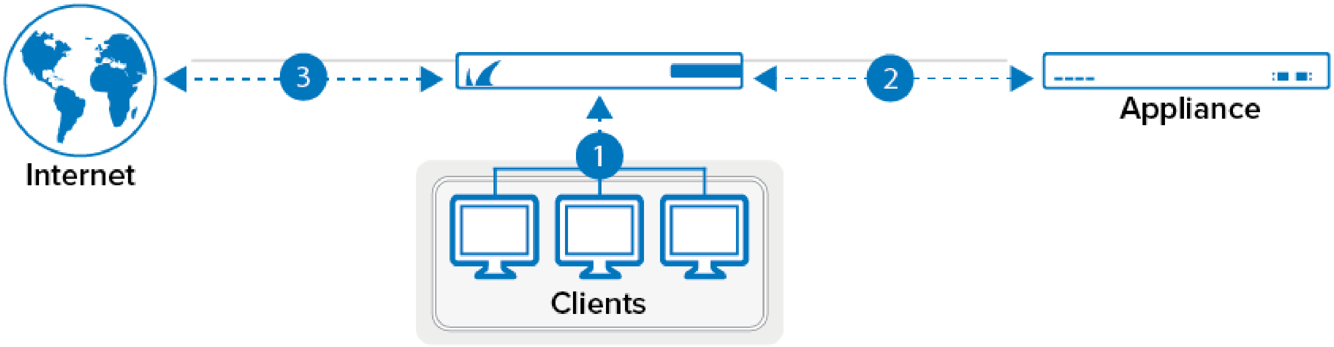
How to Configure a Transparent Redirect

https://campus.barracuda.com/doc/100371634/

> The following instructions apply to any appliance processing traffic that requires the original source and destination IP addresses to remain unmodified.

To transparently forward connections to a processing appliance located in a DMZ behind a CloudGen Firewall, configure the Dst NAT access rule to not rewrite the source and destination addresses of the connection. Using the original source and destination IP addresses allows the appliance to apply meaningful policies as if it were directly connected to the client.



Before You Begin

- Verify that the CloudGen Firewall and the proxy are directly connected to the same subnet (within the same ARP domain).
- (optional) Enable SSL Inspection in the firewall. For more information, see SSL Inspection in the Firewall.
- (optional) Configure the processing appliance to use transparent SSL Inspection.

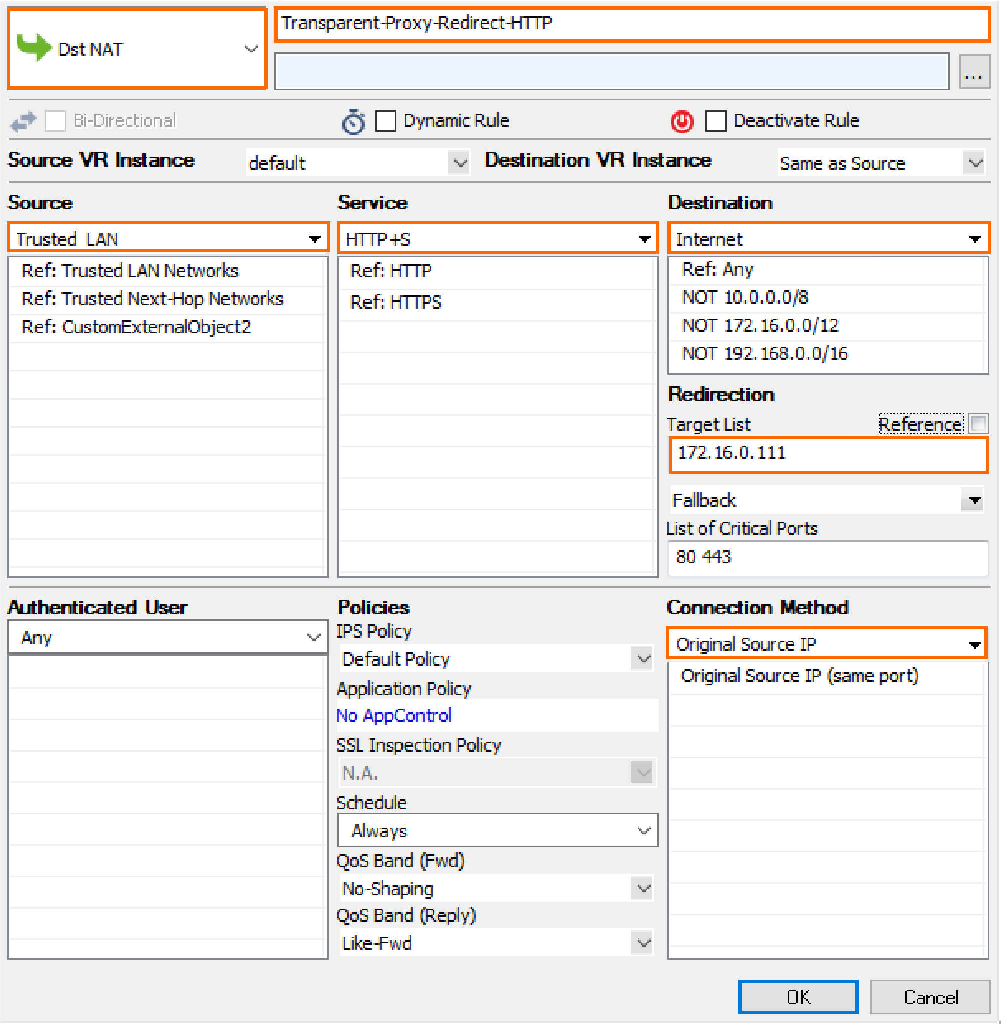
Step 1. Create a Transparent Redirect Dst NAT Access Rule

