DEFINE • DESIGN • **DEPLOY** • DEMO

Zero Trust Network Access

Deployment Guide

Version 7.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 14, 2023
Zero Trust Network Access 7.0 Deployment Guide
01-700-765857-20230414

TABLE OF CONTENTS

Change Log ... **5**
Deployment overview ... **6**
Audience ... 7
About this guide ... 7
Design considerations ... 7
ZTNA access proxy ... 7
ZTNA secure access ... 8
Summary ... 8
Success criteria ... 8
Product prerequisites ... 8
FortiClient ... 9
FortiClient EMS ... 9
FortiGate ... 10
FortiAnalyzer ... 10
FortiAuthenticator and FortiToken (recommended) ... 10
Additional component information ... 11
Deployment plan ... 12
Deployment procedures ... **13**
Configuring FortiClient EMS ... 14
Configuring connectivity from FortiGate to FortiClient EMS ... 14
Configuring a fabric connector ... 14
Authorizing the fabric connection to FortiGate ... 15
Configuring FortiClient EMS tags and rules ... 16
Configuring a rule for detecting a file ... 16
Configuring a rule for detecting AD login ... 17
Configuring Zero Trust tags to display in FortiClient ... 17
Verifying tags ... 17
Configuring ZTNA HTTPS access proxy to web servers ... 19
Configuring ZTNA TCP forwarding access proxy ... 21
Configuring the authentication scheme and rule ... 22
Configuring an authentication scheme ... 23
Configuring an authentication rule ... 24
Configuring ZTNA rules to control access ... 24
Configuring a ZTNA rule for denying access ... 24
Configuring a ZTNA rule for allowing access ... 25
Configuring ZTNA connection rules ... 25
Configuring ZTNA connection rules for RDP and SSH ... 26
Verifying receipt of connection rules ... 27
Verifying ZTNA connectivity ... 28
Verifying access to web servers ... 28
Verifying user connectivity from FortiGate ... 31
Verifying RDP access to FortiClient EMS ... 34
Verifying SSH access to FortiAnalyzer ... 35
Verifying denied access due to failed posture check ... 36

More information **37**

Change Log

Date	Change Description
2022-03-15	Initial release.
2023-03-14	Updated Configuring FortiClient EMS tags and rules on page 16.
2023-04-14	Updated FortiAnalyzer on page 10.

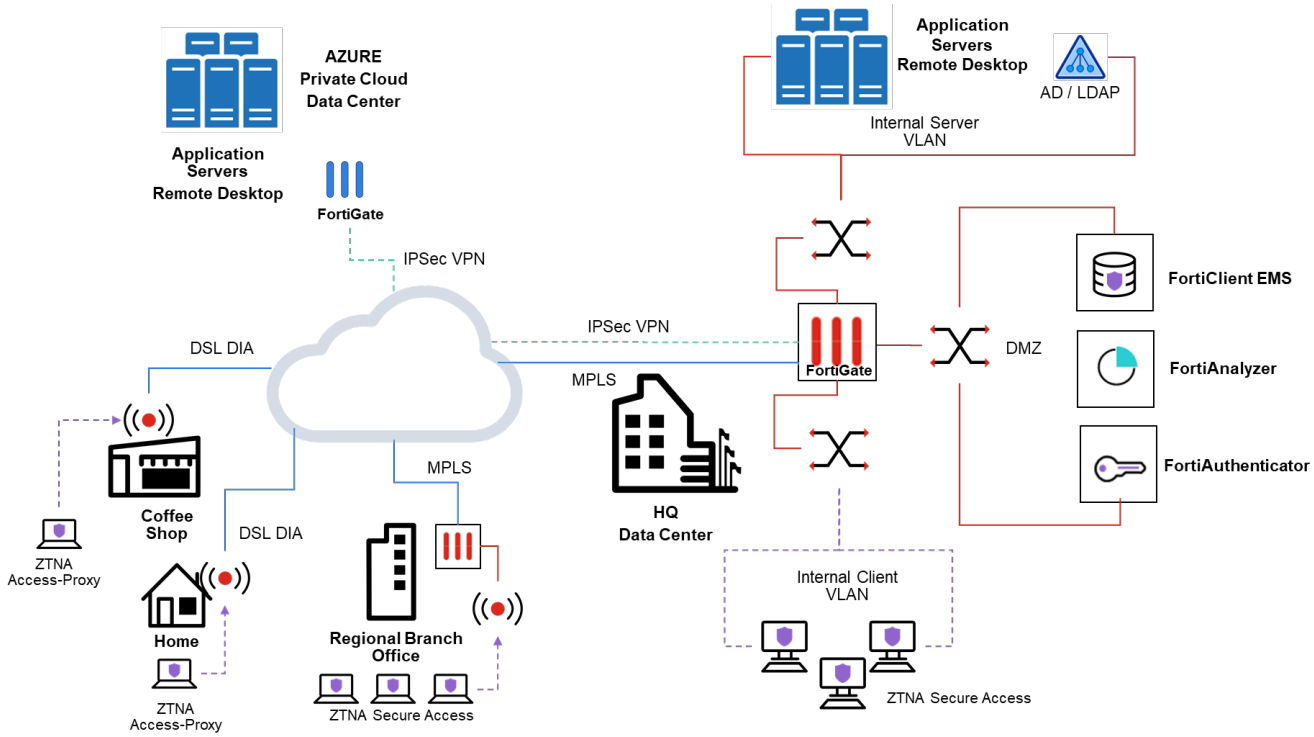
Deployment overview

This document provides a deployment example of Fortinet's Zero Trust Network Access (ZTNA), covering the following solutions:

- ZTNA access proxy
  - HTTPS and TCP access proxy solution and architecture
  - Applies to both remote access and internal access to the internal network
  - No persistent connection (such as VPN) is necessary
- ZTNA secure access
  - Remote users continue to access the internal network by using VPN, with additional layers of ZTNA device identity and ZTNA posture checking provided by rules and tagging
  - Local users access the internal network through local access policies and ZTNA posture checks

Using a similar scenario and topology example from the *ZTNA Architecture Guide*, we will walk through deploying the core components by providing configuration examples to help you migrate from dial-up VPN to ZTNA access proxy for remote users and ZTNA secure access for local users and those that still require VPN.

The goal is to reduce the reliance on dial-up VPN by adding device authentication with role-based application access. We will focus on the services located at head quarters (HQ) along with remote users currently using dial-up VPN. Concepts from this deployment guide can be applied to regional offices and even cloud datacenters.



Audience

Midlevel network and security architects in companies of all sizes and verticals should find this guide helpful. A working knowledge of FortiOS and the Fortinet Security Fabric is helpful.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. It is advisable to review the Reference Architecture Guide(s), such as the *ZTNA Architecture Guide*, if readers are still in the process of selecting the right architecture. See also the *ZTNA Concept Guide*.

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product administration guides, example guides, cookbooks, release notes, and other documents where appropriate on the Fortinet Document Library.

Design considerations

Traditionally, VPN is used to secure data flowing in an otherwise insecure connection. However, the method of access over VPN often doesn't account for the risk of infected or non-compliant endpoints infecting network devices. Given the greater risks of allowing remote devices into the network, their access is often limited.

ZTNA tackles some of these issues by securing your traffic over an SSL connection, validating the device identity, verifying that appropriate endpoint security features are turned on, and authenticating user identity. These measures help reduce security risk factors to give remote users a level of access similar to what is available when working locally in the office. This also gives rise to role-based application access, where access is granted based on the user and device roles, instead of the traffic source.

ZTNA access proxy

ZTNA access proxy allows users to securely access resources through an SSL encrypted access proxy. This simplifies remote access by eliminating the use of dial-up VPNs. ZTNA rules and tagging offer additional identity and posture checking. ZTNA access proxy has two components:

- HTTP access proxy for web applications
- TCP forwarding access proxy (TFAP) for other supported applications

ZTNA HTTP access proxy allows secure remote access to web-based applications, while ZTNA TCP forwarding access proxy is used for other applications, such as SSH, Remote Desktop Protocol (RDP), and others, whether hosted in the physical datacenter or cloud.

ZTNA secure access

ZTNA secure access uses ZTNA rules and tagging to provide additional factors of identification for role-based Zero Trust access and posture checking, typically for local On-net users or for remote users when VPN is necessary. ZTNA secure access consists of:

- ZTNA rules and tagging
  FortiClient EMS is used to configure identity and posture checks that will tag the endpoint for use.
- ZTNA client
  FortiClient is used to execute the identity and posture checks, and relay the information to FortiClient EMS for use in the Security Fabric, which provides the ZTNA rules and dynamic address lists.

Summary

As discussed in the *ZTNA Architecture Guide*, when using ZTNA access proxy, it is important to consider when to apply HTTPS access proxy or TCP forwarding access proxy. Generally, web applications will fall under the former. Non-web applications, such as RDP, will fall under the latter, which is generally most useful for securing remote access. Remember the design goal for Zero Trust Network Access: a device inside the network is trusted no more than a device outside the network. With this in mind, we use ZTNA secure access features to check the posture of devices directly connected to internal network segments and verify the identity of the users accessing the applications locally.

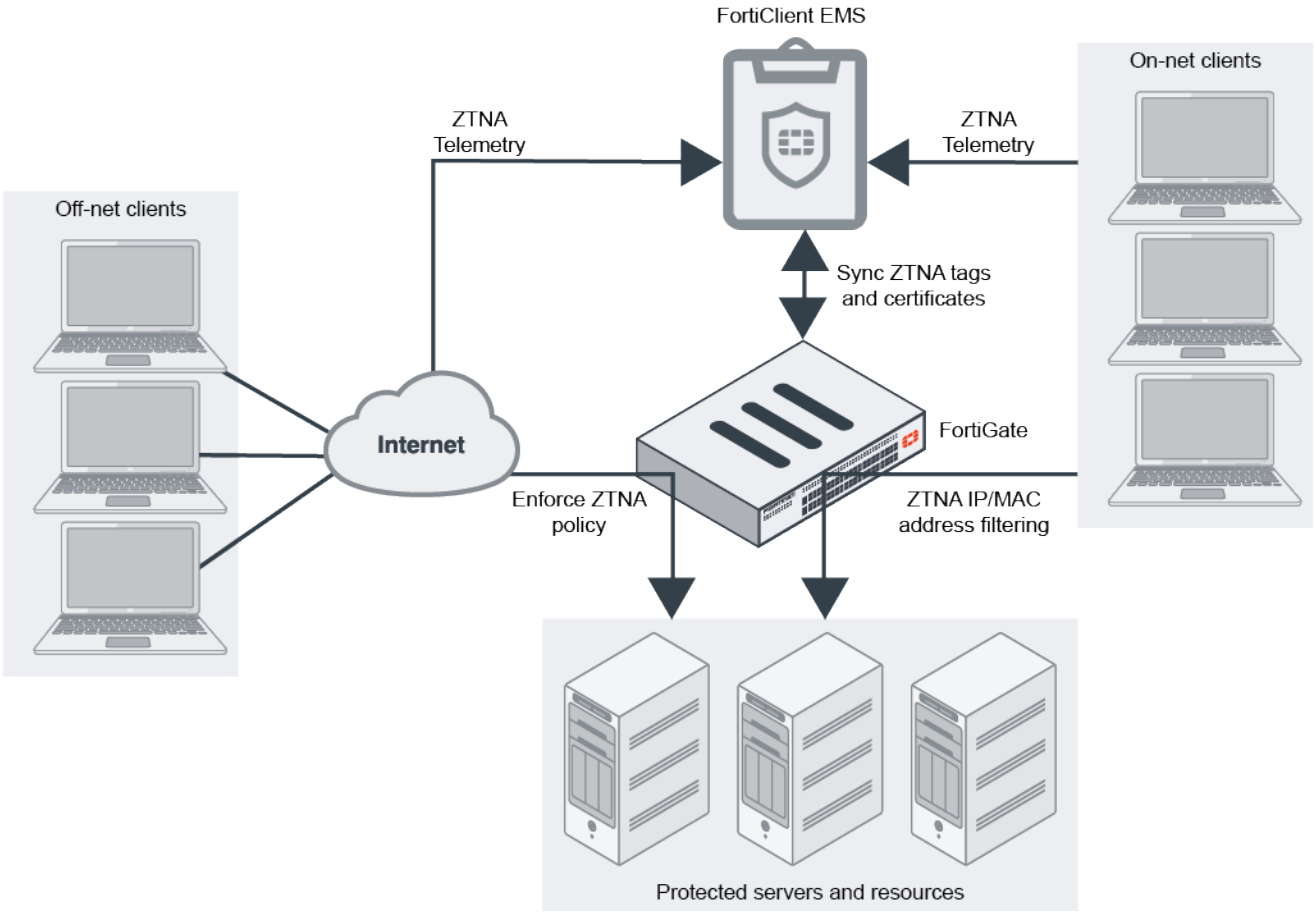
Success criteria

In the ZTNA design, the goal is to enhance security by improving identity and posture checking of devices connecting to the internal network, and by reducing the attack surface of traditional dial-up VPN. In our use case, the following success criteria is detailed:

