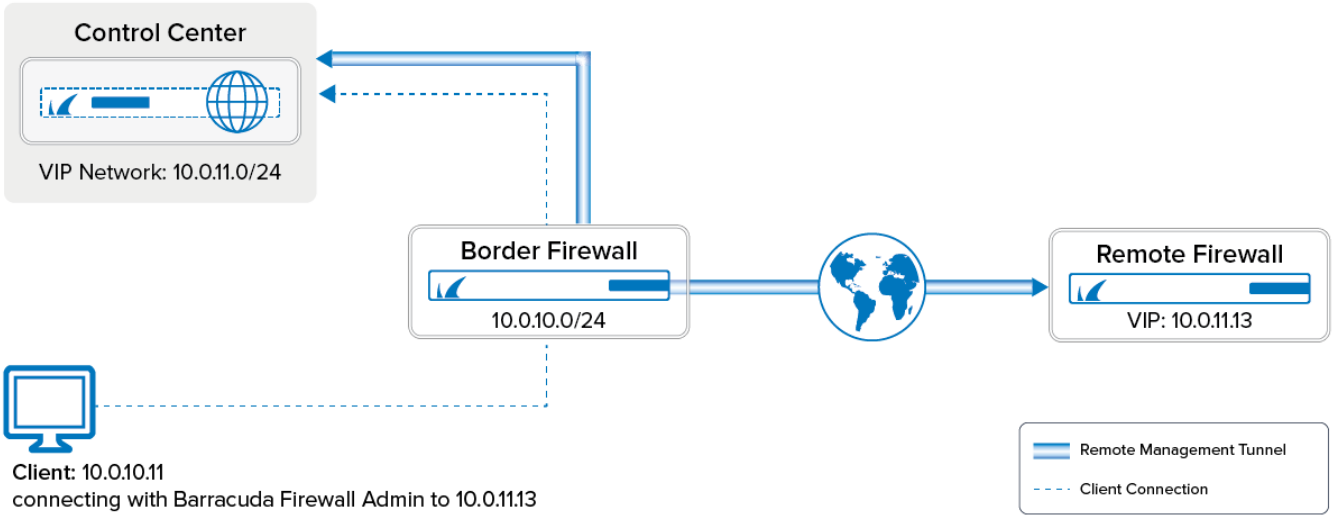
How to Configure a Remote Management Tunnel for a CloudGen Firewall

https://campus.barracuda.com/doc/100370262/

If the managed CloudGen Firewall cannot directly reach the Barracuda Firewall Control Center, it must connect via a remote management tunnel. The remote firewall 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 firewall is assigned a Virtual IP (VIP) in the local network. The VIP is used to connect to the remote firewall from the local network. Depending on whether the VIP is a subnet of the local network or a separate network, you will need access rule and route entries on the border firewall and an access rule on the CC firewall. If the remote firewall is using a IPv6 IP address to connect, the Control Center must have a global unicast IPv6 address.



Limitations

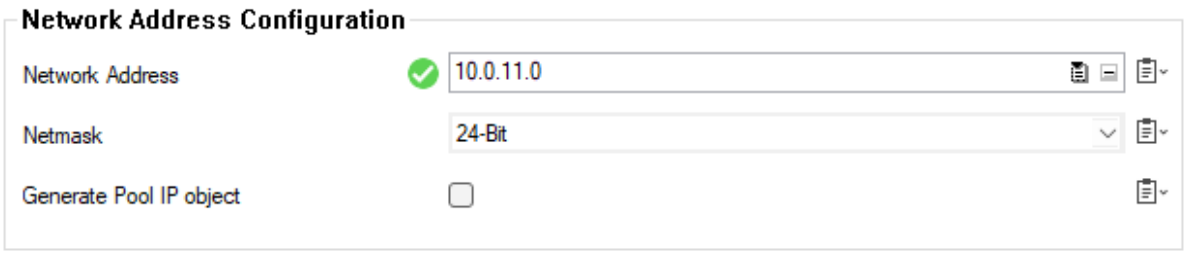
- Only IPv4 traffic can be sent through the management tunnel.