Create the Dst NAT access rule to forward all traffic to the proxy.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create an access rule to forward selected traffic coming from your clients:
   - **Action** – Select **Dst NAT**.

- **Source** – Select **Trusted Networks**. Or, you can enter the network the client using the appliance is in.
- **Destination** – Select **Internet**.
- **Service** – Select **HTTP+S**.
- **Target List** – Enter the IP address without a port. You can use multiple proxies.
  E.g.: `172.16.0.10`

  > Do not use network objects containing hostnames (DNS objects). The firewall does not redirect traffic to a hostname or FQDN.
- **Fallback/Cycle** – If you have defined multiple target IP addresses, select how the firewall distributes the traffic between the IP addresses.
  - **Fallback** – The connection is redirected to the first available IP address in the list.
  - **Cycle** – New incoming TCP connections are distributed evenly over the available IP addresses in the list on a per-source IP address basis. The same redirection target is used for all subsequent connections of the source IP address. UDP connections are redirected to the first IP address and not cycled.
- **List of Critical Ports** – Enter a space-delimited list of ports used.
- **Connection Method** – Select **Original Source IP**.
- **(optional) Application Policy** – Enable **Application Control** and **SSL Inspection** to gain deeper insight on the traffic redirected to the appliance.
  - If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see SSL Inspection in the Firewall.



Dst NAT

Transparent-Proxy-Redirect-HTTP

□ Bi-Directional □ Dynamic Rule □ Deactivate Rule

Source VR Instance default **Destination VR Instance** Same as Source

Source

Trusted LAN

- Ref: Trusted LAN Networks
- Ref: Trusted Next-Hop Networks
- Ref: CustomExternalObject2

Service

HTTP+S

- Ref: HTTP
- Ref: HTTPS

Destination

Internet

- Ref: Any
- NOT 10.0.0.0/8
- NOT 172.16.0.0/12
- NOT 192.168.0.0/16

Redirection

Target List — Reference □

172.16.0.111

Fallback

List of Critical Ports

80 443

Authenticated User

Any

Policies

IPS Policy: Default Policy

Application Policy: No AppControl

SSL Inspection Policy: N.A.

