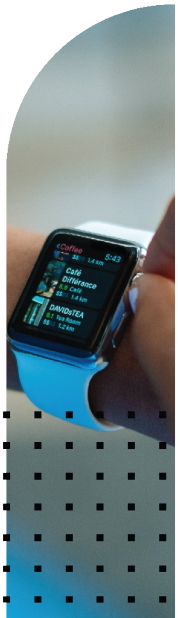
Release Notes

FortiOS 7.0.6



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

June 9, 2022
FortiOS 7.0.6 Release Notes
01-706-810291-20220609

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
Special notices **7**
Azure-On-Demand image 7
GCP-On-Demand image 7
ALI-On-Demand image 7
Unsupported websites in SSL VPN web mode 8
RDP and VNC clipboard toolbox in SSL VPN web mode 8
CAPWAP offloading compatibility of FortiGate NP7 platforms 8
FEC feature design change 8
Support for FortiGates with NP7 processors and hyperscale firewall features 9
Changes in CLI **10**
Changes in default behavior **11**
New features or enhancements **12**
Upgrade information **15**
Fortinet Security Fabric upgrade 15
Downgrading to previous firmware versions 16
Firmware image checksums 17
IPsec interface MTU value 17
HA role wording changes 17
Strong cryptographic cipher requirements for FortiAP 17
How VoIP profile settings determine the firewall policy inspection mode 18
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later 18
Add interface for NAT46 and NAT64 to simplify policy and routing configurations 18
Upgrading 19
Creating new policies 19
Example configurations 19
ZTNA configurations and firewall policies 21
Default DNS server update 22
Product integration and support **23**
Virtualization environments 23
Language support 24
SSL VPN support 25
SSL VPN web mode 25
Resolved issues **26**
Application Control 26
DNS Filter 26
Endpoint Control 26
Explicit Proxy 27

Firewall 27
FortiView 28
GUI 29
HA 30
Hyperscale 31
Intrusion Prevention 31
IPsec VPN 31
Log & Report 32
Proxy 33
Routing 34
Security Fabric 35
SSL VPN 35
Switch Controller 38
System 38
Upgrade 40
User & Authentication 41
VM 41
VoIP 42
Web Application Firewall 42
Web Filter 42
WiFi Controller 42
ZTNA 43
Known issues 44
Endpoint Control 44
Firewall 44
GUI 44
HA 45
Hyperscale 46
IPsec VPN 46
Limitations 46
Security Fabric 47
System 47
User & Authentication 47
VM 47
WAN Optimization 48
WiFi Controller 48
Built-in AV engine 49
Resolved engine issues 49
Built-in IPS engine 50
Resolved engine issues 50
Limitations 51
Citrix XenServer limitations 51
Open source XenServer limitations 51

Change Log

Date	Change Description
2022-06-07	Initial release.
2022-06-09	Updated L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later on page 18.

Introduction and supported models

This guide provides release information for FortiOS 7.0.6 build 0366.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.6 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

- Azure-On-Demand image on page 7
- GCP-On-Demand image on page 7
- ALI-On-Demand image on page 7
- Unsupported websites in SSL VPN web mode on page 8
- RDP and VNC clipboard toolbox in SSL VPN web mode on page 8
- CAPWAP offloading compatibility of FortiGate NP7 platforms on page 8
- FEC feature design change on page 8
- Support for FortiGates with NP7 processors and hyperscale firewall features on page 9

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.6 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4201F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For information about hyperscale firewall support for FortiOS 7.0.6, refer to the Hyperscale Firewall Release Notes.

Changes in CLI

Bug ID	Description

773698	Add setting in `config system ha` to support aggregate interfaces for hardware session synchronization.
	`config system ha`
	`  set hw-session-sync-dev <interface>`
	`end`

774154	Add `auth-timeout` setting in `config wireless-controller timers` to configure the waiting time after which a wireless client is considered to fail RADIUS authentication and times out (in seconds, 5 - 30, default = 5).
	`config wireless-controller timers`
	`  set auth-timeout <integer>`
	`end`

807523	Add `nat46-force-ipv4-packet-forwarding` setting in `config system npu` to enable or disable mandatory IPv4 packet forwarding when the IPv4 DF is set to 1.
	`config system npu`
	`  set nat46-force-ipv4-packet-forwarding enable`
	`end`

Changes in default behavior

Bug ID	Description
761565	Change the encryption and decryption method of backup files to AES-GCM method. The backup configuration file encrypted by the new algorithm in 7.2.1 cannot be restored on FortiGates running FortiOS 7.2.0 and earlier.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

714788	Add HA uninterruptible upgrade option, which allows users to configure a timeout value in minutes (1 - 30, default = 30) where the primary HA unit waits before the secondary HA unit is considered upgraded.
	`config system ha`
	`set uninterruptible-primary-wait <integer>`
	`end`

720631	Add fields for `source-ip` and `source-ip6` to set the source address used to connect to the ACME server.
	`config system acme`
	`set source-ip <class_ip>`
	`set source-ip6 <IPv6_address>`
	`end`

722647	Add IPsec fast path in VPN/DPDK for FG-VM (ESXi, KVM, Hyper-V, AWS, and Azure). Only GCM128 and GCM256 cyphers supported. IPv6 tunnels, anti-replay, and transport mode are not supported.
	`config dpdk global`
	`set ipsec-offload {enable | disable}`
	`end`

728408	Add handling for expect sessions created by session helpers in NGFW policy mode. For protocols that are only supported by IPS but not session helpers (IPv6 SIP), IPS falls back on using its own handling of these sessions, which is similar to profile mode.
748857	The FortiToken Cloud daemon is required to support of LDAP filters, so that synchronized LDAP users can be applied by a filter to select designated users or user groups. In the LDAP server configuration, `group-filter` (user attribute by default) `group-object-filter` can be used.
750224	To enhance BFD support, FortiOS can now support neighbors connected over multiple hops. When BFD is down, BGP sessions will be reset and try to re-establish neighbor connection immediately.
753368	Add support for 802.1X under the hardware switch interface on NP6 platforms: FG-30xE, FG-40xE, and FG-110xE.

