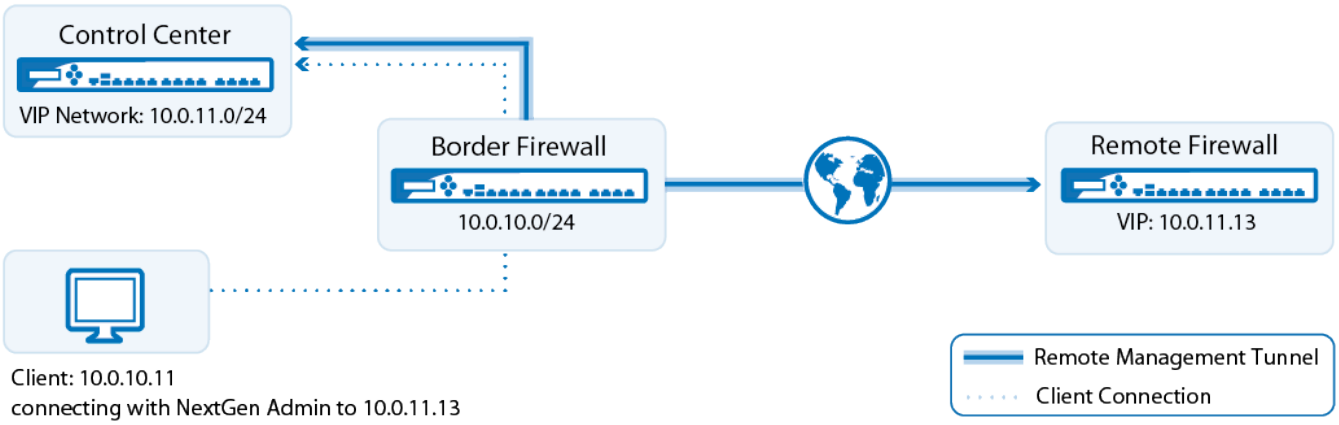
How to Configure a Remote Management Tunnel for an F-Series Firewall

https://campus.barracuda.com/doc/46208946/

If the managed NextGen Firewall F-Series cannot directly reach the NextGen Control Center, it must connect via a remote management tunnel. The remote NextGen Firewall F-Series uses the certificate keys exchanged at deployment to authenticate to the Control Center. Since it is not recommended to use an external IP address as a management IP the remote NextGen Firewall F-Series is assigned a Virtual IP (VIP) in the local network. The VIP is used to connect to the remote NextGen Firewall F-Series from the local network. Depending on whether the VIP is a subnet of the local network, or a separate network access rule and route entries on the border firewall and a access rule on the CC firewall are needed.



In this article:

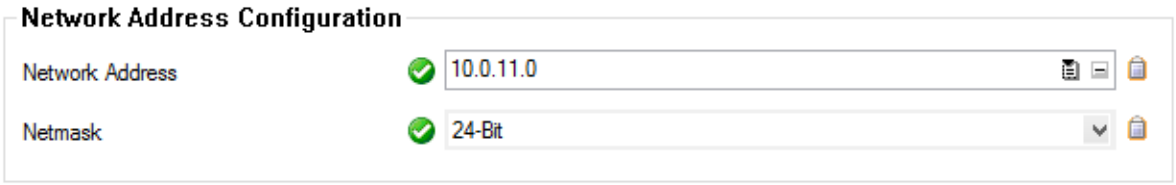
Before you Begin

- Use an available network or subnet to be used for the VIP addresses
- You need the external IP address of the border firewall.
- Firewalls in a HA cluster must have the public IP address configured on box level.

Step 1. Configure a VIP Network on the Control Center

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Box VIP Network Ranges**.