- Block unmanaged devices
- Require multi-factor authentication
- For remote users, limit direct access to the internal network for web applications or remote desktop services
- Allow only identified user groups access to only the specific applications that they need
- Dynamically deny access to devices with critical vulnerabilities both on the internal network and remote locations
- Dynamically allow access once the vulnerabilities are remediated
- Reduce the reliance on dial-up VPN

Product prerequisites

ZTNA uses several products to establish device identity and device trust context. FortiClient, FortiClient EMS, and FortiGate are all integral to ZTNA, and used to establish device identity by using client certificates, device trust context, and user identity.



FortiClient

FortiClient is a required component for ZTNA. It is the ZTNA client on each endpoint.

For licensing information, review the FortiClient data sheet found in FortiClient Endpoint Security Overview.

FortiClient endpoints provide the following information to FortiClient EMS when the endpoints register to FortiClient EMS:

- Device information (network details, operating system, model, and others)
- Logged on user information
- Security posture (On-net/Off-net, antivirus software, vulnerability status, and others)

FortiClient also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) when it registers to FortiClient EMS. FortiClient uses the certificate to identify itself to the FortiGate.

FortiClient EMS

FortiClient EMS is a required component for ZTNA.

Licensing for FortiClient EMS is included with the FortiClient ZTNA license. See also FortiClient Endpoint Security Overview.

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. The certificate is then synchronized to the FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with the FortiGate, so that the FortiGate can use it to authenticate the clients.

FortiClient EMS uses Zero Trust tag rules to tag endpoints based on the information that it has on each endpoint. The tags are also shared with FortiGate.

FortiGate

FortiGate is a required component for ZTNA.

ZTNA Licensing is included with FortiOS. The minimum recommended license bundle is Unified Threat Protection, and the recommended license bundle is Enterprise Protection. See the data sheets found in Next-Generation Firewall.

FortiGate maintains a continuous connection to FortiClient EMS to synchronize endpoint device information, including primarily:

- FortiClient UID
- FortiClient certificate serial number
- FortiClient EMS serial number
- Device credential (user/domain)
- Network (IP and MAC address and route to the FortiGate)

When a device's information changes, such as when a client moves from On-net to Off-net, or their security posture changes, FortiClient EMS is updated with the new device information, and then updates the FortiGate. FortiGate's wad daemon can use this information when processing ZTNA traffic.

FortiAnalyzer

FortiAnalyzer is a recommended component for ZTNA.

FortiAnalyzer is licensed by anticipated log volume. VM and hardware models are available. For details, see the data sheet found in FortiAnalyzer Overview.

FortiAnalyzer is used for gathering and analyzing logs as well as generating reports for Fortinet devices. FortiAnalyzer should be available from everywhere. FortiAnalyzer receives logs directly from FortiClient, and FortiAnalyzer is integral for analyzing and reporting on users and devices connected to the network. Optional SOC services are invaluable for quickly reacting to IOCs and other related security events.

FortiAuthenticator and FortiToken (recommended)

FortiAuthenticator and FortiToken are recommended components for ZTNA, but they are not required.

For licensing information, review the FortiAuthenticator and FortiToken data sheets.

FortiAuthenticator provides network and user identity authentication services to all ZTNA components. It also incorporates multi-factor authentication through FortiToken and FortiToken Cloud. By centralizing authentication services within FortiAuthenticator, the ZTNA solution can easily scale as different components connect without duplicating user configurations.

Additional component information

ZTNA Solution	Licensing	Existing Infrastructure
FortiClient ZTNA client 7.0	Review the FortiClient data sheet	Available deployment techniques include: an existing software deployment tool (for example, SCCM), native deployment through FortiClient EMS (Windows only), and a manual download location accessible for outliers.
FortiClient Endpoint Management Server (EMS) 7.0	Included with FortiClient ZTNA license	FortiClient EMS must be accessible to clients from everywhere. In this design, FortiClient EMS is deployed in a DMZ. Active Directory integration to FortiClient EMS may also be necessary for client deployment and ease of applying different endpoint profiles to corresponding groups in AD.
FortiOS ZTNA Access Proxy 7.0	Included with FortiOS Minimum recommended bundle is Unified Threat Protection Recommended bundle is Enterprise Protection	Review FortiGate performance requirements, and ensure existing FortiGates meet those requirements. In this simple deployment example, the FortiGate and Security Fabric are central to all traffic and to protect traffic flow to critical resources.
FortiOS Identity Service Provider (SP)	Included with FortiOS	The FortiGate acts as an SP and integrates with FortiAuthenticator as an IdP broker, providing integration to Active Directory and MFA services with SAML.
FortiAuthenticator Identity and Access Management (IAM)	Review FortiAuthenticator data sheet	When multiple FortiGates are deployed, FortiAuthenticator is desirable to consolidate and manage connections to IdPs, including Active Directory, LDAP, Radius, and SAML providers. In this use case, FortiAuthenticator is not strictly necessary, but is included in the deployment as an example for larger deployments.
FortiToken Multi-factor Authentication (MFA)	Review FortiToken data sheet	MFA is recommended for connecting to any critical resources. In addition to device and user authentication, another factor of authentication that utilizes one-time passwords (OTP) is desirable to help protect against stolen credentials. An existing OTP product can be integrated through SAML. In this deployment, we apply FortiToken to users in FortiAuthenticator. In smaller, single FortiGate organizations, FortiToken can be managed directly on the FortiGate.
FortiAnalyzer	Review FortiAnalyzer data sheet. VM and hardware models available. License by anticipated log volume.	FortiAnalyzer is recommended for gathering logs, analyzing logs, and generating reports for Fortinet devices. FortiAnalyzer should be available from everywhere. FortiClient ZTNA sends logs directly to FortiAnalyzer.

Deployment plan

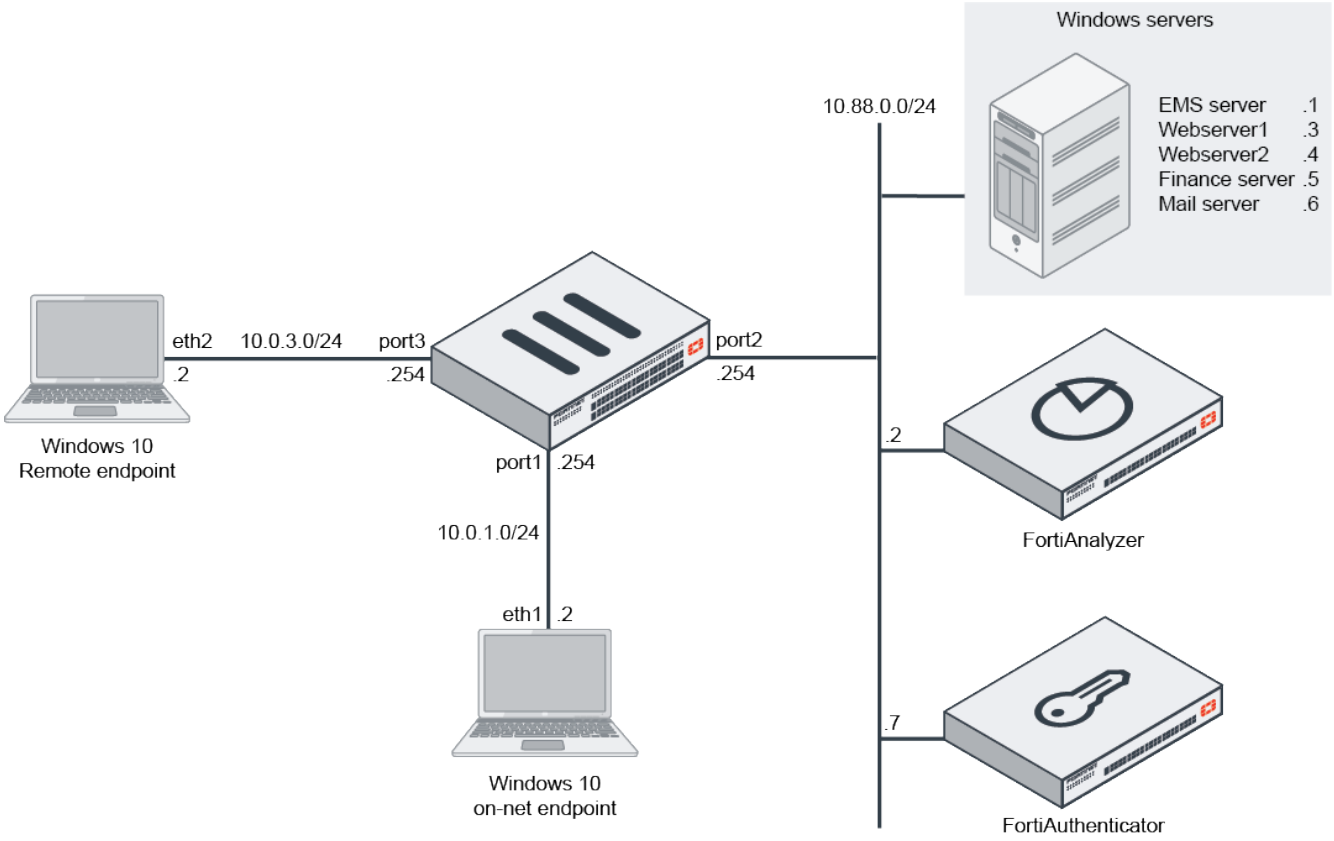
This high level ZTNA deployment plan consists of a simple network with a FortiGate configured for dial-up VPN use. FortiClient EMS is implemented and managing FortiClient for dial-up VPN. The other components are installed and placed in the appropriate segments of the network.

To deploy a ZTNA solution and reduce reliance on VPN, configure the following components in the following order:

1. In FortiClient EMS, ensure basic configuration, and learn more about key features related to ZTNA.
2. In FortiOS, configure connectivity between FortiGate and FortiClient EMS.
3. In FortiClient EMS, configure ZTNA tags and rules.
4. In FortiOS, configure ZTNA HTTPS access proxy to web servers.
5. In FortiOS, configure ZTNA TCP forwarding access proxy for RDP and SSH.
6. In FortiOS, configure an authentication scheme and policy for user authentication.
7. In FortiOS, configure ZTNA rules to control access.
8. In FortiClient EMS, configure ZTNA connection rules.

Deployment procedures

The deployment example has the following topology:



In this example, a customer uses SSL VPN for their teleworking solution, and is now migrating to using ZTNA. In this case, FortiGate has the necessary LDAP configurations to connect to the local Active Directory server. This user configuration will now be used for the ZTNA solution.