755141	The following existing options can be used to control explicit DoT handshakes.
	`config system global`
	`set ssl-min-proto-version {SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}`
	`set ssl-static-key-ciphers {enable | disable}`
	`set strong-crypto {enable | disable}`
	`end`

Bug ID	Description
756538	Add Windows 11 and macOS 12 to the SSL VPN OS check. The following options are available for `config os-check-list <name>`: `macos-bigsur-11`, `macos-catalina-10.15`, `macos-mojave-10.14`, `macos-monterey-12`, `windows-7`, `windows-8.1`, `windows-10`, and `windows-11`. Operating systems no longer supported by FortiClient were removed.
758560	Add macOS 12 and Windows 11 to SSL VPN host check. Windows 8 and macOS 10.9 to 10.13 are removed from the SSL VPN host check.
759344	NP7 CAPWAP offloading for WiFi traffic now supports VLAN-related features such as dynamic VLANs and VLAN stacking (also called QinQ or inner VLANs).
763021	Allow dedicated scan to be disabled on FortiAP F-series profiles, which then allows background scanning using the WIDS profile to be enabled on radios 1 and 2.
766158	In a video filter profile, when the FortiGuard category-based filter and YouTube channel override are used together, by default a video will be blocked if it matches either category or YouTube channel and the action is set to block. This enhancement enables the channel action to override the category action. A category can be blocked, but certain channels in that category can be allowed when the `override-category` option is enabled.
773126	Add support for Apple French keyboard layout for RDP in SSL web portal, user bookmark, and user group bookmark settings (`set keyboard-layout fr-apple`).
773530	Allow a two-hour grace period for Flex-VMs to begin passing traffic upon retrieving a license from FortiCare without VM entitlement verification from FortiGuard.
776052	Add four SNMP OIDs for polling critical port block allocations (PBAs) IP pool statistics including: total PBAs, in use PBAs, expiring PBAs, and free PBAs.

777675	By default, the connection from the ZTNA access proxy to the backend servers uses the IP of the outgoing interface as the source. This enhancement enables customers to use an IP pool as the source IP, or use the client's original IP as the source IP. This allows ZTNA to support more sessions without source port conflict.
	`config firewall proxy-policy`
	`edit <id>`
	`set type access-proxy`
	`set poolname <ip_pool>`
	`set transparent {enable | disable}`
	`next`
	`end`

779031	Add support for NTurbo port SSL mirror traffic on NP7.
787477	Add HA synchronization support for FGCP with FGSP model.

Bug ID	Description
792170	The FortiGate explicit web proxy supports the Cross-Origin Resource Sharing (CORS) protocol, which allows the FortiGate to process a CORS preflight request and an actual CORS request properly, in addition to a simple CORS request when using session-based, cookie-enabled, and captive portal-enabled SAML authentication. This allows a FortiGate explicit web proxy user with this specific configuration to properly view a web page requiring CORS with domains embedded in it other than its own domain.
799971	To synchronize Active Directory users and apply two-factor authentication using FortiToken Cloud, two-factor authentication can be enabled under the `user ldap` object definition. This enhancement reduces the number of the AD users returned by allowing the use of a group filter to synchronize only the users who meet the group filter criteria.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.0.6 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.3
FortiManager	• 7.0.3
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 17
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiSandbox	• 2.3.3 and later

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI
19. FortiTester
20. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.6. When Security Fabric is enabled in FortiOS 7.0.6, all FortiGate devices must be running FortiOS 7.0.6.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

   Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2tp.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`edit "test-vip46-1"`
`set extip 10.1.100.155`
`set mappedip 2000:172:16:200::55`
`next`
`end`
	`config firewall vip`
	`edit "test-vip46-1"`
	`set extip 10.1.100.150`
	`set nat44 disable`
	`set nat46 enable`
	`set extintf "port24"`
	`set ipv6-mappedip 2000:172:16:200::55`
	`next`
	`end`

`ippool6` object:

Old configuration	New configuration

`config firewall ippool6`
`edit "test-ippool6-1"`
`set startip 2000:172:16:201::155`
`set endip 2000:172:16:201::155`
`next`
`end`
	`config firewall ippool6`
	`edit "test-ippool6-1"`
	`set startip 2000:172:16:201::155`
	`set endip 2000:172:16:201::155`
	`set nat46 enable`
	`next`
	`end`

NAT46 policy:

Old configuration	New configuration

`config firewall policy46`
`edit 1`
`set srcintf "port24"`
`set dstintf "port17"`
`set srcaddr "all"`
`set dstaddr "test-vip46-1"`
`set action accept`
`set schedule "always"`
`set service "ALL"`
`set logtraffic enable`
`set ippool enable`
`set poolname "test-ippool6-1"`
`next`
`end`
	`config firewall policy`
	`edit 2`
	`set srcintf "port24"`
	`set dstintf "port17"`
	`set action accept`
	`set nat46 enable`
	`set srcaddr "all"`
	`set dstaddr "test-vip46-1"`
	`set srcaddr6 "all"`
	`set dstaddr6 "all"`
	`set schedule "always"`
	`set service "ALL"`
	`set logtraffic all`
	`set ippool enable`
	`set poolname6 "test-ippool6-1"`
	`next`
	`end`

`vip64` object

Old configuration	New configuration

`config firewall vip64`
`edit "test-vip64-1"`
`set extip 2000:10:1:100::155`
`set mappedip 172.16.200.155`
`next`
`end`
	`config firewall vip6`
	`edit "test-vip64-1"`
	`set extip 2000:10:1:100::155`
	`set nat66 disable`
	`set nat64 enable`
	`set ipv4-mappedip 172.16.200.155`
	`next`
	`end`