Before You Begin

- Use an available network or subnet to be used for the VIP addresses.
- (IPv4 only) You need the external IPv4 address of the border firewall.
- (IPv6 only) The Control Center must be reachable through an IPv6 global unicast address.
- 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 > VIP Networks**.
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 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 CloudGen 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 a 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 Control Center enforces the key limits. If disabled, the firewall 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.

- **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. The timeout starts after a keepalive packet is sent. Retransmissions are sent additionally within this period.

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 2. (IPv6 only) Add IPv6 Listeners to the CCVPN Service

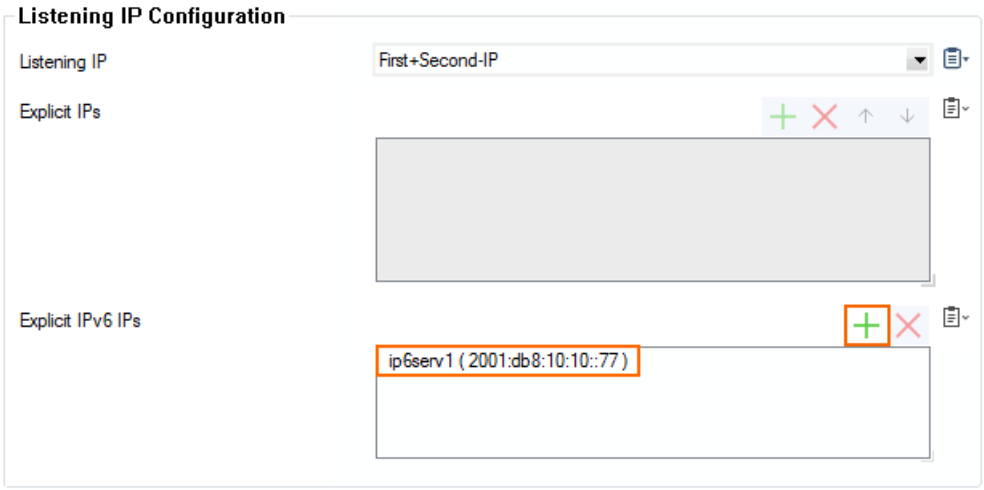
Per default the CC-VPN service only listens on IPv4 addresses. You must add the IPv6 addresses manually.

Step 2.1 Introduce the IPv6 Addresses

1. Log into the box level of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu, click **IP Configuration**.
5. Scroll down to **IP Version 6**.
6. Make sure, IPv6 is enabled.
7. In the **IPv6 Shared Networks and IPs** section, introduce the IPv6 network containing your IP addresses.
8. In the **Shared IPs in this Network** box, add the listening IPv6 addresses.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.
11. Go to **CONTROL > Box**.
12. In the **Network** section of the left menu, click **Activate new network configuration**. The **Network Activation** window opens.
13. Click **Failsafe**.

Step 2.2 Add the Addresses to the Service

1. Log into the box level of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > CCVPN > Service Properties**.
3. Click **Lock**.
4. Click **+** to add an IPv6 address to the **Explicit IPv6 IPs** to the list.
5. Double click the IPv6 in the list.



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

Step 3. Configuration of the Remote Firewall

Step 3.1. Make the External IP Address Available on the Box Layer

One external IP address must be available on the box layer of the remote firewall to ensure that the management tunnel can be initiated even if the services hosted on the firewall are down. If you are using IPv4 dynamic Internet connection, skip this step.

