DO NOT REPRINT
© FORTINET

Zero Trust Access

Study Guide

for FortiOS 7.2

FORTINET®
Training Institute

DO NOT REPRINT
© FORTINET

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

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 Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

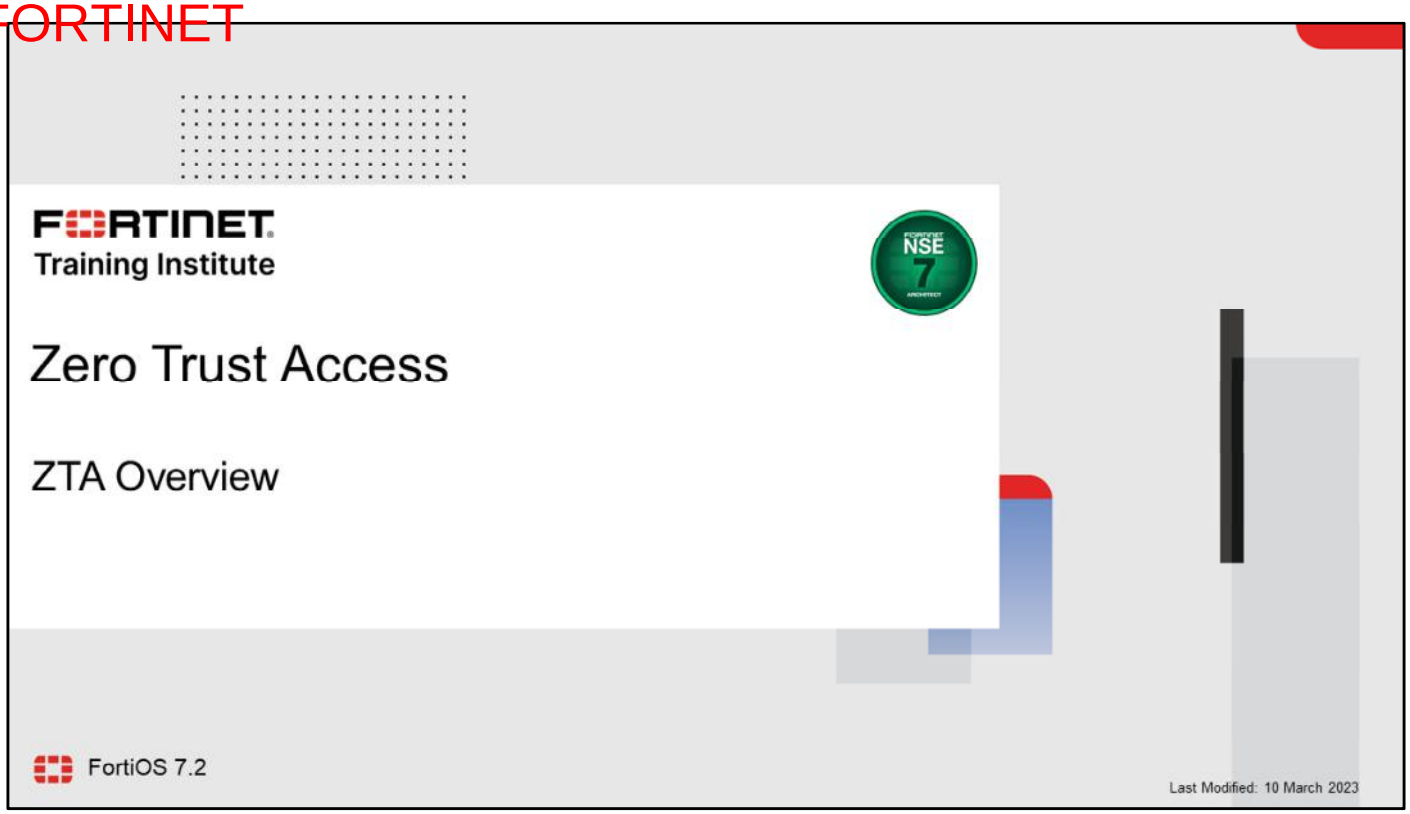
DO NOT REPRINT
© FORTINET

Brave-Dumps.com

TABLE OF CONTENTS

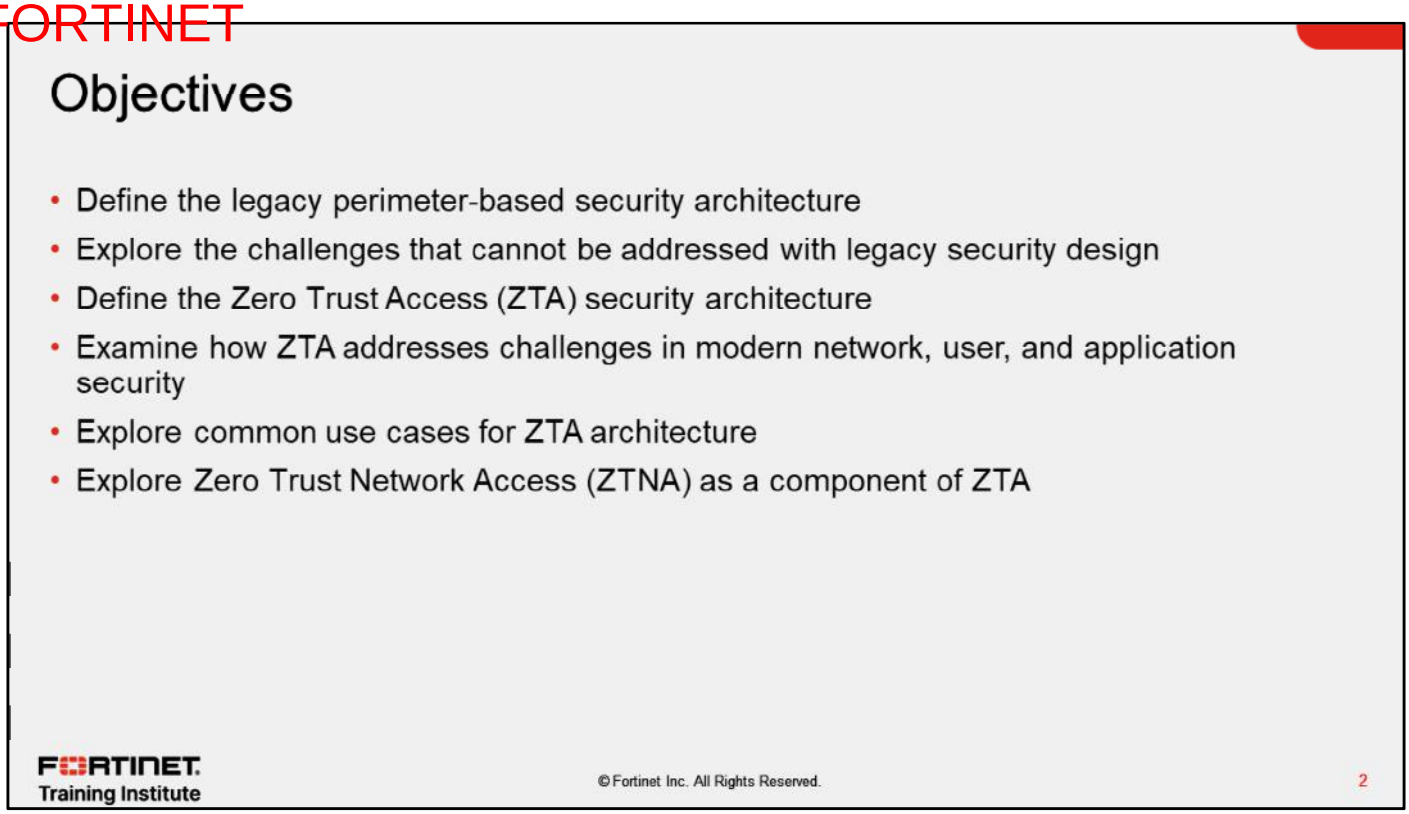
01 ZTA Overview **4**
02 ZTA Components **30**
03 Securing Network Access with FortiNAC **69**
04 Configure ZTNA for Secure Application Access **100**
05 Expanding Secure Access With Endpoint Posture and Compliance Checks **133**
06 Monitoring ZTA Enforcement and Responding to Incidents **163**

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about zero trust access (ZTA) design principles for network, user, and application security.

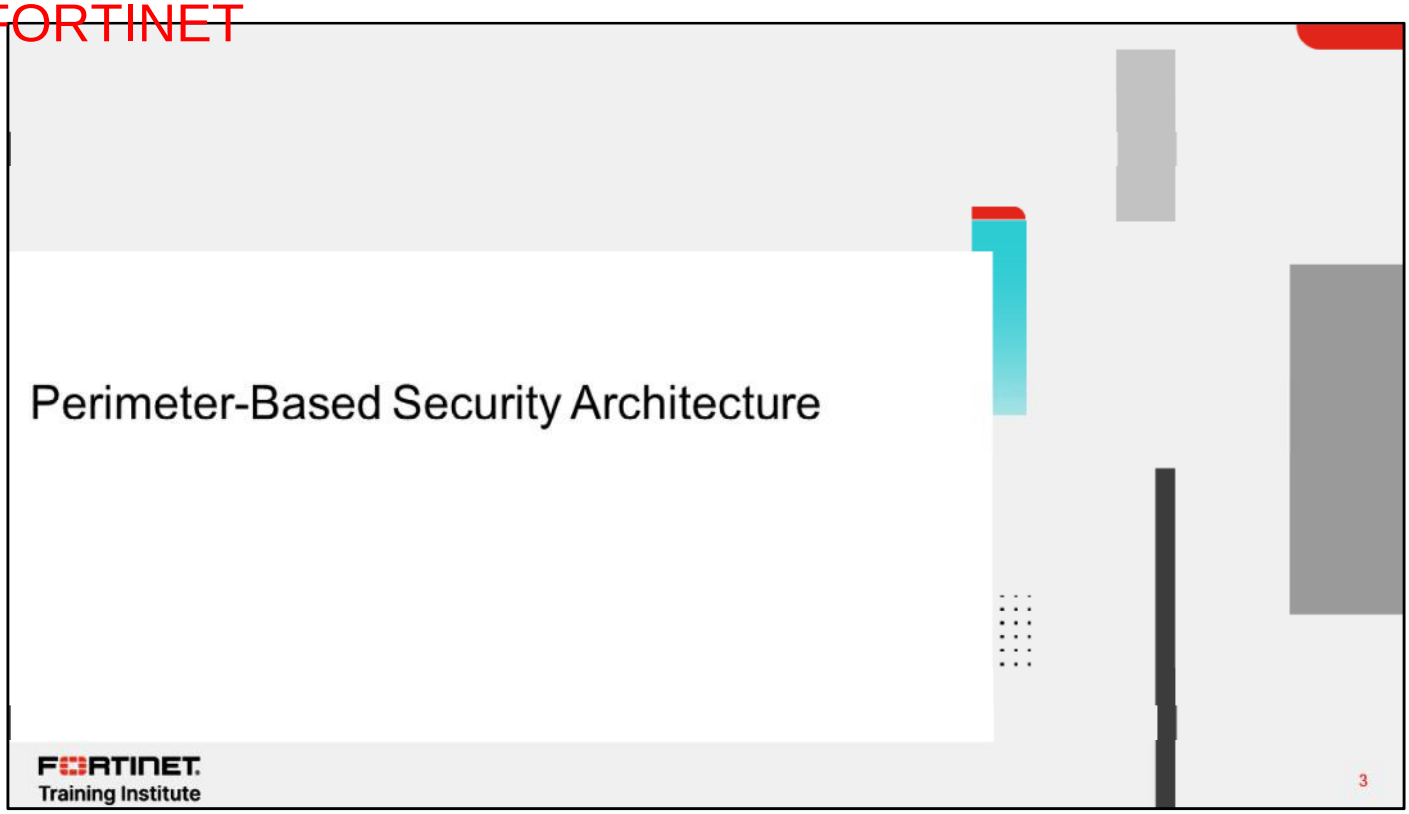
DO NOT REPRINT
© FORTINET



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

By demonstrating competence in ZTA security design principles, you will be able to describe the issues associated with legacy security design and how ZTA can help address modern problems with user, application, and network security. You will also be able to describe the fundamental technologies required to enable ZTA to be used in an environment. Finally, you will understand the differences between zero trust network access (ZTNA) and ZTA.

DO NOT REPRINT
© FORTINET

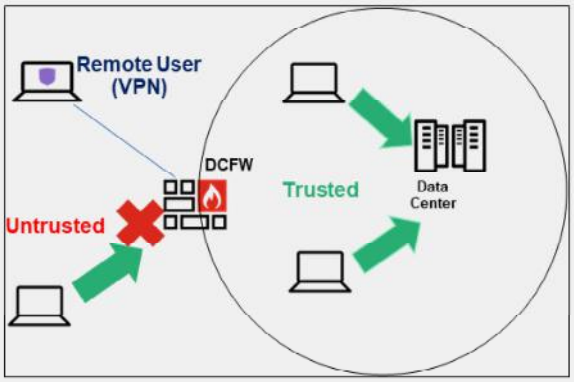


In this section, you will learn about legacy perimeter-based security architecture.

DO NOT REPRINT
© FORTINET

Perimeter-Based Security Architecture

- Traditional approach
- Entire network on premises
  - Corporate data centers
- Implicit trust is granted inside the network
  - User
  - Device location (devices outside the network are not trusted)
- Perimeter is protected by components like firewall, IDS, DMZ, and so on
- VPN is used for remote access



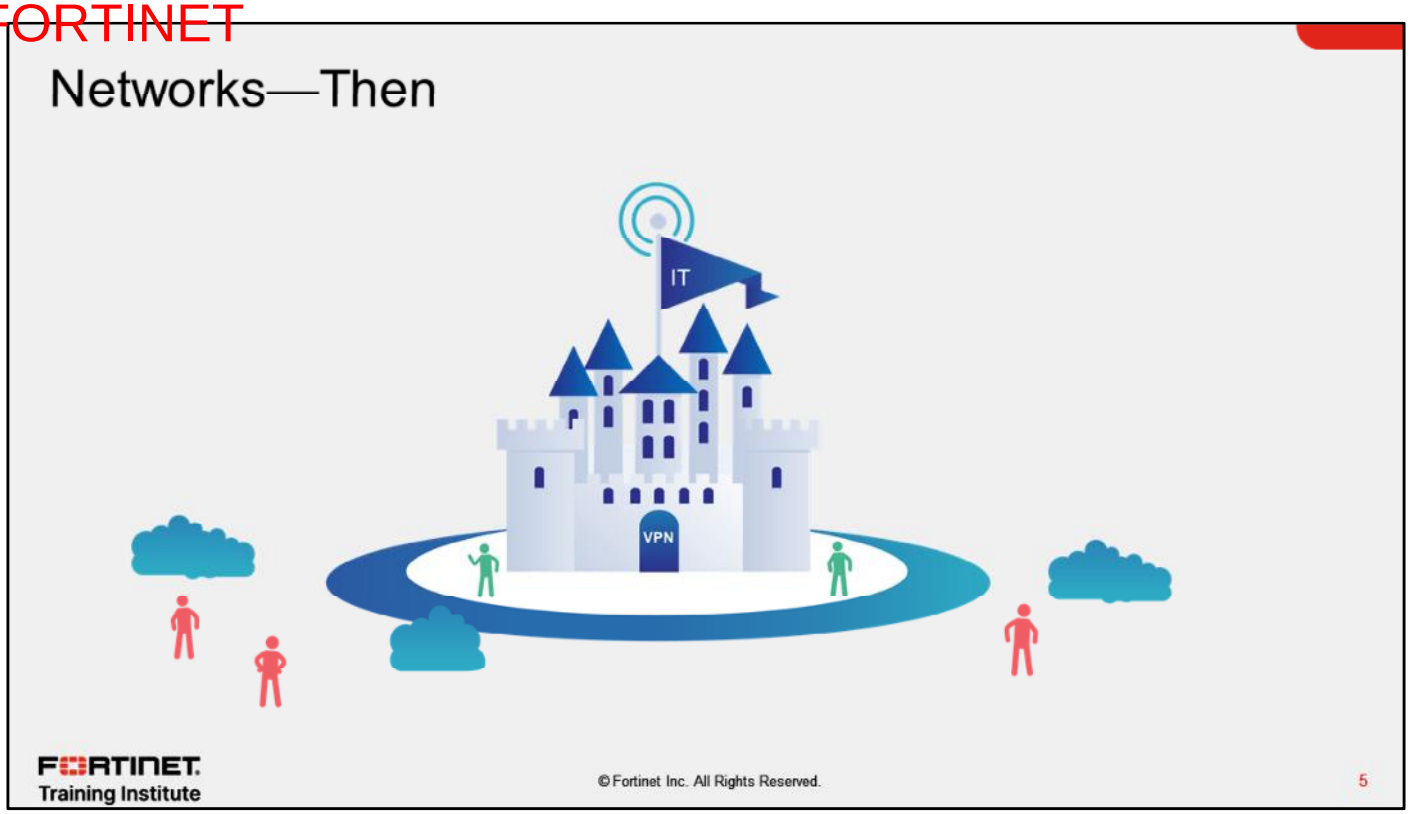
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

Perimeter-based architecture was the traditional approach to network security. In this architecture, the entire network is on premises, for example—corporate data centers. The primary idea behind perimeter-based architecture was to trust devices inside the network and not to trust devices outside the network. Once inside the network, implicit trust is granted, and the user has access to all the corporate resources. The network perimeter is protected by components like firewalls, intrusion detection system (IDS), demilitarized zone (DMZ), and so on. External users and devices are provided remote access to the network using virtual private network (VPN). Over the past decade, many flaws related to network security have been identified in this architecture model.

DO NOT REPRINT
© FORTINET

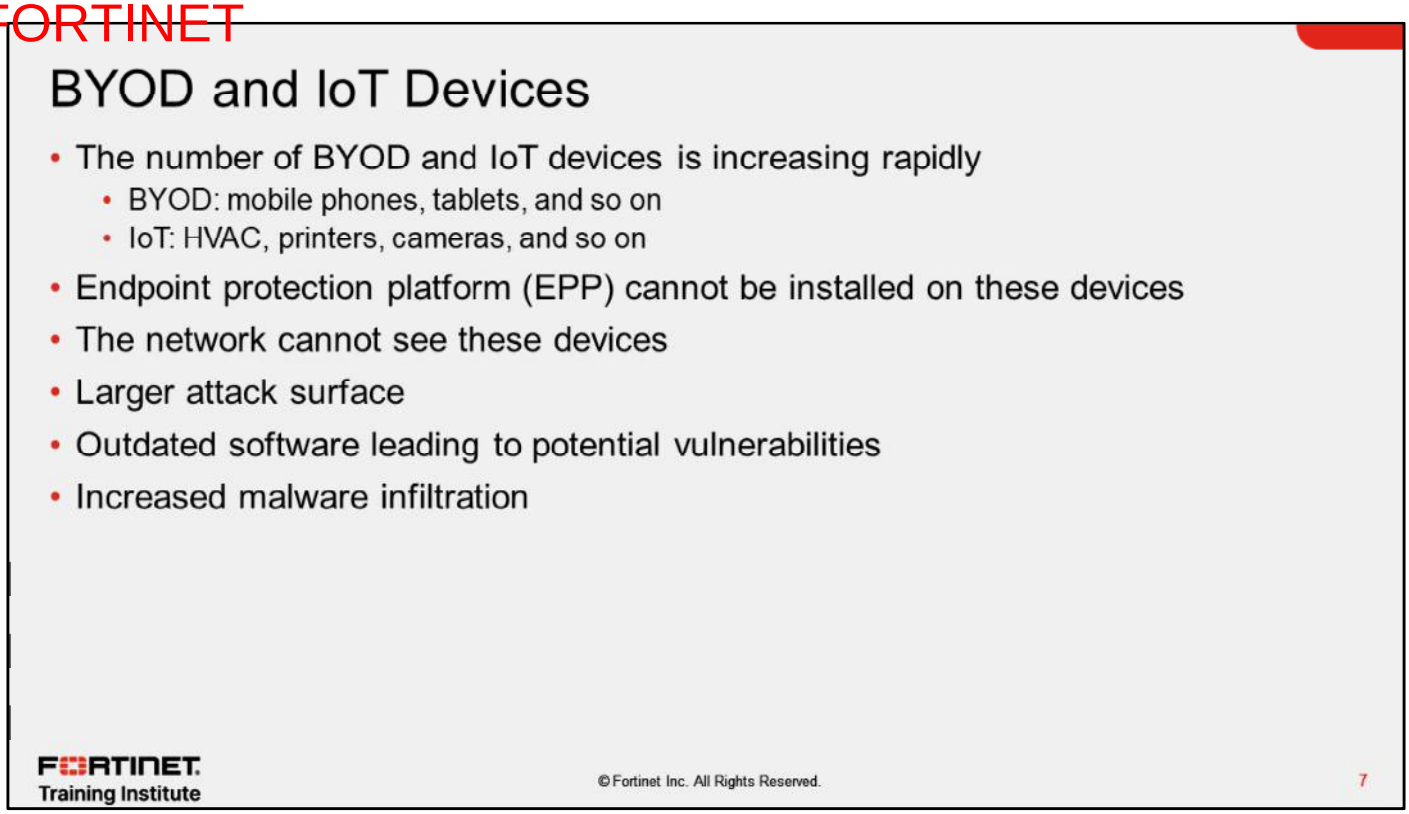


This slide shows an analogy of how networks were deployed in the earlier days and how perimeter-based security architecture can be easily implemented. Once inside the network, implicit trust is granted to the device and user.

DO NOT REPRINT
© FORTINET

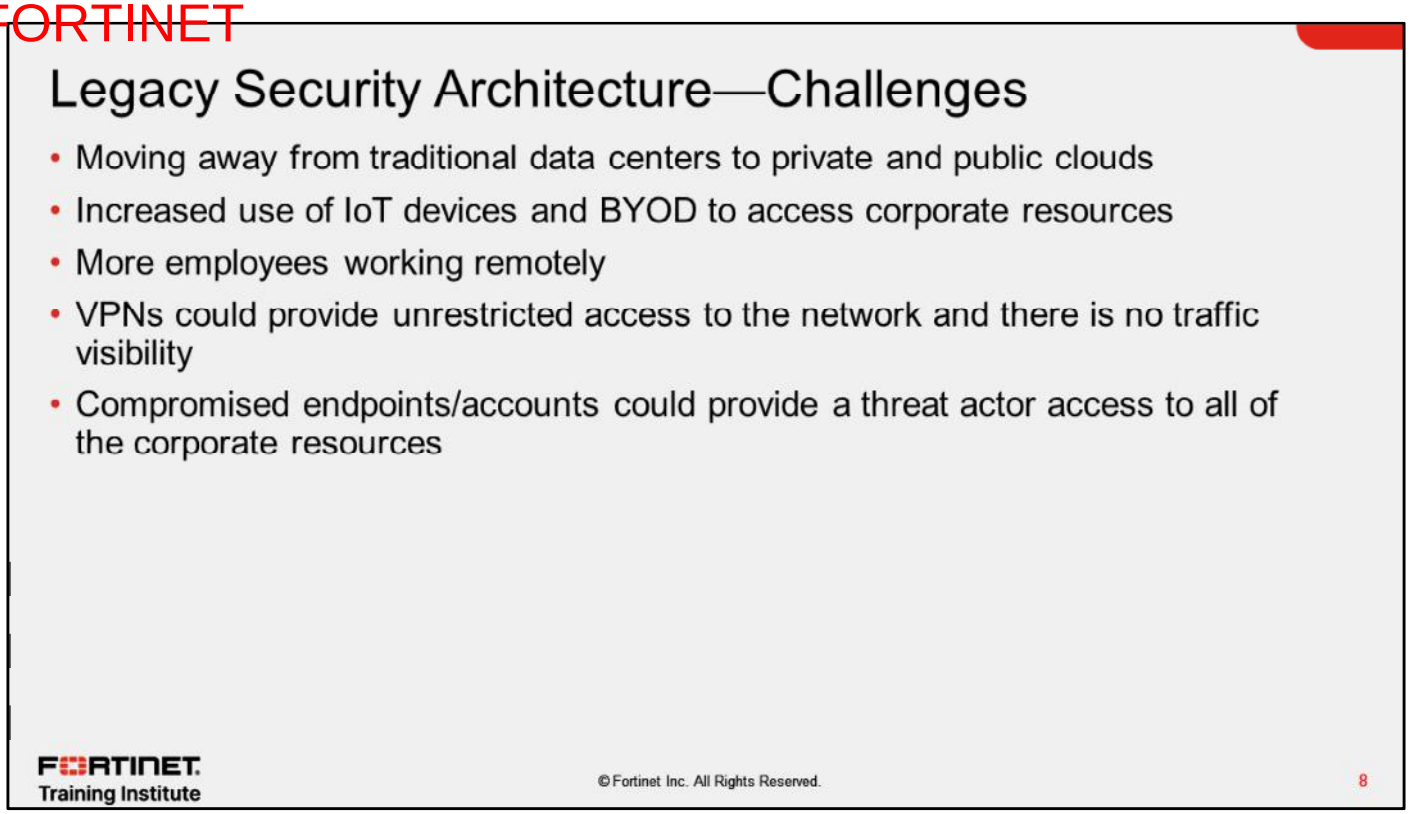
This slide shows an analogy of how networks are currently deployed. With the increase in the number of BYOD, IoT devices, and remote users working from home and remote offices, the perimeter-based architecture is deficient in meeting network security requirements.

DO NOT REPRINT
© FORTINET



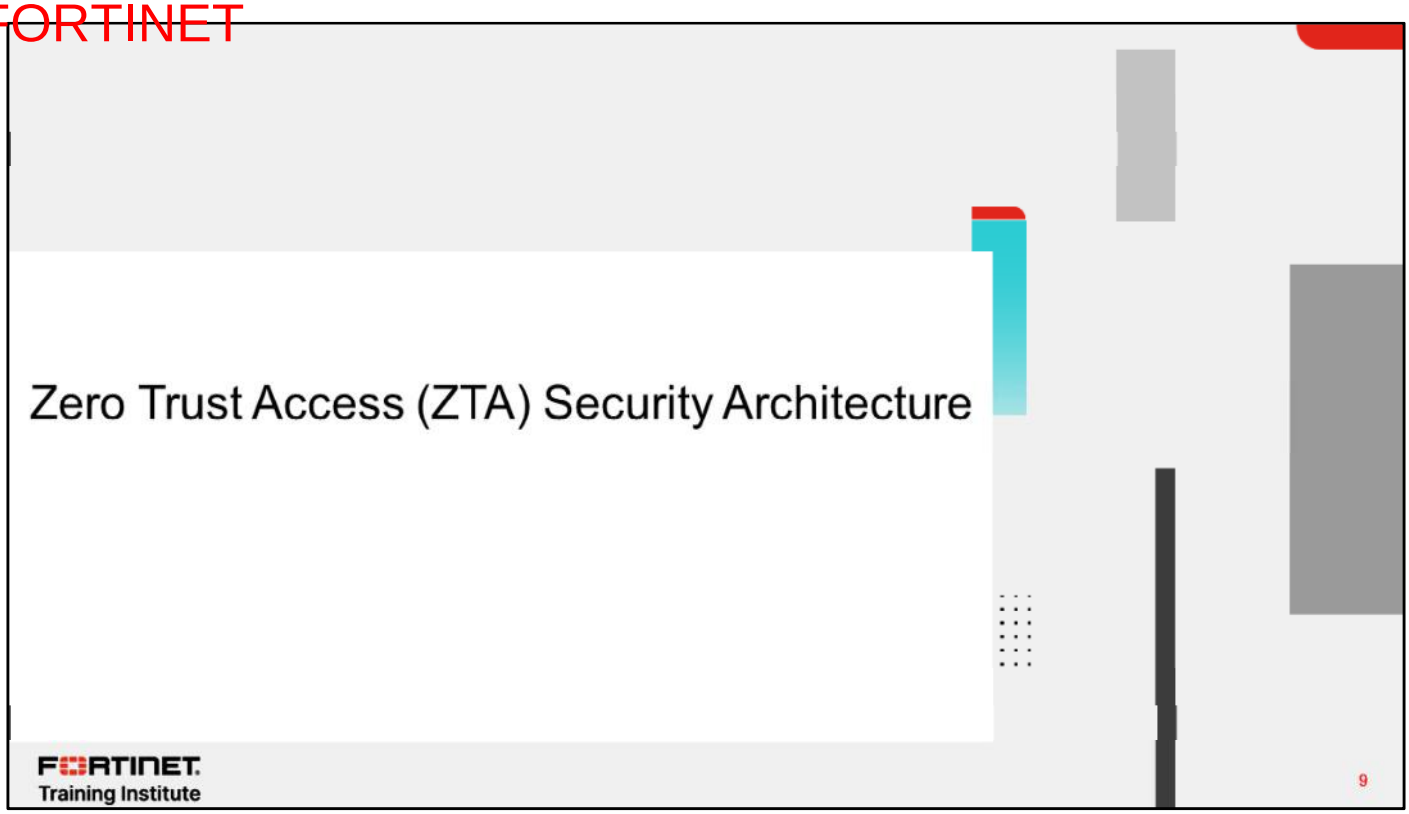
With BYOD and IoT devices increasing rapidly in today's world, it becomes essential that we have visibility of these devices. Network visibility is required to monitor devices with vulnerable software, increased malware infiltration, and so on. The real challenge is headless devices where an endpoint protection platform (EPP) cannot be installed.

DO NOT REPRINT
© FORTINET



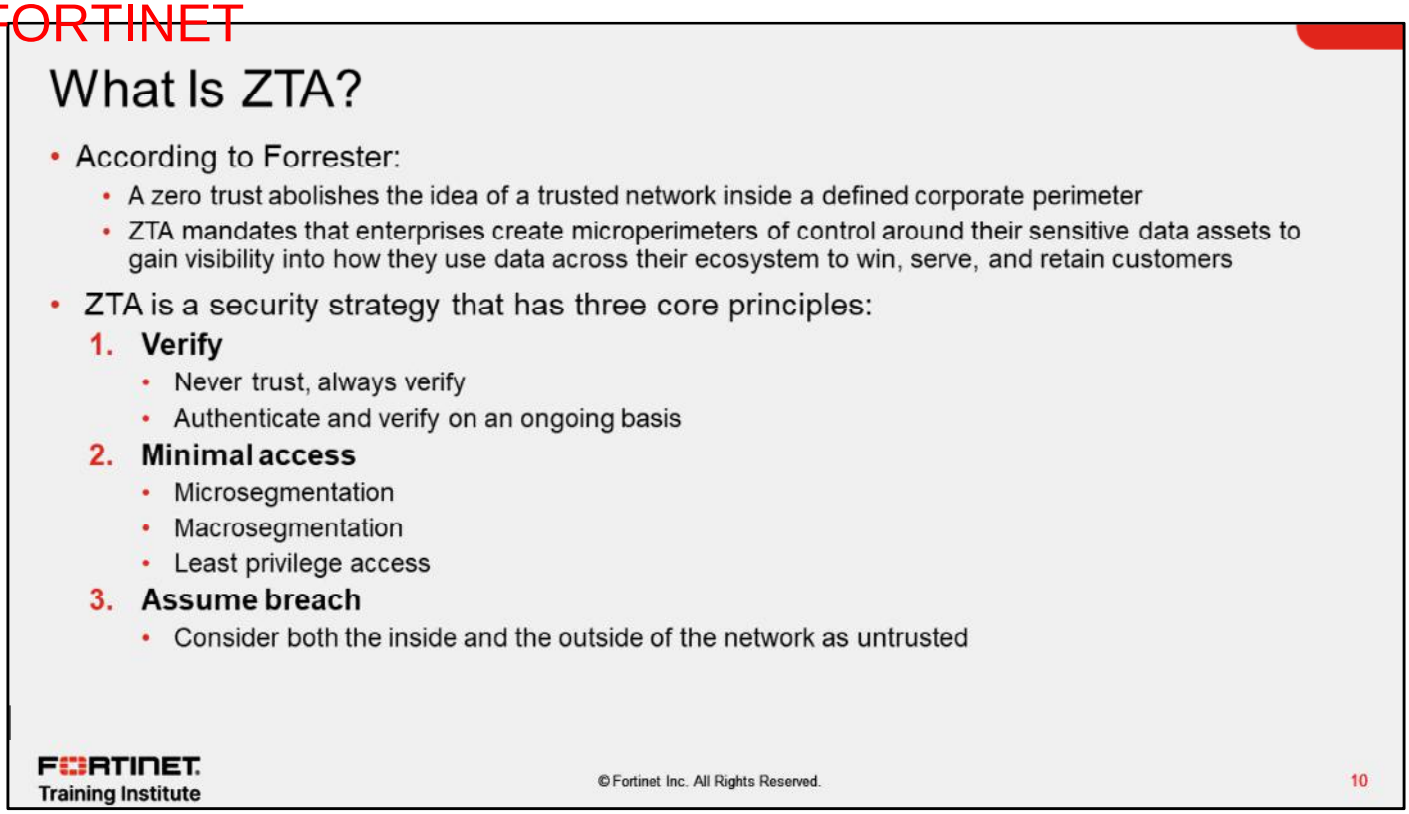
The main challenge with legacy security architecture is moving away from the traditional on-premises data center and moving toward private and public clouds. With more employees working remotely, allowing BYOD and adding IoT devices to your network increases the complexity of monitoring all these devices. VPNs can provide access to the corporate network from the public internet, but there is no visibility of what data is extracted and what malware is propagated from the compromised remote endpoints or user accounts.

DO NOT REPRINT
© FORTINET



In this section, you will learn about ZTA and review ZTA use cases.

DO NOT REPRINT
© FORTINET



According to Forrester, zero trust abolishes the idea of a trusted network inside a defined corporate perimeter. ZTA mandates that enterprises create microperimeters of control around their sensitive data assets to gain visibility into how they use data across their ecosystem to win, serve, and retain customers.

ZTA is a security strategy that has three core principles:

1. Never trust and always verify: This is not only where first-time authentication happens, but continual verification authentication for every session. For example—is the user still authenticated, does the user still have valid credentials, does the user have the proper access permissions, and so on?

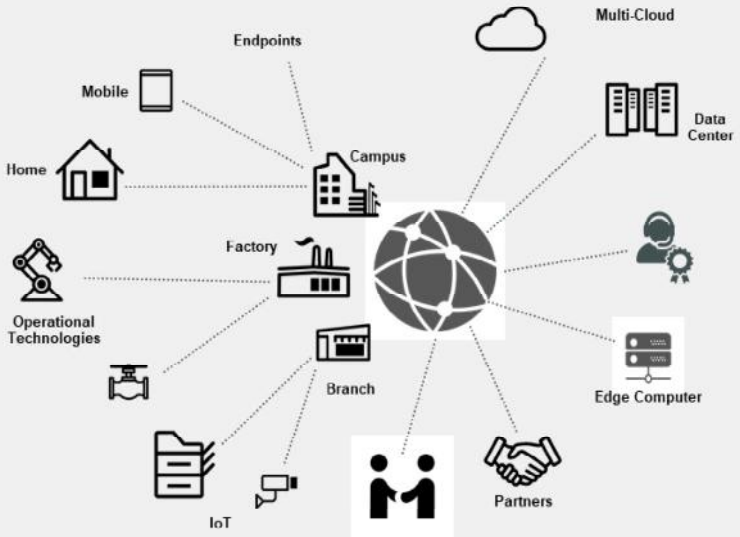
2. Minimal access: Provide users with only the required privileges to perform their jobs. This is where micromsegmentation and macrosegmentation can be deployed to control traffic flow within the network.

3. Assume breach: This is where the zero-trust principle applies. Implement security solutions and policies pretending you have been already compromised and what security measures can be taken, if compromised.

DO NOT REPRINT
© FORTINET

What Is ZTA? (Contd)

- A strategy that applies end-to-end zero trust to users, devices, and applications when they access components of the network
- Requires knowledge and control of everyone and everything on the network



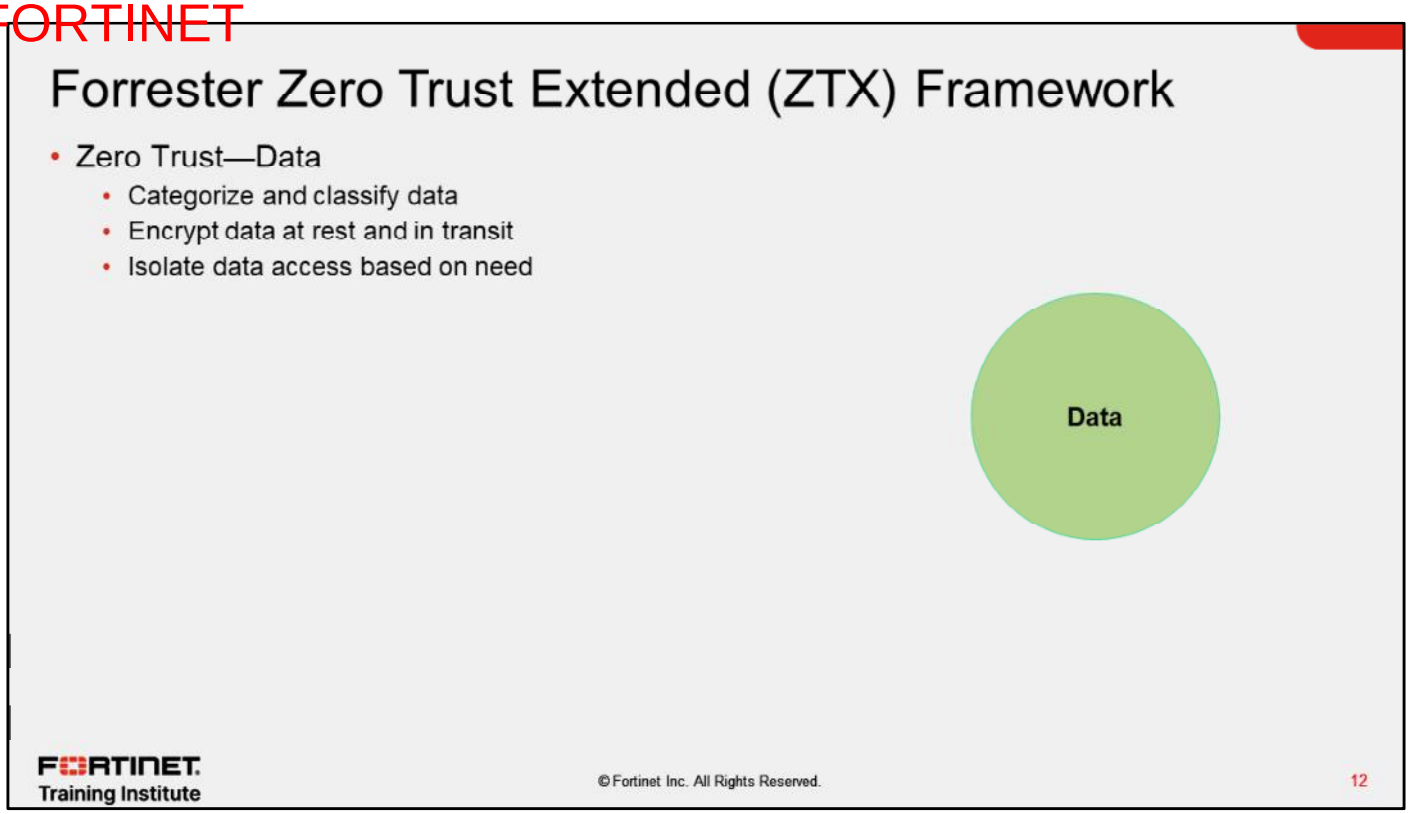
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

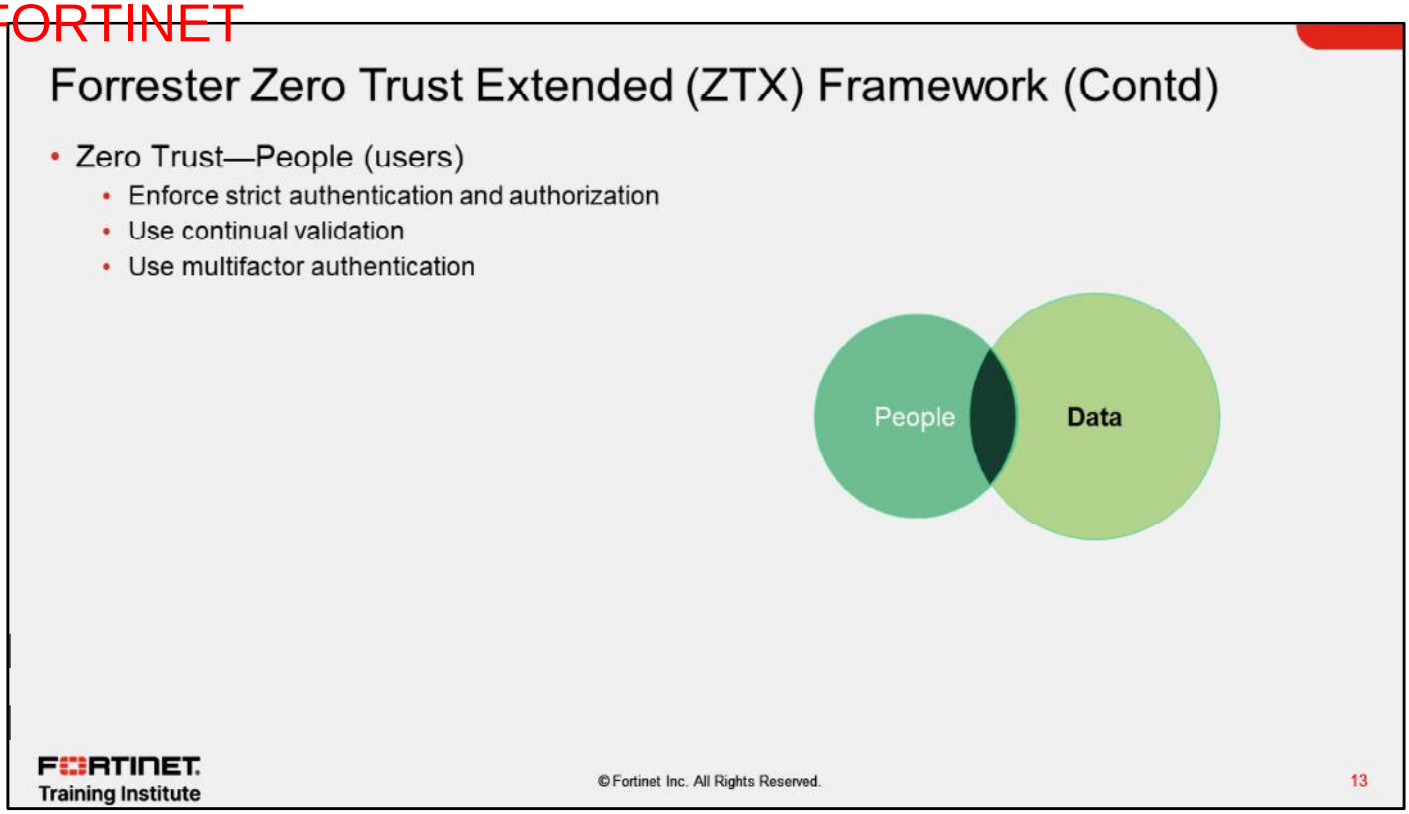
ZTA is a strategy to provide end-to-end zero trust to users, devices, and applications when they access components on the network. Zero trust requires knowing everyone and everything on the network, and controlling who and what has access to resources on the network.

DO NOT REPRINT
© FORTINET



Forrester has defined seven pillars in their ZTX framework. The first pillar represents how to secure data. Firstly, you need to know what kind of data your organization has, so that it can be categorized and classified accordingly. Then, you must decide what levels of protection and encryption are required for the data at rest and in transit. Finally, you must provide access to data on a need-only basis.

DO NOT REPRINT
© FORTINET

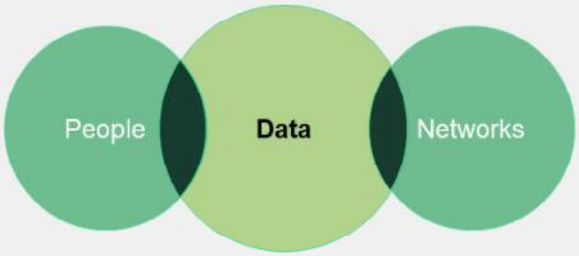


The second pillar defines how to secure users. This is where user authentication happens and where users are assigned access permissions for the data. After the initial user authentication, you should continuously monitor user validation and permissions to prevent unauthorized access to data. This type of monitoring was lacking in the traditional security architecture. Finally, use multifactor authentication (MFA) in your organization to secure user access. This should be the normal practice in today's cybersecurity world.

DO NOT REPRINT
© FORTINET

Forrester Zero Trust Extended (ZTX) Framework (Contd)

- Zero Trust—Networks
  - Segment assets into different subnets
  - Use microsegmentation for each application
  - Isolate and control access according to need, even within same subnet



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

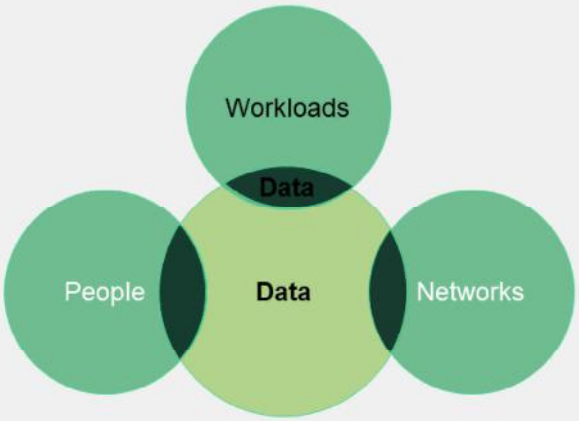
14

The third pillar defines how to secure the networks. This is where your corporate assets are segmented into subnets, VLANs, and so on. All categorized and classified data must reside in its segment with its associated access levels. Microsegmentation must be applied to endpoints and applications within the same segment to control and monitor user activity.

DO NOT REPRINT
© FORTINET

Forrester Zero Trust Extended (ZTX) Framework (Contd)

- Zero Trust—Workloads
  - Isolate and prevent unauthorized access between workloads
  - Inspect API calls between workloads
  - Protect workload file and memory to prevent tampering



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

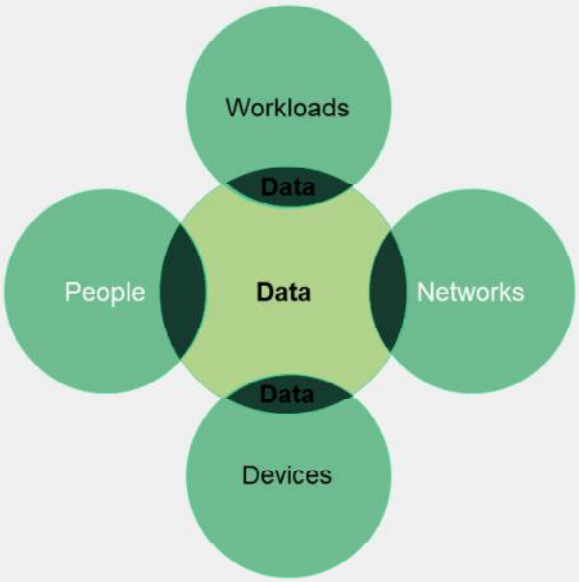
15

Workloads are front-end and back-end systems that run business and help them to win, serve, and retain customers. Just like any other area of zero trust, these connections, applications, and components must be treated as threat vectors and be protected using zero-trust controls, such as policy-based API inspection and control, container-file and active-memory protection, and guest-host firewalls. Of particular concern are workloads running in public clouds.

DO NOT REPRINT
© FORTINET

Forrester Zero Trust Extended (ZTX) Framework (Contd)

- Zero Trust—Devices
  - Discover all managed devices and headless devices
  - Detect and prevent spoofing attacks
  - Monitor users and entities to detect anomalous behavior
  - Use device security posturing



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

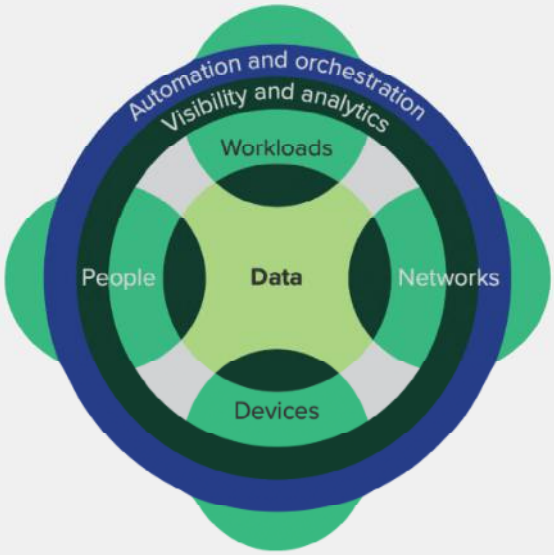
16

The fifth, and most important pillar, defines how to secure devices. This is where you gain visibility of managed and headless devices. Detect and mitigate any spoofing attacks and suspicious behavior of these devices. Finally, you should implement and continuously monitor device security posture to ensure the devices onboarded to the network are safe. For example, does the endpoint have the latest antivirus signatures, operating system updates, and so on?

DO NOT REPRINT
© FORTINET

Forrester Zero Trust Extended (ZTX) Framework (Contd)

- Automation and visibility
  - Use tools and technologies that enable security automation and orchestration (SAO) across the enterprise and cloud
  - Integrate disparate security solutions
  - Use AI for anomaly detection
  - Control configuration and allow end-to-end data visibility
  - Enforce policies consistently in both managed and unmanaged environments



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

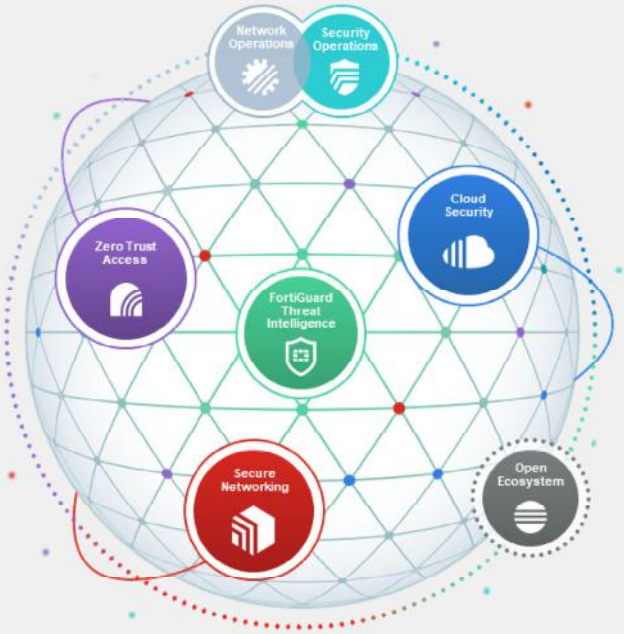
The last two defined pillars are automation and orchestration, and visibility and analytics. Organizations and security leaders need to use tools and technologies that enable security automation and orchestration (SAO) across their enterprises to shorten incident response times and integrate disparate security solutions. Orchestration extends security policies to cloud environments.

The security analyst needs to have the ability to accurately observe threats that are present and orient defenses more intelligently.

DO NOT REPRINT
© FORTINET

Fortinet Security Fabric

- Broad
  - Visibility and protection of the entire digital attack surface to better manage risk
- Integrated
  - Reduces management complexity and shares threat intelligence
- Automated
  - Consists of self-healing networks with AI-driven security for fast and efficient operations



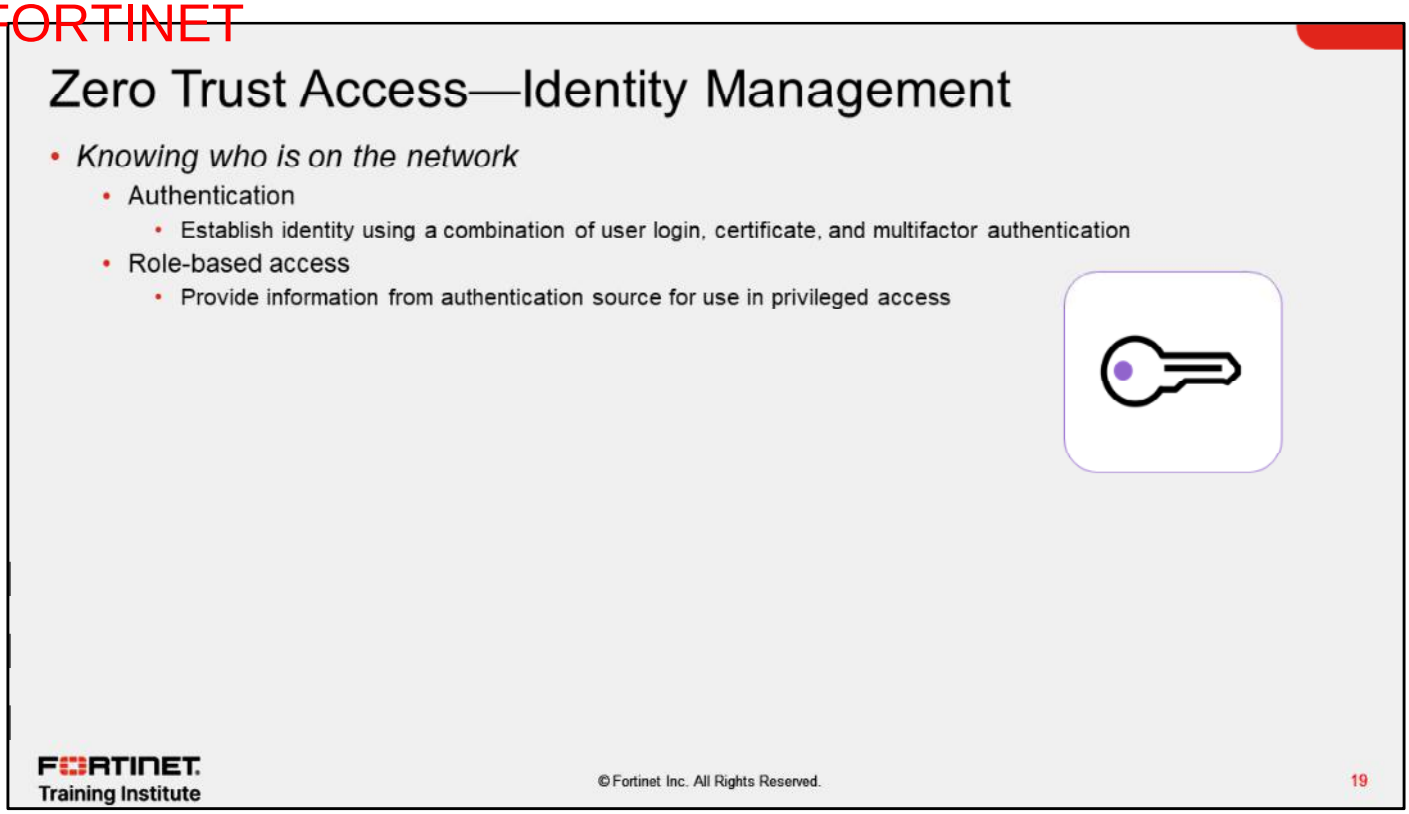
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

Fortinet takes a platform approach to cybersecurity. It uses a whole ecosystem of security products to secure the network. Within the Fortinet Security Fabric, there are several pillars, and ZTA is one of those pillars. ZTA focuses on how to onboard users and devices and enable them to access resources on the network. Fortinet Security Fabric provides the broad, integrated, and automated capabilities you need for cybersecurity.

DO NOT REPRINT
© FORTINET



Knowing who is on the network is the most common and accessible area of zero trust. From an identity management perspective, you need to know who the user is and how you will authenticate them. Are you going to be using password-only or multifactor authentication? Multifactor authentication aids a zero-trust network by increasing the number of user-specific credentials required for access. As part of zero-trust principles, role-based access can provide the minimum access necessary to perform the user's jobs.

DO NOT REPRINT
© FORTINET

Zero Trust Access—Device Profiling

- *Knowing what is on the network*
  - Device discovery and control
    - Knowing and controlling everything that is on the network
  - User access control
    - Policy-based user access controls that include who, where, when, and how metrics
    - BYOD and guest access
    - Onboarding guests and personal devices in a consistent, automated, and secure manner

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Knowing what is on the network is the most challenging area of zero trust. Organizations must discover what devices are onboarded on their network. You must not only discover the devices but also control their level of access, based on their role, location, and so on.

DO NOT REPRINT
© FORTINET

Zero Trust Access—Endpoint Access and Control

- On-net, off-net protection
  - Endpoint visibility
    - Security posture assessment
    - Endpoint telemetry
  - Endpoint protection
    - Vulnerability scanning and patching
    - Web filtering, AV, and so on
    - Dynamic grouping
    - Secure remote access
    - Dynamic access control VPN
    - SSO

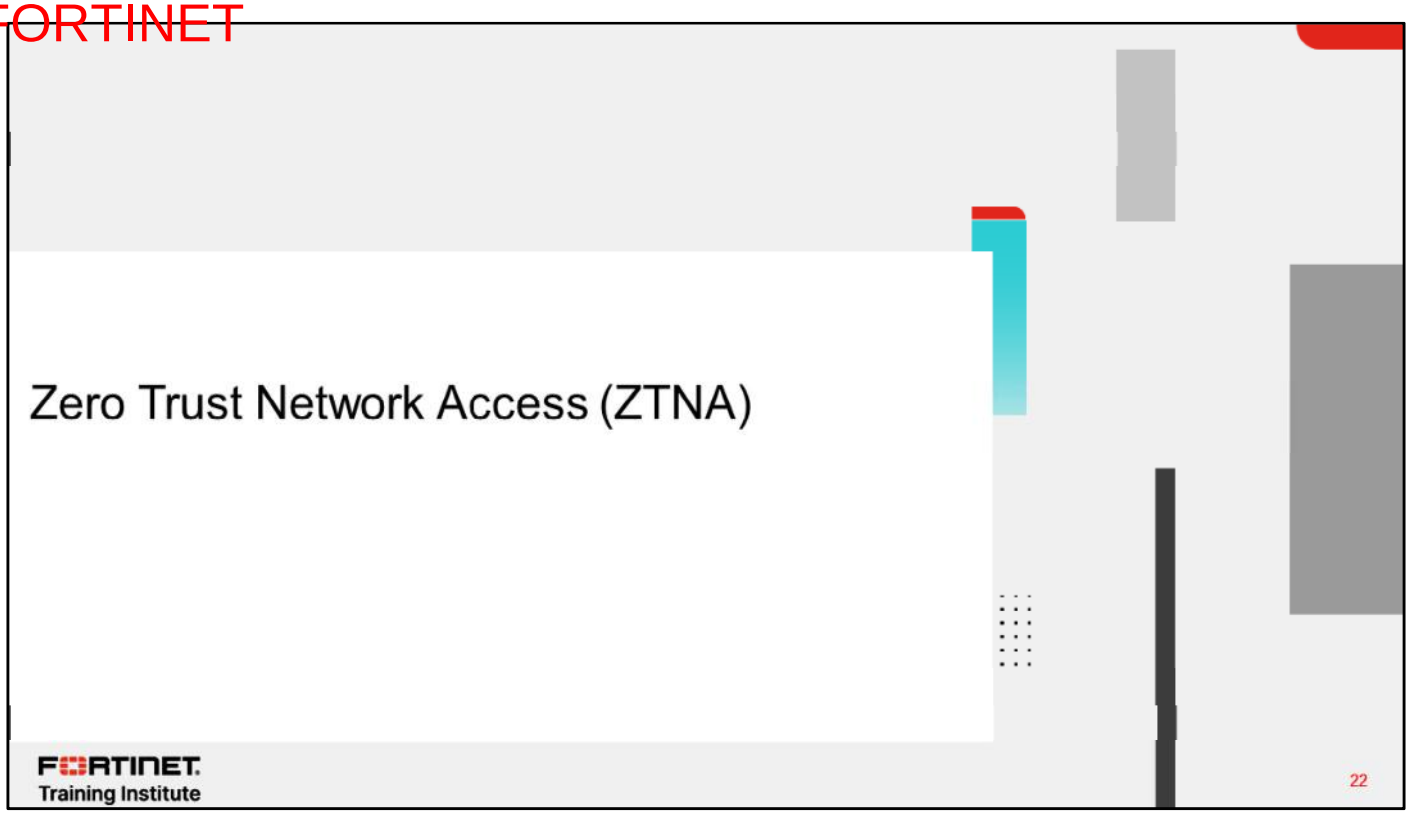
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

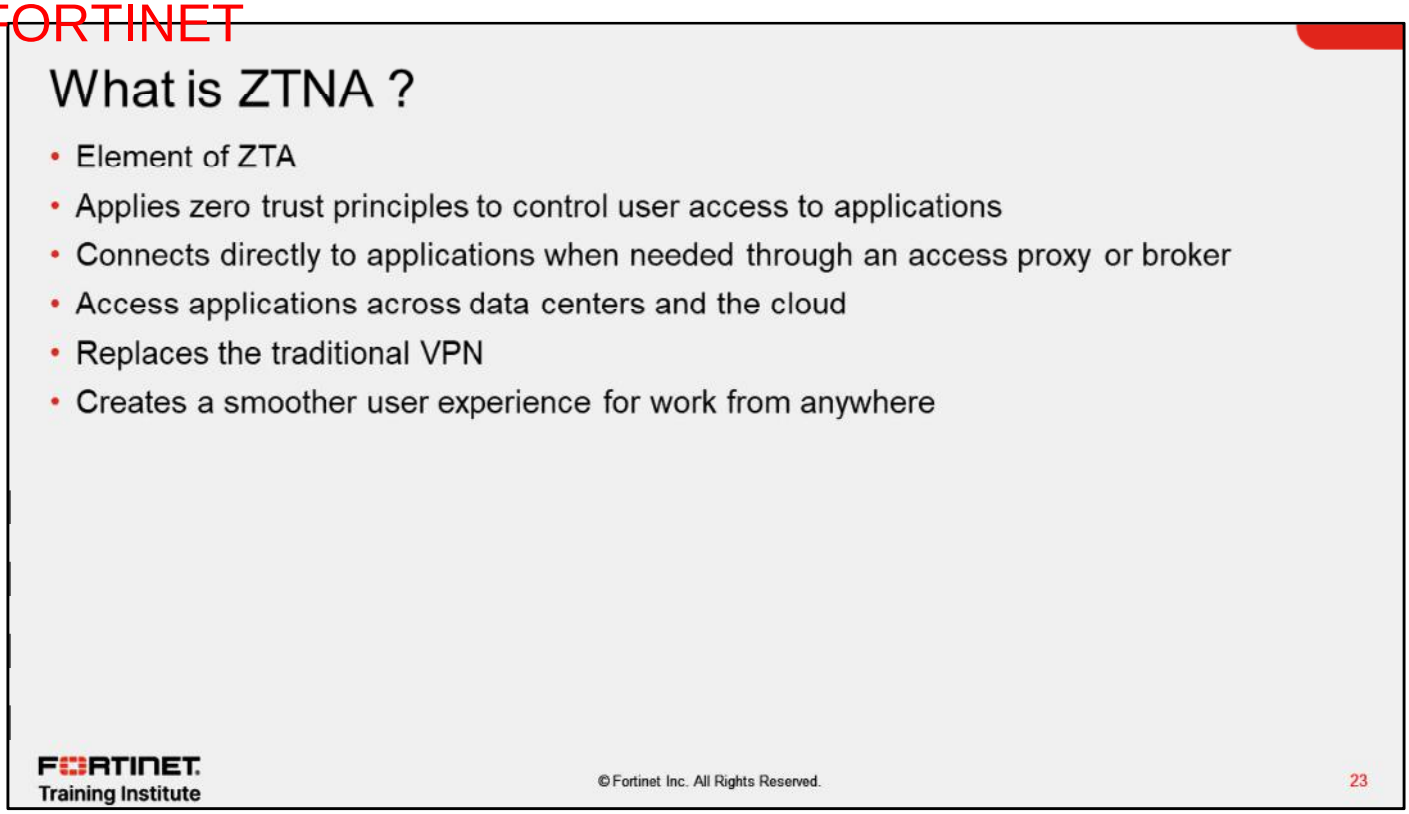
Endpoint access and control is an important area of zero trust for on-network devices, as well as for the security and ongoing control of off-network devices. Endpoint agents like FortiClient can be used to ensure endpoints are patched properly, protected from malware, have had their security posture assessed and so on. Secure access to a corporate network can be provided using a VPN with single sign-on (SSO) capabilities.

DO NOT REPRINT
© FORTINET



In this section, you will learn about ZTNA and the differences between ZTNA and VPN.

DO NOT REPRINT
© FORTINET

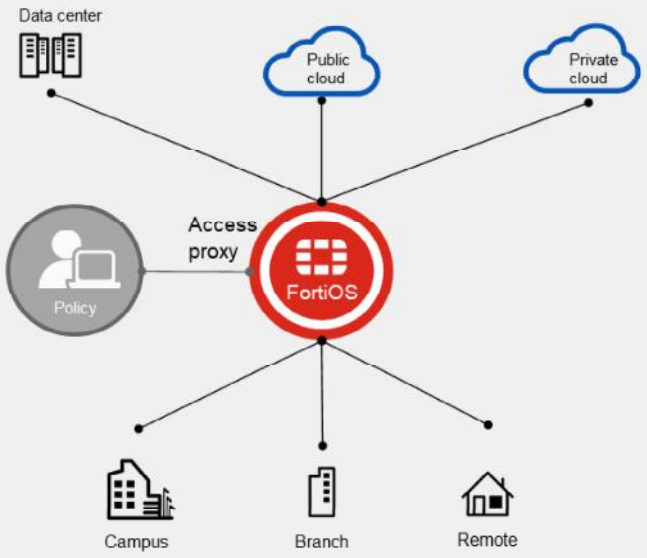


ZTNA, is an element of ZTA. ZTNA allows you to apply zero-trust principles to control which users will access what application over the network. ZTNA eliminates the need for a user to connect to a VPN before accessing an application across data centers or the cloud. Applications are accessed when needed, directly through an access proxy or broker. With ZTNA, a user can more seamlessly work from the office or remotely, which creates a smoother user experience.

DO NOT REPRINT
© FORTINET

ZTNA Flow

1. User wants to access an application and connects to an access proxy
2. Access proxy creates secure tunnel
3. Access proxy authenticates the user, and identifies the device and the device posture
4. Access proxy verifies if the user has the right access level to access the application
5. If the check is successful, the user can access the application
6. Access proxy repeats these steps each time the user tries to access the application (per session)



FORTINET Training Institute

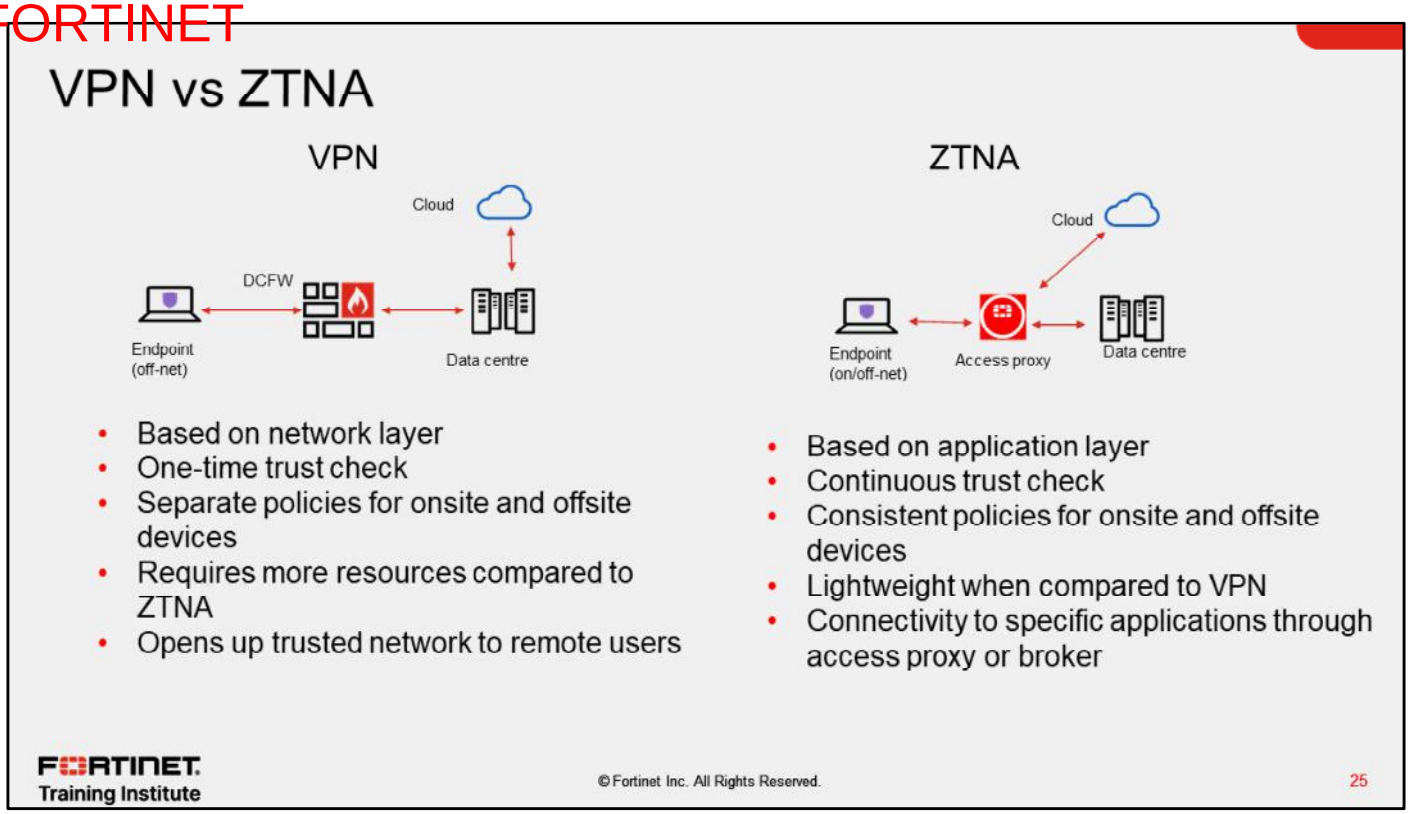
© Fortinet Inc. All Rights Reserved.

24

ZTNA connects users to applications, regardless of the user's location or application. Connection through ZTNA functions as follows:

1. The user wants to access an application and connects to an access proxy.
2. The access proxy creates a secure tunnel automatically between the user and the application.
3. The access proxy authenticates the user and identifies the device and the device posture.
4. After successfully authenticating and meeting the device posture requirements, the access proxy verifies the application access level of the user.
5. The access proxy verifies the access level and grants access to the user.
6. Whenever a new session is established, the access proxy repeats these steps to verify that the user identity, access levels, and device posture have not changed.

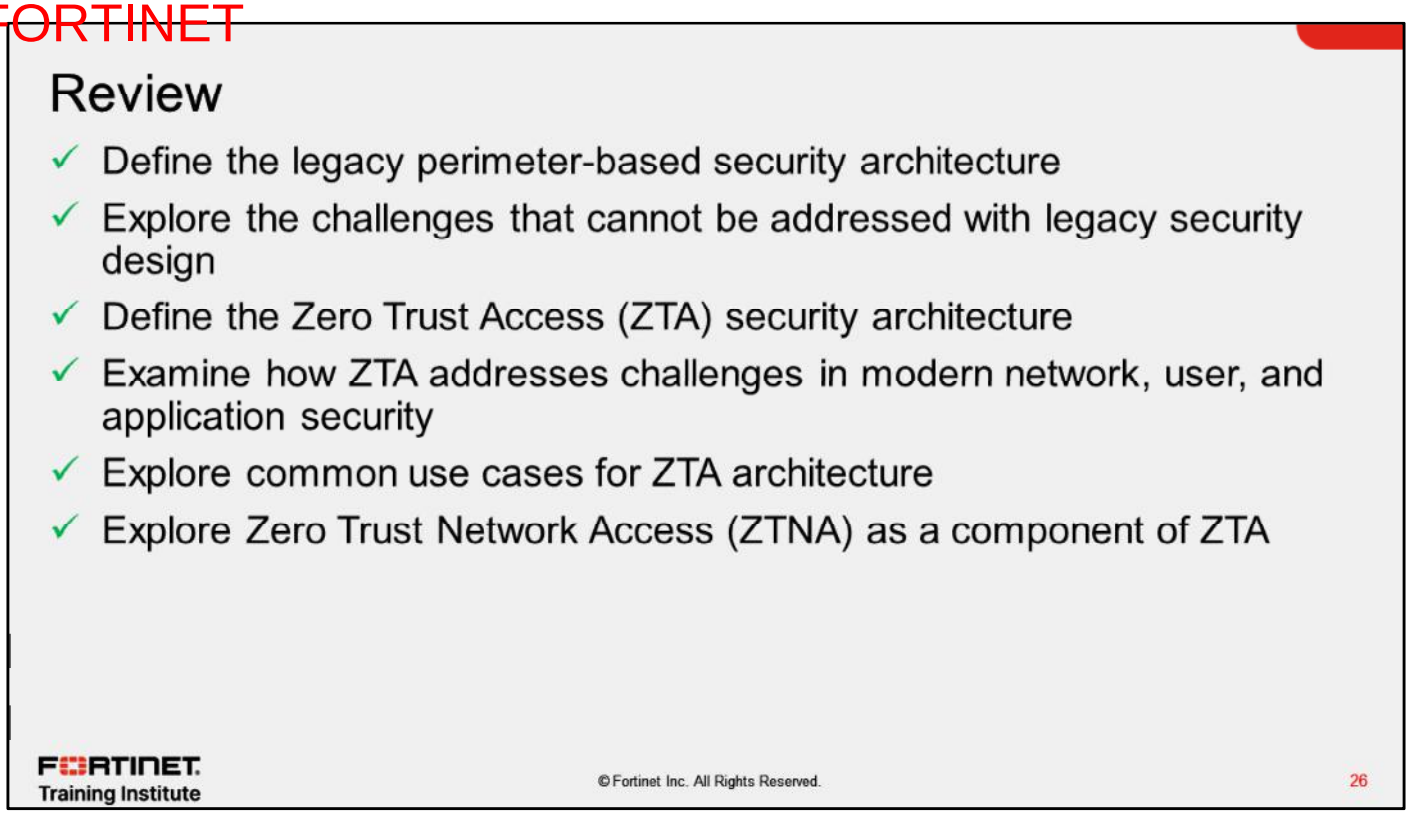
DO NOT REPRINT
© FORTINET



VPNs work at the network layer. When a user connects, a one-time trust check is applied, and then the user has access to network subnets or IP addresses. VPNS are intended to extend corporate networks to remote users, where all the resources and applications used to be on-premises. Now that most applications are on the public cloud, it causes too much overhead on VPN gateways. Trusted networks must be extended to access resources on the public cloud, and too much traffic will traverse the gateway to reach the cloud-based resources.

ZTNA changes the underlying VPN model completely. A user can connect directly to an application through an access proxy or broker on an as-needed basis. ZTNA is designed for users on-network and off-network, accessing applications in the data center or on the cloud. ZTNA follows the zero-trust principle of continuously monitoring user authentication, access levels, and device postures. ZTNA is lightweight and less resource intensive than VPN.

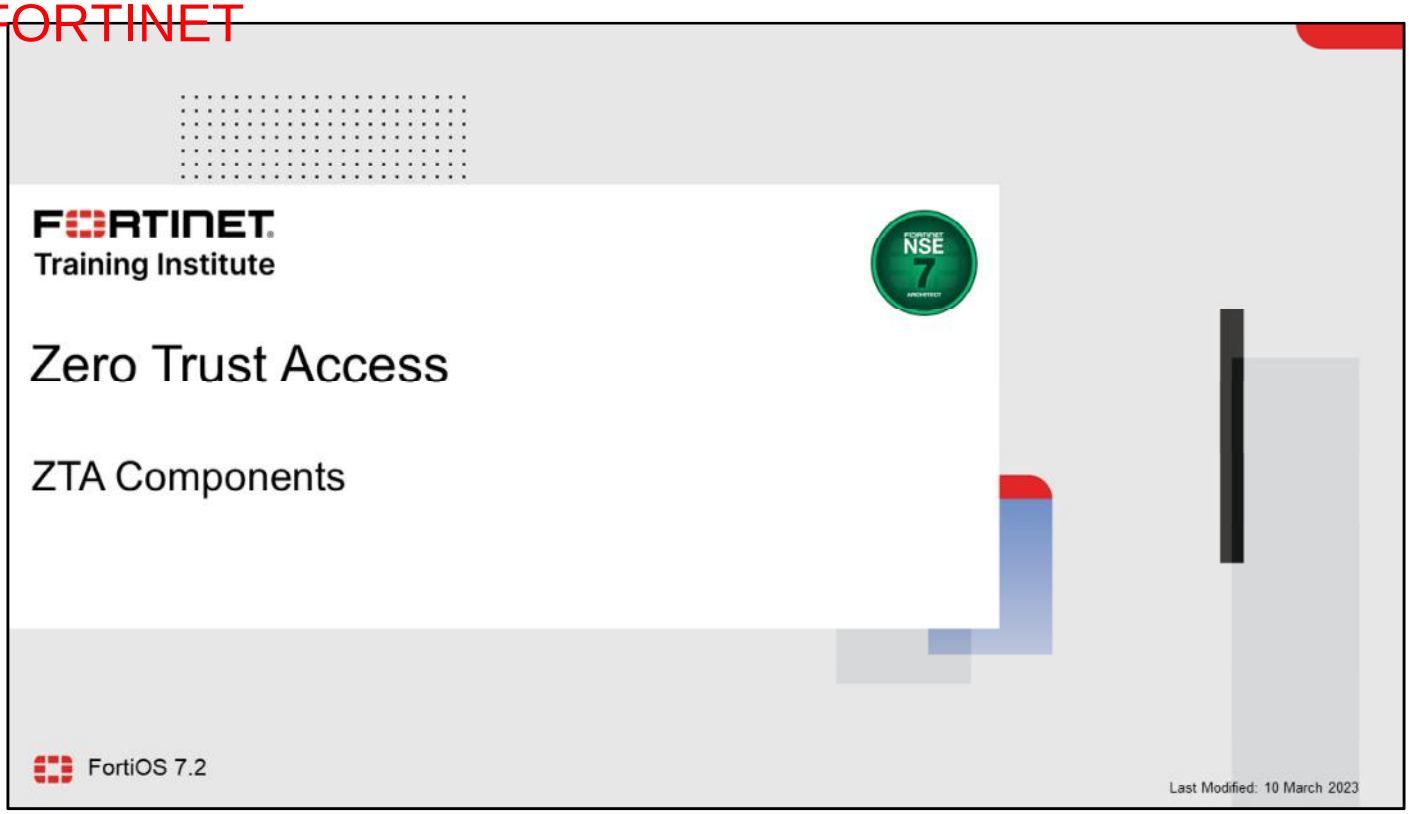
DO NOT REPRINT
© FORTINET



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

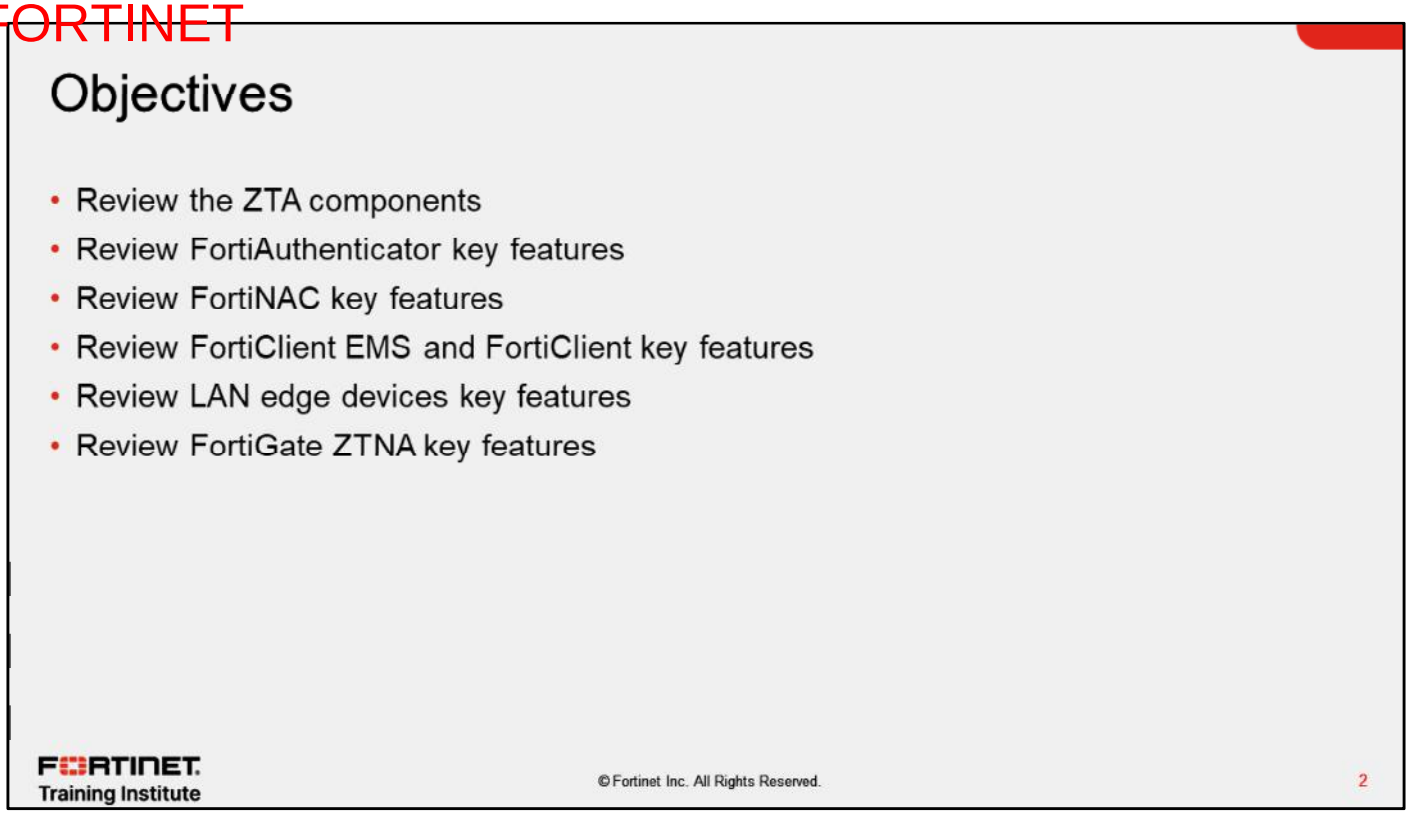
By mastering the objectives covered in this lesson, you learned ZTA security design principles the differences between ZTNA and ZTA.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the zero trust access (ZTA) components.

