
Advanced FortiGate Security Profiles

Internship Program Graduation Project

Presented to: Dr. Hussein Harb

Instructed by: Eng. Mario Aiad

Prepared by: Group A

1. Morkos Bekhit – Research and Presentation on Security Profiles
2. Youssef Tarek – Configuring and Applying Security Profiles
3. Youssef Rafeek – Implementing Monitoring and Reporting Features
4. Abdullah Ramadan – Compiling the Final Report and Presentation

Program: FortiGate Administrator Certification Internship

Organization: Digital Egypt Pioneers Initiative – Egyptian Ministry of Communications & Information Technology (MCIT)

Submission Date: Wednesday April 23, 2025

Table of Contents

1. Introduction
 2. Project Plan and Timeline
 3. Week 1: Understanding Security Profiles
 4. Week 2: Configuring Security Profiles
 5. Week 3: Monitoring and Reporting
 6. Week 4: Final Presentation and Report
 7. Risk Management and Communication
 8. Summary and Recommendations
 9. Certificate Operations Overview
 10. Appendix
-

1. Introduction

This report documents our four-week project focused on Fortinet's advanced security profiles. As recent graduates participating in the FortiGate Administrator Internship program, our objective was to understand, implement, and monitor FortiGate security profiles to improve network protection against evolving threats.

2. Project Plan and Timeline

Team Formation:

- The team consists of four members with designated roles.
- A team leader was appointed to ensure coordination and timely communication with the instructor.

Task Distribution:

- **Morkos Bekhit:** Security Profiles Research & Presentation
- **Youssef Tarek:** Configuration and Implementation
- **Youssef Rafeek:** Monitoring and Reporting
- **Abdullah Ramadan:** Final Report and Presentation Compilation

Execution Timeline:

- **Week 1:** Understanding Security Profiles (Morkos Bekhit)
- **Week 2:** Configuring Security Profiles (Youssef Tarek)
- **Week 3:** Monitoring and Reporting (Youssef Rafeek)
- **Week 4:** Final Report & Presentation (Abdullah Ramadan)



3. Week 1: Understanding Security Profiles

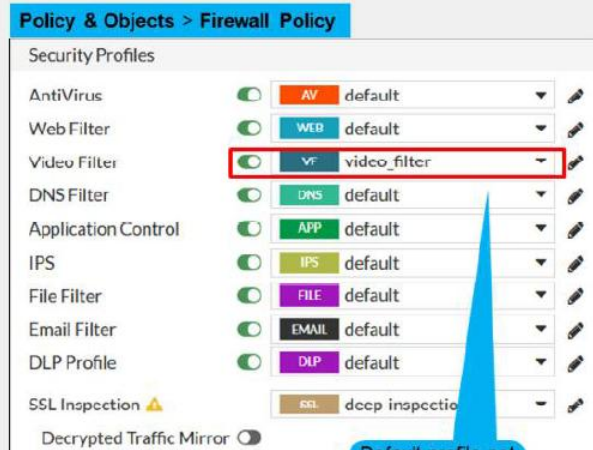
Objective: To research and understand the core FortiGate security profiles: Antivirus, Web Filtering, Application Control, IPS, and DNS Filtering, and more. Configuring security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites, It is one of the most important features that a firewall policy can apply, A security profile inspects each packet in the traffic flow, where the session has already been conditionally accepted by the firewall policy.

When inspecting traffic, FortiGate can use one of two methods: flow-based inspection or proxy-based inspection. Different security features are supported by each inspection type.

Note: By default, the **Video Filter**, **VOIP**, **Web Application Firewall** security profiles options are not visible on the policy page on GUI. We need to enable them on **Feature Visibility** page.

Security Profiles

- Firewall policies limit access to configured networks
- Security profiles configured in firewall policies protect your network by:
 - Blocking threats
 - Controlling access to certain applications and URLs
 - Preventing specific data from leaving your network



Key Concepts:

- **Antivirus:** Scans traffic for viruses, malware, and spyware.

