

# DO NOT REPRINT

## © FORTINET

## Application Control Database

- You can view complete list of applications supported by FortiGuard application control on <https://fortiguard.com/>
  - You can review the application category or request a signature for a new application from the same website.

The screenshot shows two views of the FortiGuard Application Control Database. On the left, a search interface allows filtering by Risk Level (All, Level 5, Level 4, Level 3, Level 2, Level 1), Popularity (All, 5 stars, 4 stars, 3 stars, 2 stars, 1 star), and Category (All, Proxy). A blue callout bubble points to the 'Refine search using filters' link. On the right, a detailed view of the 'Tor' application is shown. The application has ID 13363, was released on Apr 25, 2008, updated on Jul 06, 2021, and categorized as a Proxy. It has a popularity rating of 5 stars. The description notes that Tor is a free proxy software designed for anonymous communication, using a volunteer network to conceal user location and usage. The references section links to the Tor project's index page. A red arrow points from the 'Tor (Proxy)' link in the left sidebar to the detailed view on the right.

You can view the latest version of the application control database on the FortiGuard website, or by clicking an individual application signature in the application control profile.

The application control database provides details about application control signatures based on category, popularity, and risk, to name a few.

When building an application control signature, the FortiGuard security research team evaluates the application and assigns a risk level based on the type of security risk. The rating is Fortinet-specific, and not related to the common vulnerability scoring system (CVSS) or other external systems. The rating can help you decide whether or not to block an application.

On the FortiGuard website, you can read details about each signature's related application.

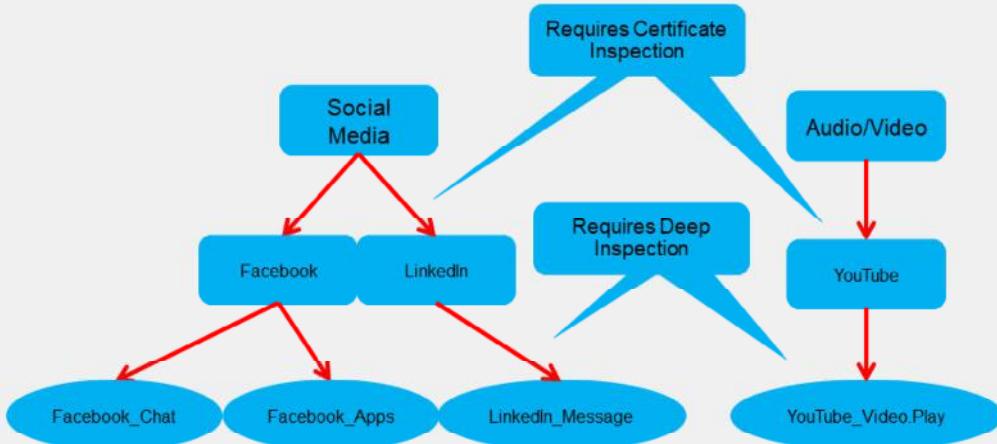
This slide shows an example for an application called Tor. Tor is a web proxy, so it belongs in the proxy category. A best practice is to create test policies that you can use to observe policy behavior.

If the most recent FortiGuard update does not include a definition for an application that you need to control, you can submit a request on the FortiGuard website to have the application added. You can also submit a request to re-evaluate an application category, if you believe an application should belong to a different category.

**DO NOT REPRINT****© FORTINET**

## Hierarchical Structure

- Application control signatures are organized in a hierarchical structure
  - The parent signature takes precedence over the child signature



Many web applications offer functionality that can be embedded in third-party websites or applications. For example, you can embed a Facebook **Like** button at the end of an article, or reference a YouTube video on an educational website. FortiOS gives administrators all the tools they need to inspect sub-application traffic. The FortiGuard application control signature database is organized in a hierarchical structure. This gives you the ability to inspect the traffic with more granularity. You can block Facebook applications while allowing users to collaborate using Facebook chat.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which statement about application control is true?

- A. Application control uses the IPS engine to scan traffic for application patterns.
- B. Application control is unable to scan P2P architecture traffic.

2. Which statement about the application control database is true?

- A. The application control database is separate from the IPS database.
- B. The application control database must be updated manually.

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Good job! You now understand basic application control functionality.

Now, you will learn about application control configuration.

**DO NOT REPRINT**  
© FORTINET

## Application Control Configuration

### Objectives

- Configure application control in profile mode
- Configure application control in next generation firewall (NGFW) policy mode
- Use the application control traffic shaping policy

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the application control operation modes that are available on FortiOS, you will be able to use application control effectively in both profile mode and NGFW policy mode.

**DO NOT REPRINT****© FORTINET**

## Application Control Profiles

- Configured when FortiGate NGFW mode is set to profile-based
- Uses flow-based scanning techniques in both inspection modes
- Allows you to filter application traffic based on:
  - Categories
    - Similar applications are grouped together
    - Can view application control signatures for that category
    - Can configure actions for predefined categories
  - Application overrides
    - Allows you to configure actions for specific signatures or applications
  - Filter overrides
    - Provides a more flexible way to create application categorization based on behavior, popularity, protocol, risk, and so on
- Must be applied to a firewall policy



© Fortinet Inc. All Rights Reserved.

14

When FortiGate or a VDOM is operating in flow-based (NGFW mode set to profile-based, policy set to flow-based) inspection mode or policy set to proxy-based inspection mode, to configure application control, administrators must create an application control *profile* and apply that profile to a firewall policy.

It is important to note that the application control profile uses flow-based scanning techniques, regardless of which inspection mode is used on the policy.

The application control profile consists of three different types of filters:

- Categories: Groups applications based on similarity. For example, all applications that are capable of providing remote access are grouped in the **Remote Access** category. You can view the signatures of all applications in a category or apply an action to a category as a whole.
- Application overrides: Provides the flexibility to control specific signatures and applications.
- Filter overrides: Useful when a predefined category does not meet your requirements and you want to block all applications based on criteria that is not available in categories. You can configure the categorization of applications based on behavior, popularity, protocol, risk, vendor, or the technology used by the applications, and take action based on that.

# DO NOT REPRINT

## © FORTINET

## Configuring an Application Control Profile

- The application control profile is available only when NGFW mode is set to profile-based inspection mode

**Security Profiles > Application Control**

111 Cloud Applications require deep inspection.  
0 policies are using this profile.

Name: wifi-default  
Comments: Default configuration for offloading WiFi traffic. 50/255

Categories:

- All Categories (highlighted with a red box)
- Business (153, △ 6)
- Email (77, △ 12)
- IoT (450)
- P2P (56)
- Social.Media (118, △ 32)
- Video/Audio (155, △ 17)
- Unknown Applications (highlighted with a red box)
- Cloud.IT (66, △ 1)
- Game (86)
- Mobile (3)
- Proxy (174)
- Storage.Backup (161, △ 19)
- VoIP (23)
- Collaboration (268, △ 16)
- General.Interest (233, △ 8)
- Network.Service (334)
- Remote.Access (95)
- Update (49)
- Web.Client (24)

Firmware & General Updates License: Licensed (Expiration Date: 2022/12/19)  
Application Control Signatures Package: Version 20.00291

Application Signatures: [View Application Signatures](#) (highlighted with a red box)

Additional Information:

- API Preview
- References
- Edit In CLI
- Documentation: Online Help, Video Tutorials

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

15

The application control profile is configured on the **Application Control** page. You can configure actions based on categories, application overrides, and filter overrides. You can also view the list of application control signatures by clicking **View Application Signatures**.

At the top of the **Application Control** profile page, you will see a summary of how many cloud applications require deep inspection. Cloud applications that use SSL encryption cannot be scanned without a deep inspection profile. FortiGate must decrypt the traffic in order to perform inspection and control application traffic.

The **Unknown Applications** setting matches traffic that can't be matched to any application control signature and identifies the traffic as **unknown application** in the logs. Factors that contribute to traffic being identified as **unknown application** include:

- How many rare applications your users are using
- Which IPS database version you are using

Identifying traffic as unknown can cause frequent log entries. Frequent log entries decrease performance.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring Additional Options

- Application control profiles include additional options that you can configure

The number to the right of the cloud symbol indicates the number of cloud applications in the category.

**Options**

- Block applications detected on non-default ports:  Allow
- Allow and Log DNS Traffic:  Allow
- QUIC:  Allow  Block
- Replacement Messages for HTTP-based Applications:  Allow  Block

The number listed to the right of the cloud symbol indicates the number of cloud applications in the category.

**Allow and Log DNS Traffic:** Enable this option to allow DNS traffic for the application sensor. Depending on the application and how often it queries DNS servers, enabling this setting can use significant system resources.

**QUIC:** QUIC is a protocol from Google that uses UDP instead of the standard TCP connections for web access. UDP is not scanned by web filtering. Allowing QUIC instructs FortiGate to inspect Google Chrome packets for a QUIC header and to generate logs as QUIC messages. Blocking QUIC forces Google Chrome to use HTTP2/TLS1.2 and FortiGate to log QUIC as blocked. The default action for QUIC is **Block**.

**Replacement Messages for HTTP-based Applications:** This setting allows you to replace blocked content from HTTP/HTTPS applications with an explanation for the user's benefit. For non-HTTP/HTTPS applications, FortiGate only drops the packets or resets the TCP connection.

After you've configured the application control profile, select the profile in the firewall policy. Like any other security profile, the settings you configure in the application control profile are not applied globally. FortiGate applies the application control profile settings only to traffic governed by the firewall policy in which you've selected the application control profile. This allows granular control.

**DO NOT REPRINT**

© FORTINET

## Protocol Enforcement

- Allows blocking or monitoring of known services on unknown ports

The screenshot shows the FortiGate Security Profiles > Application Control interface. On the left, there's a tree view of categories like Business, Email, Mobile, Proxy, Storage/Backup, VoIP, Cloud/IT, Game, Network Service, P2P, Remote Access, Update, Collaboration, General Interest, Social Media, Video/Audio, and Web Client. Below this is a table for 'Network Protocol Enforcement' with columns for Port #, Enforce Protocols, and Violation Action. It shows two entries: Port 52 with PROT DNS and Monitor action, and Port 80 with PROT HTTP and Block action. A red box highlights the 'Create New' button. To the right, a modal window titled 'Edit Default Network Service' is open for port 80. It lists 'Enforce protocols' (PROT HTTP) and 'Violation action' (Monitor, Block). A red box highlights the 'PROT HTTP' entry in the list. A blue callout box labeled 'List of known services' points to a sidebar on the right containing a list of services: DNS, FTP, PROT HTTP (highlighted in yellow), HTTPS, IMAP, NNTP, POP3, SMTP, SNMP, SSH, and TELNET.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

17

Protocol enforcement is added to the application control profile, allowing the administrator to configure network services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, and 443), while blocking those services on other ports.

The feature takes action in the following scenarios:

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is whitelisted under the server port. If it is not, then the traffic is considered a violation and IPS can take the action (for example, block) specified in the configuration.
- There is no confirmed service for network traffic. It would be considered a service violation if IPS dissectors rule out all the services enforced under its server port. For example, if port 21 is configured for FTP and IPS Dissector could not decide on the exact service but is sure it is not FTP. If the port of the non-ftp traffic is 21, it will be a violation.

# DO NOT REPRINT

## © FORTINET

### Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
  - Application and filter overrides
  - Categories

The screenshot shows the 'Edit Application Sensor' configuration page. At the top, there's a 'Name' field set to 'default' and a 'Comments' field containing 'Monitor all applications.' Below these are sections for 'Categories' and 'Application and Filter Overrides'. The 'Categories' section lists various application categories like Business, Email, Mobile, etc., each with a count of detected applications. The 'Application and Filter Overrides' section has a table with columns for Priority, Details, Type, and Action, showing 'No results'. At the bottom, there are several 'Options' checkboxes: 'Block applications detected on non-default ports' (checked), 'Allow and Log DNS Traffic' (checked), 'QUIC' (unchecked), and 'Replacement Messages for HTTP-based Applications' (unchecked). A note at the bottom says '© Fortinet Inc. All Rights Reserved.' and a page number '18'.

**FORTINET**  
Training Institute

The IPS engine examines the traffic stream for a signature match.

Then, FortiGate scans packets for matches, in this order, for the application control profile:

- Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies.
- Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories.

**DO NOT REPRINT**  
**© FORTINET**

## Order of Scan and Blocking Behavior (Scenario 1)

1. **Application Overrides:** Battle.Net and Dailymotion applications are set to **Monitor**
2. **Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
  - Contains applications from different categories – BitTorrent (P2P), Adobe Update (Update), FaceTime (VOIP), Flickr (Social.Media)
3. **Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories are set to **Monitor**

The screenshot shows the 'Security Profiles > Application Control' page. At the top, there's a table for 'Categories' with columns for Name, Count, and Action. Categories listed include Business (147), Email (77), Mobile (3), Proxy (168), Storage Backup (164), VoIP (24), Cloud.IOT (47), Game (84), Network Service (330), Remote Access (86), Update (49), WebClient (24), Collaboration (260), General Interest (226), P2P (56), Social Media (115), and Unknown Applications. The 'Game' category is highlighted with a red box and circled with a green number 3. Below this is a section for 'Network Protocol Enforcement'. The main focus is the 'Application and Filter Overrides' table, which has columns for Priority, Details, Type, and Action.

Name	Count	Action
Business	147	Monitor
Email	77	Monitor
Mobile	3	Monitor
Proxy	168	Monitor
Storage Backup	164	Monitor
VoIP	24	Monitor
Cloud.IOT	47	Monitor
<b>Game</b>	84	Block
Network Service	330	Monitor
Remote Access	86	Monitor
Update	49	Monitor
WebClient	24	Monitor
Collaboration	260	Monitor
General Interest	226	Monitor
P2P	56	Monitor
Social Media	115	Monitor
<b>Video/Audio</b>	16	Block
Unknown Applications		Monitor

Priority	Details	Type	Action
1	BattleNet Dailymotion	Application	Monitor
2	Excessive-Bandwidth	Filter	Block

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

In the example profile shown on this slide, the application control profile blocks the **Game** and **Video/Audio** categories. For applications in these categories, FortiGate responds with the application control HTTP block message. (It is slightly different from the web filtering HTTP block message.) All other categories are set to **Monitor**, except **Unknown Applications**, and are allowed to pass traffic.

In the **Application and Filter Overrides** section, you can see that some exceptions are specified. Instead of being set to **Block**, **Battle.Net (Game)** and **Dailymotion (Video/Audio)** are set to **Monitor**. Because application overrides are applied first in the scan, these two applications are allowed, and generate logs.

Next, the scan checks for **Application and Filter Overrides**. Because a filter override is configured to block applications that use excessive bandwidth, it blocks all applications using excessive bandwidth, regardless of categories that allow these applications.

This slide shows an example of how several security profile features could work together, overlap, or work as substitutes, on the same traffic.

