FORTIGATE SECURITY PROFILES

PROJECT 4: ADVANCED FORTIGATE SECURITY PROFILES

BY: NADA NASR
EMAN MOAMEN
SEIF WAEL
AHMED OSAMA
SHAHD OSAMA

UNDERSTANDING SECURITY PROFILES

The Challenge:

Traditional firewalls control where traffic can go (IP/Port), but they can't see what is inside the traffic. A malicious file or a phishing link can easily slip through.

The Solution: Security Profiles

Security Profiles are advanced, integrated security engines that inspect the content of your network traffic. They act as a deep packet inspection force, identifying and blocking modern threats like malware, ransomware, and phishing attempts before they reach your users.

WHAT ARE SECURITY PROFILES?

Antivirus: Scans files (HTTP, FTP, SMTP) in real-time against a massive database of known malware signatures.

Web Filter: Controls which websites users can visit, blocking malicious, inappropriate, or unproductive sites.

Application Control: Identifies and controls access to thousands of individual applications (e.g., Facebook, Skype, BitTorrent), regardless of the port they use.

IPS (Intrusion Prevention System): Blocks attempts to exploit vulnerabilities in your systems and applications.

ANTIVIRUS

What is the Antivirus?

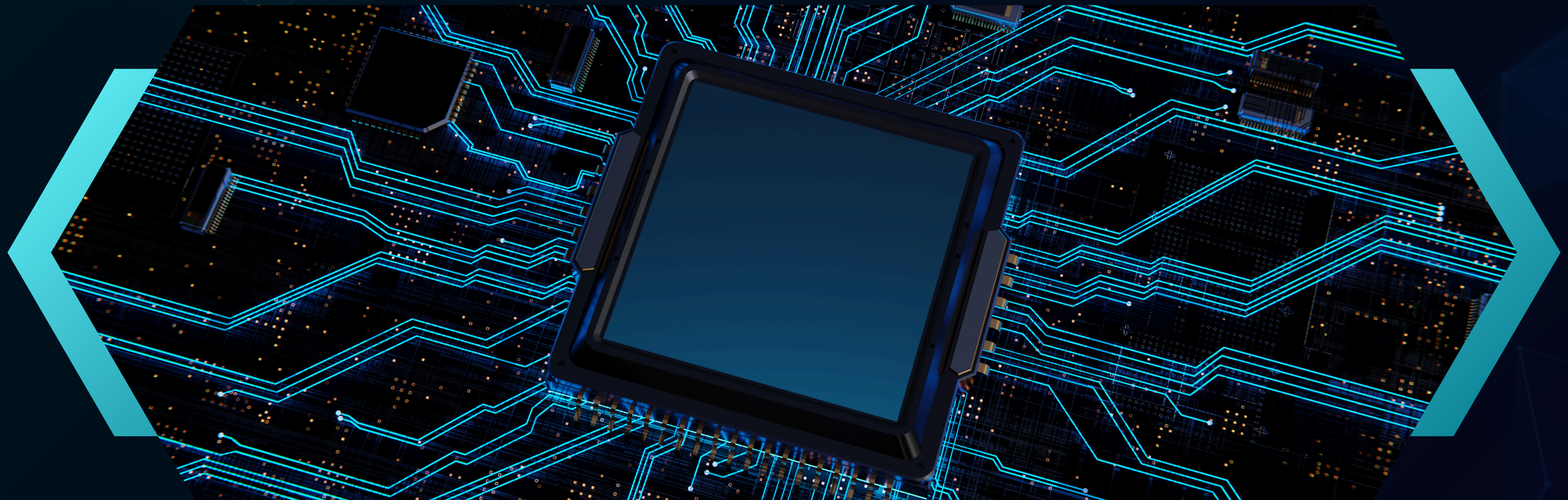
A primary function of an antivirus scan is to detect and stop viruses that could cause harm to your system or compromise the security of your connected devices. It can be installed on individual endpoints (FortiClient), or it can operate as an antivirus engine to perform traffic inspection inside a next generation firewall (NGFW).

How It Works

The Antivirus profile scans files, emails, and web traffic for malware or viruses.
It blocks or quarantines infected files before they reach the user's device.

Example

- Scans downloads and attachments
- Protects against ransomware and trojans



ANTIVIRUS TECHNIQUES

Order of scans

1 ***Antivirus Scan***

This scan is the first, fastest, simplest way to detect malware. It detects viruses that are an exact match for a signature in the antivirus database

2 ***Grayware Scan***

This scan detects unsolicited programs, known as grayware, that have been installed without the user's knowledge or consent. Often, grayware can be detected with a simple FortiGuard grayware signature.

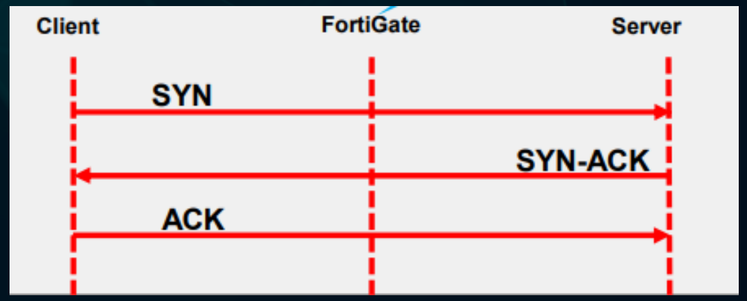
3 ***AI Scan***

Uses AI and machine learning to identify suspicious behavior or patterns in files, helping detect new and unknown threats (zero-day malware) that lack known signatures.

