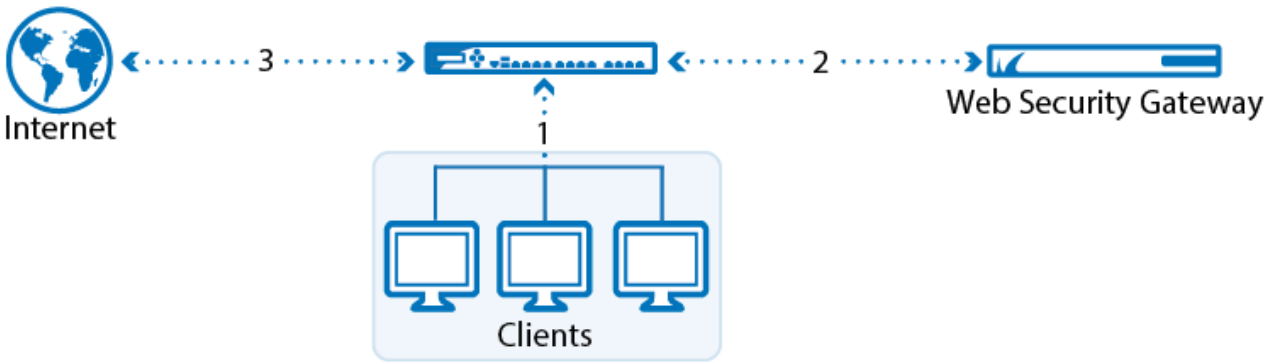
How to Configure a Transparent Redirect

https://campus.barracuda.com/doc/48202776/

To transparently forward connections to a Barracuda Web Security Gateway located in a DMZ behind a NextGen F-Series 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 Barracuda Web Security Gateway to apply filtering policies and create meaningful statistics as if it were directly connected to the client.

> The Web Security Gateway described here can be replaced by any appliance processing traffic that requires the original source and destination IP addresses to remain unmodified.



