



FortiGate Administrator

Antivirus

FortiOS 7.4

Last Modified: 8 May 2024

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

Objectives

- Configure the antivirus profile in flow-based inspection mode
- Configure the antivirus profile in proxy-based inspection mode
- Configure protocol options
- Log and monitor antivirus events
- Troubleshoot common antivirus issues

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 effectively.

Antivirus and Inspection Modes

- Antivirus scanning engine uses antivirus signature databases to identify malicious codes



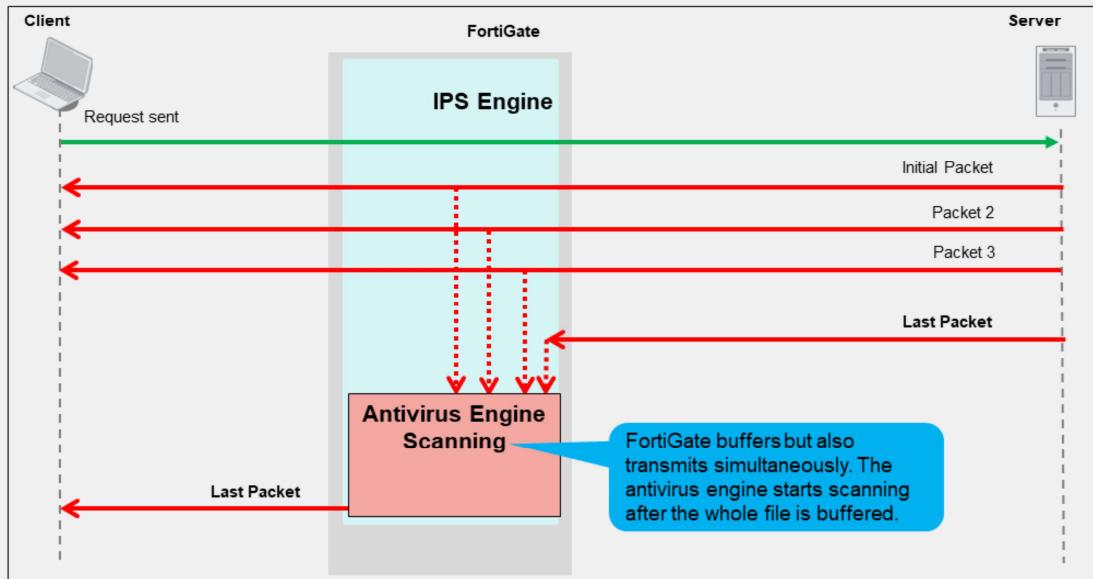
- Available inspection modes

<ul style="list-style-type: none"> • Flow-based inspection <ul style="list-style-type: none"> • Default inspection mode <p>File is scanned on a flow basis</p> <pre> sequenceDiagram participant Client participant FG as FortiGate participant Server Client->>FG: SYN FG->>Client: SYN-ACK Client->>FG: ACK </pre>	<ul style="list-style-type: none"> • Proxy-based inspection <ul style="list-style-type: none"> • Provides additional options <p>Two TCP connections</p> <pre> sequenceDiagram participant Client participant FG as FortiGate participant Server Client->>FG: SYN FG->>Client: SYN-ACK FG->>Server: SYN Client->>FG: ACK Server->>FG: ACK </pre>
--	---

FortiGate with a valid antivirus license can update antivirus signature databases from FortiGuard servers.

Antivirus can operate in flow-based or proxy-based inspection mode.

Flow-Based Inspection Mode Packet Flow



Flow-based inspection mode uses a hybrid of two available scanning modes available: 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.

This slide shows that 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, 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 then sends a block replacement message to the client instead of scanning the file again.

Because the file is transmitted at the same time, flow-based mode consumes more CPU cycles than proxy-based mode. However, depending on the FortiGate model, some operations can be offloaded to SPUs to improve performance.

Flow-Based Inspection Mode

- Default mode

The screenshot displays two configuration screens from the FortiGate management interface.