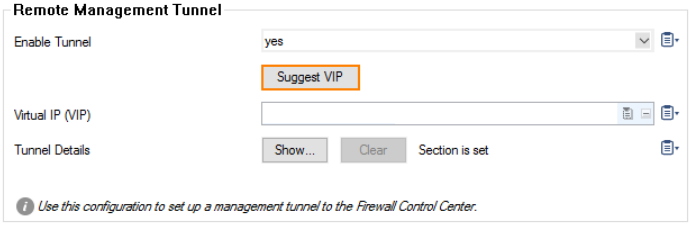
1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > your managed CloudGen Firewall > Network**.
2. In the left menu, select IP Configuration.
3. Click **Lock**.
4. Click **+** in the **Additional Local IPs** section. The **IP Address Configuration** window opens.
5. Configure the additional local IP address:
   - **Interface** – Select the interface for the Internet connection
   - **IP Address** – Enter the external IPv4 address for the managed firewall.
   - **Responds to Ping** – Select **Yes**.
   - **Default Gateway** – Enter the default gateway supplied by your ISP.
6. In the left menu, expand **Configuration Mode** and click **Switch to Advanced View**.
7. Click **+** in the **Additional IPv6 Addresses** section. The **Additional IPv6 Addresses** window opens.
8. Configure the additional local IPv6 address:
   - **Interface** – Select the interface for the Internet connection.
   - **IP Address** – Enter the external IPv6 address for the managed firewall.
   - **Associated Netmask** – Enter the netmask.
   - **Responds to Ping** – Select **Yes**.
9. Click **OK**.
10. In the left menu, click **Routing** and verify that a default IPv6 route exists. For more information,

see How to Configure IPv6 Gateway Routes.

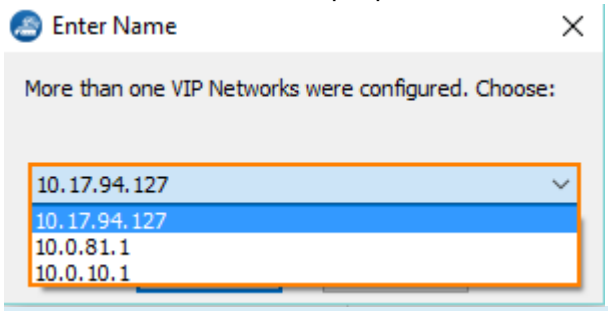
11. Click **Send Changes** and **Activate**.

Step 3.2. Remote Management Tunnel Settings

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your managed CloudGen Firewall* > Network** .
2. In the left menu, select **Management Access**.
3. Click **Lock**.
4. Set **Enable Tunnel** to **yes**.
5. To configure the **Virtual IP (VIP)** for the managed firewall, click on **Suggest VIP**.



6. For the selection of available VIP addresses, there are three options:
   1. In case no VIP network is defined on your CC, you will be informed that there are no valid VIP addresses available.
   2. In case there is only one VIP network configured in your CC, the system determines the next available VIP address based on the highest VIP already assigned in the configured VIP network. For example, if the highest VIP address already used is 10.0.80.12, you will be offered the VIP address 10.0.80.13.
   3. In case there are more than one VIP networks configured on your CC, each of these VIP networks will be checked for the availability of unused VIP addresses. The system will propose the next valid VIP address for each configured VIP network in a list. You must then select which of the proposed VIP addresses will fit your needs.



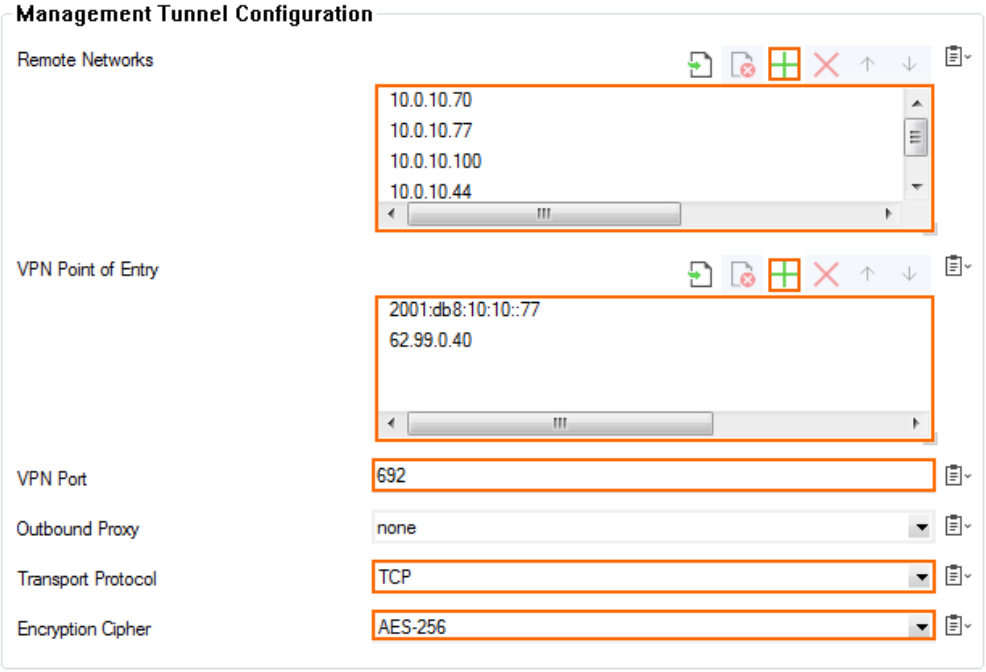
The net address x.x.x.0 and broadcast address x.x.x.255 will not be available as virtual IP addresses.