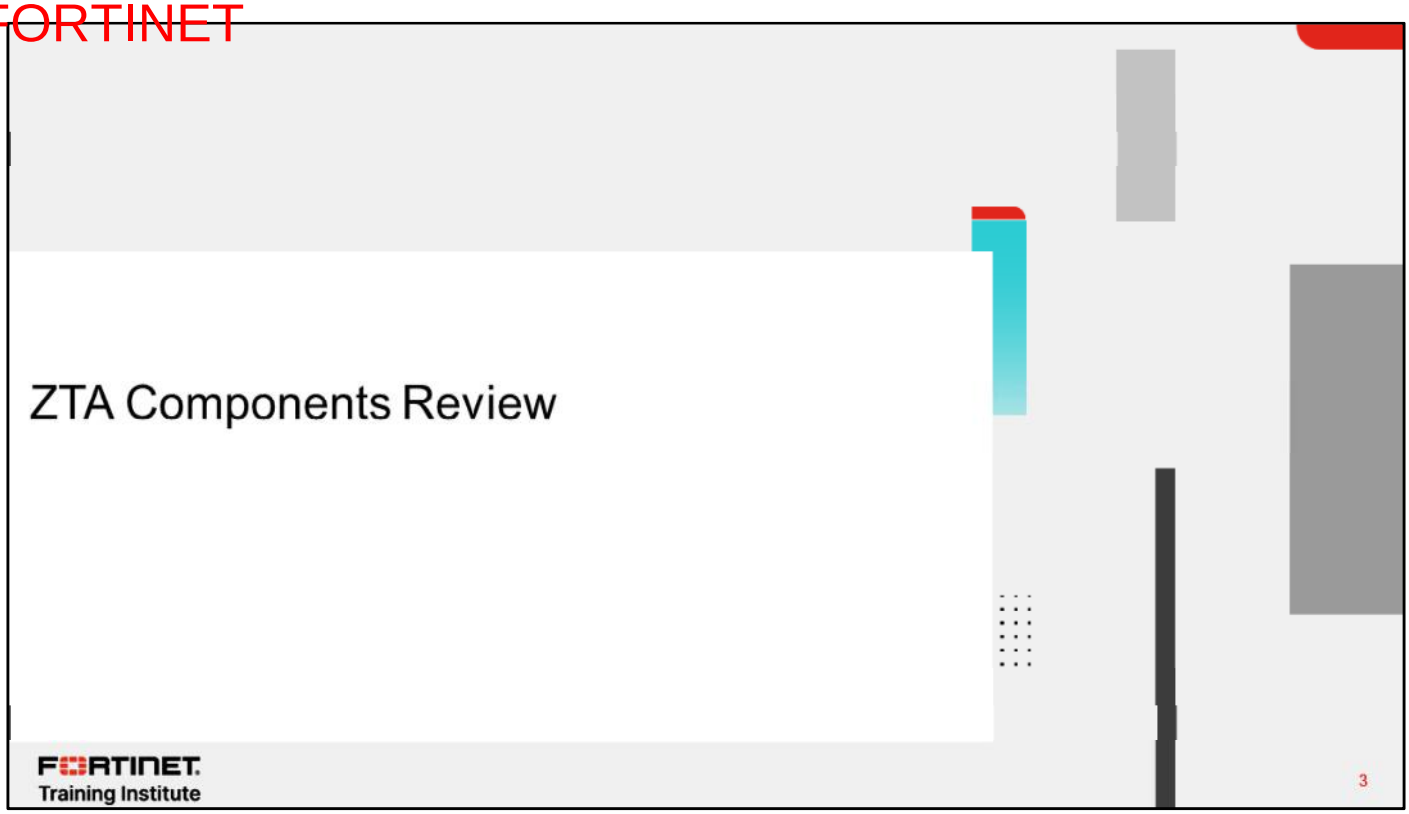
DO NOT REPRINT
© FORTINET



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

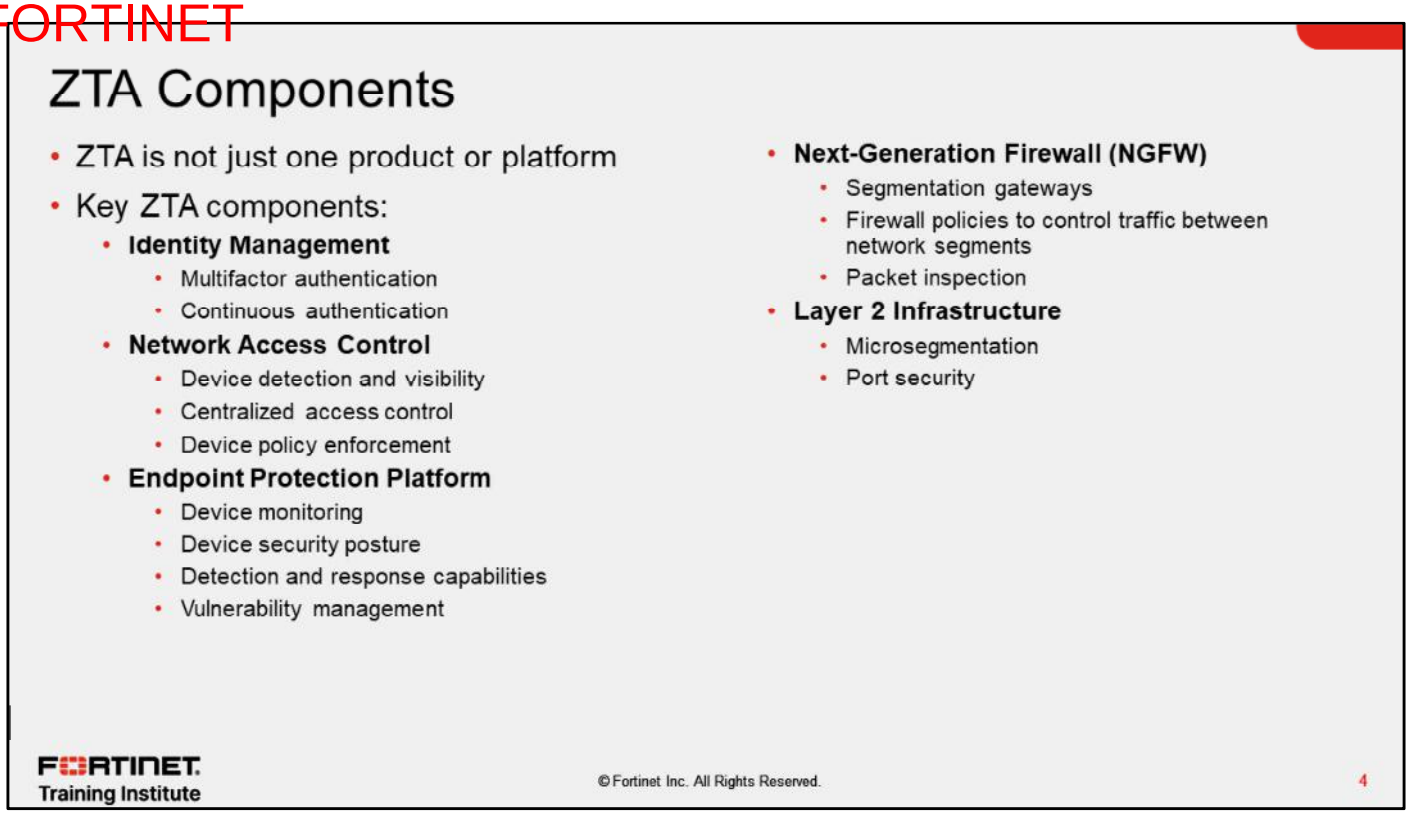
By demonstrating a competent understanding of ZTA architecture, you will be able to identify the different ZTA components.

DO NOT REPRINT
© FORTINET



In this section, you will review some of the ZTA components.

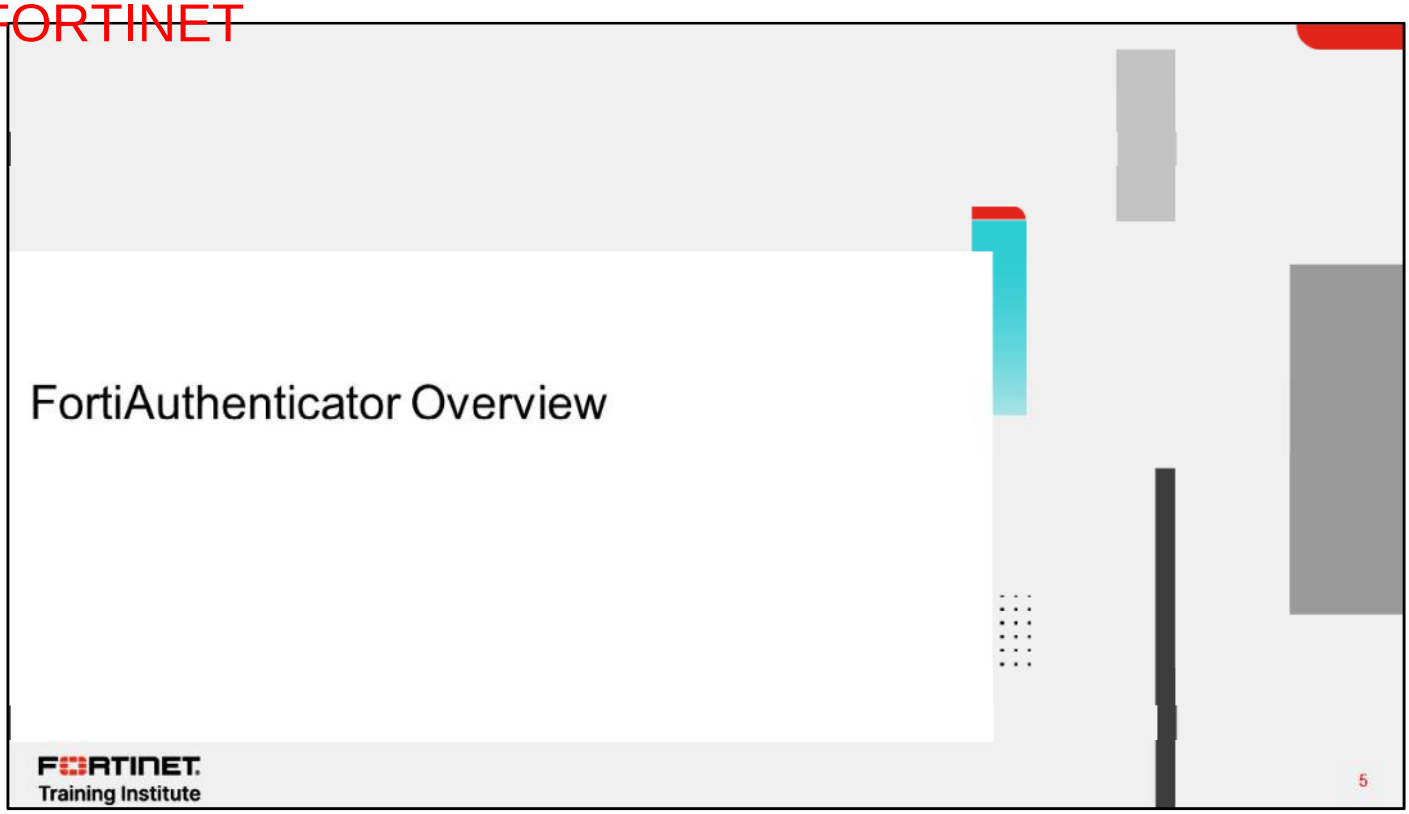
DO NOT REPRINT
© FORTINET



ZTA is not just one product or platform; it is a solution to control access to assets and applications by users and devices. Some of the key ZTA components include:

- Identity management: The zero-trust principle of multifactor and continuous authentication is applied.
- Network access control: Device visibility and centralized access control are implemented.
- Endpoint protection platform: Device security posture and endpoint vulnerability management are implemented.
- Next-generation firewall (NGFW): Network traffic is segmented and inspected. NGFW also acts as segmentation gateway.
- Layer 2 infrastructure: Securing devices on Layer 2 using port security, MAC filtering, and microsegmentation.

DO NOT REPRINT
© FORTINET



In this section, you will get an overview of FortiAuthenticator key authentication features.

DO NOT REPRINT
© FORTINET

FortiAuthenticator

- Identity and access management solution
- Provides user identity services to Fortinet Security Fabric and third-party devices
- Centralized management and storage of user identity information
- Some of the key features include:
  - Authentication-Radius, LDAP, SAML etc.
  - Two-factor authentication
  - 802.1x support for wired and wireless networks
  - Certificate management
  - Fortinet single sign on (FSSO)
  - Integration with third-party RADIUS, LDAP, and SAML authentication systems

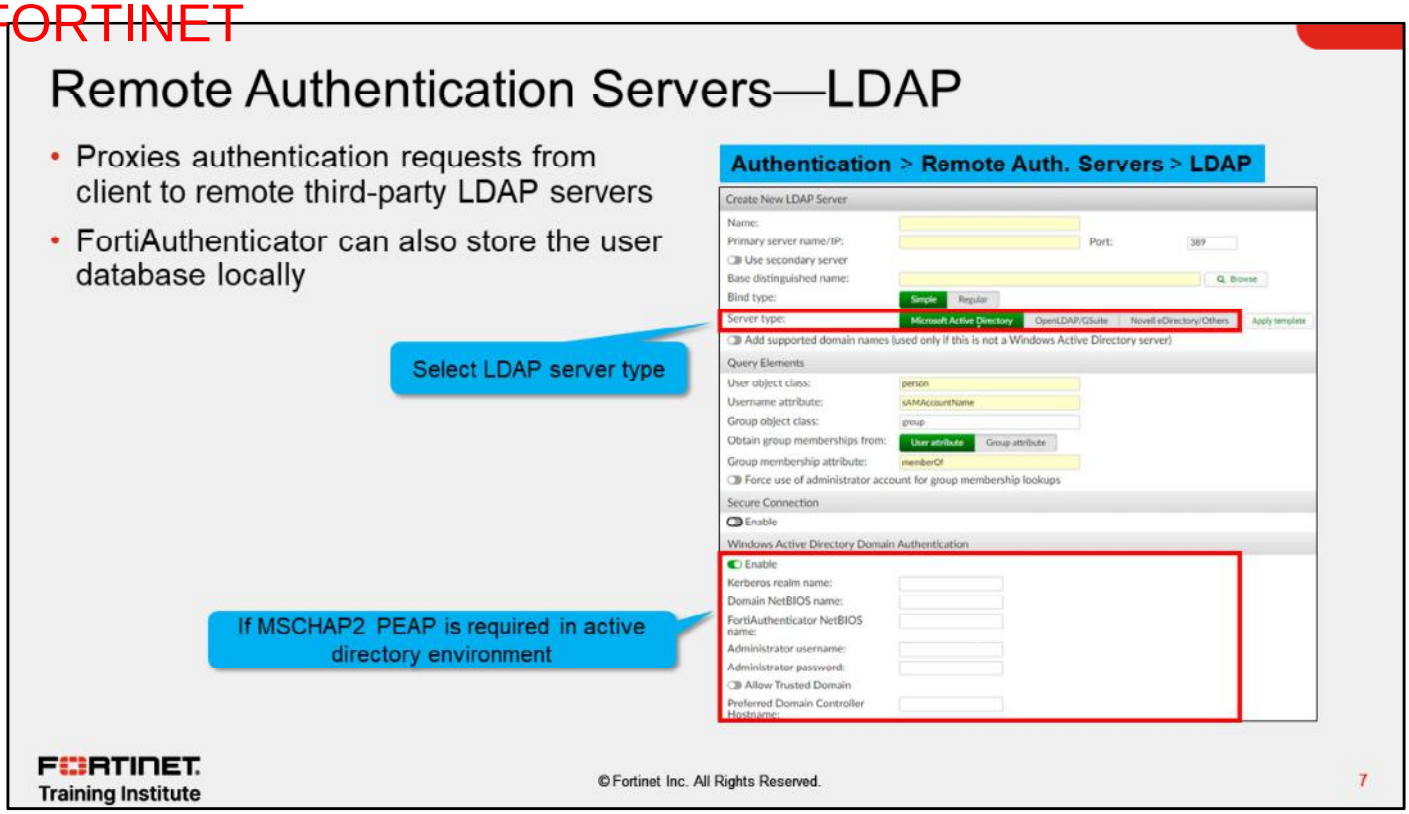
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

FortiAuthenticator is a centralized identity and access management solution. It provides user identity services to the Fortinet Security Fabric and third-party devices. The key authentication features on FortiAuthenticator include RADIUS, LDAP, and 802.1X wireless authentication, certificate management, Security Assertion Markup Language (SAML), and FSSO. FortiAuthenticator is compatible with FortiToken to provide two-factor authentication when using multiple FortiGate and third-party devices. FortiAuthenticator and FortiToken together deliver cost-effective, scalable, secure authentication to your entire network infrastructure.

DO NOT REPRINT
© FORTINET



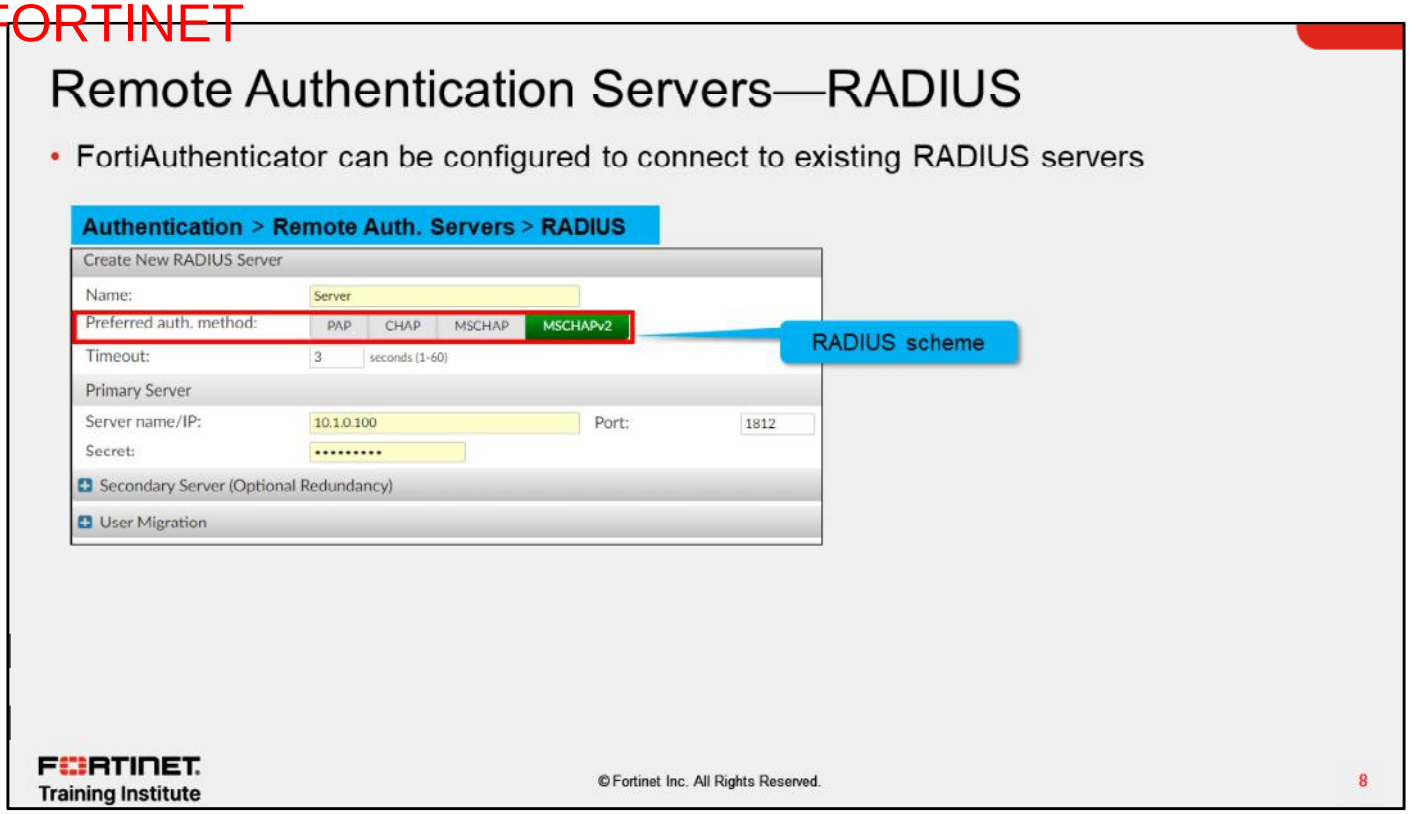
FortiAuthenticator can store the user database locally. It can also proxy authentication requests from a client to a back-end authentication server.

You must configure the following settings: **Name**, **Primary server name/IP**, **Base distinguished name**, **Bind type**, and administrator **Username** and **Password** for regular bind type. Note that the **Base distinguished name** sets the root node where LDAP starts searching for user accounts.

There are predefined LDAP templates you can select in the **Server type** field. They include default attribute settings for well-known LDAP servers, such as **Microsoft Active Directory**, **OpenLDAP**, and **Novell eDirectory**.

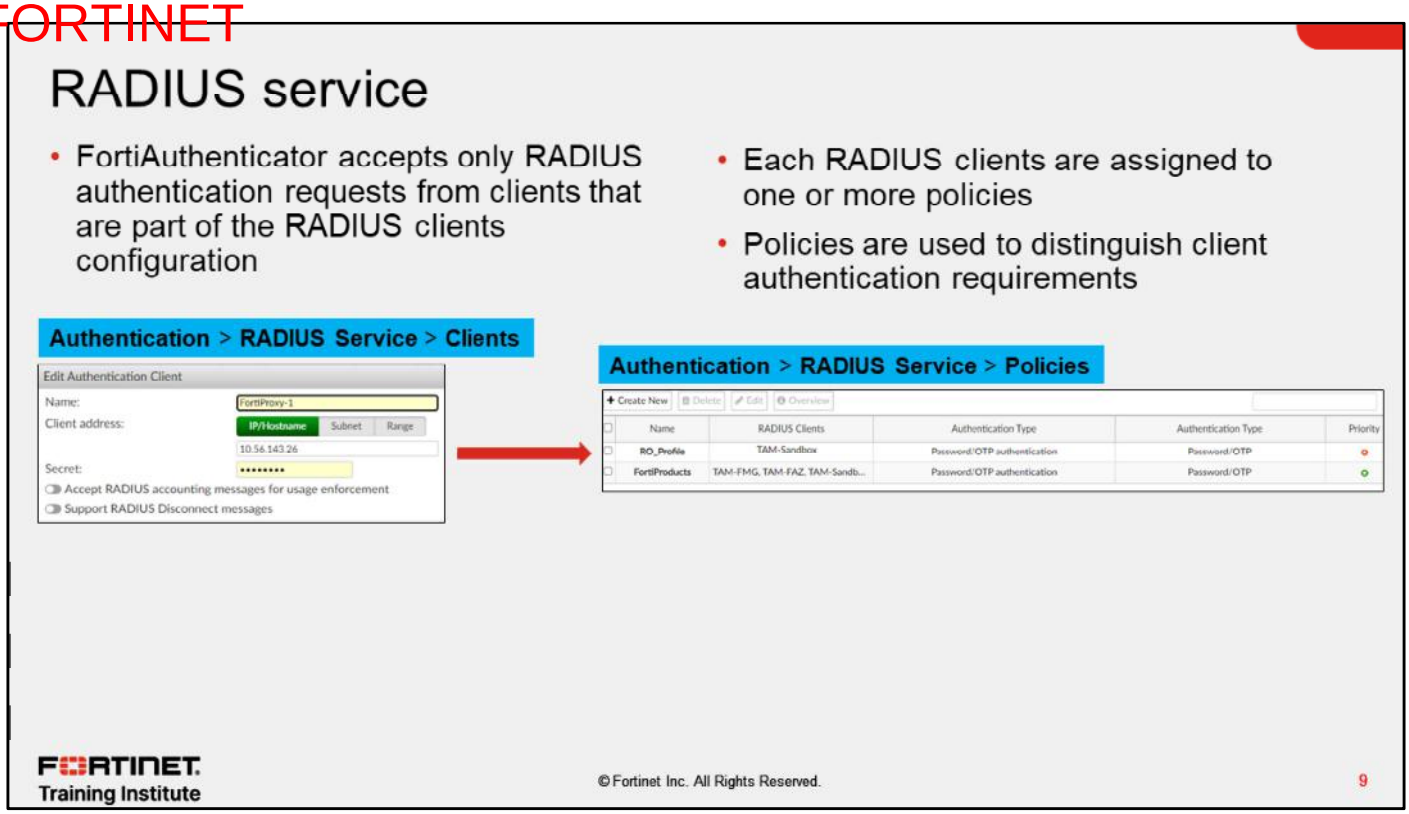
If you want FortiAuthenticator to relay CHAP, MSCHAP, and MSCHAPv2 authentication to a Windows AD server, you must enable **Windows Active Directory Domain Authentication** and enter the credentials for a Windows administrator. FortiAuthenticator logs in to the domain as a trusted device, allowing FortiAuthenticator to proxy CHAP, MSCHAP, and MSCHAP2 authentication, using NTLM.

DO NOT REPRINT
© FORTINET



The slide shows is an example of the configuration required for FortiAuthenticator to proxy authentication requests to a remote RADIUS server.

DO NOT REPRINT
© FORTINET

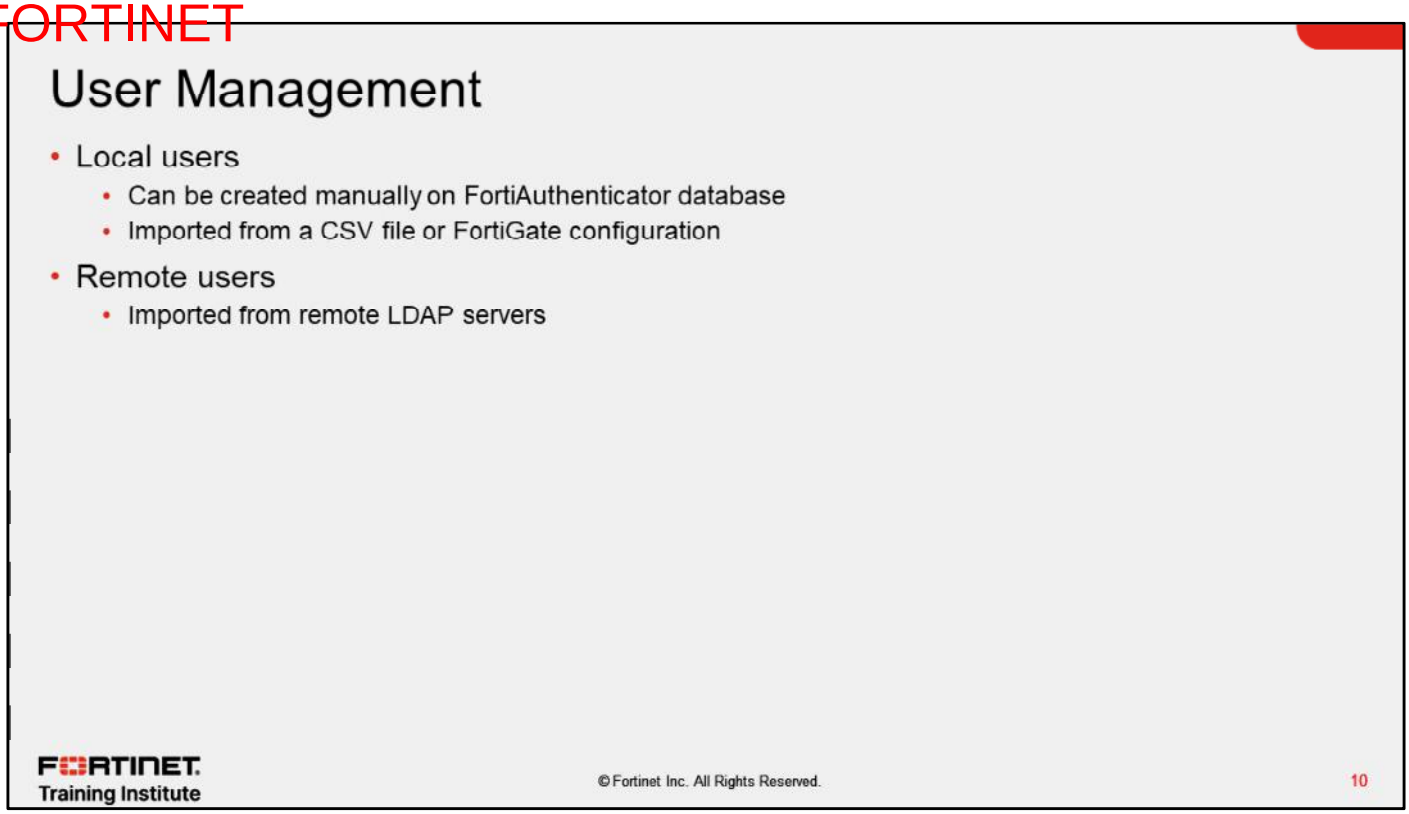


FortiAuthenticator accepts RADIUS authentication requests from only approved RADIUS clients. After you configure remote authentication servers or a local user database, you must allow FortiGate to make authentication requests to FortiAuthenticator. This is done under RADIUS clients on FortiAuthenticator.

After you configure a RADIUS client, you must assign it to one or more RADIUS policies. A RADIUS policy contains the authentication settings that FortiAuthenticator follows when processing authentication requests sent by your RADIUS client.

When FortiAuthenticator receives a RADIUS authentication request, it looks at the request attributes and then finds a matching policy using a top-down approach. If there is no matching policy, FortiAuthenticator rejects the RADIUS authentication request.

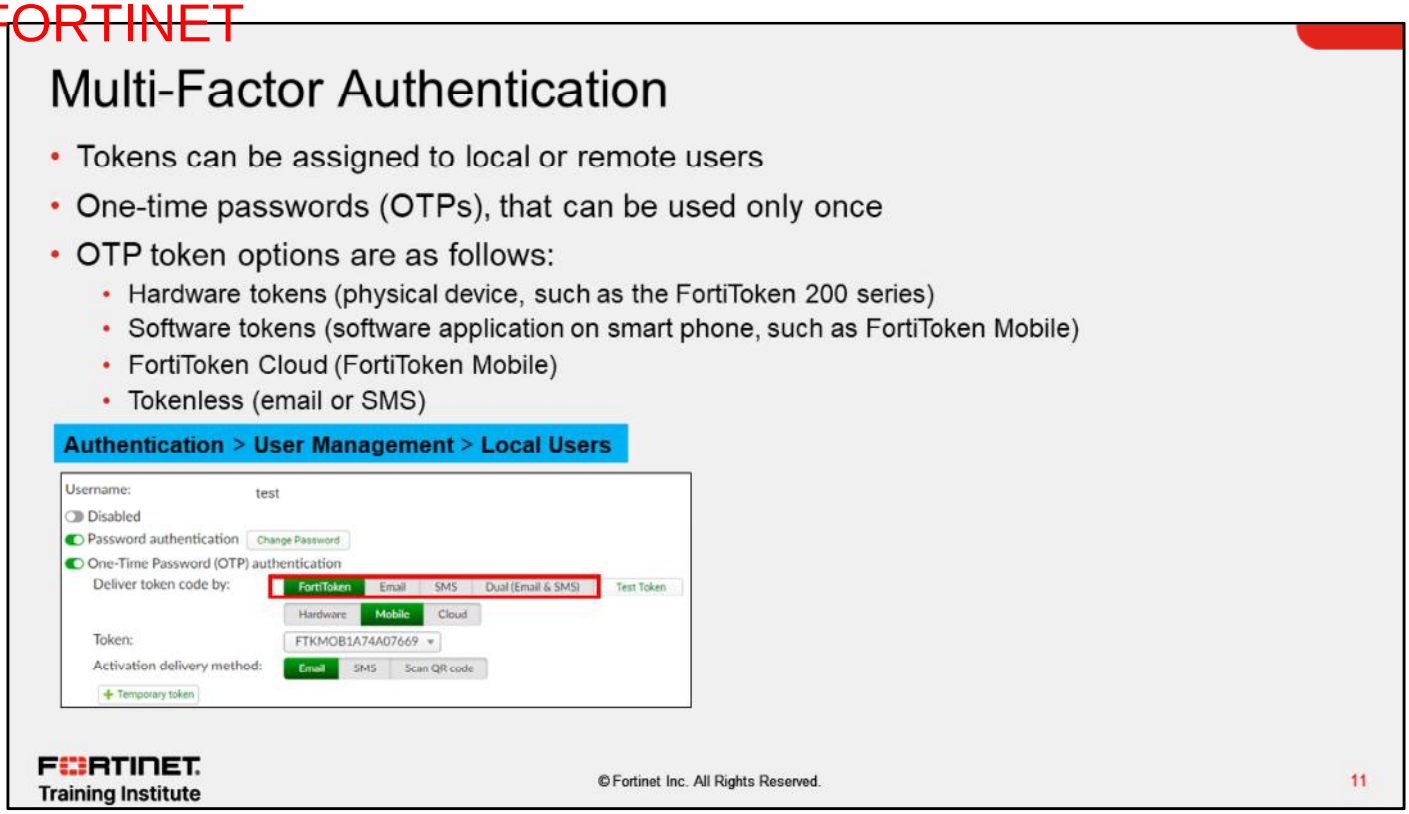
DO NOT REPRINT
© FORTINET



There are two ways you can add users to FortiAuthenticator:

- Local users can be created manually on the FortiAuthenticator database or imported from a CSV file or FortiGate configuration file.
- Remote users can be imported from remote LDAP servers.

DO NOT REPRINT
© FORTINET



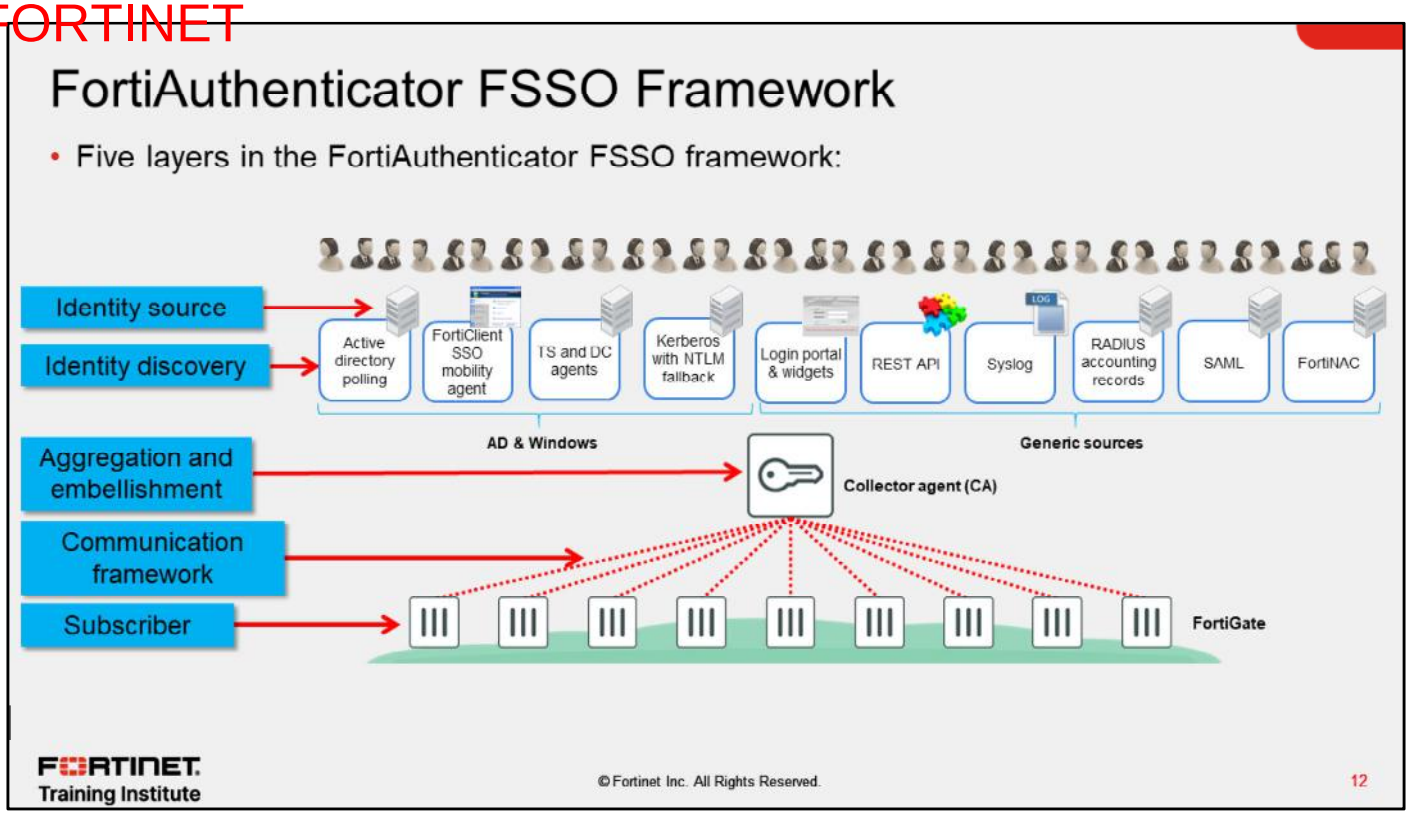
Typically, an OTP token is not used as a standalone solution, but as an additional authentication mechanism on top of a user name and static password.

OTP tokens generate passwords that can be used only once. They are more secure than static passwords because they are not vulnerable to replay attacks. For example, even if an attacker obtains an OTP, the password invalidates after a short interval (usually 60 seconds).

Because memorizing a one-time password is practically impossible, you need something that can generate them for you. There are three main ways of acquiring one-time passwords:

- Hardware tokens, which are physical devices, such as the FortiToken 200 series
- Software tokens, which are software applications on a smart phone, such as FortiToken Mobile
- FortiToken Cloud, which uses cloud-based token validation using FortiToken Mobile
- Tokenless, which use email or SMS

DO NOT REPRINT
© FORTINET



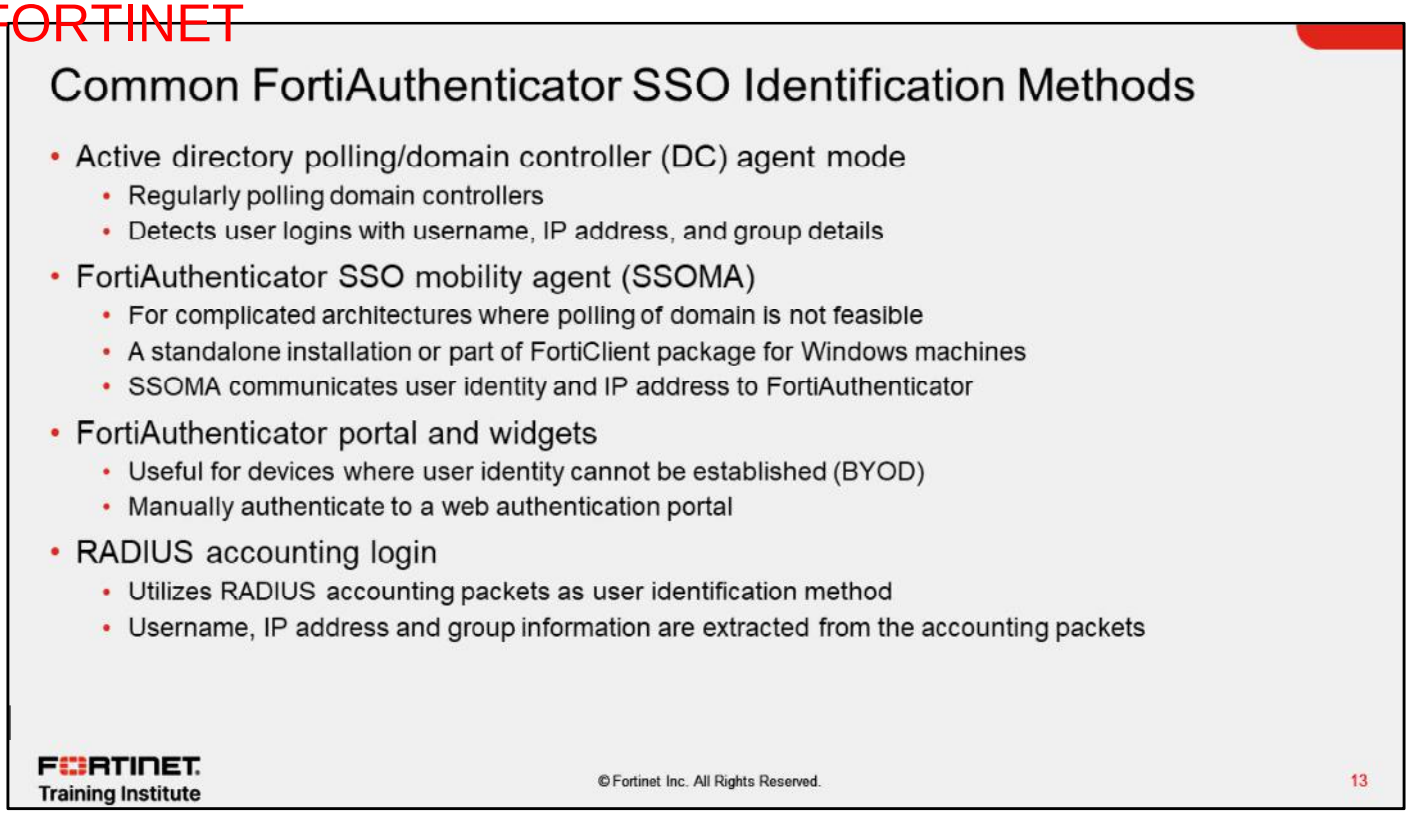
This slide shows the multitude of ways FortiAuthenticator can identify users over the FSSO framework.

The FortiAuthenticator FSSO framework has five layers:

- The first layer is the identity source: the method by which the user identity is ascertained.
- The second layer is the identity discovery: the methods by which the user identity and their location (IP) are discovered. You will learn each of these methods in the *FSSO User Identity Discovery Methods* section.
- The third layer is aggregation and embellishment: the collection of user identity and addition of any missing information, such as group, which is gathered from the external LDAP/AD.
- The fourth layer is the communication framework: the method by which the authentication information is communicated with the subscribing device.
- The fifth layer is the subscribing device: for example, FortiGate. The user information is forwarded to the subscribing device where the information can be used in firewall policies.

Note that you can also combine multiple methods. For example, Single Sign-On Mobility Agent may be used for Microsoft Windows domain PCs but fall back to the login portal with embedded widgets for non-Windows systems or unauthenticated PCs.

DO NOT REPRINT
© FORTINET



Some of the standard FortiAuthenticator SSO identification methods include:

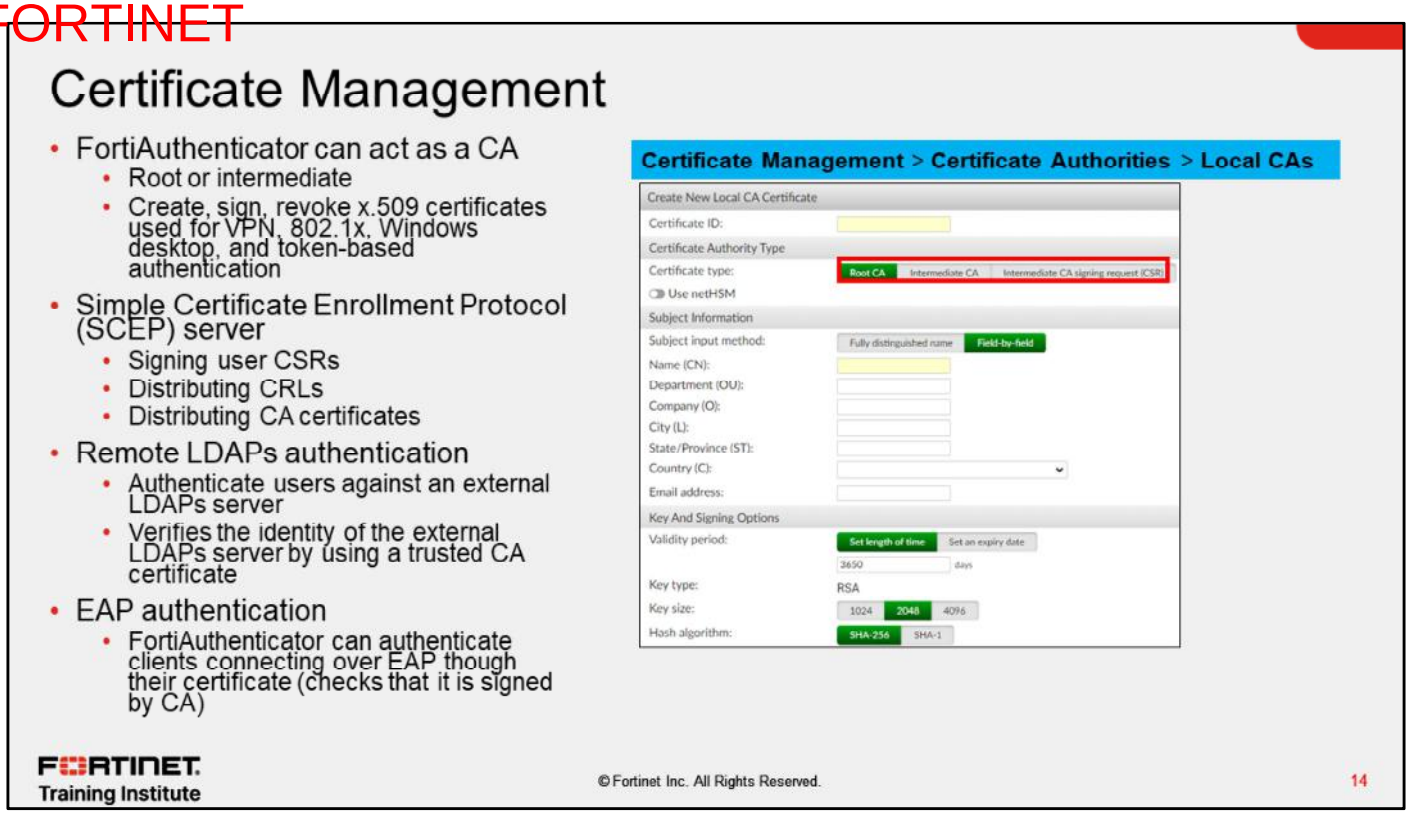
- Active directory polling/domain controller (DC) agent mode: User authentication into an active directory is detected by regularly polling domain controllers. When a user login is detected, the username, IP, and group details are entered into the FortiAuthenticator user identity management database and, according to the local policy, can be shared with multiple FortiGate devices.

- FortiAuthenticator SSO mobility agent (SSOMA): For complicated distributed domain architectures where the polling of domain controllers is not feasible or desired, an alternative is the FortiAuthenticator SSO client. Distributed as part of FortiClient or as a standalone installation for Windows PCs.

- FortiAuthenticator portal and widgets: For systems that do not support AD polling or where a client is not feasible, FortiAuthenticator provides an explicit authentication portal. This portal allows the users to authenticate to the FortiAuthenticator manually and subsequently into the network.

- RADIUS accounting login: RADIUS accounting can be used as a user identification method. This information triggers user login and provides IP and group information, removing the need for a second tier of authentication.

DO NOT REPRINT
© FORTINET



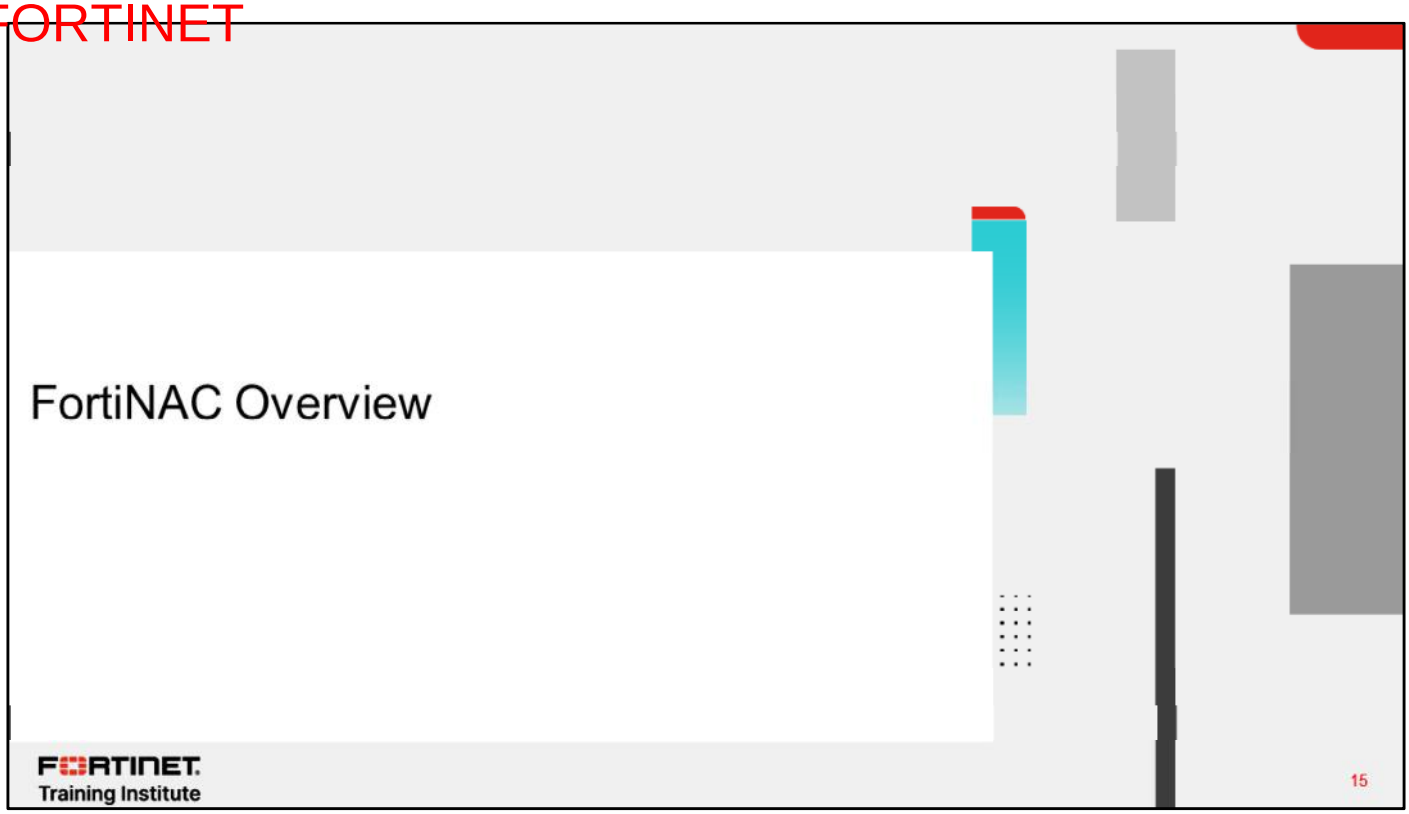
FortiAuthenticator can act as a self-signed or local CA for the creation, signing, and revoking of X.509 certificates. These certificates can be used for VPN authentication, 802.1X authentication, Windows Desktop authentication, and token-based authentication, to name a few.

FortiAuthenticator can also act as a SCEP server for:
- Signing user CSRs
- Distributing CRLs
- Distributing CA certificates

Acting as an LDAP client, FortiAuthenticator can authenticate users against an external LDAP server. It verifies the identity of the external LDAP server by using a trusted CA certificate.

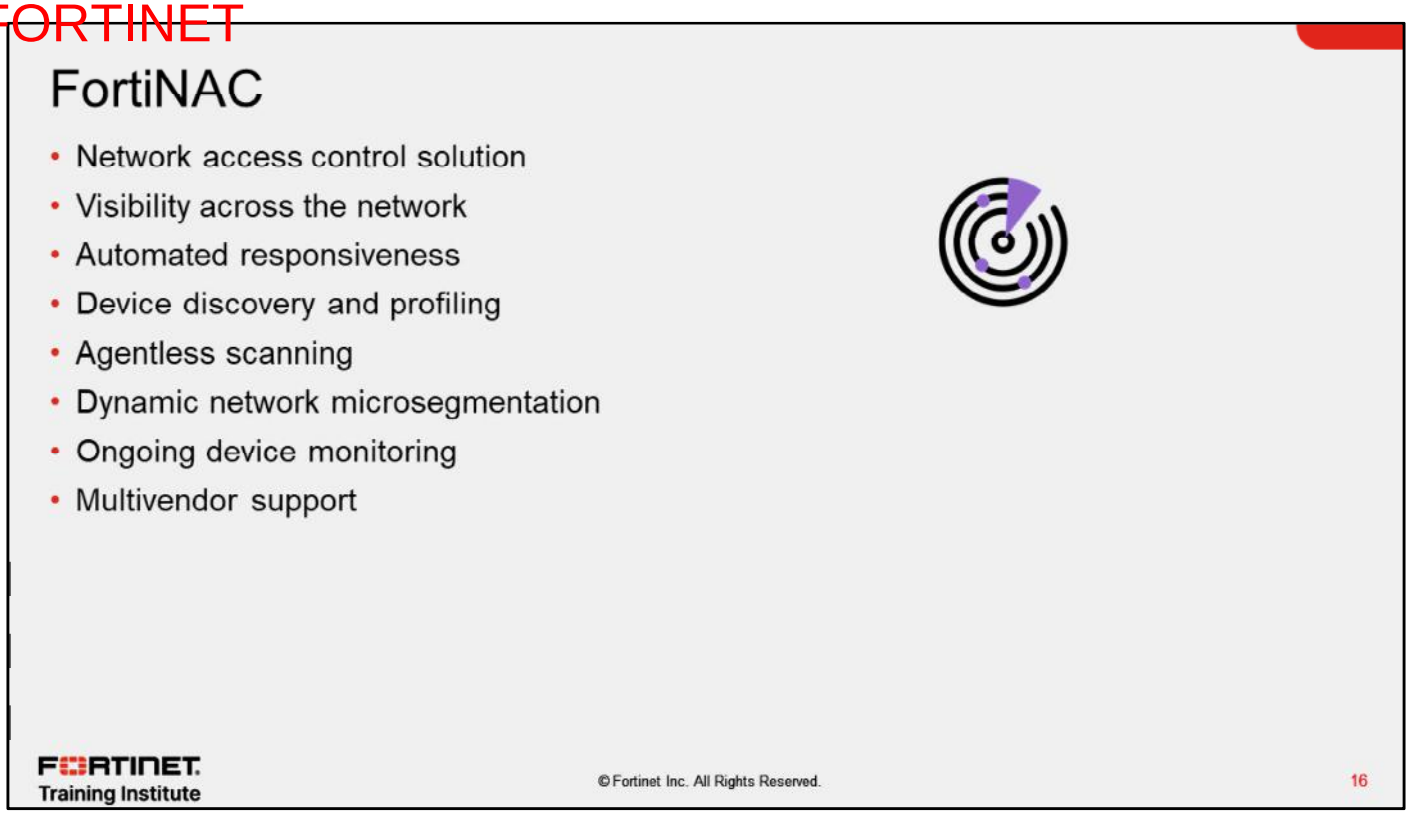
Extensible Authentication Protocol (EAP) is a type of authentication framework often used in wireless networks and point-to-point connections. In this scenario, if a client is attempting to authenticate over EAP, FortiAuthenticator can check that the client's certificate is signed by one of the configured (and authorized) CA certificates. The client certificate must also match one of the user certificates.

DO NOT REPRINT
© FORTINET



In this section, you will have an overview of FortiNAC and its key features.

DO NOT REPRINT
© FORTINET

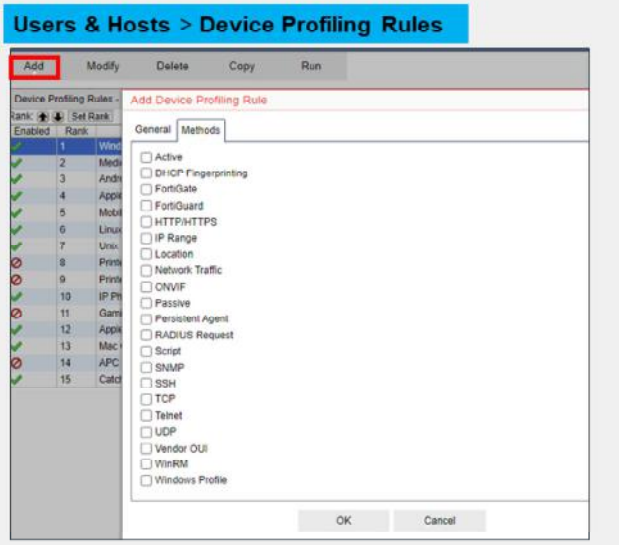


FortiNAC is a network access control solution that can be integrated with the Fortinet security fabric to enhance visibility, control, and automated response for everything that connects to the network. FortiNAC scans the network to detect and classify devices through agent or agentless to enforce dynamic network access control and segmentation.

DO NOT REPRINT
© FORTINET

Device Visibility

- Complete network visibility
- Network scanning with 21 different profiling techniques
- Device profiling based on observed characteristics and responses
- Agent and agentless support



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

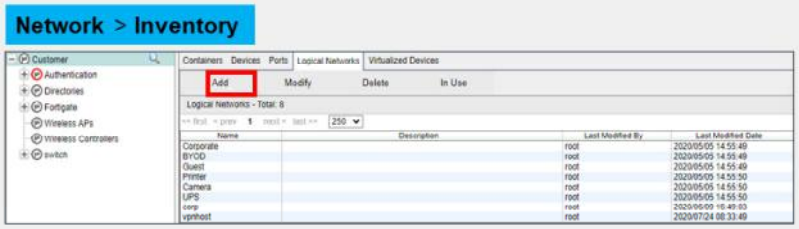
17

FortiNAC scans your network to discover every user, application, and device. With up to twenty one different techniques, FortiNAC can then profile each element based on observed characteristics and responses. Scanning can be done actively or passively and can utilize permanent agents, dissolvable agents, or no agents. Additionally, FortiNAC can assess a device to see if it matches approved profiles, noting the need for software updates to patch vulnerabilities.

DO NOT REPRINT
© FORTINET

Dynamic Network Control

- FortiNAC uses dynamic role-based network access control to create logical network segments
- FortiNAC checks device compliance and limits access to corporate resources accordingly
- FortiNAC ensures device integrity



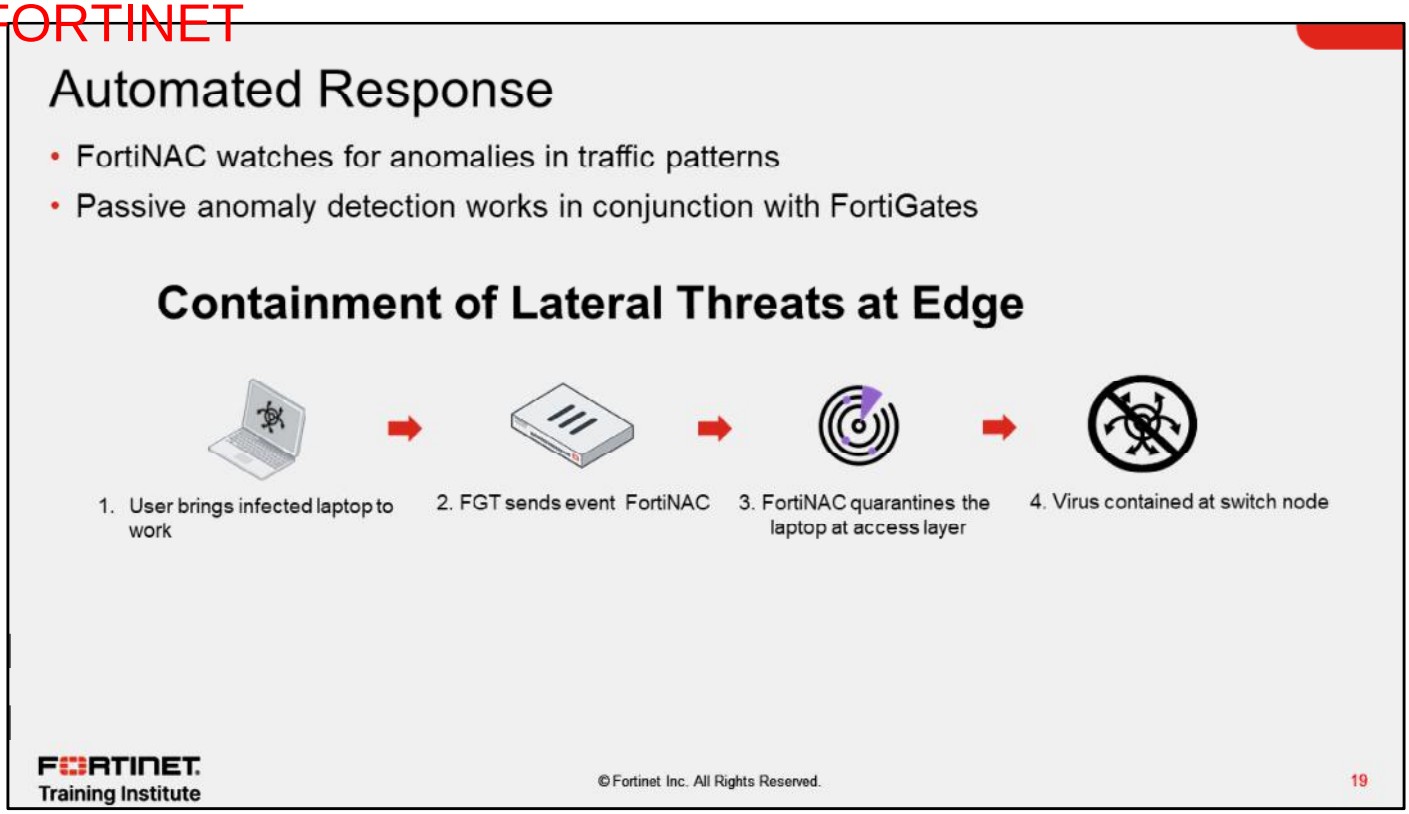
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

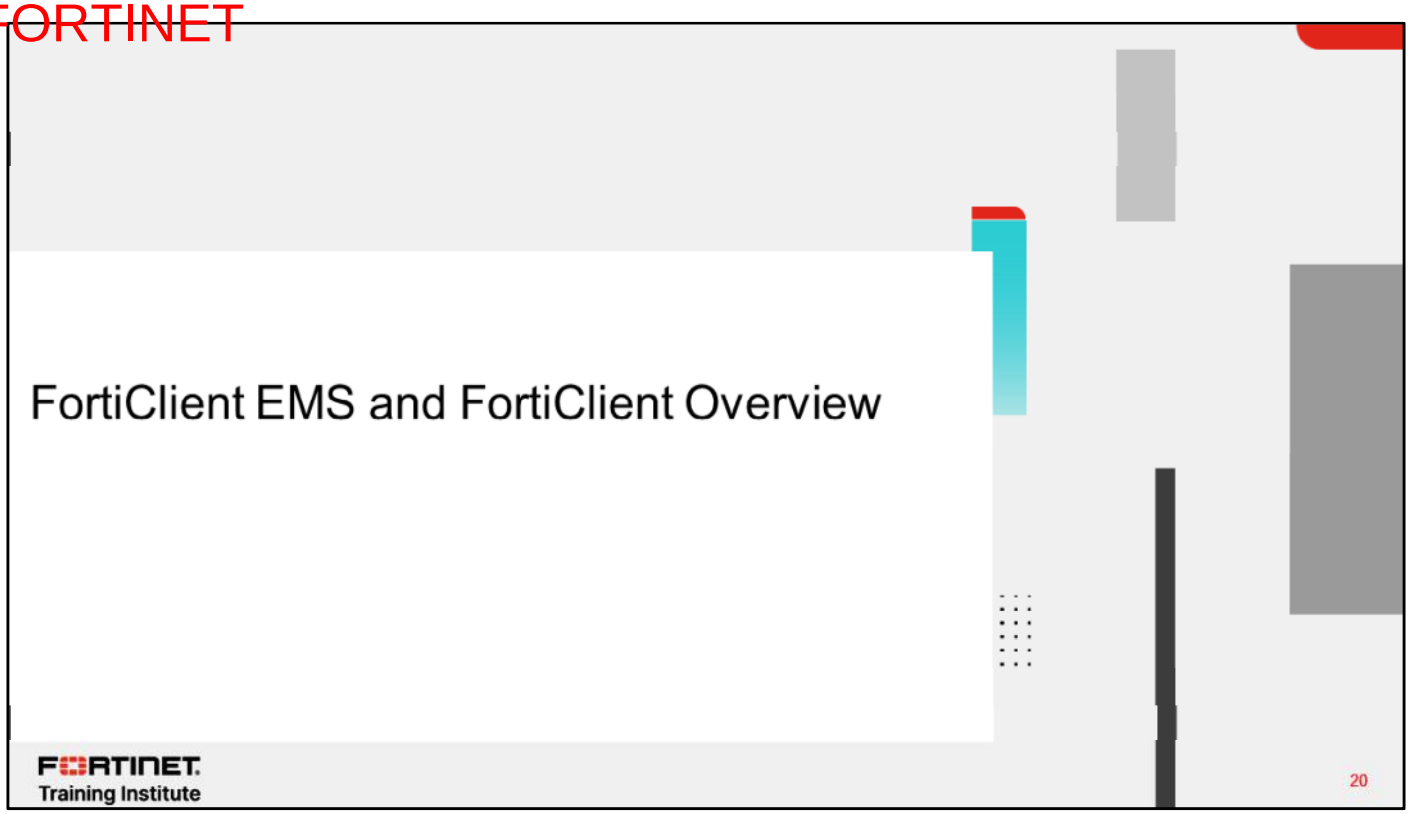
FortiNAC enables detailed segmentation of the network to enable devices and users access to necessary resources while blocking non-authorized access. FortiNAC uses dynamic role-based network access control to logically create network segments by grouping applications and like data together to limit access to a specific group of users and/ or devices. FortiNAC validates a device's configuration as it attempts to join the network to ensure integrity before they connect to the network minimizes risk and the possible spread of malware.

DO NOT REPRINT
© FORTINET



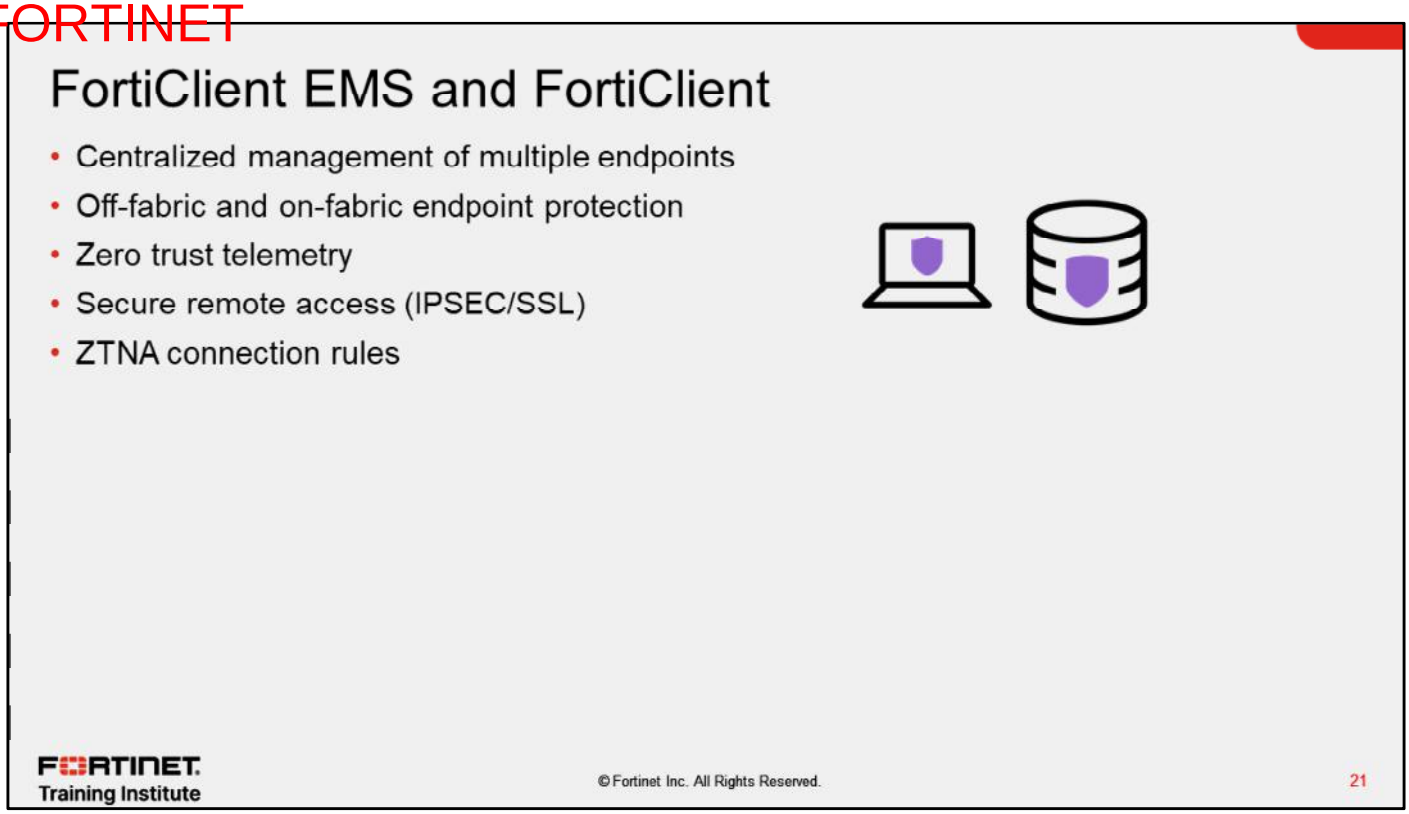
FortiNAC will monitor the network on an ongoing basis, evaluating endpoints to ensure they conform to their profile. FortiNAC can watch for anomalies in traffic patterns. This passive anomaly detection works in conjunction with FortiGate appliances. Once a compromised or vulnerable endpoint is detected as a threat, FortiNAC triggers an automated response to contain the endpoint in realtime.

DO NOT REPRINT
© FORTINET



In this section, you will have an overview of FortiClient EMS and FortClient.

DO NOT REPRINT
© FORTINET

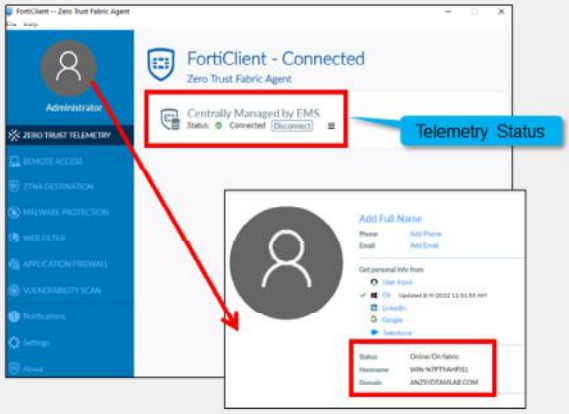


FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints. It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to off-fabric and on-fabric endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting. Some of the key features that FortiClient EMS can provide to FortiClient endpoint are zero-trust telemetry, zero trust network access (ZTNA), remote access, endpoint protection, and so on.

DO NOT REPRINT
© FORTINET

Zero Trust Telemetry

- Displays whether zero trust telemetry is connected to EMS
- FortiClient uses server IP address/FQDN or invitation code to connect zero trust telemetry
- Telemetry data
  - Hardware information, such as MAC addresses
  - Software information, such as the OS version on the endpoint
  - Identification information, such as username, avatar, and hostname
  - Vulnerability information that the vulnerability scanning module reports



FORTINET Training Institute

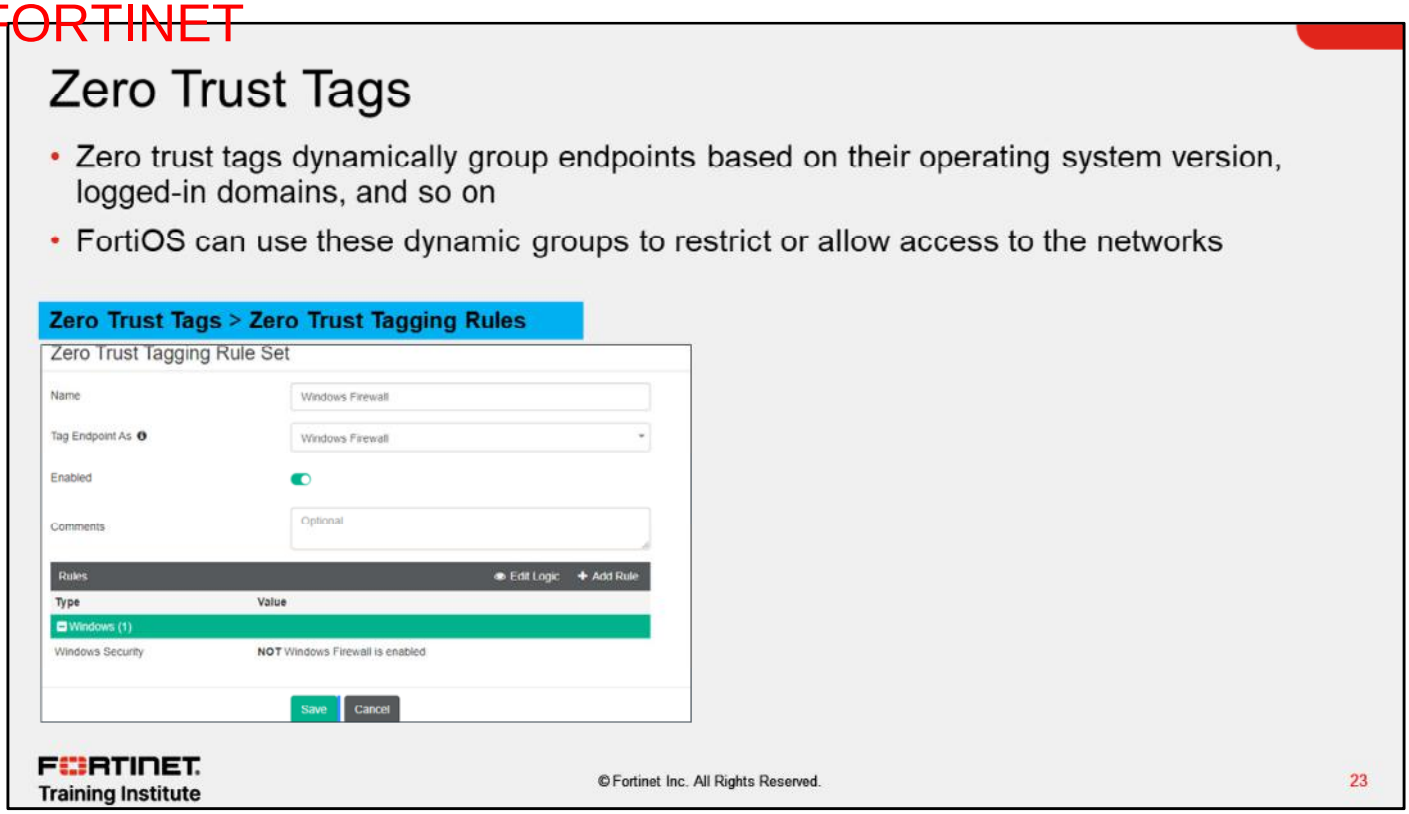
© Fortinet Inc. All Rights Reserved.

22

The **Zero Trust Telemetry** tab displays whether FortiClient telemetry is connected to EMS. You can use the **Zero Trust Telemetry** tab to manually connect FortiClient telemetry to EMS and to disconnect FortiClient telemetry from EMS.

When zero trust telemetry is connected to EMS, FortiClient collects the hardware information (MAC addresses), software information (OS version on the endpoint), identification information (username, avatar, and hostname), and vulnerability information that the vulnerability scanning module reports about the endpoint and its workload, and sends to EMS. When EMS participates in the Security Fabric, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

DO NOT REPRINT
© FORTINET

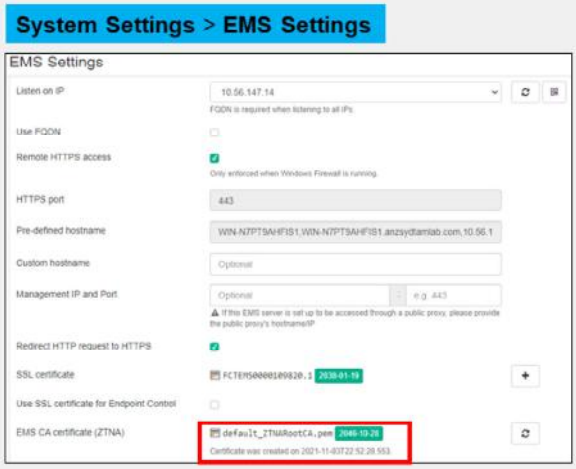


Zero trust tags can dynamically group endpoints based on their operating system version, logged-in domains, and so on. After these tags are automatically synced with FortiOS, network traffic can be allowed or denied based on these tags.

DO NOT REPRINT
© FORTINET

ZTNA Certificate Authentication

- FortiClient submits a CSR to FortiClient EMS upon registration
- FortiClient EMS acts the ZTNA certificate authority (CA)
- FortiClient EMS signs and returns the client certificate
- The certificate is stored in the endpoints certificate store
- Client certificate information is synchronized with FortiGate and is used for client identity verification



FORTINET Training Institute

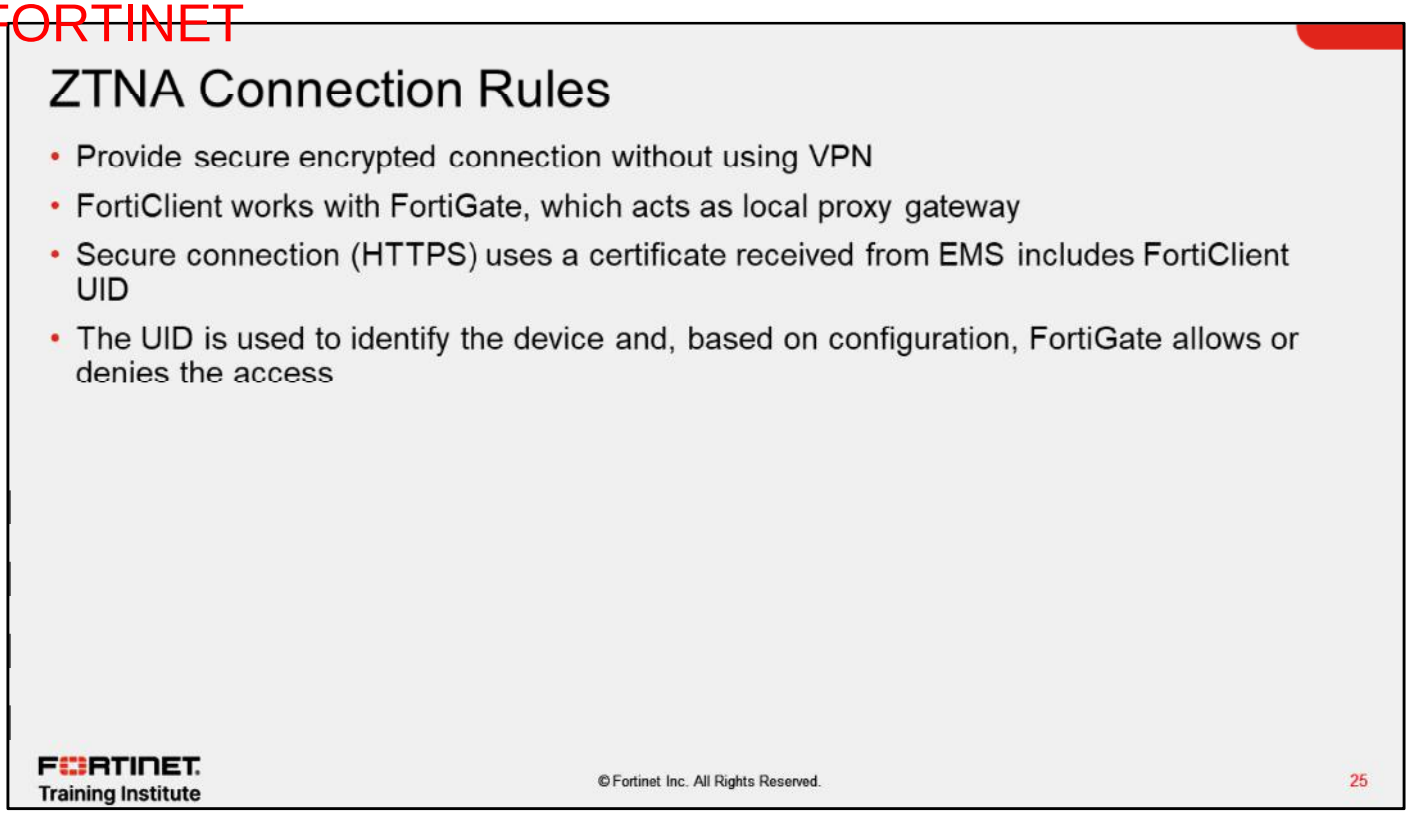
© Fortinet Inc. All Rights Reserved.

24

FortiClient EMS has a default_ZTNARootCA certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised. Click **Endpoint** > **All Endpoints**, select the client, and then click **Action** > **Revoke Client Certificate**.

Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

DO NOT REPRINT
© FORTINET



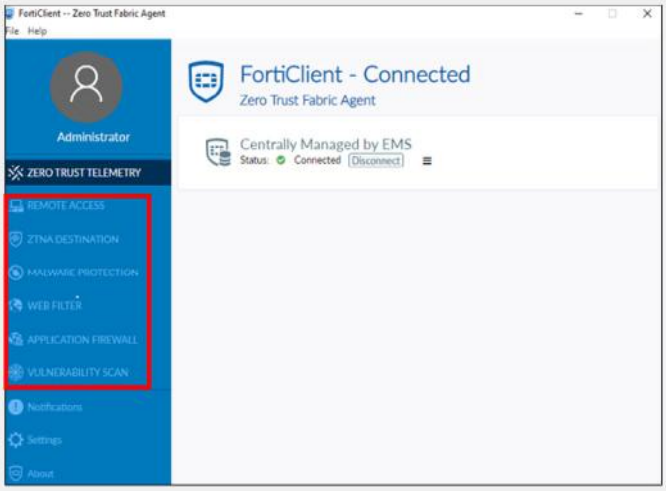
ZTNA connection rules on FortiClient create a secure encrypted connection to protected applications without using VPN. FortiClient uses the FortiGate device application proxy feature to create a secure connection through HTTPS using a certificate received from EMS that includes the FortiClient UID. FortiGate acts as a local proxy gateway.

FortiGate retrieves the UID to identify the device and check other endpoint information that EMS provides to FortiGate, which can include other identity and posture information. FortiGate allows or denies the access, as applicable.