We will also demonstrate how to use FortiAuthenticator and SAML authentication.

Remote users will utilize ZTNA access proxies, and local users will use ZTNA secure access to reach internal resources. Both methods require endpoints with FortiClient installed, registered, and connected to FortiClient EMS.

This deployment scenario will demonstrate how to use HTTP access proxy for web applications and TCP forwarding access proxy for other applications, such as RDP.

Following is an overview of the procedure:

1. In FortiClient EMS, ensure basic configuration, and learn more about key features related to ZTNA. See Configuring FortiClient EMS on page 14.
2. In FortiOS, configure connectivity between FortiGate and FortiClient EMS. See Configuring connectivity from FortiGate to FortiClient EMS on page 14.
3. In FortiClient EMS, configure ZTNA tags and rules. See Configuring FortiClient EMS tags and rules on page 16.

4. In FortiOS, configure ZTNA HTTPS access proxy to web servers. See Configuring ZTNA HTTPS access proxy to web servers on page 19.
5. In FortiOS, configure ZTNA TCP forwarding access proxy for RDP and SSH. See Configuring ZTNA TCP forwarding access proxy on page 21.
6. In FortiOS, configure an authentication scheme and policy for user authentication. See Configuring the authentication scheme and rule on page 22.
7. In FortiOS, configure ZTNA rules to control access. See Configuring ZTNA rules to control access on page 24.
8. In FortiClient EMS, configure ZTNA connection rules. See Configuring ZTNA connection rules on page 25.
9. From a remote computer, verify ZTNA connectivity. See Verifying ZTNA connectivity on page 28.

Configuring FortiClient EMS

This guide assumes that FortiClient EMS is installed and configured with basic settings. This guide includes best practice recommendations as well as references to the *FortiClient EMS Administration Guide* for further instructions. This guide also dives deeper into configuring ZTNA related configurations on FortiClient EMS.

This section includes information about ZTNA related settings on FortiClient EMS.

Increased security in communication between FortiClient EMS and FortiClient

Starting with FortiClient EMS 7.0.2, secure communication between FortiClient and FortiClient EMS is enhanced to allow the use of customer provided certificates instead of Fortinet certificates. The options are Let's Encrypt certificates through the ACME protocol, where proof of your domain is required, or customer provided certificates from a CA that is trusted by the customer devices. For further instructions, see Adding a SSL certificate to FortiClient EMS.

It is desirable to define an FQDN address for FortiClient EMS. The FQDN should map to a public address that your remote and local users can access. This FQDN can be used in the *Subject Alternative Name (SAN)* field of your certificate. Alternatively, as demonstrated in this deployment guide, we will use a wildcard certificate that is signed for **.ztnademo.com*. Users will connect to *ems.ztnademo.com* to securely reach FortiClient EMS. For further instructions, see Configuring connectivity from FortiGate to FortiClient EMS on page 14.

Configuring connectivity from FortiGate to FortiClient EMS

Once basic ZTNA settings are configured in FortiClient EMS, you can connect FortiGate to FortiClient EMS by using a fabric connector.

This section includes the following procedures:

1. In FortiOS, configure a fabric connector from FortiGate to FortiClient EMS. See Configuring a fabric connector on page 14.
2. In FortiClient EMS, authorize the fabric connection to FortiGate. See Authorizing the fabric connection to FortiGate on page 15.

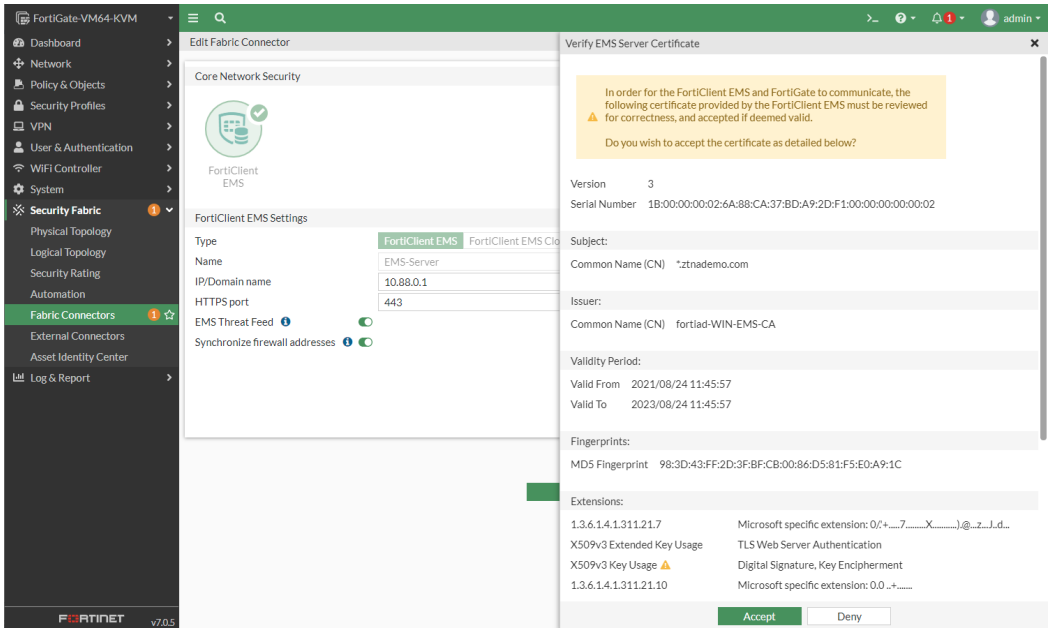
Configuring a fabric connector

In FortiOS, configure a fabric connection to FortiClient EMS.

To configure a fabric connector:

1. In FortiOS, go to *Security Fabric* > *Fabric Connectors*.
2. Create a new *FortiClient EMS* connection.
3. For *Type*, click *FortiClient EMS*.
4. In the *Name* box, type *EMS-Server*.
5. In the *IP/Domain name* box, type the IP address of FortiClient EMS, for example, *10.88.0.1*, and click *OK*.
   The *Verify EMS Server Certificate* pane displays, so you can verify the EMS server certificate.

The example uses the wildcard certificate for **.ztnademo.com*.



6. Click *Accept*.
7. Click *OK*.
   We will authorize the FortiGate through the FortiClient EMS GUI.
   In FortiOS, the status will appear *Down*, until you authorize the FortiGate in FortiClient EMS.

Authorizing the fabric connection to FortiGate

In FortiClient EMS, authorize the fabric connection to FortiGate. After you authorize the connection, you can return to FortiOS to view the connection status.

To authorize a fabric connection:

1. Go to FortiClient EMS, and log in.
   A window displays, requesting you to authorize the FortiGate.
2. Click *Authorize*.
3. Go to *Administration* > *Fabric Devices*, and authorize the FortiGate.

4. Return to FortiOS, and refresh the connection status.
   The connection status displays *Successful*.

Configuring FortiClient EMS tags and rules

Once connectivity between FortiGate and FortiClient EMS is established, you can begin defining ZTNA tags and tagging rules in FortiClient EMS. The rules help capture the security posture of endpoints by assigning ZTNA tags according to the rules. The tags are synchronized with FortiGate, and can be used in the ZTNA policies to perform posture checks and grant access.

In this example, we define ZTNA rules based on presence of a file on the endpoint, and whether the user is logged in to an Active Directory (AD) domain.

This section includes the following procedures:

1. In FortiClient EMS, configure a tagging rule for detecting a file on FortiClient endpoints running a Windows operating system. See Configuring a rule for detecting a file on page 16.
2. In FortiClient EMS, configure a tagging rule for detecting when a user logs in to a specific AD. See Configuring a rule for detecting AD login on page 17.
3. In FortiClient EMS, enable Zero Trust tags to display in FortiClient. See Configuring Zero Trust tags to display in FortiClient on page 17.
4. In FortiClient, FortiClient EMS, and FortiOS, verify Zero Trust tags. See Verifying tags on page 17.

Configuring a rule for detecting a file

In FortiClient EMS, you can configure a tagging rule that looks for a file on FortiClient endpoints running a Windows operating system.

To configure a rule for detecting a file:

1. In FortiClient EMS, and go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. On the top right, click *+Add* to create a Zero Trust tagging rule.
3. In the *Name* box, type a name, such as *Malicious-File-Detected*.
4. Beside *Tag Endpoint As*, type *Malicious-File-Detected*, and press *Enter* to create the tag.
5. Add a rule:
   a. Click *Add Rule*.
   b. Beside *OS*, select *Windows*.
   c. In the *Rule Type* list, select *File*.
   d. In the *File* box, type the filename with the path, for example, *C:\Downloads\virus.txt*.
   e. Click *Save* to save the rule.
6. Click *Save* to save the Zero Trust tagging rule.

This rule provides a method of looking for a specific file embedded in a Windows machine. You can use this method to look for a dormant virus file on a Windows machine when FortiEDR is not used. You can also use this method to look for an embedded corporate file that is buried in the file system.

Configuring a rule for detecting AD login

In FortiClient EMS, you can configure a tagging rule that detects when a user logs in to an Active Directory domain. The name of the tagging rule is *FortiAD.info*.

To configure a rule for detecting AD login:

1. In FortiClient EMS, and go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. Click *+Add* to create a Zero Trust tagging rule.
3. In the *Name* box, type a name, such as *FortiAD.Info*.
4. Beside *For Tag Endpoint As*, type *FortiAD.Info*, and press Enter to create the tag.
5. Add a rule:
   a. Click *Add Rule*.
   b. Beside *OS*, select *Windows*.
   c. In the *Rule Type* list, select *Logged In Domain*.
   d. In the *Domain* box, type *FortiAD.Info*, and press +.
   e. Click *Save* to save the rule.
6. Click *Save* to save the Zero Trust tagging rule.

Configuring Zero Trust tags to display in FortiClient

To configure the Zero Trust tags to display in FortiClient:

1. In FortiClient EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the Default profile.
3. In the top-right of the window, select *Advanced*.
4. On the *System Settings* tab, under *UI*, enable *Show Zero Trust Tag on FortiClient GUI*.
5. Click *Save*.

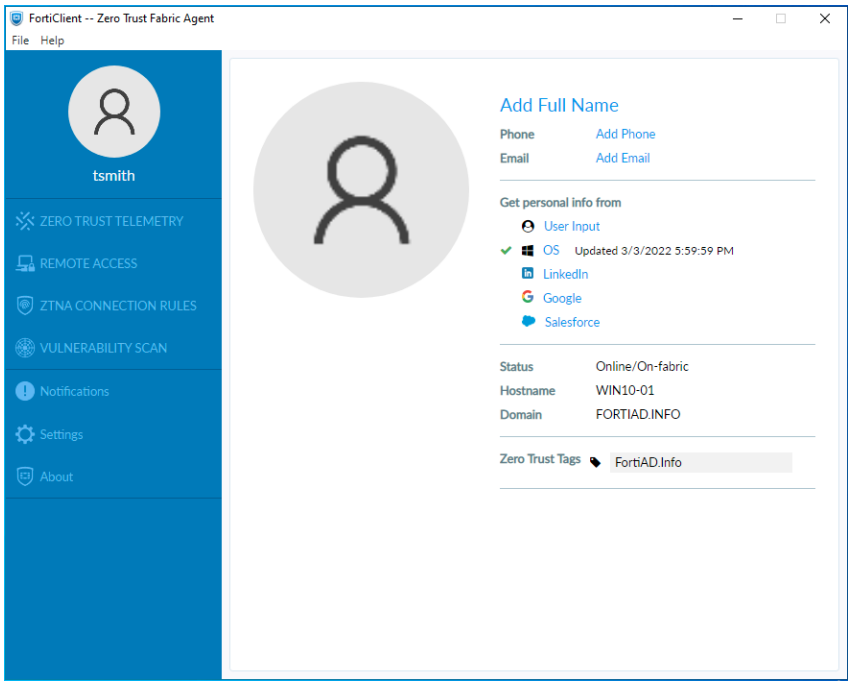
Verifying tags

This section describes how to verify tags in FortiClient, FortiClient EMS, and FortiOS.

