DIGITAL EGYPT PIONEERS (DEPI)

Antivirus

Fortinet Cybersecurity

Name: Konouze Waheed Anwar | ID: 21022740

Contents:

Objective of the Lab: Antivirus

In this lab, you will examine how to configure, use, and monitor antivirus scanning on Local-FortiGate in both flow based and proxy-based inspection modes.

- Configure antivirus scanning in both flow-based and proxy-based inspection modes
- Understand FortiGate antivirus scanning behavior
- Scan multiple protocols
- Read and understand antivirus logs
- Understand machine learning (AI) scan

Topology:

- **Local-FortiGate Firewall**: The main device for antivirus scanning, with flow-based and proxy-based inspection modes.
- **Local-Client VM**: The client machine used to download test files for antivirus scanning.
- **Full_Access Firewall Policy**: A policy used to control network traffic, where antivirus and SSL inspection are configured.
- **EICAR Test File**: Used to test the antivirus configuration, simulating a virus without causing harm.
- **SSL Inspection**: Deep inspection feature for encrypted traffic (HTTPS).

Components Used:

- **FortiGate Firewall**: A virtual or physical device for managing security and traffic, with antivirus scanning capabilities.
- **Local-Client VM**: A virtual machine acting as the client, used to download and test files.
- **Web Browser**: Used on the Local-Client VM to download test files and interact with the FortiGate firewall.
- **EICAR Test File**: A standard test file used to simulate viruses.
- **SSL Inspection Profile**: A security profile used for inspecting encrypted traffic.
- **FortiGate GUI**: The graphical interface used for configuring and monitoring antivirus scanning and firewall policies.
- **Log & Report Tools**: For viewing antivirus logs and tracking security events.

Prerequisites

Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.
3. Click **+** to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.
5. Click **OK** to reboot.

Using Antivirus Scanning in Proxy-Based Inspection Mode

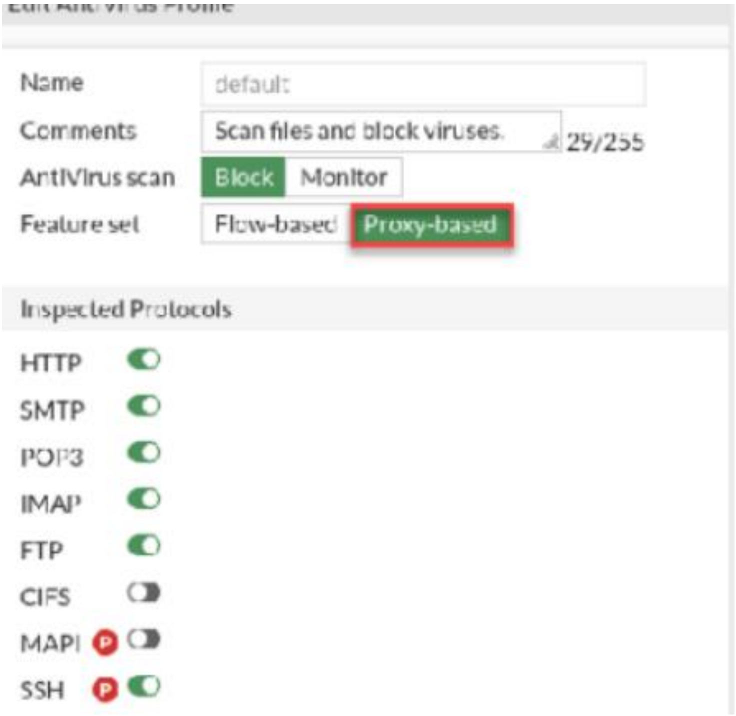
In proxy-based inspection mode, the proxy for each protocol buffers the entire file (or waits for oversize limit) and then scans it. The client must wait for the scan to finish.

Change the Antivirus Profile Inspection Mode

You will change the inspection mode in the default antivirus profile, which is applied on the firewall policy, to
inspect traffic.

To change the antivirus profile inspection mode

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.
2. Click **Security Profiles** > **AntiVirus**.
3. Right-click the **default** antivirus profile, and then click **Edit**.
4. In the **Feature set** field, select **Proxy-based**.
5. On the **SSH** protocol, toggle to enable.