DO NOT REPRINT
© FORTINET

FortiClient Endpoint Protection

- Comprehensive endpoint security:
  - Remote access (IPSec and SSL VPN)
  - Malware protection
  - Web filtering
  - Application firewall
  - Vulnerability management
  - Central management
  - Central logging
- Supports multiple platforms:
  - Windows devices
  - MAC OS devices
  - iOS devices
  - Android mobile devices
  - Chromebook



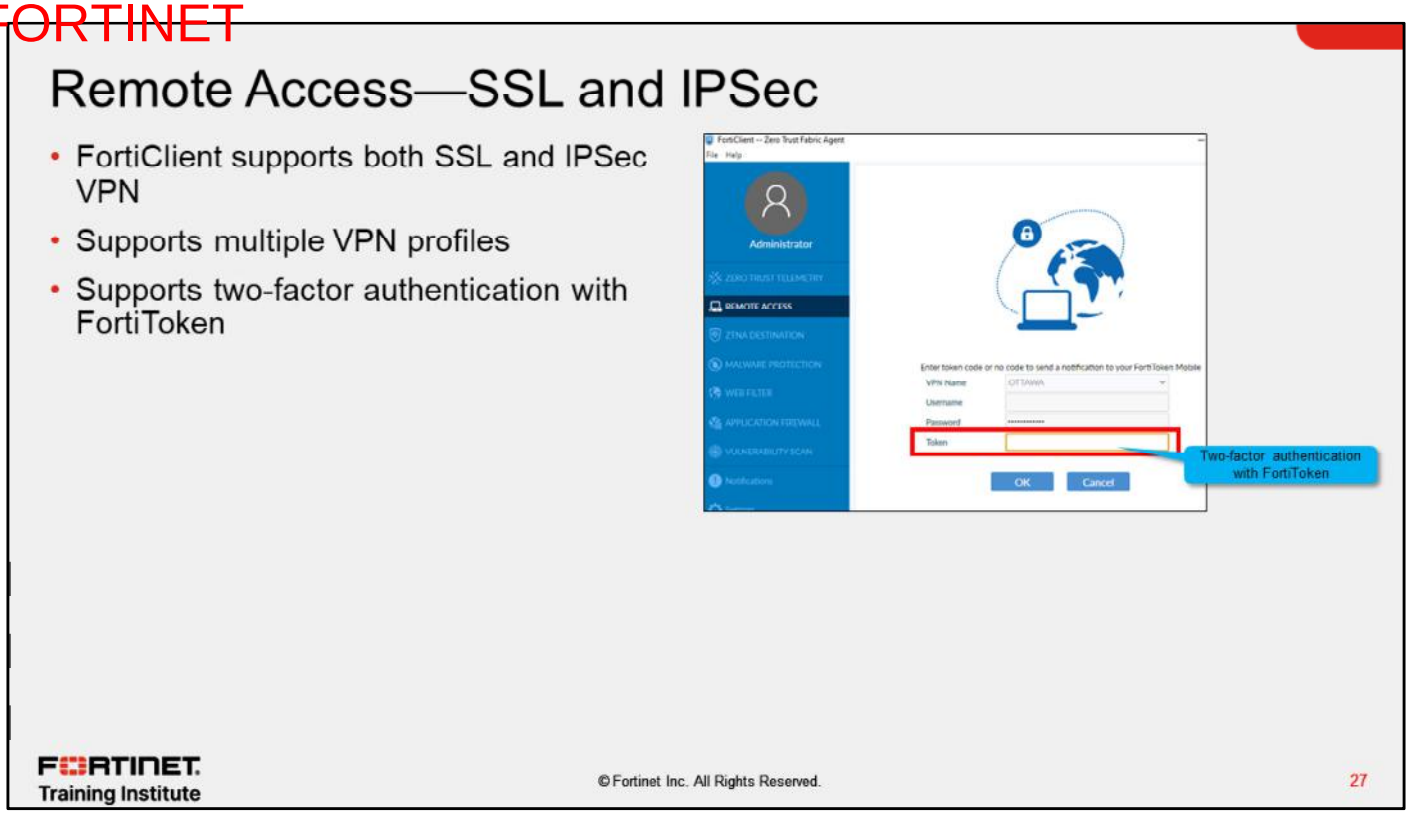
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

FortiClient provides comprehensive endpoint protection for your Windows-based, MAC-based, and Linux-based desktops, laptops, file servers, and mobile devices, such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

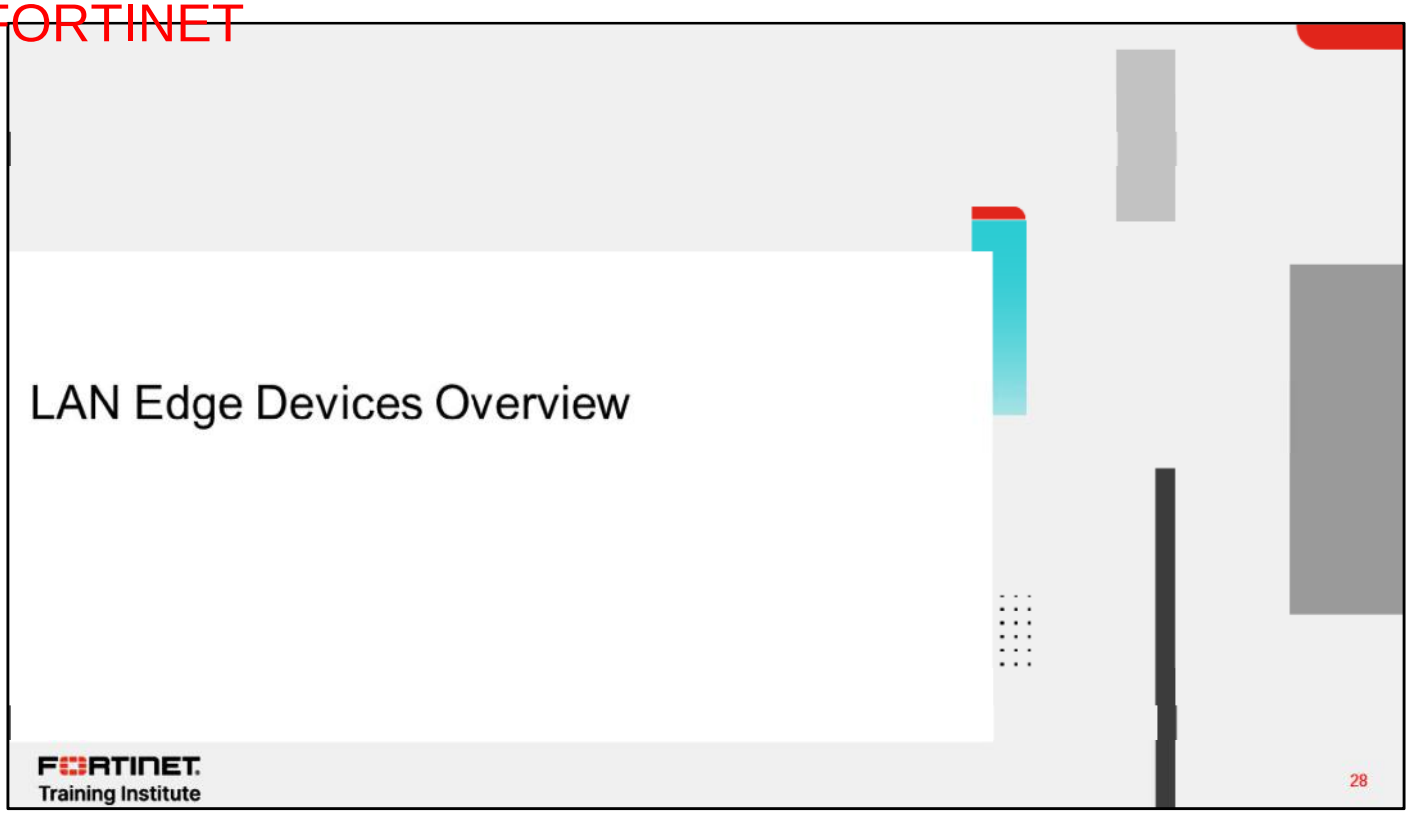
DO NOT REPRINT
© FORTINET



FortiClient supports both IPsec and SSL VPN connections to your network for remote access. The FortiClient EMS administrator can provision client VPN connections in the FortiClient profile (EMS endpoint profile) or the endpoint user can configure new connections on the FortiClient console.

You can also configure two-factor authentication using FortiToken for enhanced security for both types of VPNs on your FortiGate for FortiClient VPN connections.

DO NOT REPRINT
© FORTINET

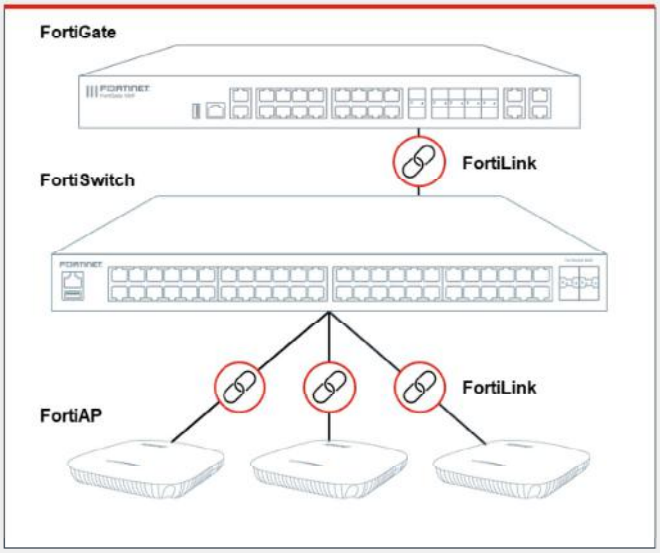


In this section, you will have an overview of Fortinet's LAN edge devices.

DO NOT REPRINT
© FORTINET

Fortinet Secure LAN Edge Through FortiLink

- Integrated security
  - A significant step beyond centralized management
  - Direct control, configuration, and management of FortiAPs and FortiSwitch through FortiOS
  - Extends the next-generation firewall (NGFW) features and inspection to the LAN
- Simplicity
  - Agile deployment and management
  - Flexible architecture to scale as needed
- Lower total cost of ownership
  - Access management included with FortiOS
  - No additional licenses required



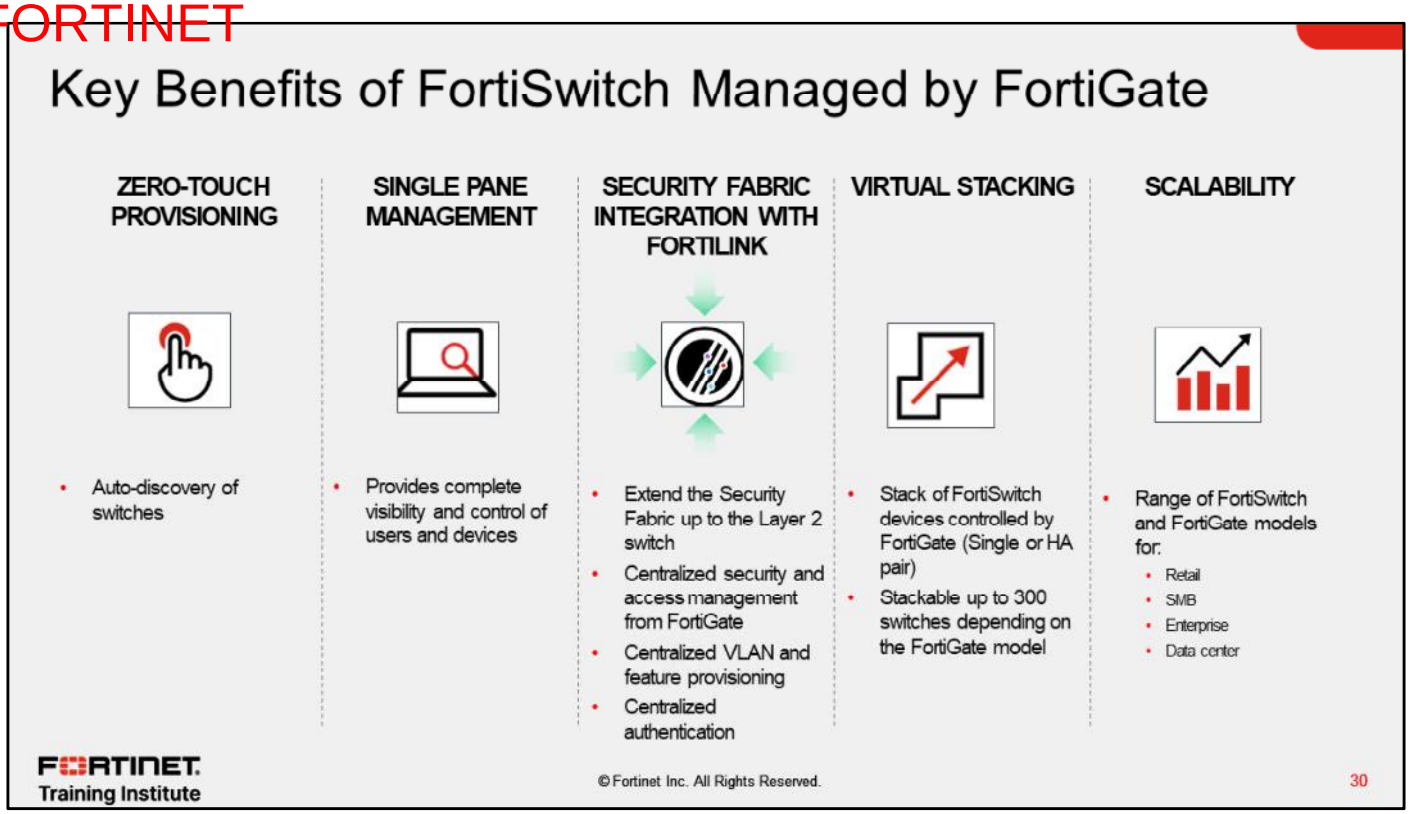
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

A key enabling technology is FortiLink; it is what enables Fortinet's unique capabilities at the LAN edge. FortiLink protocols allows FortiGate to be able to manage Fortinet's network access layer. You can manage, control, and configure FortiAPs and FortiSwitches directly through FortiOS. No additional licensing is required for you to be able to use FortiLink to manage your network access layer.

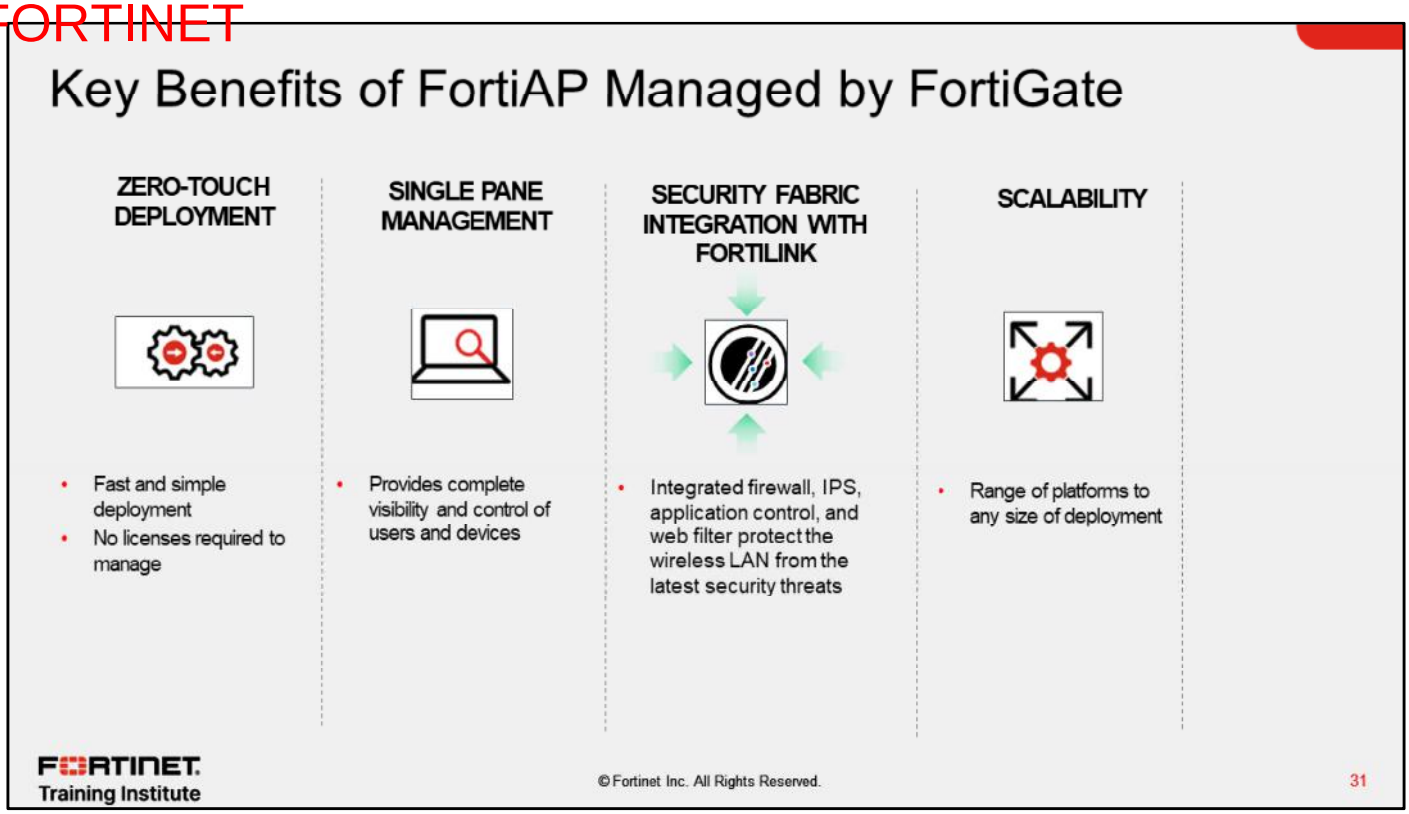
DO NOT REPRINT
© FORTINET



Managing FortiSwitch devices using FortiGate offers the following important key benefits:

- Zero-touch provisioning: When you connect FortiSwitch to a FortiGate interface that has FortiLink enabled, FortiGate automatically discovers and provisions FortiSwitch. You can also use zero-touch provisioning by configuring the FortiGate settings on FortiManager.
- Single pane management: You can manage FortiSwitch using the FortiGate GUI and CLI, or using FortiManager. Administrators are not required to log in to FortiSwitch.
- Security Fabric integration with FortiLink: FortiSwitch becomes an extension of FortiGate. You configure firewall policies using FortiSwitch VLANs in the same way as for FortiGate VLANs. Authentication and authorization are also handled centrally on FortiGate or FortiManager.
- Virtual stacking: FortiGate can manage multiple FortiSwitch devices stacked in different ways, to offer redundancy.
- Scalability: FortiGate and FortiSwitch devices come in many sizes to accommodate the needs of customers, from retail and SMB, up to data centers.

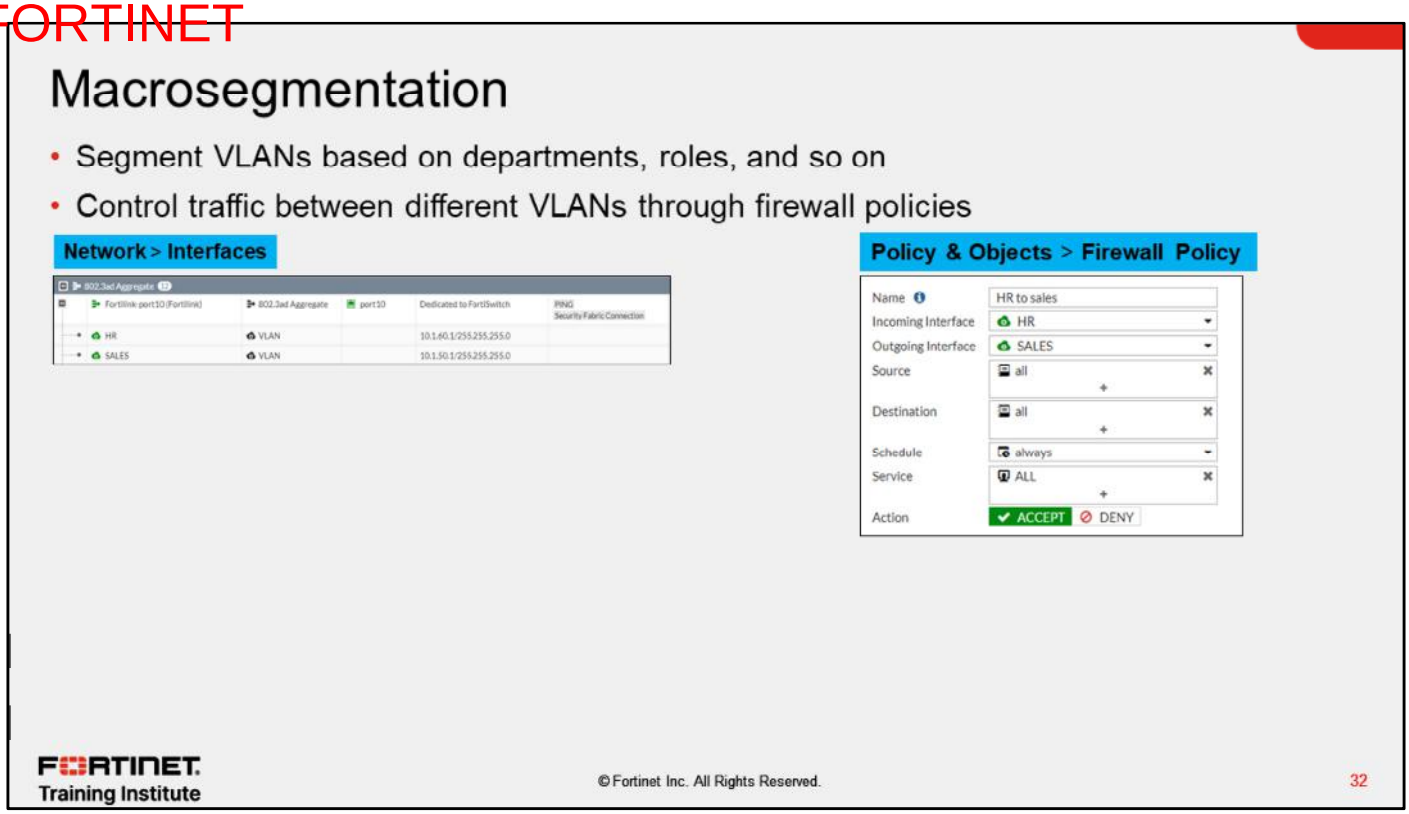
DO NOT REPRINT
© FORTINET



Managing FortiAP devices using FortiGate offers the following important key benefits:

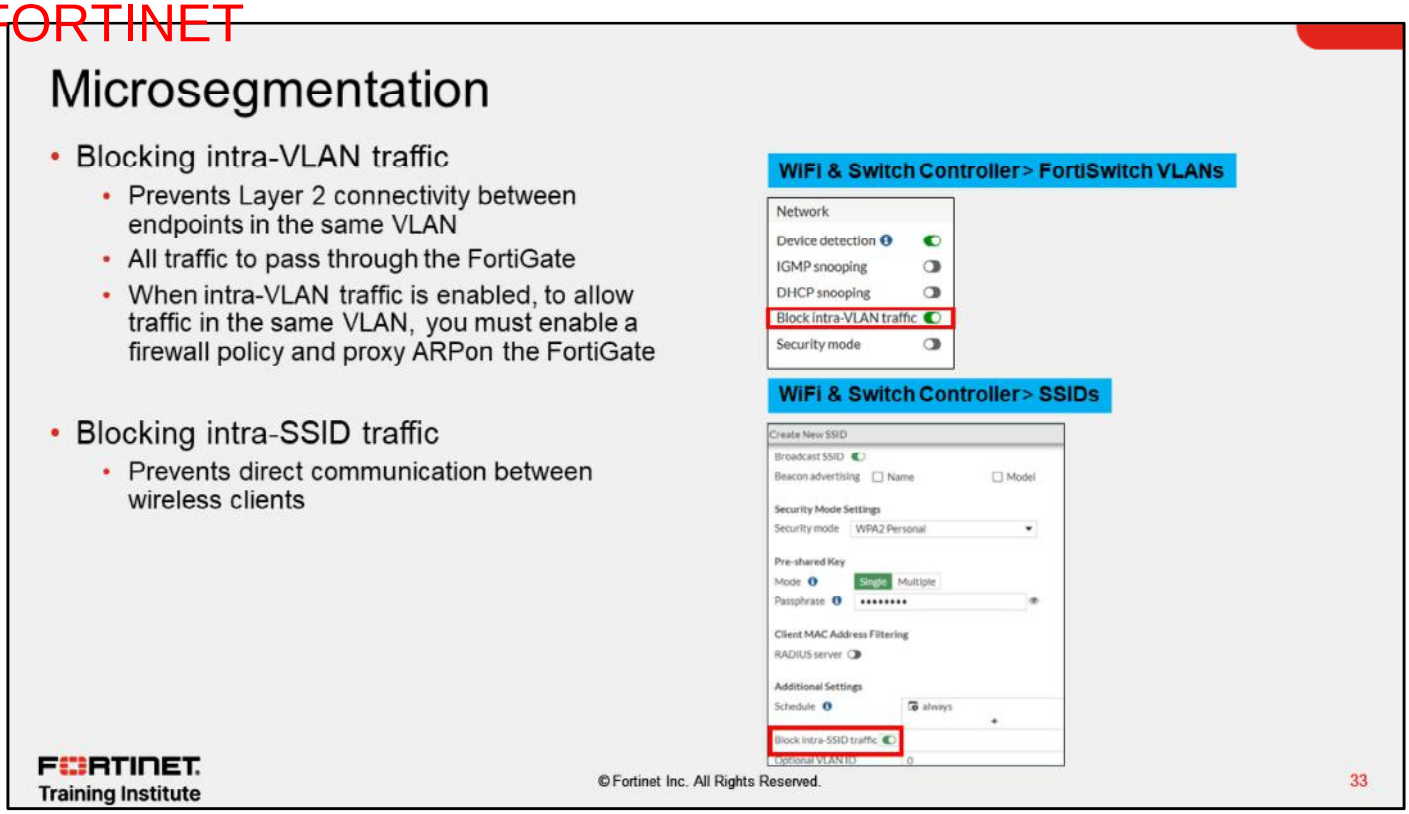
- Zero-touch deployment: When you connect FortiAP to a FortiGate interface that has FortiLink enabled, FortiGate automatically discovers and authorizes the FortiAP. There are no additional license required to mange FortiAPs from FortiGate.
- Single pane management: You can manage FortiAP using the FortiGate GUI or on FortiManager. Administrators are not required to log in to FortiAP.
- Security fabric integration with fortilink: You configure firewall policies using FortitAP SSIDs in the same way as for FortiGate interfaces. Authentication and authorization are also handled centrally on FortiGate or FortiManager.
- Scalability: FortiAPs are available in range of platforms to support any size of deployments.

DO NOT REPRINT
© FORTINET



You can segment your network subnets into different VLANs based on departments, roles, and so on. FortiGates can allow or deny traffic between different VLANs on managed FortiSwitches using firewall policies.

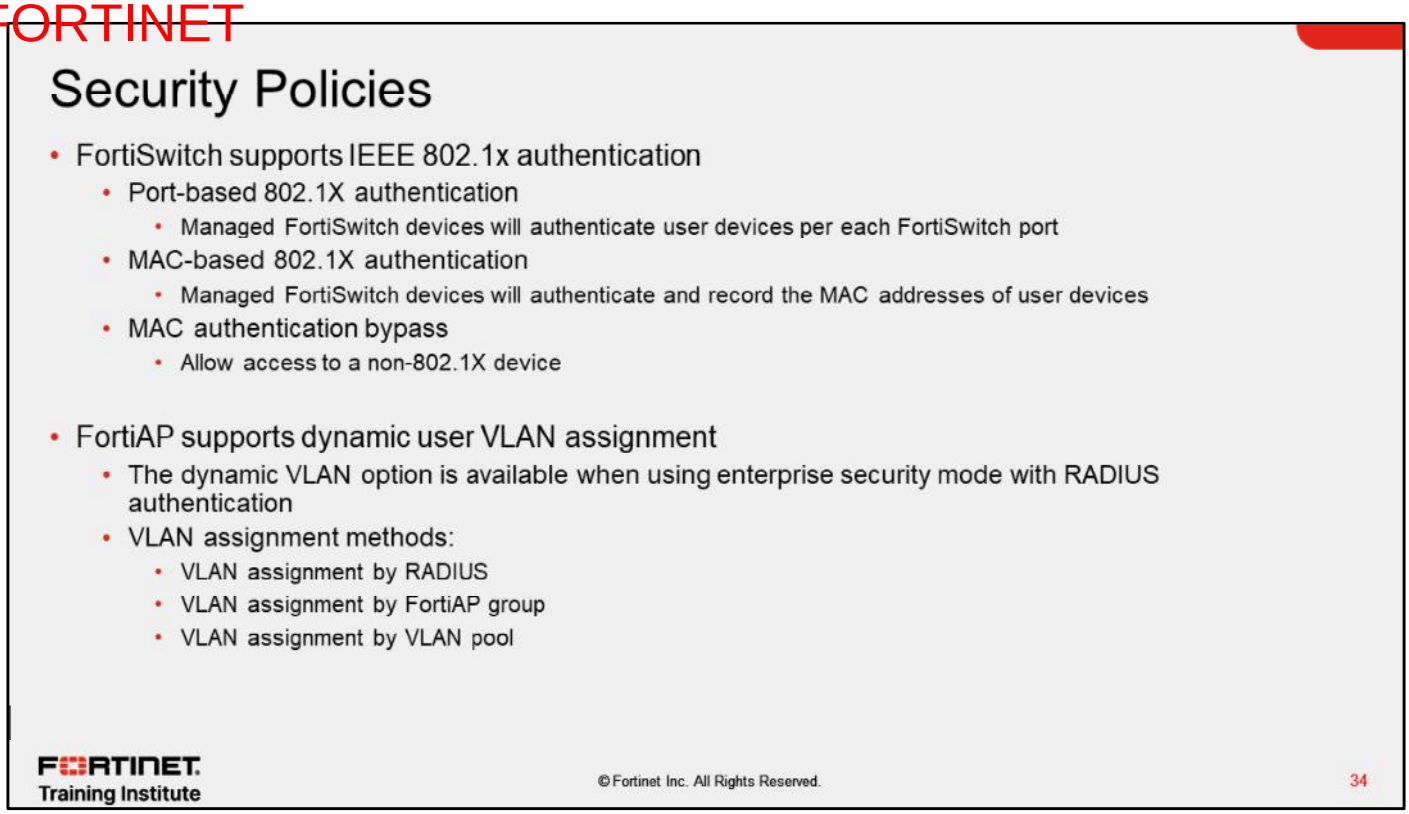
DO NOT REPRINT
© FORTINET



You can block intra-VLAN traffic on FortiSwitches managed by FortiGates. This prevents direct client-to-client traffic visibility at the Layer2 VLAN layer. Clients can communicate with FortiGate. After the client traffic reaches the FortiGate, FortiGate determines whether to allow various levels of access to the client by shifting the client's network VLAN as appropriate, if allowed by a firewall policy, and if proxy ARP is enabled.

You can also block intra-SSID traffic on the FortiAPs managed by FortiGates. This will restrict communication between two wireless clients connected on same SSID on FortiAPs.

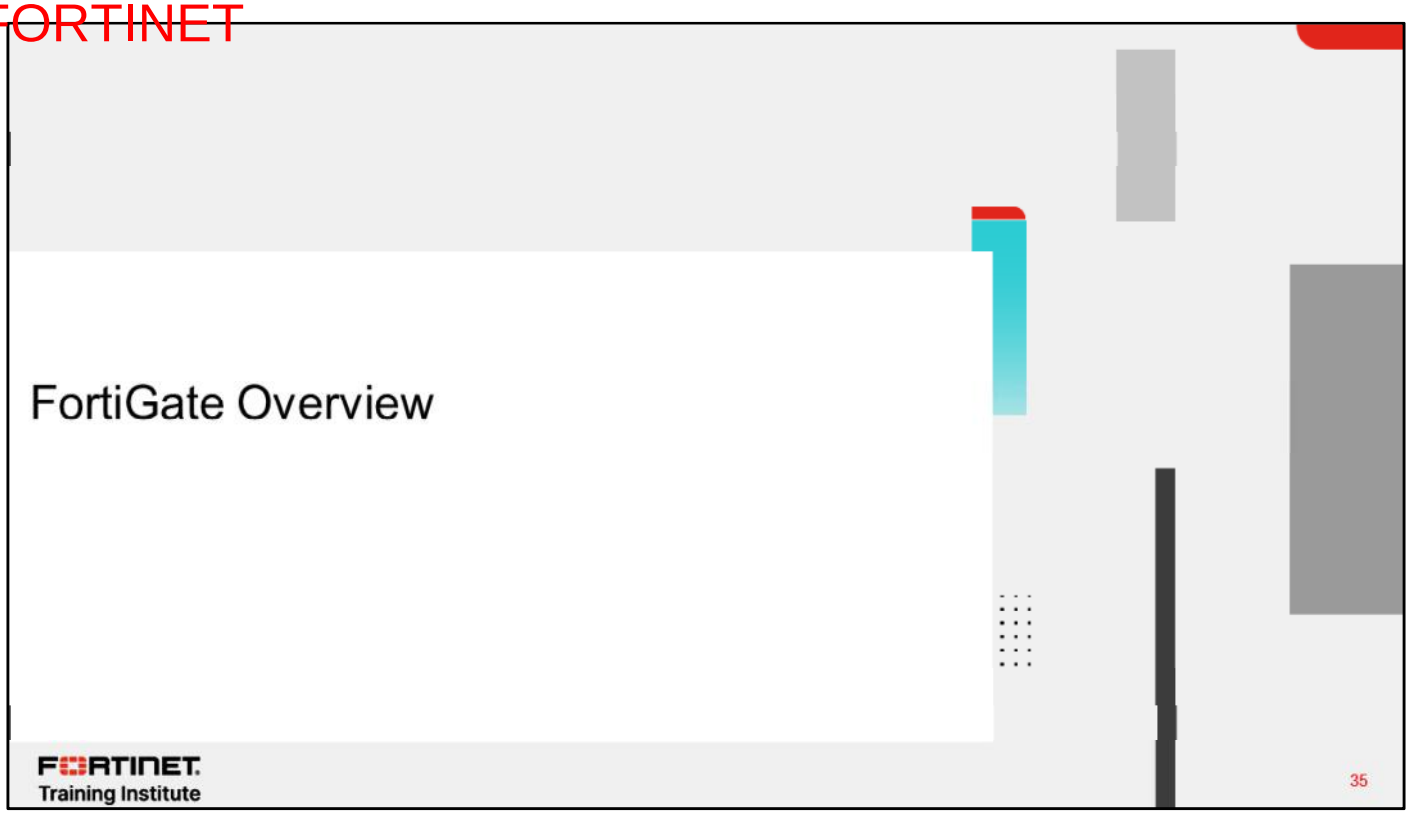
DO NOT REPRINT
© FORTINET



You can enable 802.1x authentication through security policies on FortiSwitch. Port-based authentication is preferred when you expect a single host per port to authenticate, even though there may be multiple hosts connecting to the same port. In this scenario, FortiSwitch authenticates a single host, and opens the port to other devices behind the port. A use case for this scenario is an access point (AP). After an AP authenticates against the switch, any of its connected devices can access the network, despite them using a different MAC address from the one used by the AP during authentication. In addition, all devices are granted the same access level assigned to the AP. However, if you want to authenticate each device behind a port, and optionally, grant each device a different access level based on the credentials provided, then MAC-based is required. For security, MAC-based authentication is preferred because each host (or MAC address) behind the port must authenticate to access the network. For performance, port-based is better because only a single host is required to authenticate. Alternatively, you can enable MAC authentication bypass to allow access to a non-802.1X device, provided the device MAC address is authorized on the authentication server.

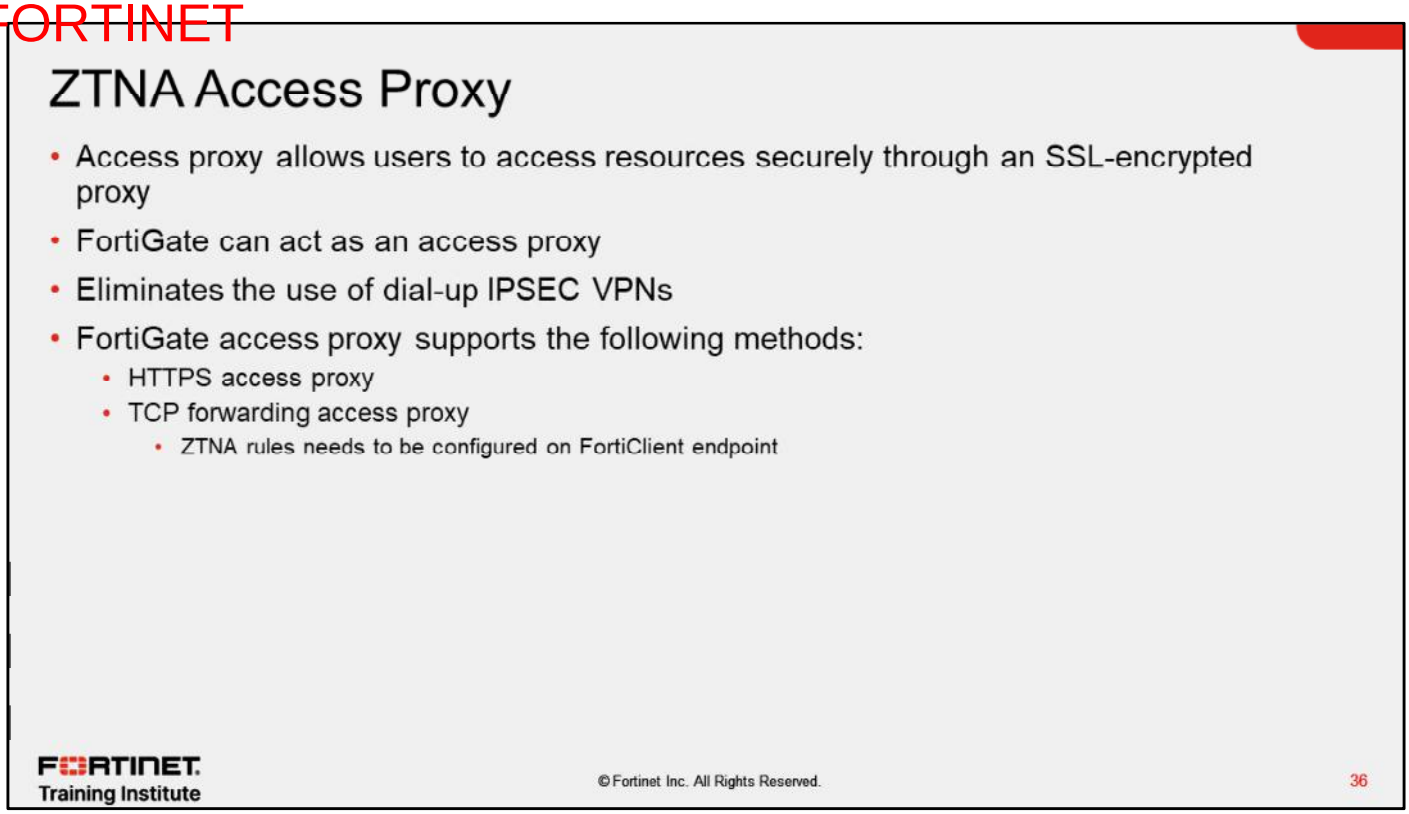
FortiAP supports dynamic user VLAN assignment, and is available when using enterprise security mode with RADIUS authentication. VLAN assignment by RADIUS is used to assign each user to a VLAN based on information stored in the RADIUS authentication server. VLANs can also be set dynamically based on FortiAP groups. Dynamic VLAN assignment allows the same SSID to be deployed to many APs, avoiding the need to produce multiple SSIDs. VLAN assignment by VLAN pool assigns multiple VLANs to a single SSID removing any client limit and preserving an efficient IP network.

DO NOT REPRINT
© FORTINET



In this section, you will have an overview of the FortiGate ZTNA features.

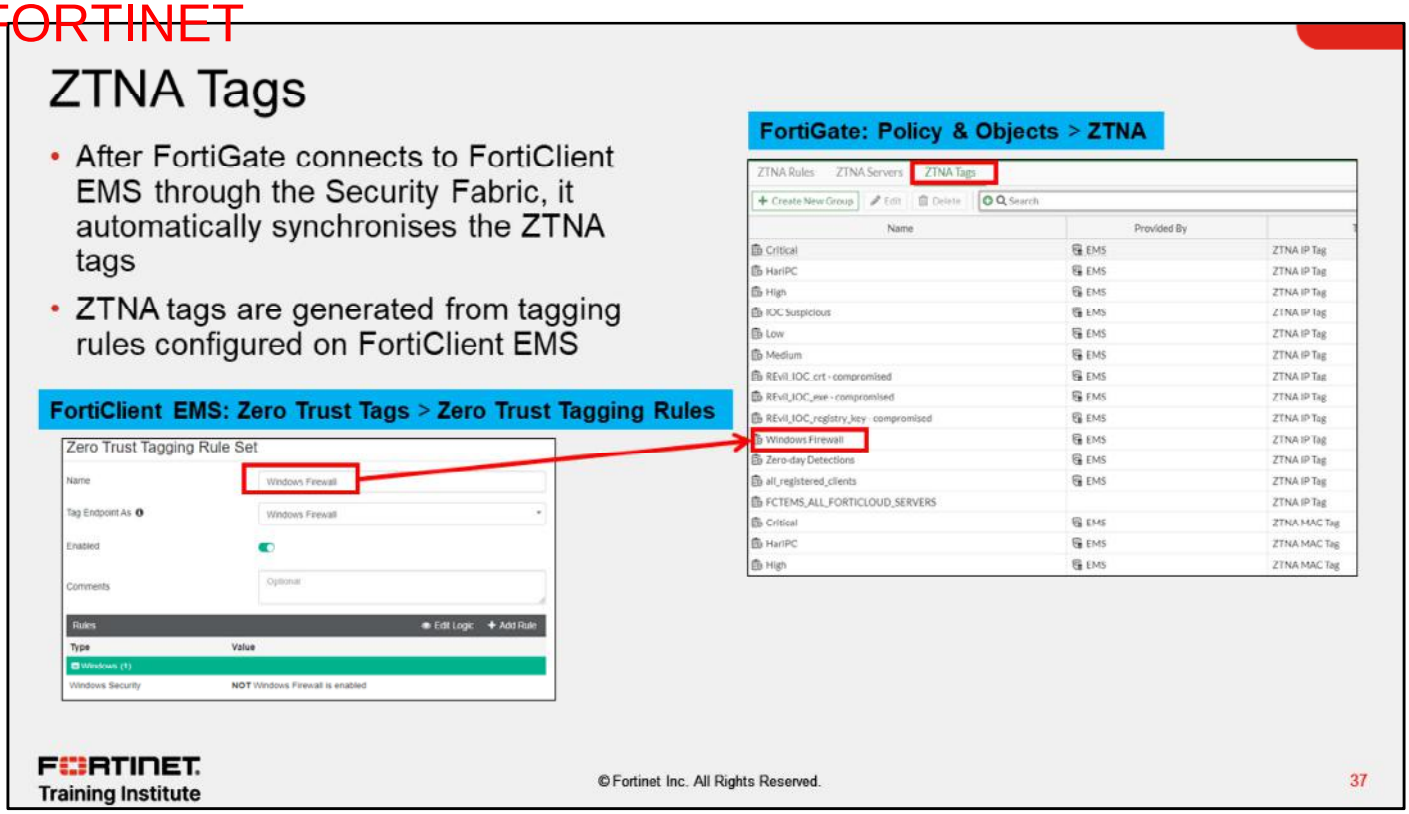
DO NOT REPRINT
© FORTINET



ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy by eliminating the user of dial-up IPSEC VPNs. FortiGate can act as an access proxy and supports the following methods:

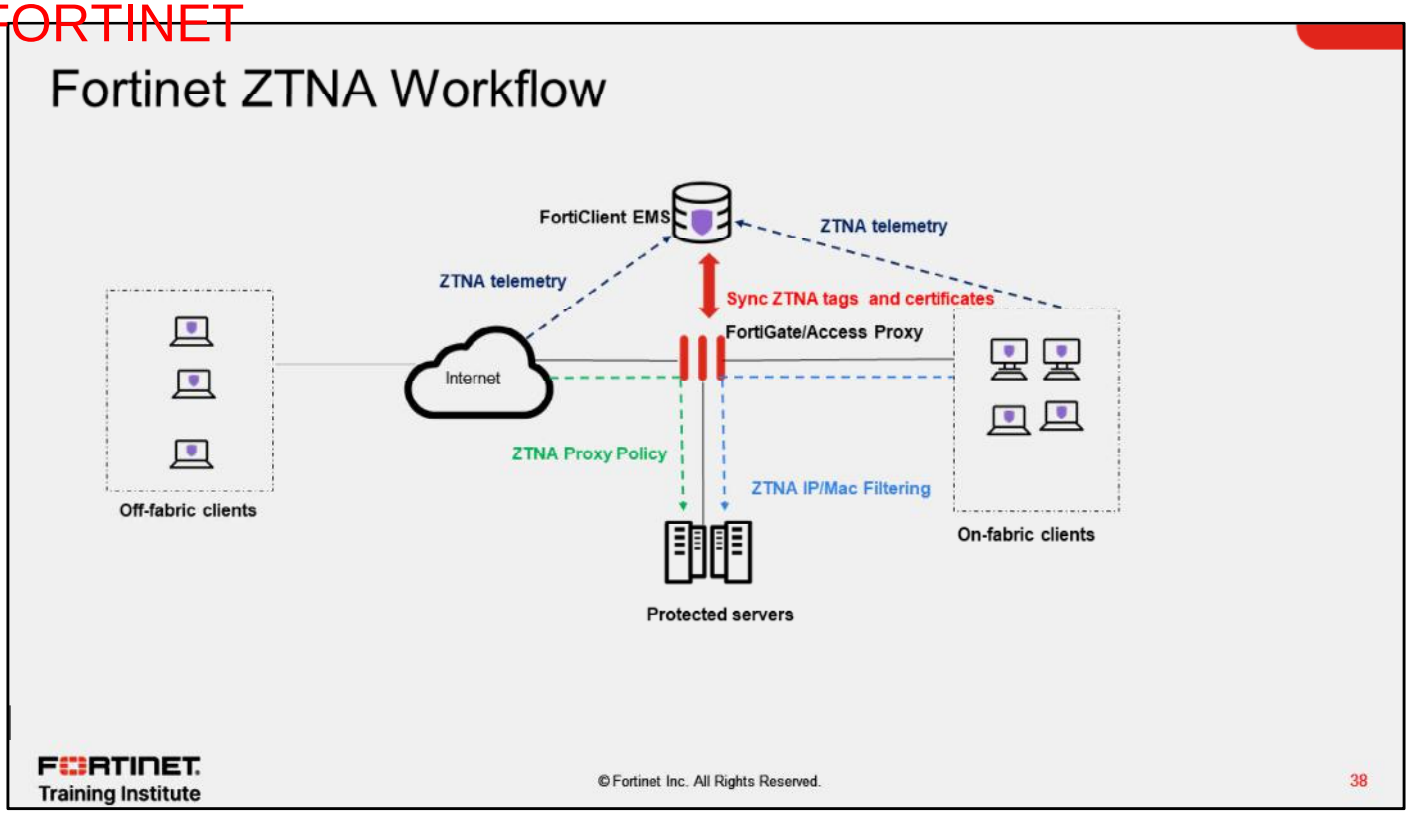
- HTTPS access proxy: works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy virtual IP (VIP). FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the FortiClient EMS.
- TCP forwarding access proxy (TFAP): is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source. ZTNA rules needs to configured on FortiClient endpoints.

DO NOT REPRINT
© FORTINET



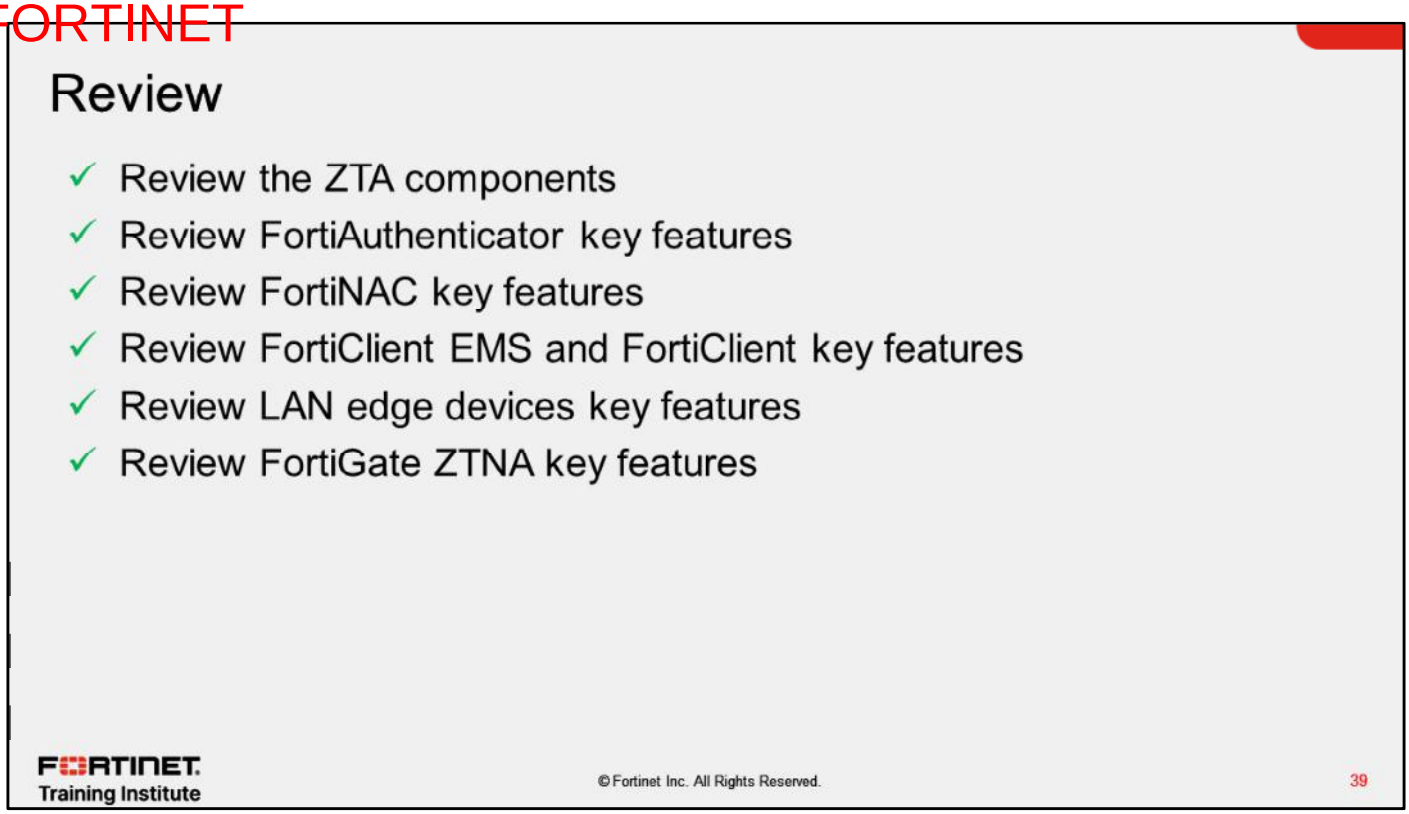
ZTNA tags are configured and generated using tagging rules on FortiClient EMS. FortiGate connects to FortiClient EMS through the Security Fabric and automatically synchronises the ZTNA tags. FortiGate can uses the ZTNA tags in firewall policies or ZTNA rules, to allow or deny network traffic.

DO NOT REPRINT
© FORTINET



This slide demonstrates ZTNA telemetry, tags, and policy enforcement. You configure ZTNA tag conditions and policies on FortiClient EMS. FortiClient EMS shares the tag information with FortiGate through Security Fabric integration. FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry. FortiGate can then use ZTNA tags to enforce access control rules to incoming traffic through ZTNA access.

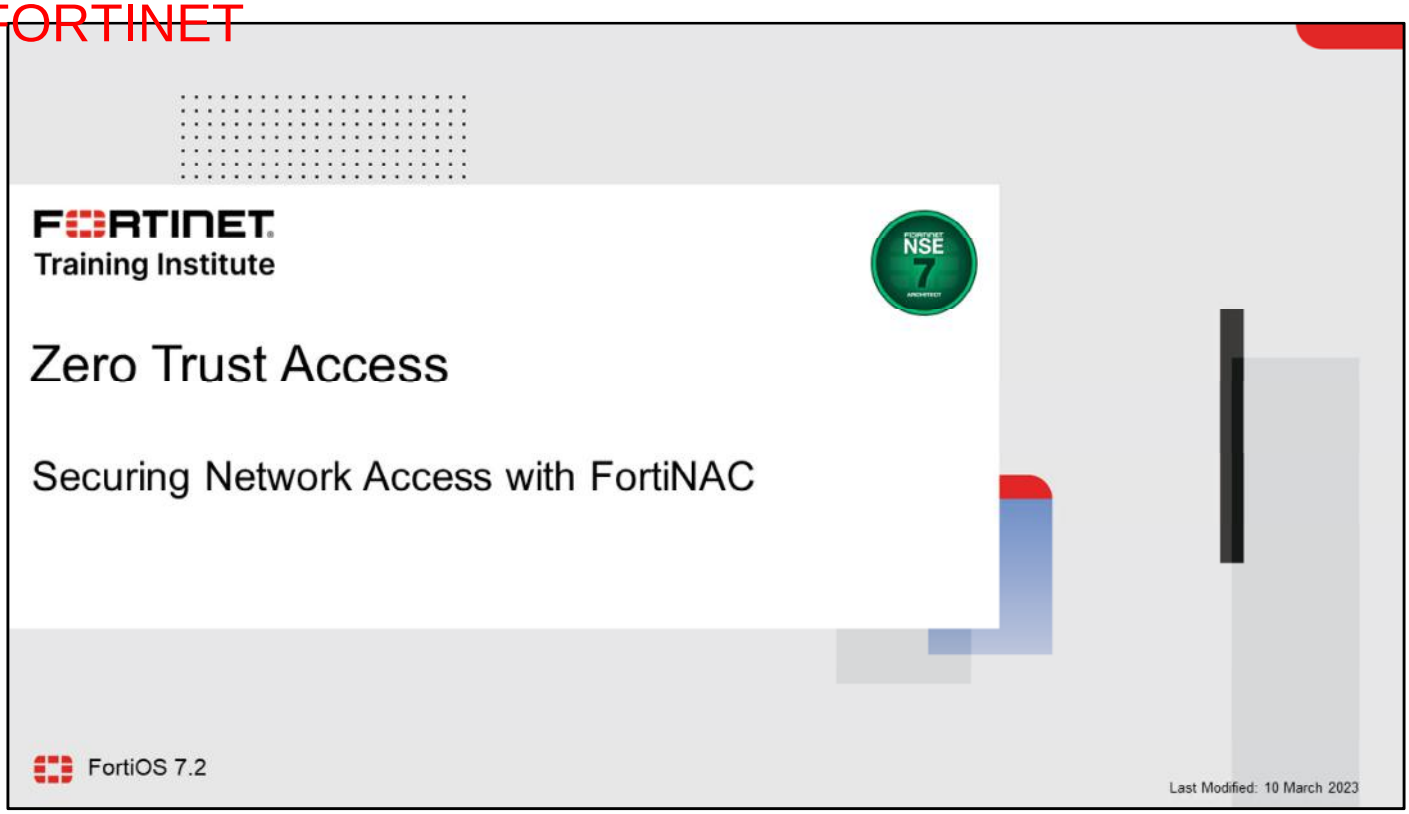
DO NOT REPRINT
© FORTINET



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

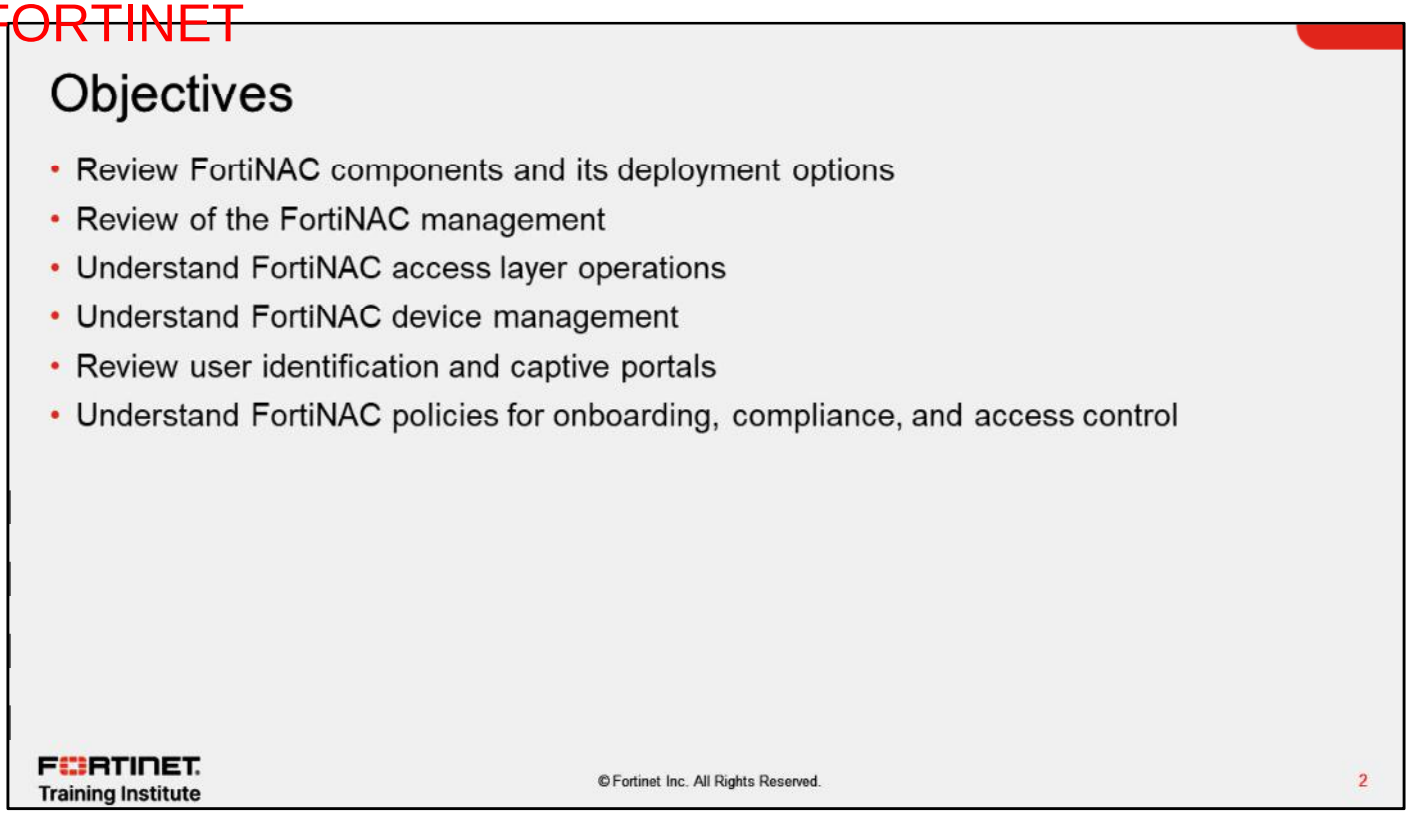
By mastering the objectives covered in this lesson, you learned about the different ZTA components.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the zero trust access (ZTA) design principles for securing network access with FortiNAC.

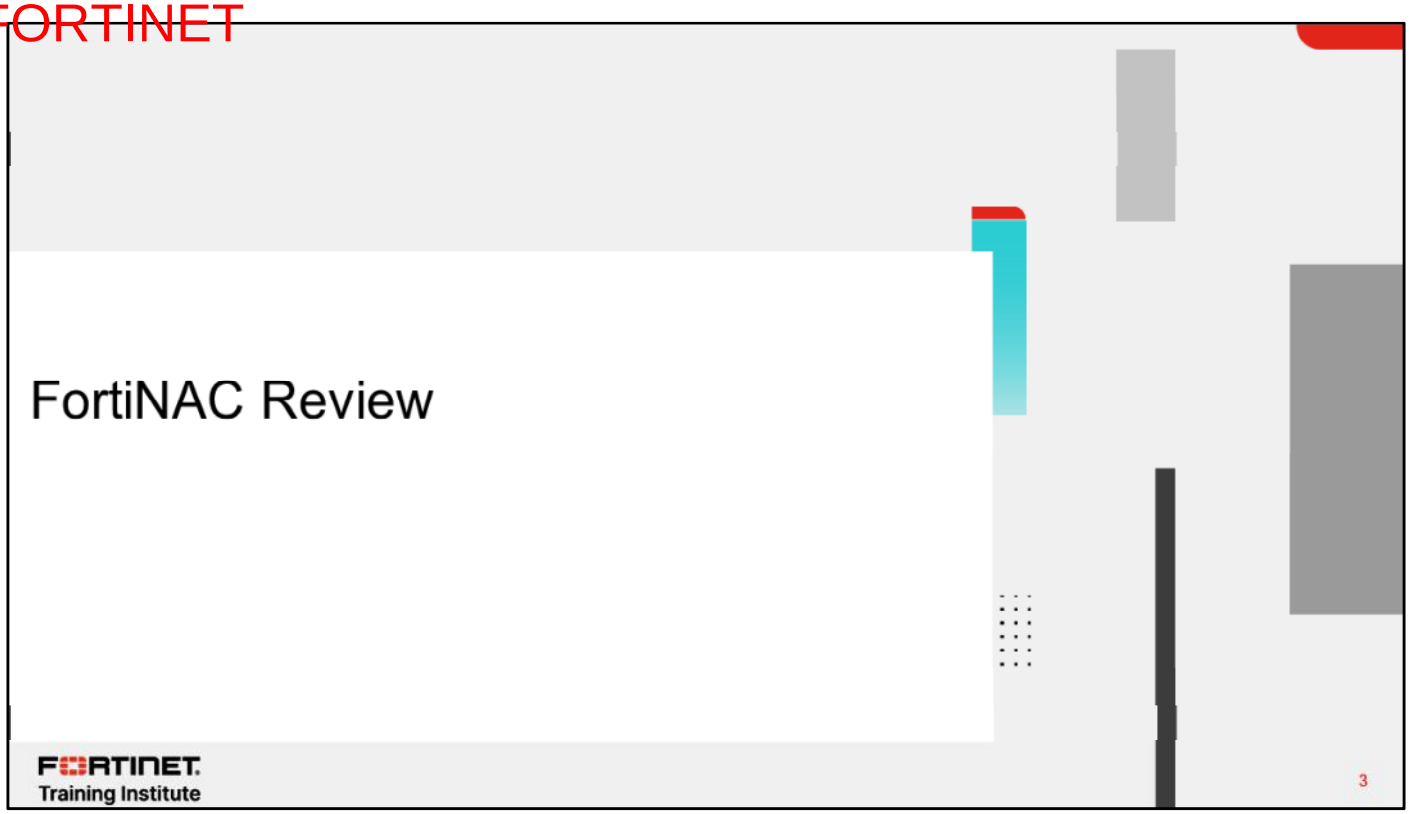
DO NOT REPRINT
© FORTINET



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

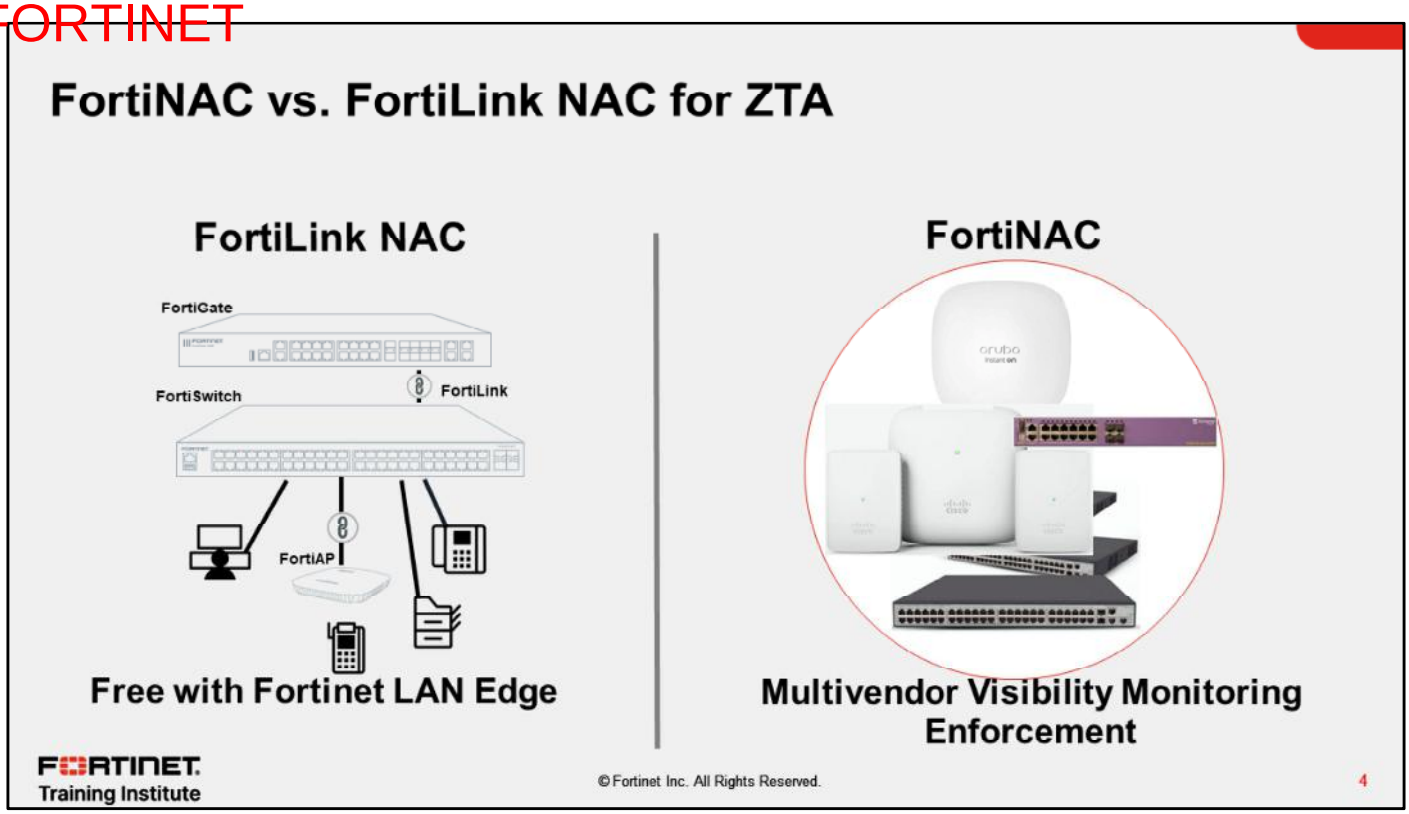
By demonstrating competence in design principles for securing network access with FortiNAC, you will understand the key features of implementing FortiNAC.

DO NOT REPRINT
© FORTINET



In this section, you will have an overview of FortiNAC and its deployment options.

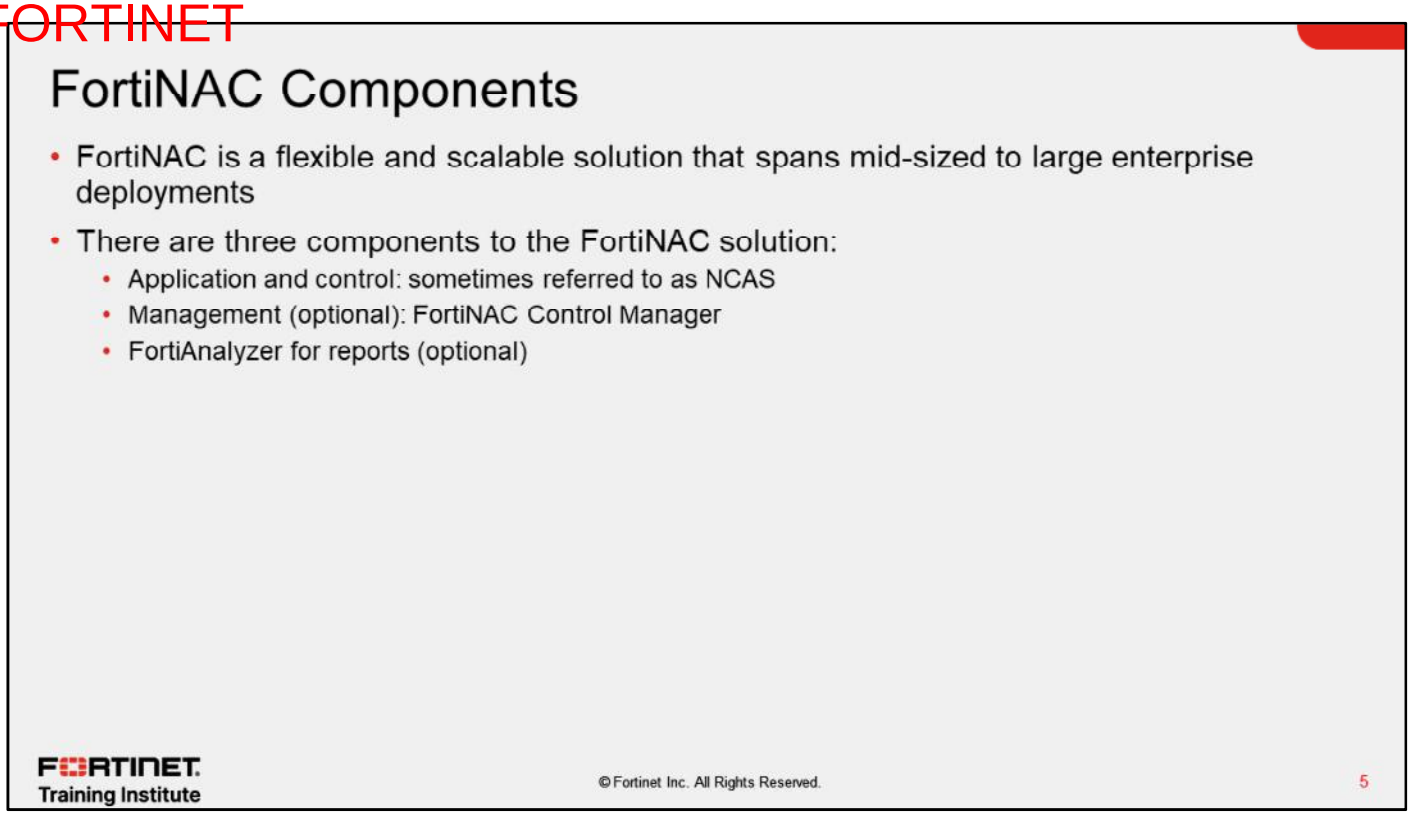
DO NOT REPRINT
© FORTINET



Fortinet believes that the visibility and control that network access control (NAC) provides are foundational to security at the edges of your network.
Fortinet offers the following NAC solutions:

- FortiLink NAC, as a feature of our LAN Edge (Fortinet wired and wireless) solution, for free. This feature provides base-level discovery and control.
- Fortinet's core offering is FortiNAC which offers a full-featured solution that encompasses not only Fortinet equipment, but also a variety of leading vendors equipment, to provide a solution to secure networks and integrate them into the Security Fabric.

DO NOT REPRINT
© FORTINET

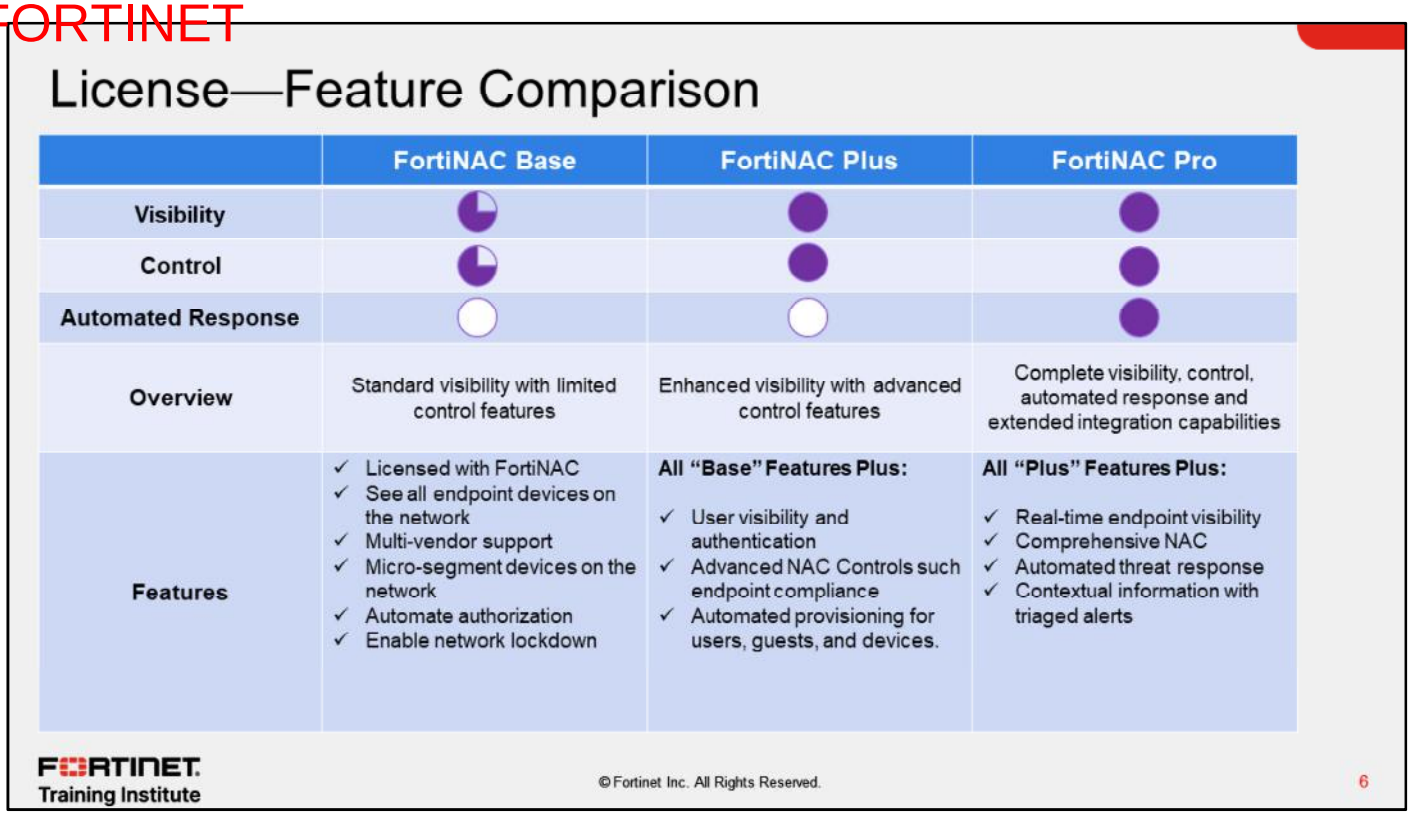


FortiNAC is a flexible and scalable solution that spans mid-sized to large enterprise deployments. There are three components in a FortiNAC deployment:

- Application and control: The network application and control server (NCAS) is where all the NAC functions are running.
- Management: FortiNAC Control Manager is suitable for large distributed environments. When deployed as a network control manager, FortiNAC can manage other FortiNAC devices.
- Reporting: FortiAnalyzer can be used for centralized logging.

You can configure and deploy FortiNAC using the NCAS; this is the only required component. FortiNAC control manager and FortiAnalyzer are optional components and can be deployed, depending on your organization's requirements.

DO NOT REPRINT
© FORTINET

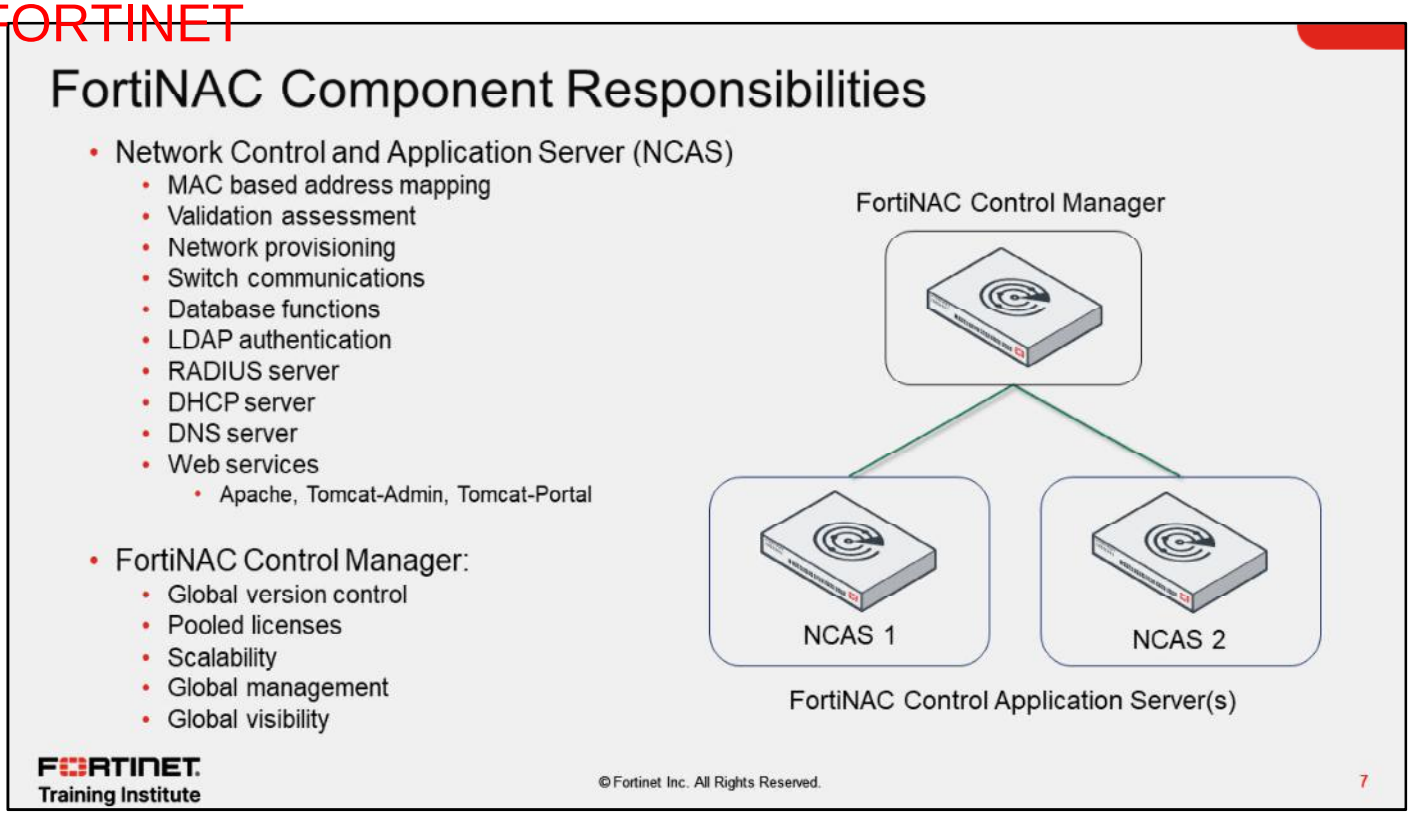


License—Feature Comparison

	FortiNAC Base	FortiNAC Plus	FortiNAC Pro
Visibility	◔	●	●
Control	◔	●	●
Automated Response	○	○	●
Overview	Standard visibility with limited control features	Enhanced visibility with advanced control features	Complete visibility, control, automated response and extended integration capabilities
Features	✓ Licensed with FortiNAC ✓ See all endpoint devices on the network ✓ Multi-vendor support ✓ Micro-segment devices on the network ✓ Automate authorization ✓ Enable network lockdown	**All "Base" Features Plus:** ✓ User visibility and authentication ✓ Advanced NAC Controls such endpoint compliance ✓ Automated provisioning for users, guests, and devices.	**All "Plus" Features Plus:** ✓ Real-time endpoint visibility ✓ Comprehensive NAC ✓ Automated threat response ✓ Contextual information with triaged alerts

FortiNAC offers three different license types. FortiNAC base includes network discovery, host profiling, and classification. FortiNAC plus consists of host registration, scanning, and access control, along with all base features. FortiNAC pro includes automated threat response (security Incidents), and all the plus and base features. FortiNAC pro license is recommended for comprehensive ZTA features.

DO NOT REPRINT
© FORTINET



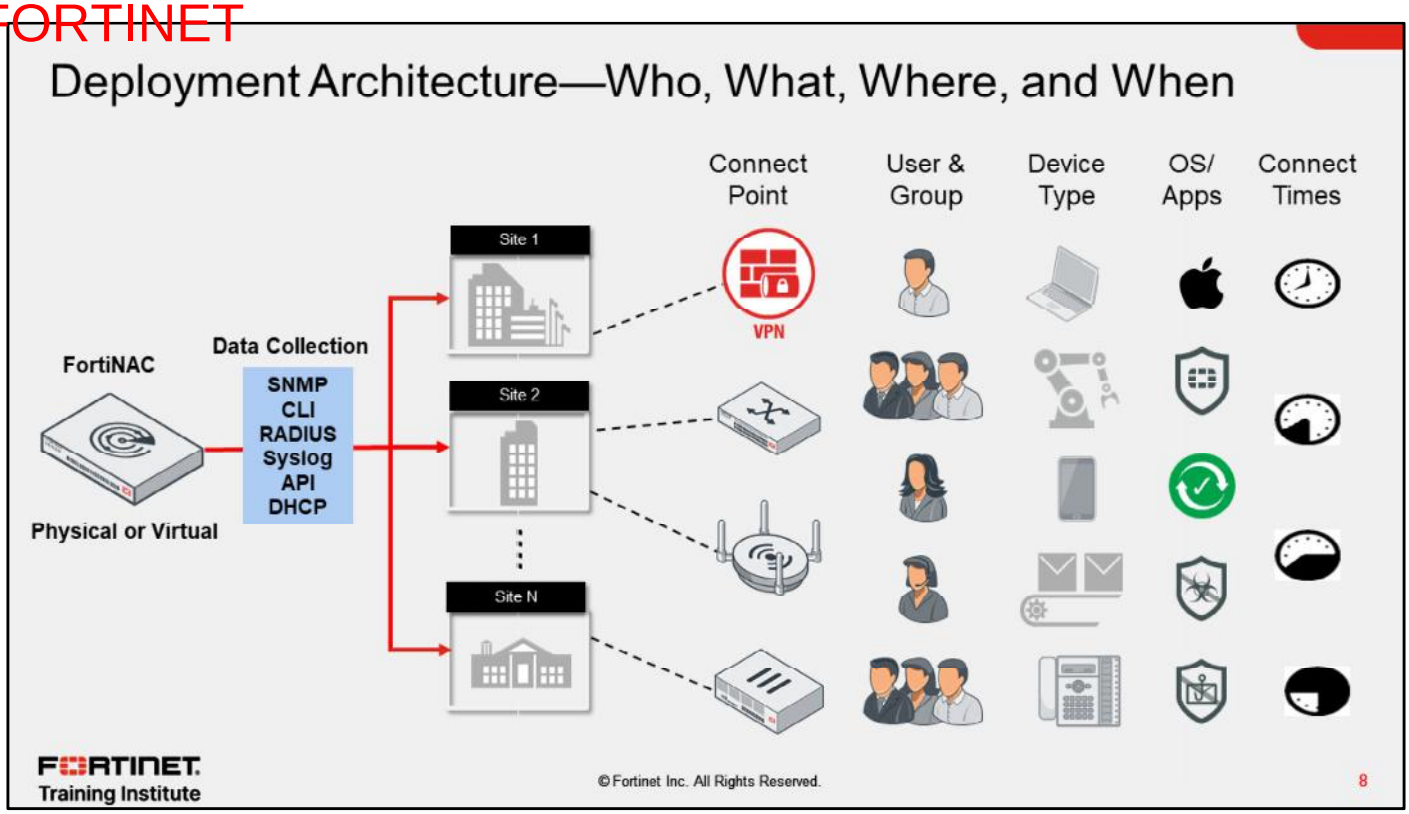
FortiNAC Control Manager provides the ability to manage multiple FortiNAC devices. FortiNAC devices are added for management, individually, to the FortiNAC Control Manager.

FortiNAC Control Manager can then update all managed FortiNAC devices to ensure that each device is operating with the same revision.

Licensing is pushed down from the FortiNAC Control Manager to the FortiNAC devices that it manages, dynamically distributing the concurrent license counts as needed. This architecture allows FortiNAC to scale to even the largest environments.

Global management and visibility provide a single, simplified administration in large distributed deployments.

DO NOT REPRINT
© FORTINET



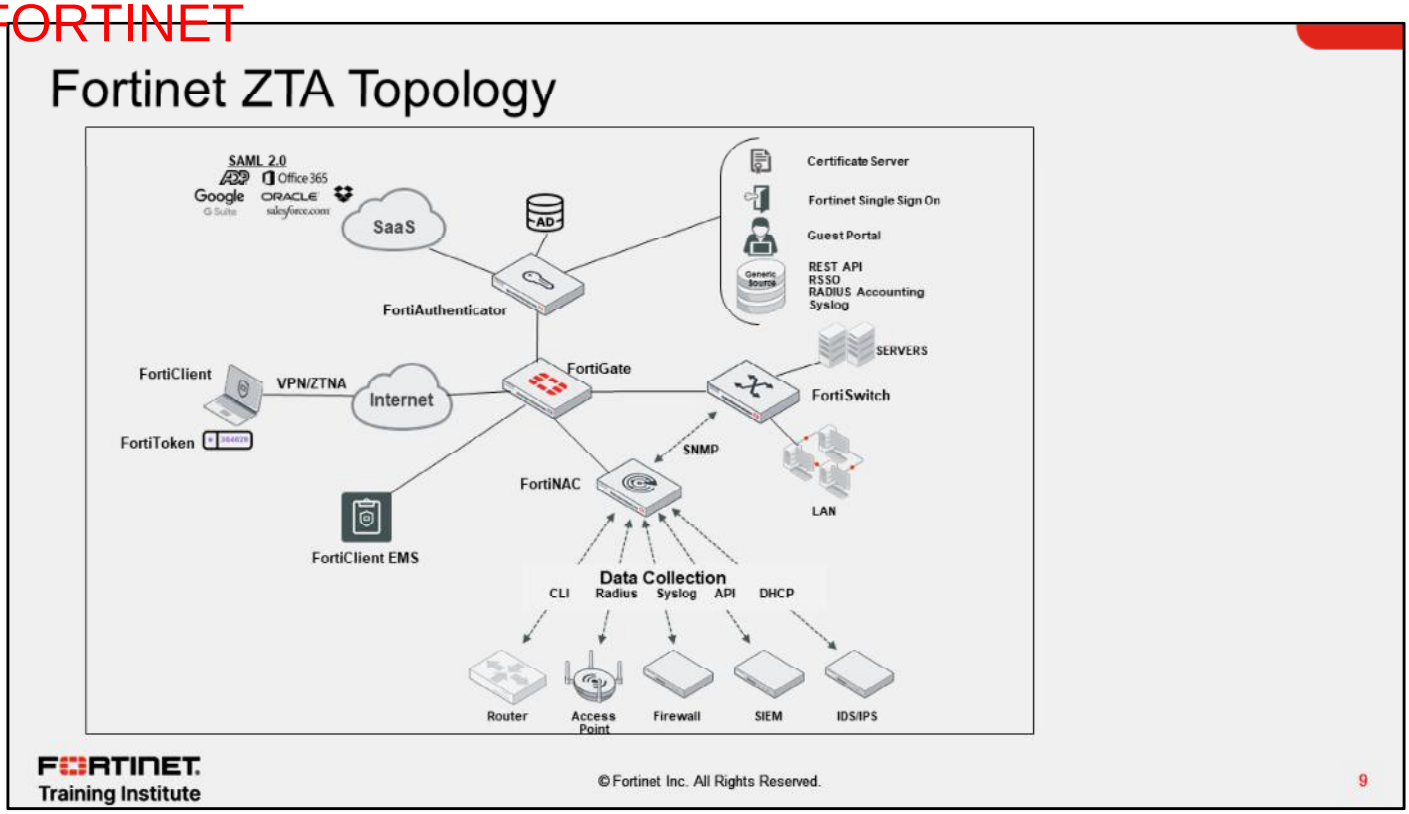
You can deploy FortiNAC as a physical device or as a virtual machine. FortiNAC communicates with infrastructure devices, such as wireless controllers, autonomous APs, switches, routers, and others. Because these infrastructure devices are inline, they can detect connected devices and connecting endpoints. They send this information back to FortiNAC, or FortiNAC gathers this information from them.

