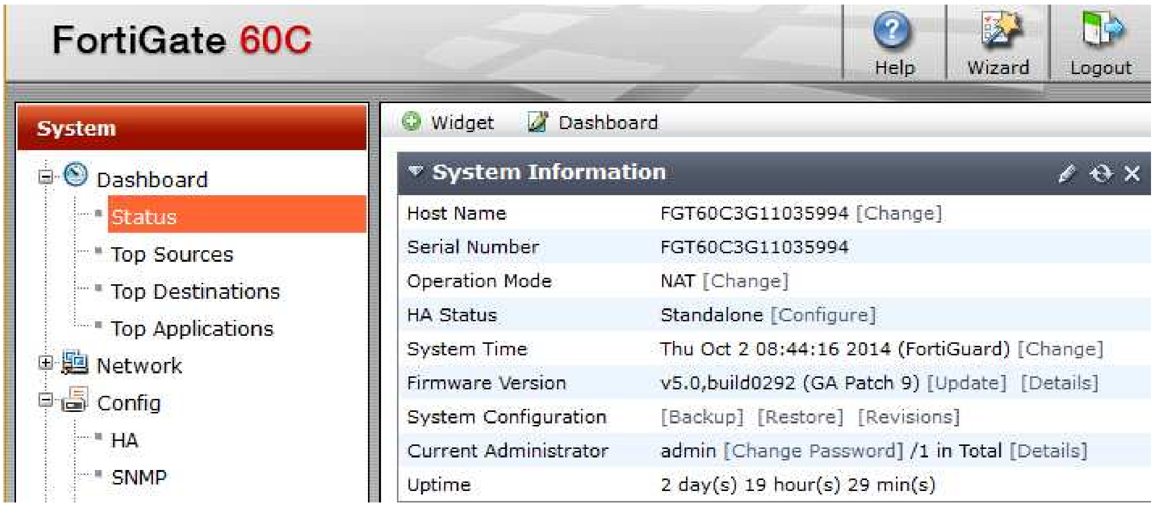
Configure a Data Link Prevention Sensor to block files by the extension.

Firmware versión 5.0.9



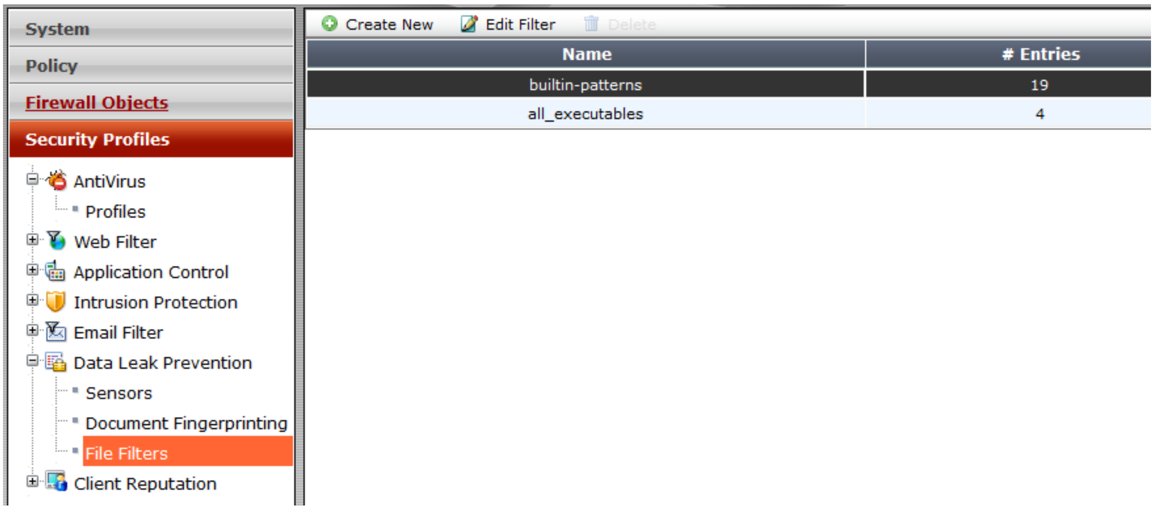
System Information

Host Name	FGT60C3G11035994 [Change]
Serial Number	FGT60C3G11035994
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Thu Oct 2 08:44:16 2014 (FortiGuard) [Change]
Firmware Version	v5.0,build0292 (GA Patch 9) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	2 day(s) 19 hour(s) 29 min(s)

