

How to Configure CloudGen Firewall and Web Application Firewall Integration

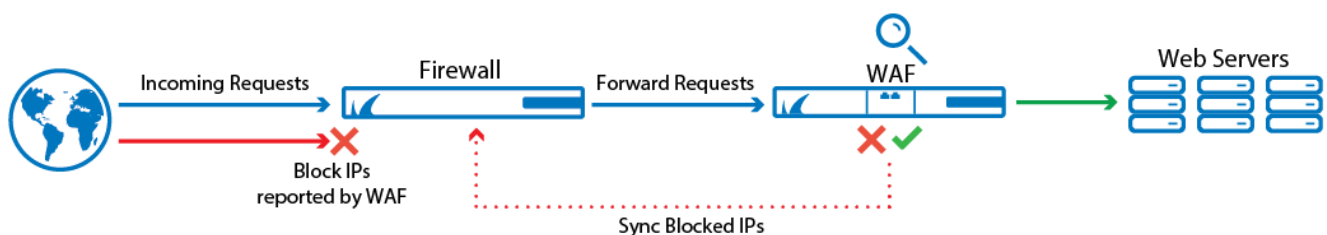
<https://campus.barracuda.com/doc/96025927/>

The Barracuda Web Application Firewall (WAF) and CloudGen Firewall can work in tandem to block IP addresses from which malicious activity was detected. While the WAF is very good at detecting application layer attacks, the CloudGen Firewall is more efficient on the network layer. Connections blocked by the firewall are never forwarded to the WAF, thereby freeing resources that would otherwise have to be used to block known-bad connections.

The CloudGen Firewall is located at the perimeter with the WAF behind it. IP addresses that are blocked by the WAF are synced to the fourth custom external network object on the firewall via REST API calls. For the WAF to see the public IP address of the request and to block the public IP address associated with the request, the WAF must use the firewall as the default gateway.

Blocking IP Addresses for a Detected Attack:

1. Incoming HTTP/HTTPS connections are forwarded to the WAF.
2. If an attack is detected by the WAF, the attack is blocked and the IP address is added to the CustomExternalNetworkObject4 on the CloudGen Firewall via REST API call.
3. Subsequent attacks from the blocked IP address are blocked on the firewall, freeing up resources on the WAF.
4. After the defined timeout, the IP address is removed from the blocked IP addresses on the WAF and removed from the custom external network object on the firewall via REST API call.



Limitations for High Availability Clusters in the Public Cloud

- The WAF can only send REST API calls to one firewall. High availability CloudGen Firewall clusters in the public cloud cannot be both updated by one REST API call. An internal load balancer between the WAF and the firewalls can be used to update only the active firewall.

Before You Begin

- The WAF must use the firewall as the default gateway.
- In the public cloud, the WAF and the firewall must be deployed into two different subnets.

Step 1. Configure Admin for Accessing the REST API

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrators**.
2. Click **Lock**.
3. In the **Administrators** section, click **+** to add an administrator account.
4. Enter **restadmin** for the **Name** and click **OK**. The **Administrators** window opens.
5. Configure the admin:
 - **Full Name** - Enter **REST Admin**.
 - **Assigned Roles** - Select **Manager**.
 - **System Level Access** - Select **No OS Login**.
 - **Authentication Level** - Select **Password**.
 - **Password Validation** - Select **Against Local Password**.
 - **Password** - Enter the password.

Account Description

Account Status	Enabled	▼	📋
Full Name	REST Admin		

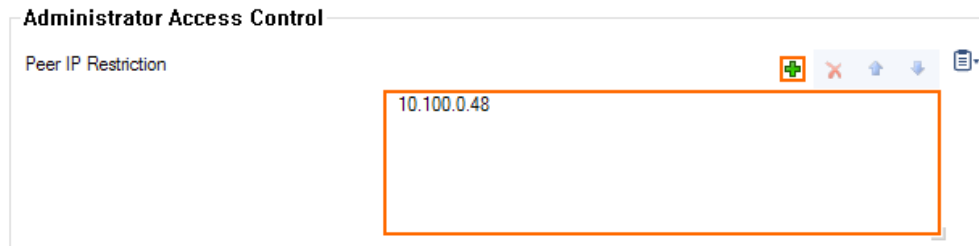
Administrator Authorization

Assigned Roles	Manager	📋
System Level Access	No OS Login	▼

Administrator Authentication

Authentication Level	Password	▼	📋
Password Validation	Against Local Password		
External Login Name			
Password	New	•••••	📋
	Confirm	•••••	
Strength			

- **(optional) Peer IP Restriction** - Add the IP address of the WAF and remove the **0.0.0.0/0** entry.



