TECHNICAL NOTE

Fortinet Distribution Network

Accessing and Debugging FortiGuard Services

FORTINET

www.fortinet.com

Fortinet Distribution Network Technical Note
Accessing and Debugging FortiGuard Services
6 June 2007
07-30000-0239-20070606

Trademarks

Contents

Introduction

This chapter introduces you to the Fortinet Distribution Network (FDN) and the following topics:

- Revision history
- About the Fortinet Distribution Network
- About this document
- Fortinet documentation
- Customer service and technical support

Revision history

Version	Date	Description of changes
First Release	30 Sept. 2005	First version.
2	9 May 2006	Changes to “FortiGuard Antivirus and IPS” on page 13: • Added “Enabling Push Updates through a NAT device” on page 17 Changes to “FortiGuard Web Filtering and Antispam” on page 21: • Rewrote this chapter because of updates to FortiGuard Antispam and Web Filtering server selection algorithms. Added new information for FortiOS v3.0 and v2.80 MR12 • Added “Using the FortiOS v2.80 web-based manager (all maintenance releases)” on page 28 and “Using the FortiOS v2.80 web-based manager (all maintenance releases)” on page 28 • Added “Troubleshooting some common FortiGuard Web Filtering and Antispam problems” on page 36.
3	6 June 2007	Updated “About the Fortinet Distribution Network” on page 7 to mention that the FDN provides many services, not just FortiGuard Antivirus, IPS, Web Filtering and Antispam. Also updated “About this document” on page 7 to reflect that this document focuses on the FortiGuard services provided by the FDN, and updated references to FortiGuard Distribution Network with Fortinet Distribution Network. Updated references to FortiManager Update Center with its new name in the FortiManager GUI, FortiGuard Center. Updated “Push” on page 14 to clarify that no update downloads occur on the push (UDP 9443) connection; it is only notification that an update is available. Updated “Pull and push update ports” on page 15 to include other services and devices that also use those ports. Generalized “Enabling Push Updates through a NAT device” on page 17 to include FortiManager units. Specified email protocols in “FortiGuard Web Filtering and Antispam” on page 21. (FortiGuard Antispam does not currently apply to webmail traffic.) Added FortiManager behavior and FortiGuard Web Filtering and Antispam database update port to “FortiGuard Web Filtering and Antispam ports” on page 24.

About the Fortinet Distribution Network

The Fortinet Distribution Network (FDN) is a geographically diverse network operated by Fortinet Inc. that provides many types of services to Fortinet products, including FortiGuard Antivirus (AV) and FortiGuard Intrusion Prevention System (IPS) updates and FortiGuard Web Filtering and FortiGuard Antispam updates and query services. This document primarily focuses on the interaction of the FortiGate product line with the FDN. The interaction of the FDN with the other products (including FortiMail, FortiClient, and FortiManager) is very similar.

About this document

This document explains the FDN components and how FortiGate units connect to and interact with the FDN to receive FortiGuard services. This document also describes the debugging commands and diagnostic methods that can be used if the FortiGate unit has problems connecting to and using FortiGuard services.

This document does not cover configuration procedures. For detailed configuration procedures, see your Fortinet product documentation (available from the Fortinet Technical Documentation web site.

This document contains the following chapters:

- FDN network architecture
- FortiGuard Antivirus and IPS
- FortiGuard Web Filtering and Antispam

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet documentation CDs

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

FDN network architecture

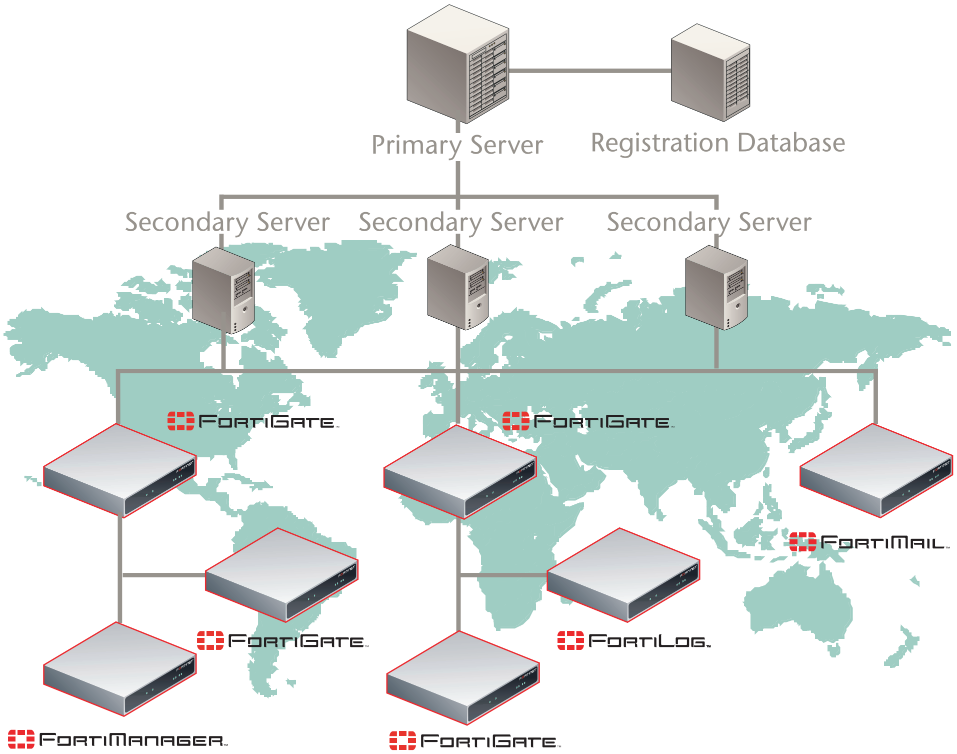
The Fortinet Distribution Network (FDN) is a geographically diverse network operated by Fortinet Inc. that provides FortiGuard Antivirus (AV) and FortiGuard Intrusion Prevention System (IPS) updates in addition to FortiGuard Web Filtering and FortiGuard Antispam services to all Fortinet products. This document primarily focuses on the interaction of the FortiGate product line with the FDN. The interaction of the FDN with the other products (including FortiMail, FortiClient, and FortiManager) is very similar.

This chapter describes:

- FortiGuard registration database
- Primary FDN server
- Secondary FDN servers
- FortiGate units and other Fortinet products
- FortiManager’s FortiGuard Center
- FDN network monitoring

Figure 1 shows the architecture of the FDN.

Figure 1: Fortinet Distribution Network architecture



FortiGuard registration database

The FortiGuard registration database contains all the customer FDN contracts for FortiGuard Antivirus, FortiGuard IPS, FortiGuard Web Filtering, and FortiGuard Antispam services. Fortinet Technical Support maintains the registration database. The registration database is changed whenever a customer contract is added or changed.

Primary FDN server

The primary FDN server provides the interface that the Fortinet FortiGuard team uses to add updates to the FDN. When updates are added, the primary server automatically pushes the updates to the secondary servers and confirms that the secondary servers are up-to-date.

The primary server also periodically retrieves new Fortinet customer contract information from the registration database and pushes updates to the secondary servers.

The primary server also maintains a list of all the IP addresses and time zones of the deployed secondary servers. Periodically, the primary server verifies that each secondary server has an up to date version of the secondary server list and pushes changes to the secondary servers as required.

Secondary FDN servers

The globally distributed secondary FDN servers provide FortiGuard updates and services to registered Fortinet products (for example, registered FortiGate units). The registered FortiGate units communicate with secondary servers, never with the primary server.

Secondary servers respond to requests from FortiGate units. When a FortiGate unit requests a FortiGuard service from a secondary server, the secondary server verifies the FortiGate unit contract information before providing the requested service.

Secondary servers also send push update notifications to FortiGate units to prompt the FortiGate units to request an update. These update requests are sent by the FortiGate unit and include identifying information.

If the secondary server cannot find the requesting FortiGate unit in its customer contract list, the secondary server checks with the primary server to determine the contract status of the FortiGate unit.

If the primary server cannot verify the status of the FortiGate unit, the primary server generates expired contracts for all FortiGuard services for this FortiGate unit and distributes this information to all secondary servers. As a result all secondary servers will refuse requests from the unregistered FortiGate unit until the FortiGate unit has been registered with Fortinet Technical Support.

When requested by a FortiGate unit, secondary servers also provide an up-to-date list of all secondary server IP addresses and associated time zones.

FortiGate units and other Fortinet products

FortiGate units and other Fortinet products communicate with secondary FDN servers to receive FortiGuard Antivirus and IPS updates and to request FortiGuard Web Filter and Antispam services. As already described, the request from the FortiGate unit includes identifying information and the secondary server verifies the contract status of the FortiGate unit before providing the requested update or service.

Depending on their configuration, FortiGate units receive push updates from secondary FDN servers, request scheduled updates, and request FortiGuard Web Filtering and Antispam services. FortiGate units also send IP address updates if the IP address of the FortiGate interface that is routable to the FDN changes.

To communicate with the FDN, FortiGate units use a selection process to determine a preferred secondary FDN server. For information about how FortiGate units select a preferred secondary server, and what happens if that secondary server does not respond, see “FDN setup and selecting a preferred secondary server” on page 13 and “Web Filtering and Antispam server selection” on page 22.

FortiManager’s FortiGuard Center

FortiManager’s FortiGuard Center can act as a local FDN server (FDS) to provide FortiGuard updates and services to FortiGate units. Using a FortiManager as a private FDS reduces the amount Internet bandwidth used for FortiGuard services, and also makes it possible for FortiGate units that cannot connect to the Internet to receive FortiGuard updates and services.

FortiManager’s FortiGuard Center automatically keeps itself up-to-date by periodically querying the closest secondary FDN server for Antivirus, IPS, Web Filtering, and Antispam updates. If updates are available, they are downloaded to the FortiManager’s FortiGuard Center for re-distribution to requesting FortiGate devices.

Contract information is not pushed from secondary servers to the FortiManager’s FortiGuard Center. Instead, the FortiManager’s FortiGuard Center periodically polls the closest secondary server for this information.