Antivirus and Inspection Modes

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

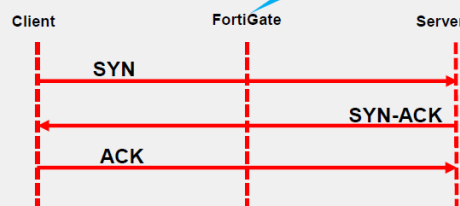


- Available inspection modes

Flow-based inspection

- Default inspection mode

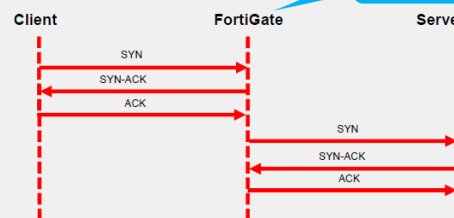
File is scanned on a flow basis



Proxy-based inspection

- Provides additional options

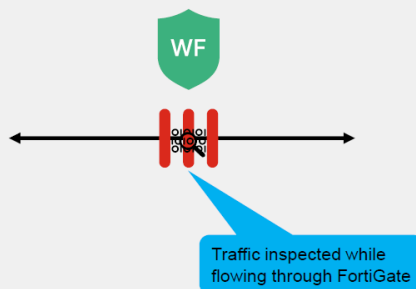
Two TCP connections



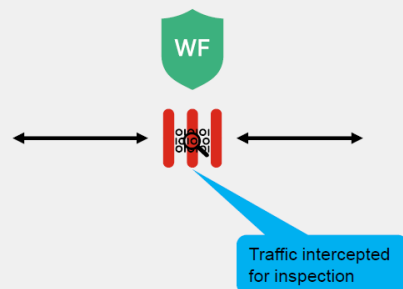
- **Web Filtering:** Controls access to web content by category or URL.

Web Filtering Inspection Modes

- Flow-based inspection
 - Default inspection mode
 - Requires fewer processing resources
 - Faster scanning



- Proxy-based inspection
 - More thorough inspection
 - Provides additional options
 - More resource intensive



Inspection Modes on Firewall Policies

- Enabling profiles has an impact on firewall throughput
- FortiGate kernel inspect sessions to enforce filtering (for example, web filter)
- Selecting the FortiGate inspection modes on firewall policies:
 - Flow-based
 - Default mode
 - Optimize performance
 - Proxy-based
 - Processed by CPU
 - Provides thorough inspection
 - Support advanced features like *safe search*

Policy & Objects > Firewall Policy

Create New Policy

Name	Internet_Access
Type	Standard ZTNA
Incoming Interface	LAN (port3)
Outgoing Interface	ISP1 (port1)
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	All
Action	ACCEPT DENY
Inspection Mode	Flow-based Proxy-based

- **Application Control:** Identifies and manages applications by behaviour and protocol.

Application Control

- Uses the IPS engine in flow-based scan
- Detects and acts on network application traffic
- Appropriate for detecting peer-to-peer (P2P) applications

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 14

- **Intrusion Prevention System (IPS):** Detects and blocks exploits, buffer overflows, and known vulnerabilities.

IPS

IPS components include:

- IPS signature databases
- Protocol decoders
- IPS engine

Flow-based detection blocking anomalies and exploits

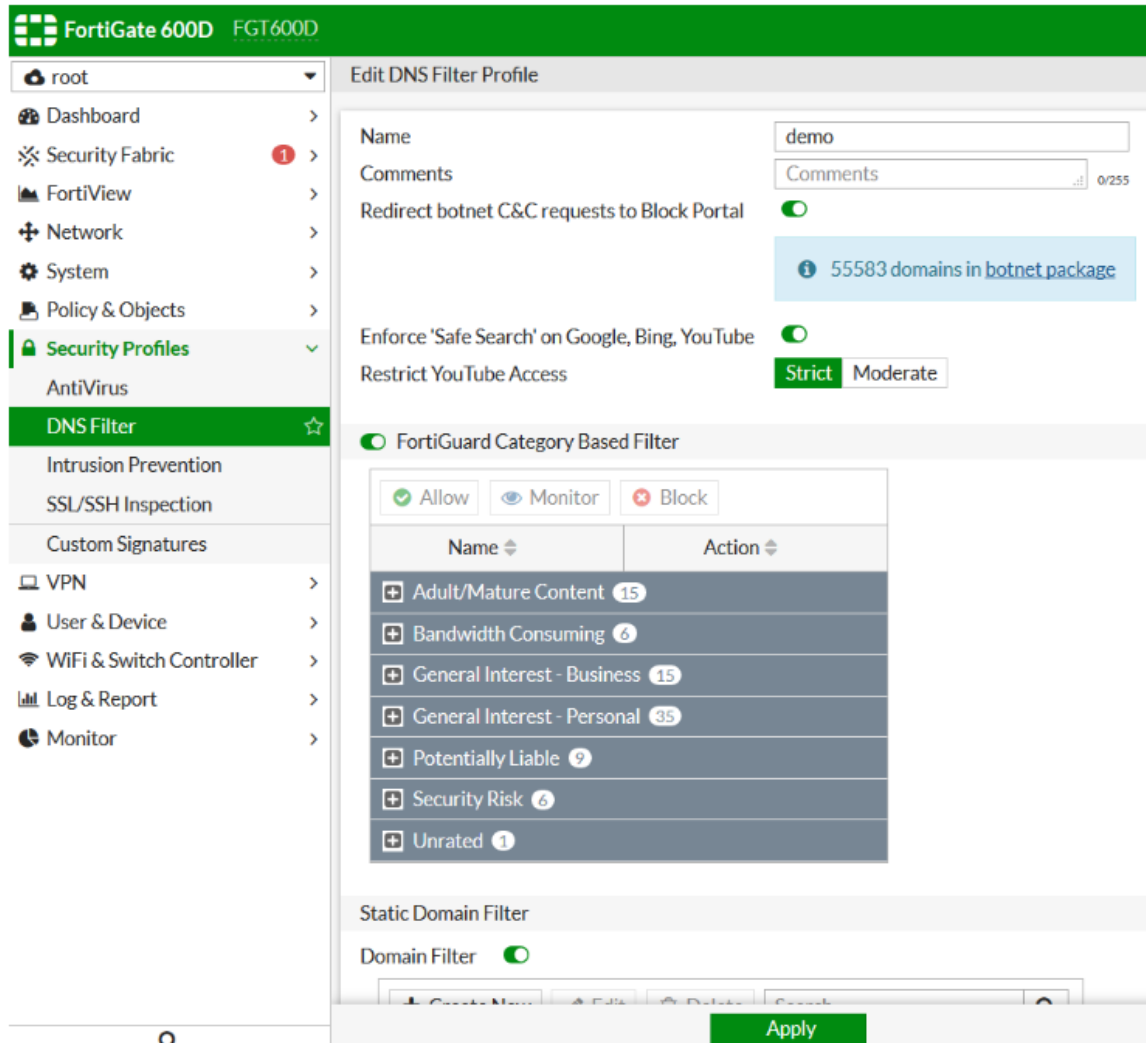
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 3

- **DNS Filtering:** Prevents access to malicious or inappropriate domains.

To create or configure DNS Filter profile in the GUI:

1. Go to *Security Profiles > DNS Filter*.
2. You can modify the default DNS Filter and enable the options you want or you can click + at the top right to create a new DNS Filter.



4. Week 2: Configuring Security Profiles

Objective: To configure and apply various security profiles within the FortiGate firewall.

Tasks Completed:

- Created custom Antivirus and Web Filtering profiles
- Applied security profiles to existing firewall policies
- Configured Application Control to block P2P and proxy apps

To verify the antivirus profile

1. Connect to the Local-FortiGate GUI, and then log in with the username
2. Click **Security Profiles > AntiVirus**.
3. Right-click the **default** antivirus profile, and then click **Edit**.
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**

Inspected Protocols

- HTTP ☒
- SMTP ☒
- POP3 ☒
- IMAP ☒
- FTP ☒**
- CIFS ☐

Best Practices:

- Assign different profiles to internal and guest networks
- Use custom categories for specific business policies

2. Locate the antivirus log message from when you tried to access the file using FTP, and then double-click the log entry to view the security details.

Date/Time	Service	Source	File Name	Virus/Botnet	User
2023/09/15 09:47:36	FTP	10.0.1.10	eicar.com	EICAR_TEST_...	
2023/09/15 09:47:36	FTP	10.0.1.10	eicar.com	EICAR_TEST_...	
2023/09/15 09:47:36	FTP	10.0.1.10	eicar.com	EICAR_TEST_...	

Log Details

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

5. Week 3: Monitoring and Reporting

Objective: To monitor traffic logs and generate reports to evaluate the effectiveness of applied security profiles. Security Profiles help to provide appropriate security for network. Proper logging configuration can also help us to analyze, diagnose, and resolve common network issues.

Monitoring Tools Used:

- FortiView
- Log & Report > Application Control, Web Filter Logs

- Custom report generation in FortiAnalyzer (if available)

Logging on FortiGate records the traffic that passes through, start from, or end on FortiGate. It records the actions during the traffic scanning process. FortiGate supports sending all log types to several log services including its local storage which is subject to the disk available on different FortiGate models.

