FortiManager FortiGuard services configuration overview

This document was initially written for firmware version 4.0, however most of this information can also apply to version 3.0. It has been updated to contain the latest changes added in 5.0 as well as within various 4.0MR3 patches.

FortiGuard services represent the anti-virus, IPS, web-filtering and anti-spam update services.
Historically the AV/IPS service has been referred to as the FDS service, and the WF/AS service as the FortiGuard service. Currently, the term "FortiGuard" covers all services, however certain FortiManager GUI or CLI configuration sections continue to refer to them using the older terminology. This document covers the various FortiGuard configuration settings that can be configured on the FortiManager, FortiGate and FortiClient, and also explains which ones are required on each device in order to function properly. A basic communication diagram displays the devices concerned and the communication direction. Some debug commands are also provided in order to help diagnose potential configuration problems.

Terminology used in this document:
FMG = FortiManager
FGT = FortiGate
FC = FortiClient
FDS = AV/IPS service
FGD = WF/AS service
FDN = Fortinet Distribution Network (public FDS service)
AV = Anti-Virus
IPS = Intrusion Prevention System
WF = Web-Filtering
AS = Anti-Spam
GUI = Graphical User Interface = Web browser interface

FortiManager FortiGuard Center

Note: New in 5.0 FOS
The following CLI configuration has been added:

```
config system central-management
       set fortimanager-fds-override enable | disable
end
```

The following CLI configuration has been removed:

```
config system fortiguard
    set srv-ovrd enable
        config srv-ovrd-list
            edit 1
                set ip x.x.x.x
            next
        end
    set client-override-status enable
    set client-override-ip x.x.x.y
end

config system autoupdate clientoverride
    set address x.x.x.x
    set status enable
end
```

```
config system autoupdate override
    set address "x.x.x.y"
    set fail-over disable
    set status enable
end
```

Note: New in FMG 4.0 MR3 Patch 3 and 5.0
A new CLI only setting was added to force the FMG to only contact the configured 'server-override' servers for av-ips & web-spam fct/fgt services. Prior to this, the FMG would fallback to a cached list of backup FDS servers should the override not be available. Configuring this new setting, will prevent this fallback from occurring.

```
config fmupdate server-override-status
set status strict
end
```

In order to allow the FMG to fallback to backup FDS servers, the setting must be set to 'loose'

```
config fmupdate server-override-status
set status loose
end
```

A GUI option for this configuration setting was added in 4.3.7 and 5.0:
System Settings -> FortiGuard Center -> Configuration -> Server Override Mode

Server-override configurations can now contain a list of servers, whereas previously it was only a single entry. Example:

```
config fmupdate av-ips fgt server-override
config servlist
edit 1
set ip 10.10.1.1
set port 443
next
edit 2
set ip 10.10.1.2
set port 443
end
end
```

Another new CLI command was added to conserve memory on systems which will not be providing Web-Filtering and AntiSpam services to Fortigates, but that still require to download these databases in order to provide them to a downstream FMG unit which will be providing that service to the FGTs. Setting the following parameter will avoid loading and caching the URL/SPAM db into memory:

```
config fmupdate multilayer
set webspam-rating disable
end
```

Note: New in FMG 4.0 MR3 Patch 4 and 5.0
A new CLI only setting was added to improve Web Filtering performance on units with at least 6GB of memory.

```
FMG1000C # conf fmupdate web-spam fgd-setting

(fgd-setting)# sh
config fmupdate web-spam fgd-setting
    set wf-cache 1000
    set wf-preload enable
end

(fgd-setting)# get
as-cache            : 300
as-preload          : disable
av-cache            : 300
av-preload          : disable
update-interval     : 6
wf-cache            : 1000
wf-preload          : enable

(fgd-setting)#
```

To load the entire web filtering db to memory, you can set the *wf-cache* value to *2800* (memory permitting).

Note: New in FMG 4.0 MR3 Patch 6 and 5.0
Changes to the FortiGuard Event and internal logging configuration.

