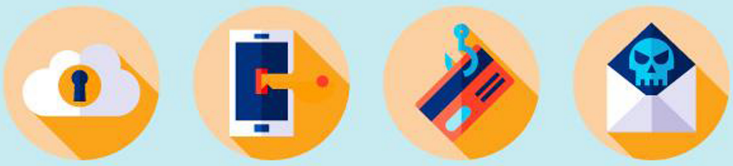
# Blocking Malware through

# Antivirus Security Profile in FortiGate



manipahlavanzadeh

**After completing this document, you will be able to achieve these objectives:**

**1- Understand why you should use antivirus protection**

**2- Explain how FortiGate antivirus works to block malware**

**3- Configure FortiGate antivirus profile in Flow-based and Proxy-based inspection mode**

**4- Configure Protocol Options**

**5- Log & Monitor antivirus events**

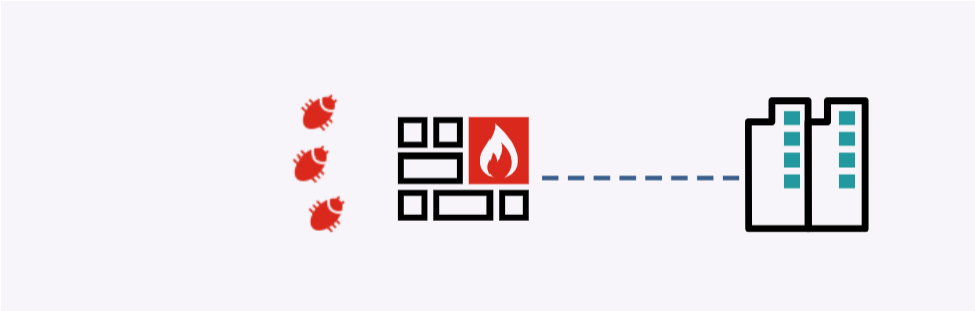
**6- Troubleshoot Common antivirus issues and best practices**

# Malware & Antivirus

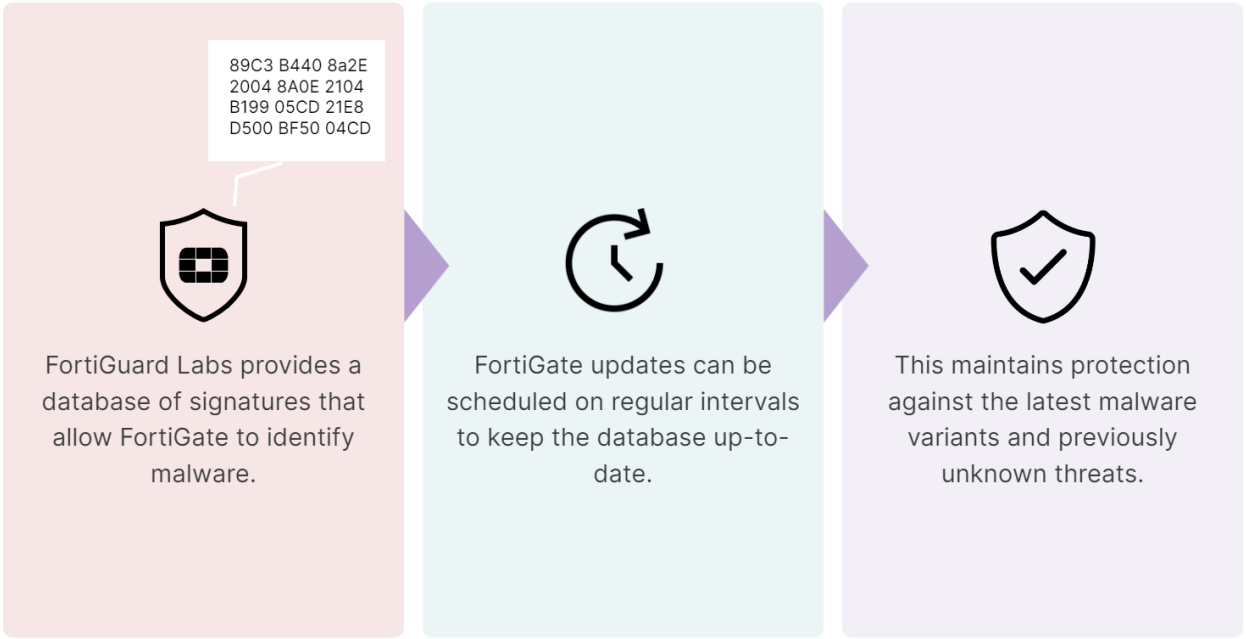
## Risk of Malware:

**Keeping malware out of your network is key to securing your organization. Cyber criminals use malware to:**

- Cause data breaches
- Extort money
- Steal intellectual property
- Disrupt business and destroy systems



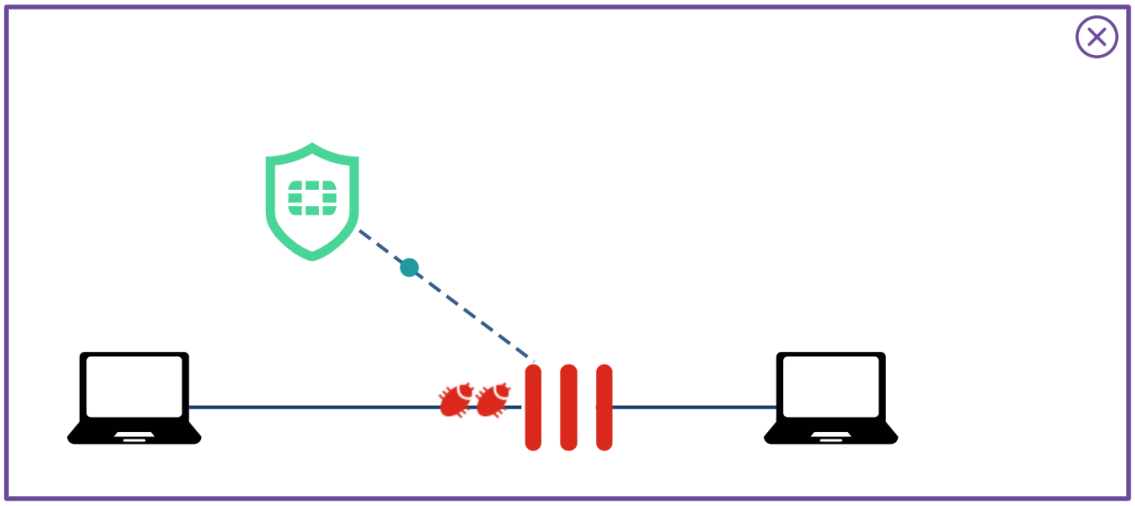
## FortiGuard Labs: FortiGate with a valid antivirus license can update antivirus signature databases from FortiGuard servers.

