

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 Enterprises Inc/Production
Integration > CloudGen Firewalls

Registration Token

Add filter Edit columns

NAME	SERIAL	CC MANAGED	MODEL
✓ France	830634	×	F180

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 [How to Configure a Caching DNS Service](#).
- On CloudGen Firewall boxes, you must enable the VPN service. For more information, see [How to Assign Services](#).

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

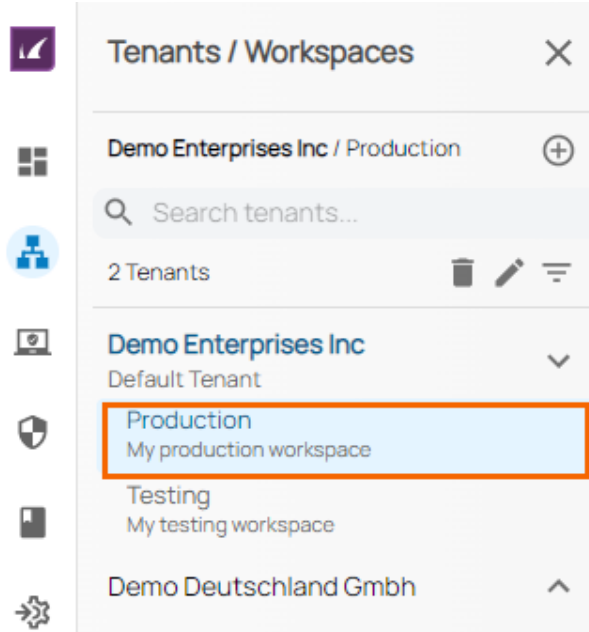
Step 1. Retrieve the Registration Token from SecureEdge

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

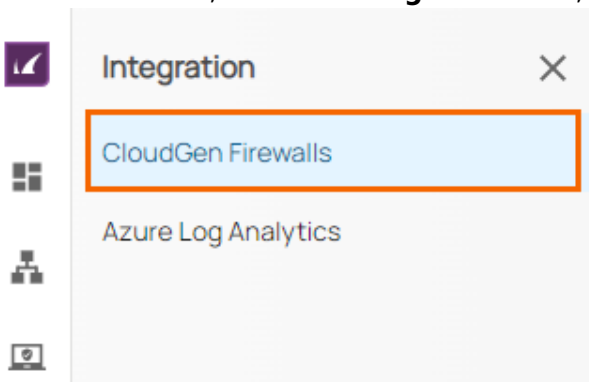
1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control

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.



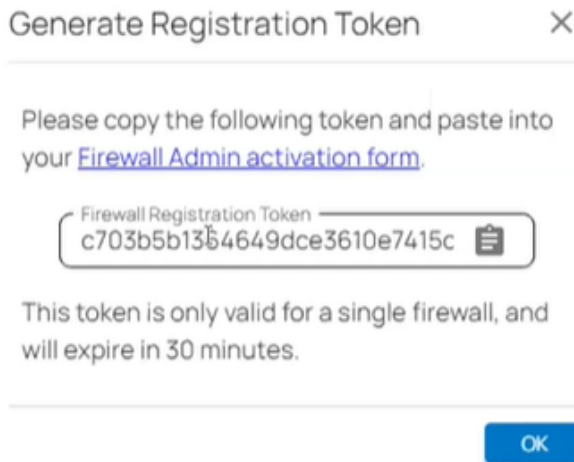
4. In the left menu, click the **Integration** icon, and select **CloudGen Firewalls**.