FortiNAC uses a variety of methods to communicate with and gather information from, the infrastructure:

- FortiNAC uses SNMP to discover the infrastructure, complete data collection, and perform ongoing management.
- SSH or Telnet through the CLI is commonly used to complete tasks related to the infrastructure. For example, FortiNAC can use SSH to connect to a device and issue commands to gather visibility information or execute control functions.
- FortiNAC can also use RADIUS across a wired or wireless connection, to gather visibility information and control access.
- FortiNAC uses syslog to stay up-to-date on visibility details, such as hosts going offline. Syslog can also provide security device integration, giving FortiNAC the ability to log and react, if configured to do so, when it receives a security alert.
- Depending on the vendor of the infrastructure device, FortiNAC may leverage available API capabilities to enhance visibility and enforce control.
- FortiNAC can use DHCP, typically through fingerprinting, to identify connected devices and gain enhanced visibility.

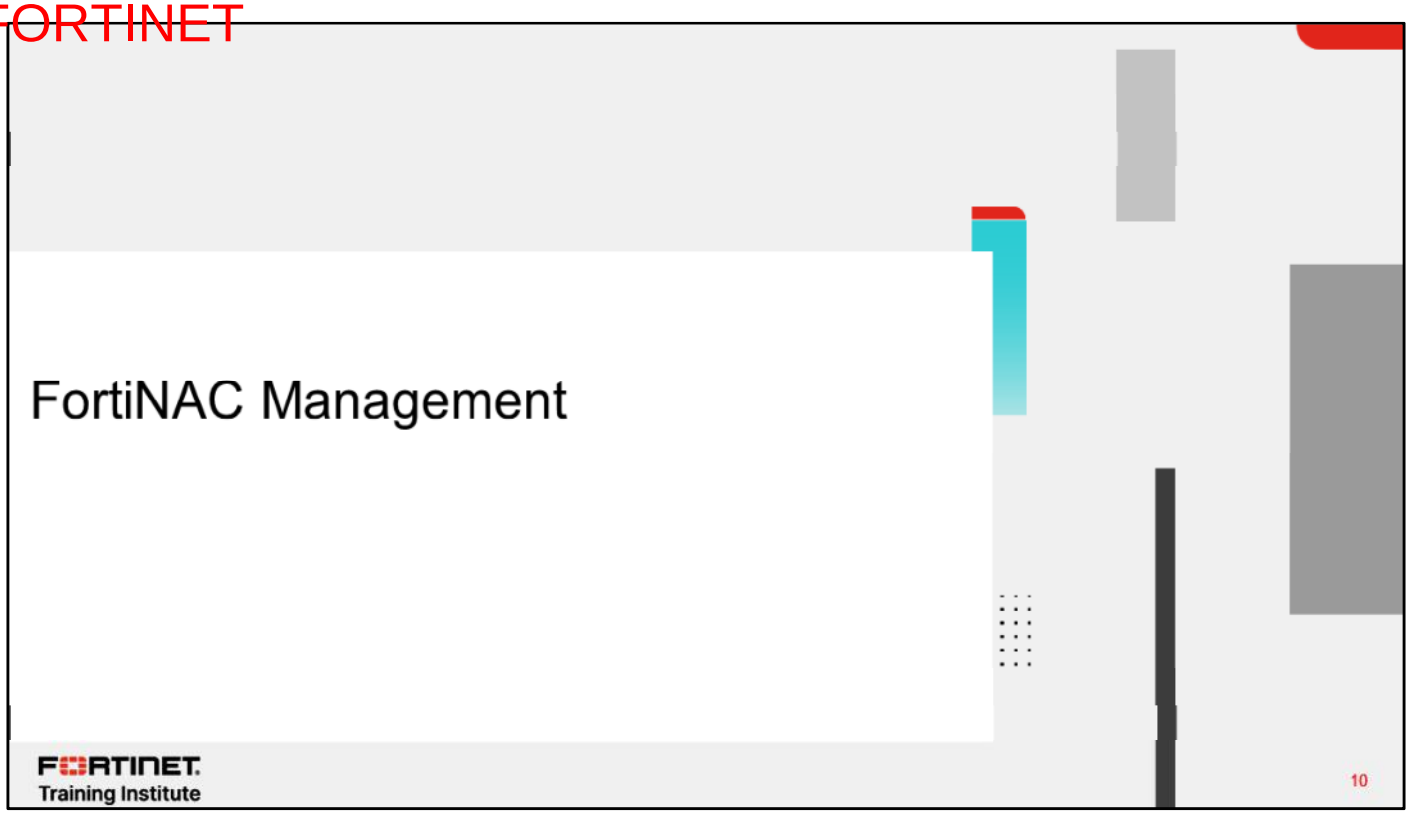
The communication methods that FortiNAC uses depend on the vendor and model of the infrastructure device that FortiNAC is trying to integrate with. After FortiNAC knows the type of device it is communicating with, it determines and uses the appropriate methods and commands to gather information and maintain control.

DO NOT REPRINT
© FORTINET



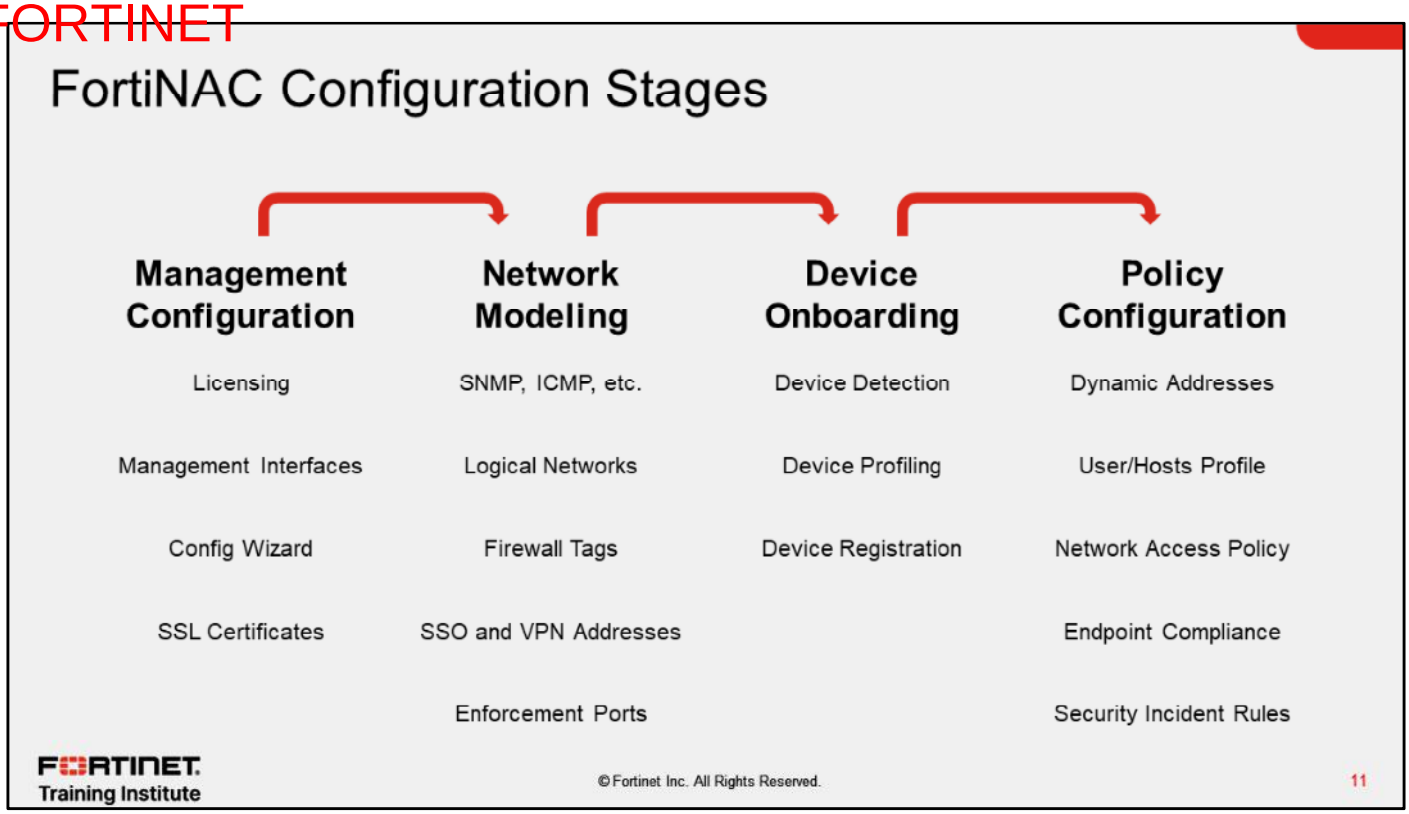
This slide shows how FortiNAC can be integrated into the ZTA architecture, along with the other ZTA components.

DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiNAC management configuration.

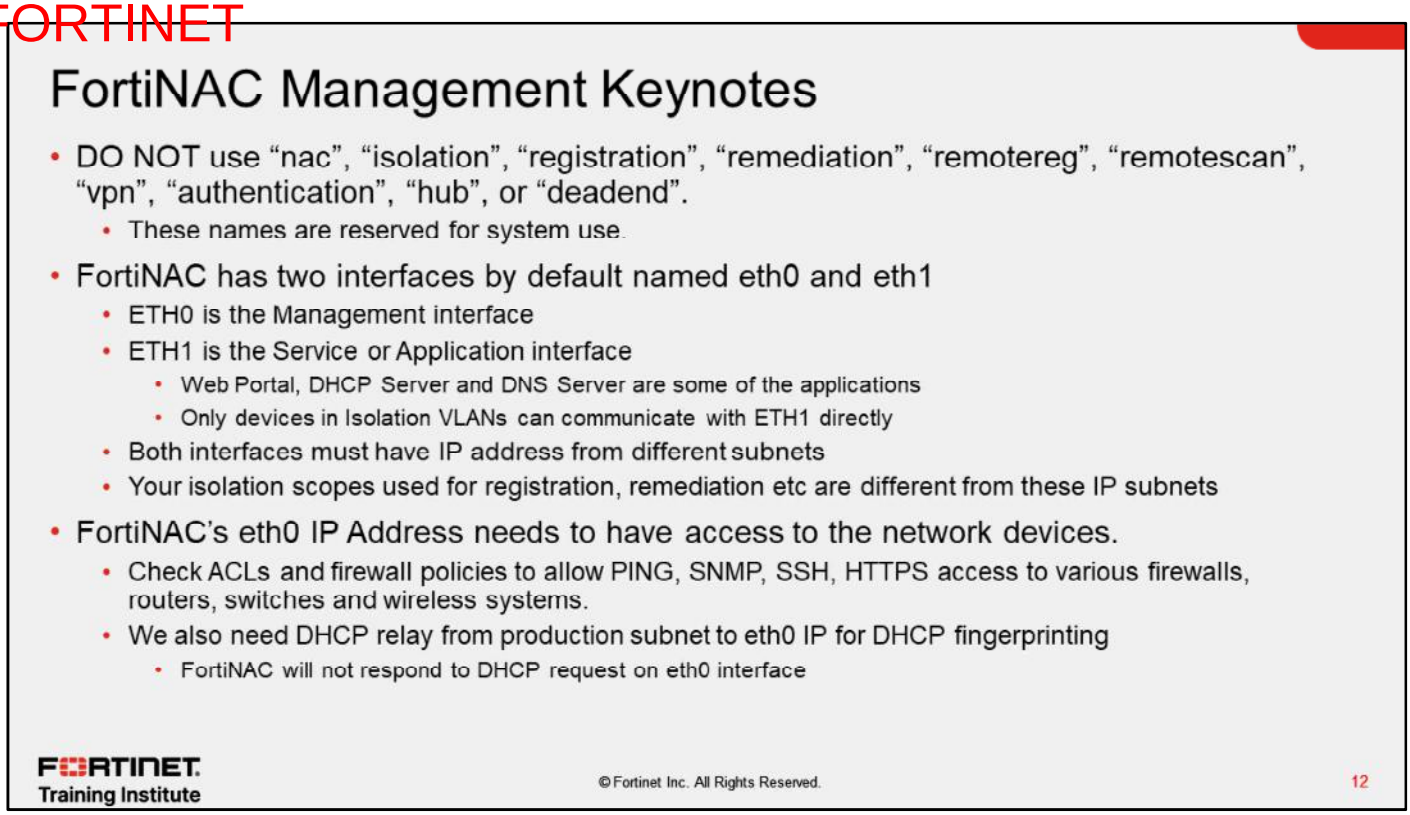
DO NOT REPRINT
© FORTINET



There are four key configuration stages in a FortiNAC deployment:

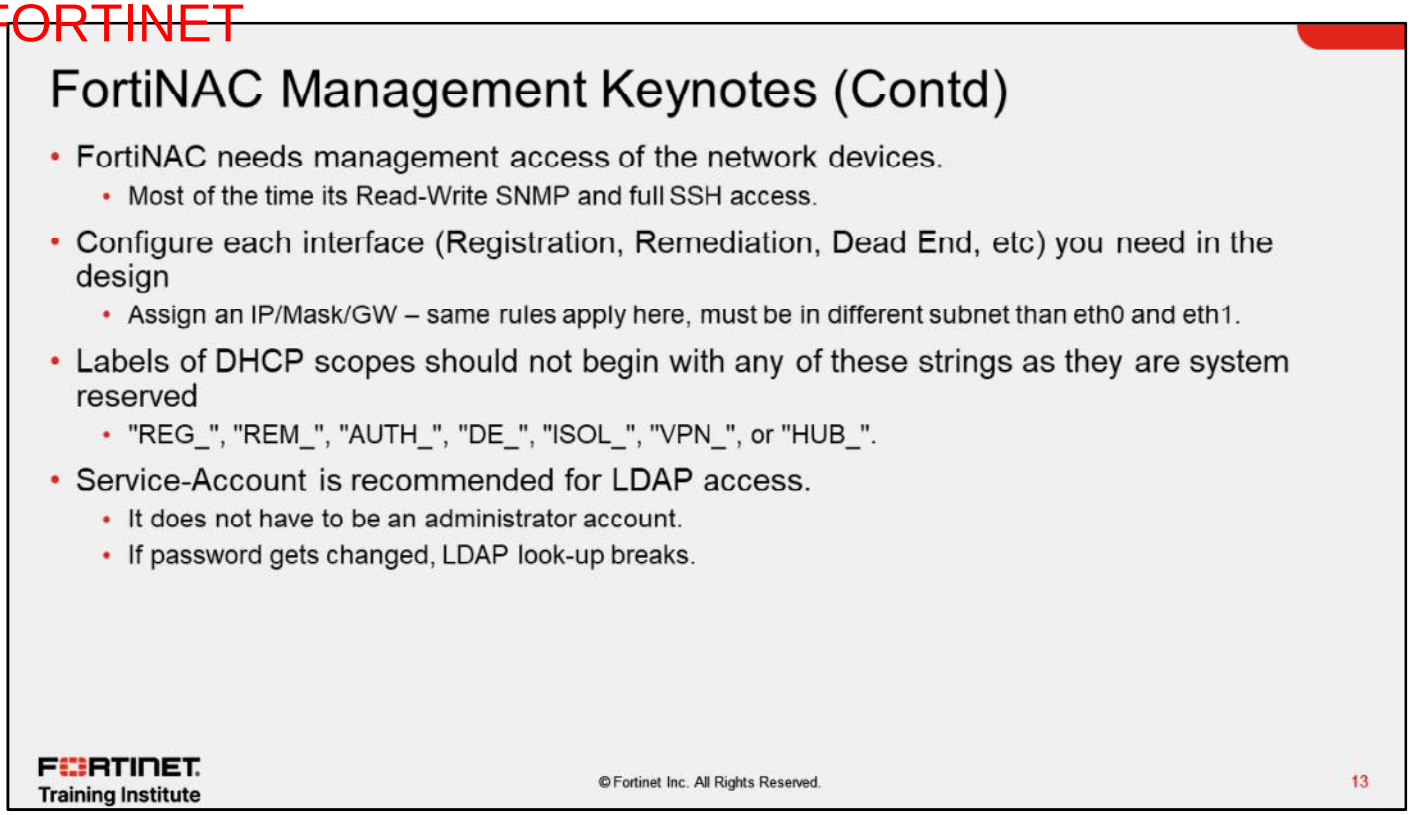
- Management configuration is where all the administrative tasks are carried out, like licensing, configuring management interfaces, uploading SSL certificates for agent communication, captive portal, and so on. The configuration wizard is used to define the FortiNAC captive networks.
- Network modeling is where you will add the devices for the endpoints to be connected, for example, FortiGate, FortiSwitch, FortiAP. To model devices, FortiNAC requires SNMP and ICMP connectivity to these devices.
- Device onboarding is where devices are detected and profiled, for example, corporate device, BYOD, IoT. After the device is detected and profiled, the device is registered and provided with different access levels based on policy configuration.
- Policy configuration decides the different access levels that can be provided to a device, based on device profiles, endpoint compliance, and so on.

DO NOT REPRINT
© FORTINET



This slide shows some of the key points you should remember while configuring FortiNAC.

DO NOT REPRINT
© FORTINET



This slide shows some more key points related to FortiNAC configuration.

DO NOT REPRINT
© FORTINET

FortiNAC SSL Certificates

- FortiNAC can use SSL certificates issued by either an internal private or public (external) Certificate Authority (CA).
- FortiNAC may require multiple SSL certificates depending functions in use

Component	Function	Certificate to use
Administration UI	Access to the FortiNAC UI	Internal or External
Persistent Agent	Persistent Agent communication	Internal or External
Captive Portal	Captive Portal access and Dissolvable Agent communication	External
Local RADIUS Server (EAP)	For use when FortiNAC is acting as the 802.1x EAP termination point.	Internal or External (avoid wildcard certificates)
RADIUS Endpoint Trust	Client-side certificate validation (EAP-TLS)	Internal or External (avoid wildcard certificates)

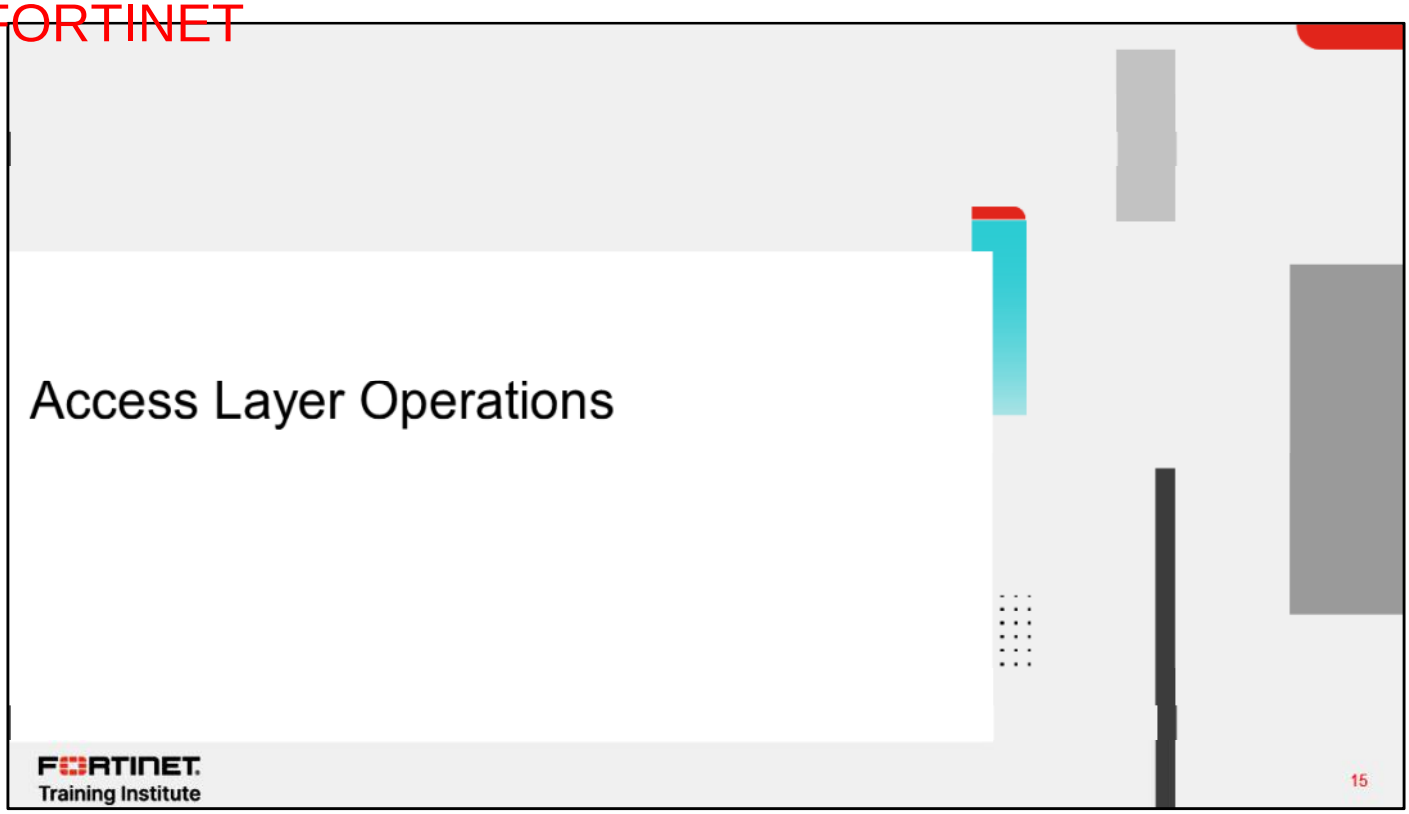
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

Depending on the SSL function, you can use an SSL certificate signed by a public or private CA on FortiNAC. This slide shows when different CA's can be used on the FortiNAC. For FortiNAC administration interface and persistent agent, you can use an SSL certificate issued by a private or public CA. FortiNAC administration interface is usually accessed through corporate devices, and the certificates can be easily managed. The SSL certificate used for the persistent agent is also easy to manage as they are usually deployed on managed devices. Using SSL certificates signed by a public CA for the captive portal is recommended to avoid certificate errors, because it will be mostly unmanaged guest devices that will be accessing the network. For EAP and EAP-TLS it is recommended to use certificates with subject alternate name (SAN) and avoid wildcard certificates.

DO NOT REPRINT
© FORTINET

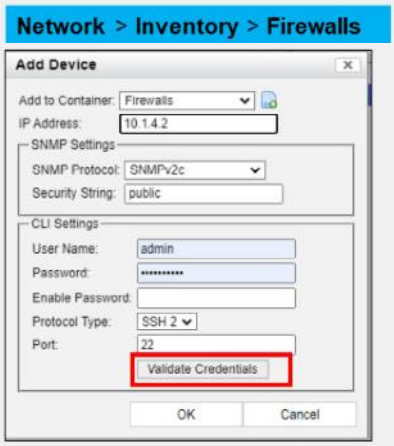


In this section, you will review the FortiNAC access layer operations.

DO NOT REPRINT
© FORTINET

Network Modeling

- FortiNAC has the following prerequisites for network modeling:
  - ICMP or PING connectivity to device to add to device inventory
  - SNMP and CLI read-write access for carrying out remote tasks
    - Manual Polling-Troubleshooting
    - Scheduled tasks-Slow detection
    - Link traps-Standard detection
- Always click **Validate Credentials**, before adding device to device inventory on FortiNAC
- FortiGate requires the following configured to be added into the FortiNAC device inventory:
  - PING, SNMP, HTTPS, and SSH enabled on management interface
  - FortiNAC added as an SNMP host



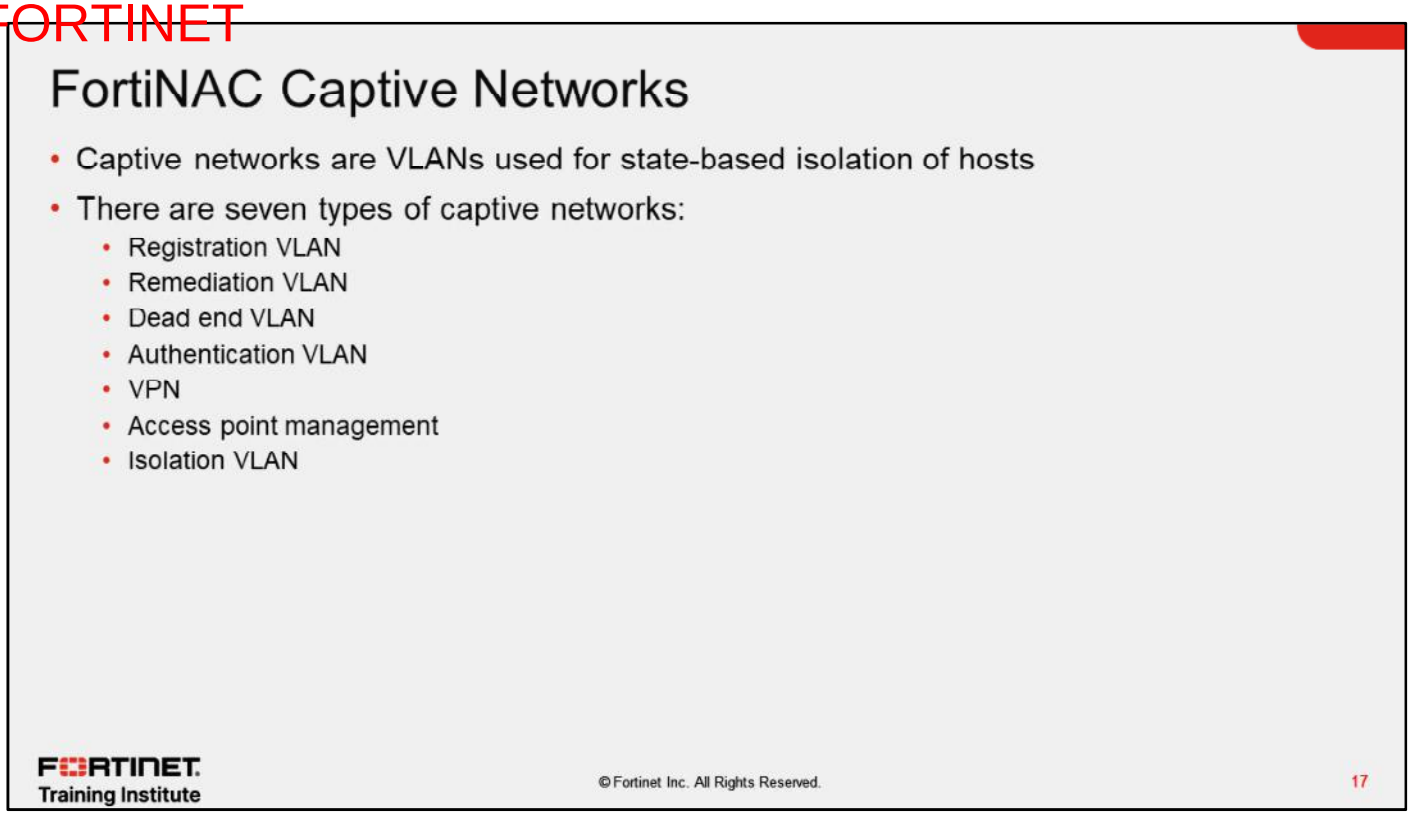
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

For network modeling, you need to add devices that the endpoints connect to the FortiNAC device inventory. FortiNAC requires ICMP or PING connectivity to the device that needs to be added. To carry out remote tasks like manual polling, scheduled tasks, and link traps, FortiNAC almost always needs SNMP and CLI read-write access to the device. When you add devices to the device inventory, always click **Validate Credentials** to confirm that SNMP and CLI connectivity is established to the device. Ensure that PING, SNMP, HTTPS, and SSH are enabled on the FortiGate management interface, and that FortiNAC is added as an SNMP host to be added to the FortiNAC device inventory. Ensure authentication and privacy protocol matches, if using SNMPv3.

DO NOT REPRINT
© FORTINET



FortiNAC captive networks are those networks used for the isolation of hosts, and the presentation of captive portals. There are seven types of captive networks:
• Registration VLAN is used to isolate unregistered rogue devices.
• Remediation VLAN is used to quarantine devices that failed endpoint compliance.
• Disabled hosts are placed in dead end VLAN.
• Authentication VLAN is used to isolate registered clients from the production network during user authentication.
• Virtual private network (VPN) is used for clients who connect to the network through VPN services.
• Access point management is used for clients that connect through devices managed by access point management.
• Isolation VLAN uses the state of the client and redirects them to the appropriate isolation web pages. If you use this VLAN type, the configuration of the other VLAN types are optional.

DO NOT REPRINT
© FORTINET

Logic to Determine Isolation

If Host State is	And System Group Membership is	Then Change VLAN to	Icon
Disabled	Physical Address Filtering (Device)	Dead End	
At-Risk	Forced Remediation (Port)	Quarantine	
Rogue	Forced Registration (Port)	Registration	
Not Authenticated	Forced Authentication (Port)	Authentication	
All	N/A	Shared Media	N/A
All Except Normal	N/A	Isolation	N/A
Normal	N/A	Policy Based or Default	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

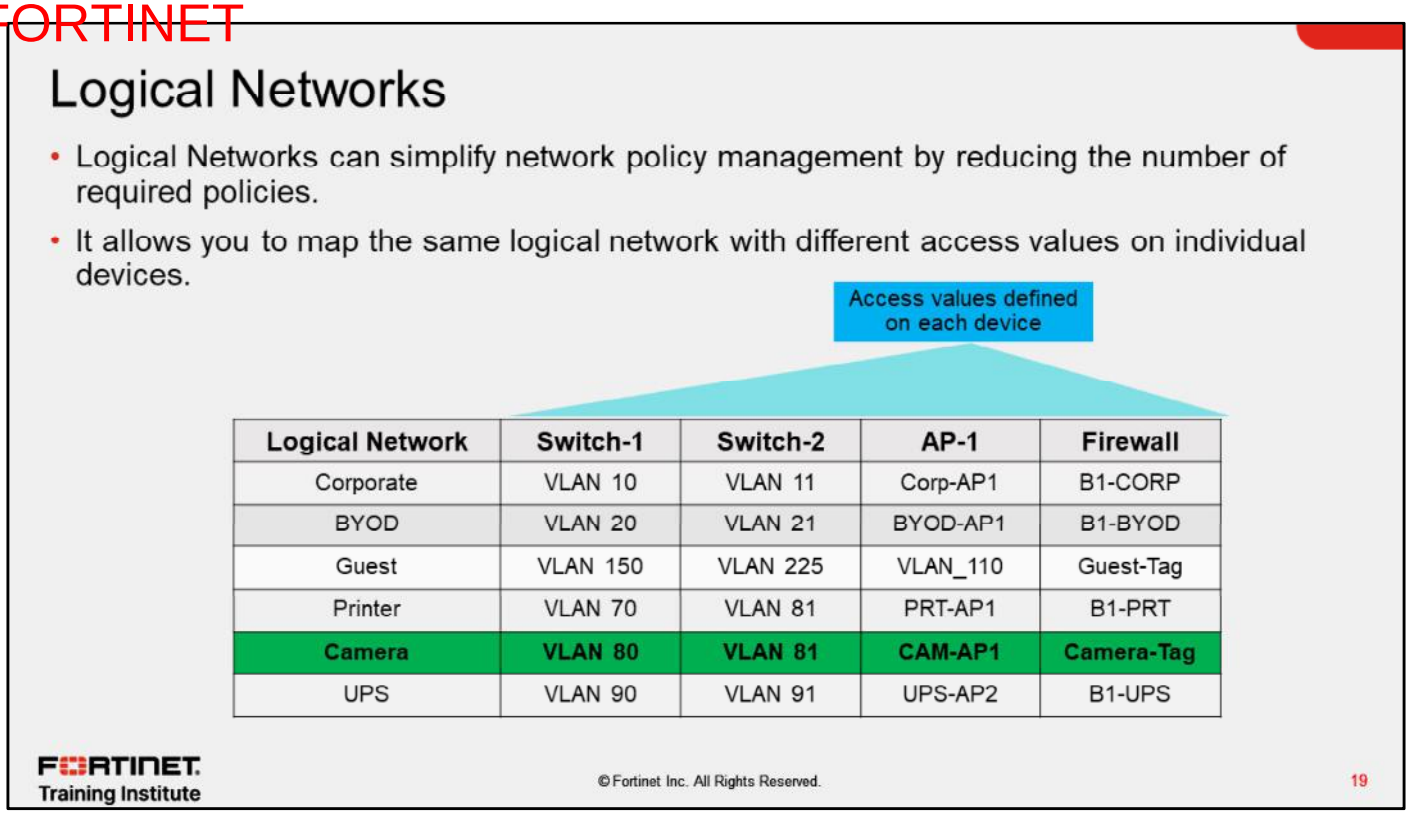
18

The logic used by FortiNAC when making the decision to isolate a host is summarized on this slide. When an endpoint connects to the network, FortiNAC looks it up in the database to determine its state. If the host does not exist in the database, and it does not match any enabled device profiling rules, it will be added and assigned the state of rogue. FortiNAC uses the **If Host State is** column as the column to key on, starting at the top and working down. For example, if a host with a state of Rogue connects to the network, FortiNAC uses the third row down to determine if isolation is necessary. After the appropriate row is identified, FortiNAC reads from left to the right, applying AND logic between the **If Host State is** and **And System Group Membership is** columns. If both columns in the same row, are true, then FortiNAC moves the host to the captive network shown in the **Then Change VLAN to** column. On the GUI, the host is represented by the icon shown in the associated row of the **Icon** column.

For example, if a host with the state of Rogue connects to a port in the **Forced Registration** port group, FortiNAC will isolate that host by moving it into the **Registration** captive network. The top four rows all function in the same way, with the slight exception of the first row, where the location parameter is defined by a device group, not a port group.

The bottom three rows consist of two special captive networks, and a row where hosts with a state of normal are provisioned.

DO NOT REPRINT
© FORTINET



This slide shows an example of how logical networks can be used.

In the example, six network access policies have been developed to support the required endpoint-based segmentation on four infrastructure devices.

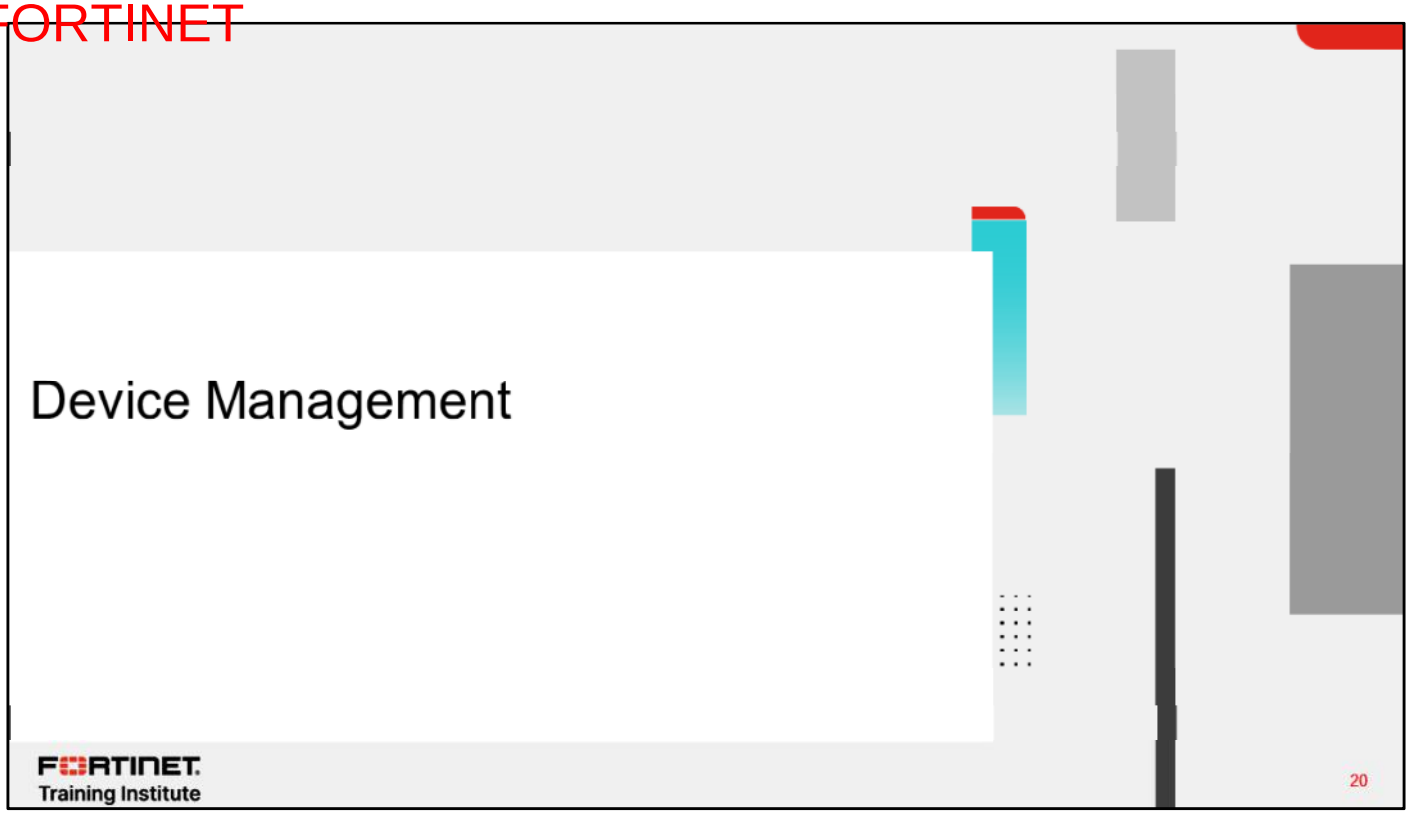
As you can see, a device identified as a camera and assigned to the logical network **Camera** is provisioned to **VLAN 80**, if it connects to **Switch-1**; is provisioned to **VLAN 81**, if it connects to **Switch-2**; and so on. The values designated in the **AP-1** column are access values that may be vendor specific, depending on the vendor of the wireless access point (AP) or controller. These values could also be VLAN names, groups, roles, interfaces names, and so on.

The **Firewall** column could represent a firewall tag that would result in the camera matching a specific firewall policy.

You can use logical networks to greatly decrease the number of network access policies, resulting in simplified policy creation and management.

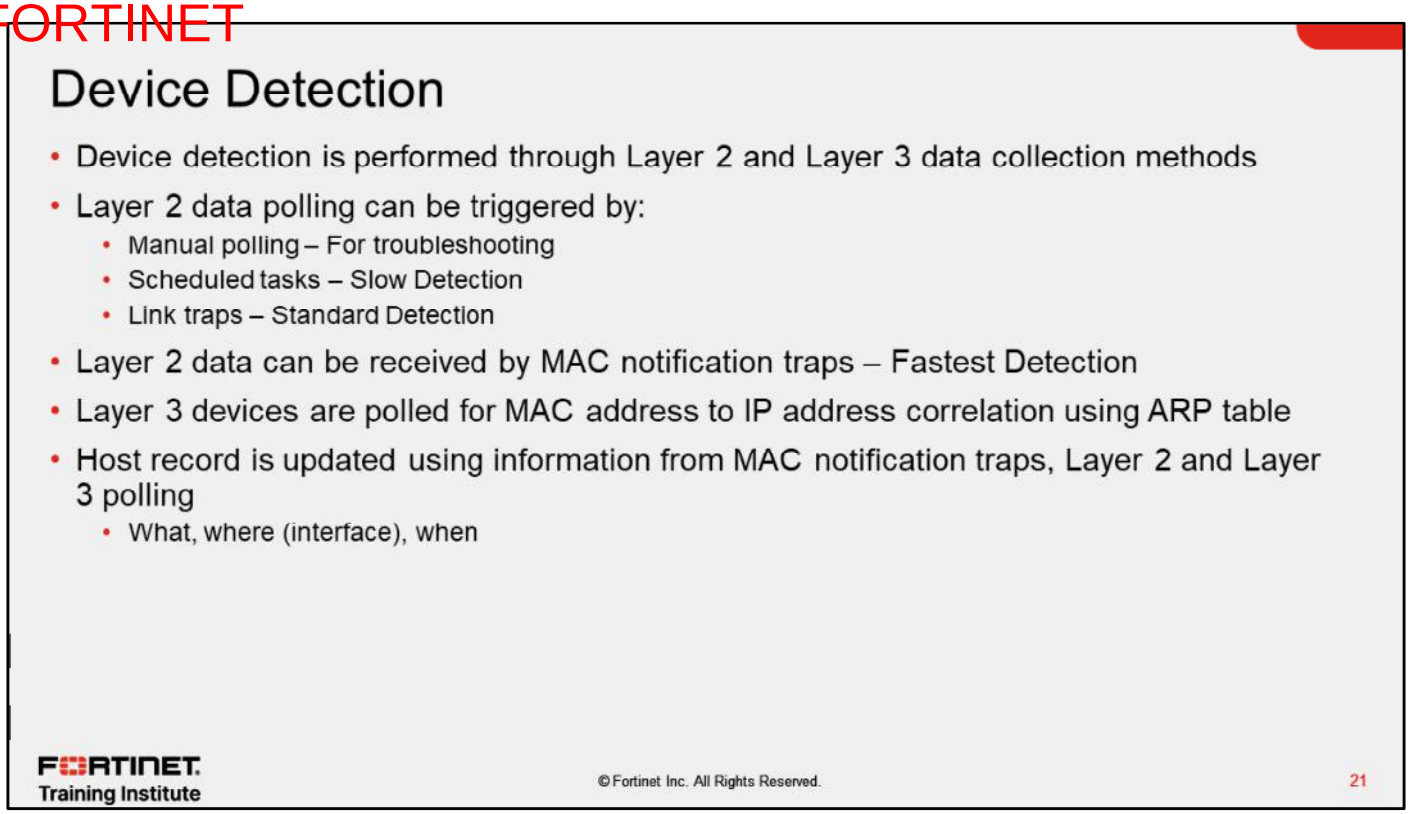
These same network access policies work for small, medium, or large environments.

DO NOT REPRINT
© FORTINET



In this section, you will learn about device management on FortiNAC.

DO NOT REPRINT
© FORTINET



Device detection is performed by FortiNAC to determine what devices are connected to the network using Layer 2 and Layer 3 data polling methods.

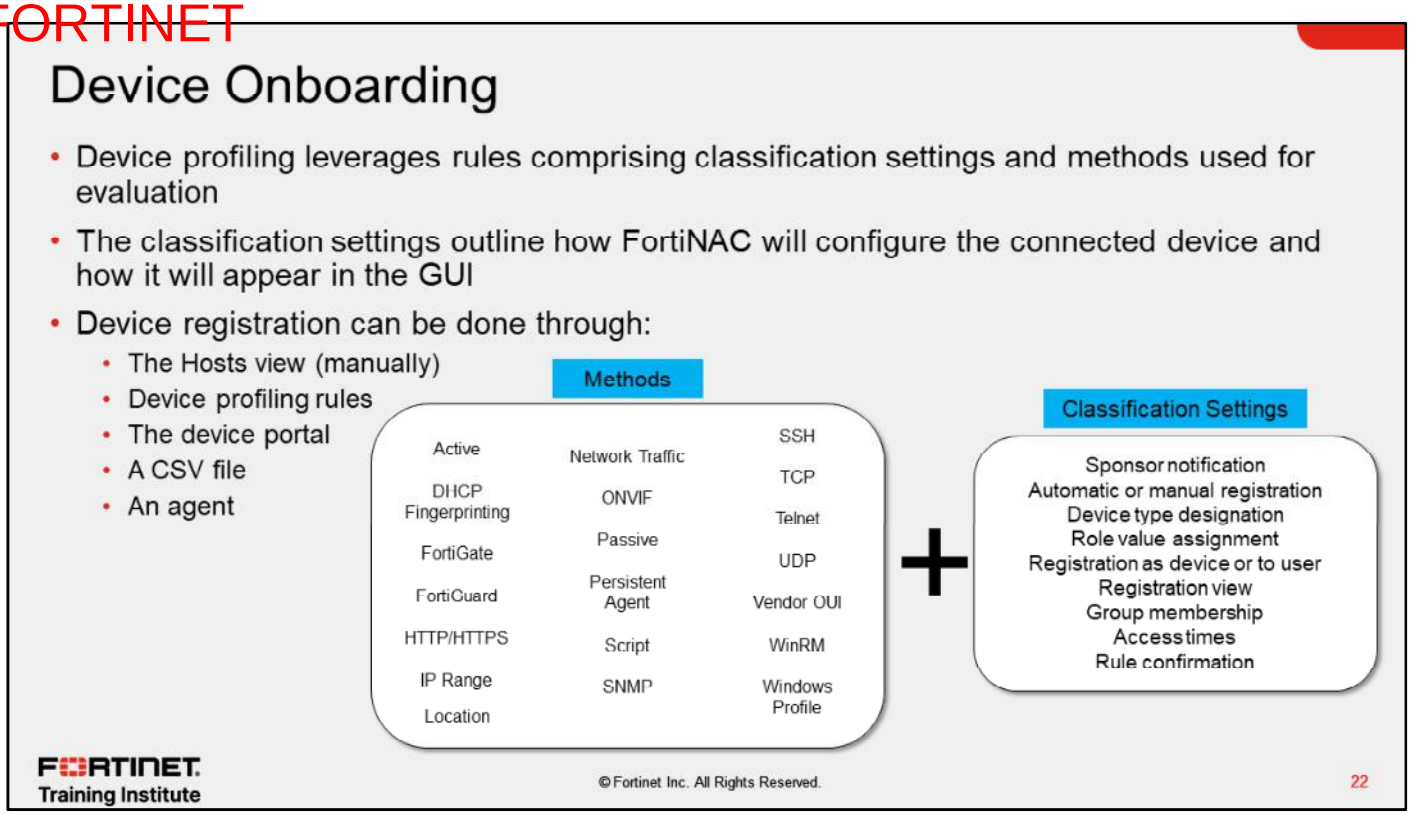
The three ways that Layer 2 polling is triggered are:

- Manual polling: Manual polling is initiated when an administrative user right-clicks the device in the topology tree and selects **Poll for L2 (Hosts) Info**, or clicks **Network** > **L2 Polling**.
- Scheduled: Layer 2 polling is scheduled in the **Network** > **L2 Polling** view. You can change the default scheduled intervals.
- Link traps: Link traps received from an edge device trigger FortiNAC to perform a Layer 2 poll to update its awareness of devices that are connected on that edge device. The traps that trigger the poll are: Linkup, Linkdown, WarmStart, and ColdStart. This trigger keeps FortiNAC up-to-date in real time as devices connect to and disconnect from edge devices.

Layer 3 IP address information is a critical piece of network visibility and is a necessary component for some FortiNAC capabilities. Layer 3 devices are polled for MAC address to IP address correlation using the ARP table.

With the information collected from Layer 2 and Layer 3 data polling, a host record is populated on FortiNAC with the device MAC and IP address (what), switch port the device is connected to (when), and the time it connected (when).

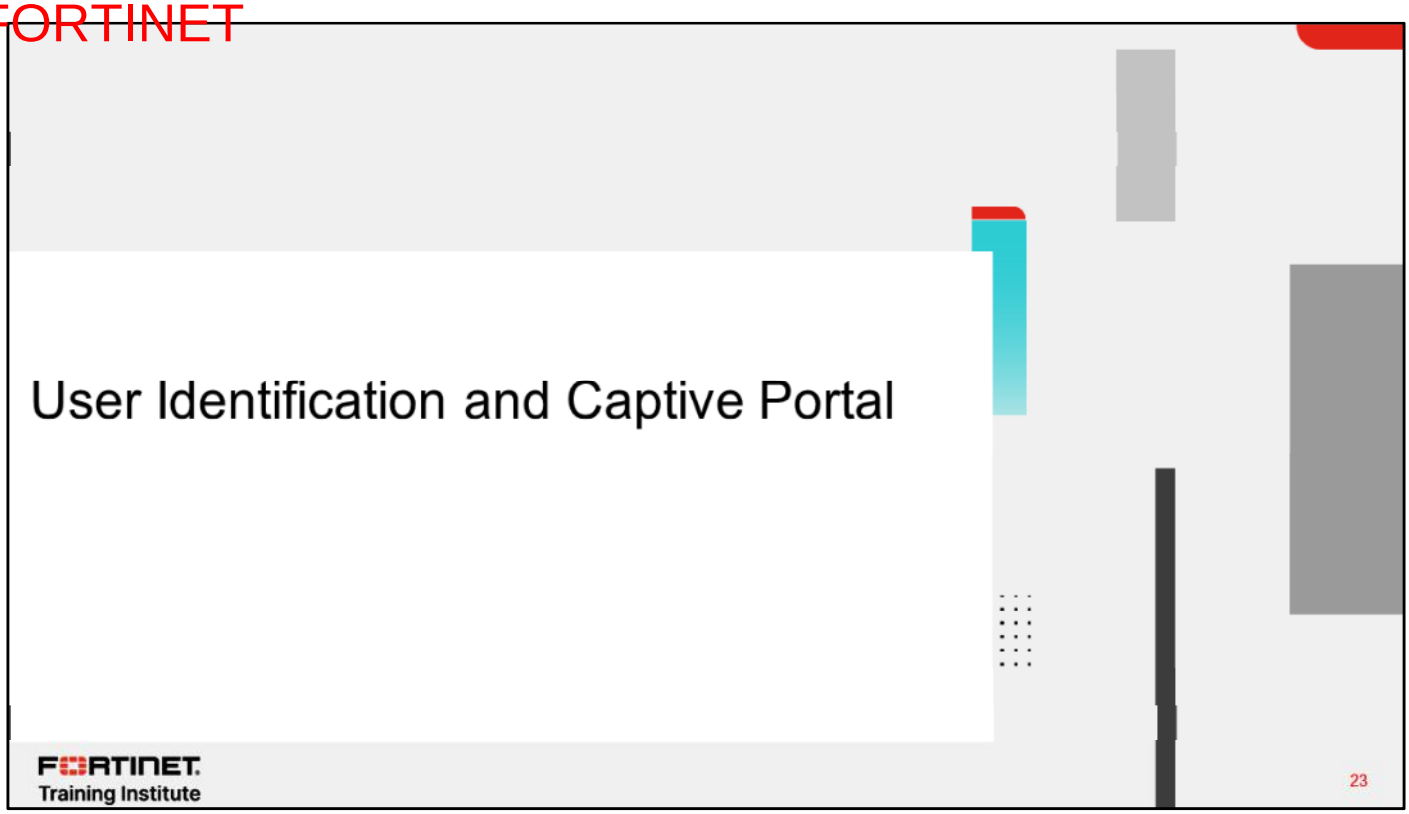
DO NOT REPRINT
© FORTINET



The methods shown on this slide are used to evaluate connected rogue devices. If more than one method is selected, the selected methods are logically added when determining if the rule is matched. Match criteria are configured for each method, because the methods are selected.

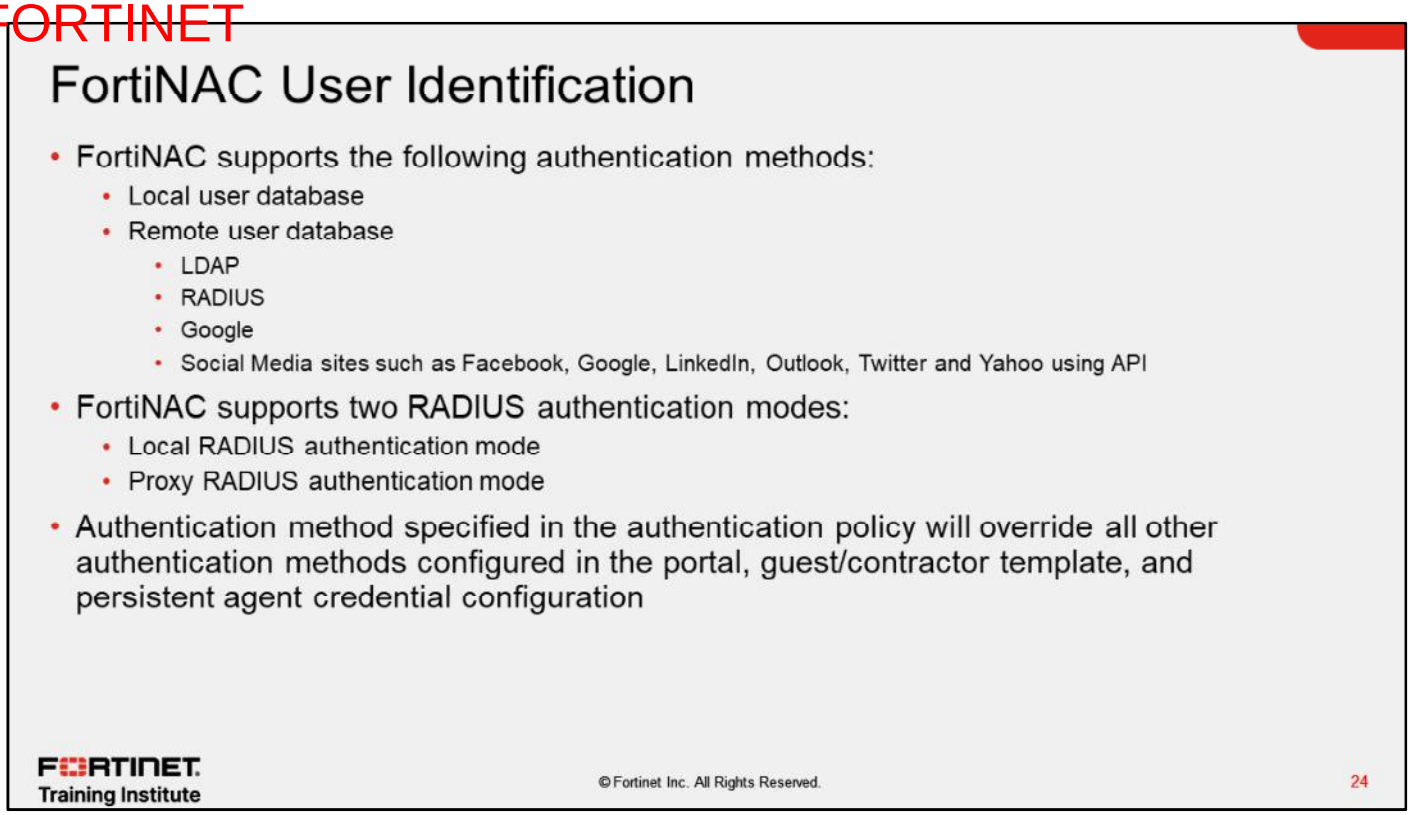
The classification settings outline how FortiNAC will configure the connected device and how it will appear in the GUI. You can leverage the device type, role, and group membership for policy enforcement. You can use access availability settings to grant networks access during specific days and times, and the **Rule Confirmation** option to revalidate previously profiled devices.

DO NOT REPRINT
© FORTINET



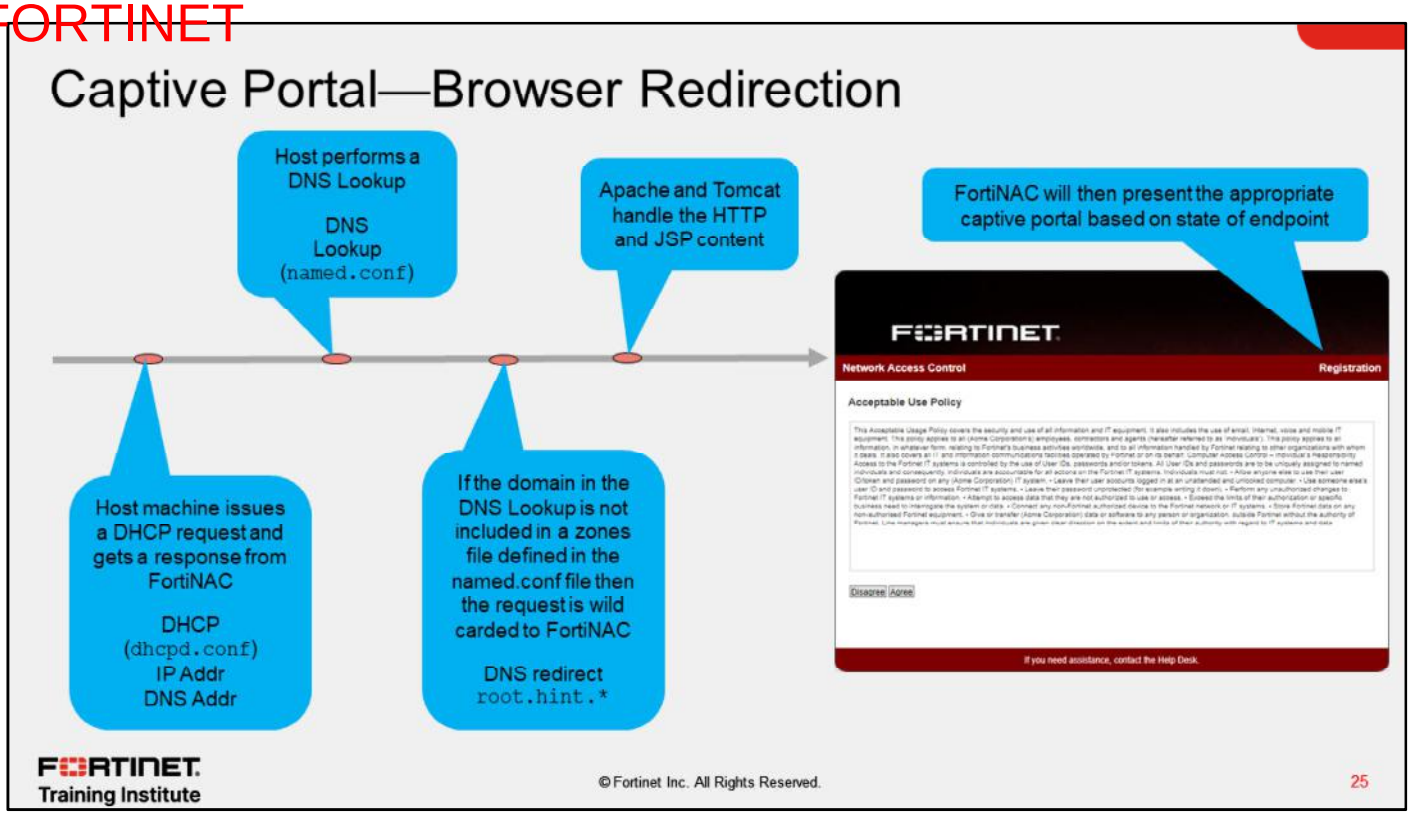
In this section, you will learn about user identification and the captive portal on FortiNAC.

DO NOT REPRINT
© FORTINET



To identify the user information, FortiNAC has an authentication VLAN for user self registration. The users can be authenticated using either a local user database on FortiNAC or remote user databases like LDAP, RADIUS, Google, and social media sites integrations using API. FortiNAC supports two RADIUS authentication methods—local RADIUS and proxy RADIUS. Local service has all the components needed to manage RADIUS connections MAB, EAP-TLS, and PEAP within FortiNAC. The proxy can be used for MAC address bypass without any need to proxy requests, and it will proxy EAP requests to another RADIUS server, for example, Microsoft NPS, FortiAuthenticator, and so on. Traditional RADIUS authentication ports—1812 or 1645—can be defined on either service, but you cannot assign the same port number to proxy and local service simultaneously. The authentication method specified in the authentication policy will override all other authentication methods configured in the portal, on the guest or contractor template, and persistent agent credential configuration.

DO NOT REPRINT
© FORTINET



When hosts have been assigned to a captive network, they will be directed to a captive portal page. The page presents the user with additional information and/or capabilities, to resolve the non-normal host state. For example, a rogue host isolated to the registration captive network will be presented, by default, with a registration page that provides options for onboarding the host. The onboarding process will classify the host.

When a host is isolated on a wired port, FortiNAC will shut down the port causing the host's link to drop, the VLAN to change, and the port to be re-enabled. This will result in the host requesting a new IP address, which begins the captive portal page presentation process. This process is shown on the slide as a timeline going from left to right.

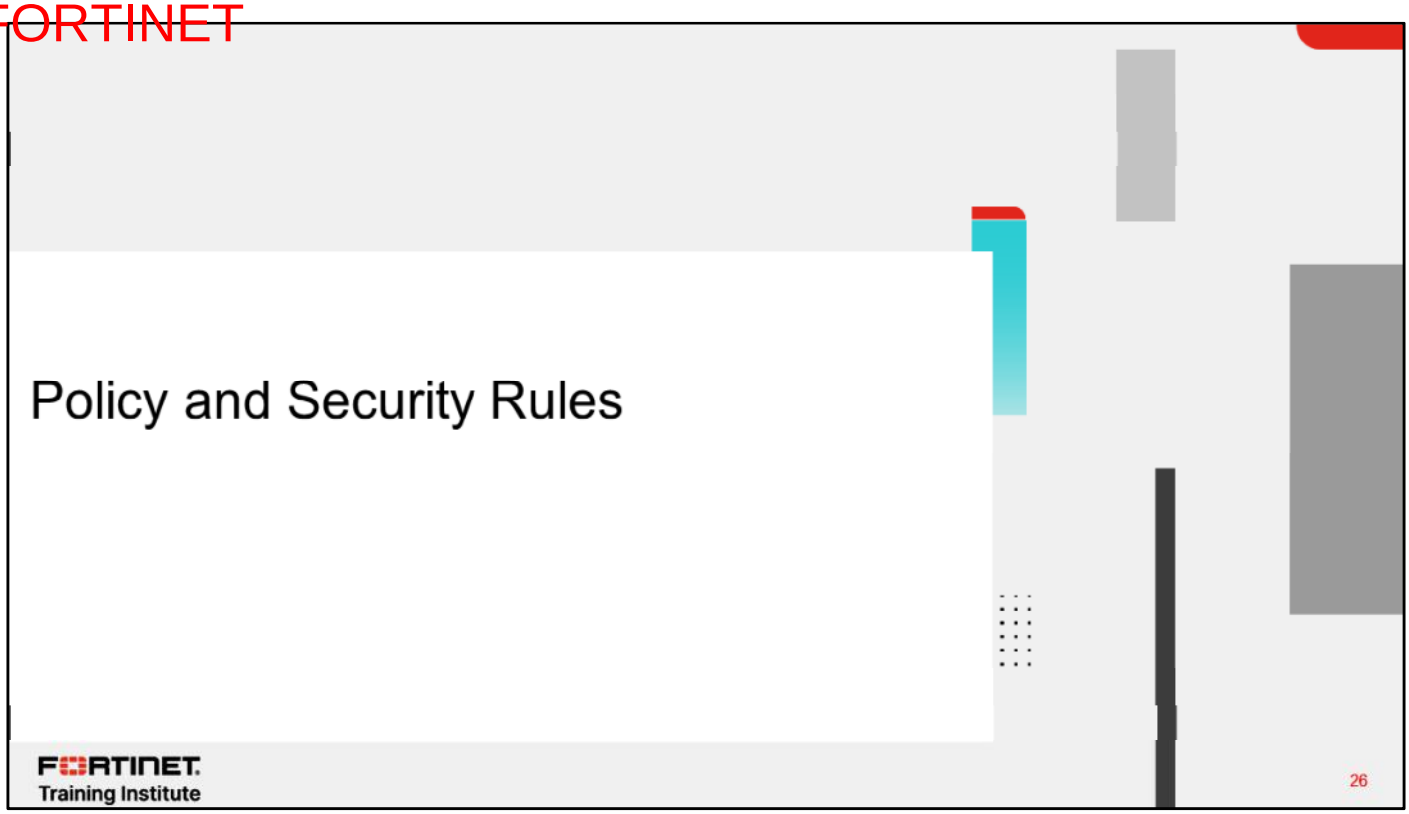
First, the host gets a new IP address appropriate for the captive network it is in, with a DNS address that is the FortiNAC captive portal interface.

When the host attempts to resolve a domain by name, FortiNAC, which has been designated as the DNS server, will respond with its own address, masquerading as the domain the host is attempting to resolve. This is the result of special `root.hint` files on FortiNAC.

FortiNAC will then present the appropriate captive portal page to the isolated host.

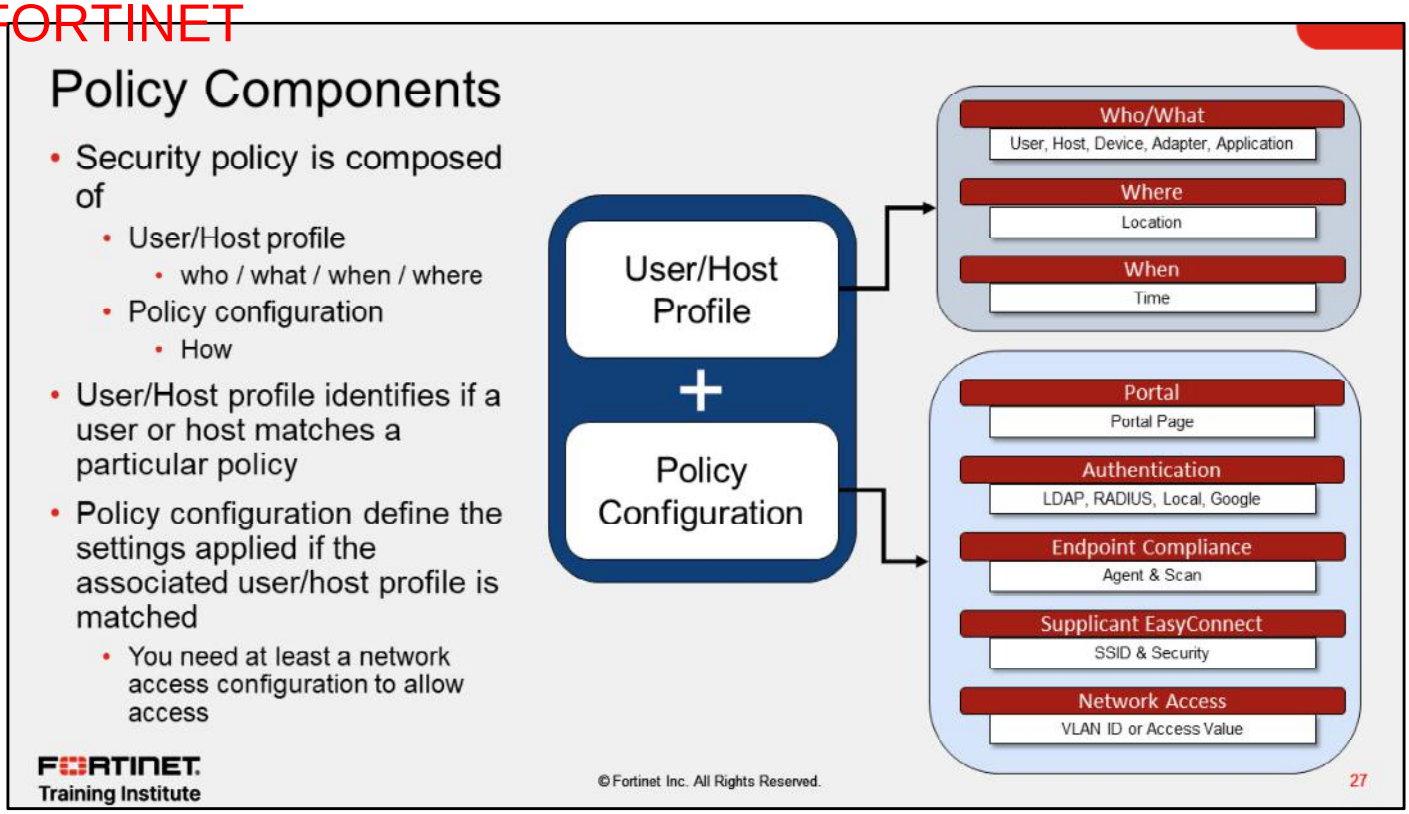
Note that there are ways to allow specific sites to resolve correctly.

DO NOT REPRINT
© FORTINET



In this section, you will review policy and security rules on FortiNAC.

DO NOT REPRINT
© FORTINET



A security policy is composed of two different pieces. The first is the user/host profile, which is the piece that identifies if a user or host matches a particular policy. The second piece is the configuration, which is the policy-specific settings applied if the associated user/host profile is matched.

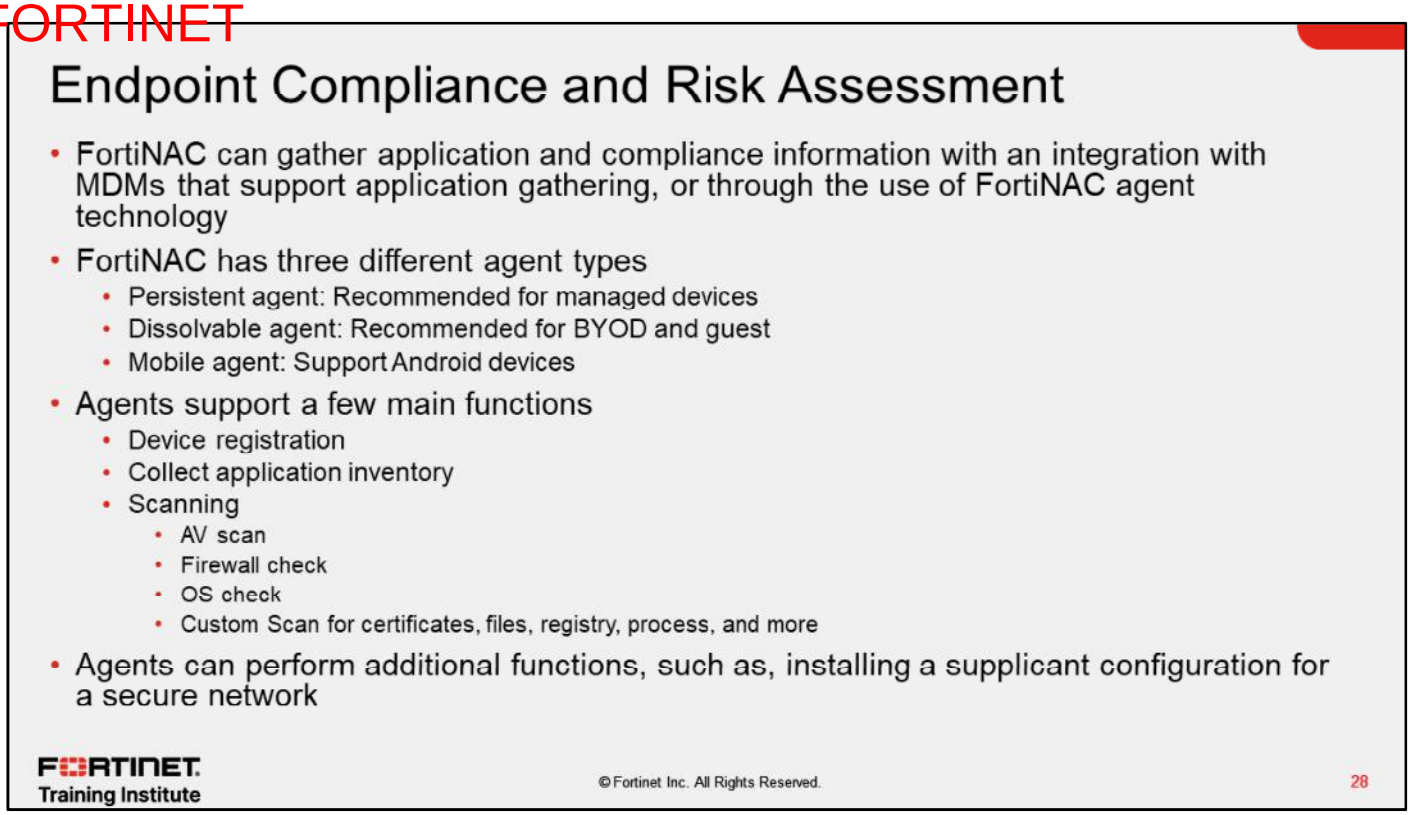
User/host profiles are a set of FortiNAC visibility parameters—the who, what, where, and when information. These profiles can range from general to very specific, keying upon individual attributes, and applying AND, OR, and NOT logic.

You can associate five different types configurations with a user/host profile:
- Portal
- Authentication
- Network access
- Endpoint compliance
- Supplicant EasyConnect

Hosts and users are continuously evaluated to identify if a user/host profile matches. Whenever FortiNAC identifies a match, the highest ranked security policy of each type, if any, are applied.

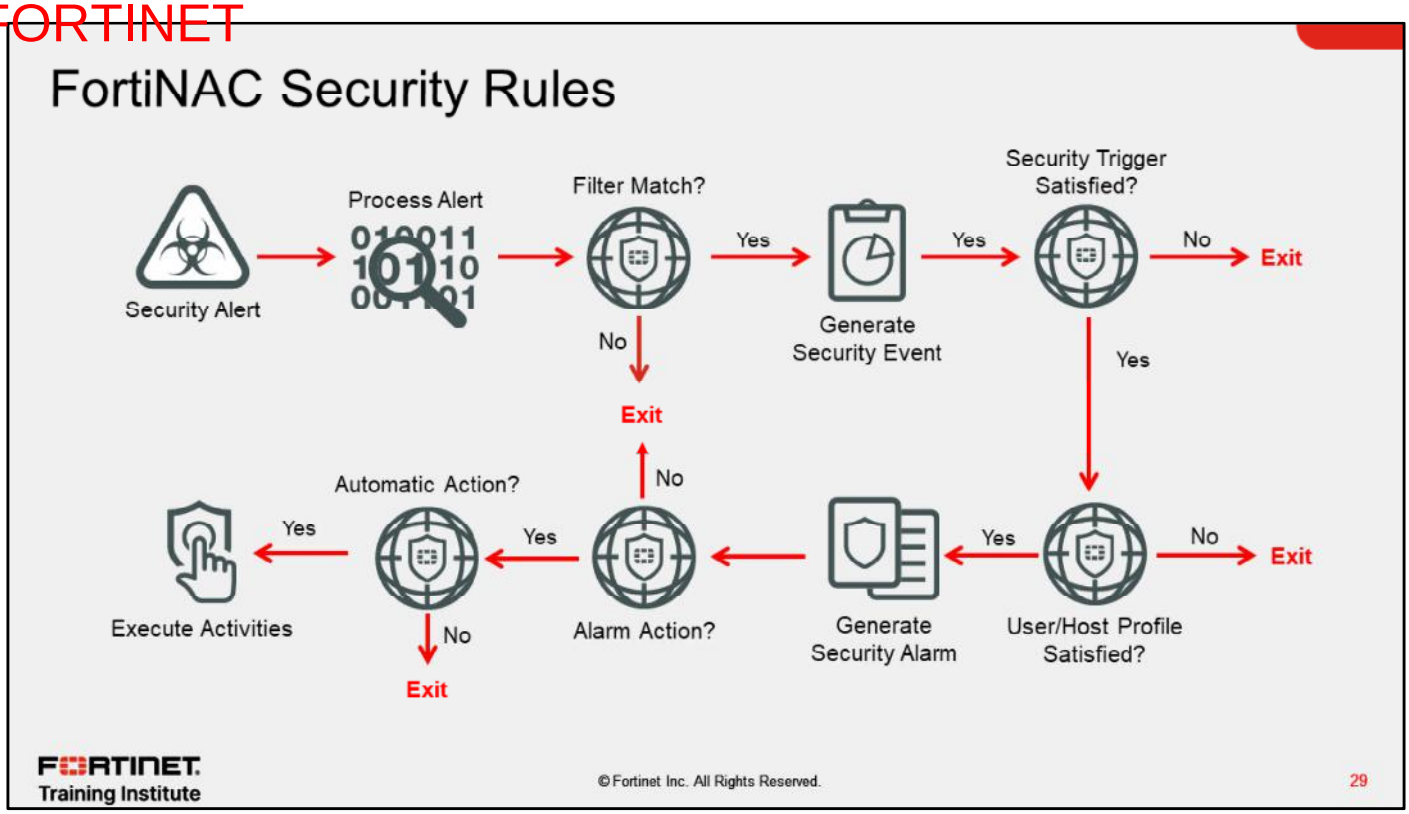
For example, if a user matches a user/host profile that identifies guest users, and that user/host profile is associated with a network access configuration, the configuration settings are applied, provisioning the access appropriately.

DO NOT REPRINT
© FORTINET



For endpoint compliance and application gathering, you can either use the FortiNAC agent or with integration of a mobile device management (MDM) system like FortiClient EMS. FortiNAC has three different types of endpoint agents. The persistent agent is installed on managed devices and stays resident on the endpoint. The dissolvable agent is a run once agent and requires manual end-user interaction within the captive portal. Once it completes and reports its results, it dissolves and leaves no footprint on the endpoint. This is a common choice for guests, contractors, or BYOD devices. The mobile agent is installed manually within the captive portal during the onboarding process and is the only agent option for Android devices. FortiNAC agents help you register the device on the network, gather application inventory, and do endpoint scans and compliance checks. All this information collected from the endpoint helps to determine the level of network access the user should be granted.

DO NOT REPRINT
© FORTINET



Understanding the terminology used, and a fairly detailed explanation of the process, goes a long way in understanding how the FortiNAC security rules work, and simplifies their development.

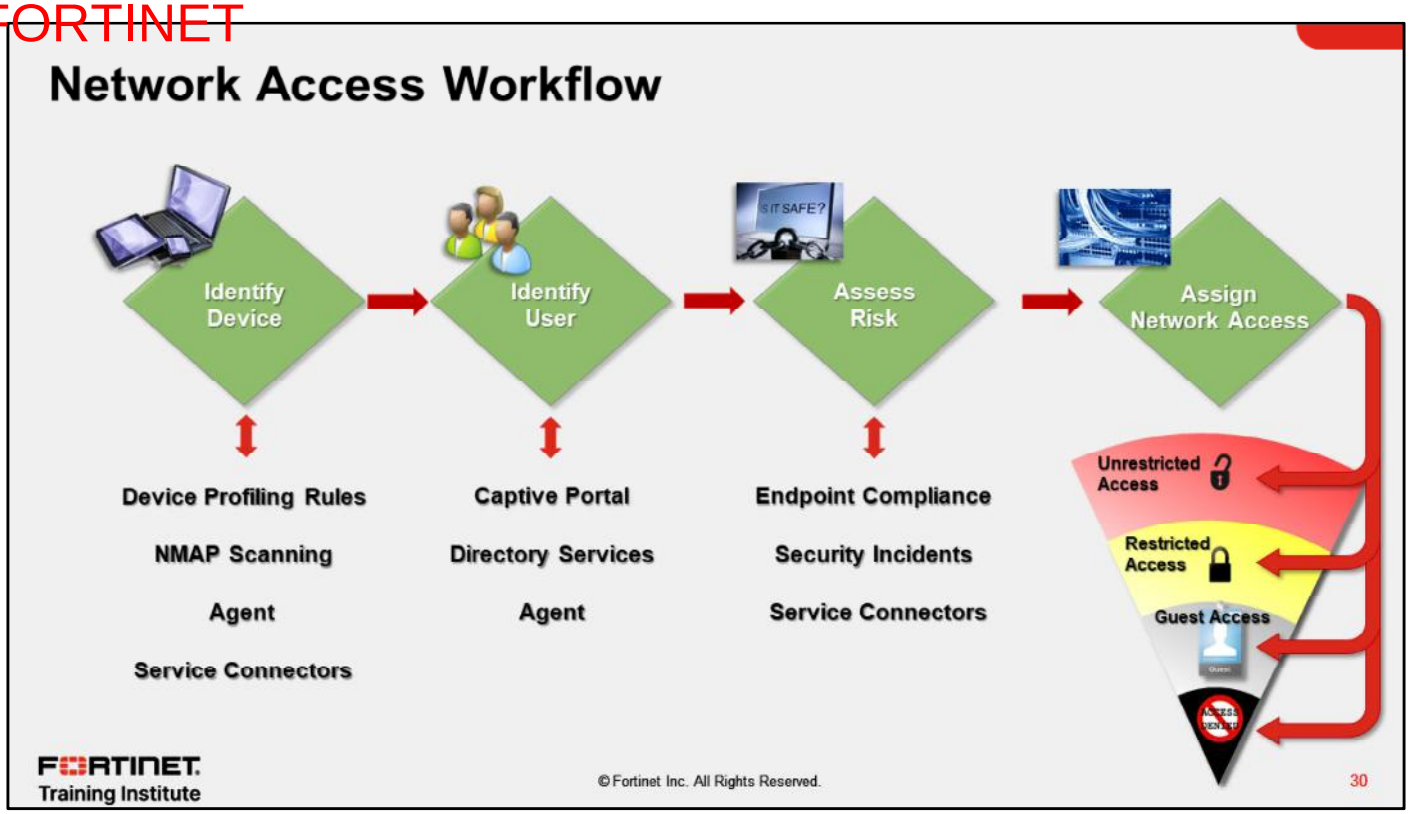
Starting with the top row in the example shown on this slide, and reading left to right, the process begins with the receipt of a security alert. A security alert is the syslog message received from an integrated security device. The alert is processed by FortiNAC, which means that the message contents are parsed and each component evaluated. The contents are then compared to all existing filters.

A filter is a user-created set of criteria. For example, a filter could simply look at the contents of column 35 of the parsed security alert and check to see if the value matches the defined requirement. Or, it could require the match of many columns of information. If no filter is matched, the process exits and nothing occurs. If a filter is matched, a security event is generated.

In this next step, FortiNAC evaluates all security triggers. A security trigger is made up of one or more filters. Logic can be applied if there is more than one filter making up a trigger, for example, one, all, or a subset of the filters may need to be matched within a defined period of time. If all criteria are matched for the trigger to be satisfied, FortiNAC evaluates any associated user/host profiles. These are the same profiles covered in the security policy lesson. Just as before, they are used here to leverage who, what, where, and when visibility information. The inclusion of a user/host profile allows an administrator to create different workflows for different endpoints, even if the trigger being matched is the same. If both the trigger and any associated user/host profile are satisfied, a security alarm is created.

