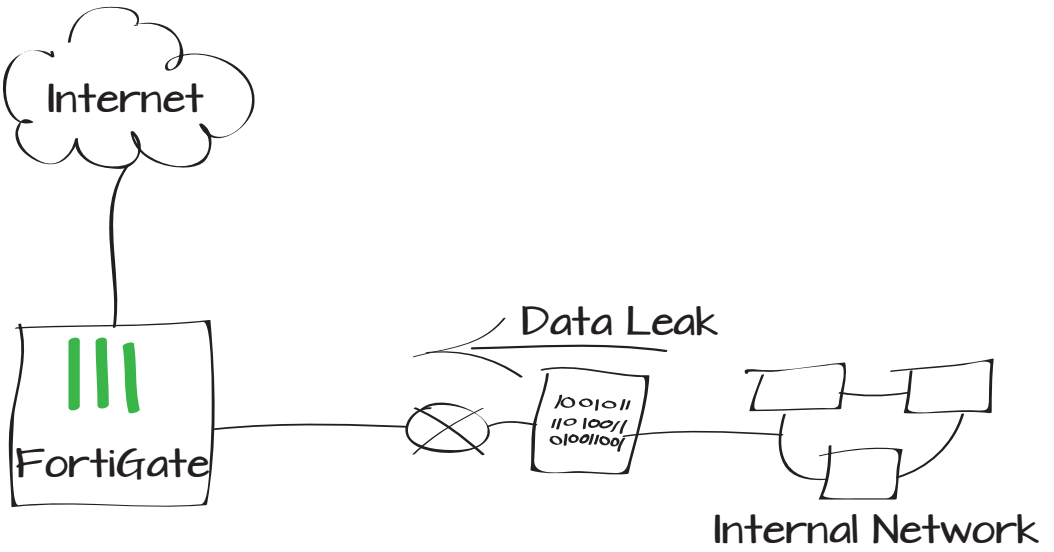
Blocking outgoing traffic containing sensitive data

Data leak prevention (DLP) analyzes outgoing traffic and blocks any sensitive information from leaving the network. In this example, DLP will be used to block files using the file's name and type.

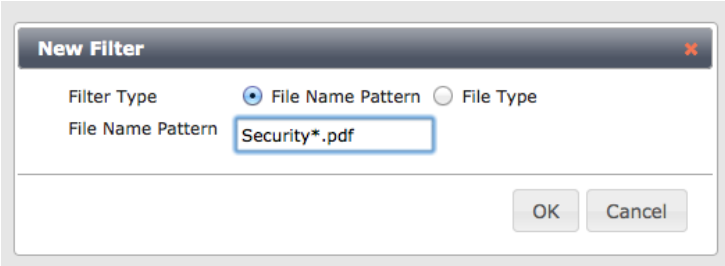
1. Creating a file filter
2. Creating a DLP sensor that uses the file filter
3. Adding the DLP sensor to a security policy
4. Results



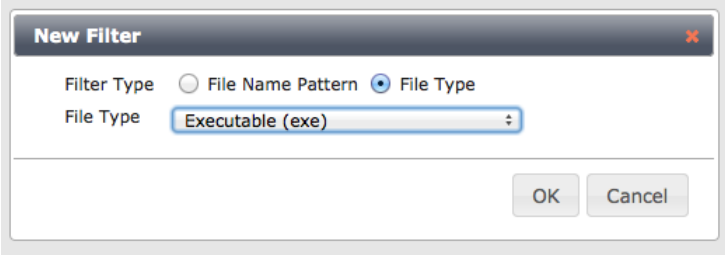
Creating a file filter

Go to **Security Profiles > Data Leak Prevention > File Filter**. Select **Create New** to make a File Filter Table.

Create a new filter in the table. Set the **Filter Type** to **File Name Pattern** and enter the pattern you wish to match. If needed, you can use a wildcard character in the pattern.

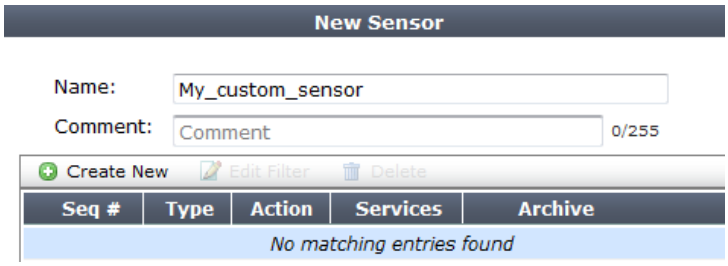


Create a second filter, this time setting the **Filter Type** to **File Type**. Select a **File Type** from the list.



Creating a DLP sensor that uses the file filter

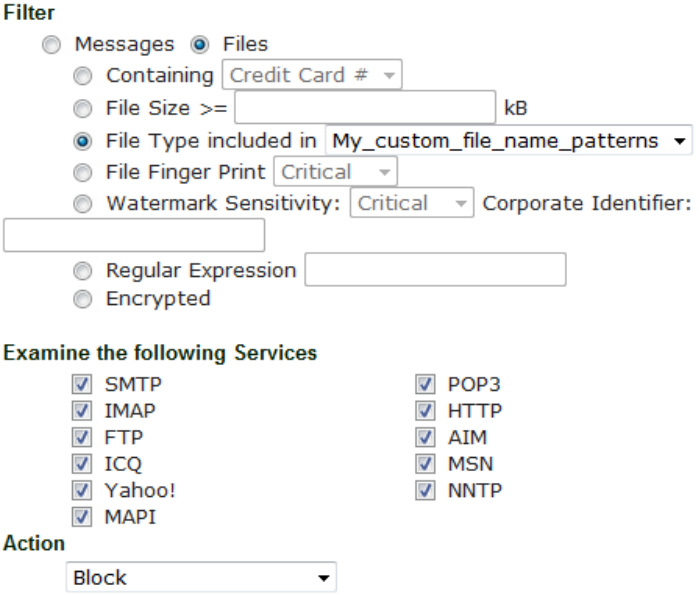
Go to **Security Profiles > Data Leak Prevention > Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.