After the application control profile scan is done, FortiGate begins other scans, such as web filtering. The web filtering scan could block Battle.Net and Dailymotion, but it would use its own block message. Also, web filtering doesn't check the list of application control overrides. So, even if an application control override allows an application, web filtering could still block it.

Similarly, static URL filtering has its own exempt action, which bypasses all subsequent security checks. However, application control occurs before web filtering, so that the web filtering exemption cannot bypass application control.

**DO NOT REPRINT**  
**© FORTINET**

## Order of Scan and Blocking Behavior (Scenario 2)

1. **Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
  - Contains applications from different categories – BitTorrent (P2P), Adobe.Update (Update), FaceTime (VOIP), Flickr (Social.Media)
2. **Application Overrides:** Battle.Net and Dailymotion applications are set to **Monitor**
3. **Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories set to **Monitor**

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Battle-Net Dailymotion	Application	Monitor

In the example profile shown on this slide, the filter override has been moved above the application override. In this scenario, the filter override (**Excessive-Bandwidth**) is blocked and, since **Dailymotion** falls under the excessive bandwidth category, Dailymotion is blocked even though it is set to **Monitor** under the **Application and Filter Overrides** section.

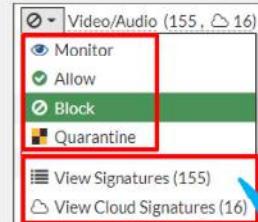
The priority in which application and filter overrides are placed takes precedence.

# DO NOT REPRINT

## © FORTINET

### Actions

- **Allow**
  - Continue to next scan or feature and do not log
- **Monitor**
  - Allow but log
    - Good for the initial study of your network traffic
- **Block**
  - Drop packets and log
- **Quarantine**
  - Block and log traffic from attacker IP address until the expiration time
    - Can set duration to days, hours, or minutes



View the list of signatures  
of native or cloud  
applications for a specific  
category

For each filter in the application control profile, you must indicate an action—what FortiGate does when traffic matches. Actions include the following:

- **Allow:** Passes the traffic and does not generate a log
- **Monitor:** Passes the traffic, but also generates a log message
- **Block:** Drops the detected traffic and generates a log message
- **Quarantine:** Blocks the traffic from an attacker IP until the expiration time is reached and generates a log message

The **View Signature** action allows you to view signatures from a particular category only and is *not* a configurable action. The **View Cloud Signatures** action allows you to view application signatures for cloud applications from a particular category.

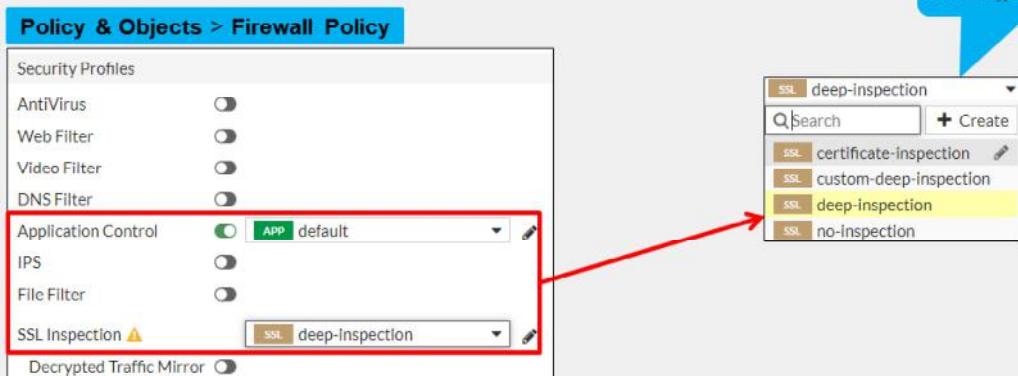
Which is the correct action to choose?

If you're not sure which action to choose, **Monitor** can be useful initially, while you study your network. Later, after you have studied your network traffic, you can fine-tune your filter selection by choosing the most appropriate action. The action you choose also depends on the application. If an application requires feedback to prevent instability or other unwanted behavior, then you might choose **Quarantine** instead of **Block**. Otherwise, the most efficient use of FortiGate resources is to block.

DO NOT REPRINT  
© FORTINET

## Applying an Application Control Profile

- You must apply the **Application Control** profile on a firewall policy to scan the passing traffic
  - You must also select **SSL/SSH Inspection** profile

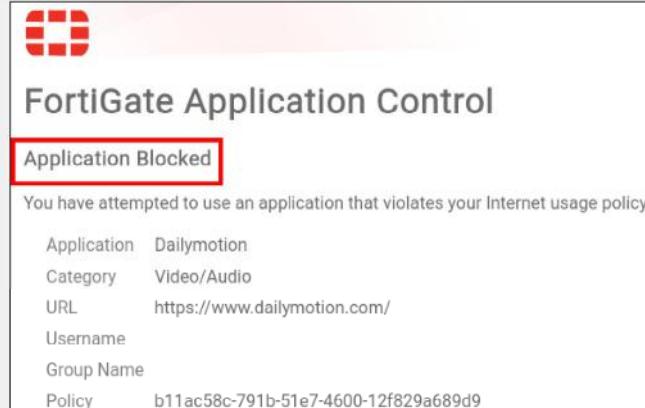


After you configure an application control profile, you must apply it to a firewall policy. This instructs FortiGate to start scanning application traffic that is subject to the firewall policy.

**DO NOT REPRINT****© FORTINET**

## Block Page

- Application control in profile mode displays similar HTTP block pages
- HTTP block page includes:
  - Category
  - Website host and URL
  - User name (if authentication is enabled)
  - Group name (if authentication is enabled)
  - Policy UUID



For HTTP-based applications, application control can provide feedback to the user about why their application was blocked. This is called a block page, and it is similar to the one you can configure for URLs that you block using FortiGuard web filtering.

It is also worth mentioning that, if deep inspection is enabled in the firewall policy, all HTTPS-based applications provide this block page.

The block page contains the following information:

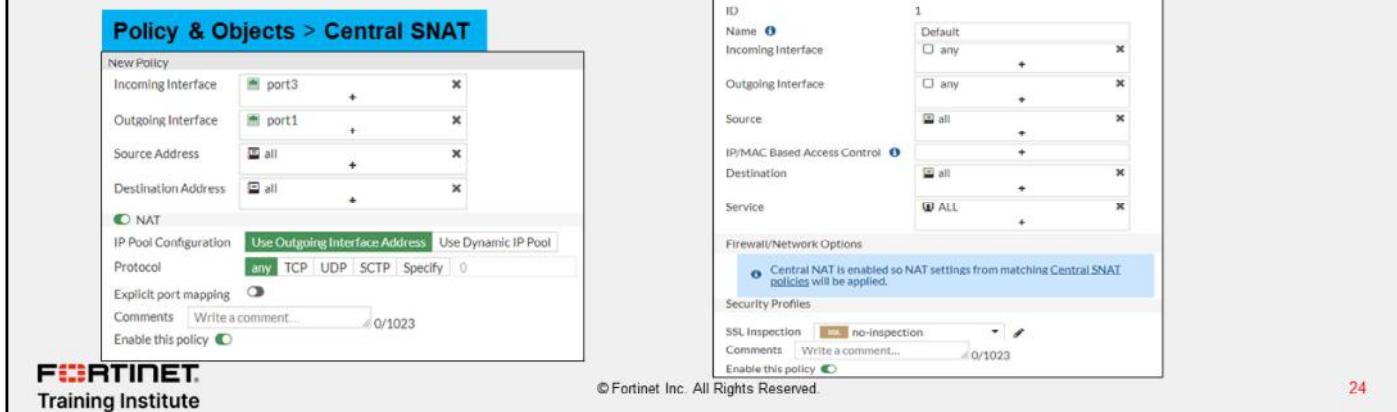
- Signature that detected the application (in this case, Dailymotion)
- Signature's category (Video/Audio)
- URL that was specifically blocked (in this case, the index page of [www.dailymotion.com](https://www.dailymotion.com/)), since a web page can be assembled from multiple URLs
- User name (if authentication is enabled)
- Group name (if authentication is enabled)
- UUID of the policy governing the traffic

The last item in this list can help you to identify which policy on FortiGate blocked the page, even if you have a large number of policies with many FortiGate devices securing different segments.

**DO NOT REPRINT**  
**© FORTINET**

## NGFW Policy-Based Mode

- Available in flow-based inspection mode only
- Application control is configured directly on the security policy
  - Cannot configure application control profile
- Must select SSL inspection profile on an SSL Inspection & Authentication (consolidated) policy
- Requires the use of central SNAT policy



The screenshot displays two configuration pages from the FortiGate management interface:

- Policy & Objects > Central SNAT**: Shows a policy named "1" with the following settings:
  - New Policy**:
    - Incoming Interface: port3
    - Outgoing Interface: port1
    - Source Address: all
    - Destination Address: all
  - NAT** checkbox is checked.
  - IP Pool Configuration**:
    - Use Outgoing Interface Address (selected)
    - Use Dynamic IP Pool
    - Protocol: any (selected)
    - TCP | UDP | SCTP | Specify (disabled)
    - Explicit port mapping: off
  - Comments**: Write a comment... / 0/1023
  - Enable this policy** checkbox is checked.
- Policy & Objects > SSL Inspection & Authentication**: Shows a policy named "1" with the following settings:
  - ID**: 1
  - Name**: Default
  - Incoming Interface**: any
  - Outgoing Interface**: any
  - Source**: all
  - IP/MAC Based Access Control**: all
  - Destination**: all
  - Service**: ALL
  - Firewall/Network Options**:
    - Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.
  - Security Profiles**:
    - SSL Inspection: no-inspection
    - Comments: Write a comment... / 0/1023
    - Enable this policy checkbox is checked.

Fortinet Training Institute logo and "© Fortinet Inc. All Rights Reserved." are visible at the bottom left, and the number "24" is at the bottom right.

When FortiGate is operating in NGFW policy-based mode, administrators can apply application control to a security policy directly, instead of having to create an application control profile first, and then apply that to a firewall policy. Eliminating the need to use an application control profile makes it easier for the administrator to select the applications or application categories they want to allow or deny in the firewall policy.

It is important to note that all security policies in an NGFW policy-based mode VDOM or FortiGate must specify an SSL/SSH inspection profile on a consolidated policy. NGFW policy-based mode also requires the use of central source NAT (SNAT), instead of NAT settings applied within the firewall policy.

**DO NOT REPRINT**  
**© FORTINET**

## NGFW Policy-Based Mode (Contd)

- You can select applications, application categories, or groups directly on a security policy
- You can apply the **ACCEPT** or **DENY** actions to allow or block selected application traffic
- If a **URL Category** is set, then applications that you add to the policy must be within the browser-based technology category
- You can apply the **AntiVirus** and **IPS** security profiles to a security policy with the action set to **ACCEPT**

The screenshot shows the FortiOS configuration interface for creating a new security policy. The 'Application' column in the list view is highlighted with a red box, and a blue callout points to it with the text 'List is searchable'. The list includes various application signatures like Acronis.Snap.Disk, ActiveCampaign, ADP, AirWatch.MDM, Alibaba, Apache.Cassandra, Appliance.CRM, Atlassian.JIRA, AutoTrack.360, Autodesk.BIM360, Autodesk.Buzzsaw, and Baidu.PC.Faster.

You can select one or more applications, application groups, and application categories on a security policy in the **Application** section. After you click the **+** icon for an application, a pop-up window opens. In that window, you can search for and select one or more application signatures, application groups, or application categories. Based on the applications, groups, and application categories applied to the policy, FortiOS applies the security action to the application traffic.

You can configure the **URL Category** within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website.

You can also configure the **Group** with multiple applications and application categories. This allows the administrator to mix multiple applications and categories.

In addition to applying a URL category filter, you can also apply **AntiVirus** and **IPS** security profiles to application traffic that is allowed to pass through.

**DO NOT REPRINT****© FORTINET**

## How Does NGFW Policy-Based Filtering Work?

- It is a three-step process:
  - Step 1—Allow all applications until they can be identified:
    - Uses only the IPv4 header information to match the policy
    - Accepts the traffic
    - Creates an entry in the session table with the `may_dirty` flag
    - Forwards all the packets to the IPS engine for inspection
  - Step 2—As soon as the IPS engine identifies the application, it adds the following to the session:
    - `dirty` flag - instructs the kernel to re-evaluate session entry
    - `app_valid` flag - indicates that IPS engine has validated the traffic
    - Application ID
  - Step 3—The `dirty` flag instructs the kernel to look up the security policy again:
    - This time the kernel uses the Layer 4 headers *and* the Layer 7 information to match the traffic
    - The action configured in the security policy is applied to the identified application traffic



© Fortinet Inc. All Rights Reserved.

26

FortiOS uses a three-step process to perform NGFW policy-based application filtering. Here is a brief overview of what happens at each step.

In step 1, FortiOS allows all traffic while forwarding packets to the IPS engine for inspection and identification of the traffic. At the same time, FortiOS creates an entry in the session table allowing the traffic to pass and it adds a `may_dirty` flag to it.

In step 2, as soon as the IPS engine identifies the application, it updates the session entry with the following information: `dirty` flag, `app_valid` flag, and an application ID.

In step 3, the FortiOS kernel performs a security policy lookup again, to see if the identified application ID is listed in any of the existing security policies. This time the kernel uses both Layer 4 and Layer 7 information for policy matching. After the criteria matches a firewall policy rule, the FortiOS kernel applies the action configured on the security policy to the application traffic.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring App Control in Policy-Based Mode

The screenshot shows the FortiGate UI for configuring a security policy. On the left, the 'Policy & Objects > Security Policy' tab is selected. A new policy is being created with the following settings:

- ID:** 0
- Name:** Internet Access
- Policy Mode:** Standard
- Incoming Interface:** port3
- Outgoing Interface:** port1
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** App Default
- Application:** Amazon.AWS (selected)
- Action:** ACCEPT

A red box highlights the 'Amazon.AWS' entry in the application list. A red arrow points from this box to a 'Select Entries' modal window titled 'Select Entries'. This window has three tabs: Application (selected), Category, and Group. The 'Category' tab is also highlighted with a red box. The 'Category' tab displays a list of application categories, with 'Amazon.AWS' highlighted in yellow.

Another red arrow points from the 'Category' tab in the 'Select Entries' window to a 'New Application Group' window. This window is titled 'New Application Group' and contains the following fields:

- Group Name:** High Bandwidth
- Type:** Application
- Members:** Dailymotion, YouTube
- Comments:** Write a comment... (0/255)

At the bottom left of the main interface is the Fortinet Training Institute logo. At the bottom right is the number 27.

Configuring application control in NGFW policy-based mode is simple. You can create a new security policy or edit an existing security policy. In the **Application** section, select the applications, categories, or groups that you want to allow or deny, and change the security policy **Action** accordingly. For applications that you selected to allow, you can further enhance network security by enabling antivirus scanning and IPS control. You can also enable the logging of **Security Events** or **All Sessions** to ensure that all application control events are logged.

