you will be able to use them, when needed, on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Acceleration

- FortiWeb enables acceleration of certain types of web traffic
  - HTML
  - JavaScript
  - CSS
- This is a separate feature from compression and caching
  - Optimized for specific protocols and traffic types
  - Reduces white space and load times in commonly used types of web content
  - Speeds up response time and reduces load on web servers
- Available in reverse proxy, true transparent proxy, and WCCP modes

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

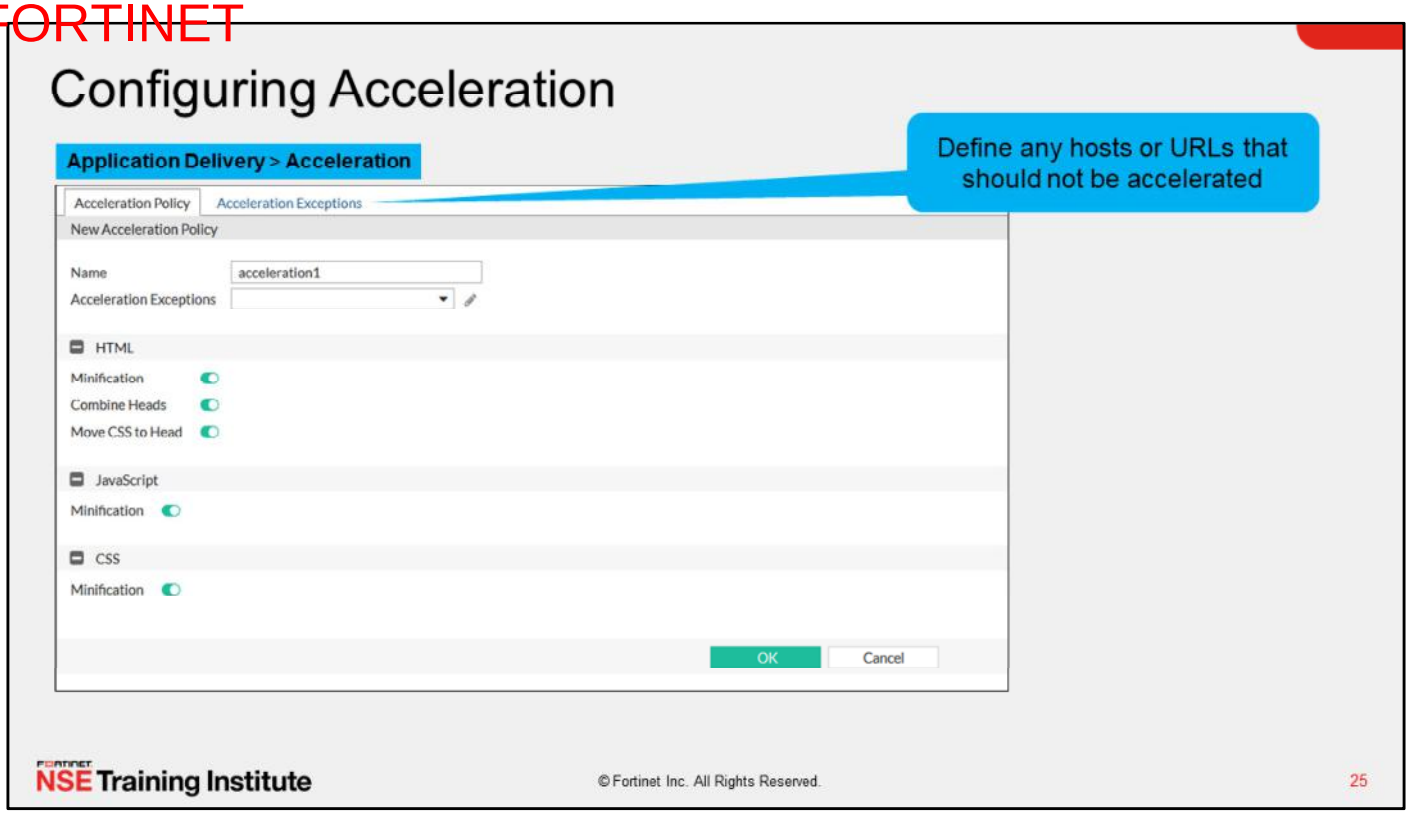
In addition to caching and compression, FortiWeb has a module that can enable some subtle web tricks to help improve server performance.

FortiWeb acceleration can perform the following tasks based on the types of content:

- For HTTP, FortiWeb can merge multiple head sections in an HTML page to minimize load time.
- For CSS, FortiWeb can remove extra whitespaces in the CSS and move them into the HTML header. This speeds up loading time because the CSS is parsed and loaded before the body is even examined.
- For JavaScript, ForiWeb can remove whitespace and comment sections to accelerate the processing and performance of JavaScript elements in pages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



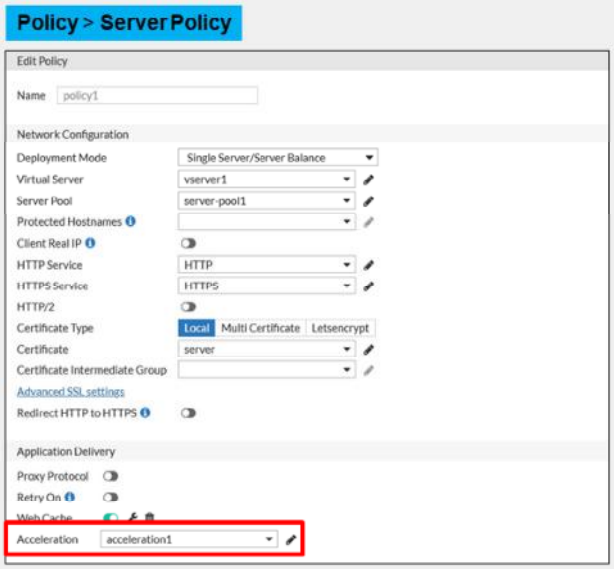
After enabling **Acceleration** as a feature under **System** > **Config** > **Feature Visibility** you can create a policy to define what types of acceleration you wish to apply to the traffic.

In addition to enabling the specific types of acceleration, you can define specific hosts and URL to exempt from acceleration. This can be useful for troubleshooting and ensuring that unusual configurations will not be modified by FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring Acceleration (Contd)



NSE Training Institute © Fortinet Inc. All Rights Reserved. 26

After an acceleration policy has been configured, it must be selected in the server policy. You may create multiple acceleration policies but can only select a single policy for each server. Use acceleration exceptions to control what traffic is accelerated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of traffic cannot be accelerated?
   A. HTML
   B. CSS
   ✓ C. PHP
   D. JavaScript

2. Which feature cannot potentially improve performance?
   A. Compression
   ✓ B. Coaching
   C. Acceleration
   D. Caching

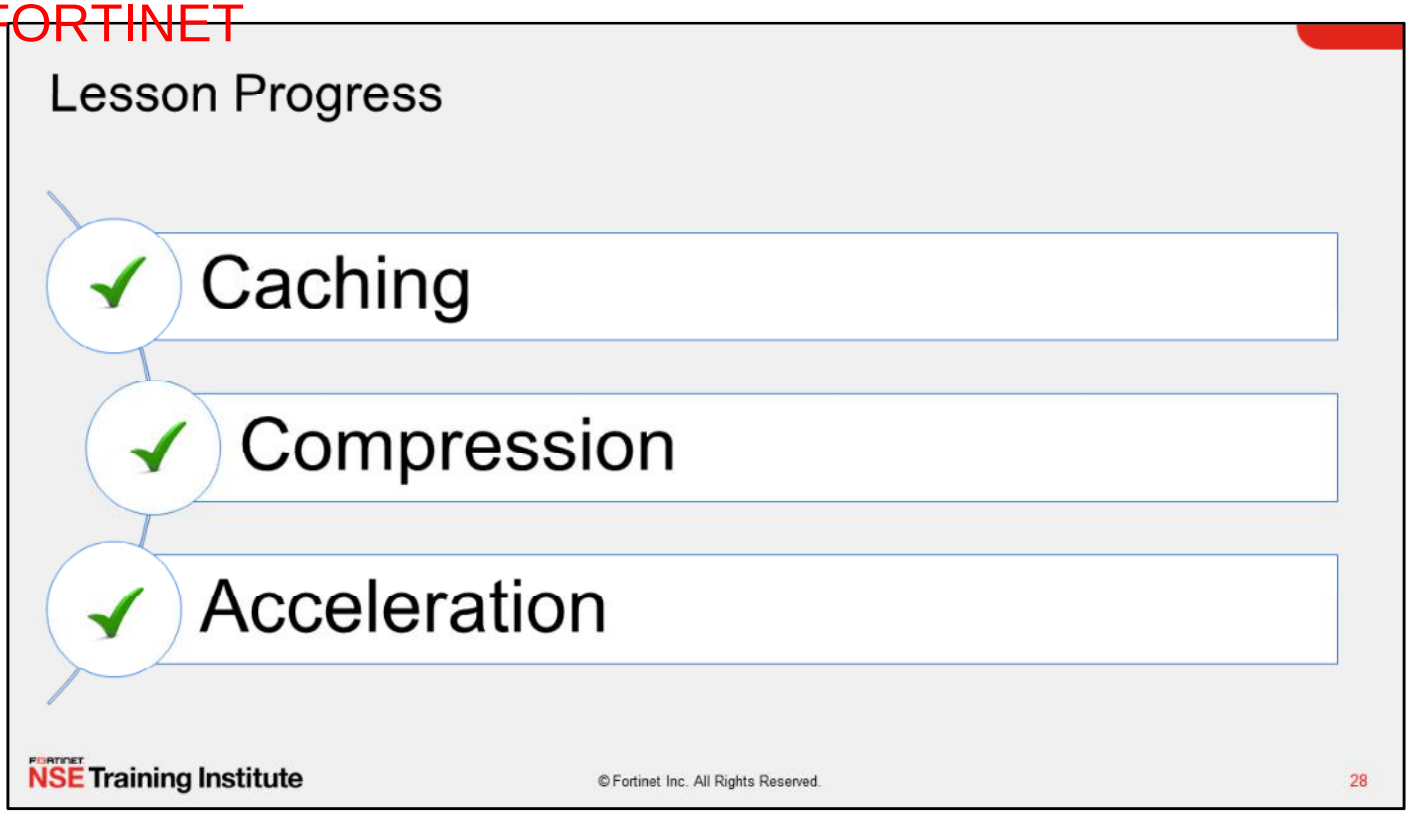
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe and discuss caching
- ✓ Configure caching
- ✓ Describe and discuss compression
- ✓ Configure compression
- ✓ Describe and discuss the benefits of web acceleration
- ✓ Configure FortiWeb web acceleration

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

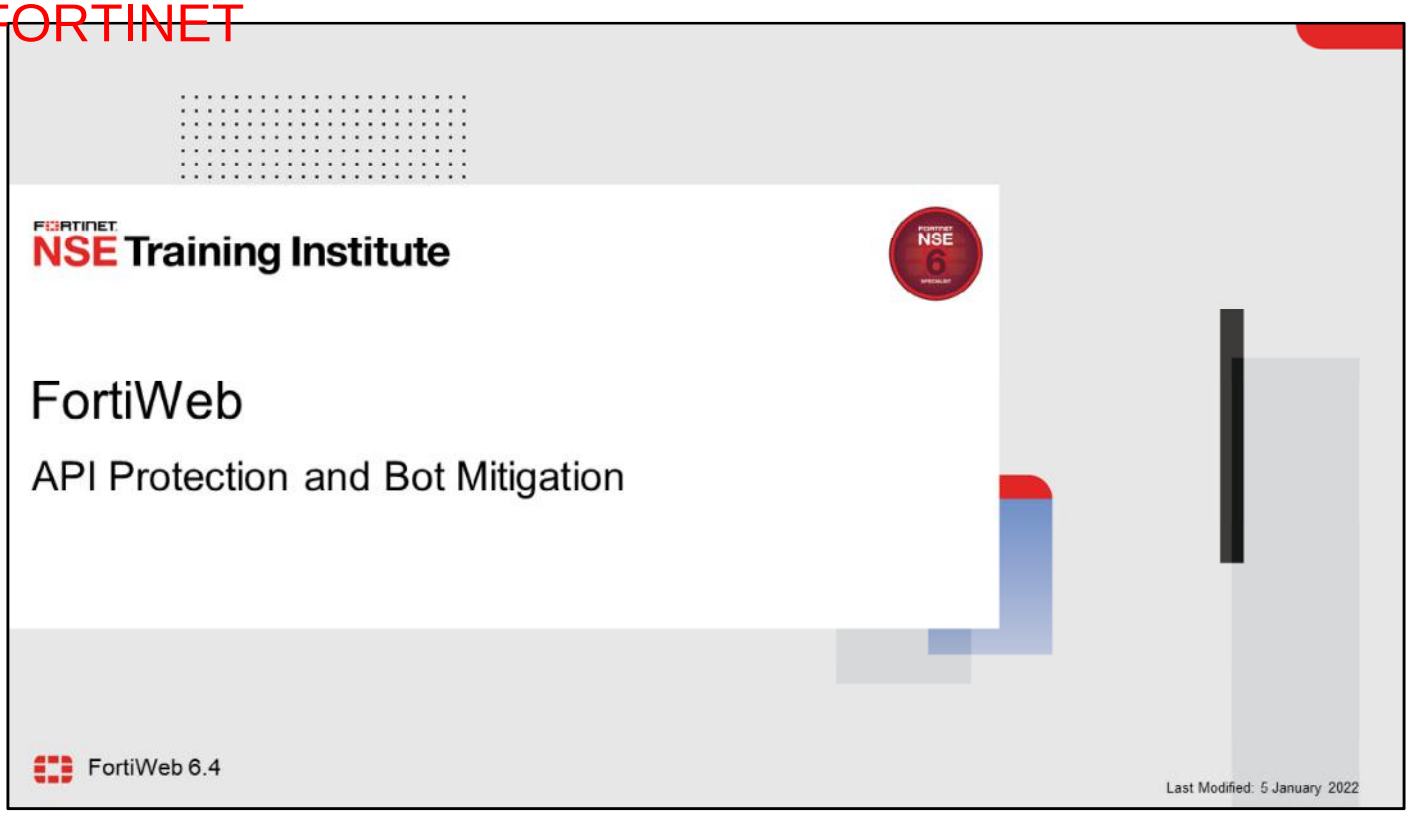
29

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you can improve the speed at which you deliver your web applications to clients using caching, compression, and web acceleration. You can also configure FortiWeb to buffer and uncompress a copy of a precompressed packet in order to scan it, or modify it, or both, before forwarding it.

Vouchers & Dumps are Available | WhatsApp +201224560923

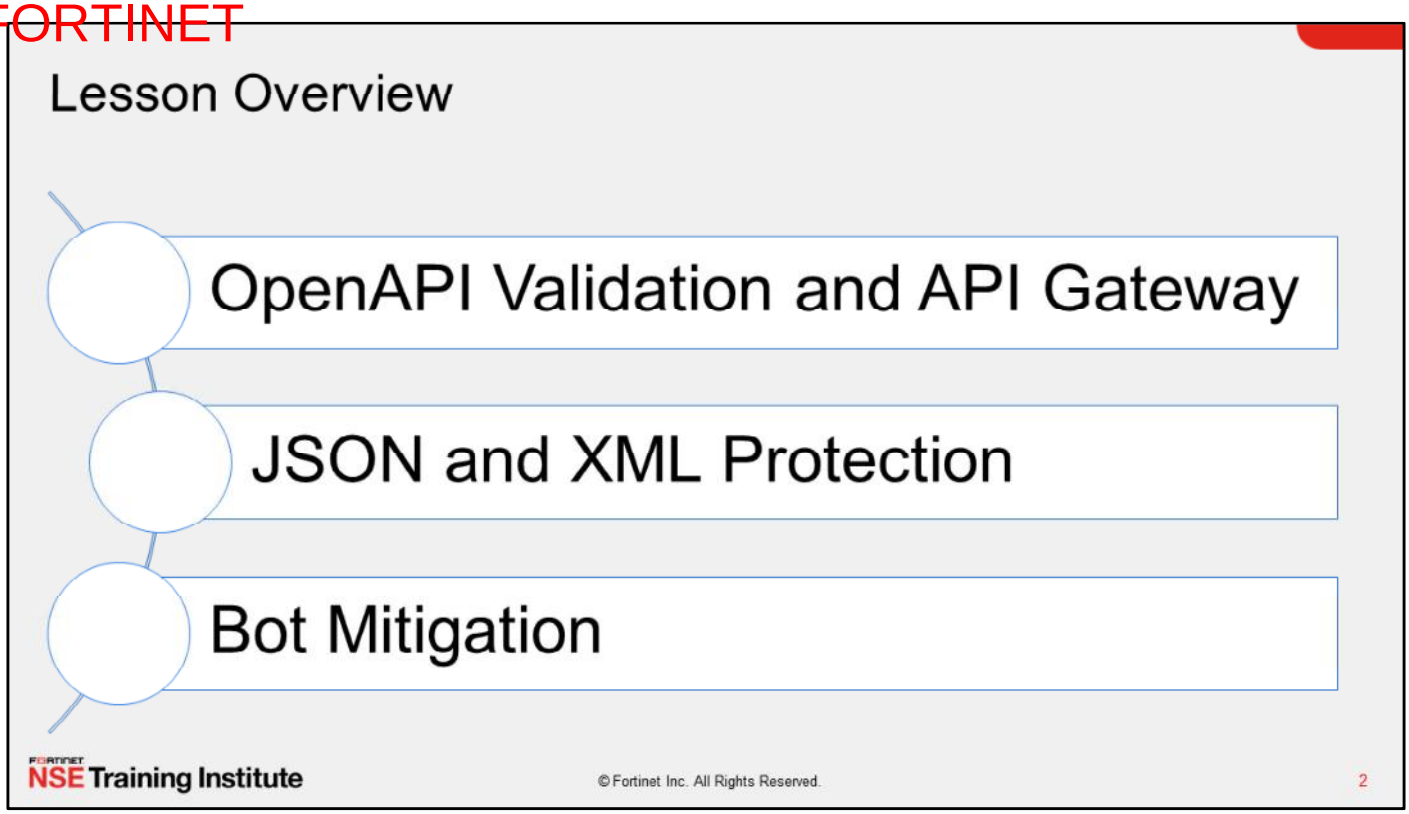
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about protecting API interfaces on your web servers and how to mitigate bot activity.

Vouchers & Dumps are Available | WhatsApp +201224560923

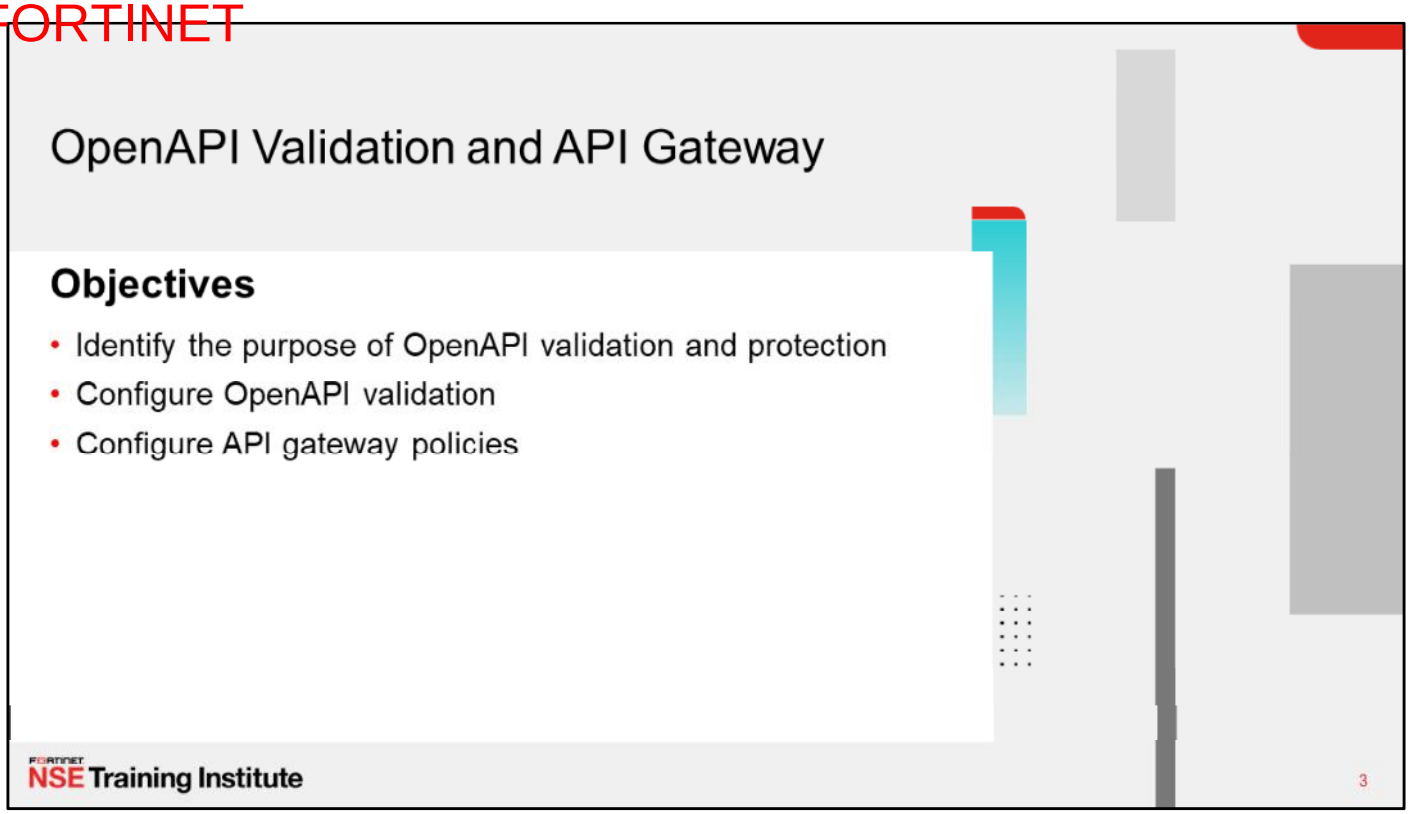
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring FortiWeb to act as an API gateway, you will learn how to protect vulnerable API interfaces on web servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OpenAPI Validation

- OpenAPI is a language commonly used to communicate to RESTful APIs
- OpenAPI Specification (OAS) defines what is allowed in these connections
- FortiWeb can monitor and validate commands sent to protected API interfaces
  1. Upload OpenAPI specification file to FortiWeb (YAML format)
  2. Create an OpenAPI validation policy
  3. Apply OpenAPI validation policy to a web protection profile
- FortiWeb supports OpenAPI 3.0.x

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

Application programming interfaces (APIs) are used by applications to talk to one another. APIs are frequently used by small applications to query web applications to gather statistics, perform small modifications to configurations, and other routine tasks. If these interfaces are internet facing and accessible by anyone, it is critically important to secure them so that unauthorized API calls cannot be used.

The easiest way to secure an API interface is with an OpenAPI specification file.

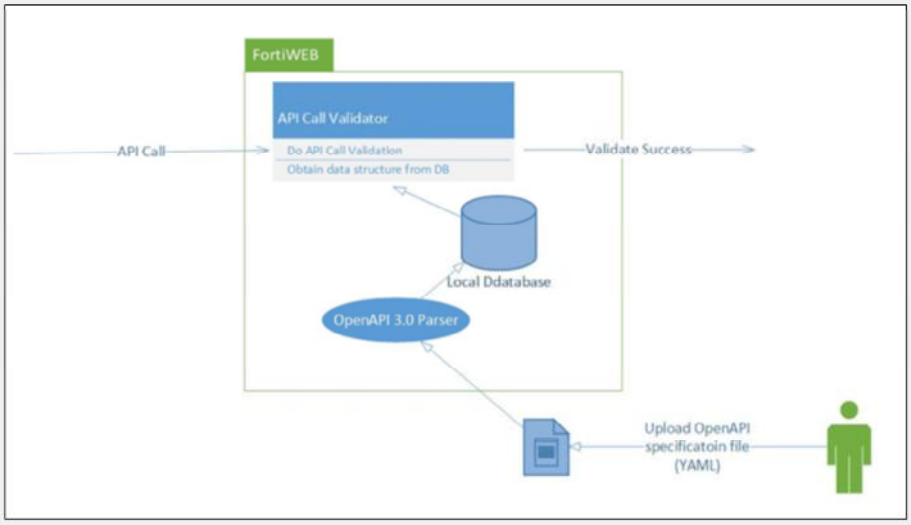
An OpenAPI specification file defines or describes the API. For example, the API URL, the parameter names in the URL, the type of data parameters should have (string, integer, and so on), the location of parameters submitted (URL, header, body, etc.), and so on. For more information about OpenAPI files, see https://github.com/OAI/OpenAPI-Specification/blob/main/README.md.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OpenAPI Validation (Contd)

- FortiWeb validates API calls before it sends them on to destination interfaces



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

FortiWeb can take a validation file and apply it to all API calls to protected servers. The information is stored in a local database for quick query and response times to validate API connections in real time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OpenAPI Specification File

- YAML file that defines what is allowed in API calls
- Very flexible, easy to modify text file format
- YAML is very format sensitive – use an editor like Swagger:
  - https://swagger.io/tools/swagger-editor/
- Simple example of restricting which servers can be accessed:

```
openapi: 3.0.0
info:
version: 1.0.0
title: FortiWeb Example API
license:
name: ABC
servers:
- url: 'http://www.example.com/v1'
- url: 'http://www.example.com/v2'
- url: 'http://10.10.10.10/v1'
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

The OpenAPI specification file is usually a YAML formatted file that contains the following information:

- Servers that this file applies to
- Paths that are to be protected on the server (like /docs or /admin)
- HTTP Methods like GET or POST
- Valid content and commands that can be sent for each individual method

This format is very flexible, but you should use an editor that can help with proper spacing and tabs. YAML is very sensitive to incorrect formatting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

OpenAPI Specification File (Contd)

- Import YAML files into FortiWeb
- Use a file editor like Atom or Swagger Editor
- Upload OpenAPI files to FortiWeb
  - You can use multiple files for different sites and queries
  - Use good titles and descriptions to keep track of configurations

openapi.yaml

