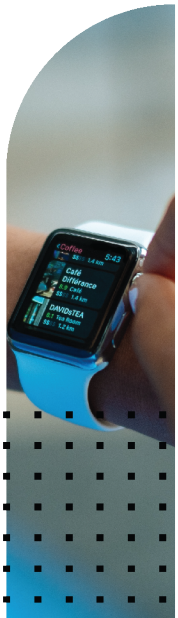
Release Notes

FortiOS 7.0.8



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

October 17, 2022
FortiOS 7.0.8 Release Notes
01-708-839377-20221017

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-13	Initial release.
2022-10-17	Updated Known issues on page 45.

Introduction and supported models

This guide provides release information for FortiOS 7.0.8 build 0418.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.8 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-ARM64-KVM, FG-ARM64-OCI, 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 branch supported models

The following models are released on a special branch of FortiOS 7.0.8. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0418.

FG-70F	is released on build 4682.
FG-71F	is released on build 4682.

Special notices

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 7.0.8 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 more information, refer to the Hyperscale Firewall Release Notes.

Changes in CLI

Bug ID	Description

729063	Change ZTNA `firewall vip6` option from `arp-reply` to `ndp-reply`.
	`config firewall vip6`
	`edit "test"`
	`set mappedip <IPv6_address>`
	`set ndp-reply {enable | disable}`
	`next`
	`end`

751715	Add command that allows users to switch between high-speed modem (USB 2.0, option `0`) and super-speed modem (USB 3.0, option `1`) operation mode. `# execute lte-modem set-usb-mode {0 | 1}`

Changes in default behavior

Bug ID	Description
802757	In order for unlicensed FortiGate VMs to be managed by FortiManager, FortiOS enables high encryption on the FGFM protocol for a secure connection between the FortiGate and FortiManager. Upon being added into the device manager, FortiManager can install VM licenses to the managed FortiGate VMs.

Changes in default values

Bug ID	Description
798091	Add speed option for 1000M auto-negotiation for FG-110xE.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

736275	Mark endpoint records and host tags as out of synchronization when failure timeout occurs for the EMS APIs, `report/fct/sysinfo` and `report/fct/host_tags`. The `out-of-sync` threshold (in seconds, 10 - 3600) can be configured from the CLI.
	`config endpoint fctems`
	`edit <name>`
	`set out-of-sync-threshold <integer>`
	`next`
	`end`

766171	When the `admin-restrict-local` setting is enabled under `config system global`, local administrators cannot be used until all remote authentication servers are down. In this enhancement, the FortiGate only checks all remote authentication servers that are applied in `config system admin` are down, instead of all remote servers configured on the FortiGate, before allowing local administrators to log in.
766704	Rename FortiAI to FortiNDR in the GUI and CLI to align with the FortiNDR rebranding. In addition, previous CLI-only settings for sending files to FortiNDR for inspection are now configurable from the *AntiVirus* profile page in the GUI.
782962	Add threshold for FG-8xF and FG-10xF platforms' serial number to enable the trap function.

795821	Support WiFi 6 Release 2 security enhancements by adding support for Hash-to-Element (H2E) only and Simultaneous Authentication of Equals Public Key (SAE-PK) for FortiAP models that support WPA3-SAE security modes.
	`config wireless-controller vap`
	`edit <name>`
	`set ssid <ssid>`
	`set security wpa3-sae`
	`set sae-h2e-only {enable | disable}`
	`next`
	`end`
	`config wireless-controller vap`
	`edit <name>`
	`set ssid <ssid>`
	`set security wpa3-sae`
	`set sae-pk {enable | disable}`
	`set sae-private-key <private_key>`
	`next`
	`end`

Bug ID	Description
796961	Add attribute under `config switch-controller igmp-snooping` to configure the `query-interval` under FortiLink, and add a check to ensure the `query-interval` is less than the `aging-time` interval.
798310	In addition to per-tunnel IPsec failover for FGSP peers, FGCP over FGSP is also supported. For additional redundancy, an FGCP cluster on one site may form FGSP peering with FGCP clusters on other sites. The FGCP over FGSP peers can still synchronize IPsec SAs and act as the primary gateway for individual tunnels for the same dialup servers. When failover happens within an FGCP cluster, tunnel traffic will fail over to the other FGCP cluster member. When an FGCP cluster fails, tunnel traffic will fail over to the other FGSP peer.