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 ○
- SSH ●

6. Click **OK**.

Enable the Antivirus Profile on a Firewall Policy

To change the firewall policy inspection mode

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the **Full_Access** policy to edit it.
3. In the **Inspection Mode** field, select **Proxy-based**.
4. In the **Protocol Options** field, verify the **default** profile is selected.
5. In the **Security Profiles** section, enable **AntiVirus**, and then select **default** from the drop-down list.
6. In the **SSL Inspection** drop-down list, keep the default **certificate-inspection** profile
7.Keep the default values for the remaining settings, and click **OK** to save the changes.

Test the Antivirus Configuration

You will download the EICAR test file to your Local-Client VM. The EICAR test file is an industry-standard virus
used to test antivirus detection without causing damage. The file contains the following characters:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To test the antivirus configuration

1. On the Local-Client VM, open a new web browser tab, and then access the following website:
http://10.200.1.254/test_av.html
2. In the **Download area** section, download any EICAR sample file

FortiGate should block the download attempt, and insert a replacement message

View the Antivirus Logs

The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and make adjustments to network security, if necessary.

To view the antivirus logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**. You may need to remove any log filters you set.
2. Locate the antivirus log message, and double-click it.
The **Details** tab shows forward traffic log information, along with the action taken.
3. Select the **Security** tab to view security logs, which provide information more specific to security events, such as filename, virus or botnet, and reference.
4. To view antivirus security logs, click **Log & Report** > **Security Events** > **AntiVirus**.

Enable SSL Inspection on a Firewall Policy

So far, you have tested unencrypted traffic for antivirus scanning. In order for FortiGate to inspect the encrypted traffic, you must enable deep inspection on the firewall policy.
After you enable this feature, FortiGate can inspect SSL traffic using a technique similar to a man-in-the-middle (MITM) attack.

To test antivirus scanning without SSL inspection enabled on the firewall policy

1. On the Local-Client VM, open a web browser, and then go to the following website:
https://10.200.1.254/test_av.html
2. Click **Advanced**.
3. Click **Accept the Risk and Continue**.
4. In the **Download area**section, download the **eicar.com** sample file.

FortiGate should not block the file, because you did not enable full SSL inspection.

To enable and test the SSL inspection profile on a firewall policy

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and click **Policy & Objects** >
Firewall Policy.
2. Double-click the **Full Access** firewall policy to edit it.
3. In the **Security Profiles** section, in the **SSL Inspection** drop-down list, select **deep-inspection**.
4. Keep the remaining default settings, and click **OK** to save the changes.
5. In the **Download area** section, try to download the same eicar.com file again.

FortiGate should block the download and replace it with a message. If it doesn't, you may need to clear your cache. In Firefox, click **Preferences** > **Privacy & Security**. Scroll to **History**, click **Clear History**, and ensure the time range to clear is set to **Everything**. Click **Clear Now**.

Configuring Flow-Based Antivirus Scanning

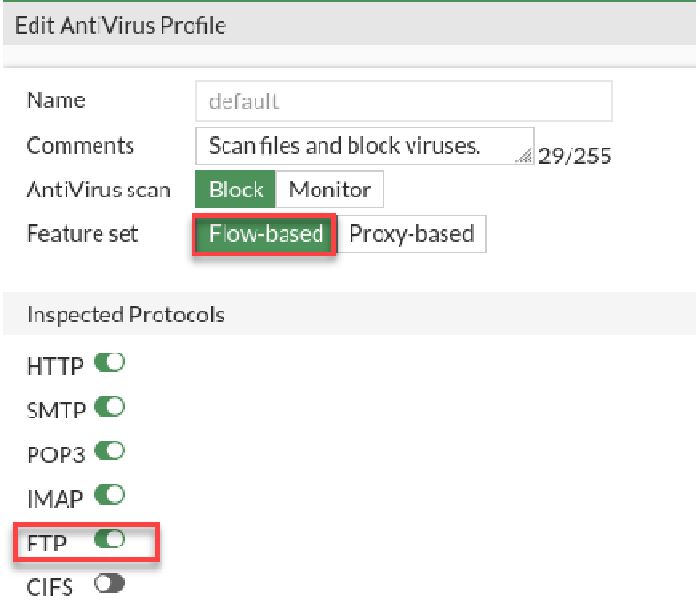
When a firewall policy’s inspection mode is set to flow, FortiGate does not buffer traffic flowing through the policy. Unlike proxy mode, FortiGate inspects the content payload passing through the policy packet by packet. FortiGate holds the very last packet until the scan returns a verdict. If FortiGate detects a violation in the traffic, it sends a reset packet to the receiver, which terminates the connection, and prevents the payload from being sent successfully.

Change the Antivirus Profile Inspection Mode

You will change the inspection mode in the default antivirus profile, which is applied on the firewall policy, to inspect traffic including FTP.