```yaml
openapi: 3.0.0
info:
  version: 1.0.0
  title: Pet Shop API Example
  description: FortiWeb Sample API
  license:
    name: ABC
servers:
  - url: 'http://www.example.com/v1'
  - url: 'http://www.example.com/v2'
  - url: 'http://10.10.10.10/v1'
paths:
  /pets:
    get:
      summary: List all pets
      operationId: listPets
      tags:
        - pets
      parameters:
        - name: limit
          in: query
          description: How many items to return at one time (max 100)
```

API Protection > OpenAPI Validation > OpenAPI File

OpenAPI Validation Policy | OpenAPI File

+ Create New | Delete | View | Search

#	Name	Title	Description	Server URL
1	openapi.yaml	Pet Shop API Example	FortiWeb Sample API	http://www.example.com/v1 +2

NSE Training Institute

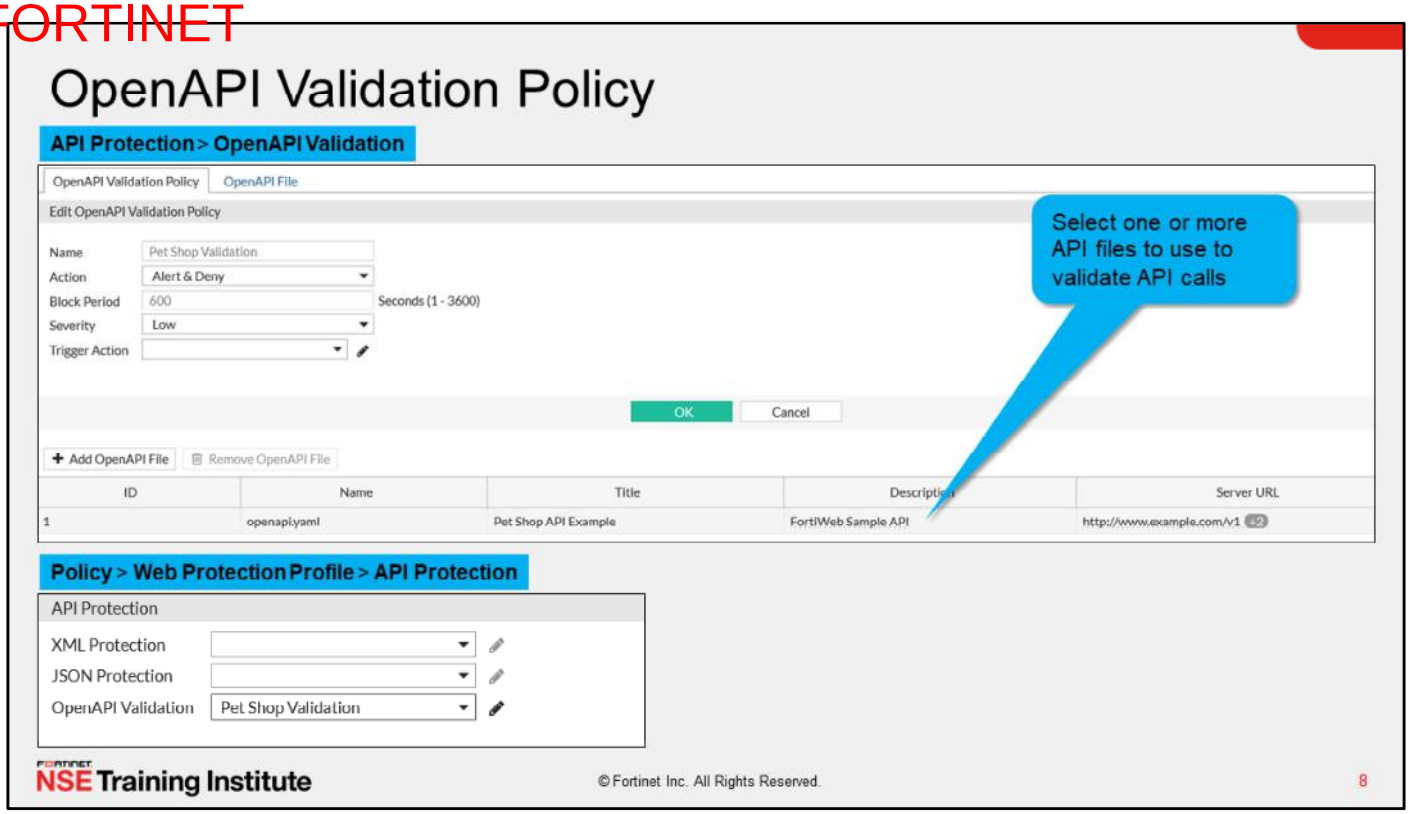
© Fortinet Inc. All Rights Reserved.

7

After you have created the OpenAPI specification file, upload the file to FortiWeb. If the file is not a valid OpenAPI 3.0.X format, FortiWeb will reject it. After the files are loaded, you can create a policy that groups the files together into a policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After creating an OpenAPI validation policy, you can select the block action and enforce individually uploaded OpenAPI files. You can trigger actions like email notification, or configure FortiWeb to trigger SNMP traps when an API violation occurs.

To enable the OpenAPI validation policy, simply select it in your inline web protection profile. Only one profile can be selected, but you can use multiple specification files to create the profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

API Gateway

- In conjunction with API validation, FortiWeb can also act as an API gateway
- An API gateway provides the following functions:
  - User management
  - Key verification
  - Access control
  - Rate limiting
  - Call rewriting
- To use this feature, enable it under **System** > **Config** > **Feature Visibility**

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

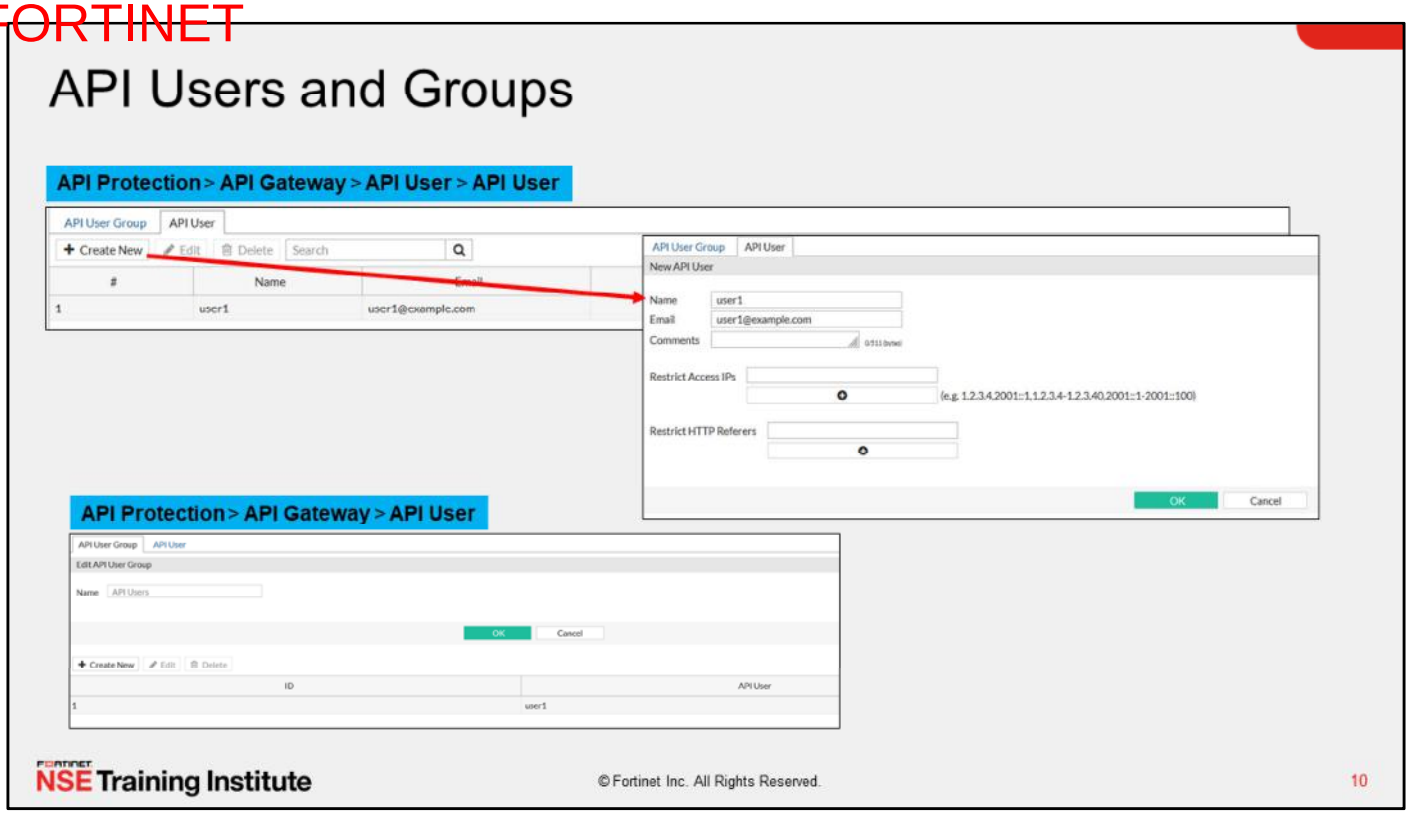
9

FortiWeb can also act as an OpenAPI gateway, proxying and verifying API calls before they are sent to your web applications. You need to enable this functionality from the feature visibility menu. The OpenAPI gateway gives administrators the ability to further restrict what can be sent to API servers in addition to verifying users, API keys, and implementing rate and access control.

You can use OpenAPI gateway and validation policies at the same time, as they do not directly conflict in areas of responsibility. API validation inspects the traffic as it is being passed to see if the syntax of the API calls themselves are valid. The API gateway verifies the connection, rate limits, and user authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



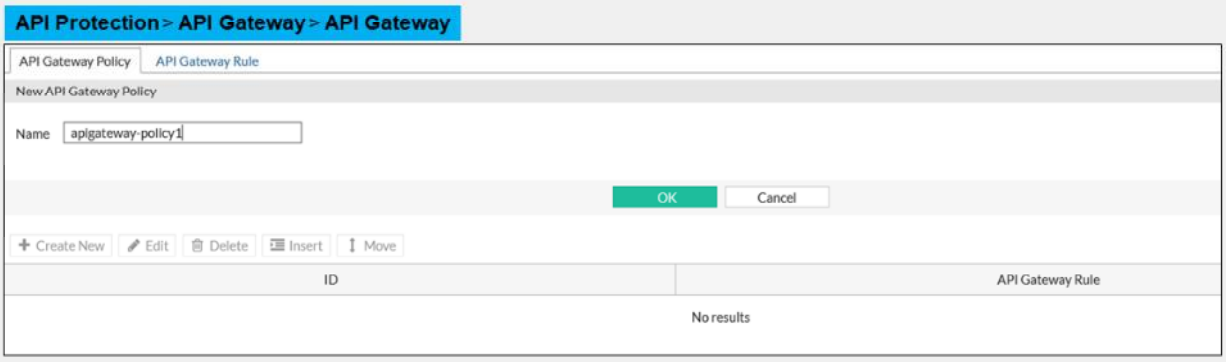
FortiWeb can verify whether a user attempting to make an API call is valid. To validate a user, you must define the username on FortiWeb. You can also assign additional restrictions like source IP address and restricted HTTP refers to a user. After you've created a set of users, you must create a user group. You can, assign the group to an API gateway policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

API Gateway Policy

- Bundles together API gateway rules



NSE Training Institute

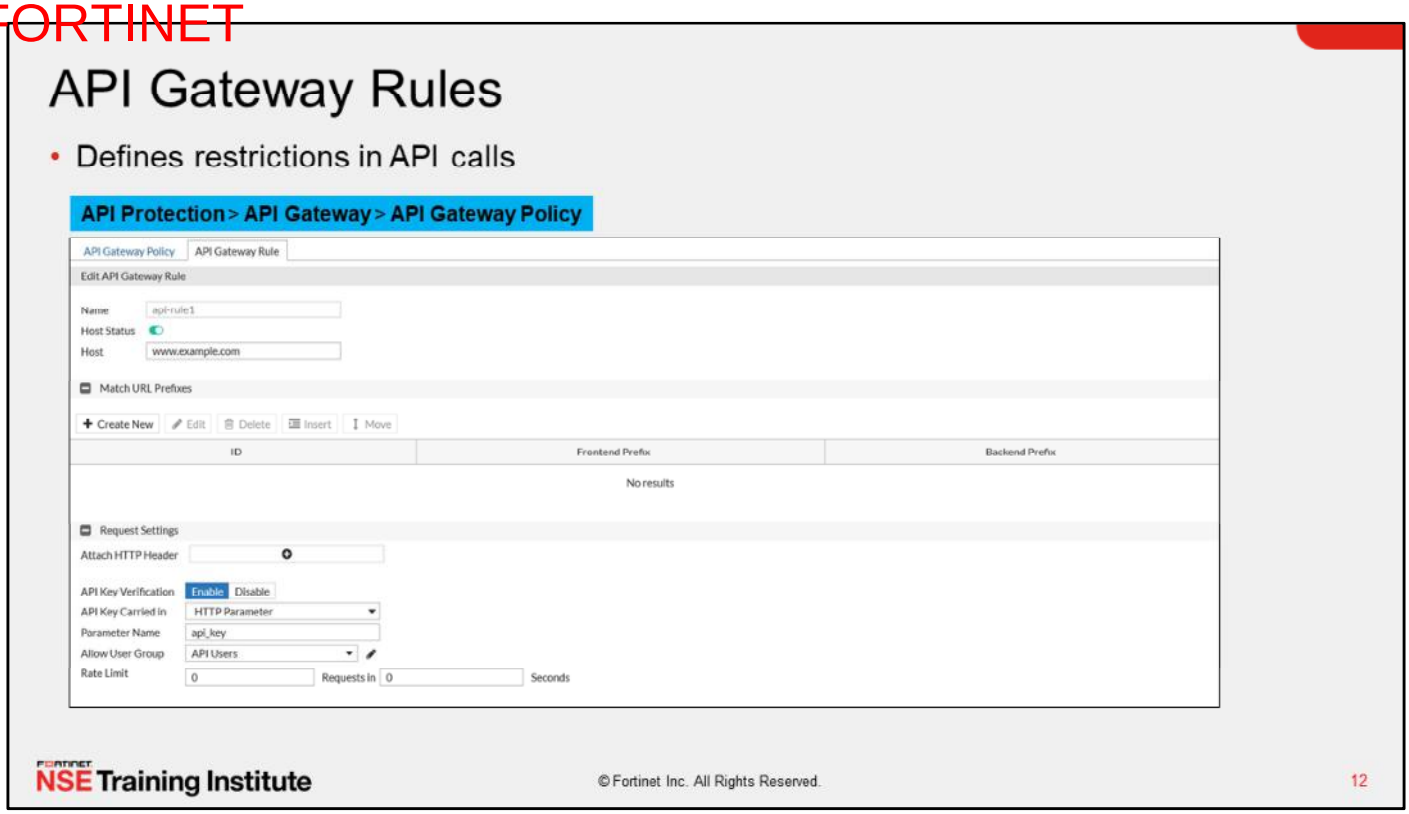
© Fortinet Inc. All Rights Reserved.

11

To select an API policy in a web protection profile you need to create the policy and add rules to it. After you create the policy, you can create API rules to restrict the type of API connections that are allowed through the API gateway.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



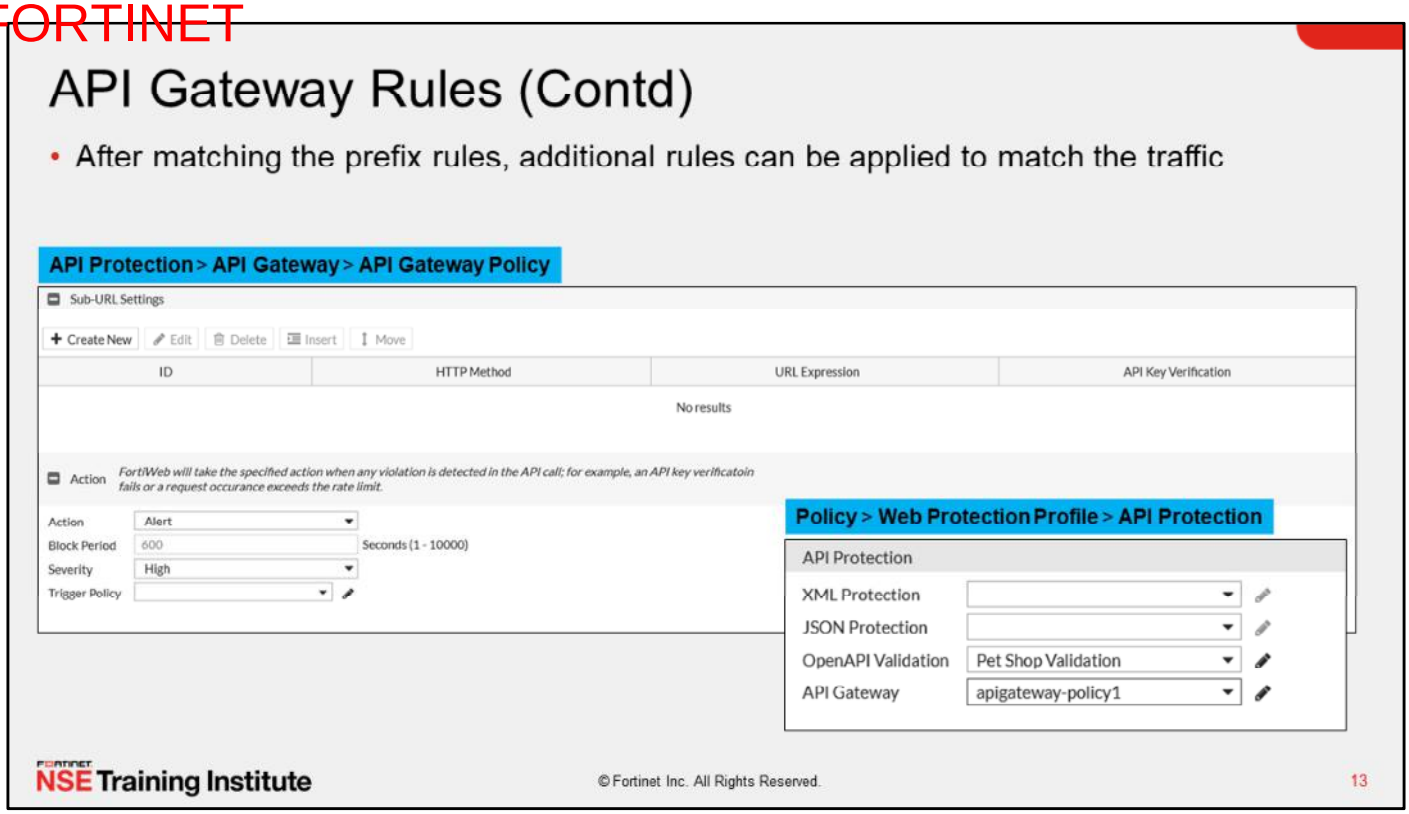
The API gateway rule is a series of restrictions that are applied to an API connection through FortiWeb. It can restrict based on:

- Hostname
- URL prefixes, such as `www.example.com/docs/api/v1/testing/`
- API user and key verification
- Rate limits

When creating API users, you don't assign a password. This is because almost all API connections use an API key. You need to define how the key is passed for FortiWeb to be able to validate the user against the API server. For example, API keys are frequently sent in an HTTP parameter called `api_key`. FortiWeb can then take the username and API key and validate it against the API interface before allowing any further communication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure regular expressions or string match rules on the entire request to further restrict traffic, in the **Sub-URL Settings** page. FortiWeb can also perform API key verification based on a new API key parameter or inherit it from the request settings.

After a trigger action, you have to select the severity and optional trigger policy in the API gateway policy and then apply it to an inline protection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What format does the OpenAPI specification file need to be to upload to FortiWeb?
   A. Microsoft Word
   B. XML
   ✓ C. YAML
   D. HTML

2. Which one can you *not* define in an API gateway policy?
   A. API username
   ✓ B. API key
   C. Rate limits
   D. URL prefixes

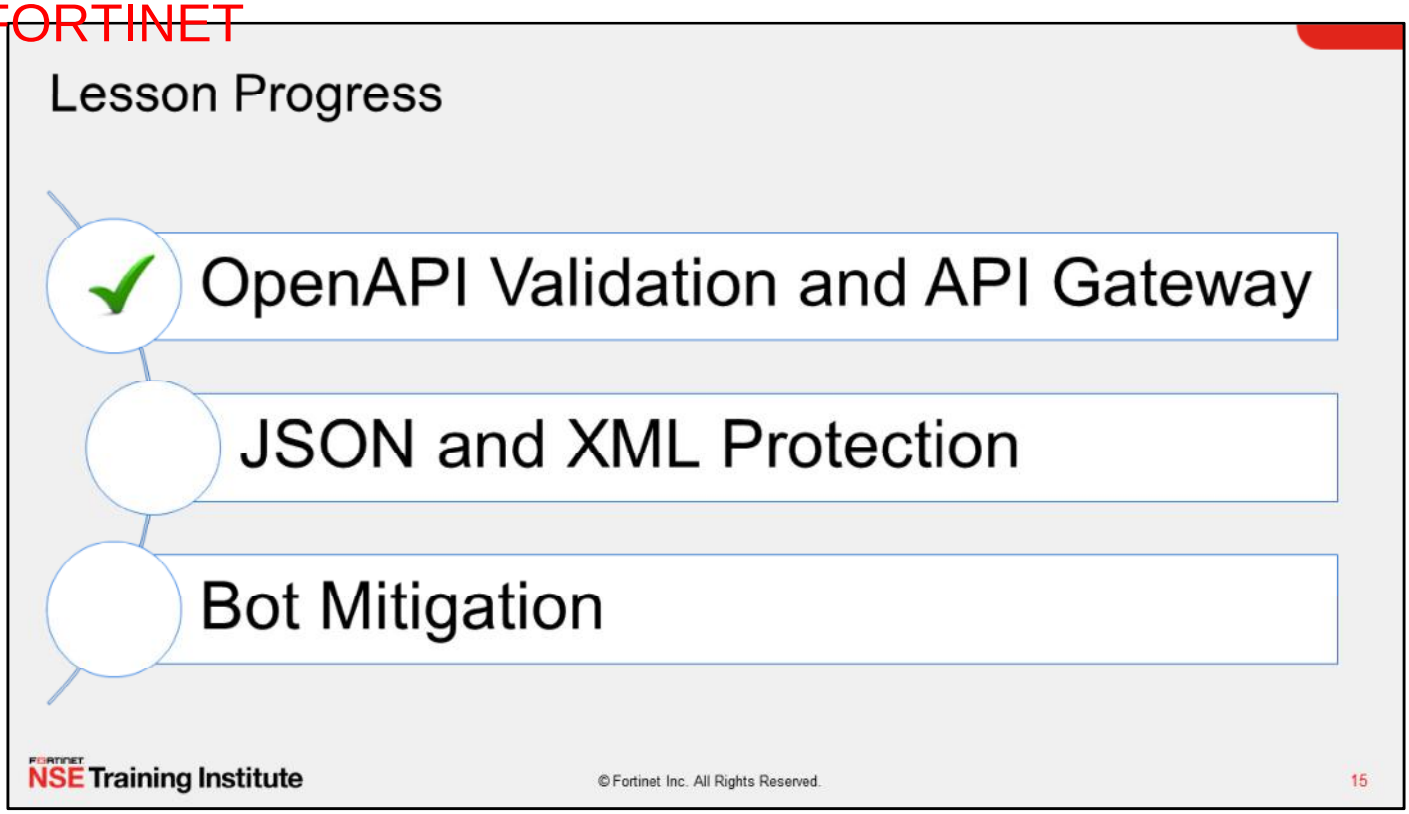
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

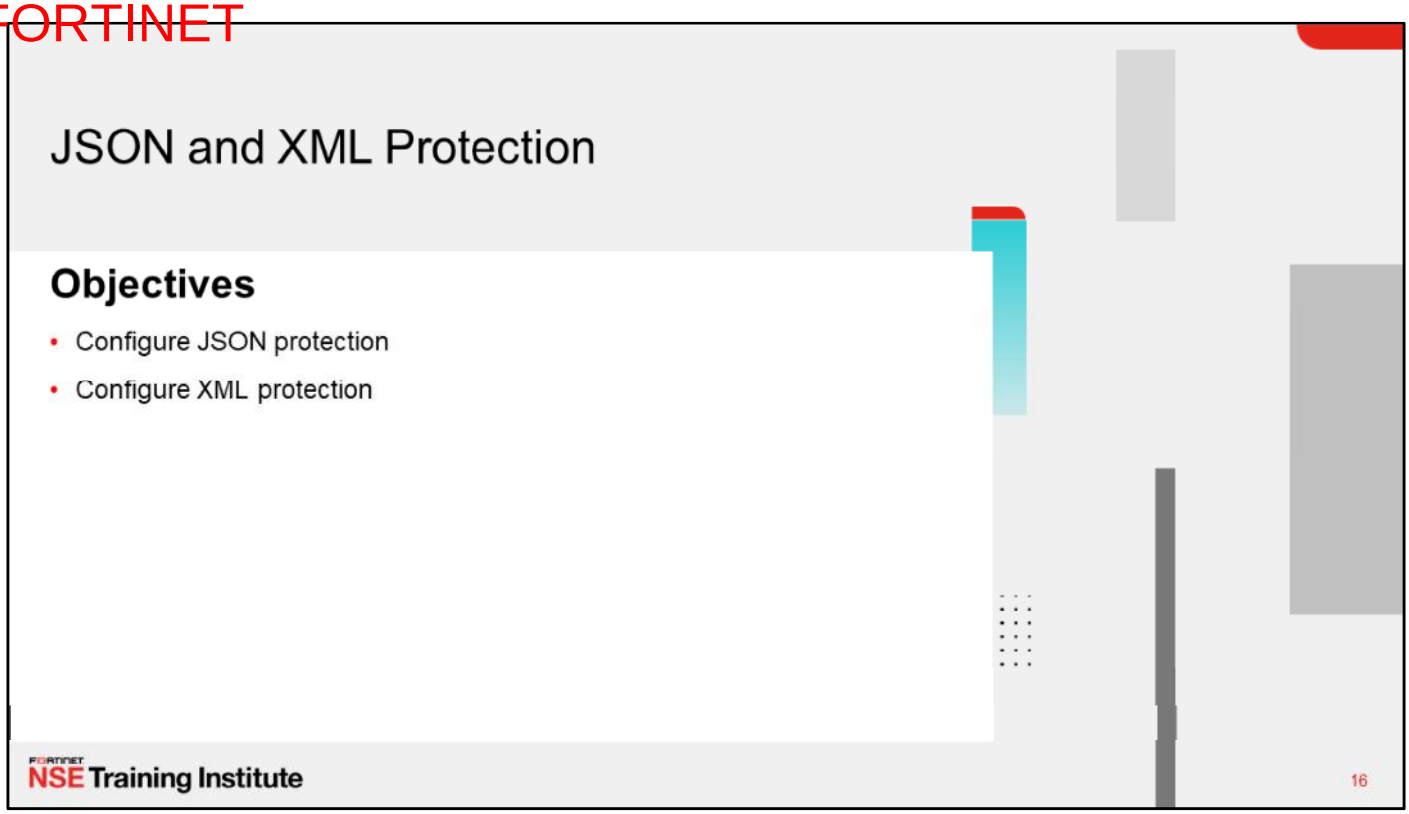


Good job! You now know how to configure FortiWeb to operate as an API gateway and validate OpenAPI connections.

Now, you will learn how to protect JSON and XML connections using FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in JSON and XML validation, you will be able to protect these types of connections from potential malicious use.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

JSON Protection

- JSON is a lightweight data interchange format, and attackers may try to exploit sensitive information in JSON code to attack web servers
- You can configure FortiWeb to validate JSON data contents in a JSON document
- Like enabling OpenAPI protection, the steps to enable JSON validation are:
  1. Import JSON schema files
  2. Create JSON protection rules
  3. Create JSON protection policies
  4. Select a JSON protection policy in a web protection profile

NSE Training Institute © Fortinet Inc. All Rights Reserved. 17

JavaScript Object Notation (JSON) uses human-readable text to transfer information. Similar to OpenAPI, JSON can use schema to define what data is expected and how it is formatted. This is very important to help prevent attackers from gleaning information or compromising web applications through cleverly crafted JSON documents.

After you upload the schema files, you need to assign them to rules, and then policies, which you can select in the web protection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

JSON Schema Files

- JSON schema files define information that is being transmitted in JSON format
- An example of the data arrays passed by JSON:

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "Product",
    "description": "A product from the catalog",
    "type": "object",
    "properties": {
        "id": {
            "description": "The unique identifier for a product",
            "type": "integer"
        },
        "name": {
            "description": "Name of the product",
            "type": "string"
        },
        "price": {
            "type": "number",
            "minimum": 0,
            "exclusiveMinimum": true
        }
    },
    "required": ["id", "name", "price"]
}
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

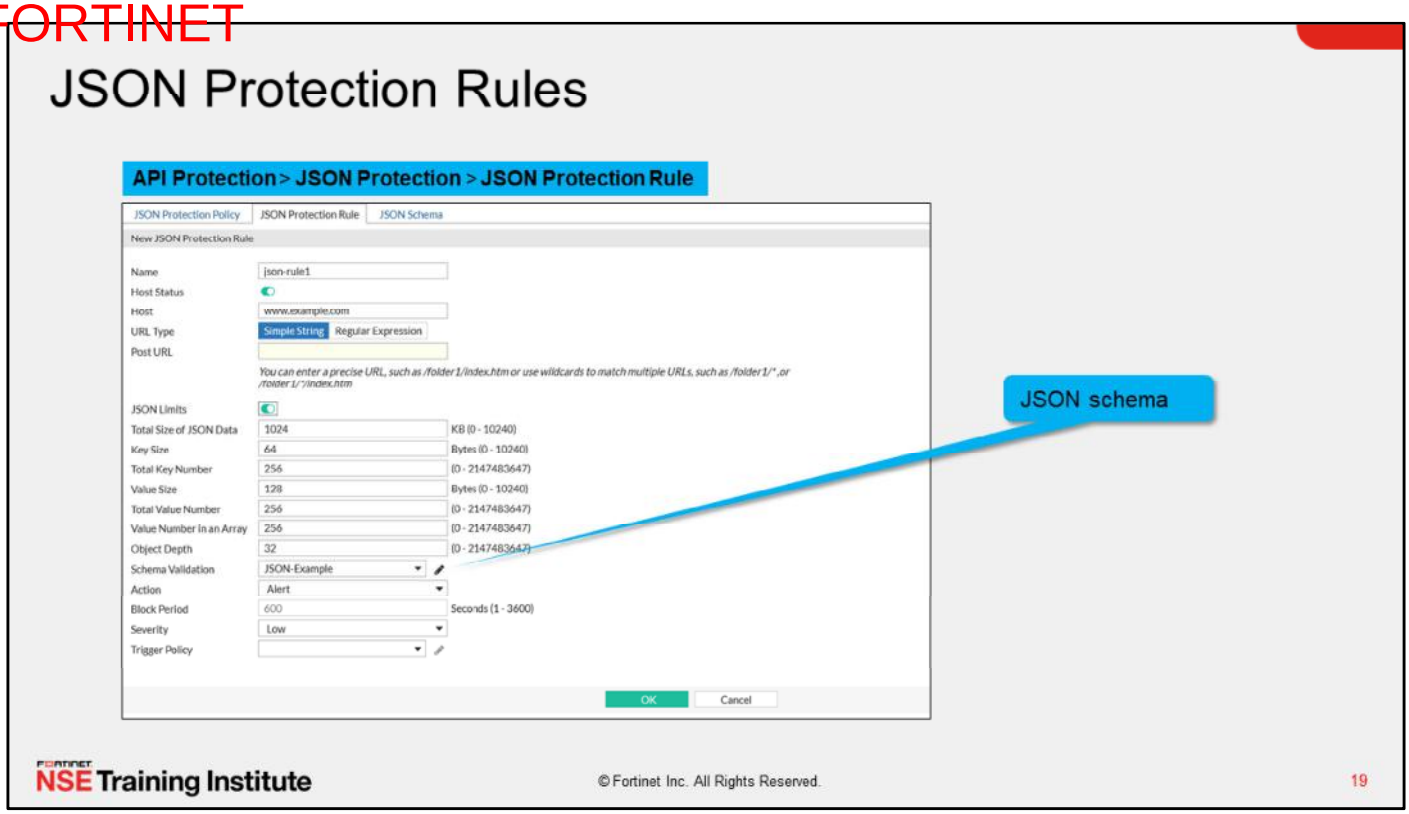
18

A JSON schema file defines the properties and information that an object must contain when it is used in a JSON connection. Several good websites and tools are available to help you to properly format and configure JSON schema. Some examples are:

- `http://json-schema.org`
- `https://jsonschemavalidator.net`

Vouchers & Dumps are Available | WhatsApp +201224560923

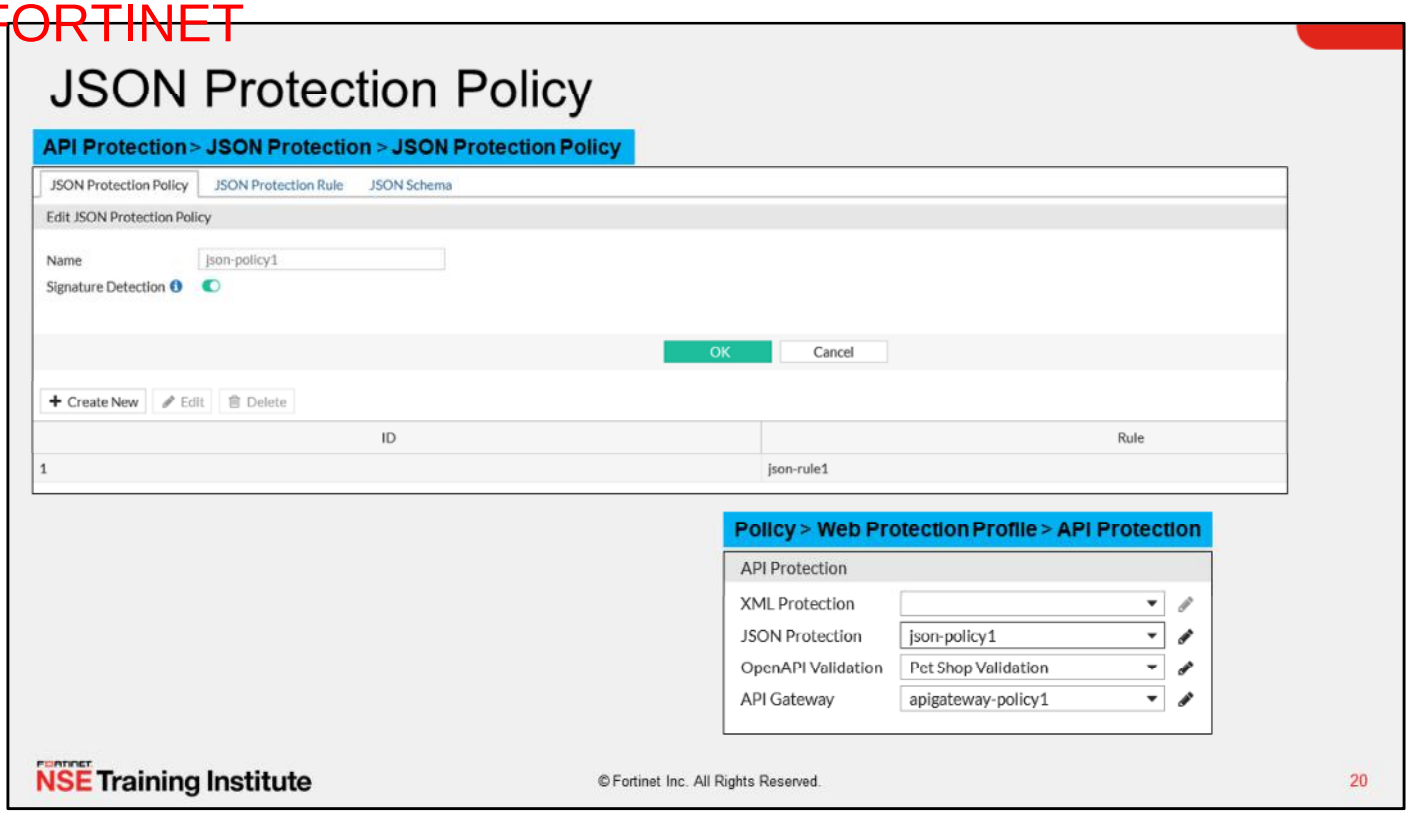
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After uploading the schema, you can select it in a **JSON Protection Rule**. You can define various other limitations, such as hostname and URL, as well as JSON data sizes to help prevent overflow attacks and other potentially harmful JSON queries.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Then like most FortiWeb policies, you can define a JSON protection policy that includes one or more rules, which you can then select in an inline web protection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

XML Protection

- XML is a commonly used data exchange format
- Attackers can send maliciously formatted XML code to servers to attempt to compromise them
  - Commonly called an XML external entity injection (XXE)
- FortiWeb can examine requests for anomalous XML code
- FortiWeb can validate the structure of XML requests with schema files

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

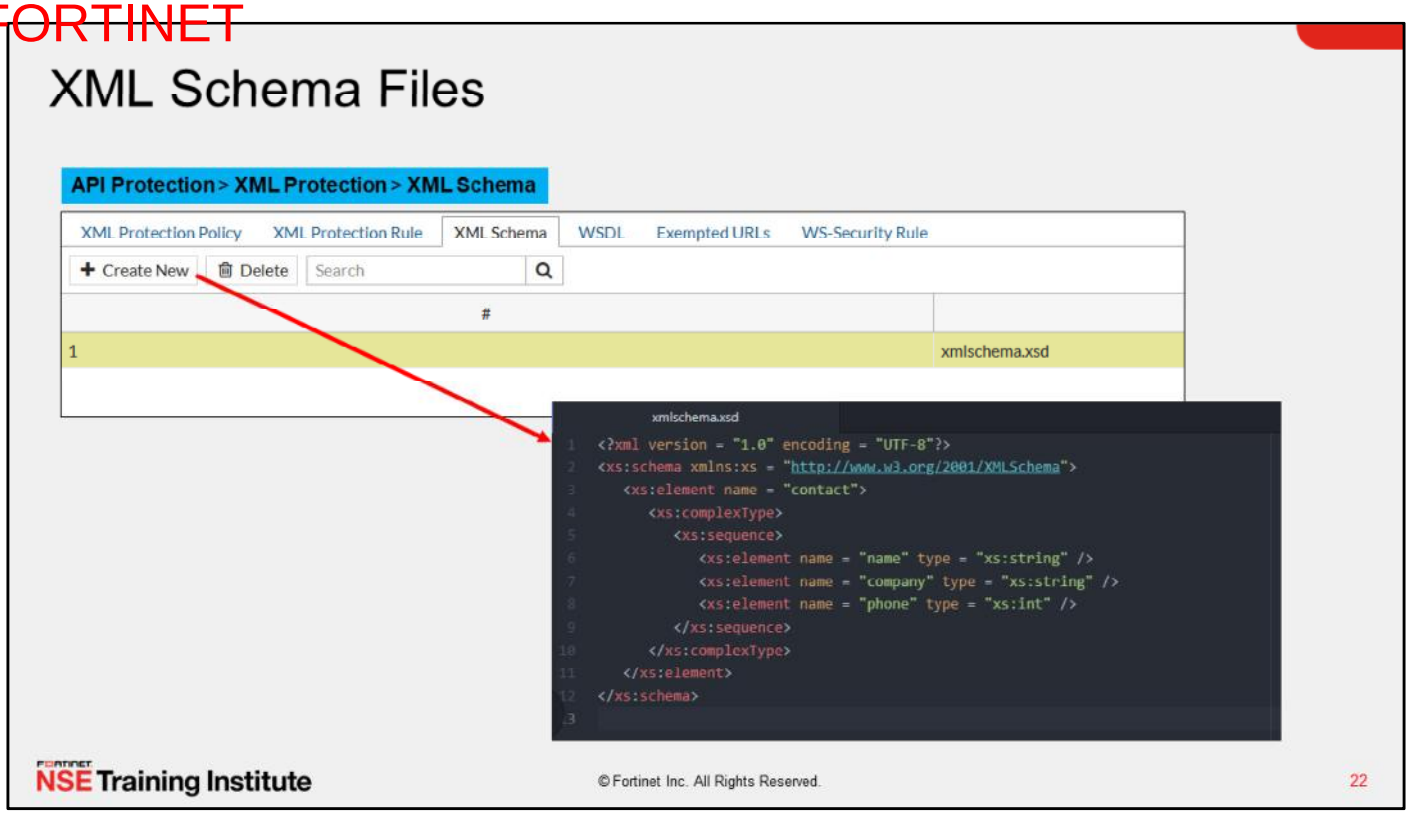
21

Extensible markup language (XML) is a data format commonly used for communicating to and building pages from web servers. Like most languages attackers can perform many different attacks using XML. One of the most well-known attacks is an XML external entity injection where the attacker formats the XML to force a browser or web server to connect to a third server that host malicious files or browse data from a remote server.

You can configure FortiWeb to examine XML requests and force them to follow a schema to prevent these types of attacks, and to secure the transactions between the client and your protected web servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

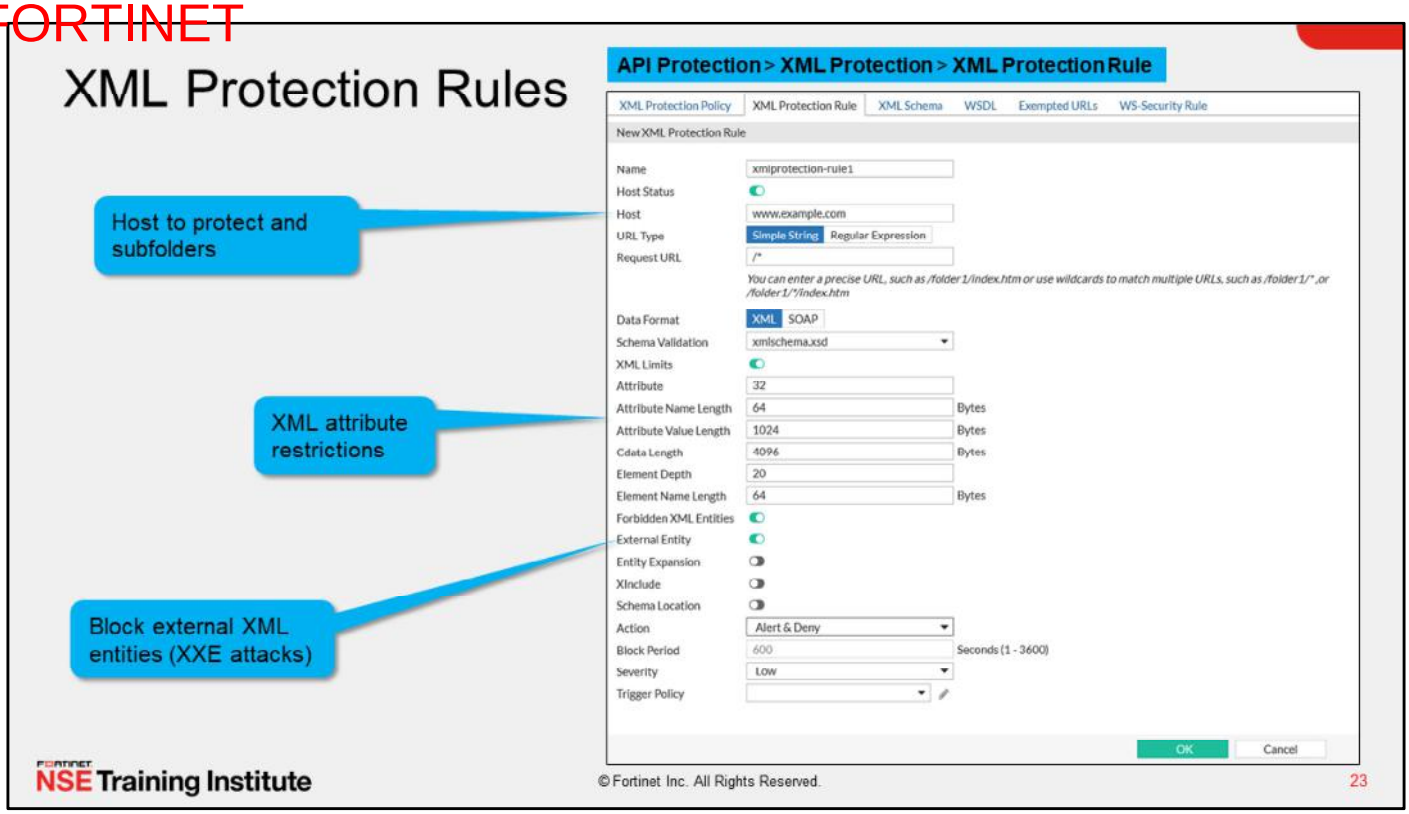
DO NOT REPRINT
© FORTINET
Brave-dumps.com



XML schema files define the data types and information that can be contained in an XML transaction. After you upload a schema file (usually a `.xsd` file), you can be select it in a rule and then a policy. For more information refer to the *FortiWeb Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

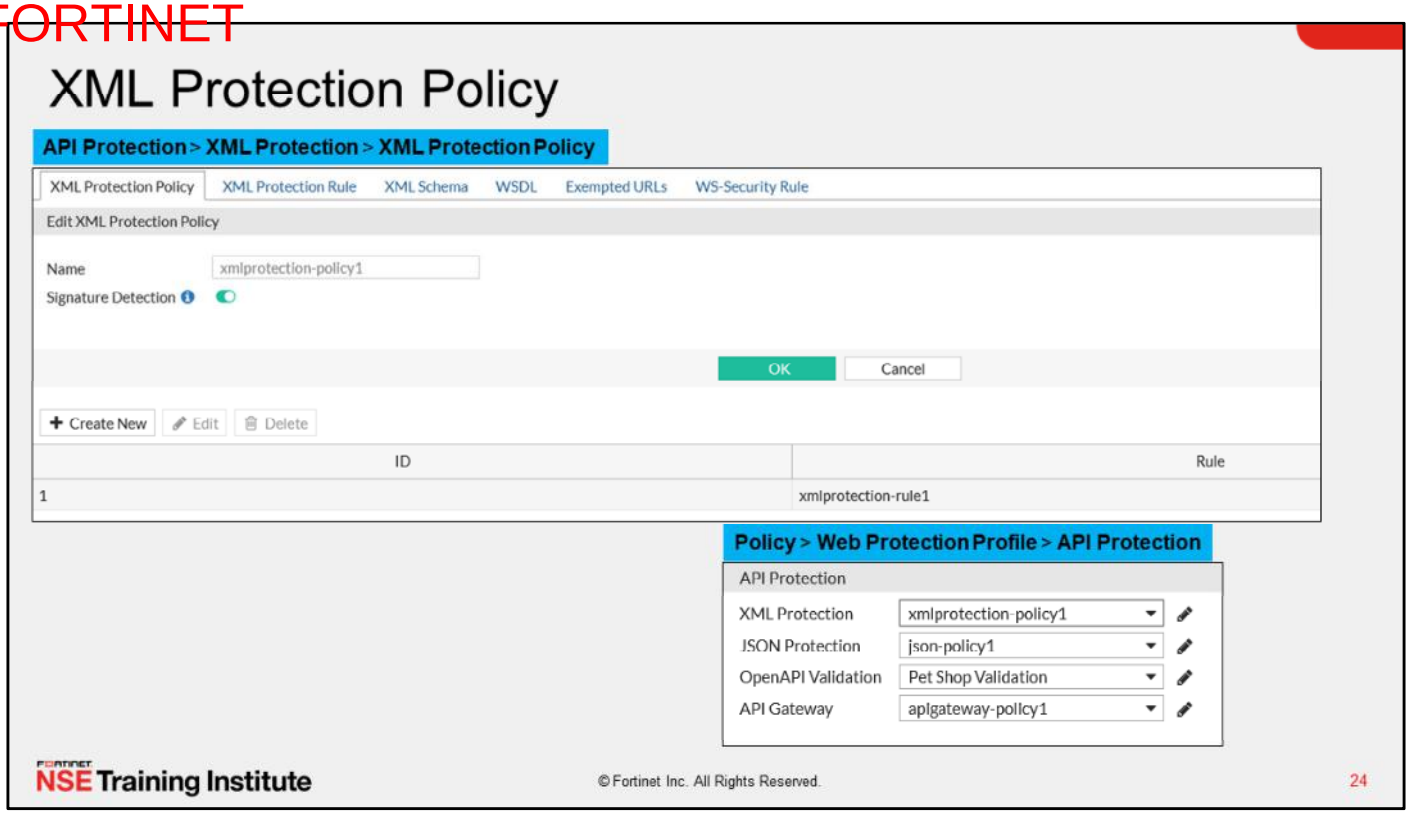


You can define the following settings in an XML protection rule:

- Restrictions on host and URL queries
- Schema file validation information
- XML attribute length and depth
- XML entity configurations, such as limit external entries, expansion, and Xinclude settings
- Block action and trigger policy

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you define a rule, you can bundle it into an XML protection policy and then apply it in a web protection rule. You can configure multiple rules in a single XML protection policy. It is a good practice to tailor your XML rules to specific web applications and directories to maximize the restrictions placed on XML queries.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Other XML Protections

- WSDL are XML schema for SOAP connections
- Exempted URLs allow whitelisting of URLs from any XML protection
- WS-Security rules allow the encrypting, decrypting, and signing of SOAP messages

API Protection > XML Protection

XML Protection Policy | XML Protection Rule | XML Schema | WSDL | Exempted URLs | WS-Security Rule

Edit Exempted URLs

Name: Exemptions

OK | Cancel

+ Create New | Edit | Delete

ID	URL Type	URL
1	Simple String	www.example.com/*

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

Web services description language (WSDL) is used to help define connections and announce web services. It is commonly used with the simple object access protocol (SOAP) protocol. FortiWeb can validate WSDL schema against traffic.

To help with troubleshooting, you can define URLs to be exempt from API protection in the **Exempted URLs** tab.

WS-Security rules further secure SOAP protocol application by allowing FortiWeb to encrypt, decrypt, and sign SOAP messages as they pass through FortiWeb to the end application.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Many web protocols can be defined and restricted using a _____.
   A. Dictionary file
   B. Schema file ✓
   C. Configuration file
   D. Password file

2. How many JSON, XML, and API protection policies can you selected in a web protection profile?
   A. 0
   B. 1 ✓
   C. 2
   D. 200

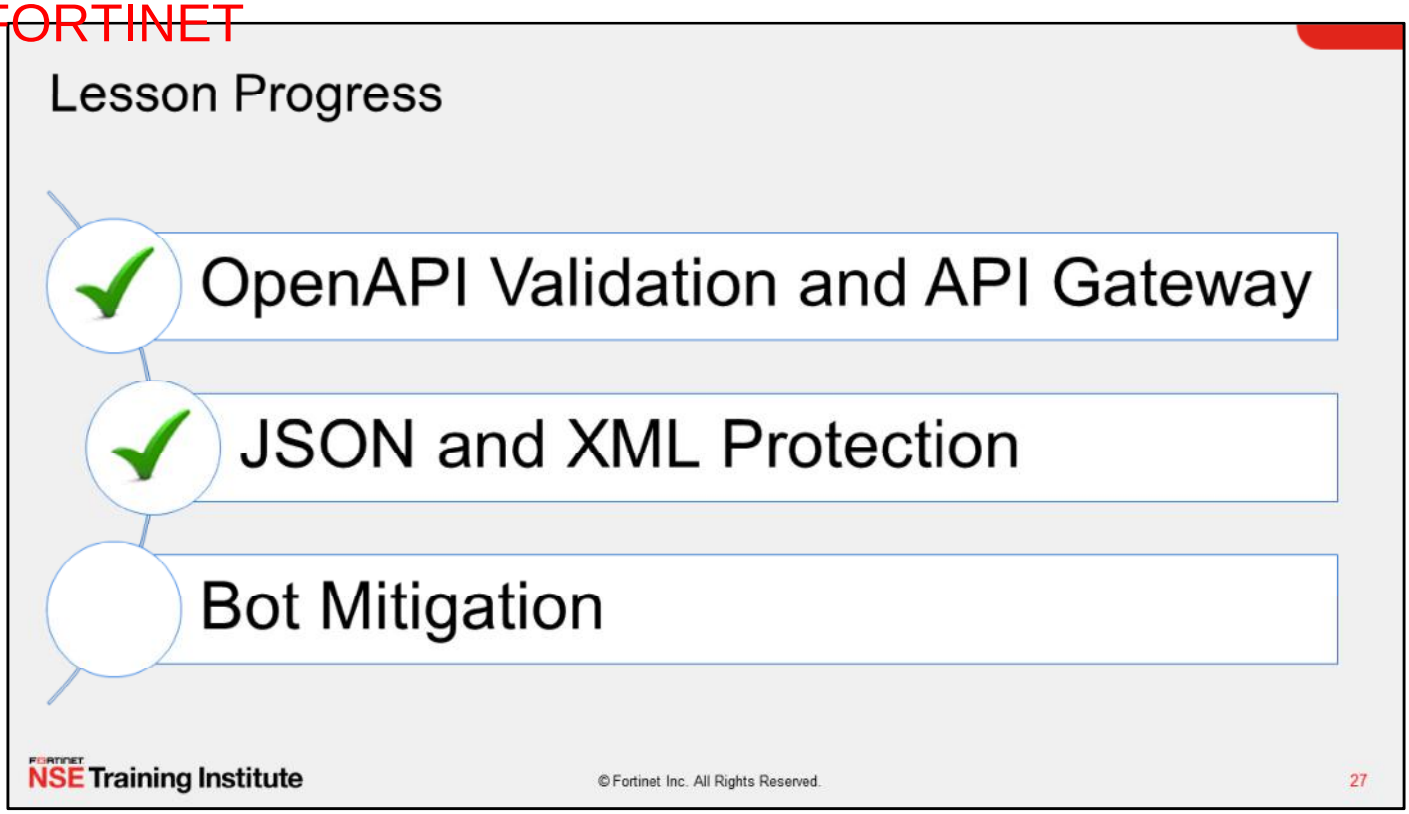
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

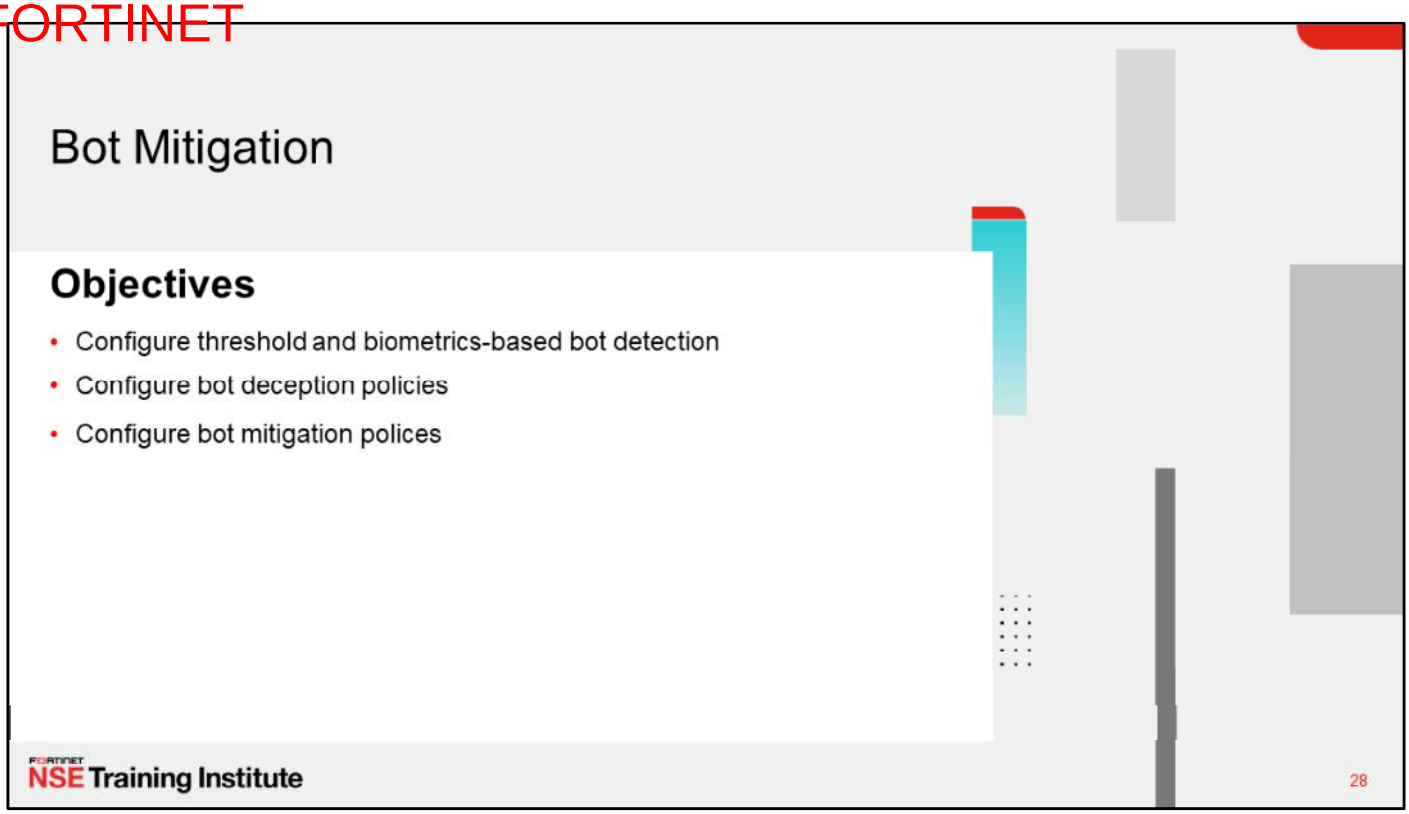


Good job! You now know how to configure FortiWeb to validate JSON and XML connections.

Now, you will learn about how to detect and mitigate attacks from internet bots.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

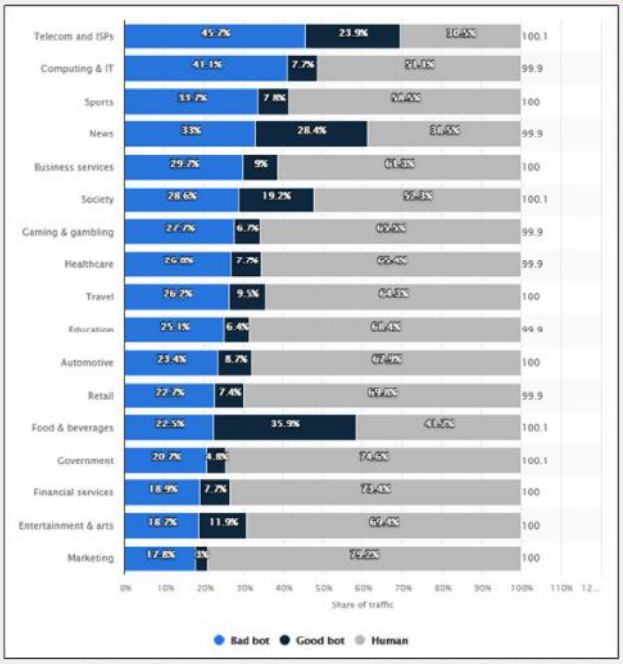
By demonstrating competence in configuring FortiWeb to mitigate bot attacks, you will be able to detect and mitigate damage caused by unwanted bot activity towards your protected web servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Internet Web Bots

- An internet web bot is a program used to automate tasks on the internet
  - Collect all data (scrapes) from websites
  - Performance and uptime logging
  - Vulnerability testing
  - Malicious activity



Source: https://www.statista.com/statistics/1264540/human-and-bot-web-traffic-share-industry/

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

Internet bots account for over 40% of total internet traffic. Despite a bad reputation, around one third of bot activity is beneficial. Many sites use bots to check uptime and functionality of their websites and companies use bots extensively to maintain up-to-date databases for search results and other useful data without causing undue impact to websites. However, bots can be used maliciously for multiple reasons including testing websites for vulnerability, slowing down connections, scraping all data from websites to find unsecured sensitive information, and much more.

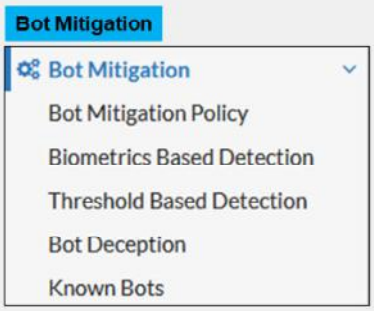
Tightly controlling which bots have access to your protected web servers can not only protect you from malicious activity, but improve bandwidth, performance, and overall server health.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiWeb Bot Mitigation

- FortiWeb has multiple tools to help deal with bots
  - Biometric — Use factors like mouse, keyboard and screen movements to detect bots
  - Threshold — Block bots based on connection and information gathering thresholds
  - Bot deception — Create a fake link to detect a bot that is crawling your websites
  - Known bots — Whitelist known good bots like search engine providers, archive sites
- All of these tools can be bundled into a bot mitigation policy



NSE Training Institute

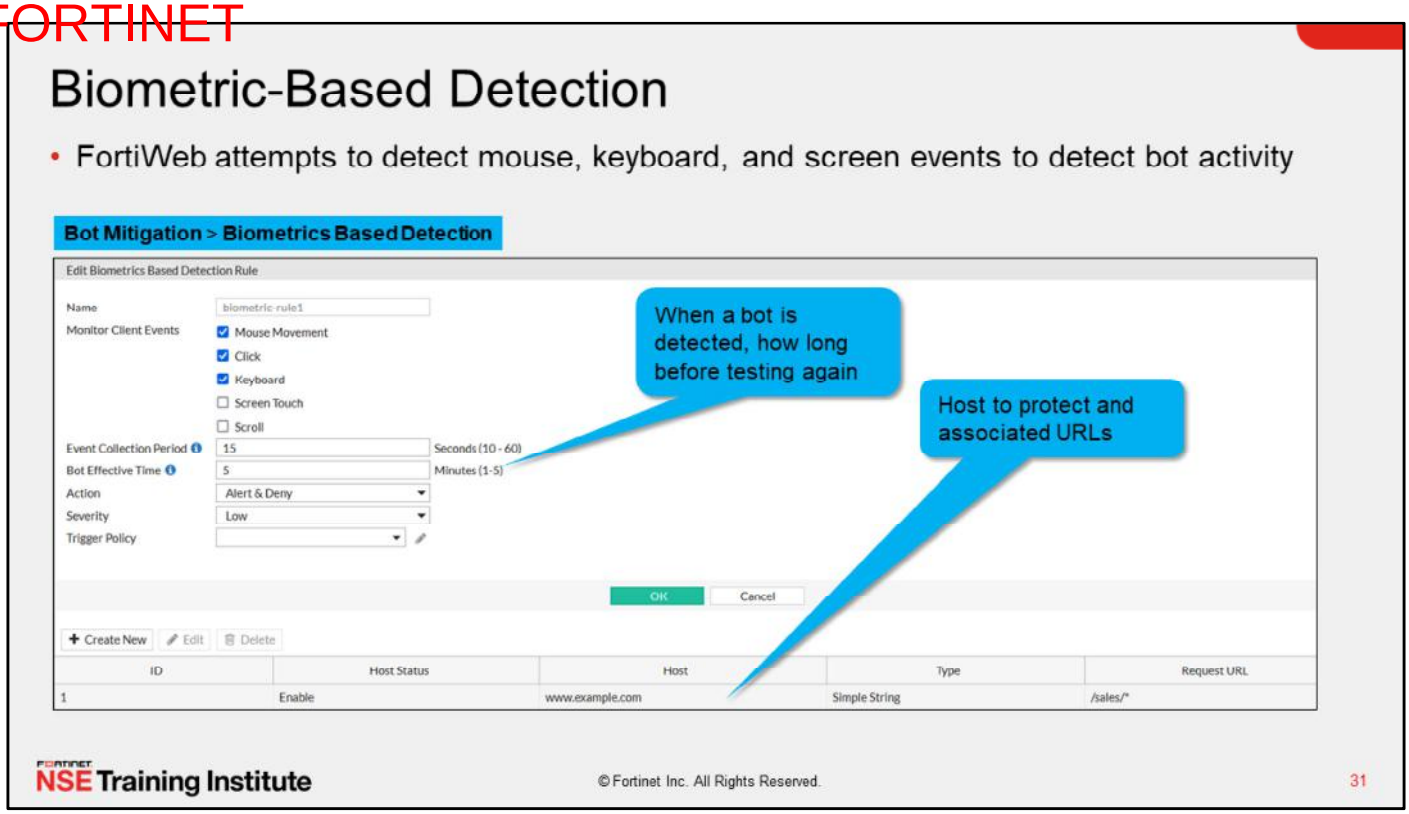
© Fortinet Inc. All Rights Reserved.

30

FortiWeb has several tools that can work together to mitigate most unwanted bot activity. These tools are combined into a bot mitigation policy that you select in the web protection profile for each protected server. You will now review each of the available tools.

Vouchers & Dumps are Available | WhatsApp +201224560923

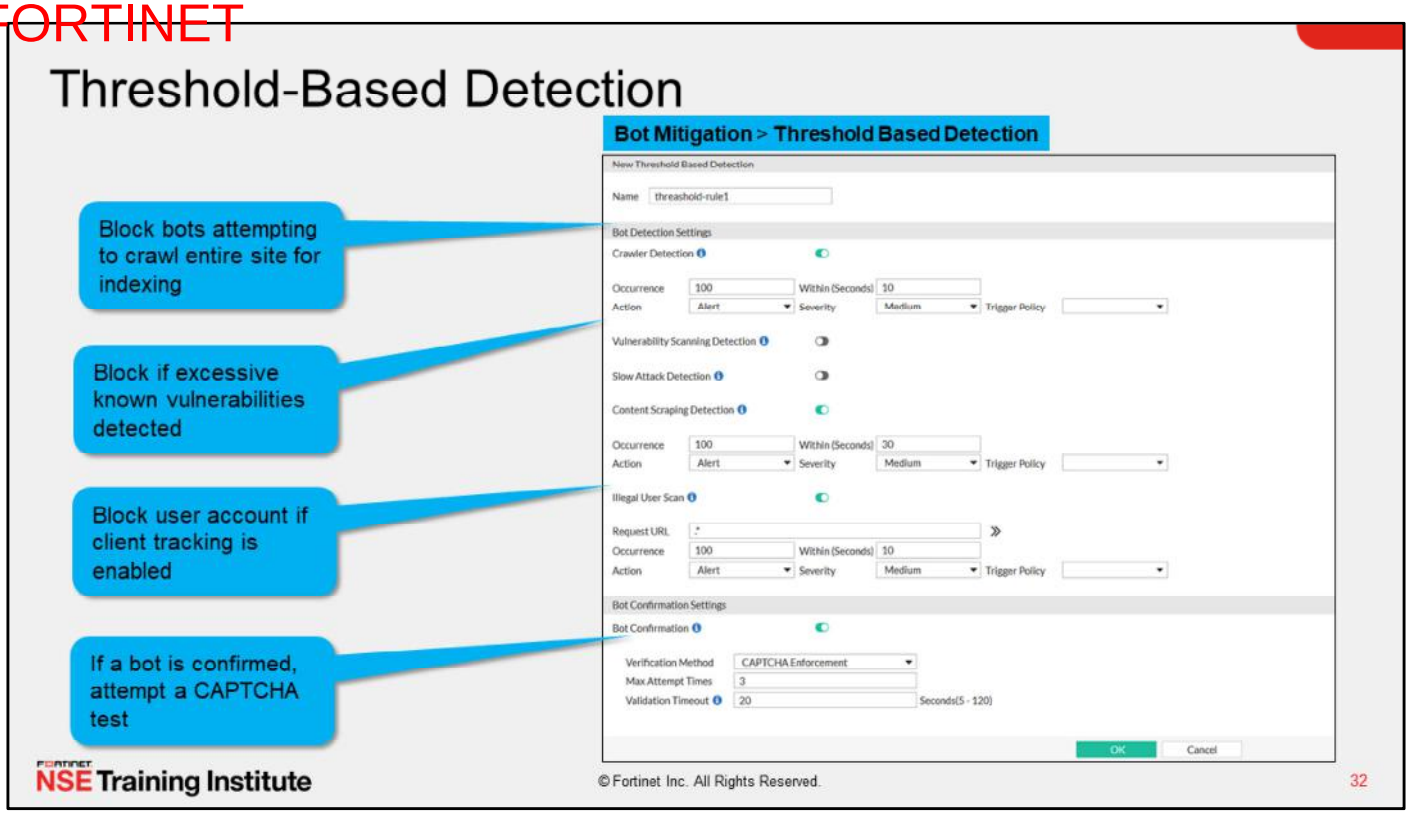
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Biometric detection attempts to use mouse and keyboard activity, screen touch, and scrolling events over a period to try and determine if a connection is human or a bot. This method works only if these types of events are announced over the web connection. Fully static web pages may not benefit from this type of detection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Threshold based detection has multiple optional settings you can enable to prevent repetitive behaviors from impacting your site.

- Crawler detection: Detects tools that browse your website for indexing purposes. Monitors the frequency of 403 and 404 response codes.
- Vulnerability scanning detection: Detects tools that scan your website for vulnerabilities. Monitors the frequency of attack signatures triggered. You need to enable the appropriate signatures in the web protection profile.
- Slow attack detection: Detects denial of service tools that try to go undetected by generating small streams of traffic.
- Content scraping detection: Detects bots that try to copy all the content from your website.
- Illegal user scan: Detects illegal website scans from a particular user. You need to enable user tracking for this feature.
- Bot confirmation: Verifies human users when any of the threshold rules are triggered to allow further access to the website.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Deception

Bot Mitigation > Bot Deception

Edit Bot Deception Policy

Name	deception-rule1
Deception URL	http://www.example.com/fake.php
Action	Alert & Deny
Block Period	600 Seconds (1 - 3600)
Severity	Low
Trigger Policy	

OK Cancel

+ Create New Edit Delete

ID	Host Status	Host	Type	Request URL
1	Enable	www.example.com	Simple String	/*

www.example.com source

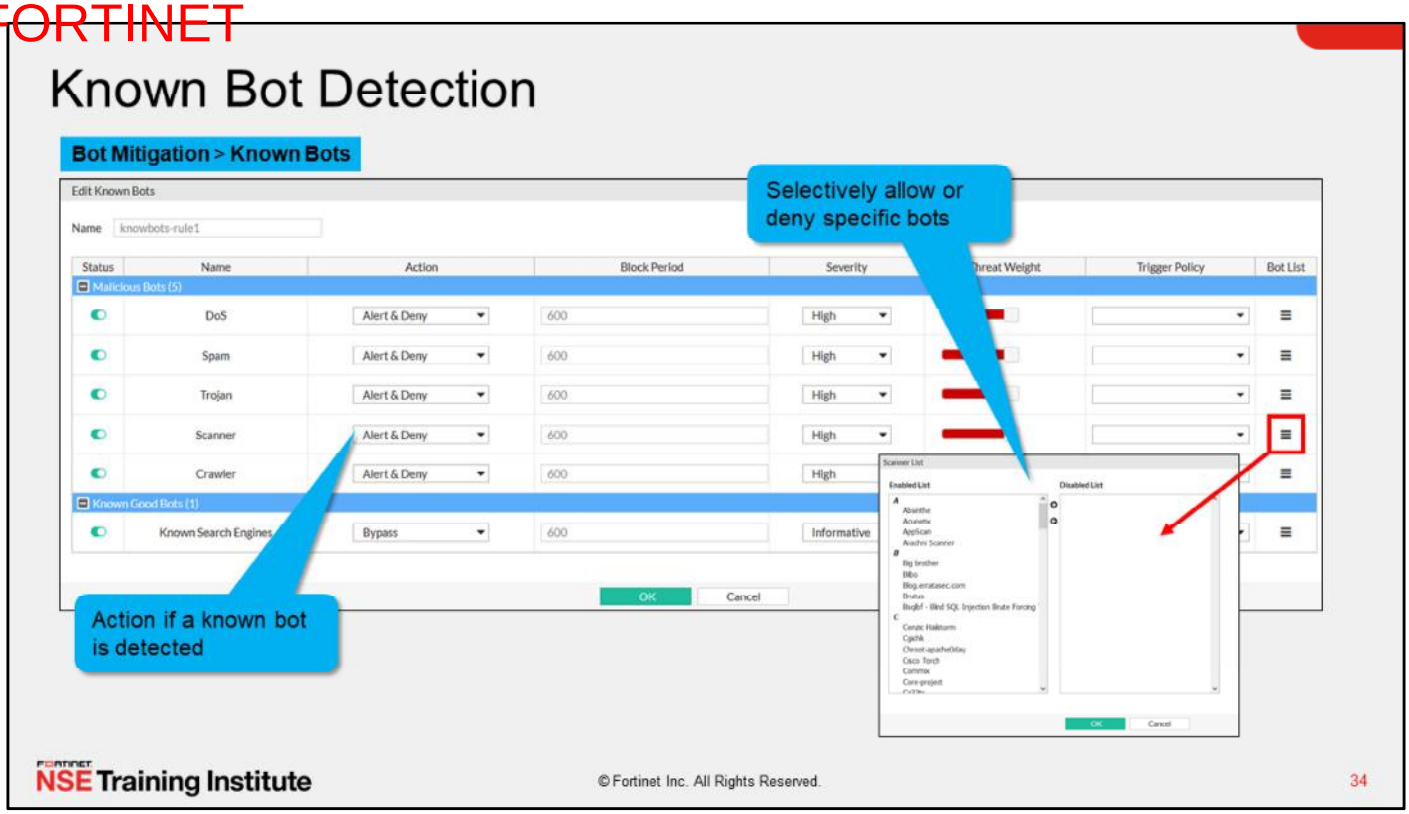
```
</div><!-- #page -->

