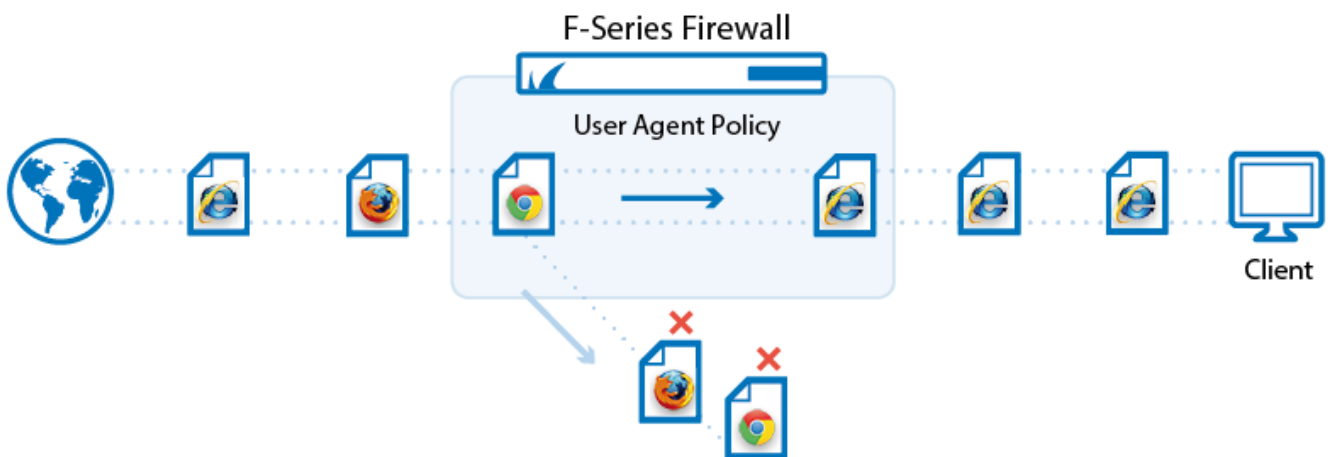


## How to Configure User Agent Filtering in the Firewall

<https://campus.barracuda.com/doc/53248709/>

The NextGen Firewall F-Series can filter HTTP and HTTPS traffic based on the user agent string of the browser. For this policy to apply, web traffic must match an access rule with Application Control and an application rule with a User Agent policy.




### Before You Begin

- Enable Application Control. For more information, see [How to Enable Application Control](#)
- Create User Agent Policies. For more information, see [How to Create User Agent Policies](#).

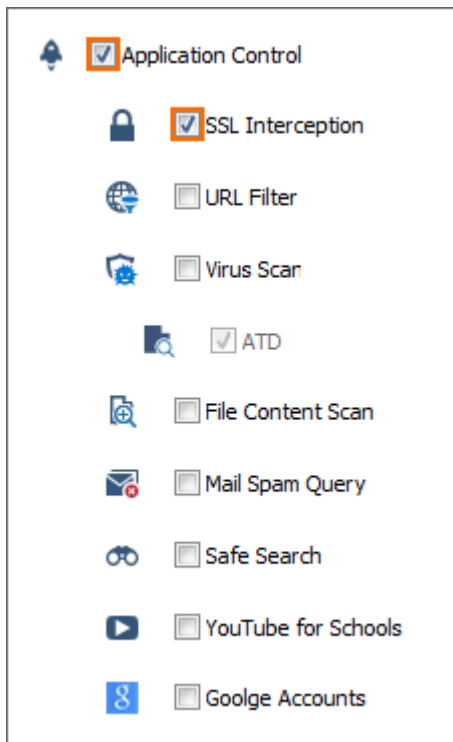
### Step 1. Create an Access Rule to Match Web Traffic

Create a PASS access rule to match HTTP and HTTPS traffic and enable Application Control and, optionally, SSL Interception.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching HTTP/HTTPS traffic.

 Pass			LAN-HTTPS-2-INTERNET		
			Allows internet access from Trusted LAN for typical applications.		
<input type="checkbox"/> Bi-Directional			<input type="checkbox"/> Dynamic Rule		
<input type="checkbox"/> Deactivate Rule					
Source	Service	Destination	Authenticated User	Policies	Connection Method
HQ-LAN 10.0.10.0/25	HTTP+S Ref: HTTP Ref: HTTPS	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16	Any	IPS Policy Default Application Policy AppControl, SSL.Int Schedule Always QoS Band (Fwd) Internet (ID 4) QoS Band (Reply) Like-Fwd	Dynamic SNAT Source-based NAT

