

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

Firmware versión 5.0.9



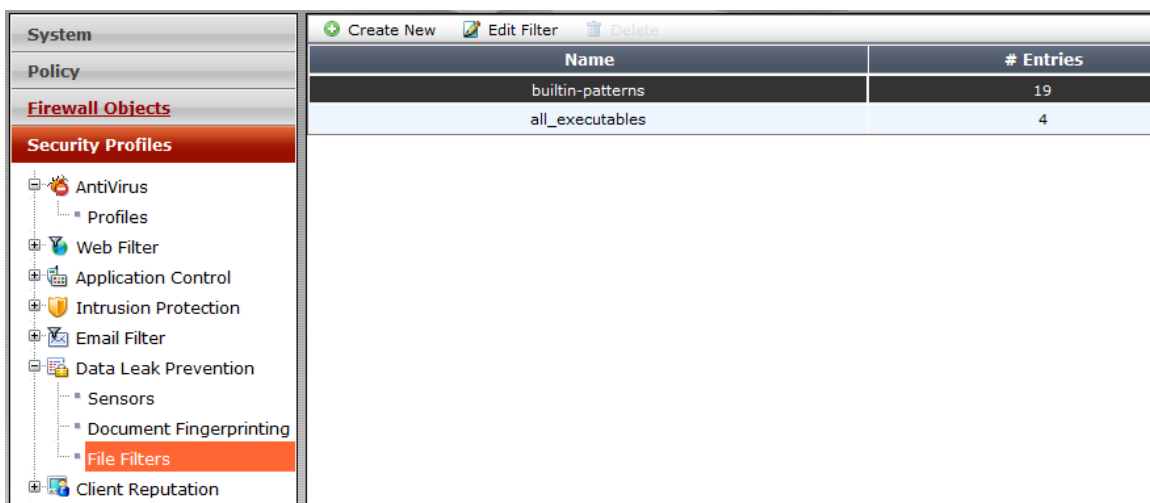
The screenshot shows the FortiGate 60C management interface. The left sidebar is expanded to 'System' > 'Status'. The main content area displays 'System Information' with the following details:

Property	Value
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.

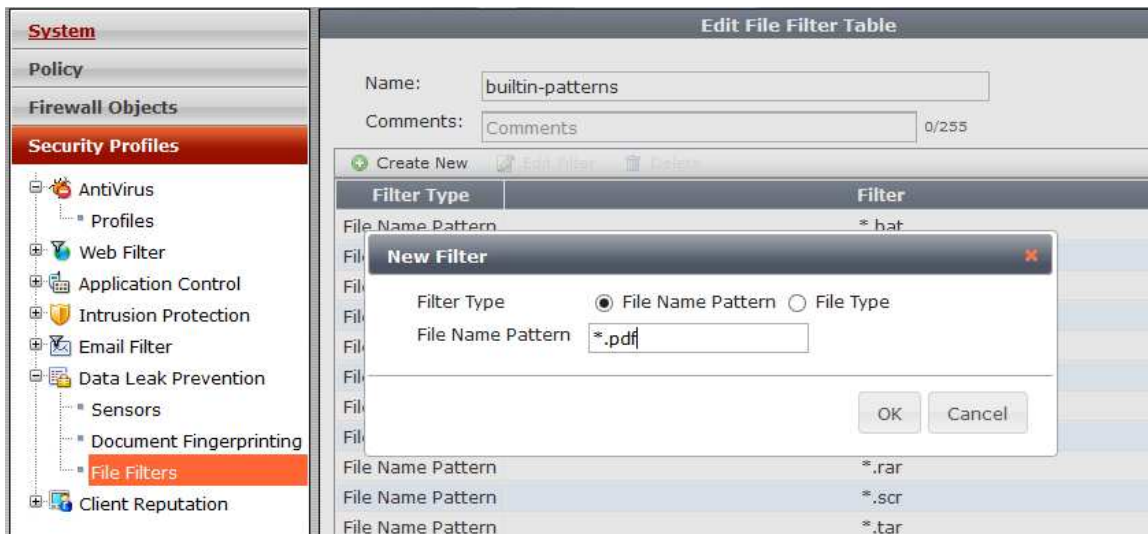
Select "builtin-patterns" and edit.