<script type='text/javascript' src='http://www.example.com/wp-includes/js/wp-embed.min.js?ver=5.2.13'></script>
    <script>/(trident|msie)/i.test(navigator.userAgent)&&document.getElementById&&window.addEventListener&&window.a

  <div id="bitnami-banner" data-banner-id="b38aa">  <style>#bitnami-banner{z-index:100000;height:80px;padding:0;wid
(function(){var banner=document.getElementById("bitnami-banner");var closeButton=document.getElementById("bitnami-c
//]]></script> </div>  <a href="http://www.example.com/fake.php" style='display:none'>login</a></body>
</html>
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 33

Bot deception inserts a hidden URL link into every page of a website being monitored. If a crawler bot attempts to visit the link it is flagged, and FortiWeb takes the defined action. This method helps to catch bots that are very slowly crawling sites in an attempt to avoid threshold detections. If a connection regularly attempts to visit the deception link, it is a good sign that the connection is being initiated by a bot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb maintains a list of known bots and their connection parameters. By default, FortiWeb blocks malicious bots and allows known search engines. You can customize which specific bots and groups that FortiWeb allows. If desired, you can deny search engines from crawling and indexing your websites, but for that you need to change the action associated with the **Known Search Engine** category.

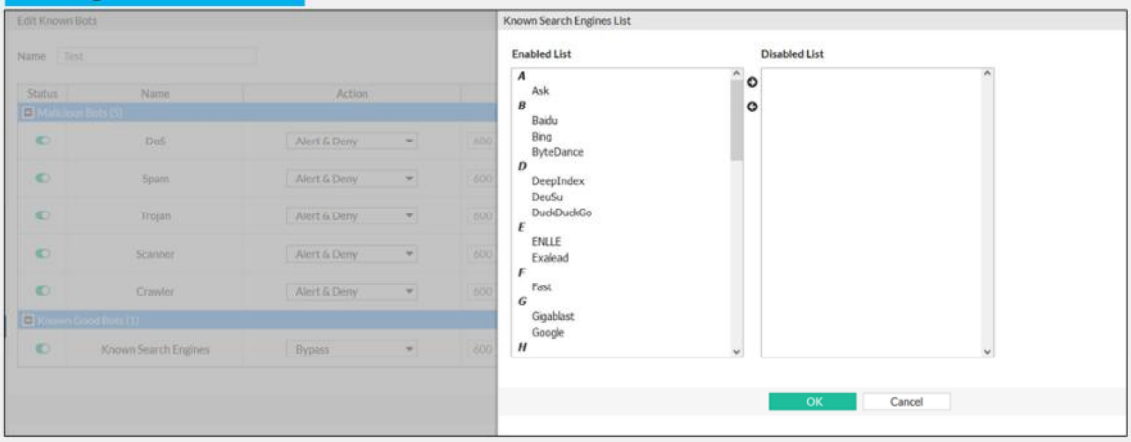
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Known Bots—Search Engines

- Maintained by FortiGuard
- Internet sites should be accessible by search engine; otherwise, they're effectively invisible

Bot Mitigation > Known Bots



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

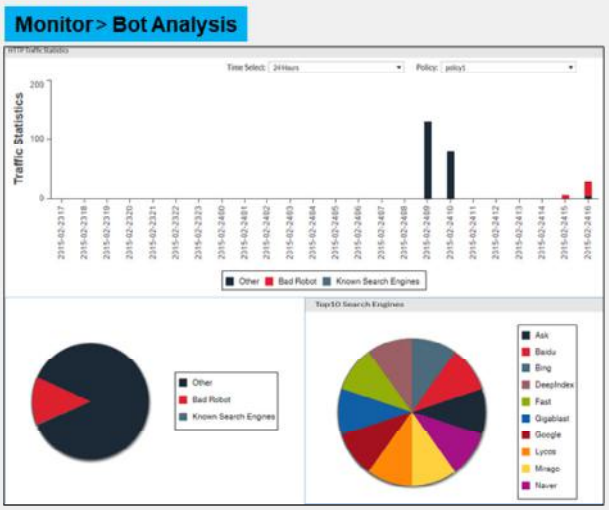
If the client isn't a person—if it's a bot—then you should use different tactics. If all your websites should be easily found on Google or Bing, for example, then you should allowlist them by their public IP address on the internet, in the list of known search engines on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Bot Analysis

- Statistics on traffic from known search engines and abusive scripts, including `ContentSmartz`, `curl`, and `wget`
- `User-Agent:` easily spoofed; known search engines uses IP addresses



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

Search engine crawlers aren't the only type of bots that may be trying to access your web applications. Blog comment spam bots and content scrapers—scripts that steal web pages, images, and videos from other websites—might also being trying to access them. These other types of bots are often used to populate sites so that their owners can get advertising revenue without paying authors.

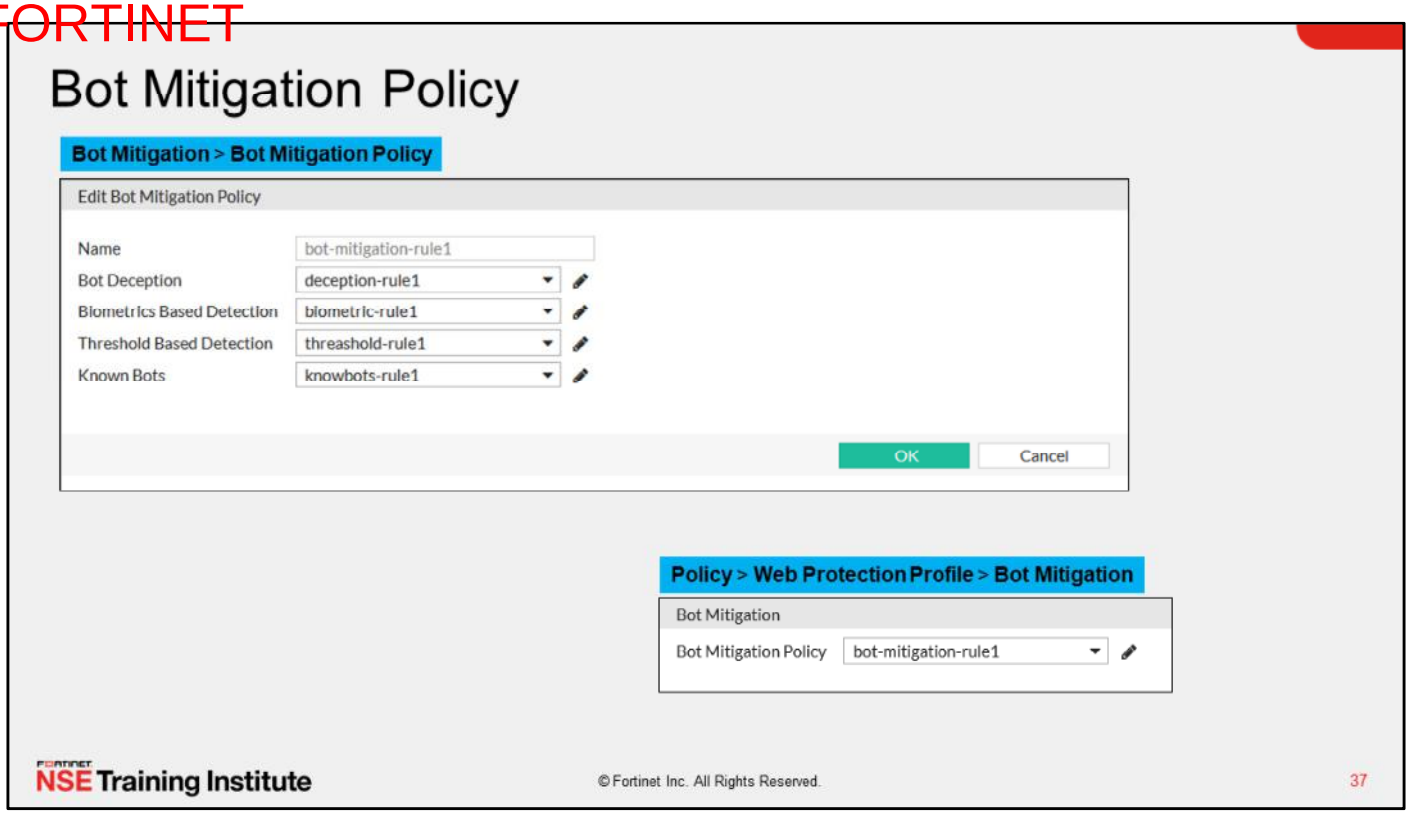
Sometimes, power users use command-line tools such as `curl` and `wget` to download web pages for offline viewing, and—unless you block them—they report their `User-Agent:` string.

Some bots, such as ContentSmartz, are designed specifically for malicious use. Because `User-Agent:` strings are not authenticated or encrypted, it's easy to fraudulently claim to be something more innocent such as `wget`. This is why the FortiWeb feature for known search engines doesn't rely on that HTTP header.

If you think that a content scraper is attacking your websites, review the **Bot Analysis** page. You may want to enable **Real Browser Enforcement** to protect your pages from theft.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you've created a bot mitigation rule, you can bundle the rules together in a bot mitigation policy, which you can then apply to a web protection profile. FortiWeb then begins to detect and block any malicious bot activity configured in the rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What makes up the majority of internet traffic?
   - ✓ A. Humans
   - B. Good bots
   - C. Bad bots

2. What type of bot may be beneficial to allow to access your website?
   - ✓ A. Search engines
   - B. Spam bots
   - C. Crawler bots

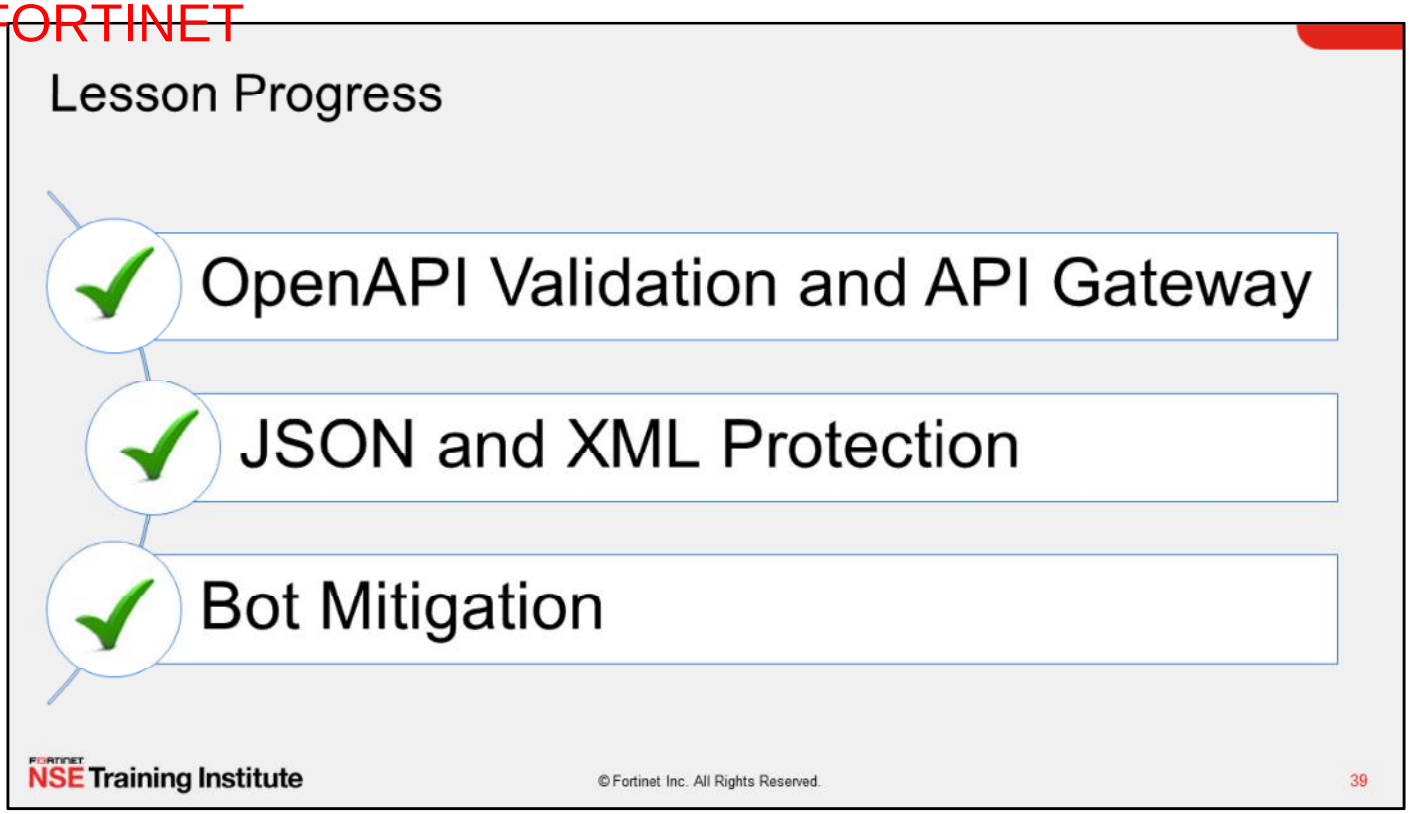
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Identify the purpose of OpenAPI validation and protection
- ✓ Configure OpenAPI validation
- ✓ Configure API gateway policies
- ✓ Configure JSON protection
- ✓ Configure XML protection
- ✓ Configure threshold and biometrics-based bot detection
- ✓ Configure bot deception policies
- ✓ Configure bot mitigation polices

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

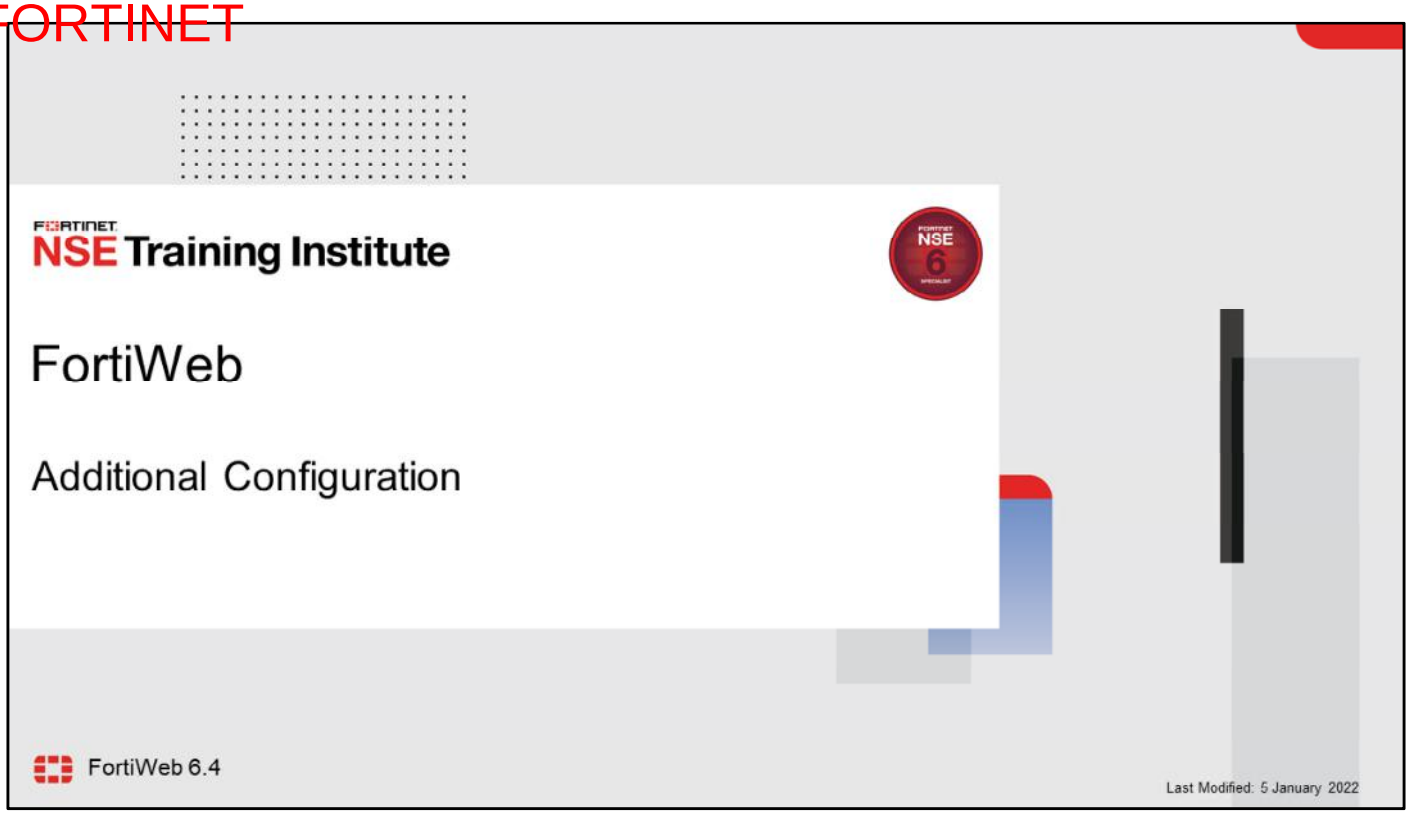
40

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure FortiWeb to protect your web servers from the most common protocols like XML, JSON, and to defend their API interfaces. You also learned how to configure the bot detection and mitigation tools on FortiWeb to allow legitimate bot connections while blocking malicious ones.

