FORTINET CERTIFIED PROFESSIONAL Security Operations

FORTINET CERTIFIED PROFESSIONAL Network Security

FORTINET CERTIFIED PROFESSIONAL Public Cloud Security

FORTINET Training Institute

FortiGate Administrator

Antivirus

FortiOS 7.4

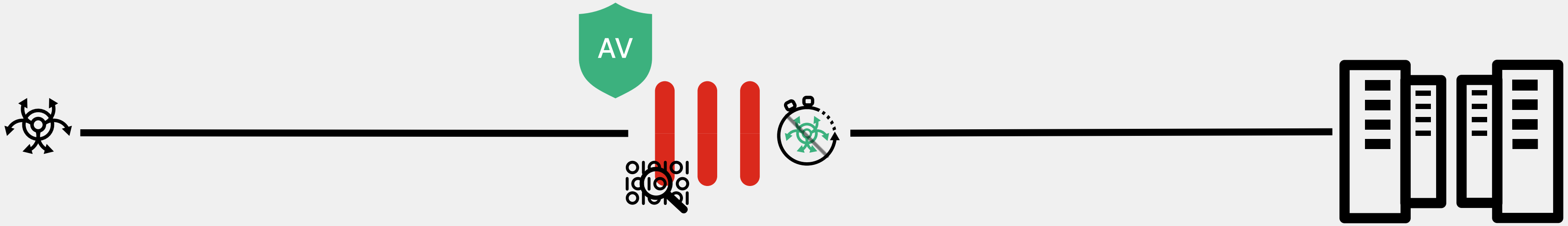
Last Modified: 18 April 2025

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

Antivirus and Inspection Modes

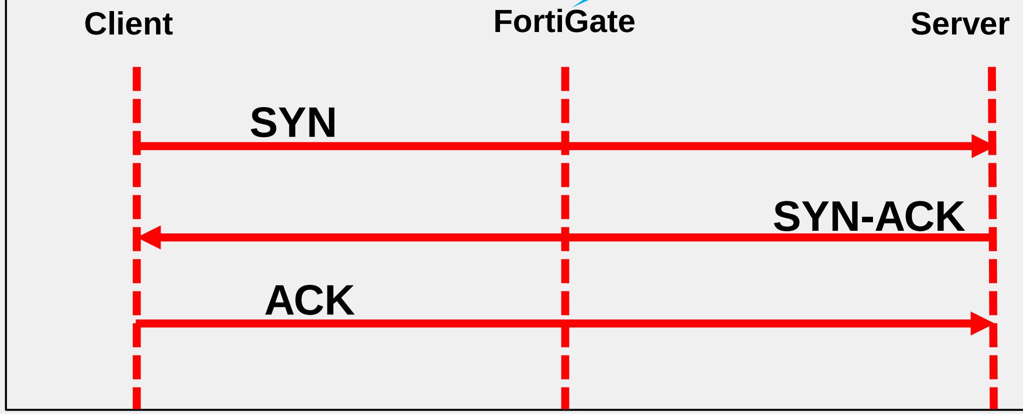
- Antivirus scanning engine uses antivirus signature databases to identify malicious codes



- Available inspection modes

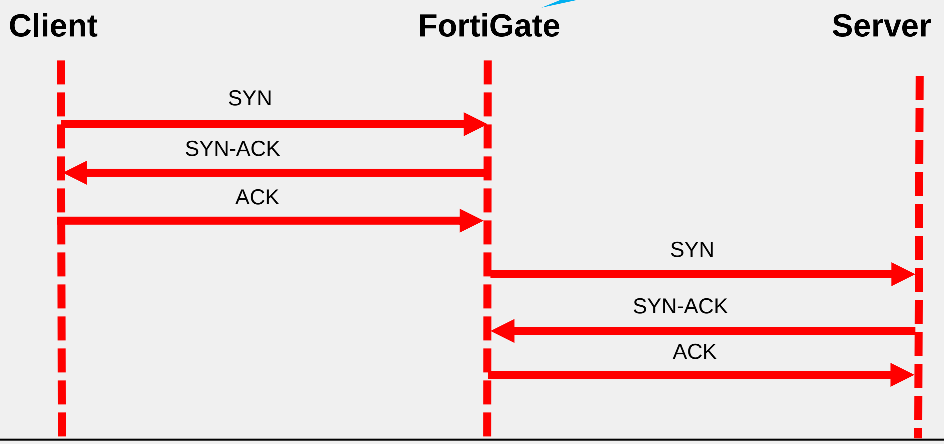
- Flow-based inspection
  - Default inspection mode