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



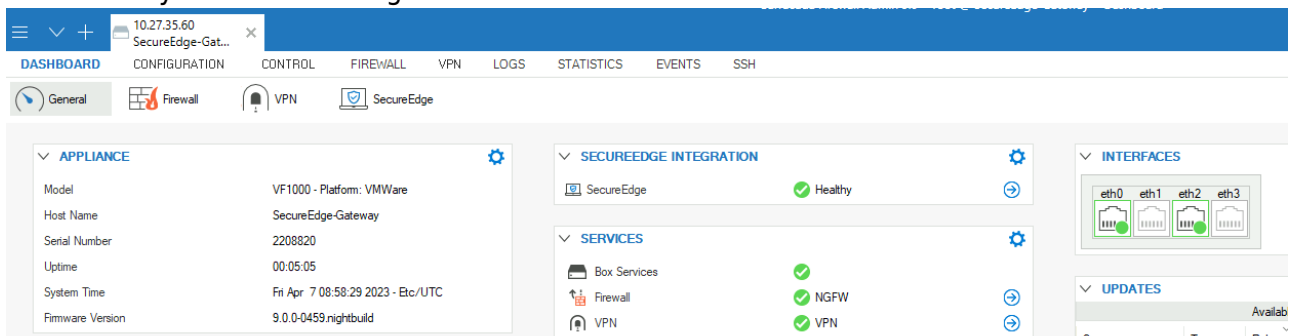
6. The **Generate Registration token** window opens.
7. Click on the clipboard icon to copy the token to your clipboard.



8. Paste the token into a text file.

Step 2. Log into the Barracuda CloudGen Firewall

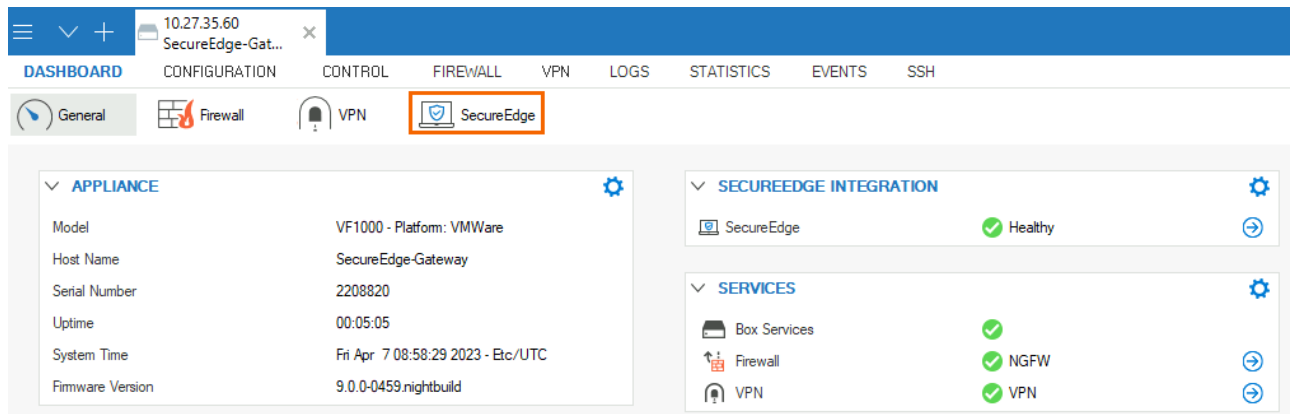
1. Connect to your firewall using Barracuda Firewall Admin.