Vouchers & Dumps are Available | WhatsApp +201224560923

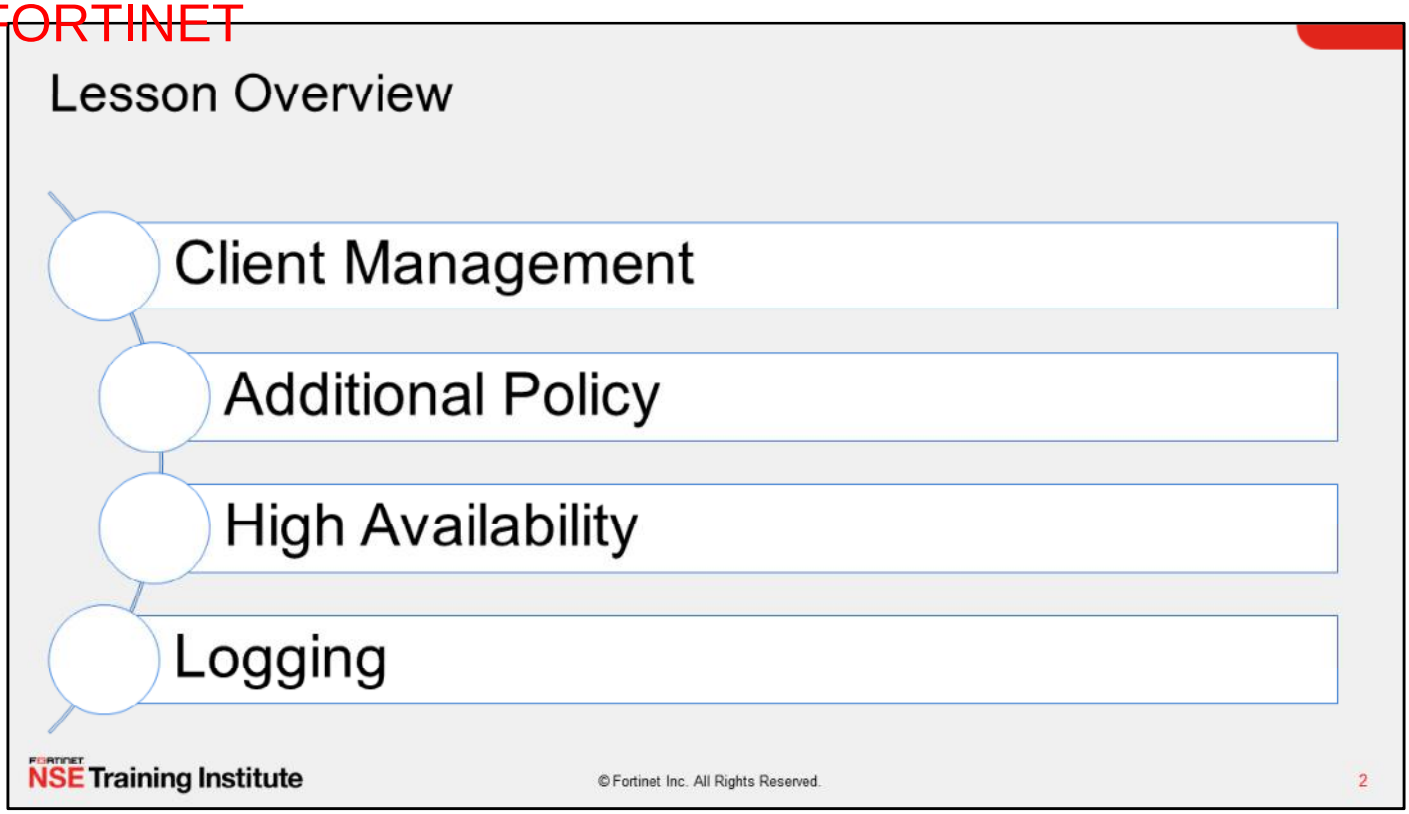
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to control client management and threat levels, secure FTP traffic, and configure high availability (HA) options on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

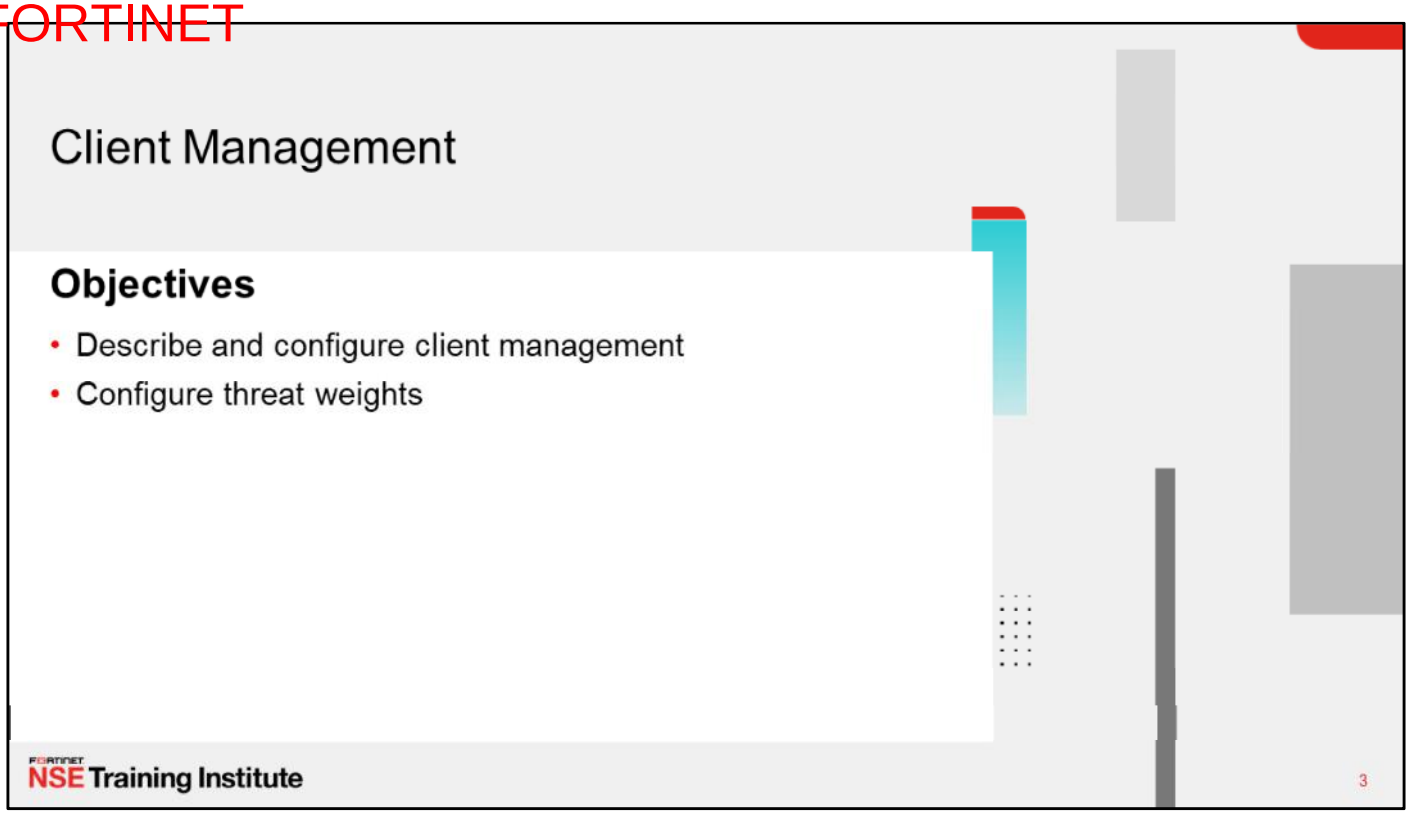
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

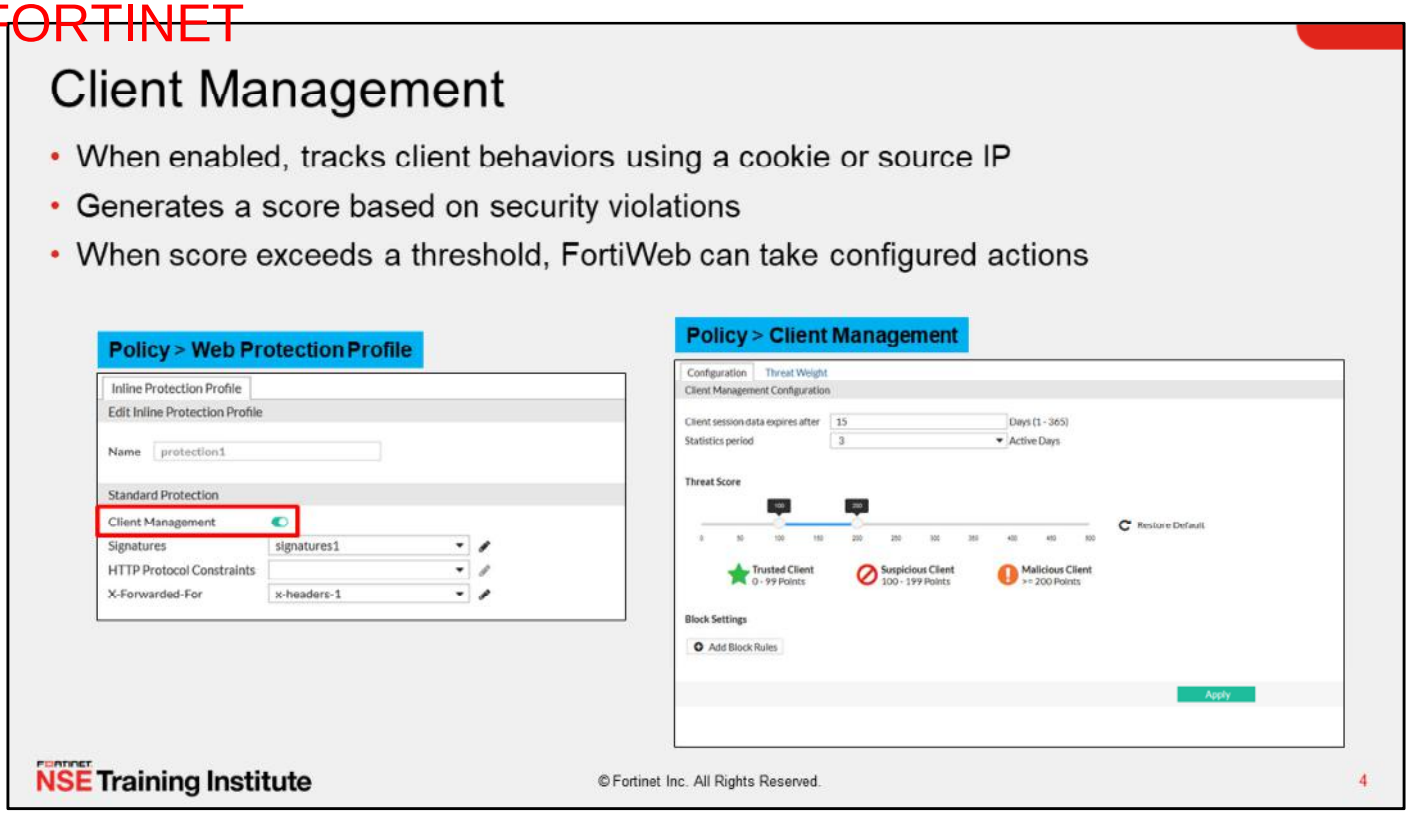


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of client management and how to configure threat weights on FortiWeb, you will be able to more finely tune your security policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



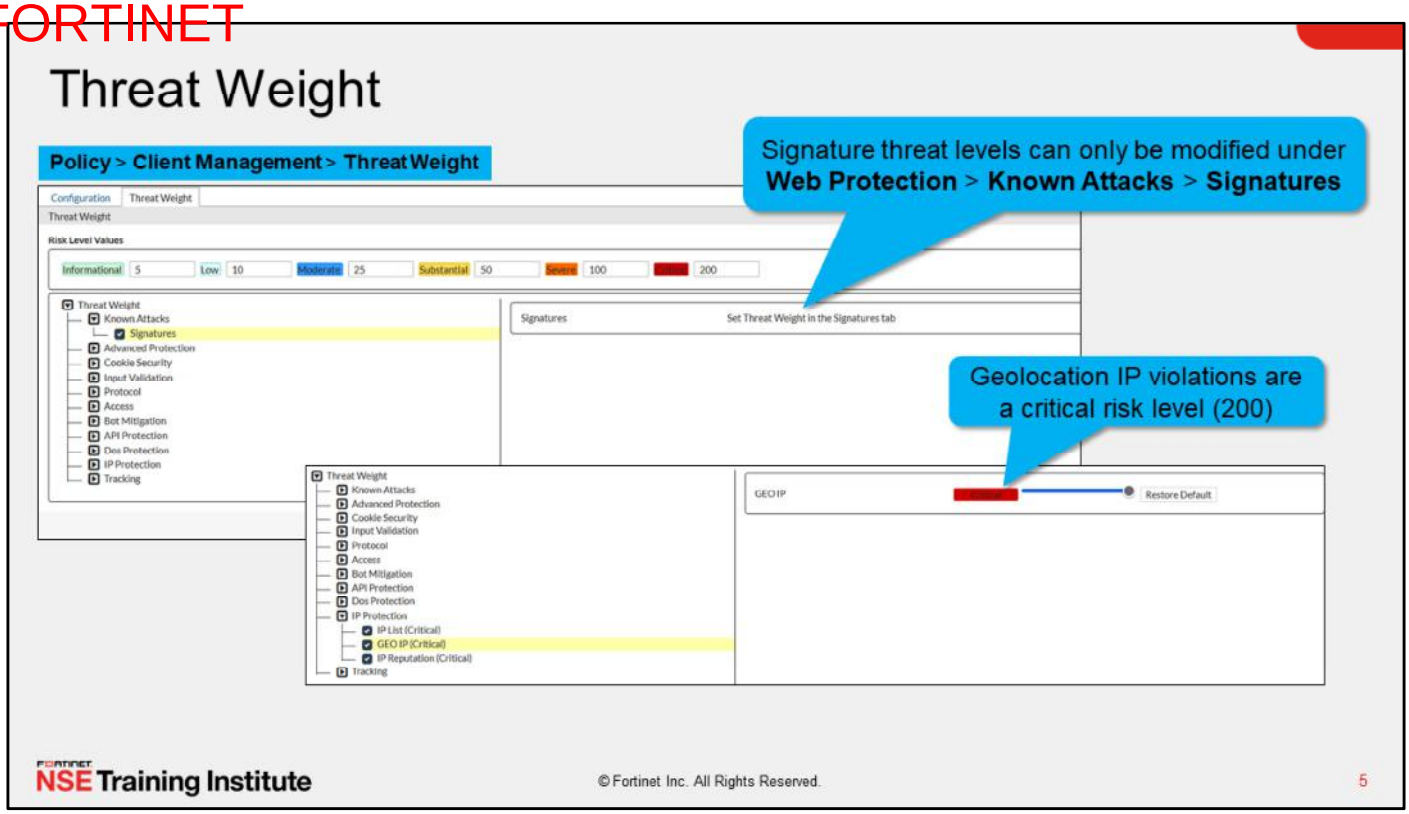
By default, client management is disabled in a web protection profile. When enabled, depending on the mode, FortiWeb will insert a tracking cookie into sessions to help track client behavior.

Based on client actions, FortiWeb will generate a configurable threat score that can then be used to spontaneously block a client if a certain level of activity is observed. This score is the sum of the values assigned to threats performed by the client.

If a client exceeds a certain threat score, ForitWeb can block access from the client for a period of time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can modify threat weights for each type of attack or suspicious activity. Each activity has a risk value that FortiWeb adds up over the monitor period. If a client's threat score exceeds the thresholds, FortiWeb applies the block actions.

While you can modify some threat levels, like IP protection, directly under **Client Management**, you have to configure most threat weights directly in their associated area of the GUI. For example, you can modify signature threat levels on the **Signature Details** tab on the GUI.

Note the default risk-level values. These are universally applied across all types of threats. For example, a *severe* signature violation, which by default is a risk level of 100, is worth the same as a *severe* input violation.

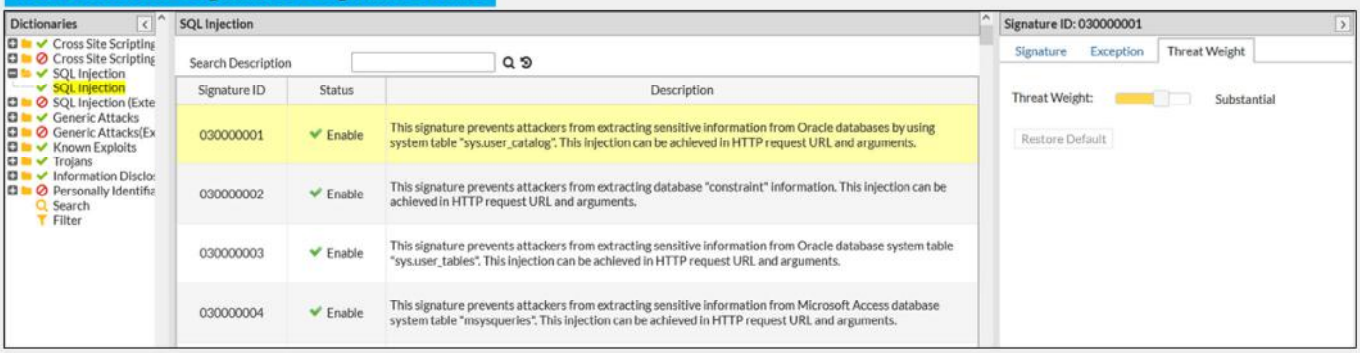
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Threat Weight (Contd)

- Threat weights can be adjusted for most types of detected attacks
- For signatures, each signature has an individual customizable threat weight

Web Protection > Signatures > Signature Details



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

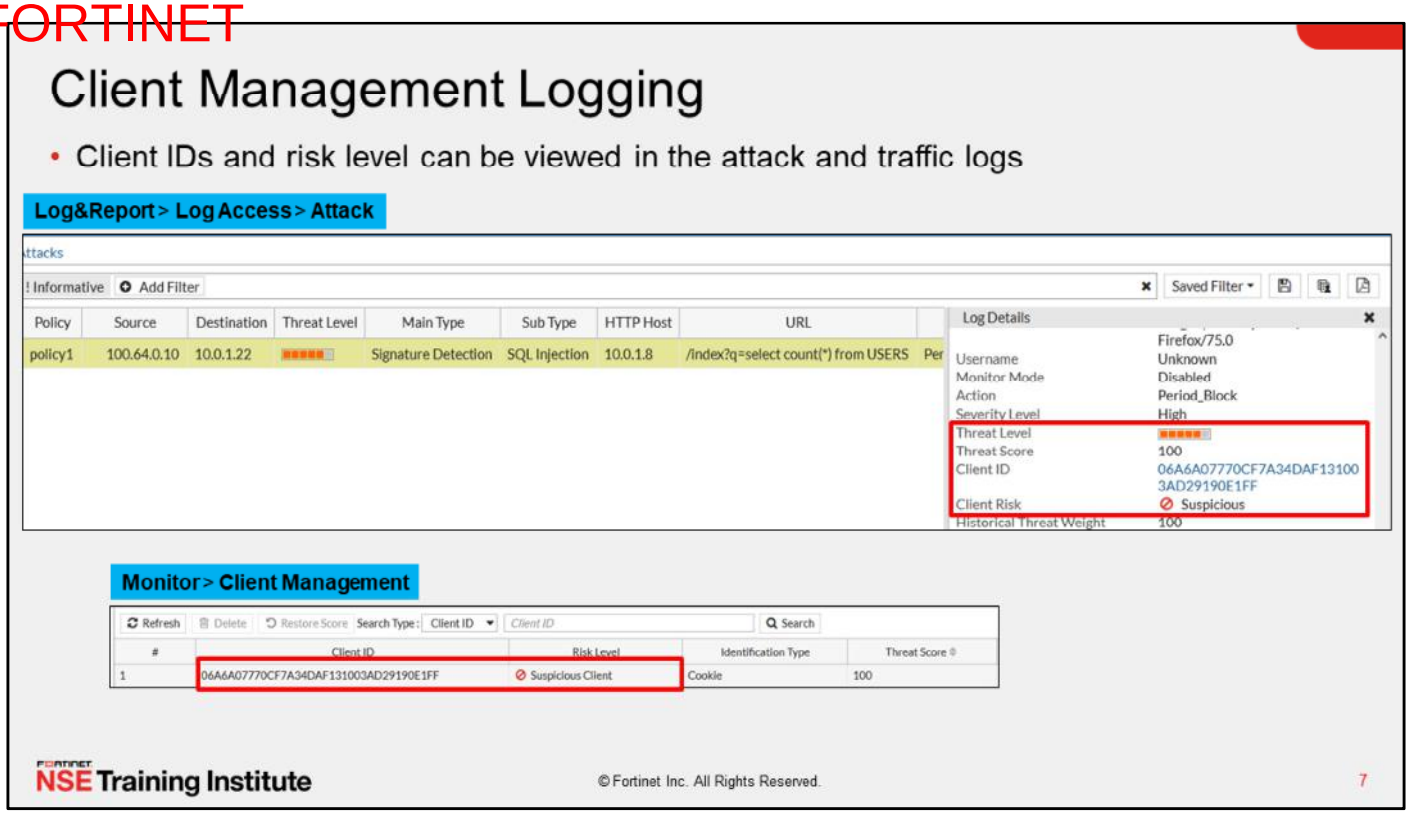
You can customize signatures and other detection policy threat weights in their individual areas of the GUI.

The slide shows an example of the SQL injection signature set. Each signature has a threat weight setting that you can modify to increase or decrease the likelihood that a client will be blocked because of their threat score.

Remember that threat weights and client management block values are global. Changing a signature threat weight changes it for every client that has client management enabled for.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view the **Client ID** in the FortiWeb traffic and attack logs. You must click **More Details** in a log entry to see the associated **Client ID**. In the case of the attack logs, the threat score and risk levels are also displayed. If FortiWeb client management blocks connections for any suspicious clients, the **Client ID,** shown in the associated logs, will also be blocked for all further connections through FortiWeb.

You can view all monitored clients and their associated threat scores on the **Client Management** page. Here you can see each client, their score, and risk level. Administrators can right-click and reset the score of any client to reset their threat level and to allow access if a client is blocked erroneously.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which item is not used to track clients using client management?
   A. Session cookie
   ✓ B. Browser type
   C. IP address

2. What happens by default when a client has a threat score of more than 200?
   A. FortiWeb blocks connections to the client for 60 minutes
   B. Client is flagged as suspicious and monitored
   C. Client receives a pop-up window warning of suspicious activity
   ✓ D. Nothing

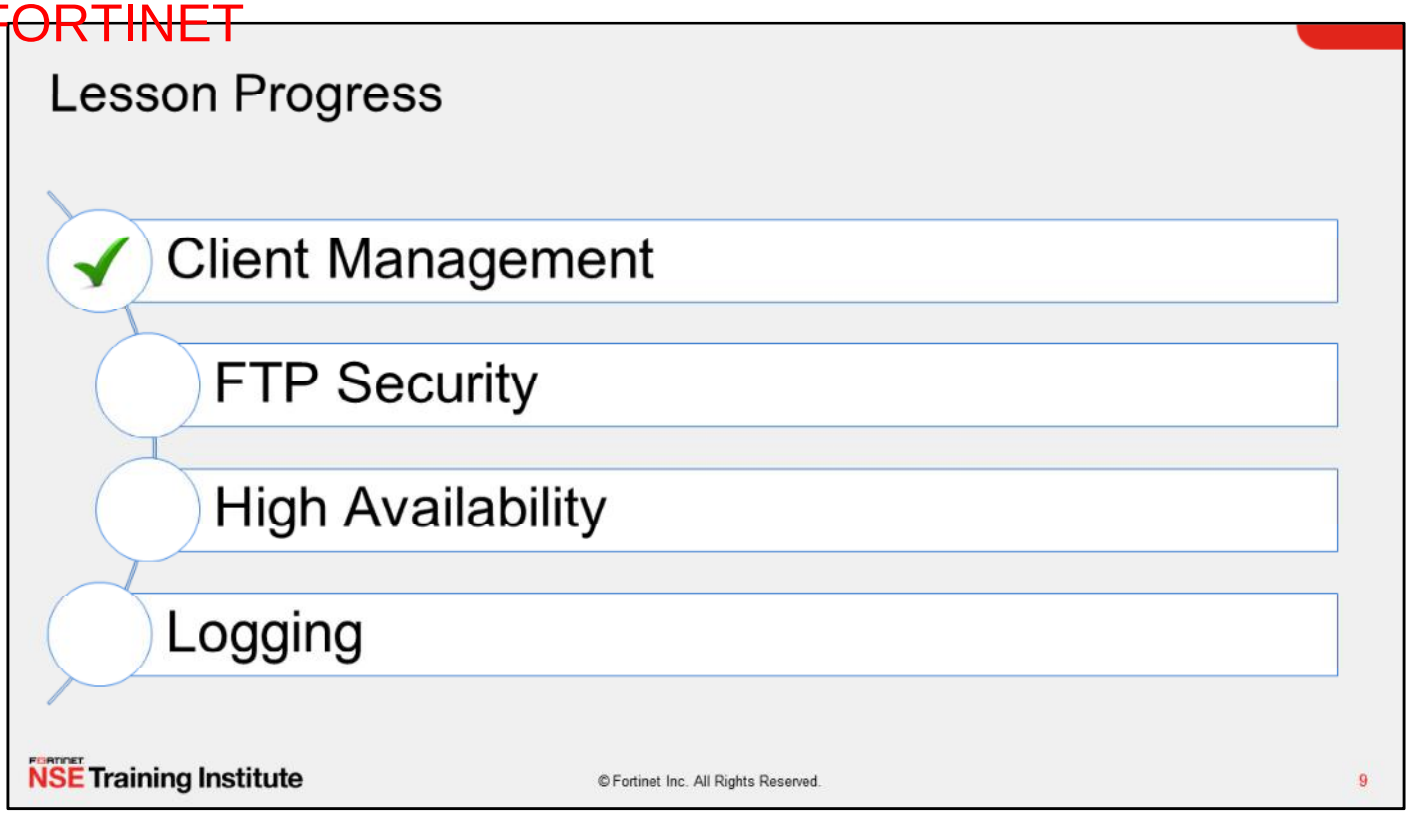
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

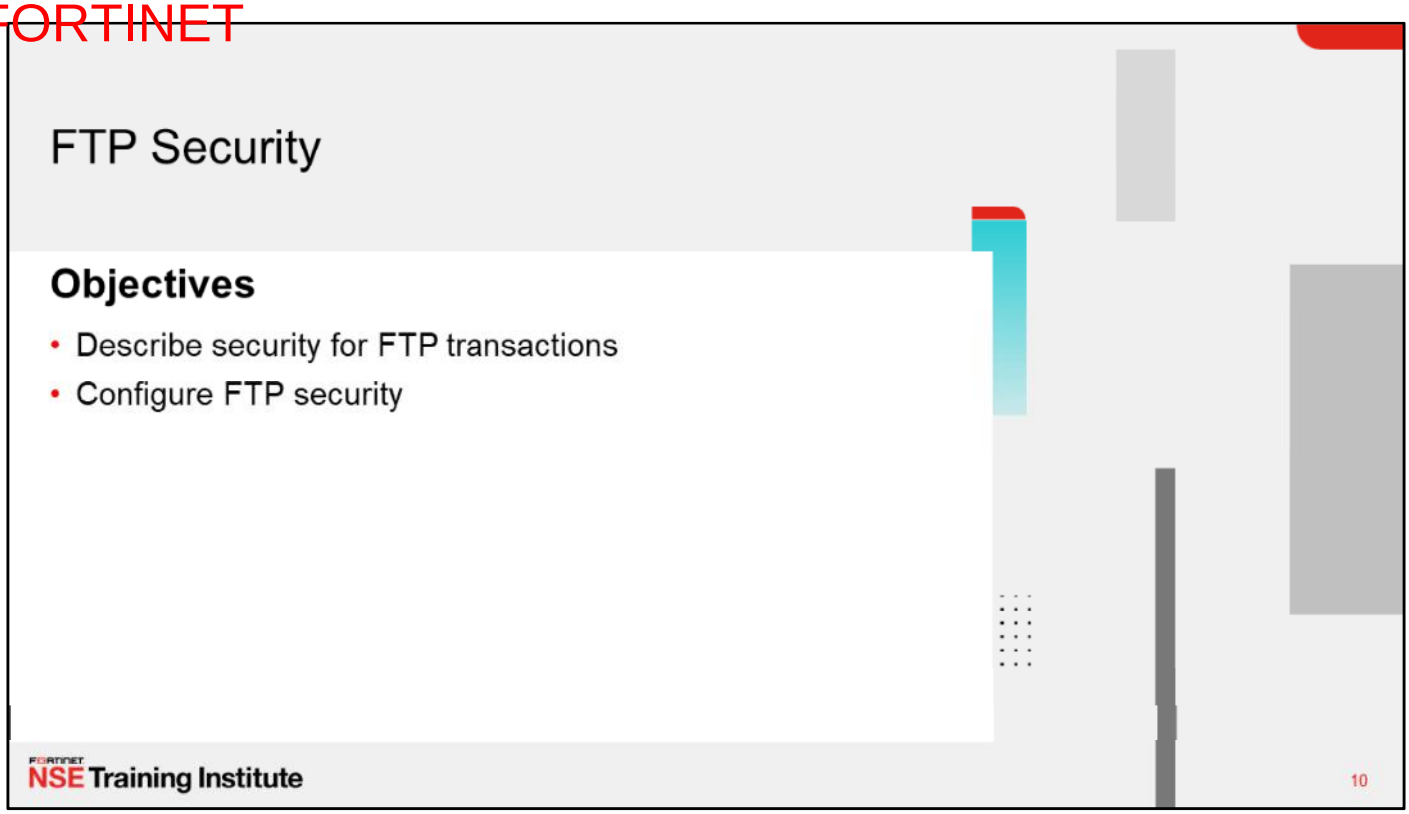


Good job! You now know how to configure redirection on FortiWeb.

Now, you will learn about FTP security on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

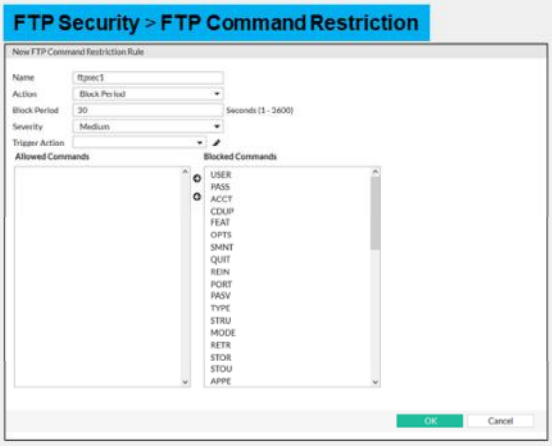
By demonstrating competence in understanding FTP security, you will be able to more granularly control and monitor FTP sessions sent through FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FTP Transactions

- FortiWeb can act as an application layer firewall for potential FTP connections to your protected servers
- Must be enabled as a feature
- Once enabled, any rules created can be selected in a server profile



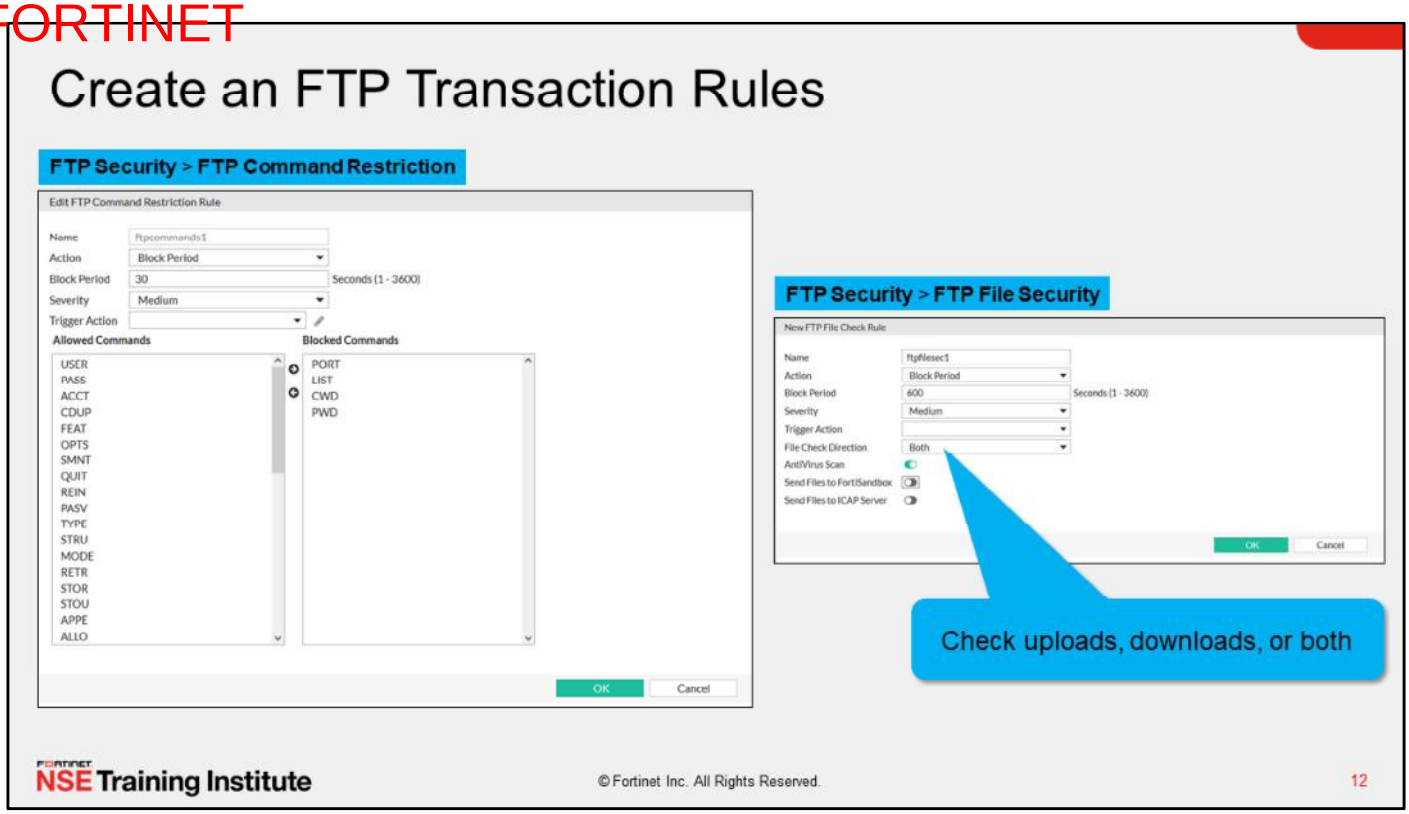
NSE Training Institute © Fortinet Inc. All Rights Reserved. 11

Just like for HTTP/HTTPS applications, you can configure FortiWeb to protect FTP servers. These can be servers hosted in the same location as your web servers, or on different machines. To configure FTP security, you need to perform the following steps:

1. Enable **FTP Security** as a feature on the GUI.
2. Configure any FTP command or file restriction rules required.
3. Create an FTP security profile.
4. Create a new FTP server pool.
5. Create a new FTP server policy, which ties the FTP security profile and server pool together.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiWeb can restrict FTP traffic based on two criteria—FTP commands and file enforcement.

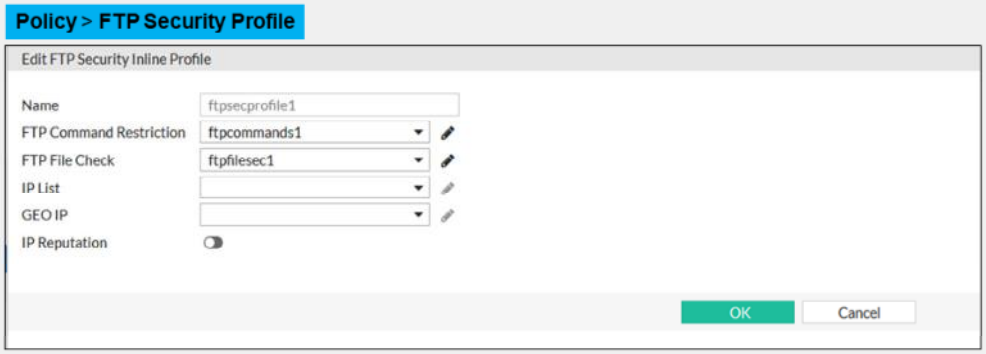
FTP Command Restriction Rules are a simple way to limit what commands are being sent to the FTP server. For example, if you want to prevent users from attempting to view the FTP file system, you need to block the `LIST`, `PWD`, and `CWD` commands. The `PORT` command is always a good command to block because it can make your server into a relay for probing the local network.

