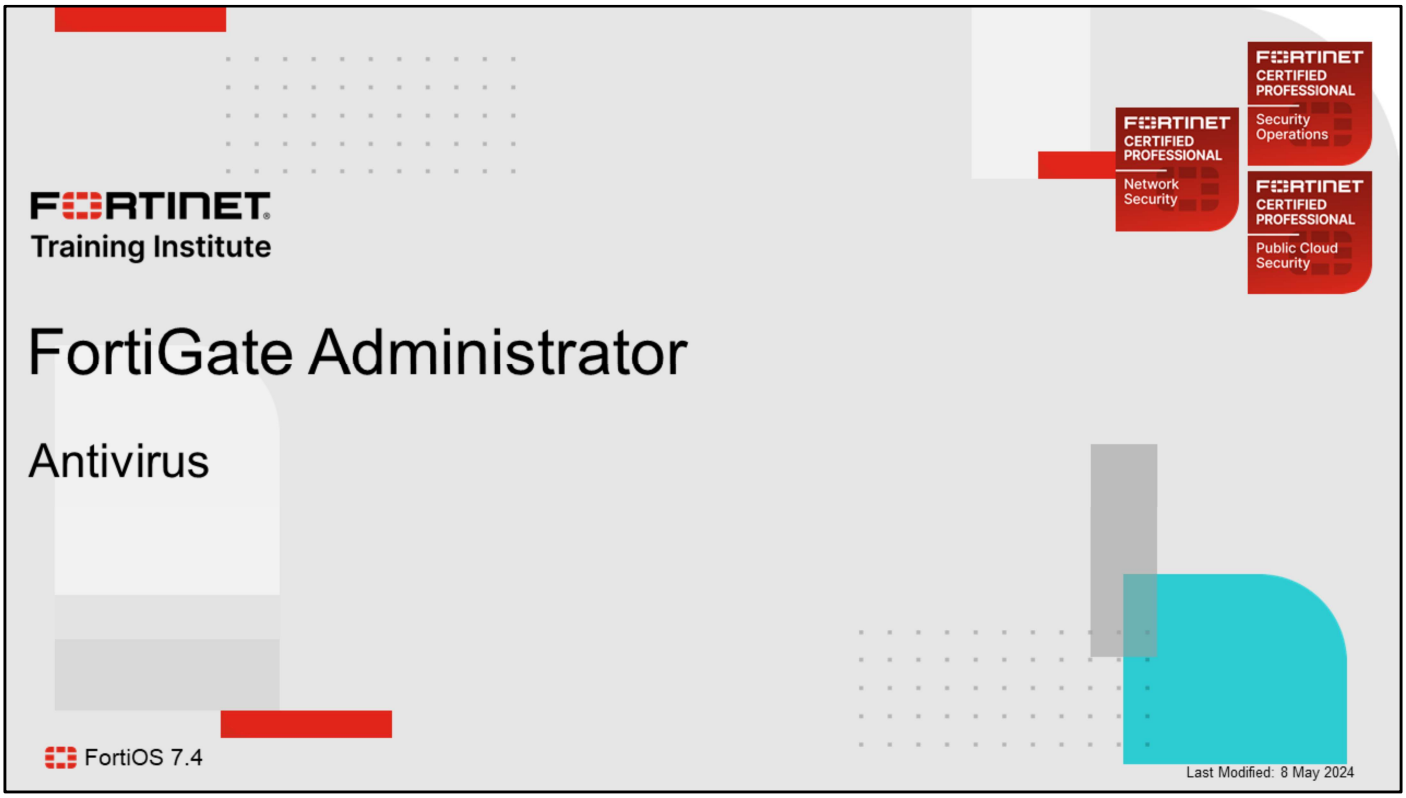


In this lesson, you will learn how to use FortiGate to protect your network against viruses.

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

FORTINET Training Institute

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

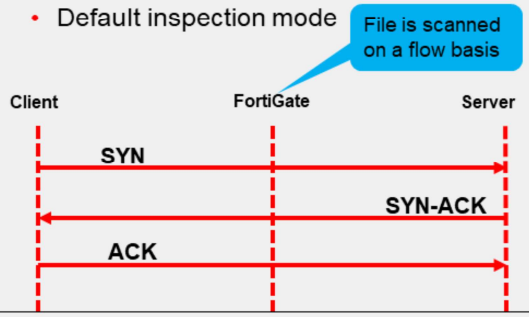
By demonstrating competence in antivirus configuration, including reviewing antivirus logs, you will be able to use the antivirus profile effectively.

Antivirus and Inspection Modes

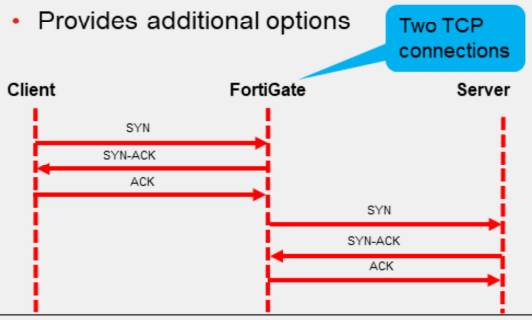
- Antivirus scanning engine uses antivirus signature databases to identify malicious codes

- Available inspection modes

- Flow-based inspection
  - Default inspection mode



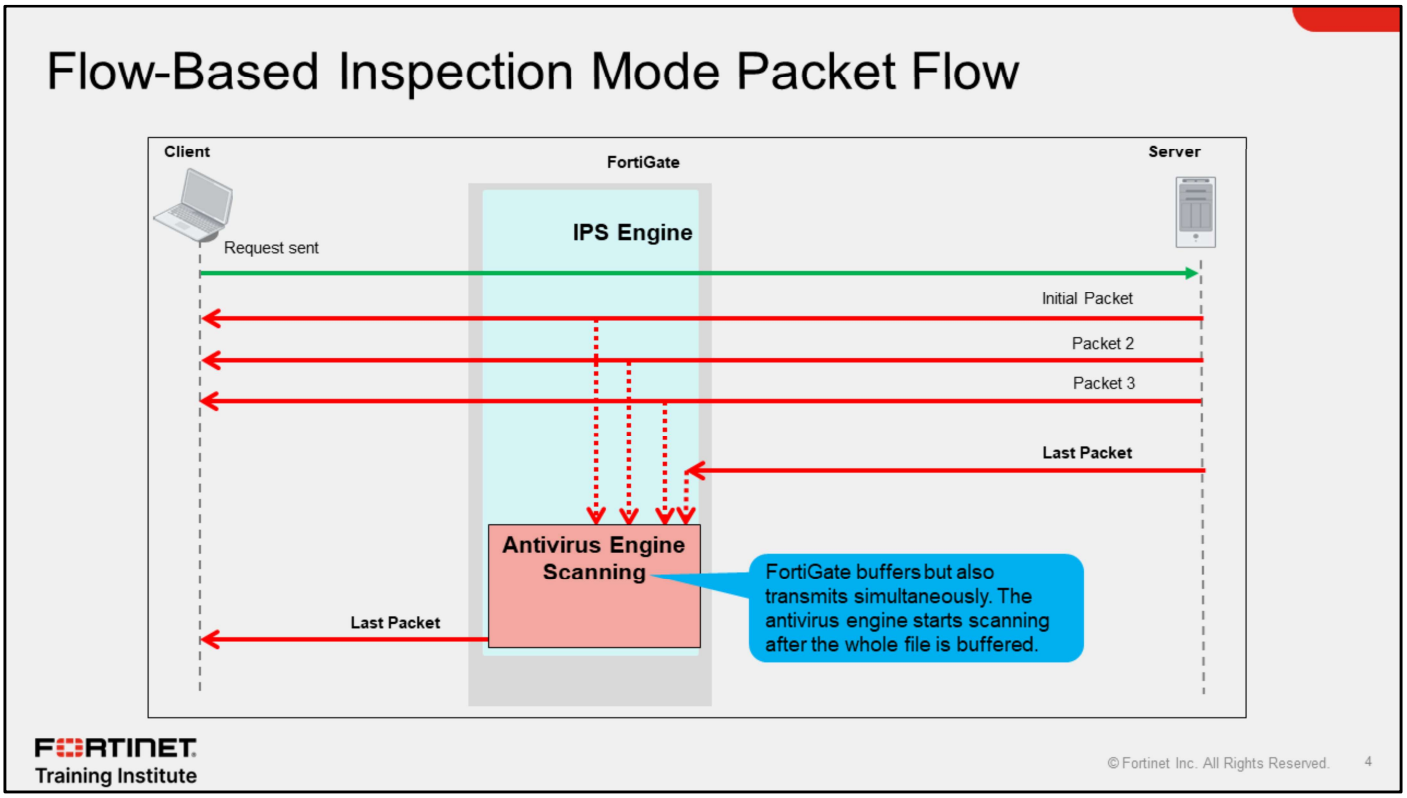
- Proxy-based inspection
  - Provides additional options



