

How to Configure User Agent Filtering in the Firewall

https://campus.barracuda.com/doc/17459/

The CloudGen Firewall 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 <u>How to Enable Application Control</u>.
- Create User Agent policies. For more information, see <u>How to Create User Agent Policies</u>.
- (optional) Enable SSL Inspection. To use SSL Inspection, the **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher. For more information, see <u>SSL Inspection in the Firewall</u>.

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 Inspection.

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

Barracuda CloudGen Firewall



- Deve	LAN-H	N-HTTPS-2-INTERNET								
Pass	Allow	s internet access from Tr	usted LAN for typ	ical applica	al applications					
rectional 📄		💍 🗌 Dynamic Rule		🕘 🗌 Deactivate Rule						
Source VR Instance	default	✓ Dest	ination VR Inst	tance Same as Source 🗸						
Source		Application		Destination						
HQ-LAN	•	HTTP+S	•	Internet		•				
10.0.10.0/25		Ref: HTTP		Ref: An	y					
		Ref: HTTPS		NOT 10.	0.0.0/8					
				NOT 17	2.16.0.0/12					
				NOT 192	2.168.0.0/16					
Authenticated User		Policies		Connect	ion Method					
Any	~	IPS Policy		Dynamic	NAT	~				
		Default Policy	\sim	Dynamic	NAT					
		Application Policy		Dynamic						
		AppControl, SSL								
		SSL Inspection Policy								
		Default	\sim							
		Schedule	,							
		Always	~							
		QoS Band (Fwd)								
		No-Shaping	\sim							
		QoS Band (Reply)								
		Like-Fwd	\sim	_						
					OK Ca	ncel				

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



Application Control									
		SSL Inspection							
	¢	URL Filter							
	G	Virus Scan							
	👌 🗌 АТР								
	æ	File Content Scan							
	6	Mail DNSBL Check							
	6	Link Protection							
	æ	Safe Search							
	D	YouTube for Schools							
	G	Google Accounts							

- 4. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see <u>SSL Inspection in the Firewall</u>.
- 5. Click **OK**.
- 6. Click Send Changes and Activate.

Step 2. Create Application Rule Using User Agent Policies

- 1. Go to CONFIGURATION > Configuration Tree > Box > 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 <u>How to Create an Application Rule</u>.
 - **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.

Barracuda CloudGen Firewall



	BlockUserAgents						
Pass 🔻							
🚓 🗌 Bi-Directional	💍 🗌 Dynamic Rule	😃 🗌 Deactivate Rul	O Deactivate Rule				
Source VR Instance d	efault 🗸						
Source	Application	Destination					
Trusted LAN	✓ Any	▼ Internet	•				
Ref: Trusted LAN Networks		Ref: Any					
Ref: Trusted Next-Hop Netwo	rks	NOT 10.0.0/8	NOT 10.0.0/8				
		NOT 172.16.0.0/12					
		NOT 192.168.0.0/16					
Authenticated User	Policies						
Any	▼ URL Eilter, Eile Content, U	er Agent 👘 Change VPN TI Sett	inas				
	<none></none>	from access rule					
	Schedule	LIRI Filter Matching					
	Always	✓ Any	•				
	Change OoS Band (Ew	d) Protocol					
	from access rule		-				
	In on accessing	Ally	•				
	QoS Band (Rej	biy)					
		▼					
		OK	Cancel				

Click the URL Filter, File Content, User Agent link.
Policies

URL Filter, File Content, User Agent

🕀 Url Filter	<none></none>
🕀 File Content	<none></none>
🚫 User Agent	<none></none>

6. Click User Agent.

7. Select a user agent policy from the list. For more information, see <u>How to Create User Agent</u> <u>Policies</u>.



- 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 <u>How to Configure Custom Block Pages and Texts</u>.



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	0	Next Hop	Application	Application Cont	Count	Last	Rule	URL Category	Info
🖨 B-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
🖨 B-92	TCP	80	10.0.10.11	eth0	mzoller	194.232.104.140			Web browsing	orf.at	3	4m 47s	App>:Block UserAgents	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

Barracuda CloudGen Firewall



Figures

- 1. user_agent_pol.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., 2025 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.