Secondary servers also update the FortiManager’s FortiGuard Center secondary server IP address and time zone list so that the FortiManager’s FortiGuard Center can also select the closest secondary server and find a backup secondary server if the closest one does not respond.

FDN network monitoring

Fortinet has installed monitors throughout the FDN to verify that all secondary servers are operating and have the latest update packages and database updates. In addition, the monitors validate that all secondary servers are able to respond to update requests properly. When a monitor detects a server failure, the Fortinet operations team is notified immediately of the problem. The operations team can quickly debug and fix the problem or replace the failed secondary server.

FortiGuard Antivirus and IPS

This chapter describes how the FDN provides antivirus and IPS updates to FortiGate units and other Fortinet products. Antivirus and IPS updates can be provided using a pull or push model or a combination of both.

Antivirus updates consist of updates to the antivirus engine as well as updates to antivirus definitions. The antivirus engine is the software that powers Fortinet antivirus detection. Antivirus definitions consist of virus signatures and related data used by the antivirus engine to detect viruses in network traffic.

IPS updates consist of updates to the IPS engine as well as updates to IPS definitions. The IPS engine is the software that powers the Fortinet IPS. IPS definitions consist of attack signatures and related data used by the IPS engine to detect attacks in network traffic. IPS is also called Intrusion Protection by some Fortinet products.

This chapter describes:

FDN setup and selecting a preferred secondary server

When a FortiGate unit starts, it sends a setup message to the FDN that includes the FortiGate unit firmware version, time zone, and preferred update method.
If push updates are configured, the setup message also includes the IP address of the FortiGate interface that is routable to the FDN and the port on which the FortiGate unit listens for push updates.

The secondary server that receives the setup message queries the primary server to determine the contract status of the FortiGate unit. The first time the FortiGate unit communicates with the FDN for updates, it uses update.fortiguard.net as the initial contact point. During the first update request, the list of secondary FDN servers are returned to the FortiGate unit and stored in a file. The FortiGate unit then sorts this list by closest time zone. For future communications with the FDN, the FortiGate unit selects a preferred secondary server using the following criteria:

1. Configured override server (typically a FortiManager’s FortiGuard Center) if enabled.
2. Update announcement sender (for push updates).
3. Secondary server in the closest time zone.
4. The next secondary server in the list according to time zone.

5 update.fortiguard.net.

The FortiGate unit uses the preferred secondary server as selected above and only drops to the next server in the list if the preferred server does not respond. The FortiGate unit uses update.fortiguard.net as a last resort if a preferred server cannot be contacted.

Full and delta FDN updates

The FDN can provide full or delta updates. Full updates include the entire update item; for example, all current antivirus definitions. Full updates can be quite large and transferring them can use a large amount of network bandwidth. The FDN can also provide delta updates that contain only the differences between the current version installed on the FortiGate unit and the latest version available from the FDN. Delta updates greatly reduce the amount of bandwidth required to deliver updates and increase the number of FortiGate units each secondary server can update in a given amount of time.

FortiGate units always receive delta updates from secondary servers if available. If the current version installed on the FortiGate unit is too out of date or if another problem occurs when retrieving a delta update, the FortiGate unit instead retrieves the full update package from the secondary server.

Tracking update status

When new updates are pushed to secondary servers by the primary server, a unique token is associated with the update package. When a FortiGate unit retrieves the update from the secondary server, this token along with the FortiGate unit serial number is returned to the primary server. This allows the primary server to track which FortiGate units are up-to-date and which are not.

Pull or scheduled updates

One method for the FortiGate unit to update itself is to use pull updates. Pull updates can be requested manually by a FortiGate administrator or are requested automatically by the FortiGate unit according to the configured update schedule.

The FortiGate unit contacts the secondary server directly and requests any applicable updates. The secondary server returns a response that includes the applicable update packages. The FortiGate unit then installs the received updates.

Push

FortiGate and FortiManager units can also be configured to receive FortiGuard Antivirus and IPS updates pushes. When new updates are available, the FDN notifies all units configured to receive update pushes, indicating that an update is available. The units then acknowledges the message, and initiate the update pull.

The FDN can send announce messages to FortiGate units because of the setup messages that each FortiGate unit sends to the secondary server. For push updates, the setup message includes the IP address of the FortiGate unit interface that is routable to the FDN and the configured push update port. When the push configuration or the IP address changes, the FortiGate unit sends another setup message to inform the FDN of the change. The secondary server periodically sends this configuration information to the primary server.

When a new update is available, the primary server compiles lists of FortiGate units requiring push updates. One list is created for each secondary server. Each list includes the FortiGate units in the nearest time zones to the secondary server. The primary server pushes each list to each secondary server.

Each secondary server sends an announce message consisting of four packets to each FortiGate unit in its push update list. The announce message informs the FortiGate unit that an update is available. Each FortiGate unit should acknowledge the announce message. The secondary server continues to send announce messages to any FortiGate units that do not respond every minute for 5 minutes.

The FortiGate unit waits a random amount of time (between 1 and 120 seconds) before requesting an update in response to the announce message. The wait time reduces the surge in traffic since every FortiGate unit receives the announce message at about the same time. The FortiGate unit requests the update from the override server (if configured) or the push announcement sender. If the update cannot be retrieved from either of these servers, the FortiGate unit follows the preferred server selection list for further attempts. The update request proceeds in the same way as a regular pull update request. For a complete description, see “Pull or scheduled updates” on page 14.

At 15 minutes and 30 minutes after the update is available, the primary server checks the update status of each FortiGate unit in its database. If any FortiGate units have not yet updated themselves in response to the announce message, the primary server regenerates the push update lists to include the FortiGate units that have not received updates. The primary server then sends these new push update lists to the secondary servers. The secondary servers then start another push update attempt.

Any FortiGate units that are not updated after these attempts are made, must wait for their configured scheduled update or for the next push update.

Pull and push update ports

The FDN provides firmware images and RVS and FortiGuard database and engine updates on TCP port 443 (port 8890 for FortiOS 2.50). Any firewalls upstream from the unit should be configured to allow SSL connections through this port from the unit to the Internet.

If push is enabled, upstream firewalls should also be configured to allow UDP packets on port 9443 from the Internet to the unit. In the event that this port is not suitable, another port can be configured for push updates (the FortiGate or FortiManager unit setup message informs the FDN of this port change).

For additional port information, see the Knowledge Center article *FDN Services and Ports*.

Debugging Antivirus and IPS update connections to the FDN

If problems are encountered when a FortiGate unit attempts to communicate with the FDN, you can use the following debugging commands to determine the source of the problem.

This section describes:

- Displaying debug information for Antivirus and IPS updates
- Diagnosing Antivirus and IPS update problems
- Enabling Push Updates through a NAT device

Displaying debug information for Antivirus and IPS updates

1 Enter the following command to display debug output on the CLI console.

```
diagnose debug enable
```

2 Enter the following command to turn on debug messages for the update process.

```
diagnose debug application update 255
```

Debug messages enable you to determine the exact problem. Two of the most common problems are DNS failures or routing failures. To turn off debug messages, enter the command `diagnose debug application update 0`.

3 Enter the following command to view a list of the last debug messages issued (as you would have seen using the debug command above).

```
diagnose test update info
```

This command also displays:

- the versions of all packages
- when the next scheduled update is set to occur
- the list of all known secondary servers

4 You can also enter the following command to capture packets to the FDN servers.

```
diagnose sniffer packet <port> 'port 443'
```

`<port>` should be the port that is routable to the FDN servers.

The filter can be made more specific by including the IP addresses returned by update.fortiguard.net (if this is the initial connection of the FortiGate unit to the FDN).

Diagnosing Antivirus and IPS update problems

1 Start a manual update and check the “Last update status” on the web-based manager.

2 If the “Last Update Status” is “network error”, check the debug output in the CLI to see whether this is a DNS or connection failure. In the event of a connection failure, use a packet capture to see if the FortiGate unit is initiating the TCP session and if the FDN server is accepting the session.

If the FortiGate unit is not initiating the session, check the FortiGate unit routing configuration.

If the secondary server is not accepting the session, check any upstream firewalls to make sure that the FortiGate unit can to connect to the secondary server on port 443.

3 If the “Last update status” is “unauthorized”, the FortiGate unit has an invalid contract. Contact your sales representative to update the contracts for this unit.

4 If SSL access through port 443 in the network must go through a proxy, make sure that the tunneling options in `config system autoupdate tunneling` match the proxy settings.

5 If a FortiManager’s FortiGuard Center is used as a local FDN server, make sure the override IP address is set properly on the FortiGate unit. Otherwise, the override server IP address should not be set.

6 If push updates are configured and the FortiGate unit is behind a NAT device, make sure that the override push IP is set to the external IP address of the NAT device. Also make sure that the NAT device is configured to forward incoming UDP packets to the FortiGate unit. The NAT device must forward incoming packets that use port 9443 or that use the push override port configured on the FortiGate unit.

7 If the problem is with push updates, use a sniffer to see if the UDP announce packets are arriving on port 9443 (this will probably require the involvement of Fortinet Technical Support to generate a test push announcement). Remember, once the announce packet arrives, it will take anywhere from 1 to 120 seconds for the FortiGate unit to initiate the update request.

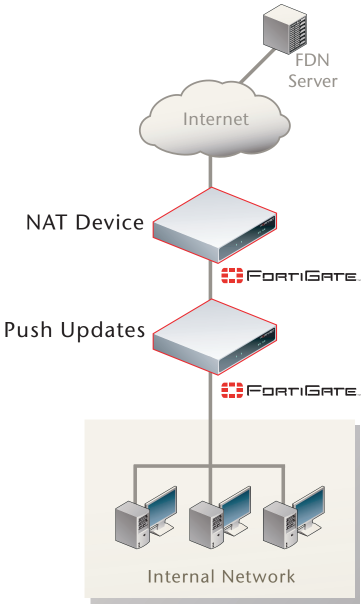
Enabling Push Updates through a NAT device

The FDN connects to the FortiGate unit using UDP on either port 9443 or an override push port that you specify.