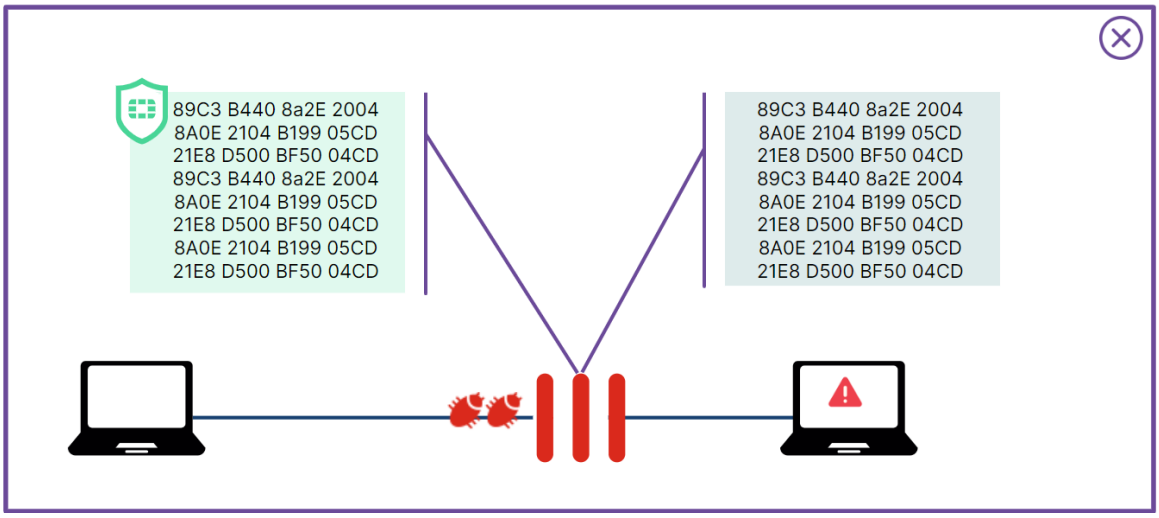


# FortiGate Antivirus Scanning:

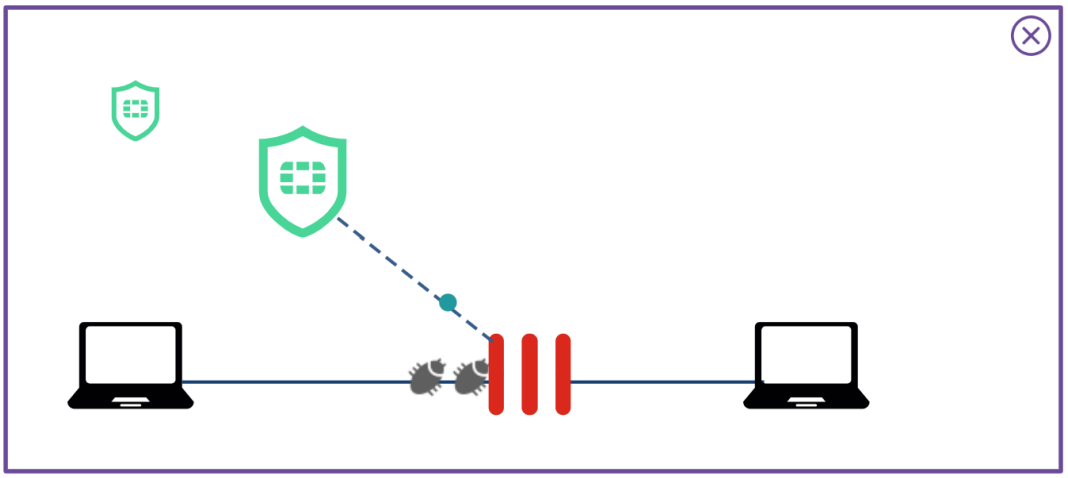
**FortiGate uses many techniques to detect viruses. These detection techniques include:**

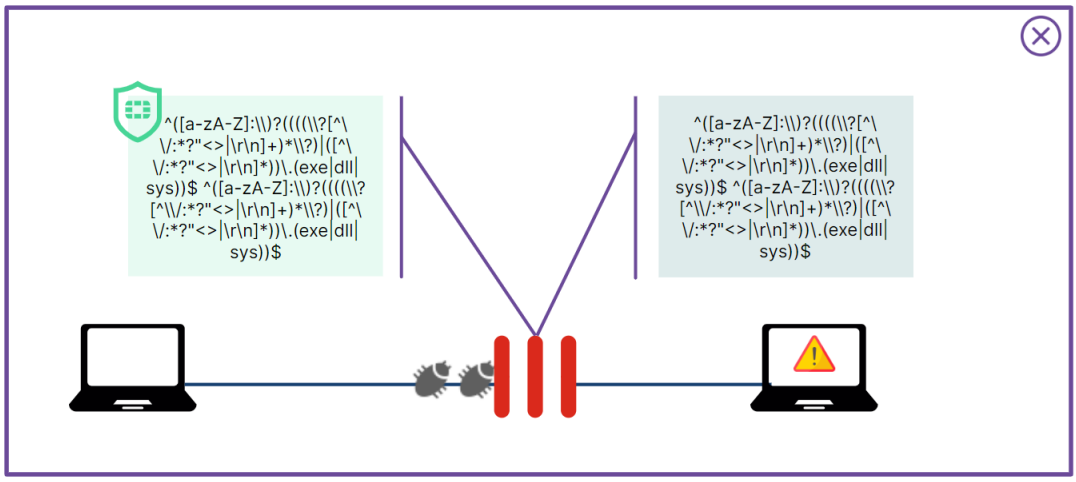
- **Antivirus scan (Signature-Based)- Antivirus scan detects known malware and is the first, fastest, and the simplest way to detect malware. FortiGate detects viruses that are an exact match for a signature in the FortiGuard antivirus database.**





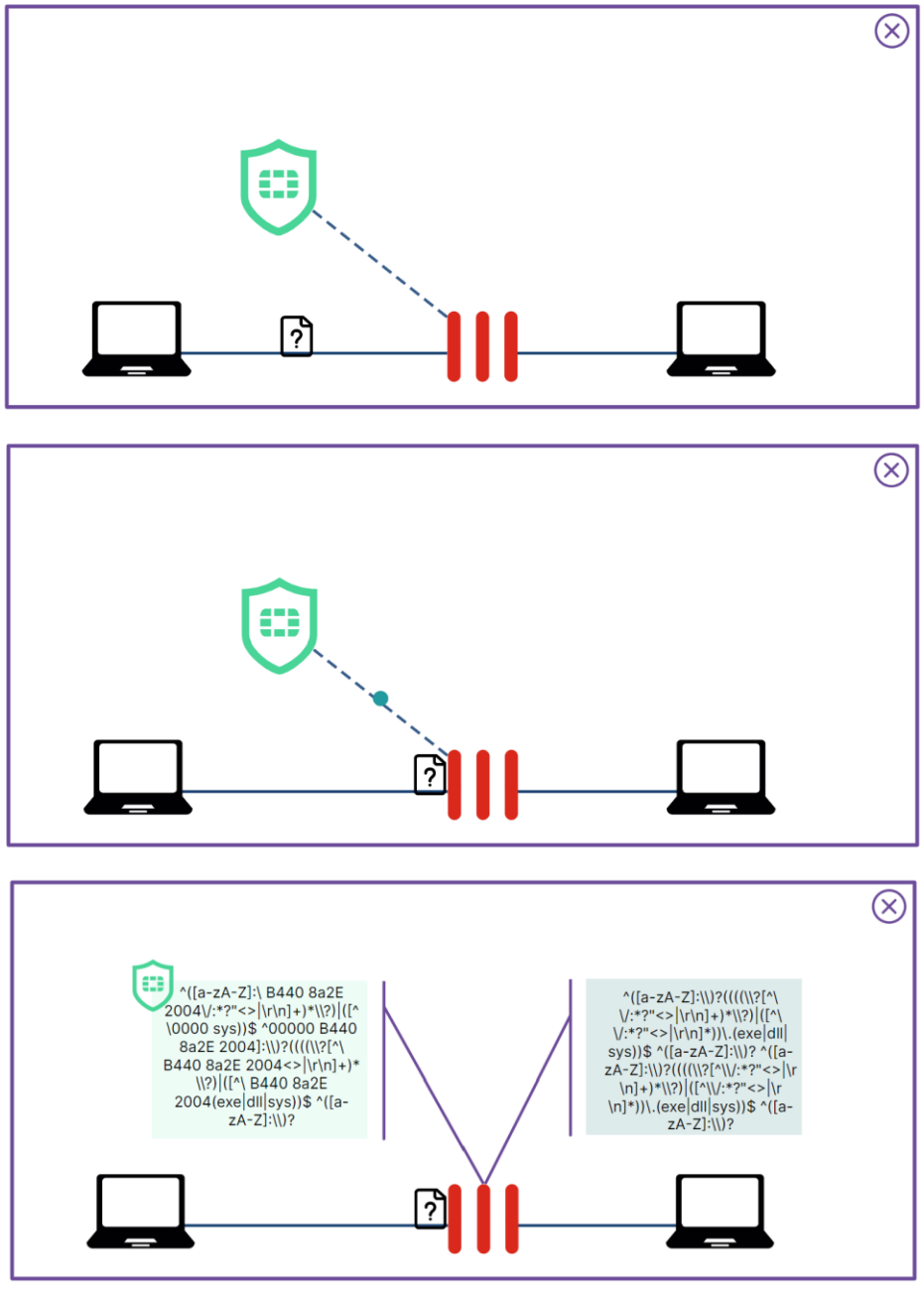
• **Grayware scan** - **Grayware scan detects unsolicited programs, known as grayware, that have been installed without the user's knowledge or consent. While grayware is not technically a virus, it can cause unwanted behavior, so FortiGate considers it to be malware. Often, FortiGate detects grayware using a FortiGuard grayware signature.**