Schedule: Always

QoS Band (Fwd): No-Shaping

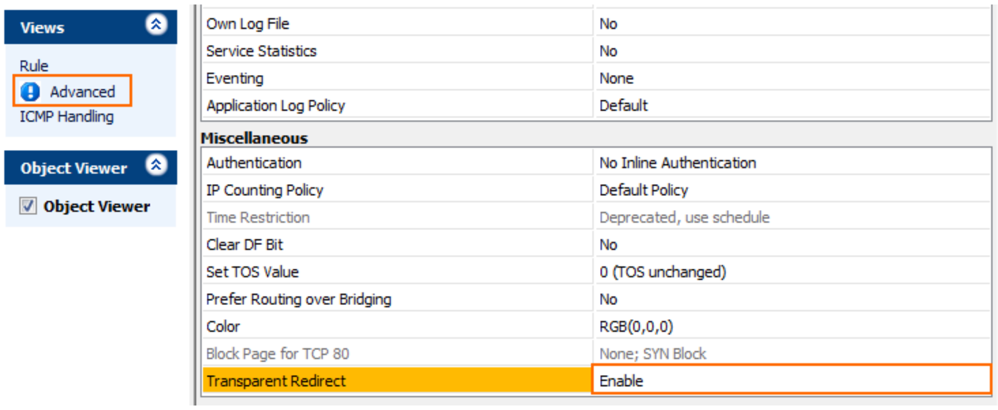
QoS Band (Reply): Like-Fwd

Connection Method

Original Source IP

Original Source IP (same port)

4. In the left menu, click **Advanced**.
5. In the **Miscellaneous** section, set **Transparent Redirect** to **Enable**.



Own Log File	No
Service Statistics	No
Eventing	None
Application Log Policy	Default
Miscellaneous	
Authentication	No Inline Authentication
IP Counting Policy	Default Policy
Time Restriction	Deprecated, use schedule
Clear DF Bit	No
Set TOS Value	0 (TOS unchanged)
Prefer Routing over Bridging	No
Color	RGB(0,0,0)
Block Page for TCP 80	None; SYN Block
Transparent Redirect	Enable

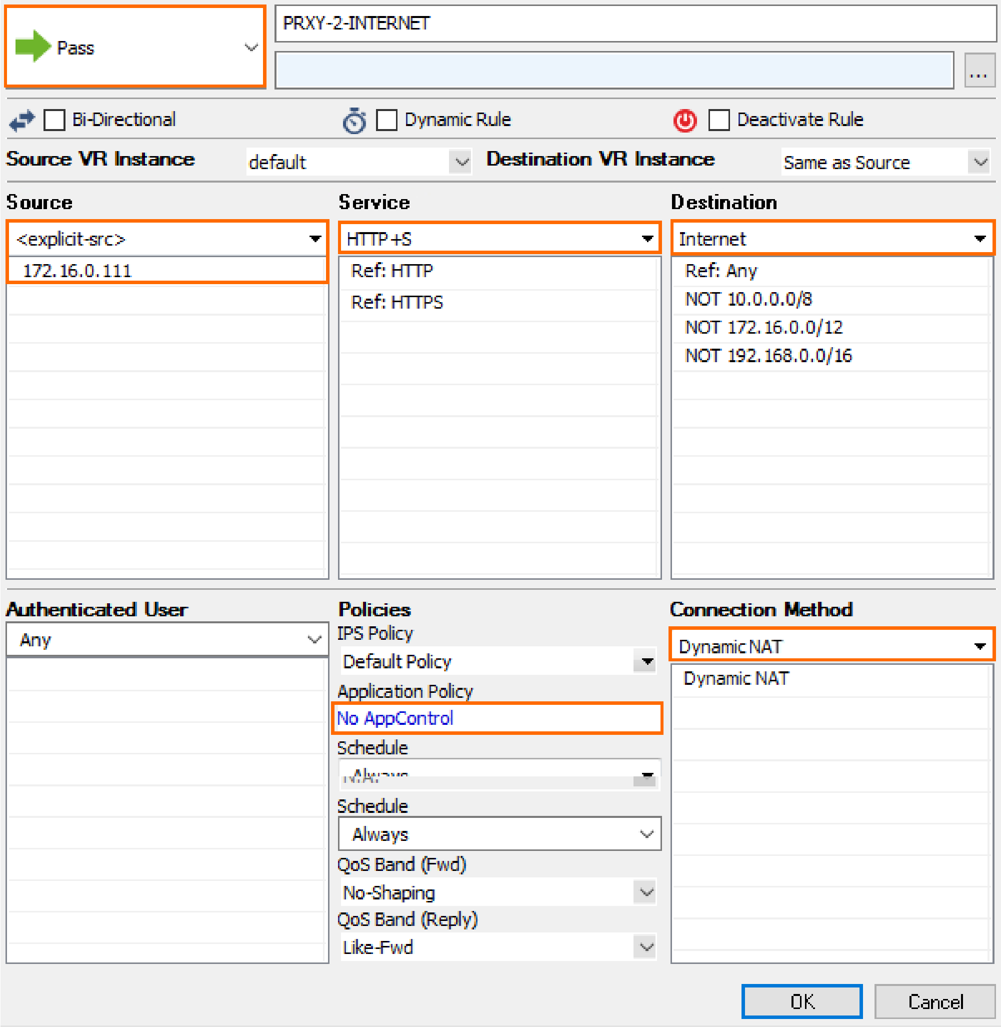
6. Click **OK**.
7. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