`ippool` object

Old configuration	New configuration
config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 next end	config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 **set nat64 enable** next end

NAT64 policy:

Old configuration	New configuration
config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end	config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept **set nat64 enable** set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end

ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System* > *Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

Default DNS server update

If both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

Product integration and support

The following table lists FortiOS 7.0.6 product integration and support information:

Web browsers	• Microsoft Edge • Mozilla Firefox version 100 • Google Chrome version 101 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00276
IPS Engine	• 7.00126

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 100 Google Chrome version 101
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 100 Google Chrome version 101
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 100 Google Chrome version 101
macOS Monterey 12.4	Apple Safari version 15 Mozilla Firefox version 100 Google Chrome version 101
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.0.6. For inquires about a particular bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
787130	Application control does not block FTP traffic on an explicit proxy.

DNS Filter

Bug ID	Description
692482	DNS filter forwards the DNS status code 1 `FormErr` as status code 2 `ServFail` in cases where the redirect server responses have no question section.
744572	In multi-VDOM with default `system fortiguard` configuration, the DNS filter does not work for the non-management VDOM.
796052	If local-in and transparent requests are hashed into the same local ID list, when the DNS proxy receives a response, it finds the wrong query for requests with the same ID and domain.

Endpoint Control

Bug ID	Description
776447	When a new device first connects to the EMS server with a customized certificate, the wrong slide-in pane appears in the GUI.
777294	Fabric connection failure between EMS and FortiOS.
793162	Sometimes the FortiGate fails to resolve a FortiClient MAC or IP in the firewall dynamic address table.

Explicit Proxy

Bug ID	Description
754191	Websites are not accessible if the `certificate-inspection` SSL-SSH profile is set in a proxy policy.
765761	Firewall with forward proxy and UTM enabled is sending TLS probe with forward proxy IP instead of real server IP.
766127	PAC file download fails with `incorrect service` error after upgrading to 7.0.2.
767951	Explicit web proxy does not bypass ICAP server inspection when the ICAP server is unreachable.
771152	GUI does not display *Source Address* field when using a proxy address group in authentication rules.
774442	WAD is NATting to the wrong IP pool address for the interface.
778339	Improve logic of removing HTTP Proxy-Authorization/Authorization header to prevent user credential leaking.
780211	`diagnose wad stats policy list` output displays information for only 20 proxy policies, so not all policies are included.
783946	Explicit proxy policy does not deny request for ClearPass object if it is used as a source.
785342	FortiGate explicit proxy does not work with SOCKS4a.
796364	Renaming a ClearPass dynamic address object that is configured in a proxy policy causes the address not to be matched.
801602	In agentless NTLM authentication, the source IP in `user domain-controller` is not applied.

Firewall

Bug ID	Description
599638	Get unexpected count for `established session count`, and `diagnose firewall iprope clear` does not work as expected.
644638	Policy with a Tor exit node as the source is not blocking traffic coming from Tor.
724145	Expiration timer of expectation session may show a negative number.
744888	FortiGate drops SERVER HELLO when accessing some TLS 1.3 websites using a flow-based policy with SSL deep inspection.
752784	Packet is dropped due to the wrong UDP header length. The NP6XLite driver and kernel drop the packet because of the transport header check.
761494	HTTP persistence not working for HTTP cookie and SSL session ID for round-robin load balancer.

Bug ID	Description
767294	The `match-vip` option is only useful for deny policies; however, its flag is not cleared after changing the policy action from deny to accept. When a policy uses a mapped FQDN VIP, the destination field of the `iprope` policy accepts the full IP range.
770541	There is a delay opening firewall, DoS, and traffic shaping policies in the GUI.
770668	The packet dropped counter is not incremented for `per-ip-shaper` with `max-concurrent-session` as the only criterion and offload disabled on the firewall policy.
775783	Get httpsd signal 11 crash when inline editing custom service from policy list page with FortiGate support tool running.
777231	*FortiView Traffic Shaping* monitor should not show an entry with no shaper.
778513	Forward traffic logs do not show MAC address object name in *Device* column.
779902	FortiGate policy lookup does not work as expected (in the GUI and CLI) when the destination interface is a loopback interface.
784939	*Dashboard* > *Load Balance Monitor* is not loading in 7.0.4 and 7.0.5.
791735	The number of sessions in `session_count` does not match the output from `diagnose sys session full-stat`.
797017	The FortiGate does not refresh the iprope group for central SNAT policies after moving a newly created SNAT policy.
797318	NAT64 is not forwarding traffic to the destination IP.
802834	In the *Traffic Shaping* > *Traffic Shapers* tab, the *Bandwidth Utilization* column is empty for per-policy reverse shapers.
803270	Unexpected value for `session_count` appears.
806113	Traffic shaping policy edit dialog shows configured reverse shaper as disabled.

FortiView

Bug ID	Description
765993	*Dashboard* > *FortiView Sources - WAN* monitor does not show data for VLAN interface.