File is scanned on a flow basis

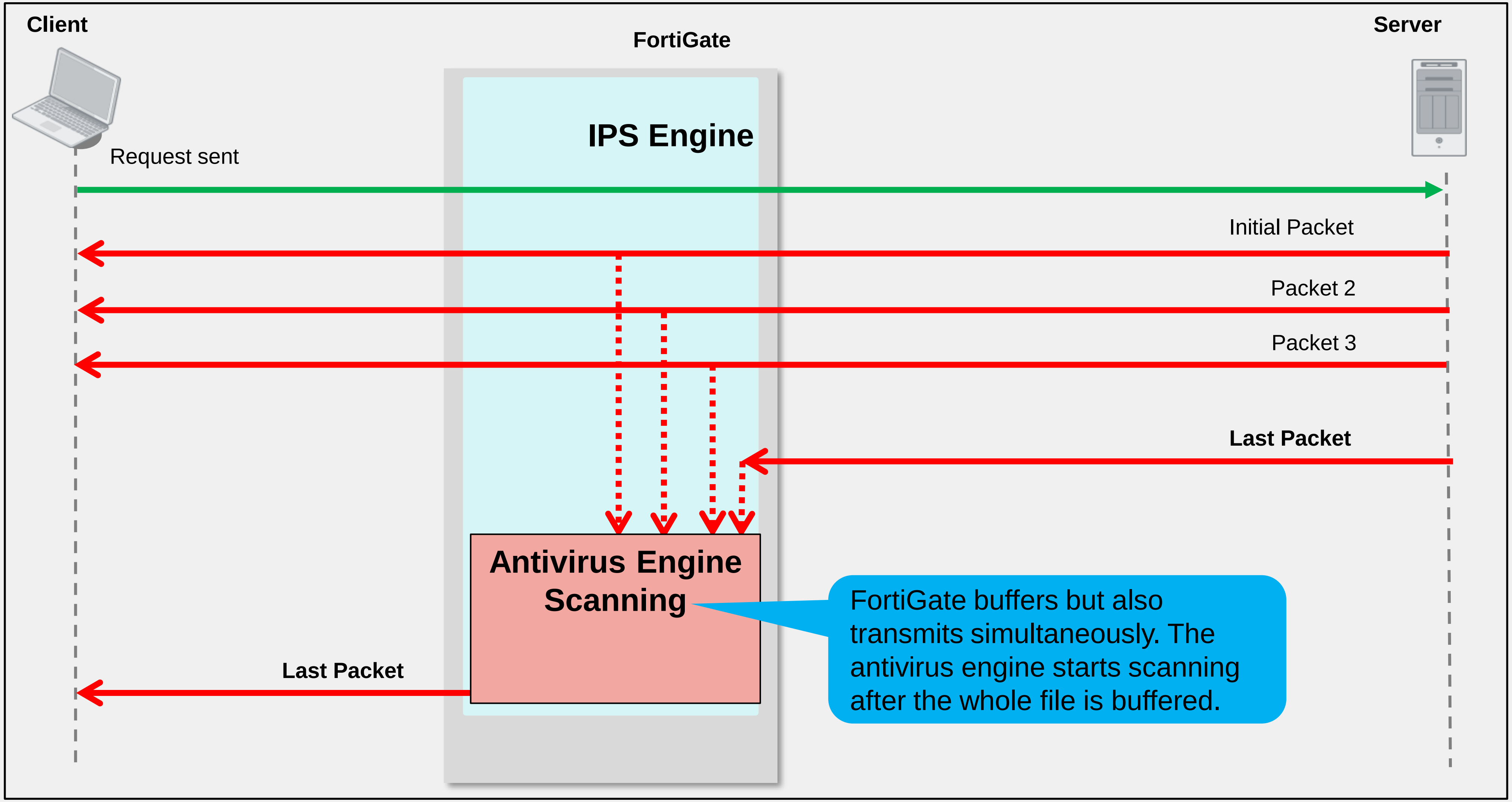


- Proxy-based inspection
  - Provides additional options

Two TCP connections



Flow-Based Inspection Mode Packet Flow

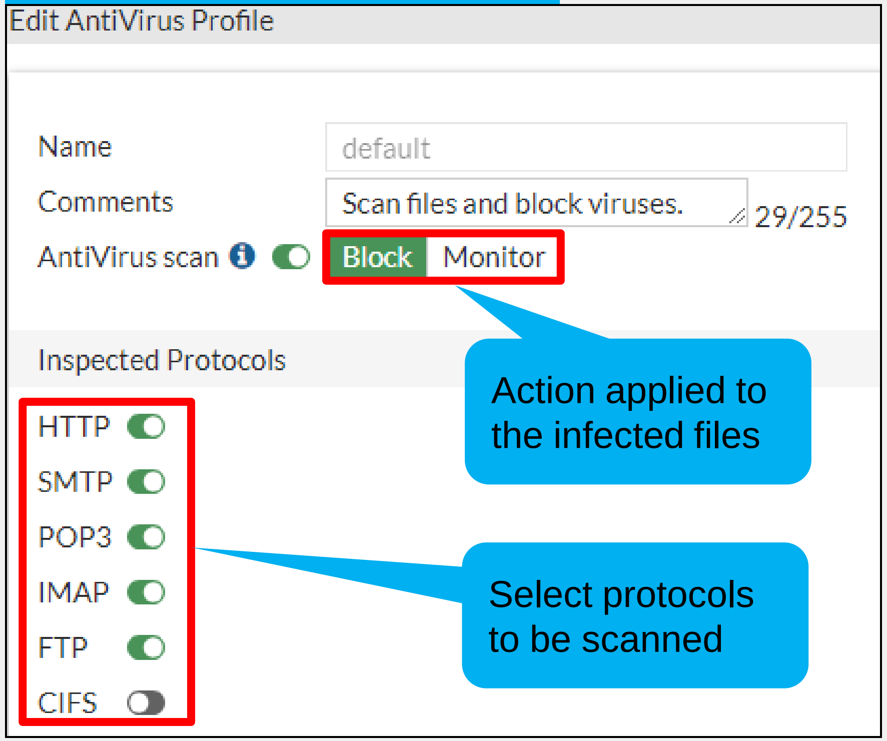


FortiGate buffers but also transmits simultaneously. The antivirus engine starts scanning after the whole file is buffered.

Flow-Based Inspection Mode

- Default mode

Security Profiles > AntiVirus



Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
AntiVirus scan	[✓ Block] Monitor

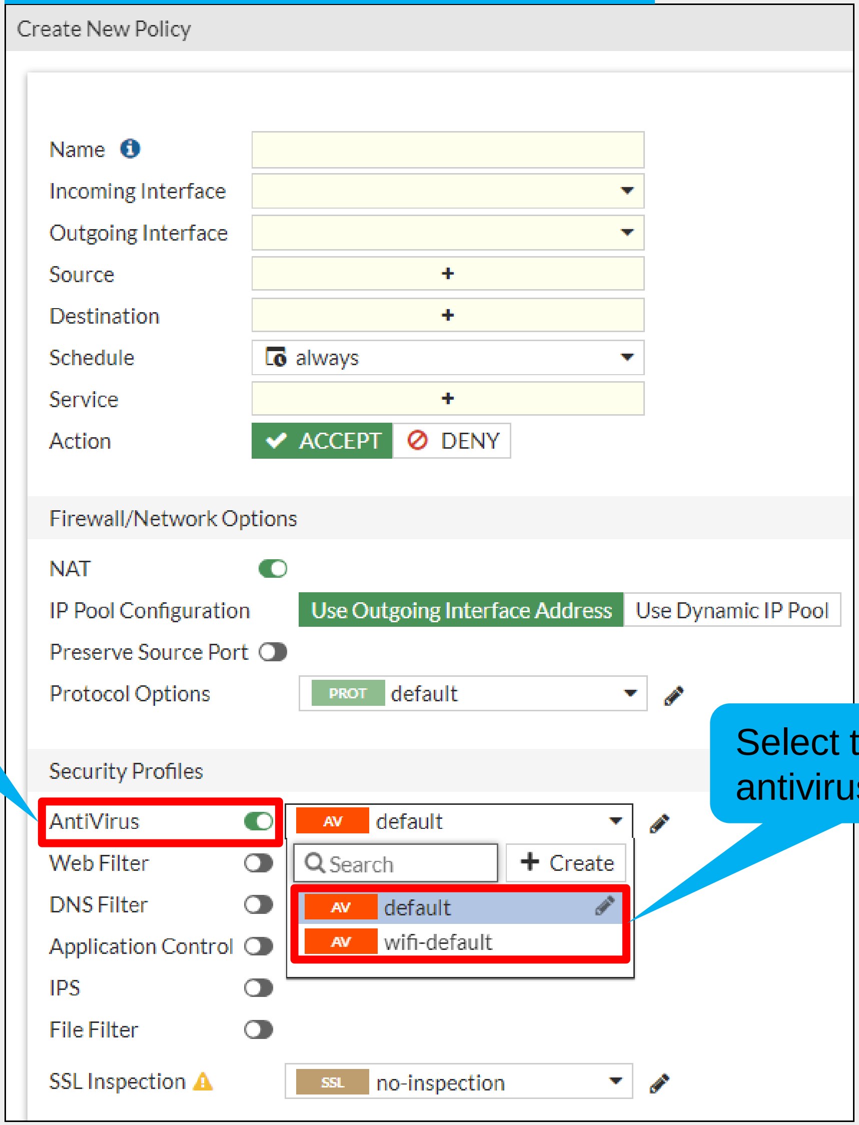
Inspected Protocols

- HTTP: on
- SMTP: on
- POP3: on
- IMAP: on
- FTP: on
- CIFS: off

Action applied to the infected files

Select protocols to be scanned

Policy & Objects > Firewall Policy



Create New Policy

Name	
Incoming Interface	
Outgoing Interface	
Source	+
Destination	+
Schedule	always
Service	+
Action	[✓ ACCEPT] DENY

Firewall/Network Options

NAT	on
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	off
Protocol Options	PROT default