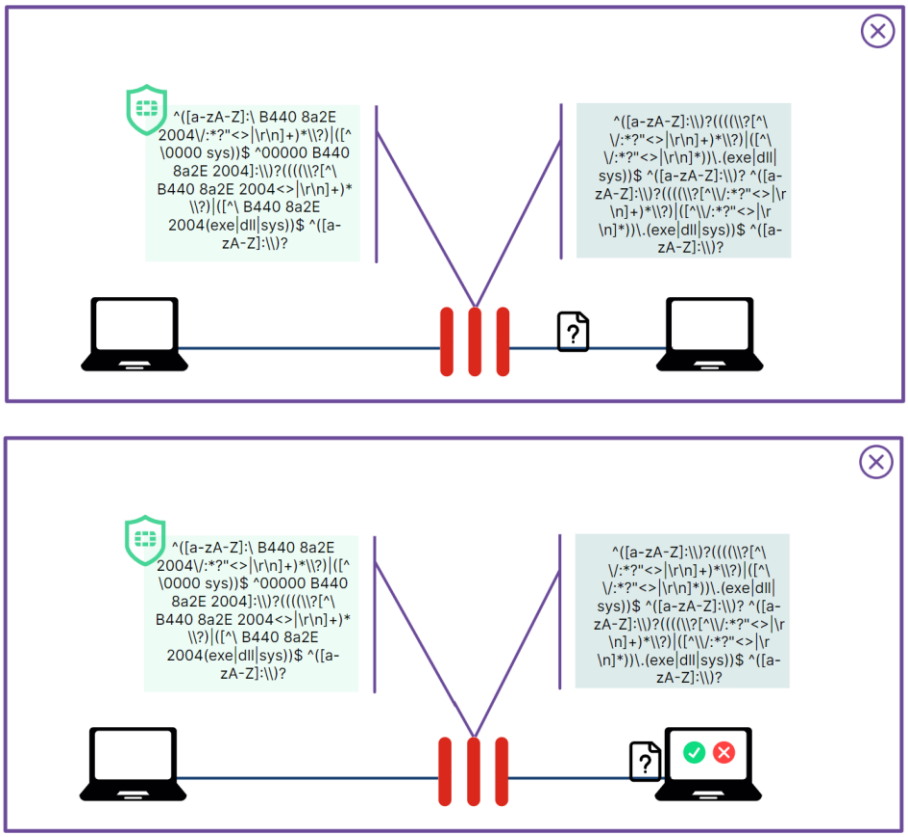




- **Machine learning/artificial intelligence scan –**

**Machine learning/artificial intelligence scan uses machine learning and artificial intelligence techniques to detect zero-day attacks containing malware that is new, unknown, and, does not yet have a matching associated signature. Because this type of scan is based on probability, using it does increase the possibility of false positives. By default, when FortiGate detects a new virus, it logs the file as suspicious but does not block it. You can choose whether to block or allow suspicious files.**



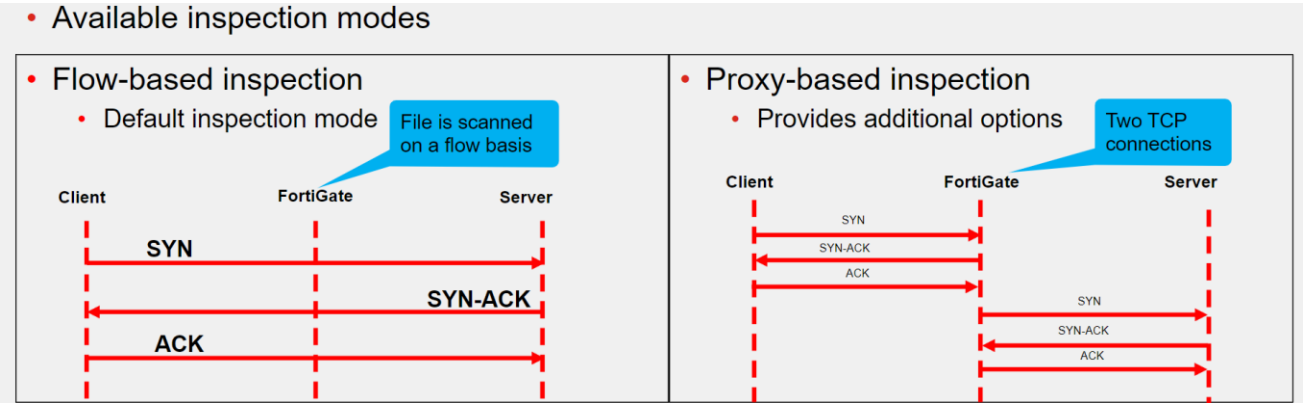






# Antivirus Inspection Mode?

**Antivirus can operate in <u>flow-based</u> or <u>proxy-based</u> inspection mode.**

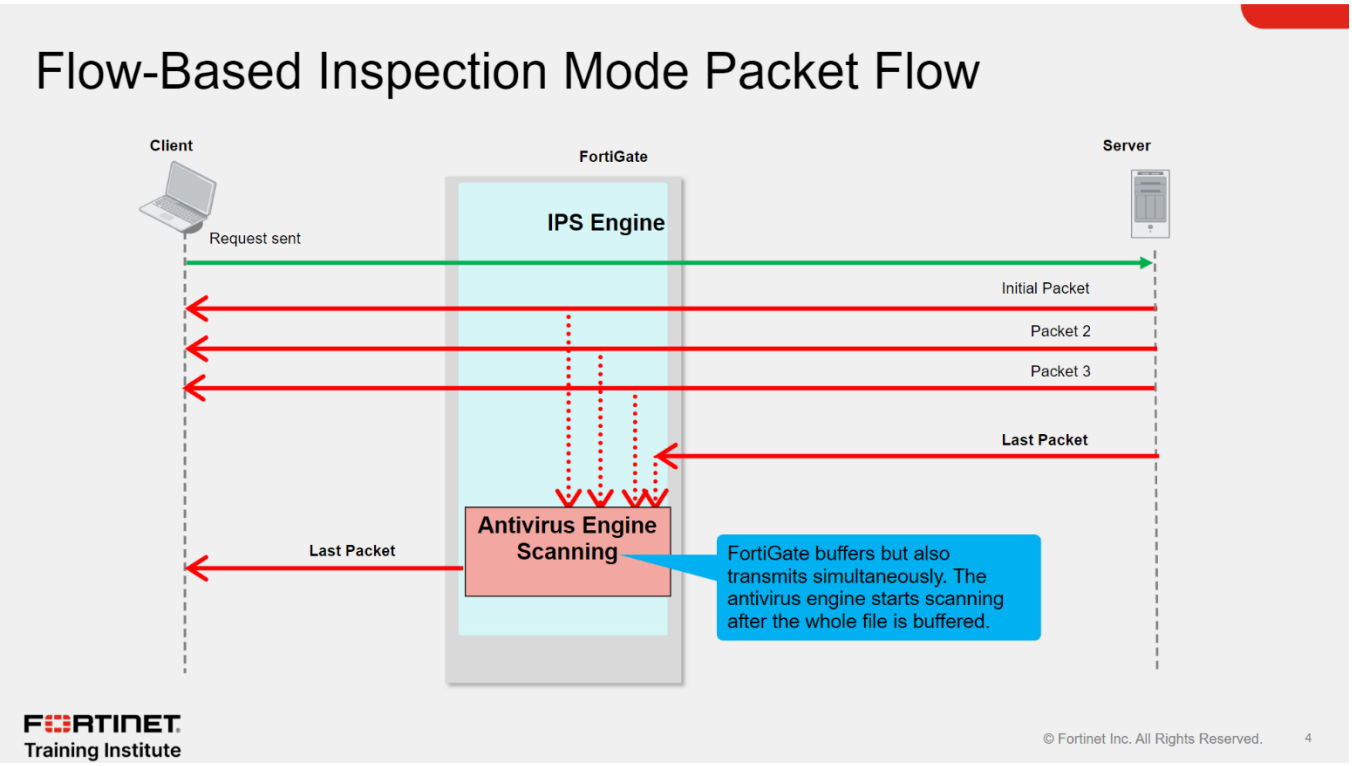


# Flow-based inspection mode

## IPS Engine:

**The IPS engine is responsible for IPS and Protocol decoders, in addition to application control, flow-based antivirus protection, web filtering, and email filtering.**

**Packet Flow**




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

- **the default scanning mode:**
  **The default mode enhances the scanning of nested archive files without buffering the container archive file.**
- **the legacy scanning mode:**
  **The legacy mode buffers the full container, and then scans it.**

Starting from 6.4.0, the scan mode option is no longer available for flow-based AV.

This means that AV no longer exclusively uses the default or legacy scan modes when handling traffic on flow-based firewall policies. Instead, AV in flow-based policies uses a **hybrid of the two scan modes**.