2. In the left menu, select **VIP Networks**.
3. Click **Lock**.
4. In the **VIP Networks** table, add an entry for the network range. Configure the following settings for the entry:
   - **Name** – A name for the network range.
   - **Network Address** – Enter the VIP Network network address. E.g., 10.0.11.0
   - **Netmask** – Select the netmask. E.g., 24-Bit



5. (optional) In the left menu, click **VPN Settings**.
6. (optional) The VPN Settings are set to sensible default values. If necessary you can change these settings:
   - **Pending Session Limitation** – Only five F-Series Firewalls are allowed to initiate management tunnels at the same time. Connection attempts exceeding the limit are blocked. This features makes sure that the Control Center is not overloaded due to too many management tunnel requests.
   - **Use Tunnels for Authentication (rarely used) –** Registers the tunnel network and credentials so that all traffic going through the management tunnel is treated as traffic from an authenticated user. You can use this criteria to create access rules in the CC firewall. To improve startup speed, disable this feature. You can see these virtual management tunnel users on the box level of the Control Center in **FIREWALL > Users**.
   - **Prebuild Cookies on Startup –** Prebuilds cookies when the VPN service is started. This might slow the VPN service startup but increases the speed of tunnel builds.
     This setting also prevents high system loads on firewalls with a large number of VPN tunnels. High system load caused by the VPN service can occur, if a large number of VPN tunnels are established simultaneously after an unit reboot or ISP outage.
7. (optional) In the left menu click on **Rekey/Alive Rates**. The rekey/alive rates are set to sensible default values. If necessary you can change these settings:
   - **Server enforces Limits** – Specifies that the VPN service of the Barracuda NextGen Control Center enforces the key limits. If disabled, the Barracuda NextGen Firewall F-Series enforces the limits.
   - **Key Time Limit [Minutes]** – The rekey period.
   - **Key Byte Limit [Mbytes]** – The rekey period after specified amount of Mbytes.
   - **Tunnel Probing [Seconds]** – The interval in which keepalive packets sent to the remote tunnel end. the
   - **Tunnel Timeout [Seconds]** – The length of time after which a tunnel is considered down if an answer has not been received by the vpnc process.

     Enter a smaller value for the **Tunnel Timeout** than the **Tunnel Probing** value.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 2. Configuration of the Managed NextGen Firewall F-Series

Step 2.1. Make the External IP Address Available on the Box Layer

One external IP address must be available on the box layer of the remote NextGen Firewall F-Series to ensure that the management tunnel can be initiated even if the virtual server hosted on the firewall is down. If you are using dynamic Internet connection, skip this step.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your managed NextGen Firewall F-Series* > Network**.
2. In the left menu, select **IP Configuration**.
3. Click **Lock**.
4. Click **+** in the **Additional Local IPs** section. The **IP Address Configuration** window opens.
5. Configure the additional local IP address:
   - **Interface** – Select the interface for the Internet connection
   - **IP Address** – Enter the external IP address for the managed NextGen Firewall F-Series.
   - **Responds to Ping** – Select **Yes**.
     Default Gateway – Enter the default gateway supplied by your ISP.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 2.2. Remote Management Tunnel Settings

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your managed NextGen Firewall F-Series* > Network**.
2. In the left menu, select **Management Access**.
3. Click **Lock**.
4. Set **Enable Tunnel** to **yes**.
5. Enter a free **Virtual IP (VIP)** for the managed NextGen Firewall F-Series.
6. Click the **Tunnel Details Edit** button. The **Tunnel Details** window opens.
7. Enter all IP addresses that need to be reached through the management tunnel to the **Remote Networks** table. Typically this would be:
   - **NextGen Control Center IP Address**
   - **NextGen Control Center box layer IP Address**
   - **Authentication Servers** IP addresses – E.g, the Active Directory server(s).
   - **External NTP servers**
8. Enter the external IP address of the border firewall in the **VPN Point of Entry** list. You can define multiple points of entry if your border firewall is using multiple ISPs. E.g., `62.99.0.40`
9. (optional) If needed you can change the advanced settings for the management tunnel. Some settings are only available in advanced configuration mode. Expand the **Configuration Mode** menu in the left menu and click **Switch to Advanced**.