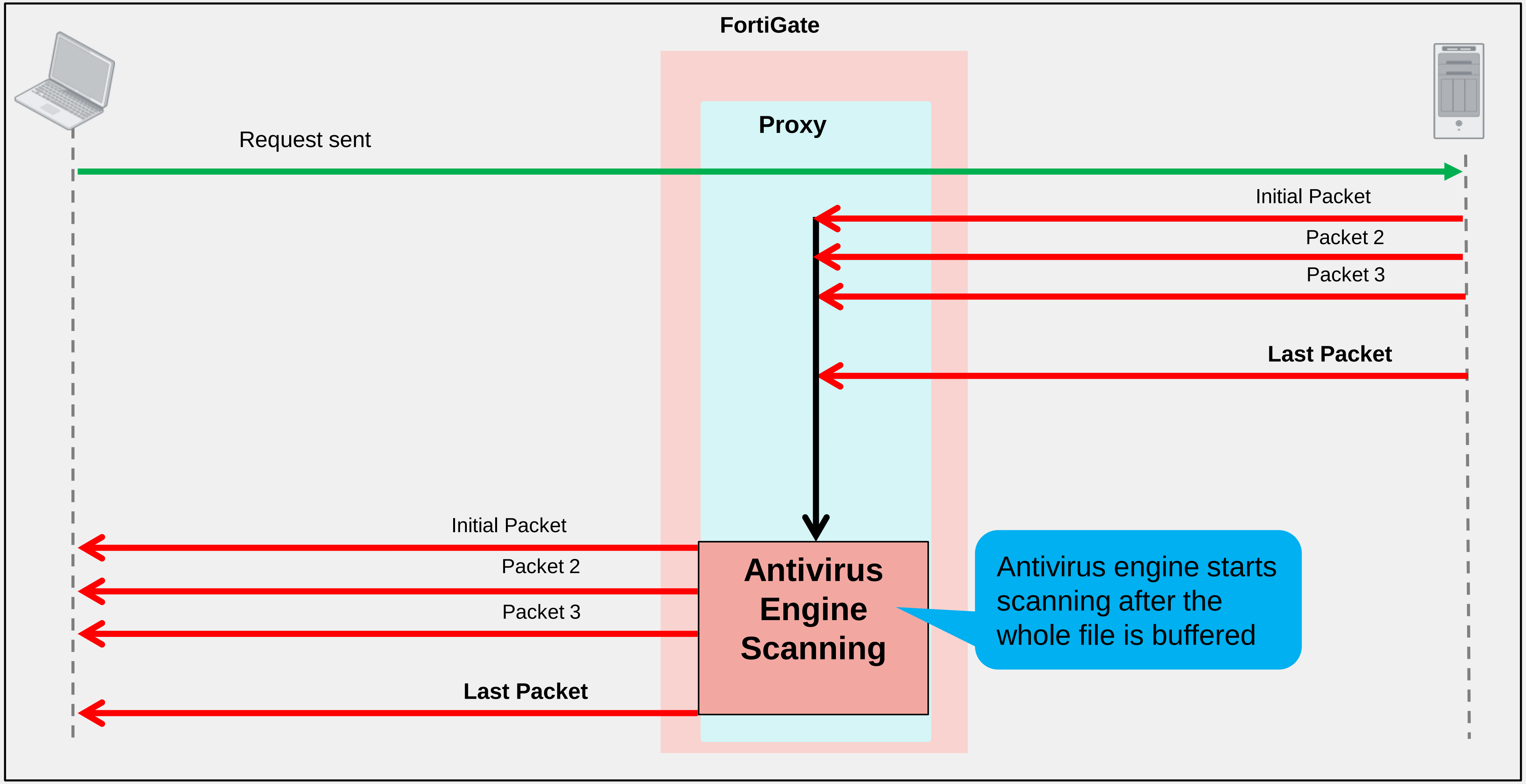
Security Profiles

AntiVirus	on — AV default
Web Filter	off
DNS Filter	off
Application Control	off
IPS	off
File Filter	off
SSL Inspection	SSL no-inspection

Enable AntiVirus profile in the firewall policy

Select the antivirus profile

Proxy Inspection Mode Packet Flow



Antivirus engine starts scanning after the whole file is buffered

FURTINET Training Institute

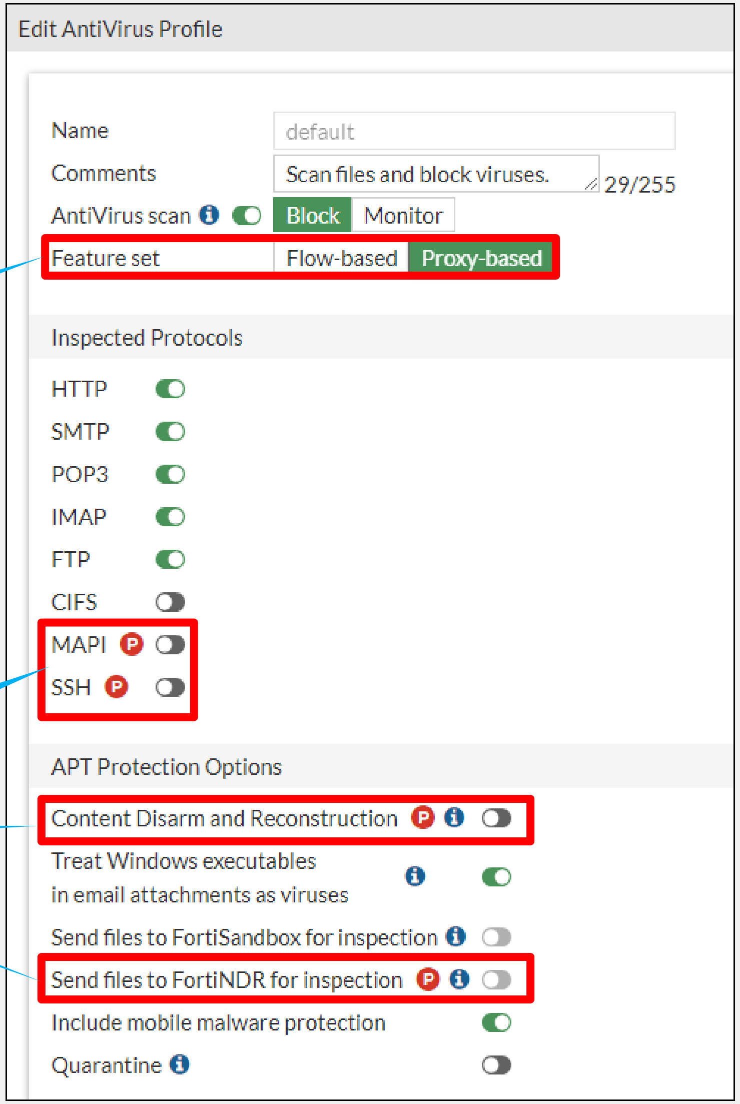
Proxy Inspection Mode Enabled

- 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

Security Profiles > AntiVirus



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ● [✓ Block] Monitor

Feature set: Flow-based [✓ Proxy-based]