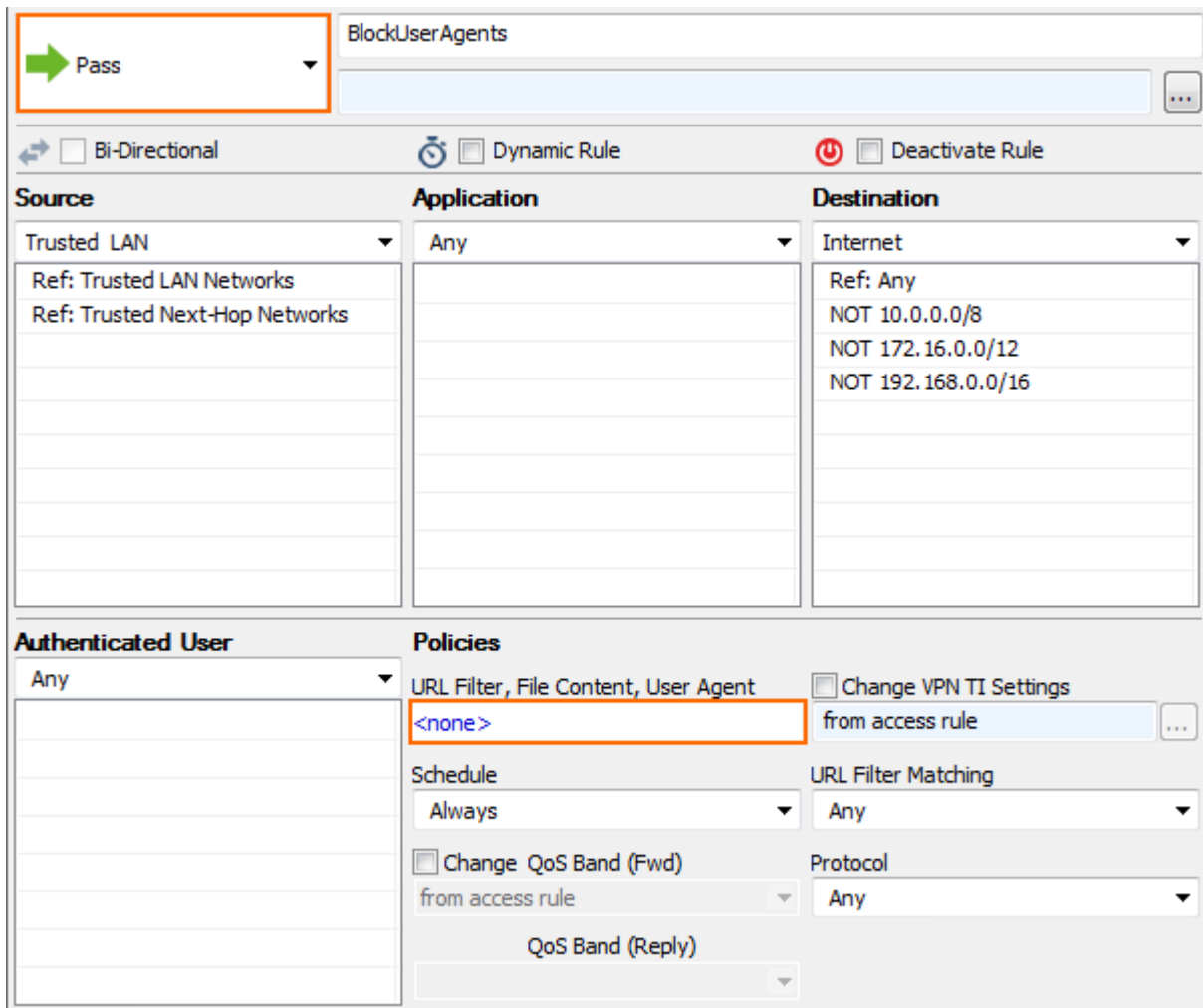
3. Click on the **Application Policy** link and select:
  - o **Application Control** - required.
  - o **SSL Interception** - optional.



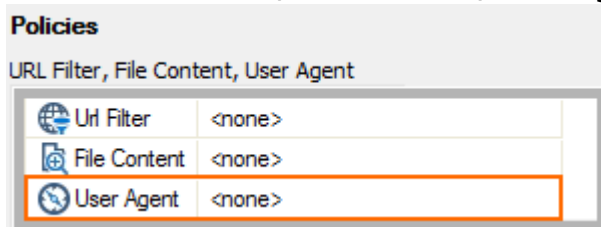
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

## Step 2. Create Application Rule using User Agent Policies

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 configure only the filter policies. Otherwise, select an application object from the drop-down list to combine Application Control and User Agent filtering.
  - **Destination** - Select the same destination used in the matching access rule.



