FortiOS - Ports and Protocols

Version 6.4.0

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

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

September 19, 2022
FortiOS 6.4.0 Ports and Protocols
01-640-619355-20220919

TABLE OF CONTENTS

Change Log ... **4**
Introduction ... **5**
FortiGate open ports ... **6**
FortiAnalyzer open ports ... **9**
FortiAP-S open ports ... **11**
FortiAuthenticator open ports ... **12**
FortiClient open ports ... **15**
FortiClient ... 15
FortiClient EMS ... 16
FortiClient for Chromebook ... 17
FortiClient EMS for Chromebook ... 18
FortiGate Cloud open ports ... **19**
FortiDB open ports ... **20**
FortiGuard open ports ... **21**
FortiMail open ports ... **23**
FortiManager open ports ... **26**
FortiPortal open ports ... **28**
FortiSandbox open ports ... **29**
Services and port numbers required for FortiSandbox ... 29
3rd-party servers open ports ... **31**
Fortinet proprietary protocols ... **33**
FGCP - FortiGate Clustering Protocol ... 34
FGSP - FortiGate Session Life Support Protocol ... 42
FGFM - FortiGate to FortiManager Protocol ... 46
SLBC - Session-aware Load Balancing Cluster ... 49
Fortinet Security Fabric ... 57
FortiGuard ... 59
Anycast and unicast services ... 61
FortiLink ... 62
FortiOS WAN optimization ... 63
FSSO - Fortinet Single Sign-On ... 67
OFTP - Optimized Fabric Transfer Protocol ... 71
FortiClient EMS - Enterprise Management Server ... 72

Change Log

Date	Change Description
2020-03-31	Initial release.
2020-05-21	Updated FortiAuthenticator open ports on page 12
2020-07-02	Added Anycast and unicast services on page 61.
2020-08-19	Updated FortiMail open ports on page 23.
2020-11-24	Updated FortiAuthenticator open ports on page 12.
2021-01-08	Updated FortiPortal open ports on page 28 and FortiGuard open ports on page 21.
2021-02-26	Updated FortiManager open ports on page 26.
2021-04-27	Updated FortiAuthenticator open ports on page 12 and 3rd-party servers open ports on page 31.
2021-11-18	Updated FortiGate open ports on page 6.
2021-11-23	Updated FortiLink on page 62.
2021-12-16	Updated FortiMail open ports on page 23.
2022-05-16	Updated FortiGate open ports on page 6.
2022-09-19	Updated FGCP - FortiGate Clustering Protocol on page 34.

Introduction

This document contains a series of diagrams and tables showing the communication ports and protocols used between various Fortinet products:

- FortiGate
- FortiAnalyzer
- FortiAP-S
- FortiAuthenticator
- FortiClient
- FortiCloud
- FortiDB
- FortiGuard
- FortiMail
- FortiManager
- FortiPortal
- FortiSandbox
- and 3rd-party servers using FSSO.

Additionally, Fortinet's proprietary protocols are documented, showing what Fortinet products they operate with, how they behave, and how they carry out their roles:

- FGCP - FortiGate Clustering Protocol
- FGSP - FortiGate Session Life Support Protocol
- FGFM - FortiGate to FortiManager Protocol
- SLBC - Session-aware Load Balancing Cluster
- Fortinet Security Fabric
- FortiGuard
- FortiLink
- FortiOS WAN optimization
- FSSO - Fortinet Single Sign-On
- OFTP - Optimized Fabric Transfer Protocol
- FortiClient EMS - Endpoint Management Server

Some protocols contain CLI syntax that control their ports and functionality.

FortiGate open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAP-S	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/443
	CAPWAP	UDP/5246, UDP/5247
FortiAuthenticator	Policy Authentication through Captive Portal	TCP/1000
	RADIUS disconnect	TCP/1700
FortiClient	Remote IPsec VPN access	UDP/IKE 500, ESP (IP 50), NAT-T 4500
	Remote SSL VPN access	TCP/443
	SSO Mobility Agent, FSSO	TCP/8001
	Compliance and Security Fabric	TCP/8013 (by default; this port can be customized)
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, and 0x8893
	HA Synchronization	TCP/703, UDP/703
	Unicast Heartbeat for Azure	UDP/730
	DNS for Azure	UDP/53
	Security Fabric	UDP/8014
FortiGuard	Management	TCP/541
	AV/IPS	UDP/9443
FortiManager	AV/IPS Push	UDP/9443
	IPv4 FGFM management	TCP/541
	IPv6 FGFM management	TCP/542
FortiPortal	API communications (FortiOS REST API, used for Wireless Analytics)	TCP/443
3rd-Party Servers	FSSO	TCP/8001 (by default; this port can be customized)

Incoming ports		
Purpose		**Protocol/Port**
Others	Web Admin	TCP/80, TCP/443
	Policy Override Authentication	TCP/443, TCP/8008, TCP/8010
	Policy Override Keepalive	TCP/1000, TCP/1003
	SSL VPN	TCP/443
	AeroScout Vendor port	UDP/1144
	External captive portal authentication with FortiAP in bridge mode	UDP/2000
	RADIUS DAS feature - RFC 5176	UDP/3799

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
FortiAuthenticator	LDAP, PKI Authentication	TCP or UDP/389
	RADIUS	UDP/1812
	FSSO	TCP/8000
	RADIUS Accounting	UDP/1813
	SCEP	TCP/80, TCP/443
	CRL Download	TCP/80
	External Captive Portal	TCP/443
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, and 0x8893
	HA Synchronization	TCP/703, UDP/703
	Unicast Heartbeat for Azure	UDP/730
	DNS for Azure	UDP/53
FortiGate Cloud	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS Update	TCP/443, TCP/8890
	Cloud App DB	TCP/9582
	FortiGuard Queries	UDP/53, UDP/8888, TCP/53, TCP/8888, TCP/443 (as part of Anycast servers)
	SDNS queries for DNS Filter	UDP/53, TCP/853 (as part of Anycast servers)
	Registration	TCP/80
	Alert Email, Virus Sample	TCP/25
	Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443
	Central Management, Analysis	TCP/541
FortiManager	IPv4 FGFM management	TCP/541
	IPv6 FGFM management	TCP/542
	Log & Report	TCP or UDP/514
	FortiGuard Queries	UDP/53, UDP/8888, TCP/80, TCP/8888
FortiSandbox	OFTP	TCP/514
Others	FSSO	TCP/8001 (by default; this port can be customized)

While a proxy is configured, FortiGate uses the following URLs to access the FortiGuard Distribution Network (FDN):

- **update.fortiguard.net**
- **service.fortiguard.net**
- **support.fortinet.com**

Enabling some services will cause additional standard ports to open as the protocol necessitates. For example, enabling BGP will open TCP port 179. See View open and in use ports for more information.

FortiAnalyzer open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAuthenticator	Logging	UDP/514
FortiAP-S	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiClient	Logs from FortiClient for Chromebook	TCP/8443
	Logs from FortiClient (FortiClient must connect to FortiGate or EMS to send logs to FortiAnalyzer)	TCP/514
FortiGate	Syslog, Registration, Quarantine, Log & Reports	TCP/514
	OFTP	TCP/514, UDP/514
FortiMail	Syslog	UDP/514
FortiManager	Syslog & OFTP	TCP/514, UDP/514
	Registration	TCP/541
FortiPortal	API communications (JSON and XML APIs respectively)	TCP/443, TCP/8080
Others	SSH CLI Management	TCP/22
	Web Admin	TCP/80, TCP/443
	REST	TCP/443
	DC Polling	TCP/445
	Logg Agg	TCP/3000
	GEIP query service	UDP/8888

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS, SMS, FTM, Licensing, Policy Override, RVS, URL/AS Update	TCP/443
FortiPortal	Log communications	TCP/514, UDP/514

Outgoing ports		
Purpose		**Protocol/Port**
(FortiPortal only receives log communications from FortiAnalyzer when it is acting as a collector)		
3rd-Party Servers	LDAP & PKI Authentication	TCP/389, UDP/389
	Log & Report	TCP/21, TCP/22
	Configuration Backups	TCP/22
	Alert Email	TCP/25
	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Report Query	TCP/389
	Syslog & OFTP	TCP or UDP/514
	RADIUS	UDP/1812

FortiAnalyzer uses the following URL to access the sprite map:

- **productapi.fortinet.com**

`productapi.fortinet.com` resolves to 96.45.36.123 or 208.91.114.142.

FortiAP-S open ports

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*
FortiCloud	Initial Discovery	TCP/443
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*
FortiGate	Syslog, Registration, Quarantine, Log & Report	TCP/443
	CAPWAP	UDP/5246*, UDP/5247*
FortiGuard	FortiGuard Queries	UDP/53, UDP/8888
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*

* - Only FortiAP models, not FortiAP-S.

FortiAuthenticator open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAuthenticator	Load-balancing HA secondary	UDP/721, UDP/1194
	Redundant HA cluster	UDP/720
	FSSO tiered architecture	TCP/8003
FortiClient	SSO Mobility Agent, FSSO	TCP/8001 (by default; this port can be customized)
FortiGate	LDAP, PKI Authentication	TCP or UDP/389
	RADIUS	UDP/1812
	FSSO	TCP/8000
	RADIUS Accounting	UDP/1813, UDP/1646
	SCEP	TCP/80, TCP/443
	CRL download	TCP/80
	External captive portal	TCP/443
FortiToken Mobile	Push approve/deny	TCP/443
	FTM device transfer	TCP/443
Others	SSH CLI	TCP/22
	Telnet	TCP/23
	HTTP & SCEP	TCP/80
	SNMP Poll	UDP/161
	Web Admin	TCP/80, TCP/443
	LDAP	TCP/389, TCP/3268
	LDAPS	TCP/636, TCP/3269
	RADIUS	UDP/1812, UDP/1813
	OCSP	TCP/2560
	Syslog	UDP/514
	SAML	TCP/443
	OAuth	TCP/443

Incoming ports		
Purpose		**Protocol/Port**
3rd-Party Servers	FSSO DC/TS agents	TCP/8002
	FortiAuthenticator Windows/OWA agent	TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
FortiAuthenticator	(HA) HA heartbeat	UDP/720
	(LB secondary) LB secondary sync	UDP/721, UDP/1194
	FSSO tiered architecture	TCP/8003
FortiGate	Policy Authentication through Captive Portal	TCP/1000
	RADIUS disconnect	TCP/1700
FortiGuard	FortiToken hardware seed retrieval	TCP/443
	FortiToken Mobile activation, provisioning, and transfer	TCP/443
	FortiToken Cloud communication	TCP/8686
	FortiGuard SMS	TCP/443
	FortiToken Mobile push proxy service (FAC 6.1.1 and later)	TCP/443
	FortiToken Mobile Apple push servers (FAC 6.1.0 and earlier)	TCP/5223, TCP/2195, TCP/2196
	FortiToken Mobile Google push servers (FAC 6.1.0 and earlier)	TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
3rd-Party Servers	SMTP	TCP/25
	DNS	UDP/53
	Windows AD	TCP/88
	NTP	UDP/123
	LDAP	TCP/389, TCP/3268
	Domain Control	TCP/445
	LDAPS	TCP/636, TCP/3269
	FSSO tiered architecture	TCP/5003
	FTP/SFTP configuration and logs backup	TCP/21, TCP/22
	SMS HTTP/HTTPS gateways	TCP/80, TCP/443
	OAuth	TCP/443
	CRL download	TCP/80, TCP/443
FortiNAC	FSSO	TCP/8000
FortiAnalyzer	Logging	UDP/514

FortiClient open ports

The following tables show the distinct communications for each FortiClient product:

- FortiClient on page 15
- FortiClient EMS on page 16
- FortiClient for Chromebook on page 17
- FortiClient EMS for Chromebook on page 18

FortiClient

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Send logs to FortiAnalyzer (FortiClient must connect to FortiGate or EMS to send logs to FortiAnalyzer)	TCP/514
FortiAuthenticator	SSO Mobility Agent, FSSO	TCP/8001
FortiClient EMS	Endpoint management	TCP/8013
FortiGate	Remote IPsec VPN access	UDP/IKE 500, ESP (IP 50), NAT-T 4500
	Remote SSL VPN access	TCP/443 (by default; this port can be customized)
	SSO Mobility Agent, FSSO	TCP/8001
	Compliance and Security Fabric	TCP/8013 (by default; this port can be customized)
FortiGuard	AV/VUL signatures update, Cloud-based behavior scan (CBBS)/applications that use cloud services	TCP/80
	Virus submission (SMTP/FortiGuard)	TCP/25
	URL rating	UDP/8888 (by default; this port can be changed to port 53 by entering fgd1.fortigate.com:53 via the XML config file)

Outgoing ports		
Purpose		**Protocol/Port**
FortiManager	Select a FortiManager to be used for FortiClient signature updates	TCP/80 (by default; this port can be customized)
	Send logs to FortiManager (FortiClient must connect to FortiGate or EMS to send logs to FortiManager)	TCP/514
FortiSandbox	File analysis	TCP/514
Syslog server	Send logs to syslog server	UDP/514