Inspected Protocols

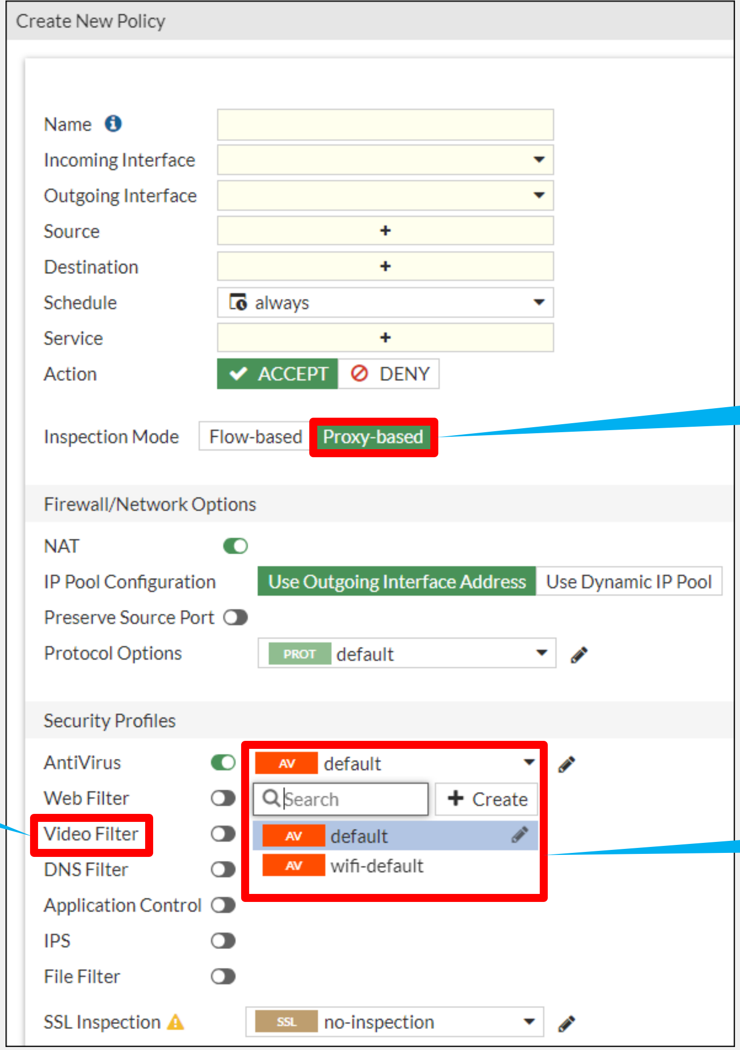
HTTP ●
SMTP ●
POP3 ●
IMAP ●
FTP ●
CIFS ○
MAPI P ○
SSH P ○

APT Protection Options

Content Disarm and Reconstruction P ○
Treat Windows executables in email attachments as viruses ●
Send files to FortiSandbox for inspection ○
Send files to FortiNDR for inspection P ○
Include mobile malware protection ●
Quarantine ○

Firewall Policy With Proxy Inspection Mode

Policy & Objects > Firewall Policy



Create New Policy

Name ℹ

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: PROT default

Security Profiles

AntiVirus ●: AV default

Search | + Create

- AV default
- AV wifi-default

Web Filter ○

Video Filter ○

DNS Filter ○

Application Control ○

IPS ○

File Filter ○

SSL Inspection ⚠: SSL no-inspection

Set **Inspection Mode** to **Proxy-based**

Available only in proxy-based inspection mode

Proxy-based and flow-based antivirus profiles available

F⊞RTINET.
Training Institute

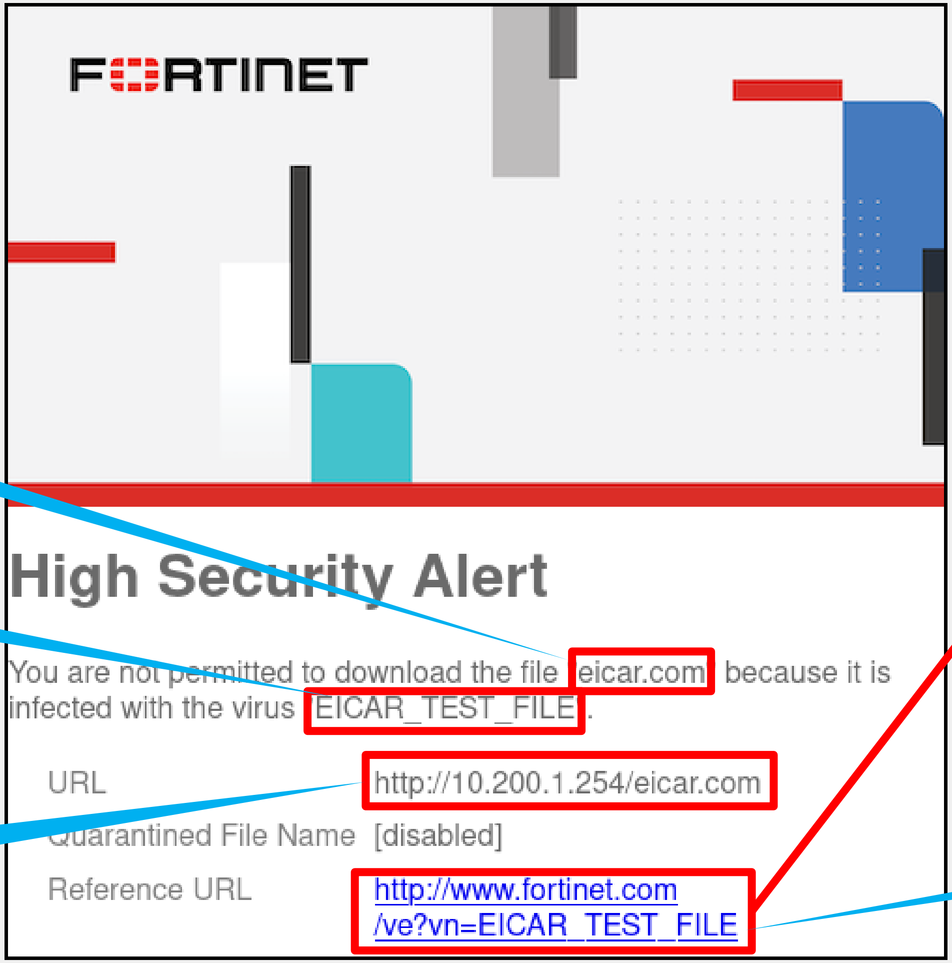
Antivirus Block Page

- Information available on the antivirus block page

File name

Virus name

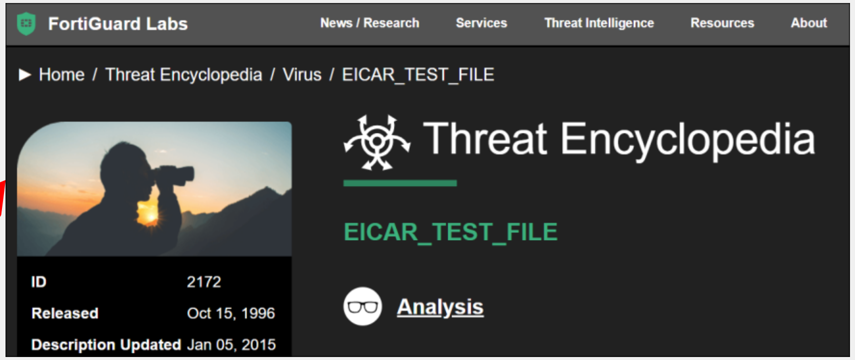
Website host or URL



High Security Alert

You are not permitted to download the file eicar.com because it is infected with the virus EICAR_TEST_FILE.

