

## FortiGuard:

Fortinet FortiGuard is a comprehensive threat intelligence and security subscription service provided by Fortinet. FortiGuard is designed to enhance the security capabilities of Fortinet's products, including their firewalls, antivirus solutions, intrusion prevention systems, and other security appliances. The FortiGuard services can be purchased and registered to your FortiGate FW unit.

FortiGuard provides real-time antivirus protection by constantly updating its signature databases to detect and block known malware, viruses, and other malicious files.

FortiGuard includes web filtering services that allow organizations to control access to websites based on categories, helping to prevent users from accessing malicious or inappropriate content.



## FortiGuard Ports:

Fortinet FortiGuard services use various ports depending on the specific service or feature being utilized. These ports are used for communication between Fortinet devices such as FortiGate firewalls and FortiGuard servers over the internet.

### 1. FortiGuard Web Filtering (HTTP/HTTPS):

- o Port 53 (DNS) for DNS queries.
- o Port 80 (HTTP) and Port 443 (HTTPS) for web traffic.

### 2. FortiGuard Antivirus Updates:

- o Port 53 (DNS) for DNS queries.
- o Port 8888 (HTTPS) for antivirus signature updates.

### 3. FortiGuard IPS Updates:

- o Port 53 (DNS) for DNS queries.
- o Port 8890 (HTTPS) for intrusion prevention system updates.

### 4. FortiGuard Application Control and URL Filtering:

- o Port 53 (DNS) for DNS queries.
- o Port 8888 (HTTPS) for application control and URL filtering updates.

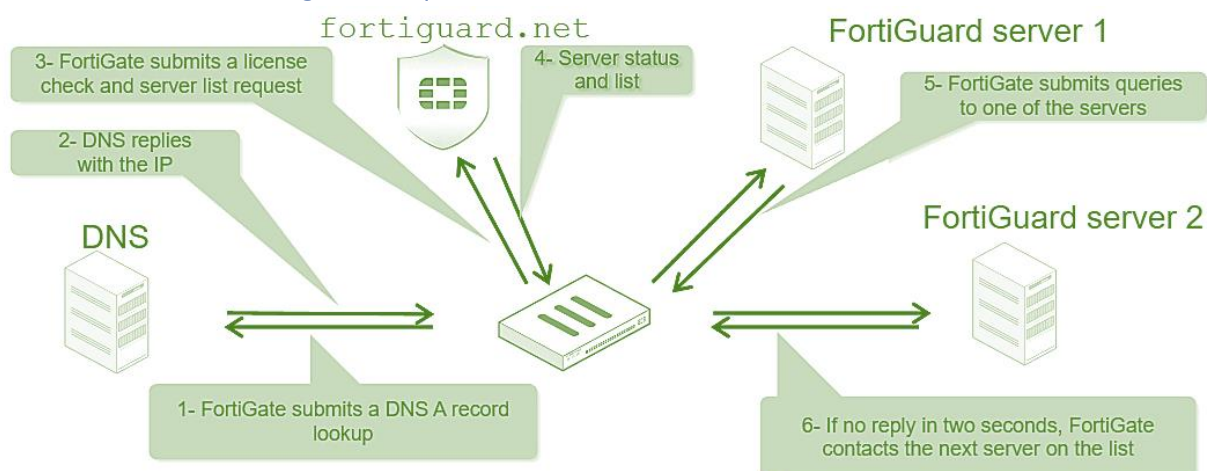
### 5. FortiGuard Anti-Spam Updates:

- o Port 53 (DNS) for DNS queries.
- o Port 8888 (HTTPS) for anti-spam updates.

### 6. FortiGuard Security Rating Services:

- o Port 53 (DNS) for DNS queries.
- o Port 8888 (HTTPS) for security rating services.

## FortiGuard Web Filtering & Antispam:



Go to **System > FortiGuard**, to see License Information & manual & automatic updates etc.