GUI

Bug ID	Description
630216	A user can browse HA secondary logs in the GUI, but when a user downloads these logs, it is the primary FortiGate logs instead.
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
720192	GUI logs out when accessing FortiView monitor page if the VDOM administrator only has `ftviewgrp` permission.
740508	Bandwidth widget shows incorrect traffic on FG-40F.
746618	Export port link status is not correct on tenant VDOM *FortiSwitch Ports* page.
763724	After the current session is disconnected, pressing the `Enter` key does not restart a new session on the GUI CLI console.
774159	Signature not found in IPS database message when editing the IPS profile from the policy.
776969	Unable to select and copy serial number from *System Information* dashboard widget.
778258	Unable to set IP address for IPsec tunnel in the GUI.
778542	Local domain name disappears from the GUI after clicking *API Preview*.
778932	MAC address name is not displayed in the *Device* column in the *Asset Identity Center*.
781310	*Policy & Objects* > *DNAT & Virtual IPs* page can take more than 30 seconds to load if there are more than 25 thousand virtual IPs.
783152	Filtering by *Status* in the *SD-WAN* widget is not working.
787007	httpsd is crashing without any interaction on the GUI at `api_cleanup_cache in api_cmdb_v2_handler`.
787550	HTTPSD daemon crashes frequently with `signal 6 (aborted) at api_v2_page_result`.
787565	When logged in as guest management administrator, the custom image shows as empty on the user information printout.
788935	GUI is slow to load when CDN is enabled and accessed on a closed network.
792045	FortiGate failed to view matched endpoints after viewing it successfully several times.
799160	*Modem 1 Health* is incorrectly displayed as *Disconnected* in the *Diagnostics and Tools* pane of the *FortiExtenders* page.
800632	Search bar on *Addresses* page does not complete loading and return a result when format is <IP>-<number>.

HA

Bug ID	Description
664929	The hatalk process crashed when creating a disabled VLAN interface in an A-P cluster.
683584	The hasync process crashed because the write buffer offset is not validated before using it.
683628	The hasync process crashes often with signal 11 in cases when a CMDB mind map file is deleted and some processes still mind map the old file.
714788	Uninterruptible upgrade might be broken in large-scale environments.
744349	Unable to connect to FortiSandbox Cloud through proxy from secondary node in an HA cluster.
752942	When the secondary is being synchronized, the GARP is sent out from the secondary device with the physical MAC address.
763214	Firmware upgrade fails when the bandwidth between `hbdev` is reduced to 26 Mbps and lower (`Check image file integrity error!`).
764873	FGSP cluster with UTM does not forward UDP or ICMP packets to the session owner.
765619	HA desynchronizes after user from a read-only administrator group logs in.
771389	SNMP community name with one extra character at the end stills matches when HA is enabled.
771391	HA uptime remains the same after `mondev` failure.
773698	`hw-session-sync-dev` does not allow LACP or multiple ports.
773901	The dnsproxy daemon is not updating HA management VDOM DNS after it is configured. The secondary also does not update.
775724	Static routes not installed after HA failover.
775837	When upgrading the secondary unit to build 1097 or later, a `root.vpn.certificate.local.Fortinet_SSL` configuration error appears.
778011	The hasync daemon crashes on FG-80E.
779180	FGSP does not synchronize the `helper-pmap` expectation session.
779512	If the interface name is a number, an error occurs when that number is used as an `hbdev` priority.
779587	When an authentication log on length is longer than the `hasync` packet length and when there is a large number of logons, `hasync` is busy.
781463	FortiGate does not respond to ARP request for `management-ip` on interface if the interface IP is changed.
782769	Unable to form HA pair when HA encryption is enabled.
783483	On the *System* > *HA* page, *Sessions* are shown as *0* after upgrading from 7.0.3 to 7.0.4.
786592	Failure in self-pinging towards the management IP.
791397	HA secondary address CMDB synchronizes incorrectly for EMS dynamic tags.

Bug ID	Description
794707	Get invalid IP address when creating a firewall object in the CLI; it synchronized to the secondary in FGSP `standalone-config-sync`.
801872	Unexpected HA failover on AWS A-P cluster when `ipsec-soft-dec-async` is enabled.
803697	The `ha-mgmt-interface` stops using the configured `gateway6`.
807322	AWS HA does not update the prefix list in the route table.

Hyperscale

Bug ID	Description
807523	On NP7 platforms the `config system npu` option for `nat46-force-ipv4-packet-forwarding` is missing.

Intrusion Prevention

Bug ID	Description
698247	Flow mode web filter `ovrd` crashes and socket leaks in IPS daemon.
715360	Each time an AV database update occurs (scheduled or manually triggered), the IPS engine restarts on the SLBC secondary blade.
721916	On SoC4 platforms, when HWDOS enabled and the anomaly action is set to `block`, the FortiGate does not block sessions that exceed the threshold in the DoS policy.
751027	FortiGate can only collect up to 128 packets when detected by a signature.
755859	The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode.
775696	Each time an AV database update occurs (scheduled or manual), the IPS engine restarts on the SLBC secondary blade. This stops UTM analysis for sessions affected by that blade.
780194	IPS engine 7.00105 has `signal 14 (Alarm clock)` crash during stress testing.

IPsec VPN

Bug ID	Description
735412	IKE HA resynchronizes the synchronized connection without an established IKE SA.

Bug ID	Description
749509	IPsec traffic dropped due to anti-replay after HA failover.
767765	Tooltip in *Dashboard* > *Network* > *IPsec*widget for phase 2 shows a *Timeout* year of 1970 in Firefox, Chrome, and Edge.
768638	Invalid IP address while creating a VPN IPsec tunnel.
770354	L2TP over IPsec stopped encrypting traffic after upgrading from 6.4 to 7.0.2.
771935	Offloaded transit ESP is dropped in one direction until session is not deleted.
773221	Traffic that goes through IPsec based on a loopback interface cannot be offloaded.
773313	FG-40F-3G4G with WWAN DHCP interface set as L2TP client shows drops in WWAN connections and does not get the WWAN IP.
777476	When FGCP and FGSP is configured, but the FGCP cluster is not connected, IKE will ignore the `resync` event to synchronize SA data to the FGSP peer.
780850	IPsec hub fails to delete selector routes when NAT IP changed and IKE crashed.
781403	IKE is consuming excessive memory.
781917	`Session clash` messages appear in event logs for new sessions from VPN towards VIP.
783597	Framed IP is not assigned to IPsec clients configured with `set assign-ip-from usrgrp`.
786409	Tunnel had one-way traffic after iked crashed.
787567	Inbandwidth and outbandwidth on IPsec is not working properly.
789705	IKE crash disconnected all users at the same time.
793863	File downloads over L2TP IPsec VPN failed when using the VIP mapped to the internal server.
798709	Shortcut fails to be triggered by interested traffic.
803686	Tooltip in *Dashboard* > *Network IPsec* widget only displays one address for the local and remote addresses of the phase2 selector.

