

# How to Configure a Barracuda CloudGen Firewall in Barracuda SecureEdge

#### https://campus.barracuda.com/doc/98223588/

Barracuda SecureEdge allows administrators to enroll Barracuda CloudGen Firewall units with the cloud service. CloudGen Firewalls can be registered with Barracuda SecureEdge as a point of enforcement for Resource Access policies and can be either stand-alone or CC-managed boxes. The registration process of a CloudGen Firewall with Barracuda SecureEdge is similar to the way Azure Cloud Gateways are registered with the service. All enrolled appliances are directly connected to the cloud service to fetch policies and endpoint configurations.

Demo Enterprise	s Inc/Production  CloudGen Firewalls				Registration Token
					Y Add filter Edit columns
	NAME	SERIAL	CC MANAGED	MODEL	
0	France	830634	×	F180	Î

#### Requirements

- On CloudGen Firewall boxes, Barracuda SecureEdge requires the Policy Profiles rule set.
- During this setup, VPN configuration (connectivity) and Remote Access policies are applied. Web Filter policies must be configured on the CloudGen Firewall.
- For HA pairs, enter the token only in the primary box. The secondary box does not require any additional configuration.
- On CloudGen Firewall boxes, Barracuda SecureEdge requires the Caching DNS to be enabled. For more information, see <u>How to Configure a Caching DNS Service</u>.
- On CloudGen Firewall boxes, you must enable the VPN service. For more information, see <u>How</u> to Assign Services.

With SecureEdge enabled, the log streaming configuration on the CloudGen Firewall may be overwritten.

#### Step 1. Retrieve the Registration Token from SecureEdge

The token is valid for 30 minutes only, and you need a separate token for each CloudGen Firewall appliance you want to enroll.

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control



account.

- 2. In the left menu, click the **Tenants/Workspaces** icon.
- 3. From the drop-down menu, select the workspace your appliance should be assigned to.



4. In the left menu, click the **Integration** icon, and select **CloudGen Firewalls**.



5. The **CloudGen Firewalls** page opens. In the top-right corner of the window, click **Registration Token.** 

0	France	830634	×	F180	i (
	NAME	SERIAL	CC MANAGED	MODEL	
					Y         Add filter         Edit columns
Demo Enterprises	CloudGen Firewalls				Registration Token

- 6. The Generate Registration token window opens.
- 7. Click on the clipboard icon to copy the token to your clipboard.

## Barracuda SecureEdge





Step 2. Log into the Barracuda CloudGen Firewall

1. Connect to your firewall using Barracuda Firewall Admin.

$\equiv \vee + \Box_{Secu}^{10.27}$	/.35.60 × reEdge-Gat												
DASHBOARD CONF	IGURATION CONTROL	FIREWALL	VPN LO	GS	STATISTICS	EVENTS	SSH						
General	Firewall	Secure Edg	ge										
✓ APPLIANCE					✓ SECUREE	0		/ INTERFACES	5				
Model	lodel VF1000 - Platform: VMWare				SecureEdg	e		Healthy	$\overline{\mathbf{\Theta}}$		eth0 eth1	eth2 eth3	5
Host Name	SecureEd	SecureEdge-Gateway											
Serial Number	2208820				✓ SERVICES				0				2
Uptime	00:05:05				Box Servi	ces							
System Time	Fri Apr 7	08:58:29 2023 - Etc/0	JTC		<b>↑</b> Firewall			NGFW	$\ominus$	`	<b>UPDATES</b>		
Firmware Version	9.0.0-045	9.nightbuild			VPN			VPN	$\overline{\mathfrak{S}}$				Availat
								-	<u> </u>		Scope	Type	Relea

2. On the Firewall Admin **Dashboard** page, the appliance details are displayed and can be noted. For example, host name and serial number.

✓ APPLIANCE	0
Model	VF1000 - Platform: VMWare
Host Name	SecureEdge-Gateway
Serial Number	2208820
Uptime	00:06:06
System Time	Fri Apr 7 08:59:30 2023 - Etc/UTC
Firmware Version	9.0.0-0459.nightbuild

3. Click the **SecureEdge** icon.



≡ ∨ +		1000			
DASHBOARD CUNFIGURATION	CUNTRUL FIREWALL	VPN LOGS	STATISTICS EVENTS	SSH	
Seneral Firewall	VPN SecureE	dge			
✓ APPLIANCE		•	✓ SECUREEDGE INTEG	GRATION	¢
Model	VF1000 - Platform: VMWare		SecureEdge	🤣 Healthy	$\overline{\mathbf{O}}$
Host Name	SecureEdge-Gateway				
Serial Number	2208820		✓ SERVICES		ø
Uptime	00:05:05		Box Services	Ø	
System Time	Fri Apr 7 08:58:29 2023 - Etc.	/UTC	tirewall	NGFW	$\ominus$
	0.0.0.0450			-	-