7. Click the **Tunnel Details Edit** button. The **Tunnel Details** window opens.
8. Enter all IP addresses that need to be reached through the management tunnel to the **Remote Networks** table. Typically this would be:
   - **Firewall Control Center IP Address**
   - **Firewall Control Center box layer IP Address**
   - **Authentication Servers** IP addresses – E.g, the Active Directory server(s).
   - **External NTP servers**
9. Enter the external IPv4 and IPv6 addresses 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`

> The **VPN Point of Entry** of your border firewall must be a static IP address. Otherwise, the remote firewall will not be able to connect through the border firewall to the Control Center.

10. (optional) Use the **up** and **down** arrow icons to sort the **VPN Point of Entry** addresses.
11. From the **Transport Protocol** list, select **TCP** or **UDP**. Default: **TCP**
12. From the **Encryption Cipher** list, select **AES-256**.



13. (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
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.
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 [m]	Specifies the interval in which tunnel keys are regenerated. Note that specifying low values causes higher system load.
Tunnel Probing [s]	The interval in which keepalive packets are sent to the remote tunnel end.

Tunnel Timeout [s]	The timeout after which the tunnel will be actively re-established after probing has failed.

Serial Console Settings (Advanced Configuration Mode)

Advanced Configuration Mode
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:

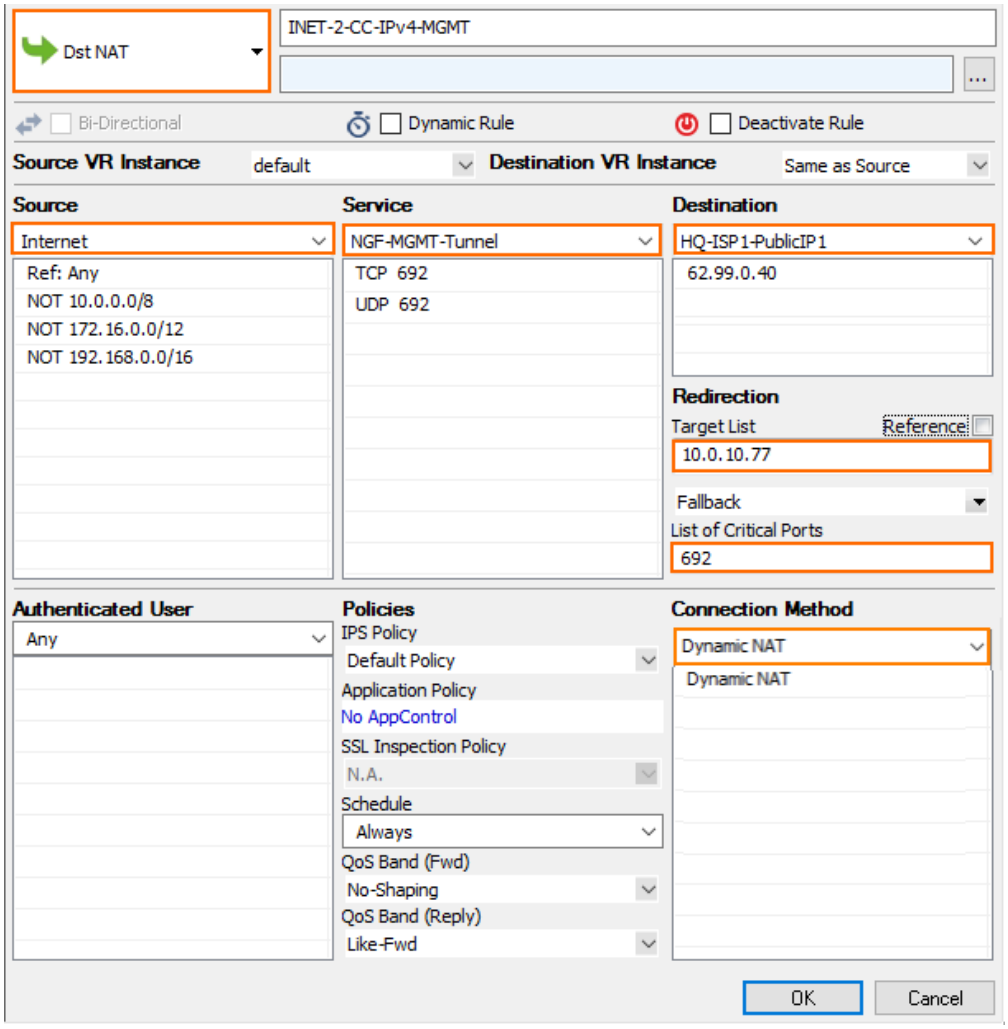
Setting	Description
PPP Remote IP	Enter the IP address of the client when connecting via the serial IP address.
PPP Local IP	Enter the IP address of the firewall. If this field is empty, the Box IP address is used.
Require PAP	Specifies if the connecting client is required to authenticate itself to the firewall [possible users: root or support user].

14. Click **OK**.
15. Click **Send Changes** and **Activate**.

Step 4. Create a Dst NAT Access Rule for IPv4 MGMT Tunnels on the Border Firewall

You must create a destination NAT access rule to forward the IPv4 management tunnel traffic to the Control Center:

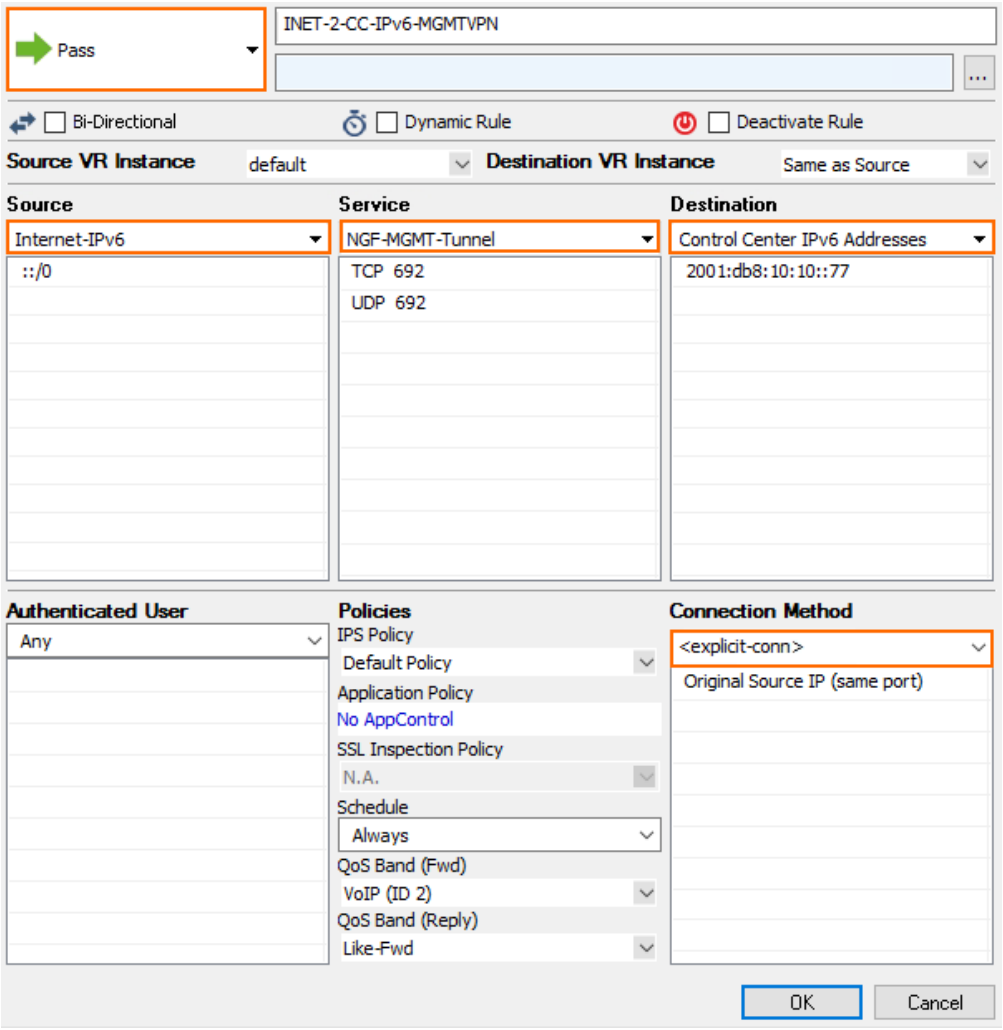
- **Action** – Select **Dst NAT**.
- **Source** – Select **Internet**.
- **Service** – Create and then select a service object to allow TCP traffic on port 692.
- **Destination** – Enter the IPv4 address configured as a **VPN Point of Entry** for the management tunnel. E.g., `62.99.0.40`
- **Target List** – Enter the IP address of the Control Center. E.g., `10.0.10.77`
- **List of Critical Ports** – Enter **692**.
- **Connection** – Select **Dynamic NAT**.