For file security, FortiWeb can perform AV scanning on uploads and downloads in addition to sending the file to FortiSandbox or an ICAP server for further inspection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Create an FTP Security Profile



NSE Training Institute

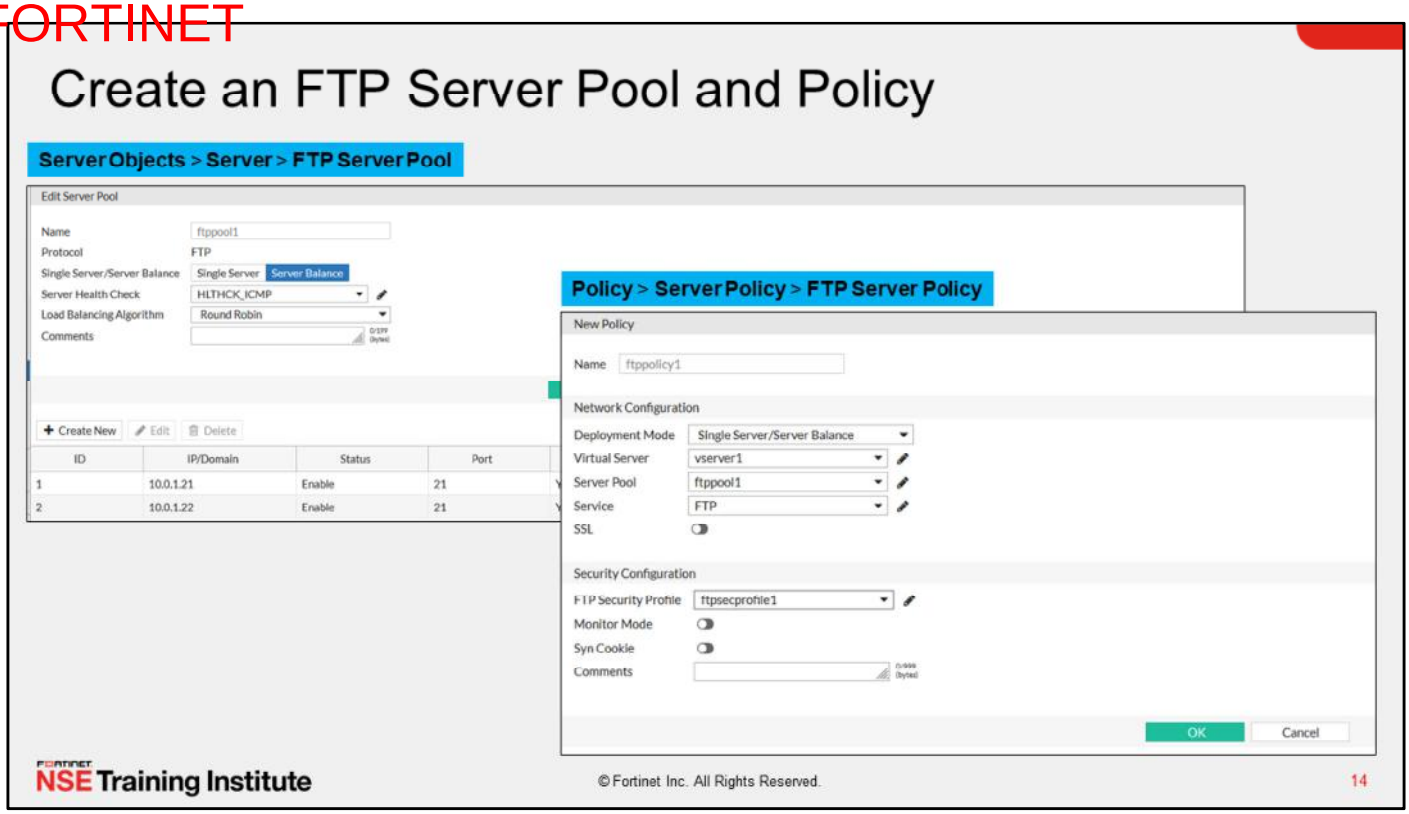
© Fortinet Inc. All Rights Reserved.

13

An FTP security profile groups together command restrictions, file checks, allowed IP addresses, and geolocation information into one profile that can then be selected as a server policy for an FTP server pool. Note this is different from a web protection profile. An FTP security profile is assigned directly to a server and its associated server pool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Just like you configure an HTTP/HTTPS server pool and policy, you must create an FTP server pool and policy.

The FTP server pool lists the available FTP servers (or a single server) and defines how FortiWeb should balance connections between them. Please note that FortiWeb can perform inspection on SSL secured FTP connections (FTPS) by enabling the SSL toggle in the policy and providing the necessary certificate.

FTP server policy ties together all the previous configurations:

1. FTP security profile
2. FTP server pool
3. Virtual server—this is usually the same as HTTP/HTTPS traffic unless you are using a different IP for FTP connections

After you configure all these pieces, FortiWeb will start allowing and scanning FTP traffic according to its associated security profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which configuration is the same for HTTP and FTP traffic through FortiWeb?
   A. Server pool
   B. Security profile
   C. Virtual server ✓

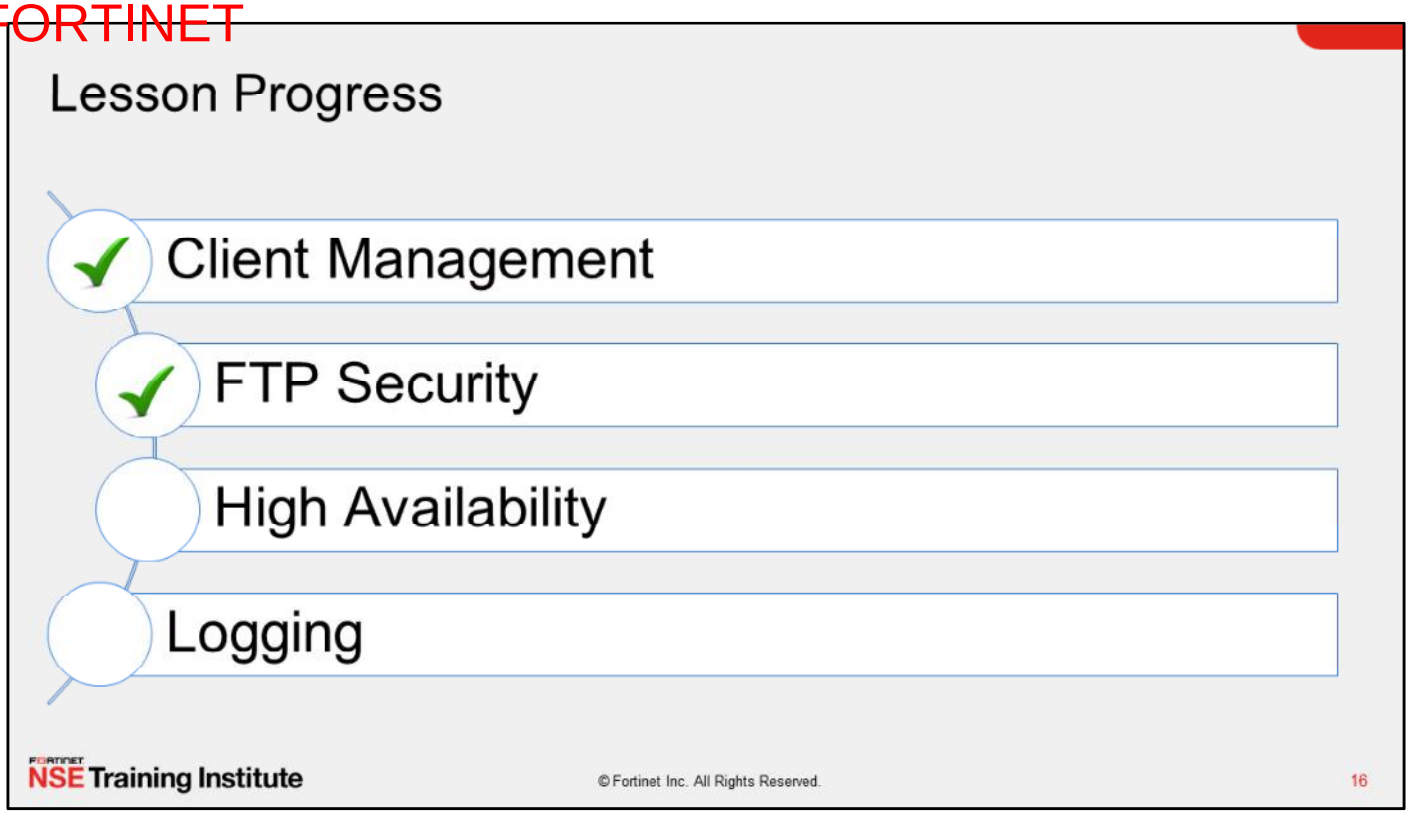
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

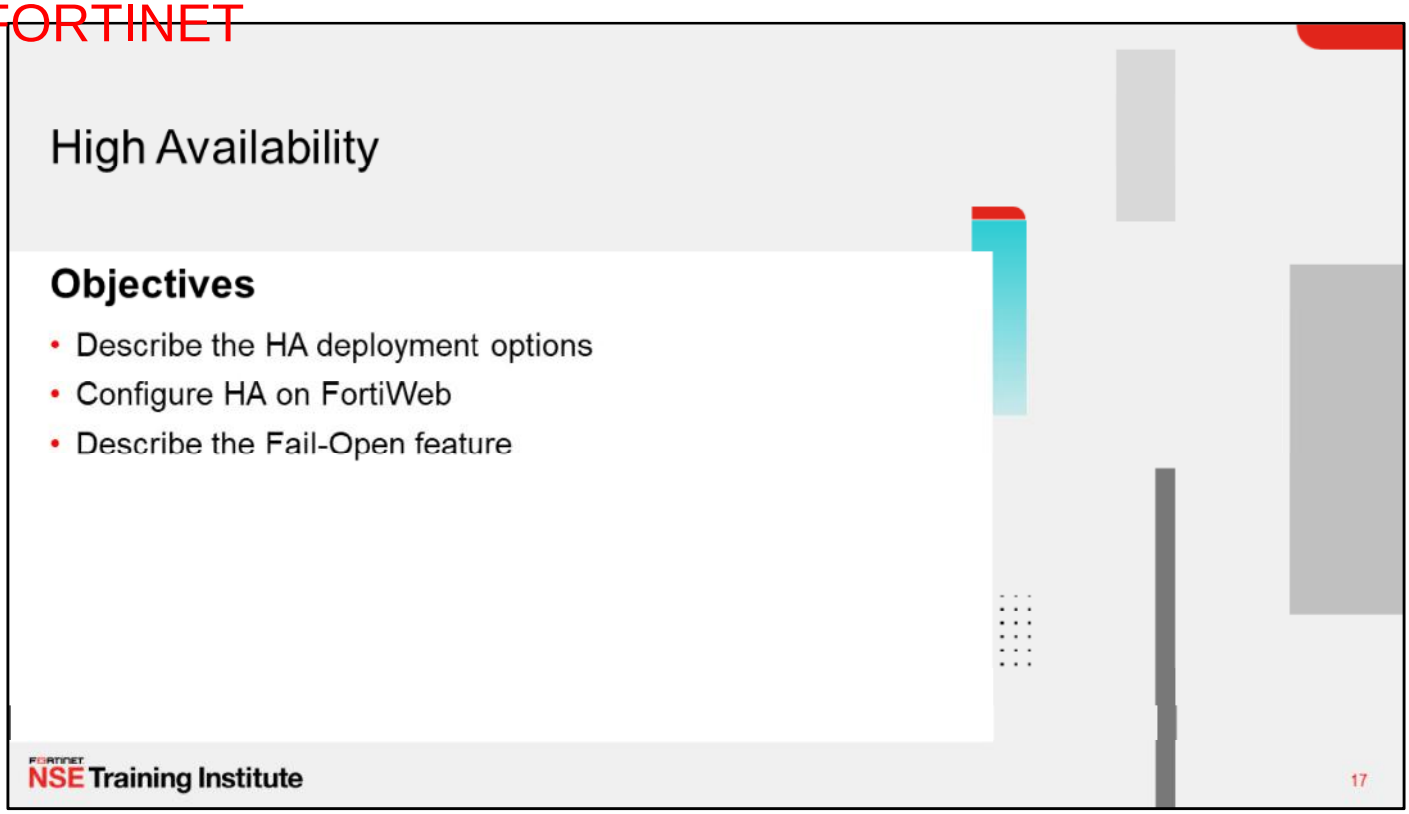


Good job! You now understand FTP security on FortiWeb.

Now, you will learn about high availability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the high availability (HA) option, you will be able to ensure the resiliency of your FortiWeb deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HA

- HA is similar to FortiGate
- Requires two or more FortiWeb devices using identical hardware, firmware, operating modes
- By default, FortiWeb devices are standalone devices
- FortiWeb supports active-passive and active-active clusters
- Active-passive cluster helps to achieve uptime SLAs using two FortiWeb devices
- Active-active cluster helps to achieve uptime SLA and higher throughput using up to eight FortiWeb devices
- External load balancer/HA solution could be used in conjunction with FortiWeb config sync

Config > Sync > Config-Synchronization

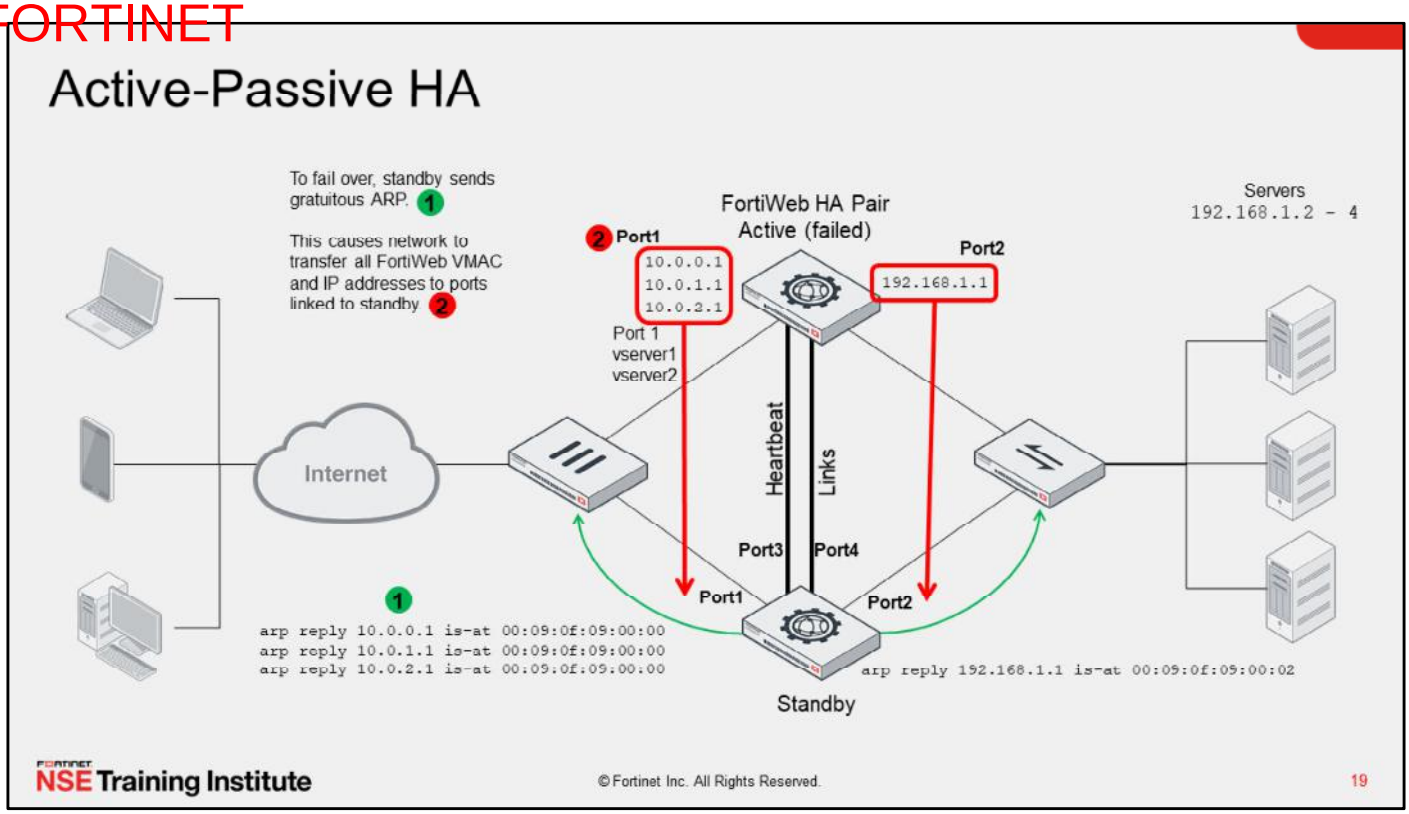
NSE Training Institute © Fortinet Inc. All Rights Reserved. 18

To configure HA, you must have identical FortiWeb models with the same firmware. You can configure FortiWeb in active-passive and active-active HA. If FortiWeb is not operating in reverse proxy mode, HA is usually implemented externally using a FortiADC load balancer.

You can configure a dedicated management interface to access each individual device. You may require direct access to a member in order to view the log messages related to the standby device, or to configure settings on the standby device, which do not synchronize. Those settings include configuring the host name and HA priority. Once HA is formed, you can continue to configure settings on the primary or active device; the standby FortiWeb will automatically sync with the active FortiWeb. If you need to copy the configuration to multiple FortiWeb devices, but don't want failover, use configuration synchronization instead of HA.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



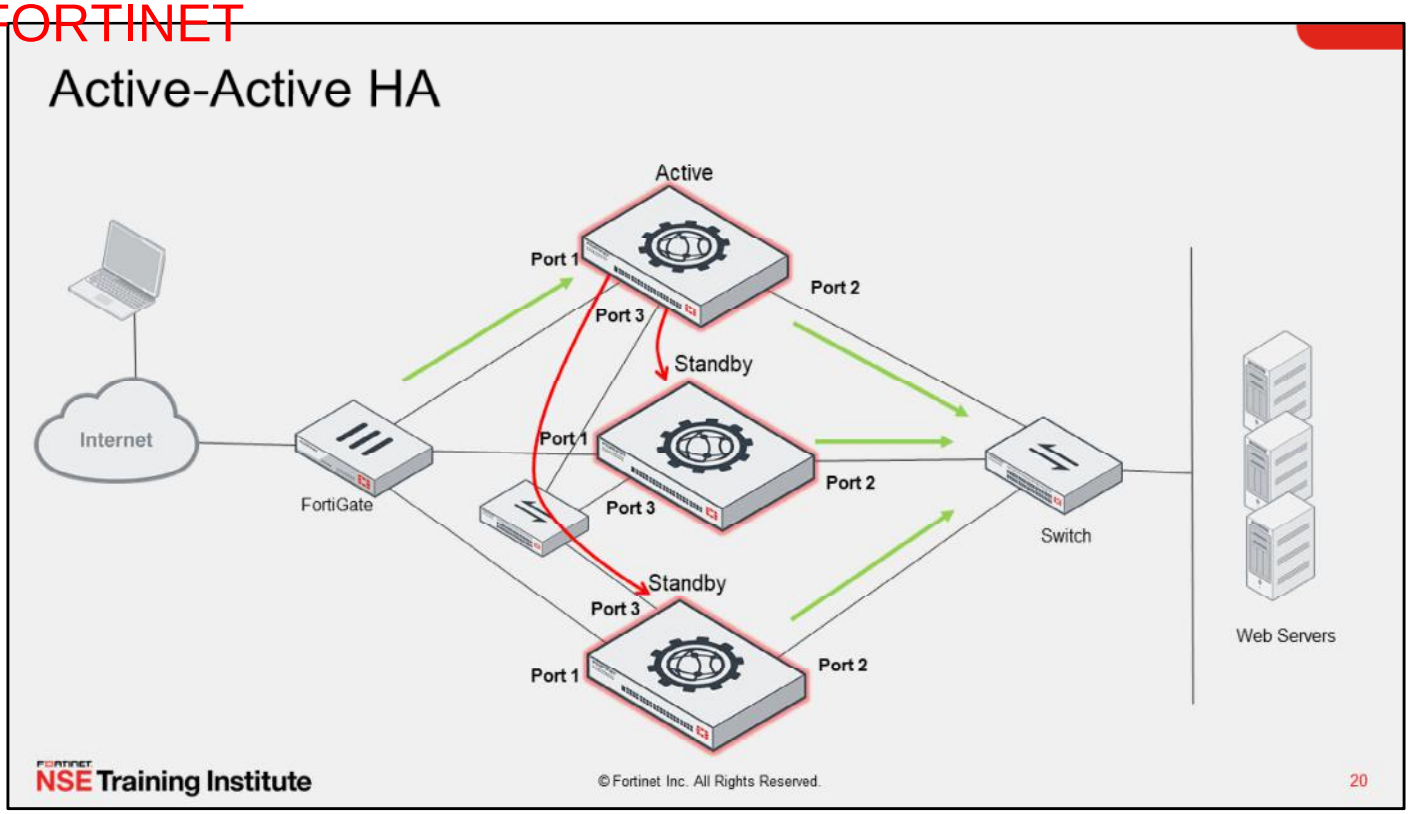
HA on FortiWeb behaves similarly to HA on other Fortinet devices. If the heartbeat fails or a monitored port does not respond, then the standby FortiWeb uses a gratuitous ARP (GARP) to advertise to the network that the FortiWeb virtual MAC address and, by extension, its IP addresses, are now available through the standby's links.

This causes switches to start forwarding frames through the standby's connected ports, as if the failed FortiWeb had been unplugged and moved to different ports on the switch. The failover is almost instantaneous.

The heartbeat interfaces need to have Layer 2 connectivity. You can connect them directly or connect them using a dedicated VLAN. The heartbeat interfaces can be both physical and VLAN interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

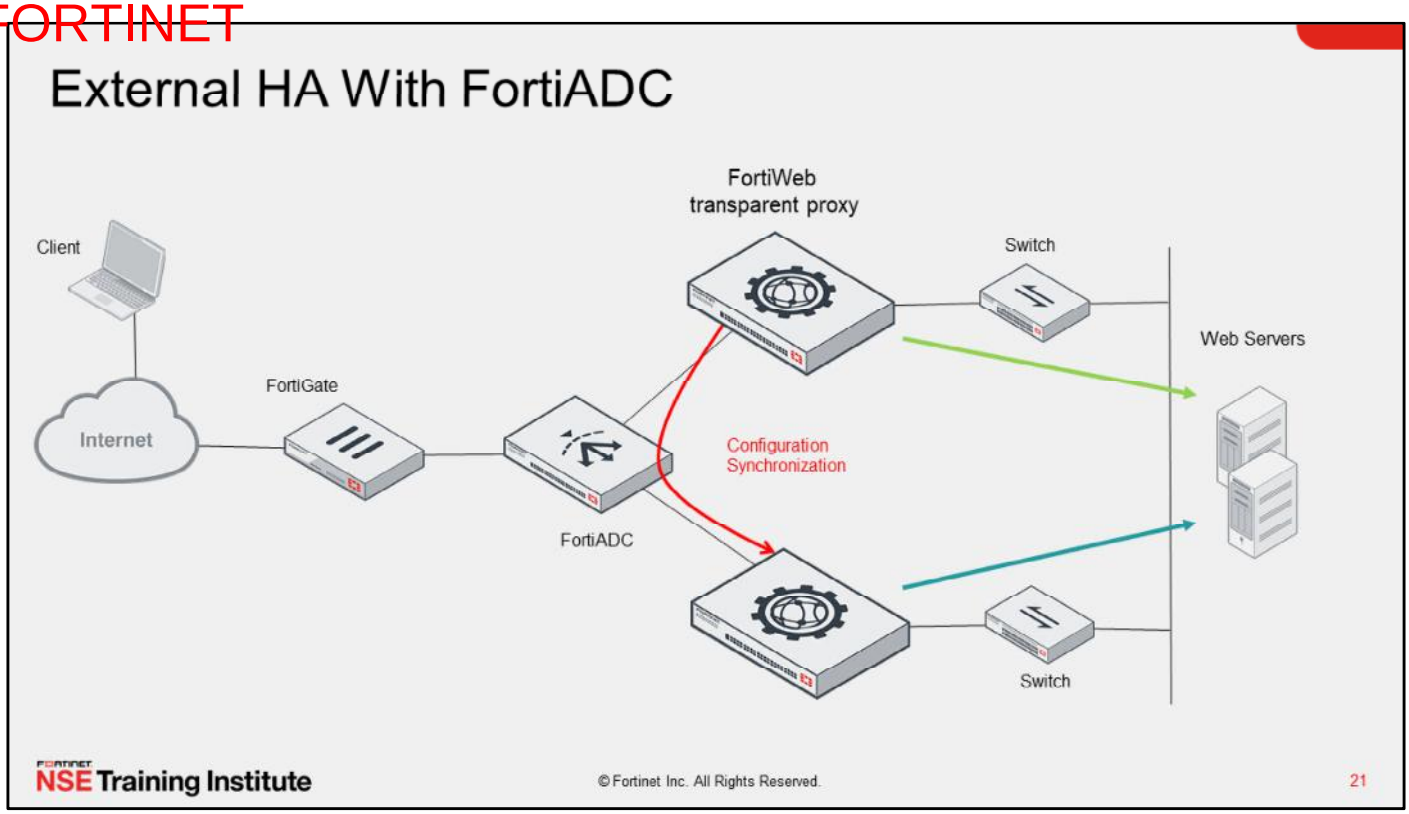


A FortiWeb active-active cluster can consist of up to eight identical FortiWeb devices. One of the cluster members is selected as the active member and the other members act as standby members. The active node receives all traffic from clients and web servers and then distributes the traffic to cluster members, including itself.

Similar to the active-passive HA deployment, the operation of an active-active HA cluster requires heartbeat detection and configuration, and session synchronization between the cluster members. If the primary device fails, one of the secondary devices will take it over. The heartbeat interfaces of all the HA devices must be connected directly with crossover cables or through switches to carry the heartbeat and synchronization traffic between the HA cluster members. The failover is almost instantaneous.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you don't configure FortiWeb to operate in reverse proxy mode, you would not usually configure an HA network topology. Configuring an HA network topology in other operation modes could require changes to your network scheme, which defeats one of the key benefits of other operating modes; they require no IP changes.

Instead, you can use an existing external load balancer or HA solution in conjunction with FortiWeb configuration synchronization, to preserve an existing active-active or active-passive topology.

Unlike FortiWeb HA, an external HA device detects when a FortiWeb has failed and then redirects the traffic stream. FortiWeb has no way of actively notifying the external HA device. To monitor the live paths through your FortiWeb configuration, you could configure your HA device to poll either a backend web server or an IP on each FortiWeb bridge (V-zone).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HA on FortiWeb VM

- No direct physical cabling
- Join with vNetwork in promiscuous mode
- Must accept MAC changes
- Heartbeat should use separate vNetwork from scanned traffic
  - Latency sensitive
- Host load can affect heartbeat reliability and failover speed
  - Allocate enough vCPU
  - If supported, prioritize HA traffic processing
  - Alternatively, set up HA in virtualization environment

NSE Training Institute

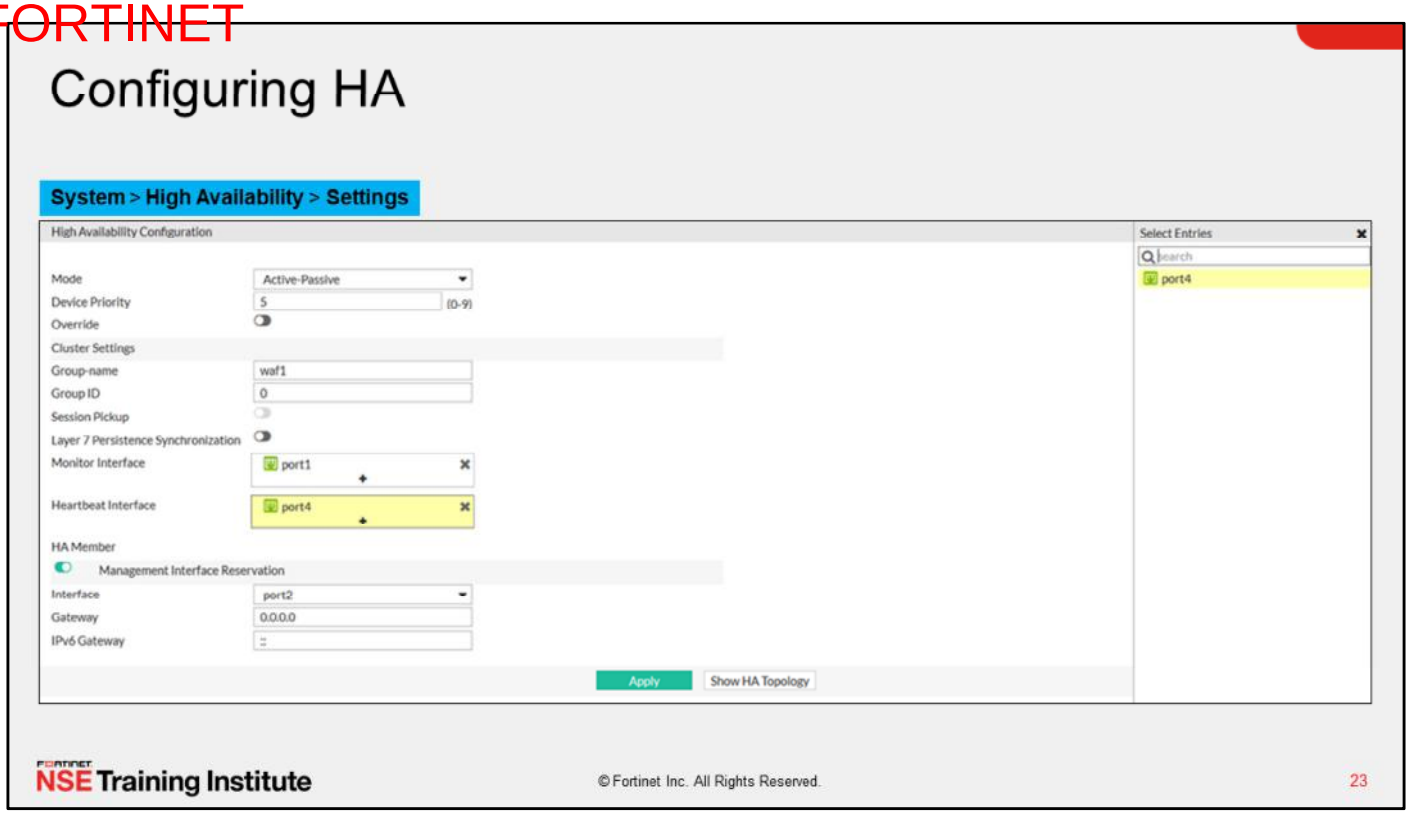
© Fortinet Inc. All Rights Reserved.

22

This slide covers a few VM-specific tips to consider if you’re using FortiWeb VM. The most important thing to consider is that the HA heartbeat and failover (ARP) are latency sensitive. So, if your FortiWeb VMs share hardware with other guest OSs, make sure that the FortiWeb VM has priority.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Link two ports that HA will use to communicate directly, then, if possible, configure HA before configuring the network interfaces. The network settings will sync, as well as other, subsequent settings. FortiGuard antivirus packages now sync between the peers, so you no longer have the initial risk after the failover period. Some data, such as logs and reports stored on the local hard drive, don't sync. See the *FortiWeb Administration Guide* for details.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HA Topology

- Connect or disconnect cluster members
- Access logs for slave members of the cluster
- View HA cluster member statistics

System > Status > HA Topology

Refresh every None — Back to HA configuration page >>

Unit	Status	Up Time	Monitor				
FV-1KD3A13800091		0 days 3 hours 50 minutes	CPU Usage 0%	Memory Usage 4%	Log Disk Usage 0%	HTTP Connections Total Connections: 0 Total Connections/Sec: 0	HTTP Throughput Throughput: 0 Kbps
FV-1KD3A13800012		0 days 3 hours 47 minutes	CPU Usage 0%	Memory Usage 4%	Log Disk Usage 0%	HTTP Connections Total Connections: 0 Total Connections/Sec: 0	HTTP Throughput Throughput: 0 Kbps

NSE Training Institute — © Fortinet Inc. All Rights Reserved. — 24

After completing your HA deployment, you can manage the HA topology and view information and statistics for each HA node.

From the **HA Topology** page, you can select the active or standby node in the cluster, and a pop-up window will open with the option to disconnect them. If you select a standby node in the cluster, the pop-up window will also provide options to view its attack logs, event logs, and traffic logs. To view logs for the active node in the cluster, go to the **Log Access** page**,** and then select the log(s) you want to view.

On the **HA Topology** page, click **View HA Statistics** in the upper-right corner of the window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fail-Open

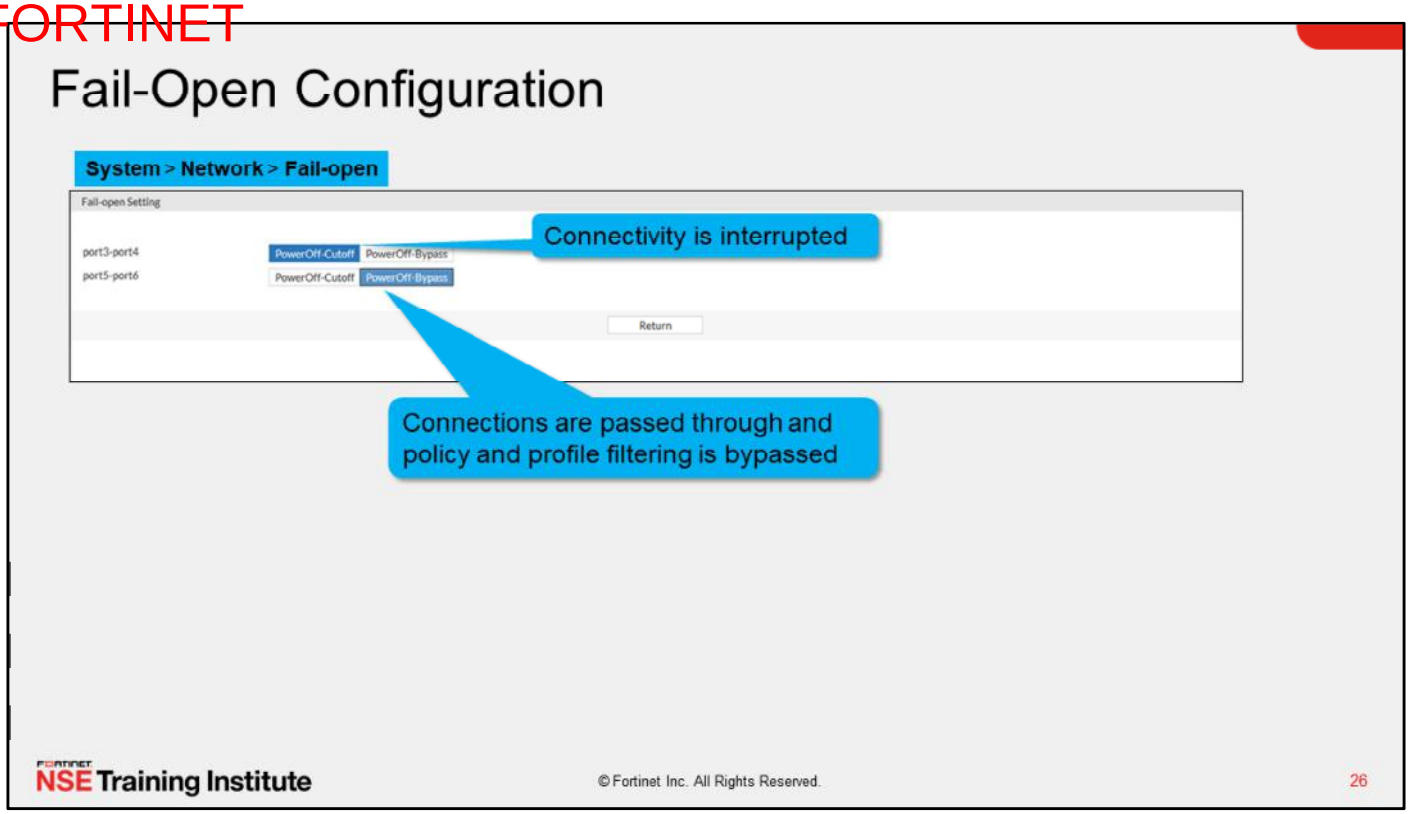
- Traffic crosses FortiWeb uninspected (like a wire)
- Triggered by:
  - Shut down
  - Restart
  - Unexpected power loss
- Requires:
  - Transparent operating mode
  - HA disabled
  - Bridge between ports wired together to the same CP7 processor (varies by model; for example, FortiWeb 1000E: port3 - port4 and port5 - port6)
- FortiWeb-400B/400C, FortiWeb HA clusters, and ports not wired to a CP7/fail-open chip do not support fail-to-wire

NSE Training Institute © Fortinet Inc. All Rights Reserved. 25

If you don't have two FortiWeb devices for HA, and you're using transparent mode, you can still prevent hardware failure from interrupting traffic. To do this, connect through port pairs and configure fail-open to bypass. Note that your websites will be totally unprotected until you replace the failed FortiWeb!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Fail-open is available only on FortiWeb models that have a specific type of ASIC chip between each port pair. When configuring fail-open options, FortiWeb programs the chip to behave as either a bypass or circuit interrupt, when FortiWeb loses power or reboots.