799987	Add support for multitenant FortiClient EMS deployments that have the *Manage Multiple Customer Sites* setting enabled with multiple sites. Since a FortiClient EMS site is no longer unique using its serial number alone, the FortiGate configuration for FortiClient EMS connectors and related diagnostic commands have been enhanced to distinguish EMS sites using serial number and tenant ID:
	• Update `config endpoint-control fctems` to predefine five FortiClient EMS Fabric connectors that are referred to using numerical IDs from 1 to 5. Administrators can configure the `status` and `name` settings, and to display the tenant ID retrieved from FortiClient EMS sites with *Manage Multiple Customer Sites* enabled.
	A single tenant EMS server or the default site on a multitenant EMS server has a tenant ID consisting of all zeros (00000000000000000000000000000000).
	• Update the FortiClient EMS Fabric connector to retrieve specific ZTNA tags from each configured FortiClient EMS site.
	• Update `diagnose endpoint record list` to return the `EMS tenant id` field retrieved from each respective FortiClient EMS server.
	• Update ZTNA and EMS debug commands to accept the EMS serial number and tenant ID as parameters.
	`# diagnose endpoint lls-comm send ztna find-uid <uid> <EMS_serial_number> <EMS_tenant_id>`
	`# diagnose wad dev query-by uid <uid> <EMS_serial_number> <EMS_tenant_id>`
	FortiClient 7.0.3 and later is required to use this feature.

801707	During FGSP per-tunnel failover for IPsec, the same IPsec dialup server configured on each FGSP member may establish tunnels with dialup clients as the primary gateway. The IPsec SAs are synchronized to all other FGSP peers that have FGSP synchronization for IPsec enabled. Other FGSP members may establish a tunnel with other clients on the same dialup server and synchronize their SAs to other peers.
	Upon the failure of the FGSP member that is the primary gateway for a tunnel, the upstream router will fail over the tunnel traffic to another FGSP member. The other FGSP member will move from standby to the primary gateway for that tunnel and continue to forward traffic.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set fgsp-sync {enable | disable}`

Bug ID	Description
	next end
801708	In conjunction with support for FGSP per-tunnel failover for IPsec, configuring DPD (dead peer detection) on an FGSP member is now permitted. This allows a failed FGSP member to send out DPD probes during failover to detect the unreachable remote peer and flush the corresponding tunnels.

805611	Support custom replacement message groups for each ZTNA virtual host. The `%%ZTNA_DETAIL_TAG%%` variable can be used in replacement messages.
	`config firewall access-proxy-virtual-host`
	`edit <name>`
	`set host <string>`
	`set replacemsg-group <string>`
	`next`
	`end`

807431	In proxy mode antivirus profiles, add option under HTTP to customize the action for files with unknown content encoding (default = block).
	`config antivirus profile`
	`edit <name>`
	`set feature-set proxy`
	`config http`
	`set unknown-content-encoding {block | inspect | bypass}`
	`end`
	`next`
	`end`

812209	This enhancement builds on the AWS SDN connector, which uses the AWS security token service (STS) to connect to multiple AWS accounts concurrently. To enhance security, the SDN connector supports the use of an External ID, which allows the target account owner to permit the role to be assumed by the source account only under specific circumstances.
818154	Allow FG-ARM64-AWS to work in Graviton3 c7g and c6gn instance types.

820902	Add option to exclude the first and last IP of a NAT64 IP pool. This setting is enabled by default.
	`config firewall ippool`
	`edit <name>`
	`set nat64 enable`
	`set subnet-broadcast-in-ippool {enable | disable}`
	`next`
	`end`

823709	Add TPM support for FG-VM64 platforms. Hypervisors with software TPM emulator packages installed will be able to support the TPM feature on FortiOS. This is currently supported on KVM and QEMU.
825308	Allow FortiGate-VMs for OCI to work on ARM-based Oracle Cloud Ampere A1 Compute instances.

Bug ID	Description

836653	Add commands to list the NPU session summary.
	`# diagnose sys npu-session list-brief`
	`# diagnose sys npu-session list-brief6`

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 7.0.8 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 20
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 7.0.8. When Security Fabric is enabled in FortiOS 7.0.8, all FortiGate devices must be running FortiOS 7.0.8.

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 "l2t.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 and later, 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

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

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 7.0.8 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 0308 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	• 6.00282
IPS Engine	• 7.00142

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 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 7.0.8. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
727067	FortiGate should fix the interface between FortiGate and FortiAnalyzer for the CDR file.
795784	Able to bypass FortiOS AV inspection on email traffic when manipulating a MIME attachment with junk and pad characters in Base64.
800731	Flow AV sends HTML files to the FortiGate Cloud Sandbox every time when HTML is not configured in file list.
805655	A scanunit crash with signal 11 occurs for SMTP and QP encoding.

DNS Filter

Bug ID	Description
790974	When the DNS static domain filter entry's action set to allow, it skips DNS translation.
800497	In flow mode with `set status disable` in the static domain filter, the entry still works when enabled in the DNS filter.

Endpoint Control

Bug ID	Description
775742	Upgrade EMS tags to include classification and severity to guarantee uniqueness.
803198	Intermittent FortiOS failure when using a redundant EMS configuration because the EMS FQDN was resolved once before, and when DNS entry expires or the DNS is used for load balancing.
817140	Device is constantly unauthorized in EMS when using `set interface-select-method sdwan`.

Explicit Proxy

Bug ID	Description
794124	HTTPS websites are not accessible if `certificate-inspection` is set in a proxy policy.
803228	When converting an explicit proxy session to SSL redirect and if this session already has connected to an HTTP server, the WAD crashes continuously with signal 11.
816879	Explicit proxy is not working when certificate inspection is enabled.

