FortiGate Offline IPS Deployment
Version 3.0 MR1

FORTINET

www.fortinet.com

FortiGate Offline IPS Deployment Technical Note
Version 3.0 MR1
May 31, 2006
01-30001-0326-20060531

Trademarks

FortiGate Offline IPS Deployment

This document covers FortiGate deployment as an offline intrusion protection system (IPS). FortiGate Antivirus Firewalls are optimized as in line security devices but it's flexible design allows the FortiGate to be deployed as an offline intrusion detection system, monitoring network traffic from mirrored or spanned switch ports or using a network tap device to forward incoming and outgoing data streams to multiple ethernet ports.

Deployment Scenarios

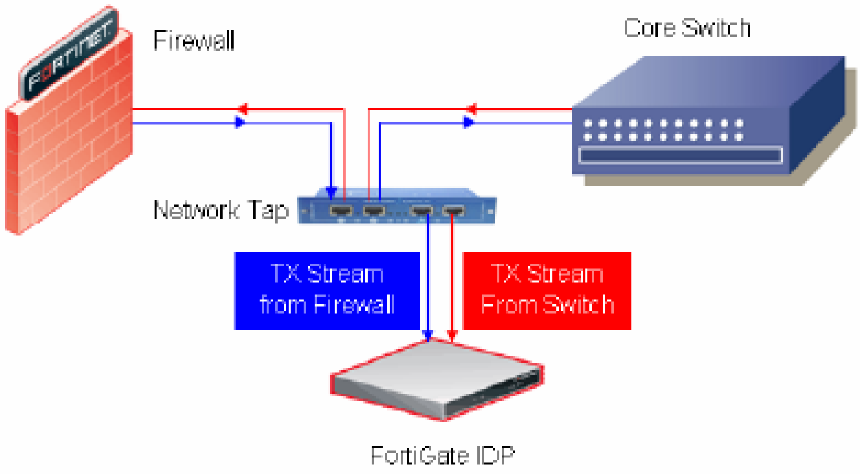
An Intrusion Detection system (IPS) is typically used as a second line of defense when deployed in conjunction with a firewall. As such, for the IPS to be effective it must be deployed in a location where it can see all the traffic that passes through the firewall before that traffic is forwarded to the trusted network.

This section will cover two scenarios. One where the Fortigate unit uses a network tap and one where it uses mirrored ports.

Scenario 1: Utilizing Network Taps

Figure 1 shows a FortiGate system deployed directly behind a firewall where it monitors and inspects all traffic coming from and going to the core switch or router. This scenario uses an external network tap which splits the incoming traffic from both the firewall and the core switch, and forwards it to the ports the FortiGate system is listening to. For fiber connections a Y-cable can be uses to redirect packets to an IPS unit.

Figure 1: FortiGate IPS monitors traffic using an external network tap or Y-cable



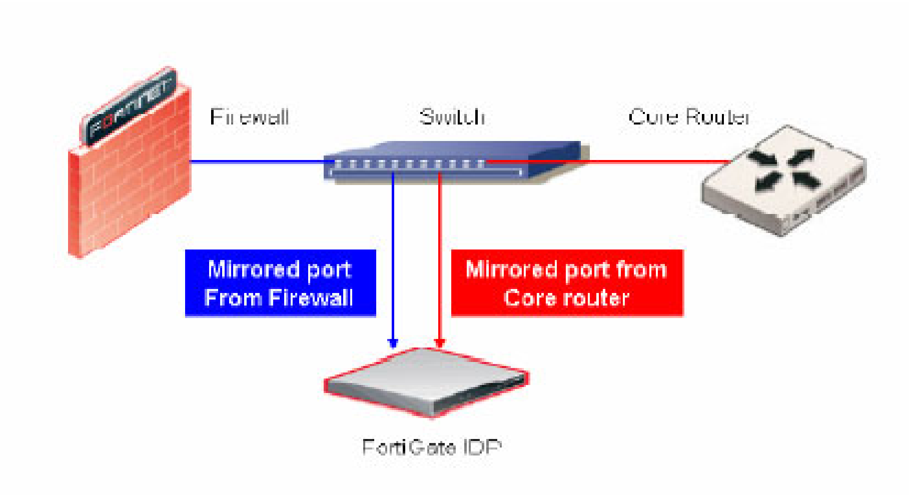
In this configuration the FortiGate system is able to send alerts and event logs to centralized reporting servers.

.

Scenario 2: Utilizing Mirrored Ports

Figure 2 shows how the fortiGate unit can be used to monitor traffic from mirrored or span switch ports.

Figure 2: FortiGate IPS monitors traffic from mirrored switch ports.



This configuration is more popular and cost effective as many modern network switches support port mirroring or port spanning. Similar to the first scenario, the FortiGate IPS unit monitors traffic incoming from the firewall and from the core internal router.

Both deployment scenarios, the FortiGate IPS configuration will be the same. An IPS protection profile will need to be created and used in two firewall policies. One policy will allow all inbound connections and the other will allow all outbound connections.

