

Security Profiles:

FortiGate firewall Security Profiles are added to the end of every security policy rules. FortiGate line combines number of security features to protect network from threats. After every packet has been allowed by the security policy, security profiles are used. In Fortigate security Profile scan packets for threats, vulnerabilities, viruses & spyware. Security Profile also scan packets for malicious URLs, and exploitation software as well. Security Profile check and scanned the traffic for suspicious file uploads or downloaded. In Fortigate allowed traffic is analyzed for virus, spyware or content using security profile. In Fortigate Threat log keeps records of Anti-Virus, Anti-Spyware that can be reviewed.

Where security policies provide the instructions to the FortiGate unit for controlling what traffic is allowed through the device, the Security profiles provide the screening that filters content coming and going on the network. Security profiles enable you to instruct the FortiGate unit about what to look for in the traffic that you don't want, or want to monitor, as it passes through the device. A security profile is a group of options and filters that you can apply to one or more firewall policies. Security profiles can be used by more than one security policy. You can configure sets of security profiles for the traffic types handled by a set of security policies that require identical protection levels and types, rather than repeatedly configuring those same security profile settings for each individual security policy. Security profiles are available for various unwanted traffic and network threats. Each are configured separately and can be used in different groupings as needed. You configure security profiles in the Security Profiles menu and applied when creating a security policy by selecting the security profile type.

Antivirus	Web Filter	DNS Filter
Application Control	Intrusion Prevention IPS	Email Filter
Data Leak Prevention DLP	VoIP Solutions	ICAP
Web Application Firewall	Inspection Modes	Overrides

	Flow Mode Inspection Policy		Proxy Mode Inspection Policy	
UTM Profile	GUI	CLI	GUI	CLI
Antivirus	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes
CIFS Inspection	No	No	No	Yes
Data Leak Prevention	No	Yes	Yes	Yes
DNS Filter	Yes	Yes	Yes	Yes
Email Filter	No	Yes	Yes	Yes
ICAP	No	No	Yes	Yes
Intrusion Prevention System	Yes	Yes	Yes	Yes
SSL/SSH Inspection	Yes	Yes	Yes	Yes
VoIP	Yes	Yes	Yes	Yes
Web Filter	Yes	Yes	Yes	Yes
Web Application Firewall	No	No	Yes	Yes

Security Profiles:

FortiGate Firewalls provide a range of security features through their security profiles. These profiles help protect your network by inspecting and controlling traffic based on various criteria.

Imagine FortiGate as a Security Guard at the entrance of a building. This guard checks everyone who wants to come in and out to make sure they're not causing trouble. Now, the guard has different tools to do this job effectively. These tools are like the FortiGate Security Profiles.

In simple terms, FortiGate Security Profiles are like different skills or tools the guard (firewall) has to keep your computer network safe. By using these tools wisely, the guard helps make sure only the good stuff comes in and the bad stuff stays out.

Antivirus (AV):

This profile scans traffic for known viruses, worms, Trojans, and other malware. It uses signature databases to identify and block malicious files.

Intrusion Prevention System (IPS):

IPS examines traffic for patterns indicative of known attacks. It helps prevent network and system vulnerabilities from being exploited.

Web Filtering:

This profile allows you to control access to websites based on categories, helping to prevent users from accessing malicious or inappropriate content.

Application Control:

This profile enables you to control access to applications and services. You can define policies to allow or block specific applications.

DNS Filtering:

FortiGate can block access to malicious or unwanted websites by filtering DNS requests based on predefined categories.