Management Tunnel Configuration

Setting	Description
Remote Networks	In this table, add the IP addresses of all management workstations that access the firewall, as well as all required external authentication servers like MSAD.
VPN Server Key	Click this button to import the public RSA key of the VPN service the tunnel client will connect to.
VPN Server	In this field, add the IP address of the tunnel the client will connect to (usually the server IP address of the system that is running the VPN service).
VPN Port	In this field, specify the VPN port.
Outbound Proxy	If the system must go through an intermittent proxy server when connecting to the target server, select the proxy server type: ∘ To use the proxy that has been configured on the **Administrative Settings** page, select **Like-System-Settings**. ∘ If you select **HTTPS** or **SOCKS4/5**, you must also specify a proxy address and port. ∘ If you select **HTTPS**, the username and password are optional.
Transport Protocol	Select **TCP** or **UDP** for VPN transports.
Encryption Cipher	Select **AES, AES-256, CAST, Blowfish, DES,** or **3DES**.
VPN Outbound IP	The IP address for establishing the tunnel. If you do not specify an IP address, the IP address is chosen according to the current routing configuration.
Proxy Server IP	If the management setup provides a proxy server, specify its IP address.
Proxy Server Port	If the management setup provides a proxy server, specify its server port.
Proxy User	If you are using HTTPS, enter the username for proxy server authentication.
Proxy Password	If you are using HTTPS, set the password for proxy server authentication.

Connection Monitoring

Setting	Description
Reachable IPs	Add the IP addresses of hosts that should be reachable through the tunnel.
No. of ICMP Probes	The number of ICMP echo packages that are sent via the VPN tunnel (default: *2*).

Waiting Period [s/probe]	The number of seconds per probe to wait for an answer (e.g. *probes=3* and *waiting period=2* results in 3x2 s waiting time; default: *1*).
Run Probe Every [s]	The i nterval in seconds that ICMP probes are run (default: *15*).
Failure Standoff [s]	If no connection is possible, time in seconds to wait before a retry (default: *45*).
Alarm Period [s]	The time in seconds after an unsuccessful connection attempt before an alarm is set off (default: *120*).

Rekey/Alive Rates

Setting	Description
Key Time Limit [Minutes]	Specifies the interval in which tunnel keys are regenerated. Note, that specifying low values causes higher system load.
Tunnel Probing [Sec]	The interval in which keep alive packets are sent to the remote tunnel end.
Tunnel Timeout [Sec]	The timeout after which the tunnel will be actively re-established after probing has failed.

Serial Console Settings

To edit the serial console settings, you must be in the advanced configuration mode. To access this mode, expand the **Configuration Mode** menu in the left navigation pane and then click **Switch to Advanced**.

Descriptions of the settings that you can configure in the **Connection Details** configuration window from the **Serial Console** section of the **Network - Management Access** page:

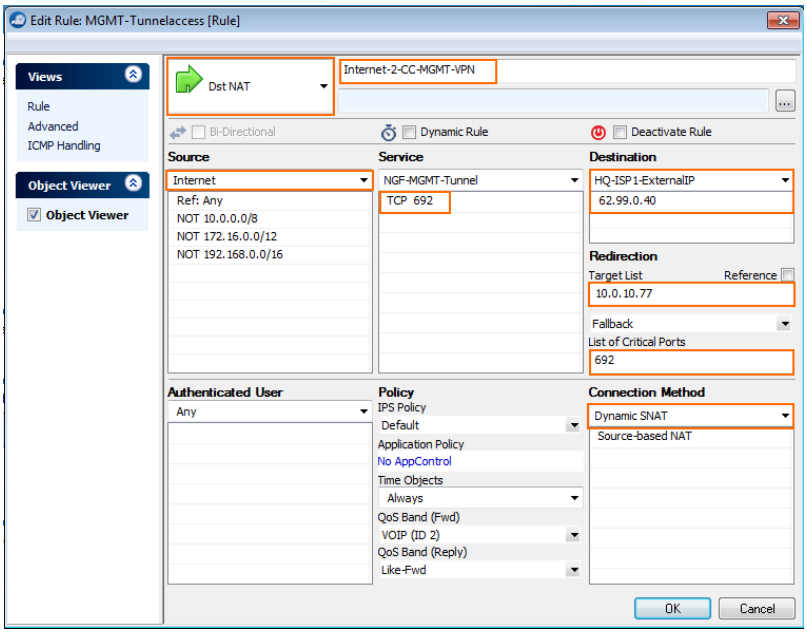
Setting	Description
PPP Remote IP	(**Advanced Configuration Mode**) Enter the IP address of the client when connecting via the serial IP address.
PPP Local IP	(**Advanced Configuration Mode**) Enter the IP address of the Barracuda NextGen Firewall F-Series. If this field is empty, the Box IP address is used.
Require PAP	(**Advanced Configuration Mode**) Specifies if the connecting client is required to authenticate itself to the Barracuda NextGen Firewall F-Series [possible users: root or support user].