The screenshot shows the 'Security Profiles' configuration page in the FortiGate interface. The 'File Filters' section is selected in the left sidebar. The main content area displays a table of file filters:

Name	# Entries
builtin-patterns	19
all_executables	4

After select; Create New and write: *.pdf



Click 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

The screenshot displays a security management interface. On the left is a navigation tree with categories: System, Policy, Firewall Objects, Security Profiles, and Sensors. The 'Sensors' category is expanded, showing sub-items like Profiles, Web Filter, Application Control, Intrusion Protection, Email Filter, Data Leak Prevention, Document Fingerprinting, File Filters, and Client Reputation.

The main window is titled 'Edit Sensor' and shows a sensor named 'default' with the comment 'summary archive email and web traffic'. Below this is a table with columns 'Seq #', 'Type', 'Action', 'Services', and 'Archive'. The table is currently empty, with the message 'No matching entries found' and an 'Apply' button below it.

A 'New Filter' dialog box is open, allowing configuration of a filter. The 'Filter' section has 'Files' selected. The 'File Type included in' dropdown is set to 'builtin-patterns'. The 'Examine the Following Services' section has checkboxes for 'HTTP-POST', 'HTTP-GET', 'SMTP', 'POP3', 'IMAP', 'MAPI', 'FTP', and 'NNTP', with 'SMTP', 'POP3', 'IMAP', and 'FTP' checked. The 'Action' dropdown is set to 'Block'. 'OK' and 'Cancel' buttons are at the bottom right of the dialog.

OK and Apply

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

The screenshot shows the 'Edit Policy' configuration window. The left sidebar contains a tree view with 'System' expanded to 'Policy'. The main area is titled 'Edit Policy' and contains the following settings:

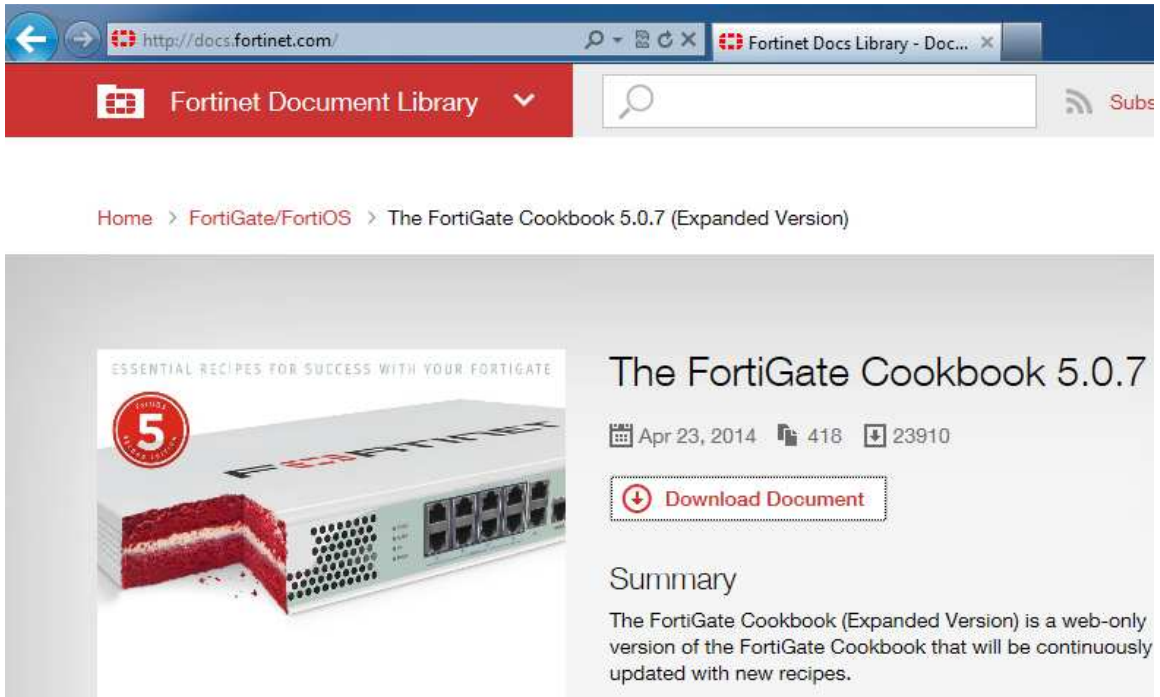
- Policy Type:** Firewall (selected), VPN
- Policy Subtype:** Address (selected), User Identity, Device Identity
- Incoming Interface:** internal
- Source Address:** all
- Outgoing Interface:** wan1
- Destination Address:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT
- Enable NAT:** checked
 - Use Destination Interface Address (selected), Fixed Port
 - Use Dynamic IP Pool: Click to add...
- Logging Options:**
 - No Log
 - Log Security Events (selected)
 - Log all Sessions
- Security Profiles:**
 - AntiVirus: OFF, default
 - Web Filter: OFF, default
 - Application Control: OFF, default
 - IPS: OFF, default
 - Email Filter: OFF, default
 - DLP Sensor: ON, default
 - Proxy Options: default
 - SSL Inspection: OFF, default
- Traffic Shaping:** unchecked
- Disclaimer:** unchecked
- Comments:** Write a comment... (0/1023)