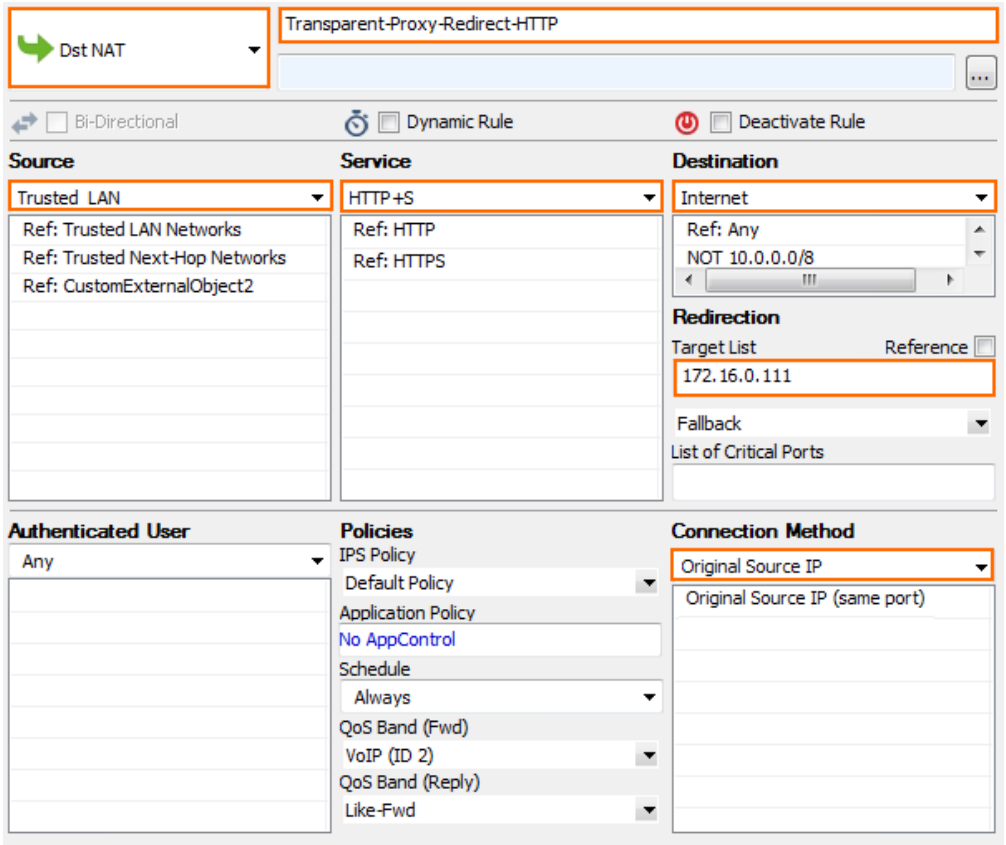
Before you begin

- 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).
- (optional) Enable SSL Inspection in the firewall. For more information, see How to Configure SSL Interception in the Firewall.
- The Web Security Gateway must be running firmware version 10.0.0 or higher and use Transparent SSL Inspection.

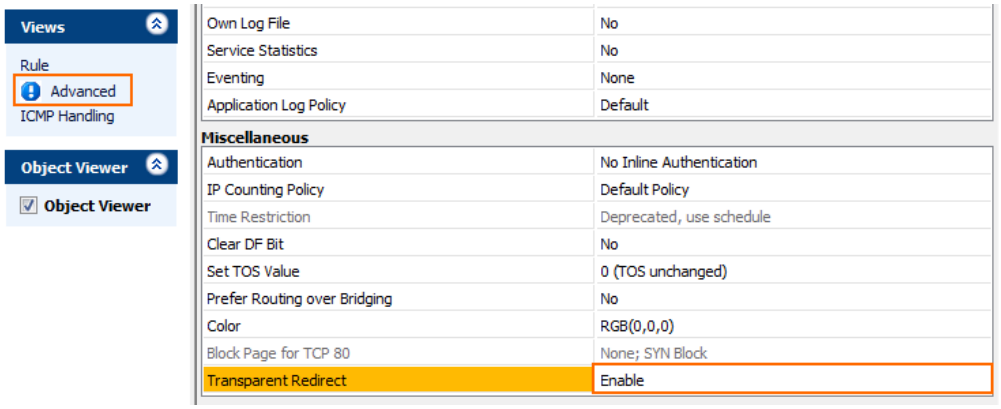
Step 1. Create a transparent redirect Dst NAT access rule

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual servers* > 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 Web Security Gateway 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 Web Security Gateway.