Firewall

Bug ID	Description
677855	cmdbsrv and other processes take CPU resources upon every configuration change in devices with over ten thousand firewall policies.
773035	Custom services name is not displayed correctly in logs with a port range of more than 3000 ports.
784766	Virtual server for exchange is returning `ERR_EMPTY_RESPONSE` message.
800730	When using NGFW policy-based mode, modifying a security policy causes all sessions to be reset.
808264	Stress test shows packet loss when testing with flow inspection mode and application control.
815565	Unable to connect to the reserved management interface allowed by the local-in policy.
824091	Promethean Screen Share (multicast) is not working on the member interfaces of a software switch.
827780	ISDB source matching is inconsistent between transparent and NAT modes.
829071	Geolocation block on VIP object failed with seemly correct configuration.
829664	Kernel panic occurs while collecting the debug flow.
830823	Traffic is dropped intermittently by the implicit deny policy, even though there is a valid policy on the FortiGate.
832217	Traffic is hitting the implicit deny policy when changes are made to a policy.

FortiView

Bug ID	Description
804177	When setting the time period to *now* filter, the table cannot be filtered by policy type.
811095	Threat type *N/A - Static URL Filter* is showing on sources that do not have the URL filter enabled.
819924	Information disappears after some time on the FortiView pages.

GUI

Bug ID	Description
729406	New IPsec design `tunnel-id` still displays the gateway as an IP address, when it should be a tunnel ID.
749843	*Bandwidth* widget does not display traffic information for VLAN interfaces when a large number of VLAN interfaces are configured.
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.
794757	Inbound traffic on the interface bandwidth widget shows *0 bps* on the VLAN interface.
798161	*System* > *Certificates* page keeps spinning when trying to access it from Safari.
802292	Logs sourced from FortiAnalyzer Big Data show the incorrect time.
804584	On the policy dialog page, the *Select Entries* box for the *Service* field does not list all service objects if an IPv6 address is in the policy.
807197	High `iowait` CPU usage and memory consumption issues caused by report runner.
819272	When a VLAN belongs to a zone, and the zone is used in a policy, editing the VLAN ID changes the policy's position in the table.
825377	*Managed FortiSwitches* page, policy pages, and some FortiView widgets are slow to load.
833774	GUI needs to allow the members of the software switch interface to be used in IPv4/IPv6 multicast policy.

HA

Bug ID	Description
722703	ISDB is not updating; last update attempt is stuck at an older date.
750829	In large customer configurations, some functions may time out, which causes an unexpected failover and keeps high cmdbsvr usage for a long time.
750978	Interface link status of HA members go down when `cfg-revert` tries to reboot post `cfg-revert-timeout`.
782734	Cluster is out-of-sync due to switch controller managed switch checksum mismatch.
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.
788702	Due to an HA port (Intel i40e) driver issue, not all SW sessions are synchronized to the secondary, so there is a difference.

Bug ID	Description
803354	After HA-AP failover, the FortiExtender WAN interface of the new primary cannot get the LTE IP address from FortiExtender.
816883	High CPU usage on secondary device, and CPU lacks the AVX feature needed to load `libdpdk.so`.
817942	Secondary cluster member's iprope traffic statistics are not updated to the original primary after an A-P HA failover.
819872	HA split brain scenario occurs after upgrading from 6.4.6 to 7.0.6, and HA heartbeats are lost followed by a kernel panic. Affected platforms: NP7 models.
822449	FGCP in standby sends GARP with physical MAC when it boots up.
823687	A cluster is repeatedly out-of sync due to external files (SSLVPN_AUTH_GROUPS) when there are frequent user logins and logouts.
824651	Certificate upload causes HA checksum mismatch.
826188	Secondary FortiGate FQDN is stuck in the queue, even if the primary FortiGate FQDN has already been resolved.
829390	When the internet service name management checksum is changed, it is out-of-sync when the auto-update is disabled on FortiManager.
830463	After shutting down the HA primary unit and then restarting it, the uptime for both nodes is zero, and it fails back to the former primary unit.

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`.
810025	Using EIF to support hairpinning does not work for NAT64 sessions.
810379	Creating an access control list (ACL) policy on a FortiGate with NP7 processors causes the npd process to crash.
812833	FortiGate still holds `npu-log-server` related configuration after removing hyperscale license.
812844	Default static route does not work well for hypsercale VDOM.

Bug ID	Description
836474	Changes in the zone configuration are not updated by the NPD on hyperscale.
837270	Disabling *Block intra-zone traffic* in a zone does not allow TCP/UDP traffic between interfaces of a zone.

ICAP

Bug ID	Description
832515	Bad gateway occurs using ICAP with explicit proxy under traffic load.

Intrusion Prevention

Bug ID	Description
695464	High IPS engine CPU usage due to recursive function call.
755859	The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode.
771000	High CPU in all cores with device running with one interface set as a one-arm sniffer.
798961	High CPU usage occurs on all cores in system space in __posix_lock_file for about 30 seconds when updating the configuration or signatures.
809691	High CPU usage on IPS engine when certain flow-based policies are active.