Step 5. Create a Pass Access Rule for IPv6 MGMT Tunnels on the Border Firewall

For the remote firewall to reach your Control Center via IPv6, you must allow TCP and UDP 692 connections from the external IP address of the firewall to your Control Center. Create the following IPv6 access rule:

- **Action** – Select **Pass**.
- **Source** – Select **Internet** or enter the public IPv6 address of the remote firewall.
- **Service** – Create and then select a service object to allow TCP and UDP traffic on port 692.
- **Destination** – Enter the IPv6 global unicast address of the Control Center. E.g., `2001:db8:10:10::77`



Step 6. Create and Deploy the PAR File to the Remote Firewall

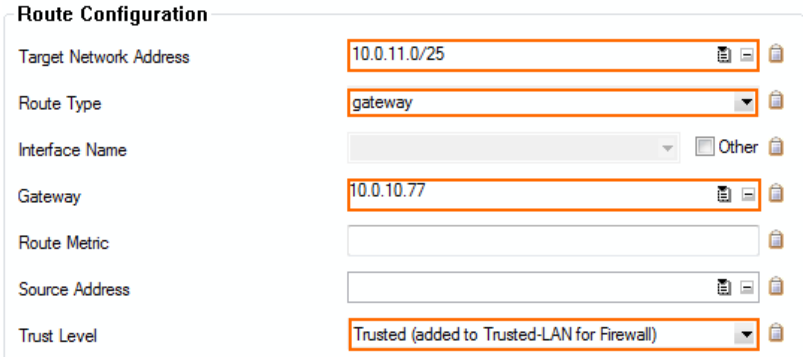
You must create a PAR file for the remote firewall on the Control Center and then deploy the configuration.

Step 7. (optional) Create Access Rules and Routing Entries for Separate VIP Networks

You only need to complete these steps if you are using VIP addresses that 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 7.1 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**.