**DO NOT REPRINT**  
**© FORTINET**

## Policy-Based Central SNAT Policy

**Policy & Objects > Central SNAT**

<b>New Policy</b>		
Incoming Interface	port3	+
Outgoing Interface	port1	×
Source Address	all	+
Destination Address	all	×
<input checked="" type="checkbox"/> NAT IP Pool Configuration: <span style="background-color: #00AEEF; color: white; padding: 2px 10px;">Use Outgoing Interface Address</span> <span style="border: 1px solid #00AEEF; padding: 2px 10px;">Use Dynamic IP Pool</span> Protocol: any TCP UDP SCTP Specify 0		

**Policy & Objects > SSL Inspection & Authentication**

<b>Edit Policy</b>		
ID	1	
Name	Default	
Incoming Interface	<input type="checkbox"/> any	
Outgoing Interface	<input type="checkbox"/> any	
Source	all	
IP/MAC Based Access Control		
Destination	all	
Service	ALL	
<b>Firewall/Network Options</b>		
Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.		
<b>Security Profiles</b>		
SSL Inspection	no-inspection	<input type="button" value="Edit"/>
Comments	Write a comment... / 0/1023	
<input checked="" type="checkbox"/> Enable this policy		

**FORTINET**  
Training Institute
© Fortinet Inc. All Rights Reserved.
28

You must have a matching central SNAT policy in NGFW policy-based mode to be able to pass traffic. FortiGate applies NAT on the traffic based on the criteria defined in the central SNAT policy.

It is extremely important to arrange security policies in **Policy & Objects**, so that the more specific policies are located at the top to ensure proper use of application control.

A default **SSL Inspection & Authentication** policy inspects traffic accepted by any of the security firewalls, and by using the **certificate-inspection** SSL inspection profile.

**DO NOT REPRINT**

**© FORTINET**

## NGFW Policy Matching

- Based on the configuration shown in the screenshot:
  - Facebook, Flickr, Instagram, and Pinterest application traffic is blocked by policy ID 1
  - All other Social.Media (for example, LinkedIn) application traffic is allowed by policy ID 2
  - All applications that belong to the P2P application category are blocked by policy ID 3
  - All other traffic and applications are allowed by policy ID 4

**Policy & Objects > Security Policy**

ID	Name	Source	Destination	Schedule	Service	Applications	Action	Security Profiles	Log
1	Blocking apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest	DENY		All
2	Allow social media	all	all	always	App Default	Social.Media	ACCEPT	default	All
3	Blocking P2P Apps	all	all	always	App Default	P2P	DENY		Disabled
4	Allow all	all	all	always	App Default		ACCEPT	default	UTM

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

29

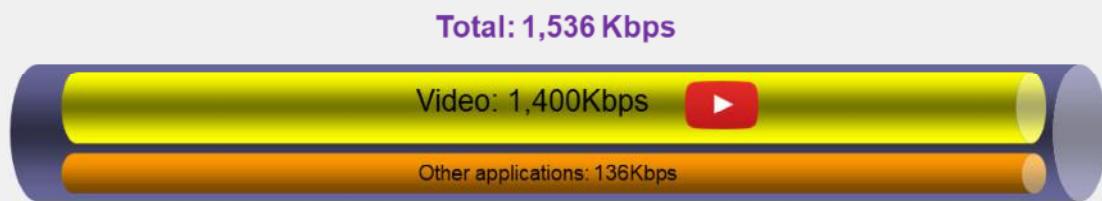
NGFW policy matching works using a top-to-bottom approach. You must have a specific policy above a more broad or open policy. For example, if you would like to block Facebook but allow the **Social.Media** category, you must place the policy blocking Facebook traffic above the policy allowing the **Social.Media** category.

# DO NOT REPRINT

## © FORTINET

## Application Control Traffic Shaping

- Granular control of bandwidth usage
- Some traffic can't be distinguished by port number/IP
  - Example: YouTube video URLs—don't say whether it is a text comment or a video  
<https://www.youtube.com/watch?v=eO2vyJDoP3M>
- Only traffic that matches the signature is shaped
  - Won't interfere with other apps on same port/protocol
  - Useful for managing bandwidth-intensive apps



If an application is necessary, but you must prevent it from impacting bandwidth then, instead of blocking it entirely, you can apply a rate limit to the application. For example, you can rate limit applications used for storage or backup leaving enough bandwidth for more sensitive streaming applications, such as video conferencing.

Applying traffic shaping to applications is very useful when you're trying to limit traffic that uses the same TCP or UDP port numbers as mission-critical applications. Some high-traffic web sites, such as YouTube, can be throttled in this way.

Examine the details of how throttling works. Not all URL requests to [www.youtube.com](http://www.youtube.com) are for video. Your browser makes several HTTPS requests for:

- The web page itself
- Images
- Scripts and style sheets
- Video

All of these items have separate URLs. If you analyze a site like YouTube, the web pages themselves don't use much bandwidth; it is the video content that uses the most bandwidth. But, since all content is transported using the same protocol (HTTPS), and the URLs contain dynamically generated alphanumeric strings, traditional firewall policies can't block or throttle the traffic by port number or protocol because they are the same. Using application control, you can rate limit only videos. Doing this prevents users from saturating your network bandwidth, while still allowing them to access the other content on the site, such as for comments or sharing links.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring the Traffic Shaping Policy

- Must ensure matching criteria aligns with the settings in your firewall policy
  - Firewall policy must allow the traffic that you wish to control bandwidth of
- Can shape traffic for application control based on:
  - Application category
  - Application
  - Application group

Used for web filtering

The screenshot shows the 'Traffic Shaping Policies' configuration screen. In the 'If Traffic Matches:' section, the 'Application' field is expanded, showing 'Dailymotion', 'Twitch', and 'YouTube'. Below this, the 'URL Category' field is also expanded. In the 'Then:' section, the 'Outgoing Interface' is set to 'port2'. Under 'Apply shaper', 'Shared shaper' is selected with 'shared-1M-pipe' applied. 'Reverse shaper' is set to 'medium-priority'. 'Per-IP shaper' is set to 'Lmitie-10-Sessions'. To the right, a sidebar titled 'Select Entries' lists various applications under 'FIREWALL APPLICATION (2,414)'.

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

31

You can limit the bandwidth of an application category, application group, or specific application by configuring a traffic shaping policy. You can also apply traffic shaping to FortiGuard web filter categories and to the application group.

You must ensure that the matching criteria aligns with the firewall policy or policies to which you want to apply shaping. It does not have to match outright. For example, if the source in the firewall policy is set to **all** (0.0.0.0/0.0.0.0), you can set the source in the traffic shaping policy to any source that is included in **all**, for example, **LOCAL\_SUBNET** (10.0.1.0/24).

If the traffic shaping policy is not visible in the GUI, you can enable it on the **Feature Visibility** page.

There are two types of shapers that you can configure on the **Traffic Shaping Policy** page, and you can apply them in the traffic shaping policy:

- **Shared shaper**: applies a total bandwidth to all traffic using that shaper. The scope can be per policy or for all policies referencing that shaper.
- **Per-IP shaper**: applies traffic shaping to all source IP addresses in the security policy. Bandwidth is equally divided among the group.

Note that the outgoing interface is usually the egress interface (WAN). The **Shared shaper** setting is applied to ingress-to-egress traffic, which is useful for restricting bandwidth for uploading. The **Reverse Shaper** setting is also a shared shaper, but it is applied to traffic in the reverse direction (egress-to-ingress traffic). This is useful for restricting bandwidth for downloading or streaming, because it limits the bandwidth from the external interface to the internal interface.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which statement about application control in an NGFW policy-based configuration is true?  
 A. Applications are applied directly to the security policies.  
 B. The application control profile must be applied to firewall policies.
  
2. Which statement about the HTTP block page for application control is true?  
 A. It can be used only for web applications.  
 B. It works for all types of applications.

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control



Best Practices and Troubleshooting

Good job! You now understand application control configuration.

Now, you will learn about logging and monitoring application control events.

**DO NOT REPRINT**

© FORTINET

## Logging and Monitoring Application Control

### Objectives

- Enable application control logging events
- Monitor application control events
- Use FortiView to see a detailed view of application control logs

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in application control configuration, including reviewing application control logs, you will be able to effectively use and monitor application control events.

**DO NOT REPRINT**  
**© FORTINET**

## Enabling Application Control Logging

- Example of NGFW policy-based mode firewall policies

ID	Name	Source	Destination	Schedule	Service	Applications	Action	Security Profiles	Log
1	Blocking.apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest	DENY	All	
2	Allow social media	all	all	always	App Default	Social.Media	ACCEPT	default	All
3	Blocking P2P Apps	all	all	always	App Default	P2P	DENY	disabled	UTM
4	Allow all	all	all	always	App Default		ACCEPT	default	UTM

**Policy & Objects > Security Policy**

© Fortinet Inc. All Rights Reserved.

35

Regardless of which operation mode application control is configured in, you must enable logging on the security or firewall policy. When you enable the logging of security events or all sessions on a security or firewall policy, application control events are also logged. You must apply application control to the security or firewall policy to enable application control event logging.

When the **Deny** action is selected on a security or firewall policy, you must enable the **Log Violations** option to generate application control events for blocked traffic.

# DO NOT REPRINT

## © FORTINET

## Logging Application Control Events

- FortiGate logs all application control events on the **Security Events** pane on the **Log & Report** page

The screenshot shows the FortiGate Log & Report interface. In the top navigation bar, there is a blue button labeled "Log & Report > Security Events". Below this, there are two tabs: "Summary" and "Details". The "Summary" tab is selected, showing a table with three rows: "Top Category" (WebClient), "Action" (Pass), "Count" (601); "NetworkService", "Pass", "279"; and "Video/Audio", "Pass", "71". A red box highlights the "Application Control" link in the top right corner of the summary table. An arrow points from this link to the "Details" tab, which is currently selected. The "Details" tab displays a table of log entries. One specific entry is highlighted with a red box: "Date/Time" 10/01/10 3 hours ago, "Source" 193.8.215.136 (dailymotion.com), "Destination" 10.0.1.10, "Application Name" Dailymotion, "Action" block, "Log Details" (expanded) showing fields like IP, Port, Country/Region, Destination Interface, Hostname, and URL. The entire "Log Details" section is also highlighted with a red box.

**FORTINET**  
Training Institute

FortiGate logs all application control events on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Application Control**.

In the example shown on this slide, the default application control profile blocks access to **Dailymotion**. You can view this information in the **Log Details** section, as well as information about the log source, destination, application, and action.

Note that application control generates this log message using a profile-based configuration. The log message for an NGFW policy-based configuration, does not include information that does not apply, such as application sensor name. The remainder of the information and structure of the log message is the same for each log, regardless of which inspection mode FortiGate is using.

You can also view the details on the **Forward Traffic** logs pane, where firewall policies record activity. You can also find a summary of the traffic to which FortiGate applied application control. Again, this is because application control is applied by a firewall policy. To find out which policy applied application control, you can review either the **Policy ID** or the **Policy UUID** fields of the log message.

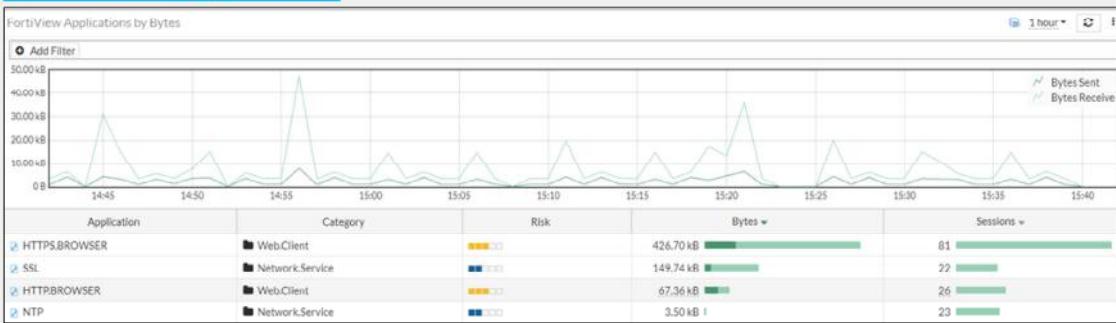
DO NOT REPRINT  
© FORTINET

## Application Control Events In Dashboard View

- Application control events are saved in a standalone dashboard on the **Top Applications** dashboard

- Requires disk logging

Dashboard > Top Applications



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

37

On the **Dashboard** menu, the **Top Applications** standalone page provides details about each application, such as the application name, category, and bandwidth. You can drill down further to see more granular details by double-clicking an individual log entry. The detailed view provides information about the source, destination, policies, or sessions for the selected application.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Where do you enable logging of application control events?  
 A. Application control logs are enabled in the firewall policy configuration.  
 B. Application control logs are enabled on the **FortiView Applications** page of FortiGate.
  
2. Which piece of information is not included in the application event log when using NGFW policy-based mode?  
 A. Application control profile name  
 B. Application name

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Good job! You now understand application control logging and monitoring.

Now, you will learn about application control best practices and troubleshooting.

**DO NOT REPRINT****© FORTINET**

## Best Practices and Troubleshooting

### Objectives

- Recognize best practices for application control configuration
- Understand how to troubleshoot application control update issues



40

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in application control best practices and troubleshooting, you will be able to configure and maintain an effective application control solution.

**DO NOT REPRINT****© FORTINET**

## Best Practices for Application Control

- Apply application control to only the traffic that requires it
  - Specify subnets (source, destination, or both) within the firewall policy, whenever possible
  - Don't apply application control to internal-to-internal traffic
- If using load balancing or failover internet connections, apply identical application control on all load balancing or redundant firewall policies
- Select **Deep-Inspection** instead of **Certificate-based** inspection as the SSL/SSH inspection method
- Use a FortiCloud account to save and view application control events in FortiView
  - FortiGate devices that don't have an internal disk for logging require FortiCloud logging to use FortiView
- Use hardware acceleration for application signature matching



© Fortinet Inc. All Rights Reserved.

41

This slide lists some best practices to keep in mind when implementing application control on FortiGate.

Not all traffic requires an application control scan. Don't apply application control to internal-only traffic.

To minimize resource use on FortiGate, be as specific as possible when creating firewall policies. This reduces resource use, and also helps you build a more secure firewall configuration.

Create identical firewall policies for all redundant internet connections, to ensure that the same inspection is performed on failover traffic. Select **Deep-Inspection** instead of **Certificate-based** inspection for the SSL/SSH inspection mode, to ensure content inspection is performed on encryption protocols.

FortiGate models that feature specialized chips, such as network processors and content processors, can offload and accelerate application signature matching for enhanced performance.

You can use a FortiCloud account to save and view application control logs in FortiView, on FortiGate devices that do not have a log disk.