FORTINET Training Institute

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

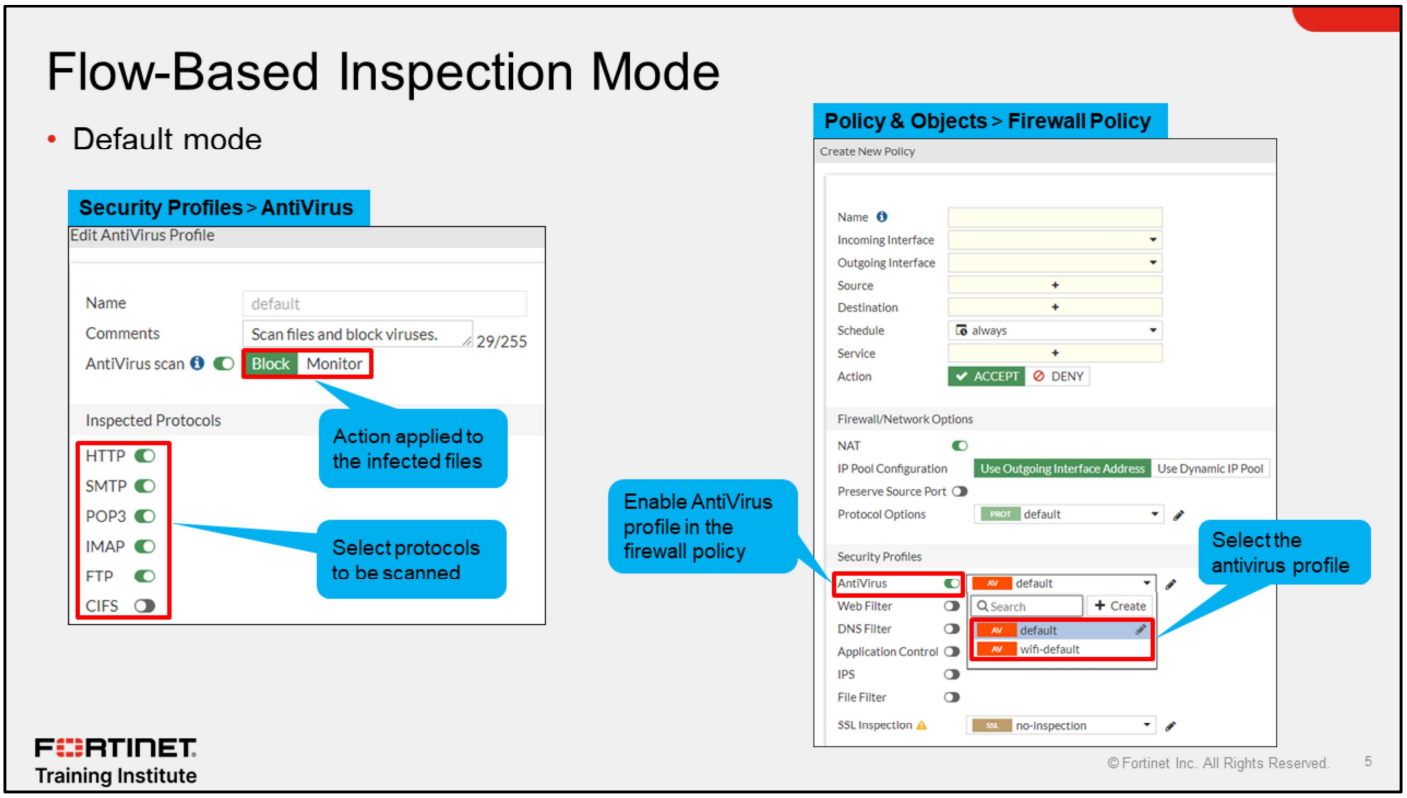
Antivirus can operate in flow-based or proxy-based inspection mode.



Flow-based inspection mode 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.

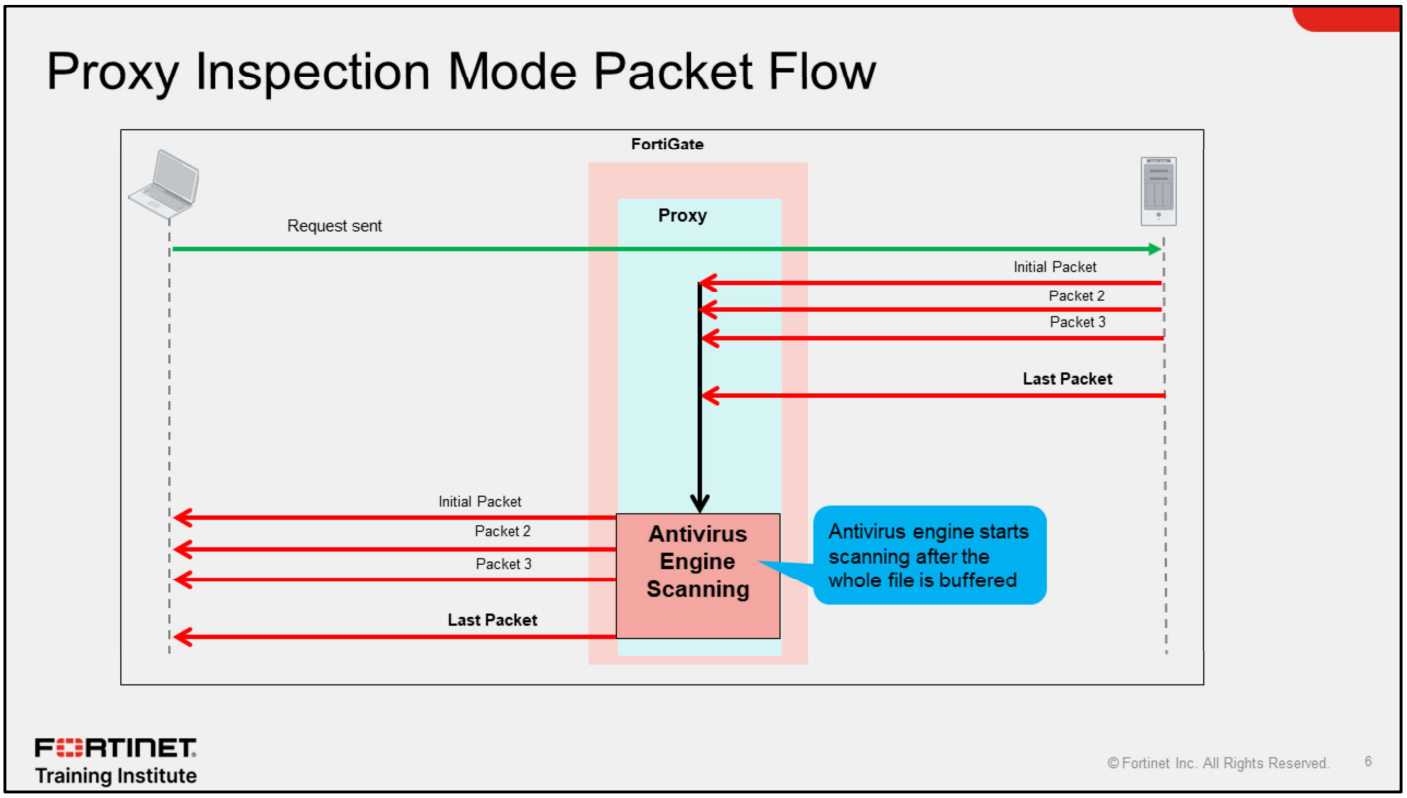
This slide shows that the client sends a request and starts receiving packets immediately, but FortiGate also caches those packets at the same time. When the last packet arrives, FortiGate caches it and puts it on hold. Then, the IPS engine extracts the payload of the last packet, assembles the whole 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 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.