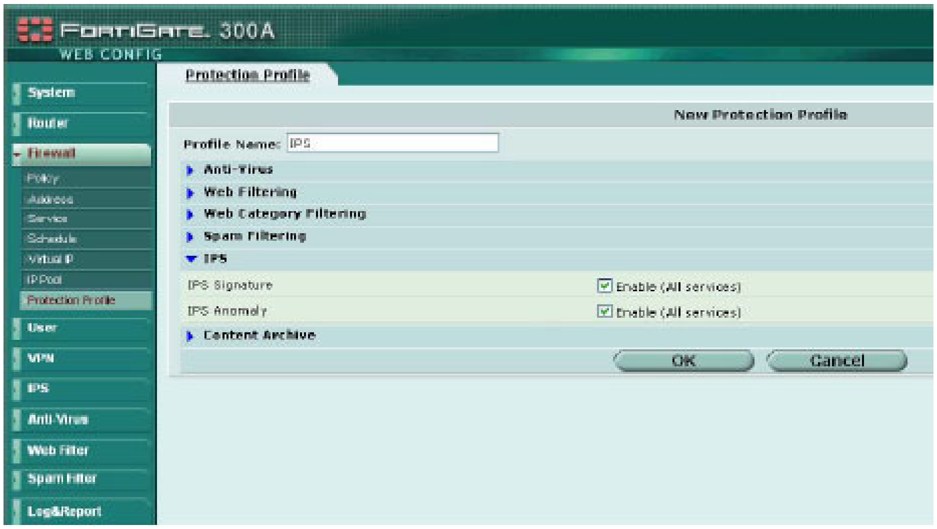
FortiGate IPS Configuration

The following sample procedure shows how to setup a fortiGate antivirus firewall system for intrusion detection and prevention monitoring.

To configure the Fortigate unit for IPS

1 Go to **Firewall > Protection Profile** to create a protection profile for IPS only.

Figure 3: Creating a firewall protection profile



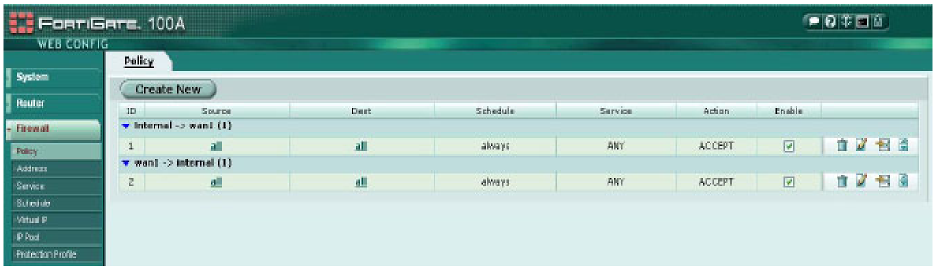
Profile Name: IPS

IPS Signature ☑ Enable (All services)

IPS Anomaly ☑ Enable (All services)

2 Go to **Firewall > Policy** to create 2 firewall policies, one for all inbound traffic and one for all outbound traffic.

Figure 4: Creating firewall policies

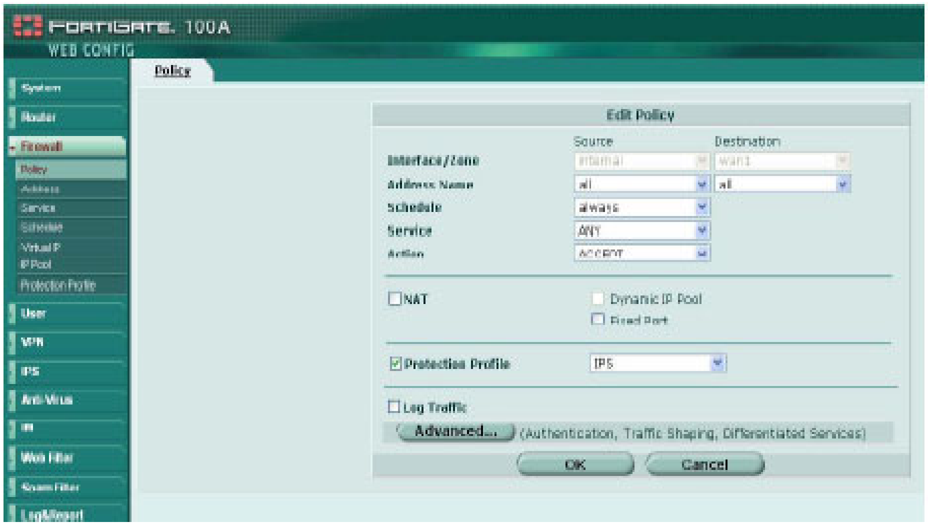


ID	Source	Dest	Schedule	Service	Action	Enable
internal -> wan1 (1)						
1	all	all	always	ANY	ACCEPT	☑
wan1 -> internal (1)						
2	all	all	always	ANY	ACCEPT	☑

Note: This example uses the Internal and Wan1 interfaces but this may be different in your design.