If the FDN can only connect to the unit through a NAT device, you must configure port forwarding on the NAT device, and add the NAT device’s virtual IP and port as a FortiGuard Center push update override.

Note: You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

Figure 2: Example network: Push updates through a NAT device



Overview

1 Register and license the unit that is on the internal network with Fortinet.

2 Configure the Update Center (FortiOS v2.80) or FortiGuard Center (FortiOS and FortiManager v3.0) of the unit on the internal network.

For detailed instructions, see "To add an IP address override to the FortiGuard Center of a FortiGate unit on the internal network" on page 18.

3 Add a virtual IP address to the NAT device, and add a policy to the NAT device that forwards push messages received on the virtual IP to the unit's internal IP address.

If the NAT device is a FortiGate unit, for detailed instructions, see "To add a virtual IP to a FortiGate in NAT mode" on page 18 and "To add a port forward to a FortiGate unit in NAT mode" on page 19.

To add an IP address override to the FortiGuard Center of a FortiGate unit on the internal network

These instructions are specific to a FortiGate unit receiving push messages. However, the instructions are similar for a FortiManager unit.

1 Go to the FDN configuration location.

- On FortiOS v2.80, go to **System > Maintenance > Update Center**.
- On FortiOS v3.0, go to **System > Maintenance > FortiGuard Center**.

2 Select Allow Push Update.

3 Select Use override push IP and enter the IP address of the external interface of the NAT device. Usually this is the virtual IP added to the interface to port forward push messages.

4 Do not change the push update port unless UDP port 9443 is blocked or used by other services on your network.

5 Select Apply.

The FortiGate unit notifies the FDN of the push IP address and port override. The FDN now will send push messages to this IP address and port.

Push updates will not actually work until you add the port forwarding policy and virtual IP to the NAT device, so that the NAT device accepts push update packets and forwards them to the FortiGate unit's internal network IP address.

Note: If the external IP address or port changes, add the changes to the Use override push configuration. Select Apply to send the updated the push information to the FDN.

To add a virtual IP to a FortiGate in NAT mode

1 Go to **Firewall > Virtual IP**.

2 Select Create New.

3 Add a port forwarding virtual IP that maps the external interface of the NAT device to the IP address of the FortiGate unit on the internal network using the push update UDP port.

FortiOS v2.80 virtual IP configuration:

Name	Add a name for the Virtual IP.
External Interface	The interface on the NAT device that connects to the Internet.
Type	Select Port Forwarding
External IP Address	The IP address that the FDN connects to send push updates to the FortiGate unit on the Internal network. This would usually be the IP address of the external interface of the NAT device. This IP address must be the same as the FortiGuard Center push update override IP of the FortiGate unit on the internal network.
External Service Port	The external service port that the FDN connects to. The external service port for push updates is usually 9443. If you changed the push update port on the FortiGate unit on the internal network, you must set the external service port to the same changed push update port.
Map to IP	The IP address of the FortiGate unit on the Internal network.
Map to Port	The map to port must be the same as the external service port.
Protocol	UDP

FortiOS v3.0 virtual IP configuration:

Name	Add a name for the Virtual IP.
External Interface	The interface on the NAT device that connects to the Internet.
Type	Static NAT.
External IP Address/Range	The IP address that the FDN connects to send push updates to the FortiGate unit on the Internal network. This would usually be the IP address of the external interface of the NAT device. This IP address must be the same as the FortiGuard Center push update override IP of the FortiGate unit on the internal network.
Mapped IP Address/Range	The IP address of the FortiGate unit on the Internal network.
Port Forwarding	Select Port Forwarding.
Protocol	UDP
External Service Port	The port that the FDN sends push messages on, usually 9443. If you changed the push update port on the FortiGate unit on the internal network, you must set the external service port to the same changed push update port.
Map to Port	The map to port must be the same as the external service port.

4 Select OK.

To add a port forward to a FortiGate unit in NAT mode

1 Add a new external to internal firewall policy.

2 Configure the policy with the following settings:

3 Select OK.

To confirm that push updates to the FortiGate unit on the internal network are working

1 Go to the FDN configuration location.

- On FortiOS v2.80, go to **System > Maintenance > Update Center**.
- On FortiOS v3.0, go to **System > Maintenance > FortiGuard Center**.

2 On FortiOS v2.80, select Refresh.

The Push Update indicator should change to solid green.

FortiGuard Web Filtering and Antispam

The FDN provides FortiGuard Web Filtering services to FortiGate units that process network traffic containing HTTP content. FortiGate units with FortiGuard Web Filtering enabled and a valid FortiGuard Web Filtering license queue network traffic containing HTTP content while sending requests to the FDN asking for web page ratings. Depending on the results returned by the FDN and on the configuration of the FortiGate unit, the web content may be blocked by the FortiGate unit or passed through to the user who requested the content.

The FDN also provides FortiGuard Antispam services for FortiGate units that process network traffic containing email (SMTP, IMAP, or POP3) content. FortiGate units with FortiGuard Antispam enabled and a valid FortiGuard Antispam license queue network traffic containing email content while sending requests to the FDN asking for spam status. Depending on the results returned by the FDN, and on the configuration of the FortiGate unit, the email content may be passed, tagged as spam and passed, blocked and discarded, or blocked and quarantined.

FortiGuard Web Filtering and Antispam services share a common protocol for communicating between FortiGate units and FDN servers that only differs in the content of the requests and responses sent and received by the FortiGate unit and the FDN. FortiGuard Web Filtering and Antispam services also share a common protocol for finding FDN servers to send requests to and for determining which FDN server can respond the fastest to a FortiGuard Web Filtering or Antispam request.

Note: FortiOS v2.80 MR11 and earlier uses an earlier FortiGuard Web Filtering and FortiGuard Antispam server selection algorithm. The selection algorithm has been updated for FortiOS v3.0 and v2.80 MR12 and later. Diagnose command changes were also made for FortiOS v3.0 and MR12 and later. However, all FortiOS v2.80 versions use the same Antispam host name (`antispam.fortigate.com`) and the same FortiGuard Web Filtering host name (`guard.fortinet.net`).

This chapter describes:

- FortiGuard Web Filtering and Antispam initial contact with the FDN
- Web Filtering and Antispam server selection
- FortiGuard Web Filtering and Antispam ports
- Debugging FortiGuard Web Filtering and Antispam connections to the FDN
- Troubleshooting some common FortiGuard Web Filtering and Antispam problems

FortiGuard Web Filtering and Antispam initial contact with the FDN

When a FortiGate unit starts or FortiGuard Web Filtering and Antispam is enabled, the FortiGate unit contacts the FDN to validate its FortiGuard license and get the current list of valid FDN servers. To contact the FDN, the FortiGate unit sends an INIT packet to the IP address of the default FDN host name. The INIT packet contains the FortiGate unit's FortiGuard licensing information. If the FortiGate unit is not licensed, the FDN responds with a license expired message. If the FortiGate unit has a valid license, the latest FortiGate license information is returned to the FortiGate unit along with a global list of all available FDN server IP addresses and their associated time zones.

- For FortiOS v2.80, the FortiGuard Web Filtering default host name is webfilter.fortiguard.net.
- For FortiOS v2.80, the FortiGuard Antispam default host name is antispam.fortiguard.net.
- For FortiOS v3.0, the default host name for FortiGuard Web Filtering and FortiGuard Antispam is service.fortiguard.net.

The default FDN host name is only used for the initial setup request. FortiGate units do not contact the default host for specific FortiGuard Web Filtering or Antispam requests. All FortiGuard Web Filtering and Antispam requests go to the FDN servers returned in response to the INIT request.

A FortiGate unit running FortiOS v2.80 MR11 and earlier sends the INIT packet to make the initial connection to the FDN. A FortiGate unit running FortiOS v3.0 and v2.80 MR12 and later re-sends the INIT packet once a day to update the list of FDN servers.

FortiGate units also send an INIT packet when there is a high rate of packet failures to known FDN servers. A high rate of packet failures indicates a problem with the known server list, so the FortiGate unit will try to retrieve an updated server list.

Web Filtering and Antispam server selection

FortiOS v2.80 maintains two FDN server lists, one of Web Filtering servers and one of Antispam servers. FortiOS v3.0 maintains one list of FDN servers that is used for both FortiGuard Web Filtering and FortiGuard Antispam requests. These lists are maintained by the FortiGate unit as weighted lists. The FortiGate unit constantly adjusts the weights of the FDN servers in the lists depending on a variety of factors. The FortiGate unit always sends requests for web filtering or Antispam services to the FDN server with the lowest weight. The FDN server with the lowest weight is always at the top of the list.

The FDN servers are also sorted according to their request response speed. Periodically the FortiGate unit sends timed NOOP requests (which only require a simple response, no query is required) to all of the FDN servers in the list to determine their response times. After sorting by the server weight, the server with the fastest response time moves to the top of the list.

Initially, the weights correspond to the server time zones plus a multiplier to ensure the requests go to the closest servers first. Every successful response from a server lowers its weight and every request failure increases its weight. This way, servers that have high packet loss (due to network conditions or load) will be dropped lower in the list; moving more reliable servers to the top of the list.

Note: FortiOS v2.80 MR11 and earlier uses an earlier FortiGuard Web Filtering and FortiGuard Antispam server selection algorithm. The selection algorithm has been updated for FortiOS v3.0 and v2.80 MR12 and later. Diagnose command changes were also made for FortiOS v3.0 and MR12 and later. However, all FortiOS v2.80 versions use the same Antispam host name (`antispam.fortigate.com`) and the same FortiGuard Web Filtering host name (`guard.fortinet.net`).

FortiOS v2.80 Antispam server selection (FortiOS v2.80 MR11 and earlier)

To make sure that requests go to closer servers first, FortiOS v2.80 sets a base weight for each FDN server that corresponds to the server’s time zone plus a multiplier. Every successful response from a server lowers its weight and every failed response increases its weight. This way, servers that have high packet loss (due to network conditions or load) will be dropped lower in the list; moving more reliable servers to the top of the list.