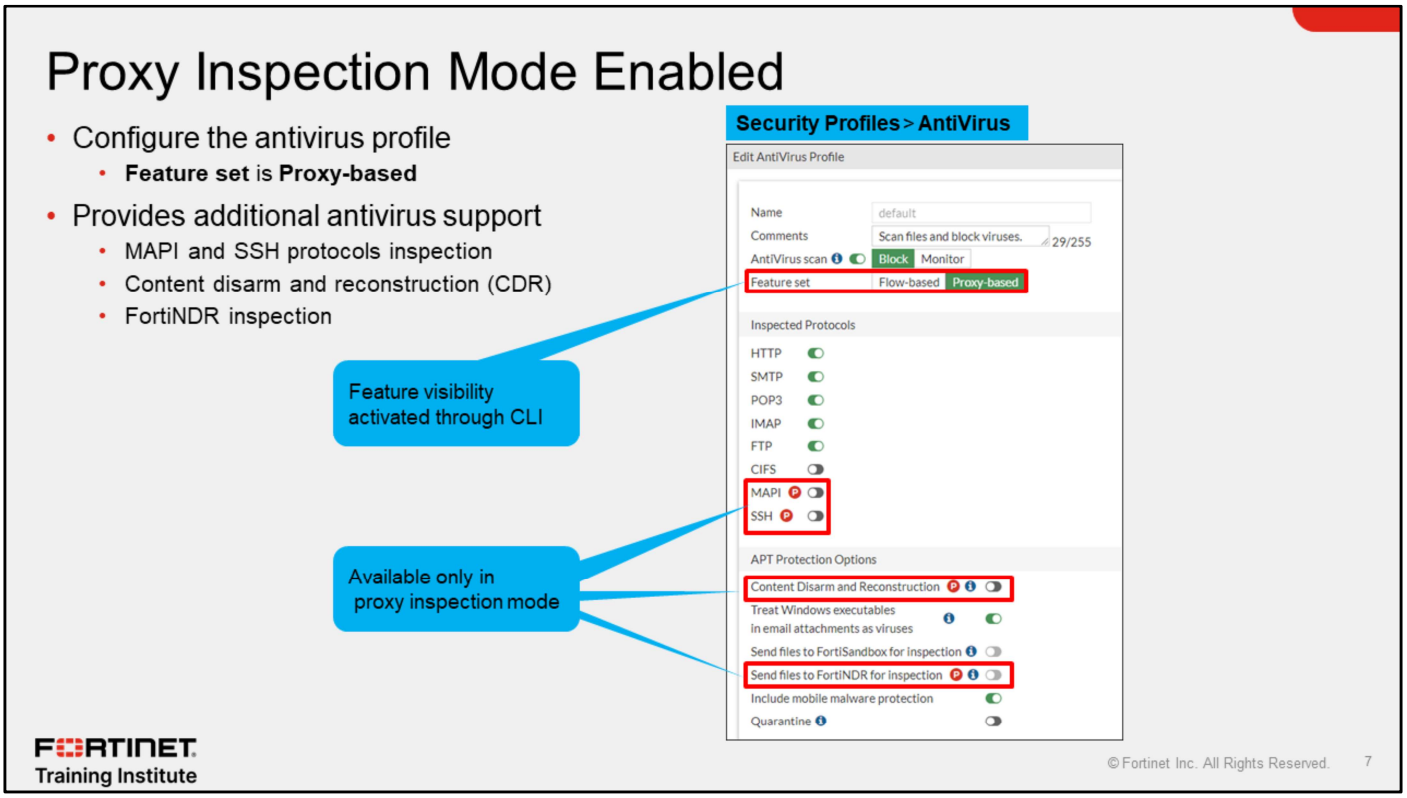


With a proxy inspection mode scan, the client sends a request and FortiGate starts buffering the whole file, then sends it to the antivirus engine for scanning. If the file is clean (without any viruses), FortiGate starts transmitting the file to the end client. If a virus is found, no packets are delivered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

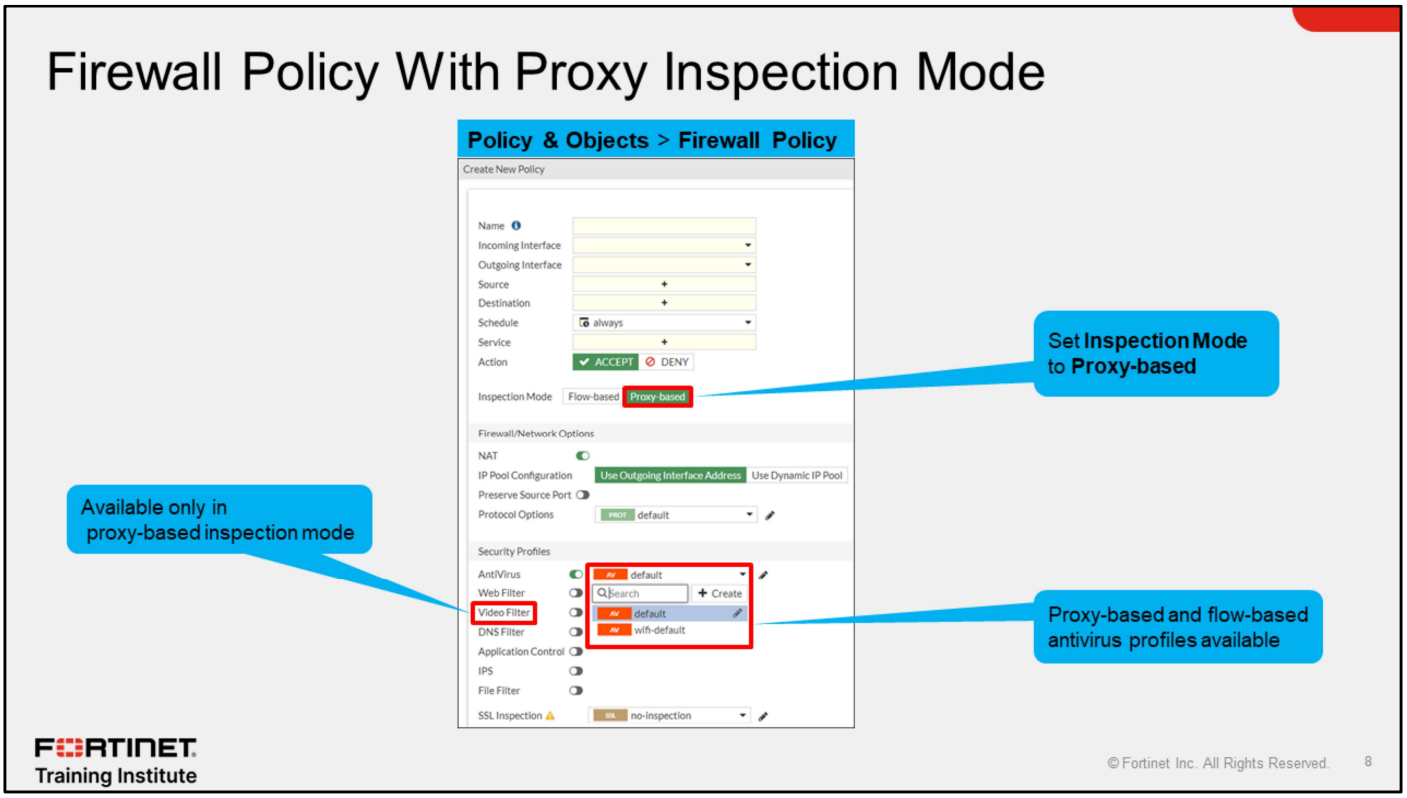
You can configure client comforting for HTTP and FTP from the `config firewall profile-protocol-options` command tree. This allows the proxy to slowly transmit some data until it can complete the buffer and finish the scan. This prevents a connection or session timeout. No block replacement message appears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

