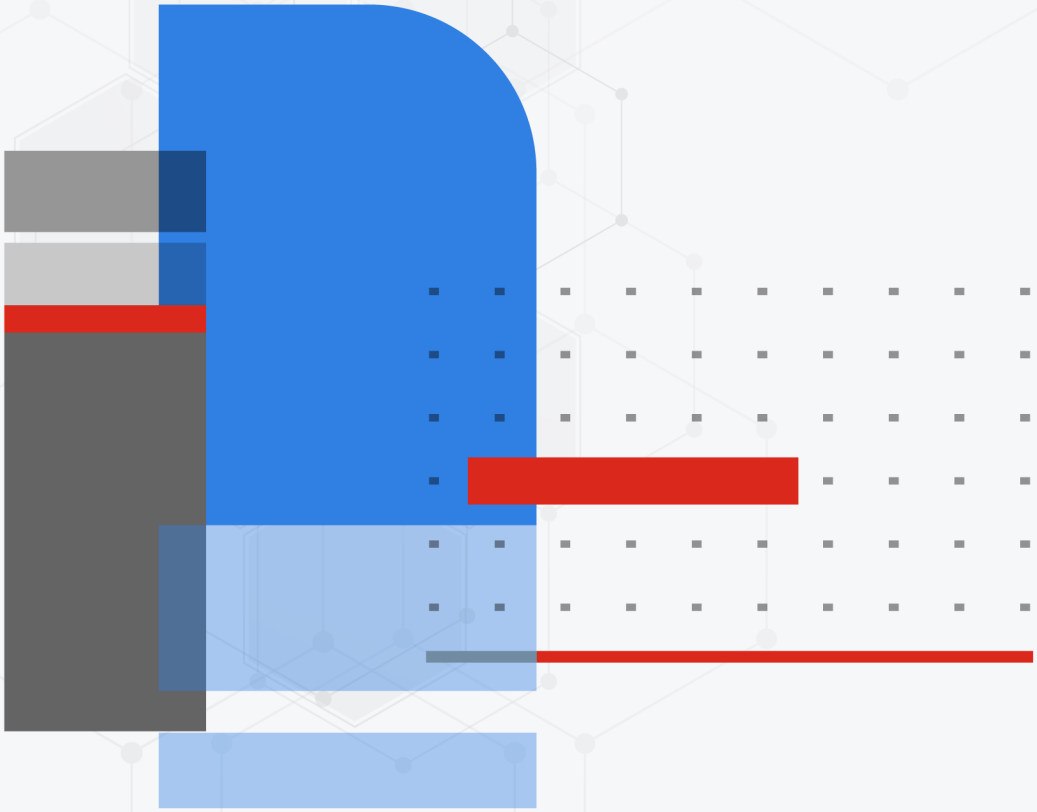
ZTNA Reference Guide

FortiProxy 7.4



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

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

November 1, 2024
FortiProxy 7.4 ZTNA Reference Guide
45-740-1094705-20241101

TABLE OF CONTENTS

Introduction

Zero trust network access (ZTNA) is an access control method that uses client device identification, authentication, and zero trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for on-net local users and off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using zero trust tags.

This document provides reference information for ZTNA.

Endpoint posture check

The following are different context-based posture checks that FortiClient EMS 7.2 supports as part of the Zero Trust solution:

Recommended posture checks

For vulnerable devices, checking for devices with high-risk vulnerabilities and above is recommended.

Rule type	Posture check	Supported operating systems
Vulnerable devices	Critical	Windows, macOS, Linux
	High or higher	
	Medium or higher	
	Low or higher	
Antivirus software	AV software is installed and running. For Windows, this feature supports third party AV applications. For macOS and Linux, this feature can only check if FortiClient AV protection is enabled and does not recognize third party AV applications.	
	AV signature is up-to-date	
Windows security	Windows Defender is enabled	Windows
	Bitlocker Disk Encryption is enabled	
	Exploit Guard is enabled	
	Application Guard is enabled	
	Windows Firewall is enabled	
	Automatic Updates are enabled	
Security	FileVault Disk Encryption is enabled	macOS
EMS management	FortiClient installed and Telemetry is connected to EMS	Windows, macOS, Linux, iOS, Android
Common vulnerabilities and exposures (CVE)	Presence of [CVE]	Windows, macOS, Linux
Firewall threat	Presence of [firewall threat ID]	Windows, macOS