AntiVirus Profile Configuration:

- Name:** default
- Comments:** Scan files and block viruses. (29/255)
- AntiVirus scan:** Action dropdown is set to **Block**.
- Inspected Protocols:** A list of protocols with checkboxes:
 - HTTP (checked)
 - SMTP (checked)
 - POP3 (checked)
 - IMAP (checked)
 - FTP (checked)
 - CIFS (unchecked)

Firewall Policy Configuration:

- Name:** (empty field)
- Incoming Interface:** (dropdown menu)
- Outgoing Interface:** (dropdown menu)
- Source:** (button with '+')
- Destination:** (button with '+')
- Schedule:** always
- Action:** ACCEPT (selected)
- Firewall/Network Options:** NAT is enabled.
- Security Profiles:** A dropdown menu shows three profiles:
 - AV default (selected)
 - AV default (disabled)
 - AV wifi-default (disabled)

Annotations provide additional context:

- A callout points to the "Action applied to the infected files" dropdown in the AntiVirus profile screen.
- A callout points to the "Select protocols to be scanned" list in the AntiVirus profile screen.
- A callout points to the "Enable AntiVirus profile in the firewall policy" dropdown in the Firewall Policy screen.
- A callout points to the "Select the antivirus profile" list in the Firewall Policy screen.

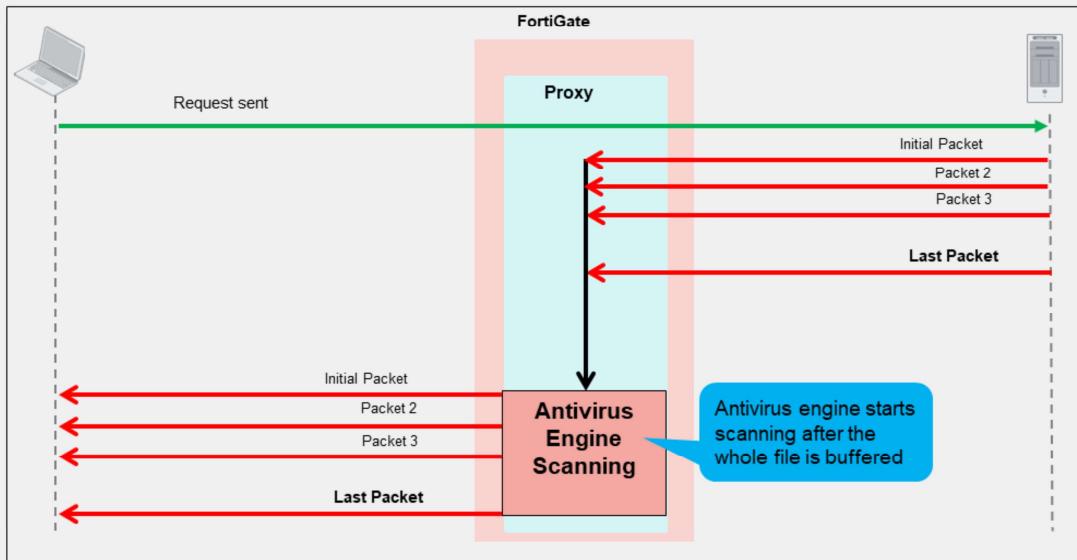
Fortinet Training Institute

© Fortinet Inc. All Rights Reserved. 5

Flow-based inspection mode is the default mode, and its configuration consists of two steps:

- Creating an **AntiVirus Profile** with the selection of the inspected protocols, and the action taken when the FortiGate detects a virus infected file.
- Applying the flow-based **Antivirus Profile** to a firewall policy.

Proxy Inspection Mode Packet Flow



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.

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 because of 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 because FortiGate is transmitting the packets to the end client.