FortiClient EMS

Incoming ports		
Purpose		**Protocol/Port**
FortiClient	Endpoint management	TCP/8013 (by default; this port can be customized)
	Download FortiClient installer created by EMS server	TCP/10443
Apache server/HTTPS	Web access to EMS	TCP/443
FSSO	Connection to FortiOS	TCP/8000

Outgoing ports		
Purpose		**Protocol/Port**
FortiClient	Endpoint probing during FortiClient deployment	ICMP
FortiGuard	FortiClient EMS AV/VUL/APP version updates	TCP/80
Samba (SMB) service	SMB during FortiClient deployment	TCP/445
SMTP server/email	EMS and endpoint alerts	TCP/25
AD server	Retrieving workstation and user information	TCP/389 (LDAP) or TCP/636 (LDAPS)
Others	Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) for FortiClient deployment	TCP/135

FortiClient for Chromebook

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Send logs to FortiAnalyzer	TCP/8443
FortiClient EMS	Connect to EMS Chromebook profile server	TCP/8443
FortiGuard	URL rating	TCP/443, TCP/3400

FortiClient EMS for Chromebook

Incoming ports		
Purpose		**Protocol/Port**
FortiClient for Chromebook	Connection to EMS	TCP/8443
Apache server/HTTPS	Web access to EMS	TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
SMTP server/email	EMS and endpoint alerts	TCP/25
Others	G Suite API calls for Google domain information	TCP/443

FortiGate Cloud open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAP-S	Initial Discovery	TCP/443
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiGate	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard	Registration	TCP/443

FortiDB open ports

Incoming ports		
Purpose		**Protocol/Port**
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443
	SNMP Traps	UDP/161
	Agent Communication	TCP/9116, TCP/9117

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard (FortiDB will use a random port picked by the kernel)	FortiGuard Updates	TCP/80
FortiMonitor	SSH, SFTP	TCP/22
3rd-Party Servers	Email Notifications/Reports	TCP/25
	SNMP Traps	UDP/162
	Syslog	UDP/514

FortiGuard open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAnalyzer	AV/IPS Updates, SMS, FTM, Licensing, Policy Overrides, RVS, URL/AS Update	TCP/443
FortiAP-S	FortiGuard Queries	UDP/53, UDP/8888
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiAuthenticator	FortiToken hardware seed retrieval	TCP/443
	FortiToken Mobile activation, provisioning, and transfer	TCP/443
	FortiToken Cloud provisioning	TCP/443
	FortiGuard SMS	TCP/443
	FortiToken Mobile push proxy service (FAC 6.1.1 and later)	TCP/443
	FortiToken Mobile Apple push servers (FAC 6.1.0 and earlier)	TCP/5223, TCP/2195, TCP/2196
	FortiToken Mobile Google push servers (FAC 6.1.0 and earlier)	TCP/443
FortiClient	AV/VUL signatures update, Cloud-based behavior scan (CBBS)/applications that use cloud services	TCP/80
	Virus submission (SMTP/FortiGuard)	TCP/25
	URL rating	UDP/8888 (by default; this port can be changed to port 53 by entering fgd1.fortigate.com:53 via the XML config file) **Note:** FortiClient for Chromebooks contacts FortiGuard for URL ratings via TCP/443
	FortiClient EMS AV/VUL/APP version updates *	TCP/80
FortiCloud	Registration	TCP/443

Incoming ports		
Purpose		**Protocol/Port**
FortiGate	AV/IPS Update, Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443, TCP/8890
	Cloud App DB	TCP/9582 (flow.fortinet.net)
	FortiGuard Queries	UDP/53, UDP/8888, TCP/53, TCP/8888, TCP/443 (as part of Anycast servers)
	SDNS queries for DNS Filter	UDP/53, TCP/853 (as part of Anycast servers)
	Registration	TCP/80
	Alert Emails, Virus Sample	TCP/25
	Central Management, Analysis	TCP/541
FortiMail	AS Rating	UDP/53
	AV/AS Update	TCP/443
FortiManager	AV/IPS Updates, URL/AS Update, Firmware, SMS, FTM, Licensing, Policy Override Authentication, Registration	TCP/443
	FortiClient updates	TCP/80
FortiPortal	Licensing	TCP/443
FortiSandbox (FortiSandbox will use a random port picked by the kernel)	FortiGuard Distribution Servers	TCP/8890
	FortiGuard Web Filtering Servers	UDP/53, UDP/8888

Outgoing ports		
Purpose		**Protocol/Port**
FortiGate	Management	TCP/541
	AV/IPS	UDP/9443
FortiMail	AV Push	UDP/9443
FortiManager	AV/IPS	UDP/9443

FortiMail open ports

When operating in its default configuration, FortiMail does not accept TCP or UDP connections on any port except port1 and port2 network interfaces, which accept:

- ICMP pings,
- HTTPS connections on TCP/443,
- and SSH connections on TCP/22.

Incoming ports		
Purpose		**Protocol/Port**
Admin by Console or PC	SSH, Telnet, HTTP, SSH, Console	TCP/443 or TCP/80 or TCP/22 or TCP/23
Email Client	Quarantine View/Retrieve	TCP/80 or TCP/443 or TCP/110
	SMTP or SMTPS	TCP/25 or TCP/465
	POP3 or POP3S	TCP/110 or TCP/995 (server mode only)
	IMAP or IMAPS	TCP/143 or TCP/993 (server mode only)
	WebDAV and CalDAV	TCP/8008
FortiMail	Base port for HA heartbeat signal	UDP/20000
	Synchronization control	UDP/20001
	File synchronization	TCP/20002
	Data synchronization	TCP/20003
	Checksum synchronization	TCP/20004
	HA service monitoring (remote SMTP)	TCP/25
	HA service monitoring (remote HTTP)	TCP/80
	HA service monitoring (remote POP3)	TCP/110
	HA service monitoring (remote IMAP)	TCP/143
	Clear Text Central Quarantine	TCP/514
	SSL Central Quarantine	TCP/6514
FortiManager	SNMP Poll	TCP/161
	Config/Firmware Push	TCP/22
FortiGuard	AV Push	UDP/9443

Incoming ports		
Purpose		**Protocol/Port**
External Email Server	SMTP or SMTPS	TCP/25 or 465
	Storage: iSCI, NFS	TCP/3260 (iSCI), TCP/2049 (NFS)
	Config Backup	SFTP / FTP
	Mail Data Backup	NFS, SMB/CIFS, SSH, external USB (direct connected), iSCSI
Protected Email Server	SMTP or SMTPS	TCP/25 or 465

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	OFTP	UDP/514
FortiManager	SNMP Traps	UDP/162
	Reg, Config Backup, Config/Firmware Pull	TCP/443
FortiGuard	AS Rating	UDP/53, UDP/8888 TCP/53, TCP/443, TCP/8888
	AV/AS Update	TCP/443, TCP/8890
FortiMail	Base port for HA heartbeat signal	UDP/20000
	Synchronization control	UDP/20001
	File synchronization	TCP/20002
	Data synchronization	TCP/20003
	Checksum synchronization	TCP/20004
	HA service monitoring (remote SMTP)	TCP/25
	HA service monitoring (remote HTTP)	TCP/80
	HA service monitoring (remote POP3)	TCP/110
	HA service monitoring (remote IMAP)	TCP/143
	Clear Text Central Quarantine	TCP/514
	SSL Central Quarantine	TCP/6514
External Email Server	SMTP or SMTPS	TCP/25 or TCP/465

Outgoing ports		
Purpose		**Protocol/Port**
Protected Email Server	SMTP or SMTPS	TCP/25 or TCP/465
	POP3 Auth	TCP/110
	IMAP Auth	TCP/143
Others	Dyn DNS	TCP/80 *
	DNS, RBL	UDP/53
	NTP	UDP/123
	Alert Email	TCP/25
	LDAP or LDAPS	TCP/389 or TCP/636
	RADIUS Auth	TCP/1812
	NAS	TCP/21, TCP/22, TCP/2049
	OCSP (for PKI user)	TCP/80, or defined by certificate
FortiSandbox / FortiSandbox Cloud	Communication	TCP/443, TCP/514

***** FortiMail generates outbound traffic and sends an HTTP SYN request via TCP/80. The Fortinet RSS Feed widget provides a convenient display of the latest security advisories and discovered threats from Fortinet. Also, if an email message contains a shortened URI that redirects to another URI, it would cause FortiMail to send an HTTP SYN request to the shortened URI to get the redirected URI.

FortiMail uses the following URLs to access the FortiGuard Distribution Network (FDN). URLs beginning with *us* apply only to FortiGates in the United States.

- **service.fortiguard.net - UDP**
- **usservice.fortiguard.net - UDP**
- **securewf.fortiguard.net - HTTPS**
- **ussecurewf.fortiguard.net - HTTPS**
- **update.fortiguard.net - TCP**

FortiManager open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiGate	IPv4 FGFM management	TCP/541
	IPv6 FGFM management	TCP/542
	Log & Report	TCP or UDP/514
	FortiGuard Queries	UDP/53, UDP/8888, TCP/80, TCP/8888 TCP/443, TCP/8890 when FortiManager is operating as a FortiGuard override server
FortiClient	Select a FortiManager to be used for FortiClient signature updates	TCP/80 (by default; this port can be customized)
	Send logs to FortiManager (FortiClient must connect to FortiGate or EMS to send logs to FortiManager)	TCP/514
FortiGuard	AV/IPS	UDP/9443
FortiMail	Registration	UDP/9443
	AV/AS Query	
FortiManager	FortiClient Manager	TCP/6028
FortiPortal	API communications (JSON and XML APIs respectively)	TCP/443, TCP/8080
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443

Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog & OFTP	TCP/514, UDP/514
	Registration	TCP/541
FortiGate	AV/IPS Push	UDP/9443
	IPv4 FGFM management	TCP/541
	IPv6 FGFM management	TCP/542

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS Updates, URL/AS Update, Firmware, SMS, FTM, Licensing, Policy Override Authentication, Registration	TCP/443
	FortiClient udpates	TCP/80
FortiMail	AV Push	
FortiManager	FortiClient Manager	TCP/6028
	Fortinet registry for management extension applications, such as FortiWLM MEA	TCP/4443
3rd-Party Servers	DNS	UDP/53
	NTP	UDP/123
	Proxied HTTPS Traffic	TCP/443
	RADIUS	UDP/1812

While a proxy is configured, FortiManager uses the following URLs to access the FortiGuard Distribution Network (FDN) for the following updates:

- **fds1.fortinet.com** - FortiGate AV/IPS package downloads
- **guard.fortinet.net** - Webfilter/Anti-Spam DB and AVfileQuery DB downloads
- **forticlient.fortinet.com** - FortiClient signature package downloads
- **fgd1.fortigate.com:8888** - FortiClient Webfilter queries to FortiGuard

FortiPortal open ports

Incoming ports		
Purpose		**Protocol/Port**
End User/MSSP Admin	FortiPortal utilization by end users and MSSP admins	TCP/443
FortiAnalyzer (FortiPortal only receives log communications from FortiAnalyzer when it is acting as a collector)	Log communications	TCP/514, UDP/514

Outgoing ports		
Purpose		**Protocol/Port**
FortiGate	API communications (FortiOS REST API, used for Wireless Analytics)	TCP/443
FortiManager	API communications (JSON and XML APIs respectively)	TCP/443, TCP/8080
FortiAnalyzer	API communications (JSON and XML APIs respectively)	TCP/443, TCP/8080
PortalDB	MySQL communications	TCP/3306
CollectorDB	MySQL communications	TCP/3306
FortiGuard	Licensing	TCP/443
Fortinet Map Server	Map Service	TCP/443

FortiSandbox open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiGate	OFTP	TCP/514
FortiClient	File analysis	TCP/514
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443
	OFTP Communication with FortiGate & FortiMail	TCP/514
	Third-party proxy server for ICAP servers	ICAP: TCP/1344 ICAPS: TCP/11344

Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard (FortiSandbox will use a random port picked by the kernel)	FortiGuard Distribution Servers	TCP/8890
	FortiGuard Web Filtering Servers	UDP/53, UDP/8888
FortiSandbox Community Cloud (FortiSandbox will use a random port picked by the kernel)	Upload detected malware information	TCP/443, UDP/53

FortiSandbox uses the following FQDNs to access the FortiSandbox Community Cloud, depending on which protocol and port is used:

- TCP/443: **fqdl.fortinet.net**
- UDP/53: **fqsvr.fortinet.net**

Services and port numbers required for FortiSandbox

The tables above show all the services required for FortiSandbox to function correctly. You can use the diagnostic FortiSandbox command `test-network` to verify that all the services are allowed by the upstream. If the result is `Passed`, then there is no issue. If there is an issue with a specific service, it will be shown in the command output, and inform you which port needs to be opened.