FortiOS v2.80 also adds weight to a server every time a request is sent to it. The increase in weight drops the server lower in the list, resulting in basic load balancing between servers. In practice this load balancing was not always successful. In some cases a FortiGate unit might end up sending requests to the closest FDN server and then to an FDN server on another continent.

FortiOS v3.0 and v2.80 MR12 and later Antispam server selection

FortiOS v3.0 and v2.80 MR12 and later sets the base weight of an FDN server to the number of hours difference between the FortiGate unit time zone and the FDN server time zone multiplied by 10.

The FortiOS v2.80 MR11 and earlier adding weight feature is not used by FortiOS v3.0. Instead, FortiOS v3.0 and v2.80 MR12 and later reduces the weight by 1 when a request to a server is successful. When a request fails, FortiOS increases the weight by 5. The more failures a server has, the higher its weight.

The way that FortiOS v3.0 and v2.80 MR12 and later calculates the weight makes it more likely that the FortiGate unit will attempt to contact FDN servers in closer time zones before FDN servers in distant time zones.

Another factor that affects whether a server is selected is how many NOOP requests the FortiGate unit must send an FDN server before receiving a response. The FortiGate unit sends up to 80 NOOP requests. If no response is received after 80 requests, the FDN server is assumed to be not responding and is moved to the bottom of the FDN server list. However, when its time for the next NOOP requests the FortiGate unit will send a request to not responding servers in case the servers are now able to respond again.

FortiGuard Web Filtering and Antispam ports

FortiGuard Web Filtering and Antispam rating queries (single URL or spam “lookups”) to the FDN or a FortiManager acting as a private FDS use UDP.

- In FortiOS v2.80, rating queries use port 8888 for web filtering requests and 8889 for antispam requests.
- In FortiOS v3.0, both services use port 53 (the same UDP port used for DNS queries) as the default, and port 8888 as an alternate. Port 53 is provided to allow a method of tunneling FortiGuard requests through upstream firewalls without changing the upstream firewall configuration, since most firewalls are configured to allow UDP requests on port 53 for DNS.

If upstream devices provide DNS caching or DNS forwarding services, the FDN protocol may not work on port 53, which is why port 8888 is also available.

Rating queries are only single item lookups. A different port and protocol is used when updating the whole rating database. For rating database update ports, see “Pull and push update ports” on page 15.

Note: FortiManager units behave like a secondary FDN server when receiving FortiGate rating queries: they do not forward rating queries to the FDN.

Debugging FortiGuard Web Filtering and Antispam connections to the FDN

If problems are encountered in getting the FortiGate unit to connect to the FDN for Web Filtering and Antispam services, you can use the information described in this section to help determine the cause of the problem and to help resolve the problem.

This section describes:

- Using the FortiOS v2.80 MR11 and earlier CLI
- Using the CLI on FortiOS v3.0 and v2.80 MR12 and later
- Using the FortiOS v2.80 web-based manager (all maintenance releases)
- Using the FortiOS v3.0 web-based manager
- Diagnosing FortiGuard Web Filtering 500 Internal Server Error problems
- Analyzing FortiGate log messages to diagnose possible Web Filtering problems

Using the FortiOS v2.80 MR11 and earlier CLI

If your FortiGate unit is operating FortiOS v2.80 MR11 and earlier, you can use the following steps from the FortiGate CLI to display information about the status of FortiGuard Web Filtering and Antispam requests.

1 Enter the following command to display detailed rating and cache statistics about recent FortiGuard Web Filter request activity.

```
diagnose webfilter catblock statistics list
```

Rating statistics include information about various types of communications failures and errors as well as the number of web pages allowed, blocked, and logged. Large numbers of errors can highlight specific problems communicating with FDN servers. For example, a large number of DNS failures may mean that there are problems with the DNS server used by the FortiGate unit. Other errors may indicate network transmission problems and so on.

Cache statistics display information about the amount of memory used by the FortiGuard Web Filtering cache and how often the cached ratings are used.

2 Enter the following command to display detailed statistics about recent FortiGuard Antispam request activity.

```
diagnose spamfilter fortishield statistics list
```

FortiGuard Antispam statistics include information about amount of memory used by the FortiGuard Antispam cache and how often the cache is used.

Other FortiGuard Antispam statistics include information about various types of communications failures and errors. Large numbers of errors highlight specific problems communicating with FDN servers. For example, a large number of data send failures may indicate problems with downstream connections to the FDN.

Statistics are also displayed about the number of requests sent to the FDN servers (also called rating servers) and the numbers of different types of responses received (for example the number of IP white list, IP Allowed, IP Spam, and so on).

This command also displays the FortiGuard AntiSpam Server list (see the next step for more information).

3 Enter one of the following commands to display FortiGuard FDN server lists.

`diagnose debug rating` (displays the FortiGuard Web Filtering server list which includes the default FortiGuard Web Filter FDN server host name which is `guard.fortinet.net`).

`diagnose spamfilter fortishield statistics list` (displays the FortiGuard Antispam server list which includes the default FortiGuard AntiSpam FDN server host name which is `antispam.fortigate.com`)

The next rating request will be sent to the server at the top of the list. Servers are listed in server weight order.

4 Analyze FortiGate log messages because they may contain detailed information that could help isolate and resolve the source of the problem. See “Analyzing FortiGate log messages to diagnose possible Web Filtering problems” on page 35.

5. If the log messages do not provide enough detail, use the following commands to view detailed debug log messages on the CLI console. These commands display information for both FortiGuard Web Filtering and Antispam.

```
diagnose debug enable
```

```
diagnose debug application urlfilter 1
```

Using the CLI on FortiOS v3.0 and v2.80 MR12 and later

If your FortiGate unit is operating with FortiOS v3.0 or v2.80 MR12 and later, you can use the following steps from the FortiGate CLI to display information about the status of FortiGuard Web Filtering and Antispam requests.

1. Enter the following command to display detailed rating and cache statistics about recent FortiGuard Web Filter request activity.

```
diagnose webfilter fortiguard statistics list
```

Rating statistics include information about various types of communications failures and errors as well as the number of web pages allowed, blocked, and logged. Large numbers of errors may highlight specific problems communicating with FDN servers. For example, a large number of DNS failures may mean that there are problems with the DNS server that the FortiGate unit uses. Other errors may indicate network transmission problems, and so on.

Cache statistics display information about the amount of memory used by the FortiGuard Web Filtering cache and how often the cached ratings are used.

2. Enter the following command to display detailed statistics about recent FortiGuard Antispam request activity.

```
diagnose spamfilter fortishield statistics list
```

FortiGuard Antispam statistics include information about the amount of memory used by the FortiGuard Antispam cache and how often the cache is used.

Other FortiGuard Antispam statistics include information about various types of communications failures and errors. Large numbers of errors indicate problems communicating with FDN servers. For example, a large number of data send failures may indicate problems with downstream connections to the FDN.

Statistics are also displayed about the number of requests sent to the FDN servers (also called rating servers) and the numbers of different types of responses received (for example the number of IP white list, IP Allowed, IP Spam, and so on). Information is also displayed about the latency associated with communicating with the FDN.

3. Enter one of the following commands to display the FortiGuard FDN server list. The display includes status information for each FDN server in the list. The following commands display the FortiGuard FDN server list.

Note: FortiOS v3.0 FortiGuard Web Filtering and Antispam use the same FDN server list (`service.fortiguard.net`). All FortiOS v2.80 MR versions use `guard.fortinet.net` for FortiGuard Web Filtering and `antispam.fortigate.com` for FortiGuard Antispam.

```
diagnose debug rating
```

```
diagnose spamfilter fortishield servers
```

For both of these commands you can add a refresh rate to have the CLI update the server list in real time. For example, the following commands update the server list display every 20 seconds (press q to stop displaying updates):

```
diagnose debug rating 20
```

```
diagnose spamfilter fortishield servers 20
```

The following shows example server list output. (Actual FDN server IP addresses have been replaced with xx.xx.xx.xx)

```
Locale       : english
License      : Contract
Expiration   : Thu Oct 12 16:00:00 2006
Hostname     : service.fortiguard.net

-=- Server List (Wed Mar 15 11:23:19 2006) -=-

IP            Weight  Round-time  TZ   Packets  Curr Lost  Total Lost
xx.xx.xx.xx        0          67  -8         4          0           0
xx.xx.xx.xx        0          90  -8         3          0           0
xx.xx.xx.xx       30         124  -5         3          0           0
xx.xx.xx.xx       30         136  -5         3          0           0
xx.xx.xx.xx       30         137  -5         3          0           0
xx.xx.xx.xx       80         204   0         3          0           0
xx.xx.xx.xx       80         204   0         3          0           0
xx.xx.xx.xx       90         223   1         3          0           0
xx.xx.xx.xx      160         262   8         3          0           0
xx.xx.xx.xx      160         295   8         3          0           0
xx.xx.xx.xx      170         223   9         3          0           0
```

IP The IP addresses of the FDN servers in the FortiGate unit FDN servers list.

Weight The weight of each FDN server in the FortiGate unit FDN server list. The list is sorted according to the server weight. The weight cannot fall below a base weight determined by the number of hours difference between the FortiGate unit time zone and the FDN server time zone multiplied by 10. When a request is successful, the weight is reduced by 1. When a request fails the weight is increased by 5. The more failures a server has, the higher its weight and the further it drops down the FDN server list. The lower a server is on the list the less often it is used by the FortiGate unit.

Round-time The round-trip time (in ms) for a NOOP request to each FDN server from the FortiGate unit. The round-trip time is used to determine the fastest server. The fastest server moves to the top of the FDN servers list. If Round-time displays `Timing` for a server, a NOOP request is in progress. If Round-time displays `No Resp` the server is unreachable and will be moved to the bottom of the FDN server list.