Creating a file filter, Go to:

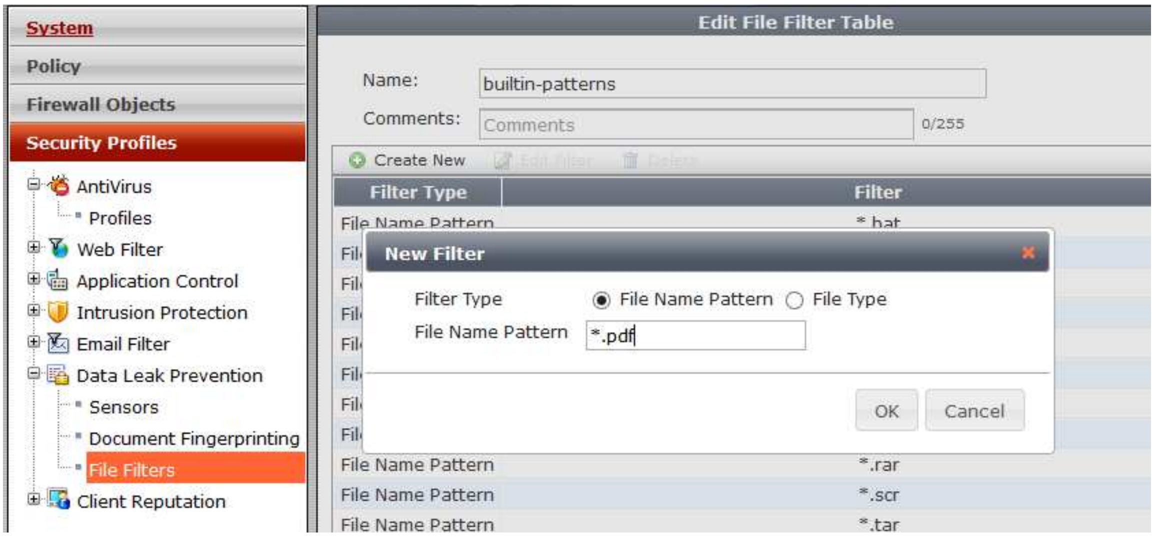
Security Profiles> Data Leak Prevention> File Filters.

Select“ builtin-patterns” and edit.



Name	# Entries
builtin-patterns	19
all_executables	4

After select; Create New and write: *.pdf



Name: builtin-patterns

Comments: Comments 0/255

Filter Type	Filter
File Name Pattern	*.bat
Fil	
Fil	
Fil	
Fil	
Fil	
Fil	
Fil	
File Name Pattern	*.rar
File Name Pattern	*.scr
File Name Pattern	*.tar

Filter Type ● File Name Pattern ○ File Type

File Name Pattern *.pdf

Clic Apply.

Creating a Sensor, Go to:

Security Profiles > Data Leak Prevention > Sensors.