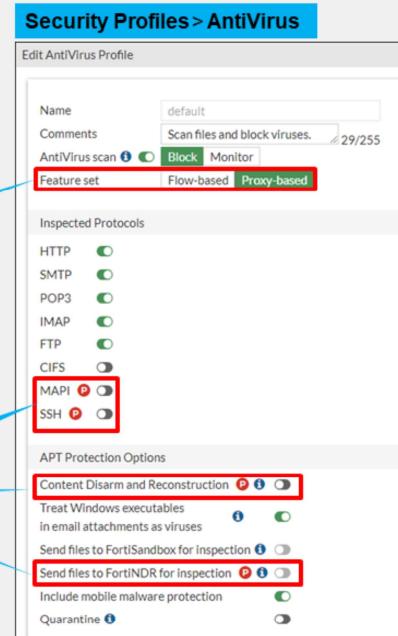
Using proxy inspection antivirus allows you to use stream-based scanning, which is enabled by default. Stream-based scanning scans large archive files by decompressing the files and then scanning and extracting them at the same time. This process optimizes memory use to conserve resources on FortiGate.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

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)
 - FortiNDR inspection

Feature visibility activated through CLI

Available only in proxy inspection mode



© Fortinet Inc. All Rights Reserved.

7

Proxy-based inspection mode is applied when you set **Feature set** to **Proxy-based**. For low-end platforms, this feature is available on the GUI when you enable the CLI command `gui-proxy-inspection`.

Unlike flow-based inspection mode, proxy-based inspection mode allows the profile to inspect the MAPI and SSH protocols traffic, as well as sanitize Microsoft documents and PDF files using the content disarm and reconstruction (CDR) feature. It can also use FortiNDR to inspect high-risk files.

Firewall Policy With Proxy Inspection Mode

The screenshot shows the 'Policy & Objects > Firewall Policy' screen. A callout bubble points to the 'Inspection Mode' dropdown, which is set to 'Proxy-based'. Another callout bubble points to the 'AntiVirus' section under 'Security Profiles', where a list of profiles is shown, including 'default', 'Search', and 'wif-default'. A third callout bubble points to the 'Available only in proxy-based inspection mode' note.

Policy & Objects > Firewall Policy

Create New Policy

Name:

Incoming Interface:

Outgoing Interface:

Source:

Destination:

Schedule: always

Service:

Action: ACCEPT DENY

Inspection Mode: Flow-based **Proxy-based**

Firewall/Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROXY default

Security Profiles

AntiVirus: default

Web Filter: default

Video Filter: default

DNS Filter: default

Application Control:

IPS:

File Filter:

SSL Inspection: no-inspection

Available only in proxy-based inspection mode

Set Inspection Mode to Proxy-based

Proxy-based and flow-based antivirus profiles available

© Fortinet Inc. All Rights Reserved. 8

The next step is to apply the proxy-based antivirus profile to a firewall policy. You must set **Inspection Mode** to **Proxy-based**.

Antivirus Block Page

- Information available on the antivirus block page

The image shows two screenshots side-by-side. On the left is the 'Antivirus Block Page' from Fortinet, featuring a 'High Security Alert' message stating that a file is infected with the virus 'EICAR_TEST_FILE'. It includes fields for 'File name', 'Virus name', 'Website host or URL', 'URL', 'Quarantined File Name [disabled]', and 'Reference URL'. A blue box labeled 'Link to FortiGuard Encyclopedia' points to the right screenshot. On the right is the 'Threat Encyclopedia' page from FortiGuard Labs, showing details for 'EICAR_TEST_FILE' with an ID of 2172, released on Oct 15, 1996, and last updated on Jan 05, 2015. It includes sections for 'Analysis' and 'Link to FortiGuard Encyclopedia'.

Antivirus Block Page Labels:

- File name
- Virus name
- Website host or URL

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 suspected malware.

Inspection Modes Use Cases

- Both use the full antivirus database

- Flow inspection mode

- Pattern matching can be offloaded to CP8 or CP9
- Priority on traffic throughput

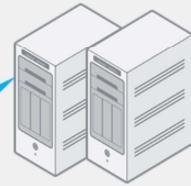
Servers providing reliable service for large numbers of concurrent users



- Proxy inspection mode

- Required for its additional options
- Priority on network security

Protecting emails received by mail servers through SMTP or MAPI



Regardless of which mode you use, both use the full antivirus database (extended or extreme—depending on the CLI command `use-extreme-db` and the FortiGate model) and the scan techniques give similar detection rates. How can you then choose between the inspection modes?