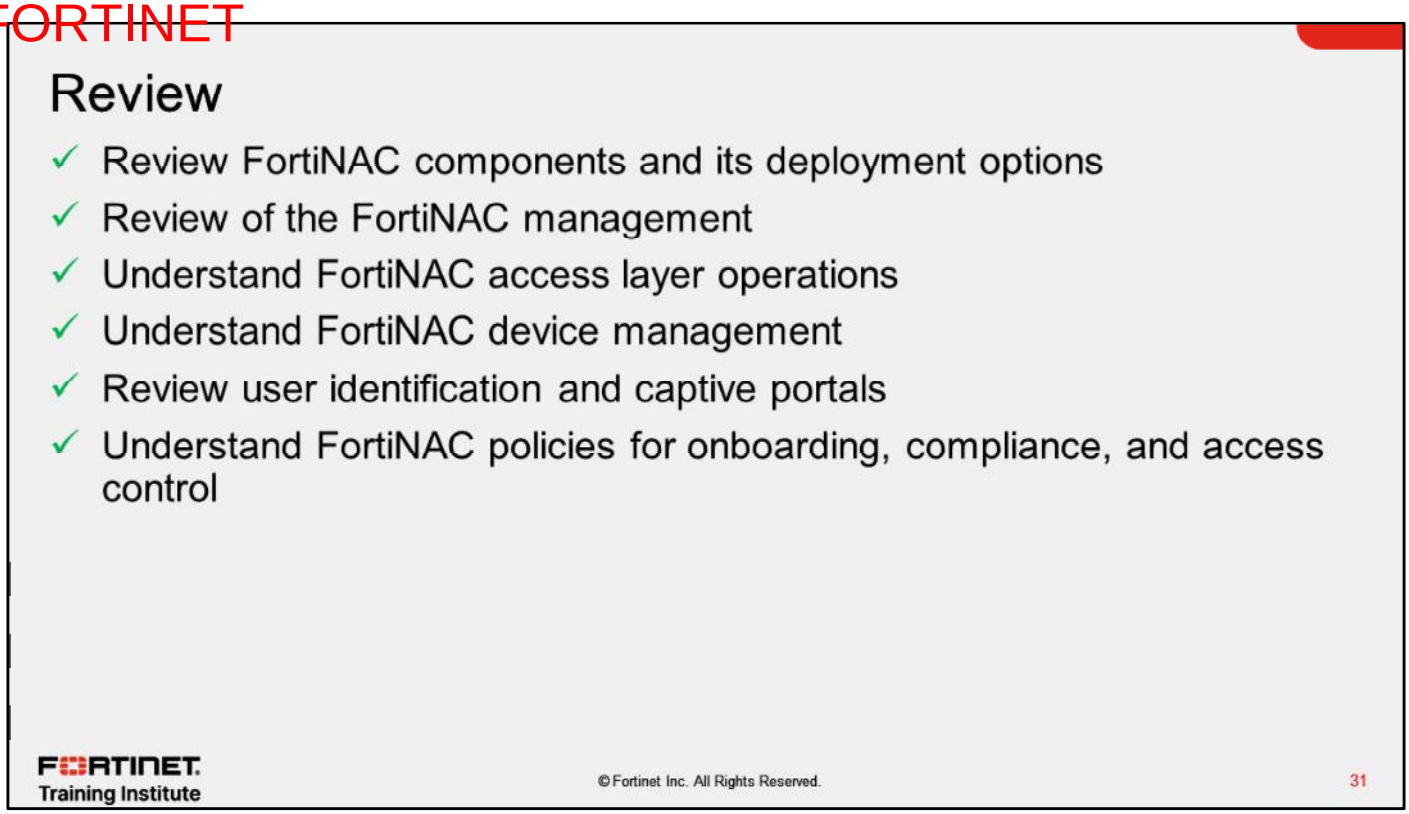
The final step is were the workflows can be defined. If the security rule has an associated action, that action can be carried out in an automated or manual manner. Actions are one or more activities. These activities are the automated responses, and can include notification actions, network access actions, or script execution.

DO NOT REPRINT
© FORTINET



This slide shows the network access workflow of FortiNAC. When a device tries to connect to the network, FortiNAC identifies the devices using device profiling rules, NMAP scanning, agents, or service connectors like MDM. After the device is identified, you will need to determine what type of authentication will be used and what authentication database—local or remote you should use to authenticate the user. Then FortiNAC uses the information gathered from agents or MDM to determine if the device is compliant. Finally, if the endpoint is determined safe, it can be assigned access, based on different security rules.

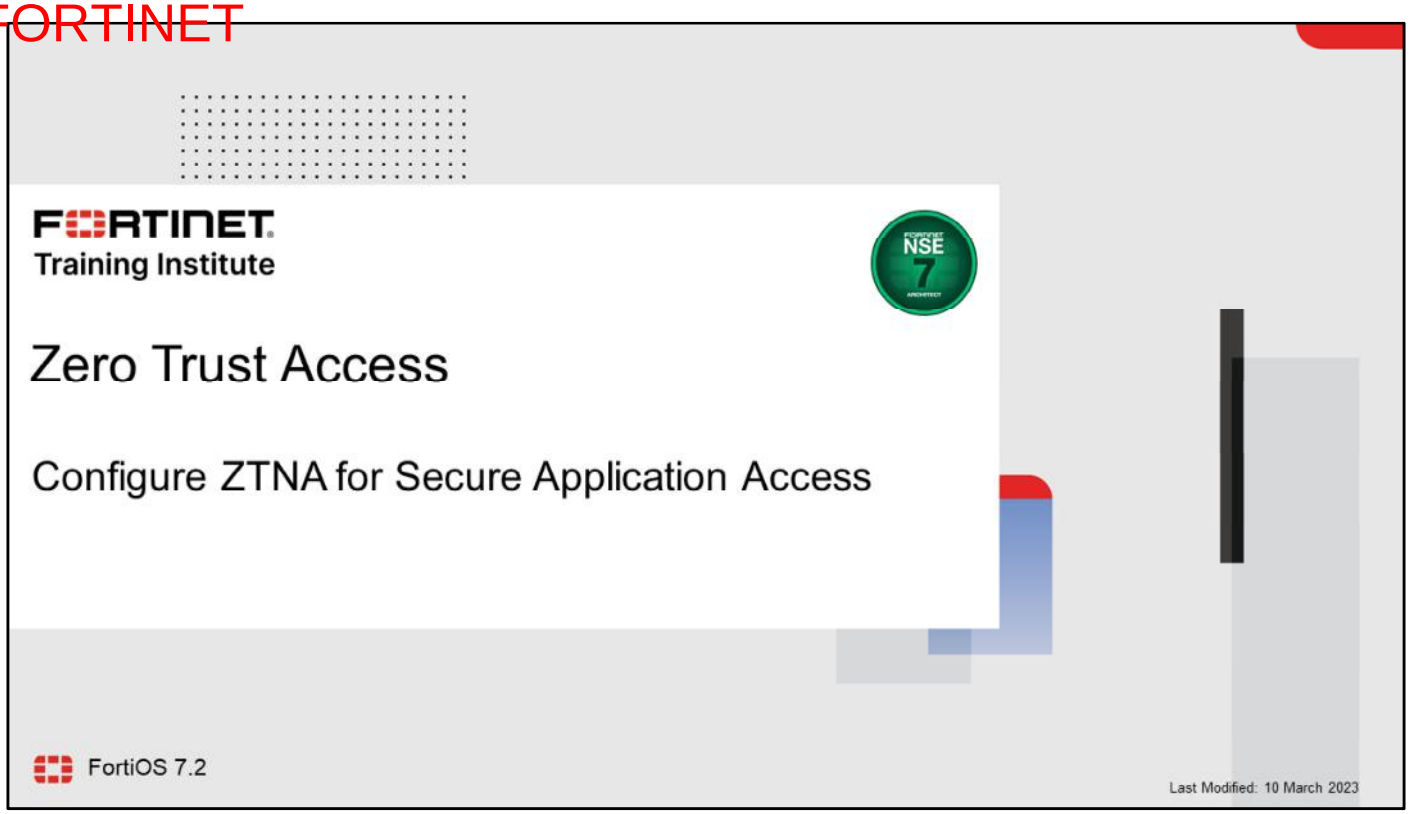
DO NOT REPRINT
© FORTINET



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

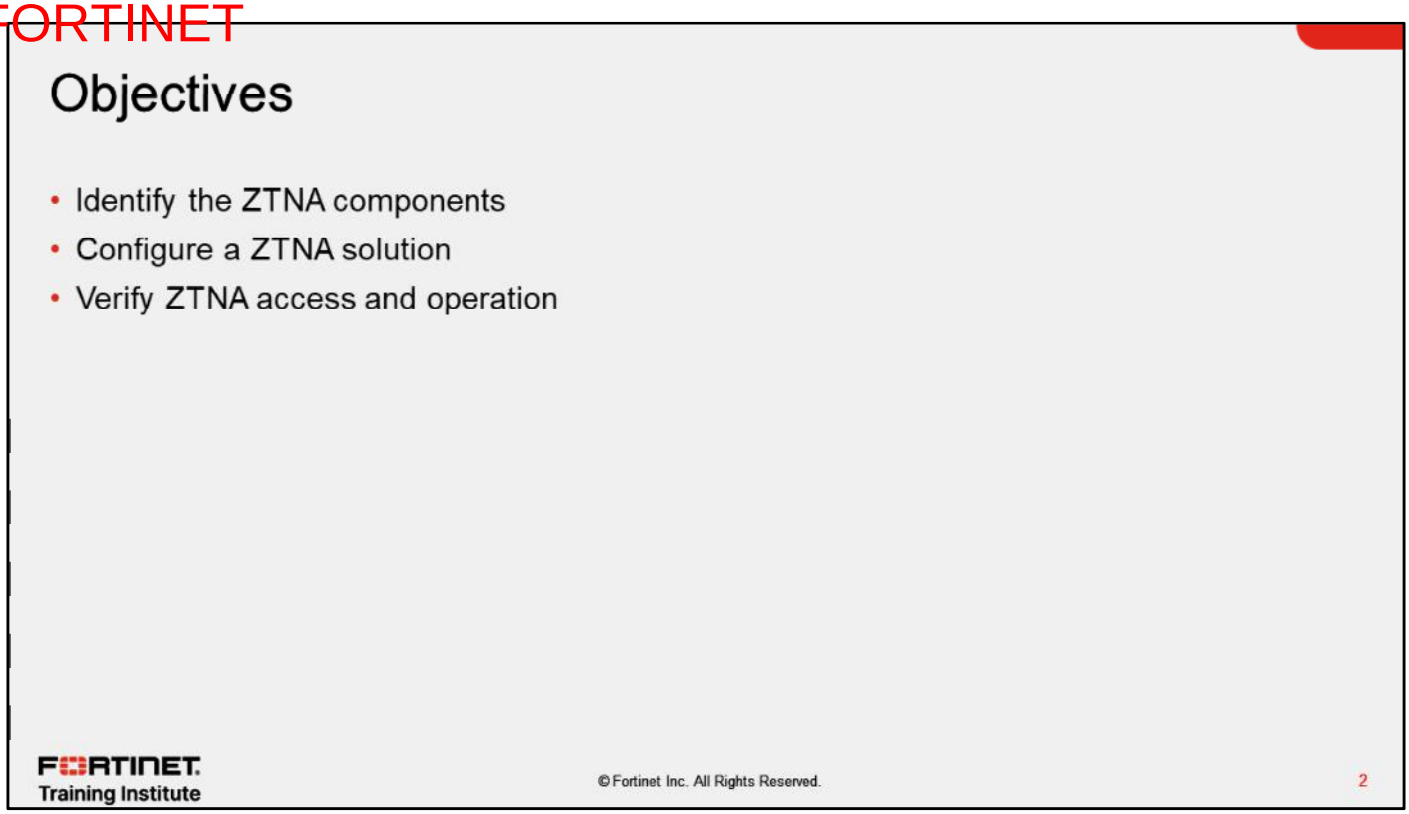
By mastering the objectives covered in this lesson, you learned the design principles for securing network access with FortiNAC and the key features of implementing FortiNAC.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about zero trust network access (ZTNA) configuration.

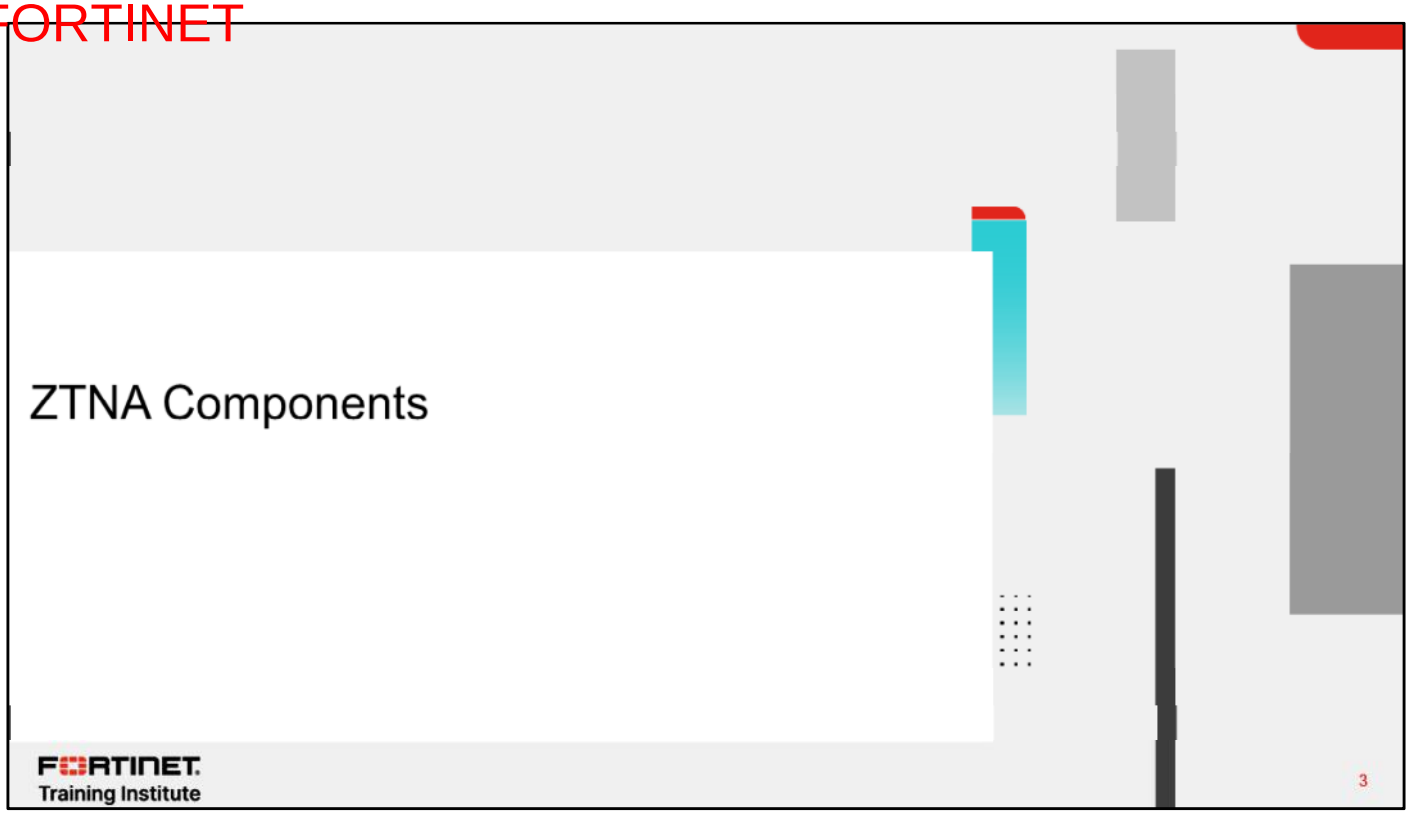
DO NOT REPRINT
© FORTINET



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

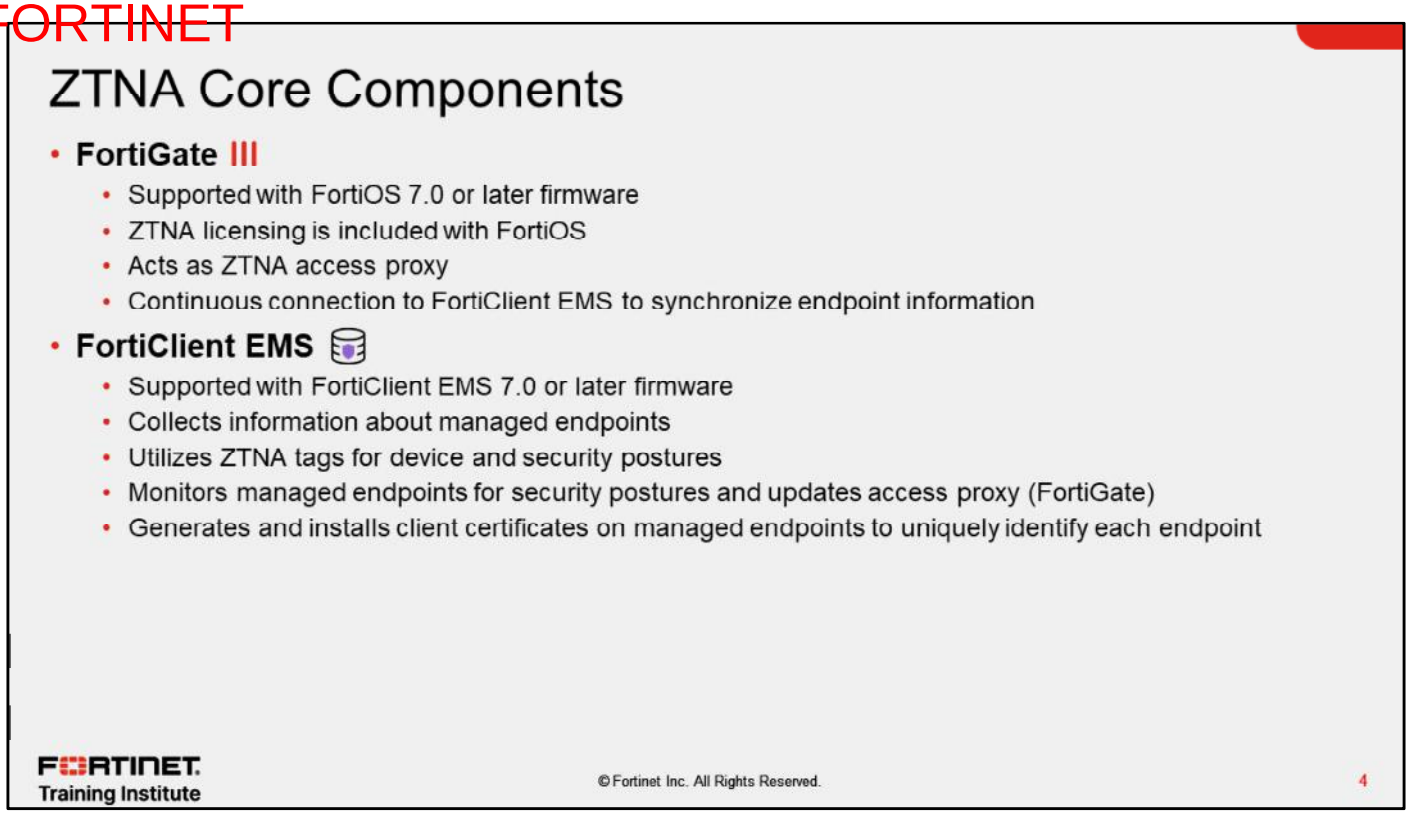
By demonstrating competence in ZTNA, you will be able to identify the ZTNA components and how to configure ZTNA.

DO NOT REPRINT
© FORTINET



In this section, you will identify the ZTNA components.

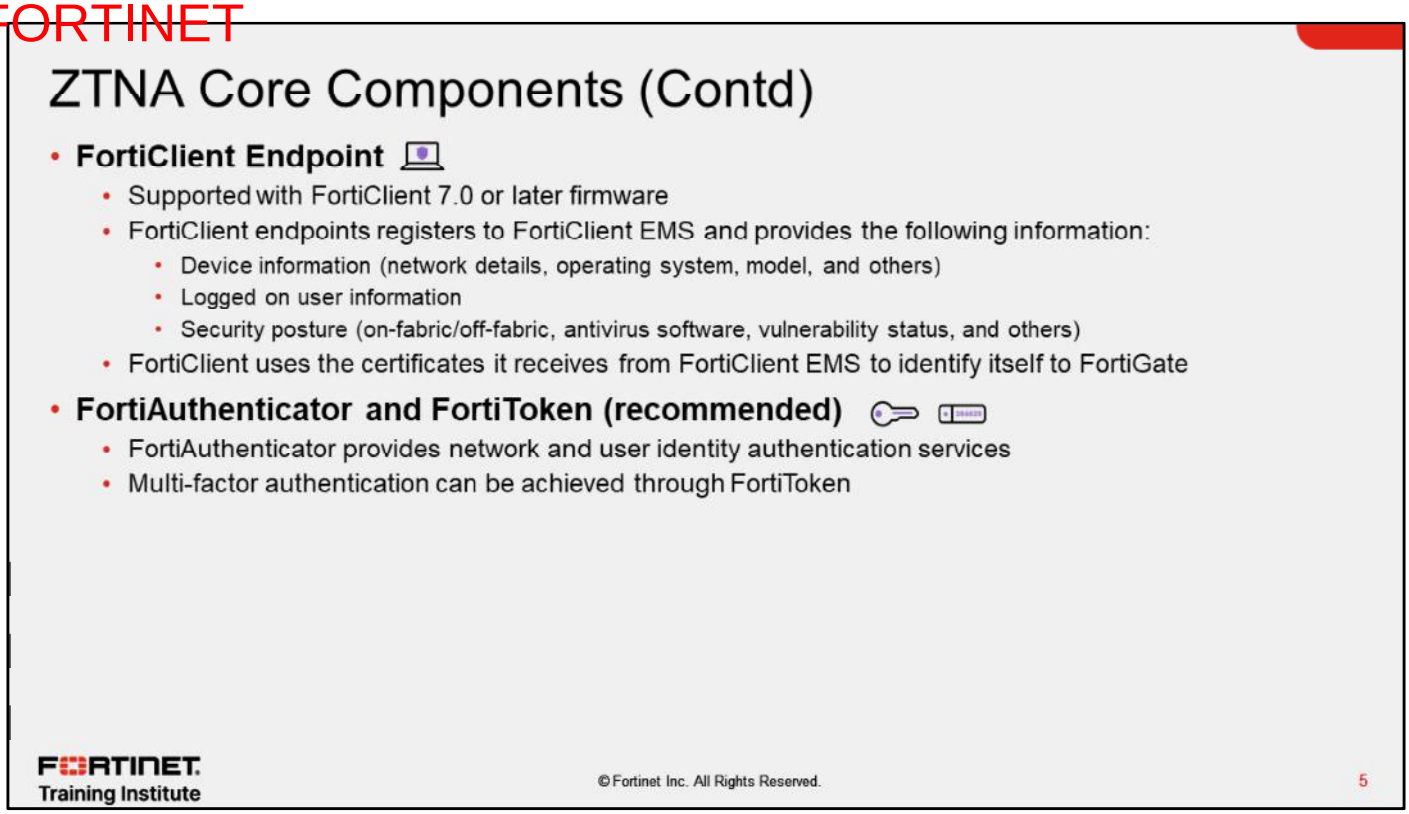
DO NOT REPRINT
© FORTINET



The Fortinet ZTNA solution includes mandatory core products like FortiGate, FortiClient EMS, and FortiClient endpoint, and recommended products like FortiAuthenticator and FortiToken. FortiOS running 7.0 or later firmware can act as a ZTNA access proxy. FortiOS maintains a continuous connection to FortiClient EMS to synchronize endpoint information and ZTNA tags. FortiOS can use these ZTNA tags to grant or deny access to the network. ZTNA licensing is included with FortiOS.

FortiClient EMS running 7.0 or later firmware supports ZTNA. FortiClient EMS uses ZTNA tags for device and security postures of managed endpoints. This information from the managed endpoints is shared with FortiGate. FortiClient EMS also generates and installs client certificates on managed endpoints to uniquely identify each endpoint.

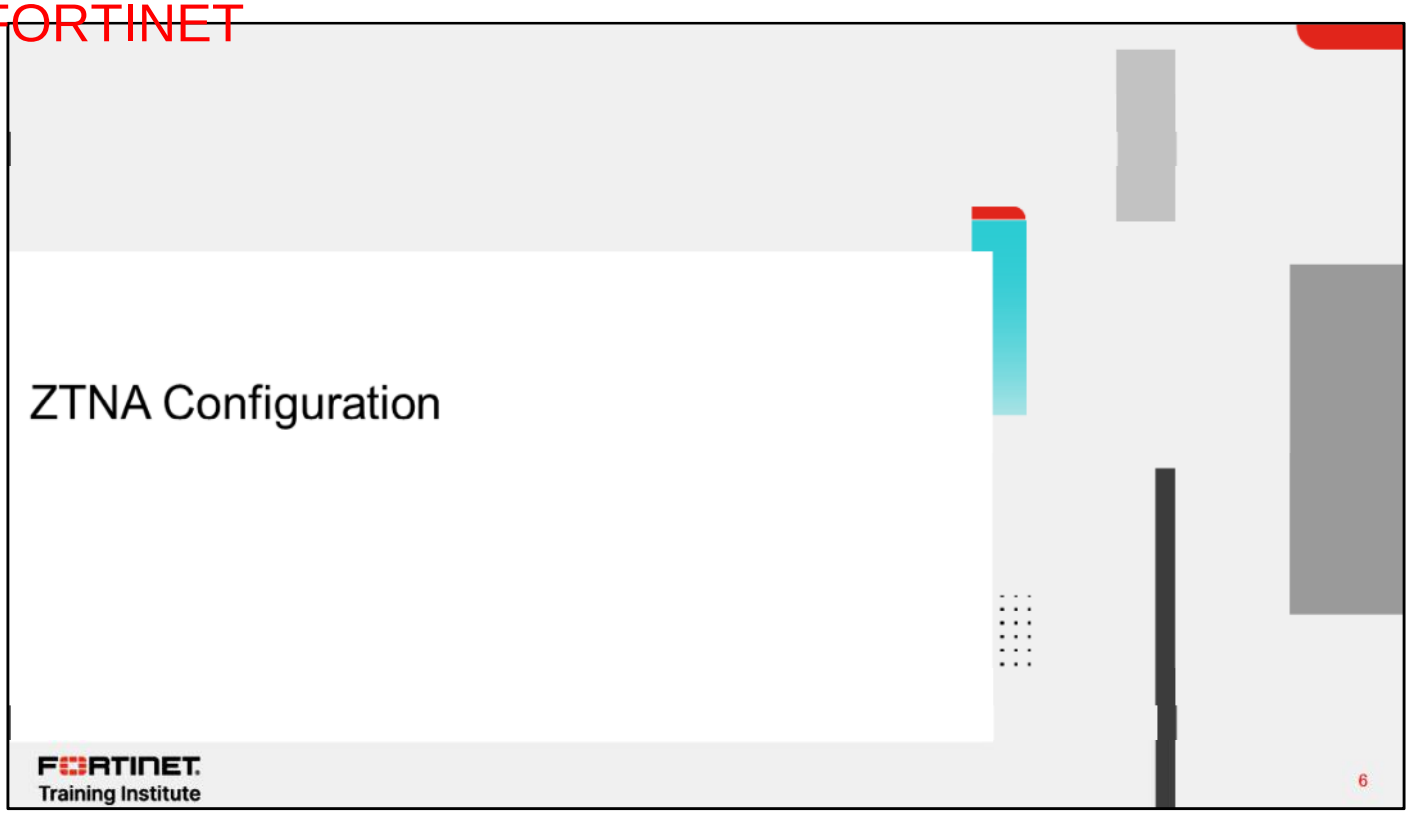
DO NOT REPRINT
© FORTINET



A FortiClient endpoint registers on FortiClient EMS using Zero Trust Telemetry and shares its device information, user information, and security postures. FortiClient uses the certificates it receives from FortiClient EMS to identify itself to FortiGate. ZTNA is supported on FortiClient with 7.0 or later firmware.

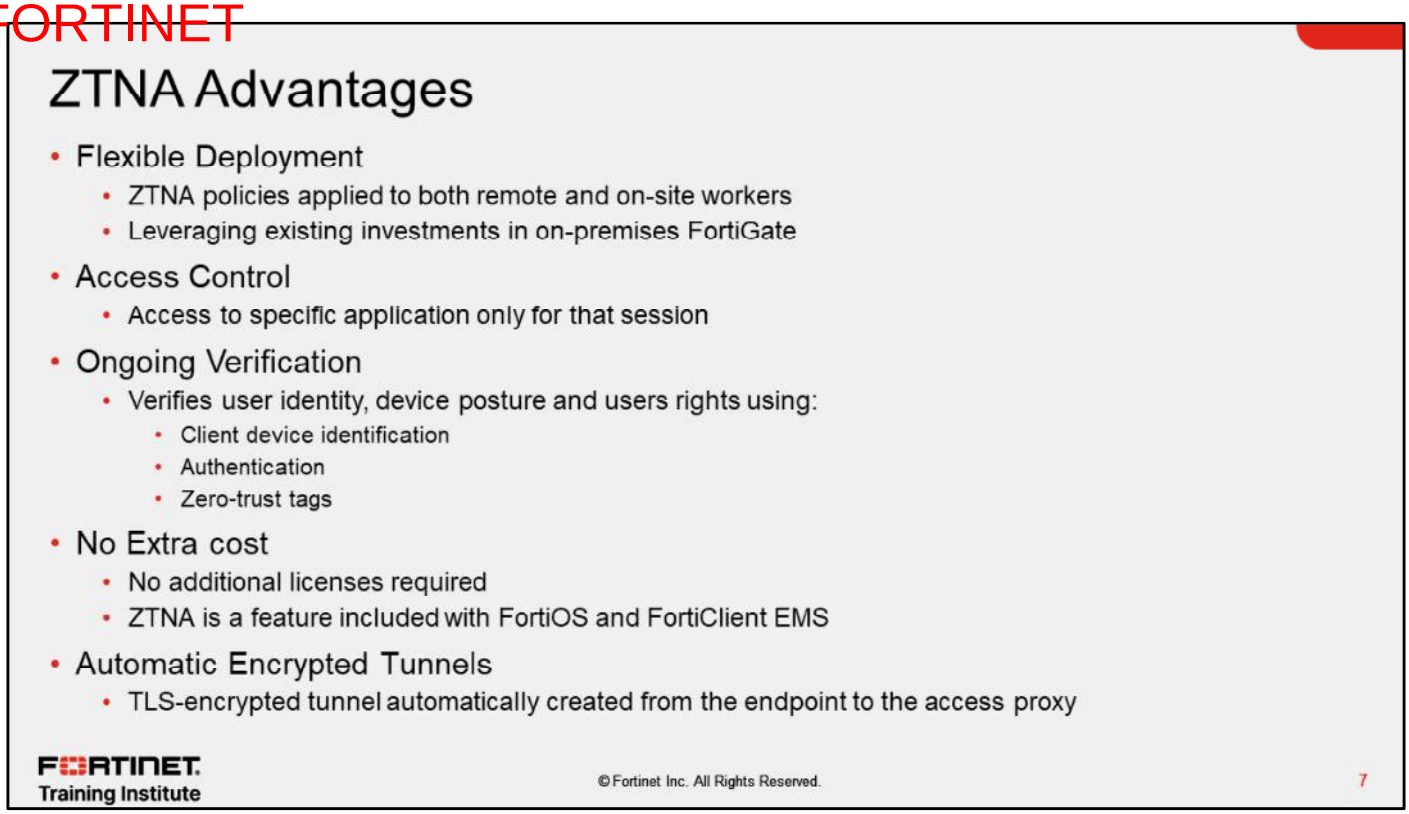
FortiAuthenticator can provide network and user identity authentication services. You can use FortiToken for multi-factor authentication. These two components are not part of the ZTNA core products but are recommended products.

DO NOT REPRINT
© FORTINET



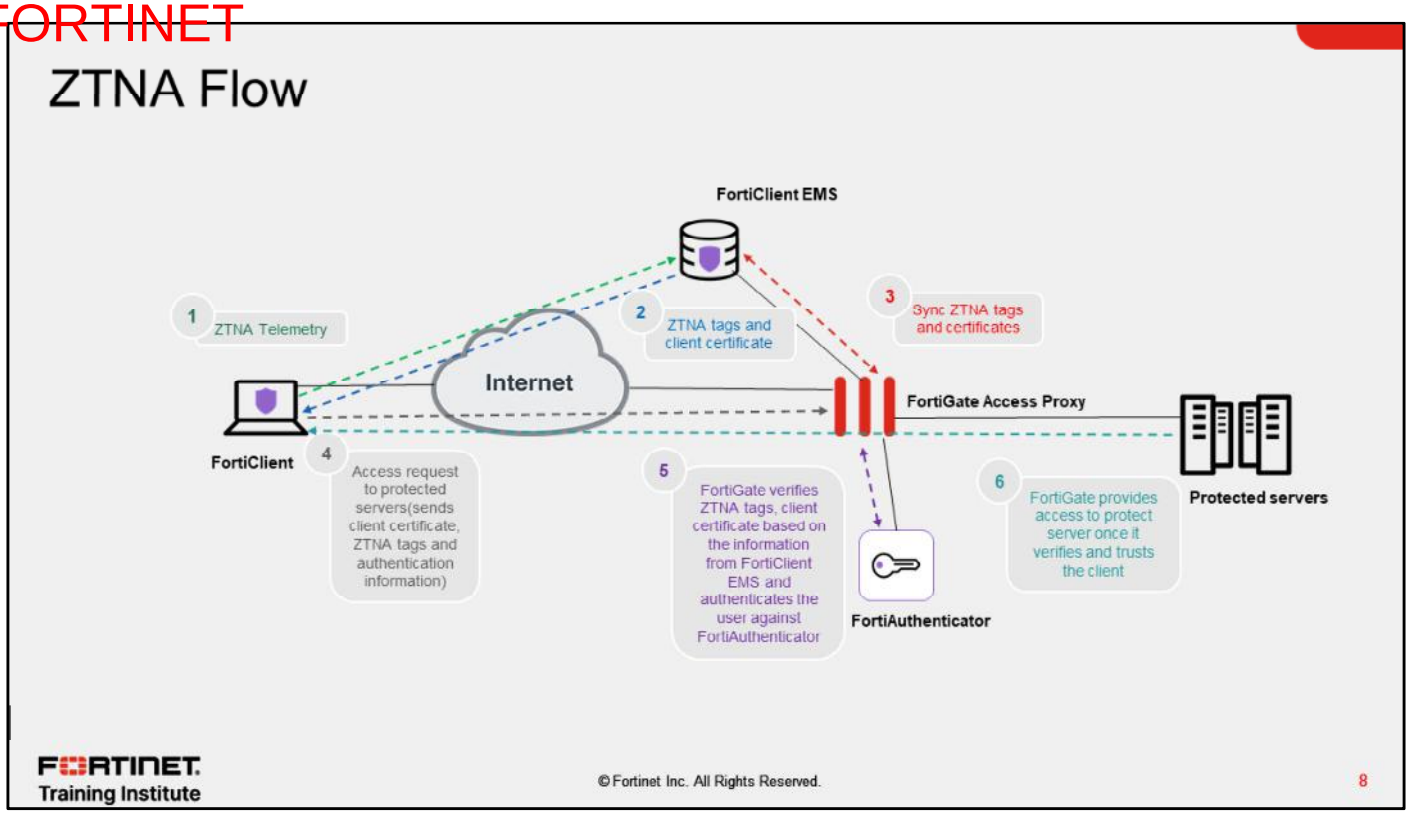
In this section, you will learn about ZTNA configuration.

DO NOT REPRINT
© FORTINET



ZTNA is an access control method that uses client device identification, authentication, and zero-trust tags to provide role-based application access. ZTNA allows administrators to manage network access for on-fabric local users and off-fabric remote users. ZTNA grants access to applications only after device verification, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero-trust tags. Fortinet leverages the existing on-premises FortiGate as part of the ZTNA solution, making it cost effective. There are no additional licenses required to run ZTNA, it is a feature that you can turn on FortiOS and FortiClient EMS.

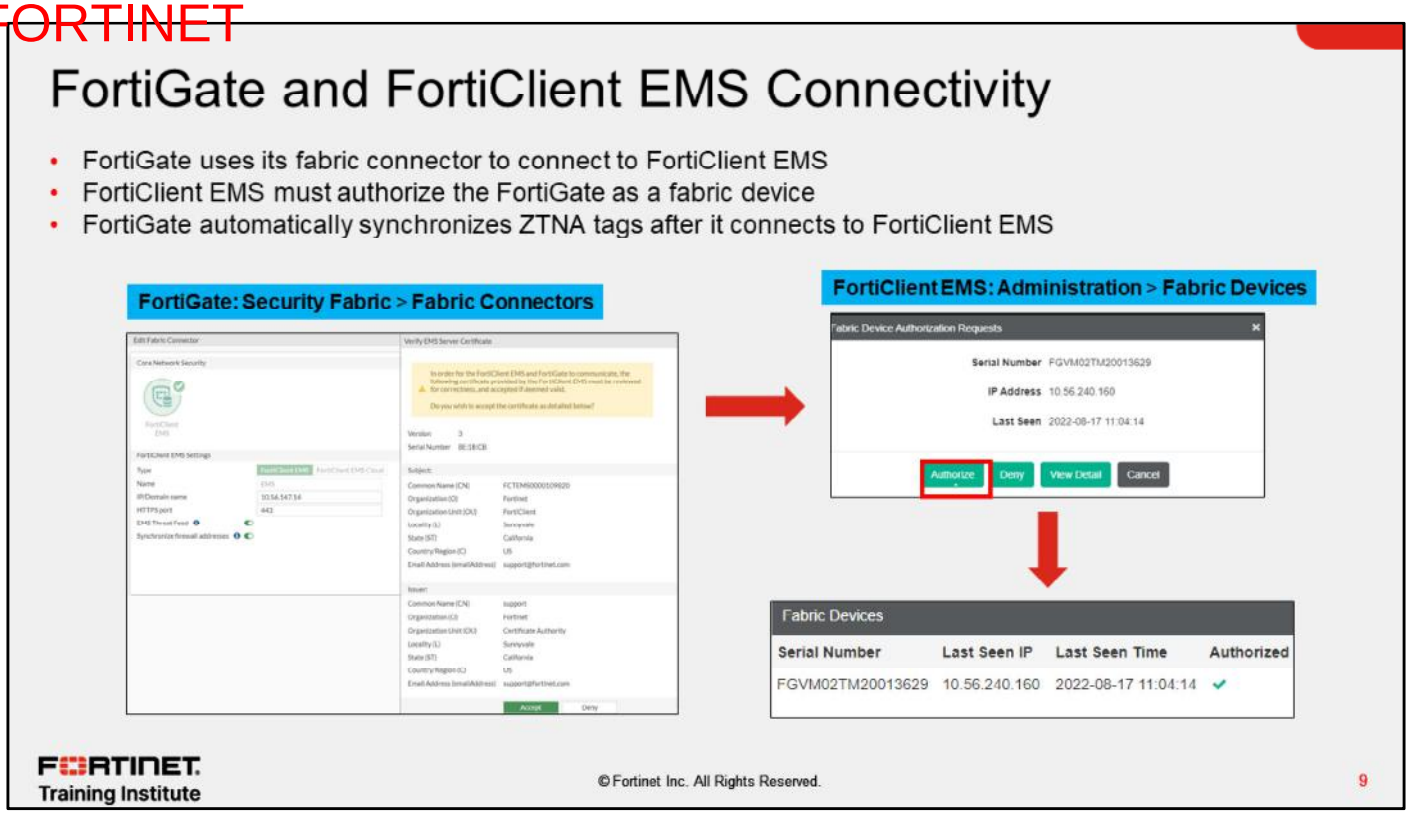
DO NOT REPRINT
© FORTINET



This slide shows the flow of events when FortiGate provides access to an off-fabric client using ZTNA.

1. FortiClient endpoints register on FortiClient EMS and share device information, log-on user information, and security posture over ZTNA telemetry with the FortiClient EMS server. Clients also make a certificate signing request to obtain a client certificate from the EMS that is acting as the ZTNA Certificate Authority (CA).
2. FortiClient EMS collects the information to create ZTNA tags and signs the client certificate.
3. FortiClient EMS synchronizes the FortiClient certificate information and ZTNA tags with FortiGate.
4. FortiClient endpoint sends a request to access the application on the protected server.
5. FortiGate performs a device check by verifying if the certificate provided by FortiClient matches the certificate on FortiGate. FortiGate then performs a user check against FortiAuthenticator and a posture check based on the ZTNA tags.
6. After the endpoint passes all of these verifications, FortiGate provides access to the application on the protected server.

DO NOT REPRINT
© FORTINET

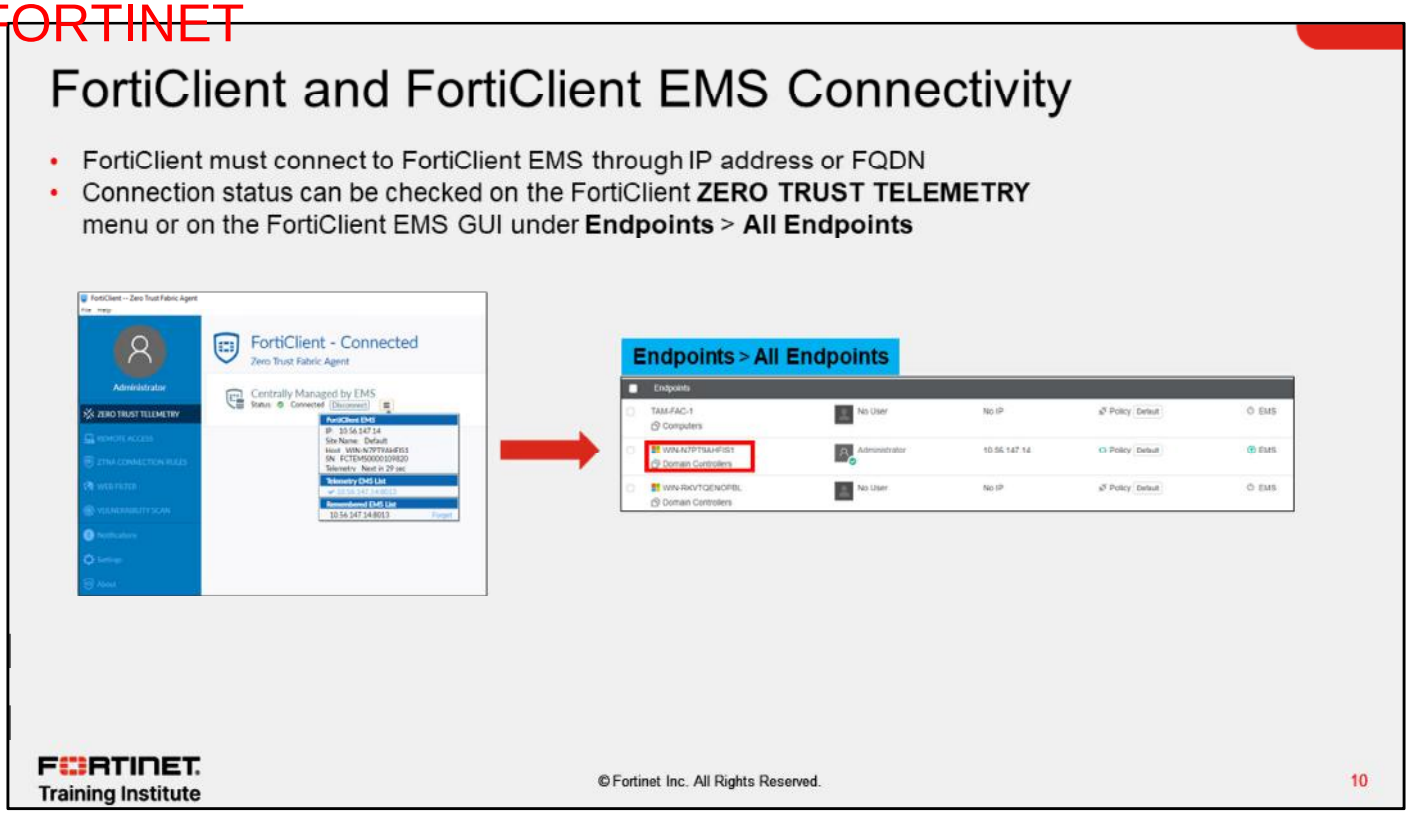


You can configure the on-premises FortiClient EMS connector on FortiGate by clicking **Security Fabric** > **Fabric Connectors**. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate. However, when you configure a new connection to the FortiClient EMS server, the certificate might not be trusted. To resolve this issue, you must manually export and install the root CA certificate on FortiGate. The FortiClient EMS certificate that is used by default for the SDN connection is signed by the CA certificate that is saved on the Windows server when you first install FortiClient EMS. This certificate is stored in the **Trusted Root Certification Authorities** folder on the server.

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click **Administration** > **Devices**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears to be down until you authorize FortiGate on FortiClient EMS.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiClient EMS.

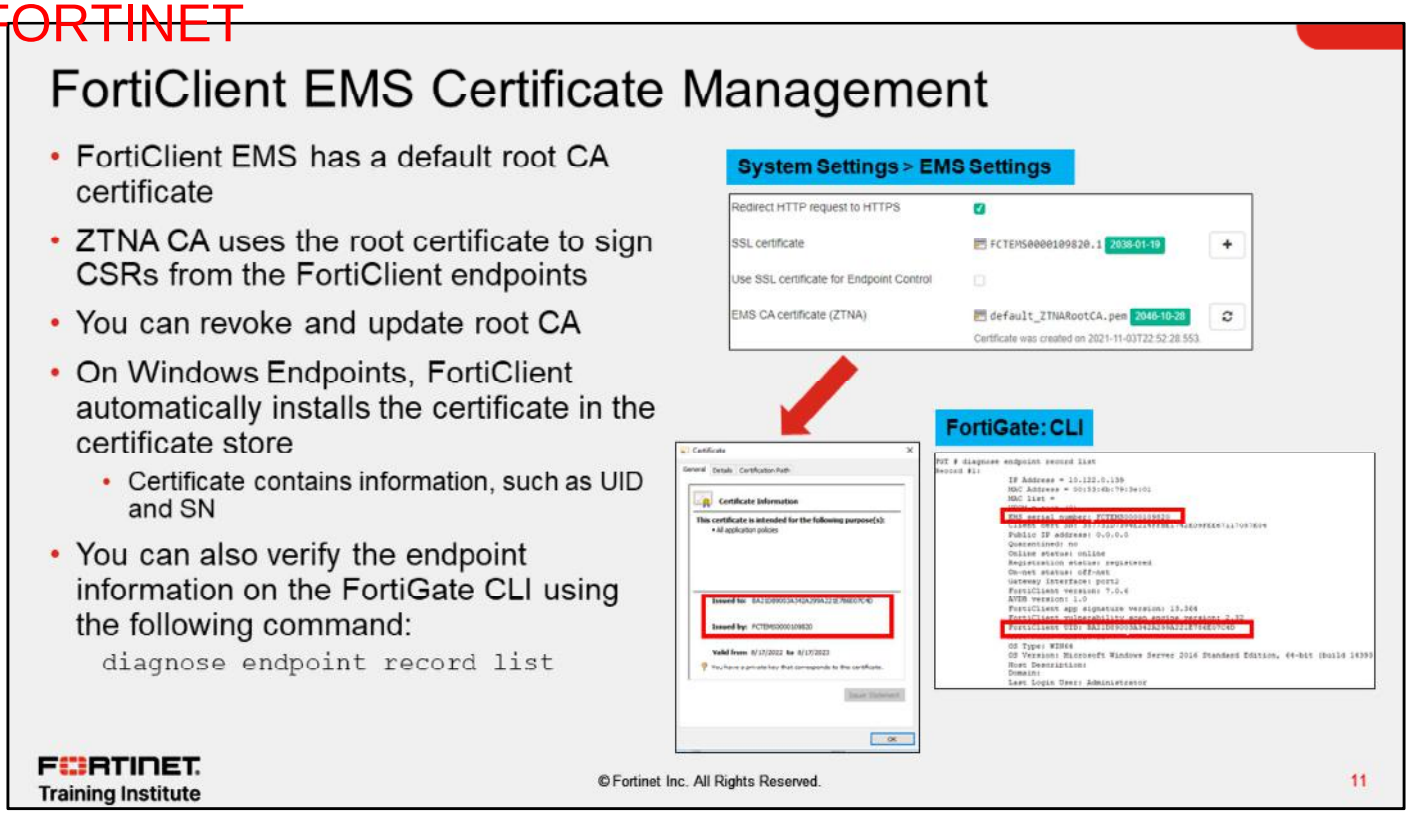
DO NOT REPRINT
© FORTINET



FortiClient must connect to FortiClient EMS. You can verify connection status on the FortiClient console in the **ZERO TRUST TELEMETRY** menu, or on FortiClient EMS by clicking **Endpoints** > **All Endpoints**.

To provide connectivity to the remote FortiClient endpoints, you must allow access to port 8013 on the FortiClient EMS through the corporate firewall. On FortiGate, you can create a VIP and inbound policy to allow access to TCP port 8013 from the internet.

DO NOT REPRINT
© FORTINET

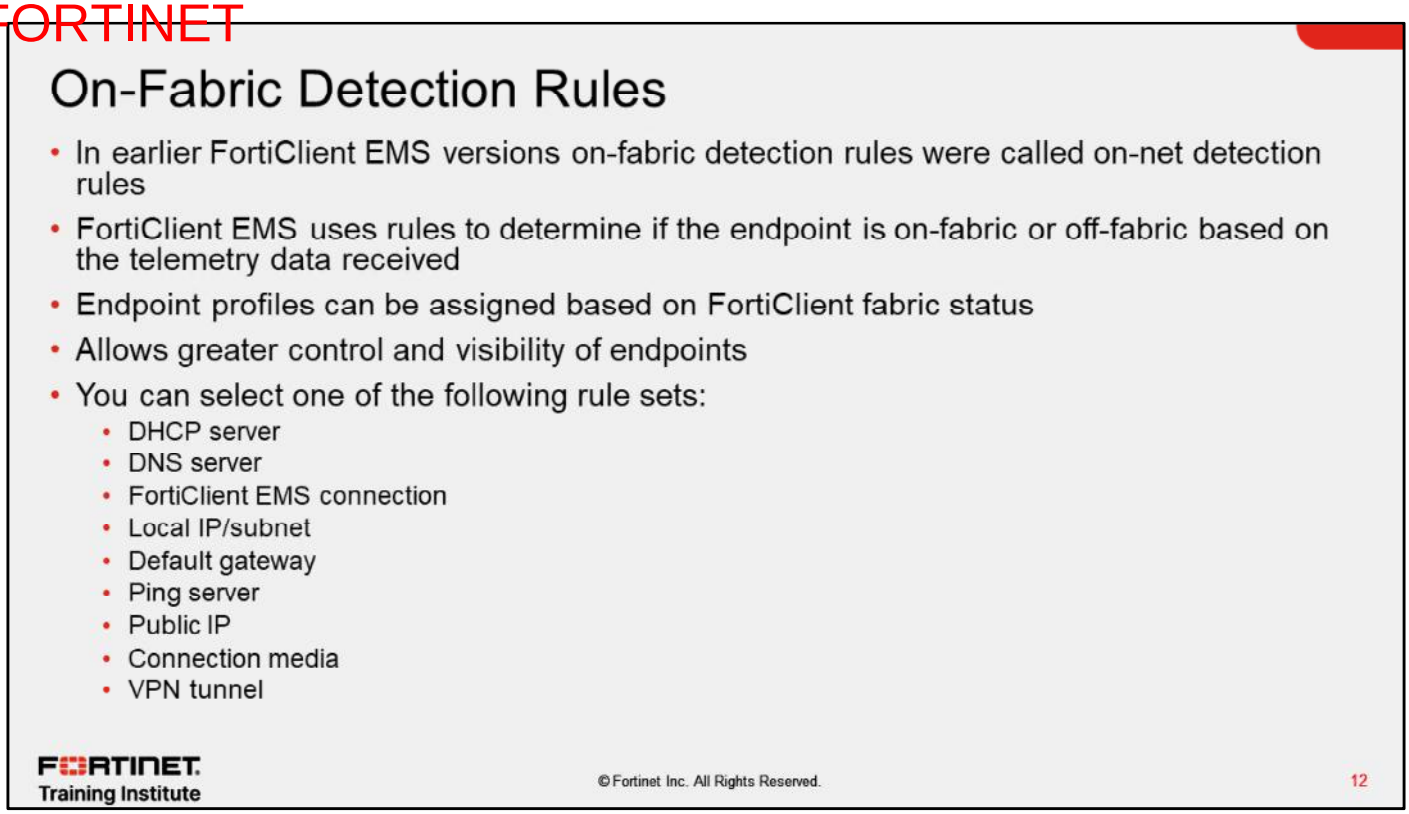


FortiClient EMS has a default_ZTNARootCA certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised.

In Windows, FortiClient automatically installs certificates into the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate. To locate certificates on other operating systems, consult the vendor documentation.

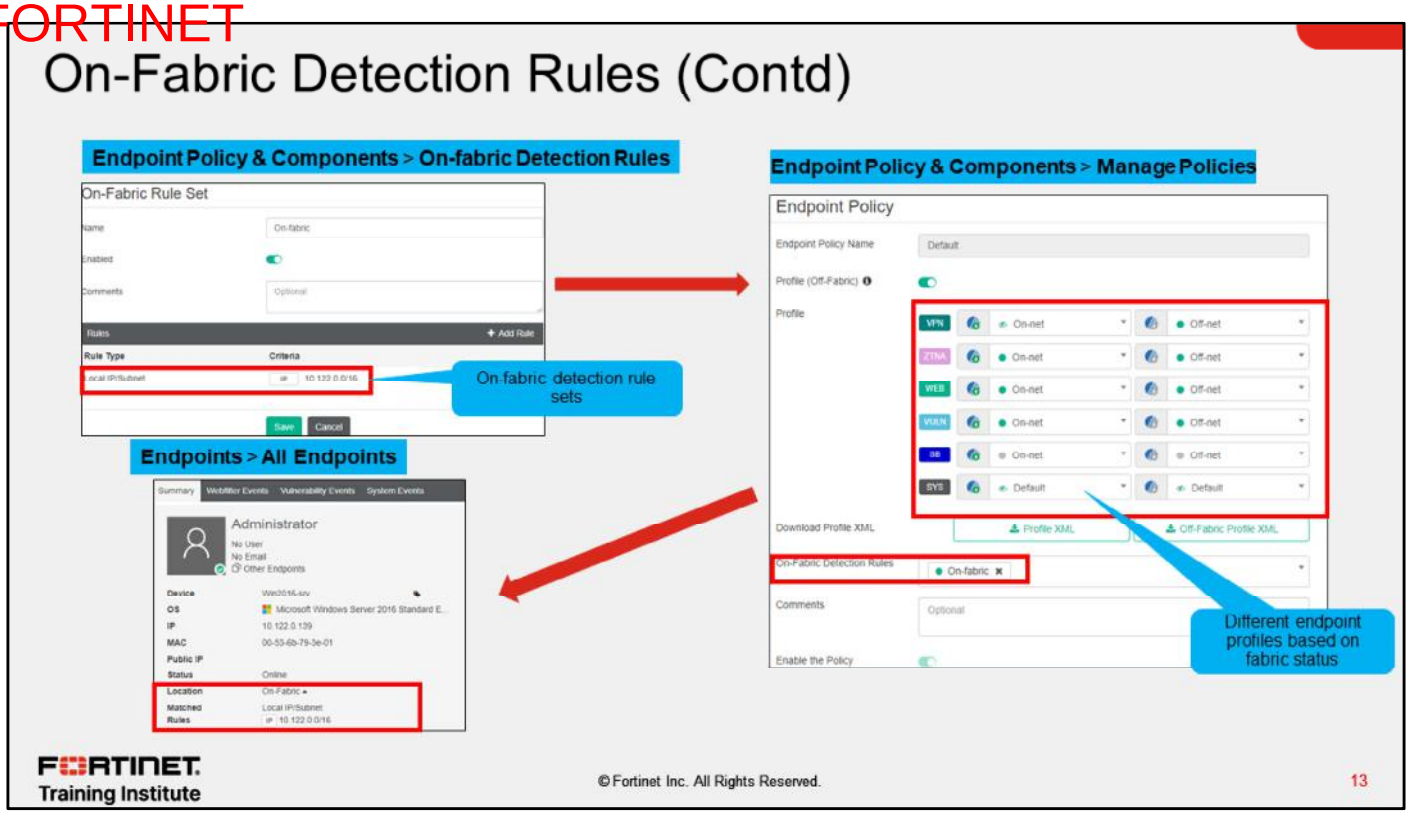
You can use the CLI command `diagnose endpoint record list` to verify the presence of a matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate the corresponding endpoint entry.

DO NOT REPRINT
© FORTINET



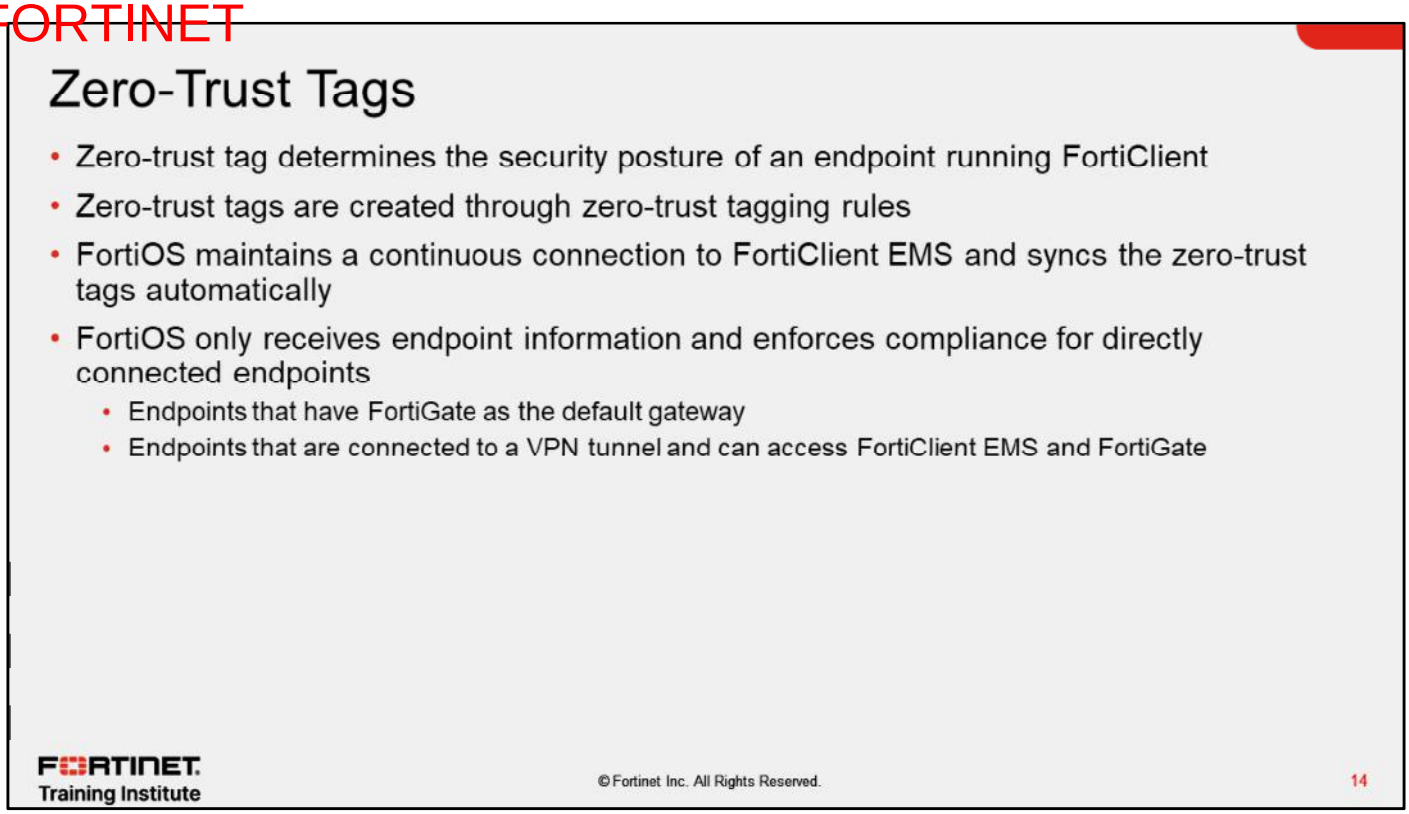
In earlier versions of FortiClient EMS, on-fabric detection rules was known as on-net detection rules. You can configure on-fabric detection rules for endpoints. FortiClient EMS uses the rules to determine if the endpoint is on fabric or off fabric. Depending on the endpoint on-fabric status, FortiClient EMS may apply a different profile to the endpoint, as configured in the applied endpoint policy. A rule set is available for on-fabric detection. If you configure rules of multiple detection types for a rule set, the endpoint must satisfy all configured rules to satisfy the entire rule set.

DO NOT REPRINT
© FORTINET



This slide shows an example of an on-fabric rule using the rule type **Local IP/Subnet**. The **Criteria** to match is 10.122.0.0/16. The FortiClient endpoint has an IP address of 10.122.0.139. This matches the on-fabric rule set and is tagged as an on-fabric device. A different endpoint profile is assigned to on-fabric and off-fabric devices per this configuration.

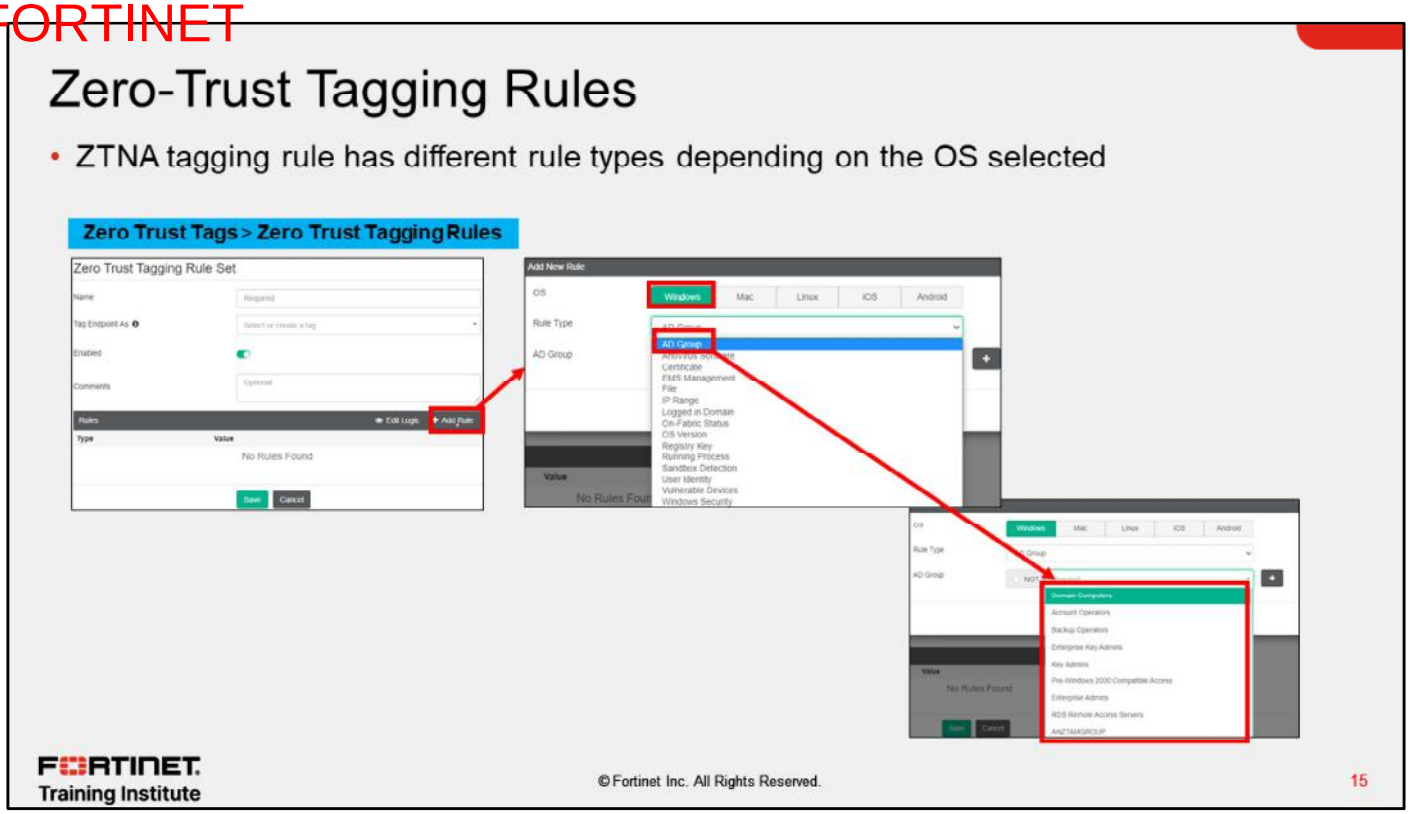
DO NOT REPRINT
© FORTINET



Zero-trust tags determines the security posture of an endpoint running FortiClient. Zero-trust tags are configured through zero-trust tagging rules on FortiClient EMS. You can create zero-trust tagging rules for Windows, macOS, and Linux endpoints based on their OS versions, antivirus software installation, logged in domains, running processes, and other criteria. FortiOS maintains a continuous connection to FortiClient EMS and syncs the zero-trust tags automatically for compliance checks.

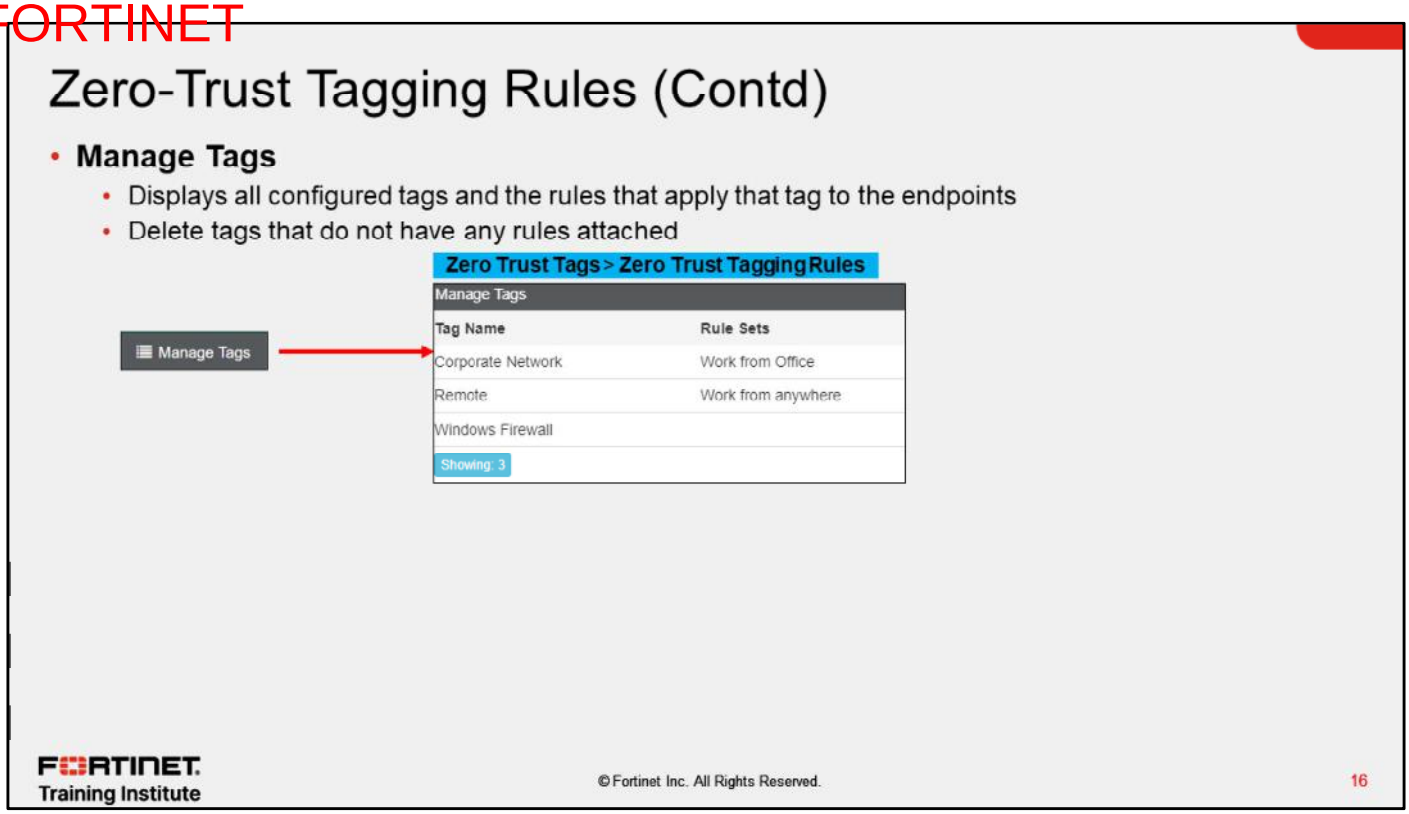
FortiOS receives endpoint information and enforces compliance only for directly connected endpoints. Directly connected endpoints that have FortiGate as the default gateway. This feature also works for endpoints that are connected to a VPN tunnel as long as they can access FortiClient EMS and the FortiOS .

DO NOT REPRINT
© FORTINET



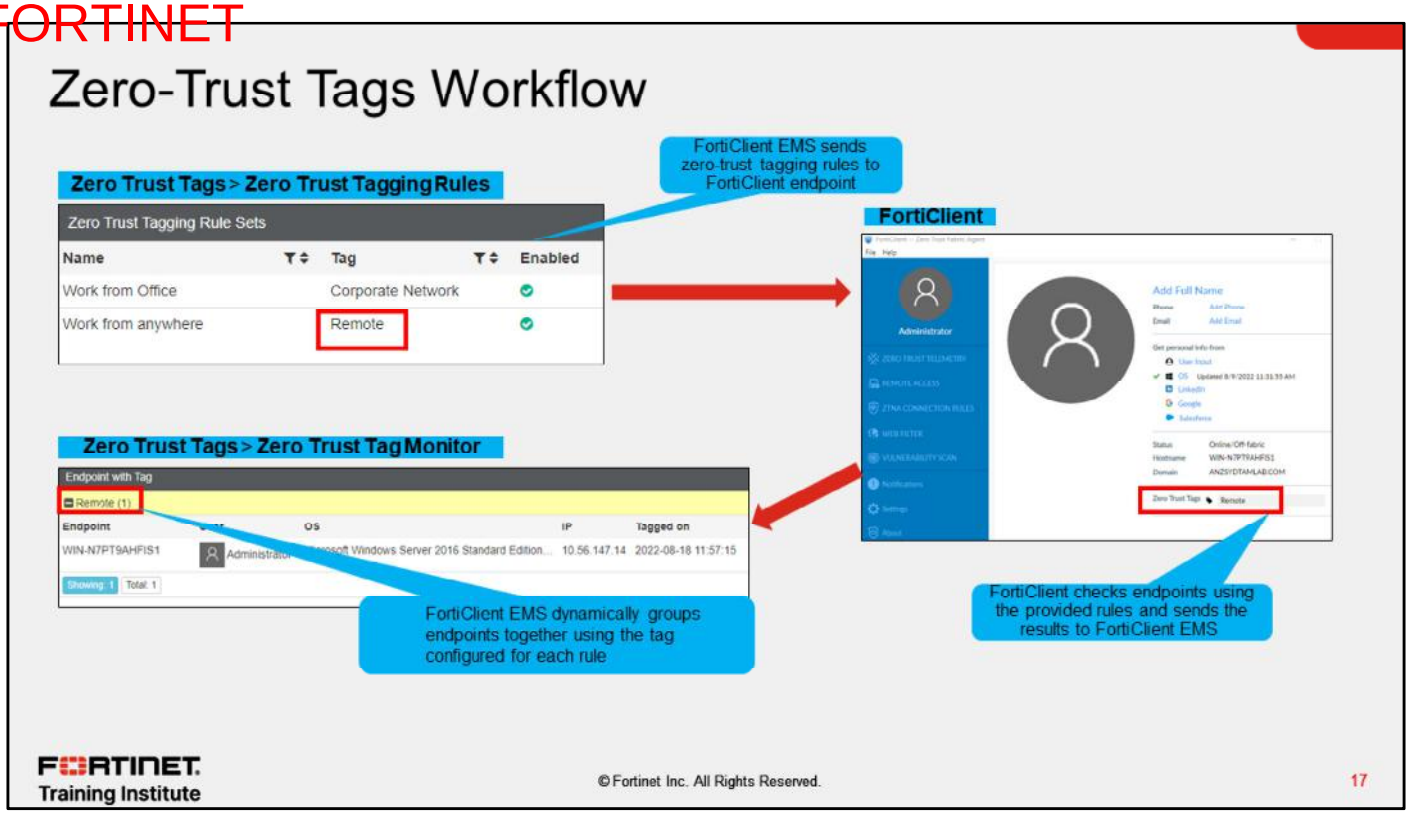
You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints.

DO NOT REPRINT
© FORTINET



The **Manage Tags** window displays all configured tags and the rules that apply the tags to endpoints that satisfy the rule. You can delete tags that do not have any rules attached.

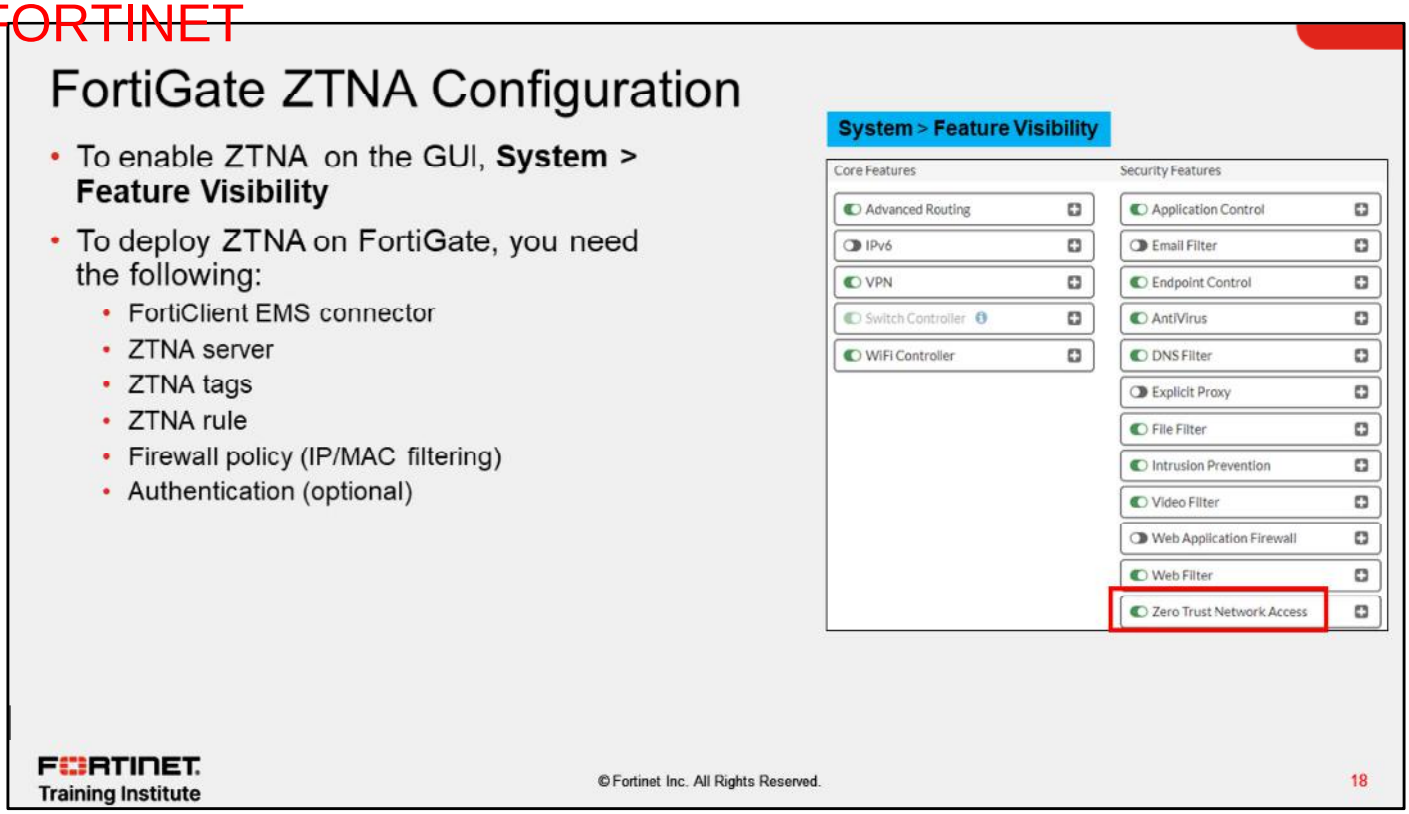
DO NOT REPRINT
© FORTINET



This slide show the zero-trust tags workflow. The following happens when using zero-trust tagging rules with FortiClient EMS and FortiClient:

- FortiClient EMS sends zero-trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiClient EMS.
- FortiClient EMS dynamically groups endpoints together using the tag configured for each rule.

DO NOT REPRINT
© FORTINET

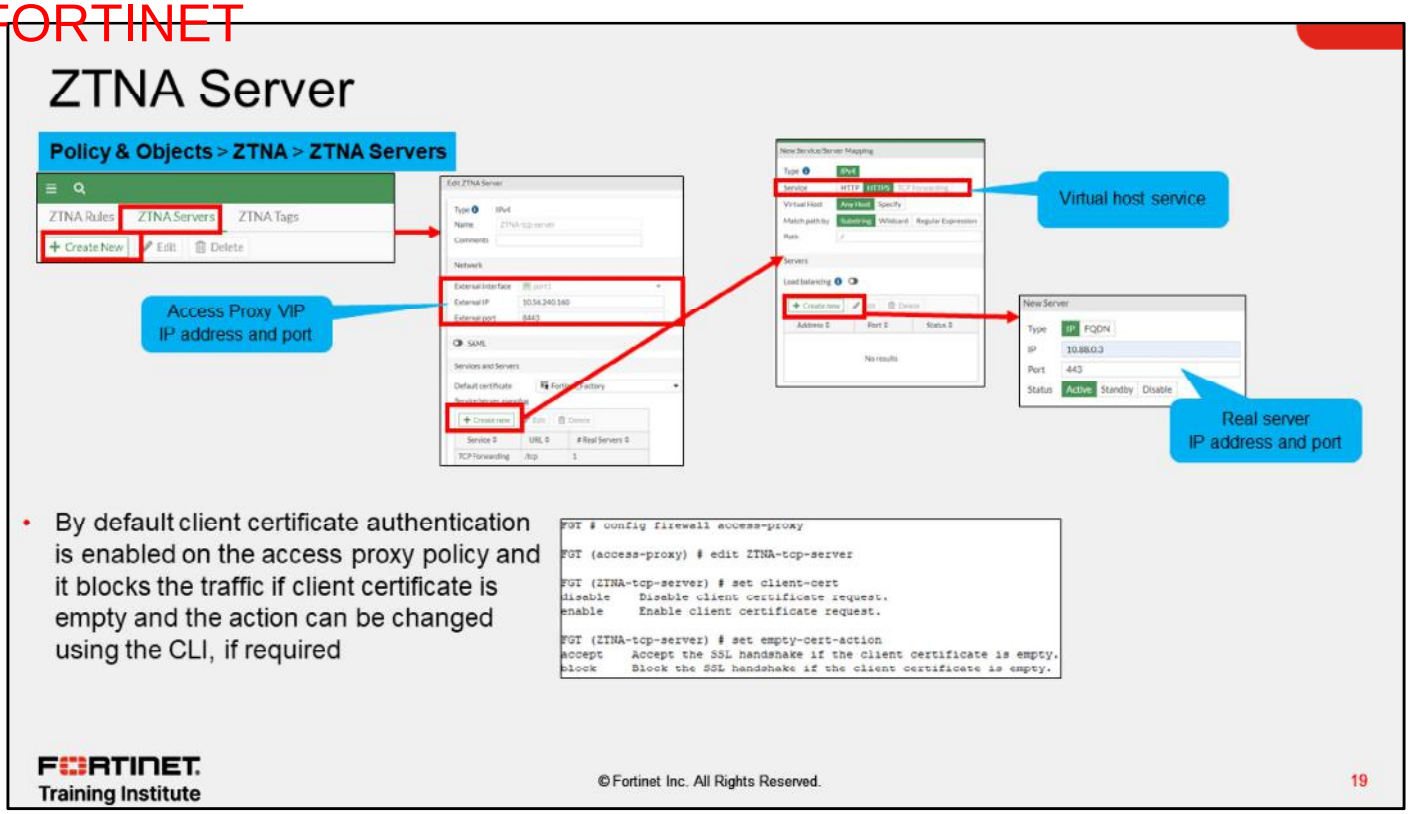


To enable ZTNA on the GUI, you must enable the feature on FortiGate **System** > **Feature Visibility**, and then enable **Zero Trust Network Access**. ZTNA configuration on FortiGate requires the following configuration:

- Add FortiClient EMS as a fabric connector in the Security Fabric. FortiGate maintains a continuous connection to the FortiClient EMS server to synchronize endpoint device information, and also automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA rules and firewall policies.
- The ZTNA server defines the access proxy VIP and the real servers that clients connect to. The firewall policy matches and redirects client requests to the access proxy VIP. You can also enable authentication.
- A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust, role-based access. You can configure security profiles to protect this traffic.

You can also configure authentication to the access proxy. ZTNA supports basic HTTP and SAML methods.

DO NOT REPRINT
© FORTINET

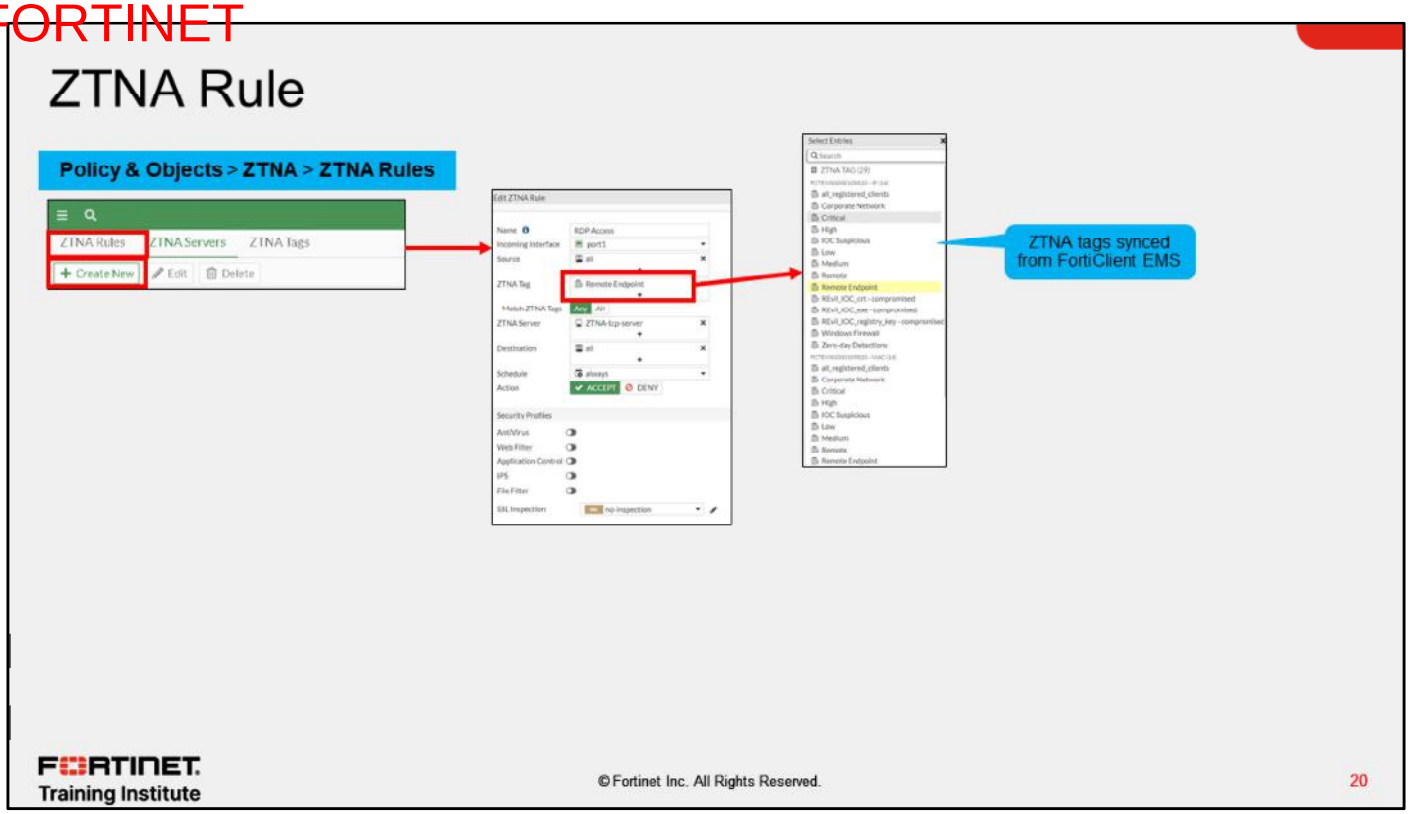


After you add FortiClient EMS as the fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

The **Servers** table, allows you to configure the real server IP address, port number, and status. You can configure multiple servers and server mappings.