**DO NOT REPRINT**  
© FORTINET

## Application Control Troubleshooting

- If FortiGuard has update issues, make sure that:
  - FortiGate has a stable connection to the internet
  - FortiGate is able to resolve DNS (`update.fortiguard.net`)
  - TCP port 443 is open
- Force FortiGate to check for new application control updates:  
`execute update-now`
- Verify that the application control signatures database version is up-to-date with the FortiGuard website



The screenshot shows the 'System > FortiGuard' section of the FortiGate management interface. It displays license information for FortiCare Support, FortiCloud Account, Hardware Version, Enhanced Support, and Virtual Machine. The 'Virtual Machine' section shows a progress bar for allocated vCPUs at 100% (1/1) and 2 GiB of RAM. A 'FortiGate VM License' button is present. The bottom left corner features the Fortinet Training Institute logo, and the bottom right corner shows the number 42.

If you are experiencing issues with a FortiGuard application control update, start troubleshooting the issue with the most basic steps:

- Make sure that FortiGate has a stable connection to the internet or FortiManager (if FortiGate is configured to receive updates from FortiManager)
- If the internet connection is stable, check DNS resolution on FortiGate
- If FortiGate is installed behind a network firewall, make sure that port443 is being allowed from FortiGate

You can check the FortiGuard website for the latest version of the application control database. If your locally installed database is out-of-date, try forcing FortiGate to check for the latest updates by running the `execute update-now` command.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which protocol does FortiGate use with FortiGuard to receive updates for application control?  
A. UDP  
 B. TCP
  
2. Which SSL/SSH inspection method is recommended for use with application control scanning to improve application detection?  
A. Certificate-based inspection profile  
 B. Deep-inspection profile

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

Now, you'll review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Understand application control
- ✓ Detect types of applications
- ✓ Understand FortiGuard application control services
- ✓ Use application control signatures
- ✓ Configure application control in profile mode
- ✓ Configure application control in NGFW policy mode
- ✓ Use the application control traffic shaping policy
- ✓ Enable application control logging events
- ✓ Monitor application control events
- ✓ Use the dashboard to see a detailed view of application control logs
- ✓ Recognize best practices for application control configuration
- ✓ Understand how to troubleshoot application control update issues



© Fortinet Inc. All Rights Reserved.

45

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use methods beyond simply blocking protocols, port numbers, or IP addresses, to monitor and control both standard and non-standard network applications.

**DO NOT REPRINT**

© FORTINET



## FortiGate Security

Antivirus



Last Modified: 13 June 2022

In this lesson, you will learn how to use FortiGate to protect your network against viruses.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



**Antivirus Basics**



**Antivirus Scanning Modes**



**Antivirus Configuration**



**Best Practices**



**Troubleshooting**

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

# DO NOT REPRINT

## © FORTINET

### Antivirus Basics

#### Objectives

- Review antivirus scanning techniques
- Enable FortiSandbox with antivirus
- Differentiate between available FortiGuard signature databases

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in antivirus basics, you will be able to understand and apply antivirus on FortiGate.

# DO NOT REPRINT

## © FORTINET

## Antivirus Scanning Techniques

- Antivirus scan:
  - Detects and eliminates malware in real time
    - Stops threats from spreading
  - Preserves the client reputation of your public IP
- Grayware scan:
  - Uses grayware signatures
  - Detects and blocks unsolicited programs
  - Antivirus actions apply
- Machine learning (AI) scan:
  - Enabled by default
  - Machine learning training model
    - Trained by FortiGuard Labs
  - Malware detection model
    - To detect Windows Portable Executables (PEs)
    - Mitigation process for zero-day attacks
    - Files detected by AI scan are identified with the W32/AI.Pallas.Suspicious signature.

Order of scan

1 Antivirus Scan

2 Grayware Scan

3 AI Scan

Like viruses, which use many methods to avoid detection, FortiGate uses many techniques to detect viruses. These detection techniques include:

- Antivirus scan: This is the first, fastest, simplest way to detect malware. It detects viruses that are an exact match for a signature in the antivirus database.
- Grayware scan: This scan detects unsolicited programs, known as grayware, that have been installed without the user's knowledge or consent. Grayware is not technically a virus. It is often bundled with innocuous software, but does have unwanted side effects, so it is categorized as malware. Often, grayware can be detected with a simple FortiGuard grayware signature.
- Machine learning (AI) scan: These scans are based on probability, so they increase the possibility of false positives, but they also detect zero-day attacks. Zero-day attacks are malwares that are new, unknown, and, therefore, have no existing associated signature. If your network is a frequent target, enabling an AI scan may be worth the performance cost because it can help you to detect a virus before the outbreak begins. Files detected by AI scan are identified with the W32/AI.Pallas.Suspicious signature.

If all antivirus features are enabled, FortiGate applies the following scanning order: antivirus scan, followed by grayware scan, followed by AI scan.

# DO NOT REPRINT

## © FORTINET

### Sandboxing

- FortiSandbox detects zero-day attacks with high certainty:
  - FortiGate uploads files to FortiSandbox Cloud or a FortiSandbox appliance
  - Two type of cloud sandboxing
    - FortiGate cloud: You must activate a FortiCloud account
    - FortiSandbox cloud: You will require an entitlement license embedded to FortiGate
  - Uploaded files are executed in an isolated environment (VMs)
  - FortiSandbox examines the effects of the software to detect new malware
- You can configure FortiGate to receive a signature database from FortiSandbox Cloud or a FortiSandbox appliance to supplement the FortiGuard database

**Security Fabric > Fabric Connectors**

FortiSandbox Settings

Status:  Enabled  Disabled

Server: 10.0.1.201

Notifier email: admin@acme.corp

**Security Fabric > Fabric Connectors**

Core Network Security

Cloud Sandbox

Cloud Sandbox Settings

Type:  FortiGate Cloud  FortiSandbox Cloud

Region: Global

You need to enable FortiSandbox cloud option on CLI under system global with the command on the CLI set gui-fortigate-cloud-sandbox enable

What if AI scans are too uncertain? What if you need a more sophisticated, more certain way to detect malware and find zero-day viruses?

You can integrate your antivirus scans with either FortiSandbox Cloud or a FortiSandbox appliance. Note you will need to enable cloud sandboxing on the CLI under system global settings for configuration options to appear on GUI. For environments that require more certainty, FortiSandbox executes the file within a protected environment (VMs), then examines the effects of the software to see if it is dangerous.

For example, let's say you have two files. Both alter the system registry and are, therefore, suspicious. One is a driver installation—its behavior is normal—but the second file installs a virus that connects to a botnet command and control server. Sandboxing would reveal the difference.

FortiGate can be configured to receive a supplementary signature database from FortiSandbox based on the sandboxed results.

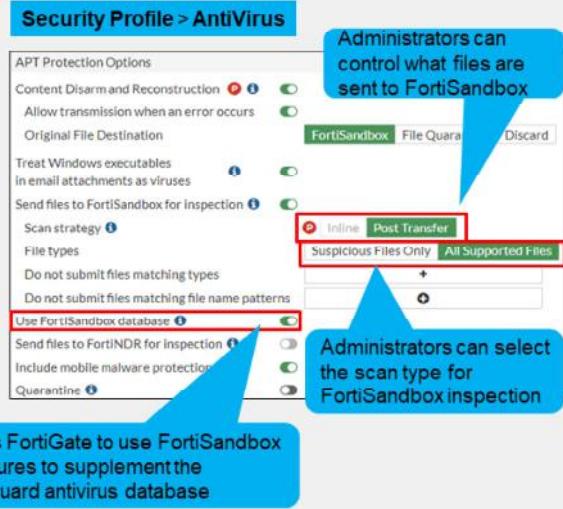
# DO NOT REPRINT

© FORTINET

## Sandboxing (Contd)

- Administrators must configure the antivirus profile to send files to FortiSandbox for inspection:
  - You can send all files, or only files deemed suspicious to FortiSandbox
  - Characteristics that are used to determine if a file is suspicious are updated by FortiGuard, based on the current threat climate
  - Inline scanning is supported only in proxy based inspection and requires a FortiSandbox appliance running version 4.2 or later
  - To enable inline scanning (CLI only)

```
config system fortisandbox
  set inline-scan {enable | disable}
end
```



FortiOS is smart when it comes to determining what files are sent to FortiSandbox. One feature FortiOS uses for this is content disarm and reconstruction (CDR), a proxy-based feature that you will learn more about in this lesson. When CDR processes files, the original documents can be saved to FortiSandbox.

FortiGuard provides FortiGate with information based on the current threat climate, that is used to determine if a file should be deemed suspicious or not. FortiGate provides the administrator with granular control when it comes to determining what type of files are sent to FortiSandbox for further investigation. Administrators also have the option to use the FortiSandbox database, in conjunction with the FortiGuard antivirus database, to enhance their network security.

FortiSandbox inline scanning is supported only in proxy inspection mode. You will need to enable inline scanning under system fortisandbox settings and then select **Inline** in the antivirus profile. When the setting is enabled, the client's file is held by FortiSandbox for inspection, and an appropriate configured action is applied once a verdict is returned. Inline scanning is not supported on FortiSandbox Cloud or FortiGate Cloud Sandbox.

**DO NOT REPRINT**  
**© FORTINET**

## Antivirus Signature Database

- Requires a subscription to FortiGuard AntiVirus

AntiVirus	Licensed (Expiration Date: 2023/01/20)
AV Definitions	Version 85.00712
AV Engine	Version 6.00258
Mobile Malware	Version 85.00712

- The antivirus scanning engine relies on the antivirus signature database
- The Mobile Malware subscription is part of the FortiGuard Antivirus license now
- Verify signatures versions on GUI or CLI commands

```
# diagnose autoupdate status
# diagnose autoupdate versions
```



© Fortinet Inc. All Rights Reserved.

7

Scheduled updates allow you to configure scheduled updates at regular intervals, such as hourly, daily, weekly, or automatically within every hour. You can also enable **AntiVirus PUP/PUA**, which allows antivirus grayware checks for potentially unwanted programs and applications.

Regardless of which method you select, you *must* enable virus scanning in at least one firewall policy. Otherwise, FortiGate will not download any updates. Alternatively, you can download packages from the Fortinet customer service and support website (requires subscription), and then manually upload them to your FortiGate. You can verify the update status and signature versions from the **FortiGuard** page on the GUI or using the CLI console.

**DO NOT REPRINT**  
**© FORTINET**

## Antivirus Signature Database (Contd)

- FortiGuard antivirus databases:
  - **Extended:** Includes common and additional recent non-active viruses
    - Available on all models
    - The default antivirus database setting
  - **Extreme:** Includes extended plus additional dormant viruses
    - Extreme is only available on select FortiGate models
- Choosing an antivirus signature database (CLI only)

```
config antivirus settings
    set use-extreme-db {enable | disable}
end
```



Multiple FortiGuard antivirus databases exist, which you can configure using CLI commands. Support for each database type varies by FortiGate model.

All FortiGate devices include the extended database. The extended database contains signatures for viruses that have been detected in recent months, as identified by the FortiGuard Global Security Research Team. The extended database also detects viruses that are no longer active.

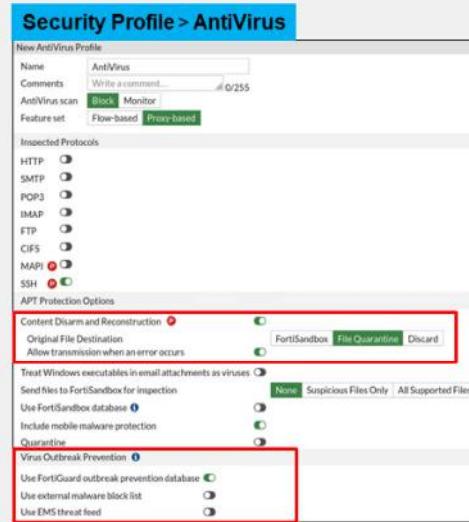
The extreme database is intended for use in high-security environments. The extreme database detects all known viruses, including viruses targeted at legacy operating systems that are no longer widely used. Most FortiGate models support the extreme database.

# DO NOT REPRINT

## © FORTINET

## FortiGuard Protection Services

- CDR
  - CDR removes exploitable content and replaces it with content that's known to be safe
- Virus outbreak prevention
  - Additional layer of protection that keeps your network safe from newly emerging malware
  - Quick virus outbreaks can infect a network before signatures can be developed to stop them
  - Outbreak protection stops these virus outbreaks until signatures become available in FortiGuard
- Malware block list
  - Manual external malware signatures to support antivirus database
  - The block list can be in the form of MD5, SHA1, and SHA256 hashes
  - Defined as a Security Fabric connector



**CDR:** The CDR removes exploitable content and replaces it with content that's known to be safe. As files are processed through an enabled antivirus profile, content that's found to be malicious or unsafe is replaced with content that allows the traffic to continue, but doesn't put the recipient at risk. Content that can be scanned includes PDF and Microsoft Office files leaving the network on CDR-supported protocols (such as HTTP, SMTP, IMAP, and POP3—MAPI isn't supported). When the client tries to download the file, FortiGate removes all exploitable content in real-time, and then sends the original file to FortiSandbox for inspection. The client can download the original file by logging in to FortiSandbox.

**Virus outbreak prevention:** This is an additional layer of protection that keeps your network safe from newly emerging malware. Quick virus outbreaks can infect a network before signatures can be developed to stop them. Outbreak protection stops these virus outbreaks until signatures become available in FortiGuard. FortiGate must have a zero-hour virus outbreak (ZHO) license. FortiGate adds hash-based virus detection for new threats that are not yet detected by the antivirus signatures. When the file is sent to the scanunit deamon, buffers are hashed and a request is sent to the urlfilter deamon. After checking against its request cache for known signatures, the urlfilter deamon sends an antivirus request to FortiGuard with the remaining signatures. FortiGuard returns a rating that is used to determine if the scanunit deamon should report the file as harmful or not. Jobs remain suspended in the scanunit deamon until the client receives a response, or the request times out.

**Malware block list:** FortiGate can enhance the antivirus database by linking a dynamic external malware block list to FortiGate. The list is hosted on a web server and is available through HTTP/HTTPS URL defined within the Security Fabric malware hash list. The hash list can be in the form of MD5, SHA1, and SHA256 hashes, and is written on separate lines on a plaintext file. The malware block list can be defined as a Security Fabric connector and configured to pull the list dynamically, by setting the refresh rate.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. If antivirus, grayware, and AI scans are enabled, in what order are they performed?  
 A. AI scan, followed by grayware scan, followed by antivirus scan  
 B. Antivirus scan, followed by grayware scan, followed by AI scan
  
2. Which databases can be manually selected for use in antivirus scanning?  
 A. Extended and Extreme  
 B. Quick, Normal, and Extreme

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand the basics of antivirus functionality.

Now, you will learn about antivirus scanning modes.

**DO NOT REPRINT**

**© FORTINET**

## Antivirus Scanning Modes

### Objectives

- Apply the antivirus profile in flow-based inspection mode
- Apply the antivirus profile proxy inspection mode
- Compare all available scanning modes

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in all antivirus scanning modes available in FortiOS, you will be able to use the antivirus profile in an effective manner.