TZ The number of hours that each FDN server time zone is offset from 0 hours coordinated universal time (UTC), also called Greenwhich Mean Time (GMT).

Packets The number of packets sent to each FDN server.

Curr Lost	The number of packets that had to be re-transmitted to connect to this FDN server during the most recent NOOP request. Curr Lost is reset when a response is received. If Curr Lost reaches 80, the FDN server is assumed to be not responding and is moved to the bottom of the FDN server list. The FortiGate unit attempts to connect to the server again with the next NOOP request.
Total Lost	The total number of re-transmissions that have had to be made to this FDN server.

4 Analyze FortiGate log messages because they may contain detailed information that could help isolate and resolve the source of the problem. See “Analyzing FortiGate log messages to diagnose possible Web Filtering problems” on page 35.

5 If the log messages do not provide enough detail, use the following commands to view detailed debug log messages on the CLI console. These commands display information for both FortiGuard Web Filtering and Antispam.

```
diagnose debug enable
```

```
diagnose debug application urlfilter 1
```

Using the FortiOS v2.80 web-based manager (all maintenance releases)

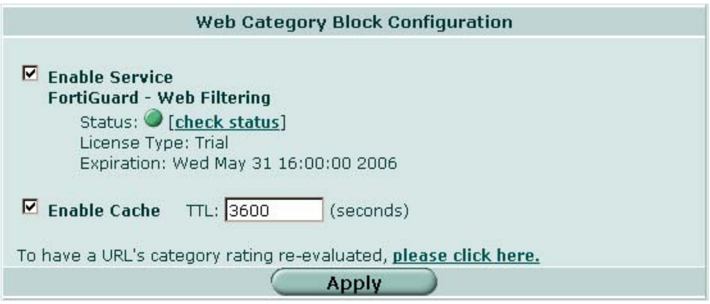
Use the following steps from the FortiOS v2.80 web-based manager to check FortiGuard Web Filtering and FortiGate Antispam status for your FortiGate unit and to help resolve status errors.

1 To check FortiGuard Web Filtering status for your FortiGate unit:

- Go to **Web Filter > Category Block > Configuration** (FortiGuard Web Filtering is called Category Blocking in FortiOS v2.80).
- Make sure Enable Service is selected if you are using FortiGuard Web Filtering.
- Select check status to confirm that the FortiGate unit can connect to the FDN and to update FortiGuard Web Filtering license information for the FortiGate unit.

If the FortiGate unit can connect to FDN, the Status indicator changes to solid green and the web-based manager displays the license type and expiration date (see Figure 3).

Figure 3: FortiGuard Web Filtering: successful connection to the FDN with a valid trial license



Web Category Block Configuration

☑ Enable Service
FortiGuard - Web Filtering
Status: ● [check status]
License Type: Trial
Expiration: Wed May 31 16:00:00 2006

☑ Enable Cache TTL: 3600 (seconds)

To have a URL's category rating re-evaluated, please click here.

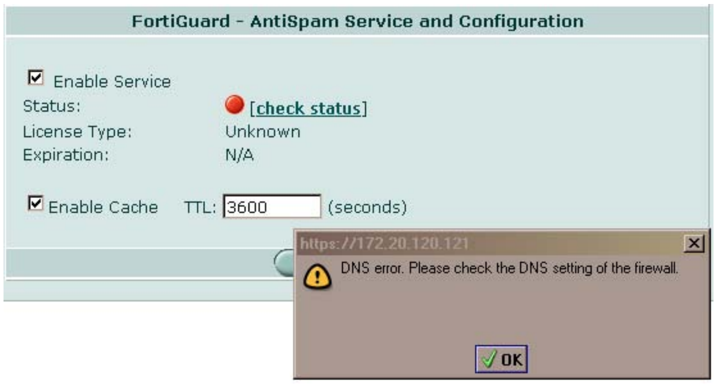
Note: From the FortiOS v2.80 MR11 and earlier CLI you can display similar information using the command `get webfilter catblock`. You can also change FortiGuard Web FIltering settings using `config webfilter catblock`.

2 To check FortiGuard Antispam status for your FortiGate unit:

- Go to **Web Filter > FortiGuard - AntiSpam > FortiGuard - AntiSpam**.
- Make sure Enable Service is selected if you are using FortiGuard Antispam.
- Select check status to confirm that the FortiGate unit can connect to the FDN and to update FortiGuard Antispam license information for the FortiGate unit.

If the FortiGate unit cannot connect to the FDN, the Status indicator flashes yellow and red and an error message is displayed (see Figure 4). The error message may help diagnose connection problems. For example, the error message may indicate that there is a problem with the FortiGate unit routing table or DNS settings.

Figure 4: FortiGuard - AntiSpam unsuccessful connection to the FDN



FortiGuard - AntiSpam Service and Configuration

☑ Enable Service

Status: ● [check status]

License Type: Unknown

Expiration: N/A

☑ Enable Cache TTL: 3600 (seconds)

https://172.20.120.121

DNS error. Please check the DNS setting of the firewall.

Note: From the FortiOS v2.80 MR11 and earlier CLI you can display similar information using the command `get spamfilter fortishield`. You can also change FortiGuard Antispam settings using `config spamfilter fortishield`.

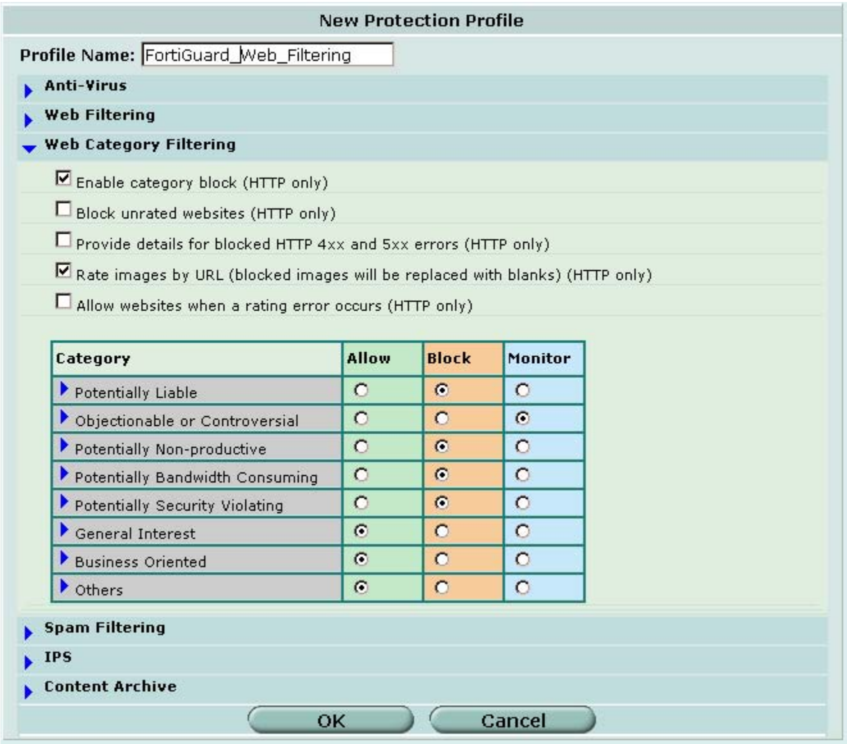
3 Take steps to correct this error and then check status again.

4 Make sure FortiGuard Web Filtering and FortiGuard Antispam is configured in protection profiles and the protection profiles are added to firewall policies.

To configure FortiGuard Web Filtering:

- Go to **Firewall > Protection Profile**.
- Edit a protection profile or add a new protection profile. (You can configure FortiGuard Web Filtering and FortiGuard Antispam in the same protection profile.)
- Select Web Category Filtering.
- Select Enable category block (HTTP only).
- Configure other Web Category Filtering options as required (see the FortiGate online help for more information).
- Select OK to save your changes.
- Go to **Firewall > Policy** and edit a firewall policy or add a new firewall policy.
- Add the protection profile containing the Web Category Filtering settings to the firewall policy.

Figure 5: Example FortiGuard Web Filtering protection profile



New Protection Profile

Profile Name: FortiGuard_Web_Filtering

☑ Enable category block (HTTP only)

□ Block unrated websites (HTTP only)

□ Provide details for blocked HTTP 4xx and 5xx errors (HTTP only)

☑ Rate images by URL (blocked images will be replaced with blanks) (HTTP only)

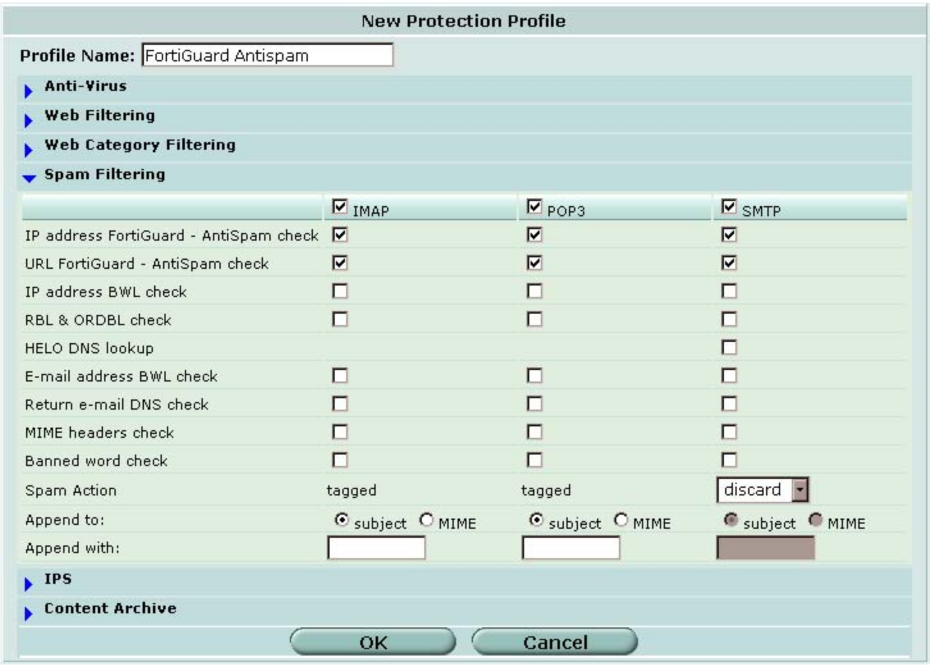
□ Allow websites when a rating error occurs (HTTP only)

Category	Allow	Block	Monitor
▸ Potentially Liable	○	●	○
▸ Objectionable or Controversial	○	○	●
▸ Potentially Non-productive	○	●	○
▸ Potentially Bandwidth Consuming	○	●	○
▸ Potentially Security Violating	○	●	○
▸ General Interest	●	○	○
▸ Business Oriented	●	○	○
▸ Others	●	○	○

To configure FortiGuard Antispam:

- Go to **Firewall > Protection Profile**.
- Edit a protection profile or add a new protection profile. (You can configure FortiGuard Web Filtering and FortiGuard Antispam in the same protection profile.)
- Select Spam Filtering.
- Enable IP address FortiGuard - AntiSpam check or URL FortiGuard - AntiSpam check, or both for the email services that you use (IMAP, POP3, and SMTP).
- Configure other Spam Filtering options such as the Spam Action for SMTP as required (see the FortiGate online help for more information).
- Select OK to save your changes.
- Go to **Firewall > Policy** and edit a firewall policy or add a new firewall policy.
- Add the protection profile containing the Spam Filtering settings to the firewall policy.