To verify tags in FortiClient:

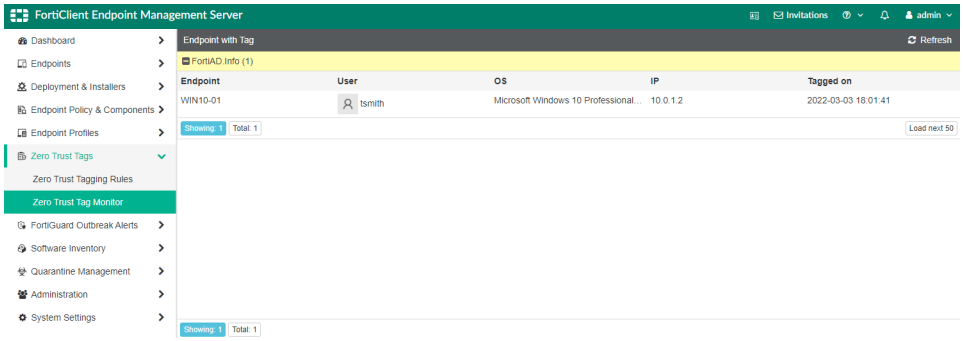
1. On a local or remote computer with FortiClient installed, register FortiClient to FortiClient EMS.
   In this example, FortiClient registers to FortiClient EMS at *ems.ztnademo.com*.

2. Once registered, click the user avatar to view currently detected Zero Trust tags.



To verify tags in FortiClient EMS:

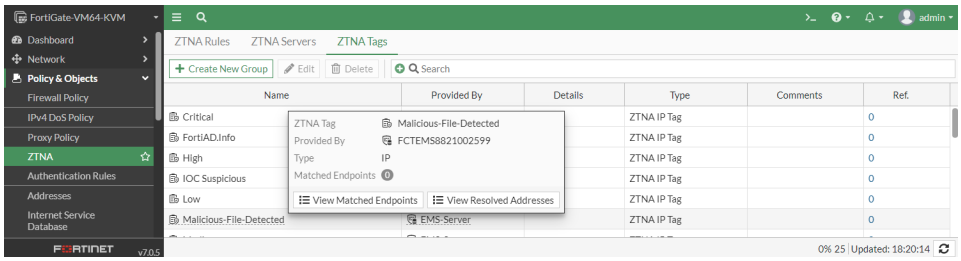
1. On FortiClient EMS, navigate to *Zero Trust Tags* > *Zero Trust Tag Monitor*.
2. Click *Refresh* to display endpoints that have been tagged by the tagging rule.



To verify tags in FortiOS:

1. On FortiOS, go to *System* > *Feature Visibility*, and enable *Zero Trust Network Access*.
2. Go to *Policy & Objects* > *ZTNA*, and click the *ZTNA Tags* tab.
   ZTNA tags created in FortiClient EMS are displayed.

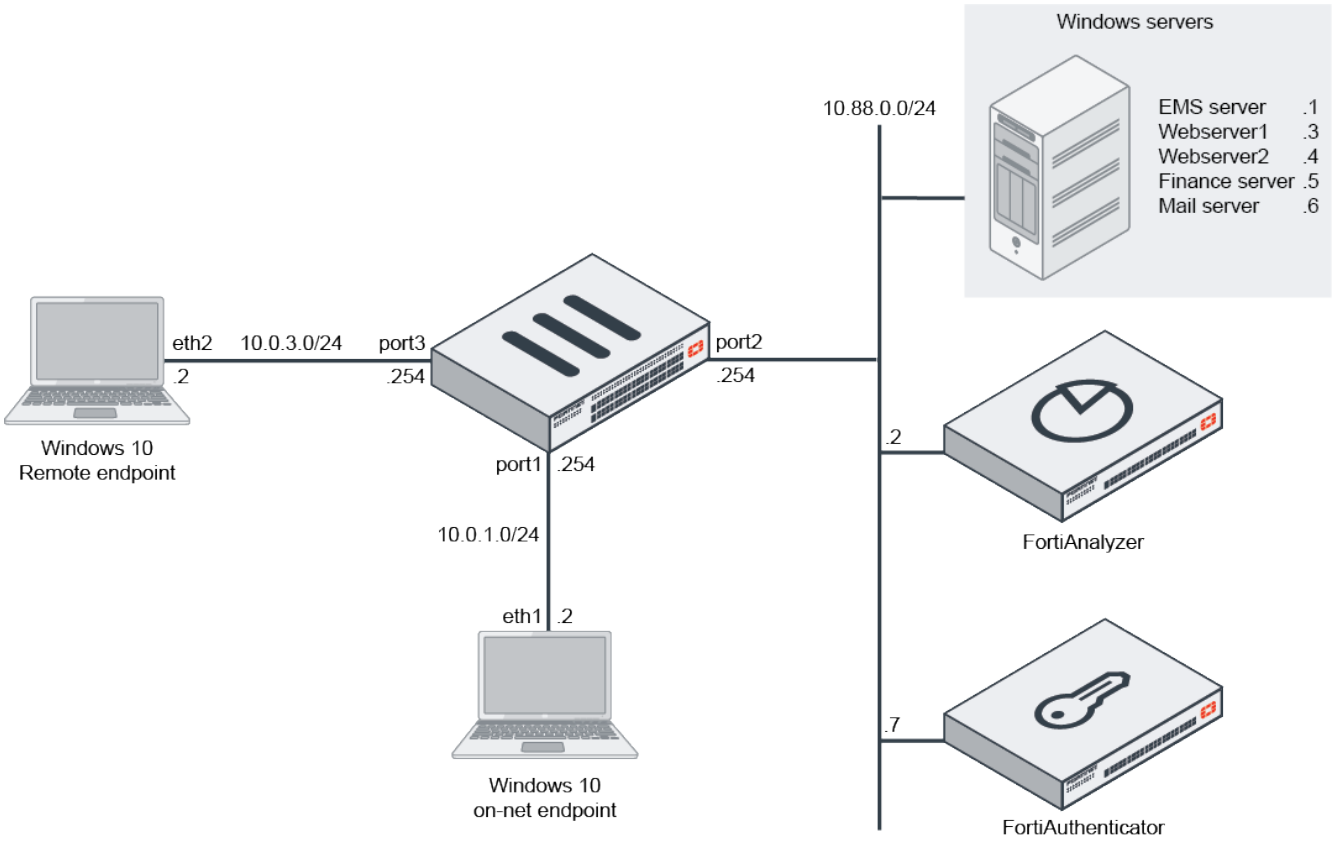
3. Hover over the *Malicious-File-Detected* tag to see the number of matched endpoints.



4. Click *View Matched Endpoints* or *View Resolved Addresses* for more information.

Configuring ZTNA HTTPS access proxy to web servers

In this section, use FortiOS to configure a ZTNA server on FortiGate that maps to multiple web servers by using HTTPS access proxy. Although optional, load balancing is enabled.



In our topology:

- We will dedicate IP address 10.0.3.10 and port 9443 for the external access-proxy VIP address.
- We have pre-configured a DNS record that maps the FQDN address *webserver.ztnademo.com* to *10.0.3.10*, which allows external access to the web server.
- Webserver1 and Webserver2 are running a simple web page.
- Traffic will be load-balanced between the web servers.

To configure ZTNA HTTP access proxy:

1. In FortiOS, go to *Policy & Objects* > *ZTNA*, and click the *ZTNA Servers* tab.
2. Click *Create New* to create a new server.
3. In the *Name* box, type *ZTNA-webserver*.
4. Define the network settings:
   a. Under *Network*, select *port3* in *External interface*.
   b. In the *External IP* box, type *10.0.3.10*.
   c. In the *External Port* box, type *9443*.
5. Under *Services and Servers*, select from the *Default certificate* list a certificate to present to clients when they connect to the access proxy VIP.
   We will use a wildcard certificate that is signed for **.ztnademo.com*.
6. Define a new service, and optionally enable load balancing:
   a. Under *Services/server mapping*, click *Create New*.
   b. Beside *Service*, select *HTTPS*.
   c. Beside *Virtual Host*, select *Any Host*.
   d. Beside *Path*, leave the default */*.

   When you specify a path, for example */fortigate*, you can match a URL, such as *webserver.ztnademo.com/fortigate*.

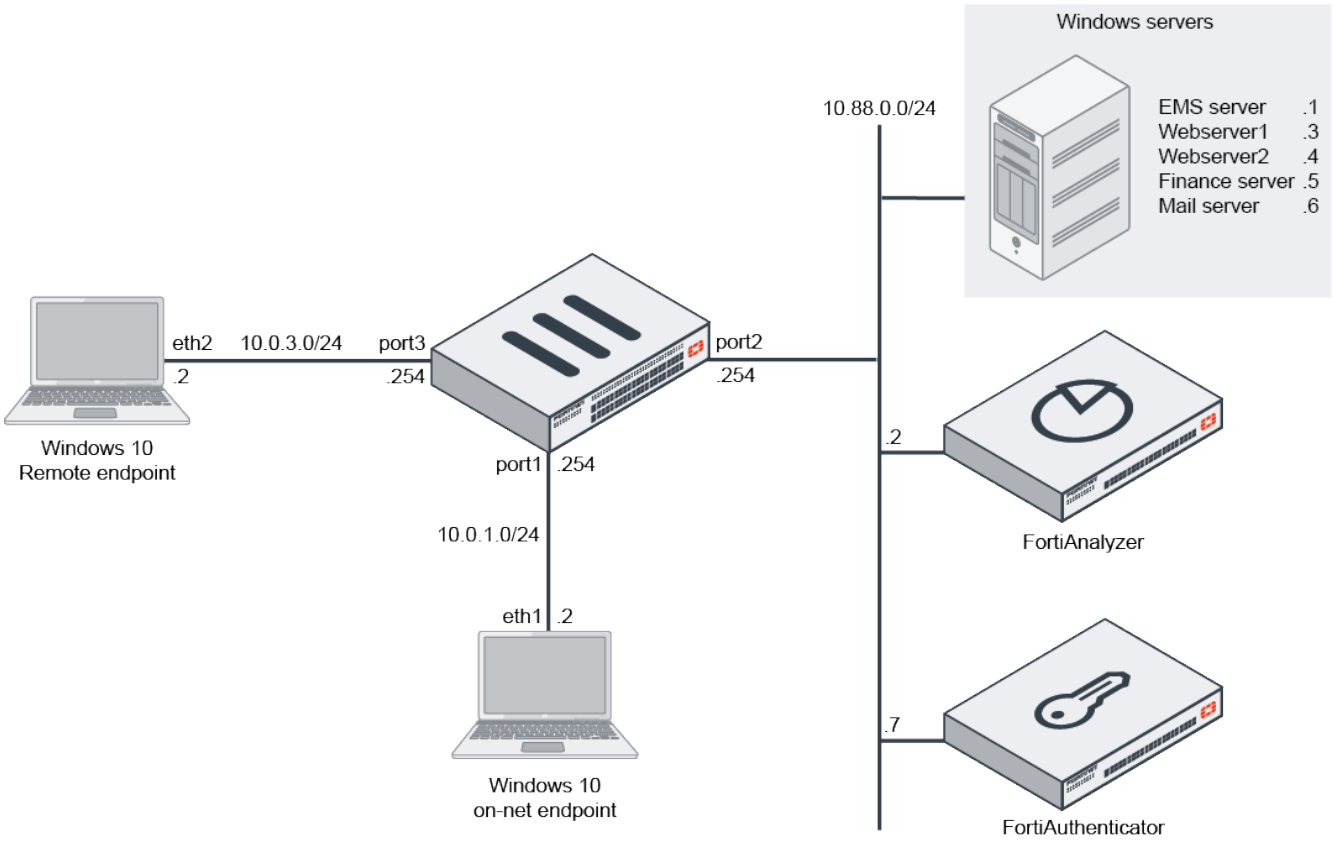
   e. (Optional) Under *Servers*, enable *Load balancing*, and choose a load-balancing method.