# DO NOT REPRINT

## © FORTINET

### Flow-Based Inspection Mode

- Uses the extended antivirus database by default
  - Extreme database on certain FortiGate models—depending on the CLI settings
- Optimized performance compared to proxy-based scan
  - Proxy-based offers two scanning modes: default scanning and legacy scanning
  - Flow-based is designed to use a hybrid of proxy-based scanning modes
- FortiGate buffers the whole file, but transmits to the client simultaneously
  - When the *last* packet arrives, the AV engine starts the scan
    - Files bigger than buffer size are not scanned—can enable logging of these files
    - Packets are not delayed by scan—*except last packet*
  - Lower perceived latency—data loads faster
- If a virus is detected, the last packet is dropped and the connection is reset
- If an identical request is made, the block replacement page is inserted immediately

The screenshot shows the 'Edit AntiVirus Profile' dialog. The 'Name' field is set to 'default'. The 'Comments' field contains 'Scan files and block viruses.' with a character count of '29/255'. The 'AntiVirus scan' dropdown is set to 'Block Monitor', with 'Flow-based' selected (highlighted in red). The 'Feature set' dropdown also has 'Flow-based' selected. Under 'Inspected Protocols', all protocols are checked except CIFS. In the 'APT Protection Options' section, 'Treat Windows executables in email attachments as viruses' is checked. There are three tabs at the bottom: 'None' (selected), 'Suspicious Files Only', and 'All Supported Files'.

AV can operate in flow-based or proxy-based inspection mode, both of which use the full AV database (extended or extreme—depending on the CLI settings).

Flow-based inspection mode uses a hybrid of the scanning modes available in proxy-based inspection: the default scanning mode and the legacy scanning mode. The default mode enhances the scanning of nested archive files without buffering the container archive file. The legacy mode buffers the full container, and then scans it.

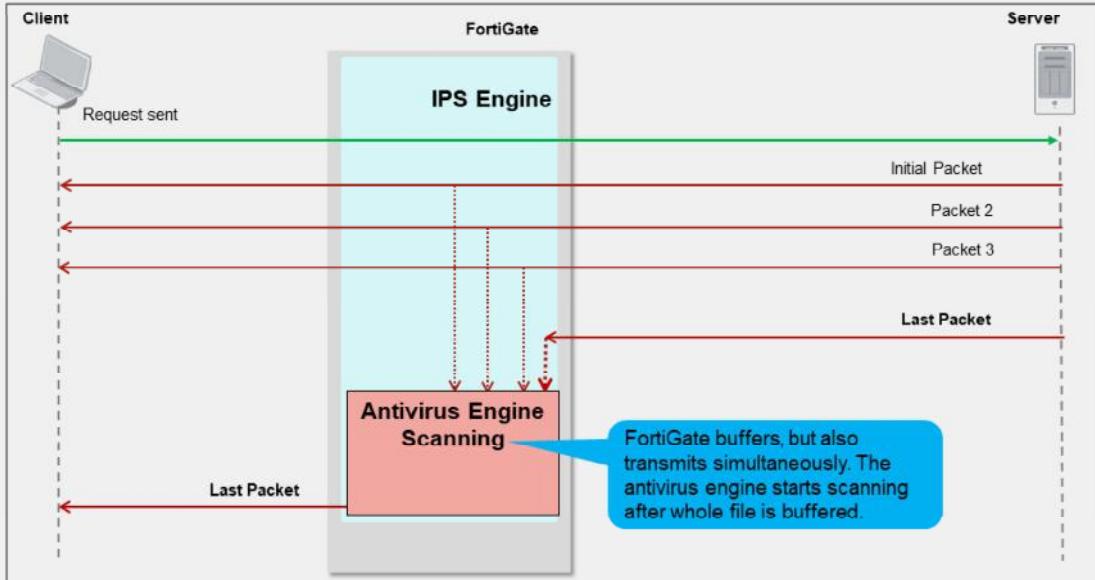
In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is transmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based. However, depending on the FortiGate model, some operations can be offloaded to SPUs to improve performance. When FortiGate receives the last packet of the file, it puts the packet on hold and sends a copy to the IPS engine. The IPS engine extracts the payload and assembles the whole file, and then sends the whole file to the AV engine for scanning.

Two possible scenarios can occur when a virus is detected:

- When a virus is detected on a TCP session where some packets have been already forwarded to the receiver, FortiGate resets the connection and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a second attempt to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
- If the virus is detected at the start of the connection, the IPS engine sends the block replacement message immediately.

DO NOT REPRINT  
© FORTINET

## Flow-Based Inspection Mode Packet Flow



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

14

As you can see on this slide, the client sends a request and starts receiving packets immediately, but FortiGate also caches those packets at the same time. When the last packet arrives, FortiGate caches it and puts it on hold. Then, the IPS engine extracts the payload of the last packet, assembles the whole file, and sends it to the antivirus engine for scanning. If the antivirus scan does not detect any viruses, and the result comes back clean, the last cached packet is regenerated and delivered to the client. However, if a virus is found, the last packet is dropped. Even if the client has received most of the file, the file will be truncated and the client will be not able to open a truncated file.

Regardless of which mode you use, the scan techniques give similar detection rates. How can you choose between the scan engines? If performance is your top priority, then flow inspection mode is more appropriate. If security is your priority, proxy inspection mode—with client comforting disabled—is more appropriate.

**DO NOT REPRINT****© FORTINET**

## Proxy Inspection Mode

- Uses extended or extreme antivirus database
- Buffers the whole file
  - Antivirus engine starts scanning after the end of the file is detected
    - Files bigger than buffer size are not scanned—can configure to pass or block
  - Packets sent to the client after scan finishes—*client must wait*
  - Highest perceived latency
- Provides granularity over performance
- Weighted towards being more thorough and easily configurable
- Displays a block message immediately if a virus is detected
- Stream-based scanning supports FTP, SFTP, and SCP
  - Optimizes memory utilization for large archive files by decompressing and scanning them on the fly
  - Viruses are detected even if they are in the middle or end of the large files



© Fortinet Inc. All Rights Reserved.

15

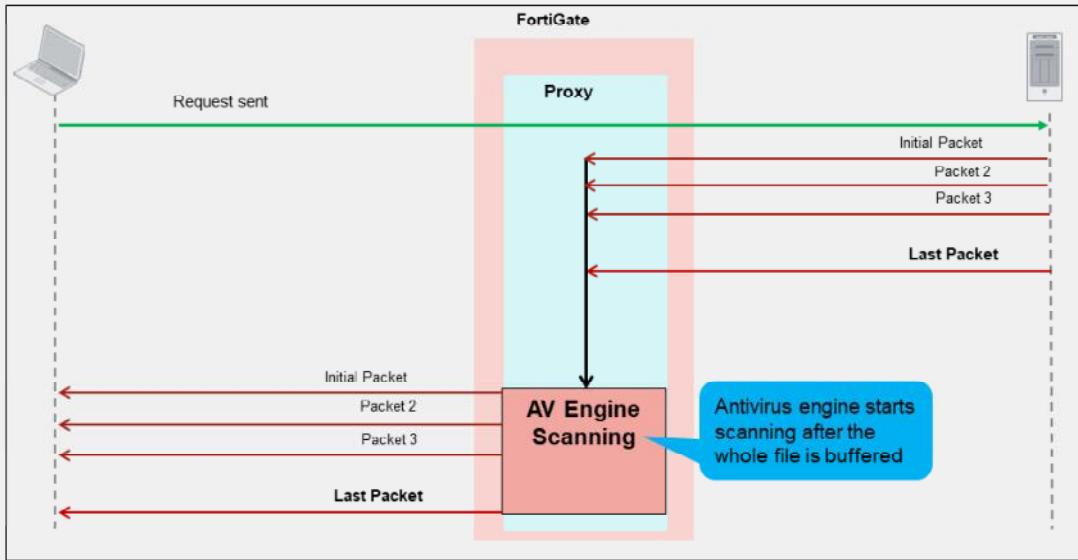
Each protocol's proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish. If a virus is detected, the block replacement page is displayed immediately. Because FortiGate has to buffer the whole file and then do the scanning, it takes a long time to scan. Also, from the client point of view, it has to wait for the scanning to finish and might terminate the connection due to lack of data.

You can configure client comforting for HTTP and FTP from the `config firewall profile-protocol-options` command tree. This allows the proxy to slowly transmit some data until it can complete the buffer and finish the scan. This prevents a connection or session timeout. No block replacement message appears in the first attempt, as FortiGate is transmitting the packets to the end client.

Using proxy inspection antivirus allow you to use the stream-based scanning, which is enabled by default. Stream-based scanning scans large archive files by decompressing the files and then scanning and extracting them at the same time. This process optimized memory utilization to conserve resources on FortiGate. Viruses are detected even if they are in the middle or towards the end of these large files.

DO NOT REPRINT  
© FORTINET

## Proxy Inspection Mode Packet Flow



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

16

With a proxy inspection mode scan, the client sends a request and FortiGate starts buffering the whole file, then sends it to the antivirus engine for scanning. If the file is clean (without any viruses), FortiGate starts transmitting the file to the end client. If a virus is found, no packets are delivered to the end client and the proxy sends the replacement block message to the end client.

# DO NOT REPRINT

## © FORTINET

### Proxy Inspection Mode Enabled

- Configure the antivirus profile
  - Feature set is Proxy-based**
- Provides additional antivirus support
  - MAPI and SSH protocols inspection
  - Content disarm and reconstruction (CDR)



- Proxy-based antivirus profiles
  - Only available if inspection mode is proxy-based
  - Can use flow-based antivirus profiles



Applying a proxy-based antivirus profile requires two sections in FortiGate configuration to use non-default settings:

1. Antivirus profile
2. Firewall policy

Antivirus profile provides the option to select a proxy-based approach as the inspection mode within the profile. This allows the profile to inspect MAPI and SSH protocols traffic, as well as to sanitize Microsoft documents and PDF files using the content disarm and reconstruction (CDR) feature.

If the inspection mode on the antivirus profile is set to **Proxy-based**, it is only available when the firewall policy inspection mode is set to **Proxy-based**.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What three additional features of an antivirus profile are available in proxy-based inspection mode?  
 A. MAPI, SSH, and CDR  
 B. Full and quick
  
2. What antivirus database is limited to specific FortiGate models?  
 A. Extended  
 B. Extreme

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus scanning modes.

Now, you will learn about antivirus configuration.

**DO NOT REPRINT**

**© FORTINET**

## Configuring Antivirus

### Objectives

- Configure antivirus profiles
- Configure protocol options
- Log and monitor antivirus events

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in antivirus configuration, including reviewing antivirus logs, you will be able to use the antivirus profile in an effective manner.

# DO NOT REPRINT

## © FORTINET

## Configuring Antivirus Profiles

Default inspection mode is flow. Inspection mode is now per policy.

FortiSandbox-related options are available only if FortiGate is configured to use FortiSandbox cloud or appliance under Security Fabric.

External malware block list can be enabled if an external threat feed security fabric is configured.

- Configure all required antivirus profile options

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

21

The antivirus profile can be configured on the **AntiVirus** page. Since the default inspection mode on a firewall policy is flow-based, **Feature set** is required to be set to **Flow-based**. If the inspection mode of the firewall policy is proxy-based, **Feature set** can be set to **Proxy-based**, which allows specific functions that are only available using proxy-based inspection mode firewall policy such as MAPI protocol and CDR.

Both feature sets provide the following options:

### APT Protection Options:

- Treat Windows executables in email attachment as viruses:** By default, this option is enabled and files (including compressed files) identified as Windows executables can be treated as viruses.
- Send files to FortiSandbox for inspection:** If FortiSandbox cloud or appliance is configured, you can configure the antivirus profile to send malicious files to FortiSandbox for behaviour analysis. If tagged as malicious, any future files matching the same behavior will be blocked if **Use FortiSandbox database** is enabled.

### Virus Outbreak Prevention:

- Use FortiGuard Virus outbreak prevention database:** FortiGuard virus outbreak prevention is an additional layer of protection that keeps your network safe from newly emerging malware. Quick virus outbreaks can infect a network before signatures can be developed to stop them. Outbreak protection stops these virus outbreaks until signatures become available on FortiGuard.
- Use external malware block List:** FortiGate can enhance the antivirus database by linking a dynamic external malware block list to FortiGate. Malware block list can be defined as a Security Fabric connector and configured to pull the list dynamically by setting the refresh rate.

In the antivirus profile, you can define what FortiGate should do if it detects an infected file. After you configure an antivirus profile, you must apply it in the firewall policy.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring Protocol Options

- More granular control
- Allows configuration of:
  - Protocol port mappings
  - Common options
  - Web and email options
- Configure for both proxy-based and flow-based firewall policies
  - From the GUI, on the **Protocol Options** page
  - From the CLI, using the `config firewall profile-protocol-options` command

```
config firewall profile-protocol-options
edit <profile_name>
config <protocol_name>
```

### Policy & Objects > Protocol Options

New Protocol Options			
Name	protocol_profile		
Comments	0/255		
Log Oversized Files	<input checked="" type="checkbox"/>	RPC over HTTP	<input checked="" type="checkbox"/>
Protocol Port Mapping			
HTTP	<input checked="" type="radio"/>	Any	Specify 80
SMTP	<input checked="" type="radio"/>	Any	Specify 25
POP3	<input checked="" type="radio"/>	Any	Specify 110
IMAP	<input checked="" type="radio"/>	Any	Specify 143
FTP	<input checked="" type="radio"/>	Any	Specify 21,22,23
NNTP	<input checked="" type="radio"/>	Any	Specify 119
MAPI	<input checked="" type="radio"/>	135	
DNS	<input checked="" type="radio"/>	53	
CIFS	<input checked="" type="radio"/>	445	
Common Options			
Comfort Clients	<input checked="" type="checkbox"/>	Block oversized file/email	<input checked="" type="checkbox"/>
Web Options			
Chunked Bypass	<input checked="" type="checkbox"/>	Email Options	
Allow Fragmented Messages	<input checked="" type="checkbox"/>	Append Signature (SMTP)	<input checked="" type="checkbox"/>

You can specify more than one port number (separated by comma)

Protocol options provide more granular control than antivirus profiles. You can configure protocol port mappings, common options, web options, and email options, to name a few.

You can configure protocol options on the **Protocol Options** page on the GUI or from the CLI. Protocol options are used by antivirus and other security profiles, such as web filtering, DNS filtering, and data loss prevention (DLP), to name a few.

Once protocol options are configured, they are applied in the firewall policy.

**DO NOT REPRINT****© FORTINET**

## Protocol Options—Large Files

- By default, FortiOS allows files that are too big for the buffer size
  - Files that are bigger than oversize limit are bypassed from scanning
- You can modify this behavior for all protocols

```
config firewall profile-protocol-options
edit <profile name>
config <protocol name>
set options oversize
set oversize-limit <integer>
end
end
```

- You can enable logging of oversize files using CLI

```
config firewall profile-protocol-options
edit <profile_name>
set oversize-log {enable|disable}
end
```



© Fortinet Inc. All Rights Reserved.