IPsec VPN

Bug ID	Description
757696	Implementing the `route-overlap` setting on phase 2 configurations brings tunnels down until a reboot is not performed on the FGSP cluster.
763205	IKE crashes after HA failover when the `enforce-unique-id` option is enabled.
765868	The packets did not pass through QTM, and SYN packets bypass the IPsec tunnel once traffic is offloaded. Affected platforms: NP7 models.
778243	When `net-device` is enabled on the hub, the tunnel interface IP is missing in the routing table.
778974	BGP route is inactive in the routing table after the hub's IPsec tunnel binding interface bounces.

Bug ID	Description
787949	FortiGate sends duplicate SNMP traps if the tunnel is brought down on the local side.
790486	Support IPsec FGSP per tunnel failover.
798045	FortiGate is unable to install SA (`failed to add SA, error 22`) when there is an overlap in configured selectors.
805301	Enabling NPU offloading in the phase 1 settings causes a complete traffic outage after a couple of ping packets pass through.
807086	ADVPN hub randomly initiates secondary tunnel to spoke, causing spoke to drop tunnel traffic for RPF check fail.
810988	GUI does not allow IP overlap for a tunnel interface when `allow-subnet-overlap` is enabled (CLI allows it).
814366	There are no incoming ESP packets from the hub to spoke after upgrading.
815253	NP7 offloaded egress ESP traffic that was not sent out of the FortiGate.
815969	Cannot apply dialup IPsec VPN settings modifications in the GUI when `net-device` is disabled.
824532	IPsec learned route disappears from the routing table.
825523	NP7 drops outbound ESP after IPsec VPN is established for some time.
827350	Dialup selector routes are not deleted after iked crash.
828467	The iked process is constantly crashing.
830252	IPsec VPN statistics are not increasing on the device.
836260	The IPsec aggregate interface does not appear in the *Interface* dropdown when configuring the *Interface Bandwidth* widget.

Limitations

Bug ID	Description
799831	Hyperscale fixed allocation CGN client is limited to 65 thousand addresses, and the CGN start port might be ignored.

Log & Report

Bug ID	Description
790893	Logging filters do not work as expected.

Bug ID	Description
814427	FortiGate error in FortiAnalyzer connectivity test on secondary device after upgrade.
814758	Get an intermittent error when running `execute log fortianalyzer-cloud test-connectivity`.
821359	FortiGate appears to have a limitation in the syslogd filter configuration.
821494	Forward traffic logs intermittently fail to show the destination hostname.
837435	Syslogd failed to send logs for some log IDs, including traffic log IDs 3, 4, 5, 6, 7, and 11.

Proxy

Bug ID	Description
745701	An issue occurs with TLS 1.3 and the 0RTT process where Firefox cannot access https.google.com using proxy-based UTM with certification inspection.
768278	WAD crashes frequently, authentication stops, and firewall freezes once proxy policy changes are pushed out.
780182	WAD crash at `wad_http_fwd_msg_body`.
793651	An expired certificate can be chosen when creating an SSL/SSH profile for deep inspection.
795360	Apple push notification service fails with proxy-based inspection.
799237	WAD crash at `wad_http_srv_cancel` when the TLS/SSL renegotiation encounters an error.
799381	WAD crash at `wad_ssl_proxy_caps_on_clt_certs` when TLS 1.2 receives the client certificate, and that server facing SSL port has been closed due to SSL bypass.
800125	Even if the policy is set to deny FTP_PUT, file uploads are permitted when the UTM feature is enabled.
803286	Inspecting all ports in deep inspection is dependent on previous protocol port mapping settings.
803380	Device is consuming high memory and going in conserve mode, possible due to a WAD memory leak.
807332	WAD does not forward the 302 HTTP redirect to the end client.
807431	File from AWS S3 fails to download with UTM, deep inspection, and proxy configured.
808831	Upgrading to 7.0.5 broke IM controls and caused Zalo chat file transfer issues.
809346	FTPS helper is not opening pinholes for expected traffic for non-standard ports.
811259	WAD memory leak occurs with IPS enabled.
813562	The `wad_m_usr_info frees` count is sometimes larger than the `allocs` count.
815313	WAD crash at `wad_ssl_cert_check_auth_status` once during stress testing.

Bug ID	Description
822271	Unable to access a website when deep inspection is enabled in a proxy policy.
823247	WAD user_info process leaks memory.
825496	Explicit proxy traffic is terminated when IPS is enabled. The exact failure happened upon certificate inspection.
830166	WAD crash signal 11 occurs.
830450	WAD crash at `wad_p2s_ciphers_filter`.
830907	WAD crash at `wad_mem_c_malloc.cold`.
834314	ICAP client timeout issue causes WAD signal 11 crash after upgrading to 7.0.6 from 6.4.
837724	WAD crash at `wad_port_general_update_dctx`.