   Load balancing is optional. You can leave load balancing disabled if desired.
7. Define a server mapping for *Webserver1*.
   a. Click *Create New* to create a new server mapping.
   b. In the *IP* box, type *10.88.0.3*.
   c. In the *Port* box, type *9443*.
   d. Beside *Status* select *Active*.
   e. Click *OK* to finish adding the server mapping.
8. Define a server mapping for *Webserver2*.
   a. Click *Create New* to create another new server mapping.
   b. In the *IP* box, type *10.88.0.3*.
   c. In the *Port* box, type *9443*.
   d. Beside *Status*, select *Active*.
   e. Click *OK* to finish adding the server mapping.
9. Click *OK* to save the new service and server mappings.
10. Click *OK* to save and complete the ZTNA server setup.

Configuring ZTNA TCP forwarding access proxy

In this section, use FortiOS to configure TCP forwarding access proxy on FortiGate to map to the RDP service on Windows server (where FortiClient EMS is installed) and the SSH service on FortiAnalyzer.



In our topology, we will:

- Dedicate IP address 10.0.3.11 and port 9443 for the external Access Proxy VIP address.
- Map to the RDP service on the Windows server/FortiClient EMS on 10.88.0.1.
- Map to the SSH service on FortiAnalyzer on 10.88.0.2.

You cannot use ZTNA connection rules and TCP forwarding on a Windows 7 endpoint.

To configure ZTNA TCP forwarding access proxy:

1. In FortiOS, go to *Policy & Objects* > *ZTNA*, and click the *ZTNA Servers* tab.
2. Click *Create New* to create a new server.
3. In the *Name* box, type *ZTNA-tcp-server*.
4. Define the network settings:
   a. Under *Network*, select *port3* in *External interface*.
   b. In the *External IP* box, type *10.0.3.11*.

   c. In the *External Port* box, type *9443*.
5. Under *Services and Servers*, select from the *Default certificate* list the wildcard certificate that is signed for **.ztnademo.com*.
6. Define a new service:
   a. Under *Service/server mapping*, click *Create New*.
   b. Beside *Service*, select *TCP Forwarding*.
7. Define the server mapping for the Windows server with FortiClient EMS:
   a. Under *Servers*, click *Create New*.
   b. In the *Address* list, click *Create* to create a new address object for FortiClient EMS, and select it.
   c. In the *Ports* box, type in *3389*. If you leave this box blank, it denotes all ports.
   d. Click *OK* to save the new server.
8. Define the server mapping for FortiAnalyzer:
   a. Under *Servers*, click *Create New*.
   b. In the *Address* list, click *Create* to create a new address object for FortiAnalyzer, and select it.
   c. In the *Ports* box, type in *22*.
   d. Enable *Enable Additional SSH Options* to allow additional host checking, client verification, and traffic scanning. See ZTNA SSH access proxy example.
   e. Click *OK* to save the new server.
9. Click *OK* again to save the new service and server mapping.
10. Click *OK* to save the new ZTNA server.

In environments where no additional, external IP addresses are available, you can choose to create a new ZTNA server by using the same IP address as the HTTPS access proxy, but use a different port. Alternatively, you can configure the TCP forwarding server mappings on the same ZTNA server definition as the HTTPS access proxy.

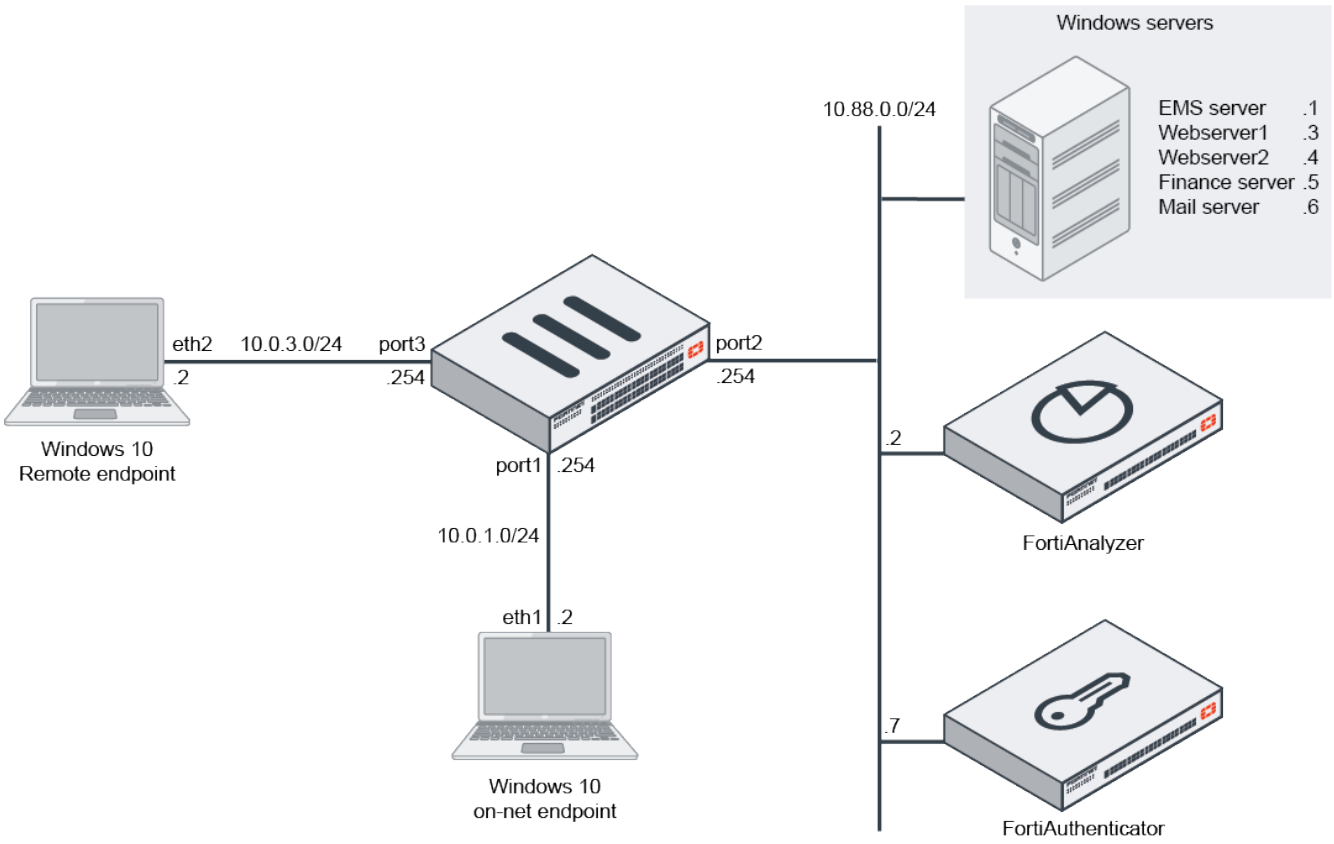
Configuring the authentication scheme and rule

In FortiOS configure the authentication scheme and rule for user authentication.

User authentication helps define users and groups for role based access control. There are many authentication methods that can be used, such as RADIUS, LDAP, Active Directory or SAML authentication. You can also centralize your solution with a FortiAuthenticator and deliver multi-factor authentication (MFA) using FortiTokens. See ZTNA access proxy with SAML and MFA using FortiAuthenticator example.

An authentication scheme and rule must be configured to trigger user authentication. The authentication scheme defines what method of authentication will be applied. It is similar to how authentication is performed for Explicit Proxy. An authentication rule specifies which proxy sources and destinations will require authentication, and which authentication scheme to apply.

When defining user authentication for ZTNA, we must configure an authentication scheme and an authentication policy before applying the user group to a ZTNA rule. This step demonstrates basic authentication using an LDAP server that connects to the Active Directory on our Windows server/FortiClient EMS.



In our topology:

- The FortiGate uses LDAP to connect to Active Directory on the Windows server/FortiClient EMS on 10.88.0.1.
- In our scenario, an LDAP server named *LDAP-fortiad* is presumed to be configured previously for an SSL VPN teleworking solution.
- Furthermore, a user group named *LDAP-Remote-Allowed-Group* is also pre-configured for SSL VPN authentication.
- The user group named *LDAP-Remote-Allowed-Group* maps to a user group named *Remote-Allowed* on the Active Directory named *Fortiad.Info*.
- These settings are reused in this ZTNA solution, allowing users in the *LDAP-Remote-Allowed-Group* access to authenticate to the ZTNA access proxy.

This section includes the following procedures:

1. In FortiOS, configure an authentication scheme. See Configuring an authentication scheme on page 23.
2. In FortiOS, configure an authentication rule, and select the authentication scheme. See Configuring an authentication rule on page 24.

Configuring an authentication scheme

To configure an authentication scheme:

1. In FortiOS, go to *Policy & Objects* > *Authentication Rules*, and select *Authentication Schemes* from the top-right.
2. Click *Create New* > *Authentication Scheme*.
3. In the *Name* box, type the name *ZTNA-Auth-scheme*.

4. From the *Method* list, select *Method Basic*.
5. Beside *User database*, select *Other*, and then select the LDAP server named *LDAP-fortiad*.
6. Click *OK* to complete.

Configuring an authentication rule

Configure an authentication rule, and select the authentication scheme that you just created.

To configure an authentication rule from GUI:

1. On the to *Policy & Objects* > *Authentication Rules* pane, click *Create New* > *Authentication Rule*.
2. In the *Name* box, type *ZTNA-Auth-rule*.
3. In the *Source Address* list, select *all*.
4. In the *Incoming interface* list, select *WAN (port3)*.
5. Leave *Protocol* set to *HTTP*.
6. Enable *Authentication Scheme*, and select *ZTNA-Auth-scheme*.
7. Beside *IP-based Authentication*, select *Enable*.
8. Beside *Enable This Rule*, select *Enable*.
9. Click *OK* to complete.

Configuring ZTNA rules to control access

Once ZTNA tags, servers, authentication scheme, and authentication rules are configured, you can create ZTNA rules to control access.

ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security profiles to scan the traffic.

In this step, use FortiOS to create a rule that denies access to endpoints with compromised security. Compromised security is identified by the presence of the *Malicious-File-Detected* tag. We will also create a rule to allow access to users who are logged in to the *FortiAD.Info* domain, which is identified by the presence of the *FortiAD.Info* tag.

This section includes the following procedures:

1. In FortiOS, configure a ZTNA rule for denying access. See Configuring a ZTNA rule for denying access on page 24.
2. In FortiOS, configure a ZTNA rule for allowing access. See Configuring a ZTNA rule for allowing access on page 25.

Configuring a ZTNA rule for denying access

To configure a ZTNA rule for denying access:

1. In FortiOS, go to *Policy & Objects* > *ZTNA*, click the *ZTNA Rules* tab.
2. Click *Create New* to create a new rule.
3. In the *Name* box, type *ZTNA-Deny-Malicious*.
4. In the *Incoming Interface* list, select *WAN (port3)*.

5. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Remote-Allowed-Group*.

When you define a user group, users would need to be authenticated first before their ZTNA tag is checked. The advantage is the username will be recorded in the violation log.

6. In the *ZTNA Tag* list, select the *Malicious-File-Detected* tag.
7. In the *ZTNA Server* list, select *ZTNA-webserver* and *ZTNA-tcp-server*.
8. In the *Destination* list, select *all*.
9. Beside Action, select *Deny*.
10. Enable *Log Violation Traffic*.
11. Enable *Enable this policy*.
12. Click *OK* to complete.