To change the antivirus profile inspection mode

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **AntiVirus**.
2. Right-click the **default** antivirus profile, and then click **Edit**.
3. In the **Feature set** field, select **Flow-based**.
4. In the **Inspected Protocols** section, verify that **FTP** is enabled.



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 ○

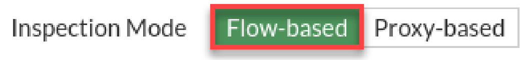
5. Click **OK**.

Change the FortiGate Inspection Mode

By default, flow-based inspection mode is enabled on the FortiGate firewall policy. In this exercise, you will
change the inspection mode from proxy-based to flow-based.

To change the firewall policy inspection mode

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Double-click the **Full_Access** policy to edit it.
4. In the **Inspection Mode** field, select **Flow-based**.



Inspection Mode [✓ Flow-based] Proxy-based

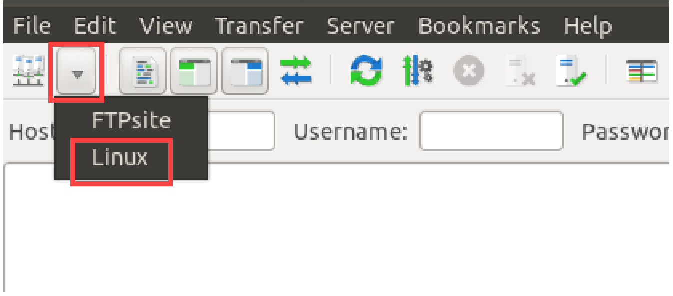
5. In the **Protocol Options** field, verify that the **default** profile is selected.
6. In the **Security Profiles** section, verify that the **default AntiVirus profile** is selected.
7. Click **OK**.

Test the Flow-Based Antivirus Profile

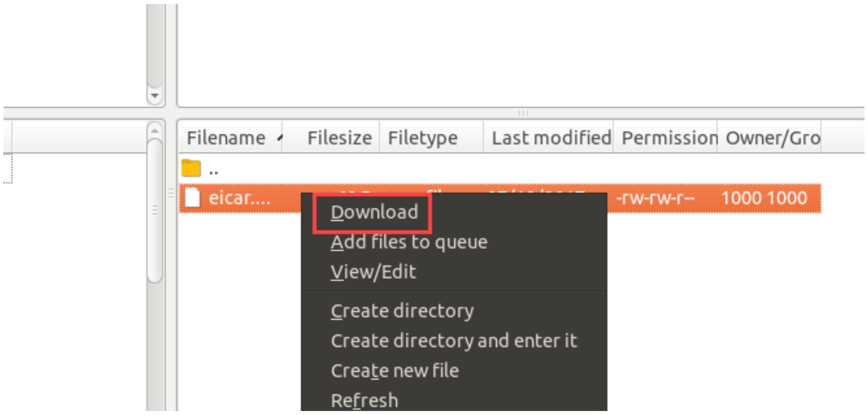
You will test the flow-based antivirus profile using FTP.

To test the antivirus configuration

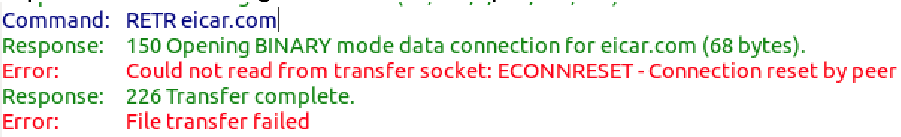
1. On the Local-Client VM, open the FileZilla FTP client software from the desktop.
2. Click the **Site Manager** icon in the upper-left corner, and then select **Linux**.



3. On the **Remote site** side of the application (right), right-click the **eicar.com** file, and then select **Download**.



The client should display an error message that the server terminated the connection. FortiGate sends the
replacement message as a server response.



```
Command:   RETR eicar.com
Response:  150 Opening BINARY mode data connection for eicar.com (68 bytes).
Error:     Could not read from transfer socket: ECONNRESET - Connection reset by peer
Response:  226 Transfer complete.
Error:     File transfer failed
```