If security is your priority, proxy inspection mode—with client comforting disabled—is more appropriate. If performance is your top priority, then flow inspection mode is more appropriate. Depending on the FortiGate model, flow-based pattern matching can be offloaded to CP8 or CP9 processors, and FortiGate models that support NTurbo can accelerate antivirus processing to enhance performance. 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. So, this acceleration does not apply to proxy-based inspection.

Configuring Protocol Options

- Available for both proxy-based and flow-based firewall policies

The screenshot shows two windows from the Fortinet FortiManager interface:

- Policy & Objects > Firewall Policy**: A window for creating a new firewall policy. It includes fields for Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule, Service, Action (ACCEPT/DENY), Inspection Mode (Flow-based/Proxy-based), and Firewall/Network Options (NAT, IP Pool Configuration, Preserve Source Port). A red box highlights the "Protocol Options" dropdown menu, which contains a "Search" field and a "Create" button.
- Policy & Objects > Protocol Options**: A window for managing protocol options. It shows a table of protocol mappings with columns for Protocol, Action, and Port. A row for FTP has its port value "21,22,23" highlighted with a red box. A blue callout box states: "Protocol options named to be applied in a firewall policy". Another blue callout box states: "You can specify more than one port number (separated by comma)".

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 11

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. Some options apply only to proxy-based inspection, like **Protocol Port Mapping**.

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.

Protocol Options—Large Files

- By default, files that are bigger than the oversize limit are bypassed from scanning
- You can modify this behavior for all protocols



- You can enable logging of oversize files and adjust settings per protocol using the CLI

```
config firewall profile-protocol-options
  edit <profile name>
    set oversize-log {enable|disable}
    config <protocol Name>
      set options oversize
      set oversize-limit <integer>
    end
  end
end
```

Oversize files logging setting

Name of the specific protocol

So, what does the additional granularity provided by protocol options include? It allows you to block large files. You can also adjust the **Threshold** for optimal performance in your network. The buffer limit varies by model. 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 must balance the two.

You can also disable the **oversize** option and adjust the **oversize-limit** per protocol from the `config firewall profile-protocol-options` command tree.

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

Protocol Options—Compressed Files

- Archives are unpacked and files and archives within are scanned separately
- Password-protected archives cannot be decompressed
- Increasing the limits impacts memory usage

```
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
```

Oversize limit specific to decompressed files

Nested archive limit

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). Usually, you shouldn't increase this setting because it increases RAM usage.

Antivirus Logs

The screenshot shows the FortiGuard Log & Report interface. At the top, there's a summary of '3 Events' under the 'AntiVirus' category. Below this is a detailed log table with columns for Date/Time, Service, Source, File Name, Virus/Botnet, User, Details, and Action. One specific entry is highlighted in red, showing an HTTP request from 'elcar.com' for 'EICAR_TEST_FILE' was blocked. To the right, a 'Log Details' window provides comprehensive information about this event, including Protocol (HTTP), Service (HTTP), Data (File Name: elcar.com), Action (Blocked), Threat (2), Policy ID (1 [Full Access]), Policy UUID (b11ac58c-791b-51e7-4600-12f829a689d9), Policy Type (Firewall), Security (Level: Warning, Threat Level: Critical, Threat Score: 50), Cellular (Service: HTTP), and AntiVirus (Profile: default, Virus/Botnet: EICAR_TEST_FILE, Virus ID: 2.172, Reference: http://www.fortinet.com/vn=ElCAR_TEST_FILE, Detection Type: cached, Direction: Incoming, Quarantine Skip: Quarantine-disabled, Submitted to FortiSandbox: false, Message: File is infected). A red arrow points from the 'AntiVirus' link in the summary to the 'AntiVirus' section in the log table. Another red arrow points from the 'AntiVirus' link in the log table to the 'Log Details' window. Blue callout boxes provide additional context: one points to the log entry in the table with the text 'Log entry when a virus is detected', and another points to the 'AntiVirus' section in the details window with the text 'Details on the virus with FortiGuard reference'.