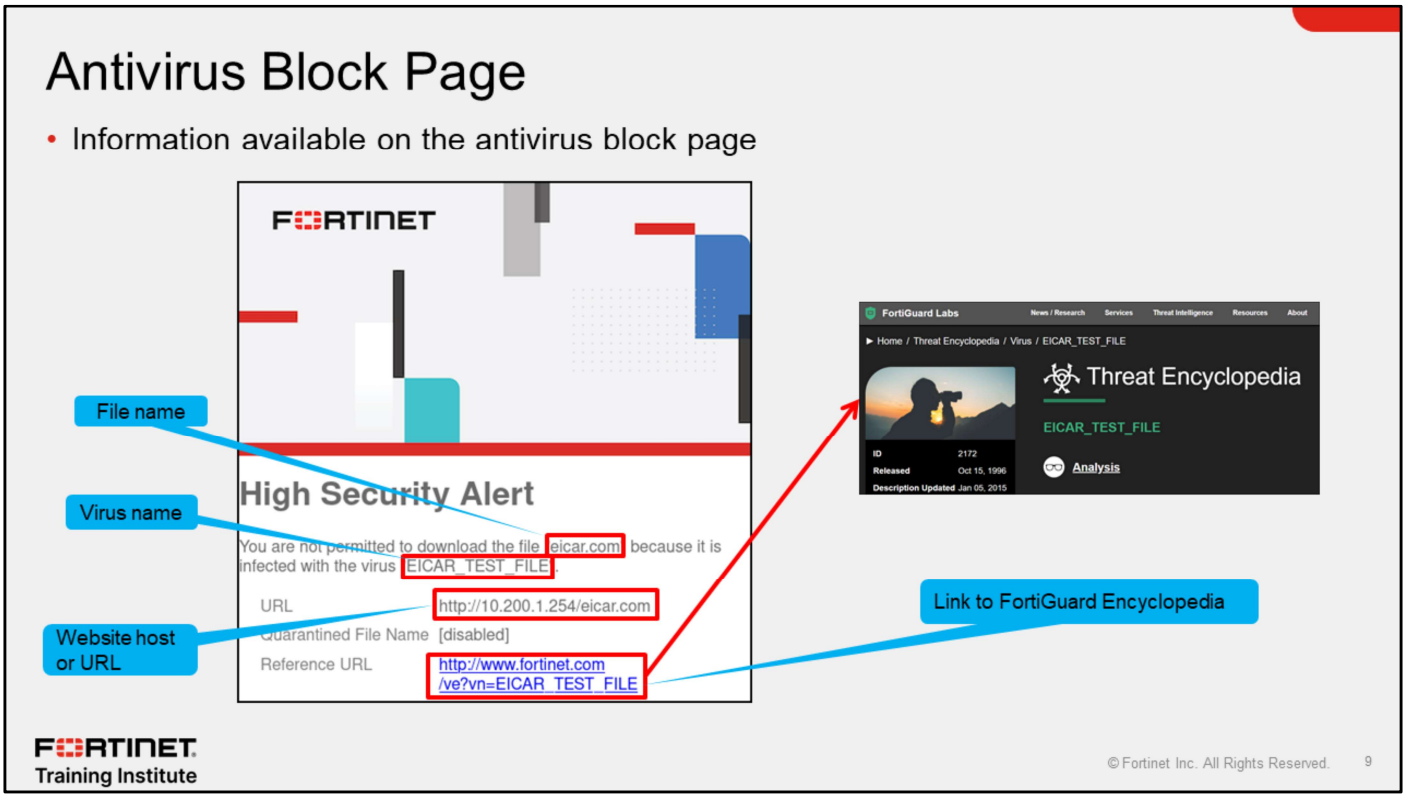


Proxy-based inspection mode is applied when you set **Feature set** to **Proxy-based**. For low-end platforms, this feature is available on the GUI when you enable the CLI command `gui-proxy-inspection`.

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.



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



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.

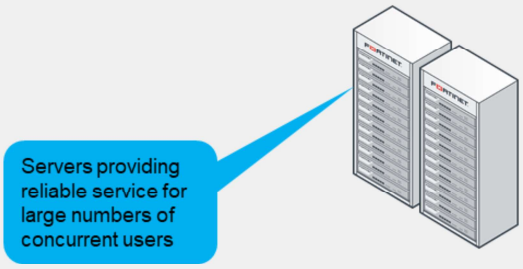
The block page includes the following:
- File name
- Virus name
- Website host and URL
- User name and group (if authentication is enabled)
- Link to FortiGuard Encyclopedia—which provides analysis, recommended actions (if any), and detection availability

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.