**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.**

## * Note that:

## Flow-based inspection mode doesn't allow the profile to inspect the MAPI and SSH protocols traffic.

# Configuration

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

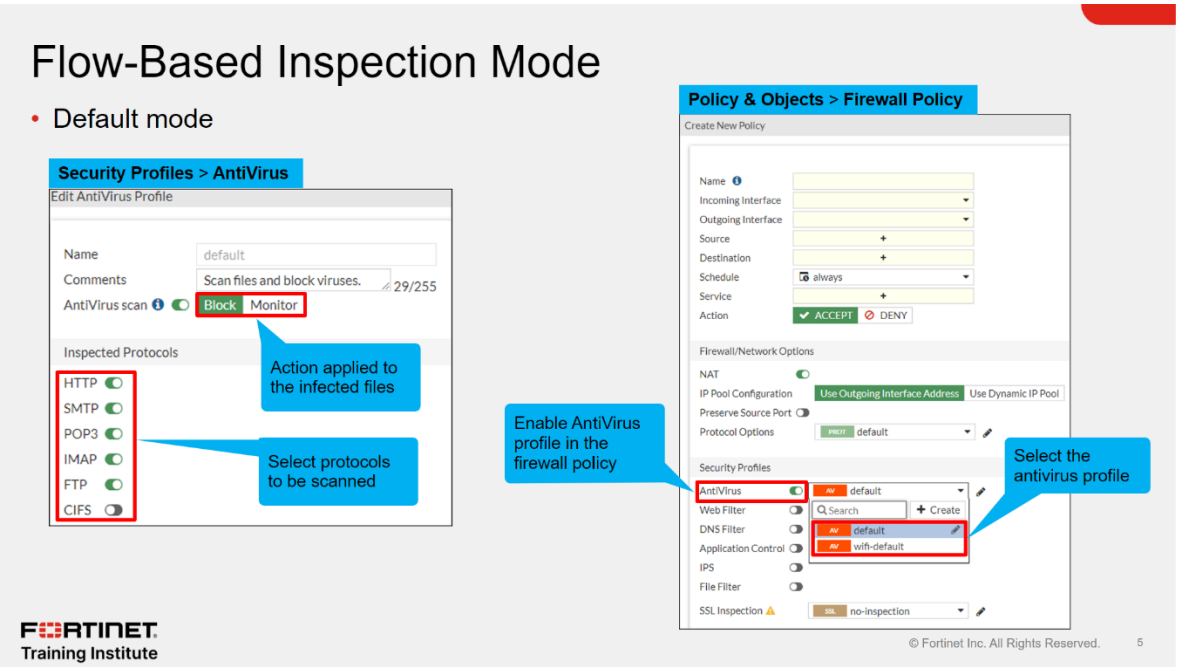
**• Creating an AntiVirus Profile with the selection of the inspected protocols, and the action taken when the FortiGate detects a virus infected file: Block, Monitor.**

FortiOS includes two preloaded antivirus profiles:

- *default*
- *wifi-default*

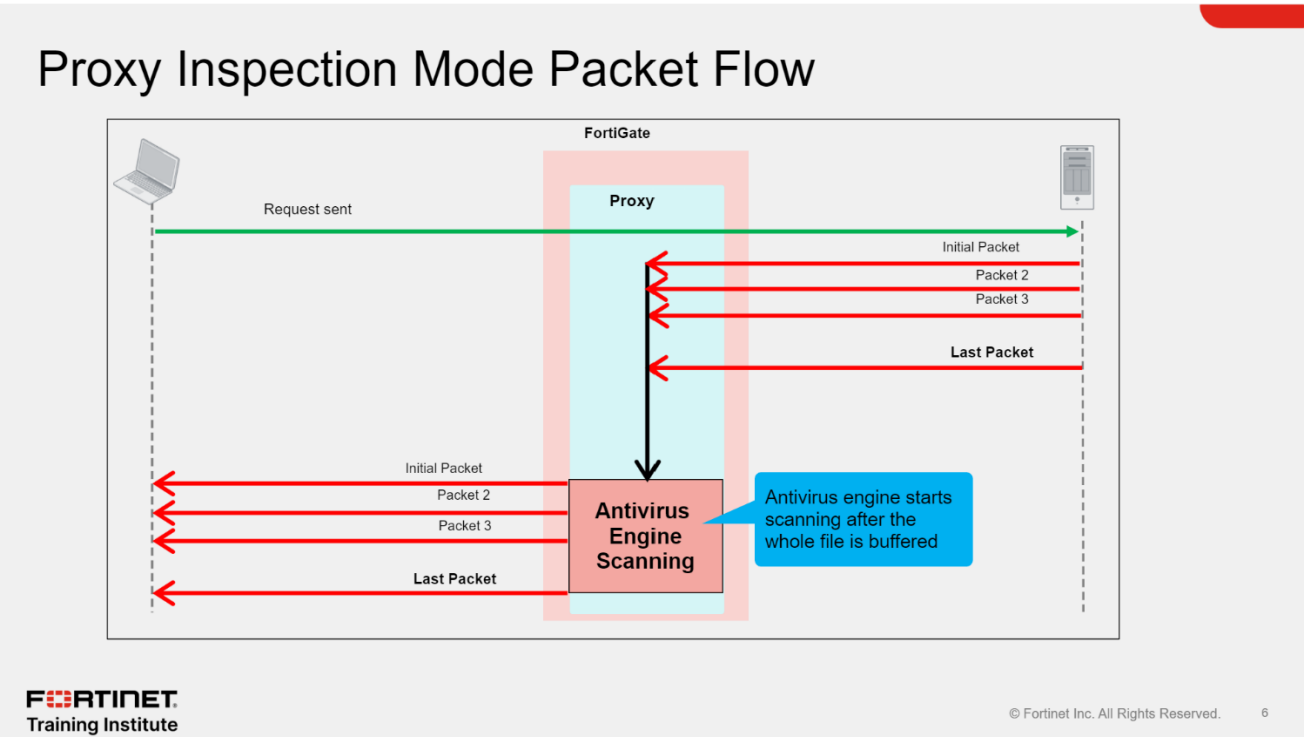
You can customize these profiles, or you can create your own to inspect certain protocols.

**• Applying the flow-based Antivirus Profile to a firewall policy.**



# Proxy-based 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.**

# Client Comforting:

## This feature is supported just in Proxy-Mode.

**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.**

# stream-based scanning:

**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.**

**In FortiOS 7.0, stream-based scan is supported in HTTP(S), FTP(S), and SCP/SFTP.**

### Stream-based scanning provides the following AV improvements:

- Archive files (ZIP, GZIP, BZIP2, TAR, ISO) that exceed the oversize limit are uncompressed and scanned for infections.
- The contents of large archive files are scanned without having to buffer the entire file.