10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 3. Create an DNAT Access Rule for the MGMT Tunnels on the Border NextGen Firewall F-Series

You must create a destination NAT access rule to forward the management tunnel traffic to the Control Center:

- **Action** – Select **Dst NAT**.
- **Source** – Select **Internet**.
- **Service** – Create and then select a service object to allow TCP traffic on port 692.
- **Destination** – Enter the VIP network or select a network object containing the VIP network.
- **Target List** – Enter the IP address of the Control Center. E.g., `10.0.10.77`
- **List of Critical Ports** – Enter **692**.
- **Connection** – Select **Dynamic SNAT**.



Step 4. Create and Deploy the PAR file to the remote NextGen Firewall F-Series

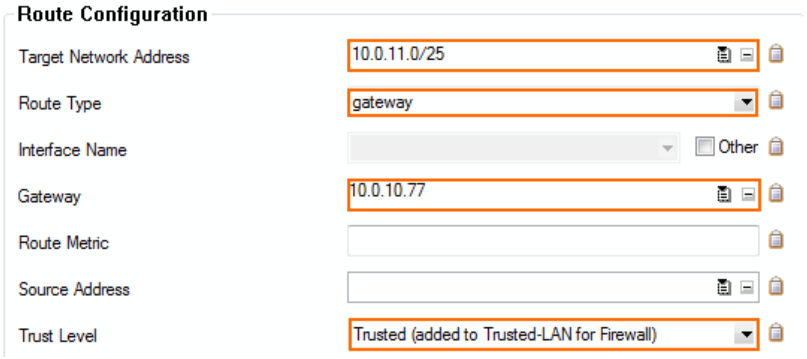
You must create a PAR file for the remote NextGen Firewall F-Series on the Control Center and then deploy the configuration.

Step 5. (optional) Create Access Rules and Routing Entries for separate VIP networks

You only need to complete these steps if you are using VIP addresses which are not part of your local network. You must have a CC firewall service running on the box level of your Control Center. For more information, see Control Center CC Firewall.

Step 5.1 Create a Routing Entry for the VIP Network on the Border Firewall

1. Open the **Network** page for your border firewall (**BOX > Network**).
2. In the left menu click **Routing**.
3. Click **Lock**.
4. Add a route for the VIP network:
   - **Target Network Address** – Enter the VIP network. E.g., `10.0.11.0./24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address of the Control Center E.g., `10.0.10.70`
   - **Trust Level** – Select **Trusted**.



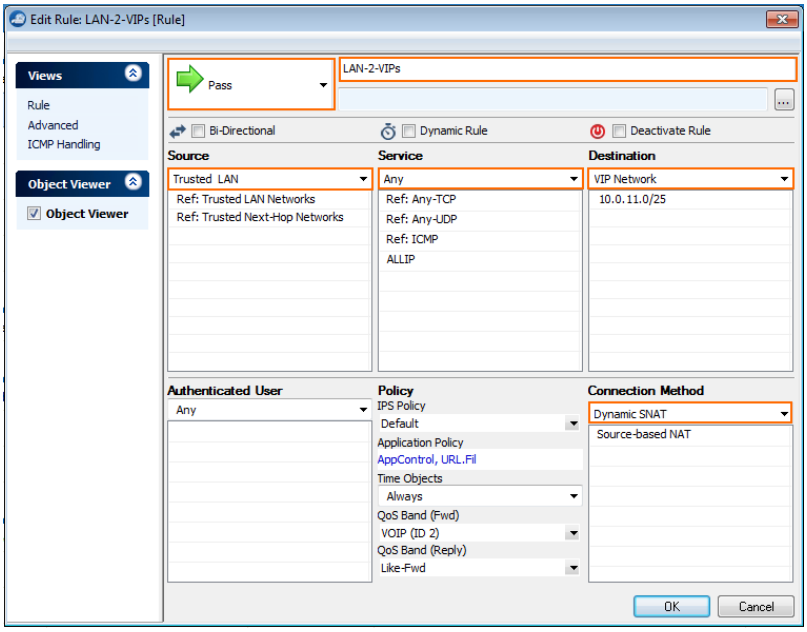
5. Click **OK.**
6. Click **Send Changes** and **Activate**.
7. Activate the network changes on the **Box** page (**CONTROL > Box**).