4. Close the FileZilla FTP client

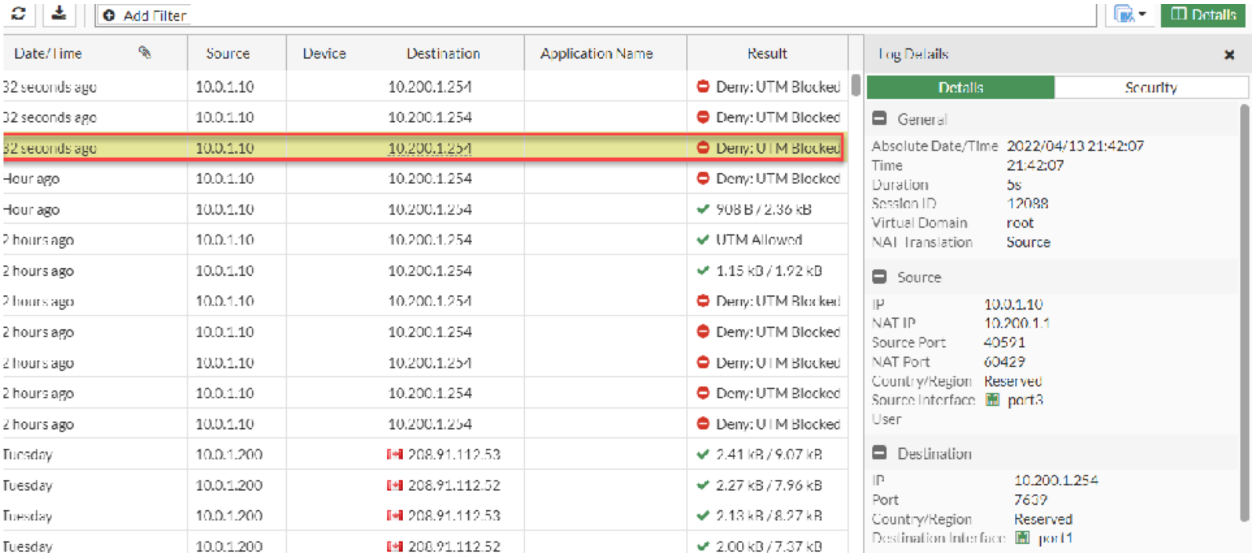
View the Antivirus Logs

You will check and confirm the logs for the test you just performed.

To view the antivirus logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Locate the antivirus log message from when you tried to access the file using FTP, and double-click the log entry toview the details.

The **Details** tab shows forward traffic log information, along with the action taken.



Date/Time	Source	Device	Destination	Application Name	Result
32 seconds ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
32 seconds ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
32 seconds ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
Hour ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
Hour ago	10.0.1.10		10.200.1.254		✓ 908 B / 2.36 kB
2 hours ago	10.0.1.10		10.200.1.254		✓ UTM Allowed
2 hours ago	10.0.1.10		10.200.1.254		✓ 1.15 kB / 1.92 kB
2 hours ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		⛔ Deny: UTM Blocked
Tuesday	10.0.1.200		208.91.112.53		✓ 2.41 kB / 9.07 kB
Tuesday	10.0.1.200		208.91.112.52		✓ 2.27 kB / 7.96 kB
Tuesday	10.0.1.200		208.91.112.53		✓ 2.13 kB / 8.27 kB
Tuesday	10.0.1.200		208.91.112.52		✓ 2.00 kB / 7.37 kB

Log Details

Details | Security

General

Absolute Date/Time	2022/04/13 21:42:07
Time	21:42:07
Duration	5s
Session ID	12088
Virtual Domain	root
NAT Translation	Source

Source

IP	10.0.1.10
NAT IP	10.200.1.1
Source Port	40591
NAT Port	60429
Country/Region	Reserved
Source Interface	port3
User	

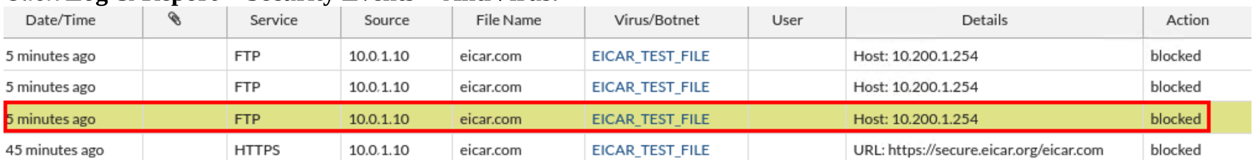
Destination

IP	10.200.1.254
Port	7639
Country/Region	Reserved
Destination Interface	port1

3. To view security log information, do one of the following:

Select the **Security** tab. This includes information more specific to the security event, such as filename, virus or botnet, reference, and so on.

Click **Log & Report** > **Security Events** > **AntiVirus**.