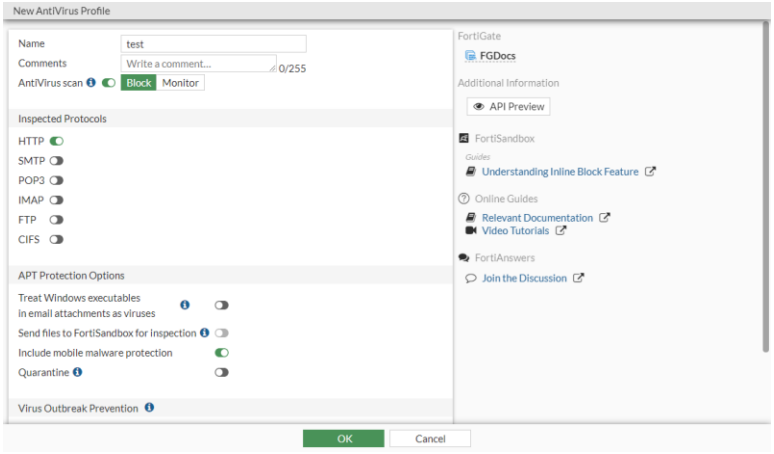
# Configuration

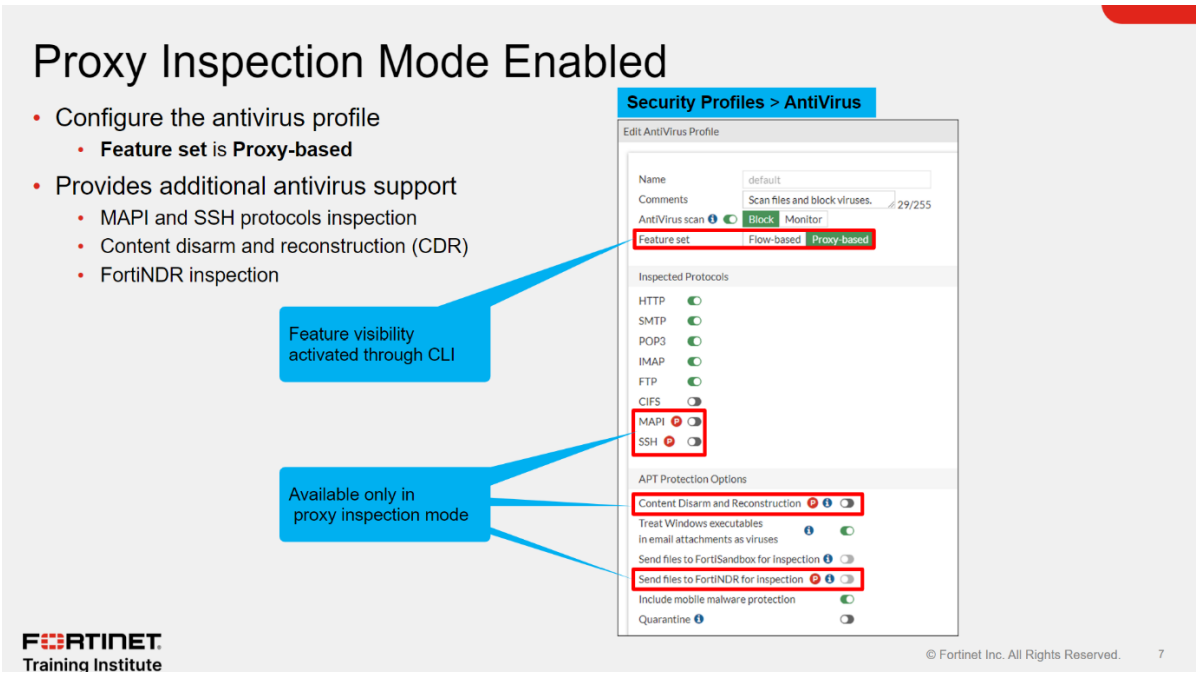
## 1. Creating an AntiVirus Profile with the selection of the inspected protocols, and the action taken when the FortiGate detects a virus infected file: Block, Monitor.

Proxy-based inspection mode is applied when you set Feature set to Proxy-based.
For lowend platforms, this feature is available on the GUI when you enable the CLI command:

```
config system settings
    set gui-proxy-inspection enable
end
```

The `gui-proxy-inspection` setting under `config system settings` is enabled on most models except for entry-level platforms with 2 GB of RAM or less. When this setting is disabled, Firewall policy pages do not have option to select a Flow-based or Proxy-based inspection mode.



## Go to Security Profiles > AntiVirus and click Create New.

## Configure the following settings:

| | |
|---|---|
| *Name* | Enter a unique name for the profile. |
| *Comments* | Enter a comment (optional). |
| *AntiVirus scan* | Enable one or more protocols for inspection, then enable *AntiVirus scan* for the selected protocols with a specified action.<br>• *Block*: block the malicious traffic.<br>• *Monitor*: log malicious traffic and allow it to pass inspection. |
| *Feature set* | Select the feature set for the profile. The feature set mode must match the inspection mode used in the associated firewall policy.<br>• *Flow-based*<br>• *Proxy-based*<br>Additional options are available in proxy-based mode and are identified in the GUI with a *P* icon. See Inspection mode feature comparison for more details.<br>If the *Feature set* option is not visible, enter the following in the CLI:<br>`config system settings`<br>`set gui-proxy-inspection enable`<br>`end` |
| *Inspected Protocols* | Enable to inspect the protocol for session inspection: HTTP, SMTP, POP3, IMAP, FTP, and CIFS. Disabled protocols are not inspected.<br>MAPI and SSH can be inspected in proxy-based mode. |
| *APT Protection Options* | This section includes options available with FortiGuard to mitigate advanced persistent threats (APT) in file-based attacks. |

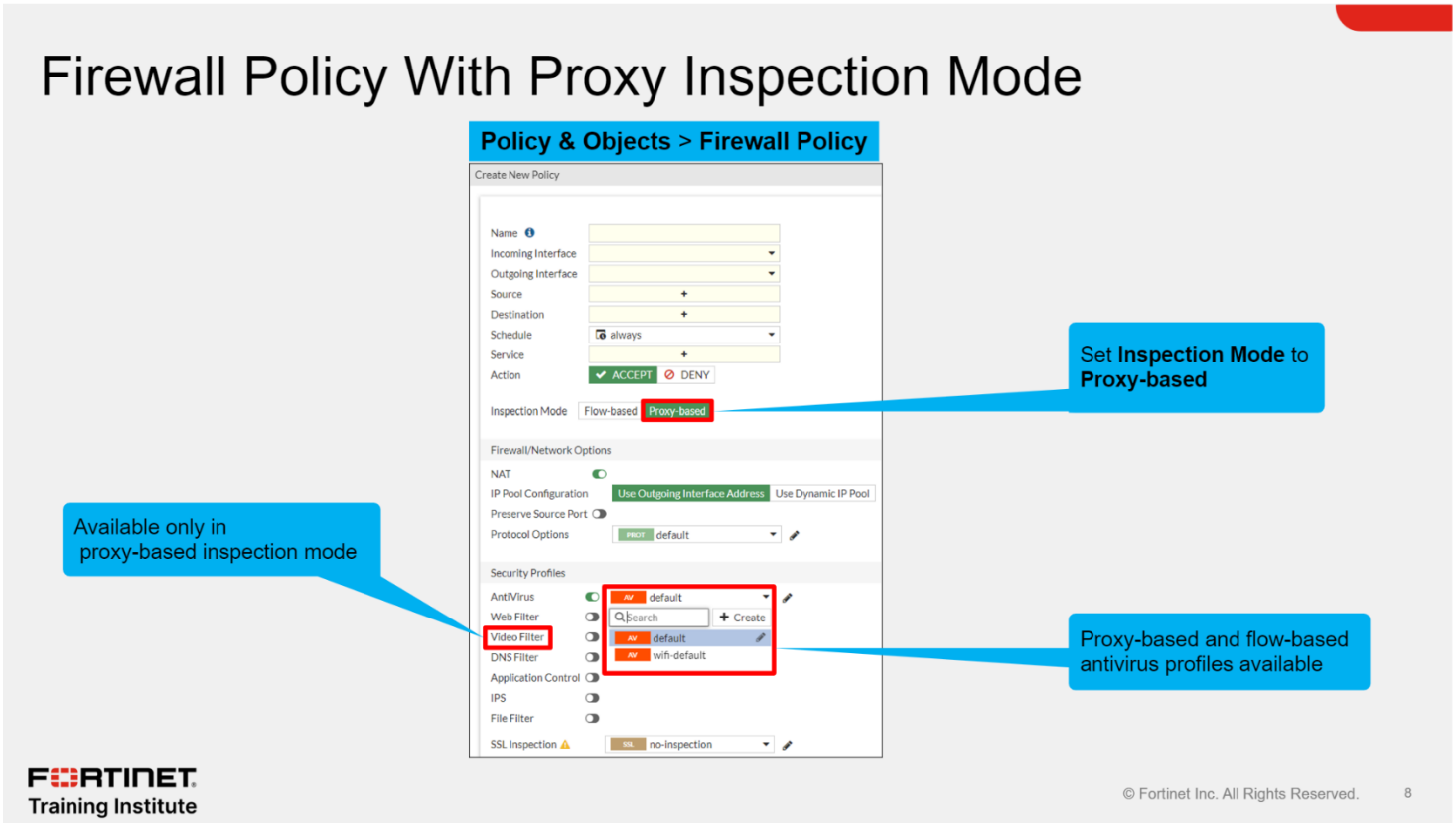
| | |
|---|---|
| *Content Disarm and Reconstruction* | This option is available in proxy-based mode when at least one protocol is enabled for inspection and *AntiVirus scan* is enabled.<br>See Content disarm and reconstruction for more details. |
| *Allow transmission when an error occurs* | Enable to allow traffic to pass when an inspection error occurs. Disable to block traffic when an inspection error occurs. |
| *Original File Destination* | Specify how to quarantine files processed by content disarm and reconstruction.<br>• *FortiSandbox*: quarantine files on FortiSandbox. The FortiSandbox must be enabled. See Using FortiSandbox post-transfer scanning with antivirus for more details.<br>• *File Quarantine*: quarantine files on FortiGate models with a hard disk.<br>• *Discard*: discard suspicious files. |
| *Treat Windows executables in email attachments as viruses* | Enable to deem all Windows executable files located in email traffic as viruses. |
| *Send Files to FortiSandbox for Inspection* | Enable to send files to FortiSandbox for inspection. The FortiSandbox must be enabled. |
| *Scan strategy* | FortiSandbox scans files inline for flow-based mode (*Inline*) and after the file transfer is complete for proxy-based mode (*Post Transfer*). See Using FortiSandbox inline scanning with antivirus and Using FortiSandbox post-transfer scanning with antivirus for more details. |

