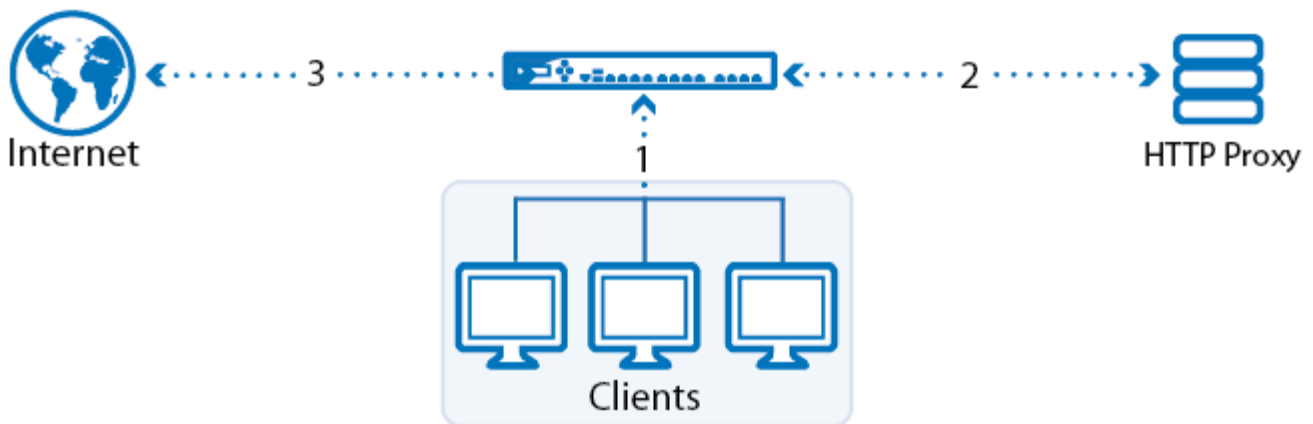


## How to Configure a Transparent Redirect

<https://campus.barracuda.com/doc/46209066/>

To transparently forward connections to a proxy behind a NextGen 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. Transparent Redirect for the Barracuda Security Gateway is limited to HTTP.



### In this article

### Before your Begin

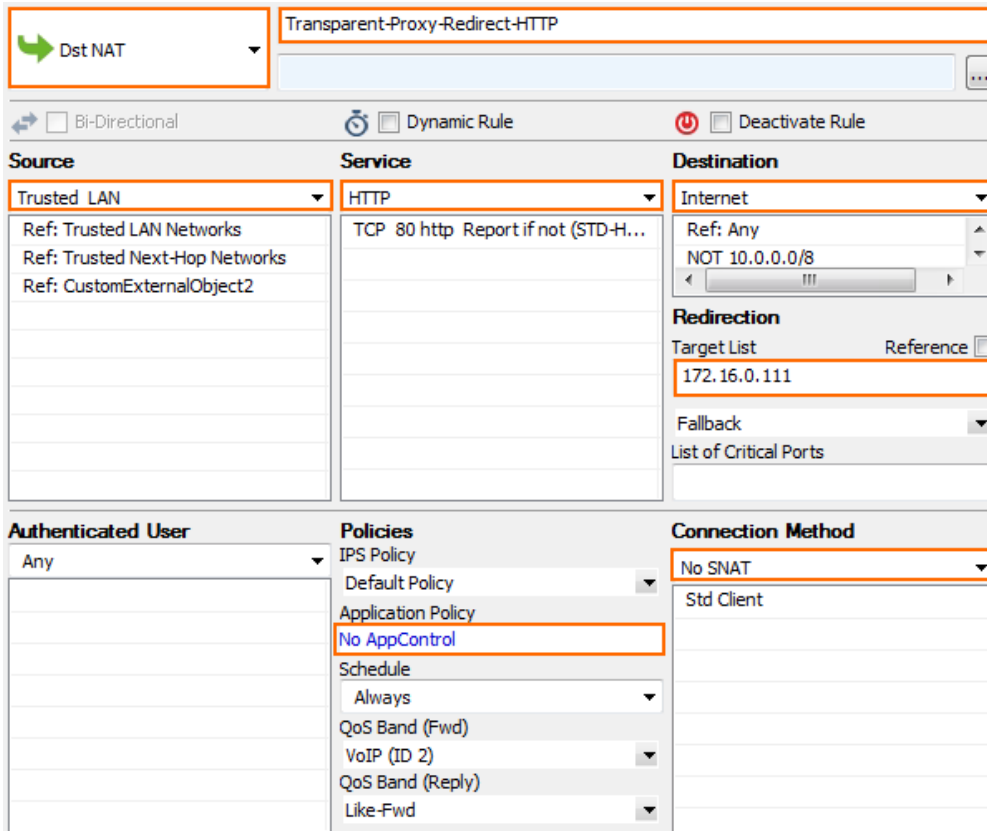
- Verify that the Forwarding Firewall service is using **Feature Level 6.1** or above.
- The F-Series Firewall and the Proxy must be directly connected to the same subnet (within the same ARP domain).