Date/Time		Service	Source	File Name	Virus/Botnet	User	Details	Action
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
45 minutes ago		HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://secure.eicar.org/eicar.com	blocked

Test the Machine learning (AI) scan

By default, machine learning detection is enabled on FortiGate and it detects zero-day attacks. In this exercise,
you will disable machine learning detection and then download an unknown malware from the FTP server. Then you will enable machine learning detection and download the same file again to test the machine learning
detection scan.

To disable machine learning detection

1. On the Local-FortiGate CLI, log in with the username admin and password password.
2. Enter the following commands to disable machine learning detection:

```
config antivirus settings
set machine-learning-detection disable
end
```

3. On the Local-Client VM, open the FileZilla FTP client software from the desktop.
4. Click the **Site Manager** icon in the upper-left corner, and then select **Linux**.
5. On the **Remote site** side of the application (right), right-click the **1132999808** file, and then select **Download**.

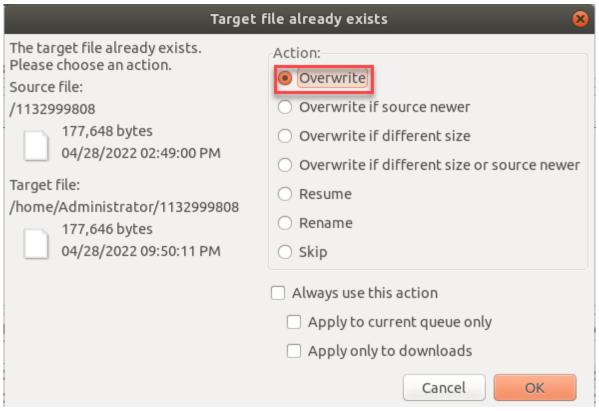
You will see that the download completed successfully.

Block the unknown malware using machine learning scan

1. Return to the Local-FortiGate CLI and enter the following commands to enable machine learning detection:

```
config antivirus settings
set machine-learning-detection enable
end
```

2. Open the FileZilla FTP client software again, right-click the **1132999808** file, and then select **Download**.
3. In the **Target file already exists** window, select **Overwrite**, and then click **OK**.



Target file already exists

The target file already exists.
Please choose an action.

Source file:
/1132999808
177,648 bytes
04/28/2022 02:49:00 PM

Target file:
/home/Administrator/1132999808
177,646 bytes
04/28/2022 09:50:11 PM

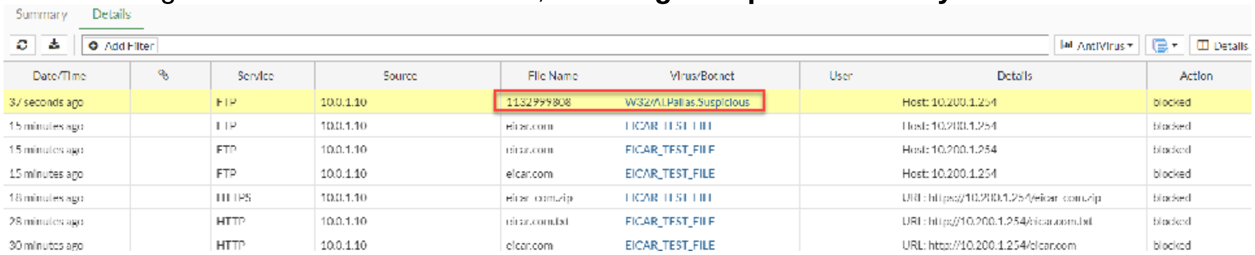
Action:

- ● Overwrite
- ○ Overwrite if source newer
- ○ Overwrite if different size
- ○ Overwrite if different size or source newer
- ○ Resume
- ○ Rename
- ○ Skip

- □ Always use this action
- □ Apply to current queue only
- □ Apply only to downloads

You will see that the download failed this time because the AI engine terminated the file transfer.

4. In the **Target file already exists** window,click **Cancel**.
5. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Security Events** > **AntiVirus**.



Date/Time		Service	Source	File Name	Virus/Botnet	User	Details	Action
37 seconds ago		FTP	10.0.1.10	1132999808	W32/AI.Pallas.Suspicious		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
18 minutes ago		HTTPS	10.0.1.10	eicar_com.zip	EICAR_TEST_FILE		URL: https://10.200.1.254/eicar_com.zip	blocked
28 minutes ago		HTTP	10.0.1.10	eicar.com.txt	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com.txt	blocked
30 minutes ago		HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	blocked