This command checks:

- VM Internet access
- Internet connection
- System DNS resolve speed
- VM DNS resolve speed
- Ping speed
- Wget speed
- Web Filtering service
- FortiSandbox Community Cloud service

3rd-party servers open ports

Incoming ports		
Purpose		**Protocol/Port**
FortiAnalyzer	LDAP & PKI Authentication	TCP/389, UDP/389
	Log & Report	TCP/21, TCP/22
	Configuration Backups	TCP/22
	Alert Emails	TCP/25
	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Report Query	TCP/389
	Syslog & OFTP	TCP or UDP/514
	RADIUS	UDP/1812
FortiAuthenticator	SMTP	TCP/25
	DNS	UDP/53
	Windows AD	TCP/88
	NTP	UDP/123
	LDAP	TCP/389, TCP/3268
	Domain Control	TCP/445
	LDAPS	TCP/636, TCP/3269
	FSSO Tiered Architecture	TCP/5003
	FTP/SFTP Configuration and Logs Backup	TCP/21, TCP/22
	SMS HTTP/HTTPS Gateways	TCP/80, TCP/443
	OAuth	TCP/443
	CRL Download	TCP/80, TCP/443
FortiManager	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Proxied HTTPS Traffic	TCP/443
	RADIUS	UDP/1812

Outgoing ports		
Purpose		**Protocol/Port**
FortiAuthenticator	FSSO DC/TS Agents	TCP/8002
	FortiAuthenticator Windows/OWA Agent	TCP/443
FortiGate	FSSO	TCP/8001 (by default; this port can be customized)

Fortinet proprietary protocols

The following section provides a full list of Fortinet's proprietary protocols, their purposes, and what ports they operate on:

- FGCP - FortiGate Clustering Protocol
- FGSP - FortiGate Session Life Support Protocol
- FGFM - FortiGate to FortiManager Protocol
- SLBC - Session-aware Load Balancing Cluster
- Fortinet Security Fabric
- FortiGuard
  - Anycast and unicast services
- FortiLink
- FortiOS WAN optimization
- FSSO - Fortinet Single Sign-On
- OFTP - Optimized Fabric Transfer Protocol
- FortiClient EMS - Enterprise Management Server

FGCP - FortiGate Clustering Protocol

In an active-passive HA configuration, the FortiGate Clustering Protocol (FGCP) provides failover protection, whereby the cluster can provide FortiGate services even when one of the cluster units loses connection. FGCP is also a Layer 2 heartbeat that specifies how FortiGate units communicate in an HA cluster and keeps the cluster operating.

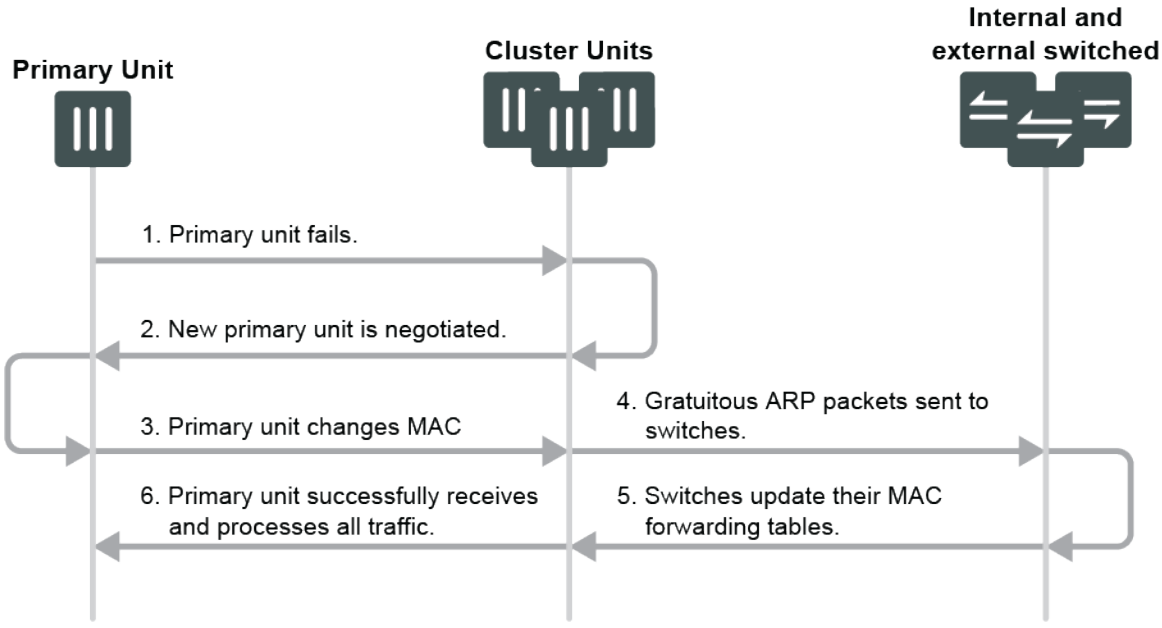
You cannot mix FGCP and SLBC clusters in the same chassis.

The FortiGate's HA Heartbeat listens on ports TCP/703, TCP/23, or ETH layer 2/8890.

Virtual MAC addresses

FGCP assigns virtual MAC addresses to each primary unit interface in an HA cluster. Virtual MAC addresses are in place so that, if a failover occurs, the new primary unit interfaces will have the same MAC addresses as the failed primary unit interfaces. If the MAC addresses were to change after a failover, the network would take longer to recover because all attached network devices would have to learn the new MAC addresses before they could communicate with the cluster.

If a cluster is operating in Transparent mode, FGCP assigns a virtual MAC address for the primary unit management IP address. Since you can connect to the management IP address from any interface, all of the FortiGate interfaces appear to have the same virtual MAC address.



When a cluster starts up, after a failover, the primary unit sends gratuitous ARP packets to update the switches connected to the cluster interfaces with the virtual MAC address. The switches update their MAC forwarding tables with this MAC address. As a result, the switches direct all network traffic to the primary unit. Depending on the cluster

configuration, the primary unit either processes this network traffic itself or load balances the network traffic among all of the cluster units.

You cannot disable sending gratuitous ARP packets, but you can change the number of packets that are sent (1-60 ARP packets) by entering the following command:

```
config system ha
  set arps <integer>
end
```

You can change the time between ARP packets (1-20 seconds) by entering the following command:

```
config system ha
  set arps-interval <integer>
end
```

Assigning virtual MAC addresses

Virtual MAC addresses are determined based on the following formula:

00-09-0f-09-<group-id_hex>-<vcluster_integer><idx>

where:

- **<group-id_hex>**: The HA group ID for the cluster converted to hexadecimal. The table below lists some example virtual MAC addresses set for each group ID:

Integer group ID	Hexadecimal group ID
0	00
1	01
2	02
3	03
...	...
10	0a
11	0b
...	...
63	3f
...	...
255	ff

- **<vcluster_integer>**: This value is 0 for virtual cluster 1 and 2 for virtual cluster 2. If virtual domains are not enabled, HA sets the virtual cluster to 1 and by default all interfaces are in the root virtual domain. Including virtual cluster and virtual domain factors in the virtual MAC address formula means that the same formula can be used whether or not virtual domains and virtual clustering is enabled.
- **<idx>**: The index number of the interface. In NAT mode, interfaces are numbered from 0 to x (where x is the number of interfaces). The interfaces are listed in alphabetical order on the GUI and CLI. The interface at the top of the interface list is first in alphabetical order by name and has an index of 0. The second interface in the list has an index of 1 and so on. In Transparent mode, the index number foe the management IP address is 0.

Every FortiGate unit physical interface has two MAC addresses: the current hardware address and the permanent hardware address. The permanent hardware address cannot be changed, as it is the actual MAC address of the interface hardware. The current hardware address can be changed, but only when a FortiGate unit is **not** operating in HA. For an operating cluster, the current hardware address of each cluster unit interface is changed to the HA virtual MAC address by the FGCP.

You cannot change an interface MAC address and you cannot view MAC addresses from the system interface CLI command.

You can use the `get hardware nic <interface_name_str>` (or `diagnose hardware deviceinfo nic <interface_str>`) command to display both MAC addresses for any FortiGate interface. This command displays hardware information for the specified interface, including the current hardware address (as `Current_HWaddr`) and the permanent hardware address (as `Permanent_HWaddr`). For some interfaces, the current hardware address is displayed as `MAC`.

Failover protection

FGCP supports three kinds of failover protection:

1. **Device failover:** Automatically replaces a failed device and restarts traffic flow with minimal impact on the network. All subordinate units in an active-passive HA cluster are constantly waiting to negotiate to become primary units. Only the heartbeat packets sent by the primary unit keep the subordinate units from becoming primary units. Each received heartbeat packet resets negotiation timers in the subordinate units. If this timer is allowed to run out because the subordinate units do not receive heartbeat packets from the primary unit, the subordinate units assume that the primary unit has failed, and negotiate to become primary units themselves. The default time interval between HA heartbeats is 200 ms.
2. **Link failover:** Maintains traffic flow if a link fails. In this case, the primary unit does not stop operating, and therefore participates in the negotiation of selecting a new primary unit. The old primary unit then joins the cluster as a subordinate unit. Furthermore, any subordinate units with a link failure are unlikely to become the primary unit in future negotiations.
3. **Session failover:** With session failover (also called session pickup) enabled, the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up-to-date with the traffic currently being processed by the cluster. This helps new primary units resume communication sessions with minimal loss of data, avoiding the need to restart active sessions.

Synchronization of configurations

The FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit. However, there are certain settings that are not synchronized between cluster units:

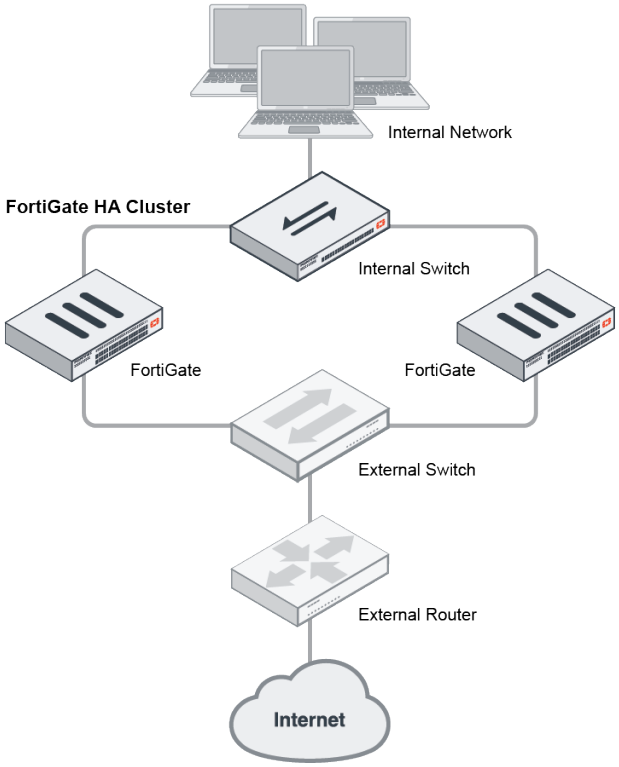
- HA override
- HA device priority
- The virtual cluster priority
- The FortiGate unit host name
- The HA priority setting for a ping server (or dead gateway detection) configuration
- The system interface settings of the HA reserved management interface
- The HA default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command.

You can disable configuration synchronization by entering the following command:

```
config system ha
   set sync-config disable
end
```

The command `execute ha synchronize` can be used to perform a manual synchronization.

The FGCP heartbeat operates on TCP port 703 with an independent IP address not assigned to any FortiGate interface. You can create an FGCP cluster of up to four FortiGate units. Below is an example of FGCP used to create an HA cluster installed between an internal network and the Internet.

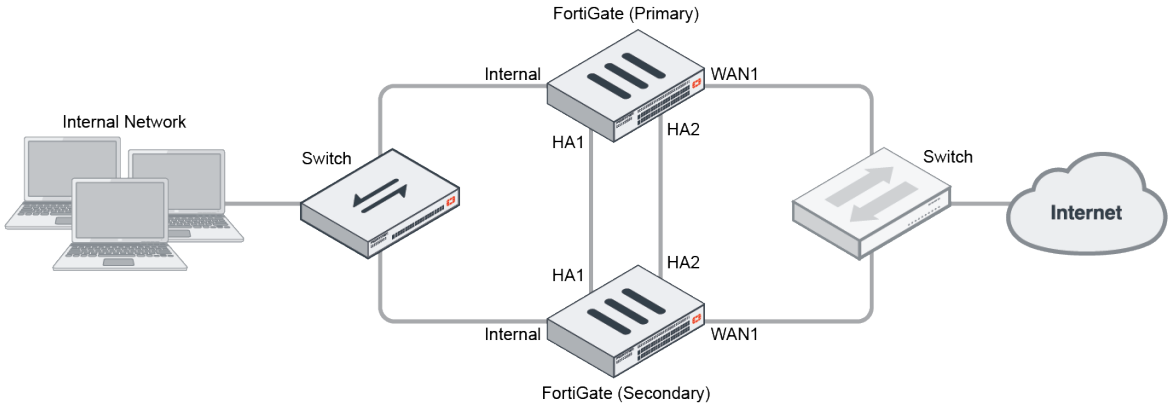


FGCP HA provides a solution for two key requirements of critical enterprise networking: enhanced reliability and increased performance, through device, link, and remote link failover protection. Extended FGCP features include full mesh HA and virtual clustering. You can also fine tune the performance of the FGCP to change how a cluster forms and shares information among cluster units and how the cluster responds to failures.