- **PowerOff-Bypass**: Behaves as a wire when the FortiWeb device is powered off. This allows connections to pass directly from one port to the other, bypassing all policy scans and modifications.
- **PowerOff-Cutoff**: Interrupts connectivity when the FortiWeb device is powered off. The bypass is disabled. This is the default setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of HA architecture does FortiWeb support?
   A. Warm standby
   ✓ B. Active-passive
   C. Cold standby
   D. Passive-passive

2. How should logging be configured in a HA configuration?
   A. Logs should be deleted every day
   B. Logs should be stored locally in the FortiWeb
   ✓ C. Logs should be sent to a central SIEM or FortiAnalyzer

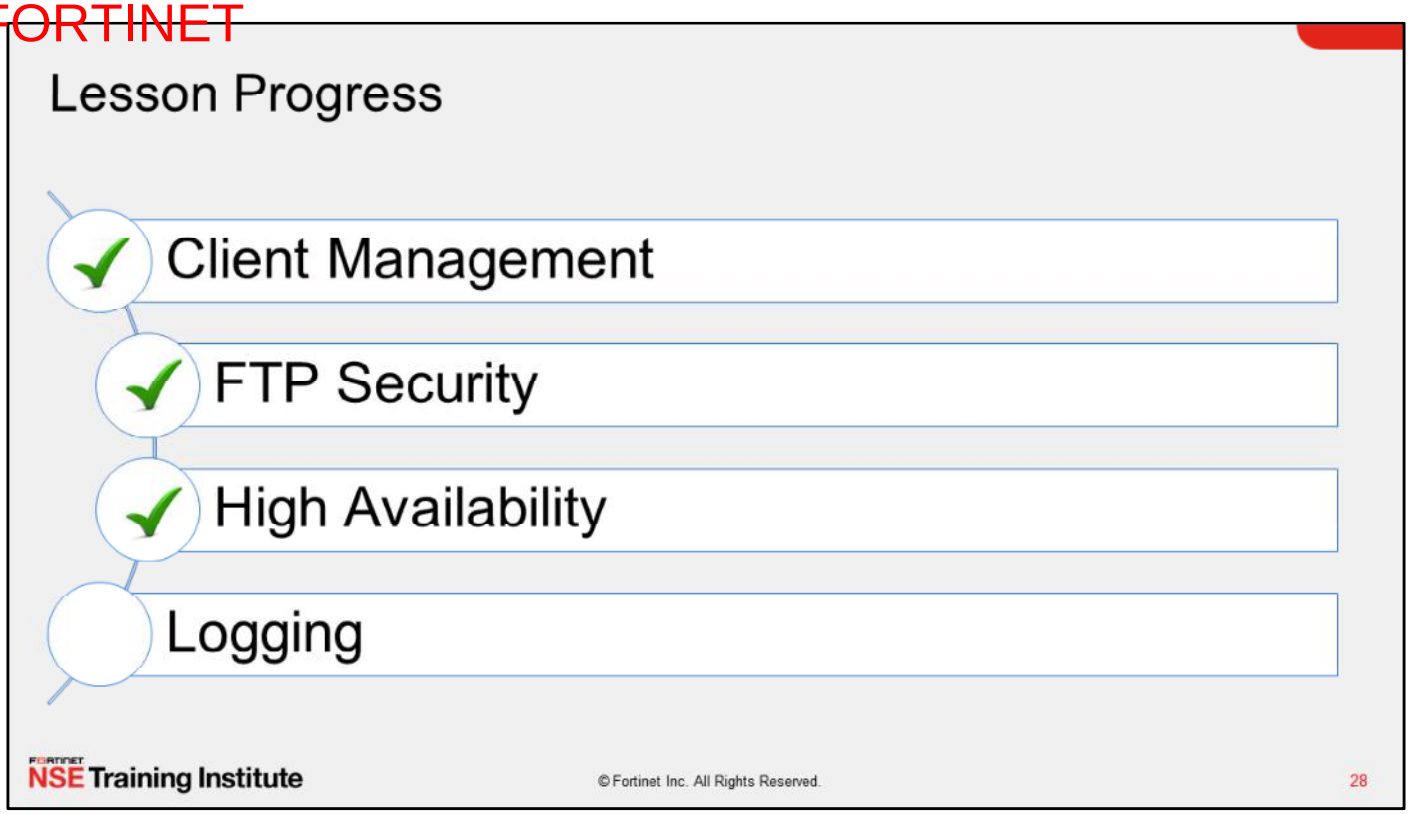
FORTINET NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

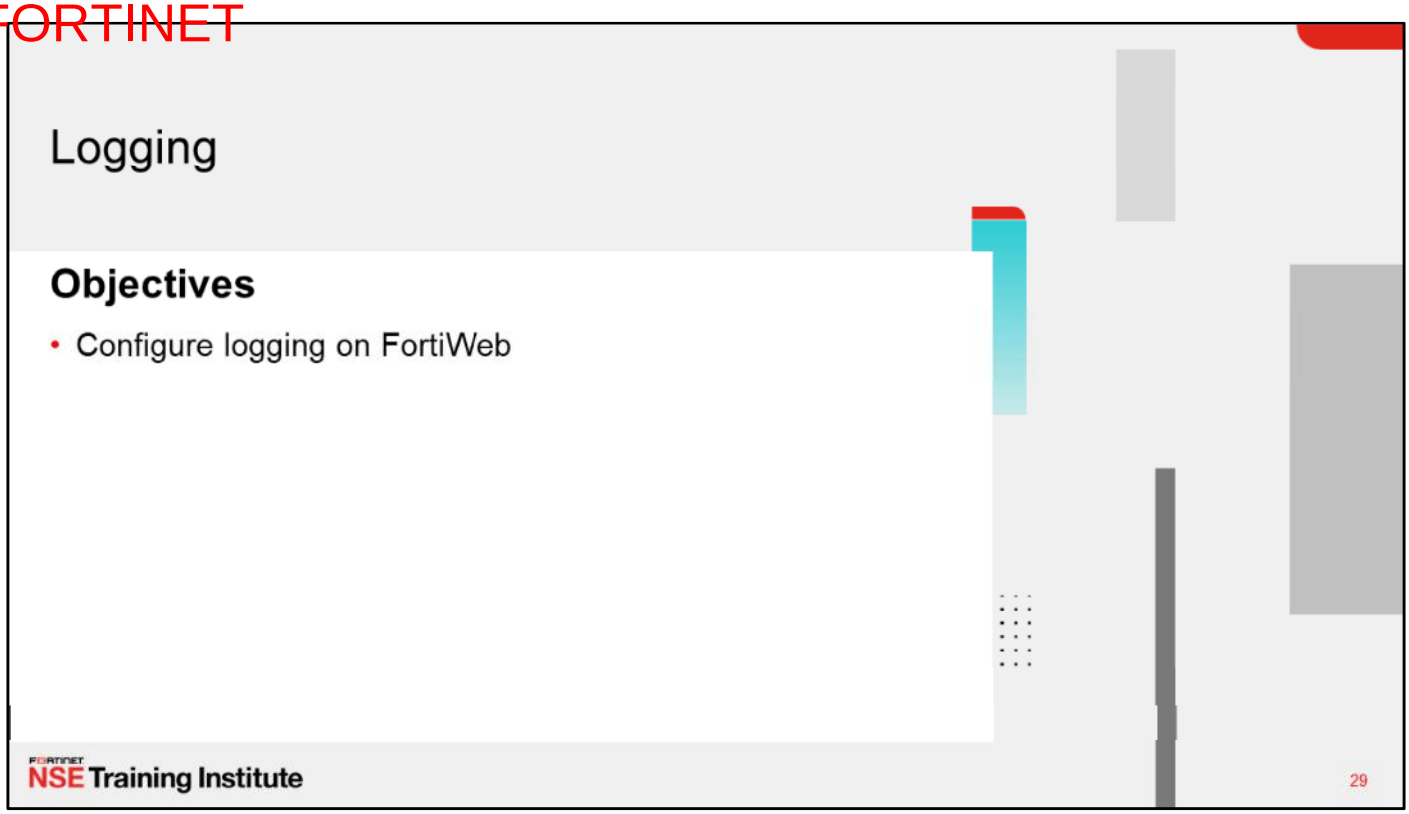


Good job! You now know how to configure HA on FortiWeb.

Now, you will learn about logging.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in configuring logging, you will be able to collect logging information from FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Logging on FortiWeb vs. Logging Externally

- Logs and reports exist on FortiWeb, but logging externally has some advantages
- Flexibility—FortiAnalyzer reports are more customizable
- Performance
  - Extensive, frequent attack and traffic logs reduce FortiWeb performance
    - Increases disk access-related CPU load
    - By default, traffic logs stored in RAM only—ephemeral (can override this through CLI)
  - Increase risk of premature hard disk failure
- Scalability
  - Not limited to local FortiWeb storage capacity
- Visibility
  - For forensics, use FortiAnalyzer or FortiSIEM to correlate logs from your network ecosystem and show the whole attack
    - FortiGate, FortiADC logs
    - Third-party logs such as Apache, IIS, nginx

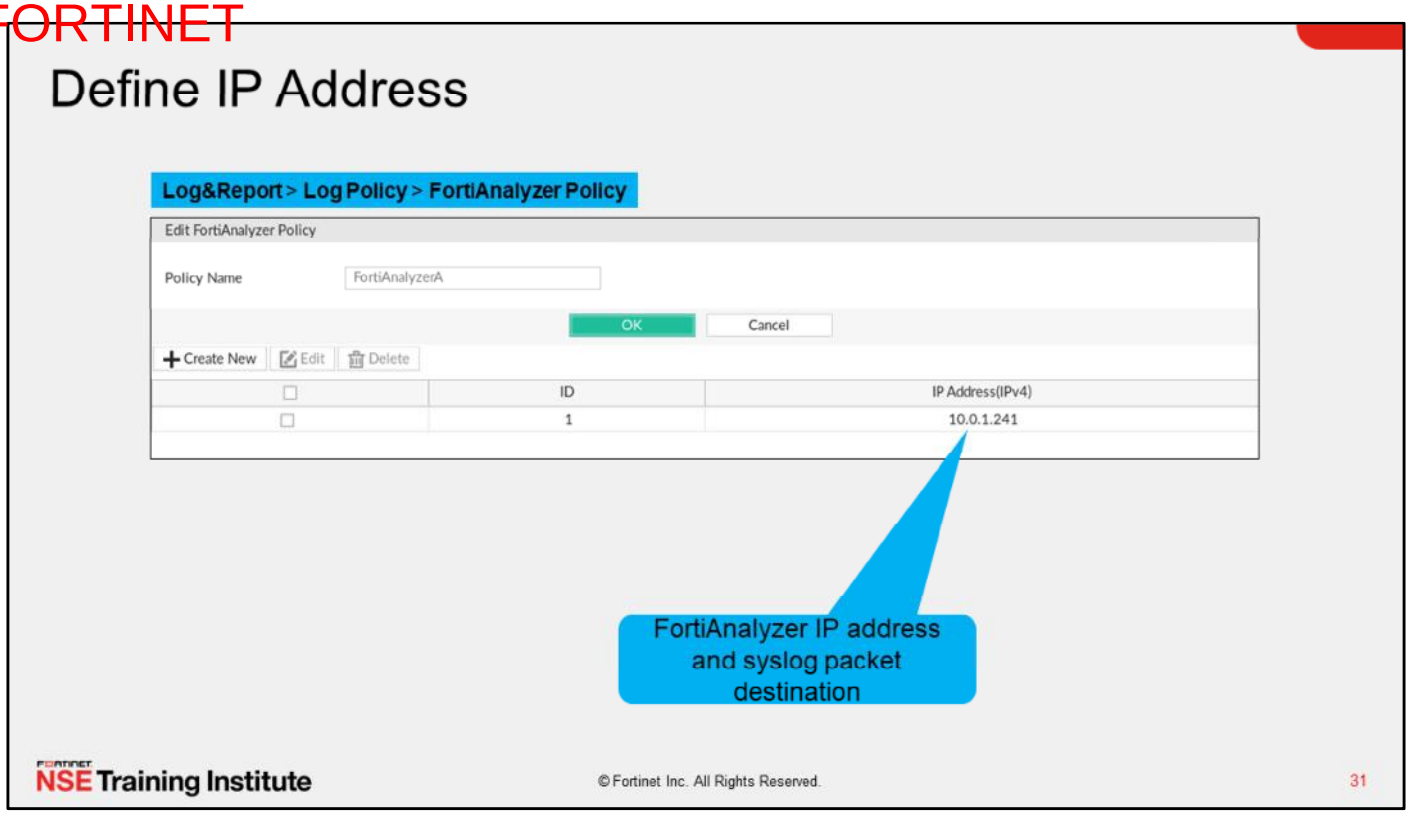
NSE Training Institute © Fortinet Inc. All Rights Reserved. 30

FortiWeb can store logs locally on its hard disk or in RAM, however, logging externally has the following benefits:

- Flexibility for reporting
- Better performance
- Better scalability
- Visibility for multidevice attack correlation

Vouchers & Dumps are Available | WhatsApp +201224560923

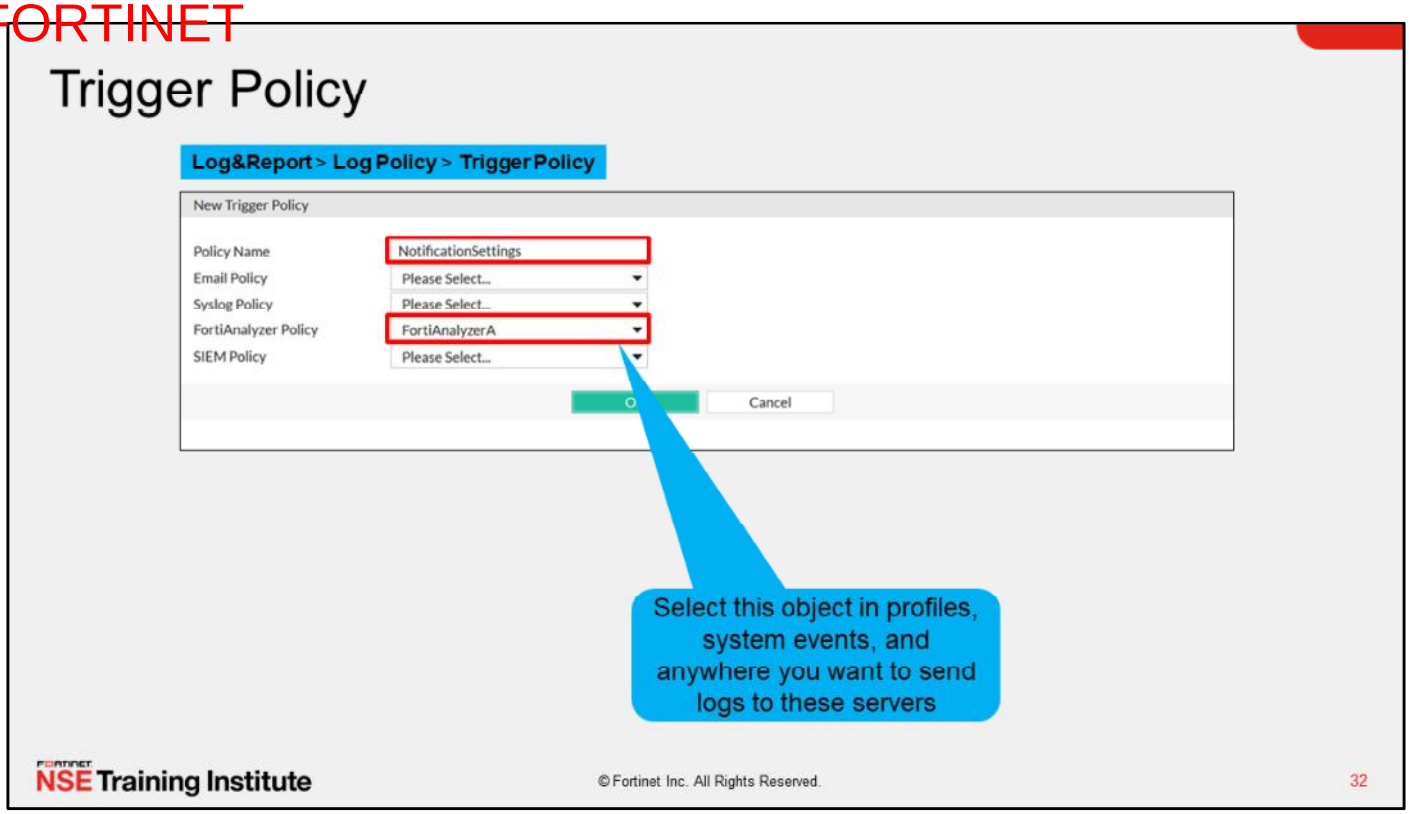
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To configure external FortiAnalyzer logging, first, define the IP address of FortiAnalyzer. This is where FortiWeb will send logs, if you've selected that destination, and they match the type, severity, and other criteria.

Vouchers & Dumps are Available | WhatsApp +201224560923

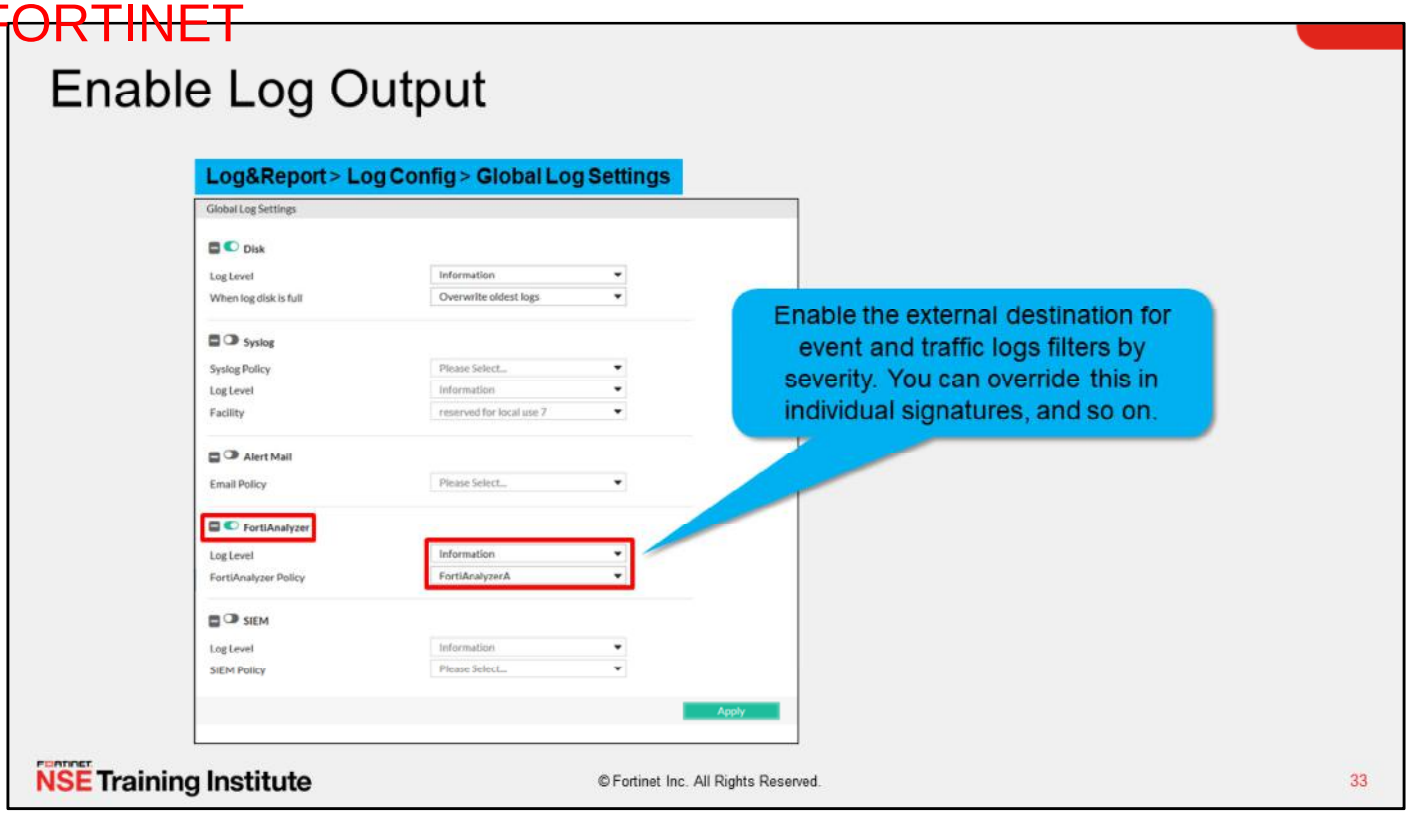
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Next, select your FortiAnalyzer definition in a trigger policy. If you also want to receive an alert email for severe logs, such as a hardware failure or DDoS attack, you can define multiple notification settings. Select your FortiAnalyzer in each one, then also define an email server and select it in the trigger policy that you use with severe events. Alternatively, you can configure your alert email in a central location, such as on FortiAnalyzer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

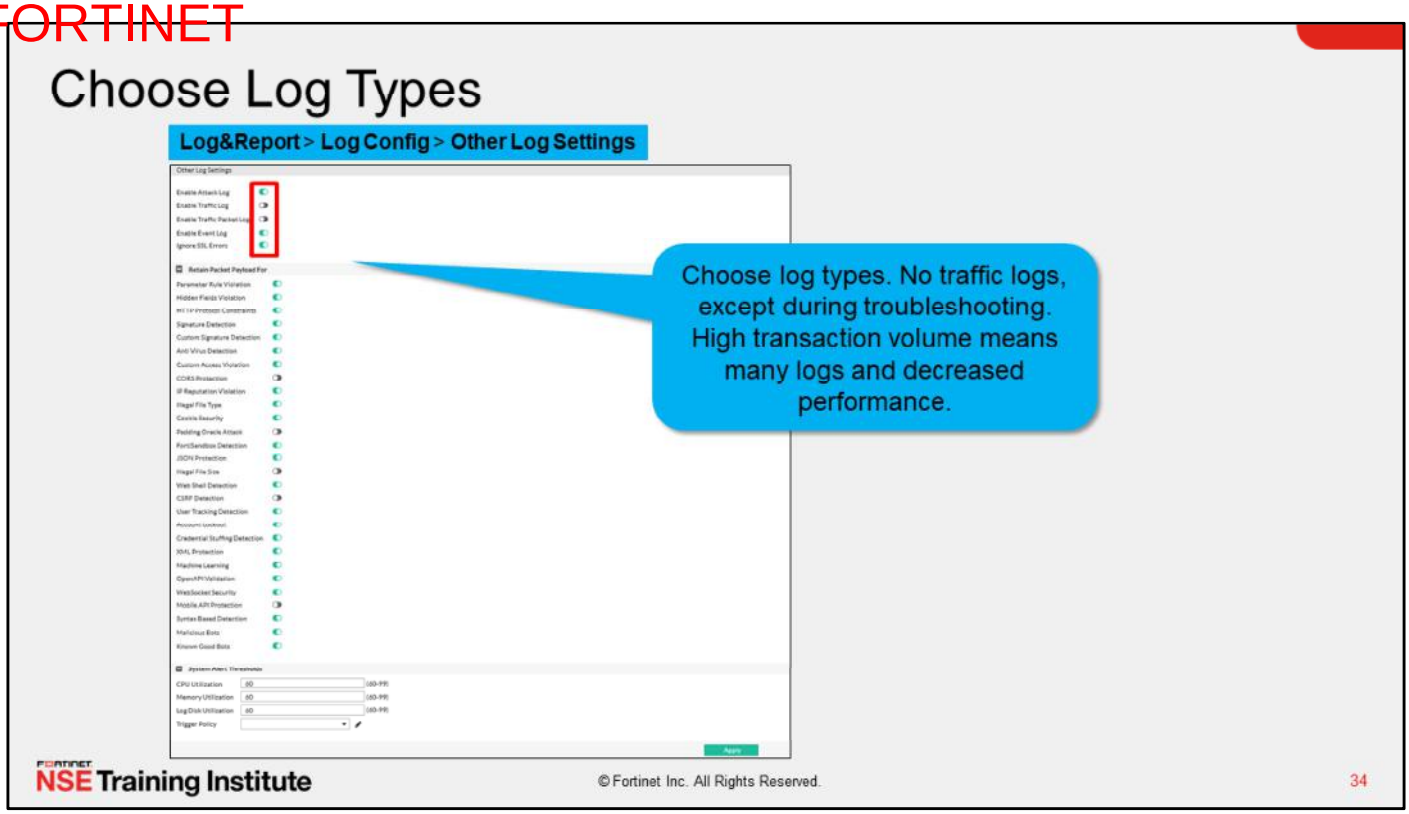


Now enable event and traffic log output to go to your FortiAnalyzer. Specify what severity of logs should be sent. Remember: logging information-level events and greater can significantly increase bandwidth usage, decrease performance, and require much more disk space on your FortiAnalyzer. After completing the configuration, verify that your FortiAnalyzer model is powerful enough to handle the log volume without dropping logs. Syslog is a UDP connectionless protocol that is lightweight but does not verify successful message transmission and storage. Also verify that you've allocated enough disk space.

For example, if you need to store three months worth of logs, see how much disk space is consumed after a normal week, then multiply it by 12 weeks. For a robust solution, also simulate logging volumes that could happen if your network is under attack. This is when your logs are most crucial.

Vouchers & Dumps are Available | WhatsApp +201224560923

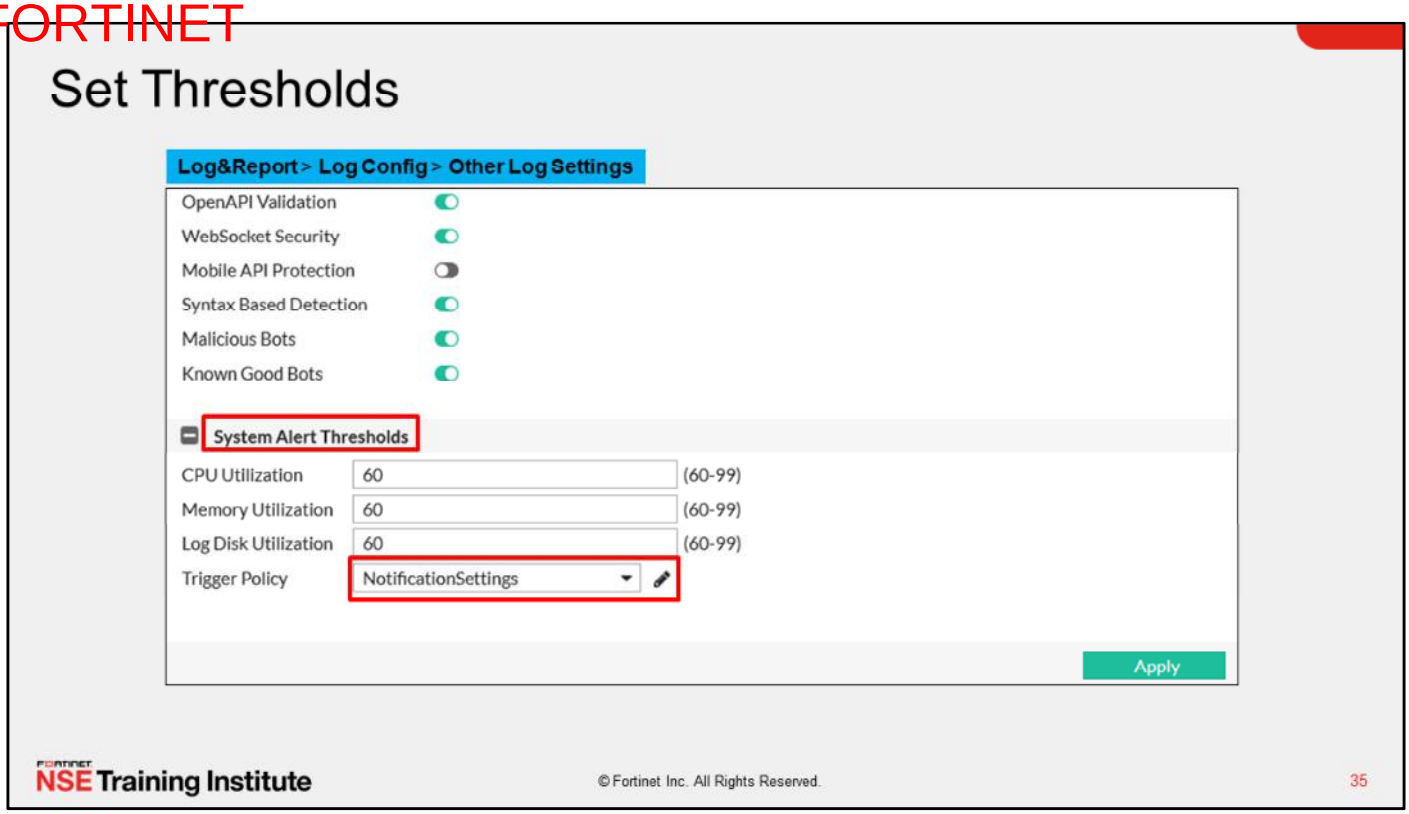
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Choose which log types to record: attack logs, event logs, and, possibly, traffic logs. Remember that packet payloads can only be stored on the FortiWeb local hard disk. Like traffic logs, they can be disk intensive. If possible, it's best to enable that option only during troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

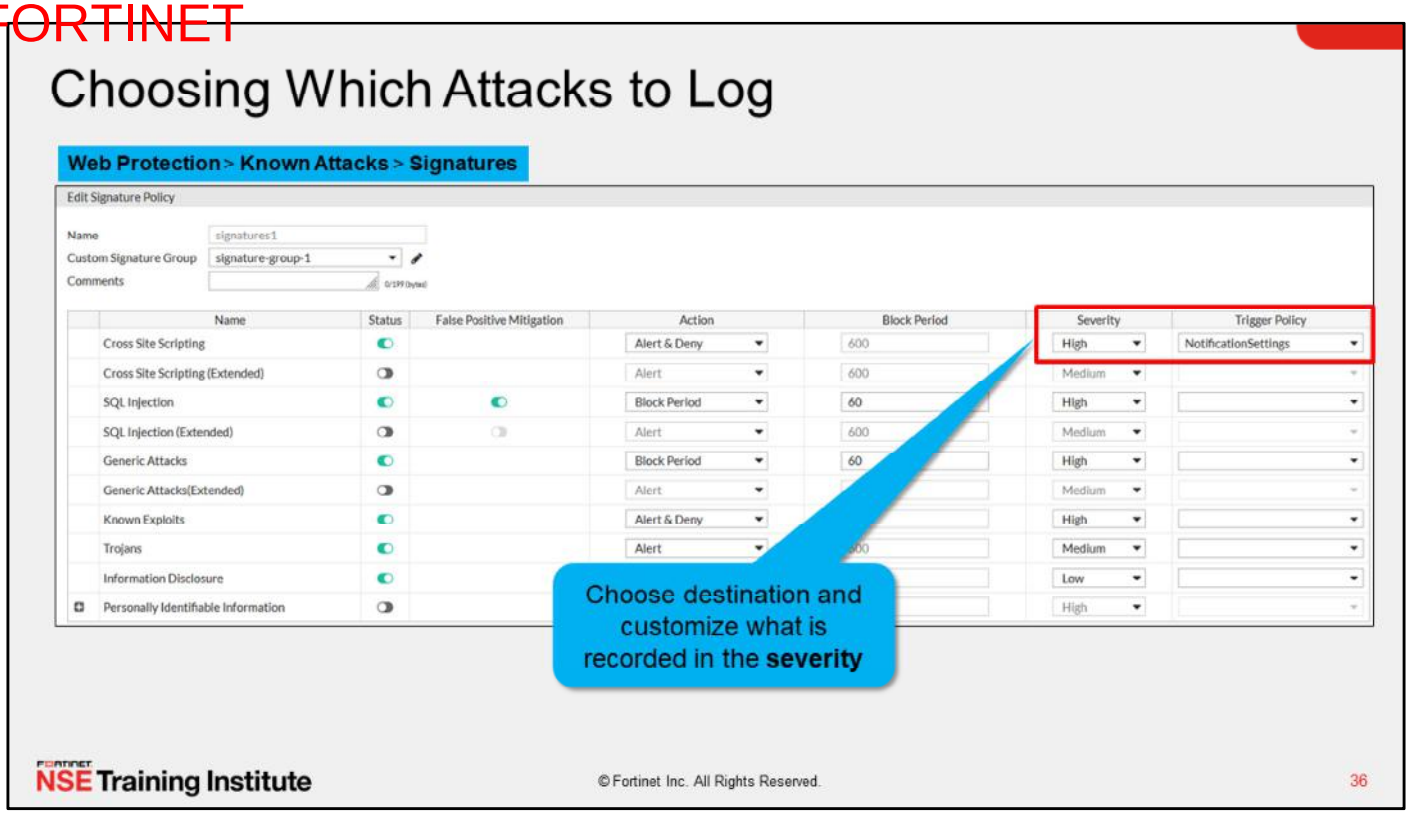
DO NOT REPRINT
© FORTINET
Brave-dumps.com



For event logs that record critical system resource usage, you have even more granular control. You can specify which levels will trigger a log message, and indicate a more specific trigger policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For the attack log, configuration is even more flexible. For each specific rule or attack signature, indicate whether to log violations, and which notification servers (if any) to use. This is where you should select the trigger policy that uses your FortiAnalyzer object.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which external device can FortiWeb send logging information to?
   - ✓ A. FortiSIEM
   - B. FortiADC

2. Which setting allows you to define when an alert email is sent?
   - A. Log output location
   - ✓ B. Trigger policy

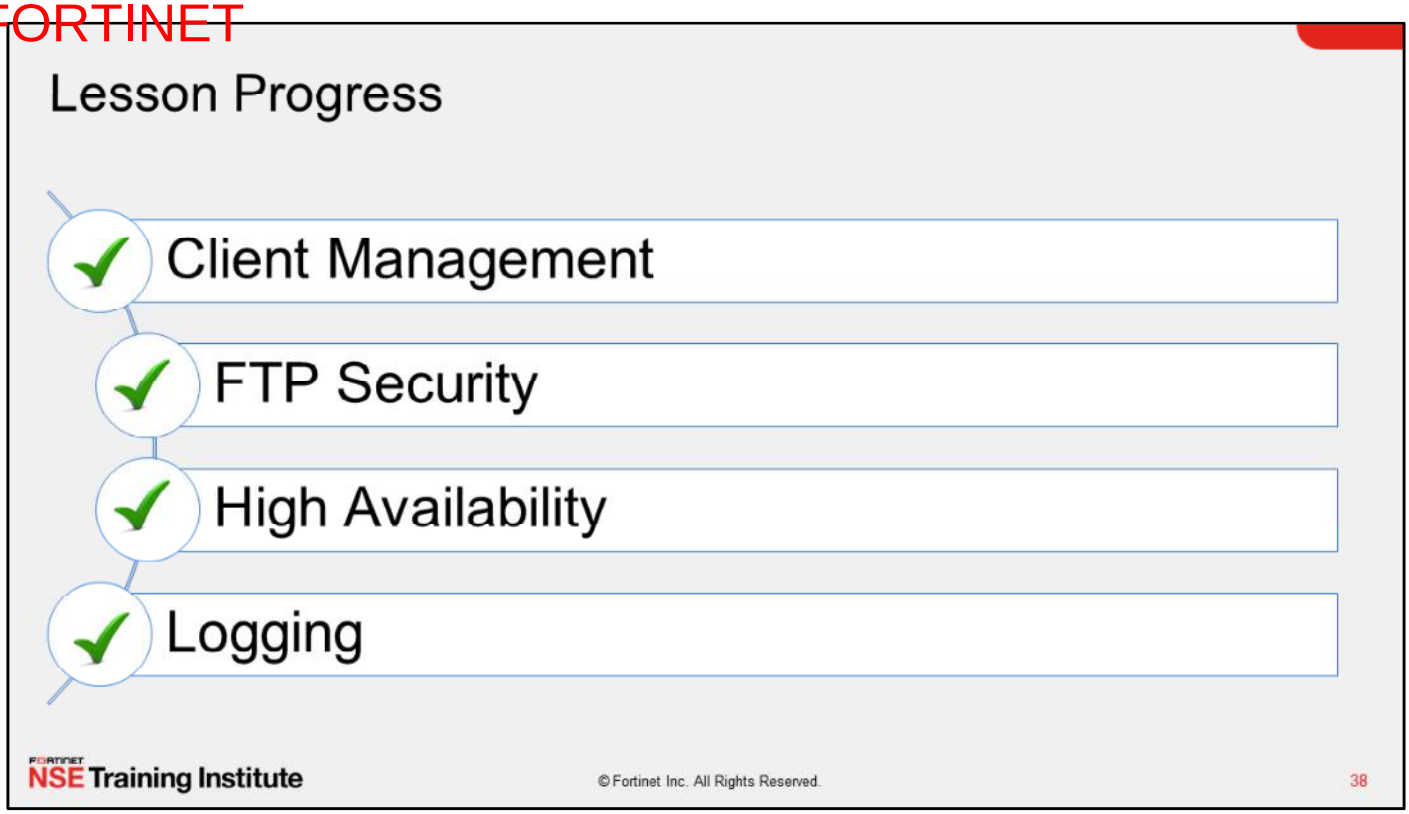
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe and configure client management
- ✓ Configure threat weights
- ✓ Describe security for FTP transactions
- ✓ Configure FTP security
- ✓ Describe the HA deployment options
- ✓ Configure HA on FortiWeb
- ✓ Configure the fail-open feature
- ✓ Configure logging on FortiWeb

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

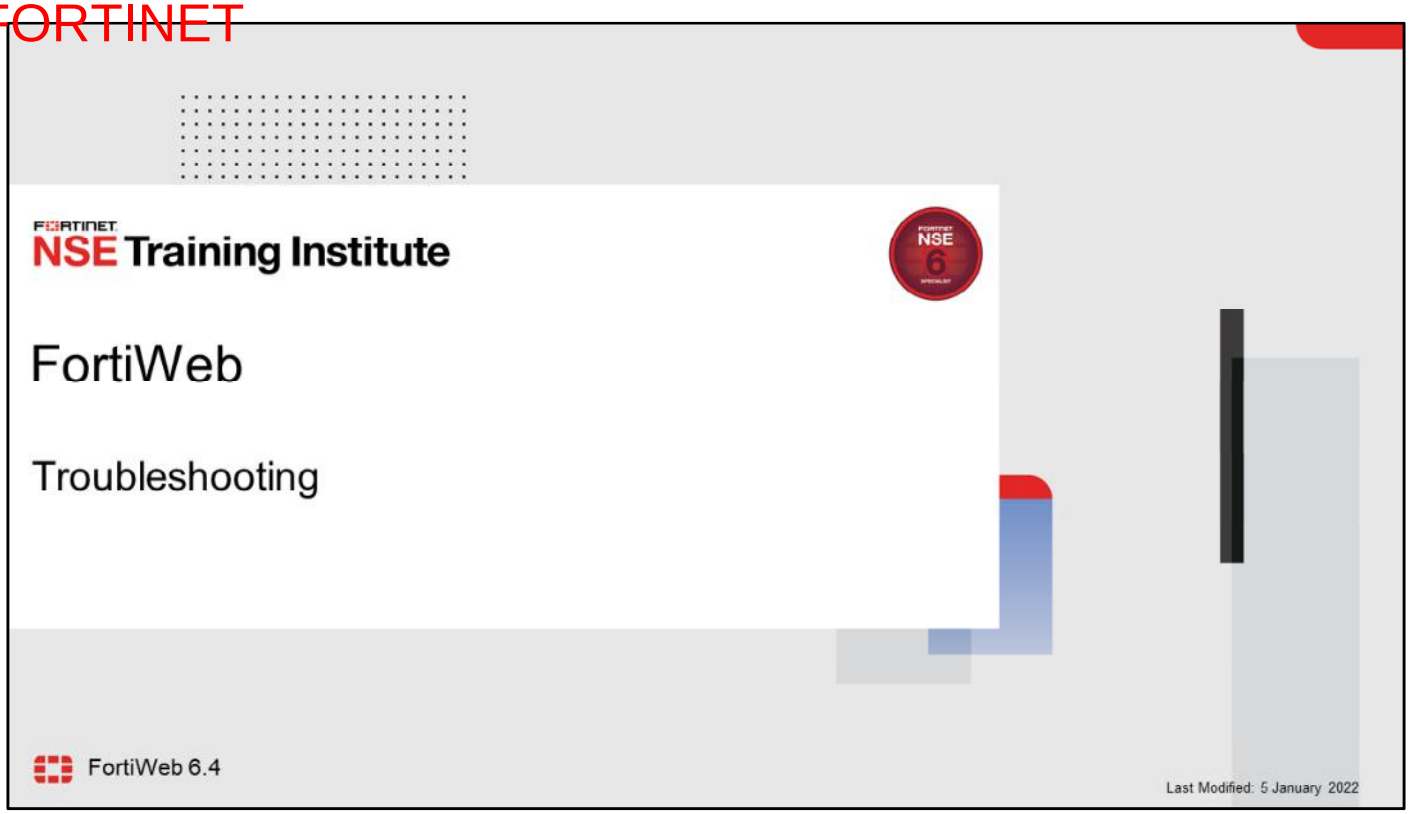
39

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned to how to configure and manage clients and threat weights, FTP security, FortiWeb HA, and local and external logging on FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