At the bottom, there are 'OK' and 'Cancel' buttons.

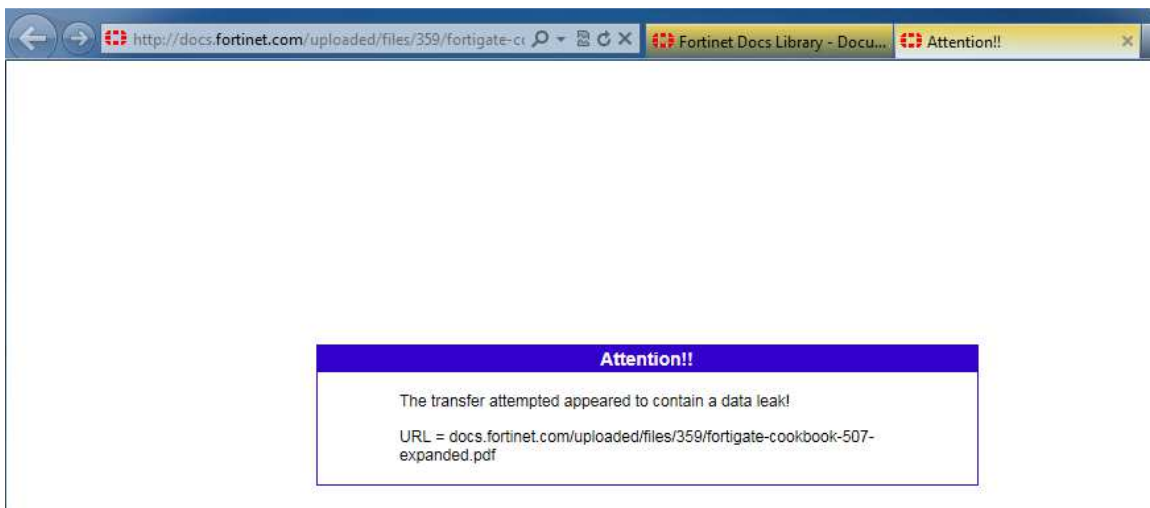
In a Laptop test open the next URL.

<http://docs.fortinet.com>

And try to download a PDF.



The screenshot shows a web browser window with the address bar containing <http://docs.fortinet.com/>. The page header includes the Fortinet logo and 'Fortinet Document Library'. The breadcrumb trail is 'Home > FortiGate/FortiOS > The FortiGate Cookbook 5.0.7 (Expanded Version)'. The main content area features a product image of a FortiGate device with a '5th Edition' badge. To the right of the image, the title 'The FortiGate Cookbook 5.0.7' is displayed, along with the date 'Apr 23, 2014', a document icon with '418', and a download icon with '23910'. A 'Download Document' button is visible. Below this, a 'Summary' section states: 'The FortiGate Cookbook (Expanded Version) is a web-only version of the FortiGate Cookbook that will be continuously updated with new recipes.'



The screenshot shows a web browser window with the address bar containing <http://docs.fortinet.com/uploaded/files/359/fortigate-cookbook-507-expanded.pdf>. The page content is mostly blank, with a prominent blue-bordered warning box in the center. The warning box has a blue header with the text 'Attention!!' and contains the following text: 'The transfer attempted appeared to contain a data leak!' and 'URL = docs.fortinet.com/uploaded/files/359/fortigate-cookbook-507-expanded.pdf'.

Regards.