Before configuring an FGCP HA cluster, make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.

How to set up FGCP clustering

This example describes how to enhance the reliability of a network protected by a FortiGate unit by adding a second FortiGate unit to create a FortiGate Clustering Protocol (FGCP) HA cluster. The FortiGate already on the network will be configured to become the primary unit by increasing its device priority and enabling override. The new FortiGate will be prepared by setting it to factory defaults to wipe any configuration changes. Then it will be licensed, configured for HA, and then connected to the FortiGate already on the network. The new FortiGate becomes the backup unit and its configuration is overwritten by the primary unit.



If you have not already done so, register the primary FortiGate and apply licenses to it before setting up the cluster. This includes FortiCloud activation and FortiClient licensing, and entering a license key if you purchased more than 10 Virtual Domains (VDOMs). You can also install any third-party certificates on the primary FortiGate before forming the cluster.

The FortiGates should be running the same FortiOS firmware version, and their interfaces should not be configured to get their addresses from DHCP or PPPoE.

Configuring the primary FortiGate

1. Connect to the primary FortiGate and go to **Dashboard > Main > System Information**. Change the unit's **Host Name** to identify it as the primary FortiGate.

   You can also enter this CLI command:

   ```
   config system global
      set hostname Primary_FortiGate
   end
   ```

2. You then need to set the HA mode to active-passive. Enter the following CLI command to set the HA mode to active-passive, set a group name and password, increase the device priority to a higher value (for example, 250) and enable override:

   ```
   config system ha
      set mode a-p
      set group-name My-HA-Cluster
      set password
      set priority 250
      set override enable
      set hbdev ha1 50 ha2 50
   end
   ```

   This command also selects ha1 and ha2 to be the heartbeat interfaces, with their priorities set to 50. Enabling override and increasing the priority ensures that this FortiGate should become the primary unit.

You can configure these settings in the GUI under **System > HA**, however the override can *only* be enabled in the CLI.

Configuring the backup FortiGate

1. Enter the CLI command below to reset the new FortiGate to factory default settings (skip this step if the FortiGate is fresh from the factory). It is recommended to set it back to factory defaults to reduce the chance of synchronization problems:
   ```
   execute factoryreset
   ```
2. Make sure to change the firmware running on the new FortiGate to the same version running on the primary unit, register, and apply licenses to it before adding it to the cluster.
3. Then go to **Dashboard > Main > System Information**. Change the unit's **Host Name** to identify it as the backup FortiGate.

   You can also enter this CLI command:
   ```
   config system global
      set hostname Backup_FortiGate
   end
   ```
4. Duplicate the primary unit's HA settings, except make sure to set the backup device's priority to a lower value and do *not* enable override.

Connecting the cluster

Connect the HA cluster as shown in the initial diagram above. Making these connections will disrupt network traffic as you disconnect and re-connect cables.

When connected, the primary and backup FortiGates find each other and negotiate to form an HA cluster. The primary unit synchronizes its configuration with the backup FortiGate. Forming the cluster happens automatically with minimal or no disruption to network traffic.

Heartbeat packet EtherTypes

Normal IP packets are 802.3 packets that have an ethernet type (EtherType) field value of 0x0800. EtherType values other than 0x0800 are understood as level 2 frames rather than IP packets.

By default, HA heartbeat packets use the following EtherTypes:

- HA heartbeat packets for NAT mode clusters use EtherType 0x8890. These packets are used by cluster units to find other cluster units and to verify the status of other cluster units while the cluster is operating. You can change the EtherType of these packets using the `ha-eth-type` option under `config system ha`.
- HA heartbeat packets for Transparent mode clusters use EtherType 0x8891. These packets are used by cluster units to find other cluster units and to verify the status of other cluster units while the cluster is operating. You can change the EtherType of these packets using the `hc-eth-type` option under `config system ha`.
- Session synchronization packets use Ethertype 0x8892. The interfaces used for session synchronization must be connected together, either directly using an appropriate cable (possible if there are only two units in the cluster) or using switches. If one of the interfaces becomes disconnected, the cluster uses the remaining interfaces for session synchronization. If all the session synchronization interfaces become disconnected, session synchronization reverts to using the HA heartbeat link. All session synchronization traffic is between the primary unit and each secondary unit.

Large amounts of session synchronization traffic can increase network congestion. It is recommended that you keep this traffic off of your network by using dedicated connections for it:

```
config system ha
    set session-sync-dev port10 port12
end
```

Session synchronization is always using UDP 708, but this will be encapsulated differently depending on `session-sync-dev` setting. If `session-sync-dev` is specified, the packets will use 0x8892 and will exit over the mentioned port. If `session-sync-dev` is not specified, the packets will use 0x8893 and will exit the heartbeat port.

- HA telnet sessions between cluster units over HA heartbeat links use EtherType 0x8893. The telnet sessions allow an administrator to connect between FortiGates in the cluster using the execute ha manage command. You can change the EtherType of these packets using the `l2ep-eth-type` option under `config system ha`.

Because heartbeat packets are recognized as level 2 frames, the switches and routers on your heartbeat network that connect to heartbeat interfaces must be configured to allow them. If level 2 frames are dropped by these network devices, heartbeat traffic will not be allowed between the cluster units.

Some third-party network equipment may use packets with these EtherTypes for other purposes. For example, Cisco N5K/Nexus switches use EtherType 0x8890 for some functions. When one of these switches receives EtherType 0x8890 packets from an attached cluster unit, the switch generates CRC errors and the packets are not forwarded. As a result, FortiGate units connected with these switches cannot form a cluster.

In some cases, if the heartbeat interfaces are connected and configured so regular traffic flows but heartbeat traffic is not forwarded, you can change the configuration of the switch that connects the HA heartbeat interfaces to allow level2 frames with EtherTypes 0x8890, 0x8891, and 0x8893 to pass.

Alternatively, you can use the following CLI options to change the EtherTypes of the HA heartbeat packets:

```
config system ha
   set ha-eth-type <ha_EtherType _4-digit_hex
   set hc-eth-type <hc_EtherType _4-digit_ex>
   set l2ep-eth-type <l2ep_EtherType _4-digit_hex>
end
```

For example, use the following command to change the EtherType of the HA heartbeat packets from 0x8890 to 0x8895 and to change the EtherType of HA Telnet session packets from 0x8891 to 0x889f:

```
config system ha
   set ha-eth-type 8895
   set l2ep-eth-type 889f
end
```

Enabling or disabling HA heartbeat encryption and authentication

You can enable HA heartbeat encryption and authentication to encrypt and authenticate HA heartbeat packets. HA heartbeat packets should be encrypted and authenticated if the cluster interfaces that send HA heartbeat packets are also connected to your networks.

If HA heartbeat packets are not encrypted the cluster password and changes to the cluster configuration could be exposed and an attacker may be able to sniff HA packets to get cluster information. Enabling HA heartbeat message

authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.

HA heartbeat encryption and authentication are disabled by default. Enabling HA encryption and authentication could reduce cluster performance. Use the following CLI command to enable HA heartbeat encryption and authentication.

```
config system ha
   set authentication enable
   set encryption enable
end
```

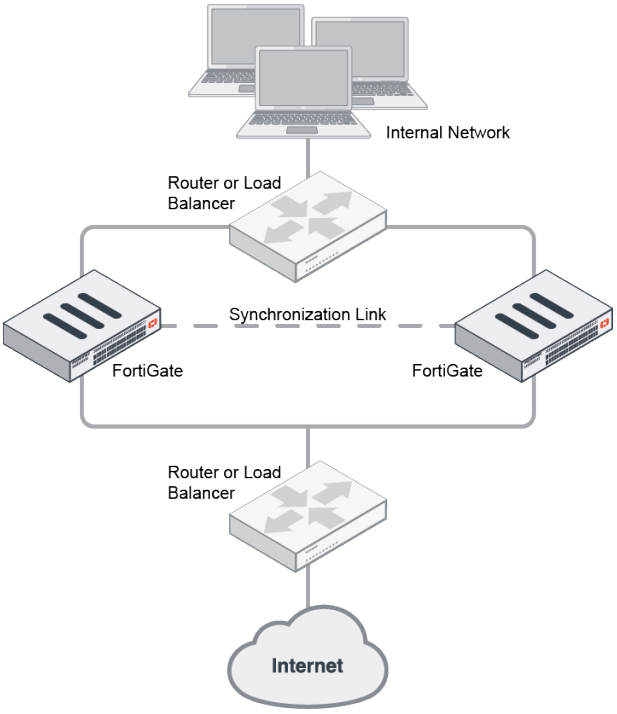
HA authentication and encryption uses AES-128 for encryption and SHA1 for authentication.

FGSP - FortiGate Session Life Support Protocol

FortiGate Session Life Support Protocol (FGSP) distributes sessions between two entities, which could be standalone FortiGates or an FGCP cluster, and performs session synchronization. If one of the peers fails, session failover occurs and active sessions fail over to the peer that is still operating. This failover occurs without any loss of data. Also, the external routers or load balancers will detect the failover and re-distribute all sessions to the peer that is still operating. FortiGates in both entities must be the same model and must be running the same firmware.

You can use the `config system cluster-sync` command to configure FGSP between two entities.

The FortiGate's HA Heartbeat listens on ports TCP/703, TCP/23, or ETH Layer 2/8890.



In previous versions of FortiOS, FGSP was called TCP session synchronization or standalone session synchronization. However, FGSP has been expanded to include both IPv4 and IPv6 TCP, UDP, ICMP, expectation, NAT sessions, and IPsec tunnels.

UDP and ICMP (connectionless) session synchronization

In many configurations, due to their non-stateful nature, UDP and ICMP sessions don't need to be synchronized to naturally failover. However, if it is required, you can configure the FGSP to also synchronize UDP and ICMP sessions by entering the following command:

```
config system ha
   set session-pickup enable
   set session-pickup-connectionless enable
end
```

Expectation (asymmetric) session synchronization

Synchronizing asymmetric traffic can be very useful in situations where multiple Internet connections from different ISPs are spread across two FortiGates.

The FGSP enforces firewall policies for asymmetric traffic, including cases where the TCP 3-way handshake is split between two FortiGates. For example, FGT-A receives the TCP-SYN, FGT-B receives the TCP-SYN-ACK, and FGT-A receives the TCP-ACK. Under normal conditions a firewall will drop this connection since the 3-way handshake was not seen by the same firewall. However two FortiGates with FGSP configured will be able to properly pass this traffic since the firewall sessions are synchronized.

If traffic will be highly asymmetric, as described above, the following command must be enabled on both FortiGates:

```
config system ha
   set session-pickup enable
   set session-pickup-expectation enable
end
```

Security profile inspection with asymmetric and symmetric traffic

Security profile inspection, flow- or proxy-based, is **not** expected to work properly if the traffic in the session is load balanced across more than one FortiGate in either direction. However, flow-based inspection should be used in FGSP deployments.

For symmetric traffic, security profile inspection can be used but with the following limitations:

- No session synchronization for the sessions inspected using proxy-based inspection. Sessions will drop and need to be reestablished after data path failover.
- Sessions with flow-based inspection will failover, and inspection of sessions after a failover may not work.

Improving session synchronization performance

Two HA configuration options are available to reduce the performance impact of enabling session failover (also known as session pickup): reducing the number of sessions that are synchronized by adding a session pickup delay, and using more FortiGate interfaces for session synchronization.

Reducing the number of sessions that are synchronized

If session pickup is enabled, as soon as new sessions are added to one unit session table they are synchronized to the peer unit. Enable the session-pickup-delay CLI option to reduce the number of sessions that are synchronized by synchronizing sessions only if they remain active for more than 30 seconds. Enabling this option could greatly reduce the number of sessions that are synchronized if a peer typically processes very many short duration sessions, which is typical of most HTTP traffic for example.

Use the following command to enable a 30-second session pickup delay:

```
config system ha
   set session-pickup-delay enable
end
```

Enabling session pickup delay means that if a failover occurs more sessions may not be resumed after a failover. In most cases short duration sessions can be restarted with only a minor traffic interruption. However, if you notice too many sessions not resuming after a failover you might want to disable this setting.

Using multiple FortiGate interfaces for session synchronization

Using the `session-sync-dev` option, you can select one or more FortiGate interfaces to use for synchronizing sessions as required for session pickup. Normally session synchronization occurs over the HA heartbeat link. Using this HA option means only the selected interfaces are used for session synchronization and not the HA heartbeat link. If you select more than one interface, session synchronization traffic is load balanced among the selected interfaces.

Moving session synchronization from the HA heartbeat interface reduces the bandwidth required for HA heartbeat traffic and may improve the efficiency and performance of the FGSP deployment, especially if the peers are synchronizing a large number of sessions. Load balancing session synchronization among multiple interfaces can further improve performance and efficiency if the peers are synchronizing a large number of sessions.