URL	http://10.200.1.254/eicar.com
Quarantined File Name	[disabled]
Reference URL	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE



▶ Home / Threat Encyclopedia / Virus / EICAR_TEST_FILE

Threat Encyclopedia

EICAR_TEST_FILE

ID	2172
Released	Oct 15, 1996
Description Updated	Jan 05, 2015

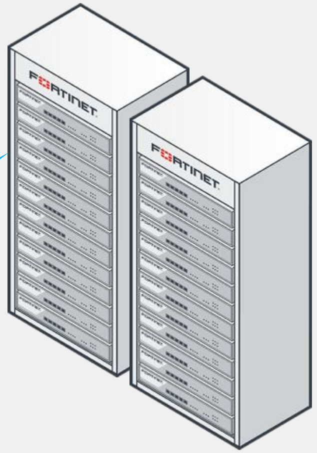
Analysis

Link to FortiGuard Encyclopedia

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

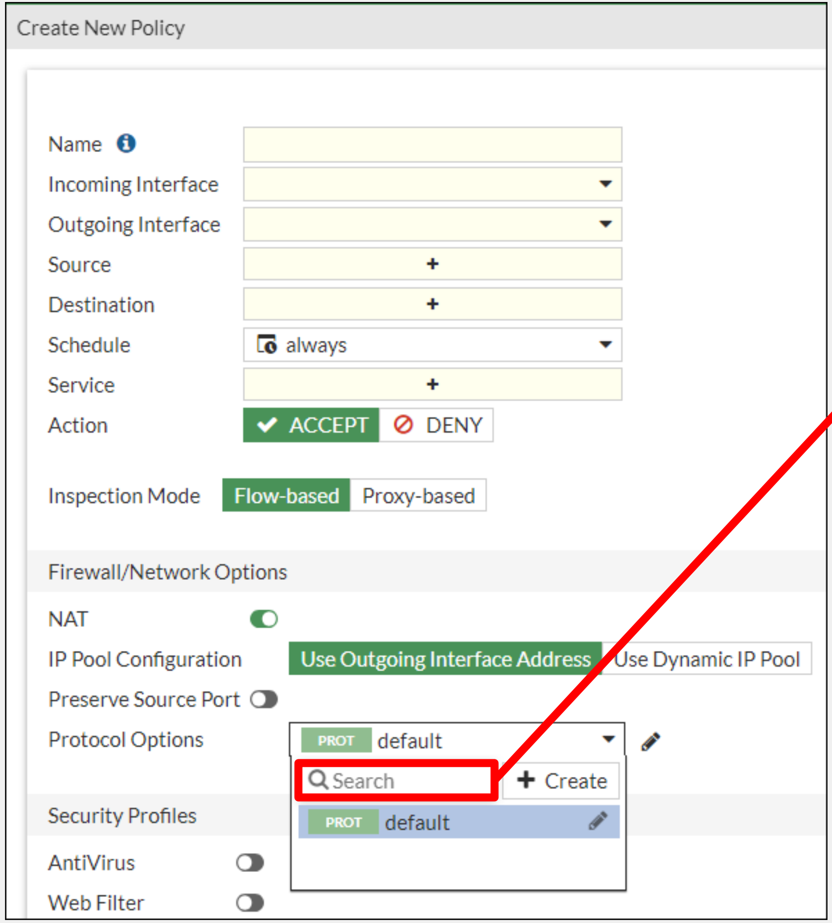
- Proxy inspection mode
  - Required for its additional options
  - Priority on network security

Protecting emails received by mail servers through SMTP or MAPI

Configuring Protocol Options

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

Policy & Objects > Firewall Policy



Create New Policy

Name ℹ	
Incoming Interface	
Outgoing Interface	
Source	+
Destination	+
Schedule	always
Service	+
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

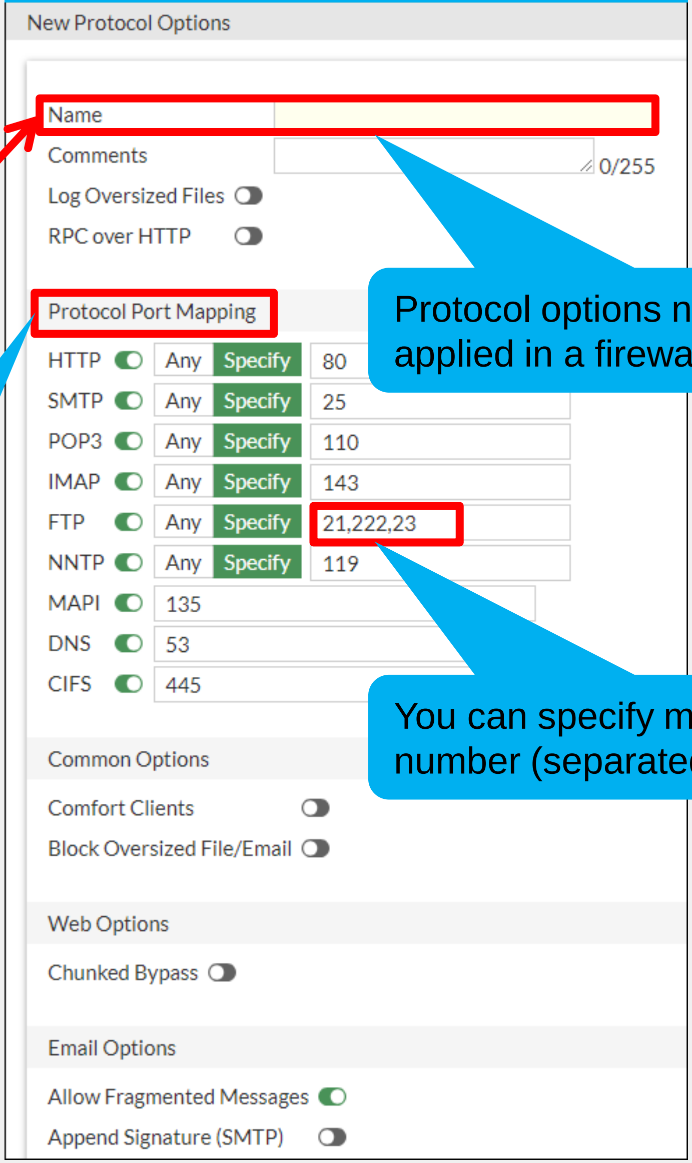
Firewall/Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default Search + Create PROT default

Security Profiles

AntiVirus	○
Web Filter	○

Policy & Objects > Protocol Options



New Protocol Options

Name	
Comments	0/255
Log Oversized Files	○
RPC over HTTP	○

Protocol Port Mapping

HTTP	●	Any [✓ Specify]	80
SMTP	●	Any [✓ Specify]	25
POP3	●	Any [✓ Specify]	110
IMAP	●	Any [✓ Specify]	143
FTP	●	Any [✓ Specify]	21,222,23
NNTP	●	Any [✓ Specify]	119
MAPI	●		135
DNS	●		53
CIFS	●		445

Common Options

Comfort Clients	○
Block Oversized File/Email	○

Web Options

Chunked Bypass	○

Email Options

Allow Fragmented Messages	●
Append Signature (SMTP)	○

Protocol options named to be applied in a firewall policy

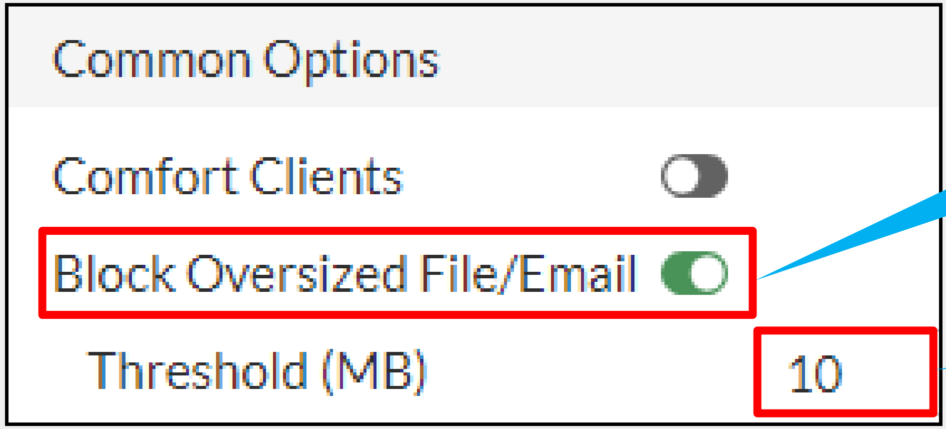
Port mapping only works in proxy-based inspection

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

FORTINET Training Institute

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



Common Options

Comfort Clients ○

Block Oversized File/Email ●

Threshold (MB) 10

Applies to all protocols

Default value is 10 MB. Maximum value is hardware dependant.