> Make sure to place the rule above all other HTTP/HTTPS rules that match this source and destination.

8. Click **Send Changes** and **Activate**.

Step 2. Create a Pass Access Rule for the Proxy to Access the Internet

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a PASS rule to allow the HTTP proxy to access the Internet:
    - **Action** – Select **Pass**.
    - **Source** – Enter the IP address of the HTTP Proxy.
    - **Destination** – Select **Internet**.
    - **Service** – Select **HTTP+S**.
    - **Connection Method** – Select **Dynamic NAT**.
    - **(optional) Application Policy** – Select Application Control policies.



Pass

PRXY-2-INTERNET

□ Bi-Directional □ Dynamic Rule □ Deactivate Rule

Source VR Instance: default

Destination VR Instance: Same as Source

Source: <explicit-src>
- 172.16.0.111

Service: HTTP+S
- Ref: HTTP
- Ref: HTTPS

Destination: Internet
- Ref: Any
- NOT 10.0.0.0/8
- NOT 172.16.0.0/12
- NOT 192.168.0.0/16

Authenticated User: Any

Policies
- IPS Policy: Default Policy
- Application Policy: No AppControl
- Schedule: Always
- Schedule: Always
- QoS Band (Fwd): No-Shaping
- QoS Band (Reply): Like-Fwd

Connection Method: Dynamic NAT
- Dynamic NAT

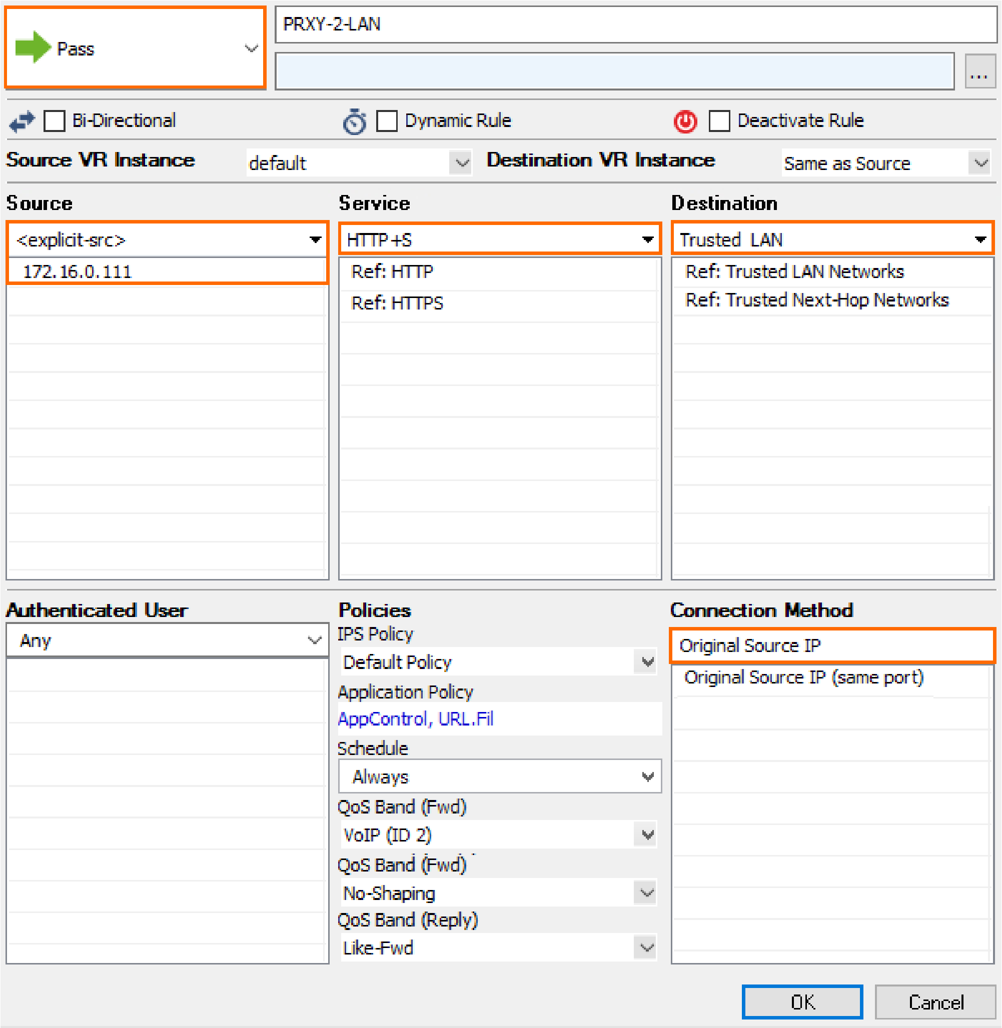
4. In the left menu, click **Advanced**.
5. In the **Dynamic Interface Handling** section, set **Source Interface** to **Any**.
6. Click **OK**.

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

Step 3. Create a Pass Access Rule for the HTTP Proxy to Access the Client Network

To allow the HTTP proxy to access the client, you must create a PASS rule:

- **Action** – Select **Pass**.
- **Source** – Enter the IP address of the appliance.
- **Destination** – Select **Trusted Networks**.
- **Service** – Select **HTTP+S**.
- **Connection Method** – Select **Original Source IP**.
- **(optional) Application Policy** – Select Application Control policies.



Pass

PRXY-2-LAN

□ Bi-Directional □ Dynamic Rule □ Deactivate Rule

Source VR Instance: default

Destination VR Instance: Same as Source

Source: <explicit-src>
172.16.0.111

Service: HTTP+S
Ref: HTTP
Ref: HTTPS

Destination: Trusted LAN
Ref: Trusted LAN Networks
Ref: Trusted Next-Hop Networks

Authenticated User: Any

Policies

IPS Policy: Default Policy

Application Policy: AppControl, URL.Fil

Schedule: Always

QoS Band (Fwd): VoIP (ID 2)

QoS Band (Fwd): No-Shaping

QoS Band (Reply): Like-Fwd

Connection Method: Original Source IP
Original Source IP (same port)

Step 4. Configure the Appliance

In order to successfully send the connection from the proxy to the Internet, you must configure the processing device:

- Route to the Internet using the firewall as the gateway.
- Route to the internal client network using the firewall as the gateway.
- Traffic must use the IP address of the appliance as the source IP address for outgoing connections.
- The appliance must accept the HTTP and HTTPS connections on the same port as the firewall.

Step 5. Import the Appliance's Root Certificate

If you are running SSL Inspection on the CloudGen Firewall, you must add the root certificate used for SSL Inspection to the **Trusted Root Certificates**.

1. Download the root certificate on the appliance.
2. On the CloudGen Firewall, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy Settings**.
3. Click **Lock**.
4. Click **+** in the **Trusted Root Certificates** list and select **Import from PEM File**.
5. Select the file containing the root certificate you previously exported from the appliance.
6. Enter a **Name**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

The certificate is now listed in the **Trusted Root Certificates** list.

Next Steps

Import the root certificates from the CloudGen Firewall and the processing appliance on the clients to avoid SSL certificate errors.

Figures

1. transparent_redir_rules-01.png
2. transparent_redirect_00.png
3. transparent_redirect_01.png
4. transparent_redirect_02.png
5. transparent_redirect_03.png