Obsolete:
```
config fmupdate fgd-log
```

Replaced by:
```
config fmupdate web-spam fgd-setting
(fgd-setting)# get
as-log              : all
av-log              : disable
max-log-quota       : 6144
stat-log-interval   : 60
update-log          : enable        <<< logs detailed activity of fgdupd process
wf-log              : all
```

Note: New in FMG 4.0 MR3 Patch 7 and 5.0
A new CLI command is added in 4.3.7 to enable the logging of the WF/AS client requests to Event log file. This will only work if the 'as-log' and 'wf-log' settings are set to 'all'. This is not recommended for regular production use, as it will reduce performance. Only use for troubleshooting.

```
conf fmupdate web-spam fgd-setting
eventlog-query      : disable
```

FMG GUI Section: System *Settings->FortiGuard Center->FortiGuard AntiVirus and IPS Settings*

GUI Setting: *Enable FortiClient Service*
CLI Setting:
```
config fmupdate fct-services
set status enable
set port 80
```
By default it is enabled to provide FDS update services to PCs running FortiClient software on port 80. FC by default uses port 443 for such updates, therefore when configured to obtain them from the FMG, the different port must be specified on the FC application. Port 443 can't be used on the FMG for this service.
Communication: FMG ← FC

FC GUI Section: *Maintenance->Update->Use this server to update*: xxx.xxx.xxx.xxx:80

GUI Setting: *Use Override Server Address for FortiClient*
CLI Setting:
```
config fmupdate av-ips fct server-override
set ip xxx.xxx.xxx.xxx
set port xxxx
set status enable
```
Use this command to override the default IP address and port that the FMG contacts when requesting Antivirus updates for FortiClient from either the public FDS network or a private upstream FMG. If configured to obtain the updates from another upstream FMG, then the port must be configured as "8891".
Communication: FC-FDS/FMG ← FMG
Debug with:
```
diag fmupdate fct-serverlist
diag fmupdate fct-log
```

GUI Setting: *Use Override Server Address for FortiGate/FortiMail*
CLI Setting:
```
config fmupdate av-ips fgt server-override
set ip xxx.xxx.xxx.xxx
set port xxxx
set status enable
```
Use this command to override the default IP address and port that the FMG contacts when requesting Antivirus and IPS updates for FortiGate units from the either the public FDS network or a private upstream FMG. If configured to obtain the updates from another upstream FMG, then the port must be configured as "8890".
Communication: FDS/FMG ← FMG
Debug with:
```
diag fmupdate fds-serverlist
diag fmupdate fds-log
```

GUI Setting: *Allow Push Update*
CLI Setting:
```
config fmupdate av-ips push-override
set ip xxx.xxx.xxx.xxx
set port xxxx
set status enable
```
Use this command to enable or disable push updates for the FMG, and to override the default IP address and port to which the FDN sends Antivirus and IPS push announcement messages. Default port is 9443 (UDP) for FGT updates and 9444 (UDP) for FC updates. The port used for FC updates will always be the one configured here, plus 1. For example, if it is configured for port 2000, then Push announcement for FC will be done to 2001. This allows the FMG to quickly retrieve AV/IPS packages from our public

FDS network. This is useful if push notifications must be sent to an IP address and/or port other than the FortiManager unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiManager unit. When configured, it will also add this IP/Port to the UDP PUSH announcement notification message which is sent to the FGT.
Communication: FC-FDS/FDS ↔ FMG → FGT
Debug with: `diag sniff packet any 'port x' 3`

GUI Setting: NONE
CLI Setting:
```
config fmupdate av-ips push-override-to-client
set status enable
config announce-ip
edit 1
set ip xxx.xxx.xxx.xxx
set port xxxx
next
end
```
When configured, this will be the only IP(s) and port(s) which will be announced to the FGT in the PUSH announcement notification, so that the FGT can connect to that IP/Port to obtain the AV/IPS update. Configure an IP (or list of IPs) different than what is on the external interface, if the FMG is NATted when accessing FGTs. When this is configured, the FMG's interface(s) IPs and "config fmupdate av-ips push-override" values are not included in the PUSH announcement.
Communication: FMG → FGT
Debug with: `diag sniff packet any 'port x' 3`

GUI Setting: *Enable AntiVirus and IPS Update Service for Private Server*
CLI Setting:
```
config fmupdate server-access-priorities
set av-ips enable
end
```
This will provide the list of configured private server IP addresses to the FGT unit as possible servers that it can contact to, in order to obtain FDS updates.
Communication: FMG ↔ FGT
Debug with:
FGT:
```
diag deb appli update 255
diag test update info
```

