

FortiGate Offline IPS Deployment Version 3.0 MR1



www.fortinet.com

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

© Copyright 2005 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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.





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.



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

	Policy									
System	Create	New								
Router	ID	Source	Dert	Schedule	Service	Action	Enable			
Firewall	- Interne	-> wan1 (1)								
Policy	1	all	all	always	ANY	ACCEPT	4	1	1	1
Address	🔻 want -)	> internal (1)								
Service	2	all	all	ahvays	ANY	ACCEPT	1	1	2	1
Linedale										
Advent #1										



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.

Policy					
44		Edit Poli	icy		
		Source		Destination	
~	Interface/Zone	internal.	18	Wan1	
Anna Cal	Address Name	al	4	al	4
vice	Schedule	always	~		
enae	Service	ANY	*		
ad P ad	Action	ACCENT	4		
ector Polie		Dimanic	ID Dool		
r i	Chan	E Fired Po	rt.		
n i i i i i i i i i i i i i i i i i i i		Lana		-	
	Protection Profile	IP'S		<u>M</u>	
- Mitta	Log Traffic				
	(Advanced) (Au	thentication, Traffic	Shaping	, Differentiat	ed Services)
A Differ	-				

Figure 5: Activating the IPS monitoring in the firewall policy

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

	Predefined Custom							
System	Name	Fachie	Laurina	Arting	Levinu	Marifi		
Router	apache	CARDIO	croping	40003	New July	A COL		
Freed	* harkdear					11		
	analysis of artist televise			ALC: N		1		
User	Nucl. Languages	ő	0	Pass	2.134	1		
	Akras Cohum		ä	Para	2134	14		
VON	America Computed 20022		0	Page 1	2.124	1		
(PC)	America Connected 20012		0	Para	0.494	1		
	America Connected 22021		0	Dear	2,134	1		
Source	America Connected 3D			Pall	2 4 3 4	1		
Anamaly	Amenda Connected 13032		0	Dava	3 134	12		
Anti-Vinas	Amanda Carrected 10		0	Date	2 1 34	17		
	CTK	0	0	Pare	2134	1		
Weblinker	Decourt 4.0 Chert Carpect	0	à	Drap	2.134	1		
Span Filter	Decorr 1 d 0 Drives		0	Dirpo Samino	2134	1		
	DeeoThroat, Cleant	0	0	Pace	2.134	17		
Logalleport	DeeoThroat Massa Crozer		ő	Pare	2 4 9 4	1		
	DeepThroat May se J Infrasteo		0	Pace	2,134	1		
	DeepTroot.Server			Pais	2.1.54	1		
	Dols J.Clent DTok	0	0	Pace	2,197	14		
	Dolls 2 Chert GURL	0	0	Para	2,137	1		
	Dolls, 2 Client HVTC	0	0	Para	2.137	12		
	Dolls 2 Client RUBA		0	Para	2.137	1		
	tiols, a client surro	0	0	Pass	2.137	1		
	Dolls 2.Client UIPC	0	ő	Para	2.137	1		
	Dols 2 Server	0	0	Pace	2,132	12		

Figure 6: IPS anomaly and inspection rules and signatures



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.