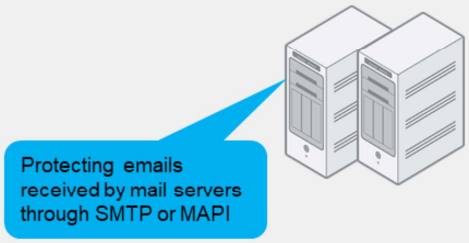
Inspection Modes Use Cases

- Both use the full antivirus database

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



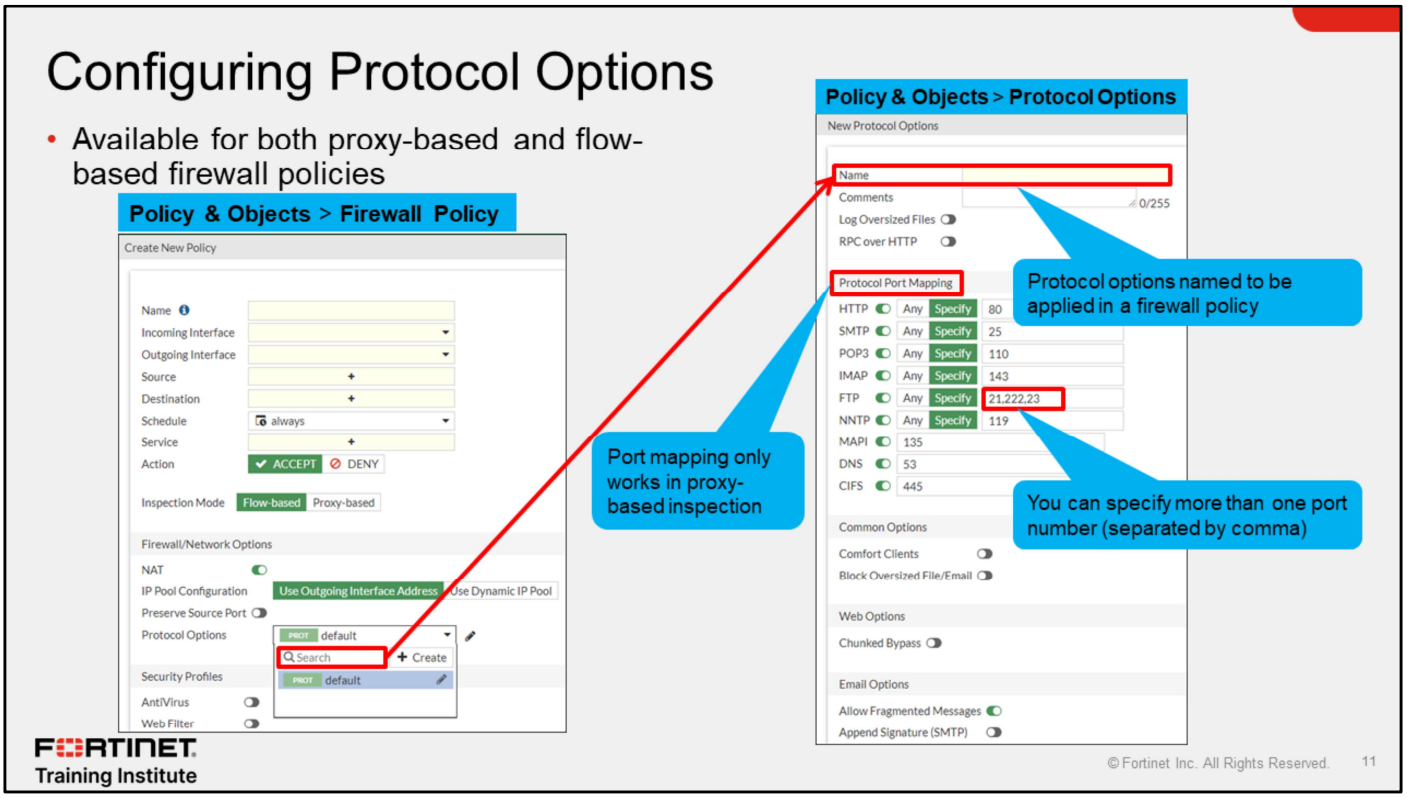
- Proxy inspection mode
  - Required for its additional options
  - Priority on network security



FORTINET Training Institute

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?

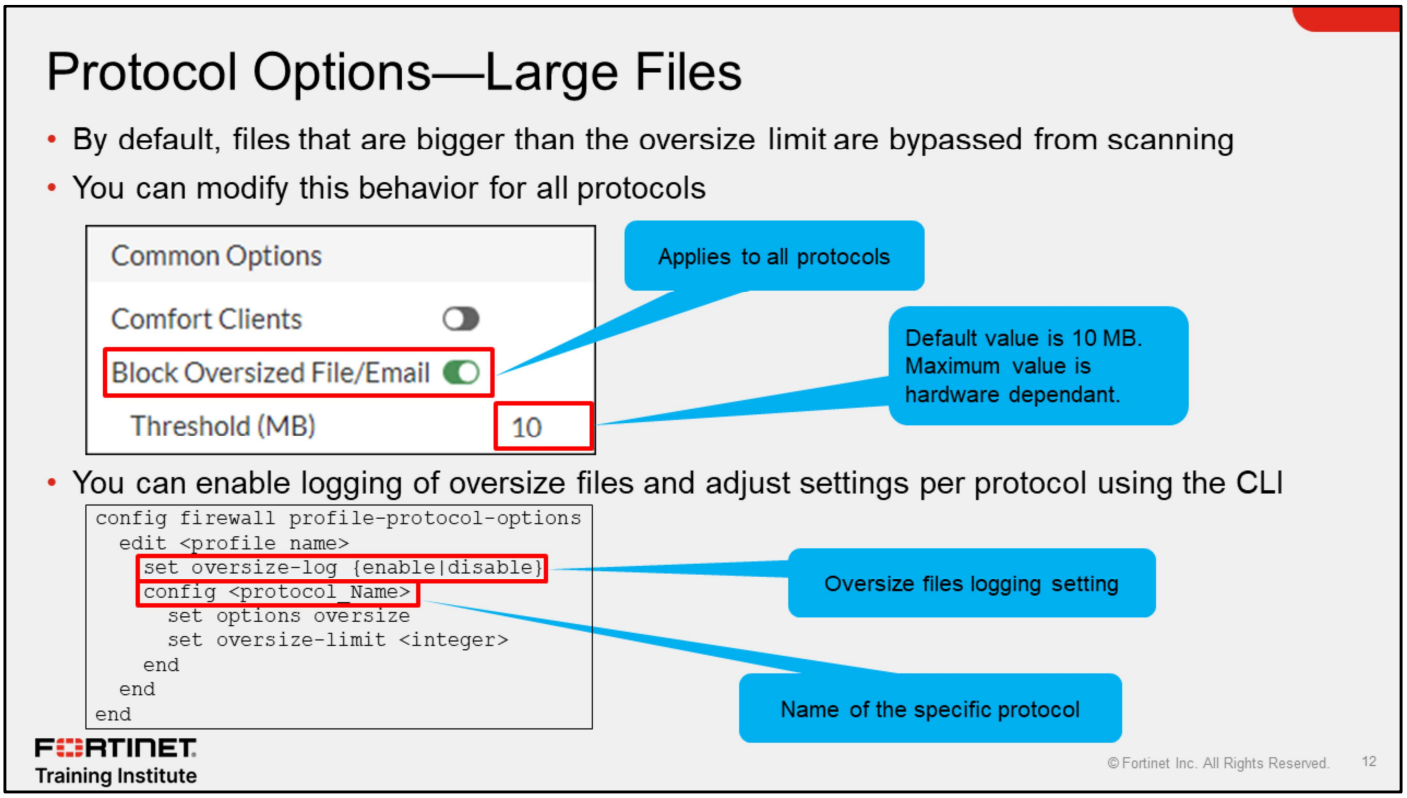
If security is your priority, proxy inspection mode—with client comforting disabled—is more appropriate. If performance is your top priority, then flow inspection mode is more appropriate. Depending on the FortiGate model, flow-based pattern matching can be offloaded to CP8 or CP9 processors, and FortiGate 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.



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.