ANTIVIRUS INSPECTION MODES

While both modes offer significant security, proxy-based mode provides more feature configuration options, while flow-based mode is designed to optimize performance.

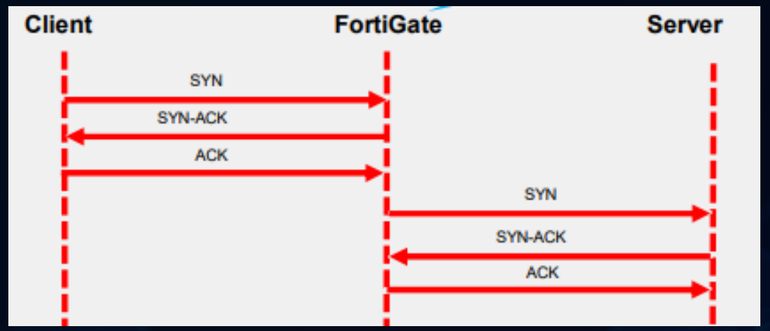
01 *Flow-based inspection*



Definition: Antivirus scans traffic through a proxy server before it reaches the user.
How it works: The proxy inspects files and web traffic for malware signatures and blocks or cleans threats before they enter the network.

Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

02 *Proxy-based inspection*



Definition: Analyzes only the first part of the data stream instead of the entire file.
How it works: It scans data “on the fly” while it’s being transferred, allowing faster detection without delaying the user’s connection.

Proxy-based inspection reconstructs content that passes through FortiGate and inspects the content for security threats.

WEB FILTERING

01 What is Web Filtering?

Web Filtering is a FortiGate security profile used to control and monitor users' access to websites.
It helps organizations block malicious, inappropriate, or non-productive websites.

The filtering process is based on categories, reputation ratings, or specific URLs.

02 Example:

- Blocking access to social media or adult content during work hours to increase productivity and maintain security.

BENEFITS OF WEB FILTERING

- Improves Security: Prevents access to malicious or phishing sites.
- Increases Productivity: Limits access to time-wasting websites.
- Protects Bandwidth: Reduces unnecessary internet traffic.
- Ensures Compliance: Helps organizations follow internet usage policies.

Web Filtering is an essential layer of network protection in any modern organization

APPLICATION CONTROL

- FortiGate provides Security Profiles to manage and protect network traffic.
- Application Control identifies and controls applications running across the network — even if they use non-standard ports or encryption.

Purpose:

- Block risky or unauthorized applications
- Limit bandwidth-hungry apps (e.g., streaming or torrents)
- Improve network visibility and security

HOW APPLICATION CONTROL WORKS

How It Works:

- FortiGate inspects traffic using deep packet inspection (DPI).
- It identifies applications by signatures, behaviors, or protocols.
- Based on configured policies, it can allow, block, monitor, or shape app traffic.

Configuration Steps:

- Go to Security Profiles → Application Control
- Create or edit a profile
- Select apps or categories to block/allow (e.g., P2P, Social Media, Gaming)
- Apply profile to a Firewall Policy
- Monitor logs under Application Control Logs

WHY USE SECURITY PROFILES

1. DEEP INSPECTION OF TRAFFIC

FortiGate firewalls don't just allow or deny traffic — security profiles let them inspect the content of packets (files, websites, applications, etc.) to find viruses, malware, or suspicious behavior.

2. LAYERED SECURITY

Each profile protects a different part of the network:

- Antivirus → stops malware and trojans
- Web Filter → blocks harmful or unwanted websites
- Application Control → controls which apps can run
- IPS → detects network attacks
- DNS Filter → stops access to malicious domains

Together, they form a multi-layered defense system.

3. PROTECTION AGAINST MODERN THREATS

Modern attacks often hide inside encrypted traffic (SSL/TLS) or come from trusted apps. Security profiles let FortiGate inspect these safely to catch hidden threats.

WHY USE SECURITY PROFILES

4. REAL-TIME THREAT INTELLIGENCE

FortiGate uses FortiGuard Labs — a global intelligence network — to update profiles automatically with new virus signatures, URL categories, and IPS rules.
This ensures the firewall is always up to date against the newest threats.

5. USER CONTROL & POLICY ENFORCEMENT

Administrators can apply security policies using profiles — for example:

- Allow employees to browse work sites only
- Block downloads of certain file types
- Monitor or restrict streaming apps

6. VISIBILITY AND REPORTING

Profiles give detailed logs and analytics — you can see what websites are visited, which apps are used, and what threats were blocked.

SUMMARY

We use FortiGate Security Profiles to provide intelligent, real-time protection against cyber threats by inspecting and controlling traffic at multiple levels — keeping the network safe, efficient, and compliant.

REFERENCES

Information collected from:

- Fortinet Documentation
- FortiGate User Guide
- Network Security Training Materials

THANK YOU

PROJECT 4: ADVANCED FORTIGATE SECURITY PROFILES