4. In the **Connect to SecureEdge** window, enter the registration token that you retrieved in Step 1.

🔊 Barracuda	a CloudGen Firewall 9.0.0	×										
Ø	Connect to SecureEdge As soon as the Barracuda CloudGen Firewall is connected to the SecureEdge Portal, the configuration of the SecureEdge Agents will be automatically retrieved. The configured VPN server certificate will not be used any longer in favor of the new certificate for the SecureEdge Agents. You can download the root certificate for the new server certificate from the											
	SecureEdge Portal and add it to the trusted CA certificates on the SecureEdge Agent machines. Enter your token 7b065f4b118d4cf2947d2c92bcc55da0											

- 5. Click **OK**.
- 6. Go back to the Barracuda SecureEdge configuration, and click **OK**.

After the configuration is finished, the appliance automatically appears in the SecureEdge Cloud UI. You can see the new appliance with host name and serial number enrolled on the **CloudGen Firewalls** page and that the connection is established between the CloudGen Firewall and Barracuda SecureEdge.

Integration > CloudGen Firewalls				Registration Token
				Y Add filter Edit columns
NAME	SERIAL	CC MANAGED	MODEL	
S France	830634	×	F180	Î v

# **Step 3. (Optional) Verify that the Barracuda CloudGen Firewall Appliance Is Enrolled**



- 1. Go to <u>https://se.barracudanetworks.com</u> and log in with your existing Barracuda Cloud Control account.
- 2. Select the workspace containing your appliance.
- 3. In the left menu, click the **Integration** icon, and select **CloudGen Firewalls**.

#### All appliances enrolled in the selected workspace are displayed.

Demo Enterprise	Inc/Production  CloudGen Firewalls				Reg	gistration Token
					Y Add filter	Edit columns
	NAME	SERIAL	CC MANAGED	MODEL		
0	France	830634	×	F180		Î

### **Remove Existing Enrolled Appliances**

If you want to remove an existing enrolled appliance,

- 1. Go to <u>https://se.barracudanetworks.com</u> and log in with your existing Barracuda Cloud Control account.
- 2. Select the workspace containing your appliance.
- 3. In the left menu, click the **Integration** icon, and select **CloudGen Firewalls**.
- 4. Click on the trash can icon next to the enrolled appliance you want to remove.

0	France	830634	×	F180	Î
	NAME	SERIAL	CC MANAGED	MODEL	
					Y Add filter Edit columns
Demo Enterprise	es Inc/Production  CloudGen Firewalls				Registration Token

- 5. Click **OK** to confirm.
- 6. Click Save.

#### Verify the Status of Barracuda SecureEdge in Barracuda Firewall Admin

- 1. Log into the CloudGen Firewall using Barracuda Firewall Admin.
- 2. The Barracuda Firewall Admin page opens.
- 3. Click the Barracuda SecureEdge icon.

#### Monitoring ZTNA Access Rules and RAC Policies in the Firewall



On a Barracuda CloudGen Firewall, ZTNA access rules are auto-generated and cannot be moved. However, if you introduce the section separators PRE-BEGIN and PRE-END and place your own rule in between, this rule is placed before the ZTNA auto-generated rules.

DASHBOARD	CONFIGURAT	TION	CONTROL	FIREWALL	VPN	LOGS	STATISTICS	EVENTS	SSH								C
Configuration Tree	↑ Forward NGFV	arding Ru V (Firew	ules - × all)											State Info	- Activate	🕤 Undo	N Disconnect
Forwarding	g Rules														Discard Im/Export	Lock	Send Changes
	^	₿₿	Main Rules												:	🗘 🔍 🖉 🏹	<∕∕┼░ቩὒዏ़⊂
V Rule Lists		1	Action		Name				Features	Policy Usage	NAT Mode	Service	Source				Destination
Access Rules		0 🖬	PRE-BEGIN (1)														
Object Viewer		1	Cony Deny		RuleNeed	ledBeforeR	AC			N.A.	N.A.	FTP TCP 21	192.168.225.1				Any 0.0.0.0/0
V Policy Profiles	s	2 4	PRE-END (12)														
SD-WAN Applications		3	→ Pass Dynamic NA	т	BOX-BAR	RACUDA-C	UDA-CONNECT			None	Explicit NAT	ScreenConnect TCP 443, TCP 8040, TCP	Ref: Trusted LAN , Ref: WIFI Network 10.17.63.0/24, 127.0.0.9				connect.barracuda.com

To view ZTNA access rules and RAC policies deployed via Cloud UI in Firewall Admin:

- 1. Log into the CloudGen Firewall using Barracuda Firewall Admin.
- 2. Go to **FIREWALL > Forwarding Rules**.