Step 5.2. Create a Access Rule to on the Border Firewall

To forward traffic from the local network through the remote management tunnel to the remote NextGen Firewall F-Series you must create a routing entry on the border firewall and a access rule permitting traffic from the local to the VIP network:

Create the following access rule on your border firewall.

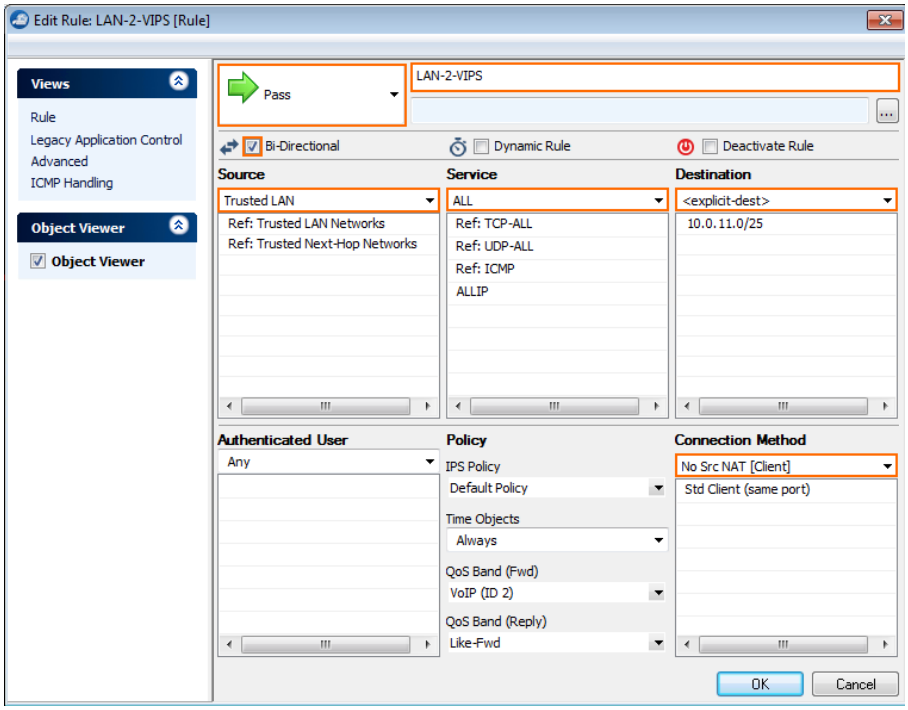
- **Action** – Select **PASS**
- **Source** – Select **Trusted LAN**
- **Service** – Select **Any**
- **Destination** – Enter the VIP network or select a network object containing the VIP network.
- **Connection** – Select **Dynamic SNAT**



Step 5.3. Create an Access Rule in the CC Firewall on the Control Center

You must be running the CC Firewall on the Control Center to create an access rule. For more information, see Control Center CC Firewall.

1. Log into the box layer of your Control Center.
2. Verify that you are running a **CC Firewall** service.
3. Go to **CONFIGURATION > Configuration Tree > Virtual Servers > S1 > Firewall > Forwarding Rules**.
4. Create an access rule with the following settings:
   - **Action** – Select **PASS**
   - **Source** – Select **Trusted Networks**
   - **Bidirectional** – Set the bidirectional checkbox.
   - **Service** – Select **Any**
   - **Destination** – Enter the VIP network or select a network object containing the VIP network.
   - **Connection** – Select **No Src NAT**



5. Click **OK.**
6. Click **Send Changes** and **Activate**.

Figures

1. cc_remote_mgmt_tunnel_01.png
2. cc_remote_mgmt_tunnel_02.png
3. MGMT_Tunnel_DNAT.png
4. MGMT_Tunnel_BorderFW_Route.png
5. MGMT_Tunnel_BorderFW_PASS.png
6. MGMT_Tunnel_CC_FW_PASS.png