REST API

Bug ID	Description
836760	The `start` parameter has no effect with the `/api/v2/monitor/user/device/query` API call.

Routing

Bug ID	Description
756955	Routing table does not reflect the new changes for the static route until the routing process is restarted when cmdbsrv and other processes take CPU resources upon every configuration change in devices with over ten thousand firewall policies.
769330	Traffic does not fail over to alternate path upon interface being down (FGR-60F in transparent mode).
774136	VPN traffic is not being metered by DoS policy when using SD-WAN.
779113	A new route check to make sure the route is removed when the link-monitor object fails on ARM based platforms.
795213	On the *Network* > *SD-WAN* page, adding a named static route to an SD-WAN zone creates a default blackhole route.
796070	Incorrect SD-WAN kernel routes are used on the secondary device.
796409	GUI pages related to SD-WAN rules and performance SLA take 15 to 20 seconds to load.
805285	SIP-RTP fails after a route or interface change.

Bug ID	Description
806939	Routing issue with ADVPN and SD-WAN if IPsec aggregate interfaces are configured.
808840	After cloning a static route, the URL gets stuck with `"clone=true"`.
812982	SD-WAN performance SLAs on a dialup IPsec VPN tunnel do not work as expected.
822659	*Secure SD-WAN Monitor* in FortiAnalyzer does not show graphs when the SLA target is not configured in SD-WAN performance SLA.
823293	Disabling BFD causes an OSPF flap/bounce.
826797	When a dynamic address fails, it becomes 0.0.0.0/0 in the SD-WAN rule.
828121	In a BGP neighbor, the `allowas-in 0` value is confusing and not accepted by the GUI for validation (1-10 required).
828345	Wrong MAC address is in the ARP response for VRRP IP instead of the VRRP virtual MAC.
830254	When changing interfaces from dense mode to sparse mode, and then back to dense mode, the interfaces did not show up under dense mode.

Security Fabric

Bug ID	Description
800986	A downstream FortiGate is sending the `config rusted-list` to FortiManager in the auto update.
803600	Automation stitch for a scheduled backup is not working.
814796	The threat level threshold in the compromised host trigger does not work.
815984	Azure SDN connector has a 403 error when the AZD restarts.
822015	Unable to resolve dynamic address from ACI SDN connector on explicit web proxy.

SSL VPN

Bug ID	Description
626311	SSL VPN users are remaining logged on past the `auth-timeout` value.
676278	Custom host check AV and firewall for macOS fails for FortiClient SSL VPN.
697142	SharePoint server (de***.sc***.gov.sa) is not working on web-based VPN.
767832	After upgrading from 6.4.7 to 7.0.1, the `Num Lock` key is turned off on the SSL VPN webpage.
780765	High CPU usage in SSL VPN using libssh2.

Bug ID	Description
784426	SSL VPN web mode has problems accessing ComCenter websites.
786056	VNC using SSL VPN web mode disconnects after 10 minutes.
789642	Unable to load Grafana application through SSL VPN web mode.
796768	SSL VPN RDP is unable to connect to load-balanced VMs.
799308	SSL VPN bookmark is not working.
805922	Unable to configure ssl.root as the `associated-interface` in a firewall address.
807268	Many SSL VPN users are disconnected periodically, and sslvpnd crashes.
809209	SSL VPN process memory leak is causing the FortiGate to enter conserve mode over a short period of time.
809473	When sslvpnd debugs are enabled, the SSL VPN process crashes more often.
810715	Web application is not loading in the SSL VPN web mode.
811007	The auto-generated URL on the *VPN* > *SSL-VPN Settings* page shows the management IP of the FortiGate instead of the SSL VPN interface port IP as defined on the *VPN* > *SSL-VPN Realms* page when a realm is created.
811492	SSL VPN should not leak information while performing Telnet.
814040	SSL VPN bookmark configuration is added automatically after client logs in to web mode.
814708	The same SAML user failed to establish a tunnel when a stale web session exists with `limit-user-logins` enabled.
816716	sslvpnd crashed when deleting a VLAN interface.
816881	TX packet loss on ssl.root interface.
817843	Logging out of SSL VPN tunnel mode does not clear the authenticated list.
818196	SSL VPN does not work properly after reconnecting without authentication and a TX drop is found.
819296	GUI should not use <server_ip> as a sender to send the SSL VPN configuration (it should use value set in `reply-to`).
823054	Internal website with JavaScript lacks some menus in SSL VPN web mode.
829955	When using SSL VPN to do auto-reconnect without authentication, it always fails the second time it tries to reconnect.
834713	Getting re-authentication pop-up window for VNC quick connection over SSL VPN web proxy.
841705	SSL VPN web mode access is not working for specific configured URLs.

Switch Controller

Bug ID	Description
794026	FortiGates quarantines are stuck at 256.
803307	The *Enable STP* security control description should be reworded to mention that Edge ports should have STP enabled once the network topology is stable.
805154	Switch controller preconfiguration of FortiSwitch 108F-POE is incorrect.
810550	Send DHCP/ARP packet failed, and get `errno = 6` in log when `config-sync` runs.
836604	The `40000cr4` port speed is not available under the `switch-controller managed-switch` port speed settings.