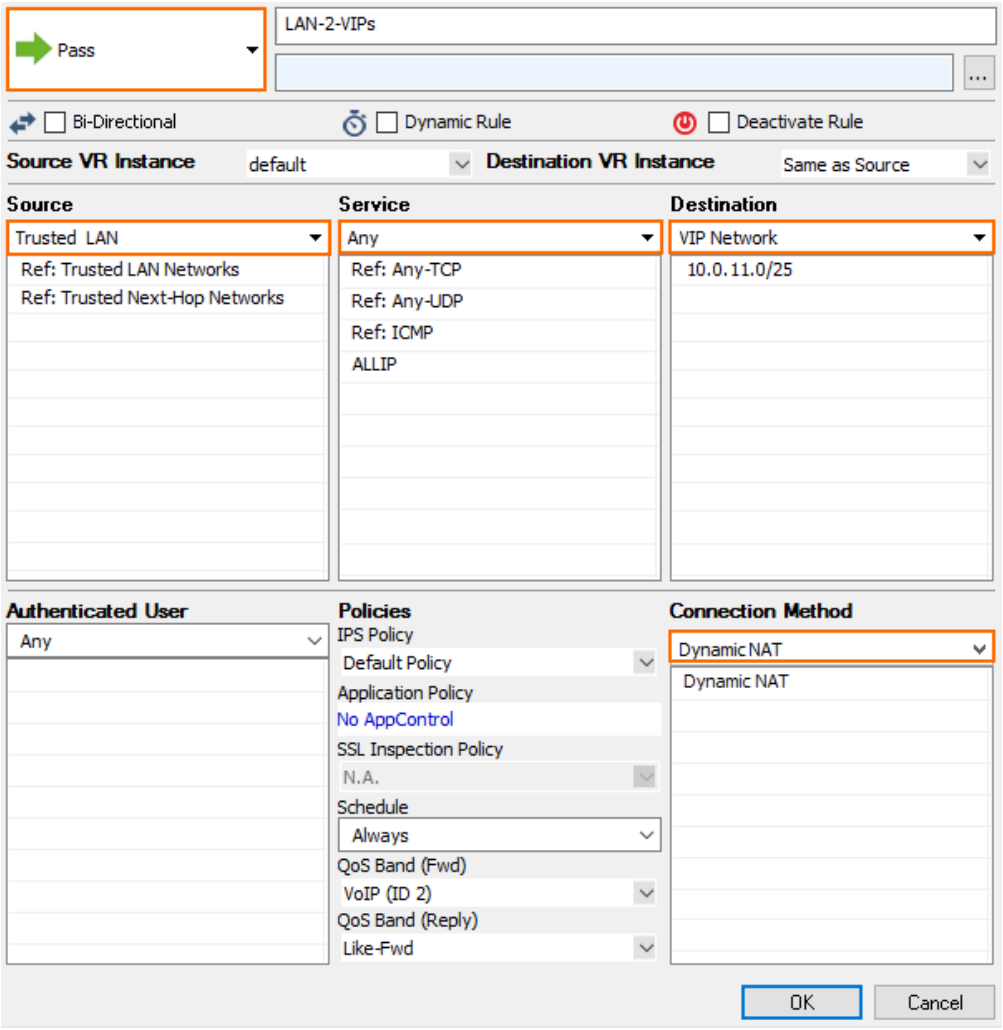
5. Click **OK**.
6. Click **Send Changes** and **Activate**.
7. Activate the network changes on the **Box** page (**CONTROL > Box**).

Step 7.2. Create an Access Rule to on the Border Firewall

To forward traffic from the local network through the remote management tunnel to the remote firewall, you must create a routing entry on the border firewall and an access rule permitting traffic from the local to the VIP network:

Create the following access rule on your border firewall.