GUI Setting: *Schedule Regular Updates*
CLI Setting: `config fmupdate av-ips update-schedule`
This configures the interval for which the FMG will contact the FDS server to check to see if there are new AV/IPS packages to download.
Communication: FDS ← FMG
Debug with:
FMG:
```
diag fmupdate fds-log
diag fmupdate fds-updatenow
```

FMG Note:
The FMG provides FDS services for FGT on port 8890 whereas our public FDS servers provide them on port 443.

FGT Note:
By default, the FGT connects to our FDS network on port 443 for AV/IPS updates. However when configured to obtain them from a FMG, the port must be changed to 8890, as follows:

FGT configuration:

```
config system autoupdate override
set status enable
set address xxx.xxx.xxx.xxx:8890
set fail-over enable | disable
end
```

If the *fail-over* option is enabled, the FGT will fallback to public FDS servers in order to obtain AV/IPS updates, if the FMG is unreachable. Set to *disable* if the FMG is the only FortiGuard server that the FGT must contact

Only once a manually triggered AV/IPS update from the FGT to the FMG is successful, can the PUSH update be configured on the FGT. If an override PUSH IP is configured on the FGT, the FGT must first send this information to the FMG via an update process and only then will the FMG send the PUSH announcement payload to the configured override IP and port. The fact that this may be configured on the FGT, and Retrieved by the FMG within *Device Manager->Configuration* is insufficient to have it send the announcement correctly. When *Allow Push Update* is enabled on the FGT, the FMG will send the UDP PUSH Notification message to the IP which the FGT used to connect to the FMG (unless the *Use override push IP* is configured on the FGT). Within the UPD Notification message payload, the FMG will include the IP address(s) of its interfaces which have the 'FortiGate Updates' service enabled, and will announce this for port 8890. Two FMG settings will modify what is announced within the PUSH notification message (see details above):

```
config fmupdate av-ips push-override
config fmupdate av-ips push-override-to-client
```

FGT configuration:

```
config system autoupdate push-update
set status enable
set override enable
set address yyy.yyy.yyy.yyy
set port xxxx (default 9443 but can be changed)
end
```

FMG GUI: ***System Settings->FortiGuard Center->FortiGuard Web Filter and AntiSpam (Email Filter) Settings***

GUI Setting: *Enable Server Override [Use Override Server Address for Fortigate/FortiMail]*
CLI Setting:

```
config fmupdate web-spam fgt server-override
set ip xxx.xxx.xxx.xxx
set port xxxx
set status enable
end
```

When configured, this will be the only FGD server (public or other private upstream FMG), that the FMG will contact to obtain WF/AS updates for FGT. If configured to connect to another upstream FMG, then the port must be specified as “8900”.
Communication: FGD/FMG ← FMG
Debug with:

```
diag fmupdate fgd-serverlist
diag fmupdate fgd-log
```

GUI Setting: NONE
CLI Setting:

```
config fmupdate web-spam fct server-override
set ip xxx.xxx.xxx.xxx
set port xxxx
```

```
end
```

When configured, this will be the only FGD server (public or other private upstream FMG), that the FMG will contact to obtain WF/AS updates for FC. If configured to connect to another upstream FMG, then the port must be specified as "8901".
Communication: FC-FGD/FMG ← FMG
Debug with:

FMG:
```
diag fmupdate fgc-log
diag fmupdate fgc-serverlist
```

GUI Setting: *Enable Web Filter and AntiSpam [Email Filter] Update Service for Private Server*
CLI Setting:
```
config fmupdate server-access-priorities
set web-spam enable
end
```

This will provide the list of configured private server IP addresses to the FGT unit, as possible servers that it can contact to in order to obtain FGD updates.
Communication: FMG ↔ FGT

GUI Setting: *Additional number of private FortiGuard servers (excluding this one)*
CLI Setting:
```
config fmupdate server-access-priorities
config private-server
edit 1
set ip xxx.xxx.xxx.xxx
end
end
```