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

Step 2. Enable REST API for HTTP or HTTPS

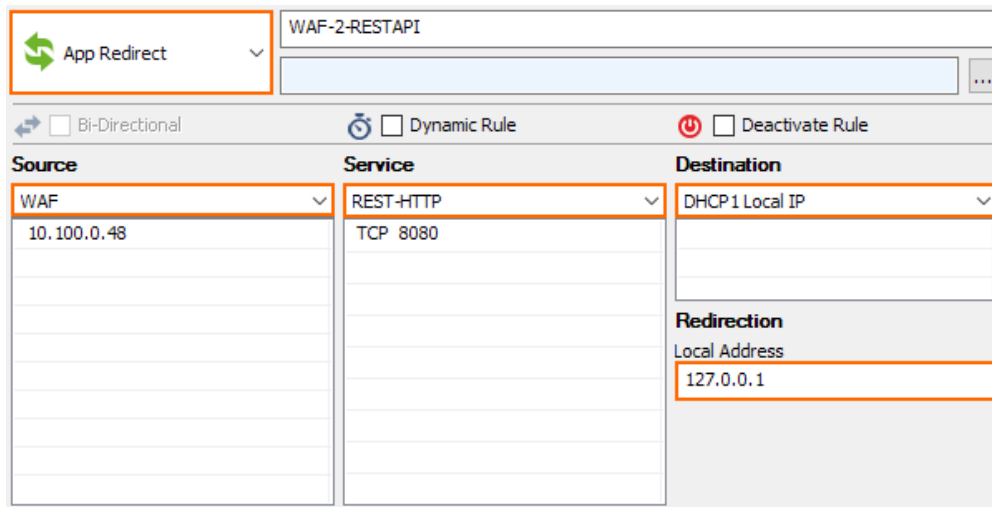
1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service**.
2. Click **Lock**.
3. Verify that either the **HTTP** or **HTTPS Interface** of the REST API is enabled. For more information, see [REST API](#).
4. Click **Send Changes** and **Activate**.

Step 3. Create App Redirect Rule for REST API Calls from the WAF

Allow REST API calls for HTTP or HTTPS from the WAF and redirect them to the rest daemon listening on 127.0.0.1:8080 (HTTP) or 127.0.0.1:8443 (HTTPS).

Create an access rule to redirect incoming REST API calls to the REST daemon:

- **Action** – Select **App Redirect**.
- **Source** – Enter the IP address of the WAF.
- **Service** – Select **HTTP** or **HTTPS**.
- **Destination** – Select the box IP address the WAF uses for the REST API call. In the public cloud, select **DHCP Local IP1**.
- **Redirection** – Enter 127.0.0.1 for the HTTP REST endpoint.