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

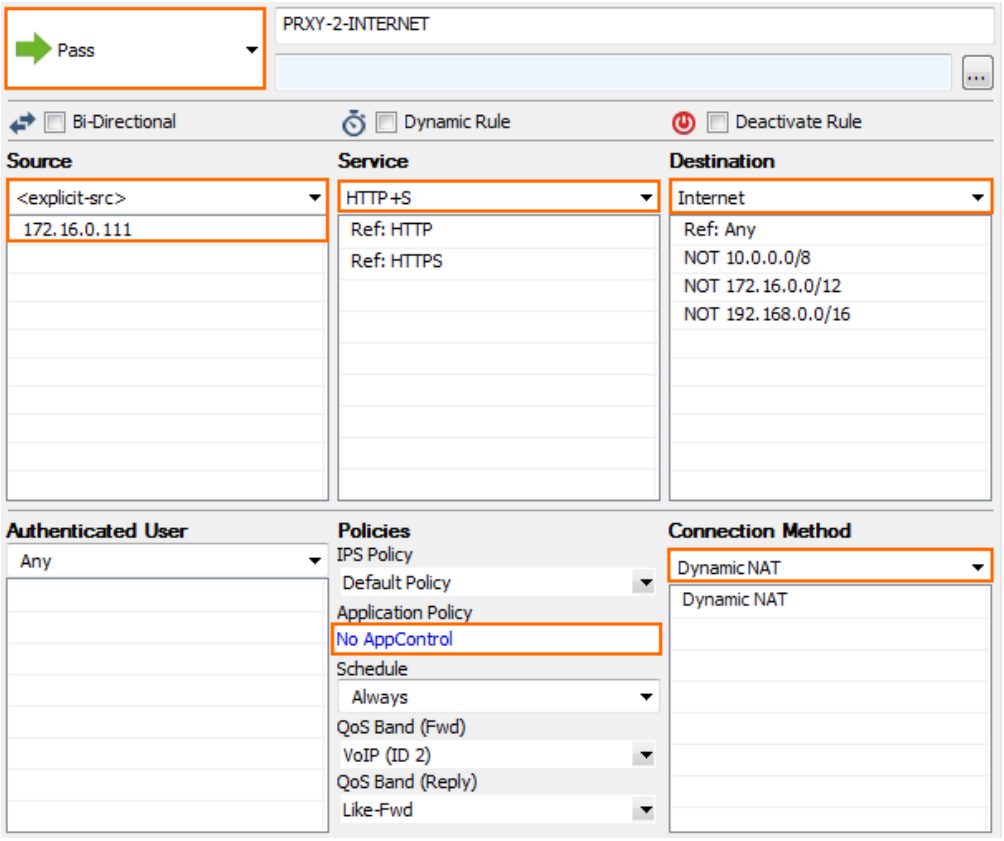


6. Click **OK**.
7. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

   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 > 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 NAT**.
   - **(optional) Application Policy** – Select Application Control policies.

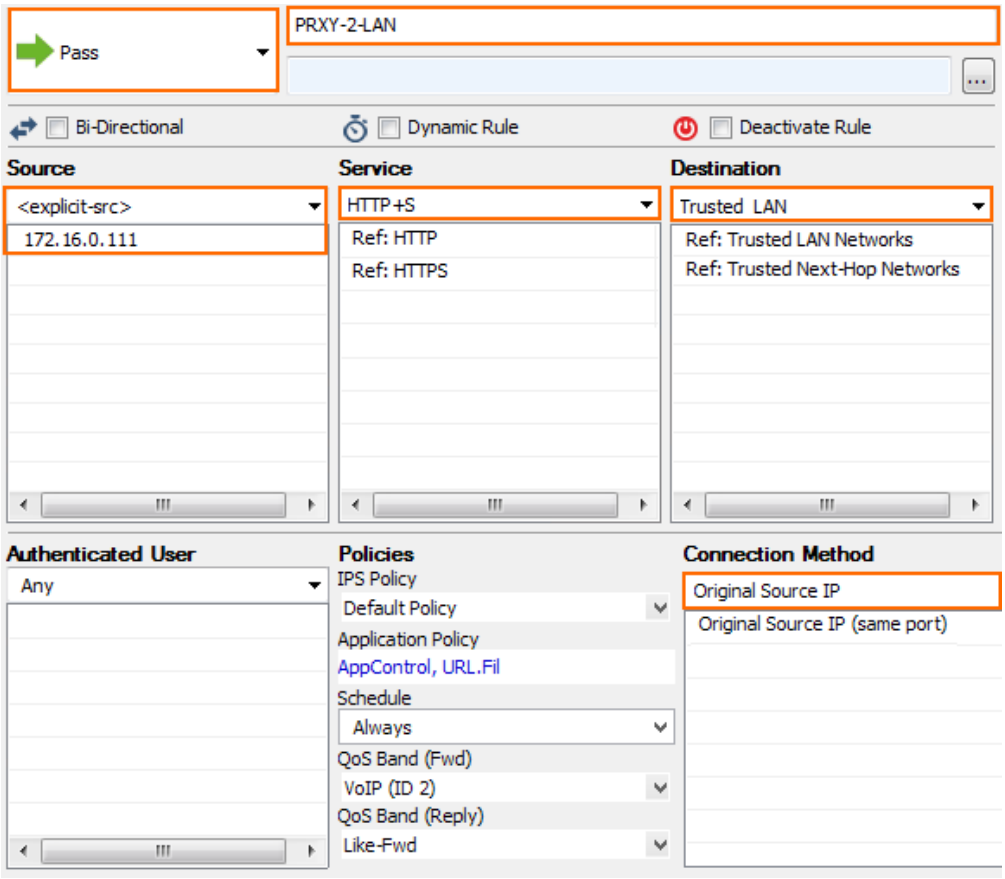


4. In the left menu, click **Advanced**.
5. In the **Dynamic Interface Handling** section, set **Source Interface** to **Any**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Create a pass access rule for the HTTP proxy to access the client 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 Web Security Gateway .
- **Destination** – Select **Trusted Networks**.
- **Service** – Select **HTTP+S**.
- **Connection Method** – Select **Original Source IP**.
- **(optional) Application Policy** – Select Application Control policies.



Step 4. Configure the Web Security Gateway

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 Web Security Gateway as the source IP address for outgoing connections.
- The Web Security Gateway must accept the HTTP and HTTPS connections on the same port as the firewall.