Log & Report > Security Events

Log Details

Protocol	HTTP
Action	Blocked
Threat	2
Policy ID	1 [Full Access]
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall
Security	Warning
Level	Critical
Threat Level	50
Cellular	HTTP
AntiVirus	default EICAR_TEST_FILE 2.172 http://www.fortinet.com/vn=ElCAR_TEST_FILE cached Incoming Quarantine-disabled false File is infected.

© Fortinet Inc. All Rights Reserved. 14

Logging is an important part of managing a secure network. When 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.

When you enable oversized files logging, a log entry is also created with the details including the message "Size limit is exceeded".

Forward Traffic Logs

The screenshot shows the FortiGate interface for viewing forward traffic logs. On the left, a table lists traffic entries. One entry from September 13, 2023, at 04:35:58 is highlighted with a red box and has a blue callout pointing to it labeled "Forward traffic log entry". On the right, a detailed log window titled "Log Details" is open, showing security-related information for the same entry. A red box highlights the "Security" tab in the top navigation of the log details window. Another blue callout points to this tab with the label "Security log details".

Date/Time	Source	Destination	Application Name	Result	Policy ID
2023/09/13 00:50:20	10.0.1.10	10.200.1.254	FTP	✓ Accept (1.61 kB / 1.73 kB)	1 (Full_Access)
2023/09/13 00:49:24	10.0.1.10	10.200.1.254	tcp/63214	✗ Deny (Deny: UTM Blocked)	1 (Full_Access)
2023/09/13 00:49:24	10.0.1.10	10.200.1.254	tcp/21070	✗ Deny (Deny: UTM Blocked)	1 (Full_Access)
2023/09/13 00:49:24	10.0.1.10	10.200.1.254	tcp/35516	✗ Deny (Deny: UTM Blocked)	1 (Full_Access)
2023/09/13 00:43:58	10.0.1.10	10.200.1.254	HTTP	✗ Deny (Deny: UTM Blocked)	1 (Full_Access)
2023/09/13 00:43:13	10.0.1.10	10.200.1.254	HTTP	✗ Deny (Deny: UTM Blocked)	1 (Full_Access)

Forward traffic log entry

Security log details

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 15

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

Security Dashboard

- Security widget and dashboard allow you to monitor your network

The screenshot shows the Fortinet Security Dashboard interface. At the top left, there's a title bar "Dashboard > Security". Below it, a card displays "Top Threats by Threat Level" with one entry: Threat EICAR_TEST_FILE, Threat Category Malware, Threat Level Critical, Threat Score 250, and Sessions 5. A "View session logs" button is present. To the right is a line chart titled "Bytes" over a 24-hour period, showing a sharp peak at 00:00. Below the chart is a table with columns Source, Destination, Device, Threat Score, Bytes, and Sessions, showing data for a source IP 10.0.1.10.

Drill down for further details

Dashboard

Advanced Threat Protection Statistics

A donut chart indicates 37 total files, with 1 being Malicious. A legend for "Port/Gate Scanned Files" shows categories: Clean (green), Malicious (red), Suspicious (blue), FortGuard Outbreak Pre- (yellow), External Malware Block L... (orange), and EMS Threat Feed (brown).

Security widget

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved. 16

You can also use the **Security** dashboard to view relevant information regarding threats to your network. The security dashboard organizes information into source and destination and allows you to drill down with session logs details.

For the **Advanced Threat Protection Statistics**, you can add the corresponding widget on the dashboard for monitoring purposes.

Troubleshooting Common Antivirus Issues

- Verify FortiGuard antivirus license

System > FortiGuard

Advanced Malware Protection	Licensed (Expiration Date: 2026/01/19)	Valid license
AI Malware Detection Model	Version 2.05360	
AntiVirus Definitions	Version 90.01635	
AntiVirus Engine	Version 7.00018	
Mobile Malware	Version 90.01635	
Outbreak Prevention	Licensed (Expiration Date: 2026/01/19)	

- Force FortiGate to check for new antivirus updates

```
# execute update-av
```

- Run the real-time update debug to isolate update-related issues

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

Viruses are constantly evolving and you must have the latest antivirus definitions version to ensure correct protection.

With a valid license, FortiGate checks regularly for updates. If an antivirus profile is applied on at least one firewall policy, you can also force an update of the antivirus definitions database with the CLI command `execute av-update`.

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 do 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.
- If you continue to see issues with the update, run the real-time debug command to identify the problem.

Troubleshooting Common Antivirus Issues (Contd)

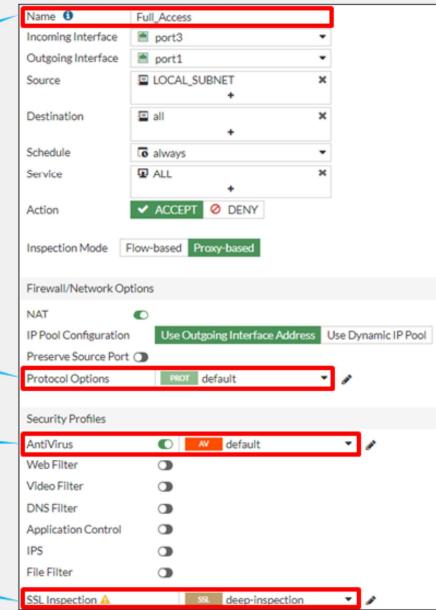
- Unable to catch viruses even with a valid contract?

Check firewall policy configuration

In proxy-based inspection mode,
verify the protocol port mapping

Verify the antivirus profile applied

For encrypted protocols,
you must select deep inspection



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 do the following to verify:

- Make sure that the correct antivirus profile is applied on the right firewall policy.
- Make sure that the right protocol port is configured when the inspection mode is proxy-based.
- Make sure that you are using the correct antivirus profile and SSL/SSH inspection on all firewall policies.

Troubleshooting Common Antivirus Issues (Contd)

- Check useful antivirus commands

```
# get system performance status
```

Virus caught: 100 total in 1 minute

Displays virus statistics for the last one minute

```
# diagnose antivirus database-info
```

version: 90.01635(04/22/0022 13:26)

atdb found 1 loaded 1

virus ID count 29630

grayware ID count 140

signature ID count 49988

etdb found 1 loaded 1

virus ID count 60712

grayware ID count 4429

signature ID count 806735

exdb found 1 loaded 0

virus ID count 0

grayware ID count 0

signature ID count 0

Displays current antivirus database information

Displays versions information

```
# diagnose autoupdate versions  
Virus Definitions
```

Version: 90.01635 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Mon Apr 25 13:52:18 2022
Last Update Attempt: Wed Sep 13 06:27:50 2023
Result: No Updates

```
# diagnose antivirus test "get scantime"  
antivirus test (manager)
```

0~5s:	0
5~10s:	0
10~15s:	0
15~20s:	0
20~25s:	0
25~30s:	0
>30s:	0

Displays scan times for infected files

To troubleshoot further common antivirus issues, you can check information provided by the following commands:

- 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.

Knowledge Check

1. Which additional features of an antivirus profile are available in proxy-based inspection mode?
 A. MAPI, SSH, CDR, and FortiNDR
 B. Full and quick

2. What does the oversize files logging setting do?
 A. Enables logging of all files that exceed the oversize limit
 B. Logs all files that are over 5 MB

3. Which type of inspection mode can be offloaded using CP processors?
 A. Proxy-based
 B. Flow-based

Review

- ✓ Apply the antivirus profile in flow-based inspection modes
- ✓ Apply the antivirus profile in proxy-based inspection modes
- ✓ Compare inspection modes
- ✓ Configure protocol options
- ✓ Log and monitor antivirus events
- ✓ Troubleshoot common antivirus issues

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.