System

Bug ID	Description
675558	SFP port with 1G copper SFP always is up.
686135	The dnp process goes to 100% CPU usage as soon as the configuration is downloaded via SCP. Affected platforms: FGR-60F and FGR-60F-3G4G.
709679	Get `can not set mac address(16)` message after downgrading.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
748409	Client traffic from VLAN to VXLAN encapsulation traffic is failing after upgrading.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.
751870	User should be disallowed from sending an alert email from a customized address if the email security compliance check fails.
764954	FortiAnalyzer serial number automatically learned from miglogd does not send it to FortiManager through the automatic update.
780315	Poor CPS performance with VLAN interfaces in firewall only mode (NP7 and NP6 platforms).
781960	A dhcpd crash log occurs.
783939	IPv4 session is flushed after creating a new VDOM.
787144	FortiExtender virtual interface on the FortiGate is not receiving the IP address when mapping FortiExtender to it.
787595	FFDB cannot be updated with `exec update-now` or `execute internet-service refresh` after upgrading the firmware in a large configuration.

Bug ID	Description
787929	Deleting a VDOM that contains EMAC interfaces might affect the interface bandwidth widget of the parent VLAN.
789153	A profile with higher privileges than the user's own profile can be set.
797428	SNMP status for NPU is not available on NP6xlite.
798091	After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation.
798303	The threshold for conserve mode is lowered.
800294	Interface migration wizard fails to migrate interfaces when VLANs have dependencies within dependencies.
800615	After a device reboot, the modem interface sometimes does not have a stable route with the local carrier.
801040	Session anomaly was incorrectly triggered though concurrent sessions on the FortiGate that were below the configured threshold.
801053	FG-1800F existing hardware switch configuration fails after upgrading.
801474	DHCP IP lease is flushed within the lease time.
805122	In FIPS-CC mode, if `cfg-save` is set to `revert`, the system will halt a configuration change or certificate purge.
805345	In some cases, the HA SNMP OID responds very slowly or does work correctly.
805412	DHCPv6 authentication option offer is not accepted from the server.
807947	Unable to create new interface and VDOM link with names that contain spaces.
809030	Traffic loss occurs when running SNAT PBA pool in a hyperscale VDOM. The NP7 hardware module PRP got stuck, which caused the NP7 to hang.
810104	Under certain trace condition scenarios, a kernel panic may be triggered on new kernel platforms after failover with HTTP CCS followed by SIP64 traffic.
810466	EHP and HRX drop on NP6 FortiGate, causing low throughput.
810583	Running `diagnose hardware deviceinfo psu` shows the incorrect PSU slot.
810879	DoS policy ID cannot be moved in GUI and CLI when enabling multiple DoS policies.
811350	Packets drop when the standby device is turned on.
811367	Ports 33-35 constantly show suspect messaging in the transceiver output. Affected platforms: FG-2600F and FG-2601F.
811449	New DNS system servers with DoT enabled, applying a DNS filter to the FortiGate DNS server fails.
812499	When traffic gets offloaded, an incorrect MAC address is used as a source.
813223	Random kernel panic occurs due to calling `timer_setup`.

Bug ID	Description
813606	DHCP relay offers to iPhones is blocked by the FortiGate.
815360	NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time.
815692	Slow upload speeds when connected to FIOS connection. Affected platforms: NP6Lite and NP6xLite.
816278	Memory increase due to iked process.
816385	When creating an inner VLAN CAPWAP interface or sending inner VLAN traffic when the FortiGate is rebooting/upgrading from `capwap-offload disable` status, these actions trigger a freeze. Affected platforms: NP7 models.
816823	NP6xLite test failed when running `diagnose hardware test pci`.
818461	When an aggregate is created after all VLANs and added to a software switch, all VLANs are lost after rebooting.
819460	There is no `1000auto` option under the ports. Affected platforms: FG-110xE.
819640	SSH public key changes after every reboot.
821366	PPPoE is not working on FG-60E wan2 interface.
823589	When pushing a script from FortiManager to FortiGate, FortiOS will sometimes send the CLI change to FortiManager with the FGFM API. If the tunnel is not up, the session will not exist and it causes a code crash.
824464	CMDB checksum is not updated when a certificate is renewed over CMP, causing a FortiManager failure to synchronize with the certificate.
826440	Null pointer causing kernel crash on FWF-61F.
829598	Constant increase (3%-4%) in memory occurs everyday.
830415	FEX-40D-NAM model support was removed after upgrading to 7.0.6 or 7.0.7.
832948	Signature updating from FortiManager does not work after cloud communication is disabled.
834138	Kernel panic occurs due to VXLAN.
834414	When the uplink modem is restarted, the FortiGate interface configured as PPPoE is unable to obtain an IP address.
834641	Unable to remove DDNS entry frequently, even if the DDNS setting is disabled.
834762	Kernel panics occurs on secondary HA node on NP7 models (7.0.6).
836049	Unexpected device reboots with the kernel panic error on NP7 models.
837110	Burst in multicast packets is causing high CPU usage on multiple CPU cores.
839190	Running `get system auto-update versions` causes newcli to crash and the prints quit at the MAC address database.
840175	Random kernel panic occurs and causes the device to reboot.