- 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

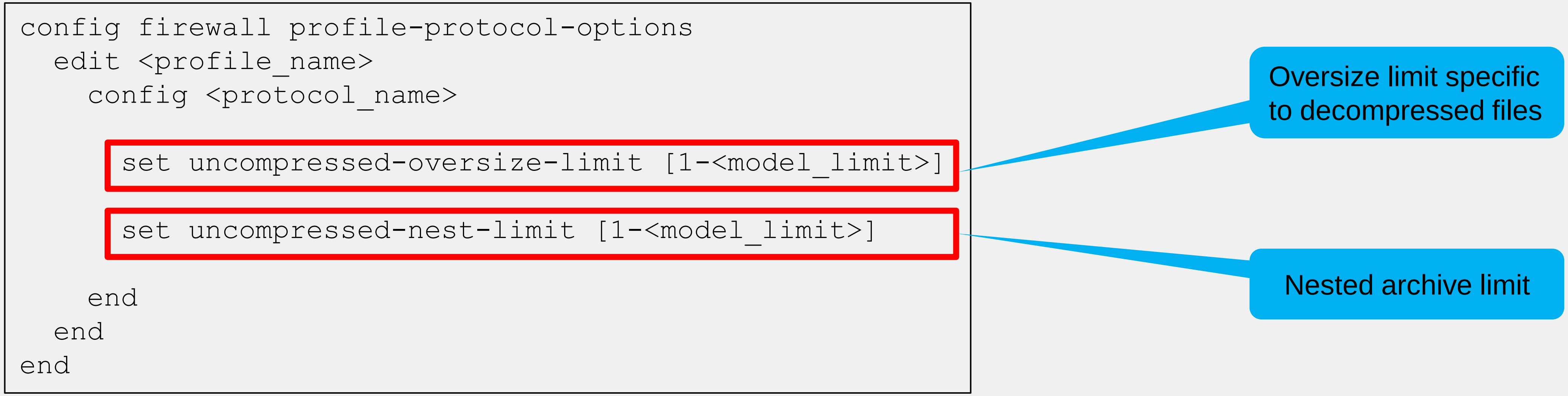
Name of the specific protocol

Training Institute

© Fortinet Inc. All Rights Reserved.

