Solution Brief

Configuring a Transparent Redirect with the Barracuda CloudGen Firewall

To transparently forward connections to a proxy behind a Barracuda CloudGen Firewall F-Series in the DMZ, you can configure the Dst NAT access rule to not rewrite the source and destination addresses of the connection. This configuration allows the proxy to apply all policies as if it were directly connected to the client. It also allows the proxy to create meaningful statistics and connection information.

The proxy as described here may be a Barracuda Web Security Gateway. The Web Security Gateway must be running firmware version 10.0 or higher and use Transparent SSL Interception. For more information, see How to Configure SSL Inspection Version 10 and Above.

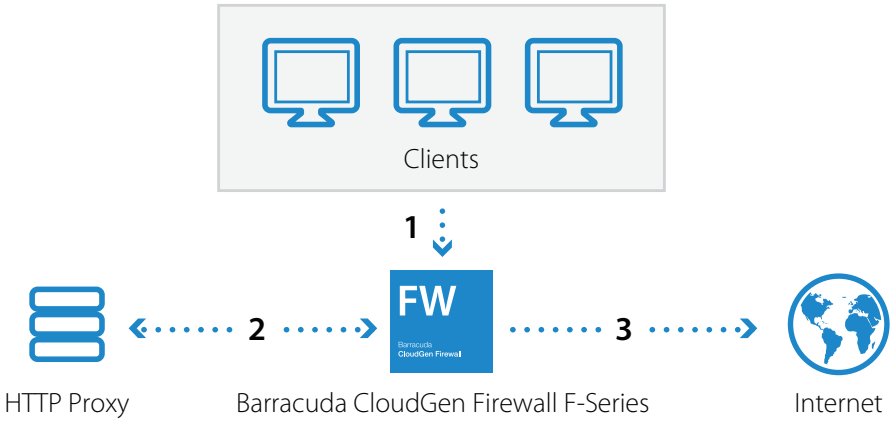


Figure 1 - Transparent Redirect Network Map

Before You Begin

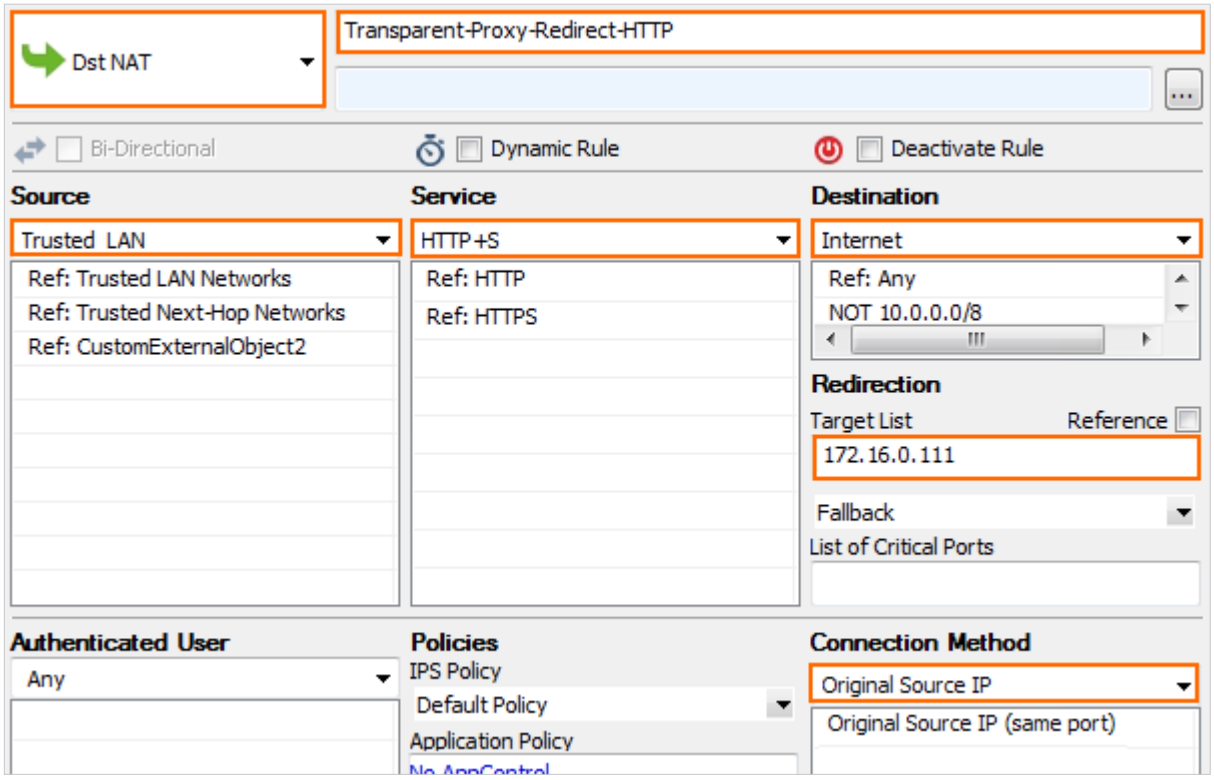
- Verify that the Forwarding Firewall service is using **Feature Level 7.0** or higher.
- The F-Series Firewall and the proxy must be directly connected to the same subnet (within the same ARP domain).

Step 1: Create a Transparent Redirect Dst NAT Access Rule

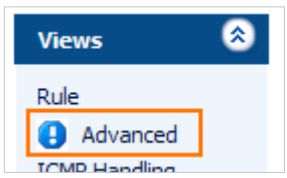
Create the Dst NAT access rule to forward all traffic to the proxy.

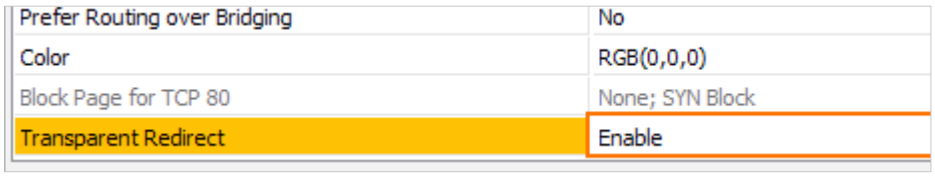
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual servers > Firewall > Forwarding Rules.**
2. Click **Lock**.

3. Create an access rule to forward selected traffic coming from your clients to the proxy:
   - **Action** – Select **Dst NAT**.
   - **Source** – Select **Trusted Networks**. Or, you can enter the network the client using the HTTP Proxy is in.
   - **Destination** – Select **Internet**.
   - **Service** – Select the service you want to forward. E.g. **HTTP+S**.
   - **Target List*** – Enter the IP address without a port. You can use multiple proxies. E.g. 172.16.0.10
   - **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 **No SNAT**.
   - **(optional) Application Policy** – Select Application Control policies.



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



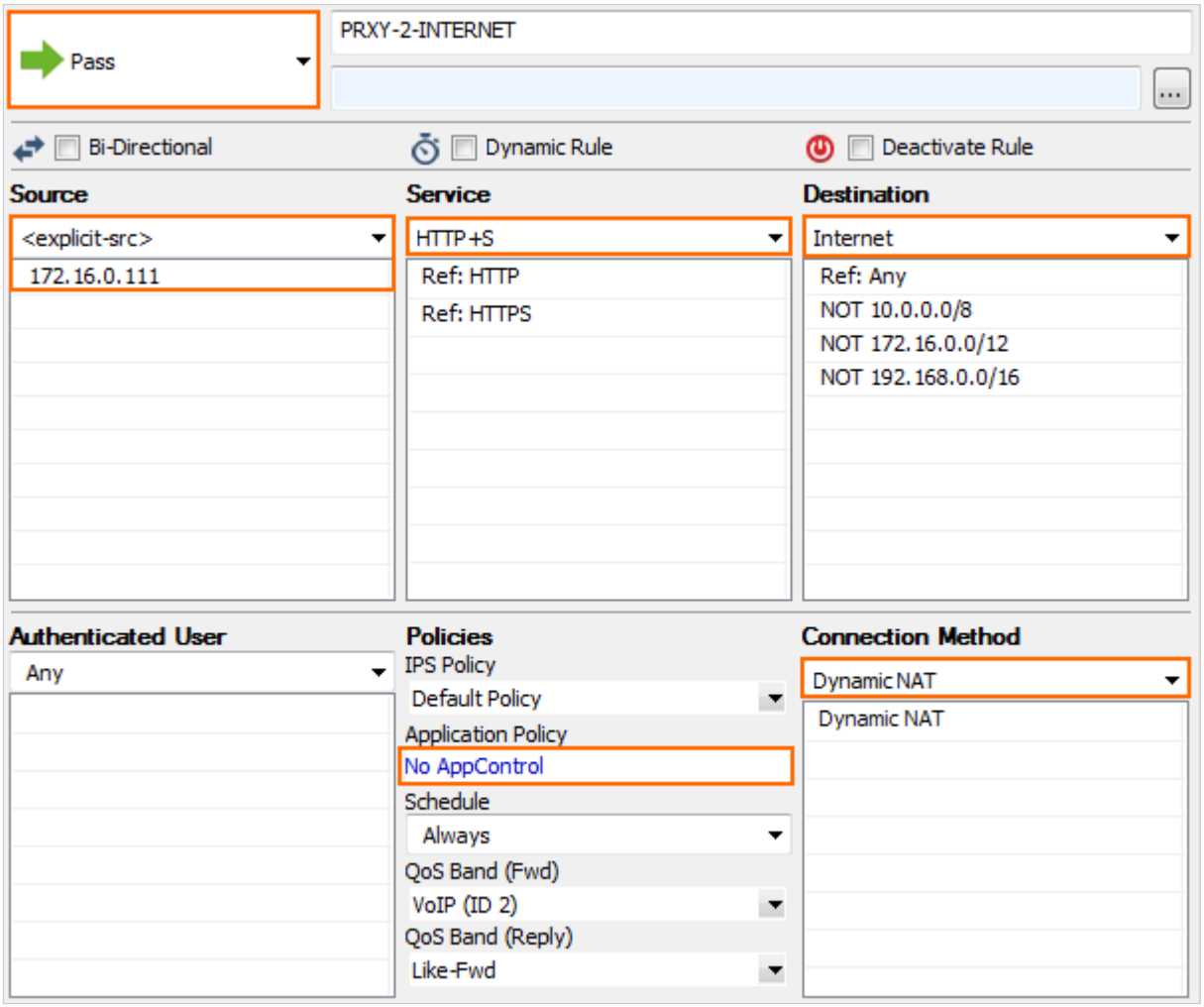


6. Click **OK**.
7. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
8. Click **Send Changes** and **Activate**.

*Do not use network objects containing hostnames (DNS objects). The firewall does not redirect traffic to a hostname or FQDN.

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual servers* > 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 SNAT**.
   - **(optional) Application Policy** – Select Application Control policies.

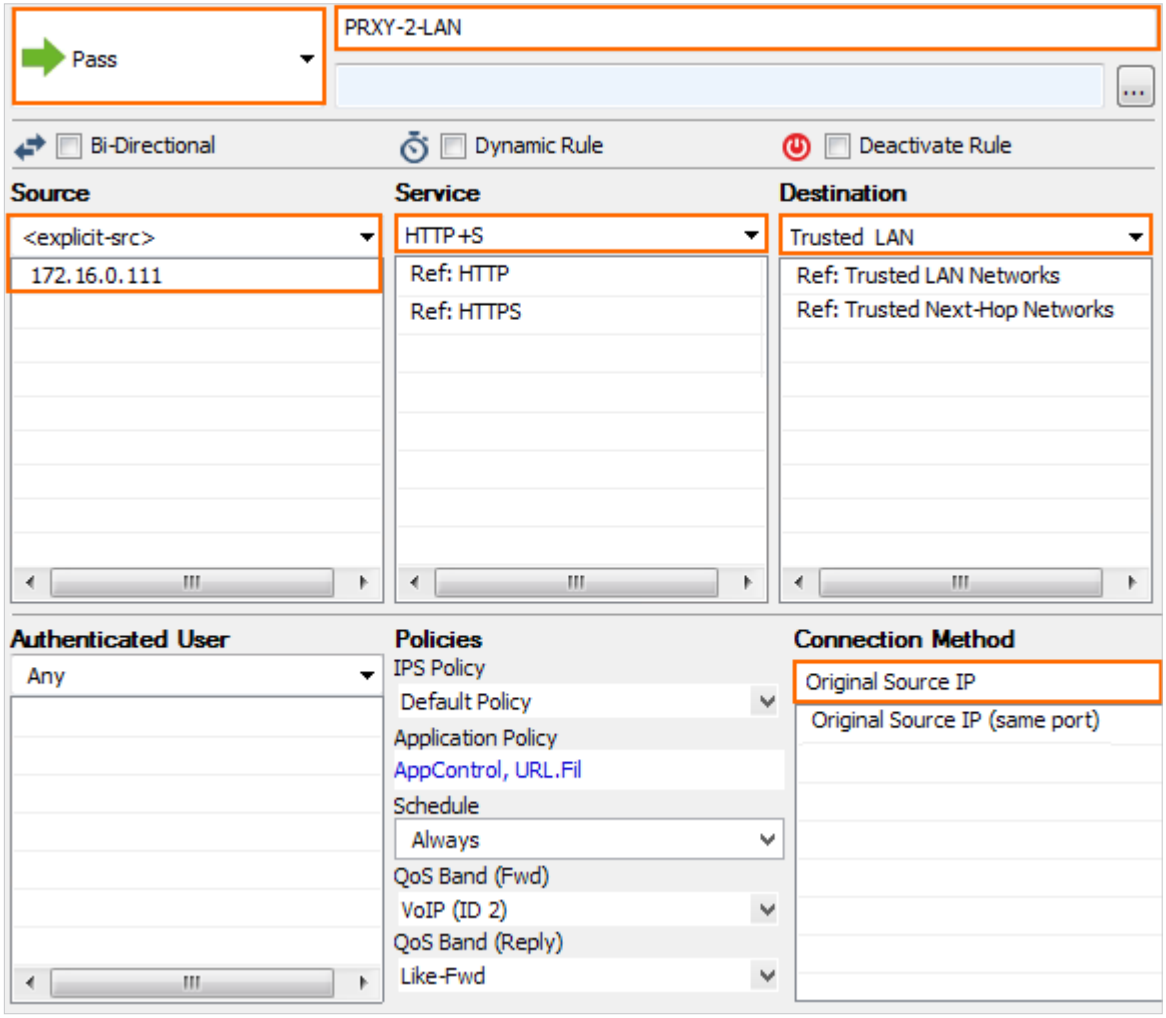


4. In the left menu, click **Advanced**.
5. In the **Dynamic Interface Handling** section, set **Source Interface** to **Any**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

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

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 HTTP proxy.
- **Destination** – Select **Trusted Networks**.
- **Service** – Select **HTTP+S**.
- **Connection Method** – Select **No SNAT**.
- **(optional) Application Policy** – Select Application Control policies.



Step 4: Configure the Proxy

In order to successfully send the connection from the proxy to the Internet, you must configure the 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 proxy as the source IP for outgoing connections.
- The proxy must accept the HTTP and HTTPS connections on the same port as the firewall.