Upgrade

Bug ID	Description
803041	Link lights on the FG-1100E fail to come up and are inoperative after upgrading.
803171	Upgrade takes longer than expected, and get `daemon_bits=0x00000040` error when HA upgrades.

User & Authentication

Bug ID	Description
749694	A fnbamd crash is caused by an LDAP server being unreachable.
813407	Captive portal authentication with RADIUS user group truncates the token code to eight characters.
822684	When multiple FSSO CA connections are configured at the same time, only the last configured FSSO connection comes up.
825505	Devices are lost in *Users & Devices* widget after a period of time (around two days) in configurations with FortiSwitch, FortiAP, and DHCP.
825759	The *Device detection* option is missing in the GUI for redundant interfaces (CLI is OK).
833802	RADIUS re-authentication is not following RFC 2865 standards.

VM

Bug ID	Description
786278	Bandwidth usage is not shown when DPDK is enabled.
793914	HA is not in sync when a dynamic AWS service SMTP address object is retrieving a dynamic update from AWS.
798717	Traffic/session logging incorrectly refers to SR-IOV secondary interfaces when the Rx is from fast path.
803219	Azure SDN connector might miss dynamic IP addresses due to only the first page of the network interface being processed.
809963	Get cmdbsvr crash on FG-KVM32 after running concurrent performance test.
820457	Dynamic address objects are removed after Azure API call failed and caused legitimate traffic drop.
825464	Every time the FortiGate reboots, the certificate setting reverts to `self-sign` under `config system ftm-push`.

WAN Optimization

Bug ID	Description
804662	WANOpt tunnels are not established for traffic matching the profile.

Web Application Firewall

Bug ID	Description
817673	Problem accessing some web servers when WAF and AV are enabled in same policy (proxy inspection mode).

Web Filter

Bug ID	Description
789804	Web filter configured to restrict YouTube access does not work.
816781	FGSP cluster with UTM blocks websites when NTurbo or offloading is enabled.

WiFi Controller

Bug ID	Description
790367	FWF-60F has kernel panic and reboots by itself every few hours.
796036	Manual quarantine for wireless client connected to SSID on multi-VDOM with `wtp-share` does not work.
807605	FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA.
807713	FortiGate is not sending RADIUS accounting message consistently to RADIUS server for wireless SSO.
809623	CAPWAP traffic is dropped when `capwap-offloading` is enabled.
811953	Configuration installation from FortiManager breaks the quarantine setting, and the VAP becomes undeletable.
821803	Wireless multicast traffic causes the cw_acd process to have high CPU usage and triggers a hostapd crash.

Bug ID	Description
824441	Suggest replacing the *IP Address* column with *MAC Address* in the *Collected Email* widget.
827902	CAPWAP data traffic over redundant IPsec tunnels failing when the primary IPsec tunnel is down (failover to backup tunnel).
831932	The cw_acd process crashes several times after the system enters conserve mode.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
846234	FortiOS 7.0.8 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684
846854	FortiOS 7.0.8 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684

Known issues

The following issues have been identified in version 7.0.8. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
818092	CDR archived files are deleted at random times and not retained.

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.

Explicit Proxy

Bug ID	Description
823319	Authentication hard timeout is not respected for firewall users synchronized from WAD user.

Firewall

Bug ID	Description
631814	*Static route configuration* should not be shown on address dialog page if the address type is an IP range.
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.

Bug ID	Description
	Workaround: rename the custom section to a unique name between IPv4 and IPv6 policies.
728734	The VIP group hit count in the table (*Policy & Objects* > *Virtual IPs*) is not reflecting the correct sum of VIP members.
835413	Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0.

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.
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.
719476	FortiLink NAC matched device is displayed in the CLI but not in the GUI under *WiFi & Switch Controller* > *NAC Policies* > *View Matched Devices*.
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.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
818426	Unable to add spokes or retrieve the configuration key from ADVPN.
831885	Unable to access GUI via HA management interface of secondary unit.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
777394	The flip timer does not start counting down when there is a ping sever failure following a previous outage.
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.
811535	HA failure occurs on pair of FG-2600s due to packet loss on heartbeat interface.
813207	Virtual MAC address is sent inside GARP by the secondary unit after a reboot.
831051	A port with a disabled status still shows in the GUI as being up. The device information in the CLI also shows the `Admin` and `link_status` as up.
839549	Secondary FortiGate unit in an HA cluster enters conserve mode due to high memory consumption by node scripts.