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
end
```

Oversize limit specific to decompressed files

Nested archive limit

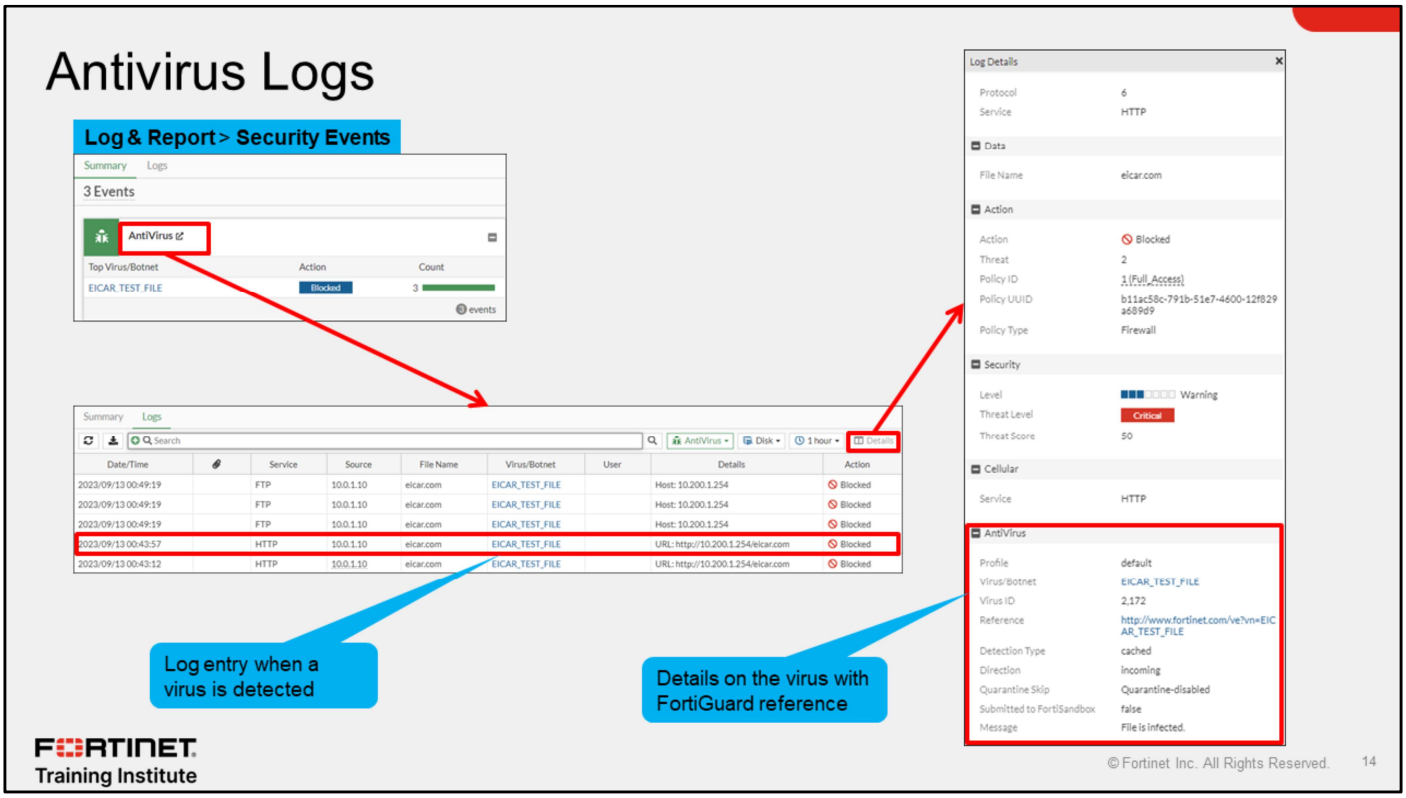
FORTINET Training Institute

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.

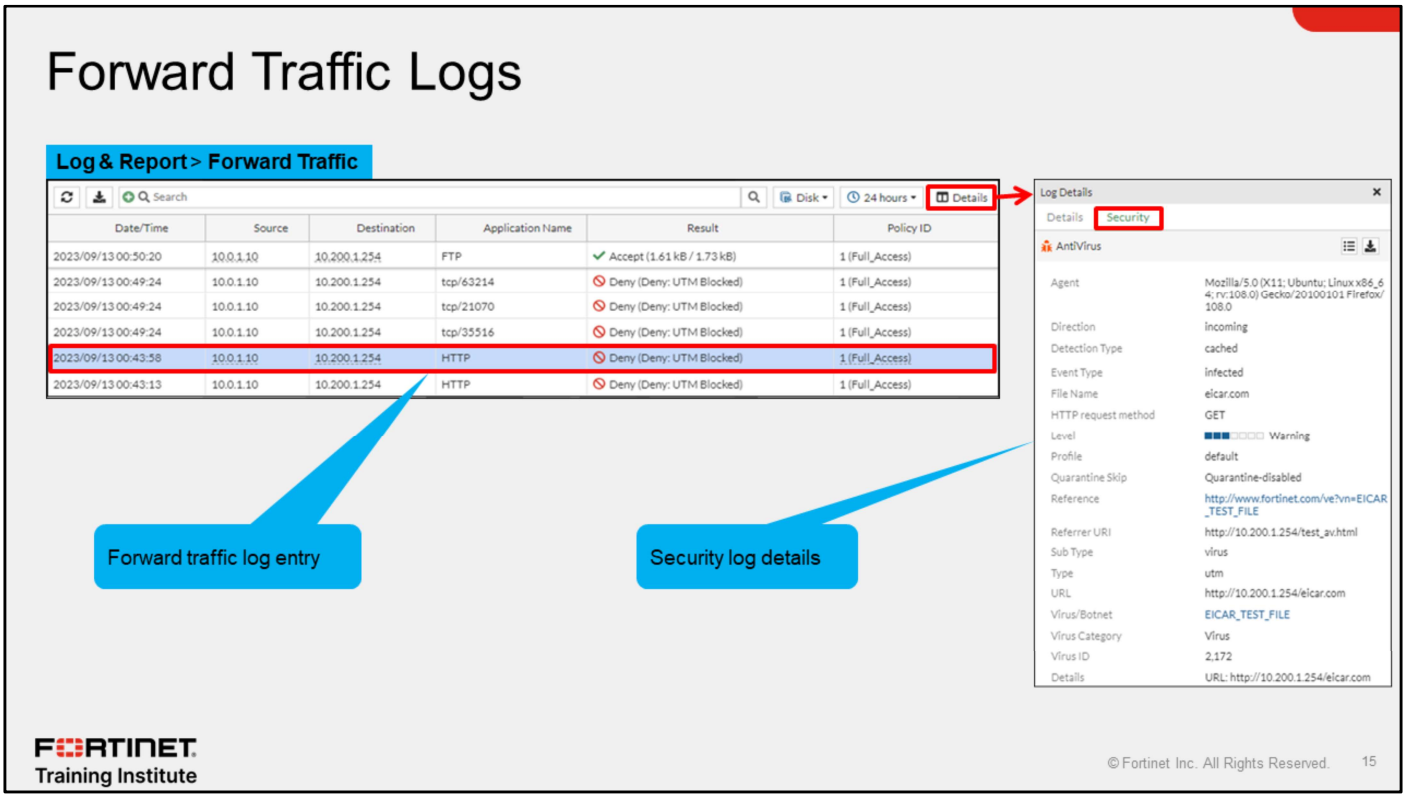
If an archive is nested—for example, if an attacker is trying to circumvent your scans by putting a ZIP file inside the ZIP file—FortiGate will try to undo all layers of compression. By default, FortiGate will attempt to decompress and scan up to 12 layers deep, but you can configure it to scan up to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



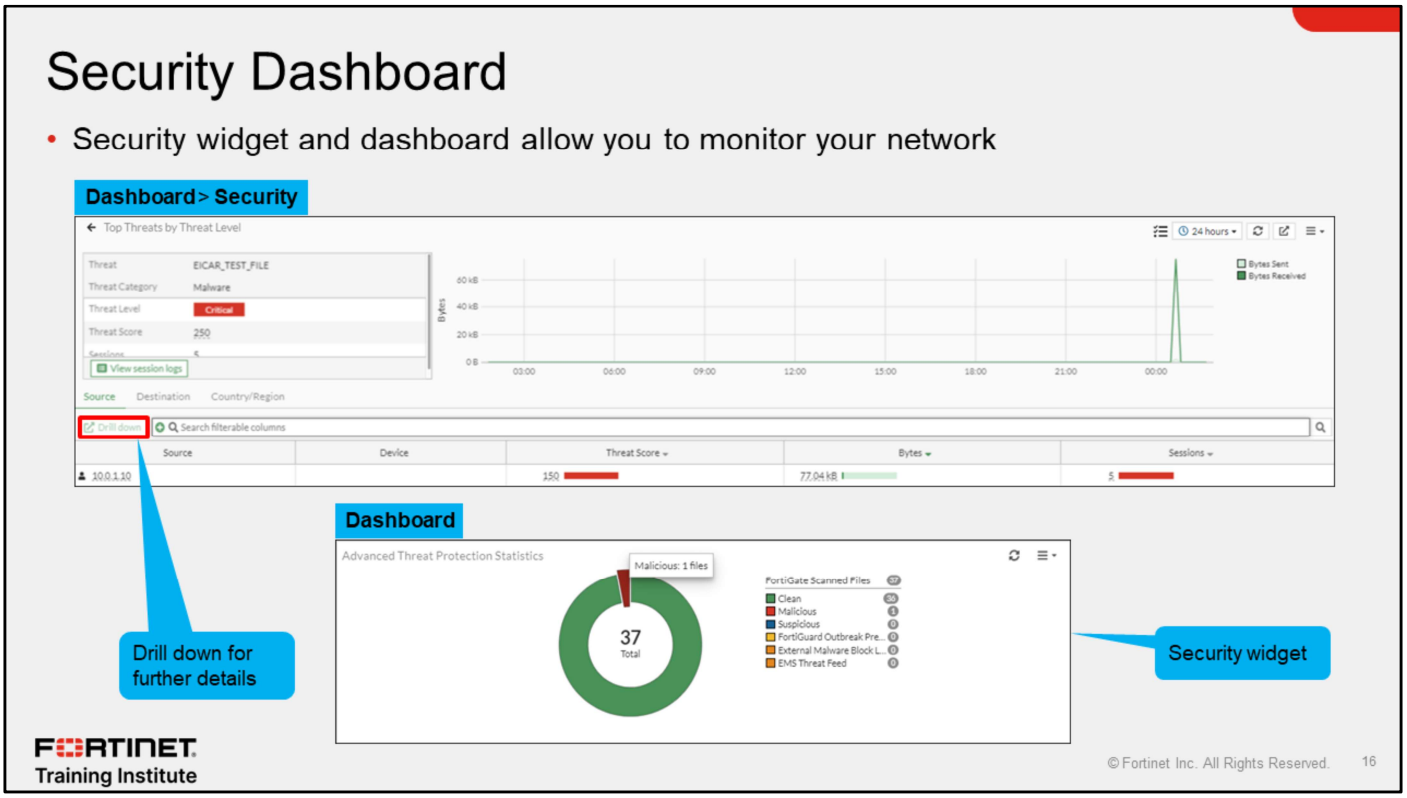