We can view traffic logs in **Logs & Reports > Forward Traffic**. Apply the filter needed to display the logs and then enter the Policy UUID in the filter field to display records that match the firewall policy. Select the source of the logs the historical time frame to reduce irrelevant log entries.

Monitor Traffic Logs

- FortiGate supports storing all type of logs in several log devices
 - FortiGate local and cloud
 - FortiAnalyzer local and cloud
 - Syslog
- View traffic logs in **Log & Report > Forward Traffic**
 - Apply filter to display relevant logs
 - Select the source of logs
 - Specify the historical time frame
- Right-click firewall policy and view matching traffic logs

The screenshot displays two main sections of the FortiGate GUI. The top section, titled 'Log & Report > Forward Traffic', shows a table of traffic logs with columns for Date/Time, Source, Destination, Application, Action, Result, and Policy ID. A red box highlights the 'Filter by ID' dropdown menu, which is set to 'Policy UUID'. A blue callout points to this filter, stating 'Apply the filter desired to reduce irrelevant log entries'. The bottom section, titled 'Policy & Objects > Firewall Policy', shows a list of policies. A red box highlights the 'Show matching logs' option in the context menu for a specific policy. A blue callout points to this option, stating 'Only logs matching the firewall policy are displayed in the forward traffic logs page'.

Observations:

- Malware downloads blocked by Antivirus profile
- High-risk websites blocked under Web Filtering
- Unauthorized proxy apps blocked through App Control

Monitoring Application Control Logging

The screenshot displays the Fortinet Security Events Log & Report interface. The top navigation bar shows 'Log & Report > Security Events'. The main content area is divided into two sections: 'Summary' and 'Logs'. The 'Summary' section shows '51 Events' and a table of top categories. The 'Logs' section shows a list of events with columns for Date/Time, Source, Destination, Application Name, and Action. A red box highlights the 'Application Control' icon in the top category list. Another red box highlights the 'Logs' tab in the top navigation bar. A third red box highlights the 'Details' button in the top navigation bar. A fourth red box highlights the 'Log Details' window, which shows application control information for a specific event. A blue callout bubble points to the 'Log Details' window with the text 'Application Control information'.

Log & Report > Security Events

Summary Logs

51 Events

Application Control

Top Category	Action	Count
Web.Client	Pass	40
Network.Service	Block	5
Video/Audio	Block	3

Logs

Date/Time	Source	Destination	Application Name	Action
2023/09/29 07:38:41	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	WebSocket	Block
2023/09/29 07:38:41	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	HTTPS.BROWSER	Pass
2023/09/29 07:38:32	10.0.1.10	105.125.190.58 (prod-ntp-5.ntp1.ps...)	NTP	Pass
2023/09/29 07:38:01	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	WebSocket	Block

Log Details

Application Control

Sensor: default

Application Name: DailyMotion

Application ID: 16072

Category: Video/Audio

Application Risk: Low

Protocol: 6

Service: HTTP

Message: Video/Audio: DailyMotion

Action

Action: Block

Policy ID: 1 (Application Control)

Policy UUID: b11ac58c-791b-51e7-4600-12f829a689d9

Policy Type: Firewall

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved. 26

6. Week 4: Final Presentation and Report

Objective: Compile all tasks and findings into a final report and presentation.

Actions Taken:

- Integrated research, configuration, and monitoring content
- Formatted slides and designed visuals for clarity
- Reviewed the report against project requirements