Log & Report

Bug ID	Description
764478	Logs are missing on FortiGate Cloud from the FortiGate.
769300	Traffic denied by security policy (NGFW policy-based mode) is shown as `action="accept"` in the traffic log.
774767	The expected reboot log is missing.
776929	When submitting files for sandbox logging in flow mode, `filetype="unknown"` is displayed for PDF, DOC, JS, RTF, ZIP, and RAR files.

Bug ID	Description
777008	The syslogd daemon encounters a memory leak.
783145	Cyrillic alphabet is not displayed correctly in file filter and DLP logs.
783725	DoT log is incorrectly categorized as a forward traffic log instead of a local traffic log.
788724	The secondary FortiGate did not send the logs to the syslog server (`sendmmsg failed to send data`).

Proxy

Bug ID	Description
650348	FortiGate refuses incoming TCP connection to FTP proxy port after explicit proxy related configurations are changed.
678815	WAD crashes with signal 11 if the client sends a client hello containing a key share that does not match the key share that the server prefers.
747915	Deep inspection of SMTPS and POP3S starts to fail after restoring the configuration file of another device with the same model.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
766158	Video filter FortiGuard category takes precedence over allowed channel ID exception in the same category.
774859	WAD signal 11 Segmentation fault crash occurs at `wad_h2_port_read_sync`.
775193	Frequent WAD crashes are causing the FortiGate to go down.
775966	Changes to address group used for full SSL exemptions are not being activated.
776989	In some cases, WAD daemon `signal 6 (Aborted) received` occurs when adding a VDOM.
781161	WAD has signal 11 crash due to invalid reading after freeing WAD user information daemon.
782426	WAD crash with signal 11 and signal 6 occurs when performing SAML authentication if the URL size is larger than 3 KB.
783112	FortiGate goes into conserve mode due to high memory usage of WAD `user-info` process. The WAD `user-info` process will query the user count information from the LDAP server every 24 hours. If any of the LDAP query messages are closed by exceptions, there is a memory leak. If `obtain-user-info` is enabled under `config user ldap`, this memory leak will be triggered on daily basis.
783438	When diagnosing WAD memory with a significant number of open HTTP sessions, the function pointer may still be called and will cause a segmentation fault.
786939	The `scan-botnet-connections block` setting does not work for TCP:443 with proxy-based inspection.

Bug ID	Description
791662	FortiGate is silently dropping server hello in TLS negotiation.
792505	Memory leak identified for WAD worker `dnsproxy_conn` causing conserve mode.
795321	WAD crash signal 11 and unit goes into conserve mode.
796910	Application wad crash (`Segmentation fault`) , which is the first crash in a series.
802935	FortiGate cannot block a virus file when using the HTTP PATCH upload method.
803136	`thumbnailPhoto` files are saved in the memory disk with the incorrect hash name.
803260	Memory increase suddenly and is not released until rebooting.

Routing

Bug ID	Description
710606	Some static routes disappear from RIB/FIB after modifying/installing static routes from the GUI script.
717086	External resource local out traffic does not follow the SD-WAN rule and specified egress interface when the `interface-select-method` configuration in `system external-resource` is changed.
745856	The default SD-WAN route for the LTE wwan interface is not created.
767225	Unable to set `tls-active-probe`.
769321	After ADVPN HA failover, BGP is not established, and tunnels are up but not passing traffic between the hub and spokes.
770420	FortiGate assigns an incorrect IP address for SNAT on `ipunnumbered` interface.
771052	The `set next-hop-self-rr6 enable` parameter not effective.
771423	BGP route map community attribute cannot be changed from the GUI when there are two 16-byte concatenated versions.
772400	IPv6 route is not created for SIT tunnel interface in SD-WAN.
774136	VPN traffic is not being metered by DoS policy when using SD-WAN.
777047	PING over IPv6 is not working from a loopback interface to any interface if the VRF on the loopback moves to `vrf1`.
778392	Kernel panic crash occurs after receiving new IPv6 prefix via BGP.
779113	When a link monitor fails, the routes indicated in the link monitor are not withdrawn from the routing database.
780210	Changing the interface weight under SD-WAN takes longer to be applied from the GUI than the CLI.
780421	SD-WAN services use a different way to handle IPv6 packets than IPv4, which causes packets loss.

Bug ID	Description
781493	After restarting IKE, ADVPN shortcuts stuck in the SD-WAN service and health check.
783168	IPv6 secondary network is removed from the routing table after reboot.
784950	The `ecmp-max-paths` are not behaving as expected.
788793	Unable to receive BGP routes on redundant tunnel interfaces.
797530	SD-WAN health check event log shows the incorrect protocol.
797590	GRE tunnel configured using a loopback interface is not working after changing the interface back and forth.
807635	BGP routes hit the wrong route map.

Security Fabric

Bug ID	Description
764825	When the Security Fabric is enabled, logging is not enabled on deny policies.
778511	PPPoE interface is unable to accept Fabric connections.
779181	Security rating report for *System Uptime* incorrectly fails the check for FortiAP, even though the FortiAP is up for more than 24 hours.
788543	Topology tree shows *No connection* or *Unauthorized* for FortiAnalyzer while sending log data to FortiAnalyzer.
791794	Unable to send alert emails using SMTP TLS in Office 365.
793234	*Fabric Management* page incorrectly shows some FortiAPs with an unregistered FortiCare status even though the FortiAP is already registered. This is just a display issue and does not impact FortiAP operation.
793474	FortiManager card has red color on *Security Fabric* > *Fabric Connectors* page.
795687	On the *Fabric Management* page, some managed FortiSwitches are not shown.
799832	GCP bearer token is too long for the header in a `google-cloud-function` automation action.

