**YASSER GABER AHMED DORGHAM**

**GROUP CODE /DEPI\_1\_ONL1\_ISS8\_G1e Fortinet Cybersecurity Engineer**

**"Enhancing Network Security: Configuring and Monitoring FortiGate Antivirus Scanning in Flow-Based and Proxy-Based Modes"**

**Objectives**

* **Configure antivirus scanning** in 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**.

**Prerequisites**

1. **Restore the FortiGate configuration file**:
   * Connect to the Local-FortiGate GUI and log in with the username admin and password password.
   * Click **admin** > **Configuration** > **Revisions**.
   * Expand the list and select the configuration with the comment "initial", then click **Revert**.
   * Click **OK** to reboot.

**Exercise 1: Using Antivirus Scanning in Proxy-Based Inspection Mode**

**Steps:**

1. **Change the Antivirus Profile Inspection Mode**:
   * Connect to the Local-FortiGate GUI and log in with the username admin and password password.
   * Click **Security Profiles** > **AntiVirus**.
   * Edit the default antivirus profile and select **Proxy-based** in the Feature set field.
   * Enable on the SSH protocol and click **OK**.
2. **Enable the Antivirus Profile on a Firewall Policy**:
   * Edit the **Full\_Access** firewall policy and change the **Inspection Mode** to **Proxy-based**.
   * Enable the default antivirus profile and use the certificate-inspection profile for SSL inspection.
3. **Test the Antivirus Configuration**:
   * Download the EICAR test file from http://10.200.1.254/test\_av.html.
   * FortiGate should block the download and display a replacement message.
   * Test using the Save Link As method to download the EICAR text file, observe the allowed download, and inspect the file content with Notepad++.
4. **View the Antivirus Logs**:
   * Navigate to **Log & Report** > **Forward Traffic** on the Local-FortiGate GUI.
   * Locate and double-click the antivirus log message to view the details.
   * Select the **Security** tab to view specific security logs, such as filename, virus, or botnet.

**Configuration Outline**

**System Global Settings**

plaintext

config system global

set admin-https-redirect disable

set admin-lockout-duration 1

set admin-lockout-threshold 10

set admin-server-cert "self-sign"

set admintimeout 480

set alias "FortiGate-VM64"

set gui-auto-upgrade-setup-warning disable

set gui-firmware-upgrade-warning disable

set hostname "Local-FortiGate"

set management-port-use-admin-sport disable

set proxy-auth-timeout 5

set timezone 04

end

**Admin Profile Configuration**

plaintext

config system accprofile

edit "prof\_admin"

set secfabgrp read-write

set ftviewgrp read-write

set authgrp read-write

set sysgrp read-write

set netgrp read-write

set loggrp read-write

set fwgrp read-write

set vpngrp read-write

set utmgrp read-write

set wanoptgrp read-write

set wifi read-write

next

end

**Interface Configuration**

plaintext

config system interface

edit "port1"

set vdom "root"

set ip 10.200.1.1 255.255.255.0

set allowaccess ping https ssh http fgfm

set type physical

set snmp-index 1

next

edit "port2"

set vdom "root"

set ip 10.200.2.1 255.255.255.0

set allowaccess ping https ssh http

set type physical

set snmp-index 2

next

edit "port3"

set vdom "root"

set ip 10.0.1.254 255.255.255.0

set allowaccess ping https ssh http telnet

set type physical

set snmp-index 3

end

**Topology**

Here is a simple network topology based on the interface configuration:

* **Port 1**: IP 10.200.1.1/24, connected to Local-Client VM.
* **Port 2**: IP 10.200.2.1/24, connected to another network segment.
* **Port 3**: IP 10.0.1.254/24, connected to a different network segment.

**Steps for Configuring and Using Antivirus Scanning**

1. **Restore FortiGate Configuration**
   * Connect to the Local-FortiGate GUI and log in.
   * Restore the configuration file to "initial" and reboot.
2. **Change Antivirus Profile Inspection Mode to Proxy-Based**
   * Edit the default antivirus profile to use **Proxy-based** mode.
3. **Enable Antivirus Profile on Firewall Policy**
   * Change the inspection mode of the **Full\_Access** policy to **Proxy-based**.
   * Enable the default antivirus profile and use the certificate-inspection profile for SSL inspection.
4. **Test the Antivirus Configuration**
   * Download the EICAR test file using different methods and ensure FortiGate blocks the download attempts.
5. **View Antivirus Logs**
   * Monitor and review antivirus logs through the Local-FortiGate GUI to ensure correct configuration and operation.

By following these steps, you will set up and understand FortiGate's antivirus scanning behavior, including proxy-based inspection and log monitoring.