23

So what is the recommended buffer limit? It varies by model and configuration. You can adjust the oversize-limit for your network for optimal performance. A smaller buffer minimizes proxy latency (for both scanning modes) and RAM usage, but that may allow viruses to pass through undetected. When a buffer is too large, clients may notice transmission timeouts. You need to balance the two.

If you aren't sure about the value to set oversize-limit to, you can temporarily enable oversize-log to see if your FortiGate is scanning large files frequently. You can then adjust the value accordingly.

Files that are bigger than the oversize limit are bypassed from scanning. You can enable logging of oversize files by enabling the oversize-log option from the CLI.

**DO NOT REPRINT**

**© FORTINET**

## Protocol Options—Compressed Files

- Often, compression algorithms can be identified using header only
- Archives are unpacked and files and archives within are scanned separately
  - Nested archives are supported (default is 12 layers)
    - Supported formats: ZIP, TAR, GZIP, RAR, LSH, CAB, ARJ, MSC, BZIP, BZIP2, 7Z, EGG, XZ, CPIO, AR, ACE, ISO, DAA, CRX, and CHM
  - Decompressed files have a separate oversize limit
  - Limit can be configured for each protocol separately

```
config firewall profile-protocol-options
edit <profile_name>
config <protocol_name>
set uncompressed-oversize-limit [1-<model_limit>]
set uncompressed-nest-limit [1-<model_limit>]
end
end
```

HTTP, FTP, and so on

- Password-protected archives cannot be decompressed
- Increasing the size will increase memory usage!

Large files are often compressed. When compressed files go through scanning, the compression acts like encryption: the signatures won't match. So, FortiGate must decompress the file in order to scan it.

Before decompressing a file, FortiGate must first identify the compression algorithm. Some archive types can be correctly identified using only the header. Also, FortiGate must check whether the file is password protected. If the archive is protected with a password, FortiGate can't decompress it, and, therefore, can't scan it.

FortiGate decompresses files into RAM. Just like other large files, the RAM buffer has a maximum size. Increasing this limit may decrease performance, but it allows you to scan larger compressed files.

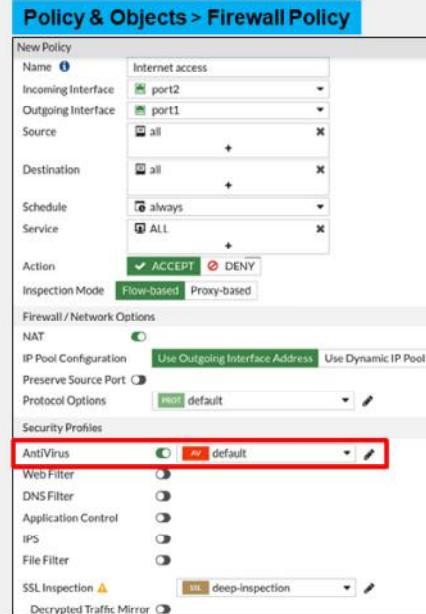
If an archive is nested—for example, if an attacker is trying to circumvent your scans by putting a ZIP file inside the ZIP file—FortiGate will try to undo all layers of compression. By default, FortiGate will attempt to decompress and scan up to 12 layers deep, but you can configure it to scan up to the maximum number supported by your device (usually 100). Often, you shouldn't increase this setting because it increases RAM usage.

# DO NOT REPRINT

## © FORTINET

### Applying the Antivirus Profile

- Apply the antivirus profile and protocol options on the firewall policy, to scan traffic
- Ensure that **deep-inspection** is selected for the **SSL/SSH Inspection** setting—required to scan encrypted protocols



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

25

Before FortiGate devices can start scanning traffic for malware, you need to apply the antivirus profile, the protocol options, and SSL/SSH inspection profiles on the firewall policy.

In full SSL inspection level, FortiGate terminates the SSL/TLS handshake at its own interface, before it reaches the server. When certificates and private keys are exchanged, it is with FortiGate and not the server. Next, FortiGate starts a second connection with the server.

Because traffic is unencrypted while passing between its interfaces, FortiGate can inspect the contents and look for matches with the antivirus signature database, before it re-encrypts the packet and forwards it.

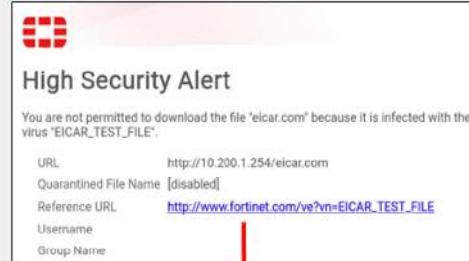
For these reasons, full SSL inspection level is the only choice that allows antivirus to be effective.

# DO NOT REPRINT

© FORTINET

## Antivirus Block Page

- Antivirus block page contains:
  - File name
  - Virus name
  - Website host and URL
  - Use name and group (if authentication is enabled)
  - Link to FortiGuard Encyclopedia



For antivirus scanning in proxy-based inspection mode (with client comforting disabled), the block replacement page is displayed *immediately* when a virus is detected.

For flow-based inspection mode scanning, if a virus is detected at the start of the stream, the block replacement page is displayed at the *first attempt*. If a virus is detected after a few packets have been transmitted, the block replacement page is *not* displayed. However, FortiGate caches the URL and can display the replacement page immediately, on the second attempt.

Note that if deep inspection is enabled, all HTTPS-based applications also display the block replacement message.

The block page includes the following:

- File name
- Virus name
- Website host and URL
- User name and group (if authentication is enabled)
- Link to FortiGuard Encyclopedia—which provides analysis, recommended actions (if any), and detection availability

You can go directly to the FortiGuard website to view information about other malware, and scan, submit, or do both, with a sample of a suspected malware.

# DO NOT REPRINT

## © FORTINET

## Antivirus Logs

The screenshot shows the FortiGate Log & Report interface. On the left, the 'Log & Report > Security Events' page is displayed, showing a table of security events. One event is highlighted with a red box and an arrow pointing to it, labeled 'AntiVirus'. On the right, a detailed log entry for this event is shown in a modal window titled 'Log Details'. The log details include:

- General:** Absolute Date/Time: 2022/04/13 19:28:24, Time: 19:28:24, Session ID: 1702, Virtual Domain: root, Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:93.0) Gecko/20100101 Firefox/93.0
- Source:** IP: 10.0.1.10, Source Port: 56320, Country/Region: Reserved, Source Interface: port3, Source UUID: 703e6f6-791a-51e7-daa0-9859ce6c1d02, User:
- Destination:** IP: 10.200.1.254, Port: 80, Country/Region: Reserved, Destination Interface: port1, Destination UUID: 7bc87d34-7916-51e7-3d5b-71812a61b98e, URL: http://10.200.1.254/elcar.com
- Data:** File Name: elcar.com, Message: File is Infected.

The 'Log & Report > Forward Traffic' page is also visible on the left, showing a list of network traffic entries. One specific entry is highlighted with a red box and an arrow pointing to it, showing a 'Deny UTM Blocked' action.

**Fortinet Training Institute**

© Fortinet Inc. All Rights Reserved.

If you enable logging, you can find details on the **AntiVirus** log page under **Security Events**.

When the antivirus scan detects a virus, by default, it creates a log about what virus was detected, as well as the action, policy ID, antivirus profile name, and detection type. It also provides a link to more information on the FortiGuard website.

You can also view log details on the **Forward Traffic** log page, where firewall policies record traffic activity. You'll also find a summary of the traffic on which FortiGate applied an antivirus action.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What is the default scanning behavior for files over 10 MB?

- A. Allow the file without scanning
- B. Block all large files that exceed the buffer threshold



© Fortinet Inc. All Rights Reserved.

28

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



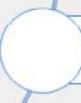
Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus configuration.

Now, you will learn about some antivirus best practices.

# DO NOT REPRINT

## © FORTINET

### Best Practices

#### Objectives

- Recognize recommended antivirus configuration practices
- Log antivirus events
- Monitor antivirus and FortiSandbox events
- Use hardware acceleration with antivirus scans

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in antivirus best practices, you will be able to configure an effective antivirus solution.

**DO NOT REPRINT****© FORTINET**

## Recommended Configuration Practices

- Perform antivirus scan on all internet traffic
  - If using load balancing or redundant internet connections, ensure all internal to external firewall policies have antivirus profiles applied on them
- Use *deep-inspection* instead of *certificate-based* inspection, to ensure that full content inspection is performed
- Use FortiSandbox Cloud or a FortiSandbox device to enable sandboxing support
  - Configure the antivirus profile to use the FortiSandbox database
- Do not increase the maximum file size to be scanned, unless it is required
  - Viruses usually travel in small files
  - More scanning means more memory utilization



© Fortinet Inc. All Rights Reserved.

31

The following are some best practices to follow when configuring antivirus scanning for use on FortiOS:

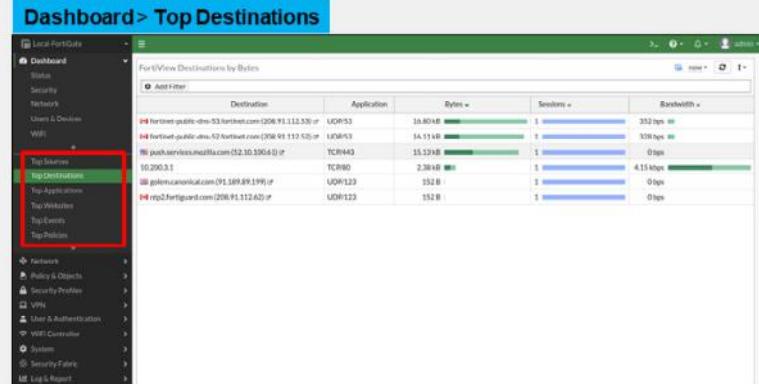
- Enable antivirus scanning on all internet traffic. This includes internal to external firewall policies, and any VIP firewall policies.
- Use *deep-inspection* instead of *certificate-based* inspection, to ensure that full content inspection is performed.
- Use FortiSandbox for protection against new viruses.
- Do not increase the maximum file size to be scanned, unless there is good reason, or you need to do so in order to meet a network requirement.

# DO NOT REPRINT

© FORTINET

## Log Antivirus Events

- Enable logging of oversized files
  - This will ensure that files that are not scanned are *logged*
- Ensure that firewall policies with antivirus applied have security events logging enabled
- Use standalone dashboard to monitor threats to your network
  - Dashboard organizes threats based on network segments on the device



Logging is an important part of managing a secure network. Enable logging for oversized files so that if there are files that are not scanned, you can be aware of it. Also, ensure that security events logging is enabled on all firewall policies using security profiles. Use the standalone dashboards to view relevant information regarding threats to your network. The standalone dashboard organizes information into network segments and breaks it down into various categories.

**DO NOT REPRINT****© FORTINET**

## Hardware Acceleration for Antivirus Scanning

- Accelerates flow-based antivirus only
- FortiGate models that feature NTurbo (NP6 or NP7) can accelerate antivirus processing to enhance performance
  - SoC4 models also support NTurbo
- Creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface

```
config ips global  
    set np-accel-mode {none | basic}  
end
```

Enable NTurbo acceleration

- Proxy inspection mode
  - Proxy-based inspection cannot be offloaded for acceleration



© Fortinet Inc. All Rights Reserved.

33

The FortiGate main CPU is responsible for performing UTM/NGFW inspection on the network traffic. FortiGate models that have specialized chips can offload inspection tasks to enhance performance while providing the same level of protection. FortiGate devices that support the NTurbo feature can offload UTM/NGFW sessions to network processors. NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface. This can improve performance by accelerating antivirus inspection, without sacrificing security.

**DO NOT REPRINT****© FORTINET**

## Hardware Acceleration for Antivirus Scanning (Contd)

- FortiGate models with content processors (CP8 or CP9) support offloading of flow-based pattern matching
- Flow-based pattern databases are compiled and downloaded to the content processors from the IPS engine and IPS database
  - Accelerates pattern matching while reducing the load on FortiGate CPU

```
config ips global
    set cp-accel-mode {none | basic | advanced}
end
```



Enable AV scan offloading to CP

- Proxy inspection mode
  - Proxy-based antivirus scanning cannot be offloaded for acceleration

FortiGate models that have CP8 or CP9 content processors can offload flow-based pattern matching to CP8 or CP9 processors. When CP acceleration is enabled, flow-based pattern databases are compiled and downloaded to the content processors from the IPS engine and IPS database. This reduces load on the FortiGate CPU because flow-based pattern matching requests are redirected to the CP hardware. Before flow-based inspection is applied to the traffic, the IPS engine uses a series of decoders to determine the appropriate security modules that can be used, depending on the protocol of the packet and policy settings. In addition, if SSL inspection is configured, the IPS engine also decrypts SSL packets. SSL decryption is also offloaded and accelerated by CP8 or CP9 processors.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which type of inspection mode can be offloaded using NTurbo hardware acceleration?
  - A. Proxy-based
  - B. Flow-based
  
2. What does the logging of oversized files option do?
  - A. Enables logging of all files that cannot be scanned because of oversize limit
  - B. Logs all files that are over 5 MB

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus best practices.

Now, you will learn about antivirus troubleshooting.

**DO NOT REPRINT**

**© FORTINET**

## Troubleshooting

### Objectives

- Troubleshoot common antivirus issues

After completing this section, you should be able to troubleshoot common issues with antivirus.

By demonstrating competence in troubleshooting common antivirus issues, you will be able to configure and maintain an effective antivirus solution.

# DO NOT REPRINT

## © FORTINET

## Troubleshooting Common Antivirus Issues

- FortiGuard update issues? Make sure that:
  - FortiGate has a stable connection to the internet
  - FortiGate is able to resolve DNS (`update.fortiguard.net`)
  - TCP port 443 is open
- Force FortiGate to check for new antivirus updates

```
# execute update-av
```
- Verify that the FortiGuard antivirus license is valid

The screenshot shows the 'System > FortiGuard' interface. On the left, there's a sidebar with options: AntiVirus, AV Definitions, AV Engine, and Mobile Malware. The main area displays the status of the 'AntiVirus' module. It shows a green checkmark icon followed by the text 'Licensed (Expiration Date: 2023/01/20)'. Below this, there are three radio buttons: 'Version 85.00732' (selected), 'Version 6.00258', and 'Version 85.00732'. To the right of the main area is a button labeled 'Upgrade Database'.

If you are having issues with the antivirus license or FortiGuard updates, start troubleshooting with basic connectivity tests. Most of the time, issues related to updates are caused by connectivity problems with FortiGuard servers. You can perform the following to handle common antivirus issues:

- Make sure that FortiGate has a stable internet connection and can resolve DNS (`update.fortinet.net`).
- If there is another firewall between FortiGate and the internet, make sure TCP port 443 is open and traffic is allowed from and to the FortiGate device.
- Force FortiGate to check for new virus updates using the CLI command: `execute update-av`.
- Verify that the FortiGate device is registered and has a valid antivirus service contract.