This configures the list of private server IPs which can provide FDS and FGD services. These are typically other FMG units, with FortiGuard services enabled, however the list can also contain one or more public FDS/FGD servers. This list would determine exactly which FDS and FGD servers the FGT would try to contact, unless configured otherwise on the FGT unit directly. The FGT obtains this list when the FGD service is initialized for the first time, and the INIT command is sent to the server.
Communication: FMG ↔ FGT
Debug with:

FGT:
```
diag deb rating
diag test appl urlfilter 15
diag test appl urlfilter 99
diag test update info
diag debug appl update 255
```

GUI Setting: *Allow FortiGates to Access Public FortiGuard servers when Private Servers are Unavailable*
CLI Setting:
```
config fmupdate server-access-priorities
set access-public enable
end
```

When enabled, the FMG will provide the complete list of public FGD servers to the FGT (which it obtains when connecting to either the default FGD server or an override public server), when the FGT initializes the FGD service with the FMG. The FGT will then have the FMG's IP (i.e. private server) on top of the list, with the rest of the public FGD servers below it.
Communication: FMG ↔ FGT
Debug with:

FGT:
```
diag deb rating
diag test appl urlfilter 15
diag test appl urlfilter 99
```

```
diag test update info
diag debug appl update 255
```
FMG:
```
diag fmupdate fgd-serverlist
```

GUI Setting: NONE
CLI Setting:
```
conf fmupdate server-access-priorities
set lookup_default_server disable
end
```
Default value is enable. Disable to prevent FortiManager connectivity to public default FDS and FGD servers (forticlient.fortinet.net, fds1.fortinet.com, fgd1.fortigate.com, guard.fortinet.net)
Communication: FC-FGD/FGD/FDS/FC-FDS ← FMG
Debug with:
```
diag fmupdate fgd-serverlist
diag fmupdate fds-serverlist
diag fmupdate fds-log
diag fmupdate fgd-log
```

GUI Setting: *Disable Communication with FortiGuard Servers* (New in 5.0)
CLI Setting:
```
conf fmupdate publicnetwork
set status enable
end
```
Disable this when the FMG is used in a closed network. When disabled, the AV/IPS/license packages must all be updated manually, and are no longer automatically retrieved from the public FDS server(s). They are manually imported via *Device Manager->Group->Service Usage->Statistics->Manual Update*. The AV/IPS packages must be first manually downloaded from support.fortinet.com. The correct .pkg file must be downloaded and properly distributed to the FGT unit. It is possible to incorrectly distribute and install the wrong AV/IPS package on the FGT. The install is done from FMG to FGT directly via the fgfm protocol or ssh/scp (FMG 3.0)
Communication: FMG → FGT

FortiManager Global Objects configuration

The following FMG Global Object configurations result in the following FGT configuration changes.

FMG GUI: *Global Objects->Device Settings->FortiGuard*

Use override server address for FortiGuard AV/IPS Service : 9.9.9.9:8890
Use override server address for FortiGuard Web Filtering and AntiSpam Service : 8.8.8.8

FGT configuration changes:

```
config system autoupdate override
set status enable
set address "9.9.9.9:8890"
end
config system fortiguard
set hostname "8.8.8.8"
set antispam-status enable
set antispam-cache disable
set webfilter-status enable
end
```

FGT FortiGuard Override and Load Balancing

Using FortiGuard override address(s) on FGT will ONLY use those IPs for FGD services. It will not use any IPs that might be configured on FMG as private or public servers. Multiple IPs may be configured here as backups:

```
config system fortiguard
    set srv-ovrd enable
        config srv-ovrd-list
            edit 1
                set addr-type ipv4
                set ip 192.168.182.242
            next
        end
     end
```

The FGT may be configured to perform load-balancing amongst various FGD servers. These servers could be configured directly on the FGT as override ones, or obtained from the FMG, and could be only private and/or public. Specify how many servers need to be used in a round-robin fashion:

```
config system fortiguard
set load-balance-servers 2
end
```

The network diagram below indicates a two-tier FMG model, where the first one connects to the public Fortinet FDS/FGD servers via the Internet, and the second one connects to the upstream FMG to obtain its updates. The FGT and FC connect to the second downstream FMG for its FortiGuard services: