Example - How to Enable Remote Management Access From the Internet

https://campus.barracuda.com/doc/46209020/

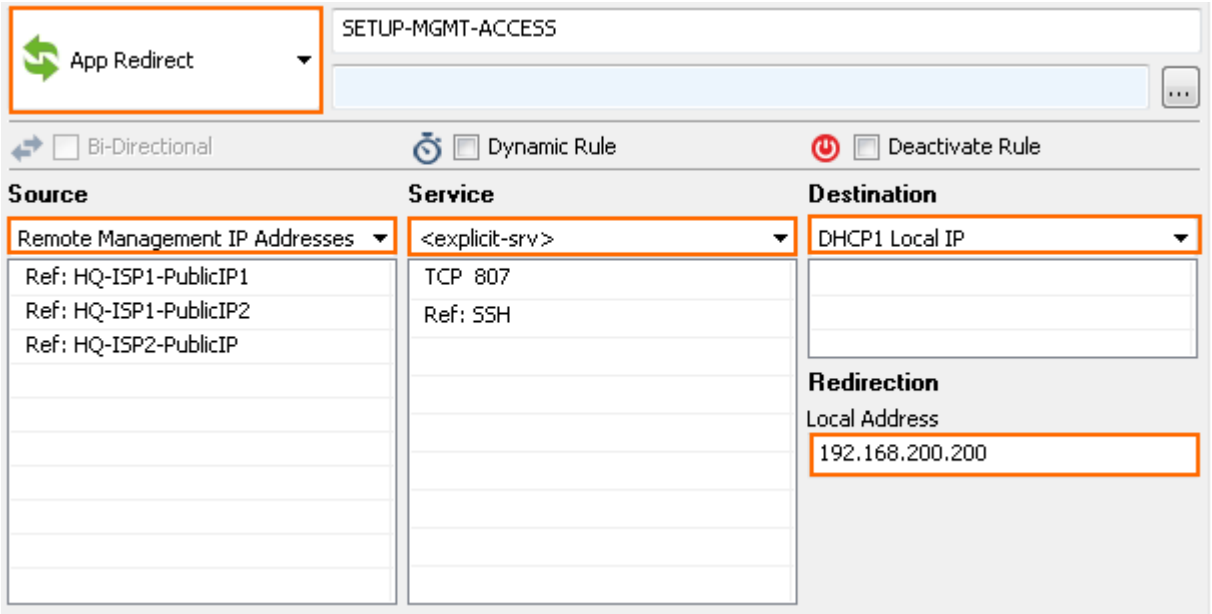
Barracuda Networks recommends that you only enable management access from the Internet for a limited period of time. Remote management access constitutes a significant security risk, especially if you allow access via SSH. To minimize risk potential, restrict access to very few trusted source addresses or networks, disable access when it is not needed, and use strong passwords or key authentication.

When you place a stand-alone F-Series Firewall at a remote site, you can enable access to it over the Internet for remote management and configuration. You can also enable remote access for Barracuda Networks Technical Support if direct access to the system is required for troubleshooting.

Create an App Redirect Access Rule

Create an App Redirect Rule for NextGen Admin SpoE (TCP 807) and optionally SSH to the internal management IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. From the **Rule Lists** menu in the left menu, select **Access Rules** .
3. Click **Lock**.
4. Create an **App Redirect** rule with the following settings:
   - **Source** – Select a network object containing the public IP addresses from which management access is allowed.
   - **Service** – Select **Explicit** and create a service for **TCP 807** and optionally add **SSH** for secure shell access.
   - **Destination** – If the firewall connects to the Internet via a dynamic address, select the network object to match your connection (**DHCP Local IP, DSL Local IP or 3G Local IP**). If the system uses a static public IP address, enter the static IP address.
   - **Redirection** – In the **Local Address** field, enter your internal management IP address (MIP) as defined in the network settings.



5. Place the rule so that it matches incoming traffic for TCP807 and SSH for the source IP addresses.
6. Click **Send Changes** and **Activate**.

Next Step

You can now connect via NextGen Admin to the public IP address of your firewall, as long as you are using one of the IP addresses listed as the **Source**.

Figures

1. RemoteManagementFWRule01.png