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
```

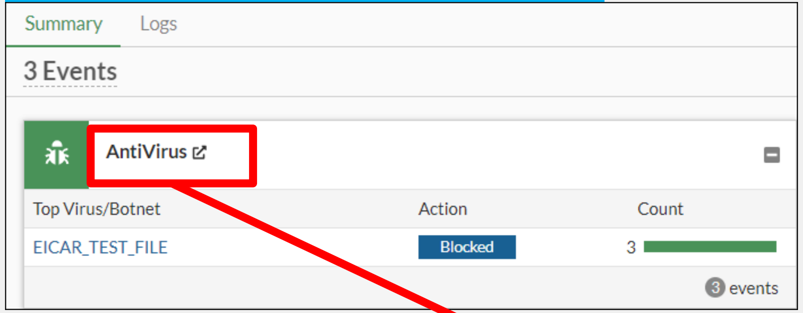
Oversize limit specific to decompressed files

Nested archive limit

Training Institute

Antivirus Logs

Log & Report > Security Events

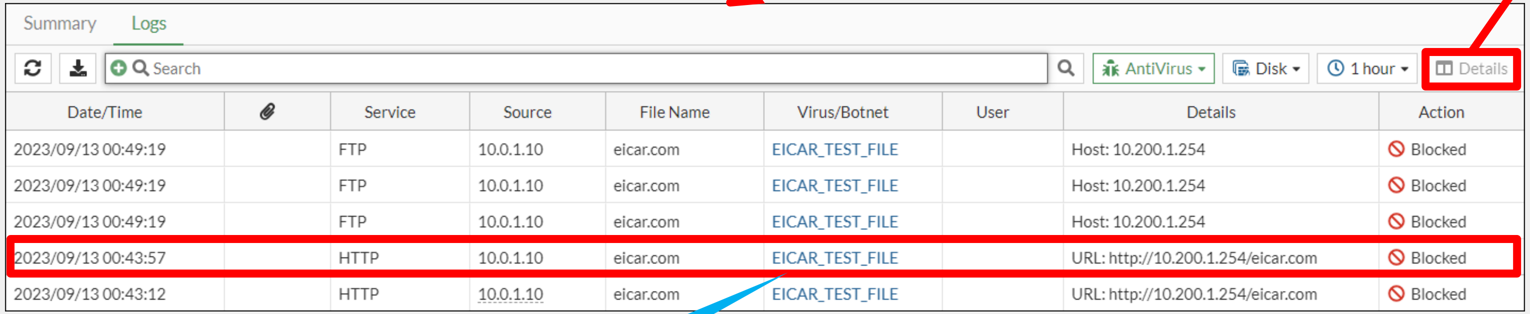


3 Events

AntiVirus

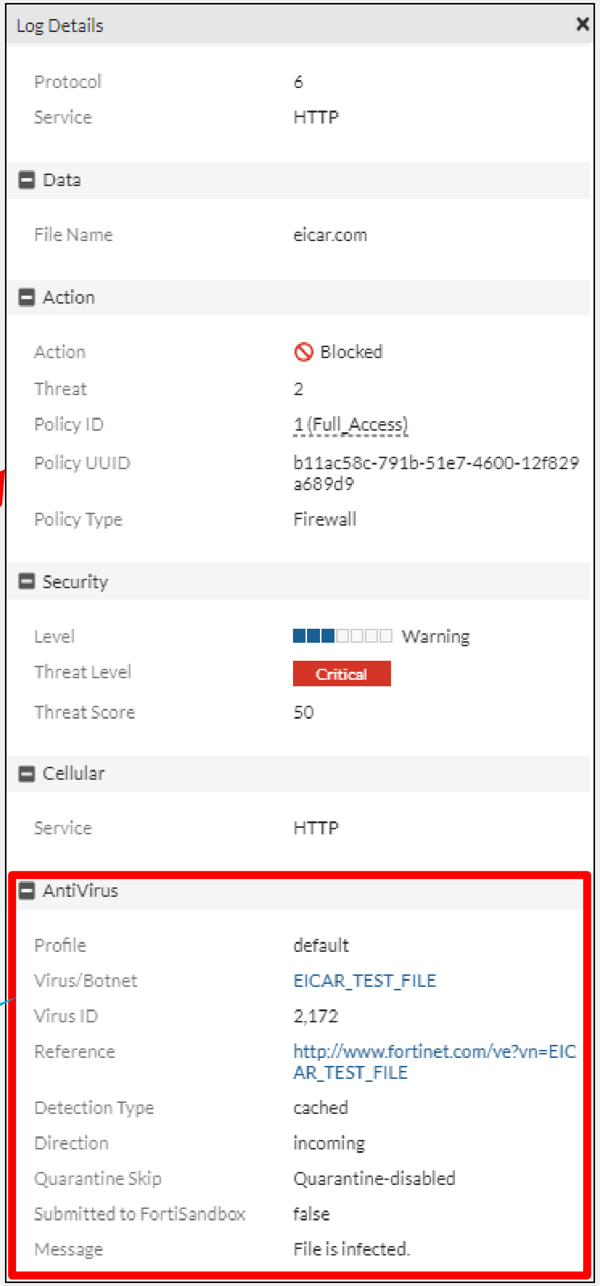
Top Virus/Botnet	Action	Count
EICAR_TEST_FILE	Blocked	3

3 events



Date/Time		Service	Source	File Name	Virus/Botnet	User	Details	Action
2023/09/13 00:49:19		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:49:19		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:49:19		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:43:57		HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	Blocked
2023/09/13 00:43:12		HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	Blocked

Log entry when a virus is detected



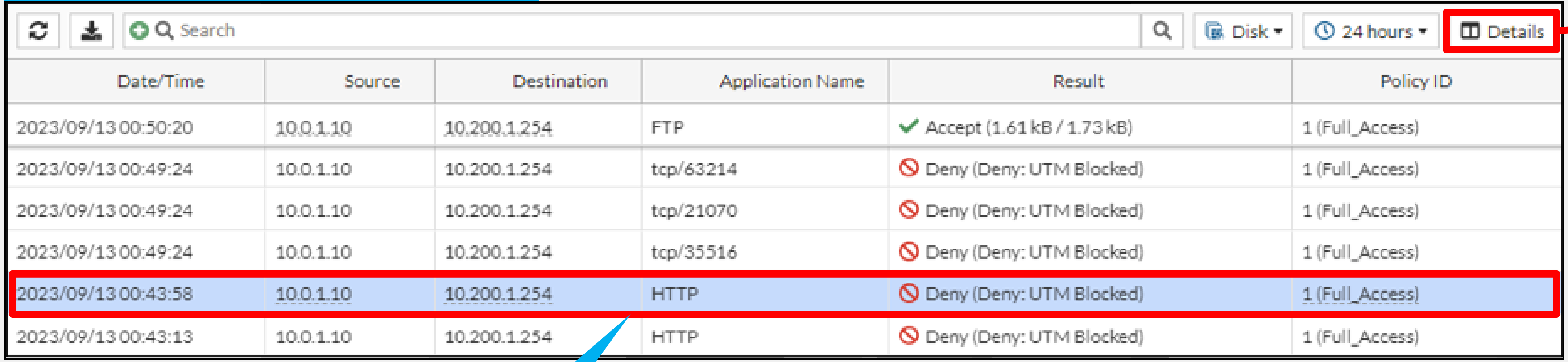
Log Details

Protocol	6
Service	HTTP
Data	
File Name	eicar.com
Action	
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
AntiVirus	
Profile	default
Virus/Botnet	EICAR_TEST_FILE
Virus ID	2,172
Reference	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Detection Type	cached
Direction	incoming
Quarantine Skip	Quarantine-disabled
Submitted to FortiSandbox	false
Message	File is infected.

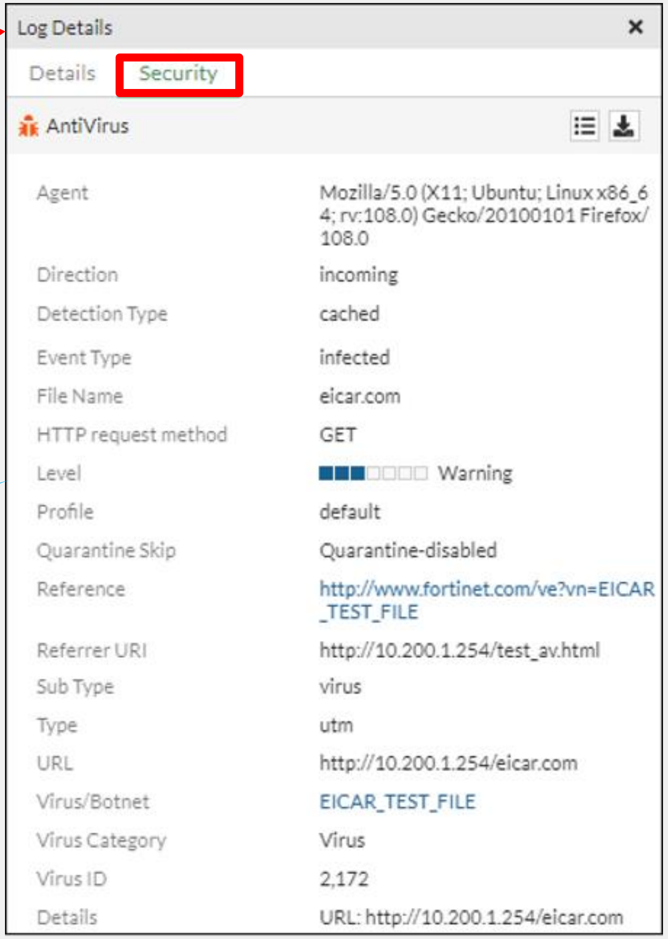
Details on the virus with FortiGuard reference

Forward Traffic Logs

Log & Report > Forward Traffic



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)



Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/108.0
Direction	incoming
Detection Type	cached
Event Type	infected
File Name	eicar.com
HTTP request method	GET
Level	■■■□□□□ Warning
Profile	default
Quarantine Skip	Quarantine-disabled
Reference	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Referrer URI	http://10.200.1.254/test_av.html