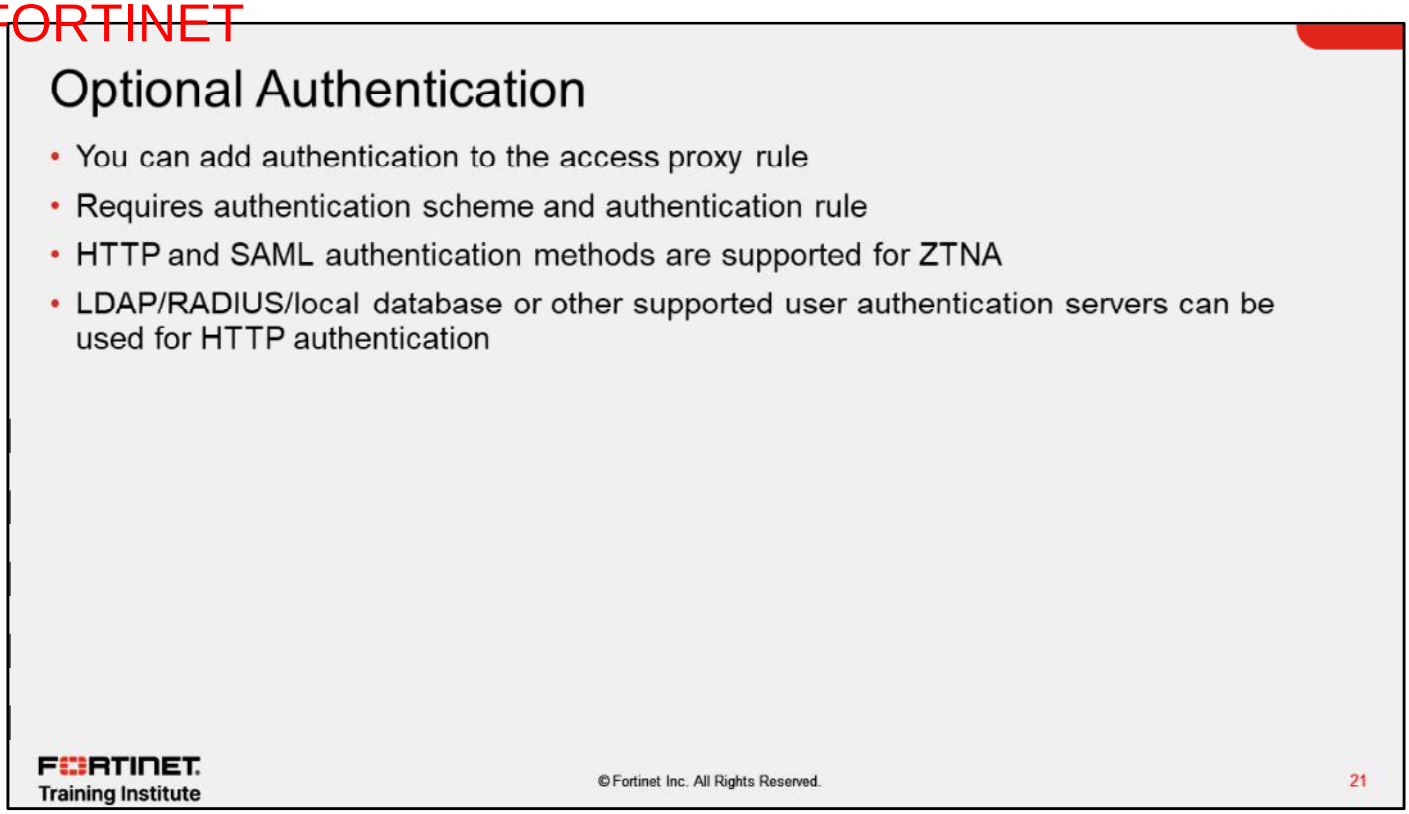
By default, client certificate authentication is enabled on the access proxy policy and it blocks the traffic if the client certificate is empty. You can change the action using the CLI, if required.

DO NOT REPRINT
© FORTINET



A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust, role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.

DO NOT REPRINT
© FORTINET



You can add authentication to the access proxy, which requires you to configure an authentication scheme and authentication rule on the FortiGate. You use authentication schemes and authentication rules to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

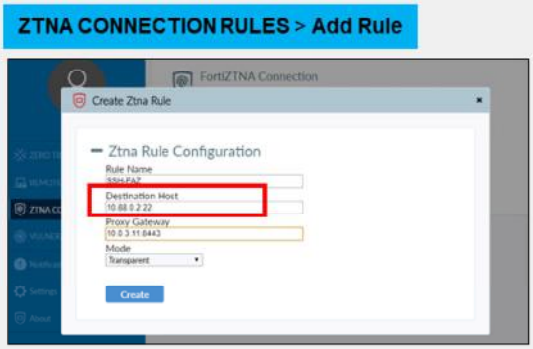
The authentication scheme defines the method of authentication that is applied. ZTNA supports basic HTTP and SAML methods. Each method has additional settings to define the data source. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they are with basic authentication. After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to.

DO NOT REPRINT
© FORTINET

ZTNA TCP Forwarding Access Proxy

- User must create a ZTNA rule on the FortiClient to connect
- You can also configure ZTNA TCP forwarding access proxy without encryption
  - Improves performance by reducing encryption overhead of an already secure underlying protocol
  - Do not use for insecure protocols



FORTINET Training Institute

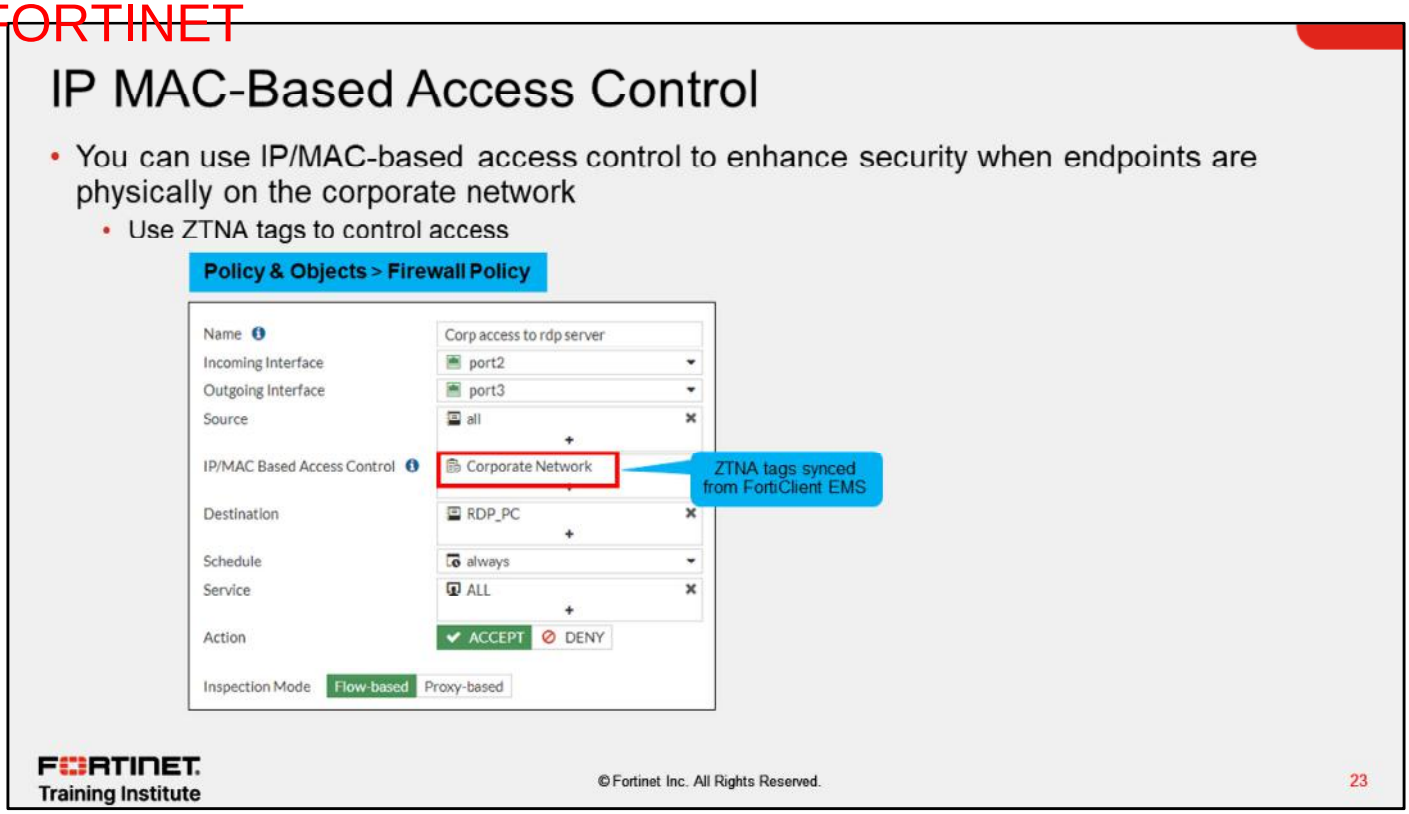
© Fortinet Inc. All Rights Reserved.

22

Before connecting, users must create a ZTNA rule on FortiClient. Note that your **Destination Host** is the real internal IP address and port of the server. The RDP and SSH connections securely proxied through the gateway.

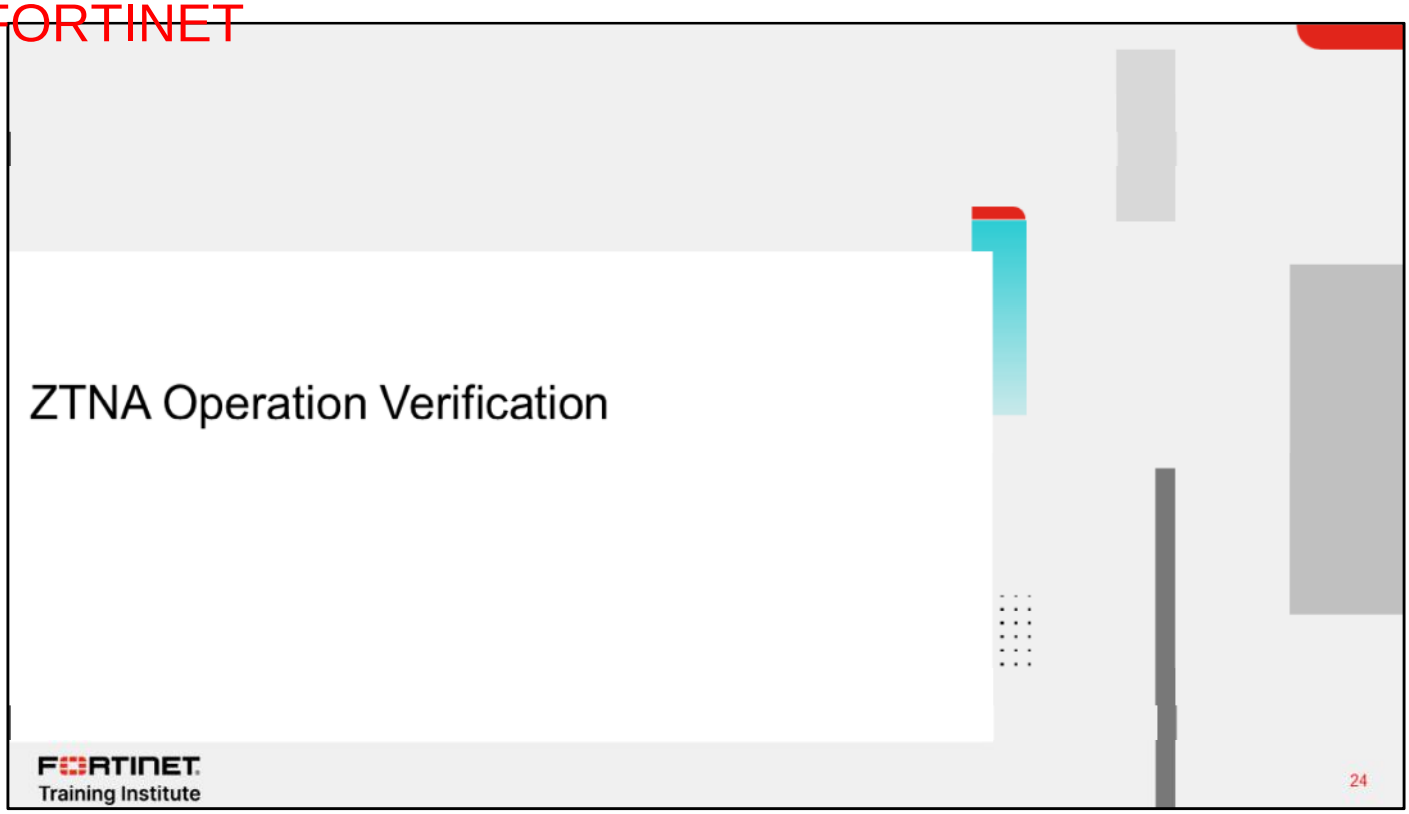
You can also configure a ZTNA TCP forwarding access proxy without encryption. The connection still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end-to-end communication between the client and server are encapsulated in the specified TCP port, but not encrypted by the access proxy. This improves performance by reducing the overhead of encrypting an already secured underlying protocol, such as RDP, SSH, or FTPS. Users should still enable the encryption option for end-to-end protocols that are insecure. In a real-life application, you should use the encryption option for an insecure protocol such as Telnet.

DO NOT REPRINT
© FORTINET



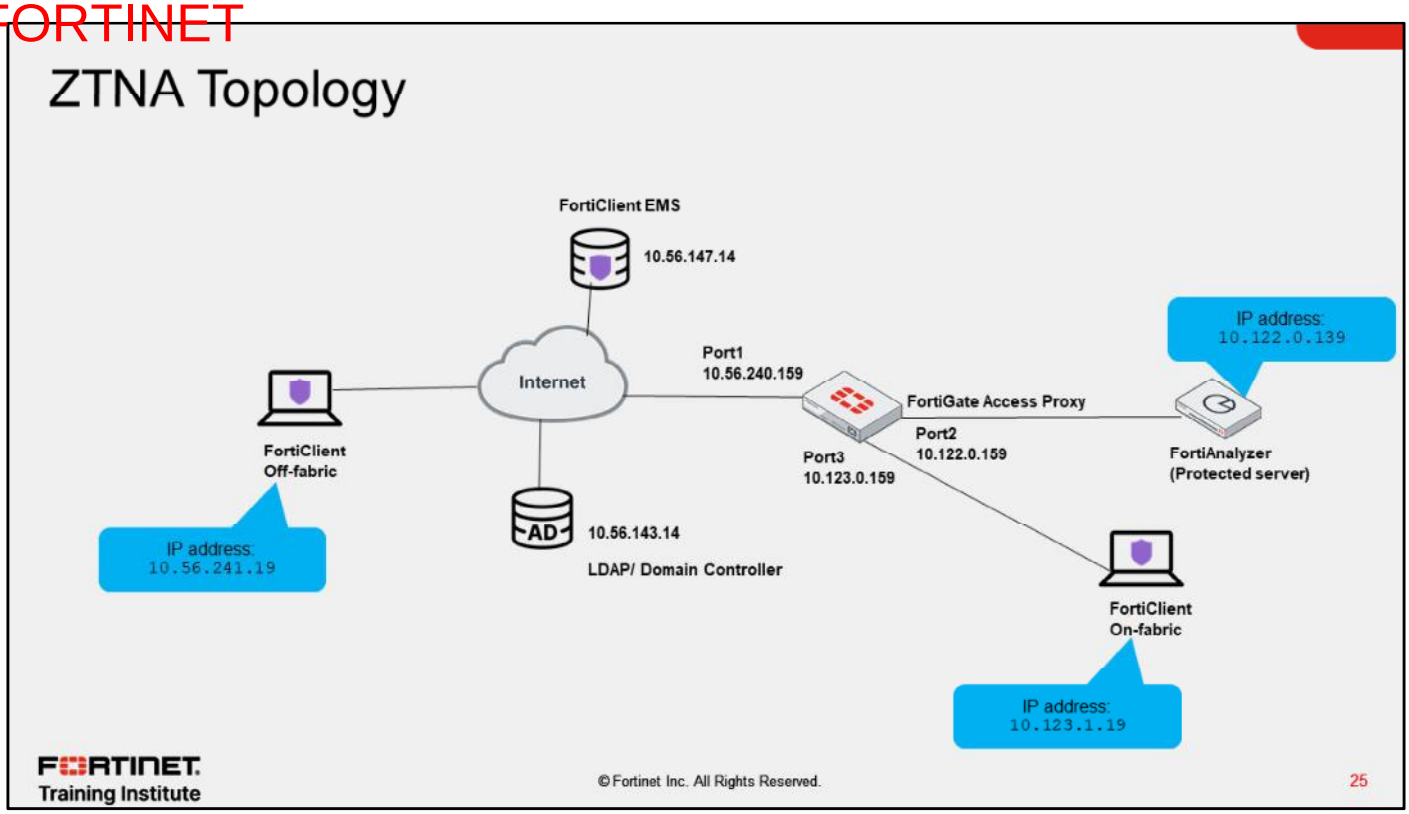
You can use IP/MAC-based access control on a firewall policy to enhance security when endpoints are physically located on the corporate network, whereas a ZTNA rule focuses on access for remote users. IP/MAC-based access control uses ZTNA tags to control access between on-fabric devices and an internal web server or the internet. This does not require the use of the access proxy, and uses only ZTNA tags for access control.

DO NOT REPRINT
© FORTINET



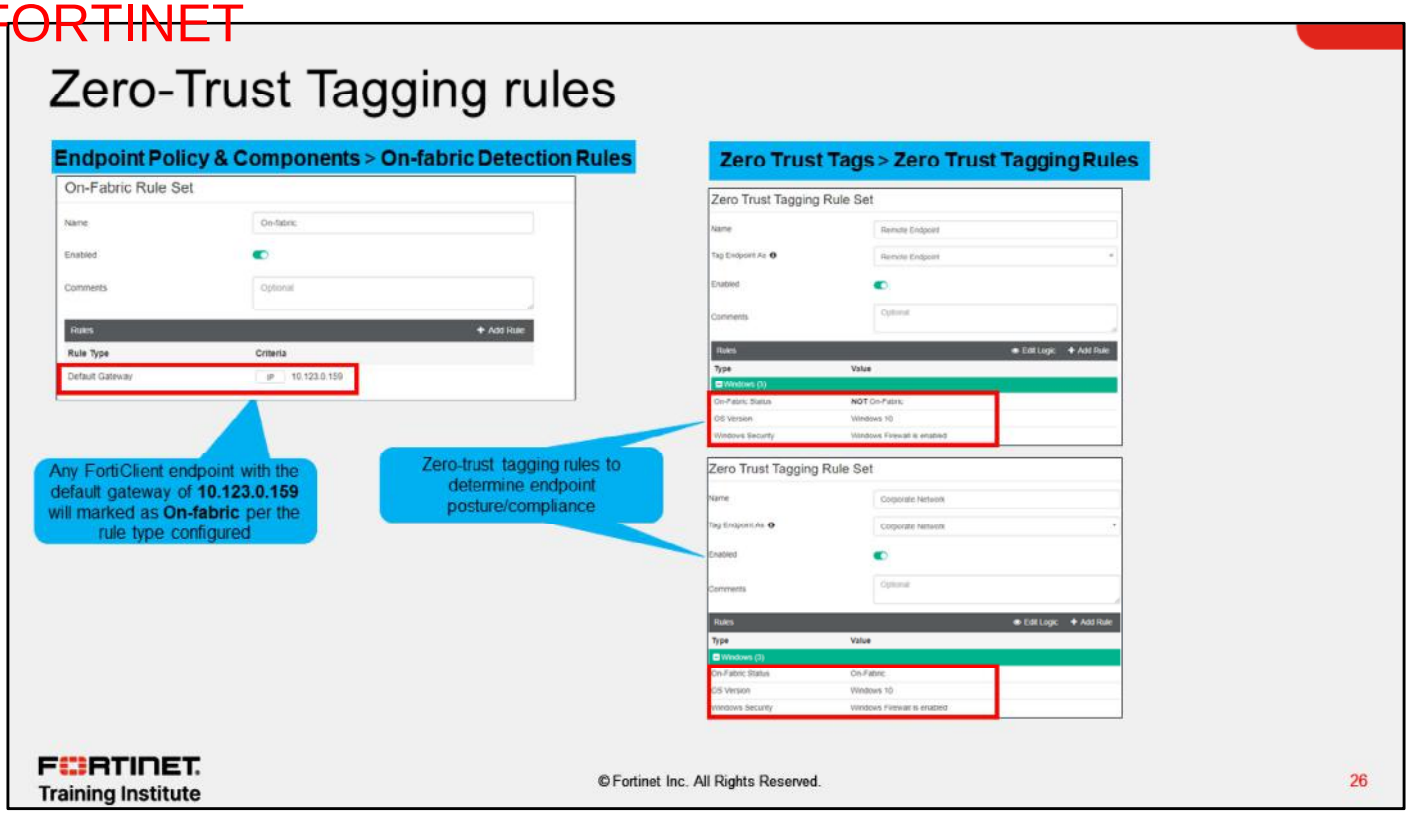
In this section, you will learn about verifying ZTNA operations.

DO NOT REPRINT
© FORTINET



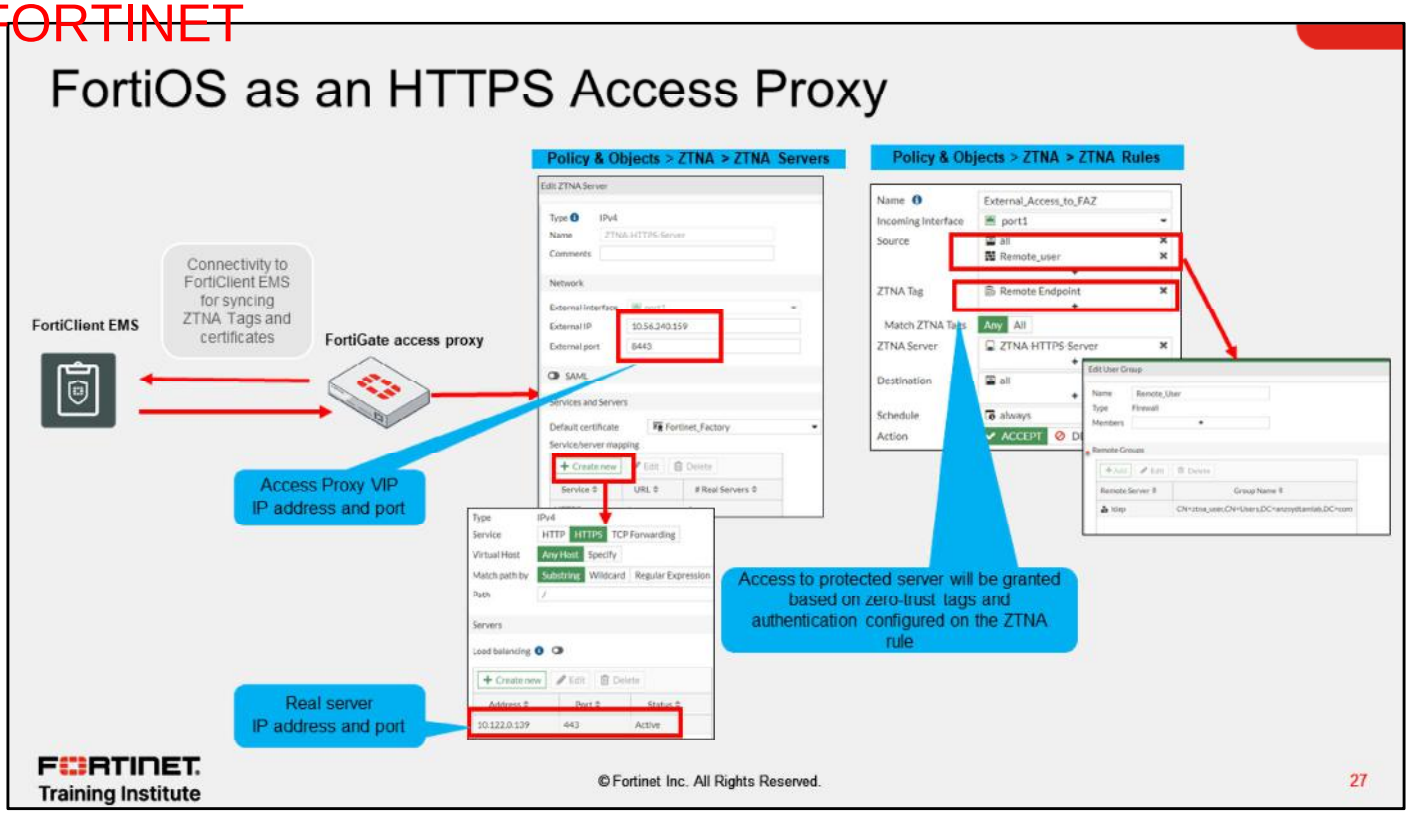
In this topology, the off-fabric client accesses the protected server FortiAnalyzer using ZTNA proxy policy. The on-fabric client accesses the same protected server using IP/MAC-based access control policy. You will review and verify the ZTNA operation for this topology.

DO NOT REPRINT
© FORTINET



The example on this slide shows a **On-Fabric Rule Set** configured with the **Rule Type** of **Default Gateway**. If an endpoint has a default gateway of `10.123.0.159`, it will be marked as on fabric. Per the **Zero Trust Tagging Rule Set,** the endpoint will be tagged as **Remote Endpoint**, if it has an off-fabric status, Windows 10 operating system, and windows firewall enabled. An endpoint will be tagged as **Corporate Network**, if it has an on-fabric status, Windows 10 operating system, and windows firewall enabled.

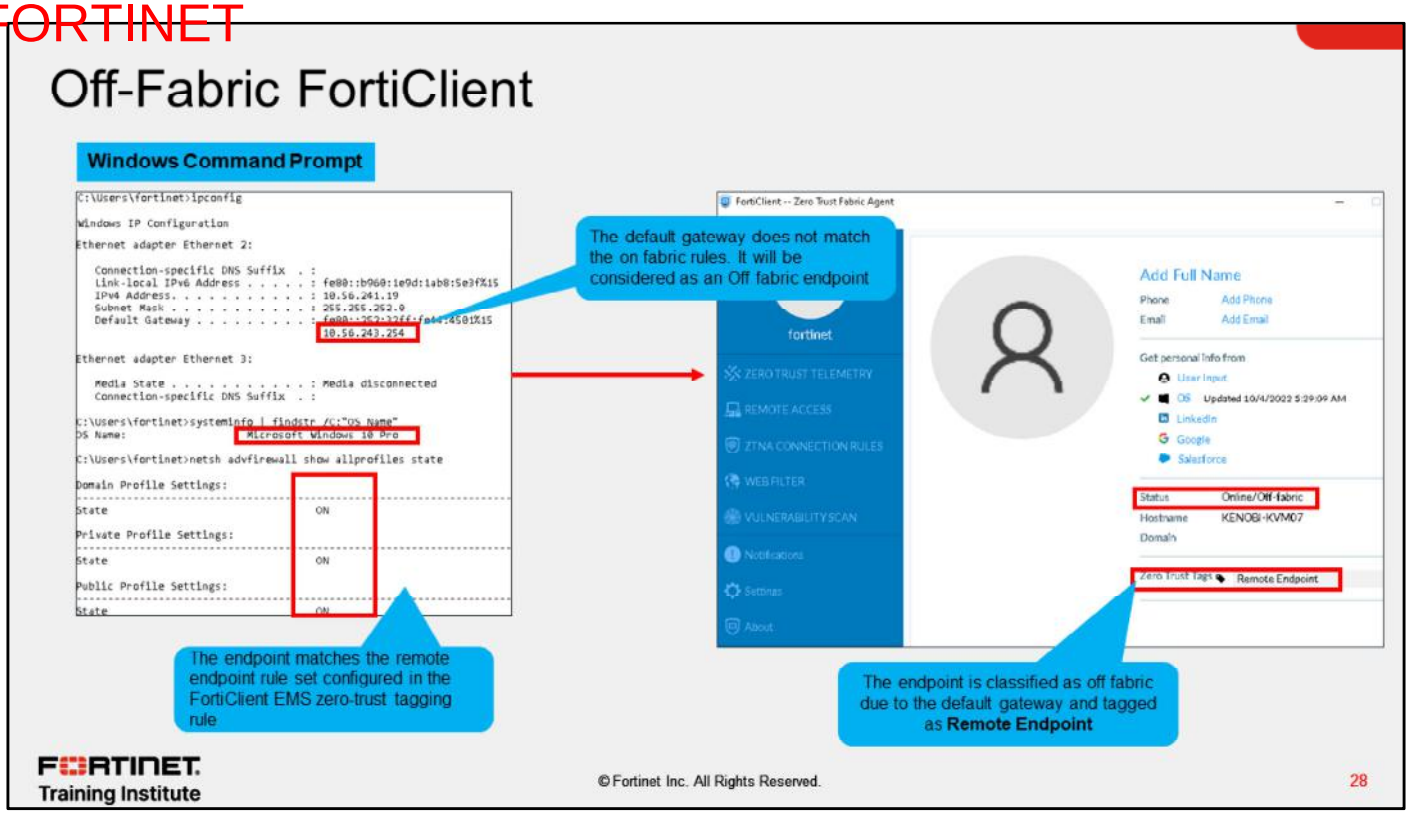
DO NOT REPRINT
© FORTINET



The configuration example on this slide shows access proxy VIP and the real server IP. The IP address `10.56.240.159` and port 8443 is an access proxy VIP that the client connects to, and then the request redirects the client to real server IP address `10.122.0.139` on port 443. In the **Service/server mapping** window, you can select **Any Host** so that any request that resolves to the access proxy VIP is mapped to the real servers.

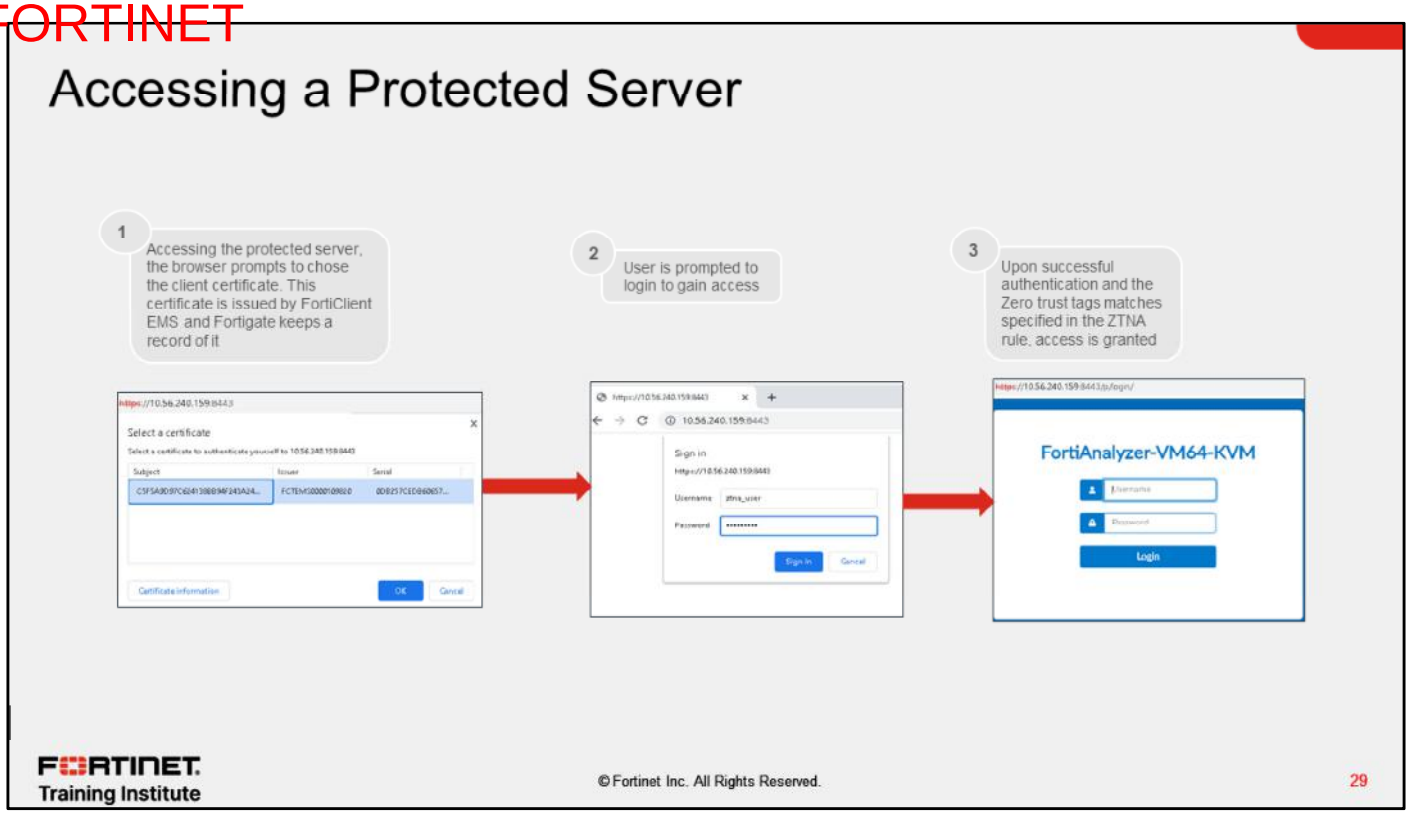
The ZTNA rule is configured to allow endpoints that are part of the user group **Remote_user** and tagged as **Remote Endpoint**. The **Remote_user** user group has an LDAP user **ztna_user** as part of it.

DO NOT REPRINT
© FORTINET



This slide shows the default gateway of the endpoint is `10.56.243.254`. It does not match the default gateway that was previously configured in the on-fabric rule set, and the endpoint is marked as **Off-fabric**. The endpoint matches all the zero trust-tagging rules of fabric status, OS version, and windows firewall state specified in the Remote Endpoint zero-trust tag. The endpoint is tagged with the zero-trust tag **Remote Endpoint**.

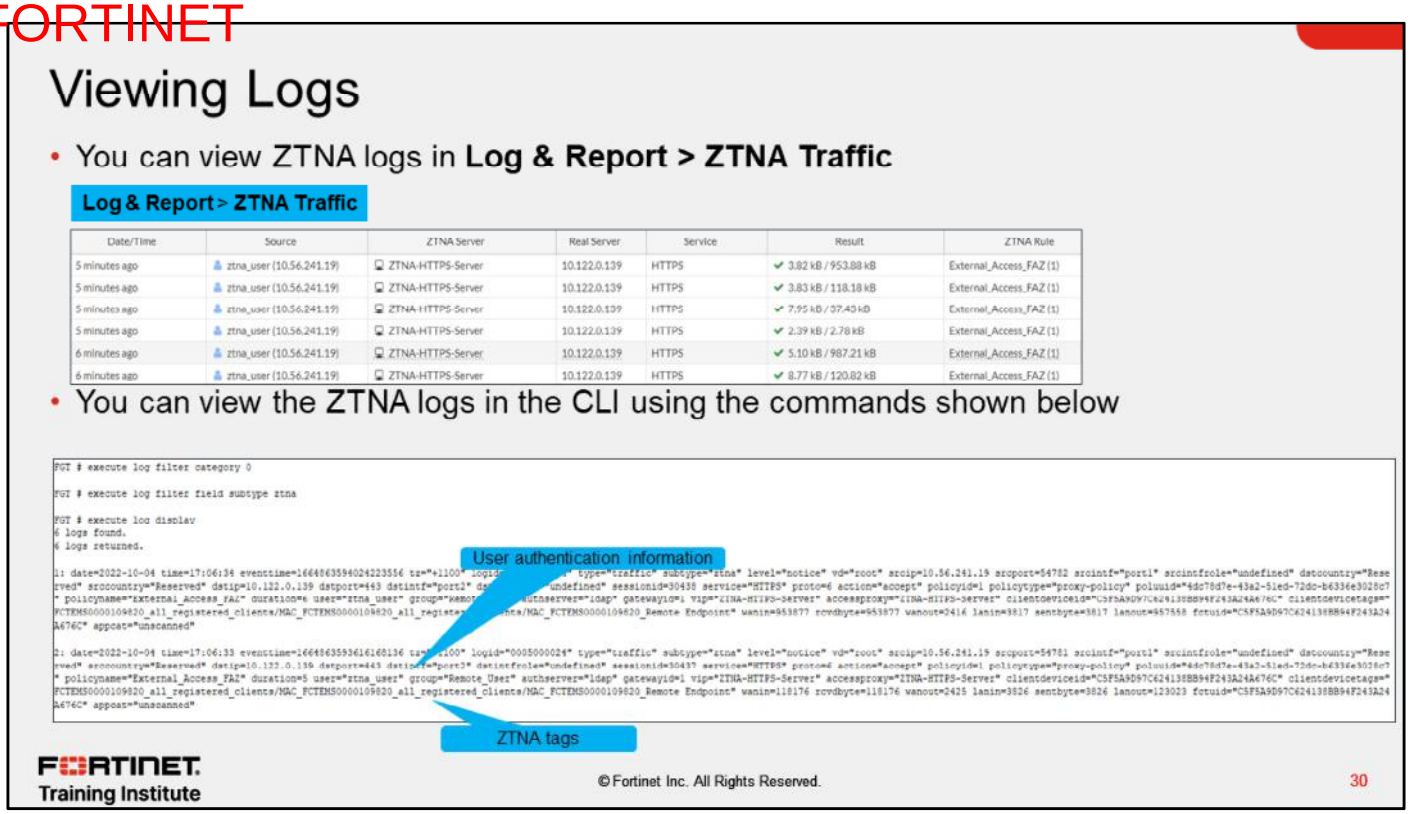
DO NOT REPRINT
© FORTINET



This slide shows the flow of events while accessing a ZTNA-protected server from an off-fabric endpoint with the ZTNA tag Remote Endpoint.

1. The end user accesses the protected server using the URL https://10.56.240.159:8443. The user is presented with the FortiClient EMS issued certificate to verify the device with the FortiGate.
2. After the certificate has been selected, the user is prompted to enter their credentials to verify the user identity.
3. Upon successful authentication, the ZTNA tags are verified by FortiGate for device posture, and access is granted to the protected server FortiAnalyzer.

DO NOT REPRINT
© FORTINET

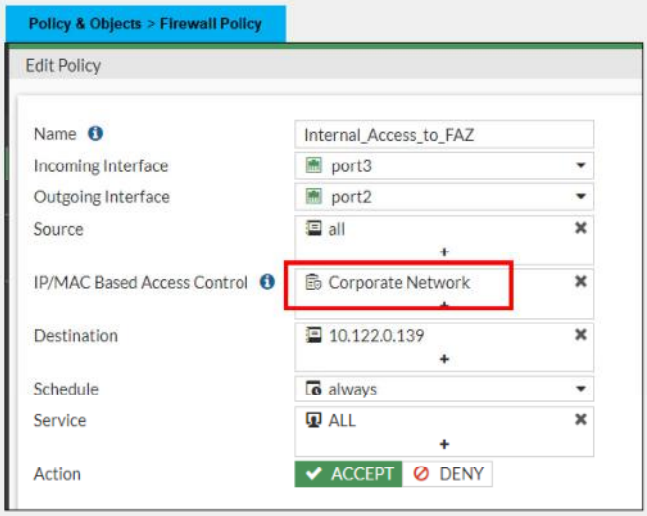


You can view the ZTNA logs by clicking **Log & Report** > **ZTNA Traffic** on the FortiGate GUI or using the CLI commands shown on this slide. The logs contains information about ZTNA tags, user authentication, client certificate validation, and so on.

DO NOT REPRINT
© FORTINET

On-Fabric FortiClient Using IP/MAC-Based Access Control

- Zero trust tags are added to regular firewall policy
- Authentication methods like FSSO, LDAP, and so on can be used as other matching criteria on the firewall policy



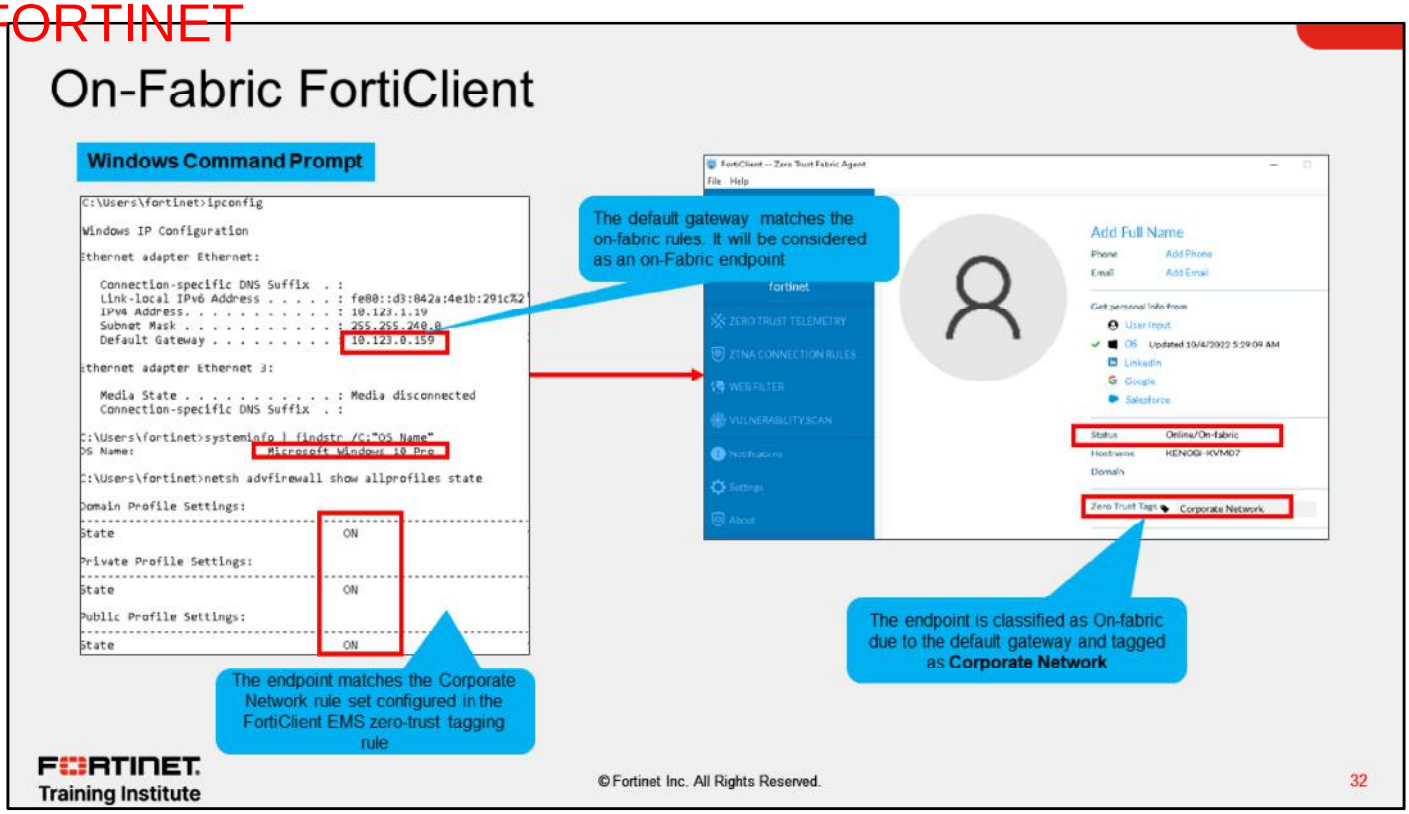
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

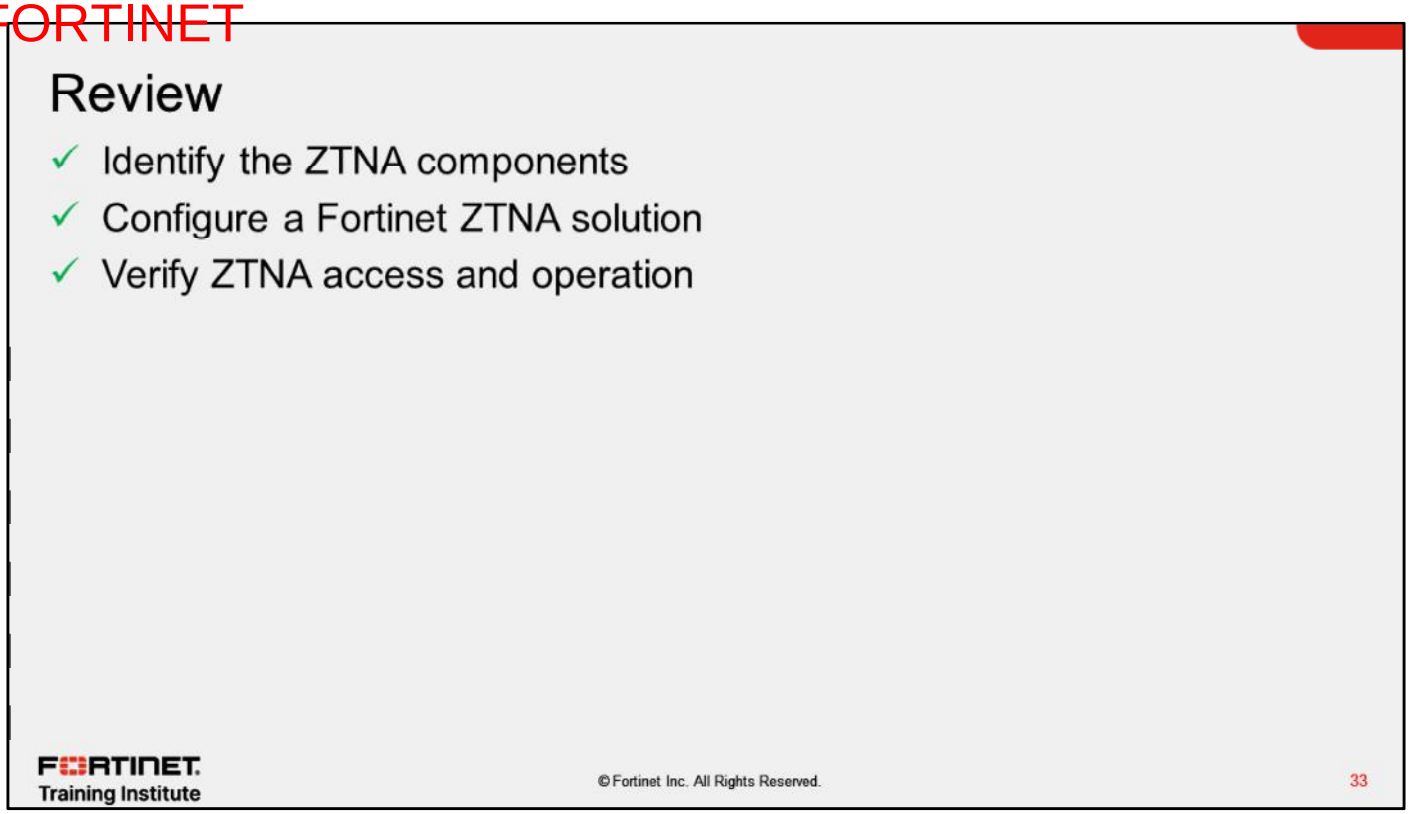
In this example, the firewall policy is configured to allow endpoints that are tagged as **Corporate Network** to access the protected server FortiAnalyzer using IP/MAC-based access control. You can use authentication methods like FSSO, LDAP, and so on as other matching criteria on the firewall policy, if required.

DO NOT REPRINT
© FORTINET



This slide shows the default gateway of the endpoint is `10.123.0.159`. It matches the default gateway that was previously configured in the on-fabric rule set and the endpoint will be marked as **On-fabric**. The endpoint matches all the zero-trust tagging rules of fabric status, OS version, and windows firewall state specified in the Corporate Network zero-trust tag. The endpoint will be tagged as **Corporate Network**. The end user on this endpoint can access the protected server FortiAnalyzer with its internal IP of `10.122.0.139` and the ZTNA tags are used for access control.

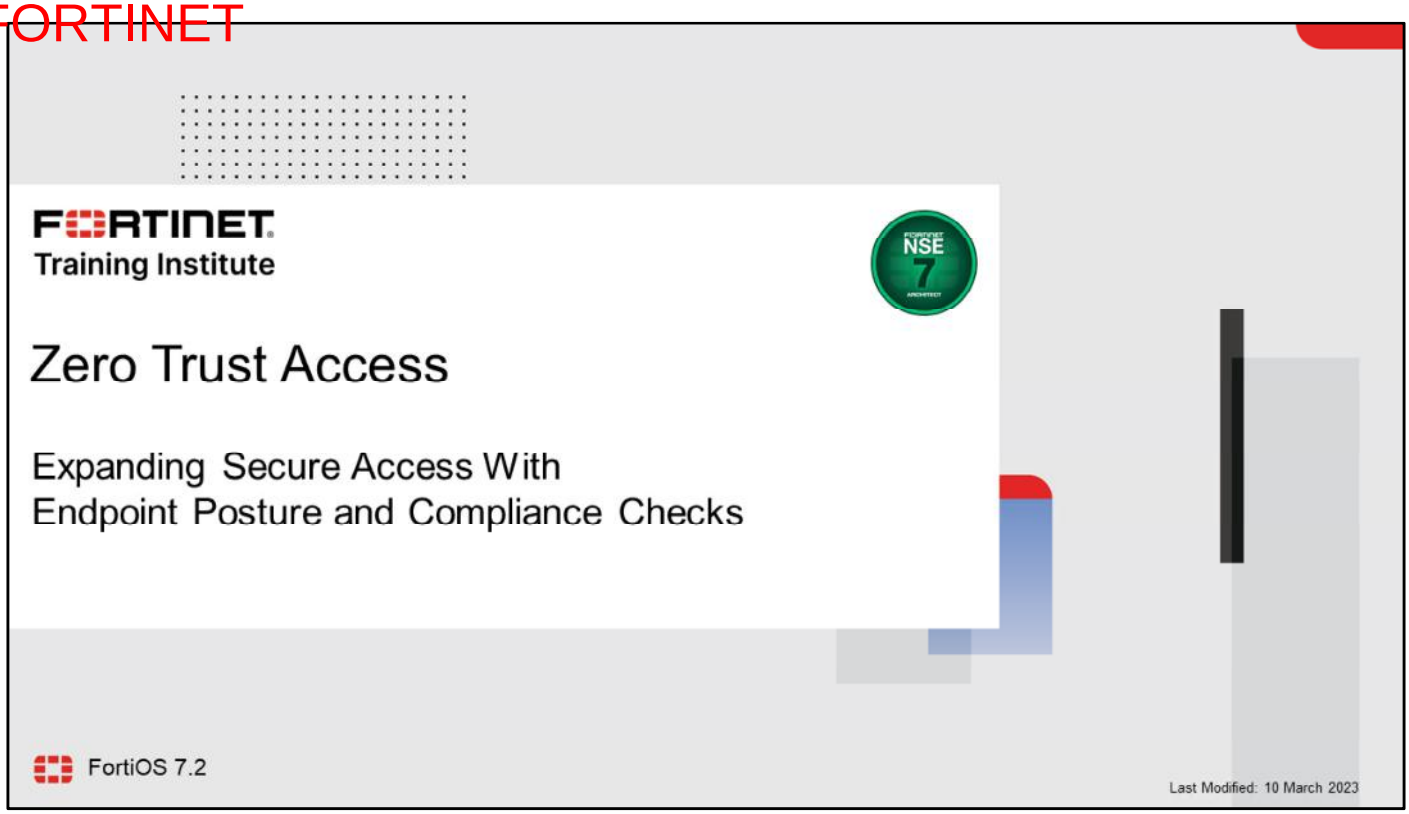
DO NOT REPRINT
© FORTINET



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

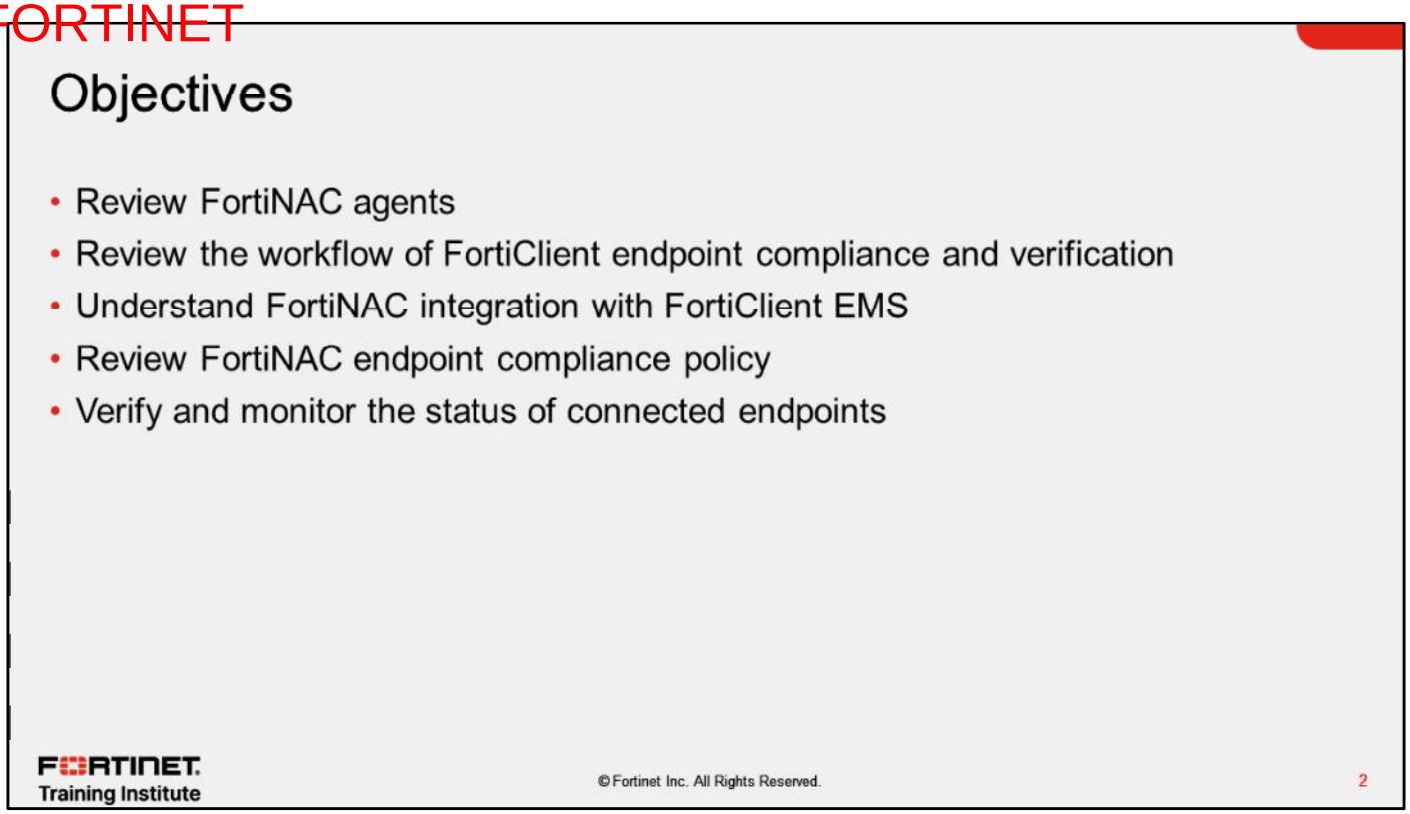
By mastering the objectives covered in this lesson, you learned about ZTNA configuration and its operation.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about expanding secure access with endpoint posture and compliance checks.

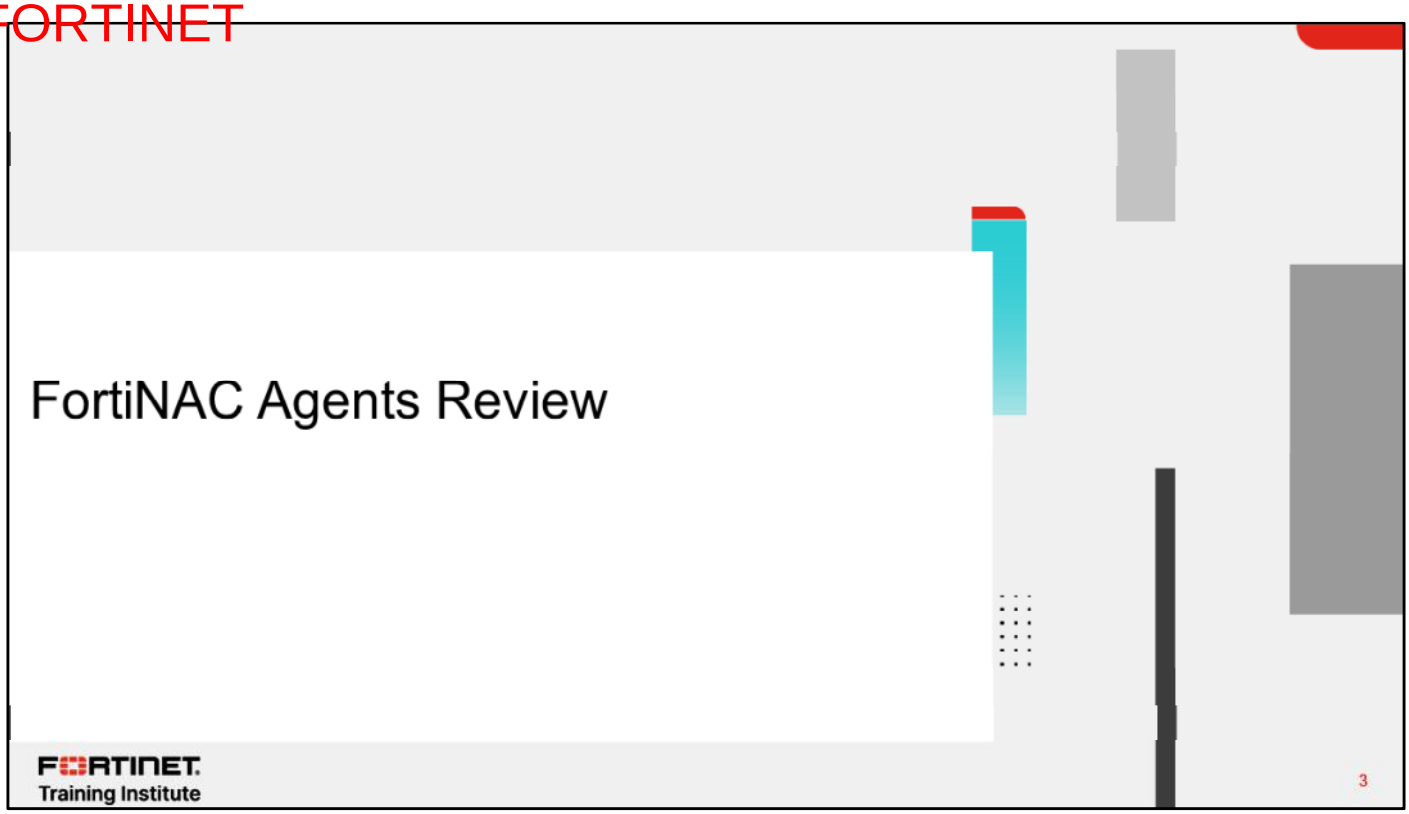
DO NOT REPRINT
© FORTINET



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

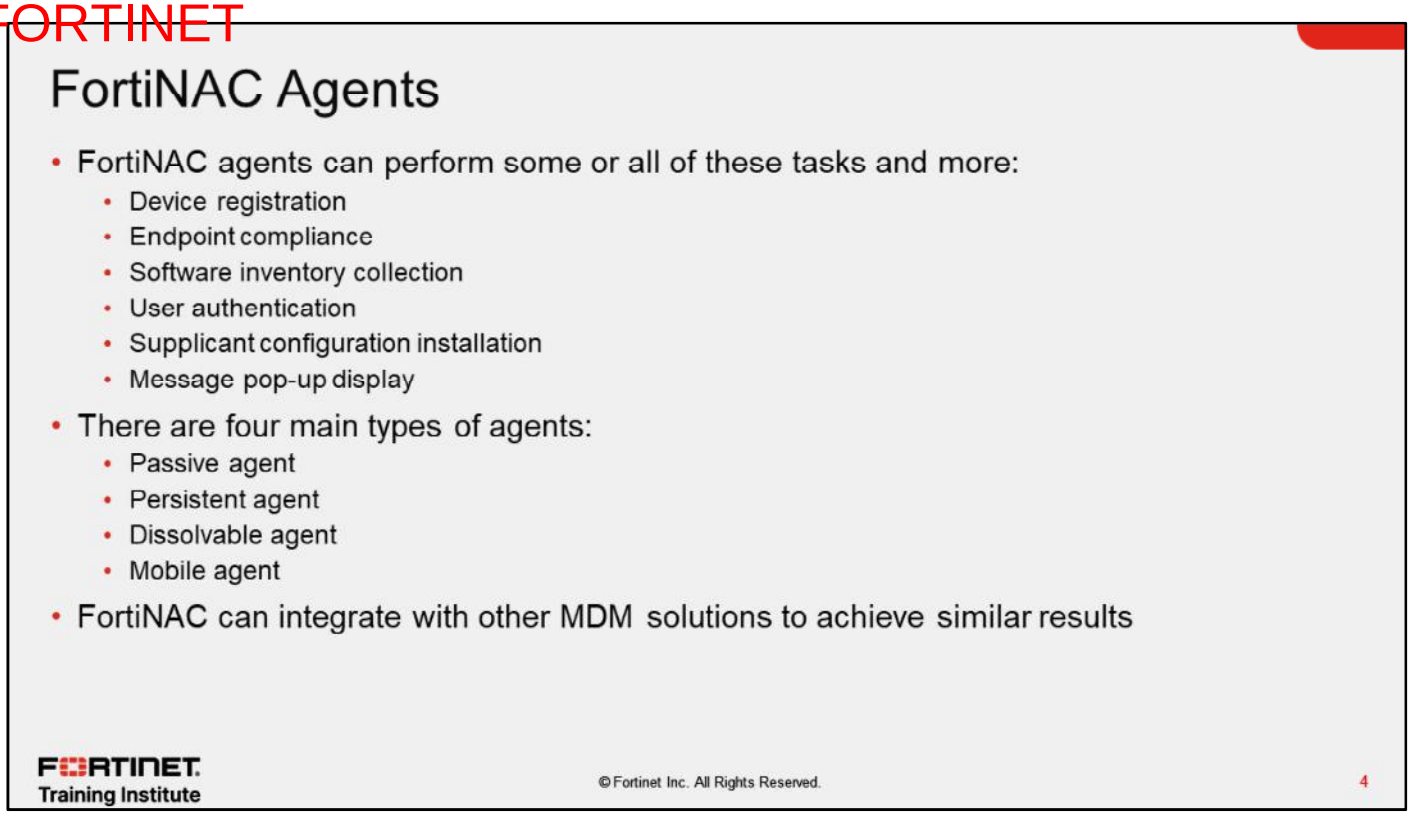
By demonstrating competence in endpoint compliance, you will understand different FortiNAC agent implementations, the workflow of FortiClient endpoint compliance, and monitoring connected endpoints. You will also be familiar with FortiNAC integration with FortiClient EMS.

DO NOT REPRINT
© FORTINET



In this section, you will learn about different FortiNAC agents.

DO NOT REPRINT
© FORTINET



Endpoint compliance is a feature set used to ensure that hosts connecting to your network comply with network usage requirements. Endpoint compliance can also use an agent on the host to ensure that compliance with established policies is maintained by scanning hosts and determining whether the host complies with the endpoint compliance policy assigned to that host. Agents can perform additional functions, such as installing a supplicant configuration for a secure network.

There are four main types of agents available with FortiNAC: the dissolvable agent, the passive agent, the persistent agent, and the mobile agent.

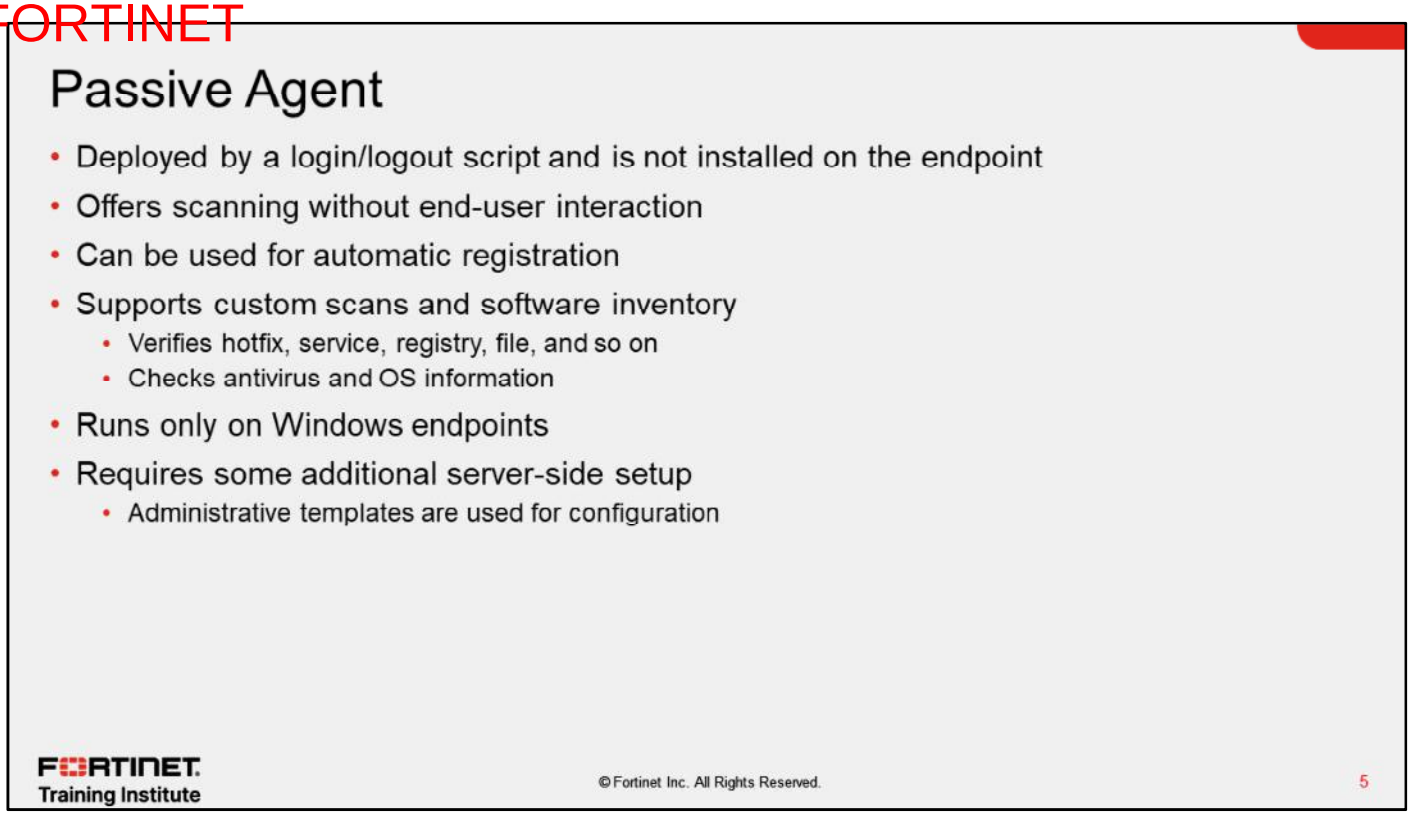
The first step in implementing endpoint compliance is determining whether you will use the persistent agent, the dissolvable agent, the passive agent, the mobile agent, or a combination.

- The persistent agent is installed on the host and remains there to scan the computer as needed.
- The dissolvable agent is downloaded to the host and removes itself once the host has passed the security scan. If the host does not pass the scan, the dissolvable agent remains on the host for the user to run again after resolving any compliance issues.
- The passive agent is deployed using login scripts, and launched when the user logs in to the domain. Users experience a slight delay while logging in, but are unaware that their hosts are being scanned.
- The mobile agent is installed on Android devices and is downloaded from either the captive portal or Google Play.

There are situations in which one agent works better than others. For example, network users who log in to your network every day might use the persistent agent while guest users might use the dissolvable agent.

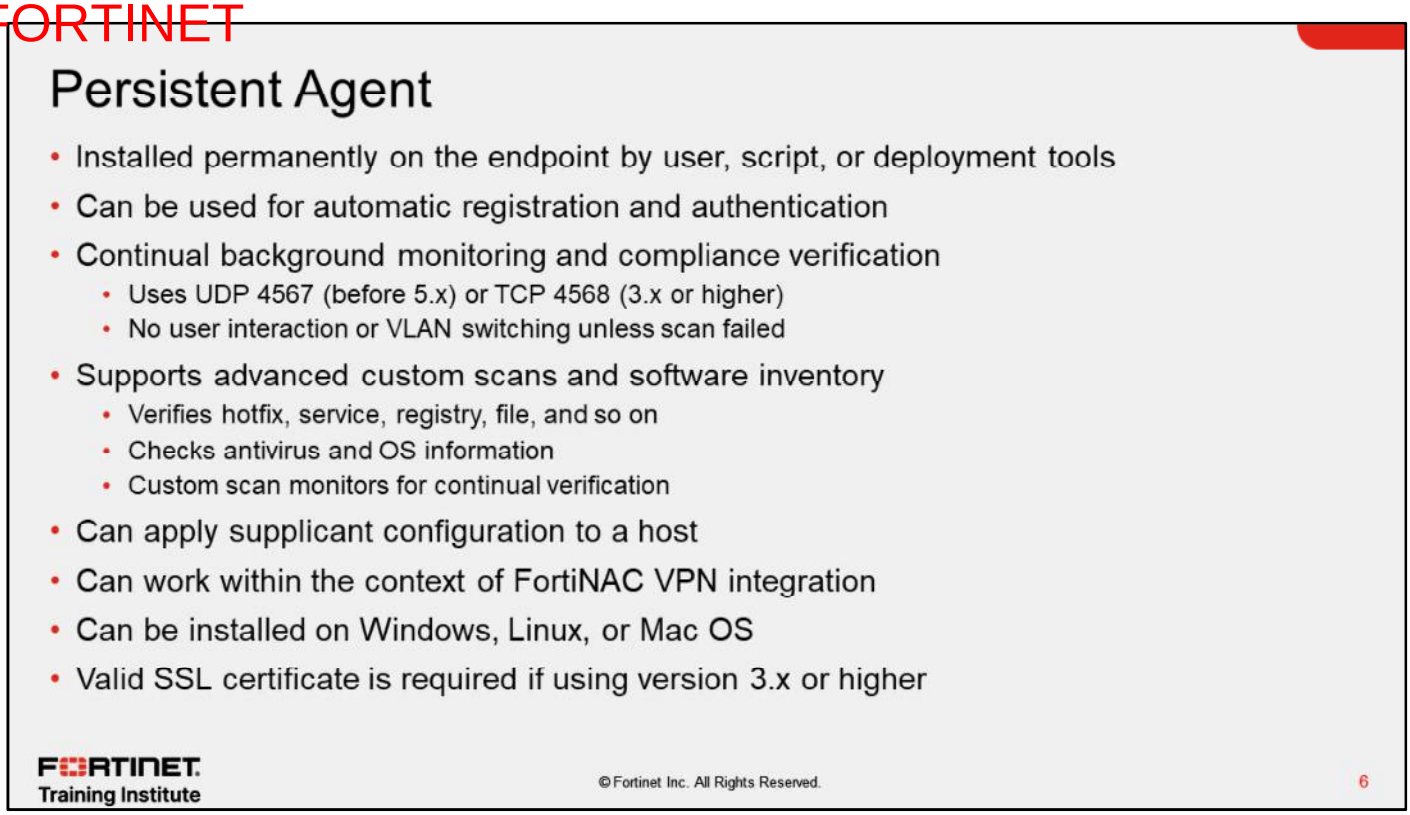
FortiNAC and the mobile device management (MDM) system work together to share data through an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network.

DO NOT REPRINT
© FORTINET



The passive agent registers and scans endpoints that are joined to a domain when a domain user logs in. You can deploy the agent using a login script, and use administrative templates to configure it. The administrative templates are installed and configured on the domain controller with the fully qualified domain name of the FortiNAC device. As a result, when the agent runs, it knows where to send the results. Place the agent executable in a user accessible location, and configure the login and logout script to execute the agent. If the endpoint is configured to register at login, it registers the first time and remains registered until it expires based on configurable aging timers. You can also use the passive agent to track users as they log in and log out of domain machines.

DO NOT REPRINT
© FORTINET

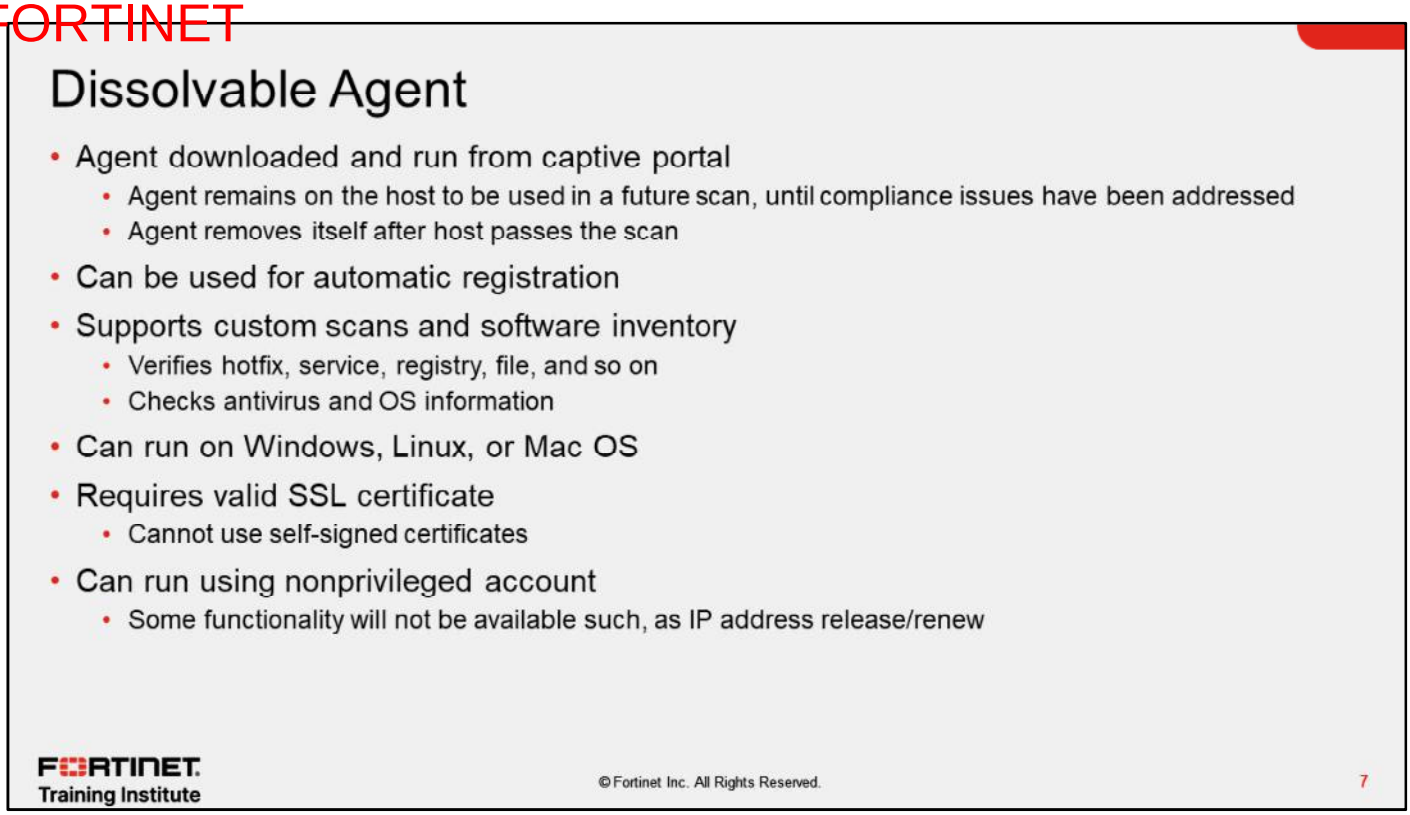


The FortiNAC persistent agent is an install-and-stay resident agent. There are several types of persistent agents available for use, depending on the method of deployment. The EXE, DMG, DEB, and RPM types are normally deployed from within the captive portal environment during endpoint onboarding. This enables the configuration of the agents through server communication, as they are installed.

The MSI is typically deployed as part of the group policy or by some other software distribution mechanism. When an agent is deployed as part of the group policy, the administrative templates can be installed on the active directory for agent configuration. When being deployed by other means, a set of registry key entries must be deployed or configured as well.

The behavior of the agent, and the FortiNAC server it communicates with, is configured in the registry on Windows systems. Similar configurations are used on Mac systems and DNS SRV records can be used. Installation scripts can be run on Linux systems for configuring these values.

DO NOT REPRINT
© FORTINET



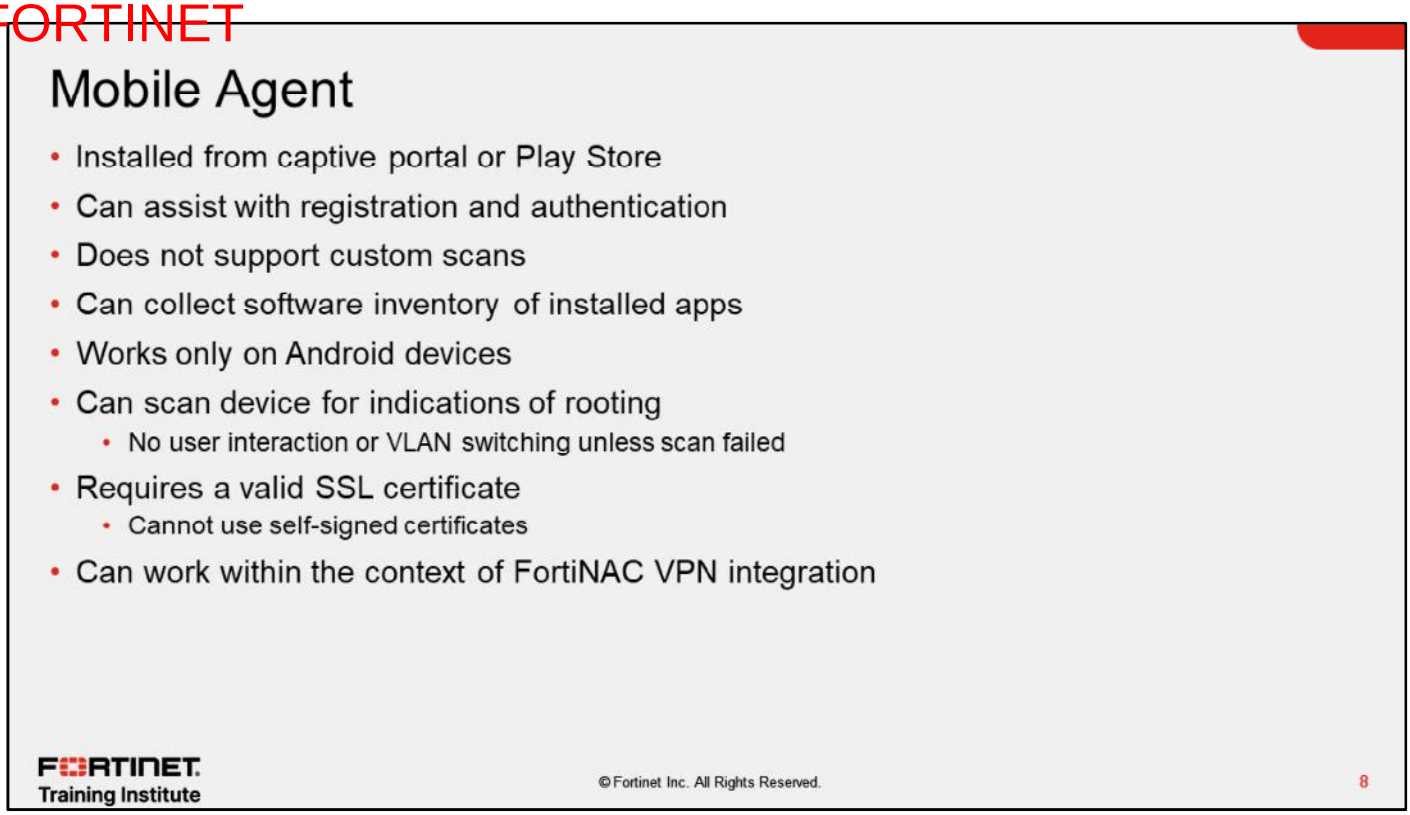
Access the passive agent rules from the **Security Configuration** > **Passive Agent** view.

Passive agent registration helps you create customized configurations that register and scan hosts that are associated with network users contained in your LDAP or active directory. Scanning requires an agent; however, the agent does not need to be installed by the user. The agent is provided using an external method, such as group policy objects, and launched when the user logs in to the domain.

When a user connects to the network and logs in, FortiNAC determines the directory group to which the user belongs. Based on that group, a passive agent configuration is used. The configuration registers the user and the associated host in FortiNAC. If enabled, the agent scans the host to verify that it is in compliance with the appropriate endpoint compliance policy. You can specify the scan in the configuration, or FortiNAC can determine it, based on the user/host profile of the user or host.

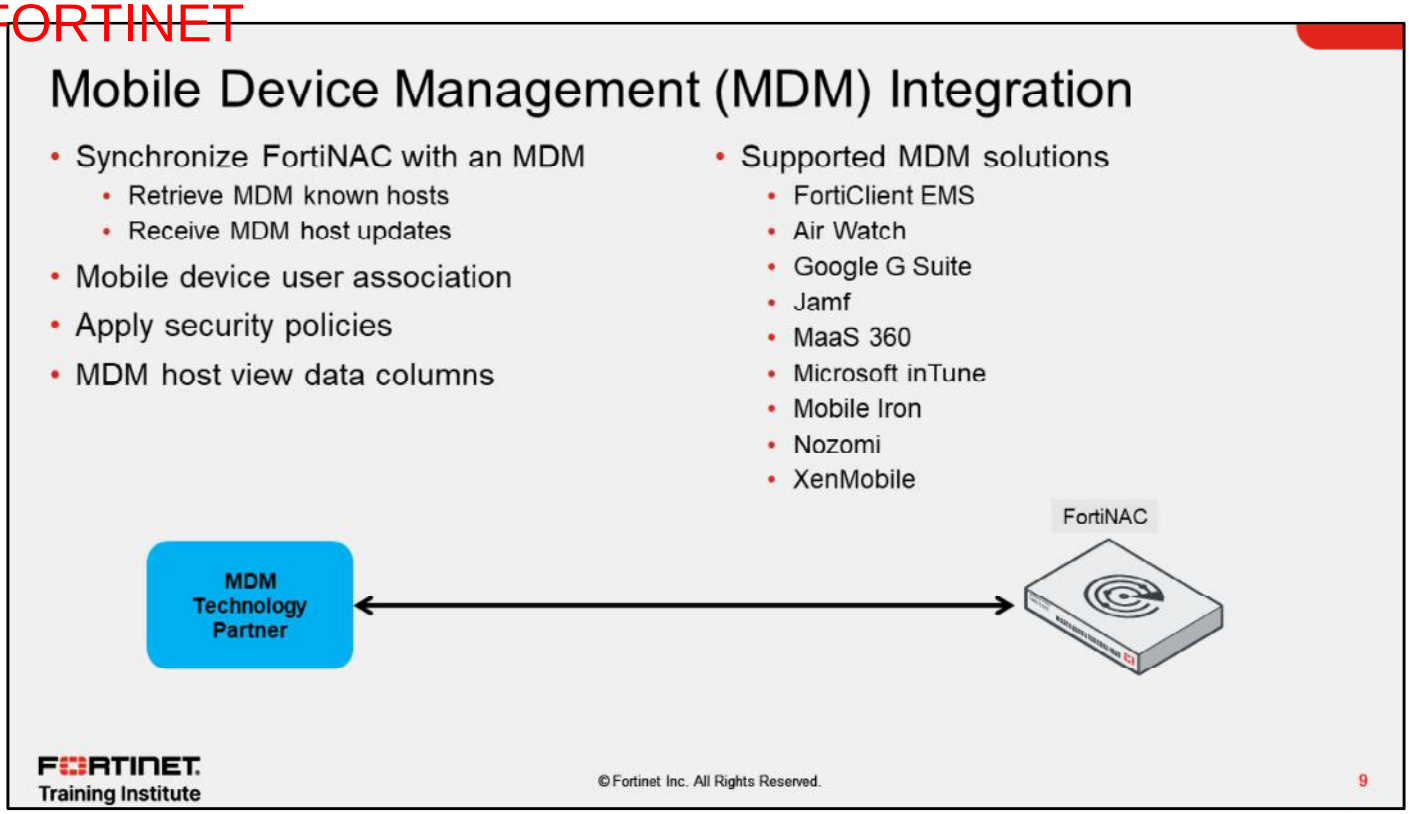
You can also use a passive agent configuration to track user logins and logouts on hosts with the persistent agent installed. To create a passive agent configuration that does not apply to any domain group members, leave the checkbox empty. The different configurations can be ranked with the more specific ones first.