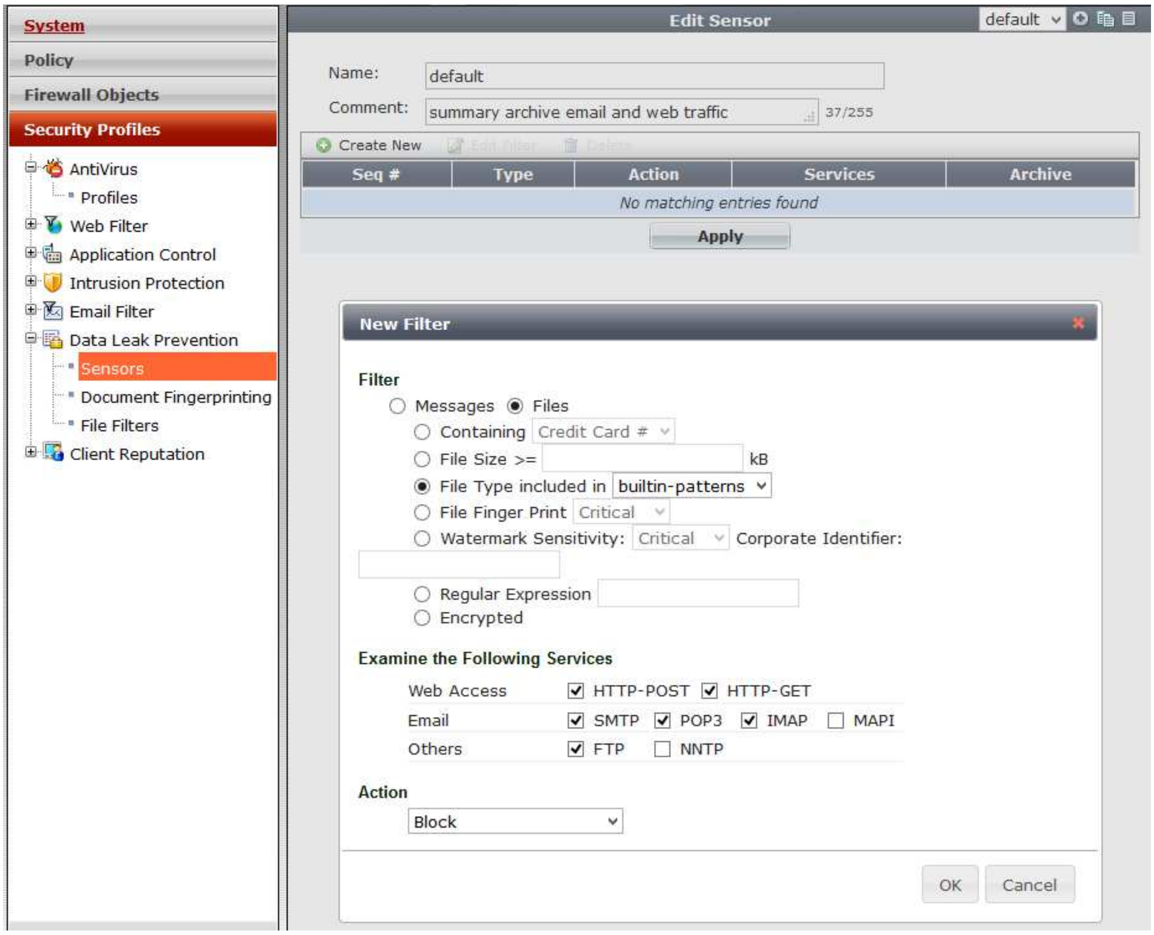
In this example we use Default Sensor.

Create New

Select Files

Select File Type include in: an enable builtin-patterns

In Action Select: Block



Name: default

Comment: summary archive email and web traffic 37/255

Seq #	Type	Action	Services	Archive
No matching entries found				

Filter

○ Messages ● Files

○ Containing Credit Card #

○ File Size >= kB

● File Type included in builtin-patterns

○ File Finger Print Critical

○ Watermark Sensitivity: Critical Corporate Identifier:

○ Regular Expression

○ Encrypted

Examine the Following Services

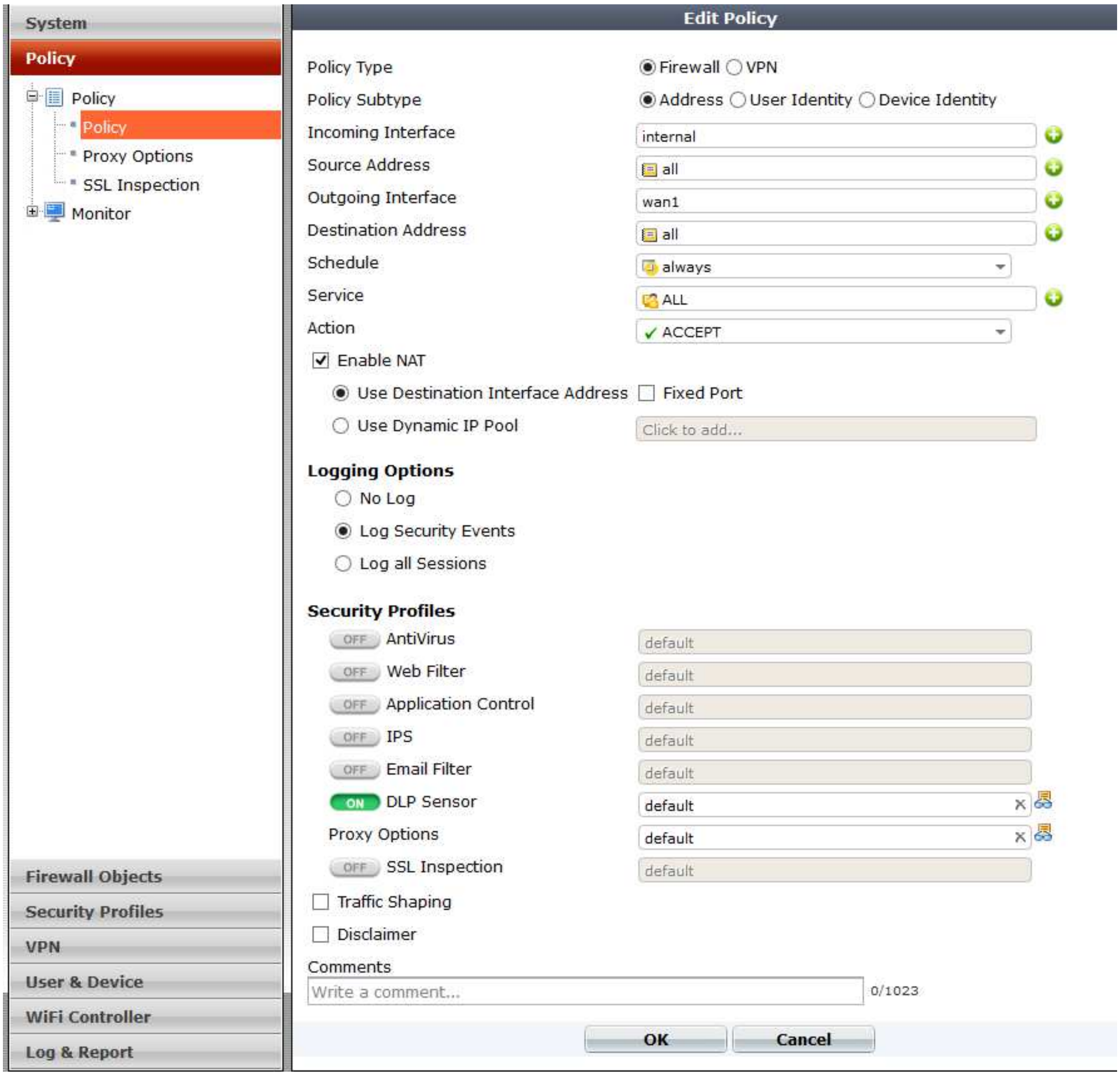
Web Access	☑ HTTP-POST	☑ HTTP-GET		
Email	☑ SMTP	☑ POP3	☑ IMAP	□ MAPI
Others	☑ FTP	□ NNTP		

Action

Block

OK and Apply

In the General Firewall Policy (you can create one for tests) enable DLP Sensor Default.



Policy Type ● Firewall ○ VPN

Policy Subtype ● Address ○ User Identity ○ Device Identity

Incoming Interface: internal

Source Address: all

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT

☑ Enable NAT

● Use Destination Interface Address □ Fixed Port

○ Use Dynamic IP Pool Click to add...