**Project Structure**

plaintext

FortiGate\_Antivirus\_Configuration\_Project/

├── README.md

├── .gitignore

├── configs/

│ ├── global\_config.txt

│ ├── admin\_profile\_config.txt

│ └── interface\_config.txt

├── lab\_guide/

│ ├── prerequisites.md

│ ├── exercise1\_proxy\_based.md

│ └── exercise1\_flow\_based.md

└── screenshots/

├── step1.png

├── step2.png

└── step3.png

**1. Create the README.md File**

README.md should include an overview of your project, objectives, prerequisites, steps for configuration, and how to test the configuration.

markdown

# Enhancing Network Security: Configuring and Monitoring FortiGate Antivirus Scanning in Flow-Based and Proxy-Based Modes

## Overview

This project demonstrates how to configure, use, and monitor antivirus scanning on Local-FortiGate in both flow-based and proxy-based inspection modes.

## Objectives

- Configure antivirus scanning in both inspection modes.

- Understand FortiGate antivirus scanning behavior.

- Scan multiple protocols.

- Read and understand antivirus logs.

- Understand machine learning (AI) scan.

## Prerequisites

Before starting, restore the configuration file to Local-FortiGate as described in the prerequisites.md file.

## Configuration Steps

1. \*\*Change the Antivirus Profile Inspection Mode\*\* (described in exercise1\_proxy\_based.md).

2. \*\*Enable the Antivirus Profile on a Firewall Policy\*\* (described in exercise1\_flow\_based.md).

3. \*\*Test the Antivirus Configuration\*\*.

4. \*\*View the Antivirus Logs\*\*.

## Testing

- Download the EICAR test file to verify the antivirus configuration.

## Directory Structure

- `configs/`: Contains the configuration files.

- `lab\_guide/`: Contains step-by-step instructions for the lab exercises.

- `screenshots/`: Contains screenshots of the configuration steps.

**2. Create the .gitignore File**

.gitignore should specify files and directories that Git should ignore.

plaintext

# Ignore log files and temporary files

\*.log

\*.tmp

**3. Create the Configuration Files**

Store your configuration snippets in the configs/ directory.

* **global\_config.txt**

plaintext

config system global

set admin-https-redirect disable

set admin-lockout-duration 1

set admin-lockout-threshold 10

set admin-server-cert "self-sign"

set admintimeout 480

set alias "FortiGate-VM64"

set gui-auto-upgrade-setup-warning disable

set gui-firmware-upgrade-warning disable

set hostname "Local-FortiGate"

set management-port-use-admin-sport disable

set proxy-auth-timeout 5

set timezone 04

end

* **admin\_profile\_config.txt**

plaintext

config system accprofile

edit "prof\_admin"

set secfabgrp read-write

set ftviewgrp read-write

set authgrp read-write

set sysgrp read-write

set netgrp read-write

set loggrp read-write

set fwgrp read-write

set vpngrp read-write

set utmgrp read-write

set wanoptgrp read-write

set wifi read-write

next

end

* **interface\_config.txt**

plaintext

config system interface

edit "port1"

set vdom "root"

set ip 10.200.1.1 255.255.255.0

set allowaccess ping https ssh http fgfm

set type physical

set snmp-index 1

next

edit "port2"

set vdom "root"

set ip 10.200.2.1 255.255.255.0

set allowaccess ping https ssh http

set type physical

set snmp-index 2

next

edit "port3"

set vdom "root"

set ip 10.0.1.254 255.255.255.0

set allowaccess ping https ssh http telnet

set type physical

set snmp-index 3

end

**4. Create the Lab Guide Files**

Provide detailed steps in the lab\_guide/ directory.

* **prerequisites.md**

markdown

# Prerequisites

Restore the configuration file to Local-FortiGate:

1. Connect to the Local-FortiGate GUI and log in.

2. Click admin > Configuration > Revisions.

3. Expand the list and select the configuration with the comment "initial", then click Revert.

4. Click OK to reboot.

* **exercise1\_proxy\_based.md**

markdown

# Exercise 1: Using Antivirus Scanning in Proxy-Based Inspection Mode

1. Change the Antivirus Profile Inspection Mode:

- Edit the default antivirus profile to use Proxy-based mode.

2. Enable the Antivirus Profile on a Firewall Policy:

- Edit the Full\_Access firewall policy to use Proxy-based inspection mode.

- Enable the default antivirus profile and use the certificate-inspection profile for SSL inspection.

* **exercise1\_flow\_based.md**

markdown

# Exercise 1: Using Antivirus Scanning in Flow-Based Inspection Mode

1. Change the Antivirus Profile Inspection Mode:

- Edit the default antivirus profile to use Flow-based mode.

2. Enable the Antivirus Profile on a Firewall Policy:

- Edit the Full\_Access firewall policy to use Flow-based inspection mode.

- Enable the default antivirus profile and use the certificate-inspection profile for SSL inspection.