Other posture checks

Rule type	Posture check	Supported operating systems
User in Active Directory (AD) group	Member of [AD Group]	Windows, macOS, Linux
Certificate	Certificate contains [Subject CN] and [Issuer CN]	
File	Presence of [File]	
IP range	Device in the [IP Range]	Windows, macOS, Linux, IOS, Android
Logged in domain	Member of [Domain]	Windows, macOS, Linux
On-Fabric status	On-Fabric	Windows, macOS, Linux, IOS, Android
OS version	Windows Server 2022	Windows
	Windows Server 2019	Windows
	Windows Server 2016	Windows
	Windows Server 2012 R2	Windows
	Windows Server 2012	Windows
	Windows Server 2008 R2	Windows
	Windows 11	Windows
	Windows 10	Windows
	Windows 8.1	Windows
	Windows 8	Windows
	Windows 7	Windows

Rule type	Posture check	Supported operating systems
OS version	Mojave	macOS
	High Sierra	macOS
	Sierra	macOS
	Catalina	macOS
	Big Sur	macOS
	Monterey	macOS
	Ventura	macOS
	Sonoma	macOS
OS version	CentOS Stream 9	Linux
	CentOS Stream 8	Linux
	CentOS 8	Linux
	CentOS 7.5	Linux
	CentOS 7.4	Linux
OS version	Red Hat 8.1	Linux
	Red Hat 8	Linux
	Red Hat 7.6	Linux
	Red Hat 7.5	Linux
	Red Hat 7.4	Linux
OS version	Ubuntu 22.04	Linux
	Ubuntu 21.10	Linux
	Ubuntu 21.04	Linux
	Ubuntu 20	Linux
	Ubuntu 18.04	Linux
	Ubuntu 16.04	Linux

Rule type	Posture check	Supported operating systems
OS version	Fedora 34	Linux
	Fedora 33	Linux
	Fedora 32	Linux
	Fedora 31	Linux
	Fedora Linux 37	Linux
	Fedora Linux 36	Linux
	Fedora Linux 35	Linux
OS version	iOS 9, 10, 11, 12, 13, 14, 15, 16	iOS
	Android 5, 6, 7, 8, 9, 10, 11, 12, 13	Android
Registry key	[Registry key]	Windows
Running process	Presence of [Running process]	Windows, macOS, Linux
Sandbox detection	Sandbox detected malware in last seven days	Windows, macOS
User identity	User-specified	Windows, macOS, Linux, iOS, Android
	Social network login	Windows, macOS, Linux, iOS, Android
	Verified user	Windows, macOS, Linux, iOS, Android
FortiEDR	FortiEDR is installed and running	Windows, macOS, Linux
FortiClient version	Presence of [Specified FortiClient version]	Windows, macOS, Linux, iOS, Android
Security status	Device fulfills configured security status, such as being jailbroken or having passcode or biometrics protection enabled.	iOS, Android

CASB SaaS application support

You can configure the FortiProxy zero trust network access (ZTNA) access proxy to act as an inline cloud access security broker (CASB) by providing access control to software-as-a-service (SaaS) traffic using ZTNA access control rules. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources. FortiProxy supports ZTNA inline CASB for SaaS application access. This topic provides information on the supported applications.