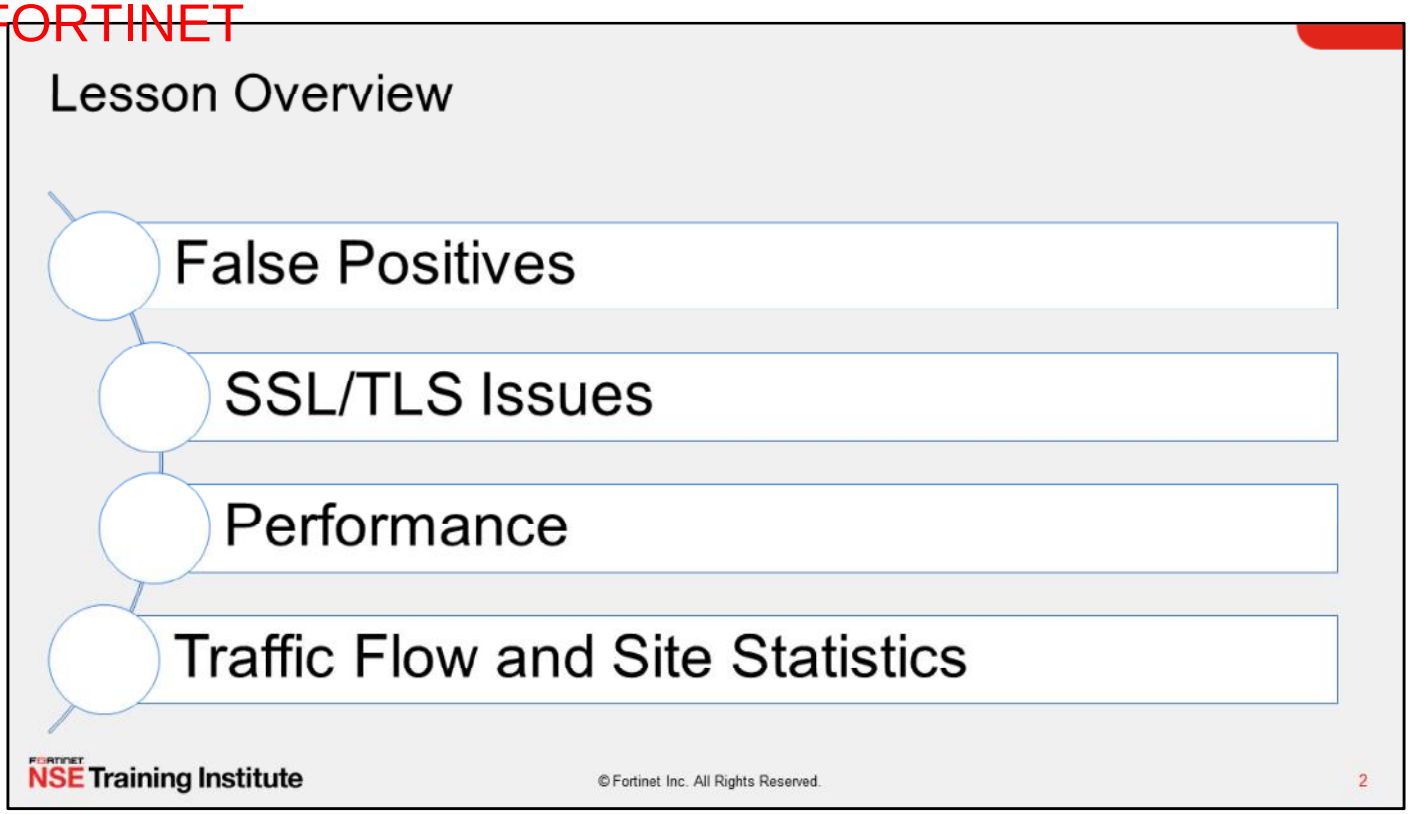
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to avoid common misconfigurations, diagnose false positives, solve connectivity and storage issues, and optimize the performance of your FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

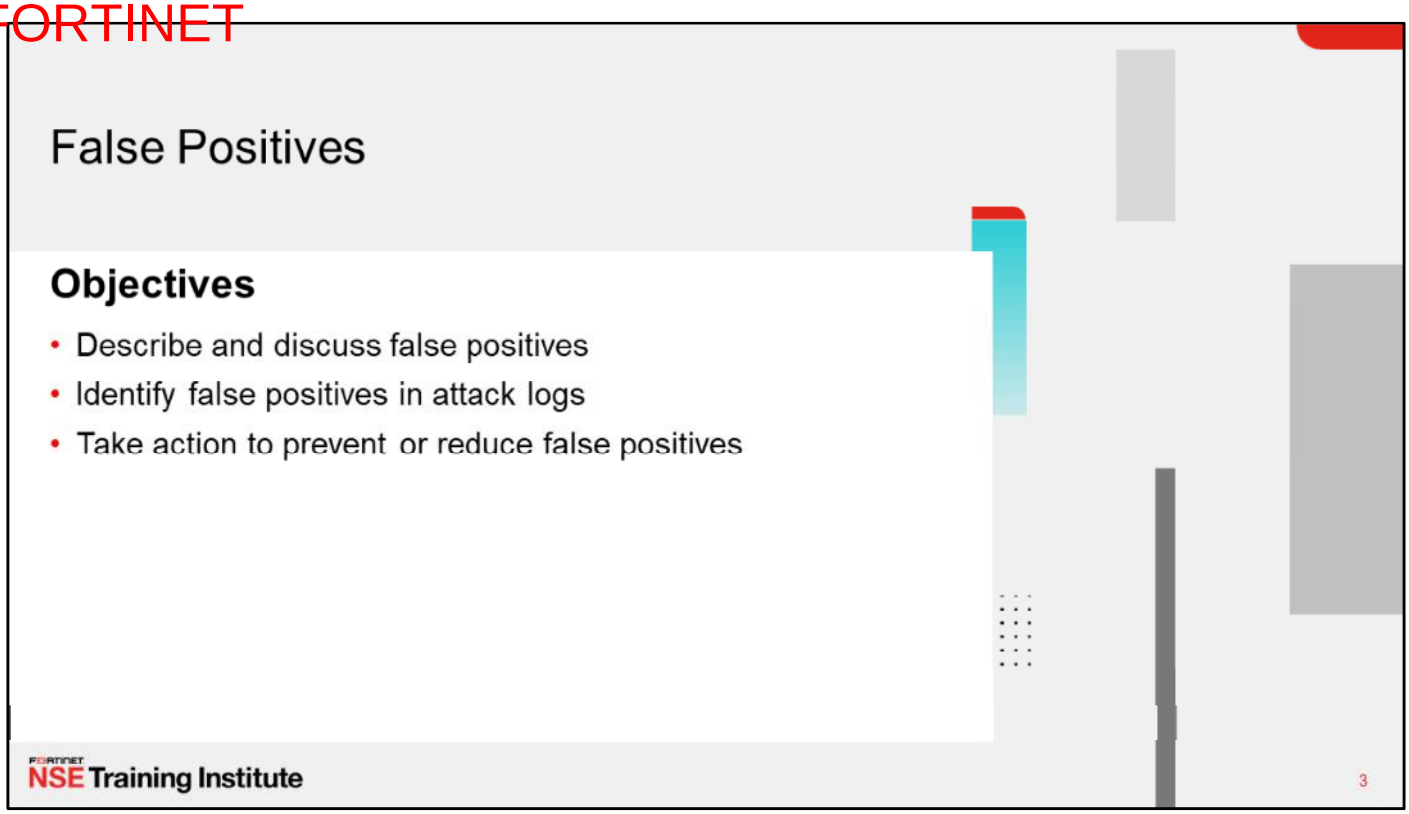
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in fine-tuning rules and signatures, you will be able to identify, and prevent or reduce false positives, especially if you are installing a new, custom web application with FortiWeb.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

False Positives—Fake Attacks

- If normal traffic looks like an attack, FortiWeb can accidentally block a genuine user
  - Example: Developer forums or webmail that allow code examples
  - Example: Password much longer or allows more characters than initially defined
  - Example: Application allows sessions initiated from some bookmarked pages
  - Example: After update, application now uses previously suspicious traffic
- In extreme cases, if a client IP is trusted, you can add it to the allowlist
  - Bypasses *most* scans
    - Not TCP flood prevention
    - Not block period list
- Primarily a concern when using custom or default signatures
  - Machine learning should prevent most false positives

NSE Training Institute © Fortinet Inc. All Rights Reserved. 4

Initially you may need to fine-tune rules and signatures to avoid some false positives, especially if you are installing a new, custom web application with FortiWeb. False positives are requests that look similar to an attack, but are normal traffic.

When deploying FortiWeb for the first time, or when beginning to protect new web applications, a common task is to find which individual signature or rule is accidentally blocking normal traffic.

Because FortiWeb can block based upon multiple factors—the source IP address, the request rate, the data type of inputs, the size of a file upload, and so on—you may need to adjust more than one setting. For a list of scans and processing that FortiWeb applies to traffic, see the sequence of scans in the *FortiWeb Administration Guide* or online help. In this list, you'll notice one effect you may not expect: items on the allowlist do not bypass all scans, just most.

Before the allowlist check, two scans occur. So, if a client begins a TCP flood, or is already being period-blocked, the allowlist does not immediately restore connectivity.

False positives are primarily a concern when using custom signatures, or default signatures that are static. Using machine learning should prevent most false positives.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Eliminate False Positives

- Use machine learning when possible
- To fix false positives:
  1. Check attack logs to identify which scan or rule is triggering
     - Could be more than one scan, IP addresses, or geolocation
     - Scan sequence list is in the *FortiWeb Administration Guide*
     - Either customize rule or signature, make exception for that specific host and URL, or disable signature or rule
     - Add exception, disable signature, or view signature directly from **Message** field of attack log
  2. Get the client's IP address
     - If the client is being temporarily bocklisted by a period block, remove IP address from list (blocked IP address)
  3. If the block is caused by a DoS sensor, you may need to do one or all of the following:
     - Enable detection of shared internet connections (SNAT)
     - Add an X-Forwarded-For: rule
     - Increase rate limits

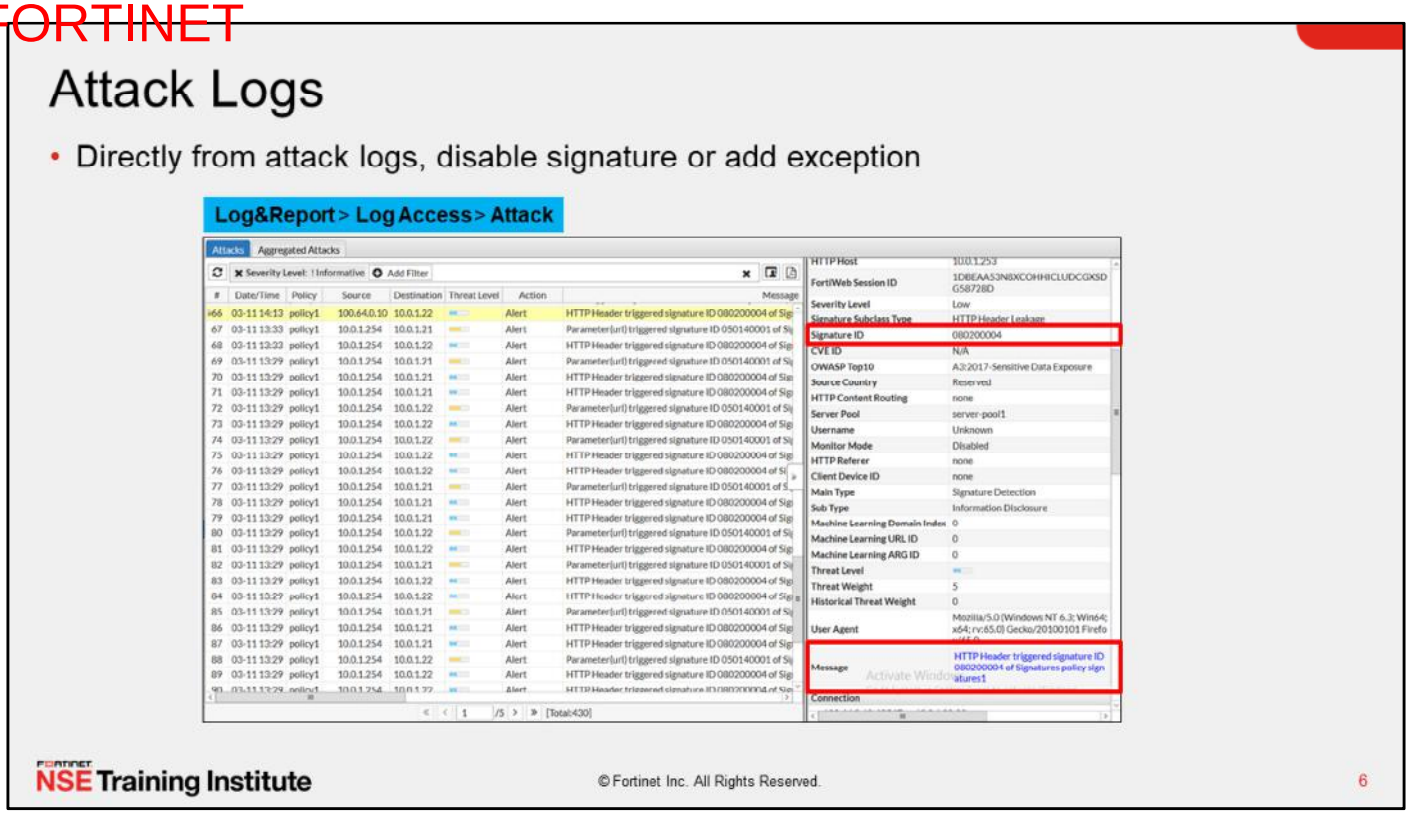
NSE Training Institute © Fortinet Inc. All Rights Reserved. 5

When you use a custom signature or a default signature, you may encounter some false positive conditions. Essentially, there are three steps to correcting most false positives.

Web application upgrades and patches can change your security requirements, causing false positives. URL structure in Microsoft Outlook on the web has changed significantly since 2003. WordPress vulnerabilities often vary by the installed plugins. Machine learning can help prevent recurring false positives, especially for HTTP constraints and input rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If there are only a couple of false positives, you can easily fix them:

1. Enable local storage of attack logs. Enable packet payloads—part of the packet that matches the rule or signature.
2. In the attack log, find an entry for an attack that is normal traffic.
3. Click the row. The log message details appear in a panel on the right side. Scroll down to the **Packet Header** section, and the part of the request or reply that matches the signature is highlighted.
4. You can customize the signature or rule so that it still blocks attacks but does not match the legitimate traffic. If you don't want to customize the signature or rule, scroll up to the message portion of the attack log panel. Click the link to either add an exception or disable the signature entirely.

If you change your mind later, you can use the advanced mode when editing a signature policy to find disabled signatures, and enable them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How to Find the Signature ID and Behavior

- For more detailed information on an attack, click its link in the attack log
- Shows signature ID
  - Can modify signature to avoid false positive, disable, or create exception

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

If you're adjusting behavior to create a custom signature, it can be helpful to know the ID and behavior of the signature that triggered a false positive.

The ID indicates the category of attack that it was intended to block. The **Found In** and **Match Sample** fields show what part of the request was being analyzed. When you create your custom signature, you should do three things:

- Defend against that same attack, if possible
- Scan the same part of the request or reply
- Match the same dangerous traffic, but avoid matching normal traffic that was recorded in the packet payload

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Delisting From Period Block

- If the client is accidentally blocked for a period, you can either:
  - Manually release their IP address from the temporary blacklist
  - Let the entry expire
- Per-ADOM, per-policy basis
- **Monitor** > **Blocked IPs**
- Related: **Server Objects** > **Global** > **Known Search Engines**
  - Bots of well-known search engines identified by public IP address, not `User-Agent`:
  - To view activity, click **Monitor** > **Bot Analysis**

NSE Training Institute © Fortinet Inc. All Rights Reserved. 8

If FortiWeb applies a period block, usually the entry on the temporary blocklist will expire before the user can contact an administrator. However, if the user try the same thing again, the user will be put on the blocklist again. Adding the IP address to an allowlist will not override an entry on the period block list. An administrator needs to remove the entry under **Blocked IPs**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Blocked IP Addresses

- Automatic delisting when block period expires
- If a trusted client often gets false positives, you can add the IP address to the allowlist
  - Avoids having to manually release
  - Use with caution—bypasses all scans except period block and TCP flood

Monitor > Blocked IPs

Refresh

ID	IP	Block Reason	Release
Policy: policy1			
1	100.64.0.10	N/A	

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

An allowlist entry is not a permanent solution. If a user's laptop gets infected with a virus, or if their phone is stolen, then that client is no longer in that user's control. FortiWeb security may be compromised.

If you're not sure how to write a custom signature, you can change the rule or signature's action to **Alert Only**. The client can use the application, but you will be notified of potential attacks. You can also continue to gather data about what normal traffic accidentally matches the signature.

Allowlists are best for individual browsers, not for search engine crawlers and known bots.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Where would you look first to identify what is causing a false positive?
   - ✓ A. Attack logs
   - B. Activity logs

2. Which one should be added to the allowlist, even though they might seem like a threat?
   - A. Content scrapers
   - ✓ B. Search engine bots
   - C. Employee workstations that triggers false positives

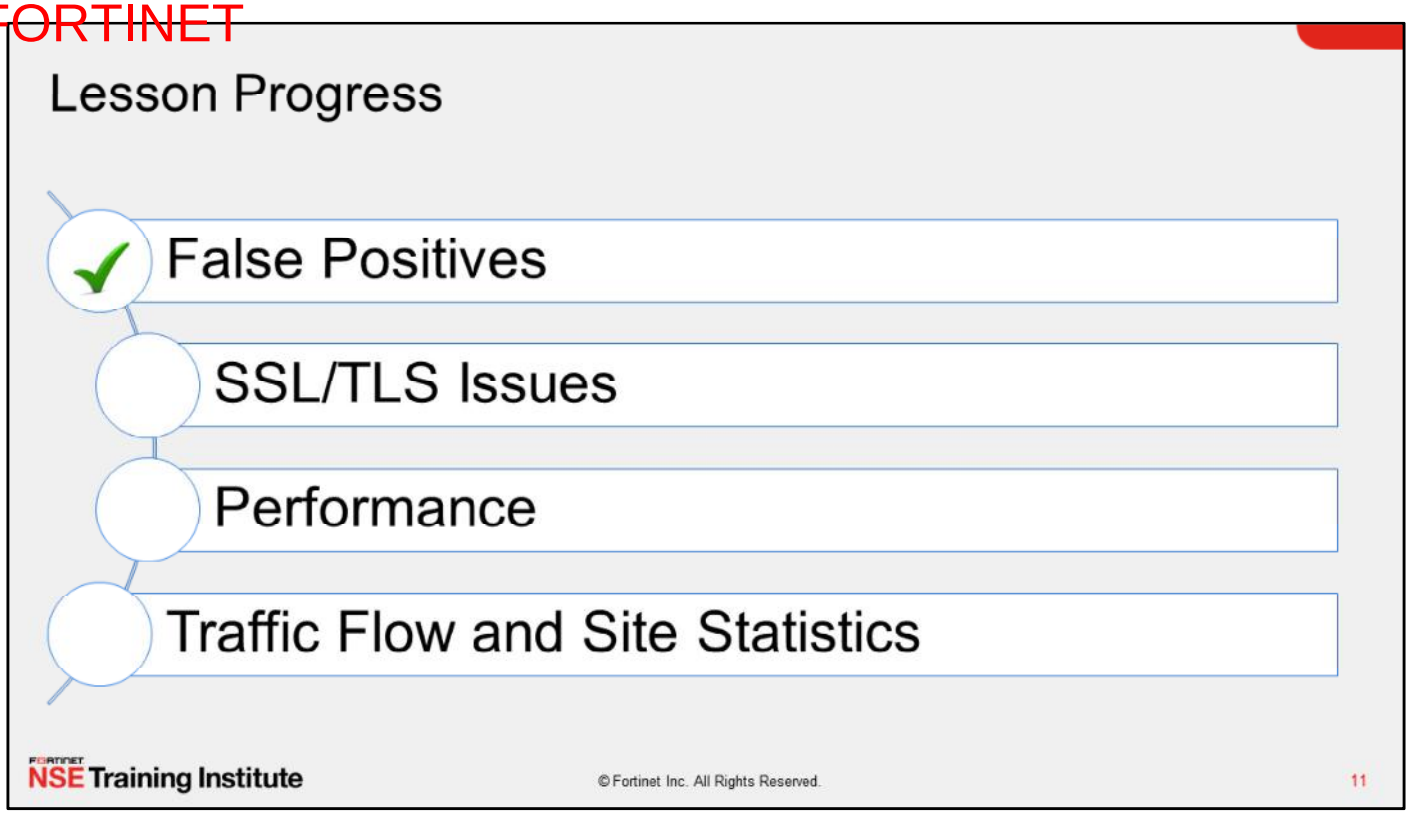
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

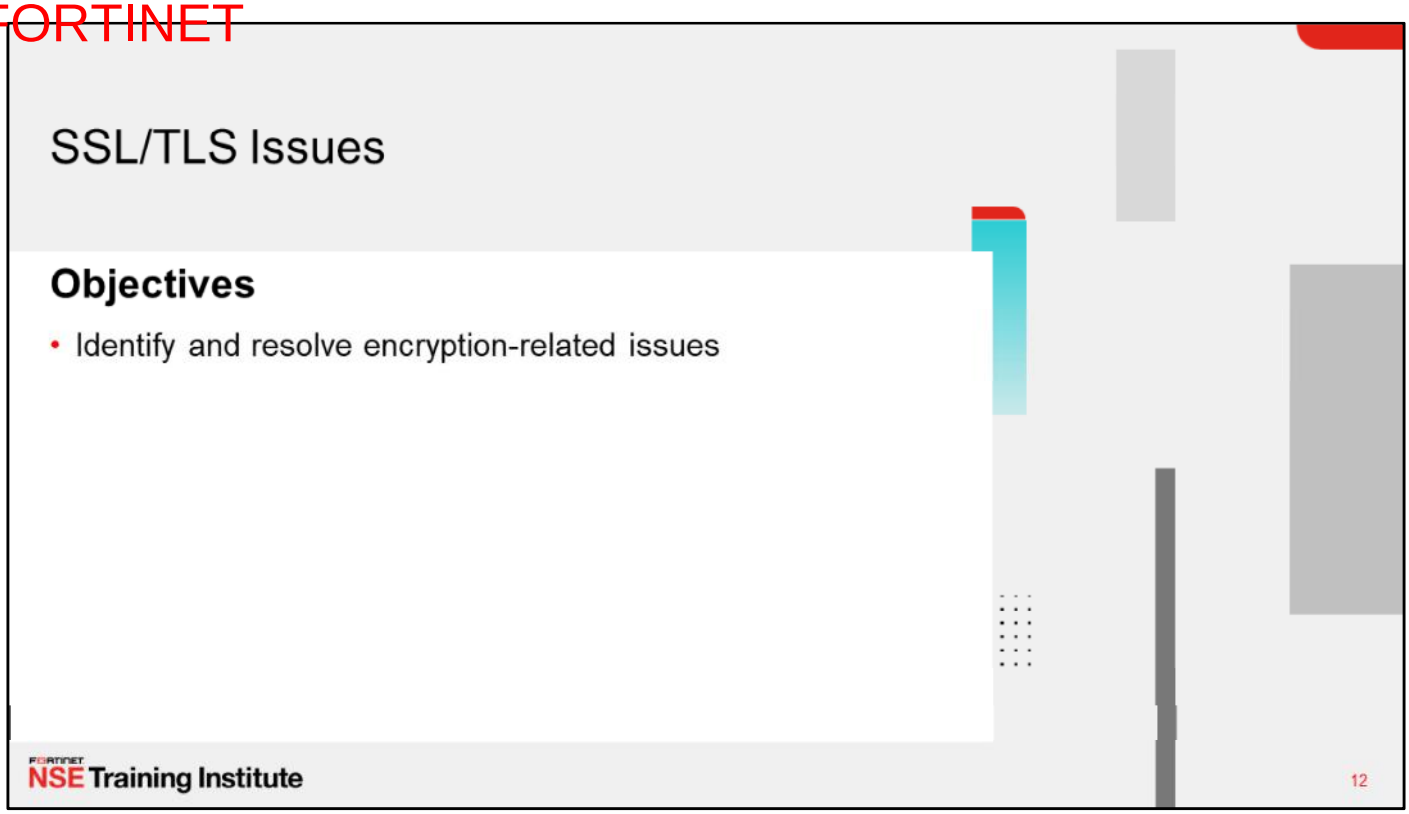


Good job! You now know how to identify and resolve false positive situations on FortiWeb.

Now, you will learn about SSL/TLS-related issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

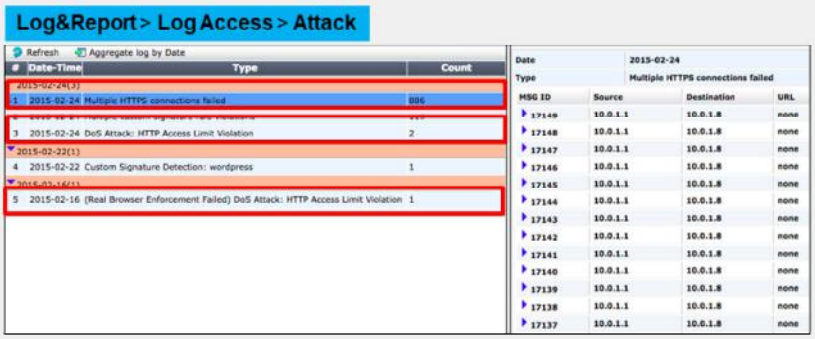
By demonstrating competence in SSL/TLS issues, you will be able to identify and resolve encryption-related issues if your FortiWeb is scanning HTTPS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL/TLS Failure—Aggregated Attack Logs

- Many failed HTTPS connections could be either:
  - Misconfiguration (not supporting enough clients, PFS with transparent mode, and more)
  - SSL/TLS DoS attempt
- Real browser enforcement or DoS sensor indicates DoS



© Fortinet Inc. All Rights Reserved.

A situation where HTTP works and HTTPS sometimes fails may indicate a legitimate attack, not a false positive.

Some versions of SSL and TLS have their own DoS vulnerabilities. Insecure session renegotiation is one. If the following conditions are true, this is a good indicator that these are real attacks, not normal traffic:

- Your DoS sensors are detecting other attacks from the same clients
- They are failing the Real Browser Enforcement test
- You are adding search engine crawlers to the allowlist

If possible, you should disable insecure renegotiation to make SSL-related DoS attacks impossible.

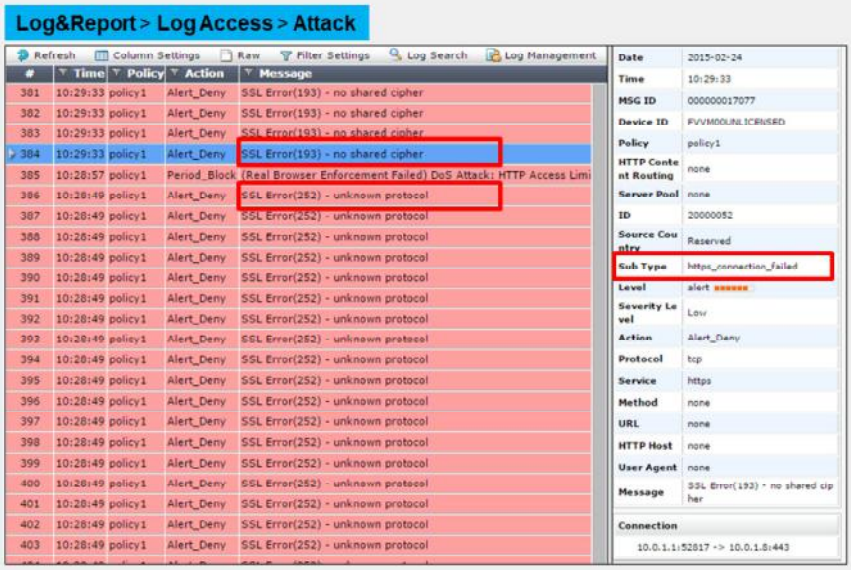
So, what are some examples of genuine misconfiguration issues?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL/TLS Failure—Attack Logs

- `no shared cipher` or `unknown protocol` = proposal mismatch



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

This slide shows examples of two common HTTPS misconfiguration issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL/TLS Mismatches

- SSL Error(252) - unknown protocol
- SSL Error(193) - no shared cipher

1. FortiWeb (virtual server) proposes protocol and possible ciphers to client
2. If disabled on FortiWeb, log shows that SSL 3.0, and so on, was unknown to client
   - If old clients, they may be OK. Expected behavior for PCI DSS compliant sites
     - Android 2.3, IE 6 on Windows XP SP1, old search indexers may not function without SSL 2.0/3.0
   - Attackers may try imaginary versions to probe error handling (for example, TLS 5.9)
     - For repeat attacks, load private key into Wireshark and analyze attack
3. Key negotiation, encryption, and tamper-proofing method mismatch
   - With 160+ cipher suites, and most using the top 3, client and server almost always find a shared cipher
   - Rare unless an attacker is probing for specific weak crypto
     - Fingerprint attacker's IP, user agent, geolocation, and others, to block

NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

If the client and SSL terminator (which is FortiWeb or your web servers, depending on your operation mode) don't use the same SSL or TLS protocol, then their proposals won't match. This causes an unknown protocol message in the attack logs.

In some cases, this is expected behavior. For example, if your environment is required to be PCI DSS compliant, you might see this error when some old clients try to use your web application.

If the protocol is known, but the client and SSL terminator don't support any of the same cipher suites, then they won't be able to negotiate a secure channel. This error is more rare, since there are currently more than 160 combinations. But it is possible, especially if your web application or clients support only a few specific, rarely used cipher suites, such as SEED, or very weak or very strong key strengths. You may want to use Geo IP or another feature to block clients that are probing your network to see if weak ciphers are supported.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Transparent Inspection Mode and PFS

- Transparent inspection mode means server and client negotiate directly
  - FortiWeb is not a termination point
  - If the server supports it, some clients like Google Chrome prefer PFS cipher suites such as ephemeral/anonymous Diffie-Hellman key exchange
- They use the secure channel to re-key
- Perfect forward secrecy (PFS) means cracking an old key won't jeopardize the privacy of subsequent data transfers; keys are unrelated
- Result: FortiWeb can't inspect
  - Virus uploads
  - XML parser attacks
  - SSL/TLS errors in logs
- To fix this, disable PFS suites on web server
  - Server won't offer them to client
  - On Apache 2:

```
SSLCipherSuite HIGH:!ADH:!EXPORT:!NULL:!MD5:!SSLv2
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 16

This case is extremely rare, but you could also see some messages that indicate that FortiWeb can't inspect the HTTPS traffic. This is caused by the combination of a specific type of cipher suite and FortiWeb operating in transparent inspection mode.

The PFS mechanism is similar to the method where IPsec Phase I keys are temporary and used to negotiate the real, more secure Phase II keys. The idea is that by periodically changing the keys inside a secure tunnel, even if one key is decrypted, only part of the conversation has been compromised—not the entire thing.

Obviously, in order to scan traffic, FortiWeb always must have the right keys to be able to decrypt the packet. Otherwise, it can only scan lower-layer headers. So, if (because of the nature of transparent inspection) FortiWeb is out-of-sync with the current keys, then packet inspection fails.

To fix this, you must disable those types of cipher suites on your web servers. This slide shows an example of how to do this in an Apache 2 configuration file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What problem might PFS cause for your FortiWeb?
   A. Unable to block DoS
   ✓ B. Unable to perform virus scan

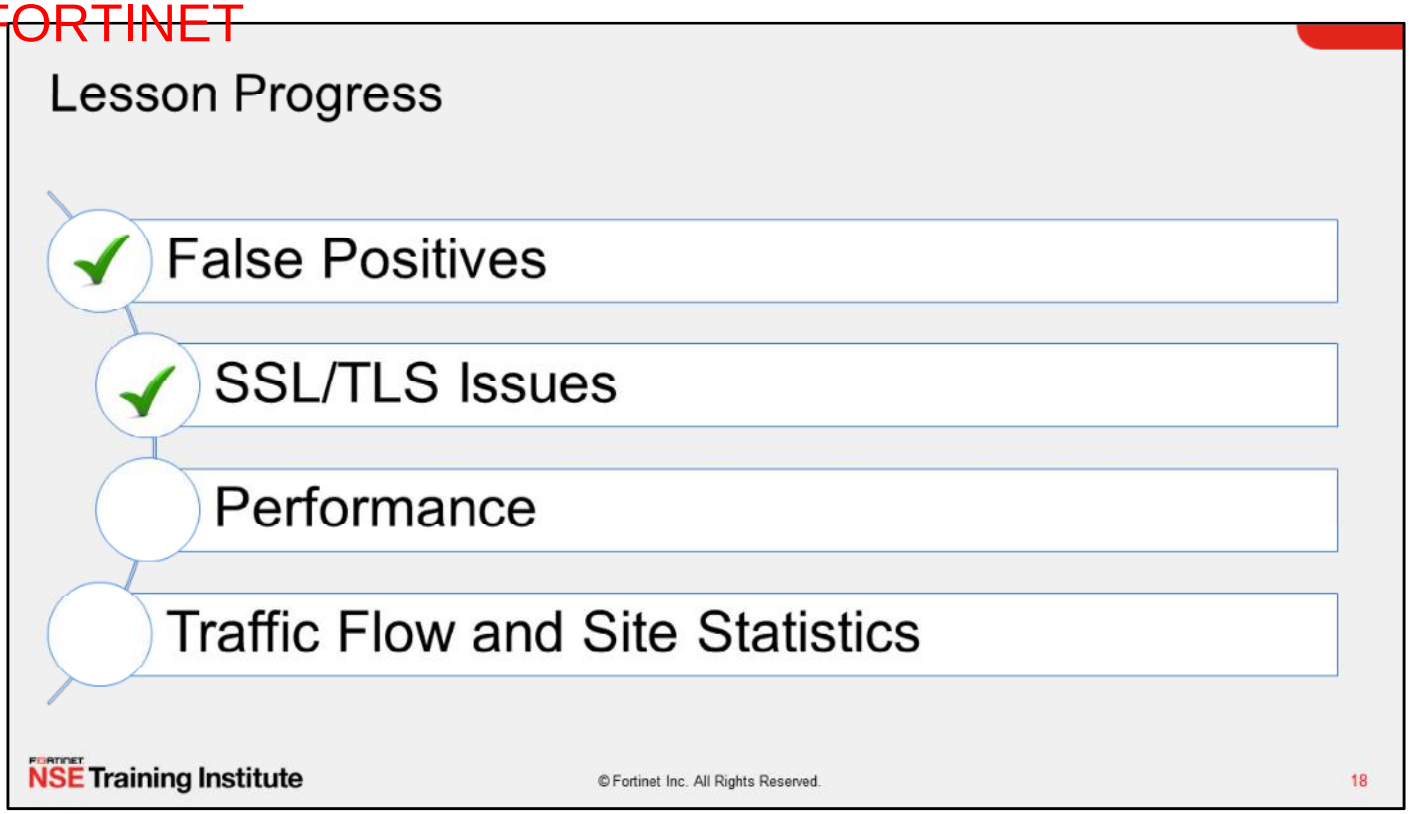
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

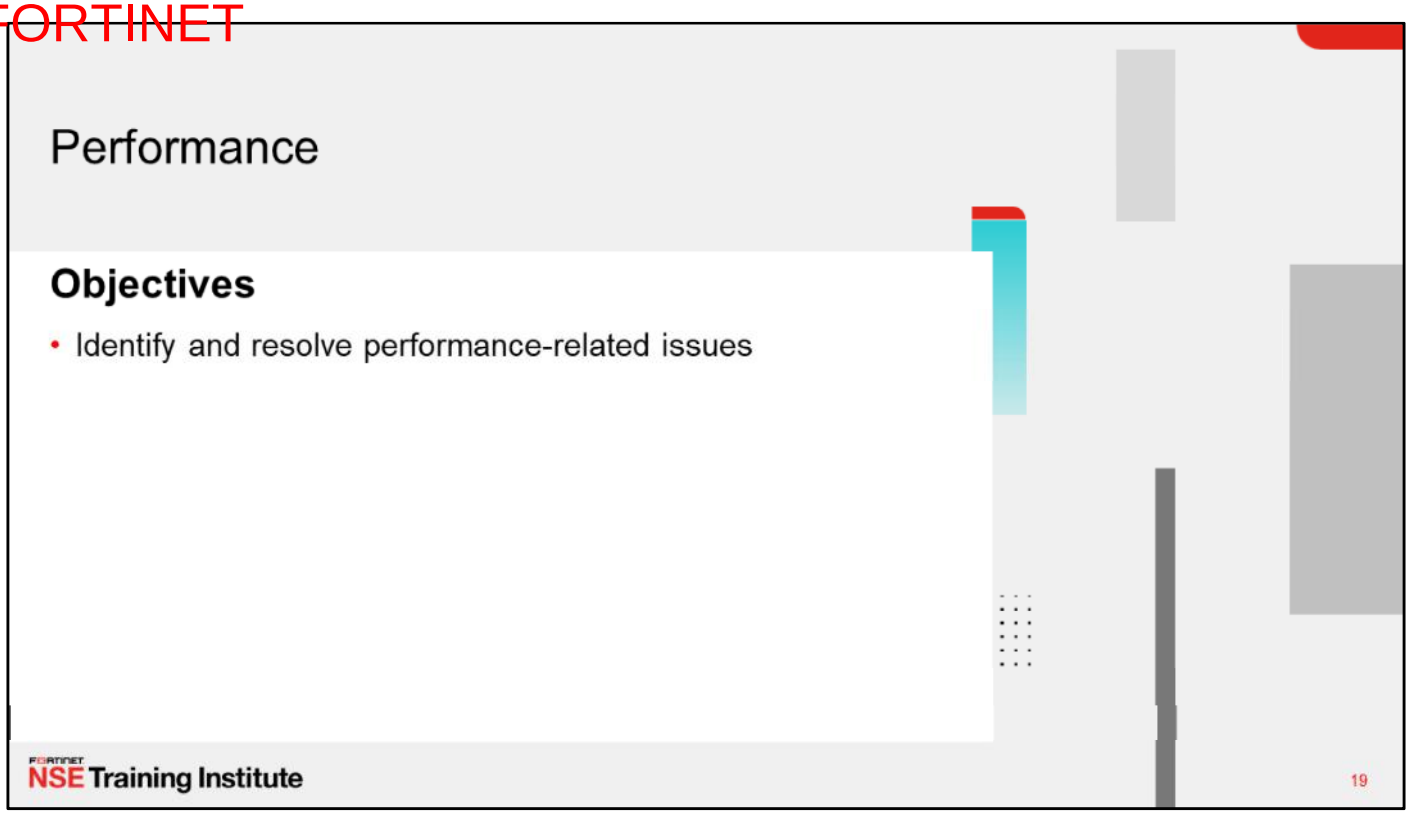


Good job! You now understand how to resolve SSL/TLS-related issues.

Now, you will learn about performance-related issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in identifying and resolving performance-related issues, you will be able to prevent security bottlenecks from occurring.

Vouchers & Dumps are Available | WhatsApp +201224560923

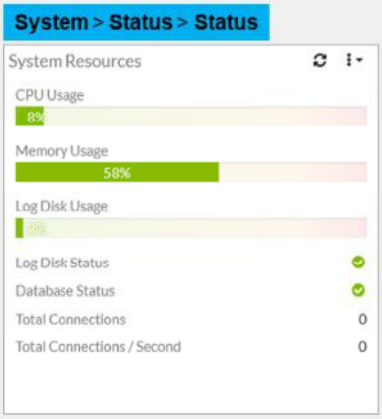
DO NOT REPRINT
© FORTINET
Brave-dumps.com

System Performance

- CLI