Select **Create New** to make a new filter. Set the type to **Files**. Enable **File Type included in** and set it to your file filter.

Under **Examine the following Services**, select the services you wish to monitor with DLP.

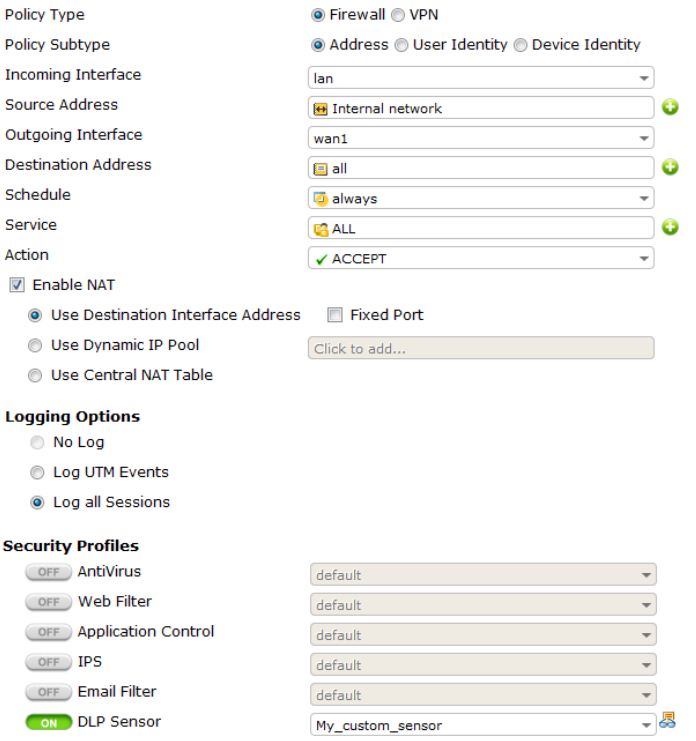
Set the **Action** to **Block**.



Adding the DLP sensor to a security policy

Go to **Policy > Policy > Policy**. Edit the security policy that controls the traffic you wish to block.

Enable **DLP Sensor** and set it to use the new sensor.

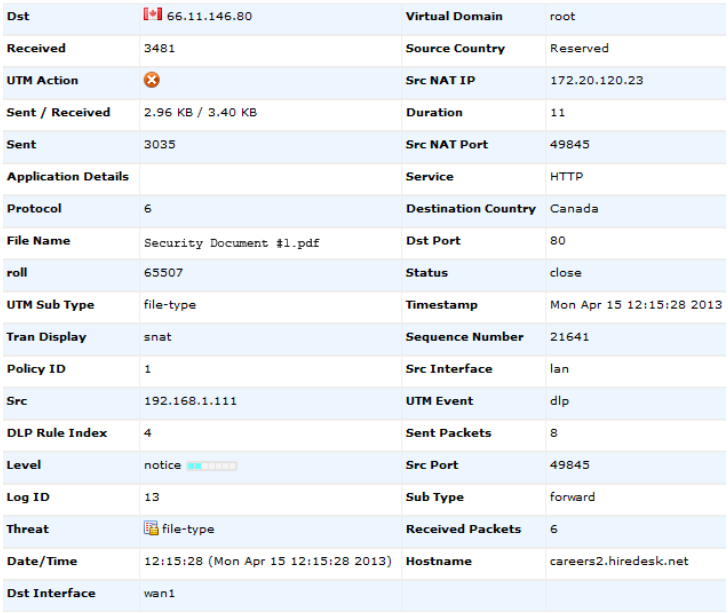


Results

Attempt to upload a file that matches the file filter criteria using FTP protocol. The file should be blocked and a message from the server should appear.

To find more information about the blocked traffic, go to **Log & Report > Traffic Log > Forward Traffic**.

The selected log message shows the name of the file that was blocked (File_pattern_text.exe), the type of file filter that blocked it (file-type), and a variety of other information which may be useful.



Dst	66.11.146.80	**Virtual Domain**	root
Received	3481	**Source Country**	Reserved
UTM Action		**Src NAT IP**	172.20.120.23
Sent / Received	2.96 KB / 3.40 KB	**Duration**	11
Sent	3035	**Src NAT Port**	49845
Application Details		**Service**	HTTP
Protocol	6	**Destination Country**	Canada
File Name	Security Document #1.pdf	**Dst Port**	80
roll	65507	**Status**	close
UTM Sub Type	file-type	**Timestamp**	Mon Apr 15 12:15:28 2013
Tran Display	snat	**Sequence Number**	21641
Policy ID	1	**Src Interface**	lan
Src	192.168.1.111	**UTM Event**	dlp
DLP Rule Index	4	**Sent Packets**	8
Level	notice	**Src Port**	49845
Log ID	13	**Sub Type**	forward
Threat	file-type	**Received Packets**	6
Date/Time	12:15:28 (Mon Apr 15 12:15:28 2013)	**Hostname**	careers2.hiredesk.net
Dst Interface	wan1		