Logging Options

○ No Log

● Log Security Events

○ Log all Sessions

Security Profiles

OFF AntiVirus: default

OFF Web Filter: default

OFF Application Control: default

OFF IPS: default

OFF Email Filter: default

ON DLP Sensor: default

Proxy Options: default

OFF SSL Inspection: default

□ Traffic Shaping

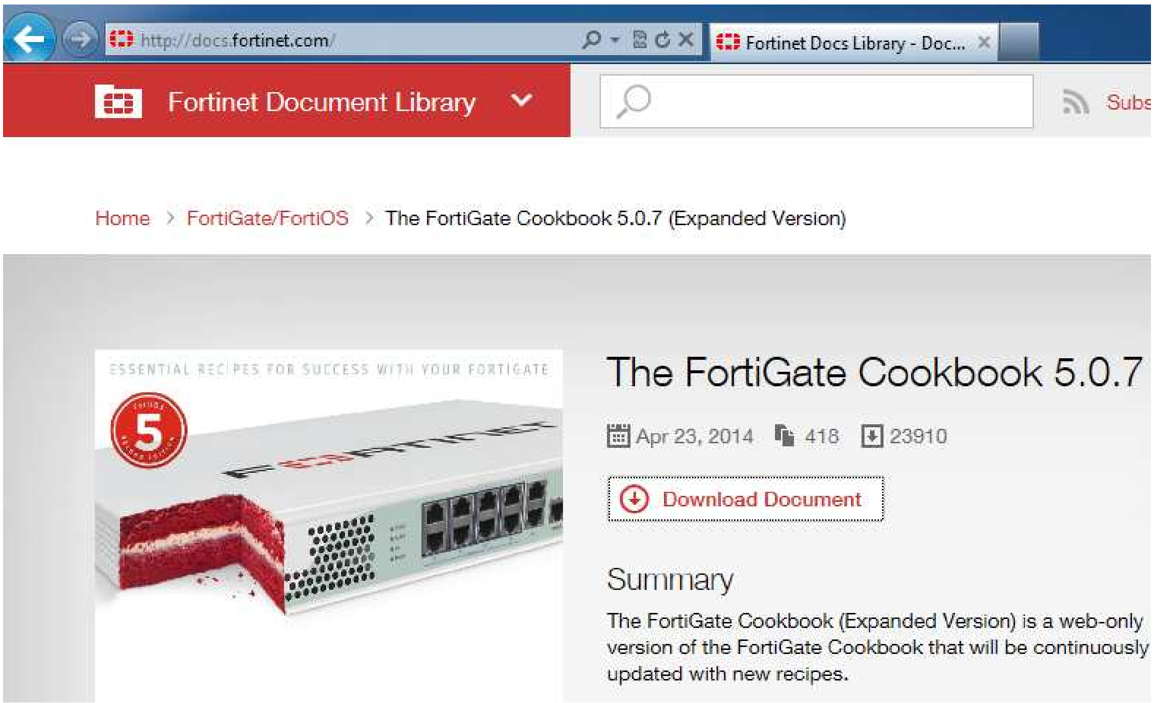
□ Disclaimer

Comments: Write a comment... 0/1023

In a Laptop test open the next URL.

http://docs.fortinet.com

And try to download a PDF.


http://docs.fortinet.com/
Fortinet Docs Library - Doc...
Fortinet Document Library
Subs
ESSENTIAL RECIPES FOR SUCCESS WITH YOUR FORTIGATE
5

Home > FortiGate/FortiOS > The FortiGate Cookbook 5.0.7 (Expanded Version)

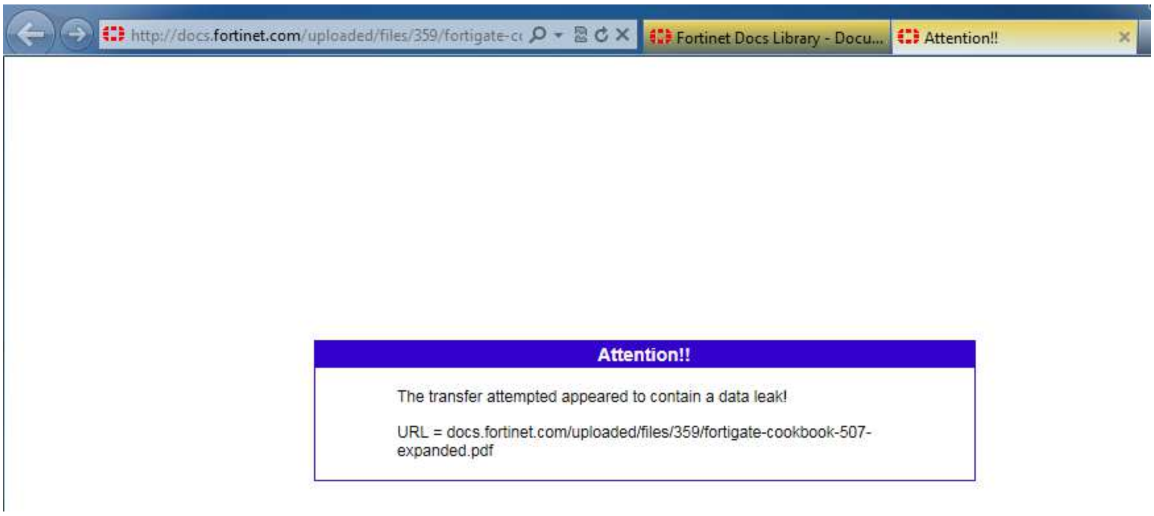
The FortiGate Cookbook 5.0.7

Apr 23, 2014 418 23910

Download Document

Summary

The FortiGate Cookbook (Expanded Version) is a web-only version of the FortiGate Cookbook that will be continuously updated with new recipes.


http://docs.fortinet.com/uploaded/files/359/fortigate-c
Fortinet Docs Library - Docu...
Attention!!

Attention!!

The transfer attempted appeared to contain a data leak!

URL = docs.fortinet.com/uploaded/files/359/fortigate-cookbook-507-expanded.pdf

Regards.