Figure 6: Example FortiGuard Antispam protection profile



New Protection Profile

Profile Name: FortiGuard Antispam

	☑ IMAP	☑ POP3	☑ SMTP
IP address FortiGuard - AntiSpam check	☑	☑	☑
URL FortiGuard - AntiSpam check	☑	☑	☑
IP address BWL check	□	□	□
RBL & ORDBL check	□	□	□
HELO DNS lookup			□
E-mail address BWL check	□	□	□
Return e-mail DNS check	□	□	□
MIME headers check	□	□	□
Banned word check	□	□	□
Spam Action	tagged	tagged	discard
Append to:	● subject ○ MIME	● subject ○ MIME	● subject ○ MIME
Append with:			

Using the FortiOS v3.0 web-based manager

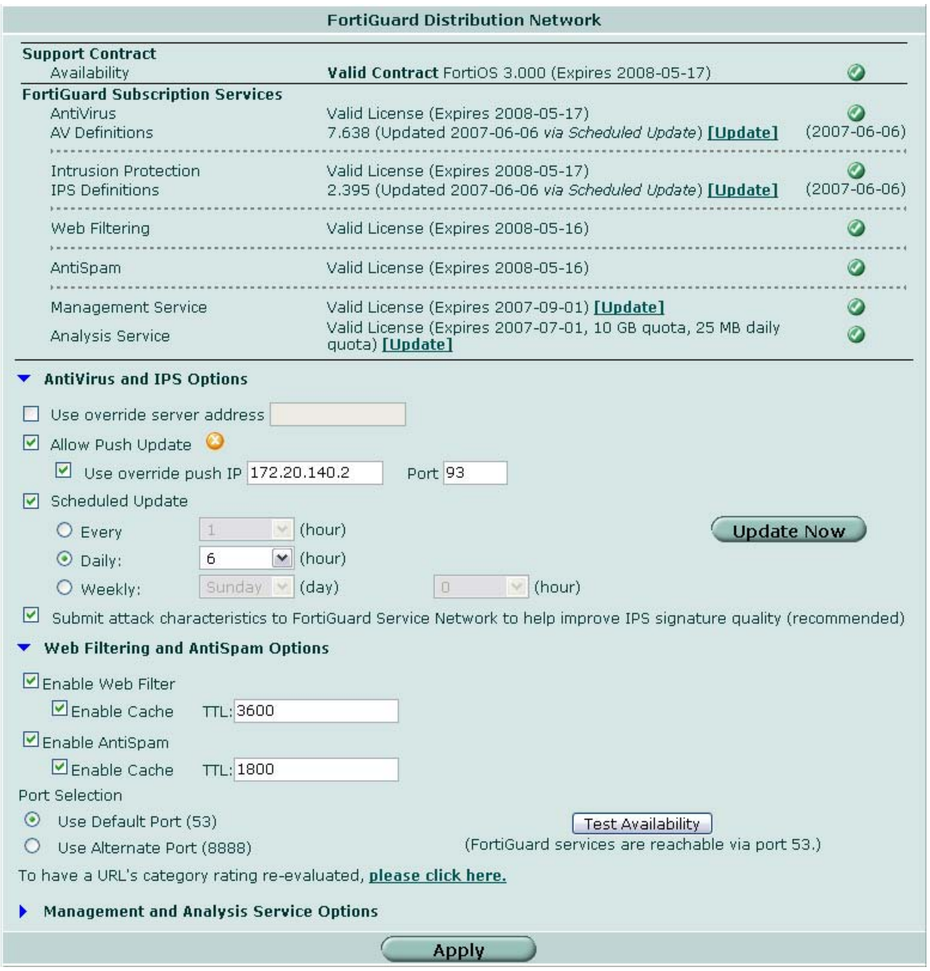
Use the following steps from the FortiOS v3.0 web-based manager to check FortiGuard Web Filtering and FortiGate Antispam status for your FortiGate unit and to help resolve status errors.

1 To check FortiGuard Web Filtering and FortiGuard Antivirus status for your FortiGate unit:

- Go to **System > Maintenance > FortiGuard Center**.
- If the FortiGate unit can connect to the FDN, the status indicator changes to solid green.
- Under FortiGuard Services, select Enable for Anti Spam and Web Filter.
- Select Test Availability to confirm that the FortiGate unit can connect to the FDN and to update FortiGuard Web Filtering and Antispam license information for the FortiGate unit.

If the FortiGate unit can connect to FDN, the FortiGuard Services Status indicators for FortiGuard Web Filtering and FortiGuard Antispam (the last column of the table at the bottom of the page) change to solid green. The web-based manager also displays the license type and expiration date for both services (see Figure 7).

Figure 7: Successful connection to the FDN with valid trial licenses



FortiGuard Distribution Network

Support Contract

Availability **Valid Contract** FortiOS 3.000 (Expires 2008-05-17) ✓

FortiGuard Subscription Services

AntiVirus Valid License (Expires 2008-05-17) ✓
AV Definitions 7.638 (Updated 2007-06-06 *via Scheduled Update*) **[Update]** (2007-06-06)

Intrusion Protection Valid License (Expires 2008-05-17) ✓
IPS Definitions 2.395 (Updated 2007-06-06 *via Scheduled Update*) **[Update]** (2007-06-06)

Web Filtering Valid License (Expires 2008-05-16) ✓

AntiSpam Valid License (Expires 2008-05-16) ✓

Management Service Valid License (Expires 2007-09-01) **[Update]** ✓
Analysis Service Valid License (Expires 2007-07-01, 10 GB quota, 25 MB daily quota) **[Update]** ✓

AntiVirus and IPS Options

□ Use override server address

☑ Allow Push Update

☑ Use override push IP 172.20.140.2 Port 93

☑ Scheduled Update

○ Every 1 (hour)

● Daily: 6 (hour)

○ Weekly: Sunday (day) 0 (hour)

☑ Submit attack characteristics to FortiGuard Service Network to help improve IPS signature quality (recommended)

Web Filtering and AntiSpam Options

☑ Enable Web Filter

☑ Enable Cache TTL: 3600

☑ Enable AntiSpam

☑ Enable Cache TTL: 1800

Port Selection

● Use Default Port (53)

○ Use Alternate Port (8888)

(FortiGuard services are reachable via port 53.)

To have a URL's category rating re-evaluated, **please click here.**

Management and Analysis Service Options

If the FortiGate unit cannot connect to the FDN, the status indicators change to a yellow colo, and an error message is displayed. The error message may help diagnose connection problems. For example, the error message may indicate that there is a problem with your routing table or DNS settings.

Note: From the FortiOS v3.0 CLI you can display similar information using the command `get system fortiguard`. You can also change FDN settings using `config system fortiguard`.

2 Take steps to correct this error and then test availability again.

For example, check your FortiGate routing table and DNS entries. Check other network settings to make sure that the FortiGate unit can connect to the Internet.

By default FortiGuard services use UDP port 53 to connect to the FDN. UDP port 53 is also used for DNS. If your network does not support connections to the Internet using port UDP 53, or if your network uses DNS caching, the FortiGate unit may not be able to connect to the FDN using UDP port 53.