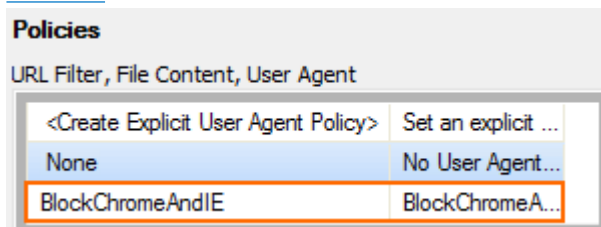
5. Click the **URL Filter, File Content, User Agent** link.



Policies	
URL Filter, File Content, User Agent	
Url Filter	<none>
File Content	<none>
User Agent	<none>

6. Click **User Agent**.

7. Select a user agent policy from the list. For more information, see [How to Create User Agent Policies](#).



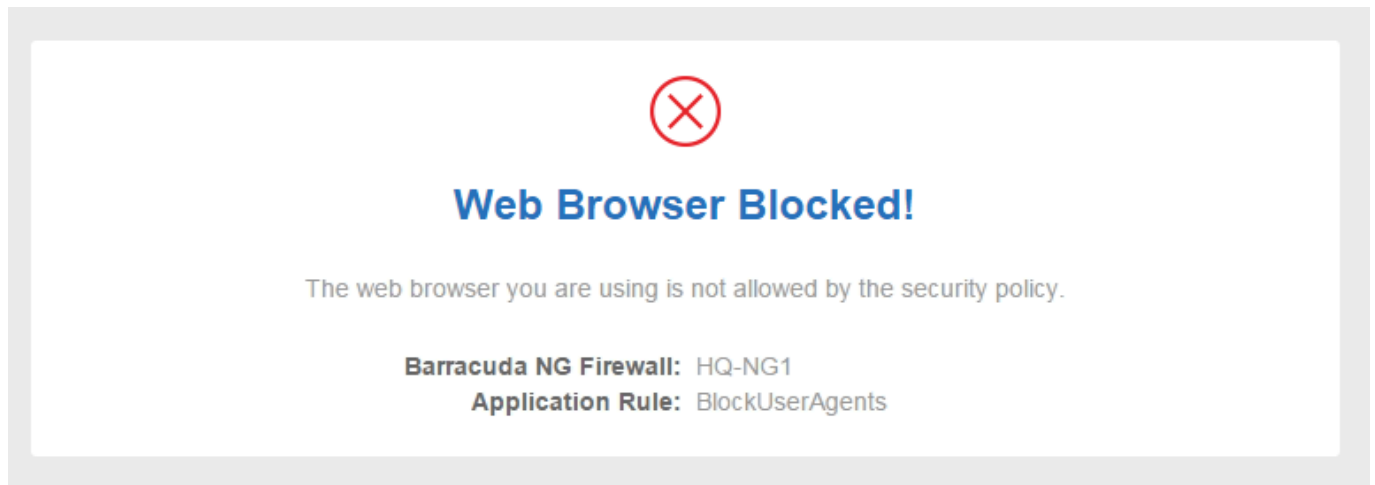
Policies	
URL Filter, File Content, User Agent	
<Create Explicit User Agent Policy>	Set an explicit ...
None	No User Agent...
BlockChromeAndIE	BlockChromeA...

8. Click **OK**.

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

When users attempt to access a service with a web browser that is not allowed in the user agent

policy, the connection is either reset or redirected to a custom block page. The block page is customizable. For more information, see [How to Configure Custom Block Pages and Texts](#).



## Monitoring

To monitor blocked connections, go to **FIREWALL > History** and check the **Info** column of blocked connections for **Detected Browser Agent not allowed by policy**.

Cache Selection				Access, Fail, Rule Block, Packet Drop				Traffic Selection				Forward, Local In, Local Out, IPv4, IPv6			
AID	IP Proto	Port	Source	Int...	User	Destination	O...	Next Hop	Application	Application Cont...	Count	Last	Rule	URL Category	Info
8-34	UDP	138	10.0.10.13	eth0	mzoller	10.0.10.127					755	4m 36s	BO-2-HQ-ALL		Block Broadcast
1397	TCP	80	10.0.10.11	eth0	mzoller	194.232.104.140	eth1	62.99.0.254			3	4m 47s	LAN-2-INTERNET		Normal Operation
8-92	TCP	80	10.0.10.11	eth0	mzoller	194.232.104.140			Web browsing	orf.at	3	4m 47s	<App>-BlockUserAgents	News	Detected Browser Agent not allowed by policy
139	TCP	443	10.0.10.11	eth0	mzoller	191.232.139.253	eth1	62.99.0.254			630	5m 07s	LAN-2-INTERNET		Normal Operation

## Figures

1. user\_agent\_policy.png
2. User\_agents\_02.png
3. User\_agents\_01.png
4. User\_agents\_03.png
5. User\_agents\_04.png
6. User\_agents\_05.png
7. User\_agents\_06.png
8. User\_agents\_07.png

© Barracuda Networks Inc., 2020 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.