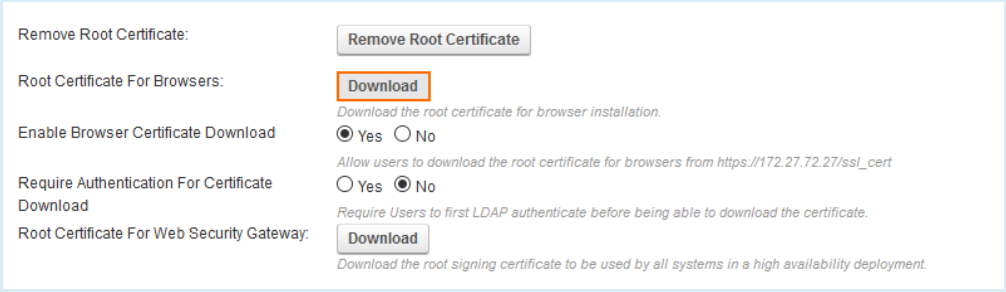
For more information, see How to Configure a Transparent Redirection from a Barracuda NextGen Firewall F-Series.

Step 5. Import the Web Security Gateway's root certificate

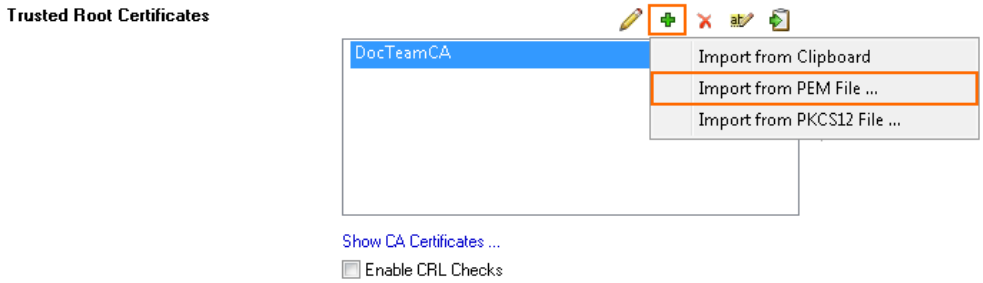
If you are running SSL Inspection on the NextGen Firewall, you must add the root certificate used for SSL Inspection on the Web Security Gateway to the **Trusted Root Certificates**

Download the root certificate on the Web Security Gateway

On the Web Security Gateway, go to **ADVANCED > SSL Inspection** and **Download** the **Root Certificate for Browsers**. You now have the **webfilter.barracuda.pem** file containing the root certificate on the client running NextGen Admin.

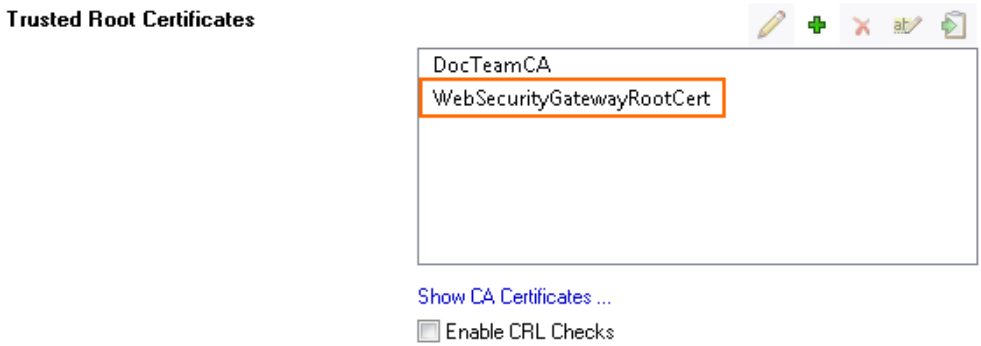


1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual servers* > Firewall > Security Policy Settings**.
2. Click **Lock**.
3. Click **+** in the **Trusted Root Certificates** list and select **Import from PEM File**. A file dialog opens.



4. Select the file containing the root certificate you previously exported from the Web Security Gateway.
5. Enter a **Name**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

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



Next Steps

Import the root certificates from the NextGen Firewall and the Web Security Gateway on the clients to avoid SSL certificate errors.

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
6. wsg_download_root_cert.png
7. import_root_cert_01.png
8. import_root_cert_02.png