| | | |
|---|---|---|
| | *File types* | Specify which files to FortiSandbox for inspection.<br>• *Suspicious Files Only*: only send suspicious files to FortiSandbox for inspection.<br>• *All Supported Files*: send all supported files to FortiSandbox for inspection. |
| | *Do not submit files matching types* | Click the + to exclude certain file types from being sent to FortiSandbox. |
| | *Do not submit files matching file name patterns* | Click the + to enter a wildcard pattern to exclude files from being sent to FortiSandbox. |
| *Use FortiSandbox database* | | Enable to use the signature database from FortiSandbox. The FortiSandbox must be enabled. |
| *Send files to FortiNDR for inspection* | | This option is available in proxy-based mode when at least one protocol is enabled for inspection, *AntiVirus scan* is enabled, and FortiNDR is enabled. See Using FortiNDR inline scanning with antivirus for more details. |
| *Include mobile malware protection* | | Enable to use the mobile malware protection database from FortiGuard for content scanning. |
| *Quarantine* | | This option is available when at least one protocol is enabled for inspection and *AntiVirus scan* is enabled.<br>Enable to quarantine infected files.<br>See also Downloading quarantined files in archive format. |
| *Virus Outbreak Prevention* | | This section includes options available with the FortiGuard Virus Outbreak Protection Service (VOS).<br>See Virus outbreak prevention and FortiGuard outbreak prevention for more details. |

| | |
|---|---|
| *Use FortiGuard outbreak prevention database* | Enable to use the outbreak prevention database that is available with Advanced Malware Protection on FortiGuard. A license is required.<br>• *Block*: block the malicious traffic.<br>• *Monitor*: log malicious traffic and allow it to pass inspection. |
| *Use external malware block list* | Enable to use one or more external blocklist file hashes.<br>• *Block*: block the malicious traffic.<br>• *Monitor*: log malicious traffic and allow it to pass inspection.<br>• *All*: use all malware block lists.<br>• *Specify*: select specific malware block lists.<br>See External malware block listand Malware hash threat feed for more details. |
| *Use EMS threat feed* | This option is available when at least one protocol is enabled for inspection and *AntiVirus scan* is enabled.<br>Enable to use malware threat feeds from FortiClient EMS. A FortiClient EMS Fabric connector with EMS threat feed enabled is required. See EMS threat feed for more details. |

# 2. Applying the Proxy-based Antivirus Profile to a firewall policy.

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




# 3. Verify the Configuration

Antivirus (AV) profiles can be tested using various file samples to confirm whether AV is correctly configured. In this topic, an AV profile is configured, applied to a firewall policy, and a user attempts to download sample virus test files hosted on eicar.org and fortiguard.com.

Different sample files are used to verify different features on the AV profile. The expectation is these files must be blocked by the AV profile, and the user should be presented with a block page.

| File | Test case |
|---|---|
| EICAR test file | A plain text EICAR test file (hosted on eicar.org over a HTTPS connection) to test basic AV scanning on the FortiGate using deep inspection. |
| AI sample file | A machine learning sample file to test AI-based malware detection on the FortiGate. |
| Virus outbreak (VO) sample file | A zero-day sample virus file to test the outbreak prevention feature of the AV profile. |
| Behavioral-based samples | Files that are detected by a sandbox. This requires FortiSandbox integration with the FortiGate. |

https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/315155/testing-an-antivirus-profile

### Example 1: EICAR test file

**EICAR hosts anti-malware test files, which are available to download from https://www.eicar.org/download-anti-malware-testfile.**

### Example 2: AI sample file

**FortiGuard provides several sample files to test the AV configuration on the FortiGate, which are available to download from**
https://www.fortiguard.com/sample-files**.**

### Example 3: VO sample file

**To test the AV profile with the VO sample file:**

1- **On the PC, go to the FortiGuard website and download the VO Sample file.**
2- **The download attempt is blocked by the FortiGate's default AV profile, and a block page appears in the PC's browser.**

## 4. Monitor Antivirus Protection

## * Note that:

Starting from 6.4.0, the scan mode option is no longer available for **flow-based** AV.
This means that AV no longer exclusively uses the default or legacy scan modes when handling traffic on flow-based firewall policies. Instead, AV in flow-based policies uses a hybrid of the two scan modes.
In contrast, **proxy mode** maintains the scan mode option, which can be toggled between default or legacy mode.

- **To configure the scan mode:**

```
config antivirus profile
    edit <name>
        set feature-set proxy
        set scan-mode {default | legacy}
    next
end
```

| | |
|---|---|
| **default** | Enable stream-based scanning (default). |
| **legacy** | Disable stream-based scanning. |

## After choosing Proxy-based:

- **You can use “Client Comforting” in this mode**
- **You can use “stream-based scanning” in this mode**
- **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 highrisk files.**

# Protocol comparison between antivirus inspection modes

| | HTTP | FTP | IMAP | POP3 | SMTP | NNTP | MAPI | CIFS | SSH |
|---|---|---|---|---|---|---|---|---|---|
| Proxy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes* | Yes |
| Flow | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No |

# Feature comparison between Antivirus inspection modes

## Feature comparison between Antivirus inspection modes

The following table indicates which Antivirus features are supported by their designated scan modes.

| Part1 | Replacement Message | Content Disarm | Mobile Malware | Virus Outbreak | Sandbox Post-Transfer Scanning | Sandbox Inline Scanning | NAC Quarantine |
|---|---|---|---|---|---|---|---|
| Proxy | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Flow | Yes* | No | Yes | Yes | Yes | No | Yes |

*IPS Engine caches the URL and a replacement message is presented after the second attempt.

| Part 2 | Archive Blocking | Emulator | Client Comforting | Infection Quarantine | Heuristics | Treat EXE as Virus |
|---|---|---|---|---|---|---|
| Proxy | Yes | Yes | Yes | Yes (1) | Yes | Yes (2) |
| Flow | Yes | Yes | No | Yes | Yes | Yes (2) |

1. Only available on FortiGate models with HDD or when FortiAnalyzer or FortiGate Cloud is connected and enabled.
2. Only applies to inspection on IMAP, POP3, SMTP, and MAPI protocols.

| Part 3 | External Blocklist | EMS Threat Feed | AI/ML Based Detection | FortiNDR Inline Detection |
|---|---|---|---|---|
| Proxy | Yes | Yes | Yes | Yes |
| Flow | Yes | Yes | Yes | No |

# Inspection Mode Use Cases

## Databases:

**The antivirus scanning engine uses a virus signatures database to record the unique attributes of each infection. The antivirus scan searches for these signatures and when one is discovered, the FortiGate determines if the file is infected and takes action.**

**All FortiGates have the normal antivirus signature database. Some models have additional databases that you can use. The database you use depends on your network and security needs, and on your FortiGate model.**

**The extended virus definitions database is the default setting and provides comprehensive antivirus protection. Entry-level and some mid-range FortiGates cannot support the extreme database. The FortiGate 300D is the lowest model that supports the extreme database. All VMs support the extreme database.**

| | |
|---|---|
| Extended | This is the default setting. This database includes currently spreading viruses, as determined by the FortiGuard Global Security Research Team, plus recent viruses that are no longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared. |
| Extreme | This includes the extended database, plus a large collection of zoo viruses. These are viruses that have not spread in a long time and are largely dormant. Some zoo viruses might rely on operating systems and hardware that are no longer widely used. |

### To change the antivirus database:

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

**Regardless of which mode you use, both use the full antivirus database (extended or extreme— depending on the CLI command use-extremedb 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.**