				Barracuda	a Firewall A	dmin 9.0 -		- Firewall / Forwarding	g Rules						– o ×
= ~ + =	Auto-des	ing Sector	× 🗖												
DASHBOARD CC	INFIGUR	ATION	CONTROL FIREW	ALL VPN LOGS STATISTICS EVENT	rs ssh	ł									Ç
O Monitor	Live	1	History Q Threat Scan	💽 Shaping 🕂 Users 🍝 Dynamic 🔇	+ Host Rules	C: Forwa	rding						Ċ	(efresh F5)	Not Disconnect
Parts Links		F	orwarding Rules - I	Rules											
<ul> <li>Kule Lists</li> </ul>		闘	Main Rules <racpol></racpol>										🗘 🛈 🤉	ŀ ^ X∦	ⅈ┼ᇲቬὒዏҀ
Access Rules			Action	Name	Features	Policy Usage	NAT Mode	Service	Source	Destination	User	Sche	QoS	Usage	Comment
		0	<ul> <li>PRE-BEGIN (6)</li> </ul>												
V Policy Profiles		1	Conv Deny	RuleNeededBeforeRAC		N.A.	N.A.	FTP TCP 21	192.168.225.1	Any 0.0.0.0/0	Any	Always	N.A.		
SD-WAN Applications		2	Block	RAC-ZTNA-BLOCK-CONF-DNS-ENCRYPTED		N.A.	N.A.	UDP 853, TCP 853, TCP 443	0.0.0.0/0 pvpn84 0.0.0.0/0 dev pvpn84	Ref: Root DNS , Ref: DNS 10.17.6.120, 192.112.36.4,	Any	Always	N.A.		ZTNA service aut
O URL Filtering		3	Block	RAC-ZTNA-BLOCK-DNS-OVER-TLS		N.A.	N.A.	UDP 853 . TCP 853	0.0.0.0/0 pvpn84 0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	N.A.		ZTNA service aut
SSL Inspection		4	← App Redirect → 127.0.0.1:53	RAC-ZTNA-DNS-LOCAL-REDIR		N.A.	N.A.	Ref: DNS TCP 53, UDP 53	0.0.0.0/0 pvpn84 0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	ID 2		ZTNA service aut
IPS File Content		5	$\rightarrow \frac{Pass}{SD-WAN}$	RAC-ALLOW-INTERNET-PVPN84		All Policy Pr	N.A.	Any ALLIP, ECHO, TCP *, TCP	0.0.0.0/0 pvpn84 0.0.0.0/0 dev pvpn84	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8,	Any	Always	N.A.		ZTNA service aut
User Agent		6	$\rightarrow_{\text{SD-WAN}}^{\text{Pass}}$	RAC-ALLOW-PVPN84		All Policy Pr	N.A.	Any ALLIP, ECHO, TCP *, TCP	0.0.0.0/0 pvpn84 0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	N.A.		ZTNA service aut
✓ Firewall Objects		7	PRE-END (12)												
Networks		8	→ Pass Dynamic NAT	BOX-BARRACUDA-CUDA-CONNECT		None	Explicit NAT	ScreenConnect TCP 443, TCP 8040, TCP	Ref: Trusted LAN , Ref: WI 10.17.63.0/24, 127.0.0.9	connect barracuda.com	Any	Always	ID 2		CudaConnect is a

3. Next to the **Main Rules** tab, a new tab **<RACPOL>** has been introduced (if applicable).

The **<RACPOL>** tab shows the policies the administrator has configured in the cloud service as Zero Trust Access rules.

#### **Enable Security Inspection for Connected Firewalls**

On Barracuda CloudGen Firewall version 9.0.1, the forwarding ruleset blocks UDP port 443 per default via rule **BOX-BLOCK-UDP443**. However, for security inspection to work on CloudGen Firewalls used as SecureEdge Point of Entry, QUIC traffic must be denied manually. To block the QUIC protocol on UDP 443, you must create a new rule and place it on top of the cloud-maintained/autogenerated rules. For more information, see: <u>How to Block UDP Port 443 on CloudGen Firewalls</u>.

#### **Additional Information**



- On a CloudGen Firewall box, enabling SecureEdge will replace the original VPN server certificate. The new root certificate can be downloaded via the Cloud UI, if needed (i.e., to import it into Trusted Root Cert stores on computers running NAC/VPN Client).
- When enabling SecureEdge on a box with an existing X.509-based C2S-VPN configuration, the VPN server will always try to extract the username from the Common Name (CN) field.



#### Figures

- 1. cgf-enrolled.png
- 2. workspace-production-9.0.png
- 3. goto-cgf.png
- 4. cgf-reg-token.png
- 5. generate\_token\_firewall.png
- 6. dashboard-firewall-admin.png
- 7. appliance-detail.png
- 8. click secureedge.png
- 9. connect -to- secure-edge.png
- 10. cgf-enrolled.png
- 11. cgf-enrolled.png
- 12. cgf-del.png
- 13. rac\_rule\_01.png
- 14. rac\_rule\_00.png

© Barracuda Networks Inc., 2024 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.