Logging is an important part of managing a secure network. When you enable logging, you can find details on the **AntiVirus** log page under **Security Events**.

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”.

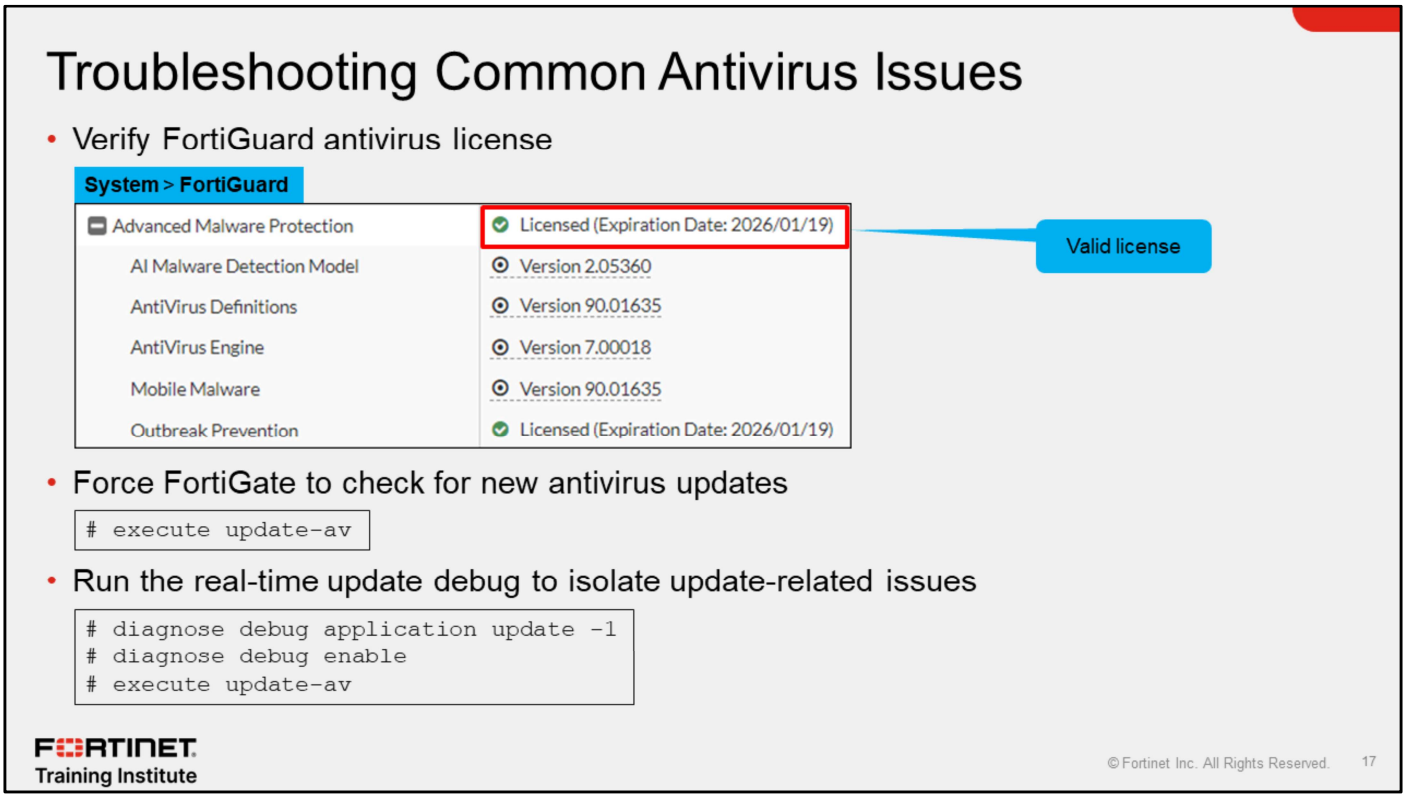


You can also view log details on the **Forward Traffic** log page, where firewall policies record traffic activity. You'll find a summary of the traffic on which FortiGate applied an antivirus action in the corresponding security details.



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.

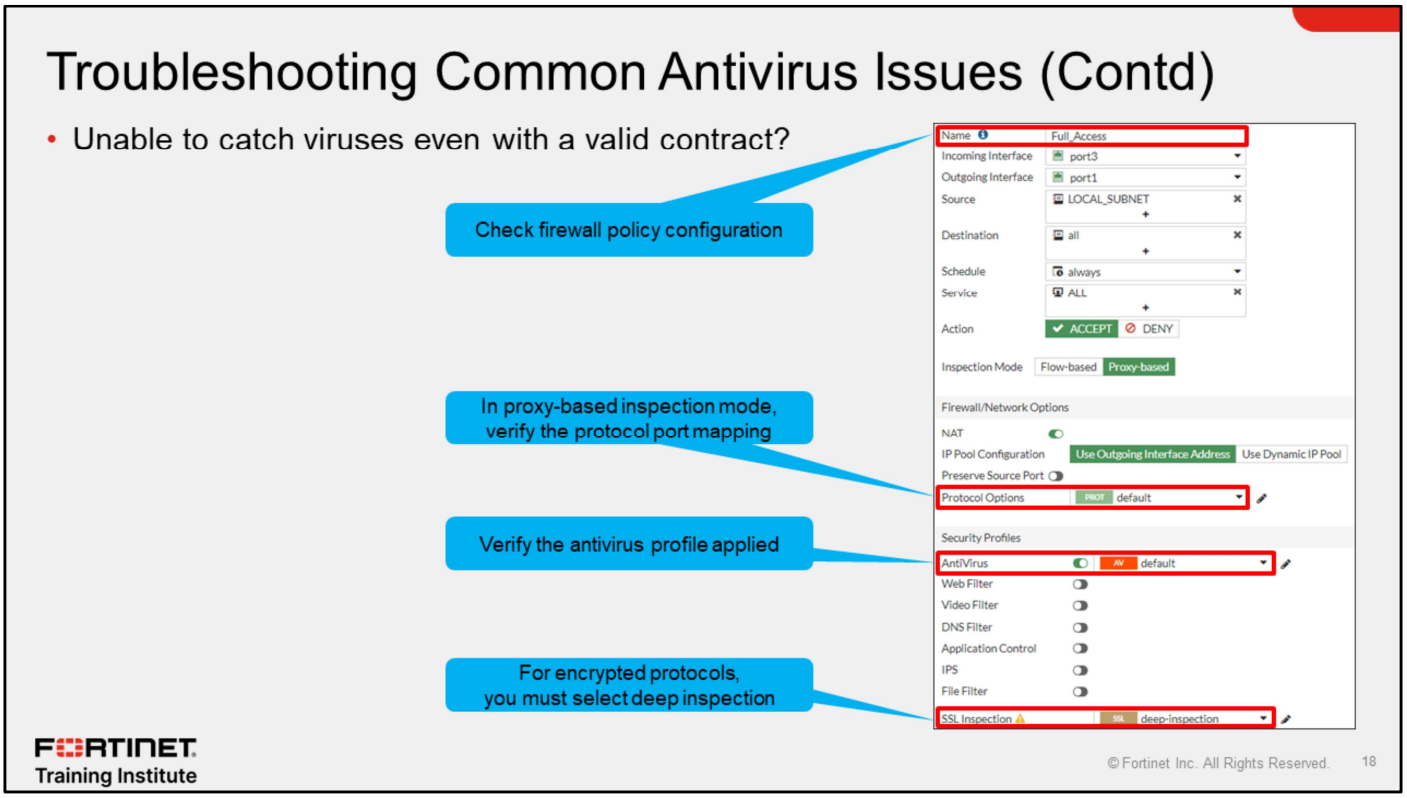
For the **Advanced Threat Protection Statistics**, you can add the corresponding widget on the dashboard for monitoring purposes.