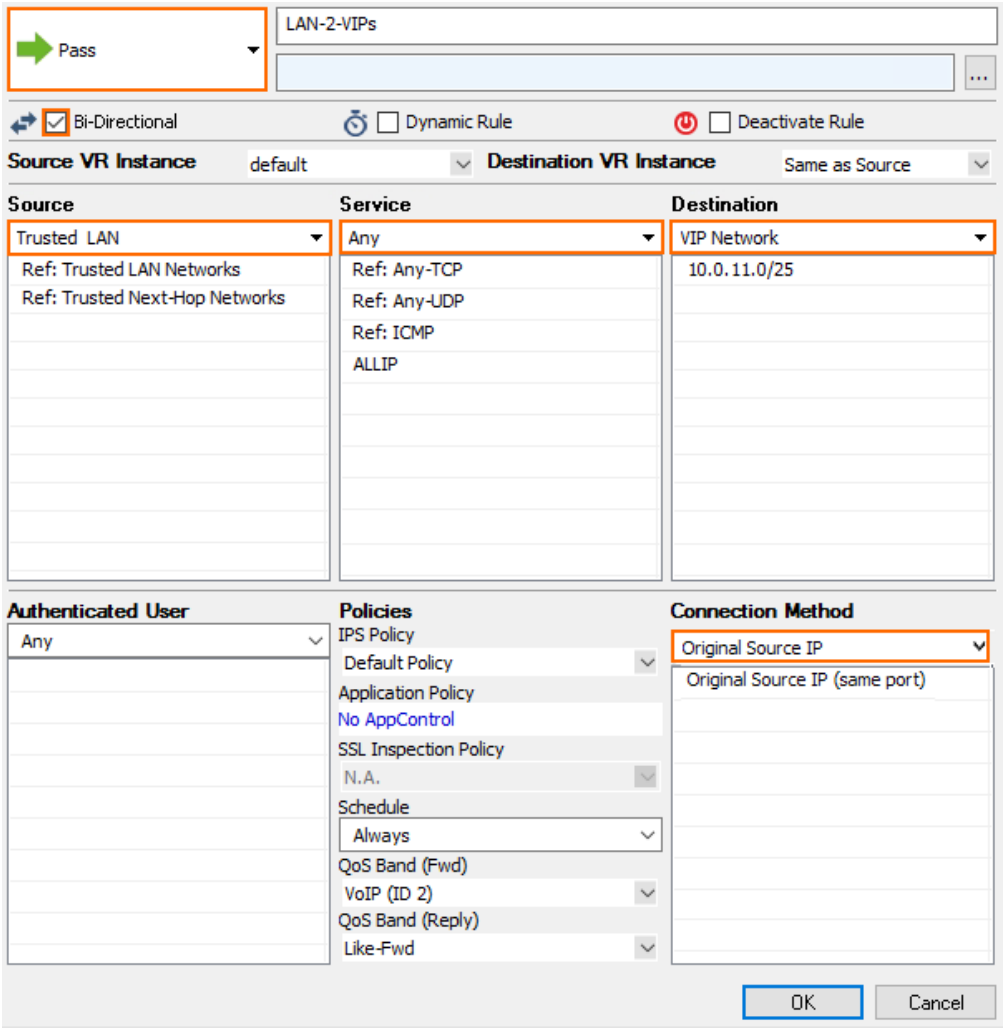
- **Action** – Select **PASS**.
- **Source** – Select **Trusted LAN**.
- **Service** – Select **Any**.
- **Destination** – Enter the VIP network or select a network object containing the VIP network.
- **Connection** – Select **Dynamic NAT**.



Step 7.3. Create an Access Rule in the CC Firewall on the Control Center

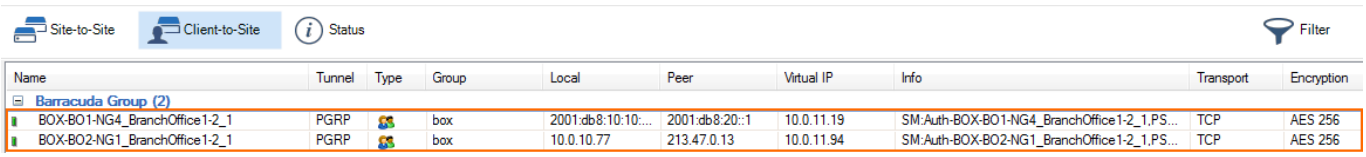
You must be running the CC Firewall on the Control Center to create an access rule. For more information, see Control Center CC Firewall.

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 > Assigned Cervices > 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 **Original Source IP**.



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

Log in to the box level of your Control Center and go to **VPN > Client-to-Site** to see the connected remote firewalls.



Figures

1. cc_remote_mgmt_tunnel01.png
2. cc_remote_mgmt_tunnel_02.png
3. ipv6_listener_ccvpn.png
4. suggest_vip.png
5. select_vip_network.png
6. mgmt_tunnel_network_settings.png
7. mgmt_tunnel_ipv4_rule_v.01.png
8. mgmt_tunnel_ipv6_rule.png
9. MGMT_Tunnel_BorderFW_Route.png
10. MGMT_Tunnel_BorderFW_PASS.png
11. MGMT_Tunnel_CC_FW_PASS.png
12. mgmt_tunnel_CC_VPN.png