Accept push updates	Enable to allow updates to be sent automatically to your FortiGate. New definitions will be added as soon as they are released by FortiGuard.
Use override push	Only available if Accept push updates is enabled.
Scheduled Updates	Enable to schedule updates to be sent to FortiGate at specified time.
Improve IPS quality	Enable to send info to the FortiGuard servers when an attack occurs.
Use extended IPS signature package	Enable to use the extended IPS database, that includes protection from legacy attacks, along with the regular IPS database that protects against the latest common and in-the-wild attacks.
Update AV & IPS Definitions	Click to manually initiate an FDN update.

Filtering

Web Filter Cache

☒

Clear cache after

60

Minutes

Anti-Spam Cache

☒

Clear cache after

30

Minutes

FortiGuard Filtering Protocol

HTTPS

UDP

FortiGuard Filtering Port

443

53

8888

Filtering Services Availability

🔄

Check Again

Web Filtering

⬇️




Anti-Spam

⬇️

Request re-evaluation of a URL's category

Web Filter Cache	Enable/disable web filter cache and set the amount of time that the FortiGate will store a blocked IP address or URL locally. After the time expires, the FortiGate contacts the FDN to verify the address.
Anti-Spam Cache	Enable/disable email filter cache and set the amount of time that the FortiGate will store an email address locally.
FortiGuard Filtering Protocol	Select the protocol for contacting the FortiGuard servers.
FortiGuard Filtering Port	Select the port assignments for contacting the FortiGuard servers.
Filtering Service Availability	The status of the filtering service. Click Check Again if the filtering service is not available.
Request re-evaluation of a URL's category	Click to re-evaluate a URL category rating on the FortiGuard web filter service.

## Override FortiGuard Servers

 Create New	 Edit	 Delete
Server Address	Server Type	
No matching entries found		

### Override FortiGuard Servers:

- o FortiOS will update signature packages & query rating servers using public FortiGuard.
- o This FortiGuard Service list can be overridden by adding servers to the override server list.
- o Also, it is possible to communication with public FortiGuard servers can also be disabled.

#### Change Update Server Location

```
HQ-FW # config system fortiguard
HQ-FW (fortiguard) # set update-server-location usa
HQ-FW (fortiguard) # end
```

```
HQ-FW # config system fortiguard
HQ-FW (fortiguard) # set update-server-location automatic
HQ-FW (fortiguard) # end
```

```
HQ-FW # config system fortiguard
HQ-FW (fortiguard) # set update-server-location eu
HQ-FW (fortiguard) # end
```

#### FortiGuard Commands

```
HQ-FW # diagnose debug rating
HQ-FW # diagnose debug rating refresh
HQ-FW # diagnose autoupdate versions
```

#### Enable FortiGuard Real-Time debug

```
HQ-FW # diagnose debug application update -1
HQ-FW # diagnose debug enable
```

#### Force an Update

```
HQ-FW # execute update-now
```

#### Web Filtering Real-Time Debug

```
HQ-FW # diagnose debug application urlfilter -1
HQ-FW # diagnose debug enable
```

#### FortiGuard servers available for antivirus and IPS updates

```
HQ-FW # diagnose test application dnsproxy 7
HQ-FW # diagnose autoupdate status
```

### FortiGuard databases and engines installed

HQ-FW # diagnose autoupdate versions

### Configure scheduled updates









HQ-FW # config system autoupdate schedule

HQ-FW (schedule) # set status enable

HQ-FW (schedule) # set frequency automatic

HQ-FW (schedule) # end

Verify system event logs (ID **0100041000**), they are generated approximately every 10 minutes.

		 Log ID: 0100041000 	 Add Filter
Date/Time	Level	Message	Log Description
13 minutes ago		Fortigate scheduled update fcni=yes fdni=yes fsci=yes from 173.243....	FortiGate update succeeded
28 minutes ago		Fortigate scheduled update fcni=yes fdni=yes fsci=yes from 173.243....	FortiGate update succeeded
28 minutes ago		Fortigate update now fcni=yes fdni=yes fsci=yes virdb(91.09963) etd...	FortiGate update succeeded

### FortiGuard Updates

Scheduled updates



Every

Daily

Weekly

Automatic