Use the following command to perform peer session synchronization using the port10 and port12 interfaces:

```
config system ha
   set session-sync-dev port10 port12
end
```

Session synchronization packets use Ethertype 0x8892. The interfaces to use for session synchronization must be connected together either directly using the appropriate cable (possible if there are only two units in the deployment) or using switches. If one of the interfaces becomes disconnected, the peer uses the remaining interfaces for session synchronization. If all of the session synchronization interfaces become disconnected, session synchronization reverts back to using the HA heartbeat link.

Since large amounts of session synchronization traffic can increase network congestion, it is recommended that you keep this traffic off of your network by using dedicated connections for it.

"Unsetting" `session-sync-dev` by entering `unset session-syn-dev` has the following effects:

- Session synchronization will use the ports defined as HA heartbeat interfaces (`set hbdev`).
- Session synchronization packets will be sent over UDP/708 instead of Ethertype 0x8892.

NAT session synchronization

NAT sessions are not synchronized by default. You can enable NAT session synchronization by entering the following command:

```
config system ha
   set session-pickup enable
   set session-pickup-nat enable
end
```

After a failover with this configuration, all sessions that include the IP addresses of interfaces on the failed FortiGate unit will have nowhere to go since the IP addresses of the failed FortiGate unit will no longer be on the network. If you want NAT sessions to resume after a failover you should not configure NAT to use the destination interface IP address, since the FGSP FortiGate units have different IP addresses. To avoid this issue, you should use IP pools with the type set to `overload` (which is the default IP pool type), as shown in the example below:

```
config firewall ippool
   edit FGSP-pool
      set type overload
      set startip 172.20.120.10
      set endip 172.20.120.20
   next
```

```
end
```

In NAT mode, only sessions for route mode security policies are synchronized. FGSP is also available for FortiGate units or virtual domains operating in transparent mode. Only sessions for normal transparent mode policies are synchronized.

IPsec tunnel synchronization

When you use the `config system cluster-sync` command to enable FGSP, IPsec keys and other runtime data are synchronized between peer units. This means that if one of the peer units goes down, the peer unit that is still operating can quickly get IPsec tunnels re-established without re-negotiating them. However, after a failover, all existing tunnel sessions on the failed FortiGate have to be restarted on the still operating FortiGate.

IPsec tunnel sync supports both static and dialup IPsec tunnels. The interfaces on both FortiGates that are tunnel endpoints must have the same IP addresses and external routers must be configured to load balance IPsec tunnel sessions to the FortiGates in the deployment.

Automatic session synchronization after peer reboot

The following command allows you to configure an automatic session synchronization after a peer FGSP unit has rebooted. FGSP will send out heartbeat signals (every 1–10 seconds, as shown below) if one FortiGate is rebooting and the other FortiGate fails.

To configure automatic session synchronization:

```
config system session-sync
   edit 1
      set down-intfs-before-sess-sync <interfaces> -- List of interfaces to be turned down
           before session synchronization is complete.
      set-hb-interval <integer> -- (1 - 10 seconds)
      set hb-lost-threshold <integer> -- (1 - 10)
   next
end
```

FGFM - FortiGate to FortiManager Protocol

The FortiGate to FortiManager (FGFM) protocol is designed for FortiGate and FortiManager deployment scenarios, especially where NAT is used. These scenarios include the FortiManager on public internet while the FortiGate unit is behind NAT, FortiGate unit is on public internet while FortiManager is behind NAT, or both FortiManager and FortiGate unit have routable IP addresses.

The FortiManager unit's Device Manager uses FGFM to create new device groups, provision and add devices, and install policy packages and device settings.

Port 541 is the default port used for FortiManager traffic on the internal management network. Port 542 is also used to establish IPv6 connection.

Adding a FortiGate to the FortiManager

Adding a FortiGate unit to a FortiManager requires configuration on both devices. This section describes the basics to configure management using a FortiManager device.

FortiGate configuration

Adding a FortiGate unit to FortiManager will ensure that the unit will be able to receive antivirus and IPS updates and allow remote management through the FortiManager system, or FortiCloud service. The FortiGate unit can be in either NAT or transparent mode. The FortiManager unit provides remote management of a FortiGate unit over TCP port 541.

You must first enable *Central Management* on the FortiGate so management updates to firmware and FortiGuard services are available:

1. Go to *Security Fabric* > *Settings*.
2. Enable *Central Management* and set *Type* to *FortiManager*.
3. Enter the FortiManager's *IP/Domain Name* in the field provided.

To configure the previous steps in the CLI, enter the following - note that `fmg` can be set to either an IP address or FQDN:

```
config system central-management
   set fmg <string>
end
```

To use the registration password, enter the following:

```
execute central-mgmt register-device <fmg-serial-no> <fmg-register-password>
```

FGFM is also used in ADOMs (Administrative Domains) set to Normal Mode. Normal Mode has Read/Write privileges, where the administrator is able to make changes to the ADOM and manage devices from the FortiManager. FortiGate units in the ADOM will query their own configuration every five seconds. If there has been a configuration change, the FortiGate unit will send a revision on the change to the FortiManager using the FGFM protocol.

To configure central management on the FortiGate unit, enter the following on the FortiGate:

```
config system central-management
   set mode normal
   set fortimanager-fds-override enable
   set fmg <string>
```

```
end
```

Configuring an SSL connection

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for *High*, *Medium*, and *Low* follow the openssl definitions below:

Encryption level	Key strength	Algorithms used
High	Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.	DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3- MD5:DHE-RSA-AES128-SHA:AES128-SHA
Medium	Key strengths of 128 bit encryption.	RC4-SHA:RC4-MD5:RC4-MD
Low	Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites.	EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5

An SSL connection can be configured between the two devices and an encryption level selected. To configure the connection in the CLI, enter the following:

```
config system central-management
   set status enable
   set enc-algorithm (default | high | low)
end
```

Note that `default` automatically sets high and medium encryption algorithms.

FortiManager configuration

Use the *Device Manager* pane to add, configure, and manage devices.

You can add existing operational devices, unregistered devices, provision new devices, and add multiple devices at a time.

Adding an operating FortiGate HA cluster to the *Device Manager* pane is similar to adding a standalone device. Type the IP address of the primary device. The FortiManager will handle the cluster as a single managed device.

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, enter the following CLI command:

```
diagnose dvm supported-platforms list
```

See the FortiManager Administration Guide for full details on adding devices, under **Device Manager**.

Replacing a FortiGate in a FortiManager configuration

FGFM can be used in order to re-establish a connection between a FortiGate unit and a FortiManager configuration. This is useful for if you need a FortiGate unit replaced following an RMA hardware replacement. This applies to a FortiGate running in HA as the primary units; it does not apply to subordinate units.

When the FortiGate unit is replaced, perform a Device Manager Connectivity check or Refresh on the FortiManager to establish the FGFM management tunnel to the FortiGate. If it fails to establish, you can force the tunnel by executing the following command on the FortiManager:

```
execute fgfm reclaim-dev-tunnel <device_name>
```

Debugging FGFM on FortiManager

- To display diagnostic information for troubleshooting, set the debug level of the FGFM daemon (enter a device name to only show messages related to that device):
  ```
  diagnose debug application fgfmsd <integer> <device_name>
  ```
- To view installation session, object, and session lists:
  ```
  diagnose fgfm install-session
  diagnose fgfm object-list
  diagnose fgfm session-list <device_ID>
  ```
- To reclaim a management tunnel (device name is optional):
  ```
  execute fgfm reclaim-dev-tunnnel <device_name>
  ```
- To view the link-local address assigned to the FortiManager:
  ```
  diagnose fmnetwork interface list
  ```

Debugging FGFM on FortiGate

- To view information about the Central Management System configuration:
  ```
  get system central-management
  ```
- To produce realtime debugging information:
  ```
  diagnose debug application fgfmd -1
  ```
- To view the link-local address assigned to the FortiManager:
  ```
  diagnose fmnetwork interface list
  ```

FortiOS DHCP options and auto DNS hostname for FortiManager details

A diagnose command can be used to show the FortiManager autodiscovery status for the secure sending of FortiManager details to FortiGate.

FortiGate is occasionally required in large deployments where a Zero Touch Provisioning (ZTP) of the unit is required.

Rather than using the CLI Console to configure system settings one at a time, ZTP can help to reduce errors, save time in automated device configuration, and enhance scalability.

This functionality is designed to work even in a closed network with no Internet access.

To verify the FortiManager autodiscovery status, use the following command:

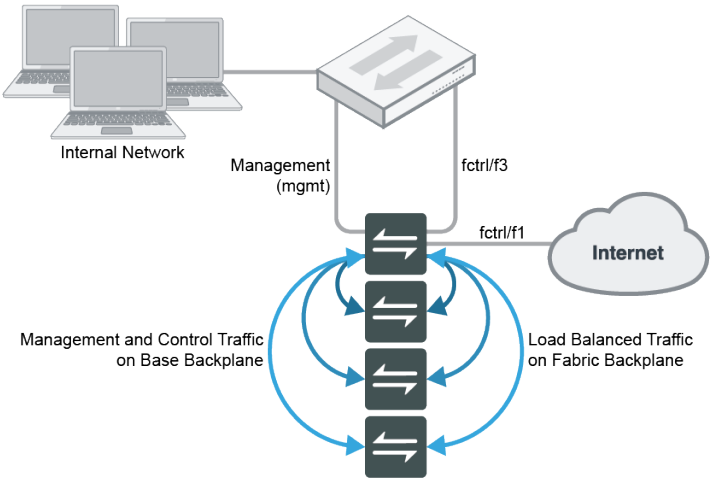
```
diagnose fdsm fmg-auto-discovery-status
```

SLBC - Session-aware Load Balancing Cluster

The Session-aware Load Balancing Cluster (SLBC) protocol is used for clusters consisting of FortiControllers that perform load balancing of both TCP and UDP sessions. As session-aware load balancers, FortiControllers, with FortiASIC DP processors, are capable of directing any TCP or UDP session to any worker installed in the same chassis. It also means that more complex networking features such as NAT, fragmented packets, complex UDP protocols and others such as Session Initiation Protocol (SIP), a communications protocol for signaling and controlling multimedia communication sessions, can be load balanced by the cluster.

Currently, only three FortiController models are available for SLBC: FortiController-5103B, FortiController-5903C, and FortiController-5913C. Supported workers include the FortiGate-5001B, 5001C, 5101C, and 5001D.

FortiGate-7000 series products also support SLBC.



You cannot mix FGCP and SLBC clusters in the same chassis.

An SLBC with two FortiControllers can operate in active-passive mode or dual mode. In active-passive mode, if the active FortiController fails, traffic is transferred to the backup FortiController. In dual mode both FortiControllers load balance traffic and twice as many network interfaces are available.

SLBC clusters consisting of more than one FortiController use the following types of communication between FortiControllers to operate normally:

- **Heartbeat:** Allows the FortiControllers in the cluster to find each other and share status information. If a FortiController stops sending heartbeat packets it is considered down by other cluster members. By default heartbeat traffic uses VLAN 999.
- **Base control:** Communication between FortiControllers on subnet 10.101.11.0/255.255.255.0 using VLAN 301.
- **Base management:** Communication between FortiControllers on subnet 10.101.10.0/255.255.255.0 using VLAN 101.
- **Session synchronization:** If one FortiController fails, session synchronization allows another to take its place and maintain active communication sessions. FortiController-5103B session sync traffic uses VLAN 2000.

FortiController-5903C and FortiController-5913C session sync traffic between the FortiControllers in slot 1 uses VLAN 1900 and between the FortiControllers in slot 2 uses VLAN 1901. You cannot change these VLANs.

Note that SLBC does not support session synchronization between workers in the same chassis. The FortiControllers in a cluster keep track of the status of the workers in their chassis and load balance sessions to the workers. If a worker fails the FortiController detects the failure and stops load balancing sessions to that worker. The sessions that the worker is processing when it fails are lost.

Changing the heartbeat VLAN

To change the VLAN from the FortiController GUI, from the *System Information* dashboard widget, beside *HA Status*, select *Configure*. Change the *VLAN to use for HA heartbeat traffic(1-4094)* setting.

You can also change the heartbeat VLAN ID from the FortiController CLI. For example, to change the heartbeat VLAN ID to `333`, enter the following:

```
config system ha
   set hbdev-vlan-id 333
end
```

Setting the mgmt interface as a heartbeat interface

To add the mgmt interface to the list of heartbeat interfaces used, on the FortiController-5103B, enter the following:

```
config system ha
   set hbdev b1 b2 mgmt
end
```

This example adds the mgmt interface for heartbeats to the B1 and B2 interfaces. The B1 and B2 ports are recommended because they are 10G ports and the mgmt interface is a 100Mbit interface.

FortiController-5103B is currently the only model that allows its mgmt interface to be added to the heartbeat interfaces list.

Changing the heartbeat interface mode

By default, only the first heartbeat interface (usually B1) is used for heartbeat traffic. If this interface fails on any of the FortiControllers in a cluster, then the second heartbeat interface is used (B2).