Configuring a ZTNA rule for allowing access

To configure a ZTNA rule for allowing access:

1. Go to *Policy & Objects* > *ZTNA* and click the *ZTNA Rules* tab.
2. Click *Create New*.
3. In the *Name* box, type *ZTNA-Allow-Access*.
4. In the *Incoming Interface* list, select *WAN (port3)*.
5. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Remote-Allowed-Group*.
6. In the *ZTNA Tag* list, select the *FortiAD.Info* tag.
7. In the *ZTNA Server* list, select *ZTNA-webserver* and *ZTNA-tcp-server*.
8. In the *Destination* list, select *all*.
9. Beside *Action*, select *Accept*.
10. Enable *Security Profiles* as desired.
11. In the *Logging Options* section, enable *Log Allowed Traffic*, and select *All Sessions*.
12. Enable *Enable this policy*.
13. Click *OK* to complete.

Configuring ZTNA connection rules

In this step, use FortiClient EMS to configure ZTNA connection rules for any traffic through TCP forwarding access proxy.

With ZTNA TCP forwarding, FortiClient endpoints forward traffic destined for a server or service to the FortiGate access proxy. Therefore, the FortiClient endpoint needs to configure ZTNA connection rules to identify the destination server and services. The best way to centrally manage these is through FortiClient EMS.

In addition to this topic, you can also find more information in the following topics on the Fortinet Docs Library:

- FortiClient EMS: Configuring encrypted ZTNA rules
- FortiClient: Using ZTNA Connection rules for TCP forwarding access proxy
- FortiOS: ZTNA TCP forwarding access proxy with FQDN example

In this section, we will configure the XML rules on FortiClient EMS that will create ZTNA connection rules for connecting to FortiClient EMS through RDP and FortiAnalyzer through SSH. We will verify that these rules are pushed to the FortiClient endpoint.

This section includes the following procedures:

1. On FortiClient EMS, configure ZTNA connection rules. See Configuring ZTNA connection rules for RDP and SSH on page 26.
2. On FortiClient endpoints, verify connection rules have been received. See Verifying receipt of connection rules on page 27.

Configuring ZTNA connection rules for RDP and SSH

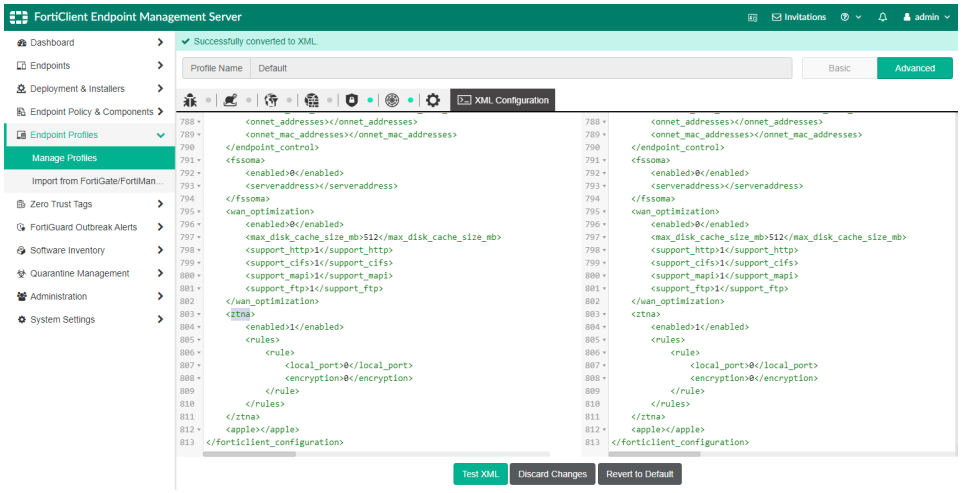
Use FortiClient EMS to configure ZTNA connection rules for RDP and SSH, and push the rules to FortiClient endpoints.

To configure ZTNA connection rules:

1. On FortiClient EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the *Default* profile, and click *Edit*.
3. In the Default profile, click *Advanced* in the top-right to enable advanced settings.
4. Click the *XML Configuration* tab.

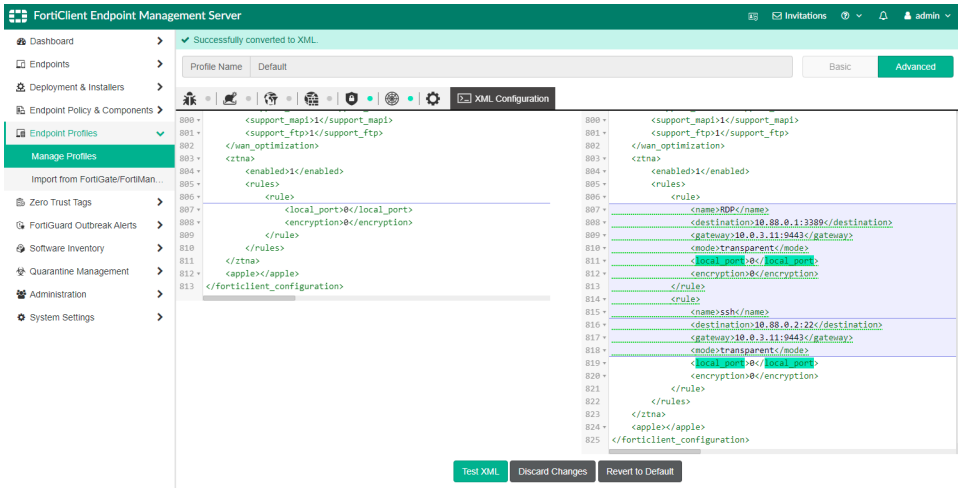
The *XML Configuration* tab is hidden until you click *Advanced* in the top-right of the pane.

5. In the bottom middle of the screen, click *Edit*, then scroll down to the ZTNA section.
You can search using your browser's search function. Look for the section shown in the following image:



The left side pane is the existing configuration, and the right side is where you will edit the XML.

6. Create rules in the rules element:
   You can create a new rule by clicking to the right of the existing *<rule>* sample element, and pressing *Enter* on your keyboard to create a new line.
   a. Create a rule for RDP to FortiClient EMS by entering the following XML elements:
   ```
   <rule>
      <name>RDP</name>
      <destination>10.88.0.1:3389</destination>
      <gateway>10.0.3.11:9443</gateway>
      <mode>transparent</mode>
      <local_port>0</local_port>
      <encryption>0</encryption>
   </rule>
   ```
   Note that encryption is disabled because RDP is already a secure protocol. Therefore, it does not require the additional overhead to encrypt the connection between FortiClient and the FortiGate access proxy.
   b. Create another rule for SSH to FortiAnalyzer by entering the following XML elements under the first rule:
   ```
   <rule>
      <name>ssh</name>
      <destination>10.88.0.2:22</destination>
      <gateway>10.0.3.11:9443</gateway>
      <mode>transparent</mode>
      <local_port>0</local_port>
      <encryption>0</encryption>
   </rule>
   ```
   Encryption is disabled for the same reason as the rule for RDP to FortiClient EMS.
   The completed ZTNA configuration should look like this.



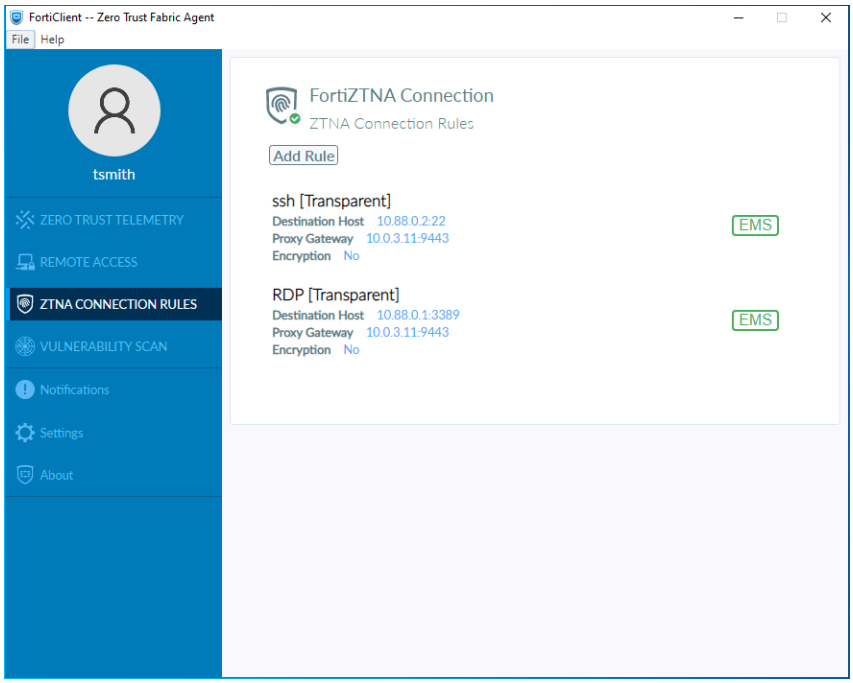
   c. At the bottom of the pane, click *Test XML* to verify XML formatting, and look for a message at the top of the screen stating XML is valid.
   d. Click *Save* to save the ZTNA connection rules.

Verifying receipt of connection rules

Shortly after completing the connection rules on FortiClient EMS, registered FortiClient endpoints will receive a notification for a *Configuration Update* from the Endpoint Management Server (EMS).

To verify receipt of connection rules:

1. In FortiClient, go to *ZTNA Connection Rules*.
   Two rules from FortiClient EMS are displayed. Tags indicate *EMS* rules.



Verifying ZTNA connectivity

Now that FortiClient EMS and FortiGate ZTNA are configured, you can verify connectivity by completing the following steps:

1. On a remote computer, verify access to web servers. See Verifying access to web servers on page 28.
2. In FortiOS, verify user connectivity. See Verifying user connectivity from FortiGate on page 31.
3. On a remote computer, verify RDP access to FortiClient EMS. See Verifying RDP access to FortiClient EMS on page 34.
4. On a remote computer, verify SSH access to FortiAnalyzer. See Verifying SSH access to FortiAnalyzer on page 35.
5. On a remote computer, verify denied access due to failed posture check. See Verifying denied access due to failed posture check on page 36.

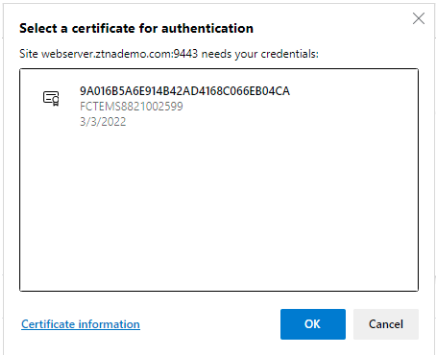
Verifying access to web servers

To verify access to web servers:

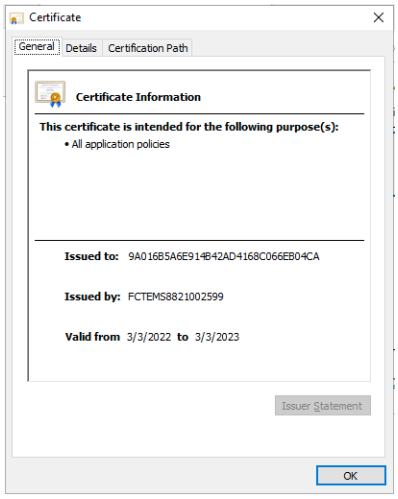
1. On a remote computer, open FortiClient, and go to *Zero Trust Telemetry*.
2. Connect to FortiClient EMS by entering the FQDN address of FortiClient EMS.
   In this example, we are using *ems.ztnademo.com*.

Once connected to FortiClient EMS, wait for FortiClient to retrieve updates from FortiClient EMS and update its configuration.