SSL VPN

Bug ID	Description
486837	SSL VPN with external DHCP servers is not working.
616896	Link in SSL VPN portal to FortiClient iOS redirects to legacy FortiClient 6.0 rather than the latest 6.2.

Bug ID	Description
741674	Customer internal website (https://cm***.msc****.com/x***) cannot be rendered in SSL VPN web mode.
749857	Web mode and tunnel mode could not reflect the VRF setting, which causes the traffic to not pass through as expected.
755296	SSL VPN web mode has issues accessing https://e***.or***.kr.
756561	Outdated OS support for host check should be removed.
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.
757726	SSL VPN web portal does not serve updated certificate.
760407	Unable to add domain entry in `split-dns` if `set domains` contains an underscore character (_).
760875	SSL VPN PKI users fail to log in when a special character is included in the CN or subject matching field.
762479	Telnet connection gets disconnected after three to four minutes in SSL VPN web mode while the connection is idle.
762685	Punycode is not supported in SSL VPN DNS split tunneling.
763611	If dual-stack is enabled, the user connects to the tunnel with IPv6 and the tunnel is established successfully. When the user tries to access the IPv4 server to upload or download files, the network speed is very slow.
764853	SSL VPN bookmark of VNC is not using ZRLE compression and consumes more bandwidth to end clients.
765216	Extend `skip-check-for-unsupported-os` to support the same OS type but different OS versions.
765258	Endpoint event is not reported when FortiClient 7.0 connects to SSL VPN.
767230	Issues with user log out request with Okta as an identity provider for SAML authentication.
767818	SSL VPN bookmark issues with internal website.
767869	SCADA portal will not fully load with SSL VPN web bookmark.
768323	Certain websites do not load properly in SSL VPN web mode.
768362	Default resolution for RDP/VNC in SSL VPN web mode cannot be configured.
768983	SSL VPN web mode access to the FortiGate GUI is slow after upgrading to 7.0.3.
768994	SSL VPN crashed when closing web mode RDP after upgrading.
770452	Clicking an SSL VPN web portal bookmark web link displays blank page.
770919	Internal website (*.blt.local) is not loading in SSL VPN web mode.
771162	Unable to access SSL VPN bookmark in web mode.
772191	Website is not loading in SSL VPN web mode.
774661	Unable to load SSL VPN web portal internal webpage.

Bug ID	Description
774831	Comma character (,) is acting as delimiter in authentication session decoding when CN format is `Surname, Name`.
776069	The sslvpn daemon crashes due to memory access after it has been freed.
778031	SSL VPN web mode HTTP throughputs drop over 50%.
778034	FortiGate GUI in SSL VPN web mode is very slow.
780305	SSL VPN web mode is unable to redirect from port 62843 to port 8443.
781542	Unable to access internal SSL VPN bookmark in web mode.
781550	HTTPS link is not working in SSL VPN web mode.
782732	Webpages of back-end server behind https://vpn-***.sys***.pl/remote/ could not be displayed in SSL VPN web mode.
783508	After upgrading to 6.4.8, NLA security mode for SSL VPN web portal bookmark does not work.
784335	Unable to load internal website in SSL VPN web mode.
784426	SSL VPN web mode has problems accessing ComCenter websites.
784522	When trying to create a support ticket in Jira with SSL VPN proxy web mode, the dropdown field does not contain any values.
784887	A blank page appears after logging in to an SSL VPN bookmark.
786179	Cannot reach local application (dat***.btn.co.id) while using SSL VPN web mode.
787978	Unable to load NFMT routing display through SSL VPN web mode.
788641	Internal site not loading in SSL VPN web mode.
789267	SSO SSL VPN web mode user cannot connect to RDP intermittently.
789642	Unable to load Grafana application through SSL VPN web mode.
789644	Internal site not loading completely using SSL VPN web mode bookmark.
791700	SSL VPN crashes and disconnects users at the same time.
794800	SSL VPN /remote/logoutok screen loads in basic text.
795730	Non-Google CAPTCHA cannot be displayed in SSL VPN web mode.
801308	FortiGuard should only provide an installer for FortiClient VPN, instead of the full FortiClient version.
801588	After Kronos (third-party) update from 8.1.3 to 8.1.13, SSL VPN web portal users get a blank page after logging in successfully.
802379	SSL VPN has memory leaks and crashes.
803622	High CPU in SSL VPN once SAML is used with FortiAuthenticator and an LDAP server.

Switch Controller

Bug ID	Description
774441	FortiLink topology only displays partially.
774848	Bulk MAC addresses deletions on FortiSwitch is randomly causing all wired clients to disconnect at the same time and reconnect.
776442	FortiSwitch VLANs cannot be created in the FortiGate GUI for a second FortiLink.

System

Bug ID	Description
540389	Remote administrator password renewal shows remote token instead of new password (CLI and GUI).
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
679059	The ipmc_sensord process is killed multiple times when the CPU or memory usage is high.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
706543	FortiGuard DDNS does not update the IP address when the PPPoE reconnects.
708228	A DNS proxy crash occurs during `ssl_ctx_free`.
716250	Incorrect bandwidth utilization traffic widget for VLAN interface based on LACP interface.
722781	MAC address flapping on the switch is caused by a connected FortiGate where IPS is enabled in transparent mode.
724085	Traffic fails over EMAC VLAN interface with parent interface in another VDOM on FG-2600F.
734912	When VDOMs are enabled, changing system settings causes the GUI to display a failure to save message.
735761	VLAN ID is not taken into consideration at the session level for traffic crossing NP7 platforms.
736144	AirCard 340U LTE Modem does not work.
738423	Unable to create a hardware switch with no member.
749613	Unable to save configuration changes and get `failed: No space left on device` error.
750533	The cmdbsvr crashes when accessing an invalid `firewall vip` mapped IP that causes traffic to stop traversing the FortiGate.

Bug ID	Description
751044	There is no sensor trap function and related logs on SoC4 platforms.
753912	FortiGate calculates faulty FDS weight with DST enabled.
755268	When changing a `per-ip-shaper`, if there is ongoing traffic offloaded by NPU and it attaches that shaper, the new shaper's quota will not get updated.
756139	When split port is enabled on four 10 GB ports, only one LACP port is up, and the other ports do not send/receive the LACP PDU.
757478	Kernel panic results in reboot due the size of inner Ethernet header and IP header not being checked properly when the SKB is received by the VXLAN interface.
758490	The value of the `extra-init` parameter under `config system lte-modem` is not passed to the modem after rebooting the device.
760661	DDNS interface update status can get stuck if changes to the interface are made rapidly.
760942	dnsproxy signal 11 crash at `libcrypto.so.1.1` on FWF-61F.
761971	AirCard 340U LTE modem does not work on FG-61F.
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
764483	After restoring the VDOM configuration, `Interface <VLAN> not found in the list!` is present for VLANs on the aggregate interface.
767778	Kernel panic occurs while adding and deleting LAG members on FG-1101E.
768979	On a FortiGate with many FortiSwitches and FortiAPs, the *Device Inventory* widget and `user-device-store list` are empty.
771267	Zone transfer with FortiGate as primary DNS server fails if the FortiGate has more than 241 DNS entries.
771331	Incorrect bandwidth utilization traffic widget for VLAN interface on NP6 platforms.
771442	Discrepancy between session count and number of active sessions; sessions number creeps high, causing high memory utilization.
773067	CLI help text for link monitor `failtime` and `recoverytime` range should be `(1 - 3600, default = 5).`
773702	FortiGate running startup configuration is not saved on flash drive.
774443	SCP restore TCP session does not gracefully close with FIN packet.
775529	Hardware switch is not passing VRRP packets.
777044	On a FortiGate only managed by FortiManager, the FDNSetup Authlist has no FortiManager serial number.
778116	Restricted VDOM user is able to access the root VDOM.
778629	Disabling NP6XLite offloading does not work with VLAN interface on LAG one-arm scenario.

Bug ID	Description
779241	DCE-RPC expectation session expires and never times out (`timeout=never`).
779523	Negative `tunnel_count` in `diagnose firewall gtp profile list` for FGSP peer.
782392	ICMP traceroute with more than one probe is not working, and drops are seen on NP6 platforms.
783545	Backing up to SFTP does not work when the username contains a period (.).
785766	Memory leak and httpsd crashes.
786255	Cached topology reports causes the FortiGate to run out of flash storage on low-end models.
789203	High memory usage due to DoT leak at `ssl.port_1way_client_dox leak\wad_m_dot_conn leak\sni leak` when the DoX server is 8.8.8.8.
790446	The vwl process is spiking CPU and memory, which triggers conserve mode.
790656	DNS fails to correctly resolve hosts using the DNS database.
792544	A request is made to the remote authentication server before checking `trusthost`.
793401	The fcnacd process keeps using 99% CPU.
793864	Repeated FortiDDNS failed messages are in the system event logs output.
799255	Any configuration changes on FG-2601F causes cmbdr crash with signal 6 and traffic to stop flowing.
800295	NTP server has intermittent unresolvable logs after upgrading to 6.4.
800333	DoS offload does not work and the npd daemon keeps crashing if the `policy-offload-level` is set to `dos-offload` under `config system npu`. Affected platforms: NP6XLite.
801477	Disabling forward error correction is not working on FG-3500F.
801738	Kernel panic occurs on FG-2610F when collecting debug flow information.
802917	PPPoE virtual tunnel drops traffic after logon credentials are changed.

Upgrade

Bug ID	Description
754180	MAC address group is missing in the configuration after upgrading if it has members with other address groups that come behind the current one.
766472	After upgrading, the diagnostic command for redundant PSU is missing on FG-100F.
790823	VDOM links configuration is lost after upgrading.

User & Authentication

Bug ID	Description
667150	Add GUI support for FortiToken Mobile push notification and FortiToken Cloud based on two-factor authentication, which is already supported by authd.
749488	On an HA standby device, certain certificates (such as Fortinet_CA_SSL) regenerate by themselves when trying to edit them in CLI. This also causes issues when backing up configurations on the standby device.
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.
767844	User ID/password shows as blank when sending the guest credentials via a custom SMS server in *Guest Management*.
777004	Local users named pop or map do not work as expected when trying to add then as sources in a firewall policy.
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.
781992	fssod crashes with signal 11 on `logon_dns_callback`.
790941	Unable to add widget in dashboard after logging in with RADIUS authentication.
792924	Incorrect captive portal page certificate is used after upgrading from 7.0.3 to 7.0.5.

VM

Bug ID	Description
735441	Low performance when copying files from server behind FG-VM to another site via IPsec VPN.
774599	FG-VM64 with specific configuration halted while upgrading from 7.0.2.
781879	Flex-VM license activation failed to be applied to FortiGate VM in HA. Standalone mode is OK.
782073	IBM HA is unable to fail over route properly when route table has a delegate VPC route.
785234	GCP HA failover for external IP does not work when using Standard Tier.
785353	Azure performance issue on MLX5 when an unrelated VPN is up.
789223	Azure China uses the wrong API endpoint to get meta data after secondary becomes the new primary.
793914	HA is not in sync when a dynamic AWS service SMTP address object is retrieving a dynamic update from AWS.
799536	Data partition is almost full on FG-VM64-KVM.

VoIP

Bug ID	Description
794517	VoIP daemon memory leak occurs when the following conditions are met: • The SIP call is on top of the IPsec tunnel. • The call fails before the setup completes (session gets closed in a state earlier than `VOIP_SESSION_STATE_RUNNING`).

Web Application Firewall

Bug ID	Description
785743	When a web application firewall profile has version constraint enabled, HTTP 2.0 requests will be blocked.

Web Filter

Bug ID	Description
770941	Unable to block https://cle***.com/oauth/dis***-pic*** using URL filter; content from cle***.com is still shown.
781515	The urlfilter daemon continuously crashes on the secondary unit.
798557	Static URL filter order is not retained after saving.
801792	IPS daemon has socket FD leaks.

WiFi Controller

Bug ID	Description
489759	Consistent error messages, `internal_add_timer`, appear on console when running an automation script.
630085	A cw_acd crash is observed on the FortiGate when the FortiAP is deleted from the managed AP list.
745642	Consider not generating rogue AP logs once a certain AP has been marked as accepted.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.

Bug ID	Description
750425	In RADIUS MAC authentication, the FortiGate NAS-IP-Address will revert to `0.0.0.0` after using the FortiGate address.
757189	A batch of APs in cluster are exhibiting control messages that the maximal retransmission limit reached, and the APs disconnect from the FortiGate.
773027	*Client limit* description tooltip displayed in the GUI shows incorrect information.
773742	Two-factor authentication and WPA2-Enterprise WiFi conflict on `remoteauthtimeout` setting.
775157	A packet with the wrong IP header could not be processed by the CAPWAP driver, which randomly causes the FortiGate to reboot.
776576	FortiAP upgrade panel still prompts to upgrade to latest firmware, even when FortiAP is operating latest firmware.
780732	Unable to import MPSK keys in the GUI (CSV file into an SSID). An *Invalid file content* error appears.
783209	The `arrp-profile` table cannot be purged if no entry is in use.
783752	Improve `arrp-profile` configuration to avoid confusion.
790367	FWF-60F has kernel panic and reboots by itself every few hours.
791761	CAPWAP tunnel traffic over WPA2-Enterprise SSID is dropped when offloading is enabled on FG-1800F.
792738	The cw_acd process uses high CPU, which causes issues for FortiAP connecting with CAPWAP.

ZTNA

Bug ID	Description
770350	ZTNA tags do not follow the correct policy when bound in a single policy. They also do not work with groups.
770877	Traffic was blocked by mismatched ZTNA EMS tags in a forwarding firewall policy.
777669	The secondary IP address in the EMS dynamic address table does not match the expected policy.
799530	Found wad crash at `wad_sched.c` upon device tag matching.
802715	ZTNA failed to match the policy when a tag is found for an endpoint in the EMS response.

Known issues

The following issues have been identified in version 7.0.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.
775742	Upgrade EMS tags to include classification and severity to guarantee uniqueness.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic. **Workaround**: rename the custom section to a unique name between IPv4 and IPv6 policies.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.

Bug ID	Description
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
777145	*Managed FortiSwitches* page incorrectly shows a warning about an unregistered FortiSwitch even though it is registered. This only impacts transferred or RMAed FortiSwitches. This is only a display issue with no impact on the FortiSwitch's operation. **Workaround**: confirm the FortiSwitch registration status in the FortiCare portal.
780832	Managed FortiAPs list fails to load if there is an invalid or unsupported FortiAP.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
751072	HA secondary is consistently unable to synchronize any sessions from the HA primary when the original HA primary returns.
785514	In some situations, the fgfmd daemon is blocked by a query to the HA secondary checksum, which causes the tunnel between the FortiManager and FortiGate to go down.
811535	HA failure occurs on pair of FG-2600s due to packet loss on heartbeat interface.

Hyperscale

Bug ID	Description
804742	After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS 7.0.6 may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions.
805846	In the FortiOS MIB files, the trap fields `fgFwIppStatsGroupName` and `fgFwIppStatsInusePBAs` have the same OID. As a result, the `fgFwIppStatsInusePBAs` field always returns a value of `0`.
807476	On a FortiGate licensed for hyperscale firewall features, using the `cfg-save` option of the `config system global` command to revert configuration changes may result in error messages displaying in the CLI.
810025	Using EIF to support hairpinning does not work for NAT64 sessions.
810379	Creating an access control list (ALC) policy on a FortiGate with NP7 processors causes the npd process to crash.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.

Limitations

Bug ID	Description
617042	ACI dynamic address table size is limited to 1000 entries on FortiGate per EPG.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.

System

Bug ID	Description
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
743831	When global daylight saving time (DST) is disabled, the system time in the GUI still shows the time with DST.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
776646	Configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server in the GUI fails with a CLI internal error.
815360	NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time.

User & Authentication

Bug ID	Description
813407	Captive portal authentication with RADIUS user group truncates the token code to eight characters.

VM

Bug ID	Description
667153	Consume the licensed amount of CPUs without running `execute cpu add` and rebooting when a license is upgraded.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used. **Workaround**: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`.

WiFi Controller

Bug ID	Description
796036	Manual quarantine for wireless client connected to SSID on multi-VDOM with `wtp-share` does not work.

Built-in AV engine

Resolved engine issues

Bug ID	Description
771025	Fixed false PDF encryption detection by having PDFs with permission passwords to be consistently reported as not encrypted.
775415	Added additional safeguards in CDR to manage orphaned files that may cause memory leaks.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
695464	IPS engine has high CPU utilization.
806083	DNS local domain filter is not working in flow mode.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com