### Flow inspection mode:

**Priority on Traffic Throughput**

### Proxy inspection mode:

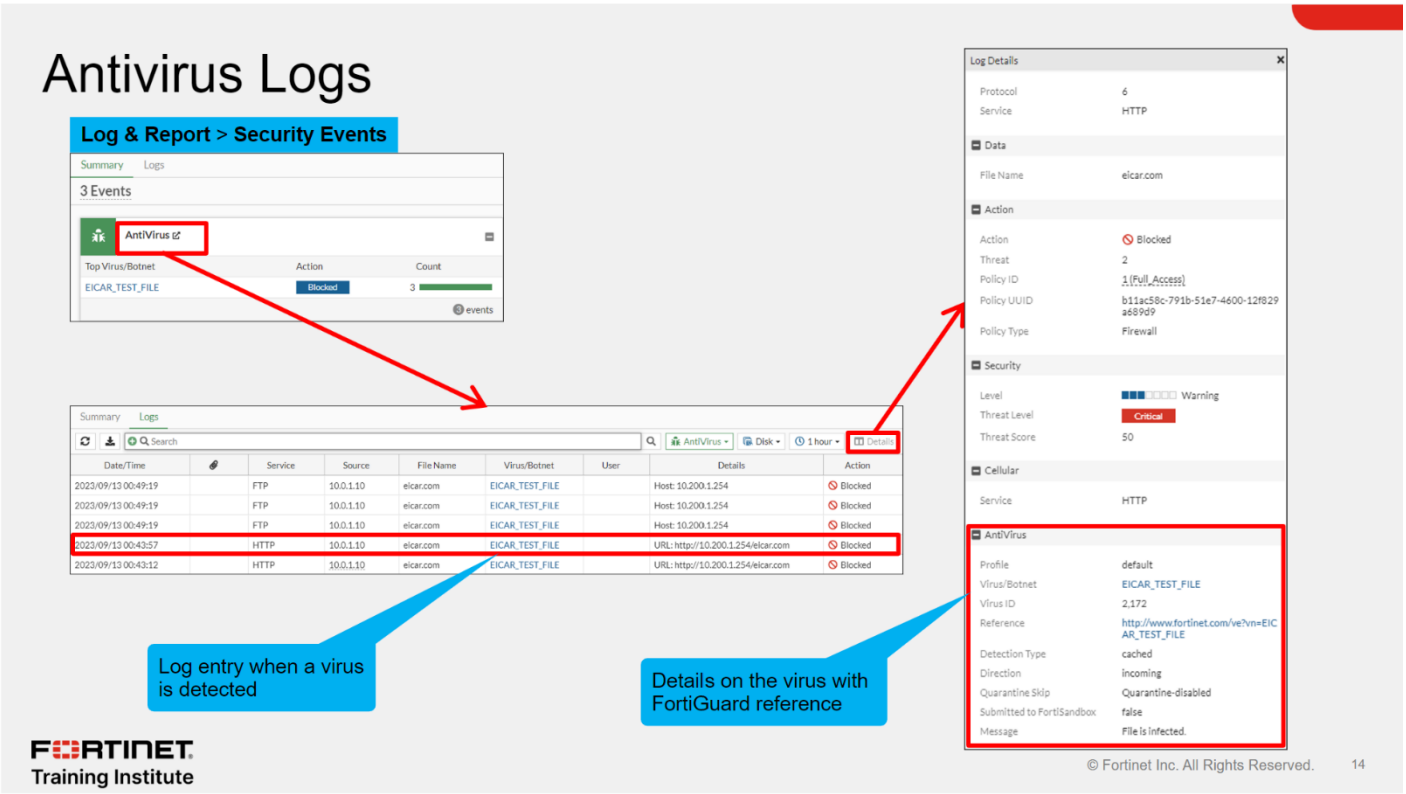
**Priority on Network Security**

# Antivirus Logs

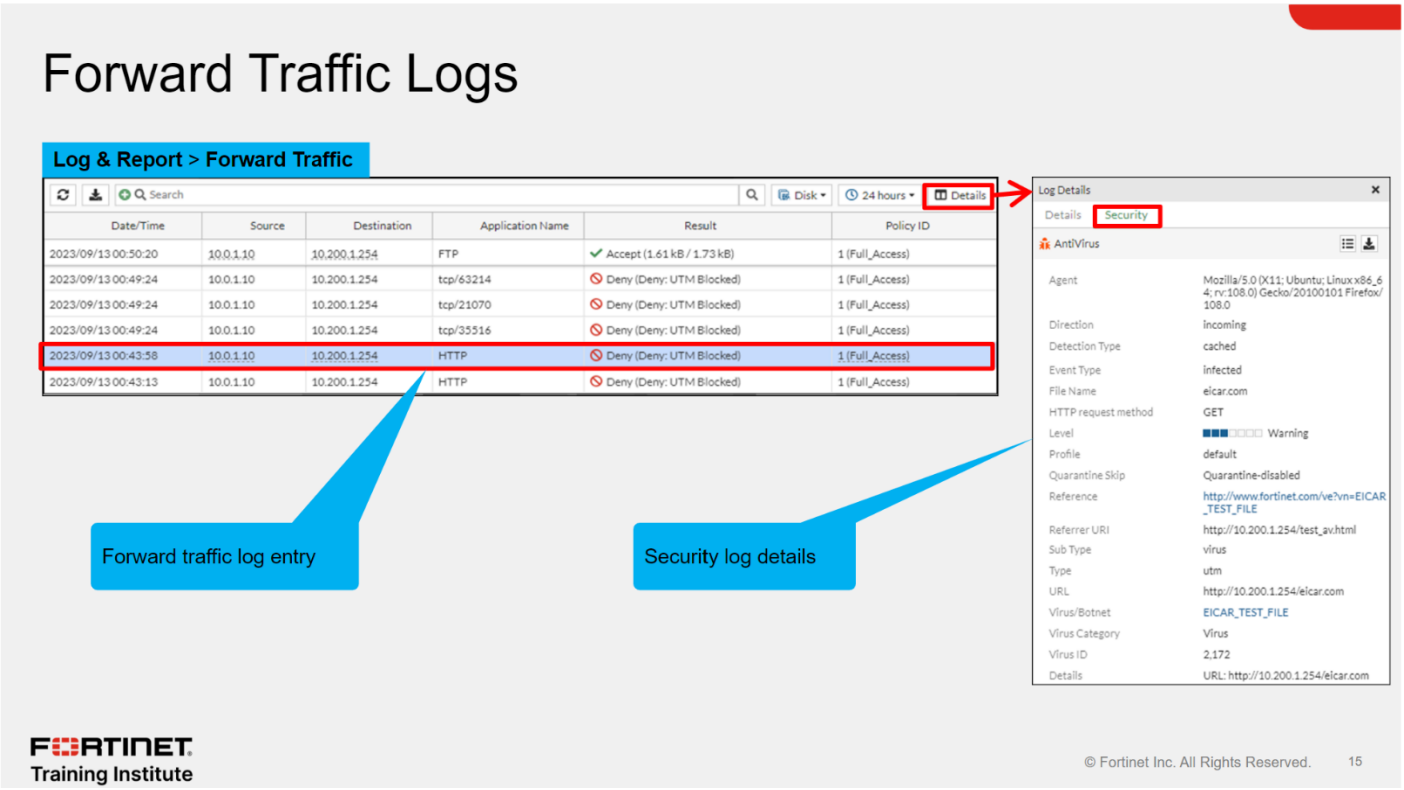
Logging is an important part of managing a secure network. When you enable logging, you can find details on Two ways:

**1.** **Log & Report** > **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.

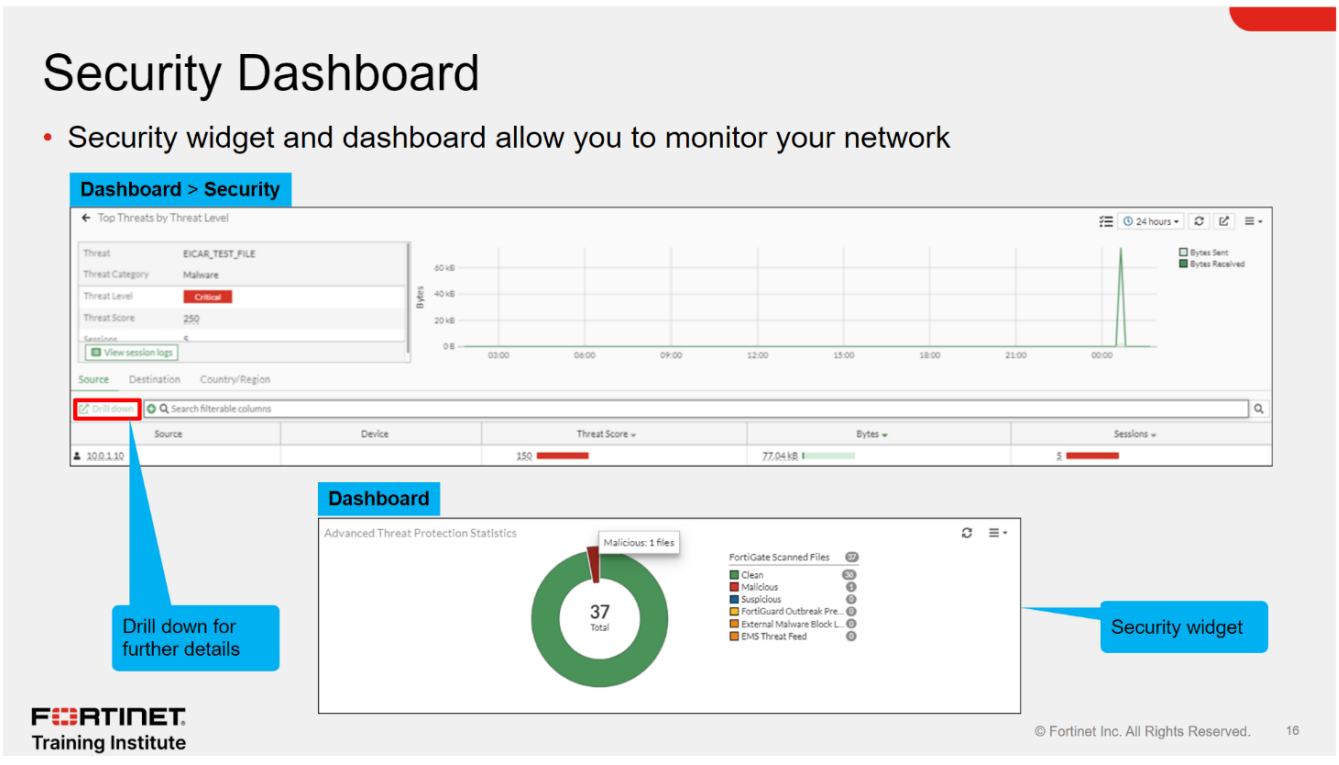
When you enable oversized files logging, a log entry is also created with the details including the message “Size limit is exceeded”.