Deliverable: Final PDF Report and PowerPoint Presentation

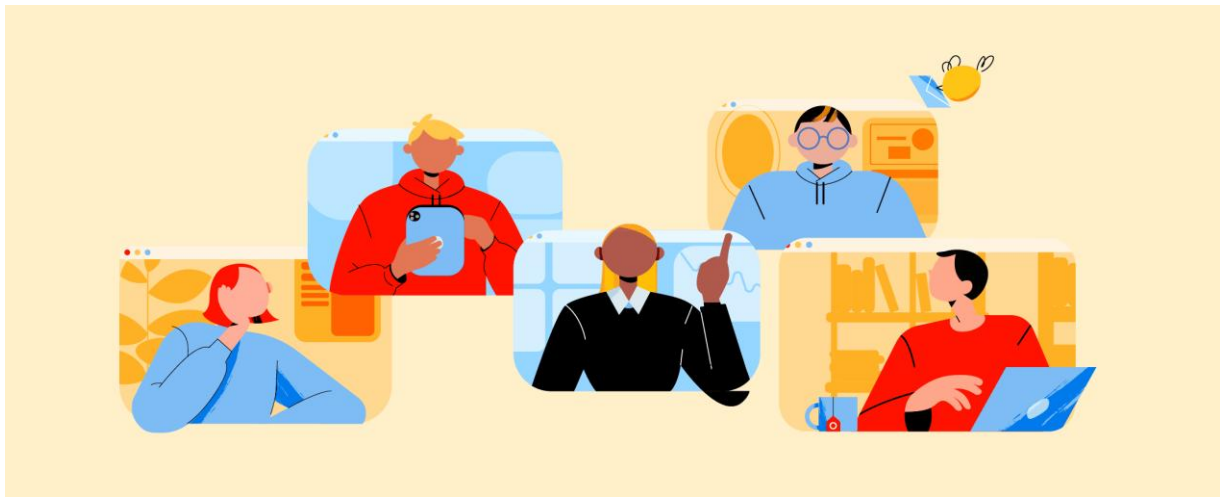
7. Risk Management and Communication

Risk Management:

- **Delay in configuration setup:** Assigned a backup member to assist
- **Lack of understanding of FortiGate settings:** Referred to Fortinet course documentation/labs and online resources
- **Ineffective coordination:** Regularly team check-ins and clear role assignments resolved this

Communication Strategy:

- Used Microsoft Teams, What's App and Google Drive for Docs collaboration
- Regularly virtual meetings to track progress



8. Summary and Recommendations

Summary:

Over four weeks, the team effectively:

- Understood FortiGate security profiles
- Configured and applied real use-case scenarios
- Monitored their effectiveness with Fortinet tools

Recommendations:

- Enable SSL deep inspection for full content visibility
- Use FortiAnalyzer (if available) for detailed insights and history
- Automate log backup and periodic report generation

9. Certificate Operations Overview

Although not the central focus, certificate management plays a crucial role in securing advanced FortiGate features such as SSL deep inspection and secure web filtering.

FortiGate Uses digital Certificates for inspections, mainly outbound or inbound traffic inspection, if FortiGate trusts the certificate, it permits the connection. But if FortiGate does not trust the certificate, it can prevent the connection, FortiGate also inspect certificates to identify people and devices, before it permits a person or device to make a full connectio to the entity that it is protecting.

Why Does FortiGate Use Digital Certificates?

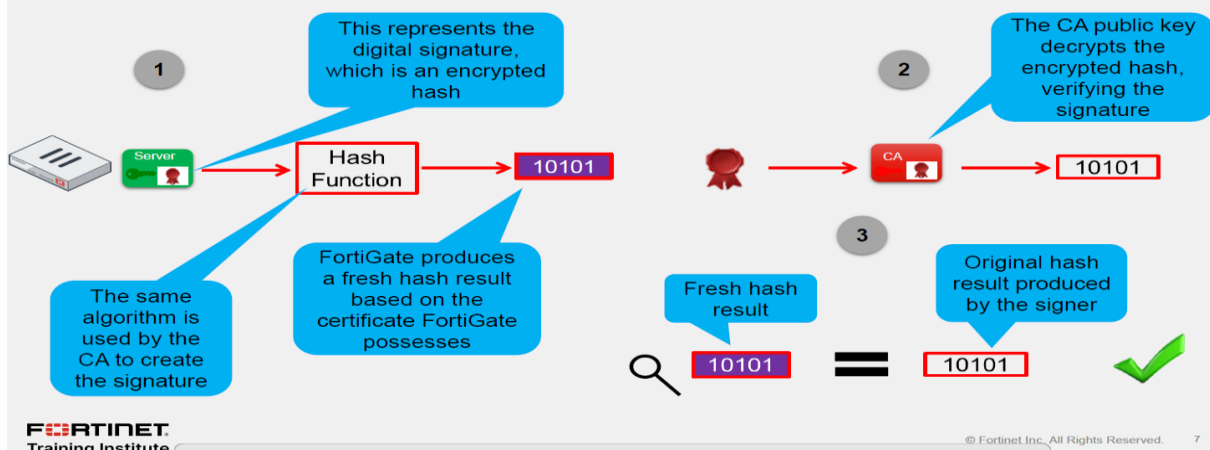
- Inspection
 - SSL/SSH and HTTPS traffic inspection
 - Inbound or outbound traffic through FortiGate
 - Traffic to and from FortiGate
- Privacy
 - Ensure privacy for exchanges with other devices, such as FortiGuard
- Authentication
 - User authentication for network access
 - User authentication for VPN connection
 - As second-factor authentication for FortiGate administrator

Certificate Operations Summary:

- Uploaded and installed SSL certificates to FortiGate for web filtering and VPN inspection
- Applied certificates to SSL inspection profiles
- Validated certificate trust on endpoint devices to prevent browser security alerts

FortiGate Uses SSL to ensure that data remains private when connecting with servers, such as FortiGuard, and with clients, such as a web browser. Another Feature of SSL is that FortiGate can use it to identify one or both parties using certificates.