App Redirect

WAF-2-RESTAPI

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

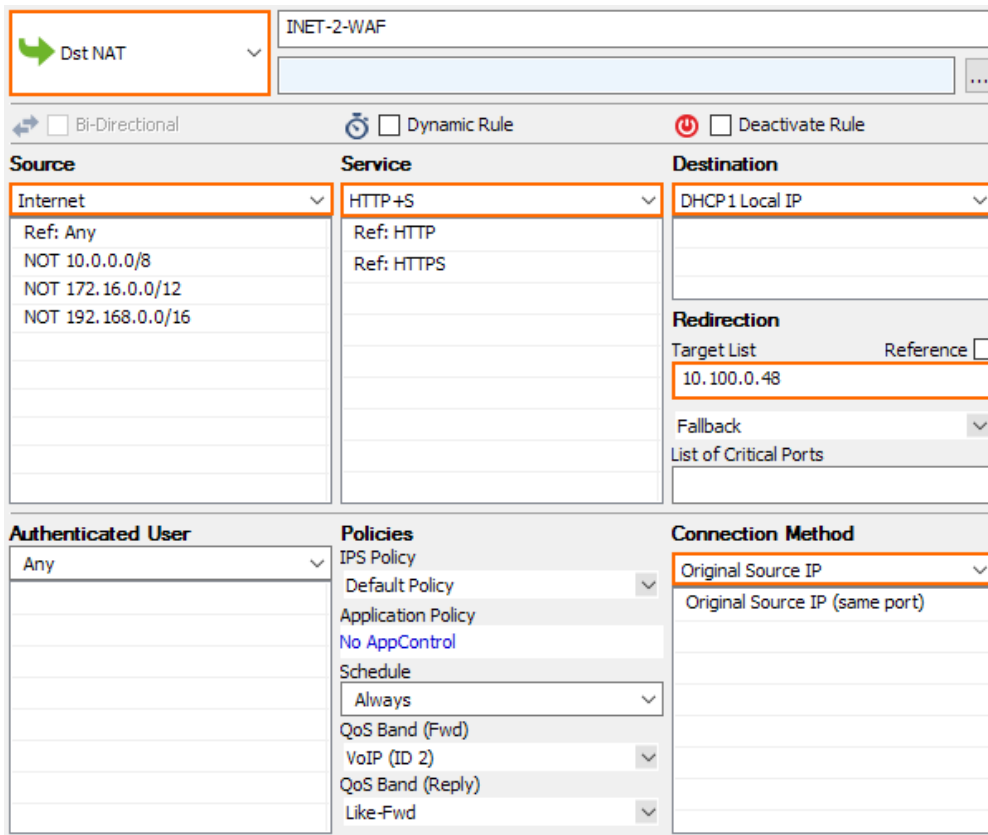
Source	Service	Destination
WAF	REST+HTTP	DHCP1 Local IP
10.100.0.48	TCP 8080	

Redirection
Local Address
127.0.0.1

Step 3. Create a DST NAT Rule to Forward Web Traffic to the WAF

Create an access rule to forward all incoming HTTP and/or HTTPS traffic to the WAF:

- **Action** – Select **Dst NAT**.
- **Source** – Select **Internet**.
- **Service** – Select **HTTP**, **HTTPS**, or **HTTP+S** depending on the type of web traffic forwarded to the WAF.
- **Destination** – Enter the public IP address of the firewall, or the network object for the dynamic WAN connection.
- **Redirection** – Enter the IP address for the WAF.
- **Connection Method** – Select **Original Source IP**.



Rule Name: INET-2-WAF

Action: Dst NAT

Options: ☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16	HTTP+S Ref: HTTP Ref: HTTPS	DHCP1 Local IP

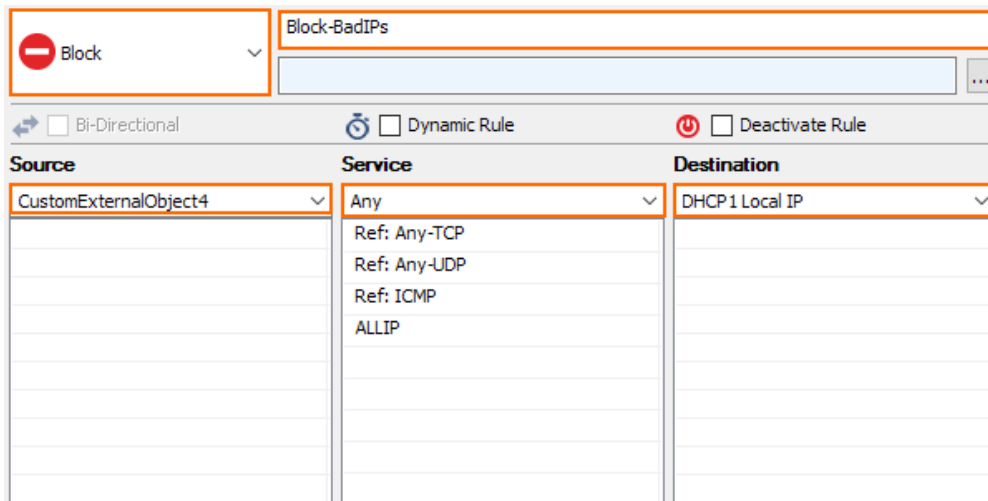
Redirection:
 Target List: 10.100.0.48
 Reference: ☐
 Fallback:
 List of Critical Ports:

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl Schedule: Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	Original Source IP Original Source IP (same port)

Step 4. Create an Access Rule to Block Malicious IP Addresses

Create an access rule to block the malicious IP address stored in the custom external object number 4.