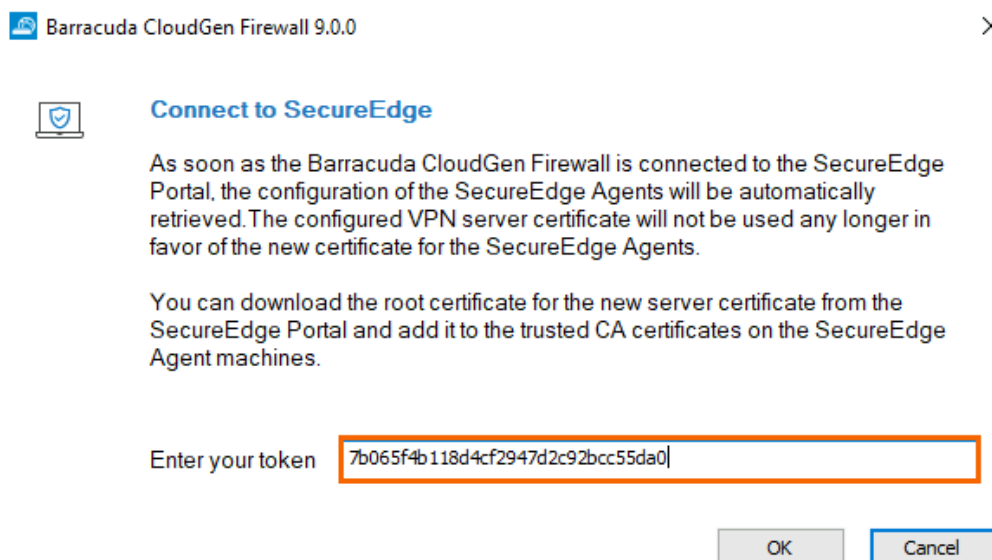
2. On the Firewall Admin **Dashboard** page, the appliance details are displayed and can be noted. For example, host name and serial number.



3. Click the **SecureEdge** icon.

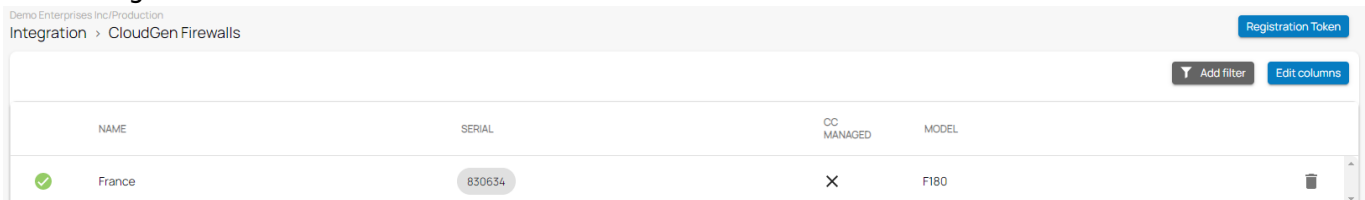


4. In the **Connect to SecureEdge** window, enter the registration token that you retrieved in Step 1.



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.



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

1. Go to <https://se.barracudanetworks.com> 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 Enterprises Inc/Production
Integration > CloudGen Firewalls

Registration Token

Add filter Edit columns

	NAME	SERIAL	CC MANAGED	MODEL	
✓	France	830634	X	F180	🗑️

Remove Existing Enrolled Appliances

If you want to remove an existing enrolled appliance,

1. Go to <https://se.barracudanetworks.com> 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.

Demo Enterprises Inc/Production
Integration > CloudGen Firewalls

Registration Token

Add filter Edit columns

	NAME	SERIAL	CC MANAGED	MODEL	
✓	France	830634	X	F180	🗑️

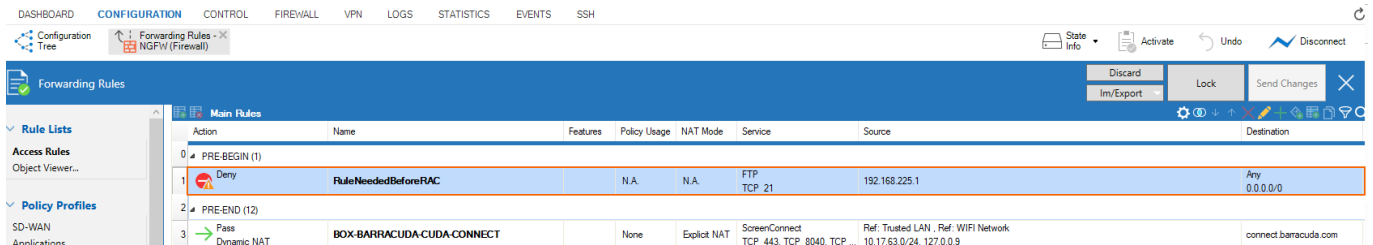
5. Click **OK** to confirm.
6. Click **Save**.