3 Select the IPS protection profile to activate the IPS monitoring for each firewall policy created.

Figure 5: Activating the IPS monitoring in the firewall policy



Edit Policy

	Source	Destination
Interface/Zone	internal	wan1
Address Name	all	all
Schedule	always	
Service	ANY	
Action	ACCEPT	

□ NAT □ Dynamic IP Pool
□ Fixed Port

☑ Protection Profile IPS

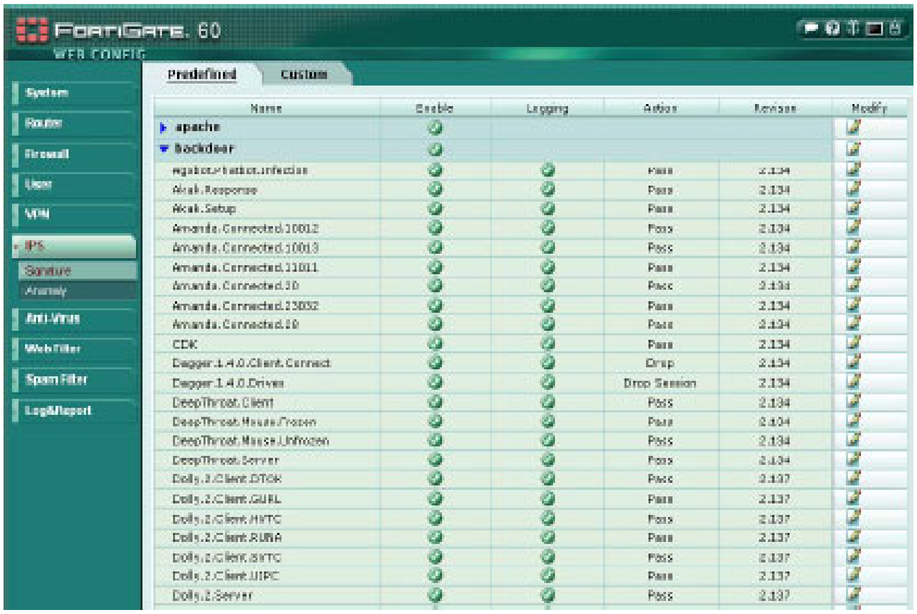
□ Log Traffic

Advanced... (Authentication, Traffic Shaping, Differentiated Services)

OK Cancel

4 Go to **IPS > Signature** to adjust the IPS anomaly rules and signatures if needed.

Figure 6: IPS anomaly and inspection rules and signatures



Name	Enable	Logging	Action	Revision	Modify
▸ apache	✓				✎
▾ backdoor	✓				✎
Agobot/Phatbot.Infection	✓	✓	Pass	2.134	✎
Akak.Response	✓	✓	Pass	2.134	✎
Akak.Setup	✓	✓	Pass	2.134	✎
Amanda.Connected.10012	✓	✓	Pass	2.134	✎
Amanda.Connected.10013	✓	✓	Pass	2.134	✎
Amanda.Connected.11011	✓	✓	Pass	2.134	✎
Amanda.Connected.10	✓	✓	Pass	2.134	✎
Amanda.Connected.23032	✓	✓	Pass	2.134	✎
Amanda.Connected.20	✓	✓	Pass	2.134	✎
CDK	✓	✓	Pass	2.134	✎
Dagger.1.4.0.Client.Connect	✓	✓	Drop	2.134	✎
Dagger.1.4.0.Drives	✓	✓	Drop Session	2.134	✎
DeepThroat.Client	✓	✓	Pass	2.134	✎
DeepThroat.Mouse.Frozen	✓	✓	Pass	2.134	✎
DeepThroat.Mouse.Unfrozen	✓	✓	Pass	2.134	✎
DeepThroat.Server	✓	✓	Pass	2.134	✎
Dolly.2.Client.DTOK	✓	✓	Pass	2.137	✎
Dolly.2.Client.GURL	✓	✓	Pass	2.137	✎
Dolly.2.Client.HKTC	✓	✓	Pass	2.137	✎
Dolly.2.Client.RUNA	✓	✓	Pass	2.137	✎
Dolly.2.Client.SKTC	✓	✓	Pass	2.137	✎
Dolly.2.Client.UIPC	✓	✓	Pass	2.137	✎
Dolly.2.Server	✓	✓	Pass	2.137	✎

Note: FortiNet enables all IPS signatures and anomaly inspection routines when they are activated in the protection profile. Not all suspicious traffic is blocked but all attacks and suspicious traffic patterns are logged. You can customize each signature, attack response, and logging feature to meet your specific needs.

For more information on how to customize IPS signatures and anomaly detection routines, please refer to the FortiGate Administrator's Guide for the hardware and FortiOS version you are using.