FortiGate Verifies a Digital Signature

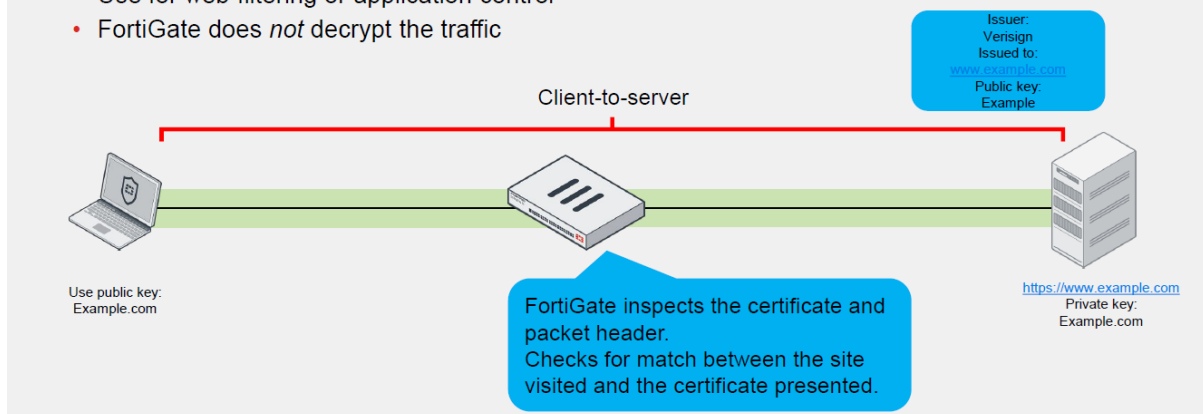


Example Tasks Performed:

- Generated and imported a local certificate into FortiGate
- Assigned the certificate to a deep inspection profile
- Tested browsing behaviour to verify SSL decryption and re-encryption

SSL Inspection Modes

- SSL certificate inspection
 - Relies on extracting the FQDN of the URL from either
 - TLS extension server name indication (SNI)
 - SSL certificate **Subject** or Subject Alternative Name (**SAN**) fields
 - Use for web filtering or application control
 - FortiGate does *not* decrypt the traffic



Example Screenshot:

Certificates enhance the accuracy of threat inspection, ensuring encrypted traffic can be scanned while maintaining user trust.

How Does FortiGate Trust Certificates?

- FortiGate does the following checks against a certificate before trusting it and using it:
 - Revocation check
 - CA certificate possession
 - FortiGate uses the **Issuer** value to determine if FortiGate possesses the corresponding CA certificate
 - Without the corresponding CA certificate, FortiGate cannot trust the certificate
 - Validity dates
 - Digital signature validation
 - The verification of the digital signature on the certificate must pass

Field	Value
Version	V3
Serial number	0cacbf0403e86fc4ba3da5f26b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	Sunday, 26 February 2023 02:...
Valid to	Thursday, 28 March 2024 01:...
Subject	training.fortinet.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=c03152cd5a50c3827c7...
Subject Key Identifier	54c8bdc749bd966ac110f515d...
Subject Alternative Name	DNS Name=training.fortinet.c...
Enhanced Key Usage	Server Authentication (1.3.6...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
SCT List	v1, eecdd064d5db1acec55cb7...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	5a09781b2bc9d911f18c2d285...

10. Appendix

FortiOS Version: [V7.0.x - v7.4.x]

Device Model: FortiGate Administration (Lab Environment)

Sample Policy Configuration:

```
config firewall policy
  edit 10
    set name "Secure-Access"
    set srcintf "lan"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set av-profile "AV-Custom"
    set webfilter-profile "WF-Strict"
    set application-list "App-Control-1"
  next
end
```

Teamwork Members:

Morkos Bekhit – Security Profiles Research

Youssef Tarek – Configuration & Testing

Youssef Rafeek – Monitoring & Logging

Abdullah Ramadan – Reporting & Documentation

Thank you for your time,