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`.

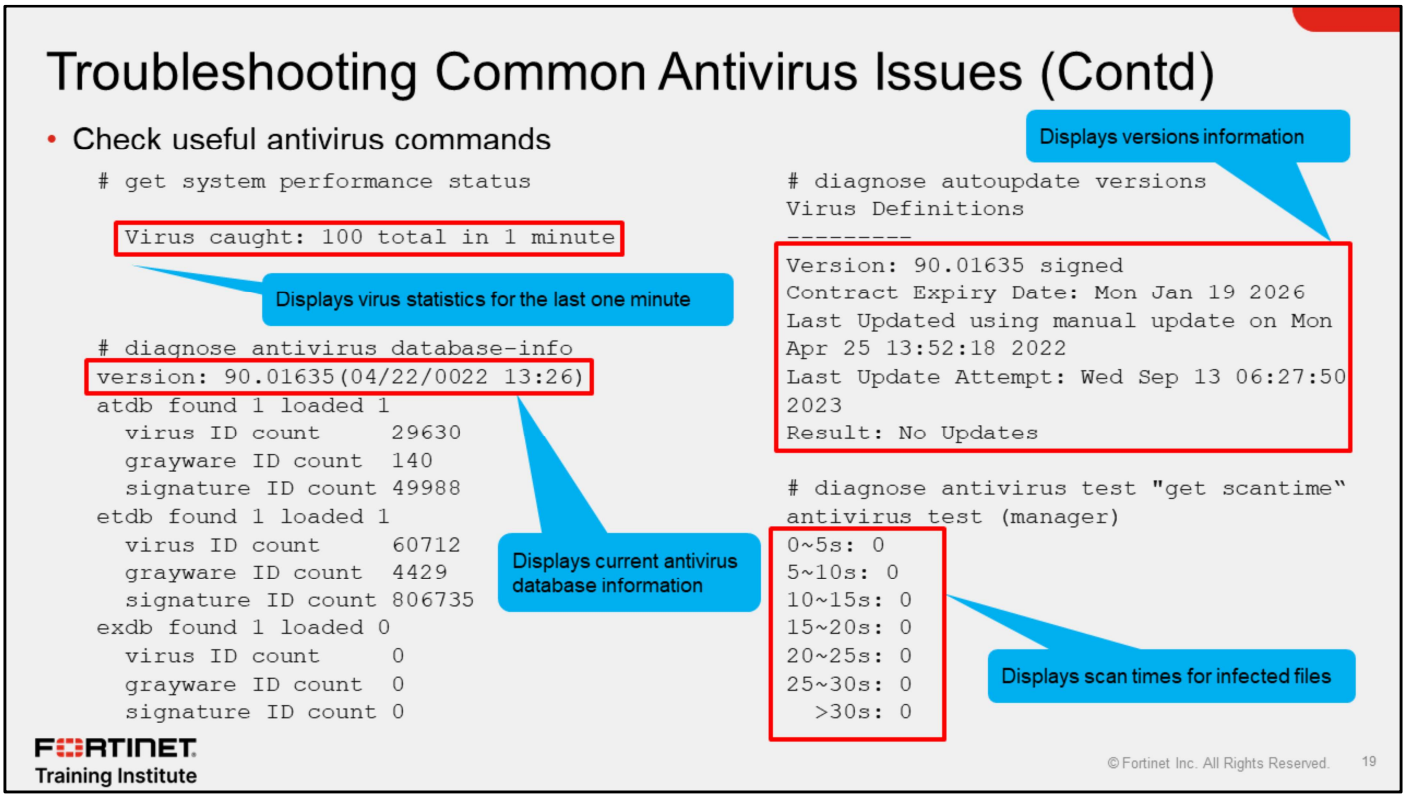
If you are having issues with the antivirus license or FortiGuard updates, start troubleshooting with basic connectivity tests. Most of the time, issues related to updates are caused by connectivity problems with FortiGuard servers. You can do the following to handle common antivirus issues:

- 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.



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.



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

FORTINET Training Institute

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.