To simultaneously use all heartbeat interfaces for heartbeat traffic, enter the following command:

```
config load-balance-setting
   set base-mgmt-interface-mode active-active
end
```

Changing the base control subnet and VLAN

You can change the base control subnet and VLAN from the FortiController CLI. For example, to change the base control subnet to `10.122.11.0/255.255.255.0` and the VLAN ID to `320`, enter the following:

```
config load-balance setting
   set base-ctrl-network 10.122.11.0 255.255.255.0
   config base-ctrl-interfaces
```

```
      edit b1
      set vlan-id 320
      next
      edit b2
      set vlan-id 320
   end
end
```

Changing the base management subnet and VLAN

You can change the base management subnet from the FortiController GUI under *Load Balance* > *Config* and changing the *Internal Management Network*.

You can also change the base management subnet and VLAN ID from the FortiController CLI. For example, to change the base management subnet to `10.121.10.0/255.255.255.0` and the VLAN to `131`, enter the following:

```
config load-balance setting
   set base-mgmt-internal-network 10.121.10.0 255.255.255.0
   config base-mgt-interfaces
      edit b1
      set vlan-id 131
      next
      edit b2
      set vlan-id 131
   end
end
```

If required, you can use different VLAN IDs for the B1 and B2 interface.

Changing this VLAN only changes the VLAN used for base management traffic between chassis. Within a chassis the default VLAN is used.

Enabling and configuring the session sync interface

To enable session synchronization in a two chassis configuration, enter the following command:

```
config load-balance setting
   set session-sync enable
end
```

You will then need to select the interface to use for session sync traffic. The following example sets the FortiController-5103B session sync interface to `F4`:

```
config system ha
   set session-sync-port f4
end
```

The FortiController-5903C and FortiController-5913C use B1 and B2 as the session sync interfaces so no configuration changes are required.

FGCP to SLBC migration

You can convert an FGCP virtual cluster (with VDOMs) to an SLBC cluster. The conversion involves replicating the VDOM, interface, and VLAN configuration of the FGCP cluster on the SLBC cluster primary worker, then backing up the configuration of each FGCP cluster VDOM. Each of the VDOM configuration files is manually edited to adjust interface

names. These modified VDOM configuration files are then restored to the corresponding SLBC cluster primary worker VDOMs.

For this migration to work, the FGCP cluster and the SLBC workers must be running the same firmware version, the VDOMs are enabled on the FGCP cluster, and the SLBC workers have been registered and licensed. However, the FGCP cluster units do not have to be the same model as the SLBC cluster workers.

Only VDOM configurations are migrated. You have to manually configure primary worker management and global settings.

Conversion steps

1. Add VDOM(s) to the SLBC primary worker with names that match those of the FGCP cluster.
2. Map FGCP cluster interface names to SLBC primary worker interface names. For example, you can map the FGCP cluster port1 and port2 interfaces to the SLBC primary worker fctl/f1 and fctl/f2 interfaces. You can also map FGCP cluster interfaces to SLBC trunks, and include aggregate interfaces.
3. Add interfaces to the SLBC primary worker VDOMs according to your mapping. This includes moving SLBC physical interfaces into the appropriate VDOMs, creating aggregate interfaces, and creating SLBC trunks if required.
4. Add VLANs to the SLBC primary worker that match VLANs in the FGCP cluster. They should have the same names as the FGCP VLANs, be added to the corresponding SLBC VDOMs and interfaces, and have the same VLAN IDs.
5. Add inter-VDOM links to the SLBC primary worker that match the FGCP cluster.
6. Backup the configurations of each FGCP cluster VDOM, and SLBC primary worker VDOM.
7. Use a text editor to replace the first four lines of each FGCP cluster VDOM configuration file with the first four lines of the corresponding SLBC primary worker VDOM configuration file. Here are example lines from an SLBC primary worker VDOM configuration file:
   ```
   #config-version=FG-5KB-5.02-FW-build670-150318:opmode=0:vdom=1:user=admin
   #conf_file_ver=2306222306838080295
   #buildno=0670
   #global_vdom=0:vd_name=VDOM1
   ```
8. With the text editor, edit each FGCP cluster VDOM configuration file and replace all FGCP cluster interface names with the corresponding SLBC worker interface names, according to the mapping you created in step 2.
9. Set up a console connection to the SLBC primary worker to check for errors during the following steps.
10. From the SLBC primary worker, restore each FGCP cluster VDOM configuration file to each corresponding SLBC primary worker VDOM.
11. Check the following on the SLBC primary worker:
    - Make sure `set type fctrl-trunk` is enabled for SLBC trunk interfaces.
    - Enable the global and management VDOM features that you need, including SNMP, logging, connections to FortiManager, FortiAnalyzer, and so on.
    - If there is a FortiController in chassis slot 2, make sure the worker base2 interface status is up.
    - Remove `snmp-index` entries for each interface.
    - Since you can manage the workers from the FortiController you can remove management-related configurations using the worker mgmt1 and mgmt2 interfaces (Logging, SNMP, admin access, etc.) if you are not going to use these interfaces for management.

How to set up SLBC with one FortiController-5103B

This example describes the basics of setting up a Session-aware Load Balancing Cluster (SLBC) that consists of one FortiController-5103B, installed in chassis slot 1, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5.

This SLBC configuration can have up to eight 10Gbit network connections.

Configuring the hardware

1. Install a FortiGate-5000 series chassis and connect it to power. Install the FortiController in slot 1. Install the workers in slots 3, 4, and 5. Power on the chassis.
2. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally. (To check normal operation LED status see the FortiGate-5000 series documents available here.)
3. Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

Configuring the FortiController

To configure the FortiController, you will need to either connect to the FortiController GUI or CLI with the default IP address of http://192.168.1.99. Log in using the admin account (no password).

1. Add a password for the admin account. Use the *Administrators* widget in the GUI, or enter the following CLI command:
```
config admin user
   edit admin
      set password <password>
   next
end
```
2. Change the FortiController mgmt interface IP address. Use the *Management Port* widget in the GUI, or enter the following CLI command:
```
config system interface
   edit mgmt
      set ip 172.20.120.151/24
   next
end
```
3. If you need to add a default route for the management IP address, enter the following command:
```
config route static
   edit route 1
      set gateway 172.20.121.2
   next
end
```
4. To set the chassis type that you are using, enter the following CLI command:
```
config system global
   set chassic-type fortigate-5140
end
```
5. Go to *Load Balance* > *Config* and add workers to the cluster by selecting *Edit* and moving the slots that contain workers to the *Member* list. The Config page shows the slots in which the cluster expects to find workers. Since the workers have not been configured yet, their status is *Down*.
   Configure the *External Management IP/Netmask*. Once the workers are connected to the cluster, you can use this IP address to manage and configure them.
6. You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:
```
config load-balance setting
   config slots
      edit 3
      next
      edit 4
      next
      edit 5
```

```
      next
    end
  end
```

7. You can also enter the following command to configure the external management IP/Netmask and management access to the following address:
```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

Adding the workers

Before you begin adding workers to the cluster, make sure you enter the `execute factoryreset` command in the CLI so the workers are set to factory default settings. If the workers are going to run FortiOS Carrier, add the FortiOS Carrier licence instead - this will reset the worker to factory default settings.

Also make sure to register and apply licenses to each worker, including FortiClient licensing, FortiCloud activation, and entering a license key if you purchased more than 10 Virtual Domains (VDOMs). You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers. FortiToken licenses can be added at any time, which will also synchronize across all of the workers.

1. Log in to each of the worker's CLI and enter the following CLI command to set the worker to operate in FortiController mode:
```
config system elbc
  set mode fortincontroller
end
```
   Once the command is entered, the worker restarts and joins the cluster.
2. On the FortiController, go to *Load Balance* > *Status*. You will see the workers appear in their appropriate slots. The worker in the lowest slot number usually becomes the primary unit.

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the *External Management IP*. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

Managing the devices in an SLBC with the external management IP

The External Management IP address is used to manage all of the individual devices in a SLBC by adding a special port number. This special port number begins with the standard port number for the protocol you are using and is followed by two digits that identify the chassis number and slot number. The port number can be calculated using the following formula:

service_port x 100 + (chassis_id - 1) x 20 + slot_id

Where:

- **service_port** is the normal port number for the management service (80 for HTTP, 443 for HTTPS and so on).
- **chassis_id** is the chassis ID specified as part of the FortiController HA configuration and can be 1 or 2.
- **slot_id** is the number of the chassis slot.

By default, chassis 1 is the primary chassis and chassis 2 is the backup chassis. However, the actual primary chassis is the one with the primary FortiController, which can be changed independently of the chassis number. Additionally, the **chassis_id** is defined by the chassis number, *not* whether the chassis contains the primary FortiController.

Some examples:

- HTTPS, chassis 1, slot 2: 443 x 100 + (1 - 1) x 20 + 2 = 44300 + 0 + 2 = 44302:
  browse to: https://172.20.120.100:44302
- HTTP, chassis 2, slot 4: 80 x 100 + (2 - 1) x 20 + 4 = 8000 + 20 + 4 = 8024:
  browse to http://172.20.120.100/8024
- HTTPS, chassis 1, slot 10: 443 x 100 + (1 - 1) x 20 + 10 = 44300 + 0 + 10 = 44310:
  browse to https://172.20.120.100/44310

Single chassis or chassis 1 special management port numbers

Slot number	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 1	8001	44301	2301	2201	16101
Slot 2	8002	44302	2302	2202	16102
Slot 3	8003	44303	2303	2203	16103
Slot 4	8004	44304	2304	2204	16104
Slot 5	8005	44305	2305	2205	16105
Slot 6	8006	44306	2306	2206	16106
Slot 7	8007	44307	2307	2207	16107
Slot 8	8008	44308	2308	2208	16108
Slot 9	8009	44309	2309	2209	16109
Slot 10	8010	44310	2310	2210	16110
Slot 11	8011	44311	2311	2211	16111
Slot 12	8012	44312	2312	2212	16112
Slot 13	8013	44313	2313	2213	16113
Slot 14	8014	44314	2314	2214	16114

Chassis 2 special management port numbers

Slot number	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 1	8021	44321	2321	2221	16121
Slot 2	8022	44322	2322	2222	16122
Slot 3	8023	44323	2323	2223	16123

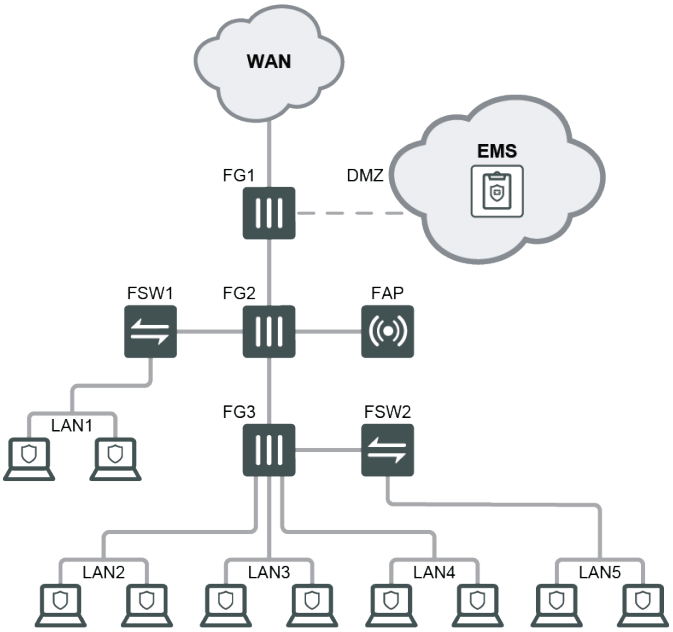
Slot number	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 4	8024	44324	2324	2224	16124
Slot 5	8025	44325	2325	2225	16125
Slot 6	8026	44326	2326	2226	16126
Slot 7	8027	44327	2327	2227	16127
Slot 8	8028	44328	2328	2228	16128
Slot 9	8029	44329	2329	2229	16129
Slot 10	8030	44330	2330	2230	16130
Slot 11	8031	44331	2331	2231	16131
Slot 12	8032	44332	2332	2232	16132
Slot 13	8033	44333	2333	2233	16133
Slot 14	8034	44334	2334	2234	16134

For more detailed information regarding FortiController SLBC configurations, see the FortiController Session-Aware Load Balancing Cluster Guide.

Fortinet Security Fabric

The Fortinet Security Fabric spans across an entire network linking different security sensors and tools together to collect, coordinate, and respond to malicious behavior in real time. Security Fabric can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS). Security Fabric supports FortiOS 5.4.1+, FortiSwitchOS 3.3+, and FortiClient 5.4.1+.

Port TCP/8009 is the port FortiGate uses for incoming traffic from the FortiClient Portal, as user information (such as IP address, MAC address, avatar, and other profile information) is automatically synchronized to the FortiGate and EMS.



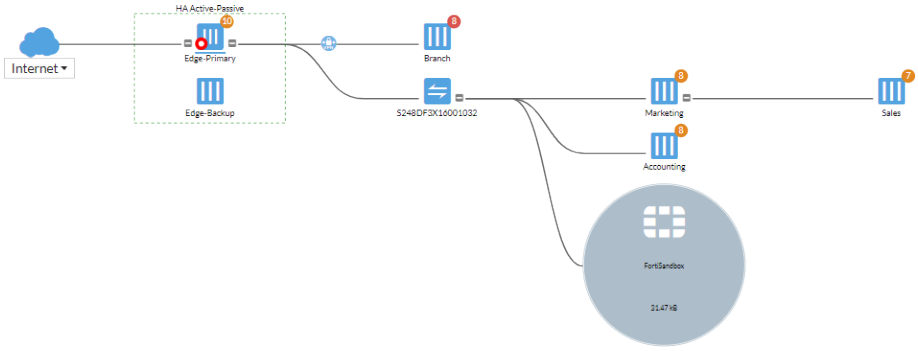
The brief example below assumes that FortiGatw Telemetry has been enabled on the top-level FortiGate (**FGT1**), OSPF routing has been configured, and that policies have been created for all FortiGate units to access the Internet.

For more details on how to configure a security fabric between FortiGate units, see Fortinet Security Fabric.

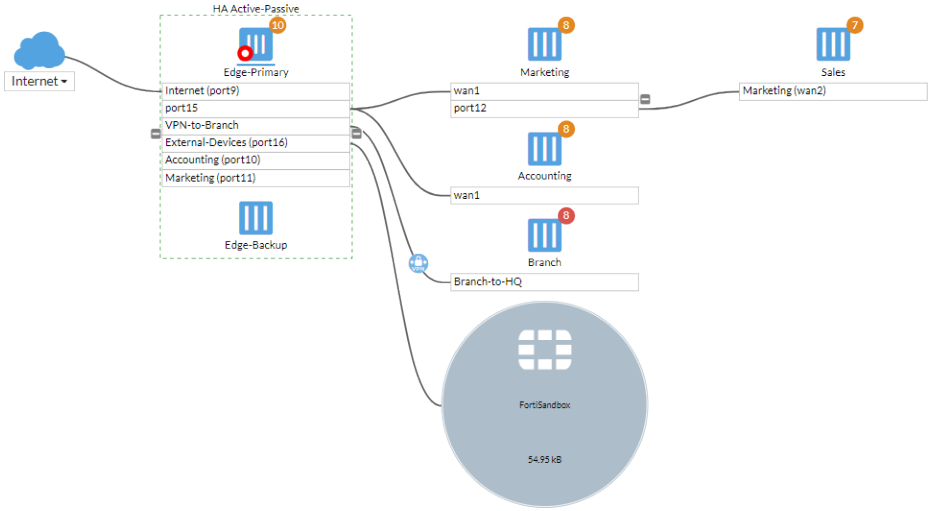
Enabling Security Fabric on the FortiGate:

1. On the upstream FortiGate (FGT1), go to *Security Fabric* > *Settings* and enable *FortiGate Telemetry*.
2. Enter a *Group name* and *Group password* for the fabric.
3. On a downstream FortiGate (such as FGT2 or FGT3), configure the same fabric settings as were set on FGT1.
4. Enable *Connect to upstream FortiGate*.
   Be sure you do not enable this on the topmost-level FortiGate (in this example, FGT1).
5. In *FortiGate IP*, enter the FGT1 interface that has *Security Fabric Connection* enabled. The *Management IP* can be left to use the WAN IP or optionally specified.
   Once set up, you can view your network's Security Fabric configuration under *Security Fabric* through two topology dashboards.

6. On the top-level FortiGate, go to *Security Fabric* > *Physical Topology*. This dashboard shows a visualization of all access layer devices in the fabric.



7. Go to *Security Fabric* > *Physical Topology* to view information about the interfaces (logical or physical) that each device in the fabric is connected to.



Other Security Fabric configurations for your network are available in the Fortinet Cookbook: Fortinet Security Fabric.

FortiGuard

The FortiGuard communication protocol is used by FortiGuard to communicate with Fortinet devices.

FortiGuard services can be purchased and registered to your FortiGate unit. The FortiGate must be connected to the internet in order to automatically connect to the FortiGuard Distribution Network (FDN) to validate the license and download FDN updates.

If accepting push updates is enabled, the FDN sends notice that a FortiGuard AV and IPS update is available on UDP/9443.

When the FortiGuard protocol is configured to use HTTPS (default), third party certificate verification and OCSP stapling check is implemented for all FortiGuard servers that are connected to FortiOS. The default FortiGuard access mode is anycast.

See Anycast and unicast services on page 61 for a list of services.

For more information, see FortiGuard in the FortiOS Administration guide.

Submission of malware statistics to FortiGuard

FortiGates periodically send encrypted Antivirus, IPS, botnet IP list, and Application Control event statistics to FortiGuard. Included with these malware statistics is the IP address and serial number of the FortiGate and the country in which the FortiGate is located. This information is never shared with external parties (Fortinet Privacy Policy).

The malware statistics are used to improve various aspects of FortiGate malware protection. For example, antivirus data allow FortiGuard to determine what viruses are currently active. Signatures for those viruses are kept in the Active AV Signature Database that is used by multiple Fortinet products. Inactive virus signatures are moved to the Extended AV Signature Database (see Configuring antivirus and IPS options in the FortiOS Administration guide.). When events for inactive viruses start appearing in the malware data, the signatures are moved back into the AV Signature Database.

The FortiGate and FortiGuard servers go through a 2-way SSL/TLS 1.2 authentication before any data is transmitted. The certificates used in this process must be trusted by each other and signed by Fortinet CA server.

Fortinet products only accepts data from authorized FortiGuard severs. Fortinet products use DNS to find FortiGuard servers and periodically update their FortiGate server list. All other servers are provided by a list that is updated through the encrypted channel.

Malware statistics are accumulated and sent periodically (by default every 60 minutes).

To configure sharing this information:

```
config system global
   set fds-statistics {enable | disable}
   set fds-statistics-period <minutes>
end
```

The submission of malware data is in accordance with Fortinet's “Automatically-Collected Information” detailed in the Fortinet Privacy Policy, and the purpose of this collection is outlined in the “Use of your Information” section of the privacy policy.

There is no sensitive or personal information included in these submissions. Only malware statistics are sent.

Fortinet uses the malware statistics collected in this manner to improve the performance of the FortiGate services and to display statistics on the Fortinet Support website for customers registered FortiGate devices.

Fortinet may also publish or share statistics or results derived from this malware data with various audiences. The malware statistics shared in this way do not include any customer data.

In addition to secure submission of statistics to FortiGuard, there are other mechanisms in place to prevent unauthorized FortiGuard updates from clients:

- The server certificate has to be authenticated by FortiGates, and it only trusts Fortinet's root certificate.
- Proprietary encryption (including FGCP, an application-level proprietary protocol) that only Fortinet's own servers/devices can prepare.

FortiGates can only accept data from Fortinet's own list of servers, although the list can be updated through previously connected servers. DNS is used on the initial server, but all other servers are provided by a list that is updated through SSL, meaning that only FortiGates accept data from those servers.

Automatic update at every GUI login

FortiGates running FortiOS 5.6.1 and above may perform automatic "update now" updates when one of the "core" licenses is unavailable: Application Control, IPS, or Antivirus. Please note that this automatic update is triggered even if the following CLI command is set:

```
config system autoupdate schedule
   set status disable
end
```

FortiGuard related CLI commands

To set the FDN push update port:

```
config system autoupdate push-update
   set port <integer>
end
```

To set the proxy server port that the FortiGate will use to connect to the FortiGuard Distribution Network (FDN):

```
config system autoupdate tunneling
   set port <integer>
end
```

To set the port that scheduled FortiGuard service updates will be received on:

```
config system fortiguard
   set port {53 | 8888 | 80}
```

```
end
```

To enable or disable ports that are used for HTTPS/HTTP override authentication and disable user overrides:

```
config webfilter fortiguard
   set close-ports {enable | disable}
end
```

For more information, including FortiGuard execute commands used to manage FortiCloud domains and operations, see the CLI Reference.

Anycast and unicast services

The following services are accessed by FortiGate:

Service	Non-Anycast FQDN addresses	Anycast Domain name
FortiGuard Object download	update.fortiguard.net	globalupdate.fortinet.net
Querying service (web-filtering, anti-spam ratings) over HTTPS	securewf.fortiguard.net	globalguardservice.fortinet.net
Querying service (web-filtering, anti-spam ratings) over UDP	service.fortiguard.net	Service only in Unicast
Device info Collection	Service only in Anycast	globaldevcollect.fortinet.net
Device info Query	Service only in Anycast	globaldevquery.fortinet.net
FortiGate Cloud logging	logctrl1.fortinet.com	globallogctrl.fortinet.net
FortiGate Cloud management	mgrctrl1.fortinet.com	globalmgrctrl.fortinet.net
FortiGate Cloud messaging	msgctrl1.fortinet.com	globalmsgctrl.fortinet.net
FortiGate Cloud sandbox	aptctrl1.fortinet.com	globalaptctrl.fortinet.net
Product API used by OCVPN registration and GUI icon download	productapi.fortinet.net	globalproductapi.fortinet.net
FortiCare registration	directregistration.fortinet.com	globalregistration.fortinet.net
Secure DNS	sdns.fortinet.net	globalsdns.fortinet.net
FortiCloud FortiClient	forticlient.fortinet.net	globalfctupdate.fortinet.net
FortiMobile Tokens	directregistration.fortinet.com	globalftm.fortinet.net
EMS cloud	forticlient-emsproxy.forticloud.com	Service only in Unicast
DDNS	ddns.fortinet.net	globalddns.fortinet.net
GeoIP	gip.fortinet.net	globalgip.fortinet.net
IP blocklist	ipbl.fortinet.net	N/A

FortiLink

FortiGate units can be used to remotely manage FortiSwitch units, which is also known as using a FortiSwitch in FortiLink mode. FortiLink defines the management interface and the remote management protocol between the FortiGate and FortiSwitch.

For more information see the Devices Managed by FortiOS guide.

FortiOS WAN optimization

Organizations with multiple locations or businesses using the cloud can provide license-free WAN optimization using FortiOS.

WAN Optimization is a comprehensive solution that maximizes your WAN performance and provides intelligent bandwidth management and unmatched consolidated security performance. WAN optimization reduces your network overhead and removes unnecessary traffic for a better overall performance experience. Efficient use of bandwidth and better application performance will remove the need for costly WAN link upgrades between data centers and other expensive solutions for your network traffic growth.

WAN optimization is available on FortiGate models with internal storage that also support SSL acceleration. Internal storage includes high-capacity internal hard disks, AMC hard disk modules, FortiGate Storage Modules (FSMs) or over 4 GB of internal flash storage.

WAN optimization tunnels use port 7810.

The following features below are available through WAN optimization:

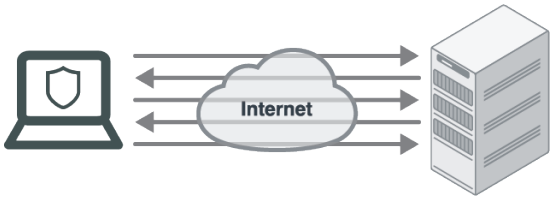
Protocol optimization

Protocol optimization is effective for applications designed for the LAN that do not function well on low bandwidth, high latency networks. FortiOS protocol optimization improves the efficiency of CIFS, FTP, HTTP, MAPI, and general TCP sessions.

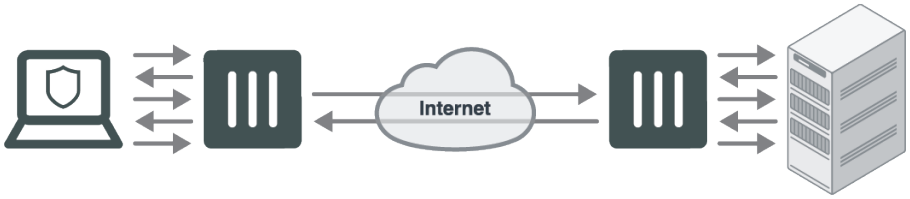
CIFC, for example, requires many background transactions to successfully transfer a single file. When transferring the file, CIFS sends small chunks of data and waits sequentially for each chunk's arrival and acknowledgment before sending the next chunk. This large amount of requests and acknowledgements of traffic can delay transfers. WAN Optimization removes this complexity and improves the efficiency of transferring the file.

TCP protocol optimization uses techniques such as SACK support, window scaling and window size adjustment, and connection pooling to remove common WAN TCP bottlenecks.

Regular bandwidth usage



Improved bandwidth usage with FortiGate protocol optimization



Byte caching

Byte caching improves caching by accelerating the transfer of similar, but not identical content. Byte caching reduces the amount of data crossing the WAN when multiple different emails with the same or similar attachments or different versions of an attachment are downloaded from a corporate email server to different locations over the WAN.

Byte caching breaks large units of application data, such as email attachments or file downloads, into smaller chunks of data. Each chunk of data is labeled with a hash, and chunks with their respective hashes are stored in a database on the local FortiGate unit. When a remote user requests a file, WAN optimization sends the hashes, rather than the actual data. The FortiGate unit at the other end of the WAN tunnel reassembles the data from its own hash database, only downloading the chunks it is missing. Deduplication, or the process of eliminating duplicate data, will reduce space consumption.

Byte caching is not application specific, and assists by accelerating all protocols supported by WAN optimization.

Web caching

WAN optimization reduces download times of content from central files repositories through web caching. FortiOS Web caching stores remote files and web pages on local FortiGate devices for easy local access to commonly accessed files. There is little impact on the WAN, resulting in reduced latency for those requesting the files.

In addition, web caching also recognizes requests for Windows or MS Office updates, and downloads the new update file in the background. Once downloaded to the cache, the new update file is available to all users, and all subsequent requests for this update are rapidly downloaded from the cache.

Traffic shaping

Controls data flow for specific applications, giving administrators the flexibility to choose which applications take precedence over the WAN. A common use case of traffic shaping would be to prevent one protocol or application from flooding a link over other protocols deemed more important by the administrator.

SSL acceleration

SSL is used by many organizations to keep WAN communications private. WAN Optimization boosts SSL acceleration properties of FortiGate FortiASIC hardware by accelerating SSL traffic across the WAN. The FortiGate unit handles SSL encryption/decryption for corporate servers providing SSL encrypted connections over the WAN.

Explicit web proxy server

Allows users on the internal network to browse the Internet through the explicit web proxy server.

Explicit FTP proxy server

Allows users on the internal network to access FTP servers through the explicit FTP proxy server.

Reverse proxy

The web and FTP proxies can be configured to protect access to web or FTP servers that are behind the FortiGate using a reverse proxy configuration. Reverse proxies retrieve resources on behalf of a client from one or more servers. These resources are then returned to the client as if they originated from the proxy server.

WCCP

The Web Cache Communication Protocol (WCCP) allows you to offload web caching to redundant web caching servers. This traffic redirection helps to improve response time and optimize network resource usage.

WAN optimization and HA

You can configure WAN optimization on a FortiGate HA cluster. The recommended HA configuration for WAN optimization is active-passive mode. Also, when the cluster is operating, all WAN optimization sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance WAN optimization sessions. HA also does not support WAN optimization session failover.

Configuring an explicit proxy with WAN optimization web caching

For this configuration, all devices on the wireless network will be required to connect to the proxy at port 8080 before they can browse the Internet. WAN Optimization web caching is added to reduce the amount of Internet bandwidth used and improve web browsing performance.

Enabling WAN optimization and configuring the explicit web proxy for the wireless interface

1. Go to *System* > *Feature Visibility*. Ensure that *Explicit Proxy* is enabled.
   To make WAN optimization and web caching settings available in the GUI, enter the following CLI command:
   ```
   config system settings
      set gui-wanopt-cache enable
   end
   ```
2. Go to *Network* > *Interfaces*, edit the wireless interface and select *Enable Explicit Web Proxy*.
3. Go to *Network* > *Explicit Proxy*. Enable *Explicit Web Proxy*. Make sure that *Default Firewall Policy Action* is set to *Deny*.

Adding an explicit web proxy policy

1. Go to *Policy & Objects* > *Proxy Policy* and create a new policy.
2. Set *Proxy Type* to *Explicit Web*, the *Outgoing Interface* to the Internet-facing interface, and the remaining fields as required.
   For more information, see Explicit web proxy.

Configuring devices on the wireless network to use the web proxy

To use the web proxy, all devices on the wireless network must be configured to use the explicit proxy server. The IP address of the server is the IP address of the FortiGate's wireless interface (for example, 10.10.80.1) and the port is 8080. Some browsers may have to be configured to use the device's proxy settings.

- For Windows 10, right-click the Windows start-icon and select *Network Connections*. Select *Proxy* and configure the proxy settings.
- For Windows Vista/7/8, open *Internet Properties*. Go to *Connections* > *LAN Settings* and enable and configure the *Proxy Server*.
- For Mac OS X, open *System Preferences* > *Network* > *Wi-Fi* > *Advanced* > *Proxies*. Select *Web Proxy (HTTP)* and configure the proxy settings.
- For iOS, go to *Settings* > *Wi-Fi*. Edit the wireless network. Scroll down to *HTTP PROXY*, select *Manual*, and configure the proxy settings.
- For Android, in WiFi network connection settings, edit the wireless network. Select *Show advanced options*, configure a *Manual* proxy, and enter the proxy settings.

Force HTTP and HTTPS traffic to use the web proxy

Block HTTP and HTTPS access to the Internet from the wireless network so that the only path to the Internet is through the explicit proxy. You can edit or delete policies that allow HTTP or HTTPS access. You can also add a policy to the top of the list that *Denies* HTTP and HTTPS traffic.

FSSO - Fortinet Single Sign-On

Fortinet Single Sign-On (FSSO), formerly known as FortiGate Server Authentication Extension (FSAE), is the authentication protocol by which users can transparently authenticate to FortiGate, FortiAuthenticator, and FortiCache devices. The FortiAuthenticator unit identifies users based on their authentication from a different system, and can be authenticated via numerous methods:

- Users can authenticate through a web portal and a set of embeddable widgets.
- Users with FortiClient Endpoint Security installed can be automatically authenticated through the FortiClient SSO Mobility Agent.
- Users authenticating against Active Directory can be automatically authenticated.
- RADIUS Accounting packets can be used to trigger an FSSO authentication.
- Users can be identified through the FortiAuthenticator API. This is useful for integration with third-party systems.

Below are the TCP/UDP ports used by the multiple FSSO modes:

Purpose	Protocol/Port
LDAP group membership lookup (Global Catalog)	TCP/3268
LDAP domain controller discovery and group membership lookup	TCP/389
DC Agent keepalive and push logon info to CA	UDP/8002
CA keepalive and push logon info to FortiGate	TCP/8000
NTLM	TCP/8000
CA DNS	UDP/53
Workstation check, polling mode (preferred method)	TCP/445
Workstation check, polling mode (fallback method)	TCP/135, TCP/139, UDP/137
Remote access to logon events	TCP/445
Group lookup using LDAP	TCP/389
Group lookup using LDAP with global catalog	TCP/3268
Group lookup using LDAPS	TCP/636
Resolve FSSO server name	UDP/53

Configuring the FortiAuthenticator

The FortiAuthenticator unit can be integrated with external network authentication systems, such as RADIUS, LDAP, Windows AD, and FortiClients to poll user logon information and send it to the FortiGate unit.

To configure FortiAuthenticator polling:

1. Go to *Fortinet SSO Methods* > *SSO* > *General*.
2. In the *FortiGate* section, leave *Listening port* set to *8000*, unless your network requires you to change this. The FortiGate unit must allow traffic on this port to pass through the firewall. Optionally, you can set the *Login expiry* time (default is *480* minutes, or eight hours). This is the length of time users can remain logged in before the system logs them off automatically.
3. Select *Enable authentication* and enter the *Secret key*. Be sure to use the same secret key when configuring the FSSO Agent on FortiGate units.
4. In the *Fortinet Single Sign-On (FSSO)* section, enter the following information:

Enable Windows event log polling (e.g. domain controllers/Exchange servers)	Select for integration with Windows Active Directory
Enable RADIUS Accounting SSO clients	Select if you want to use a Remote RADIUS server.
Enable Syslog SSO	Select for integration with Syslog server.
Enable FortiClient SSO Mobility Agent Service	Once enabled, also select *Enable authentication* to enable SSO by clients running FortiClient Endpoint Security. Enter the *Secret key*. Be sure to use the same secret key in the FortiClient Single Sign-On Mobility Agent settings.

5. Select *OK*.

For more detailed information for each available setting, see the FortiAuthenticator Administration Guide.

Configuring the FortiGate

The FortiAuthenticator unit needs to be added to the FortiGate as an SSO agent that will provide user logon information.

To add a FortiAuthenticator unit as SSO agent:

1. Go to *Security Fabric* > *Fabric Connectors* and select *Create New*.
2. Under *SSO/Identity*, select *Fortinet Single-Sign-On Agent*.
3. Enter a *Name*, set *Primary FSSO Agent* either to the IP address of the FortiAuthenticator unit or a name, and enter a *Password*.
4. Set *Collector Agent AD access mode* to either *Standard*, where you can specify *Users/Groups*, or *Advanced*, where you can specify an *LDAP Server*.
5. Select *OK*.
   The FortiGate unit receives a list of user groups from the FortiAuthenticator unit or LDAP server. When you open the server, you can see the list of groups. You can use the groups in identity-based security policies.

FSSO user groups

You can only use FortiAuthenticator SSO user groups directly in identity-based security policies. You must create an FSSO user group, then add FortiAuthenticator SSO user groups to it. These FortiGate FSSO user groups will then become available for selection in identity-based security policies.

To create an FSSO user group:

1. Go to *User & Device* > *User Groups* and select *Create New*.
2. Enter a *Name* for the group.
3. Set *Type* to *Fortinet Single Sign-On (FSSO)*.
4. Add *Members*. The groups available to add as members are SSO groups provided by SSO agents.
5. Select *OK*.

Configuring the FortiClient SSO Mobility Agent

In order for the user to successfully set up the SSO Mobility Agent in FortiClient, they must know the FortiAuthenticator IP address and pre-shared key/secret.

To configure FortiClient SSO Mobility Agent:

1. In FortiClient, go to *File* > *Settings*.
2. Under *Advanced*, select *Enable Single Sign-On mobility agent*.
3. In *Server address*, enter the IP address of the FortiAuthenticator.
4. In *Customize port*, enter the listening port number specified on the FortiAuthenticator unit. You can omit the port number if it is *8005*.
5. Enter the *Pre-shared key*.
6. Select *OK*.

For more detailed FSSO configurations, see the FortiOS Administration Guide.

CLI syntax

The following section contains commands to control FSSO.

user fsso

The following command will set the server address, port, and password for multiple FSSO agents.

```
config user fsso
   edit <name_str>
      set name <string>
      set [server | server2 | server3 | server4 | server5] <string>
      set [port | port2 | port3 | port4 | port5] <integer>
      set [password | password2 | password3 | password4 | password5] <password>
   next
end
```

user fsso-polling

The following command will set the Active Directory server port.

```
config user fsso-polling
   edit <name_str>
      set port <integer>
   next
end
```

OFTP - Optimized Fabric Transfer Protocol

The Optimized Fabric Transfer Protocol (OFTP) is used when information is synchronized between FortiAnalyzer and FortiGate. Remote logging and archiving can be configured on the FortiGate to send logs to a FortiAnalyzer (and/or FortiManager) unit.

OFTP listens on ports TCP/514 and UDP/514.

You can connect to a FortiAnalyzer unit from a FortiGate unit using Automatic Discovery, so long as both units are on the same network. Connecting these devices in this way does not use OFTP. Instead, the Fortinet Discovery Protocol (FDP) is used to locate the FortiAnalyzer unit.

When you select Automatic Discovery, the FortiGate unit uses HELLO packets to locate any FortiAnalyzer units that are available on the network within the same subnet. When the FortiGate unit discovers the FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer unit and begins sending log data.

CLI command - To connect to FortiAnalyzer using automatic discovery:

```
config log fortianalyzer setting
   set status [enable | disable]
   set server <ip_address>
   set gui-display [enable | disable]
   set address-mode auto-discovery
end
```

If your FortiGate unit is in Transparent mode, the interface using the automatic discovery feature will not carry traffic.

To send logs from FortiGate to FortiAnalyzer:

1. Go to *Log & Report* > *Log Settings* and enable *Send logs to FortiAnalyzer/FortiManager* (under *Remote Logging and Archiving*).
2. Enter the FortiAnalyzer unit's IP address in the *IP address* field provided.
3. For *Upload option*, select either *Real Time* to upload logs as they come across the FortiGate unit, or *Every Minute*, or *Every 5 Minutes*.
4. Logs sent to FortiAnalyzer can be encrypted by enabling *SSL encrypt log transmission*.

FortiClient EMS - Enterprise Management Server

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints. Benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs.
- Updating profiles for endpoint users regardless of access location, such as administering antivirus, web filtering, VPN, and signature updates.
- Administering FortiClient endpoint registrations, such as accepting, deregistering, and blocking registrations.
- Managing endpoints, such as status, system, and signature information.
- Identifying outdated versions of FortiClient software.

Required services

You must ensure that required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with clients and servers running associated applications.

Communication	Service	Protocol	Port
FortiClient endpoint registration	File transfers	TCP	8013 (default)
Computer browser service	Enabled		
Samba (SMB) service During FortiClient deployment, endpoints may connect to the FortiClient EMS server using the SMB service.	Enabled		445
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default connection		389
Windows	HTTP	TCP	80
Internet Information Services (IIS)	HTTPS	TCP	443, 10443
SQL server			

For more information about FortiClient EMS, including other requirements, installation, and management, see the FortiClient EMS Administration Guide.