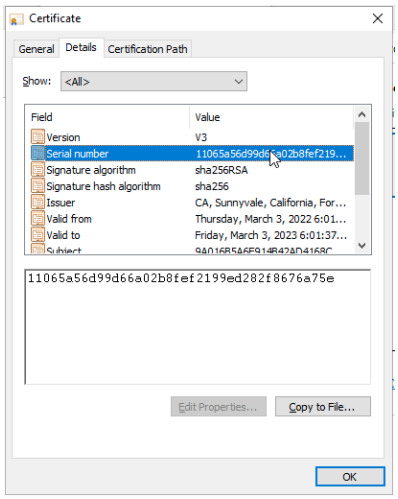
3. Optionally, log in to FortiClient EMS and go to *Endpoints* > *All Endpoints* to verify the remote host has registered, connected and synchronized.
4. On the remote computer, open a browser, and enter the FQDN address and port defined for the web server's ZTNA access proxy.
   In this example, we are using *https://webserver.ztnademo.com:9443*.
   The first time that you connect, the ZTNA access proxy will request client certificate verification.



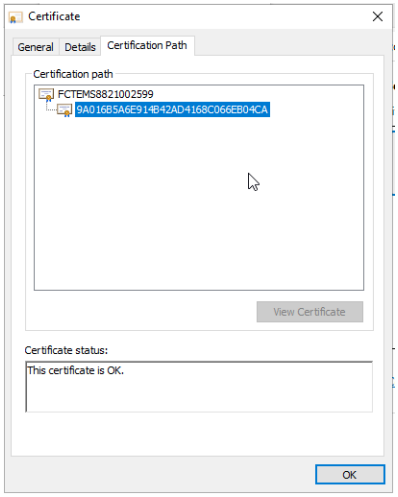
5. Select the certificate issued by FortiClient EMS, and click *Certificate information* to view this client certificate.
   On the *General* tab, the *Issued to* field shows the FortiClient ID:



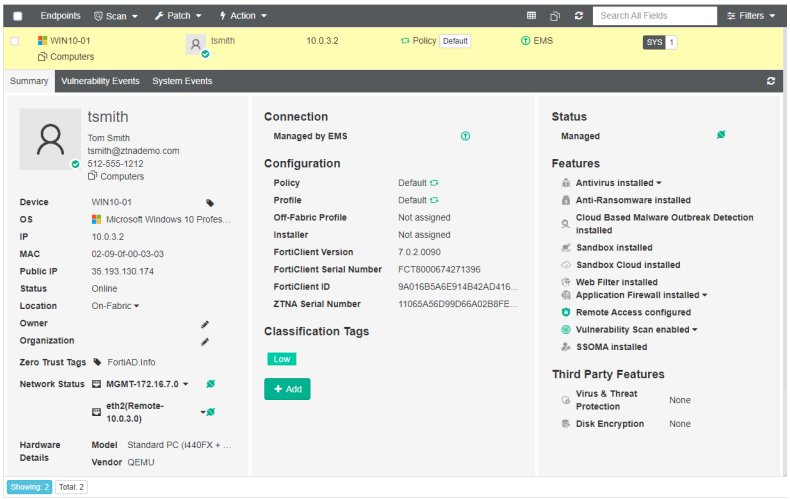
   On the *Details* tab, the *Serial Number* of the certificate should match the serial number in FortiClient EMS, and the information is synchronized to FortiGate:



Following is an example of the *Certification Path* tab:

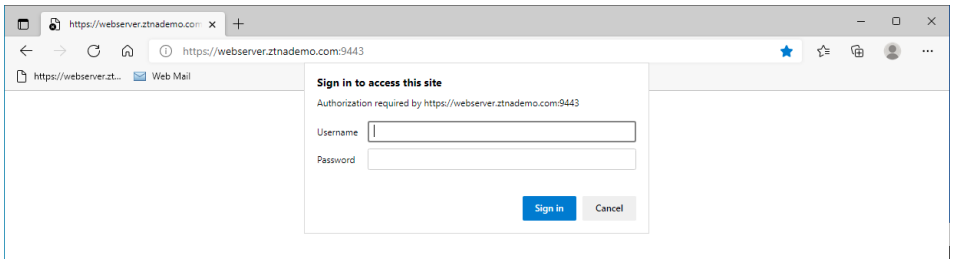


Following is the information on FortiClient EMS that is synchronized to FortiGate.



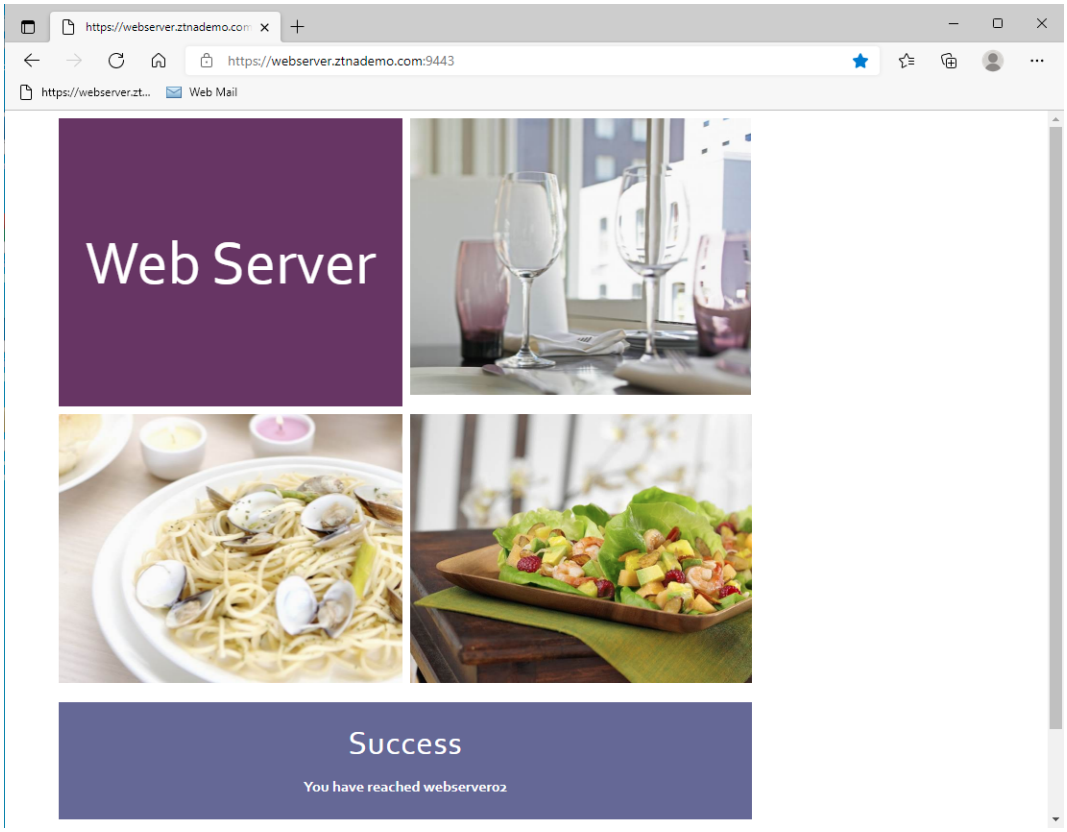
6. On the browser, select the certificate, and click *OK* to complete the client certificate verification. The browser prompts you to sign in.

7. Enter your Active Directory credentials to log in.



Once user authentication is successful, FortiGate checks the security posture of the endpoint. If the endpoint has the necessary ZTNA tags to pass this check, the user will be able to access the website.

Since we configured server load-balancing with round-robin, refresh the web page to open a connection to the second web server.



Verifying user connectivity from FortiGate

From the FortiGate, there are various debugs and logs that help you troubleshoot and verify user connectivity.

To verify user connectivity from FortiGate:

1. View the endpoint's information by using the following debug command:

```
# diagnose endpoint record list
Record #1:
   IP Address = 10.0.3.2
   MAC Address = 02:09:0f:00:03:03
```

```
   MAC list = 02:09:0f:00:04:03;02:09:0f:00:03:03;
   VDOM = (-1)
   EMS serial number: FCTEMS8821002599
   Client cert SN: 11065A56D99D66A02B8FEF2199ED282F8676A75E
   Public IP address: 35.193.130.174
   Quarantined: no
   Online status: online
   Registration status: registered
   On-net status: on-net
   Gateway Interface:
   FortiClient version: 7.0.2
   AVDB version: 1.0
   FortiClient app signature version: 20.269
   FortiClient vulnerability scan engine version: 2.31
   FortiClient UID: 9A016B5A6E914B42AD4168C066EB04CA
   Host Name: WIN10-01
   OS Type: WIN64
   OS Version: Microsoft Windows 10 Professional Edition, 64-bit (build 19042) (version
        2009)
   Host Description:
   Domain: fortiad.info
   Last Login User: tsmith
   Owner:
   Host Model: Standard PC (i440FX + PIIX, 1996)
   Host Manufacturer: QEMU
   CPU Model: Intel(R) Xeon(R) CPU @ 2.30GHz
   Memory Size: 8192
   AV Feature: 1
   FW Feature: 1
   WF Feature: 1
   AS Feature: 0
   VS Feature: 1
   VN Feature: 1
   Last vul message received time: N/A
   Last vul scanned time: N/A
   Last vul statistic: critical=0, high=0, medium=0, low=0, info=0
   Avatar fingerprint: 05b9940c015425a375caafa28096d695be6e9ad2
   Avatar source username: Tom Smith
   Avatar source email: tsmith@ztnademo.com
   Avatar source: OS
   Phone number: 512-555-1212
   Number of Routes: (0)
online records: 1; offline records: 0; quarantined records: 0
```

From the above record, we can confirm FortiGate has the information for the endpoint with the same FortiClient UID and Certificate Serial Number.

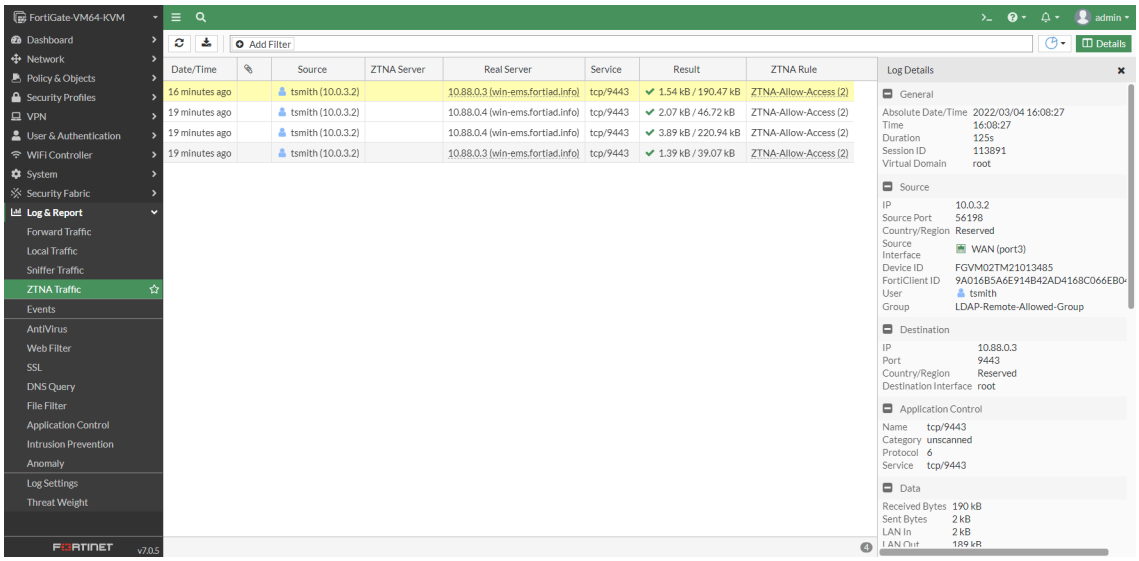
2. View the information cached by the FortiGate's wad daemon when a remote computer connects to the ZTNA access proxy by using the following debug command:

```
# diagnose test application fcnacd 7
ZTNA Cache V2:
Entry #1:
   - UID: 9A016B5A6E914B42AD4168C066EB04CA
   - EMS SN: FCTEMS8821002599
   - Domain: fortiad.info
   - User: tsmith
   - Owner:
   - Certificate SN: 11065A56D99D66A02B8FEF2199ED282F8676A75E
```

```
   - online: true
   - Tags (3):
   -- Tag (#0): Low
   -- Tag (#1): all_registered_clients
   -- Tag (#2): FortiAD.Info
lls_idx_mask = 0x00000001,
```

These debugs show essential info about the remote endpoint that allows FortiGate to perform access control. In the above debugs, the remote client has the *FortiAD.Info* ZTNA tag to match the ZTNA allow policy.