- **Action** – Select **Block**.
- **Source** – Select **CustomExternalObject4**.
- **Service** – Select **HTTP**, **HTTPS**, or **HTTP+S** depending on the type of application.
- **Destination** – Enter the public IP address of the firewall, or the network object for the dynamic WAN connection.

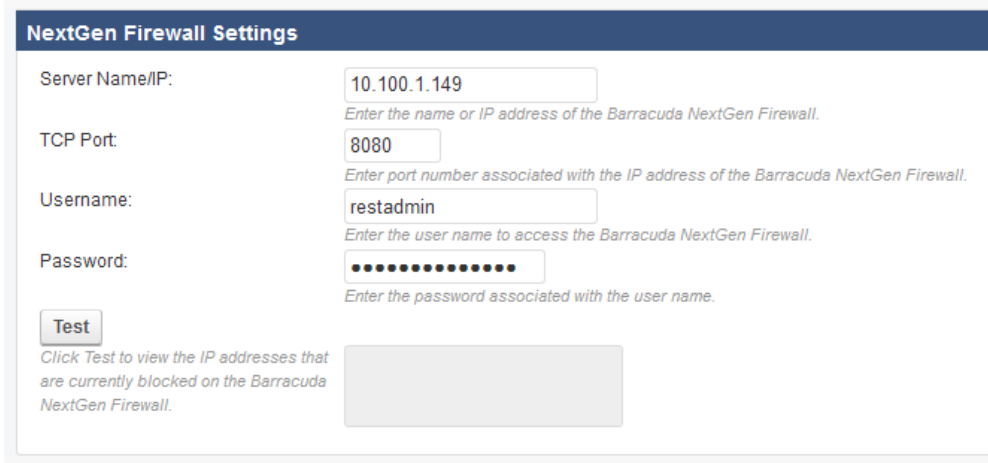


Source	Service	Destination
CustomExternalObject4	Any	DHCP 1 Local IP

Ref: Any-TCP
Ref: Any-UDP
Ref: ICMP
ALLIP

Step 5. Configure the Barracuda Web Application Firewall

Go to **ADVANCED > CloudGen Firewall Settings** and configure the IP address and user for the REST API calls. Go to **SECURITY POLICIES > Action Policies** to edit the Attack action for the security policies to use **Block Client-IP** as the **Follow Up Action**.



NextGen Firewall Settings

Server Name/IP: 10.100.1.149
Enter the name or IP address of the Barracuda NextGen Firewall.

TCP Port: 8080
Enter port number associated with the IP address of the Barracuda NextGen Firewall.

Username: restadmin
Enter the user name to access the Barracuda NextGen Firewall.

Password:
Enter the password associated with the user name.

Test
Click Test to view the IP addresses that are currently blocked on the Barracuda NextGen Firewall.

Edit Attack Action		Help
Attack Action Name	Invalid Header	
ID	invalid-header	
Numeric ID	121	
Action:	<div>Protect and Log</div> <p><i>Specifies what to do when this attack is encountered. The actual protection method varies from attack to attack. Most attacks on the request cause the request to be denied, for which, the Deny Response decides how the request is denied.</i></p>	
Deny Response:	<div>Send Response</div> <p><i>Specifies how the request should be denied (applicable only for those attacks whose protection method is to deny the request).</i></p>	
Redirect URL:	<div></div> <p><i>Specifies the URL to be used to redirect the request if the deny response is set to "Permanent Redirect" or "Temporary Redirect". The URL should start with a "/" or should be a fully qualified URL like http://domain/url or https://domain/url. When using the "Follow Up Action" as "Challenge with CAPTCHA", configure a %s to redirect to the original URL, or a %b to redirect to the base part of the original URL if desired.</i></p>	
Response Page:	<div>default</div> <p><i>Specifies the response page to be sent to the client if the "Deny Response" is set to "Send Response".</i></p>	
Follow Up Action:	<div>Block Client-IP</div> <p><i>Specifies the follow up action to be taken if any protection action is taken.</i></p>	
Follow Up Action Time:	<div>60</div> <p><i>Specifies the time in seconds to block the client IP if "Follow Up Action" is set to "Block Client IP".</i></p>	

For more information, see [Upstream Firewall Configuration](#) and [Security Policies](#).

Figures

1. ngf_waf_integration.png
2. WAF_01a.png
3. WAF_01b.png
4. WAF_02.png
5. WAF_03.png
6. WAF_04.png
7. WAF_05.png
8. WAF_06.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.