**DO NOT REPRINT****© FORTINET**

## Troubleshooting Common Antivirus Issues (Contd)

- Valid contract but antivirus database is out-of-date?
  - Check FortiGuard website for latest antivirus database version
    - <https://fortiguard.com/updates/antivirus>
  - Make sure the antivirus profile is applied on at least one firewall policy
- Run the real-time update debug to isolate update-related issues

```
# diagnose debug application update -1  
# diagnose debug enable  
# execute update-av
```



© Fortinet Inc. All Rights Reserved.

39

What if FortiGate shows a valid license but the antivirus database is out-of-date?

Check the current database version installed on your FortiGate and compare the version number with the current release on the FortiGuard website. FortiGate may not update the antivirus database if it is not being used (applied on a firewall policy). Make sure the antivirus profile is applied on at least one firewall policy. If you continue to see issues with the update, run the real-time debug command to identify the problem.

**DO NOT REPRINT**  
**© FORTINET**

## Troubleshooting Common Antivirus Issues (Contd)

- Unable to catch viruses even with a valid contract?
  - Check all internal to external firewall policies for configuration errors
  - Ensure that the proper antivirus profile, along with the correct protocol options and SSL/SSH inspection profiles are applied
  - Make sure the same antivirus profile and SSH/SSL inspection are applied on all redundant internet connection firewall policies
  - Check the **Advanced Threat Protection Statistics** widget for virus statistics
- Some useful antivirus commands are:

```
# get system performance status          Displays virus statistics for the last one minute
# diagnose antivirus database-info       Displays current antivirus database information
# diagnose autoupdate versions          Displays current antivirus engine and signature versions
# diagnose antivirus test "get scantime" Displays scan times for infected files
# execute update-av                      Forces FortiGate to check for antivirus updates from FortiGuard server
```

What if you have a valid contract and updated database, and you are still having issues catching viruses? Start troubleshooting for basic configuration errors. Most of the time, issues are caused by misconfiguration on the device. You can verify them as following:

- Make sure that the correct antivirus profile is applied on the right firewall policy.
- Make sure that you are using the same antivirus profile and SSL/SSH inspection on all internet connection firewall policies.
- Add and use advanced the threat protection statistics widget to get the latest virus statistics from the unit.

These are some of the commands that can be used to retrieve information and troubleshoot antivirus issues:

- `get system performance status`: Displays statistics for the last one minute.
- `diagnose antivirus database-info`: Displays current antivirus database information.
- `diagnose autoupdate versions`: Displays current antivirus engine and signature versions.
- `diagnose antivirus test "get scantime"`: Displays scan times for infected files.
- `execute update-av`: Forces FortiGate to check for antivirus updates from the FortiGuard server.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What command do you use to force FortiGate to check for new antivirus updates?  
A. execute update antivirus  
 B. execute update-av



© Fortinet Inc. All Rights Reserved.

41

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Review antivirus scanning techniques
- ✓ Enable FortiSandbox with antivirus
- ✓ Differentiate between available FortiGuard signature databases
- ✓ Apply the antivirus profile in flow-based and proxy-based inspection modes
- ✓ Compare all available scanning modes
- ✓ Configure antivirus profiles and protocol options
- ✓ Log and monitor antivirus events
- ✓ Recognize recommended antivirus configuration practices
- ✓ Log and monitor antivirus and FortiSandbox events
- ✓ Use hardware acceleration with antivirus scans
- ✓ Troubleshoot common antivirus issues



© Fortinet Inc. All Rights Reserved.

43

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiGate features and functions to protect your network against viruses.

**DO NOT REPRINT**

© FORTINET



## FortiGate Security

### Intrusion Prevention and Denial of Service



In this lesson, you will learn how to use FortiGate to protect your network against intrusions and denial of service (DoS) attacks.

Last Modified: 13 June 2022

**DO NOT REPRINT**

© FORTINET

## Lesson Overview



**Intrusion Prevention System**



**Denial of Service**



**Best Practices**



**Troubleshooting**

In this lesson, you will learn about the topics shown on this slide.

**DO NOT REPRINT****© FORTINET**

## Intrusion Prevention System

### Objectives

- Differentiate between exploits and anomalies
- Identify the different components of an IPS package
- Manage FortiGuard IPS updates
- Select an appropriate IPS signature database
- Configure an IPS sensor
- Identify the IPS sensor inspection sequence
- Apply IPS to network traffic

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in intrusion prevention systems (IPS), you should be able to implement an effective IPS solution to protect your network from intrusion.

**DO NOT REPRINT****© FORTINET**

## Exploits and Anomalies

### Anomaly

- Can be zero-day or DoS attacks
- Detected by behavioral analysis:
  - Rate-based IPS signatures
  - DoS policies
  - Protocol constraints inspection
- Example:
  - Abnormally high rate of traffic (DoS/flood)

### Exploit

- A known, confirmed attack
- Detected when a file or traffic matches a signature pattern:
  - IPS signatures
  - WAF signatures
  - Antivirus signatures
- Example:
  - Exploit of known application vulnerabilities



© Fortinet Inc. All Rights Reserved.

4

It's important to understand the difference between an anomaly and an exploit. It's also important to know which FortiGate features offer protection against each of these types of threats.

*Exploits* are known attacks, with known patterns that can be matched by IPS, web application firewall (WAF), or antivirus signatures.

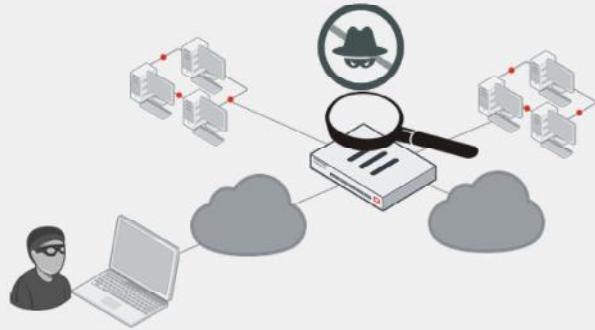
*Anomalies* are unusual behaviors in the network, such as higher-than-usual CPU usage or network traffic. Anomalies must be detected and monitored (and, in some cases, blocked or mitigated) because they can be the symptoms of a new, never-seen-before attack. Anomalies are usually better detected by behavioral analysis, such as rate-based IPS signatures, DoS policies, and protocol constraints inspection.

# DO NOT REPRINT

## © FORTINET

### IPS

- Flow-based detection and blocking
  - Known exploits that match signatures
  - Network errors and protocol anomalies
- IPS components
  - IPS signature databases
  - Protocol decoders
  - IPS engine
    - Application control
    - Antivirus (flow-based)
    - Web filter (flow-based)
    - Email filter (flow-based)



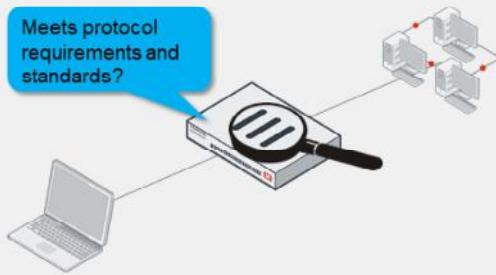
IPS on FortiGate uses signature databases to detect known attacks. Protocol decoders can also detect network errors and protocol anomalies.

The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering.

**DO NOT REPRINT**  
© FORTINET

## What Are Protocol Decoders?

- Decoders parse protocols
- IPS signatures find parts of a protocol that don't conform
  - For example, too many HTTP headers, or a buffer overflow attempt
- Unlike proxy-based scans, IPS often does not require IANA standard ports
  - Automatically selects decoder for protocol at each OSI layer



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

How does the IPS engine determine if a packet contains an attack or anomaly?

Protocol decoders parse each packet according to the protocol specifications. Some protocol decoders require a port number specification (configured on the CLI), but usually, the protocol is automatically detected. If the traffic doesn't conform to the specification—if, for example, it sends malformed or invalid commands to your servers—then the protocol decoder detects the error.

**DO NOT REPRINT****© FORTINET**

## FortiGuard IPS Updates

- IPS packages are updated by FortiGuard
  - IPS signature databases
  - Protocol decoders
  - IPS engine
- Regular updates are required to ensure IPS remains effective
- The default update setting is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions
- The botnet signature subscription is part of a FortiGuard IPS license

**System > FortiGuard**

Entitlement	Status
FortiCare Support	Registered
Virtual Machine	Valid
Firmware & General Updates	Licensed (Expiration Date: 2023/01/18)
Intrusion Prevention	Licensed (Expiration Date: 2023/01/18)
IPS Definitions	Version 18.00052
IPS Engine	Version 7.00018
Malicious URLs	Version 2.00970
Botnet IPs	Version 7.01436
Botnet Domains	Version 2.00721

**System > FortiGuard**

Scheduled updates:  Every  Daily  Weekly  Automatic

Improve IPS quality:

Use extended IPS signature package:

AntiVirus PUP/PUA:

Update server location:

Lowest latency locations:  Restrict to:  US only  EU only

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

7

By default, an initial set of IPS signatures is included in each FortiGate firmware release. FortiGuard updates the IPS signature database with new signatures. That way, IPS remains effective against new exploits. Unless a protocol specification or RFC changes (which doesn't happen very often), protocol decoders are rarely updated. The IPS engine itself changes more frequently, but still not often.

The FortiGuard IPS service updates the IPS signatures most often. The FortiGuard research team identifies and builds new signatures, just like antivirus signatures. So, if your FortiGuard Services contract expires, you can still use IPS. However, just like antivirus scans, IPS scans become increasingly ineffective the longer the signatures are not updated—old signatures won't defend against new attacks.

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. Starting in FortiOS 7.0, the frequency is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions. The update interval is within one hour.

For example, an FG-501E has 78% valid contracts. Based on this device model, FortiOS calculates the update schedule to be every 10 minutes. You can verify the system event logs, which are generated approximately every 10 minutes.

IPS is a FortiGuard subscription, and includes a botnet signature database. The botnet IP database is part of the ISDB updates. The botnet domains database is part of the AV updates, and only the botnet signatures require the FortiGuard IPS license subscription.

**DO NOT REPRINT**  
© FORTINET

## Choosing the Signature Database

- Regular
  - Common attacks with fast, certain identification (default action is block)
- Extended
  - Performance intensive



The IPS signature database is divided into the regular and extended databases. The regular signature database contains signatures for common attacks whose signatures cause rare or no false positives. It's a smaller database, and its default action is to block the detected attack.

The extended signature database contains additional signatures for attacks that cause a significant performance impact, or don't support blocking because of their nature. In fact, because of its size, the extended database is not available for FortiGate models with a smaller disk or RAM. But, for high-security networks, you might be required to enable the extended signatures database.

**DO NOT REPRINT**  
**© FORTINET**

## List of IPS Signatures

**Security Profiles > Intrusion Prevention**

**Edit IPS Sensor**

Name: default  
Comments: Prevent critical attacks. 25/255  
Block malicious URLs:

**IPS Signatures and Filters**

+ Create New | Edit | Delete | Details | Exempt IPs | Action | Packet Logging  
Details:  Default  Disabled

**Botnet C&C**

Scan Outgoing Connections to Botnet Sites | Disable | Block | Monitor

**IPS Signatures**

FortiGate Local-FortiGate

IPS Signatures: View IPS Signatures

Additional Information

**Default action**

**Active signature database**

**IPS Signatures**

13995 Total | Severity: High (Orange), Critical (Red), Medium (Yellow), Low (Blue), Information (Green)

17733 Total | Target: Server (Green), Client (Orange)

23023 Total | OS: Windows (Green), Linux (Orange), MacOS (Purple), All (Red), BSD (Blue), Solaris (Pink)

**IPS Signature (13,995)**

Name	Severity	Target	OS	Action	CVE-ID
2Wire.Wireless.Router.XSRF.Password.Reset	Medium (Yellow)	Server Client	Linux	<input checked="" type="radio"/> Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.File...	High (Orange)	Server	Windows	<input checked="" type="radio"/> Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	High (Orange)	Server	Windows	<input checked="" type="radio"/> Block	CVE-2005-0277

© Fortinet Inc. All Rights Reserved.

9

After FortiGate downloads a FortiGuard IPS package, new signatures appear in the signature list. When configuring FortiGate, you can change the **Action** setting for each sensor that uses a signature.

The default action setting is often correct, except in the following cases:

- Your software vendor releases a security patch. Continuing to scan for exploits wastes FortiGate resources.
- Your network has a custom application with traffic that inadvertently triggers an IPS signature. You can disable the setting until you notify Fortinet so that the FortiGuard team can modify the signature to avoid false positives.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring IPS Sensors

- Add individual signatures
- Add groups of signatures using filters

The screenshot displays two windows from the FortiGate management interface. On the left, the 'New IPS Sensor' configuration page shows fields for Name (IPS profile), Comments (Write a comment...), and Block malicious URLs (checkbox). Below these are tabs for Details, Exempt IPs, Action, and Packet Logging, all currently showing 'No results'. A red arrow points from the 'Create New' button in the Details tab to the 'Signature' filter window on the right. On the right, the 'Add Signatures' window shows a list of signatures with various status and action settings. Another red arrow points from the 'Signature' button in this window to the detailed signature list window below it. This detailed list shows multiple entries with columns for Name, Severity, Target, OS, Action, and CVE-ID.

Name	Severity	Target	OS	Action	CVE-ID
74CMS.Config.Controller.Remote.Code.Execu...	■■■■■	Server	Windows	Block	CVE-2019-10684
2Wire.Wireless.Router.XSRF.Password.Reset	■■■■■	Client	Linux	Block	CVE-2007-4387
3CX.Phones.System.VAD.Deploy.Arbitrary.FI...	■■■■■	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Buffer.Overflow...	■■■■■	Server	Windows	Block	CVE-2005-0278
3Com.3CDaemon.FTPServer.Information.D...	■■■■■	Client	Windows	Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Infor...	■■■■■	Server	Windows	Block	CVE-2005-0278

There are two ways to add predefined signatures to an IPS sensor. One way is to select the signatures individually. After you select a signature in the list, the signature is added to the sensor with its default action. Then, you can right-click the signature and change the action.

The second way to add a signature to a sensor is using filters. FortiGate adds all the signatures that match the filters.