### Step 1. Create a Transparent Redirect DNAT Access Rule

Create the DNAT 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.** Alternatively 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
 



Do not use network objects containing host names (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 **No SNAT.**
  - **Application Policy** - Disable **Application Control.**



The screenshot shows the configuration for a rule named "Transparent-Proxy-Redirect-HTTP". The rule is configured as follows:

- Action:** Dst NAT
- Source:** Trusted LAN (References: Trusted LAN Networks, Trusted Next-Hop Networks, CustomExternalObject2)
- Service:** HTTP (TCP 80 http Report if not (STD-H...))
- Destination:** Internet (Ref: Any, NOT 10.0.0.0/8)
- Redirection:** Target List: 172.16.0.111
- Fallback:** (Dropdown menu)
- List of Critical Ports:** (Text input field)
- Authenticated User:** Any
- Policies:**
  - IPS Policy: Default Policy
  - Application Policy: No AppControl
  - Schedule: Always
  - QoS Band (Fwd): (Dropdown menu)
  - VoIP (ID 2): (Dropdown menu)
  - QoS Band (Reply): (Dropdown menu)
  - Like-Fwd: (Dropdown menu)
- Connection Method:** No SNAT

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

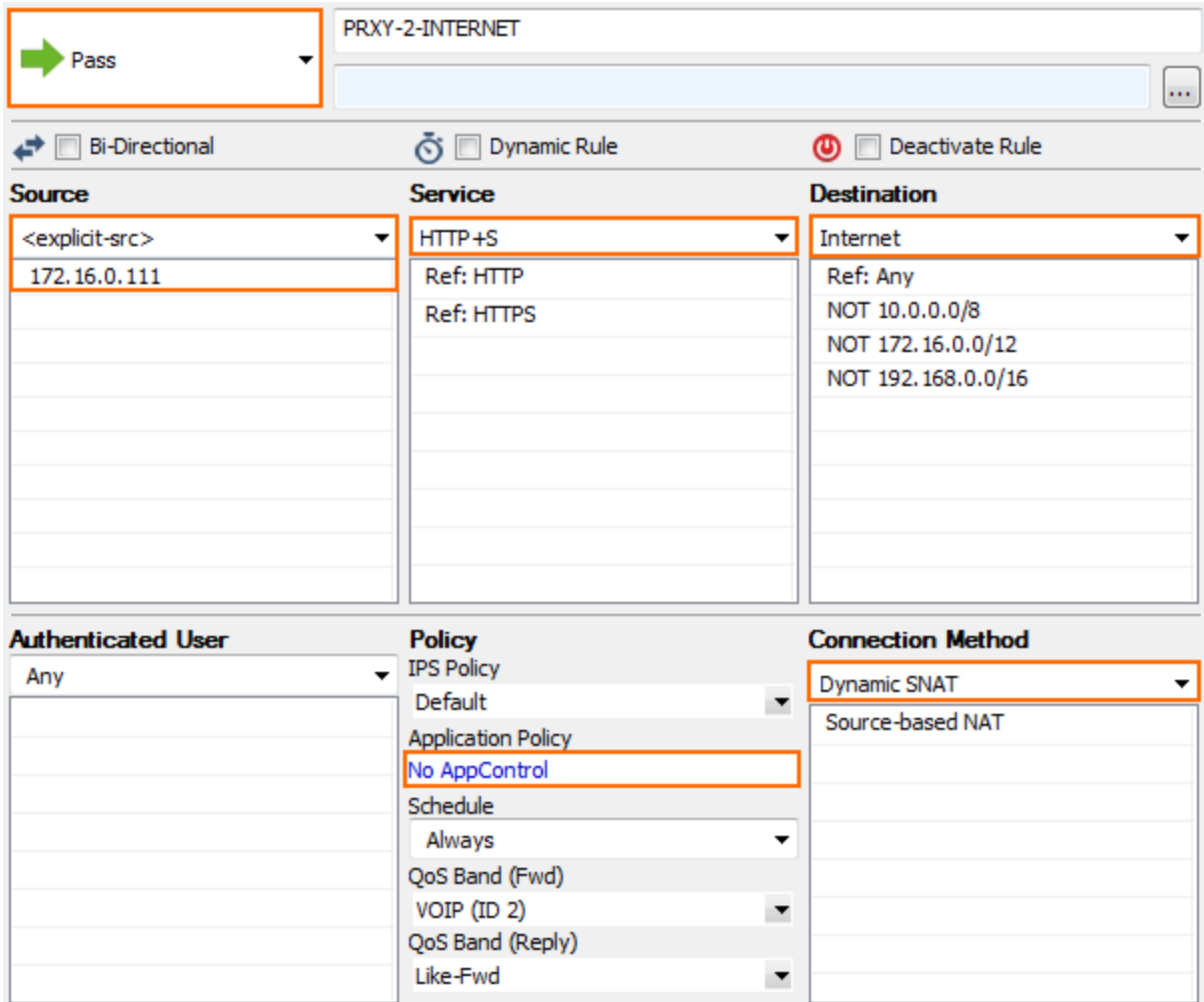
<b>Views</b> 		
Rule		
<b>Advanced</b>		
ICMP Handling		
<b>Object Viewer</b> 		
<input checked="" type="checkbox"/> Object Viewer		
	Own Log File	No
	Service Statistics	No
	Eventing	None
	Application Log Policy	Default
	<b>Miscellaneous</b>	
	Authentication	No Inline Authentication
	IP Counting Policy	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
	<b>Transparent Redirect</b>	<b>Enable</b>

- Click **OK**.
- 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.
- Click **Send Changes** and **Activate**.

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

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual servers > Firewall > Forwarding Rules**.
- Click **Lock**.
- 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**.
  - Application Policy** – Disable **Application Control**.



PRXY-2-INTERNET

Pass

Bi-Directional Dynamic Rule Deactivate Rule

Source	Service	Destination
<explicit-src> 172.16.0.111	HTTP+S Ref: HTTP Ref: HTTPS	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

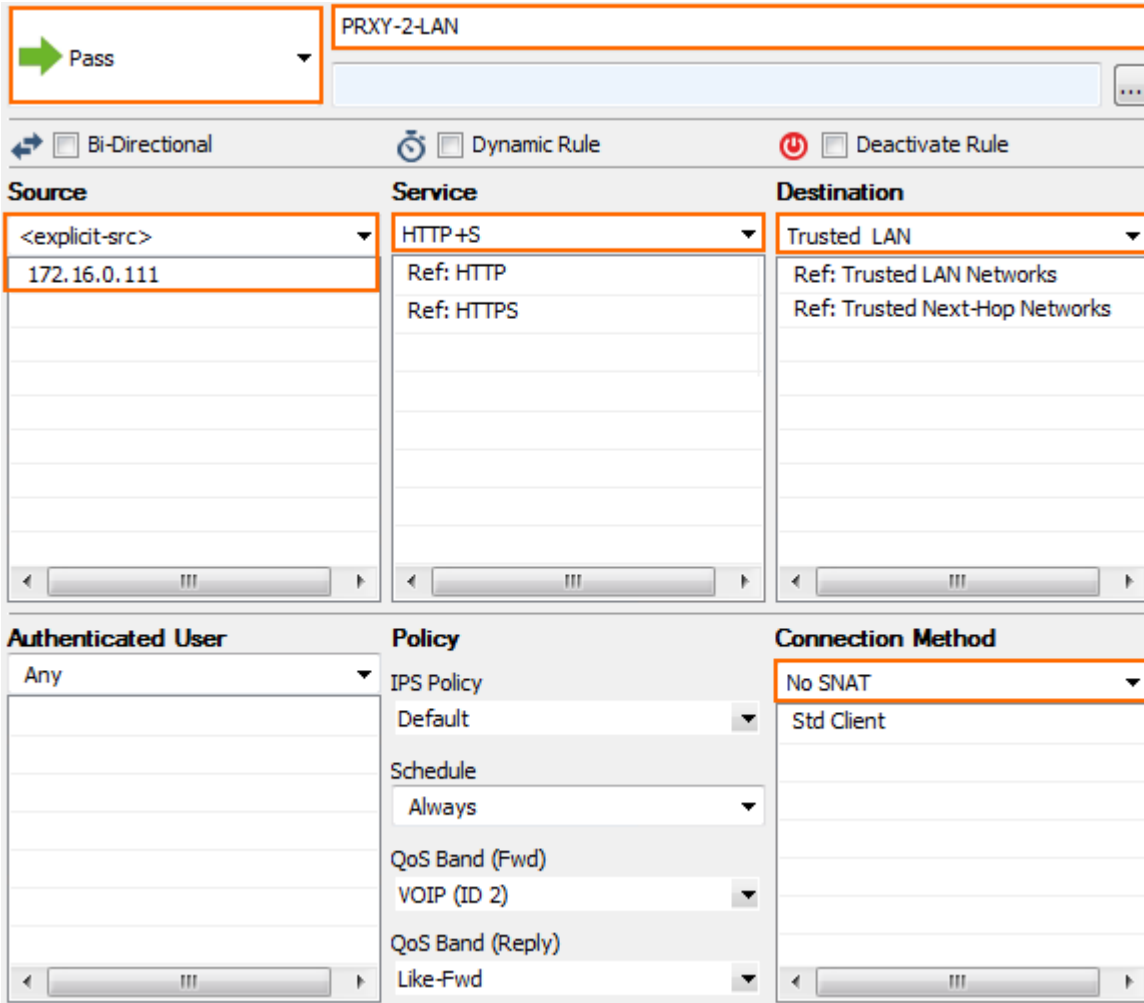
Authenticated User	Policy	Connection Method
Any	IPS Policy Default Application Policy No AppControl Schedule Always QoS Band (Fwd) VOIP (ID 2) QoS Band (Reply) Like-Fwd	Dynamic SNAT Source-based NAT

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

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**.
- **Application Policy** – Disable **Application Control**.



The screenshot shows the configuration for a rule named "PRXY-2-LAN". The rule is set to "Pass" and is not Bi-Directional, Dynamic, or Deactivated. The configuration is as follows:

Source	Service	Destination	Authenticated User	Policy	Connection Method
<explicit-src> 172.16.0.111	HTTP+S Ref: HTTP Ref: HTTPS	Trusted LAN Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks	Any	IPS Policy Default Schedule Always QoS Band (Fwd) VOIP (ID 2) QoS Band (Reply) Like-Fwd	No SNAT Std Client

#### Step 4. Configure the Proxy

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

- Route to the Internet using the F-Series Firewall as the gateway.
- Route to the internal client network using the F-Series 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.

## Figures

1. transparent\_redirect\_rules.png
2. transparent\_redirect\_00.png
3. transparent\_redirect\_01.png
4. transparent\_redirect\_02.png
5. transparent\_redirect\_03.png

© Barracuda Networks Inc., 2020 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.