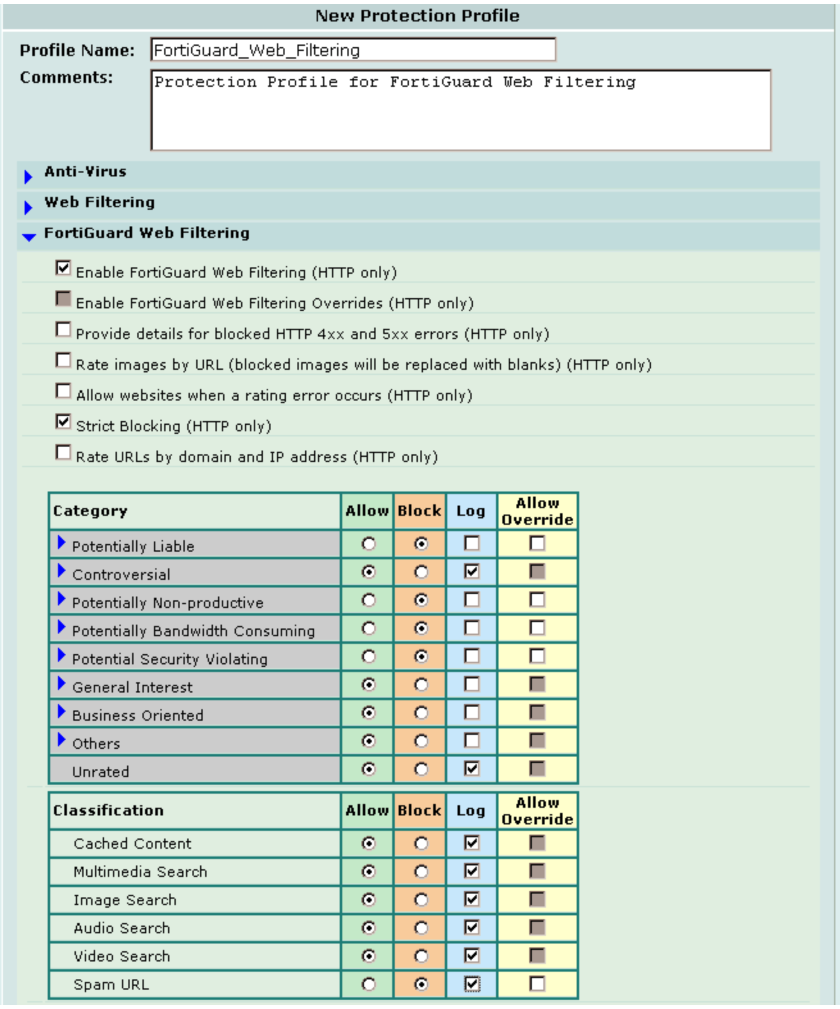
The Test Availability button tests connectivity to the FDN using UDP port 53 and UDP port 8888 and reports the results of both tests under the button. If the FortiGate unit can only connect to the FDN using UDP port 8888, select Use Alternate Port (8888). If the FortiGate unit can connect to the FDN using UDP port 53 (or both 53 and 8888) keep the Use Default Port (53) setting.

3 Make sure FortiGuard Web Filtering and FortiGuard Antispam is configured in protection profiles and the protection profiles are added to firewall policies.

To configure FortiGuard Web Filtering:

- Go to **Firewall > Protection Profile**.
- Edit a protection profile or add a new protection profile. (You can configure FortiGuard Web Filtering and FortiGuard Antispam in the same protection profile.)
- Select FortiGuard Web Filtering.
- Select Enable FortiGuard Web Filtering (HTTP only).
- Configure other FortiGuard Web Filtering options as required (see the FortiGate online help for more information).
- Select OK to save your changes.
- Go to **Firewall > Policy** and edit a firewall policy or add a new firewall policy.
- Add the protection profile containing the FortiGuard Web Filtering settings to the firewall policy.

Figure 8: Example FortiGuard Web Filtering protection profile



New Protection Profile

Profile Name: FortiGuard_Web_Filtering

Comments: Protection Profile for FortiGuard Web Filtering

☑ Enable FortiGuard Web Filtering (HTTP only)
▨ Enable FortiGuard Web Filtering Overrides (HTTP only)
□ Provide details for blocked HTTP 4xx and 5xx errors (HTTP only)
□ Rate images by URL (blocked images will be replaced with blanks) (HTTP only)
□ Allow websites when a rating error occurs (HTTP only)
☑ Strict Blocking (HTTP only)
□ Rate URLs by domain and IP address (HTTP only)

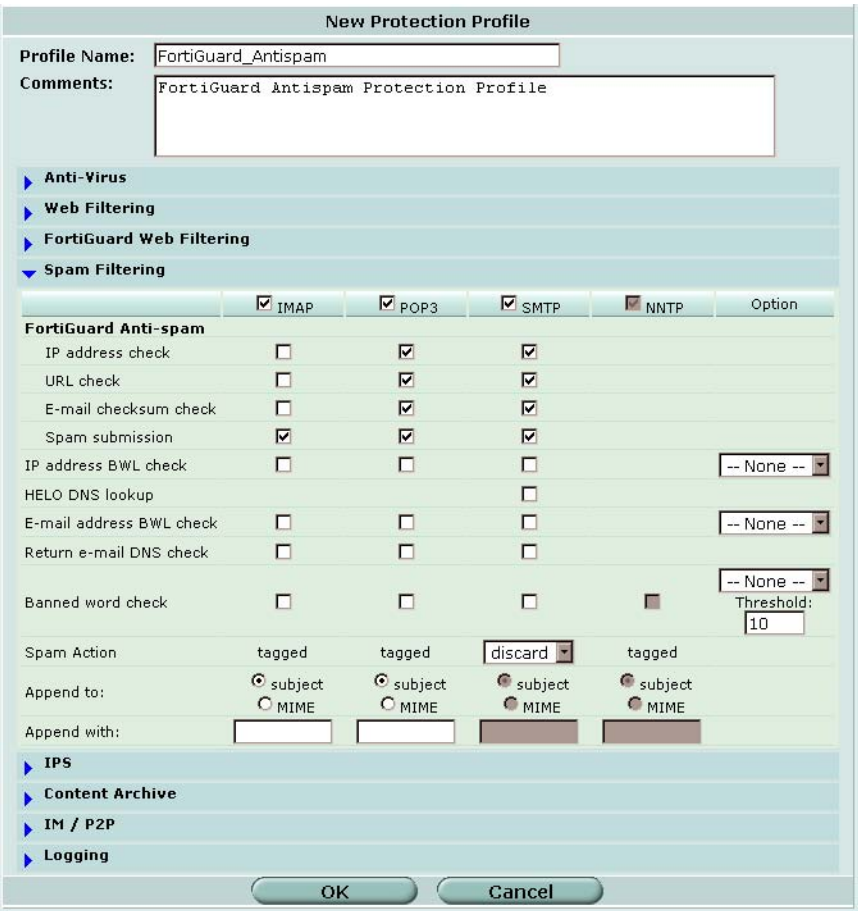
Category	Allow	Block	Log	Allow Override
▸ Potentially Liable	○	●	□	□
▸ Controversial	●	○	☑	▨
▸ Potentially Non-productive	○	●	□	□
▸ Potentially Bandwidth Consuming	○	●	□	□
▸ Potential Security Violating	○	●	□	□
▸ General Interest	●	○	□	▨
▸ Business Oriented	●	○	□	▨
▸ Others	●	○	□	▨
Unrated	●	○	☑	▨

Classification	Allow	Block	Log	Allow Override
Cached Content	●	○	☑	▨
Multimedia Search	●	○	☑	▨
Image Search	●	○	☑	▨
Audio Search	●	○	☑	▨
Video Search	●	○	☑	▨
Spam URL	○	●	☑	□

To configure FortiGuard Antispam:

- Go to **Firewall > Protection Profile**.
- Edit a protection profile or add a new protection profile. (You can configure FortiGuard Web Filtering and FortiGuard Antispam in the same protection profile.)
- Select Spam Filtering.
- Enable FortiGuard - Anti-spam settings for the email services that you use (IMAP, POP3, and SMTP).
- Configure other Spam Filtering options such as the Spam Action for SMTP as required (see the FortiGate online help for more information).
- Select OK to save your changes.
- Go to **Firewall > Policy** and edit a firewall policy or add a new firewall policy.
- Add the protection profile containing the Spam Filtering settings to the firewall policy.

Figure 9: Example FortiGuard Antispam protection profile



New Protection Profile

Profile Name: FortiGuard_Antispam

Comments: FortiGuard Antispam Protection Profile

▸ Anti-Virus

▸ Web Filtering

▸ FortiGuard Web Filtering

▾ Spam Filtering

	☑ IMAP	☑ POP3	☑ SMTP	☑ NNTP	Option
FortiGuard Anti-spam					
IP address check	☐	☑	☑		
URL check	☐	☑	☑		
E-mail checksum check	☐	☑	☑		
Spam submission	☑	☑	☑		
IP address BWL check	☐	☐	☐		-- None --
HELO DNS lookup			☐		
E-mail address BWL check	☐	☐	☐		-- None --
Return e-mail DNS check	☐	☐	☐		
Banned word check	☐	☐	☐	☐	-- None -- Threshold: 10
Spam Action	tagged	tagged	discard	tagged	
Append to:	● subject ○ MIME	● subject ○ MIME	● subject ○ MIME	● subject ○ MIME	
Append with:					

▸ IPS

▸ Content Archive

▸ IM / P2P

▸ Logging

Diagnosing FortiGuard Web Filtering 500 Internal Server Error problems

Receiving “500 Internal Server Error” in response to all web pages is caused by a a FortiGuard rating error. To diagnose this problem check your FortiGuard Web Filtering license status.

Check the status messages on the FortiGuard Web Filtering page of the FortiGate web-based manager or enter one of the following commands from the FortiGate CLI.

FortiOS v2.80 (all maintenance releases):

```
get webfilter catblock
```

```
get spamfilter fortishield
```

FortiOS v3.0:

```
get system fortiguard
```

If your licenses have not expired, check log messages or the debug output on the console to determine the exact cause of the error. To view debug output on the CLI console, enter the following commands:

```
diagnose debug enable
```

```
diagnose debug application urlfilter 1
```

Analyzing FortiGate log messages to diagnose possible Web Filtering problems

Log messages with message ID 99000 and 99001 are Web Filter log messages that can help diagnose FortiGuard Web Filtering problems. These log messages have various formats and message levels. The error message can be `Policy denies URLs when a rating error occurs` or `Policy allows URLs when a rating error occurs` depending on whether allow errors is configured in the FortiGuard Web Filtering protection profile.

A typical format for these messages is the following:

```
user=<administrator_name> src=<source_IP_address>
sport=<source_port> dst=<destination_IP_address>
dport=<destination_port> service=http hostname=<domain_name>
url=<url_address> status=passthrough error=Failed to send
request to urlfilter. Policy allows URLs when a rating error
occurs.
```

Use the information in the error field to help diagnose FortiGuard Web Filtering problems. See Table 1 for a list of error field messages and a description of the problems that they indicate.

Table 1: Content of the error field

Error Field	Description
`FortiGuard license is expired`	The FortiGuard license has expired.
`Invalid license`	The FortiGuard license is unknown or expired.
`Rating timeout`	The FortiGate unit is unable to retrieve a rating from the FDN.
`Bad network connection`	More than 100 requests have timed out.

