

How to Configure File Content Filtering in the Firewall

<https://campus.barracuda.com/doc/48202696/>

To enforce a file content policy in the firewall, you must create an access rule to match your HTTP, HTTPS, FTP, SMTP, or SMTPS traffic. Enable Application Control, File Content Scan, and, optionally, SSL Interception. You can also combine File Content Scan with URL Filter and User Agent policies. The policy objects are configured as a part of the application rule.

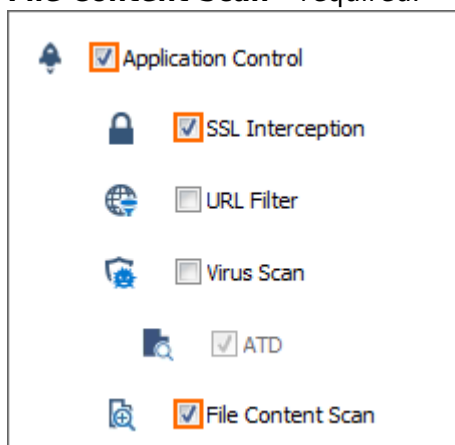
Before You Begin

- Create File Content Policies. For more information, see [How to Create File Content Policies](#).
- Verify that the **Firewall Feature Level** is 6.2 or higher.

Step 1. Enable File Content Scanning in a PASS Access Rule

Enable Application Control, File Content Scan, and, optionally, SSL Interception for the access rule handling HTTP, HTTPS, FTP, SMTP, and/or SMTPS traffic.

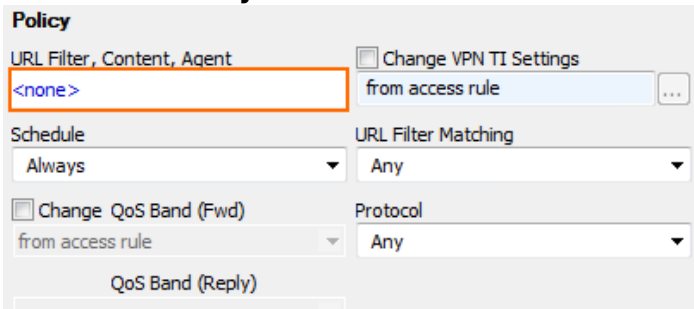
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Double-click to open the access rule you want to apply the file content policy for.
4. Click on the **Application Policy** link and select:
 - **Application Control** - required.
 - **SSL Interception** - optional.
 - **File Content Scan** - required.



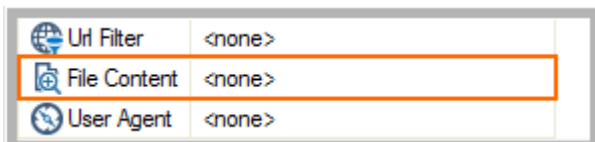
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 2. Create Application Rule using File Content Filter Objects

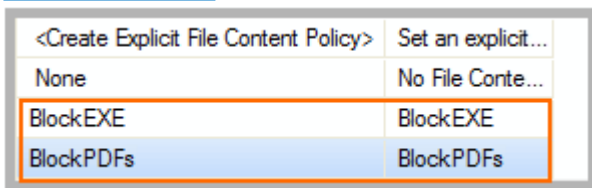
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules**.
3. Click **Lock**.
4. Create a PASS application rule. For more information, see [How to Create an Application Rule](#).
 - **Source** - Select the same source used in the matching access rule.
 - **Application** - Select **Any** to use only policy filtering. Otherwise, select an application object from the drop-down list to combine Application Control and File Content filtering.
 - **Destination** - Select the same destination used in the matching access rule.
5. Click on the **Policy** link.



6. Click **File Content**.



7. Click on the **File Content Policy** in the list. For more information, see [How to Create File Content Policies](#)



8. Click **OK**.

Policy

URL Filter, Content, Agent Change VPN TI Settings

<none>, BlockPDFs, <none> from access rule ...

Schedule URL Filter Matching

Always Any

Change QoS Band (Fwd) Protocol

from access rule Any

QoS Band (Reply)

9. Click **Send Changes** and **Activate**.

Monitoring File Content Filtering in the Firewall































Firewall Live View

Go to **FIREWALL > History View** and check the **Info** column for connections that were blocked due to the detected content.

Cache Selection		Access, Fail, Rule Block, Packet Drop		Traffic Selection		Forward, Local In, Local Out, IPv4, IPv6		Destination		172.16.0.*			
AID	IP...	Port	Source	Int...	User	Destination	O...	A...	Application Context	C...	Last	Rule	Info
- B-50	TCP	29391	10.0.10.11	eth0		172.16.0.13	eth3		PDF/SSLVPN.pdf	2	44m 12s	LAN-2-FTPServers	Detected Content not allowed by policy
- B-49	TCP	52721	10.0.10.11	eth0		172.16.0.13	eth3		PDF/Test.pdf	2	44m 12s	LAN-2-FTPServers	Detected Content not allowed by policy
+ 304	TCP	29391	10.0.10.11	eth0		172.16.0.13			SSLVPN.pdf	1	44m 12s	<App>.FileContent-from-FTPSRV	Application Detect
+ 303	TCP	52721	10.0.10.11	eth0		172.16.0.13			Test.pdf	1	44m 12s	<App>.FileContent-from-FTPSRV	Application Detect
+ 37	TCP	21	10.0.10.11	eth0	mzoller	172.16.0.13				33	44m 12s	<App>.FileContent-from-FTPSRV	Application Detect

Firewall Monitor

Check the **CONTENT** element on the **FIREWALL > Firewall Monitor** page to see a summary. You can filter and drill down based on source, time, and the associated action (allow, blocked, ...).

CONTENT		GROUP	X
 Web Files		2	<input type="text"/>
 HTML		2	<input type="text"/>
 XML		0	<input type="text"/>
 Picture Files		1	<input type="text"/>
 GIF		1	<input type="text"/>
 PNG		0	<input type="text"/>
 JPEG		0	<input type="text"/>
 Office Document Files		0	<input type="text"/>
 PDF		0	<input type="text"/>
 Executeables		0	<input type="text"/>
 EXE		0	<input type="text"/>
 Compressed and Uncompr...		0	<input type="text"/>
 DEB		0	<input type="text"/>
 BZIP2		0	<input type="text"/>
 CAB		0	<input type="text"/>

Figures

1. file_content_fw_01.png
2. FC_02.png
3. FC_03.png
4. FC_04.png
5. FC_05.png
6. FC_06.png
7. FC_07.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.