Hyperscale

Bug ID	Description
763966	FGSP synchronizes NP sessions of all VDOMs when syncvd is only set for hyperscale VDOM.
782674	A few tasks are hung on issuing `stat verbose` on the secondary device.
795853	VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM.
807476	After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
836976	Traffic impact on changing from log to hardware to log to host during runtime (with PPA enabled).
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
842008	After HA failover, session count cannot synchronize on secondary FortiGate.
842659	`srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS.

Bug ID	Description
843132	After dynamically adding an ACL policy, the existing matched session is not cleared immediately.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
843266	Diagnose command should be available to show `hit_count/last_used` for policy route and NPU session on hyperscale VDOM.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.
844421	The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.

Intrusion Prevention

Bug ID	Description
813727	Custom signatures are not shown in the list when filters (server, client, or critical severity) are applied in an IPS sensor.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
819276	After changing the password policy to enable it, all non-conforming IPsec tunnels were wiped out after rebooting/upgrading.

Log & Report

Bug ID	Description
820940	On the *Log Settings* page, a VDOM administrator can force a FortiCloud log out of for all VDOMs.
836846	Packet captured by firewall policy cannot be downloaded.

Proxy

Bug ID	Description
727629	WAD encounters signal 11 crash at `wad_http_marker_uri`.
836101	WAD memory leak occurs.

Routing

Bug ID	Description
618684	Static route will still in routing table after HA failover, and the BFD is down on the new primary.
817670	IPv6 route redistribution metric value is not taking effect.
833800	The `speed-test-server` list cannot be loaded due to limited buffer size.
847037	FortiGate is sometimes not following the policy route to forward traffic and sens unreasonable ARP requests.

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.
825291	FortiAnalyzer connection security rating fails for FortiAnalyzer Cloud.

SSL VPN

Bug ID	Description
719740	The *No SSL-VPN policies exist* warning should not be shown in the GUI when a zone that has ssl.root as a member is set in an SSL VPN policy.
746230	SSL VPN web mode cannot display certain websites that are internal bookmarks.
803576	Comments in front of `<html>` tag are not handled well in HTML file in SSL VPN web mode.
808569	sslvpnd crashes when no certificate is specified.

Bug ID	Description
820536	SSL VPN web mode bookmark incorrectly applys a URL redirect.
822432	SSL VPN crashes after copying a string to the remote server using the clipboard in RDP web mode when using RDP security.

Switch Controller

Bug ID	Description
813216	FortiLink goes down when CAPWAP offloading is enabled or disabled.
818116	Add link status to managed FortiSwitch switch ports.

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.
799487	The debug zone uses over 400 MB of RAM.
813162	Kernel panic occurs after traffic goes through IPsec VPN tunnel and EMAC VLAN interface.
818795	Kernel panic observed on FG-3700D.
847314	NP7 platforms may encounter random kernel crash after reboot or factory reset.
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.

User & Authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work as expected.

Bug ID	Description
813969	SAML SSO login for VDOM administrator still works when logging in to the FortiGate and the connecting interface does not belong to that VDOM.
836082	LLDP packets are not being received if mgmt is used as an HA management reservation interface.
846683	Downloading the CSR certificate from global with a custom account profile (read/write) causes GUI/CLI errors due to unauthorized requests.

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`.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

ZTNA

Bug ID	Description
832508	The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.2.1 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`. After upgrading from 7.2.0 to 7.2.1, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled. **Workaround**: unset the `ztna-ems-tag` in the ZTNA firewall proxy policy, and then set it again.
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
590623	Strange padding occurs in certificate after deep inspection (`ICAgICAg...`).
673117	TFTP traffic does not work well when TFTP application is set in security policy.
687885	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing.
757322	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing using frame size 68 and SR-IOV interface.
781110	Lost packets with security (UTM) profiles and third party WAN optimizer (Riverbed).
789861	Globus file transfer traffic breaks when web filter profile is enabled along with certificate inspection.
791175	Unable to access specific website after upgrading the IPS engine version.
798961	High CPU usage occurs on all cores in system space in __posix_lock_file for about 30 seconds when updating the configuration or signatures.
800524	IPS engine version 6.004.114 has crash with signal 11.
800730	When using NGFW policy based mode, modifying a security policy causes all sessions to be reset.
800731	Flow mode AV sends HTML files every time to the FortiGate Cloud Sandbox when it is not configured in the file list.
802683	IPS debug filter is not working.
804500	Changes to the custom URL filter cause a network degradation that impacts customers.
810105	Signal 14 (alarm clock) received when updating and during hasync crash.
811551	Traffic drop in NGFW mode post upgrading.
816032	Security policy with FSSO authentication sporadically does not match.
816759	IPS engine 5.00272 crash on `ovrd_ssl_read`.
817902	IPS engine 6.004.128 crashes with signal 11.
827253	Only traffic to pure IPv6 is blocked, and traffic to obfuscated IPv6 is not detected by FortiOS.
839679	IPS engine version 6.004.139 has crash with signal 11.
840232	The hostname in syslog is short.
841269	When using SSL certificate inspection, no block page appears when application control and web filter are enabled on the same policy.

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