Table 1: Content of the error field

Error Field	Description
`Shutdown FortiGuard service`	A request was purged when shutting down the FortiGuard service.
`No correct FortiGuard information`	Unable to contact the DNS server to retrieve the FortiGuard server list.
`Downloading category list`	Retrieving a new category list from the FDN. No FortiGuard Web Filtering requests can be handled while this is in progress.
`Failed to resolve Fortiguard hostname`	Able to contact the DNS server but hostname was not found.
`Too many URL requests in waiting list`	The maximum number of FortiGuard Web Filtering requests that can be processed at one time has been reached. New requests are dropped.
`Not enough resources`	The FortiGate unit is out of memory.

Troubleshooting some common FortiGuard Web Filtering and Antispam problems

This section describes the following FortiGuard Web Filtering and Antispam troubleshooting topics:

- General FortiGuard Web Filtering and Antispam troubleshooting steps
- Users cannot connect to the spam submission server (FortiOS v3.0)
- The FortiGate unit cannot connect to the FDN (FortiOS v2.80)
- The FortiGate unit cannot connect to the FDN (FortiOS v3.0)
- FortiGuard services stop working after adding an IPSec firewall policy
- FortiGuard Antispam tags or blocks email that is not spam
- FortiGuard Web Filtering incorrectly categorizes a web page

General FortiGuard Web Filtering and Antispam troubleshooting steps

1 Verify that FortiGuard Web Filtering and FortiGuard Antispam are enabled.

FortiOS v2.80 (all maintenance releases)

FortiGuard Web Filtering

- Go to **Web Filter > Category Block > Configuration**.
- Verify that Enable Service is selected.
- Select Check Status.

  Status indicator should become solid green. License Type and Expiration should be correct.

FortiGuard Antispam

- Go to **Web Filter > FortiGuard - AntiSpam > FortiGuard - AntiSpam**.
- Verify that Enable Service is selected.
- Select Check Status.

  Status indicator should become solid green. License Type and Expiration should be correct.

FortiOS v3.0

FortiGuard Web Filtering

- Go to **System > Maintenance > FortiGuard Center**.
- Verify that Enable Service is selected for Web Filter and Antispam.
- Select Test Availability.

  Web Filter and Antispam status indicators should become solid green. License and Expires should be correct.

2 Verify that there is no upstream firewall or other device blocking FDN traffic.

This is a common problem when the FortiGate unit is running in Transparent mode or is otherwise behind an external firewall.

FortiOS v2.80 (all maintenance releases)

The FortiGate unit should be able to connect to the Internet using UDP port 8888.

FortiOS v3.0

- From the FortiGuard center, test availability to confirm that the FortiGate unit can connect to the Internet using UDP port 53 or 8888.
- The FortiGate unit should be able to connect to the Internet using UDP port 53. If port 53 is blocked or if the network uses a DNS cache, from the FortiGuard Center, select Use Alternate Port (8888) to use UDP port 8888.

3 Make sure that you can ping FortiGuard host names from the FortiGate CLI.

If you cannot connect to the following host names, check your FortiGate DNS configuration and make sure your DNS server is operating.

FortiOS v2.80 (all maintenance releases)

Ping guard.fortinet.net, webfilter.fortiguard.net, and antispam.fortiguard.net

FortiOS v3.0

Ping service.fortiguard.net.

4 IF DNS resolution is not working, you can override the FortiGuard default host names with IP addresses:

FortiOS v2.80 (all maintenance releases)

Override the FortiGuard Web Filtering default host name with the IP address 1.2.3.4:

```
# config webfilter catblock
    set ftgd_hostname: 1.2.3.4
end
```

Override the FortiGuard Web Filtering default host name with the IP address 1.2.3.4:

```
# config spamfilter fortishield
    set hostname: 1.2.3.4
end
```

FortiOS v3.0

Override the FortiGuard Web Filtering and FortiGuard Antispam default host name with the IP address 1.2.3.4:

```
# config system fortiguard
    set hostname: 1.2.3.4
end
```

Users cannot connect to the spam submission server (FortiOS v3.0)

For FortiOS v3.0, if you select Spam submission in a protection profile, every time a policy using this protection profile identifies an email message as spam, the FortiGate unit adds a spam submission link to the email message. If the email message is not spam, the receiver of the message can select the spam submission link to inform the FortiGuard spam submission server that this message should not be tagged as spam. Usually the spam submission link points to http://www.nospammer.net.

You can go to **System > Config > Replacement Messages** and edit the spam submission replacement message to change the content of the message that is added with the spam submission link.

If users cannot connect to the spam submission server you can check the email message to see if the FortiGate unit is adding the correct spam submission link. You can also check the setting of the `spam-submit-srv` keyword of the `config spamfilter fortiguard` CLI command. This keyword is used to set the host name of the FortiGuard Spam Submission Server link. Usually the `spam-submit-srv` keyword is set to `www.nospammer.net`.

Verify that the spam submission server host name is set correctly. If the host name is correct, contact Fortinet Technical support.

The FortiGate unit cannot connect to the FDN (FortiOS v2.80)

For all maintenance releases of FortiOS v2.80, the FortiGate unit connects to the FDN using default host names. These default host names are set using CLI commands. Normally you should not change these default host names. However, if the FortiGate unit cannot connect to some FortiGuard services, or for the following reasons, you may need to change some of the FDN host names:

- Your DNS server cannot find one or more of the default FDN host names
- You are or have been using FortiManager as the FDN server for one or more FDN services
- An FDN host name has been changed for some reason
- Fortinet changes one or more of the default FDN host names

To change the FortiGuard Antispam host name

You may need to change the FortiGuard Antispam host name if the FortiGate unit cannot connect to the FDN for FortiGuard Antispam services.

1 From the FortiGate CLI, enter the following command:

```
config spamfilter fortishield
    set hostname <url_str>
end
```

Where the default `<url_str>` is `antispam.fortigate.com`. You can change `<url_str>` to be any host name or IP address.

To change the FortiGuard Web Filtering host name

You may need to change the FortiGuard Web Filtering host name if the FortiGate unit cannot connect to the FDN for FortiGuard Web Filtering services.

1 From the FortiGate CLI, enter the following command:

```
config webfilter catblock
    set ftgd_hostname <url_str>
end
```

Where the default `<url_str>` is `guard.fortinet.net`. You can change `<url_str>` to be any host name or IP address.

To override the FortiGuard Antivirus and IPS updates host name

You may need to override the default FortiGuard Antivirus and IPS updates host name if the FortiGate unit cannot connect to the FDN for antivirus or IPS updates or if you are using FortiManager for antivirus and IPS updates.

1 From the FortiGate CLI, enter the following command:

```
config system autoupdate override
    set address <address_str>
    set status enable
end
```

You a `<address_str>` to be any host name or IP address.

The FortiGate unit cannot connect to the FDN (FortiOS v3.0)

The FortiGate unit connects to the FDN for all FortiGuard services using the default host name `service.fortiguard.net`. Normally you should not change this default host name except for the following reasons:

- The FortiGate unit cannot connect to some or all FortiGuard services
- Your DNS server cannot find the default FortiGuard host name
- You are or have been using FortiManager for FDN services
- The FDN host name has been changed for some reason
- Fortinet changes the default FDN host name

To change the default FDN host name

1 From the FortiGate CLI, enter the following command:

```
config system fortiguard
    set hostname <url_str>
end
```

Where the default `<url_str>` is `service.fortiguard.net`. You can change `<url_str>` to be any host name or IP address.

FortiGuard services stop working after adding an IPSec firewall policy

After adding an IPSec firewall policy some or all of the following stop working:

- Some or all FortiGuard services (antivirus and IPS updates, FortiGuard Antispam, FortiGuard Web Filtering)
- FortiGate DNS lookups
- FortiGate Email Alerts
- FortiGate SNMP Traps
- FortiGate log messages being sent to FortiAnalyzer or to a remote syslog server

Some or all of these problems may occur if an IPSec firewall policy includes All (0.0.0.0/0.0.0.0) (FortiOS v3.0) external_all (0.0.0.0/0.0.0.0) (FortiOS v2.80) as a destination subnet. Adding the All address may cause some or all FortiGate generated traffic to be added to the IPSec tunnel, instead of being sent to un-encrypted onto the Internet.

The solution is to modify the IPSec policy to use a specific Destination (and Source) network instead of the general All firewall address.

FortiGuard Antispam tags or blocks email that is not spam

If FortiGuard Antispam produces unexpected results, such as tagging as spam email that is not spam (false positive) or allowing spam to pass through the FortiGate unit, you can go do the FortiGuard Center FortiGuard Antispam page at http://www.fortinet.com/FortiGuardCenter/antispam/antispam.html to do the following:

- Check whether an IP address in a false positive email message is blacklisted in the FortiGuard Antispam IP reputation database
- Check whether a URL or email address in a false positive message is in the FortiGuard Antispam signature database
- Submit an email message that should be tagged as spam to the FortiGuard Antispam database
- Submit a false positive email message to the FortiGuard Antispam database

The FortiGuard Center FortiGuard Antispam page contains web tools for completing these tasks as well as instructions for how to do them.

FortiGuard Web Filtering incorrectly categorizes a web page

If you feel that FortiGuard Web Filtering has placed web pages in the wrong categories or you just want to review the FortiGuard Web Filtering categories of a web page you can:

For all maintenance releases of FortiOS v2.80 or FortiClient v2.0 connect to the FortiClient Web Filtering 1.0 web page at:
http://www.fortinet.com/FortiGuardCenter/webfiltering/webfiltering1.html

For FortiOS v3.0 or FortiClient v3.0 connect to the FortiClient Web Filtering 2.0 web page at:
http://www.fortinet.com/FortiGuardCenter/webfiltering/webfiltering2.html

From these pages you can check the FortiGuard category of a URL. If you disagree with the category (or if the URL is not rated), you can suggest a different category and also leave a comment about the URL.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com