**2.** **Log & Report** > **Forward Traffic**. 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.




**3.** **Dashboard** > **Security**. 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

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`**.

```
FGT # execute update-av
```

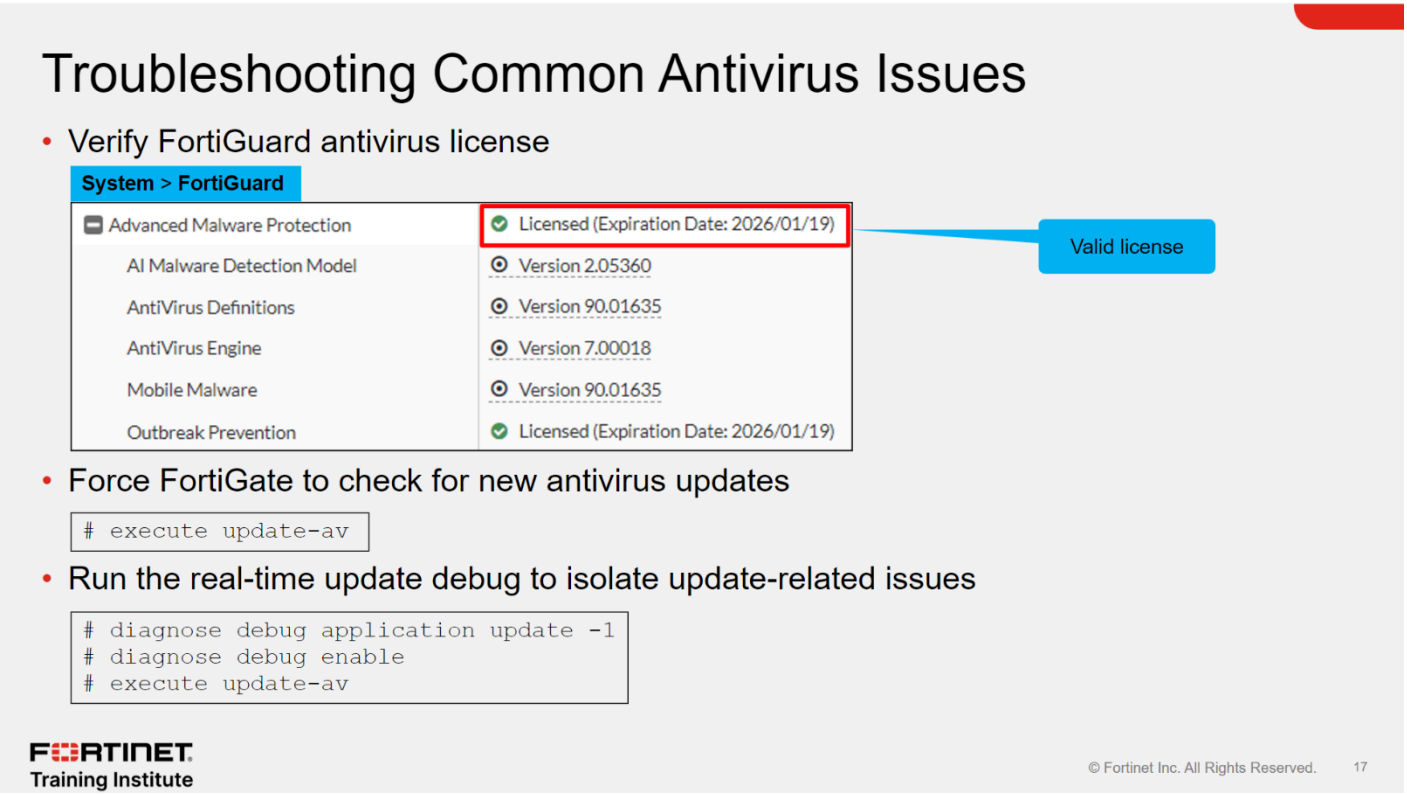
**1.** If you are having issues with the antivirus license or FortiGuard updates, start troubleshooting with basic connectivity tests. Most of the time, issues related to updates are caused by connectivity problems with FortiGuard servers. You can do the following to handle common antivirus issues:

• 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.

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

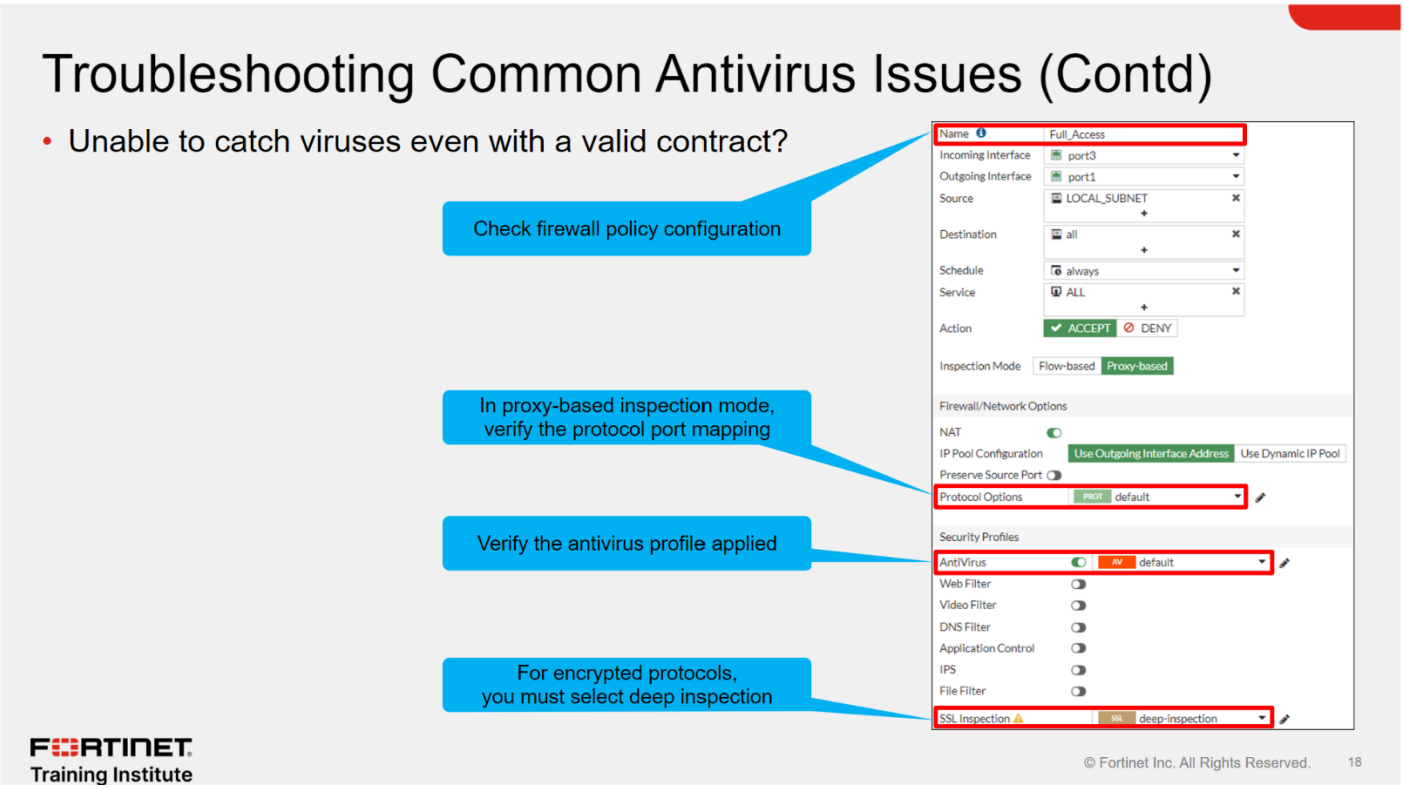



**2.** What if you have a valid connection and updated database, and you are still having issues catching viruses? Start troubleshooting for basic configuration errors. Most of the time, issues are caused by misconfiguration on the device. You can do the following to verify:

• 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. (For encrypted protocols, you must select **deep inspection**)




**3.** 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.

# 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