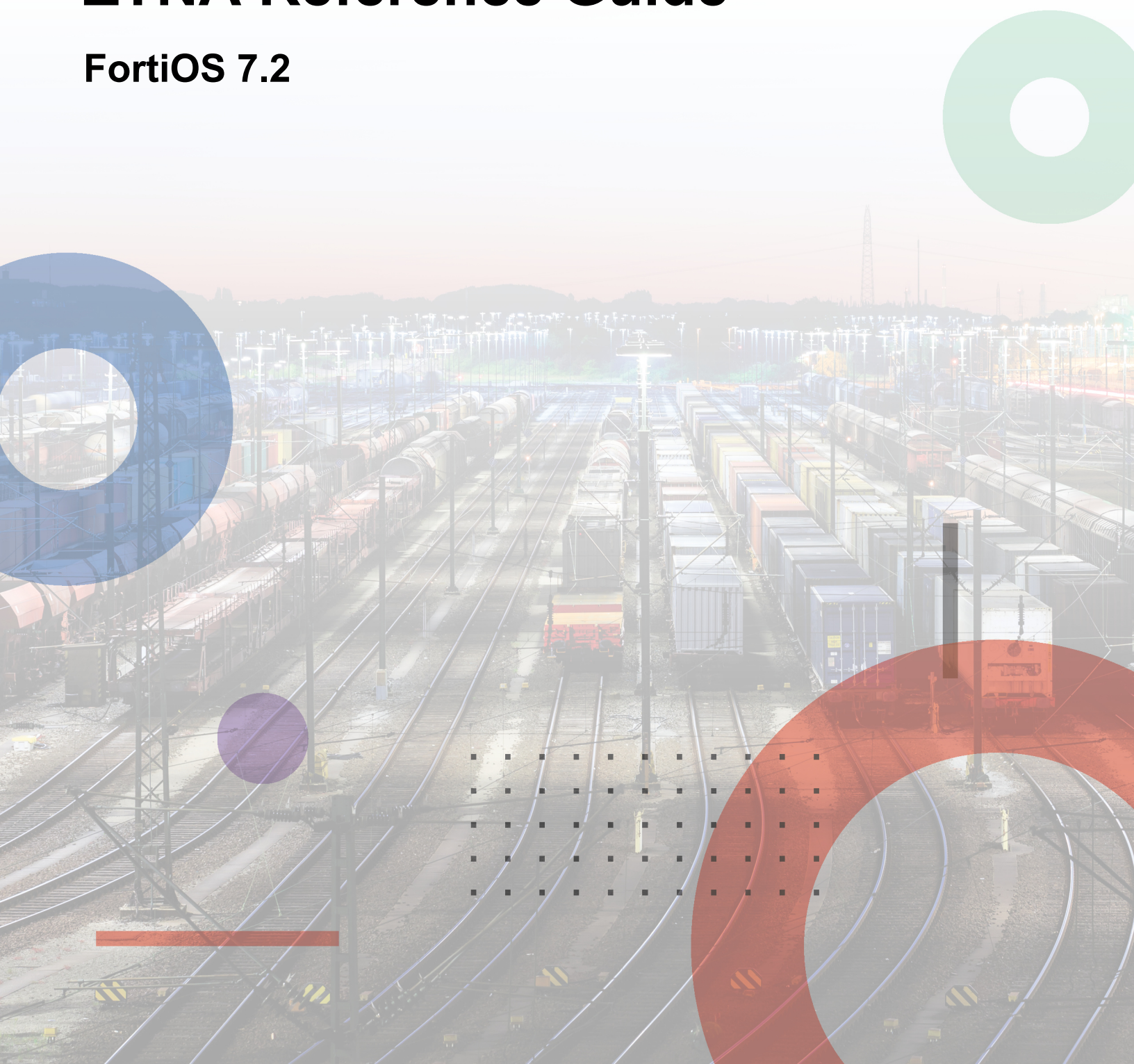
ZTNA Reference Guide

FortiOS 7.2



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

NSE 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

August 04, 2022
FortiOS 7.2 ZTNA Reference Guide
01-720-828971-20220804

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 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	Windows, macOS, Linux
	Medium or higher	Windows, macOS, Linux
	Low or higher	Windows, macOS, Linux
Antivirus (AV) 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.	Windows, macOS, Linux
	AV signature is up-to-date	Windows, macOS, Linux
Windows security	Windows Defender is enabled	Windows
	Bitlocker Disk Encryption is enabled	Windows
	Exploit Guard is enabled	Windows
	Application Guard is enabled	Windows
	Windows Firewall is enabled	Windows
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, iOS, Android
Firewall threat	Presence of [Firewall threat ID]	Windows, macOS, Linux, iOS, Android

Other posture checks

Rule type	Posture check	Supported operating systems
Active Directory (AD) group	Member of [AD Group]	Windows, macOS
Certificate	Certificate contains [Subject CN] and [Issuer CN]	Windows, macOS, Linux
File	Presence of [File]	Windows, macOS, Linux
IP range	Device in the [IP Range]	Windows, macOS, Linux, IOS, Android
Logged in domain	Member of [Domain]	Windows, macOS
On-Fabric status	On-Fabric	Windows, macOS, Linux, IOS, Android

Rule type	Posture check	Supported operating systems
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
	Mojave	macOS
	High Sierra	macOS
	Sierra	macOS
	Catalina	macOS
	Big Sur	macOS
	Monterey	macOS
	CentOS 7.5	Linux
	CentOS 7.4	Linux
	CentOS 8	Linux
	Red Hat 7.6	Linux
	Red Hat 7.5	Linux
	Red Hat 7.4	Linux
	Red Hat 8	Linux
	Red Hat 8.1	Linux
	Ubuntu 18.04	Linux
	iOS 9, 10, 11, 12, 13, 14	iOS
	Android 5, 6, 7, 8, 9, 10, 11	Android
Registry key	[Registry Key]	Windows

Rule type	Posture check	Supported operating systems
Running process	Presence of [Running Process]	Windows, macOS, Linux
Sandbox detection	Sandbox detected malware in last 7 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

CASB SaaS application support

You can configure the FortiGate 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. FortiOS 7.2.1 and later versions support ZTNA inline CASB for SaaS application access. This topic provides information on the supported applications.

The inline CASB database, as of version 1.00025, 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
salesforce	Salesforce
sap	SAP
sharepoint	SharePoint
webex	Webex
workplace	Workplace
youtube	YouTube
zendesk	Zendesk
zoom	Zoom

The inline CASB database, as of version 1.00025, supports the following SaaS application groups:

ZTNA access proxy application name	SaaS application group
Google	Google SaaS
MS	Microsoft SaaS

Change log

Date	Change Description
2022-08-04	Initial release.

www.fortinet.com