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

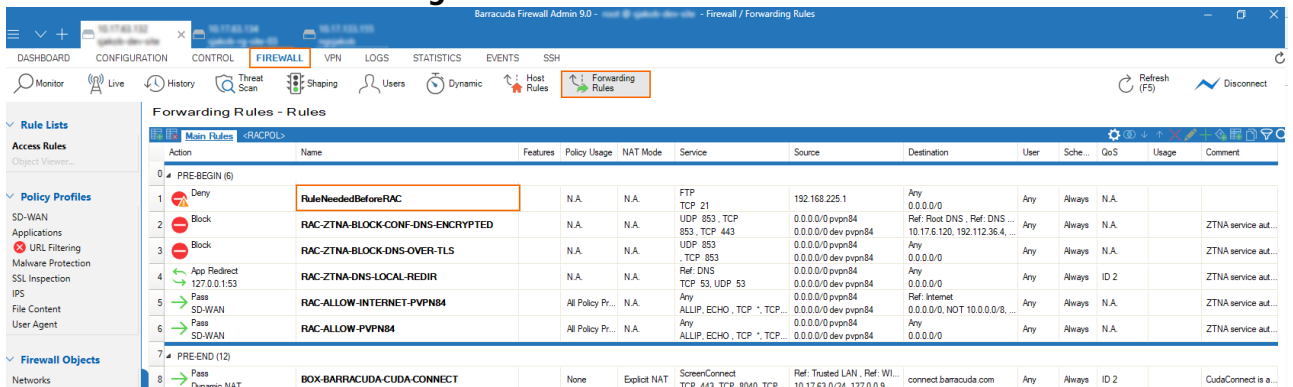
On a Barracuda CloudGen Firewall, ZTNA access rules are auto-generated and cannot be moved. However, if you introduce the section separators PRE-BEGIN and PRE-END and place your own rule in between, this rule is placed before the ZTNA auto-generated rules.



Action	Name	Features	Policy Usage	NAT Mode	Service	Source	Destination
Deny	RuleNeededBeforeRAC		N.A.	N.A.	FTP TCP 21	192.168.225.1	Any 0.0.0.0/0
Pass	PRE-END (12)						
Pass	BOX-BARRACUDA-CUDA-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**.



Action	Name	Features	Policy Usage	NAT Mode	Service	Source	Destination	User	Sche...	QoS	Usage	Comment
Deny	RuleNeededBeforeRAC		N.A.	N.A.	FTP TCP 21	192.168.225.1	Any 0.0.0.0/0	Any	Always	N.A.		
Block	RAC-ZTNA-BLOCK-CONF-DNS-ENCRYPTED		N.A.	N.A.	UDP 853, TCP 443	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...
Block	RAC-ZTNA-BLOCK-DNS-OVER-TLS		N.A.	N.A.	UDP 853	0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	N.A.		ZTNA service aut...
App Redirect	RAC-ZTNA-DNS-LOCAL-REDIR		N.A.	N.A.	Ref: DNS TCP 53, UDP 53	0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	ID 2		ZTNA service aut...
Pass	RAC-ALLOW-INTERNET-PVPN84		All Policy Pr...	N.A.	Any ALLIP, ECHO, TCP *, TCP...	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...
Pass	RAC-ALLOW-PVPN84		All Policy Pr...	N.A.	Any ALLIP, ECHO, TCP *, TCP...	0.0.0.0/0 dev pvpn84	Any 0.0.0.0/0	Any	Always	N.A.		ZTNA service aut...
Pass	PRE-END (12)											
Pass	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: [How to Block UDP Port 443 on CloudGen Firewalls](#).

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.