DO NOT REPRINT
© FORTINET



After the persistent agent is deployed, it initiates communication back to the FortiNAC server every 15 minutes. The persistent agent performs scheduled scans in the background that are transparent to the end user. To use system messaging, go to the **Bookmarks** menu, or right-click a specific host in the host view and select **Send Message**.

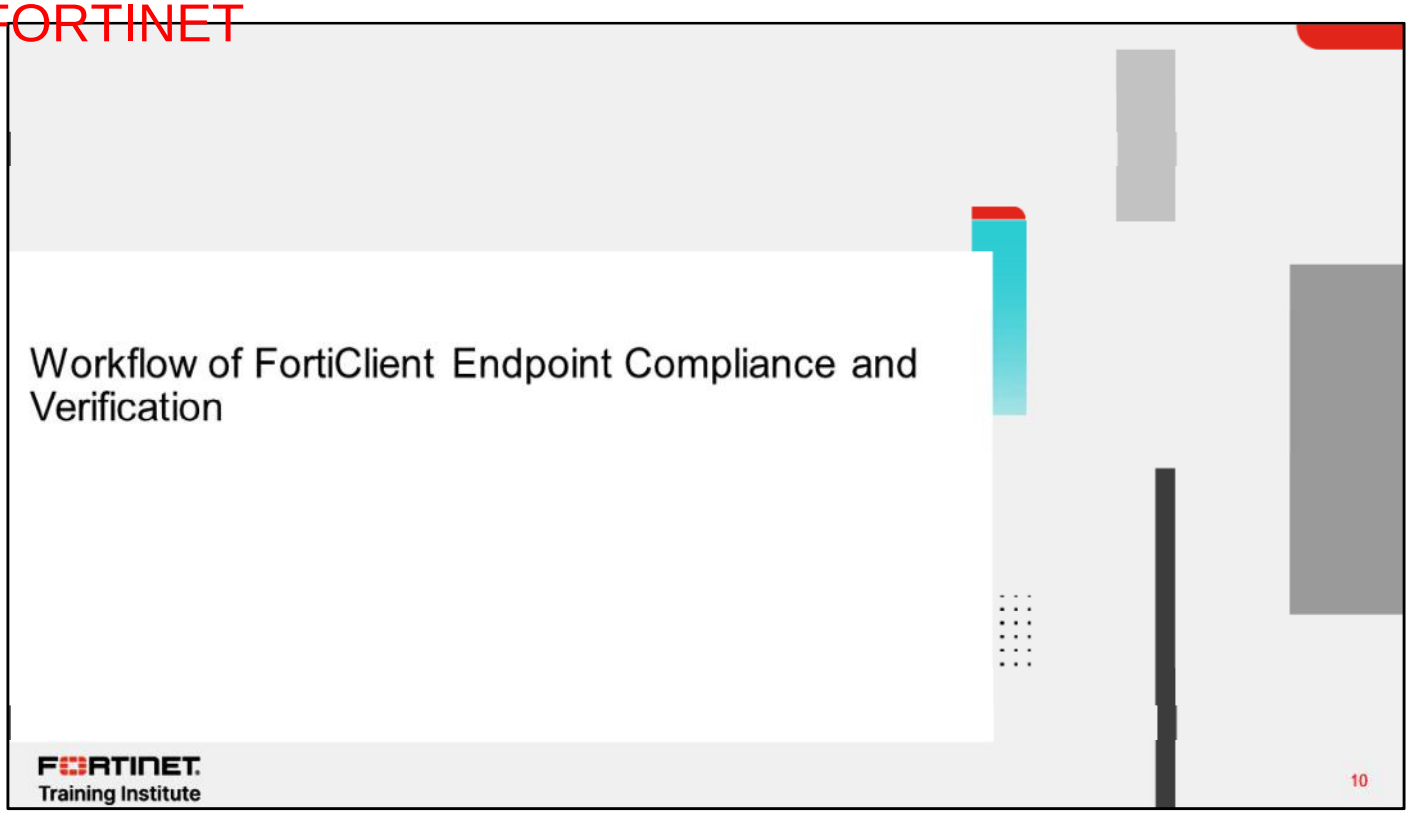
DO NOT REPRINT
© FORTINET



MDM services help you configure the connection or integration between FortiNAC and an MDM. FortiNAC and the MDM system work together to share data through an API, to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network. You can pull down device application inventories from some MDMs to enhance the visibility of connecting mobile devices. You can use email addresses to make user associations between existing users and newly added devices. You can also leverage security policies by matching attributes that are passed down from the MDM, and see additional host information that is available within the host view.

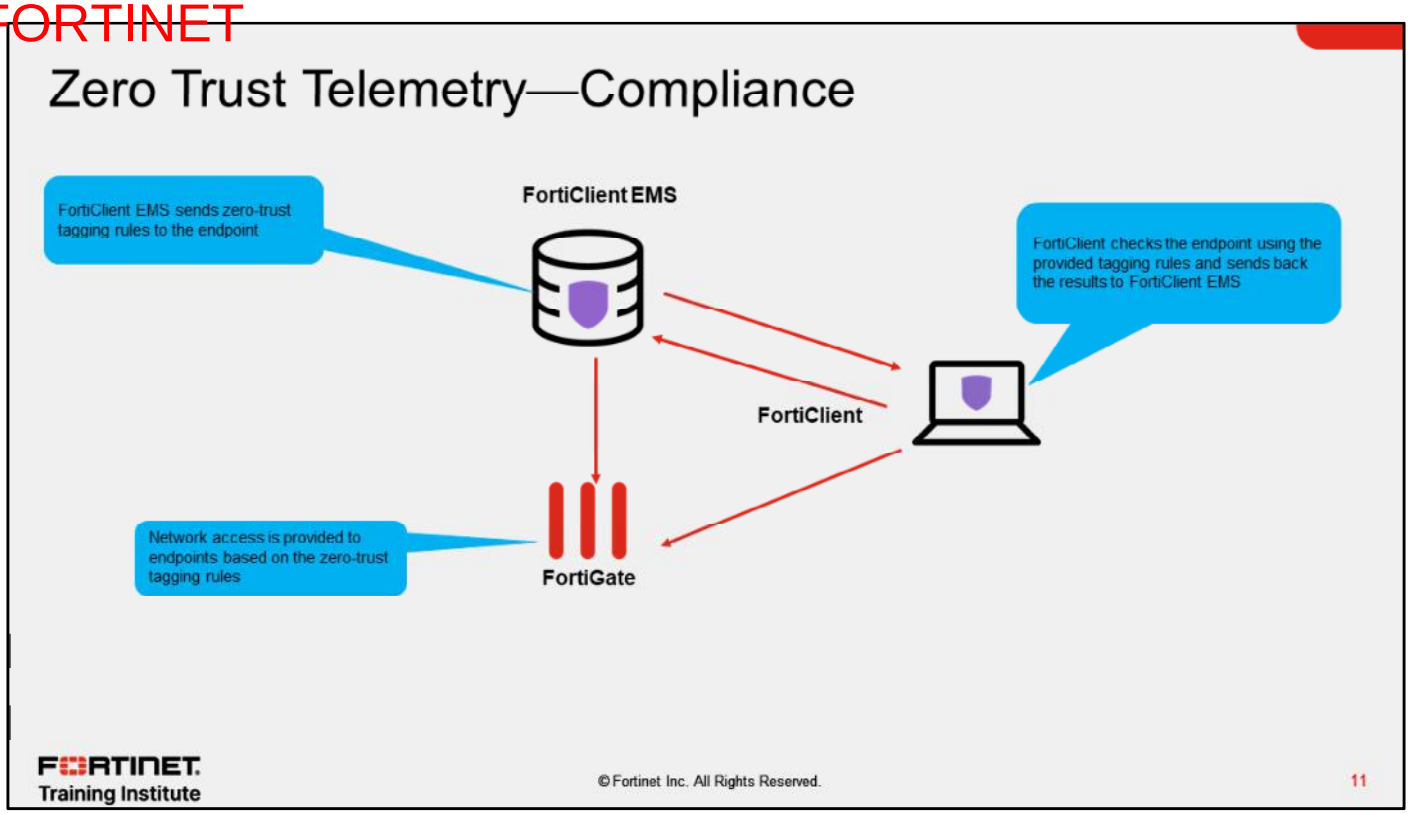
The supported vendors are: AirWatch, FortiClient EMS, Google G Suite, Jamf, MaaS360, Microsoft In Tune, Mobile Iron, Nozomi, and XenMobile.

DO NOT REPRINT
© FORTINET



In this section, you will learn the workflow of FortiClient endpoint compliance and verification.

DO NOT REPRINT
© FORTINET



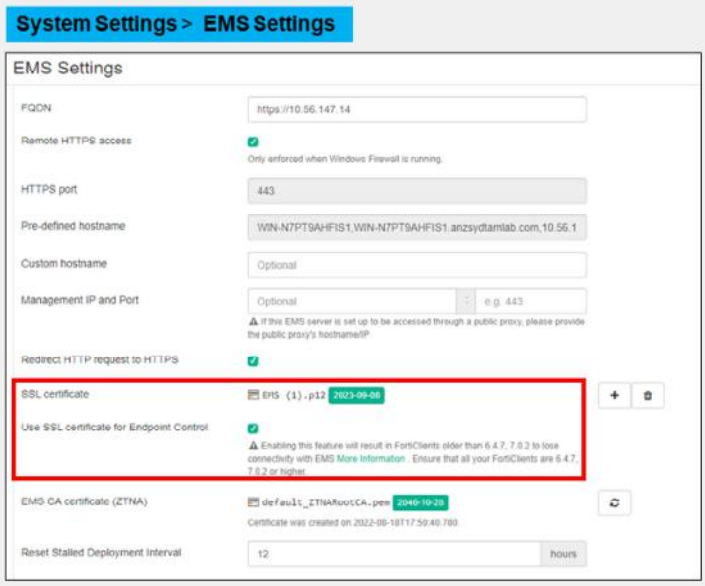
This slide shows how FortiClient EMS and FortiGate check for compliance:

1. FortiClient EMS is connected to FortiGate as a participant in the Security Fabric.
2. FortiClient Telemetry attempts to connect to FortiClient EMS. Based on the FortiClient EMS configuration, FortiClient may receive an SSL certificate from EMS to verify the connection.
3. FortiClient EMS sends the endpoint information received through FortiClient Telemetry to FortiOS.
4. Zero-trust tagging rules are configured in FortiClient EMS, based on criteria such as certificates, the logged in domain, files present, OS versions, running processes, registry keys, and so on.
5. FortiClient EMS sends zero-trust tagging rules to the endpoint.
6. FortiClient checks the endpoint using the provided zero trust tagging rules and sends back the results to FortiClient EMS
7. FortiClient EMS dynamically groups the endpoint, based on the zero-trust tagging rules.
8. FortiOS can receive the dynamic endpoint groups from FortiClient EMS and use them to create dynamic firewall policies.
9. Network access is provided to the endpoint, based on the zero-trust tagging rules.

DO NOT REPRINT
© FORTINET

Endpoint Control Security

- The connection from FortiClient to FortiClient EMS uses TCP and TLS 1.3
- FortiClient EMS sends FortiClient a server certificate during SSL connection
- Server certificate can be configured on FortiClient EMS GUI in **System Settings > EMS Settings**
- **Use SSL certificate for Endpoint Control** can be enabled in **System Settings > EMS Settings**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

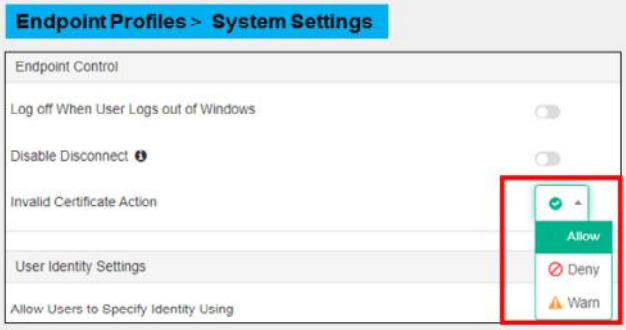
12

The connection from FortiClient to FortiClient EMS uses TCP and TLS 1.3. During the SSL connection setup, FortiClient EMS sends a server certificate to FortiClient. You can configure the certificate that FortiClient EMS sends to FortiClient in **System Settings** > **EMS Settings**.

DO NOT REPRINT
© FORTINET

Endpoint Control Security (Contd)

- FortiClient checks for the following criteria to confirm its validity:
  - Domain or fully qualified domain name (FQDN) that FortiClient is connecting to matches the domain to which the certificate is issued
  - Validation process correctly handles wildcards in the domain name in the certificate
  - Validation process considers both the common name (CN) in the subject or subject alternative name (SAN)
  - The certificate expiry date is in the future
  - The certificate issuer or the root certificate in the certificate chain is from a publicly trusted certificate authority (CA)
- If the EMS server certificate is valid, FortiClient connects silently
- If the EMS server certificate is invalid, actions can be configured in **Endpoint Profile** > **System Settings**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

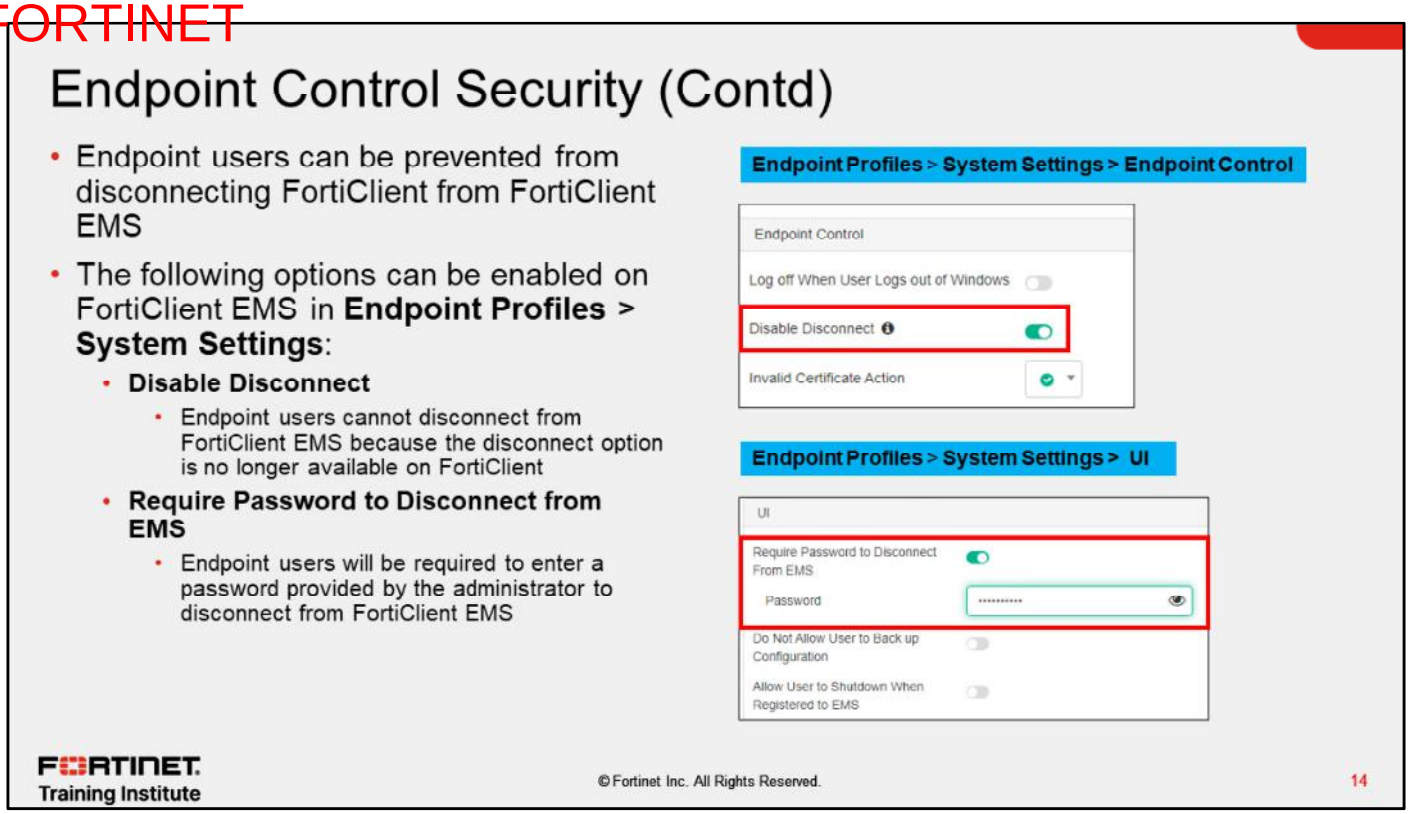
13

FortiClient validates certificates using the following industry standards:

- The domain or FQDN that FortiClient is connecting to matches the domain to which the certificate is issued.
- The validation process correctly handles wildcards in the domain name in the certificate.
- The validation process considers both the CN in the subject or the SAN.
- The certificate expiry date is in the future. The certificate has not expired.
- The certificate issuer or the root certificate in the certificate chain is from a publicly trusted CA. Trusted CAs are read from the operating system.

If the FortiClient EMS server certificate is valid, FortiClient silently connects without displaying a message. If the server certificate is invalid, the required actions can be configured in **Endpoint Profile** > **System Settings** on FortiClient EMS.

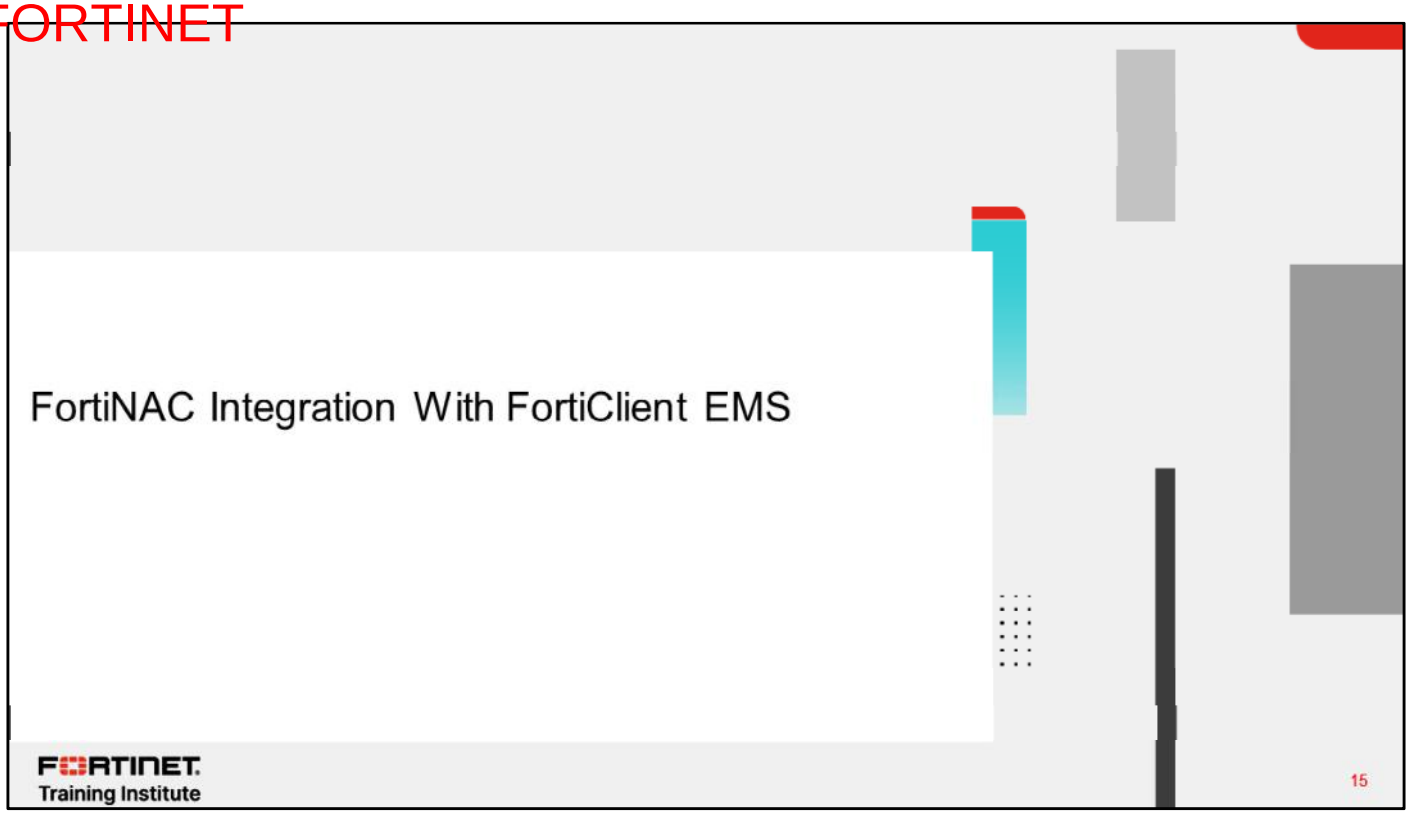
DO NOT REPRINT
© FORTINET



As part of endpoint control security, you can prevent users from disconnecting FortiClient from FortiClient EMS. You can configure the following settings in **Endpoint Profiles** > **System Settings** on FortiClient EMS:

- **Disable Disconnect**: Endpoint users cannot disconnect from FortiClient EMS because the disconnect option is no longer available on FortiClient.
- **Require Password to Disconnect from EMS**: Endpoint users will be required to enter a password provided by the administrator to disconnect from FortiClient EMS.

DO NOT REPRINT
© FORTINET

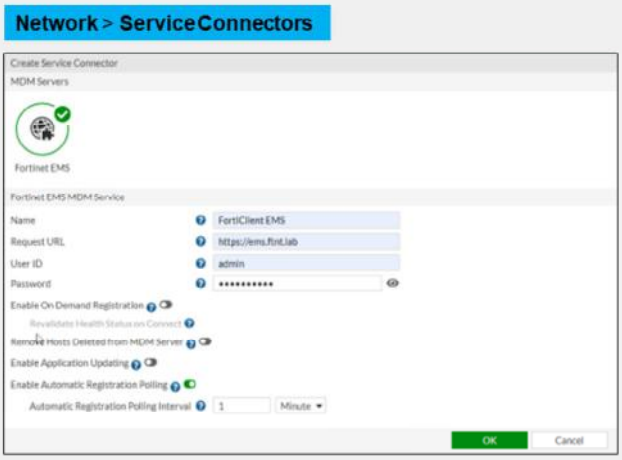


In this section, you will learn about FortiNAC integration with FortiClient EMS.

DO NOT REPRINT
© FORTINET

Configuring FortiNAC Integration With FortiClient EMS

- You can configure FortiClient EMS as a service connector in **Network > Service Connectors**
- This integration speeds up the registration process of devices that have been registered with FortiClient EMS
- Devices connecting to the network can be registered in FortiNAC using host data from FortiClient EMS



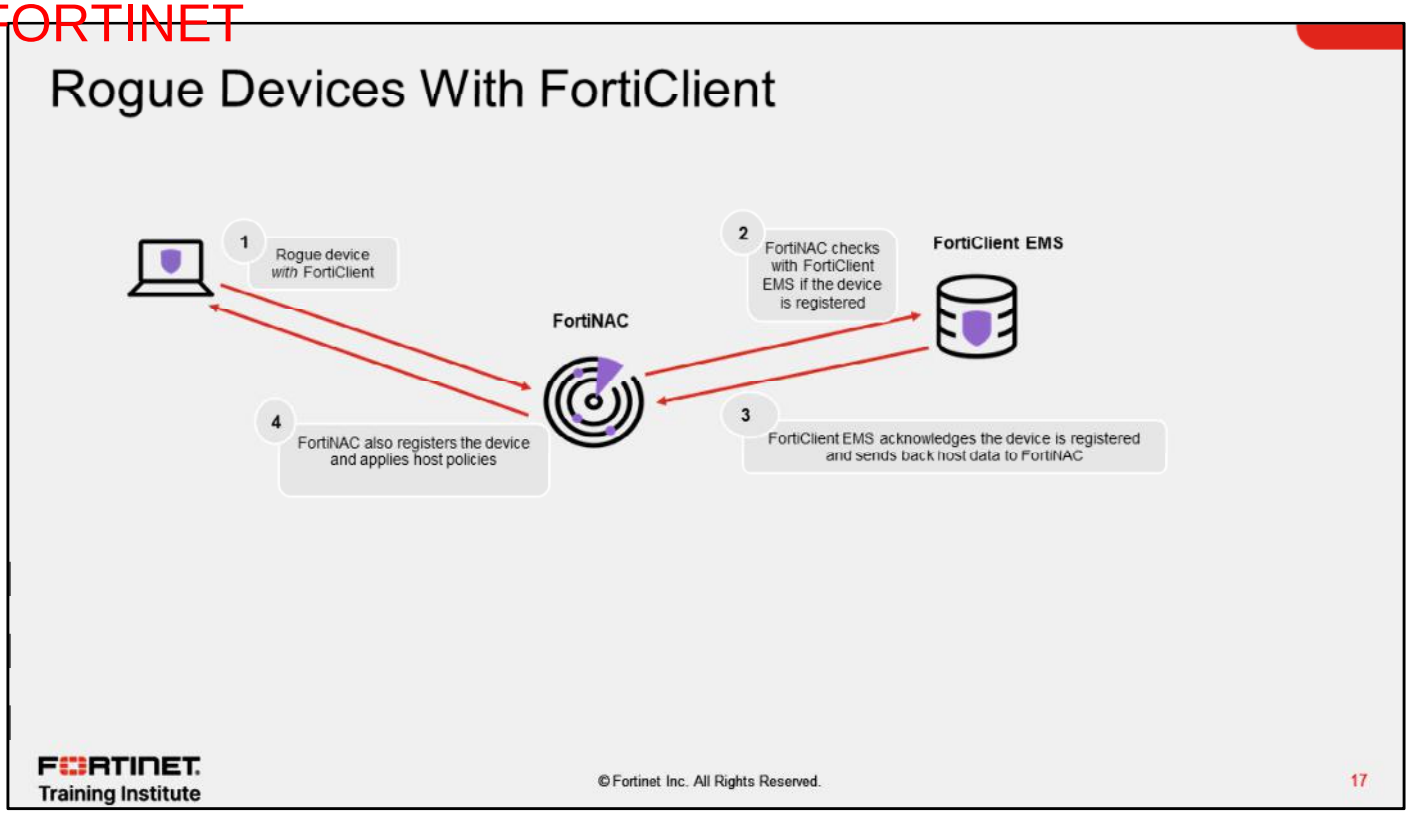
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

To integrate FortiNAC with FortiClient EMS, you must configure FortiClient EMS as a service connector on FortiNAC in **Network** > **Service Connectors**. Enter a name for FortiClient EMS, the request URL for FortiClient EMS, the username with administrator privileges, and a password. This integration speeds up the registration process of devices that have been registered with FortiClient EMS. The devices connecting to the network can be registered in FortiNAC using host data from FortiClient EMS.

DO NOT REPRINT
© FORTINET

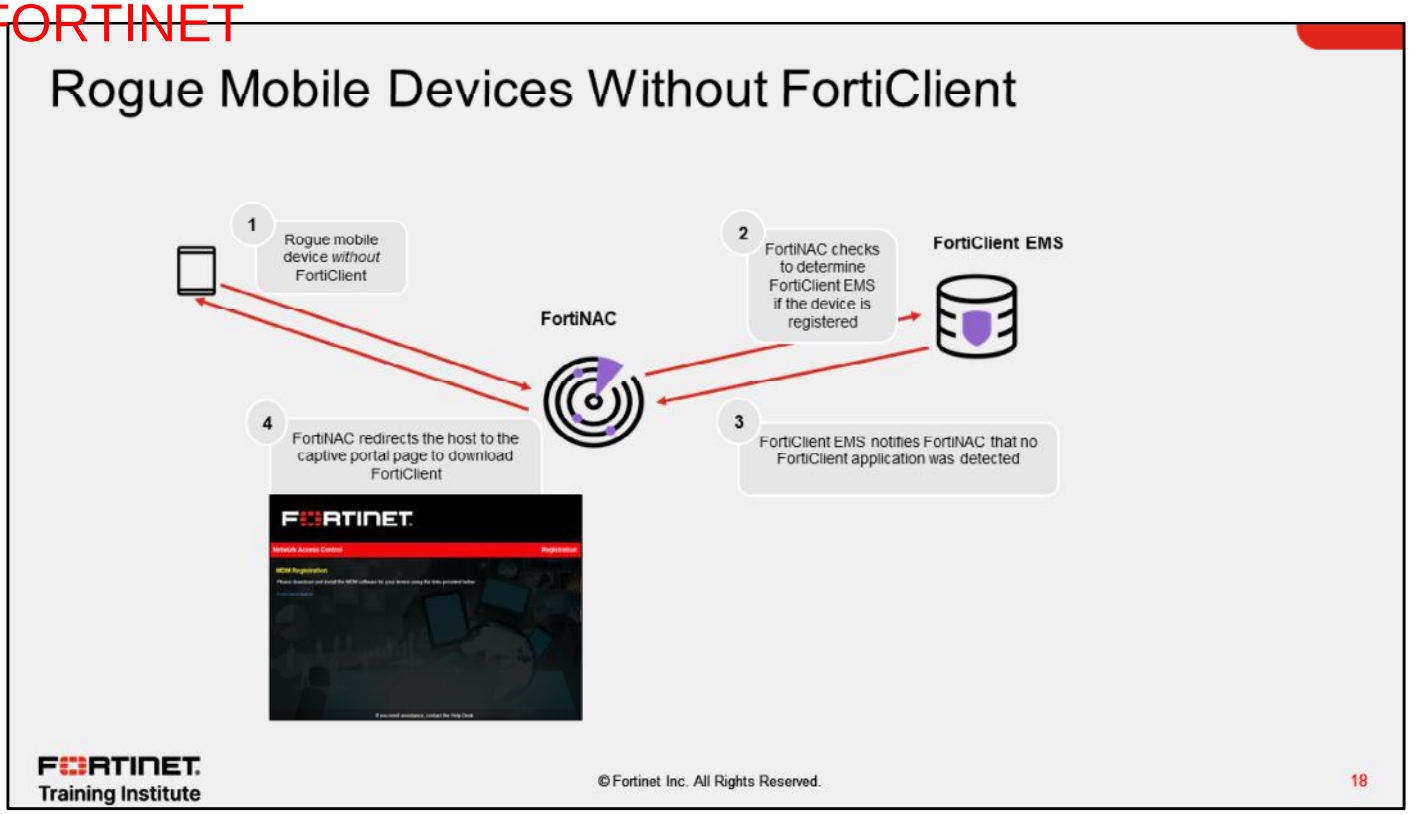


This slide shows the flow of events when a rogue device with FortiClient installed is detected on the network.

1. A rogue device with FortiClient installed is detected on the network.
2. FortiNAC communicates with FortiClient EMS to verify that the device is registered.
3. FortiClient EMS acknowledges that the host is registered and sends host data—device type, operating system, user, host name, and compliance status—back to the FortiNAC.
4. FortiNAC also registers the device and applies the relevant configured host policies.

FortiNAC polls FortiClient EMS periodically in order to update the records of those hosts that are already registered in FortiNAC.

DO NOT REPRINT
© FORTINET

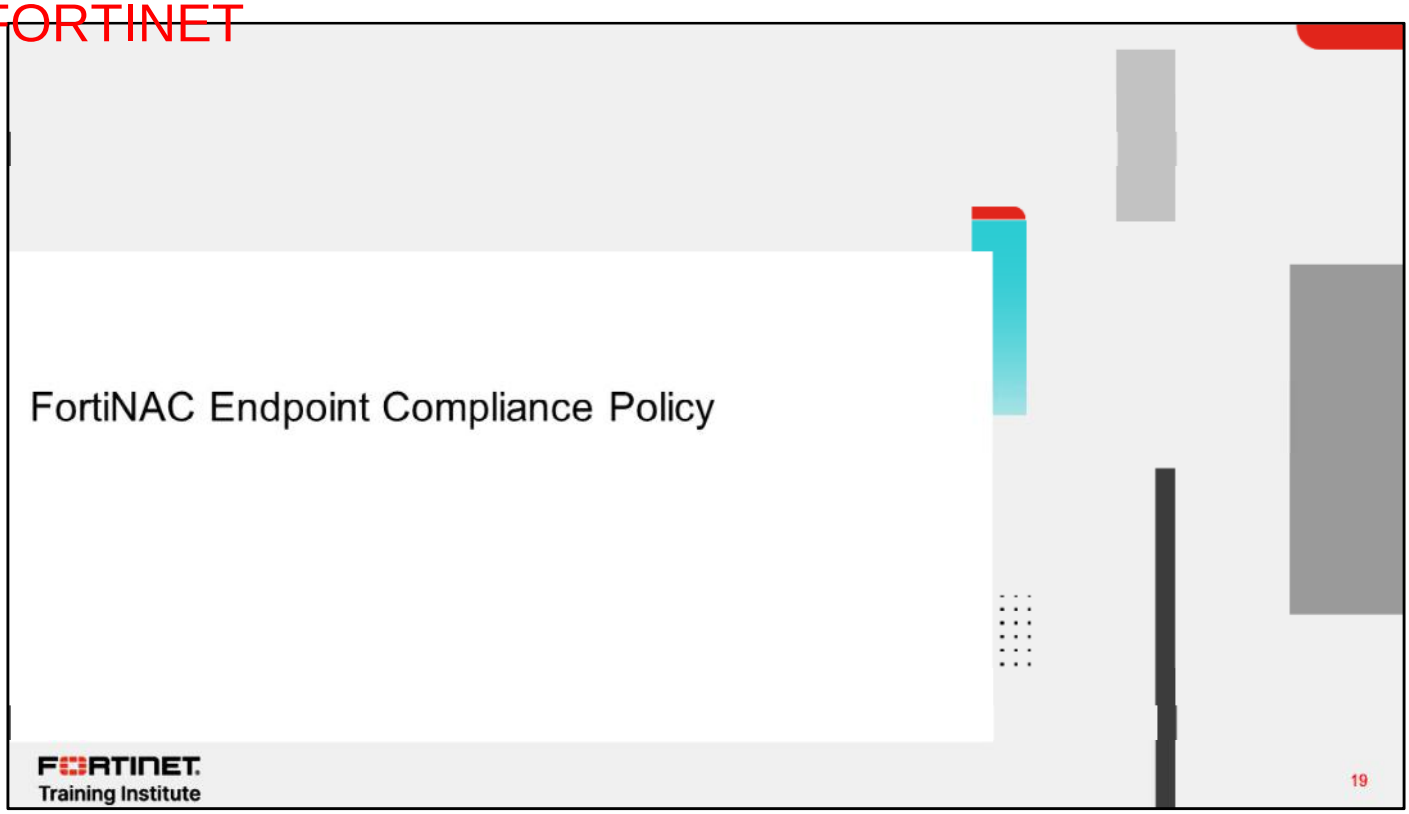


Currently only mobile devices, such as cellphones and tablets, support redirection to a captive portal page if FortiClient is not detected. The captive portal displays a message indicating that no MDM agent was detected and links to the appropriate site to download FortiClient are displayed.

This slide shows the flow of events when a rogue mobile device without FortiClient installed is detected on the network.

1. A rogue mobile device without FortiClient installed is detected on the network.
2. FortiNAC communicates with FortiClient EMS to verify that the device is registered.
3. FortiClient EMS notifies FortiNAC that no FortiClient application detected.
4. FortiNAC redirects the rogue mobile device to the captive portal to download FortiClient.

DO NOT REPRINT
© FORTINET

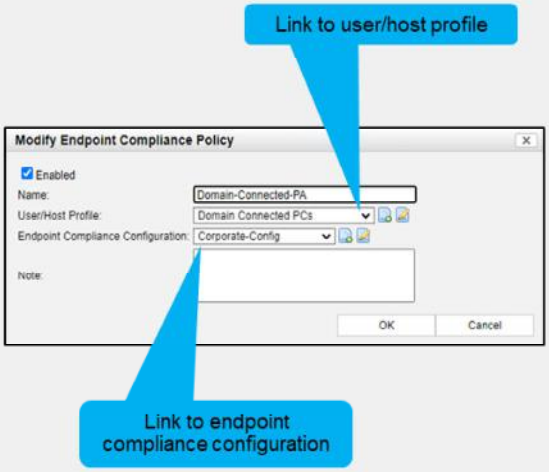


In this section, you will review the FortiNAC endpoint compliance policy.

DO NOT REPRINT
© FORTINET

Endpoint Compliance Policy

- The endpoint compliance policy contains two main components:
  - User/host profile
  - Endpoint compliance configuration
- The user/host profile defines the who, what, where, and when components
- The endpoint compliance configuration defines the type of scan and agents to be used to assess compliance



FORTINET Training Institute

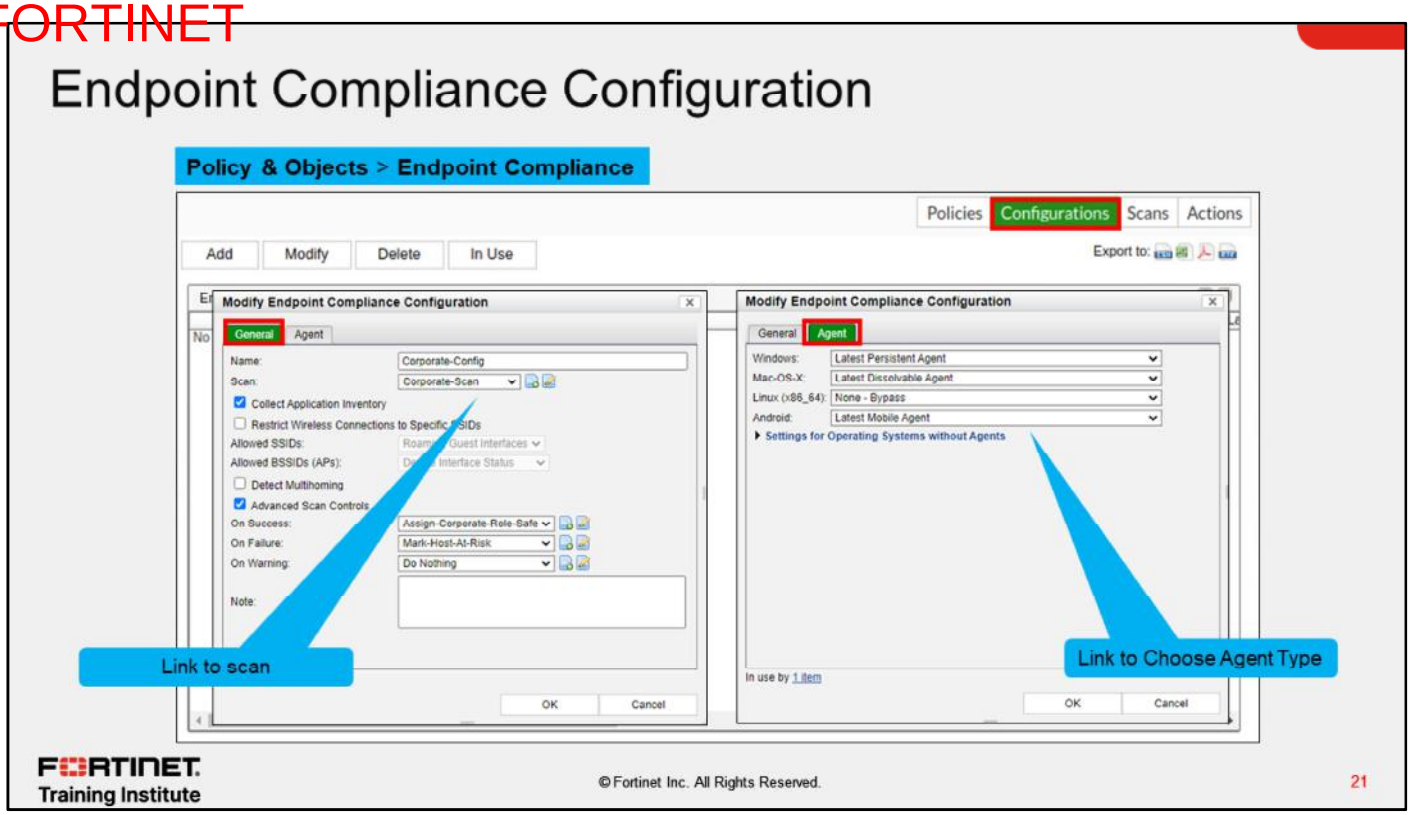
© Fortinet Inc. All Rights Reserved.

20

You associate the desired **User/Host Profile** with the appropriate **Endpoint Compliance Configuration** on the **Add Endpoint Compliance Policy** window. In the example shown on this slide, the policy is named `Domain-Connected-PA`. The **User/Host Profile** field is a drop-down list that contains all currently existing user/host profiles.

The **Endpoint Compliance Configuration** field is a drop-down list of all existing network access configurations.

DO NOT REPRINT
© FORTINET



The **Add Endpoint Compliance Configuration** window presents several configuration settings and options across two tabs: **General** and **Agent**. On the **General** tab, you must give the endpoint compliance configuration a unique name. In the example shown on this slide, the **Name** is `Corporate-Config`.

The **Scan** field is a drop-down list of all existing scan configurations.

One way to further enhance endpoint visibility is to collect installed application information. There are two ways that application information can be gathered: through an integration with MDMs that support application gathering, or through the use of FortiNAC agent technology. The **Collect Application Inventory** option uses agent technology to gather all installed applications on an endpoint.

The **Advanced Scan Controls** option allows you to take actions based upon the results of the scan. You can take these actions **On Success**, **On Failure**, or **On Warning**.

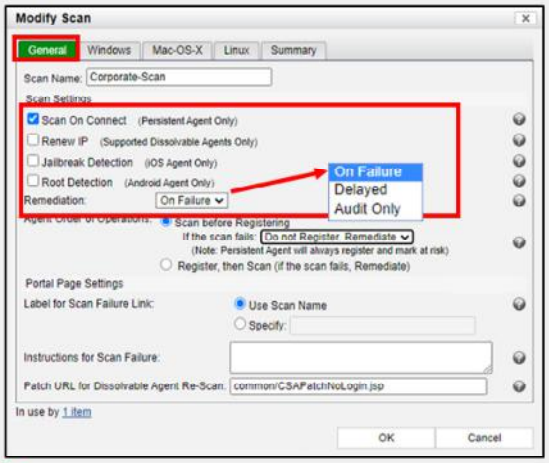
The **Agent** tab is where you specify which type of agent, if any, is provided to hosts within the isolation captive portal. The agent type is specified by operating system, and there are six available options:

- **FortiNAC Persistent Agent**: is available for Windows, Mac OS X, and Linux operating systems.
- **FortiNAC Dissolvable Agent**: is available for Windows, Mac OS X, and Linux operating systems.
- **FortiNAC Mobile Agent**: is available for the Android operating system.
- **None – Bypass**: This option grants the host access with no scan performed, and is available to all operating systems.
- **None – Deny Access**: This option denies access with no scan performed, and is available to all operating systems.

DO NOT REPRINT
© FORTINET

Scan Creation

- The **Scan on Connect** and **Renew IP** options allow extended flexibility, based on agent type
- You can configure a custom scan and set monitors for continual monitoring



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

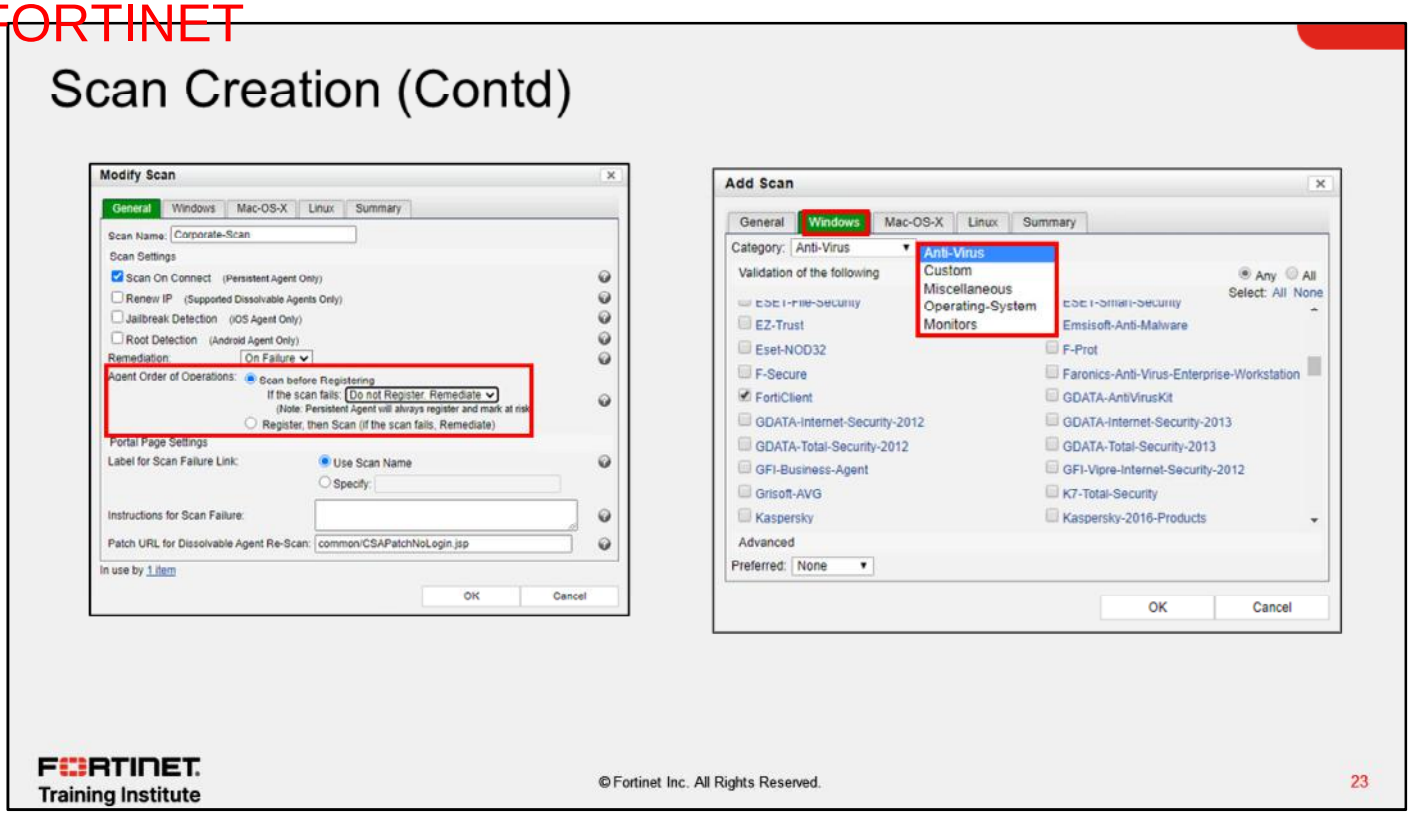
22

The **Add Scan** window consists of five tabs: **General**, **Windows**, **Mac-OS-X**, **Linux**, and **Summary**.

The **General** tab contains a variety of agent-specific settings that define agent behavior, as well as remediation page presentation options. The **Scan Settings** section provides the following agent-specific options:

- **Scan On Connect**: FortiNAC performs a policy validation scan each time a host's state changes from offline to online. A host must be registered and have the persistent agent installed to use this option.
- **Renew IP**: The agent initiates a release and renewal of the host IP address at the completion of the scan. This option applies to only Windows or Mac OS hosts using the dissolvable agent.
- **Jailbreak Detection**: When this option is selected, FortiNAC determines if an iOS device has been subject to jailbreak. This option applies to iOS devices using the iOS agent. Note that this setting is for backward compatibility of devices using the iOS agent, which has been deprecated.
- **Root Detection**: If you select this option, FortiNAC determines if an Android device has been rooted. This option applies only to Android devices that have the mobile agent.
- **Remediation**: There are three options that you can select to determine how a host is treated when a scan fails.
    - **On Failure** will move the host to the quarantine isolation network immediately.
    - **Delayed** will move the host to the quarantine isolation network after a user-defined period of time, if the failure has not been addressed.
    - **Audit Only** will report scan results to FortiNAC, but the host state will not change and the host will not be isolated.

DO NOT REPRINT
© FORTINET



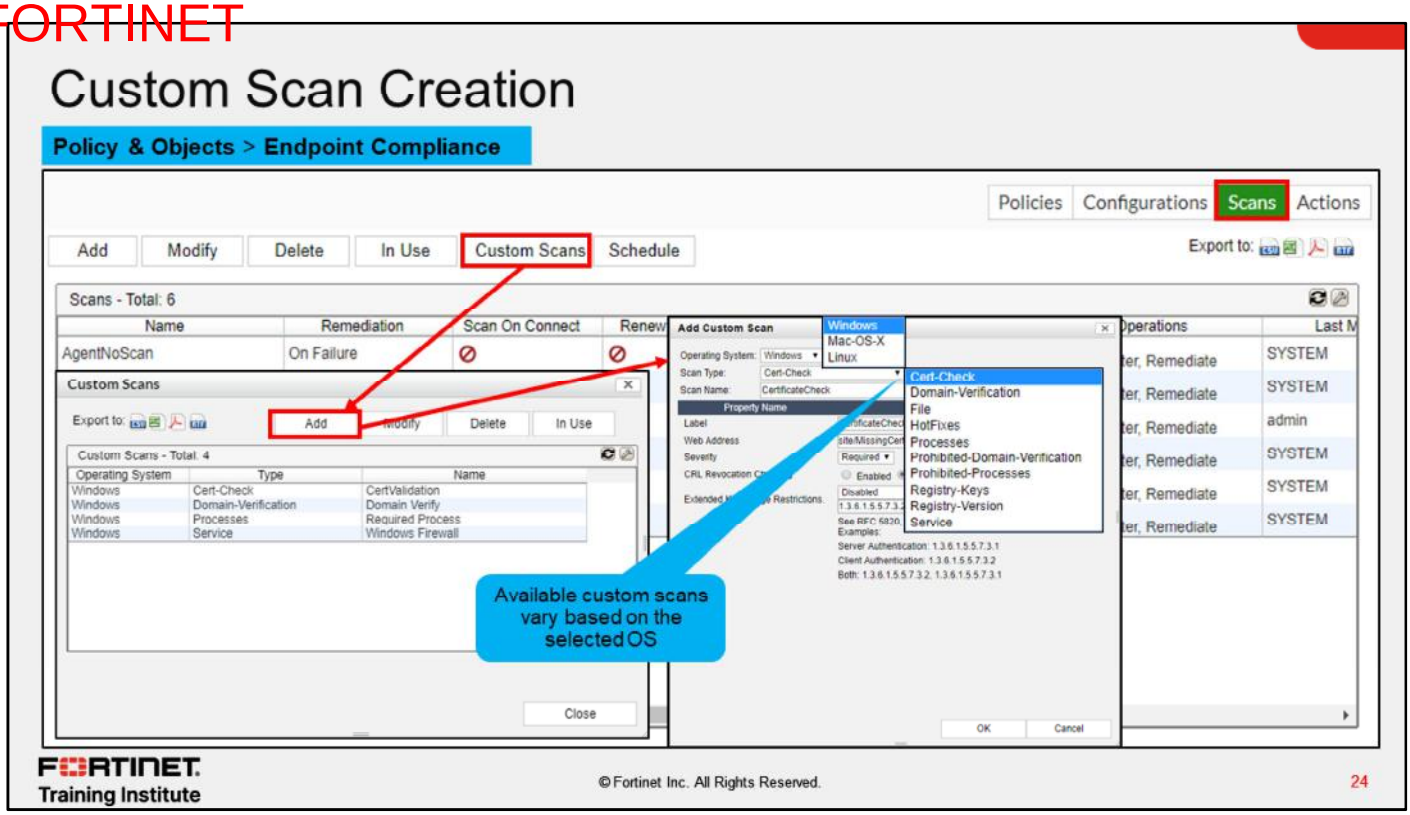
The **Agent Order of Operations** field is available only if **Remediation** is set to **On Failure**. There are two options with this setting:

- **Scan before Registering** scans the host in the registration isolation network. There are two additional options with this setting:
  - **Do not Register, Remediate**: keeps the host in the registration network until the scan is passed.
  - **Register and mark At Risk**: registers the host and moves it to the quarantine isolation network.
- **Register, then Scan (if the scan fails, Remediate)**: This option registers the host in the registration isolation network, and then moves the host to the quarantine isolation network for downloading of the agent and scanning. The **Remediation** options apply only to dissolvable agents.

The **Windows** tab is where you select all of the policy requirements by category for Windows hosts. The **Category** field contains the following options:

- **Anti-Virus**
- **Custom**
- **Miscellaneous**
- **Operating-System**
- **Monitors**

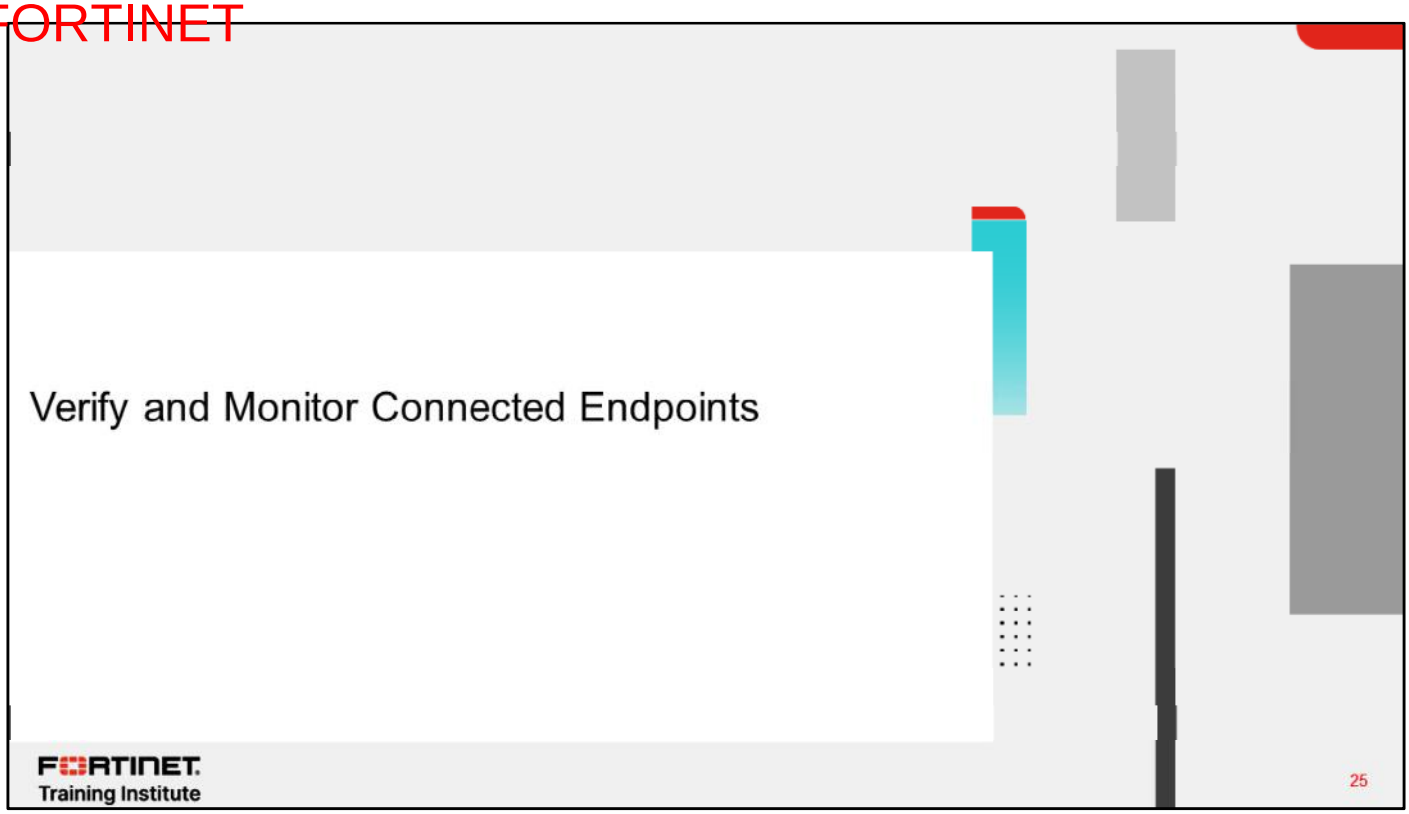
DO NOT REPRINT
© FORTINET



When you create policy scans for endpoint compliance validation, you can create optional custom scans. You can use custom scans within the actual policy scan configurations, allowing for specific OS-based criteria for Windows, Mac OS X, and Linux systems.

You can create custom scans on the **Endpoint Compliance** window. There are no default custom scans.

DO NOT REPRINT
© FORTINET

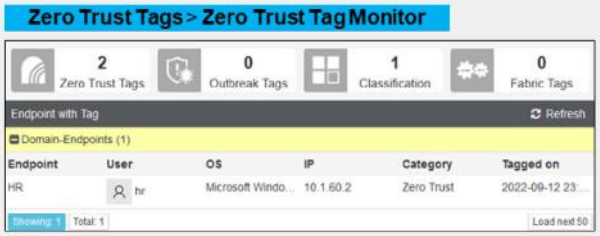


In this section, you will learn about endpoint verification and monitoring.

DO NOT REPRINT
© FORTINET

Endpoint Monitoring on FortiClient EMS

- FortiClient EMS creates dynamic groups based on zero-trust tags, and synchronizes with FortiGate to grant or deny network access
- The following information can be viewed in the zero-trust tag monitor:
  - The zero-trust tag the endpoint is tagged to
  - Endpoint hostname
  - Name of the user logged into the endpoint
  - OS currently installed on the endpoint
  - Endpoint IP address
  - Date and time that FortiClient EMS added the endpoint to the dynamic endpoint group



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

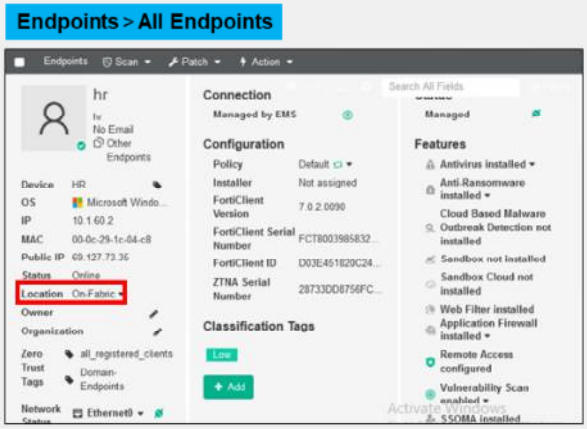
26

You can view all dynamic endpoint groups and information like zero-trust tags assigned, hostname, user information, OS installed, IP address, and the date and time the endpoint was added to the dynamic group in **Zero Trust Tags** > **Zero Trust Tag Monitor**. FortiClient EMS creates dynamic endpoint groups based on the tag configured for each rule. All this information is synchronized with FortiGate for network access.

DO NOT REPRINT
© FORTINET

Endpoint Monitoring on FortiClient EMS (Contd)

- FortiClient EMS keeps a track of the location of the endpoint based on the on-fabric detection rules configured



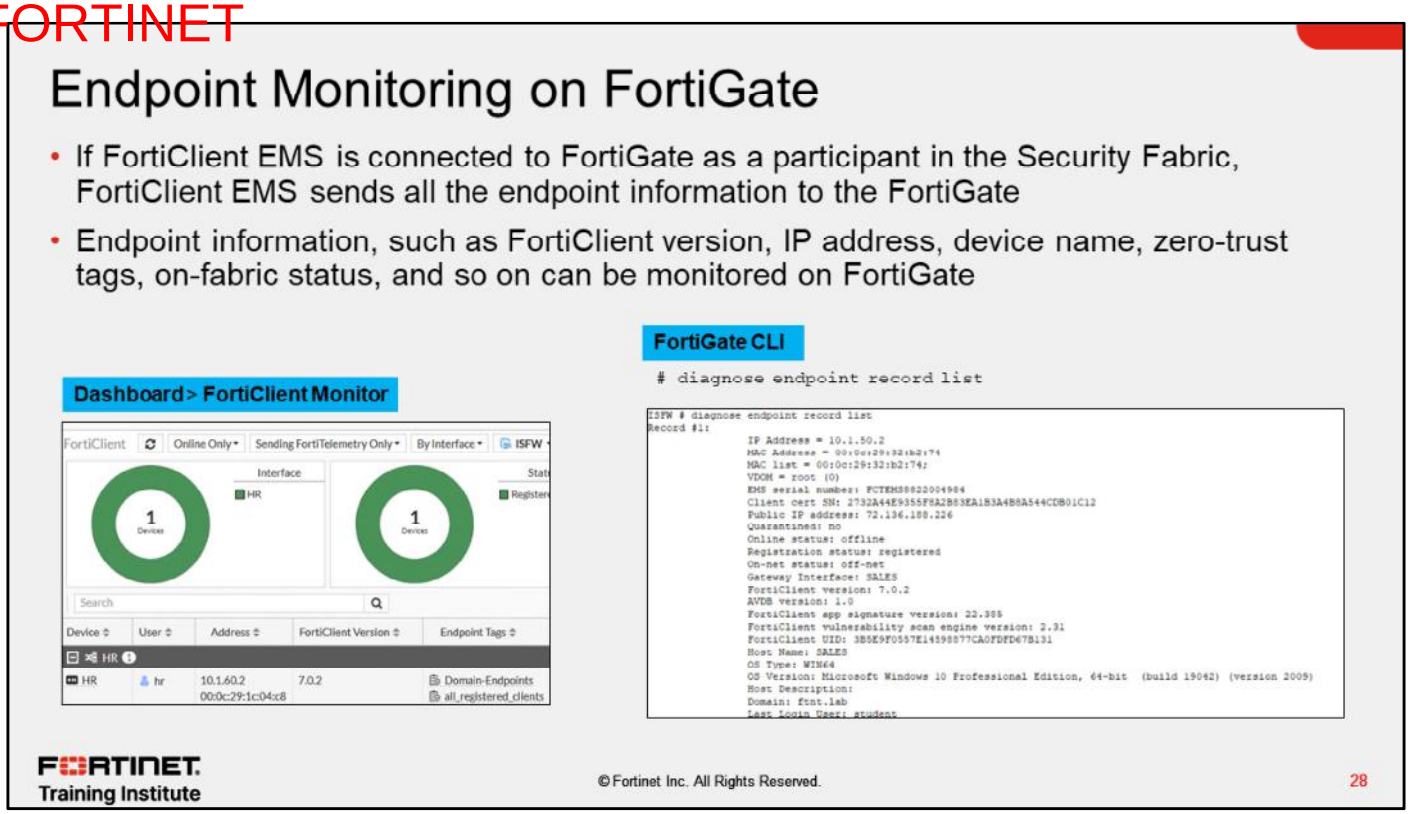
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

You can also monitor FortiClient endpoint information, such as policy assignment, FortiClient version, vulnerability information, and fabric status by clicking the endpoint name in **Endpoints** > **All Endpoints.**

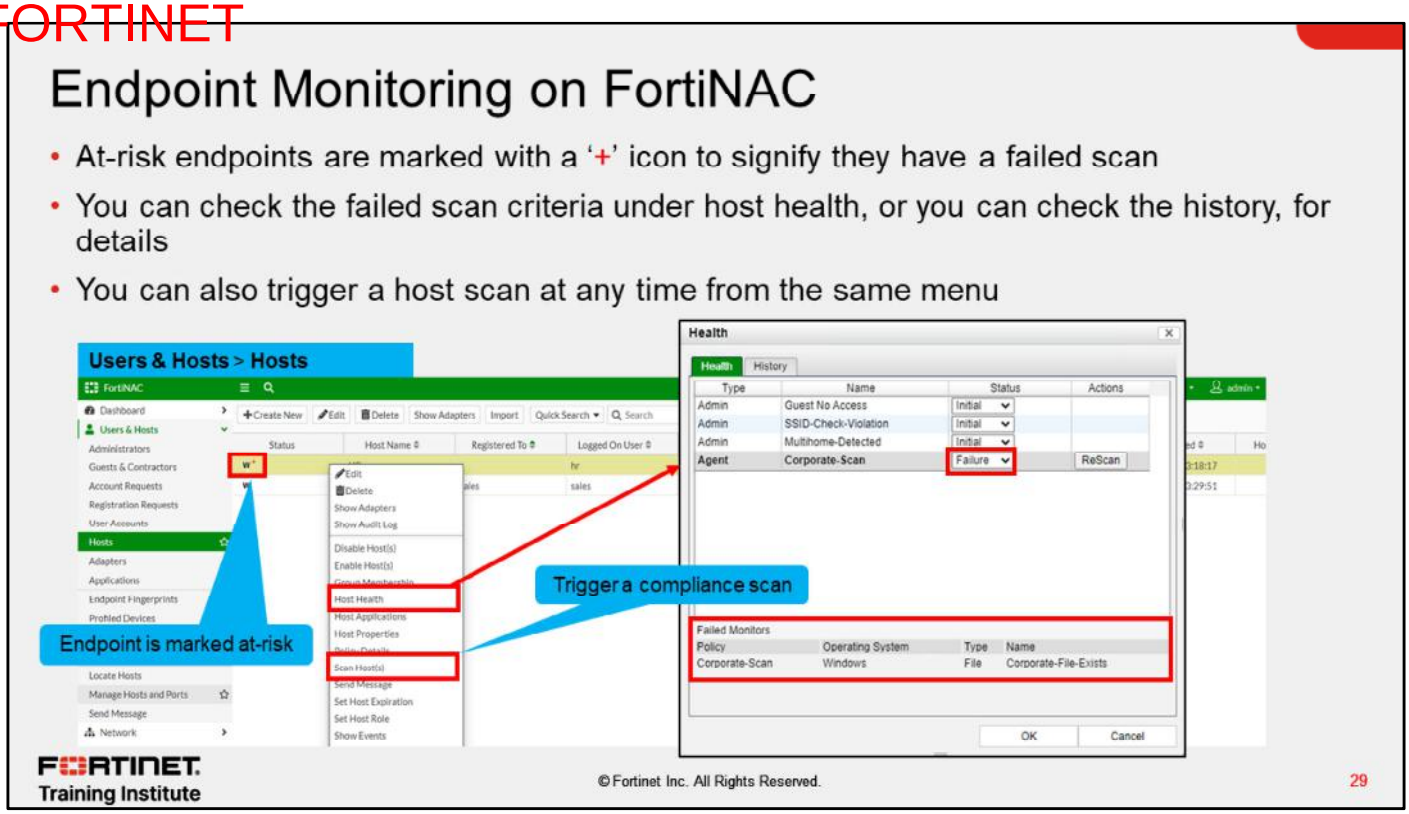
DO NOT REPRINT
© FORTINET



You can monitor FortiClient endpoint information, such as FortiClient version, IP address, device name, zero-trust tags, and on-fabric status on FortiGate in **Dashboard** > **FortiClient Monitor**. This information is available on FortiGate, if FortiClient EMS is connected to FortiGate as a participant in the Security Fabric.

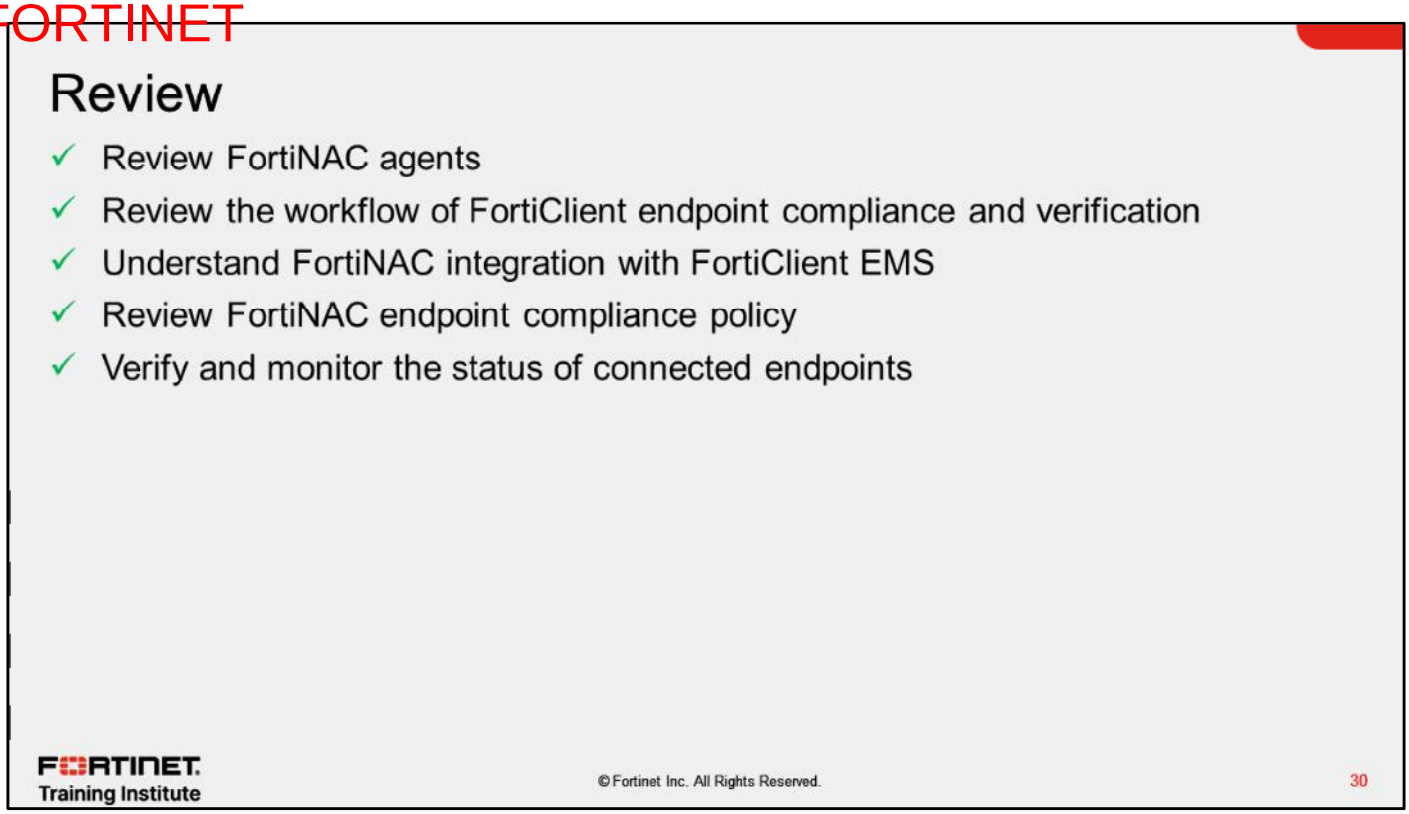
You can also use the `diagnose endpoint record list` command to show the network, registration, client certificate, and device information. It also shows the vulnerability status and position relative to FortiGate.

DO NOT REPRINT
© FORTINET



On FortiNAC, the endpoint compliance scan will be enforced on the ports after the endpoint compliance has been configured and all forced remediation groups have been applied to the required ports. Anytime a scan or a monitor fails, the endpoint will be marked with a red plus icon in **Users** & **Hosts** > **Hosts**. You can check the reason for the failed compliance by right-clicking the host, and then clicking **Host Health**.

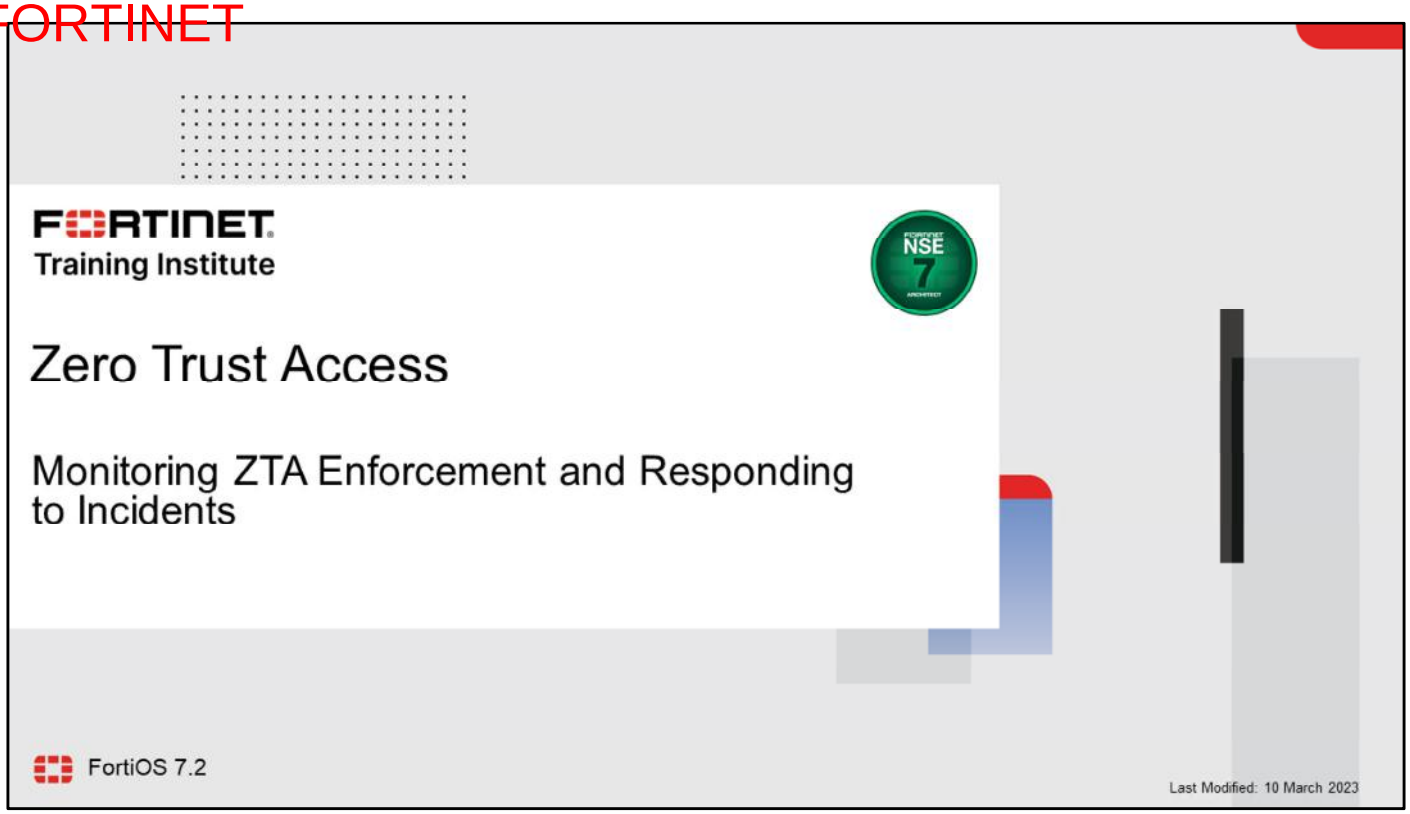
DO NOT REPRINT
© FORTINET



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

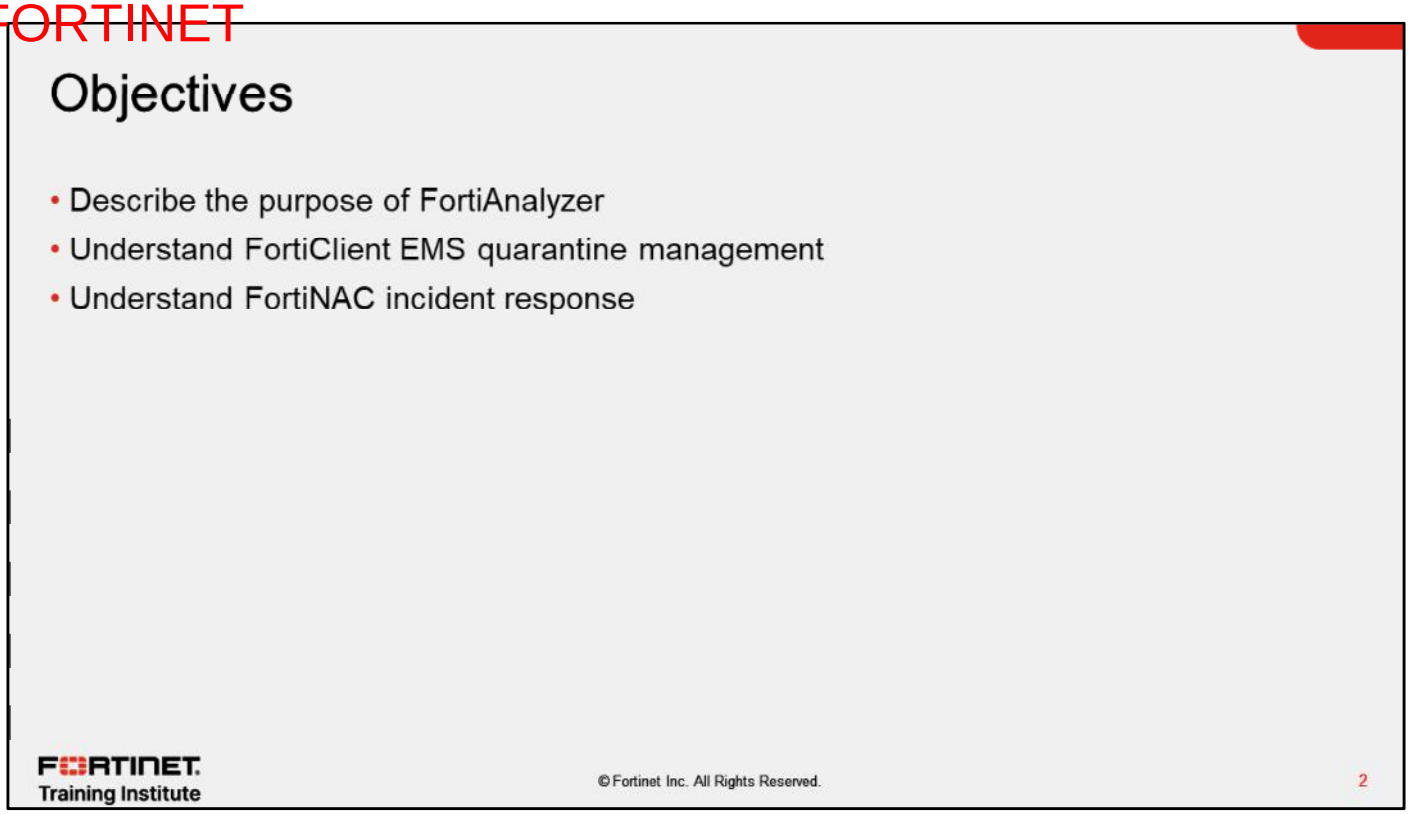
By mastering the objectives covered in this lesson, you learned about the different FortiNAC agent implementations, the workflow of FortiClient endpoint compliance, and monitoring connected endpoints. You also learned about FortiNAC integration with FortiClient EMS.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about monitoring zero trust access (ZTA) enforcement and responding to incidents.

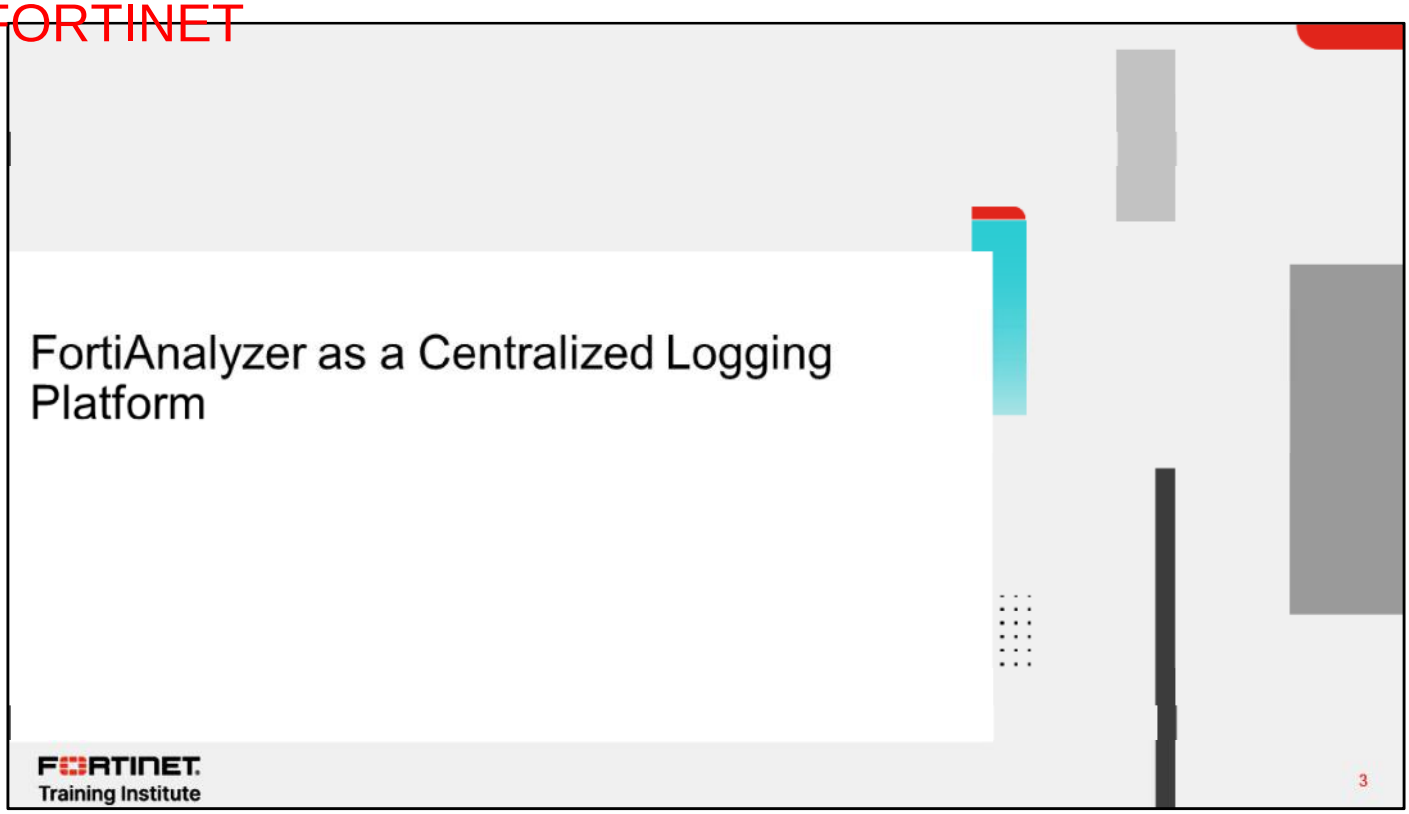
DO NOT REPRINT
© FORTINET



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

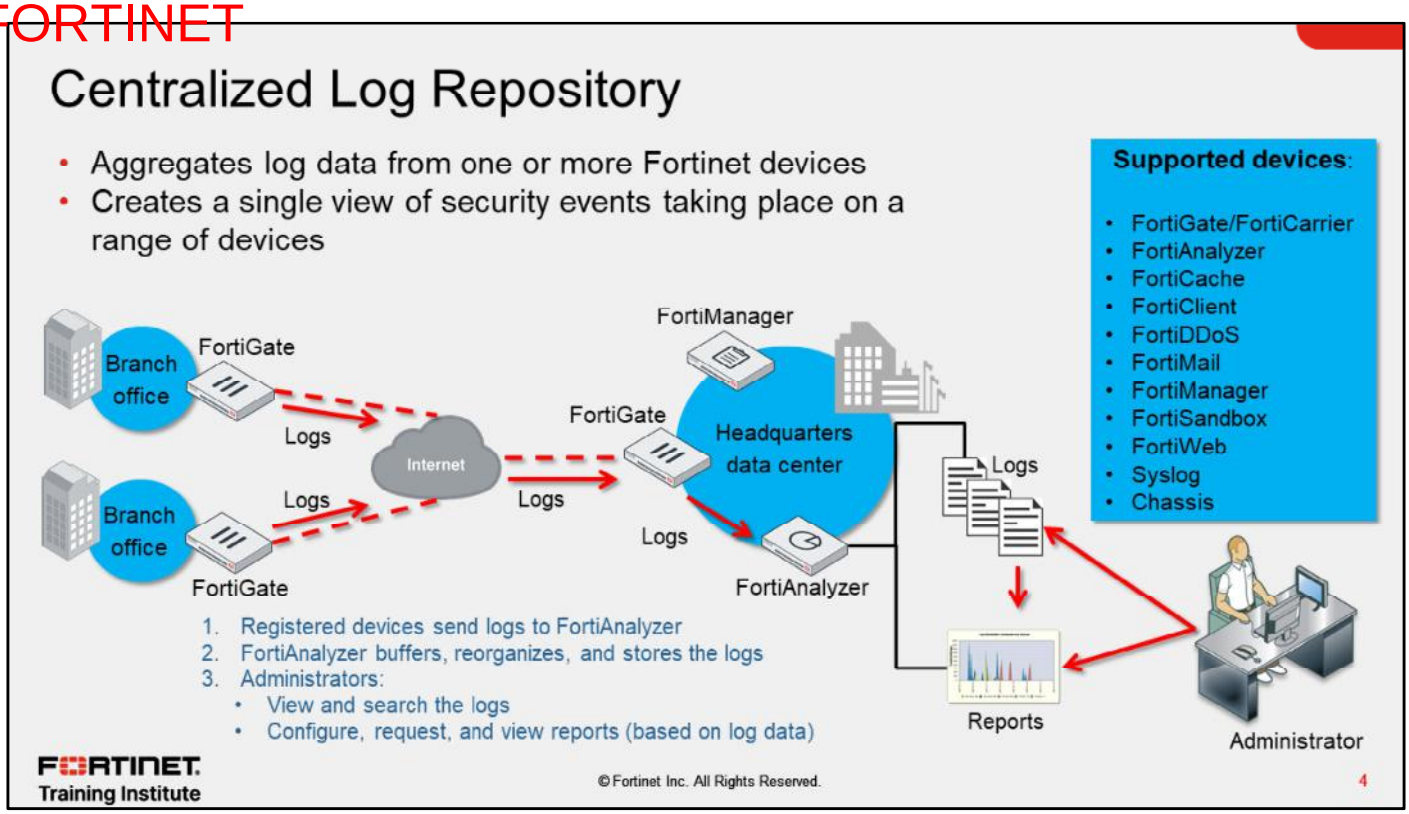
By demonstrating competence in understanding ZTA enforcement and responding to incidents, you will be able to describe the purpose of FortiAnalyzer. You will also understand how FortiClient EMS quarantine management works. Finally, you will understand the FortiNAC incident response.

DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiAnalyzer as a centralized logging platform.

DO NOT REPRINT
© FORTINET



The purpose of FortiAnalyzer is to aggregate log data from one or more devices, thereby acting as a centralized log repository. Log aggregation provides a single channel for accessing your complete network data, so you don't need to access multiple devices several times a day.

Although FortiAnalyzer is designed to work with logs from Fortinet devices, it can also work with devices that use the syslog standard.

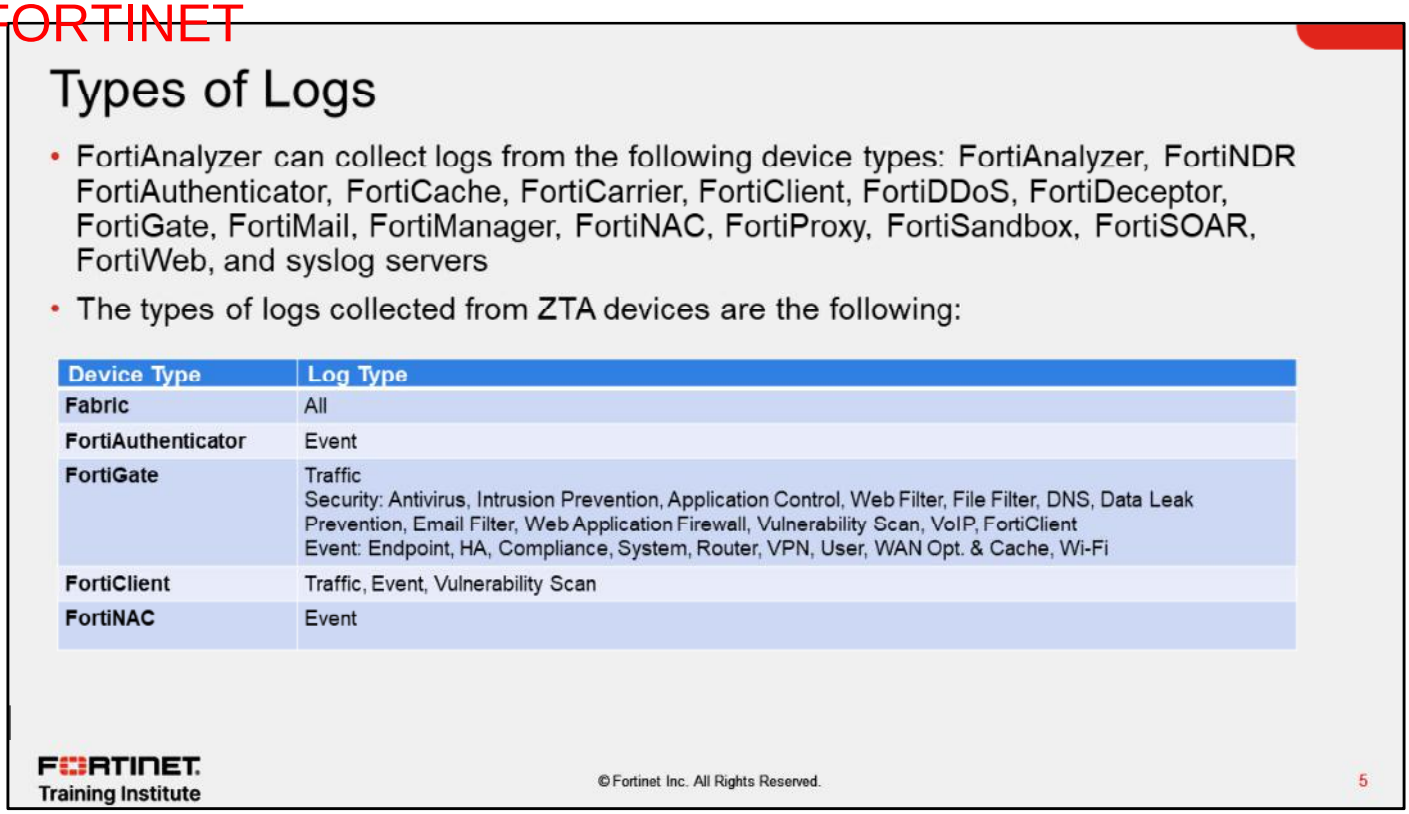
The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.

2. FortiAnalyzer collates and stores those logs in a way that makes it easy to search and run reports.

3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually, or generate reports to look at the data in different formats. You can also use the CLI to perform administrative tasks.

DO NOT REPRINT
© FORTINET

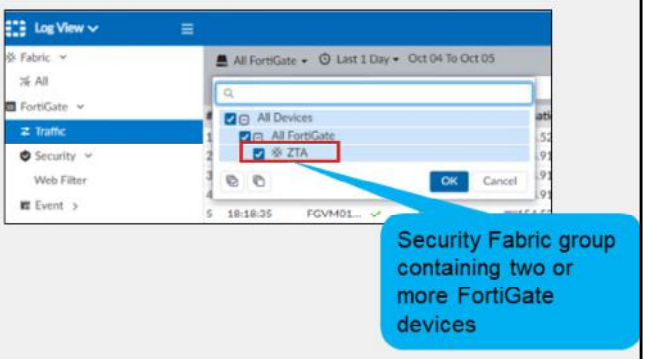


FortiAnalyzer can collect logs from various Fortinet devices and syslog servers. The slide shows the types of logs collected from core ZTA devices.

DO NOT REPRINT
© FORTINET

Security Fabric Logging

- FortiAnalyzer can recognize a Security Fabric group of devices and display all units in the group
- FortiAnalyzer stores and analyzes the logs from the units in a Security Fabric group as if the logs are from a single device
- FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions/bandwidth together with its UTM threats
- You can go to **Device Manager** on FortiAnalyzer and right-click any of the Security Fabric devices and select **Fabric Topology** to see the logging topology



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

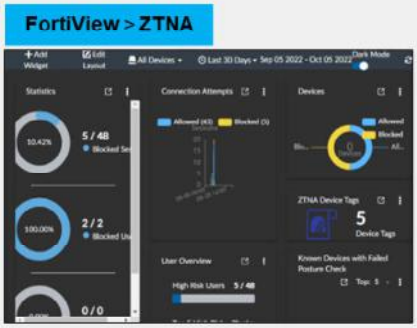
6

FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the units in a Security Fabric group as if the logs are from a single device. FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions and bandwidth together with its UTM threats. No additional configuration is required for this to take place because FortiAnalyzer performs this function automatically.

DO NOT REPRINT
© FORTINET

Security Fabric Analytics

- Analytics and Reporting
  - Full visibility of network devices, systems, and users
  - Correlated data and analysis of real-time and historical events
  - Reports for compliance or historical analysis purposes
- FortiView
  - Provides multilevel views
  - Summaries of real-time critical alerts
- Monitors
  - Customizable SOC and NOC dashboards/widgets
  - Monitor events in real-time through the predefined dashboard
- Log View
  - Utilize search filters on managed device logs
  - Log drill down, formatted or raw logs, log import/export, custom views, and log groups



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

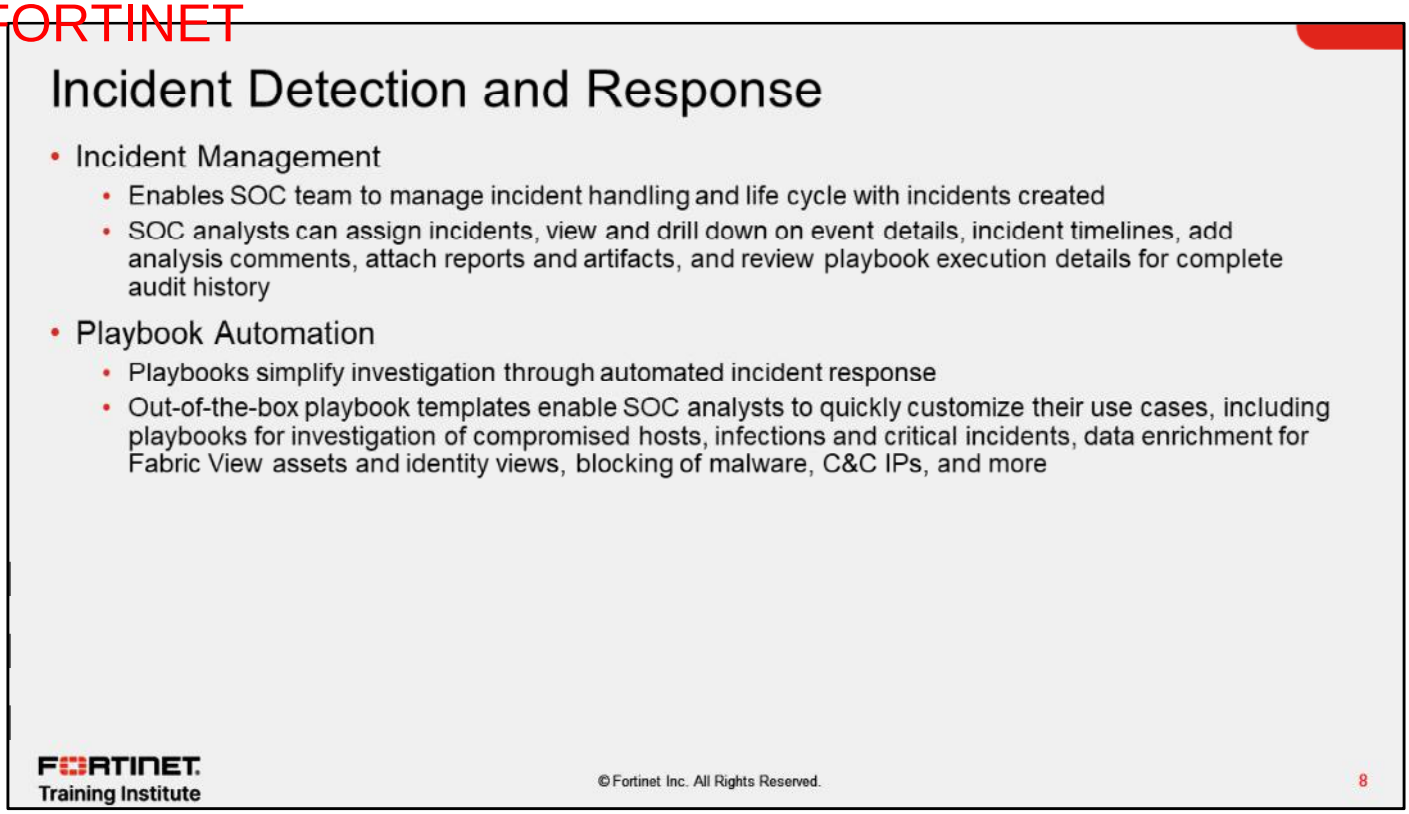
FortiAnalyzer automation-driven analytics empowers security teams by providing full visibility of network devices, systems, and users, with correlated log data for threat intelligence and analysis of real-time and historical events. You can archive and filter the network knowledge you glean from these reports, as well as mine it for compliance or historical analysis purposes.

FortiView is a comprehensive monitoring solution that provides multilevel views and summaries of real-time critical alerts and information, such as top threats and indicators of compromise (IOC) to your network, including botnet and command-and-control (C&C) servers, and so on.

The Monitors view provides operations teams with customizable NOC and SOC dashboards and widgets. Monitor events in real-time through the predefined dashboard views for SD-WAN, VPN, Wi-Fi, Incoming/Outgoing Traffic, Applications and Websites, FortiSandbox Detections, Endpoint Vulnerabilities, Software Inventory, Top Threats, Shadow IT (monitoring service), ZTNA, and many more.

Log View enables analysts to expand their investigation and utilize search filters on managed device logs, with log drill down, and formatted or raw logs.

DO NOT REPRINT
© FORTINET



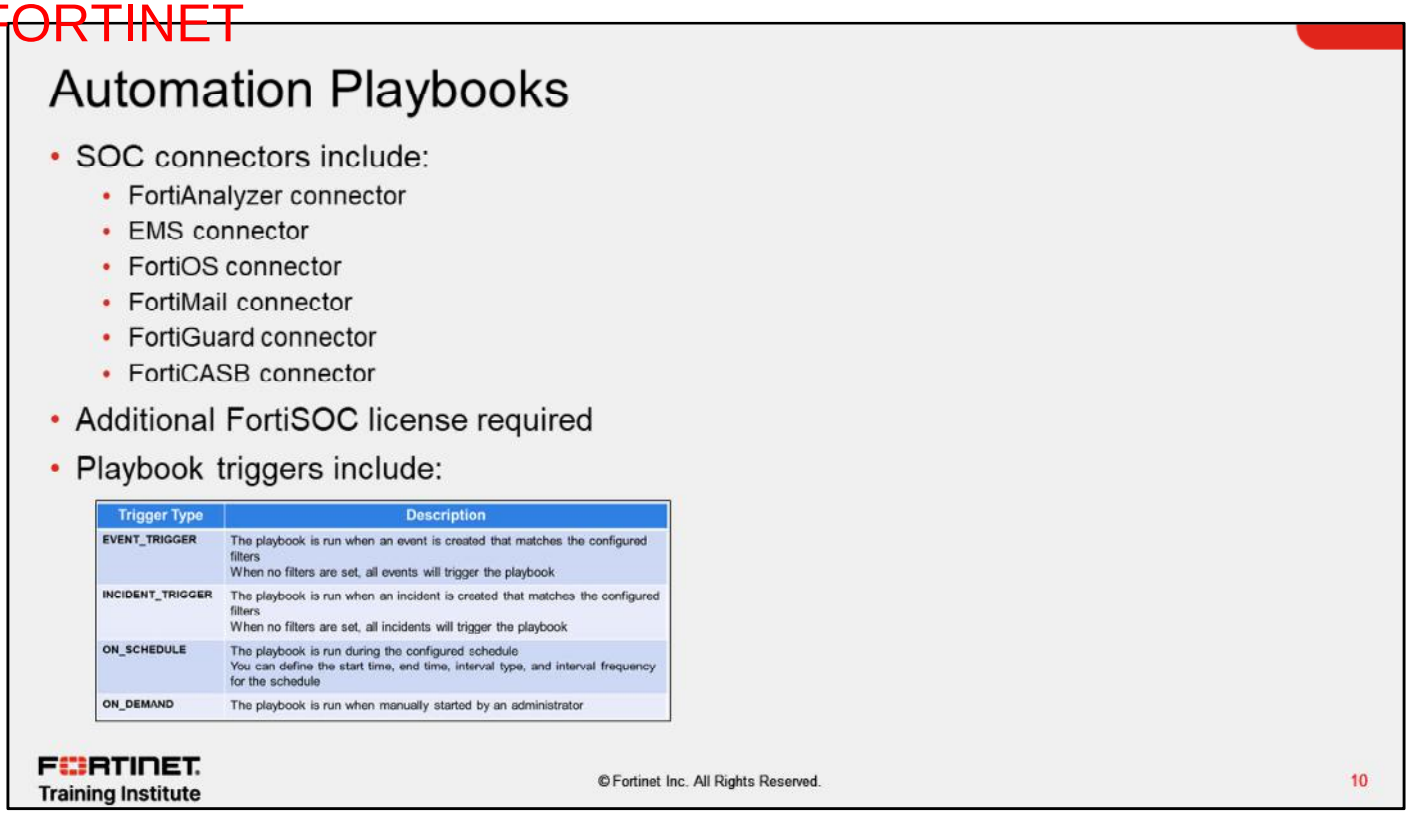
The incidents component in FortiSOC enables security operations teams to manage incident handling and life cycle with incidents created from events to show affected assets, endpoints, and users. Analysts can assign incidents, view and drill down on event details, incident timelines, add analysis comments, attach reports and artifacts, and review playbook execution details for complete audit history.

Out-of-the-box FortiAnalyzer playbook templates enable SOC analysts to quickly customize their use cases with playbooks for investigation of compromised hosts, infections and critical incidents, data enrichment for Fabric View assets and identity views, blocking malware, C&C IPs, and more.

DO NOT REPRINT
© FORTINET

In this section, you will learn about FortiClient EMS quarantine management using Security Fabric devices.

DO NOT REPRINT
© FORTINET



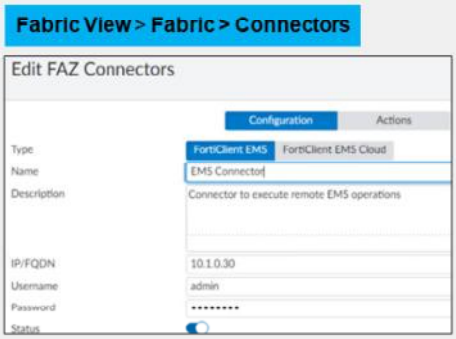
FortiAnalyzer can be integrated with the following SOC connectors: FortiAnalyzer connector, EMS connector, FortiOS connector, FortiMail connector, FortiGuard connector, and FortiCASB connector. FortiAnalyzer offers playbooks where one or more actions offered by SOC connectors can be executed manually or automatically. FortiSoC is a subscription service that enables playbook automation for security operations on FortiAnalyzer.

Triggers determine when a playbook is to be executed. Triggers are always the first step in a playbook, and each playbook can include only one trigger. Once a playbook has been triggered, it flows through the remaining tasks as defined by the routes in the playbook using the trigger as a starting point. The playbook triggers available on FortiAnalyzer are shown on this slide.

DO NOT REPRINT
© FORTINET

Quarantine Automation Using FortiAnalyzer

- You can integrate FortiClient EMS as a Security Fabric connector on FortiAnalyzer
- FortiClient EMS connector includes predefined actions like quarantine endpoint, unquarantine endpoint, get vulnerabilities on endpoint, perform AV scans, and so on
- FortiAnalyzer performs actions on FortiClient EMS using an API



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

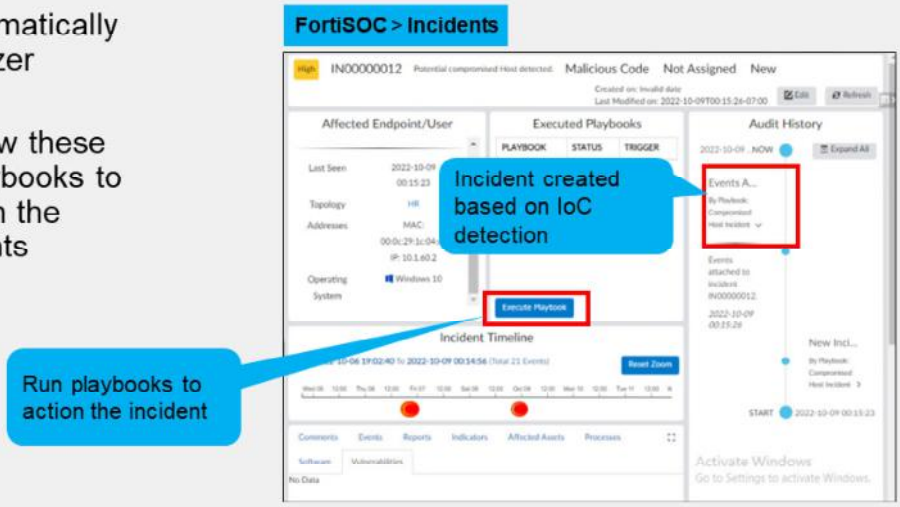
11

To integrate FortiAnalyzer with FortiClient EMS, you must configure FortiClient EMS as a Security Fabric connector on FortiAnalyzer in **Fabric View** > **Fabric** > **Connectors**. Enter a name for the FortiClient EMS, then enter the IP address for FortiClient EMS, and the username with administrator privileges and password. The FortiClient EMS connector includes predefined actions, such as quarantine endpoint, unquarantine endpoint, get vulnerabilities on endpoint, perform AV scans, and so on. FortiAnalyzer performs actions on FortiClient EMS using an API.

DO NOT REPRINT
© FORTINET

Quarantine Automation using FortiAnalyzer (Contd)

- Incidents can be automatically created by FortiAnalyzer playbooks
- SOC analysts can view these incidents and run playbooks to take further actions on the compromised endpoints



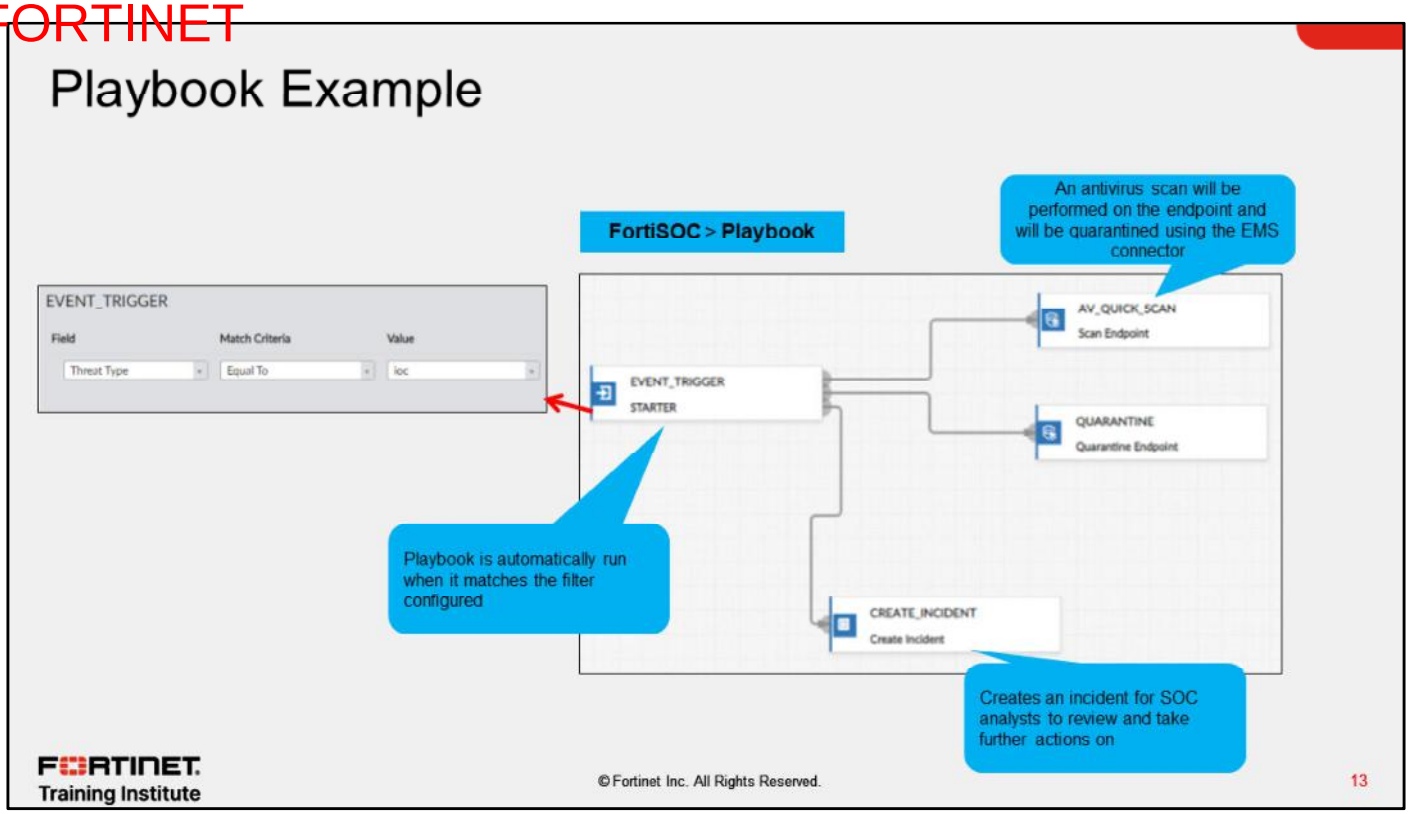
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

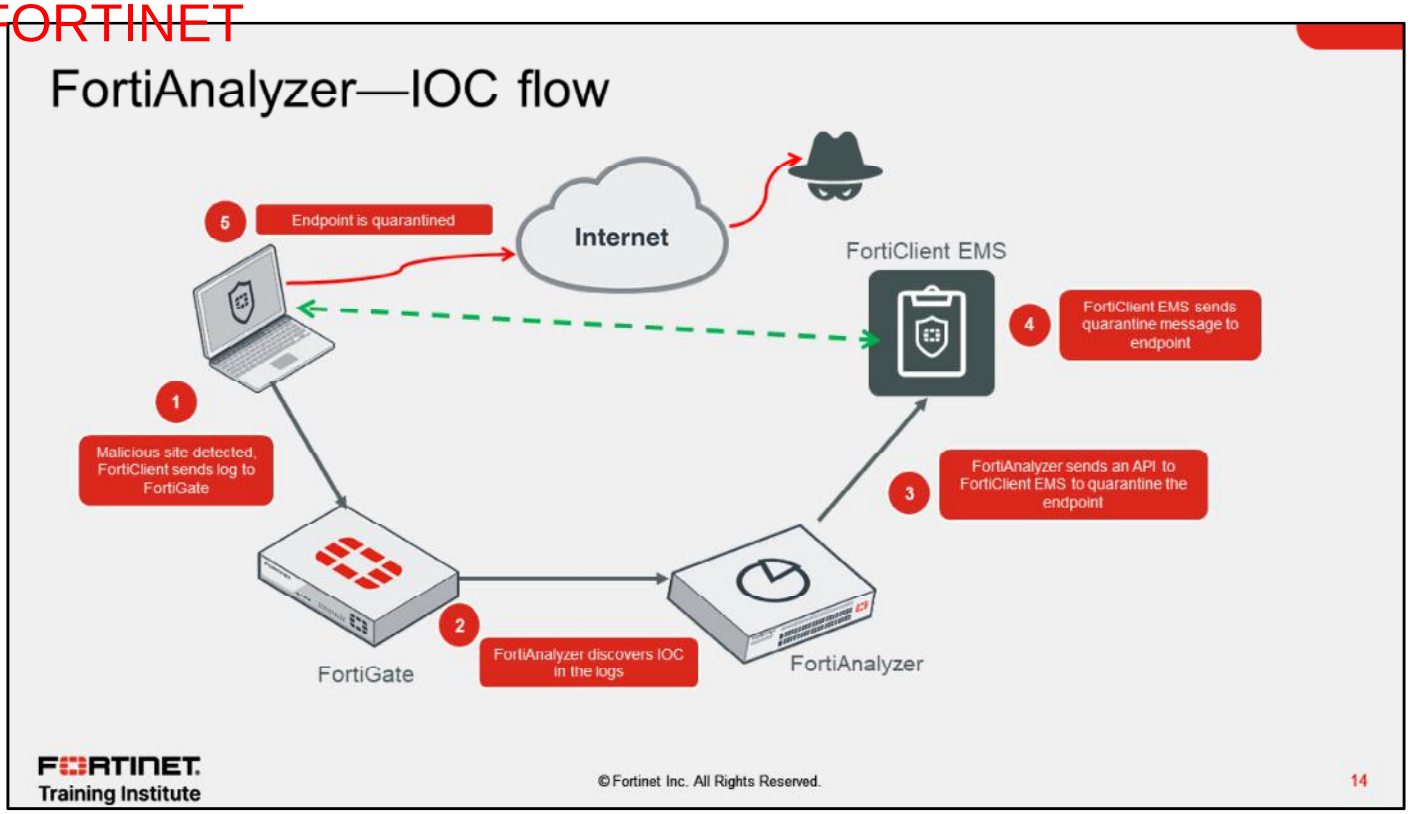
Security incidents can be automatically created on FortiAnalyzer based on the playbook configuration. SOC analysts can view and investigate these incidents to determine if the endpoints are compromised. They can take further actions on these incidents by running additional playbooks.

DO NOT REPRINT
© FORTINET



In the example shown on this slide, the playbook is configured to run when a IOC threat is detected. Once the playbook has been triggered, it scans and quarantines the endpoint using the EMS connector. The playbook will also create an incident automatically on FortiAnalyzer for the SOC analysts to review.

DO NOT REPRINT
© FORTINET



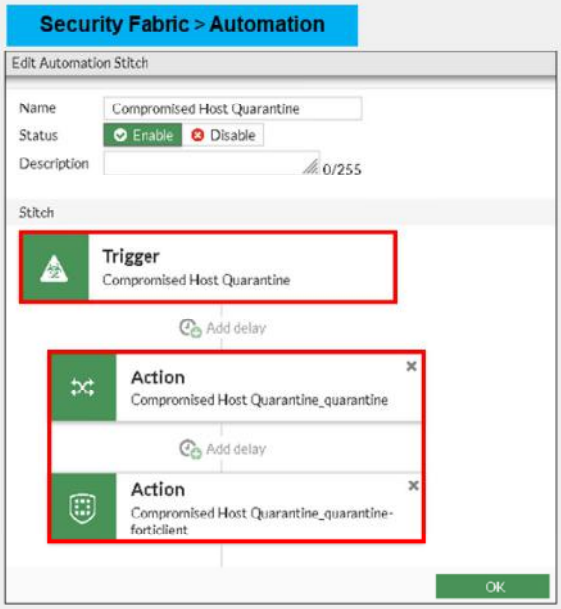
This configuration functions as follows:

1. FortiClient sends logs to FortiGate.
2. FortiGate sends logs to FortiAnalyzer. FortiAnalyzer discovers IOCs in the logs.
3. When an IOC threat type is detected on FortiAnalyzer, a playbook is triggered. As per the playbook configuration, FortiAnalyzer sends an API to FortiClient EMS to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic.

DO NOT REPRINT
© FORTINET

Quarantine Automation Using FortiAnalyzer and FortiOS

- You can quarantine an endpoint from FortiOS using EMS using an API
- The following network components are required:
  - FortiGate
  - FortiAnalyzer
  - FortiClient EMS
  - FortiClient
- Security Fabric, which includes the above network devices, can automatically quarantine an endpoint on which an IOC is detected



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

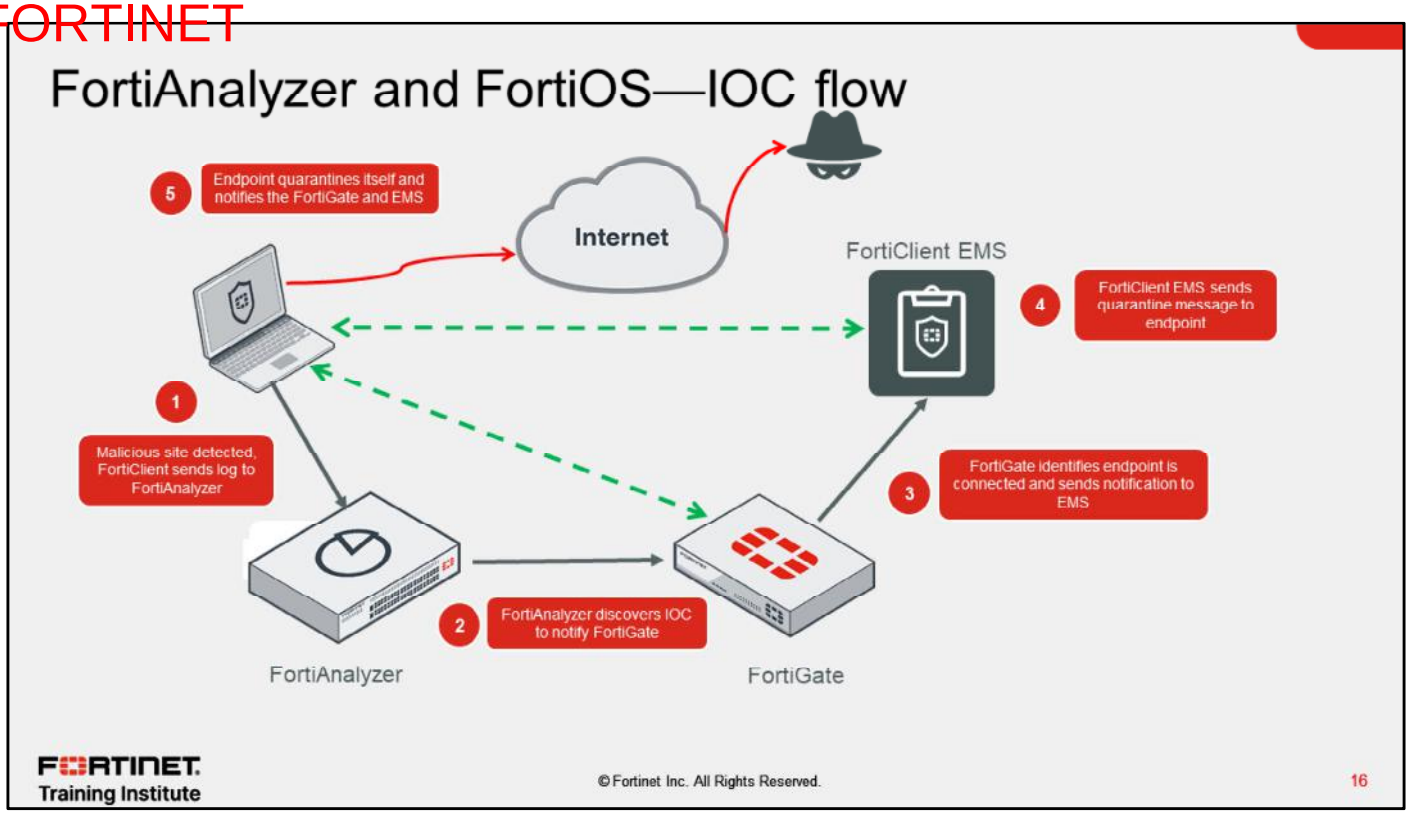
15

The Security Fabric offers visibility of endpoints at various monitoring levels. When the Security Fabric includes network devices listed here, you can configure the system to automatically quarantine an endpoint on which an IOC is detected. This requires the following network devices:

- FortiGate
- FortiAnalyzer
- FortiClient EMS
- FortiClient

You must connect FortiClient to both the EMS and FortiGate. FortiGate and FortiClient must both be sending logs to FortiAnalyzer. You must configure the EMS IP address on FortiGate, as well as administrator login credentials.

DO NOT REPRINT
© FORTINET



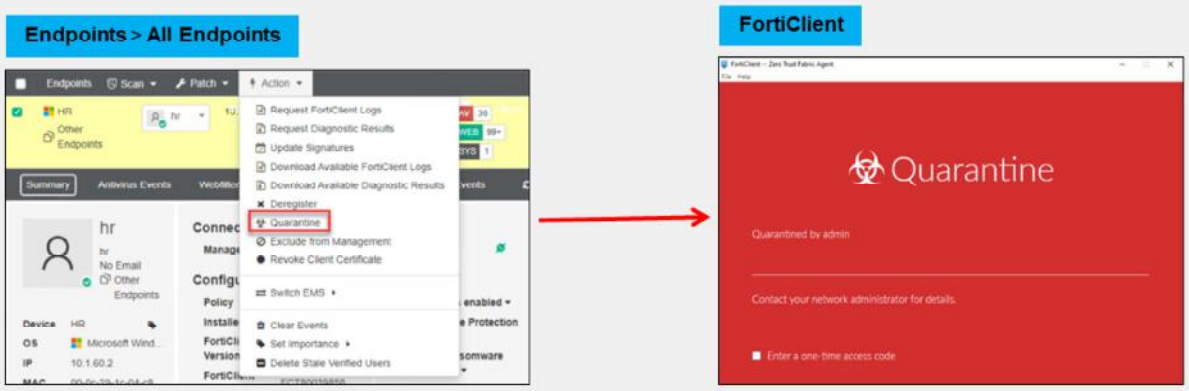
This configuration functions as follows:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IOCs in the logs and notifies FortiGate.
3. FortiGate identifies if FortiClient is a connected endpoint, and if it has the login credentials for the FortiClient EMS that FortiClient is connected to. With this information, FortiGate sends a notification to FortiClient EMS to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.

DO NOT REPRINT
© FORTINET

Manual Quarantine

- FortiClient endpoints can be manually quarantined on the FortiClient EMS console
- Quarantined endpoints are isolated from the network



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

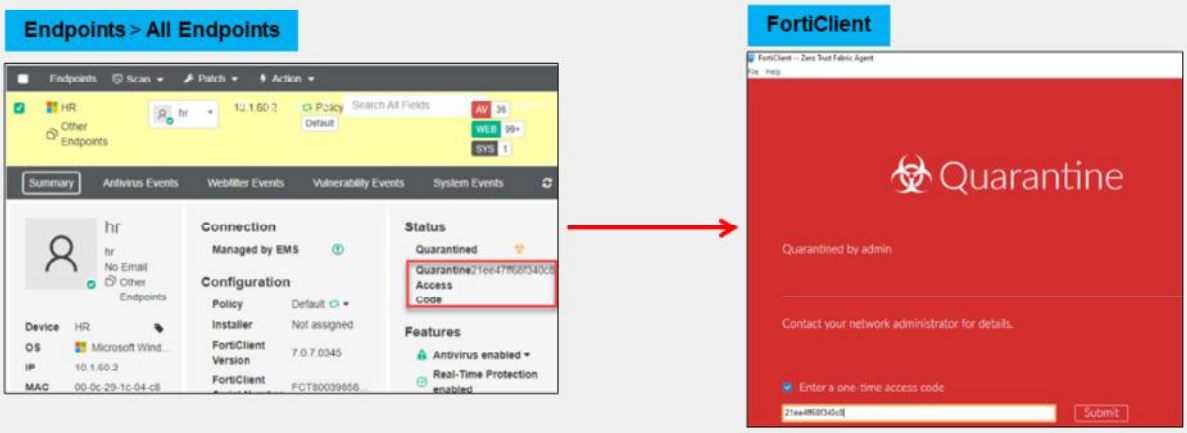
17

FortiClient endpoints can be manually quarantined on the FortiClient EMS console. You can click on **Endpoints** > **All Endpoints**, and select the endpoint. Click the **Action** menu and select **Quarantine**. Once the endpoint is quarantined it is isolated from the network.

DO NOT REPRINT
© FORTINET

Remove FortiClient From Quarantine List

- There are a few ways to remove a FortiClient endpoint from quarantine
  - FortiAnalyzer playbooks using API
  - Unquarantine from FortiEMS console by selecting the quarantined endpoint
  - Unquarantine the endpoint from FortiClient using the Quarantine Access Code



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

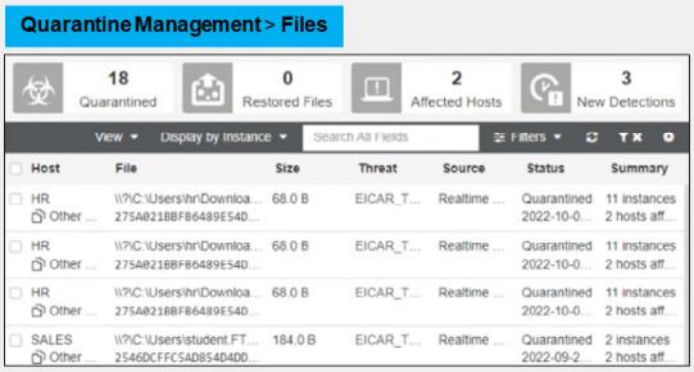
18

You can unquarantine a FortiClient endpoint in a few ways. You can remove the endpoint from the FortiClient EMS console or on the FortiClient endpoint by using a quarantine access code, usually provided by the FortiClient EMS administrator. Another way to unquarantine an endpoint is by FortiAnalyzer playbooks using an API.

DO NOT REPRINT
© FORTINET

View Quarantined and Allowlist Files

- Viewing quarantined files
  - FortiClient sends quarantined file information to FortiClient EMS
  - You can view the list of quarantined files on the **Files** pane
  - You can filter the file list
- Allowlisting quarantined file
  - You can allowlist and restore quarantined files from EMS
  - You can view the lost allowlisted files in the **Allowlist** pane
  - You can filter, edit the file description, and delete allowlisted files



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

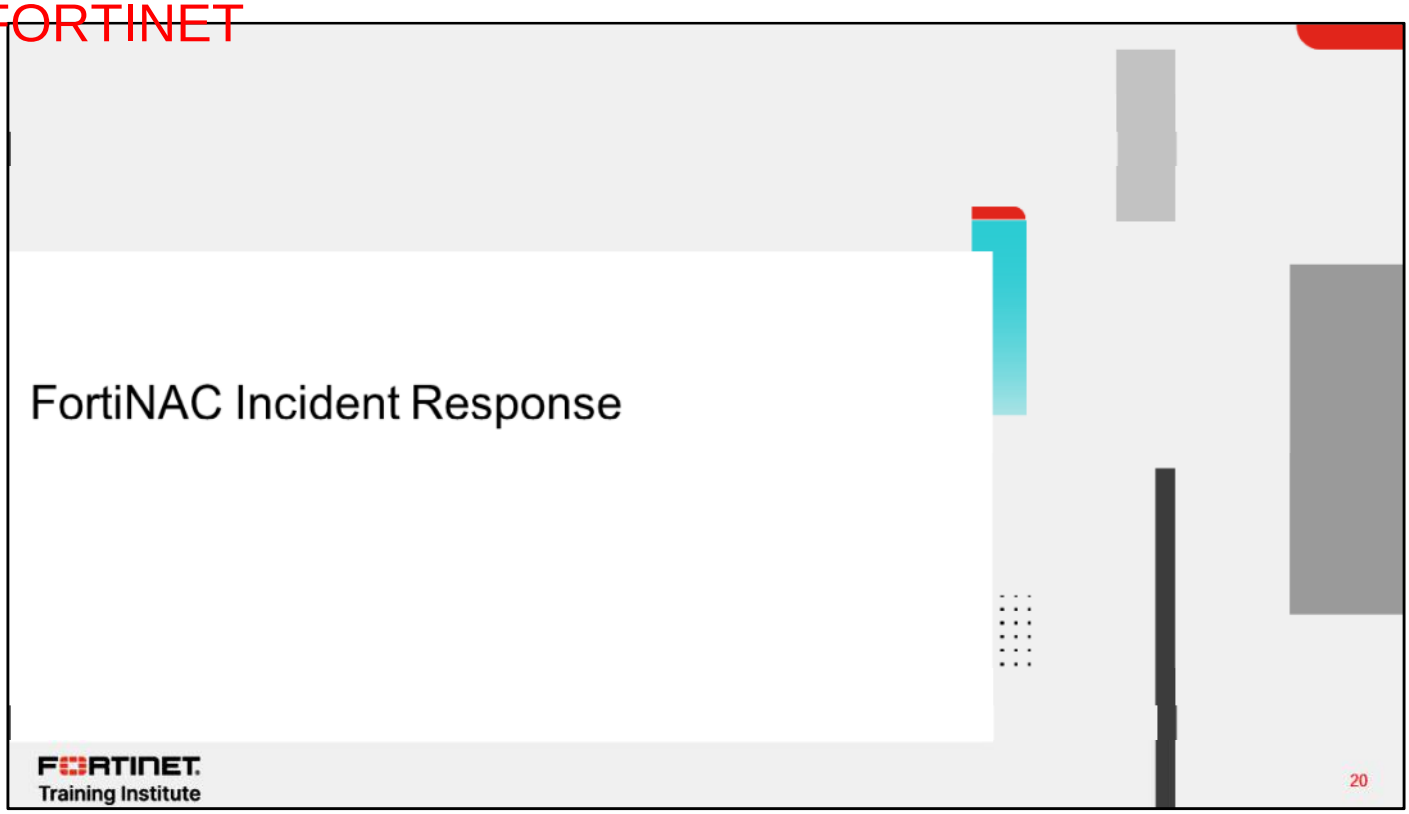
On the **Files** pane, the FortiClient EMS administrator can view quarantined file information for all managed endpoints, and allowlist files from FortiClient EMS, if needed.

FortiClient sends quarantined file information to FortiClient EMS. After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files in **Quarantine Management** on the **Files** pane. You can also view details about each quarantined file and use filters to access quarantined files that have specific qualities.

You can allowlist and restore quarantined files from EMS. This releases the files from quarantine and makes them accessible on the endpoint with the next telemetry communication between FortiClient EMS and FortiClient. The file status changes to **Quarantined & Allowlisted**.

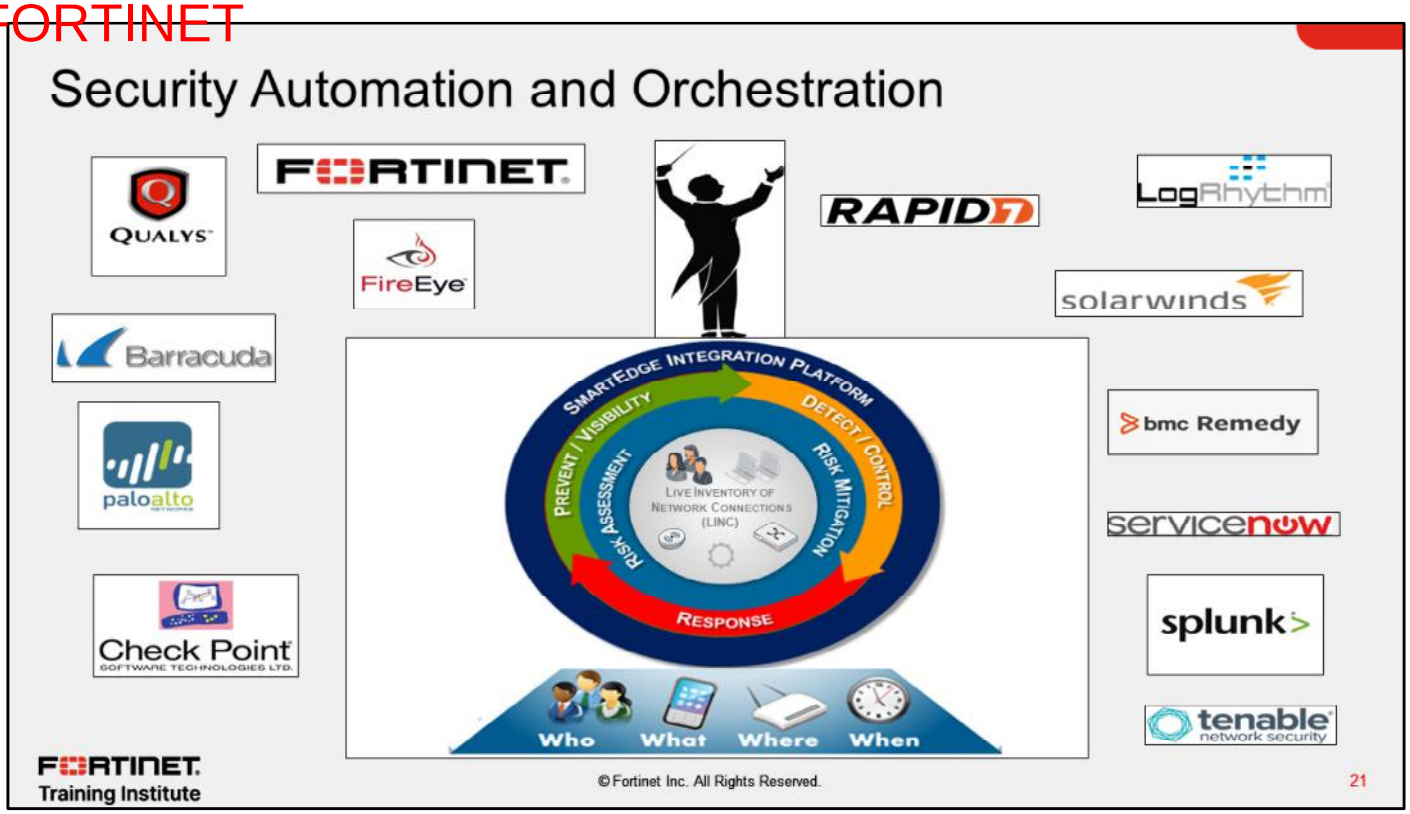
Note that the FortiClient console doesn't allow you to restore and delete quarantined files. These options are grayed out on the FortiClient GUI.

DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiNAC incident response.

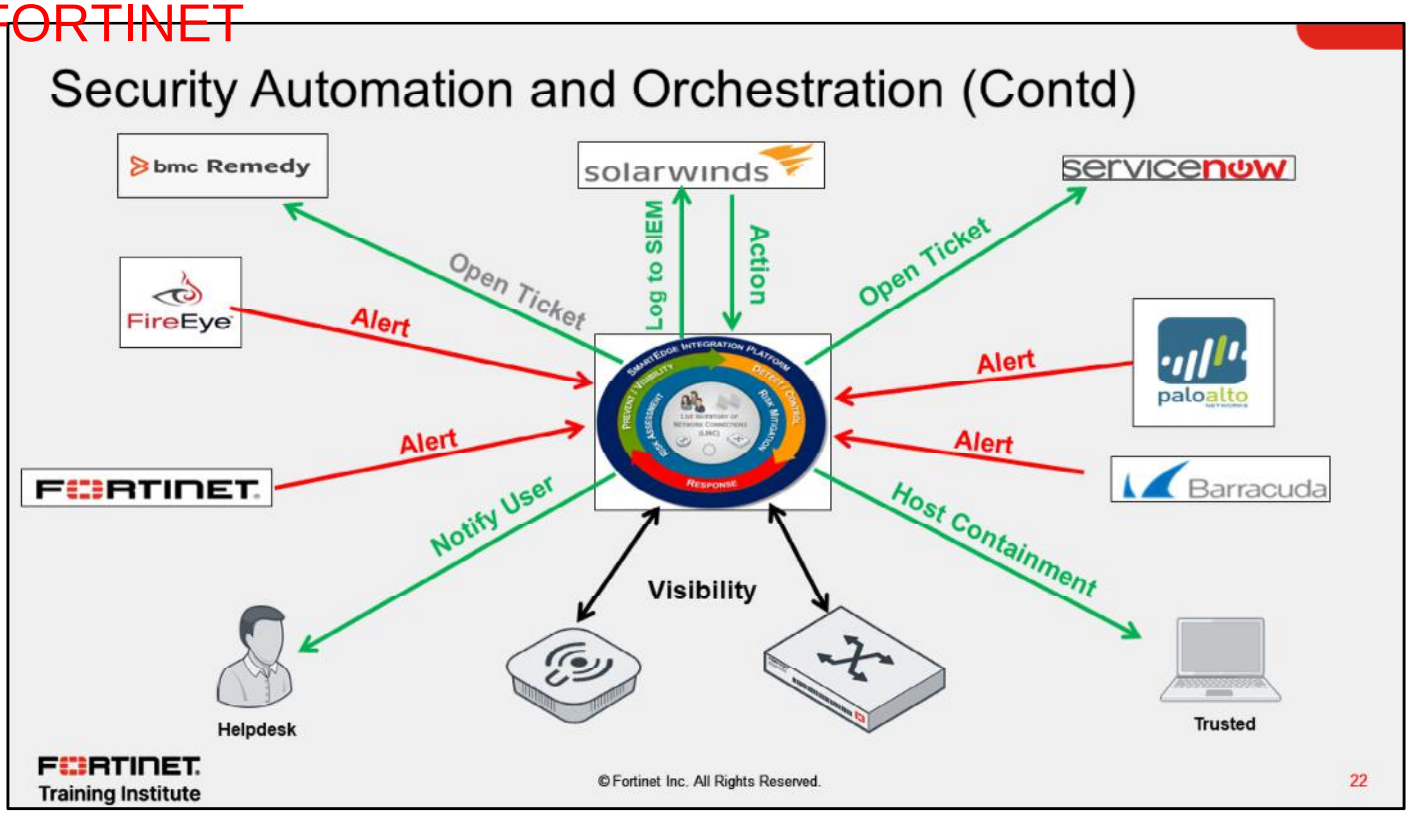
DO NOT REPRINT
© FORTINET



The ability to orchestrate network security processes with FortiNAC empowers an organization to automatically control network access, and respond using detailed workflows designed around received security alerts.

Visibility provides the context necessary to correlate received alerts, and control provides the ability to mitigate or notify based on administrator-defined work flows. The ability to integrate with nearly any device expands the endpoint-based visibility to include real-time knowledge of potentially threatening behavior. The integration is bi-directional, meaning FortiNAC can pass detailed information upstream as well as receive it.

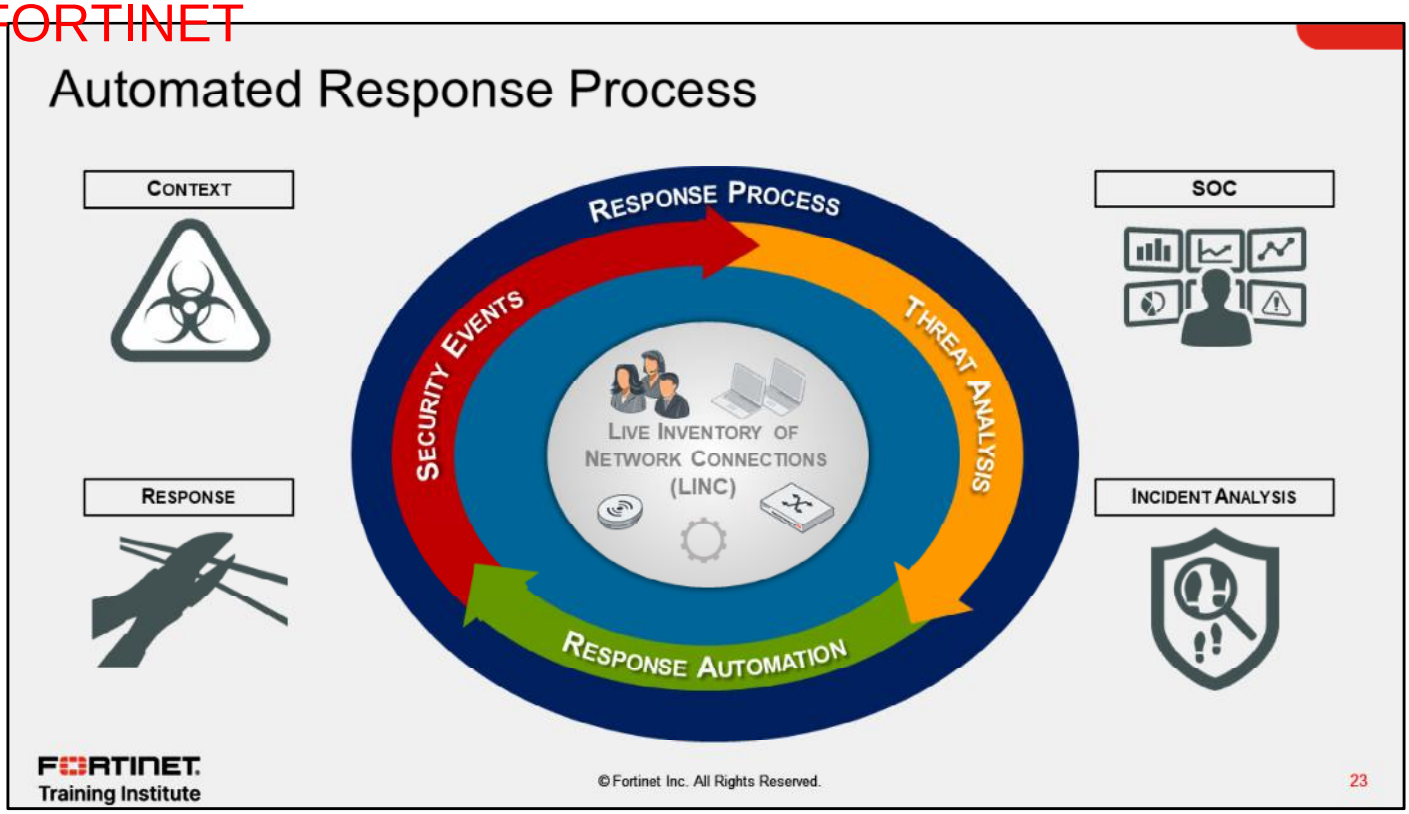
DO NOT REPRINT
© FORTINET



The policy-based platform, leveraging complete end-to-end visibility with the integration of these tools enables the creation of preventative network access and threat triage processes to automate NOC provisioning and SOC threat response procedures.

Security orchestration is the combining of the visibility, detection, control, and response capabilities to create automated prevention processes. The detailed workflows are created to notify, update, log, and provision based on the alerts received from external sources in conjunction with visibility details stored in the FortiNAC database.

DO NOT REPRINT
© FORTINET

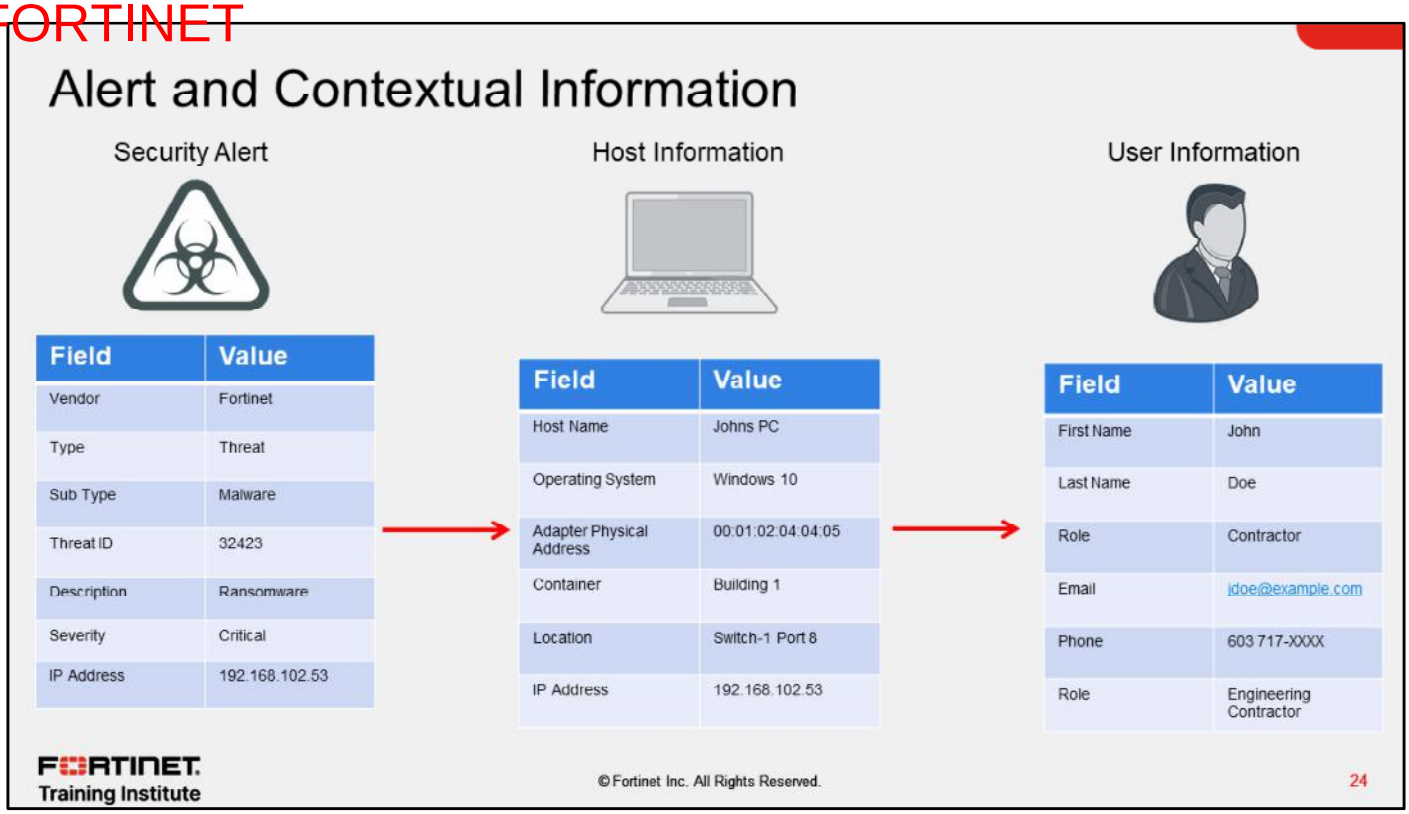


FortiNAC processes the inbound security events, correlates the contextual visibility information, performs detailed analysis of the events against defined security rules, and performs the appropriate action or response to take for that specific incident.

The development of these security rules follows a circular process. Security alerts are processed. The organization determines the desired response to the specific situation, for example, a particular security alert caused by a specific host or user. Then a security rule is created to respond the next time the situation occurs.

Then the process begins again. As more and more security rules are created, there'll be fewer and fewer alerts that need to be manually processed or evaluated.

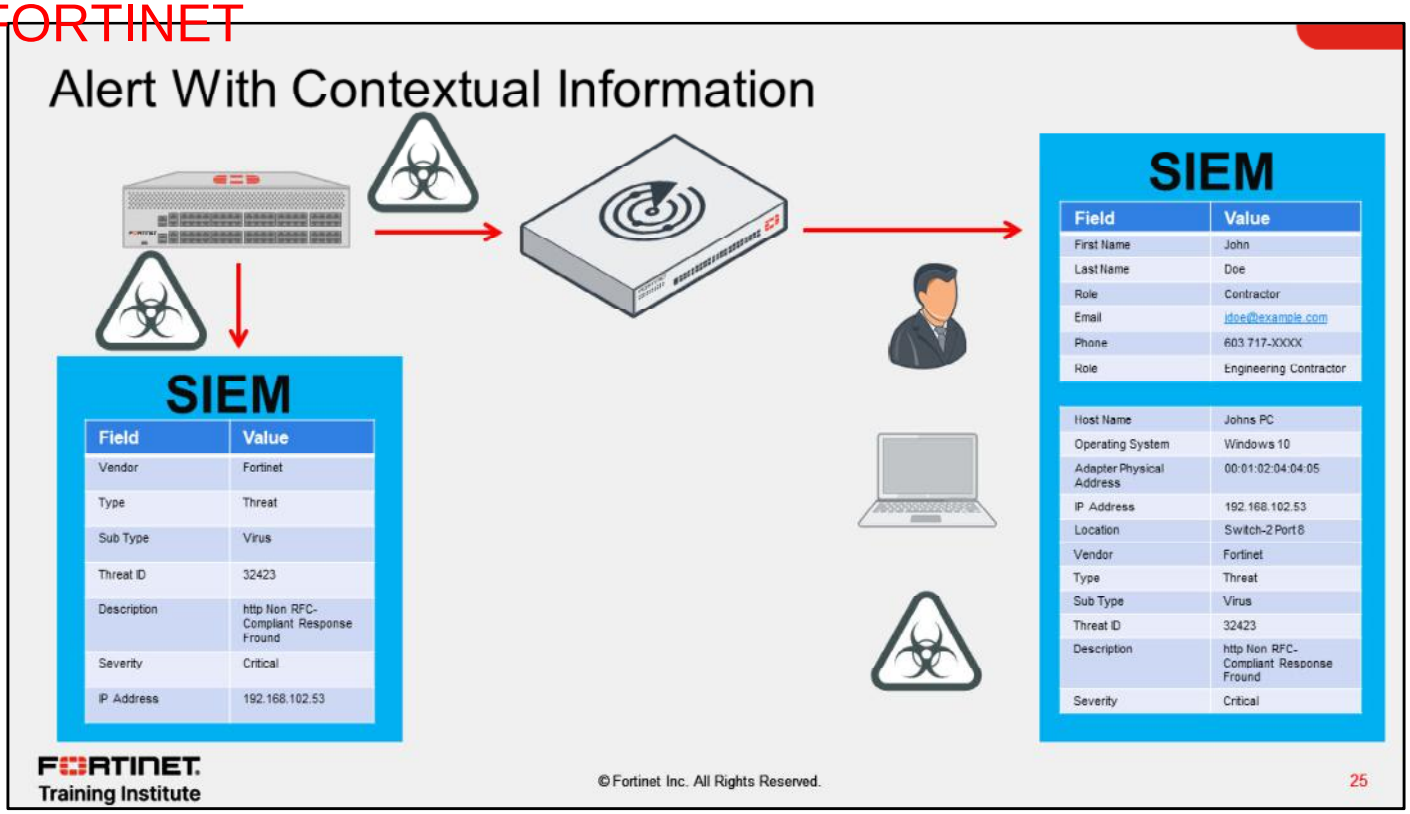
DO NOT REPRINT
© FORTINET



The example shown on this slide displays some of the information that may be received by FortiNAC in the form of a security alert. This information will be combined with the visibility information that exists within the FortiNAC database and will include all of the host and user attributes. For example, you would know the host by name, physical address, IP address, location, and so on, as well as the user information, such as name, email, and phone extension. This provides important information to those that are making the decisions on how to handle this particular type of alert, and helps determine what type of work flow should be designed.

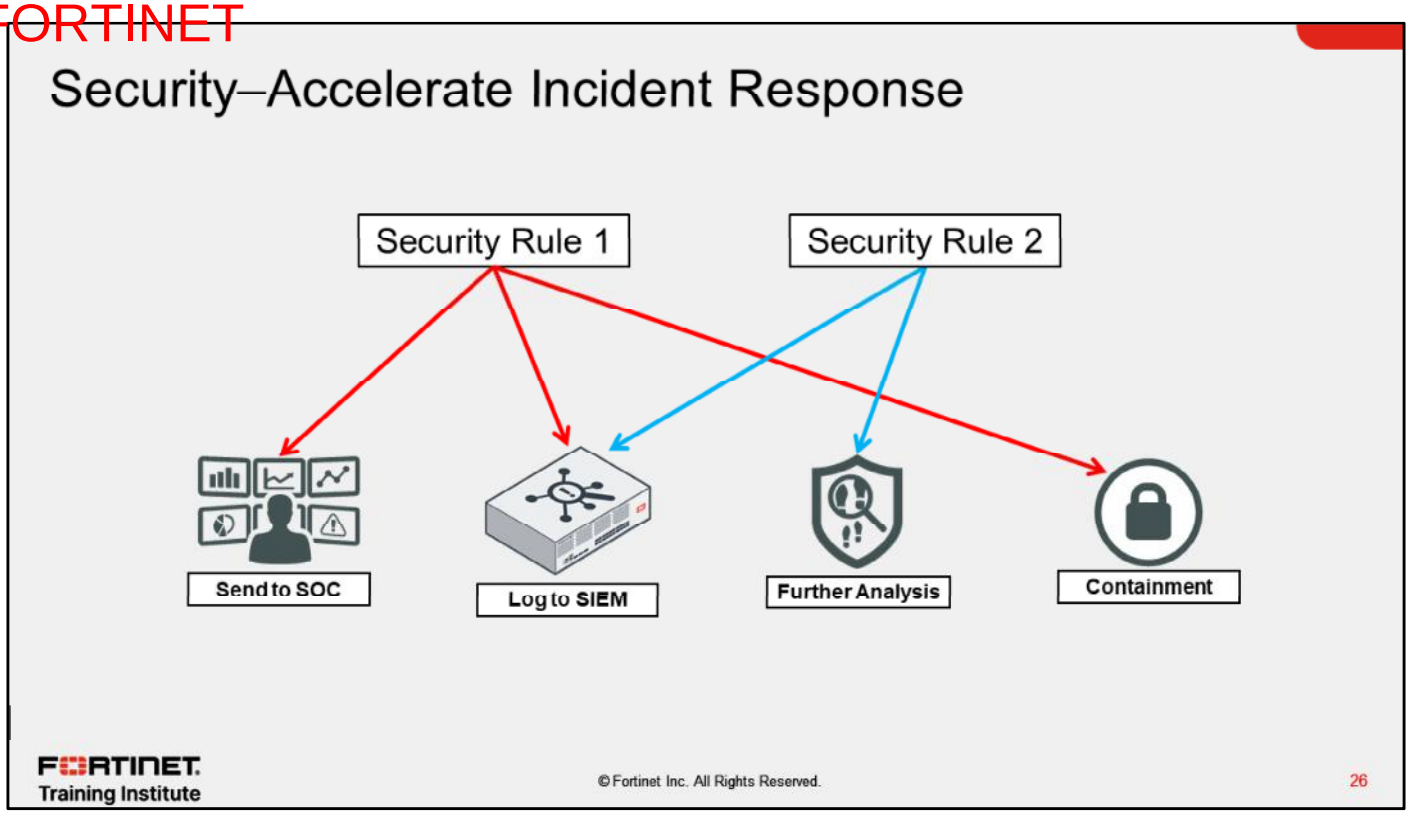
The key attribute that makes the association between the security alert and the host is the IP address. The user information can be both the user that registered the device in a BYOD situation, and the currently logged on user.

DO NOT REPRINT
© FORTINET



Adding the detailed contextual information can be done by directing security alerts to FortiNAC. FortiNAC could then be configured to forward the combined information, alert, host, and user details upstream by designating a log host, as discussed in a previous lesson.

DO NOT REPRINT
© FORTINET

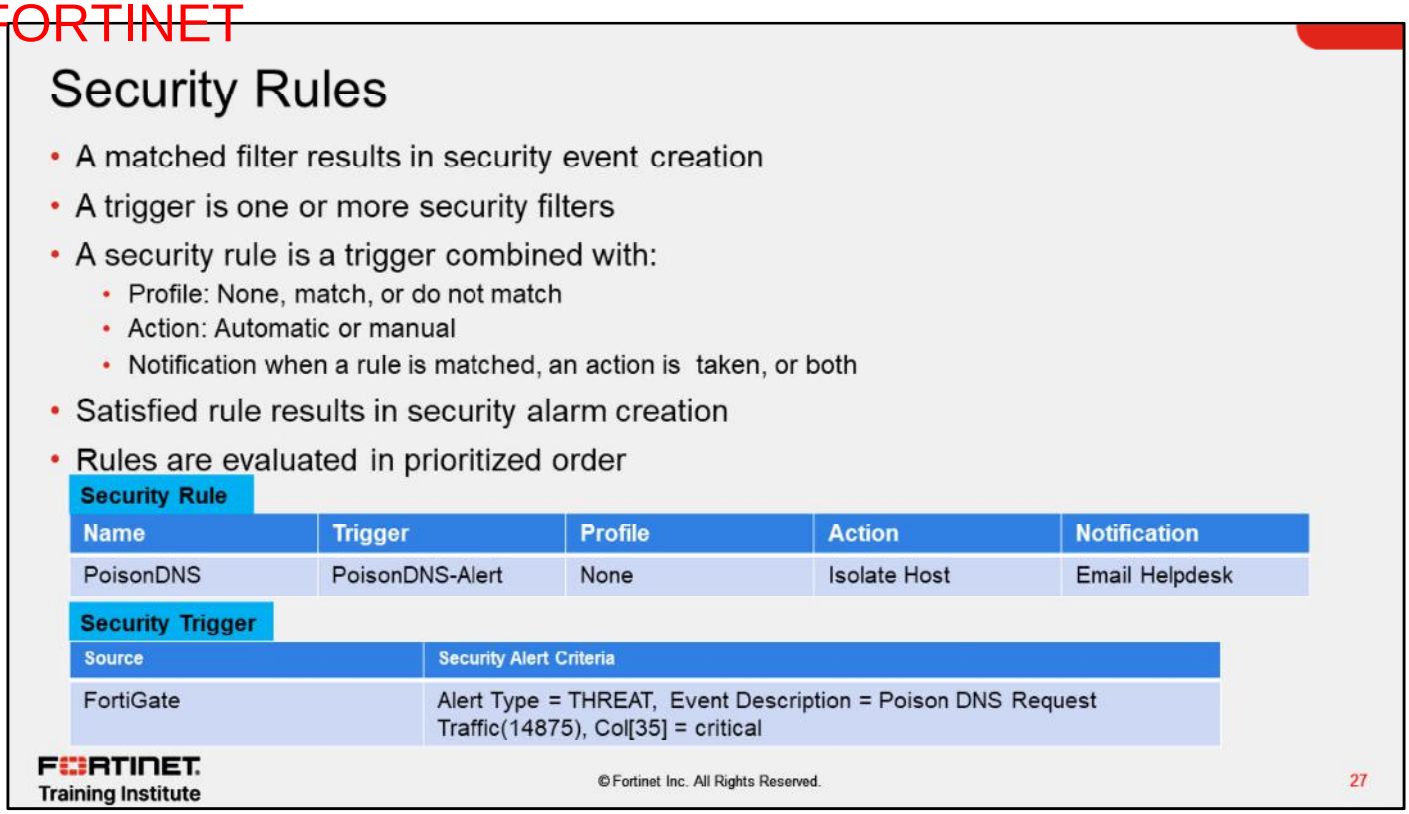


Security automation is enabled through the creation of security rules. These rules can include the actions, or work flows, desired for automated response. Each security rule can execute any number of associated tasks, allowing you to create responses with varying levels of detail. Security rules are ranked and each received security alert is evaluated against each rule in the ranked order until a match is found. If no match is found, no action is taken.

The example shown on this slide depicts two security rules, each with multiple associated actions. If a security alert is received by FortiNAC that matches security rule 1, the associated host will be moved to the quarantine isolation network, the alert, host, and user information will be logged on the SIEM and a notification with those details will be sent to the SOC. If security rule 2 is matched, the alert, host, and user information will be sent to the SIEM and passed along for further analysis.

Security alert information passed along for further analysis is normally the starting point for new rule creation. As the alerts are more fully understood, new work flows can be created to automate the responses and new rules can be created to leverage those work flows.

DO NOT REPRINT
© FORTINET



A filter is a set of defined criteria evaluated against the contents of a parsed security alert. Any field contained in the security alert can be used as part of a filter. Some fields are normalized, meaning they are mapped to specific field names, such as Severity, Source Address, and so on. Other fields will be identified using column numbers or tag values. When a filter is evaluated, all designated criteria must match for a true result. When a filter evaluation returns a true result, a **Security Event** is generated.

A trigger is one or more filters. A time occurrence requirement can be configured defining a window of time setting for two or more filters. For example, the trigger could be satisfied if all or a subset of the filters are matched within 2 minutes. If all trigger criteria are satisfied, a user/host profile requirement can be added.

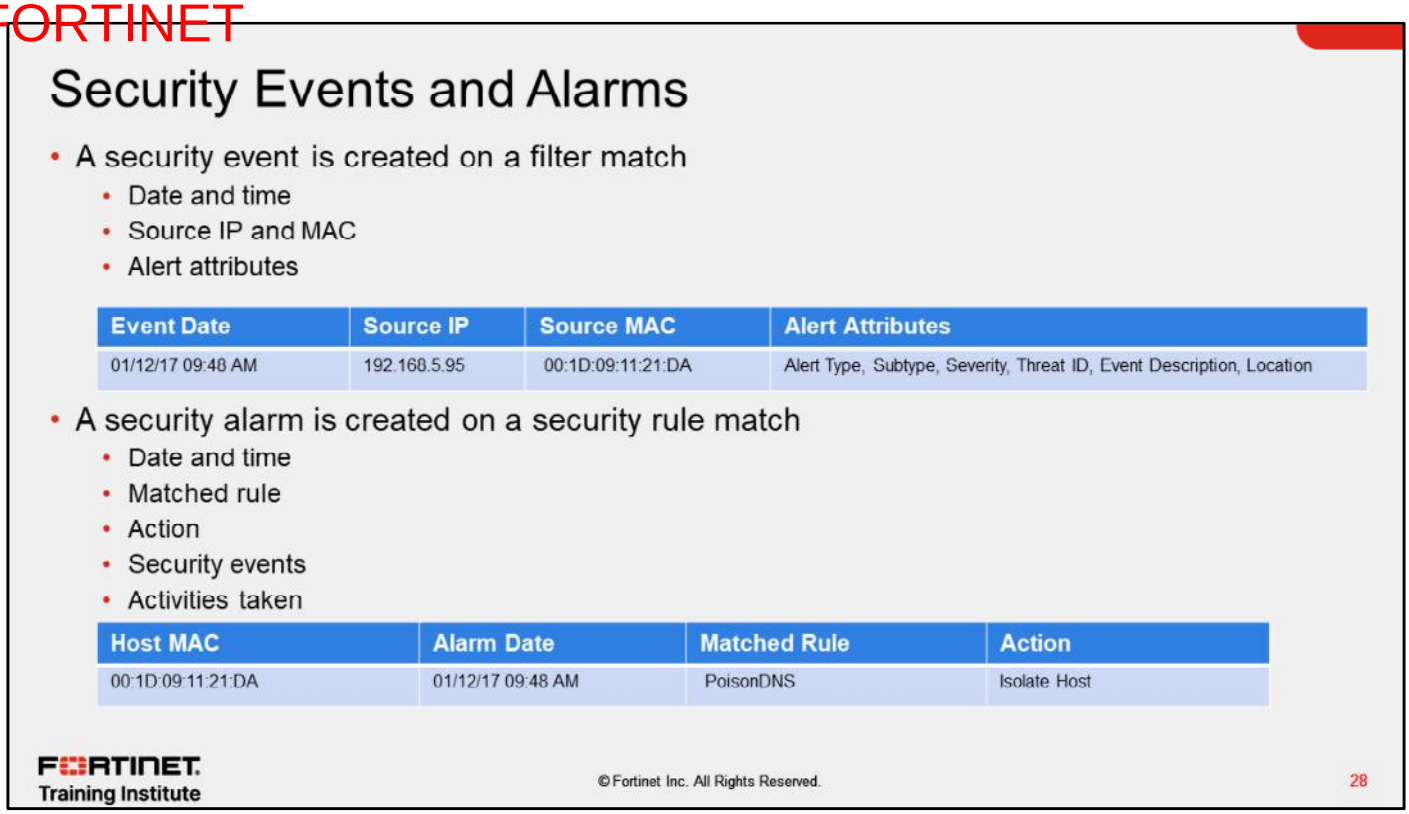
The logic that can be applied to the user/host profile requirement options are:
- **None**: No user/host profile requirement
- **Match**: The user or host element associated with the security event must match the profile
- **Do Not Match**: The user or host element associated with the security event must not match the profile

If the trigger is satisfied, and the user/host profile requirement is met, a **Security Alarm** is generated and any associated actions are executed. An action consists of one or more activities. Activities are the wide variety of tasks FortiNAC can perform. For example, an action could consist of the activities needed to mark a host at risk, change the host's role value, and/or send a message to the host.

Security rules are evaluated in order of priority.

The examples shown on the bottom of this slide highlight the components of a **Security Rule** as well as those of a **Security Filter**.

DO NOT REPRINT
© FORTINET



Any time a filter is matched, a security event is generated. Security events will contain the following information about the host that caused the security alert to be issued:

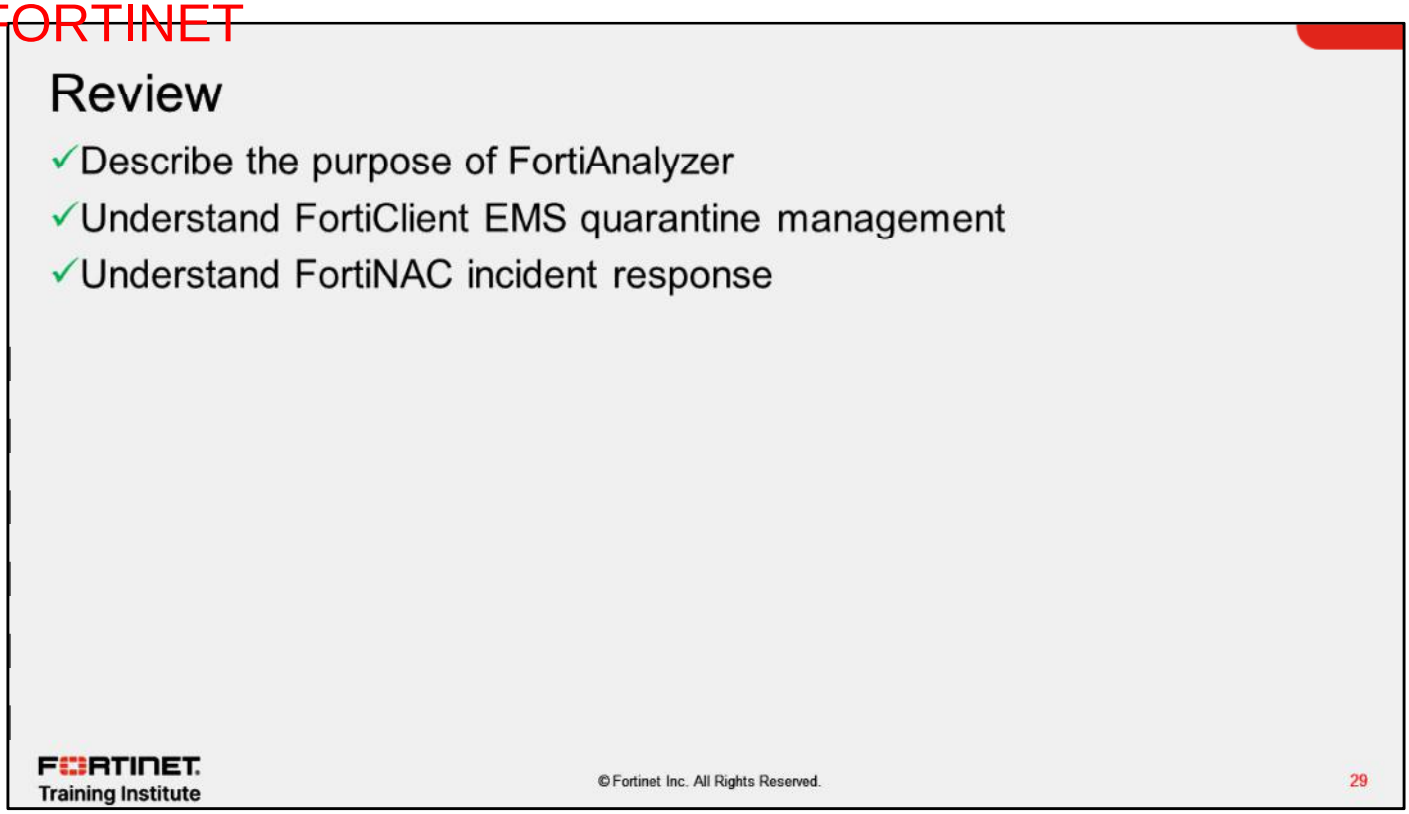
- Date and time
- Source IP
- Source Mac
- Destination IP
- Location

The security event will also contain the Alert Type, Subtype, Severity, Threat ID, and Event Description of the security alert.

A security alarm will contain the host MAC, alarm date and time, the security rule that was matched, and any actions taken.

Note, that for each security alarm generated, there will be at least one associated security event. Recall that a trigger could contain more than one filter, and each matched filter would generate a security event. For example, a trigger that requires two filters to be matched, would have two security events associated with the security alarm each time the trigger was satisfied.

DO NOT REPRINT
© FORTINET



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

By mastering the objectives covered in this lesson, you learned about the purpose of FortiAnalyzer, FortiClient EMS quarantine management, and FortiNAC incident response.

DO NOT REPRINT
© FORTINET

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© 2023 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.