Sub Type	virus
Type	utm
URL	http://10.200.1.254/eicar.com
Virus/Botnet	EICAR_TEST_FILE
Virus Category	Virus
Virus ID	2,172
Details	URL: http://10.200.1.254/eicar.com

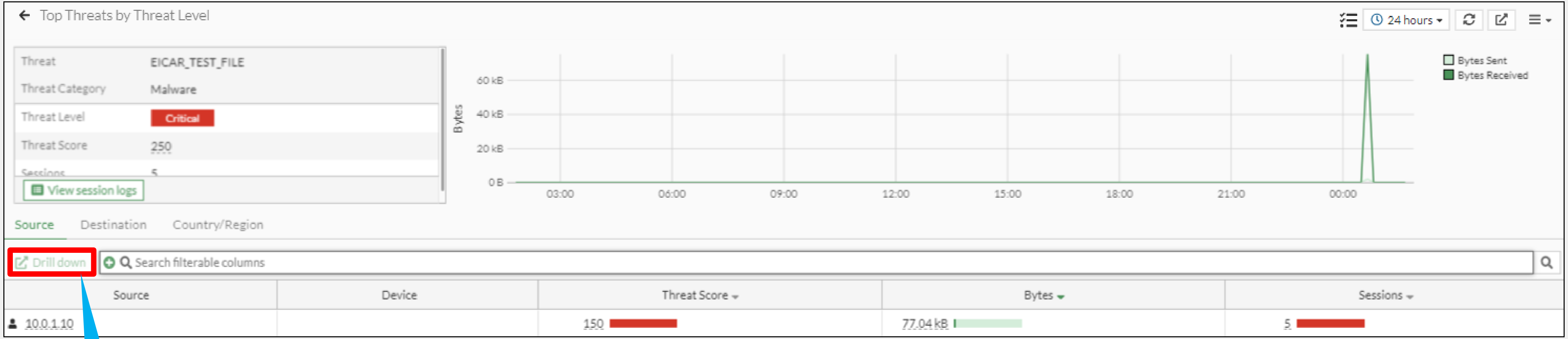
Forward traffic log entry

Security log details

Security Dashboard

- Security widget and dashboard allow you to monitor your network

Dashboard > Security

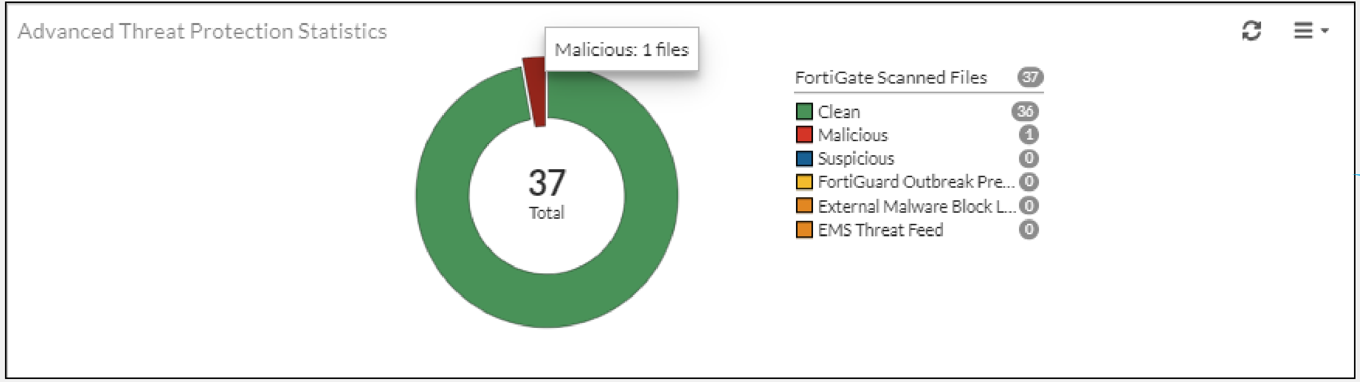


Threat	EICAR_TEST_FILE
Threat Category	Malware
Threat Level	Critical
Threat Score	250
Sessions	5

Source	Device	Threat Score	Bytes	Sessions
10.0.1.10		150	77.04 kB	5

Drill down for further details

Dashboard



FortiGate Scanned Files	37
🟩 Clean	36
🟥 Malicious	1
🟦 Suspicious	0
🟧 FortiGuard Outbreak Pre...	0
🟧 External Malware Block L...	0
🟧 EMS Threat Feed	0

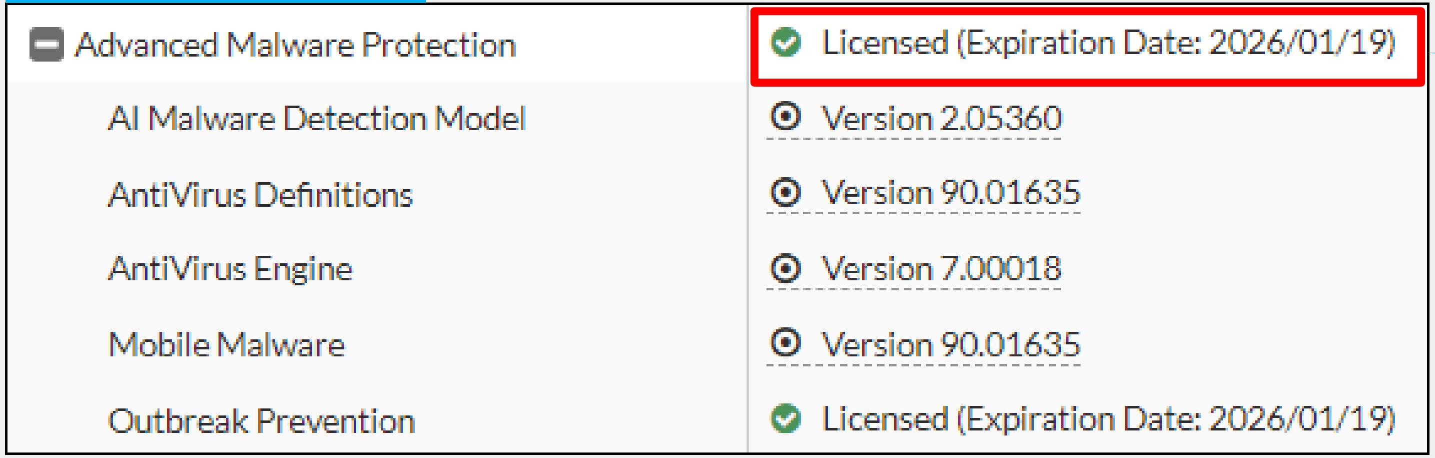
Security widget

FORTINET Training Institute

Troubleshooting Common Antivirus Issues

- Verify FortiGuard antivirus license

System > FortiGuard



⊟ Advanced Malware Protection	✓ Licensed (Expiration Date: 2026/01/19)
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)

Valid license

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

Troubleshooting Common Antivirus Issues (Contd)

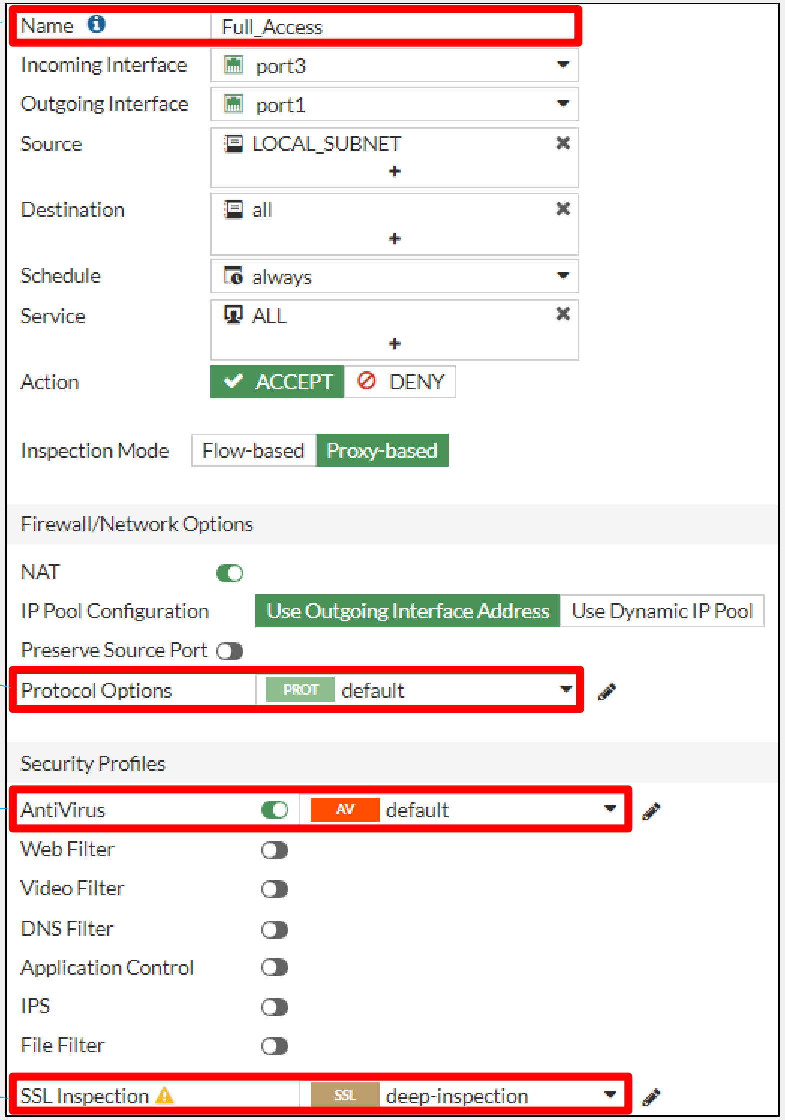
- Unable to catch viruses even with a valid contract?

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



Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
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	PROT default

Security Profiles

AntiVirus	● AV default
Web Filter	○
Video Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection ⚠	SSL deep-inspection

FORTINET Training Institute

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

FORTINET
Training Institute

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