```
# get system performance
CPU states:    4% used, 96% idle
Memory states: 20% used
Up:            0 days,  1 hours,  35 minutes
```

- GUI



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

Is performance normal? How do you know?

Begin by observing your system resources and bandwidth usage while FortiWeb is idle and during low traffic periods, such as nighttime and weekends. Then, observe system resource usage on weekdays and holidays, including expected traffic spikes such as marketing campaigns or quarterly financial reports to stockholders.

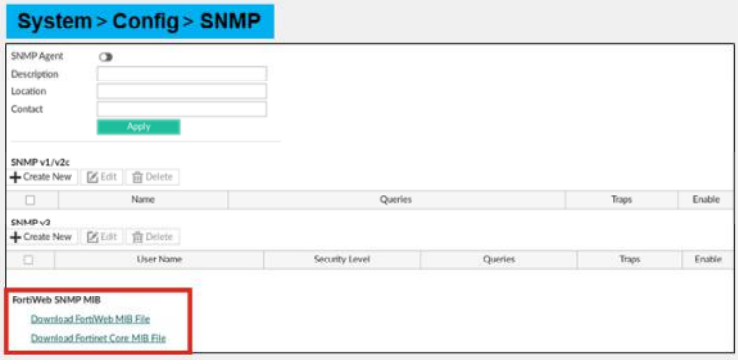
What is the normal range? What is the expected rate of growth?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SNMP Traps and Queries

- SNMP v1, v2c, or v3
- Standard Fortinet MIB, plus FortiWeb-specific ones
  - "Network link down," "CPU usage is high"
  - "Invalid hidden field detected", and so on
- Download MIB from FortiWeb directly



NSE Training Institute © Fortinet Inc. All Rights Reserved. 21

If you have an SNMP manager, such as FortiManager or Cactus, SNMP traps and queries are a good way to track traffic and system resource changes over time. You can use the collected data to help you plan for network upgrades as your organization grows.

If SNMP shows sustained high resource usage, related traps can help you find the cause.

For example, if the high resource usage correlates with an attack detected by a signature, then you may need to optimize a custom signature's regular expression.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Event Logs

- System events including high RAM or CPU usage

Log&Report > Log Access > Event

#	Date/Time	Level	User Interface	Action	Message
66	10:33:58		GUI	restore	User admin restored the configuration failed from GUI(100.64.0.10)
67	10:33:42		GUI	restore	User admin restored the configuration failed from GUI(100.64.0.10)
68	10:33:11		GUI	restore	User admin restored the configuration failed from GUI(100.64.0.10)
69	10:00:02		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is up
70	09:59:57		GUI	edit	User admin changed server-pool server-pool1 pserver-list 2 from GUI(100.64.0.10)
71	09:03:17		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is up
72	09:01:50		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is up
73	09:01:06		daemon	check-resource	all servers in server pool server-pool1 are down
74	09:01:06		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is down
75	09:01:06		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is down
76	09:00:38		daemon	update	update network error:failed to connect servers.
77	09:00:17		sys	start	Backup daemon started
78	09:00:17		sys	start	FortiWeb started
79	09:00:17		daemon	edit	Seeding successfully from the old method
80	03-12 19:52		console	shutdown	System shut down
81	03-12 19:50		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is up
82	03-12 19:50		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is up
83	03-12 19:50		GUI	edit	User admin changed health check list 1 from GUI(100.64.0.10)
84	03-12 19:41		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is up
85	03-12 19:40		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is up
86	03-12 19:39		daemon	check-resource	all servers in server pool server-pool1 are down
87	03-12 19:39		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is down
88	03-12 19:38		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is up
89	03-12 19:37		daemon	check-resource	all servers in server pool server-pool1 are down

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

High RAM or CPU usage can also be tracked in the logs. If you have a FortiWeb model with less RAM, you may need to adjust your system alert thresholds. That way, you won't receive alert email or many log messages and traps during normal load. You can specify the thresholds in **Log&Report** > **Log Config** > **Other Log Settings**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Alert Email

- SMTPS and SMTP over STARTTLS supported
- Configurable interval and severity threshold
  - During a DoS attack, frequent logs and alerts would make resource shortage worse
  - FortiWeb records one message for multiple instances during a DoS attack
  - Won't flood your inbox
- Can be centralized through FortiAnalyzer or FortiSIEM

NSE Training Institute © Fortinet Inc. All Rights Reserved. 23

You wouldn't transmit your security logs over the internet without encryption, right? The same principle applies to alert email.

Since your mail servers may not be in the same data center as FortiWeb, FortiWeb now supports secure mail protocols to protect the messages while they are in transit.

To preserve performance while you are under a DoS attack, FortiWeb records only one log and sends one alert email for multiple instances. This also prevents your inbox from being flooded. While the attack continues, FortiWeb periodically records the event. The interval between recordings varies slightly, depending on the type of attack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Resource Usage

```
# diagnose sys top
     Mem: 2566980K used, 1480872K free, 61436K shrd, 168672K buff, 722024K cached
     CPU:  1.0% usr  1.8% sys  0.0% nic 91.1% idle  5.5% io  0.0% irq  0.4% sirq
     Load average: 2.44 2.52 2.52 1/226 15645
      PID  PPID USER     STAT   VSZ %VSZ CPU %CPU COMMAND
      1957  1908 root     S    1822m 45.9   0  1.0 /data/bin/mysqld --defaults-file=/
      1927     1 root     S    1242m 31.3   0  0.7 /bin/proxyd
      1929     1 root     S     980m 24.7   0  0.0 /bin/bot_daemon
      1928     1 root     S     973m 24.5   1  0.2 /bin/ml_daemon
      1916     1 root     S     786m 19.8   1  0.0 /bin/monitord
      1934     1 root     S     525m 13.2   0  0.0 /bin/sandboxd
      1923     1 root     S     469m 11.8   0  0.0 /bin/wvsd
      1936     1 root     S     436m 10.9   1  0.0 /data/bin/shibd -F -f -p /var/run/
     12581  1907 root     S     420m 10.5   0  0.0 /bin/httpsd
     15379  1907 root     S     420m 10.5   1  0.0 /bin/httpsd
      9037  1907 root     S     420m 10.5   1  0.0 /bin/httpsd
      1907     1 root     S     414m 10.4   0  0.0 /bin/httpsd

# diagnose sys kill 9 1957
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

As on FortiGate and other Fortinet products, if a process is consuming an abnormal amount of RAM, you can immediately terminate the process. It may be respawned, so this is not a permanent solution, but it can provide temporary relief while you enable debug logging.

In the example shown in this slide, a specific policy is consuming an abnormally high amount of RAM. If you kill the process, and notice that it initially starts with much lower RAM usage, it could indicate a memory leak. This would require a firmware upgrade to fix. In other cases, high RAM usage can be caused by misconfiguration.

Debug logs can help both you and Fortinet Technical Support locate the cause of abnormal resource usage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Optimizing Buffers

- Too many buffers or very large buffers require more RAM usage
  - HTTP and HTML pages often require long string buffers
  - Exceeding physical RAM causes OS to page to disk, reducing throughput
- Decrease body and DLP cache sizes in **System > Config > Advanced**
- Block files larger than free RAM with file upload policy
- HTTP protocol constraints can restrict number and length of other buffers
  - In CLI, can configure more FortiWeb buffers and block or pass behavior, when request won't fit in buffer limits
  - If attack is *not* repeated, period-block action does *not* lower CPU usage, but will increase RAM usage

NSE Training Institute © Fortinet Inc. All Rights Reserved. 25

Just like your web applications, FortiWeb has its own memory buffers. It uses them to temporarily store information until it is finished processing. Many of these buffers are configurable, so if you aren't careful, your configuration can decrease performance.

Avoid increasing the body cache and DLP cache sizes, unless necessary. To harden your security, configure FortiWeb with HTTP constraints that block any part that is too large to fit its HTTP or HTML parser buffers.

Also be aware that the period-block action does not always improve performance. Like any cache, it is a shortcut to avoid repetitive CPU processing that has the same results. So, if a client tries an attack only once, then its entry in the cache is still consuming RAM, but not providing any benefit. Using period block improves performance only when the same client frequently attacks your web applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Optimizing Cache

- Keep session management cookie timeouts short, if possible
  - 1200 seconds is 20 minutes. Are clients ever idle that long?

```
config waf web-cache-policy
 edit <web-cachce-policy_rule_name>
       set max-cached-page-size <page_size>
       set cache-buffer-size <cache_size>
       set default-cache-timeout 30
 next
end
```

Don't cache responses larger than free RAM

Age cache appropriately

- If configuration is optimized, but RAM usage remains high, plan to upgrade to a FortiWeb model with more RAM or vRAM

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

You can test for persistent, disk-stored cache by rebooting FortiWeb. Usually, cache is ephemeral, stored in RAM.

Reduce RAM usage by keeping HTTP session timeouts, response cache, authentication session caches, and others as low as possible without affecting normal traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Storage Structure

- Composed of:
  - RAM disk (running OS, configuration)
  - Flash memory (firmware images, configuration file, X.509 certificates)
  - Hard disk (event, attack and traffic logs, anti-defacement files, reports)
- To display hard disk partitions:

```
# diagnose system mount list
  Filesystem          1M-blocks      Used Available Use% Mounted on
  /dev/ram0                  97        81        16  83% /
  none                      150         0       150   0% /tmp
  none                      501         0       501   0% /dev/shm
  /dev/sda1                  97        43        49  46% /data
  /dev/sda3                 378        16       342   4% /home
  /dev/sdb1               30238       212     28490   0% /var/log
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 27

Besides the OS and configuration, there are some files that FortiWeb stores on a flash disk or hard disk.

All files and databases are kept in persistent storage that won't be lost when you power off FortiWeb. Each physical disk can be subdivided into logical partitions, which are then mounted on a file system pointer in RAM.

In the example shown on this slide, you can see that logs are stored on a partition that is about 30GB in size. Currently, it contains very little data relative to its total capacity. But the 97MB /data partition is almost half full. Is this normal?

To answer that question, we need to know whether `/data` indicates the hard disk or the flash disk.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Storage Maintenance

- To format the log disk partition:

```
# execute formatlogdisk
```

- To format the *entire* hard disk, must load a special image
  - Required by some firmware updates

- To list all firmware installed on partitions:

```
# diagnose system flash list
have 4 partitions
Image#  Version                          TotalSize(KB)  Used(KB)  Use%  Active
1       FV-KVM-6.4.0-build1444-210629    371048         218380    59%   No
2       FV-KVM-6.4.1-build1464-210903    371048         219052    59%   Yes
3       2021-09-28 10:37                 92760          52        0 %   No
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 28

Normally, you don't need to repartition the disks; however, there can be exceptions. When FortiWeb added the data analytics feature, it required more storage for the data analytics file. So, before loading the firmware update, you were required to upload a special image to repartition the disk. As always, read your release notes to see if there are any special instructions for upgrading.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Log Indexing

- Like FortiAnalyzer, required for search and report to function

```
# diagnose index all show
        time span starts from 2021-11-11 09:47:50.000000
                Total time span is 80908.233065 seconds
                Currently processing/Last processed file
'/var/log/fwlog/root/disklog/elog(2021-09-28-10:46:27).log'
                event log processed ok: 4294, failed: 0
                Currently processing/Last processed file
'/var/log/fwlog/root/disklog/tlog(2021-11-11-11:24:16).log'
                traffic log processed ok: 14, failed: 0
                Currently processing/Last processed file
'/var/log/fwlog/root/disklog/alog(2021-11-11-11:29:35).log'
                attack log processed ok: 2, failed: 0

# execute db rebuild
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 29

Logs and data analytics statistics are both stored in a database. So, if your FortiWeb experiences an unexpected power failure, you may need to check the hard disk for errors, and then you may also need to reindex the database. Otherwise, features that depend on them may fail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Current Administrator Sessions

```
# execute disconnect-admin-session <tab>
<integer>    Index of admin to be disconnected
Currently connected users:
INDEX USERNAME        TYPE  FROM                  TIME
    0 admin           web   100.64.0.10           Tue Aug 27 09:45:54 2021

    1 admin           cli   jsconsole             Tue Aug 27 13:17:27 2021
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 30

If you restart FortiWeb, it terminates all current administrator sessions. If multiple people configure FortiWeb, notify them to save their changes before you enter the `execute reboot` command. You can use this command to show which accounts are currently logged in.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Application Troubleshooting

- In 6.4.1 additional application debug options were enabled:
  - RE/CAPTCHA (`rbe`)
  - User tracking (`user-tracking`)
  - ADFS proxy (`adfsproxy`)
  - Web cache (`web-cache`)
  - Chunk decoding (`chunk-decode`)
  - Compression/decompression (`compress-uncompress`)
  - Acceleration (`web-acceleration`)
- You can use these options with the `diagnose debug` application command to debug application performance and status

```
# diagnose debug enable
# diagnose debug application user-tracking 7
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

Troubleshooting individual modules on the FortiWeb can be difficult. Sometimes it can help to increase the logging level for debugging specific applications.

Remember when finished debugging to enter `diagnose debug disable` and to reset any application-level debugging back to 0, which disables it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which one displays high RAM or CPU usage?
   A. Traffic log
   B. System Performance Dashboard ✓
   C. User Monitor
   D. System check

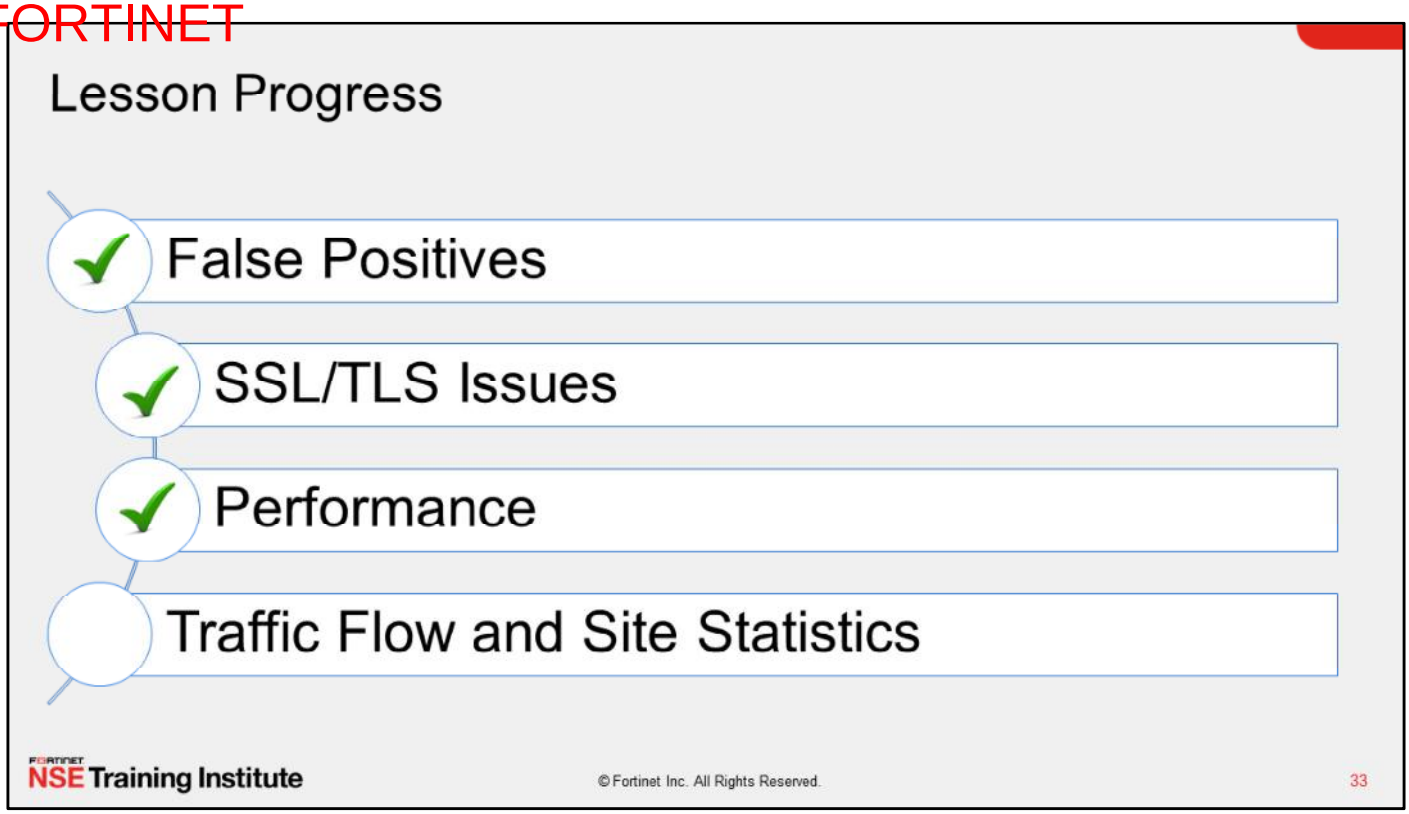
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

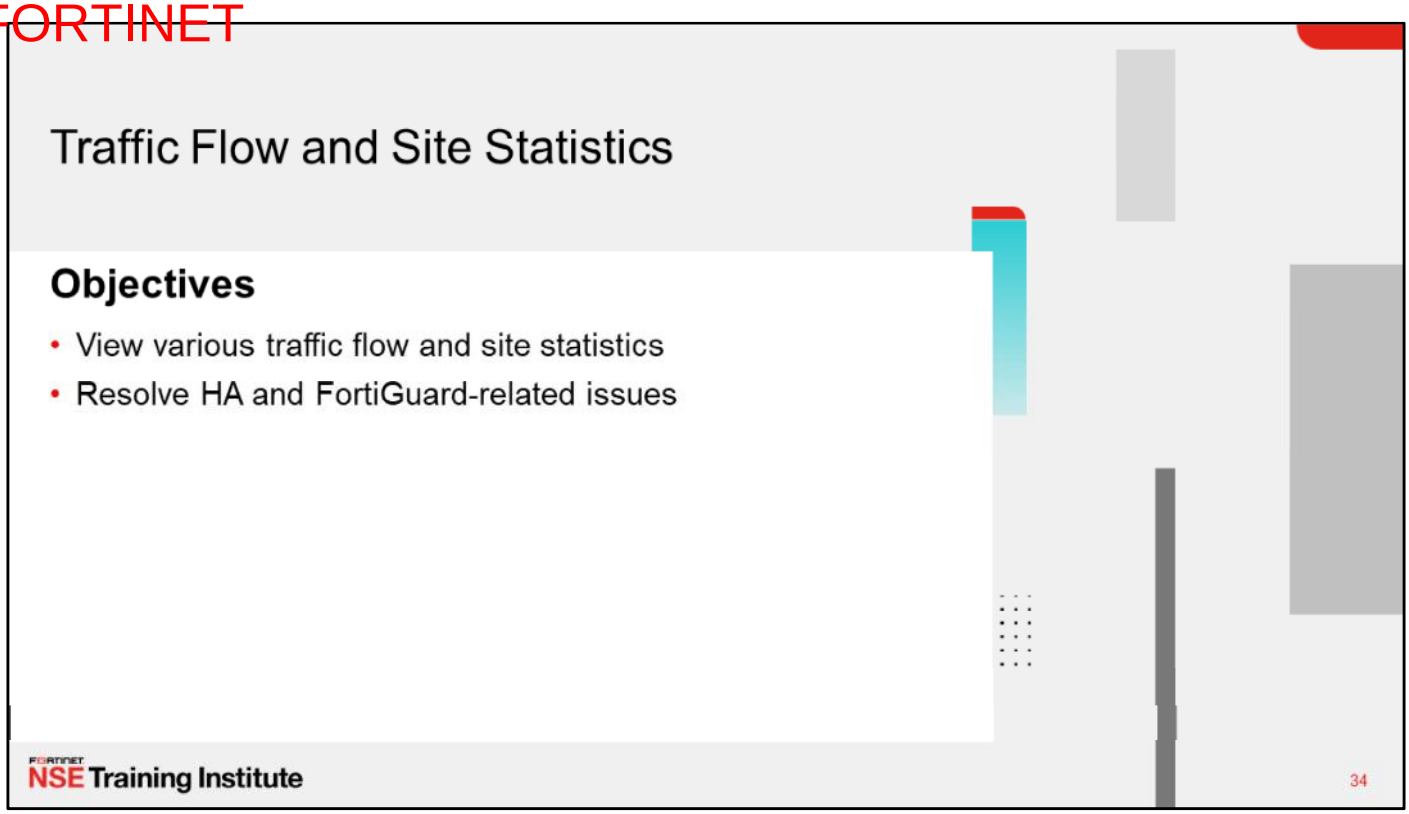


Good job! You now understand how to identify and resolve performance-related issues.

Now, you will learn about traffic flow and site statistics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in traffic flow and site statistics, you will be able to resolve HA and FortiGuard-related issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Network Interface Statistics

```
# diagnose hardware nic list port1
driver                          e1000
version                         7.3.21-k8-NAPI
firmware-version
bus-info                        0000:02:00.0
Supported ports                 TP
Supported link modes            10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Supports auto-negotiation:      Yes
Advertised link modes:          10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Advertised auto-negotiation:    Yes
Speed:                          1000Mb/s
Duplex:                         Full
Port:                           Twisted Pair
PHYAD                           0
Transceiver:                    internal
Auto-negotiation                on
Supports Wake-on                d
Wake-on                         d
Current message level           0x00000007 (7)
```

```
Link detected          yes
Link encap             Ethernet
HWaddr                 00:0C:29:F3:4F:3F
INET addr              10.0.1.7
Bcast                  10.0.1.255
Mask                   255.255.255.0
FLAG                   UP BROADCAST RUNNING MULTICAST
MTU                    1500
MEtric                 1
RX packets             78658
RX errors              0
RX dropped             0
RX overruns            0
RX frame               0
TX packets             100457
TX errors              0
TX dropped             0
TX overruns            0
TX carrier             0
TX collisions          0
TX queuelen            1000
RX bytes               17027027 (16.2 Mb)
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

If you need to analyze your network at a lower level, FortiWeb has many of the same network diagnostic tools as FortiGate.

When viewing the NIC statistics, the FortiWeb VM displays a slightly different output.

For example, the driver shown is for the virtual hardware, provided by Xen or VMware. The virtual MAC is usually dynamically generated at load time—it is not static. Unless you use a distributed virtual switch, you shouldn't notice any transmission errors. Separate vSwitches should also mean that there are no transmission errors. Some will be emulated. There is no actual twisted pair cable in a host-only virtualized network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

ARP Table

- To display the ARP table:

```
# diagnose network arp list
port2: 10.0.1.2  00:50:56:fb:af:21 stale
lo: 127.0.0.1  00:00:00:00:00:00 noarp
lo: 10.0.1.7  00:00:00:00:00:00 noarp
port3: 10.0.1.21  00:0c:29:59:03:56 reachable
port1: 10.0.1.1  00:50:56:c0:00:02 delay
port2: 10.0.1.10  00:0c:29:0e:64:85 stale
lo: ::1  0: 0: 0: 0: 0: 0 noarp
```

- To remove a specific ARP entry:

```
# diagnose network arp delete <port_name> <IP>
```

- To add a static ARP entry:

```
# diagnose network arp add <port_name> <IP> <MAC>
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

You can view the ARP table if you need to find an IP address conflict and you can also use it to diagnose HA issues. If you suspect a split-brain scenario—that is, both devices believe that they are the primary, and that they should assign the IP addresses and virtual MAC address to their physical ports, then log in to the local console on each device. In a split-brain scenario, the ARP list shows that the ports on both devices have the same virtual MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Connectivity Test Commands

- To investigate network connectivity issues:
  - Ping:

```
execute ping {<IPv4> | <host_fqdn>}
execute ping6 {<IPv6> | <host_fqdn>}
```

  - Traceroute:

```
execute traceroute {<IPv4> | host_fqdn>}
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

To test your routing paths, use the FortiWeb `ping` and `traceroute` commands.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Packet Capture—CLI

```
# diagnose network sniffer <interface> <filter> <level> [count] [a]
```

- `<interface>` Physical interface name; or `any` to capture on all interfaces
- `<filter>` Which packets to capture; Berkeley Packet Filtering (BPF) syntax
  - Example: Show `UDP port 1812` traffic between `example.com` and either `google.com` or `duckduckgo.com`
    - 'udp and port 1812 and src host example.com and dst (google.com or duckduckgo.com)'
- `<level>`: Level of information to capture
  - `1`: Basic IP header; omits checksum, TTL, TOS/DSCP, and more
  - `2`: All output from `1`, plus packet payload in both hexadecimal, and ASCII
  - `3`: All output from `2`, plus link layer (Ethernet) header
  - `4`: All output from `1`, plus interface name
  - `5`: All output from `2`, plus interface name
  - `6`: All output from `3`, plus interface name
- `[count]`: Number of packets to capture; otherwise, press Ctrl+C to stop
- `[a]`: Absolute UTC timestamp; otherwise, relative to packet capture's start

NSE Training Institute © Fortinet Inc. All Rights Reserved. 38

Also like FortiGate, you can use the CLI to capture packets that arrive on or leave one of the FortiWeb network interfaces. If you save the output to a file, you can use the `fgt2eth.pl` Perl script to convert it to a format that Wireshark can load.

You can download the converter here:
`https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-import-diagnose-sniffer-packet-data-to/ta-p/191727`

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example: Packet Capture on FortiWeb (Verbosity 1)

```
# diagnose network sniffer port1 none 1 3
  filters=[none]
  2.969258 arp who-has 10.0.1.21 tell 10.0.1.7
  2.969492 arp who-has 10.0.1.22 tell 10.0.1.7
  3.523396 10.0.1.7.22 -> 10.0.1.10.10927: psh 908262810 ack 3725488367
  3 packets recieved by filter
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

Now you will review a couple of examples.

If all you need to know is whether packets from a client using a specific protocol are arriving at FortiWeb on a specific interface, this basic packet capture may be enough. It doesn't filter out any packets. It shows only a few main parts of the IP header, as indicated by the verbosity level number 1.

Because the command automatically stops after three packets, you don't have to press `Ctrl+C` to stop the capture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example: Packet Capture (Filter and Verbosity 6)

```
# diagnose network sniffer packet any 'tcp port 443' 6
filters=[tcp port 443]
interface=[port1]
12.230428 10.0.1.10.11020 -> 10.0.1.8.443: syn 2188166743
0x0000   000c 29f3 4f3f 000c 290e 6485 0800 4500        ..).O?..).d...E.
0x0010   0034 75a2 4000 8006 6f10 0a00 010a 0a00        .4u.@...o.......
0x0020   0108 2b0c 01bb 826c c657 0000 0000 8002        ..+....l.W......
0x0030   2000 c373 0000 0204 05b4 0103 0308 0101        ...s............
0x0040   0402                                           ..

interface=[port1]
12.230457 10.0.1.8.443 -> 10.0.1.10.11020: syn 1895238276 ack 2188166744
0x0000   000c 290e 6485 000c 29f3 4f3f 0800 4500        ..).d...).O?..E.
0x0010   0034 0000 4000 4006 24b3 0a00 0108 0a00        .4..@.@.$.......
0x0020   010a 01bb 2b0c 70f7 0a84 826c c658 8012        ....+.p....l.X..
0x0030   3908 1638 0000 0204 05b4 0101 0402 0103        9..8............
0x0040   0301                                           ..

interface=[port1]
12.230514 10.0.1.10.11021 -> 10.0.1.8.443: syn 4238907980
0x0000   000c 29f3 4f3f 000c 290e 6485 0800 4500        ..).O?..).d...E.
0x0010   0034 75a3 4000 8006 6f0f 0a00 010a 0a00        .4u.@...o.......
0x0020   0108 2b0d 01bb fca8 9a4c 0000 0000 8002        ..+......L......
0x0030   2000 7541 0000 0204 05b4 0103 0308 0101        ..uA............
0x0040   0402                                           ..
...
caught  signo SIGINT
39 packets recved from  port1
39 packets recved by filter
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 40

This is the packet capture that Fortinet Technical Support is likely to request. It contains much more detailed information, as indicated by verbosity level 6. This capture includes higher-level payloads that you can load into a packet analyzer, such as Wireshark, to troubleshoot HTTP and other application-layer issues. To avoid capturing distracting, irrelevant information, we've used the packet filter `tcp port 443` to focus on HTTPS traffic.

Stopping after three packets usually doesn't gather enough information. In the example shown on the slide, the command runs until the administrator presses `Ctrl+C`.

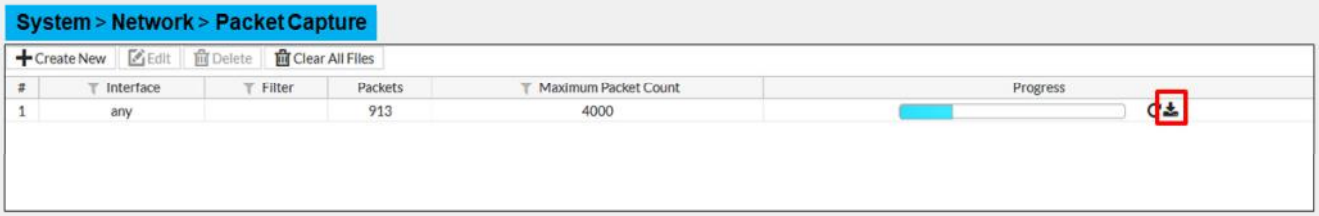
By default, terminal emulators such as PuTTY or TeraTerm have limited buffer in RAM. To use the Perl script to convert this output to Wireshark format, you must configure the terminal client to save the buffer to a plain text file on your computer. If you've never done this before, see the *FortiWeb CLI Reference*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Packet Capture—GUI

- GUI-based packet capture utility
- Captures are in PCAP format
- Downloaded capture files can be opened directly in PCAP tools such as Wireshark



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

FortiWeb features a GUI-based packet capture tool, as well as the traditional CLI commands. Before using this tool, you should have a good understanding of `tcpdump` and filter expressions. You must have read-write permission for system settings.

Capture results are collected in a PCAP format file, which you can download and open in any tool supporting PCAP format, such as Wireshark

Go to `http://www.tcpdump.org/manpages/pcap-filter.7.html` for more information on the `tcpdump` utility.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGuard Connectivity

- Initially FortiWeb connects to default FQDN `update.fortiguard.net`
  - Gets list of FortiGuard servers
- Later, FortiWeb connects to an FQDN server in same time zone
- Connections use HTTPS

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

42

In most cases, FortiWeb can connect easily to FortiGuard. If your firewall blocks outgoing traffic however, this information can help you to configure policies to allow it.

FortiWeb needs DNS, NTP, and HTTPS connectivity to the internet. Depending on your configuration, it may need other protocols too, such as SMTPS for alert email. For a complete list of protocols and default port numbers used by the FortiWeb features, see the *FortiWeb Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGuard Troubleshooting

- DNS must correctly resolve update.fortiguard.net
- FortiWeb must have access to the internet through TCP port 443
- Debug commands:

```
diagnose debug application fds 7
diagnose debug enable
execute update-now
```

  - Also triggers FortiWeb license authentication

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

43

If FortiGuard updates fail, the debug commands shown on this slide can help you to discover the cause.

The `execute update-now` command can also be useful if you have a FortiWeb and you want to force it to immediately authenticate its license, instead of waiting for the next retry interval.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VM and FortiGuard License Validation

- If HA or FortiGuard services don't function after failover
  - Solution: License VM/FortiGuard on all appliances
- If Internet connection is not reliable after 24 hours, license status will change to invalid until connectivity is restored
  - Symptom: Port flapping, complete/high packet loss
  - Solution: Reduce collision domain, signal noise; check outbound firewall
  - Solution: Use a local FortiManager to provide FortiGuard services and licenses
- If slow HA failover
  - Symptoms:
    - Raising number of gratuitous ARPs and increasing `boot-time` appear to improve the issue, but some pings are still lost
    - Licenses do not immediately validate
  - Solution: Don't dynamically SNAT FortiWeb internet connections
    - If upstream router or firewall applies SNAT to connection from FortiWeb, it can look like other machines have stolen the license

NSE Training Institute © Fortinet Inc. All Rights Reserved. 44

Like FortiGate, FortiGuard services on FortiWeb are licensed for each device, not for each cluster.

FortiWeb VM must be able to authenticate its license, just like FortiGuard services. This means that the FortiWeb VM must have a reliable connection to the internet. It also means that you should not apply dynamic source NAT to outbound connections from FortiWeb to FortiGuard, because this can make it look like the VM license has been moved to a different location—or stolen. This can cause unexpectedly related symptoms, such as slow ARP retraining during HA failover.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which command should you use to investigate a connectivity issue?
   A. `diag ping <ip address>`
   ✓ B. `execute ping <ip adress>`

2. What key benefit does the GUI-based packet capture offer over the CLI tool?
   A. More detailed results
   ✓ B. PCAP file output

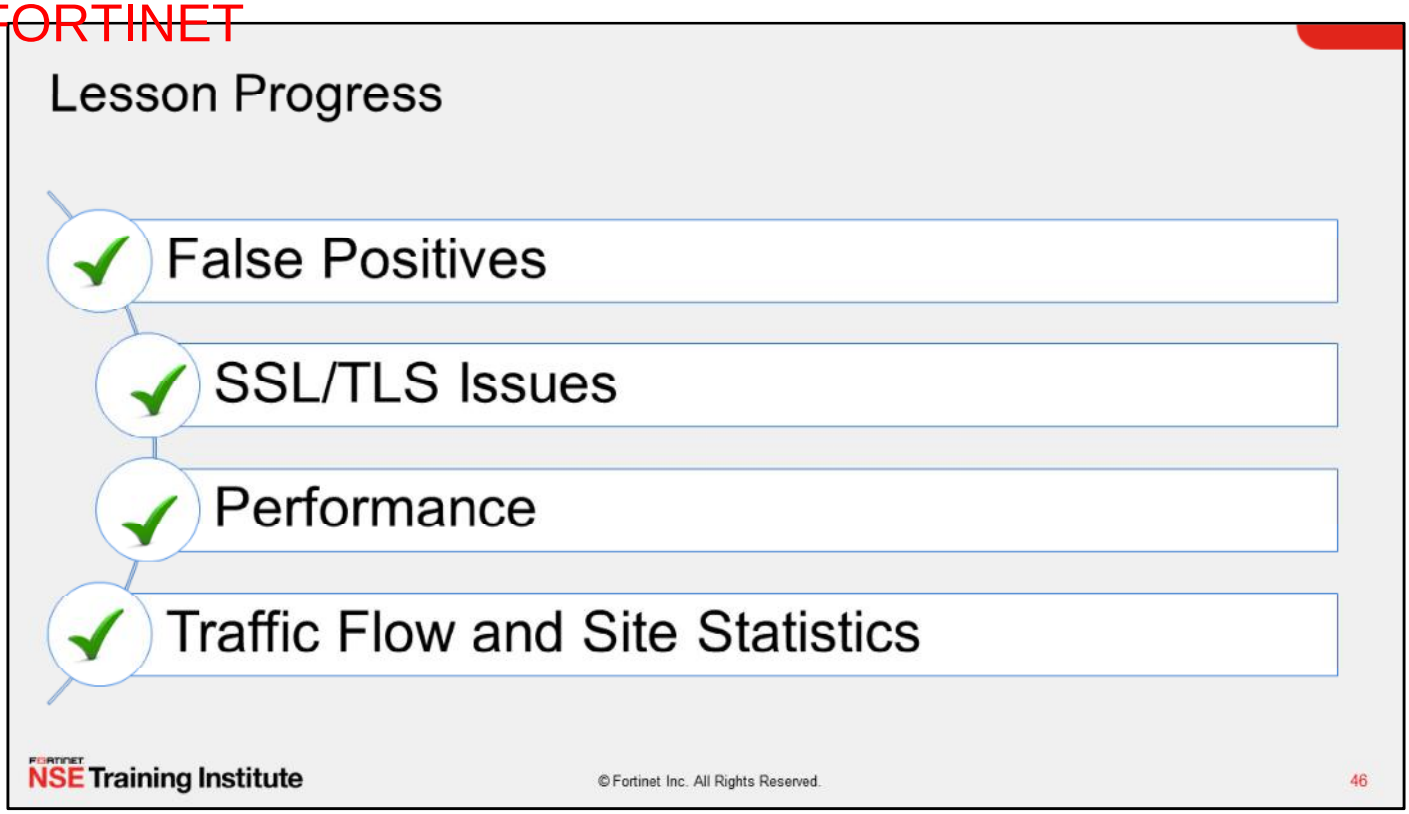
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe and discuss false positives
- ✓ Identify false positives in attack logs
- ✓ Take action to prevent or reduce false positives
- ✓ Identify and resolve encryption-related issues
- ✓ Identify and resolve performance-related issues
- ✓ View various traffic flow and site statistics
- ✓ Resolve HA and FortiGuard-related issues

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to either fix rules and signatures, create exceptions for specific URLs, or disable the signature when they accidentally block innocent traffic. You also learned how to handle content scrapers and search engine crawlers, which often have different settings than web browsers. You learned how to monitor CPU, RAM, bandwidth, and disk space for abnormal usage. You learned that while period block often improves performance, there are cases when that is not true. Finally, you learned how to fix connectivity issues, including ones with FortiGuard and HA clusters.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923