The inline CASB database, as of version 1.00031, supports the following SaaS applications:

ZTNA access proxy application name	SaaS application
adobe	Adobe services domains
adp	ADP
atlassian	Atlassian
aws-s3	AWS S3
azure	Azure
box	Box
citrix	Citrix
confluence	Confluence
docusign	DocuSign
dropbox	Dropbox
egnyte	Egnyte
github	GitHub
gmail	Gmail
google-cloud	Google Cloud
google-drive	Google Drive
google-office	Google Office
google-web	Google Web Search domains
jira	Jira
ms-excel	Microsoft Excel
ms-exchange	Microsoft Exchange
ms-onedrive	Microsoft OneDrive
ms-outlook	Microsoft Outlook
ms-powerpoint	Microsoft PowerPoint

ZTNA access proxy application name	SaaS application
ms-teams	Microsoft Teams
ms-word	Microsoft Word
oracle-cloud	Oracle Cloud
salesforce	Salesforce
sap	SAP
Servicenow	ServiceNow
sharepoint	SharePoint
twilio-video-cloud	Twilio video cloud
webex	Webex
workplace	Workplace
youtube	YouTube
zendesk	Zendesk
zoom	Zoom

The inline CASB database, as of version 1.00031, supports the following SaaS access control:

ZTNA access proxy access control name	SaaS access control
box-download	Box download
box-upload	Box upload
dropbox-download	Dropbox download
dropbox-upload	Dropbox upload
gmail-getAttach	Gmail download attachment
azure	Azure
ms-onedrive-download	MS OneDrive download
ms-outlook-getAttach	MS Outlook download attachment

The inline CASB database, as of version 1.00031, supports the following SaaS application groups:

ZTNA access proxy application name	SaaS application group
MS	Microsoft SaaS

For a complete list, use the following CLI commands to retrieve the corresponding lists.

Display the list of applications:

```
# diagnose saas show apps
```

Display details of each application:

```
# diagnose saas show details
```

Error codes and replacement messages

The following table summarizes the replacement message errors based on error code and category available in FortiProxy.

Error code	Error category	Error message	Description
001	Invalid ZTNA Certificate	The page you requested has been blocked because the ZTNA certificate is invalid.	The client endpoint has an invalid certificate that the FortiProxy cannot recognize.
002	Invalid ZTNA Certificate	The page you requested has been blocked because the ZTNA certificate is empty.	The client endpoint did not provide a client certificate for the FortiProxy to verify.
003	Invalid ZTNA Certificate	The page you requested has been blocked because the device is manageable but with an empty ZTNA certificate.	The client endpoint has FortiClient installed (hence manageable), but did not provide a client certificate for the FortiProxy to verify.
021	ZTNA Application Not Found	The page you requested has been blocked because no API gateway was matched.	The client endpoint is looking for a page or service that is not configured in the FortiProxy's ZTNA settings.
022	ZTNA Application Not Found	The page you requested has been blocked because the real server in the API gateway cannot be found.	The FortiProxy is unable to serve the requested page or service because it cannot find the real server.
023	ZTNA Application Not Found	The page you requested has been blocked because ZTNA FQDN DNS failed.	The FortiProxy cannot resolve the FQDN in the client endpoint's request.
041	ZTNA Portal Error	The page you requested has been blocked because SSL VPN bookmark address failed.	The FortiProxy is unable to match a bookmark in the SSL VPN web portal used by the ZTNA application gateway.
061	ZTNA Policy Deny	The page you requested has been blocked because no policy was matched.	There is no ZTNA policy that matches the destination page that the client endpoint is requesting.
062	ZTNA Policy Deny	The page you requested has been blocked because a policy with action deny was matched.	The traffic matched a ZTNA deny policy.

Error code	Error category	Error message	Description
063	ZTNA Policy Deny	The page you requested has been blocked because the client cert has been revoked.	The endpoint client is using a client certificate issued by FortiClient EMS that has been revoked.
064	ZTNA Policy Deny	The page you requested has been blocked because the tags matched a deny policy.	The endpoint client has a ZTNA tag that matches a ZTNA deny policy.
065	ZTNA Policy Deny	The page you requested has been blocked because the tags didn’t match any policy.	The endpoint client's ZTNA tags did not match any ZTNA policies, and its traffic is implicitly denied.
066	ZTNA Policy Deny	The page you requested has been blocked because no device info was found.	The FortiProxy cannot find any device information for the client endpoint, resulting in a failed verification of the client.
067	ZTNA Policy Deny	The page you requested has been blocked because the device is offline.	The client endpoint is not connected to FortiClient EMS, hence is considered offline and blocked by the FortiProxy.

Change log

Date	Change description
2024-11-01	Initial release.

www.fortinet.com