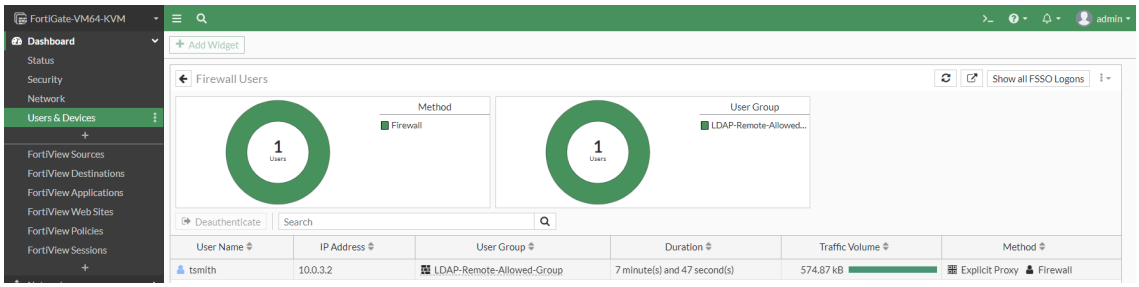
3. View ZTNA logs in the GUI by going to *Log & Report* > *ZTNA traffic*.



Alternately, you can view these logs from the CLI by using the following commands:

```
# execute log filter category 0
# execute log filter field subtype ztna
# execute log display
1: date=2022-03-04 time=16:08:27 eventtime=1646438907754697037 tz="-0800"
      logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
      srcip=10.0.3.2 srcport=56198 srcintf="port3" srcintfrole="wan"
      dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.3 dstport=9443
      dstintf="root" dstintfrole="undefined" sessionid=113891 service="tcp/9443" proto=6
      action="accept" policyid=2 policytype="proxy-policy" poluuid="b64e29d6-9b94-51ec-
      dcf2-a960b7f68517" policyname="ZTNA-Allow-Access" duration=125 user="tsmith"
      group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" gatewayid=1 vip="ZTNA-
      webserver" accessproxy="ZTNA-webserver"
      clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="MAC_
      FCTEMS8821002599_FortiAD.Info/FCTEMS8821002599_all_registered_clients/MAC_
      FCTEMS8821002599_all_registered_clients" wanin=190472 rcvdbyte=190472 wanout=1304
      lanin=1545 sentbyte=1545 lanout=189089 fctuid="9A016B5A6E914B42AD4168C066EB04CA"
      appcat="unscanned"
```

4. View the authenticated user in the GUI by going to *Dashboard* > *User & Devices*, and opening the *Firewall Users* widget.



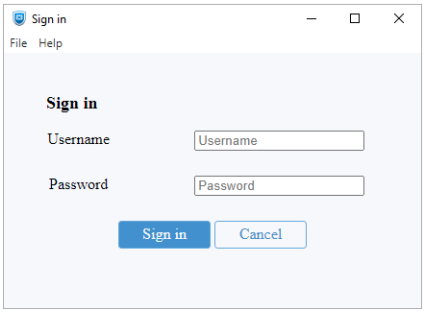
Alternately, use either of the following debugs commands:

```
# diagnose wad user list
ID: 2, VDOM: root, IPv4: 10.0.3.2
      user name : tsmith
      worker : 0
      duration : 372
      auth_type : IP
      auth_method : Basic
      pol_id : 2
      g_id : 3
      user_based : 0
      expire : no
      LAN:
      bytes_in=79557 bytes_out=463555
      WAN:
      bytes_in=432893 bytes_out=64777
# diagnose firewall auth list
10.0.3.2, tsmith
   type: fw, id: 0, duration: 549, idled: 39
   expire: 561, allow-idle: 600
   packets: in 81 out 90, bytes: in 53406 out 29933
   group_id: 3
   group_name: LDAP-Remote-Allowed-Group
----- 1 listed, 0 filtered ------
```

Verifying RDP access to FortiClient EMS

To verify RDP access to FortiClient EMS:

1. On a remote computer, open FortiClient, and go to *ZTNA Connection Rules*.
2. Under *RDP*, copy the IP address and port in the *Destination Host* field, for example, *10.88.0.1:3389*.
3. Open a new Remote Desktop connection, and paste the address and port of the remote server.
   If this is the first time connecting, FortiClient prompts you to log in to the access proxy.



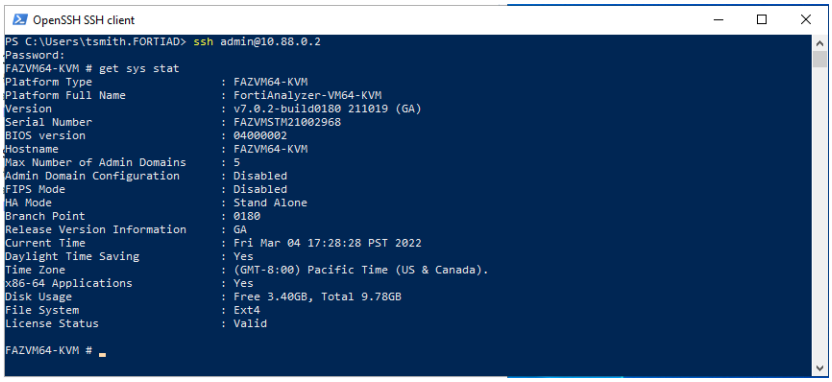
4. Enter the Active Directory user credentials, and click *Sign In*.
   Upon a successful authentication, FortiGate will verify your security posture. If that is also successful, the RDP session will start. You will be prompted for the RDP credentials.
5. Once RDP authentication is successful, you can access your remote computer.
6. From the FortiGate, review the ZTNA traffic logs to see the user's RDP session.

```
# execute log display
1: date=2022-03-04 time=17:10:37 eventtime=1646442637669726761 tz="-0800"
      logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
      srcip=10.0.3.2 srcport=56301 srcintf="port3" srcintfrole="wan"
      dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.1 dstport=3389
      dstintf="root" dstintfrole="undefined" sessionid=120190 service="RDP" proto=6
      action="accept" policyid=2 policytype="proxy-policy" poluuid="b64e29d6-9b94-51ec-
      dcf2-a960b7f68517" policyname="ZTNA-Allow-Access" duration=16 user="tsmith"
      group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" gatewayid=1 vip="ZTNA-
      tcp-server" accessproxy="ZTNA-tcp-server"
      clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="MAC_
      FCTEMS8821002599_FortiAD.Info/FCTEMS8821002599_all_registered_clients/MAC_
      FCTEMS8821002599_all_registered_clients" wanin=1588 rcvdbyte=1588 wanout=1040
      lanin=2854 sentbyte=2854 lanout=5105 fctuid="9A016B5A6E914B42AD4168C066EB04CA"
      appcat="unscanned"
```

Verifying SSH access to FortiAnalyzer

To verify RDP access to FortiClient EMS:

1. On a remote computer, open FortiClient, and go to *ZTNA Connection Rules*.
2. Under *ssh*, copy the IP address and port in the *Destination Host* field for FortiAnalyzer, for example, *10.88.0.2:22*.
3. From an SSH client, open a SSH session by typing *ssh admin@10.88.0.2*
   Since user authentication for ZTNA was previously successful, the FortiGate checks the security posture and allows the SSH session to continue.
4. Use your SSH session to log in to FortiAnalyzer and perform actions.



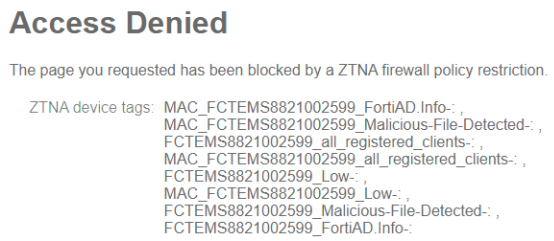
5. From the FortiGate, review the ZTNA traffic logs to see the user's SSH session.

```
#execute log display
2: date=2022-03-04 time=17:27:41 eventtime=1646443661553613902 tz="-0800"
      logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
      srcip=10.0.3.2 srcport=56329 srcintf="port3" srcintfrole="wan"
      dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.2 dstport=22
      dstintf="root" dstintfrole="undefined" sessionid=121810 service="SSH" proto=6
      action="accept" policyid=2 policytype="proxy-policy" poluuid="b64e29d6-9b94-51ec-
      dcf2-a960b7f68517" policyname="ZTNA-Allow-Access" duration=18 user="tsmith"
      group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" gatewayid=1 vip="ZTNA-
```

```
tcp-server" accessproxy="ZTNA-tcp-server"
clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="MAC_
FCTEMS8821002599_FortiAD.Info/FCTEMS8821002599_all_registered_clients/MAC_
FCTEMS8821002599_all_registered_clients" wanin=1837 rcvdbyte=1837 wanout=1761
lanin=3597 sentbyte=3597 lanout=5376 fctuid="9A016B5A6E914B42AD4168C066EB04CA"
appcat="unscanned"
```

Verifying denied access due to failed posture check

1. On a remote computer, trigger the *Malicious-File-Detected* ZTNA tag by placing a *virus.txt* file in the designated directory.
2. On the FortiClient, verify the presence of the Malicious-File-Detected tag.
3. Open the browser and browse to *https://webserver.ztnademo.com:9443*.
   Since the ZTNA tag matches the deny policy, the access will be blocked. The user will see a replacement message with Access Denied.



4. From the FortiGate, review the ZTNA traffic logs to see the denied traffic log.

```
# execute log display
1: date=2022-03-04 time=17:50:49 eventtime=1646445050030746165 tz="-0800"
     logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
     srcip=10.0.3.2 srcport=56368 srcintf="port3" srcintfrole="wan"
     dstcountry="Reserved" srccountry="Reserved" dstip=10.0.3.10 dstport=9443
     dstintf="root" dstintfrole="undefined" sessionid=123985 service="tcp/9443" proto=6
     action="deny" policyid=1 policytype="proxy-policy" poluuid="74fa4e06-9b94-51ec-
     7141-990cff1cfee0" policyname="ZTNA-Deny-Malicious" duration=1 user="tsmith"
     group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" gatewayid=1 vip="ZTNA-
     webserver" accessproxy="ZTNA-webserver"
     clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="MAC_
     FCTEMS8821002599_FortiAD.Info/MAC_FCTEMS8821002599_Malicious-File-
     Detected/FCTEMS8821002599_all_registered_clients" msg="Denied: proxy-policy action
     is deny" wanin=0 rcvdbyte=0 wanout=0 lanin=1545 sentbyte=1545 lanout=528
     fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned" crscore=30
     craction=131072 crlevel="high"
```

More information

The following product models and firmware were used in this guide:

Product	Model	Firmware
FortiGate	FortiGate-VM	FortiOS 7.0.4
FortiClient	FortiClient Windows	7.0.2
FortiClient EMS	FortiClient EMS	7.0.2

www.fortinet.com