The purpose of the IPS feature is to protect the inside of the network from outside threats.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring IPS Sensors (Contd)

- Add rate-based signatures to block traffic when the threshold is exceeded during a time period
  - Track the traffic based on source or destination IP address

Security Profiles > Intrusion Prevention

Add Signatures

Type	Filter: Signature
Action	<input checked="" type="radio"/> Default
Packet logging	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Status	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input checked="" type="radio"/> Default
Rate-based settings	Default <input type="radio"/> Specify
Threshold	0
Duration (seconds)	60
Track By	<input checked="" type="radio"/> Any <input type="radio"/> Source IP <input type="radio"/> Destination IP
Exempt IPs	0   Edit IP Exemptions

These parameters are applicable to the signatures selected at the bottom

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 13.995					
2Wire.Wireless.Router.XSRF.Password.Reset	Low	Server Client	Linux	<input checked="" type="radio"/> Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.Fi...	Medium	Server	Windows	<input checked="" type="radio"/> Block	
3Com.3CDaemon.FTPServer.Buffer.Overflow...	Medium	Server	Windows	<input checked="" type="radio"/> Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Information.D...	Low	Client	Windows	<input checked="" type="radio"/> Block	CVE-2005-0278

© Fortinet Inc. All Rights Reserved.

11

You can also add rate-based signatures to block specific traffic when the threshold is exceeded during the configured time period. You should apply rate-based signatures only to protocols you actually use. Then, configure **Duration** to block malicious clients for extended periods. This saves system resources and can discourage a repeat attack. FortiGate does not track statistics for that client while it is temporarily blocklisted.

**DO NOT REPRINT**  
**© FORTINET**

## IPS Sensor Inspection Sequence

The screenshot shows the 'Security Profiles > Intrusion Prevention' section of the FortiGate management interface. A new IPS sensor named 'Server IPS Profile' is being configured. The 'Block malicious URLs' option is selected. The 'IPS Signatures and Filters' table lists a single rule:

Details	Exempt IPs	Action	Packet Logging
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow TGT Server SEV <span style="color: orange;">     </span> SEV <span style="color: red;">     </span> OS Windows	0	Monitor <input checked="" type="radio"/>	Disabled <input checked="" type="radio"/>

A blue callout bubble points to the 'Create New' button with the text 'New entries will be placed at the bottom of the list'. Another blue callout bubble points to the table with the text 'IPS signatures and filters are processed in sequence'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

When the IPS engine compares traffic with the signatures in each filter, order matters. The rules are similar to firewall policy matching; the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters.

So, position the most likely matching filters, or signatures, at the top of the list. Avoid making too many filters, because this increases evaluations and CPU usage. Also, avoid making very large signature groups in each filter, which increase RAM usage.

In the event of a false-positive outbreak, you can add the triggered signature as an individual signature and set the action to **Monitor**. This allows you to monitor the signature events using IPS logs, while investigating the false-positive issue.

DO NOT REPRINT  
© FORTINET

## Configuring IP Exemptions

- Exempt specific source or destination IP addresses from specific signatures
- Only configurable under individual IPS signatures

The screenshot shows two windows from the FortiGate management interface:

- IPS Signatures and Filters** window:
  - Header: Security Profiles > Intrusion Prevention
  - Table:

Details	Exempt IPs	Action	Packet Logging
3Com.3CDaemon.FTP.Server.Information.Disclosure	1	Monitor	Disabled
TGT Server		Default	Disabled
SEV			
SEV			
OS Windows			
  - Buttons: +Create New, Edit, Delete.
- Edit IP Exemptions** window:
  - Header: Edit IP Exemptions
  - Table:

Source IP/Netmask	Destination IP/Netmask
10.0.1.10/32	0.0.0.0/0
  - Buttons: +Create New, Delete.

A red arrow points from the number '1' in the 'Exempt IPs' column of the first table to the 'Source IP/Netmask' field in the second table, indicating the relationship between the exemption count and the configuration details.

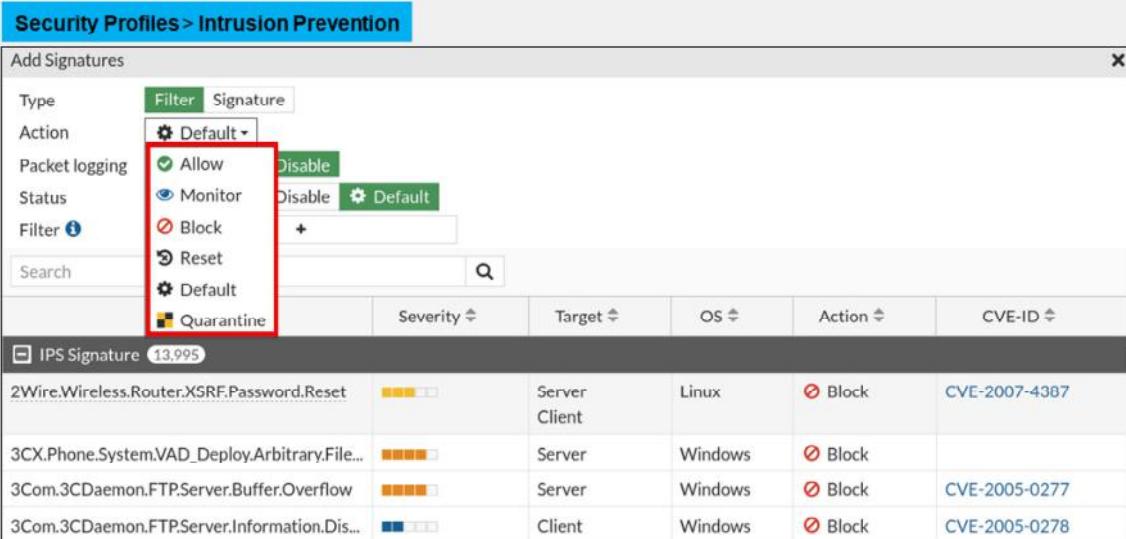
Sometimes it is necessary to exempt specific source or destination IP addresses from specific signatures. This feature is useful during false-positive outbreaks. You can temporarily bypass affected endpoints until you investigate and correct the false-positive issue.

You can configure IP exemptions on individual signatures only. Each signature can have multiple exemptions.

**DO NOT REPRINT**  
**© FORTINET**

## IPS Actions

- Choose what action to take when a signature is triggered



The screenshot shows the FortiGate management interface for managing security profiles. The main window title is "Security Profiles > Intrusion Prevention". A sub-dialog titled "Add Signatures" is open. On the left of this dialog, there is a sidebar with fields for "Type" (set to "Signature"), "Action" (with a dropdown menu highlighted by a red box containing "Allow", "Monitor", "Block", "Reset", "Default", and "Quarantine"), "Packet logging" (checkbox checked), "Status" (checkbox checked), and "Filter" (checkbox checked). Below the sidebar is a search bar and a "Q" icon. The main area lists "IPS Signature" entries with a count of 13,995. The first four entries are shown in detail:

Signature	Severity	Target	OS	Action	CVE-ID
2Wire.Wireless.Router.XSRF.Password.Reset	Medium	Server Client	Linux	Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.File...	Medium	Server	Windows	Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	Medium	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Dis...	Low	Client	Windows	Block	CVE-2005-0278

At the bottom of the dialog, there is a footer with the Fortinet logo, "Training Institute", "© Fortinet Inc. All Rights Reserved.", and a page number "14".

When you create a new entry to add signatures or filters, you can select the action by clicking **Action**.

Select **Allow** to allow traffic to continue to its destination. Select **Monitor** to allow traffic to continue to its destination and log the activity. Select **Block** to silently drop traffic matching any of the signatures included in the entry. Select **Reset** to generate a TCP RST packet whenever the signature is triggered. Select **Default** to use the default action of the signatures.

**Quarantine** allows you to quarantine the attacker's IP address for a set duration. You can set the quarantine duration to any number of days, hours, or minutes.

If you enable **Packet logging**, FortiGate saves a copy of the packet that matches the signature.

**DO NOT REPRINT**  
**© FORTINET**

## IPS Signature Filter Options—CVE Pattern

- IPS signature filter options include CVE pattern
  - Allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard
  - For example, to configure CVE patterns for CVE-2010-0177
- For example, the CVE of the IPS signature Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution is CVE-2010-0177
- This matches the CVE filter in the IPS sensor, so traffic is blocked and logged

```
# config ips sensor
  edit "cve"
    set comment "cve"
    config entries
      edit 1
        set cve "cve-2010-0177"
        set status enable
        set log-packet enable
        set action block
      next
    end
  next
end
```

date=2022-04-13 time=15:44:56 logid="0419016384"
type="utm" subtype="ips" eventtype="signature"
level="alert" vd="vd1" eventtime=1594593896666145871
tz="-0700" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=172.16.200.55
srcintf="port2" srcintfrole="undefined"
dstintf="port1" dstintfrole="undefined"
sessionid=1638 action="dropped" proto=6
service="HTTPS" policyid=1
attack="Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution" srcport=58298 dstport=443
hostname="172.16.200.55" url="/Mozilla"
direction="incoming" attackid=20853 profile="sensor-1" ref="http://www.fortinet.com/ids/VID20853"
incidentserialno=124780667 msg="web client:
Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution
," crscore=50 craction=4096 crlevel="critical"



© Fortinet Inc. All Rights Reserved.

15

IPS signature filter options include the CVE pattern. The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

**DO NOT REPRINT**  
**© FORTINET**

## Enabling Botnet Protection

- The botnet database:
  - Part of the IPS contract
  - Should be used with the IPS profile to maximize the protection of internal endpoints
- Can be enabled only on the IPS profile
- Administrators can set the action to **Block** or **Monitor**
- IPS logs are generated

The screenshot shows the 'Edit IPS Sensor' configuration page under 'Security Profiles > Intrusion Prevention'. The sensor is named 'high\_security' and has a comment indicating it blocks critical/high/medium vulnerabilities and some low-severity ones. It is configured to 'Block malicious URLs'. Under 'IPS Signatures and Filters', there is a table with four rows. The first three rows have 'Action' set to 'Block' and 'Disabled'. The fourth row is labeled 'Default' and also has 'Disabled'. At the bottom, there is a section for 'Botnet C&C' with a red box around the 'Scan Outgoing Connections to Botnet Sites' button, which is currently set to 'Disable'. There are also 'Block' and 'Monitor' buttons.

Details	Exempt IPs	Action	Packet Logging
SEV (Yellow)		<input checked="" type="radio"/> Block	<input type="radio"/> Disabled
SEV (Orange)		<input checked="" type="radio"/> Block	<input type="radio"/> Disabled
SEV (Red)		<input checked="" type="radio"/> Block	<input type="radio"/> Disabled
SEV (Grey)		<input checked="" type="radio"/> Default	<input type="radio"/> Disabled

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

16

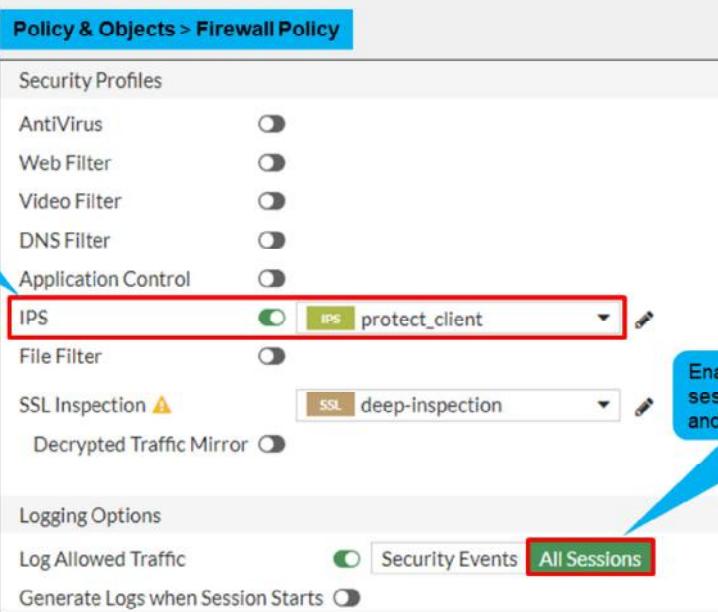
Since the botnet database is part of the FortiGuard IPS contract, administrators can enable scanning of botnet connections to maximize their internal security. You enable botnet scanning on the IPS profile that you applied the firewall policy on. You can also enable scanning of botnet connections using the CLI.

There are three possible actions for botnet and C&C:

- Disable:** Do not scan connections to botnet servers
- Block:** Block connections to botnet servers
- Monitor:** Log connections to botnet servers

**DO NOT REPRINT**  
**© FORTINET**

## Applying IPS Inspection



The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Security Profiles' section, the 'IPS' profile is selected and highlighted with a red box. A blue callout bubble points to this selection with the text: 'Add IPS sensors as security profiles to firewall policies'. Below the IPS profile, there are other security profiles like AntiVirus, Web Filter, Video Filter, DNS Filter, and Application Control, each with a corresponding circular switch.

In the 'Logging Options' section, there are two radio button options: 'Log Allowed Traffic' (selected) and 'All Sessions' (highlighted with a red box). A blue callout bubble points to this option with the text: 'Enable this option to log all sessions including blocked and allowed traffic'.

At the bottom right of the interface, there is a copyright notice: '© Fortinet Inc. All Rights Reserved.' and a page number '17'.

To apply an IPS sensor, you must enable **IPS** and then select the sensor in a firewall policy. By default, FortiGate logs all security events. This means you can see any traffic that is being blocked by IPS.

If you think some traffic should be blocked but is passing through the policy, you should change the **Log Allowed Traffic** method to **All Sessions**. This will log all traffic processed by that firewall policy, and not just the traffic that is blocked by the security profiles. This can help you in identifying false negative events.

**DO NOT REPRINT**  
**© FORTINET**

## IPS Logging

Log & Report > Security Events

Date/Time	%	Severity	Source	Protocol	User	Action	Log Details
2 seconds ago	██████	6	10.200.1.254	6		dropped	General Absolute Date/Time: 2022/04/21 22:44:13 Time: 22:44:13 Session ID: 10137 Virtual Domain: root Agent: Mozilla/5.00 (Nikto/2.1.5) (Evasion:None) (Test:004131)
2 seconds ago	██████	6	10.200.1.254	6		detected	
2 seconds ago	██████	6	10.200.1.254	6		detected	
2 seconds ago	██████	6	10.200.1.254	6		detected	
12 seconds ago	██████	6	10.200.1.254	6		dropped	
22 seconds ago	██████	6	10.200.1.254	6		dropped	
32 seconds ago	██████	6	10.200.1.254	6		dropped	
42 seconds ago	██████	6	10.200.1.254	6		dropped	
53 seconds ago	██████	6	10.200.1.254	6		dropped	
Minute ago	██████	6	10.200.1.254	6		dropped	

**FORTINET.**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

18

If you enabled security events logging in the firewall policies that apply IPS, you can view events are logged on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Intrusion Prevention**.

You should review IPS logs frequently. The logs are an invaluable source of information about the kinds of attacks that are being targeted at your network. This helps you develop action plans and focus on specific events, for example, patching a critical vulnerability.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which IPS action allows traffic and logs the activity?

- A. Allow
- B. Monitor

2. Which IPS component is updated most frequently?

- A. Protocol decoders
- B. IPS signature database



© Fortinet Inc. All Rights Reserved.

19

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Intrusion Prevention System



Denial of Service



Best Practices



Troubleshooting

Good job! You now understand the IPS on FortiGate.

Now, you will learn about DoS.