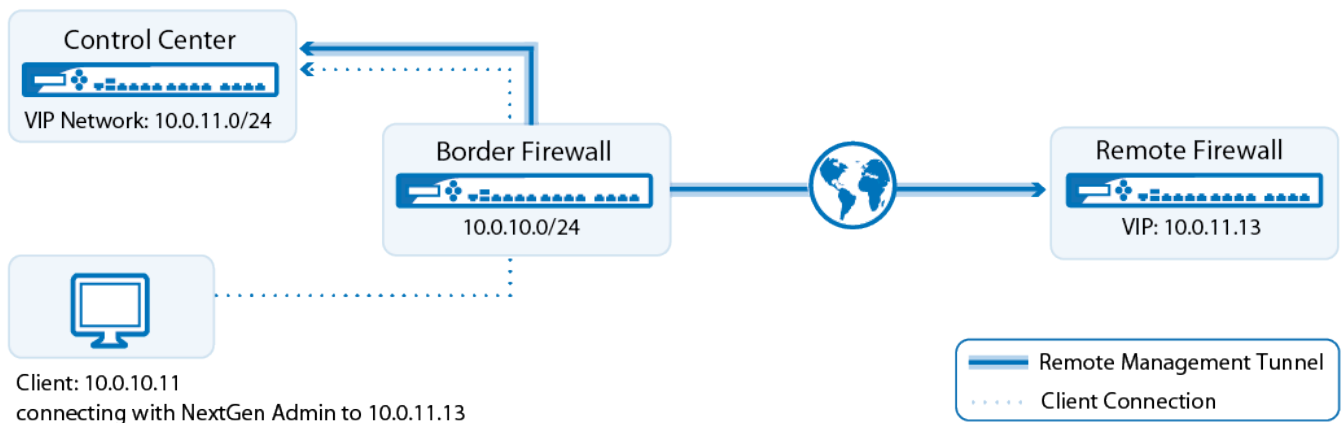


## How to Configure a Remote Management Tunnel for an F-Series Firewall

<https://campus.barracuda.com/doc/53248884/>

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 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

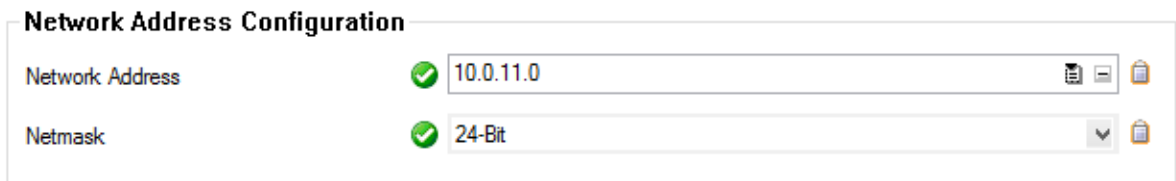
- Only IPv4 traffic can be sent through the management tunnel.

### 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 an 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 F-Series Firewalls are allowed to initiate management tunnels at the same time. Connection attempts exceeding the limit are blocked. This feature 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 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.
  - **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 CCVPN Service

Per default, the CC-VPN service only listens on the first and second IPv4 virtual server IP address. You must add the IPv6 addresses manually.

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



The screenshot shows the 'Service Properties' window for a CCVPN service. It has three main sections: 'Service Availability' with a dropdown set to 'First+Second-IP'; 'Explicit Service IPs' which is an empty list; and 'Explicit IPv6 Service IPs' which contains one entry, 'ip6serv1 (2001:db8:10:10::77)', highlighted with an orange border. Each section has a '+' icon to add items and a '-' icon to remove them.

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

**Management Tunnel Configuration**

Remote Networks

10.0.10.70  
10.0.10.77  
10.0.10.100  
10.0.10.44

VPN Point of Entry

2001:db8:10:10::77  
62.99.0.40

VPN Port

692

Outbound Proxy

none

Transport Protocol

TCP

Encryption Cipher

AES-256

12. (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
<b>VPN Server Key</b>	Click this button to import the public RSA key of the VPN service the tunnel client will connect to.
<b>VPN Server</b>	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).
<b>VPN Port</b>	In this field, specify the VPN port.
<b>Outbound Proxy</b>	<p>If the system must go through an intermittent proxy server when connecting to the target server, select the proxy server type:</p> <ul style="list-style-type: none"> <li>To use the proxy that has been configured on the <b>Administrative Settings</b> page, select <b>Like-System-Settings</b>.</li> <li>If you select <b>HTTPS</b> or <b>SOCKS4/5</b>, you must also specify a proxy address and port.</li> <li>If you select <b>HTTPS</b>, the username and password are optional.</li> </ul>
<b>VPN Outbound IP</b>	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.
<b>Proxy Server IP</b>	If the management setup provides a proxy server, specify its IP address.

<b>Proxy Server Port</b>	If the management setup provides a proxy server, specify its server port.
<b>Proxy User</b>	If you are using HTTPS, enter the username for proxy server authentication.
<b>Proxy Password</b>	If you are using HTTPS, set the password for proxy server authentication.

#### Connection Monitoring

Setting	Description
<b>Reachable IPs</b>	Add the IP addresses of hosts that should be reachable through the tunnel.
<b>No. of ICMP Probes</b>	The number of ICMP echo packages that are sent via the VPN tunnel (default: 2 ).
<b>Waiting Period [s/probe]</b>	The number of seconds per probe to wait for an answer (e.g. <i>probes=3</i> and <i>waiting period=2</i> results in 3x2 s waiting time; default: 1 ).
<b>Run Probe Every [s]</b>	The interval in seconds that ICMP probes are run (default: 15 ).
<b>Failure Standoff [s]</b>	If no connection is possible, time in seconds to wait before a retry (default: 45 ).
<b>Alarm Period [s]</b>	The time in seconds after an unsuccessful connection attempt before an alarm is set off (default: 120 ).

#### Rekey/Alive Rates

Setting	Description
<b>Key Time Limit [m]</b>	Specifies the interval in which tunnel keys are regenerated. Note that specifying low values causes higher system load.
<b>Tunnel Probing [s]</b>	The interval in which keepalive packets are sent to the remote tunnel end.
<b>Tunnel Timeout [s]</b>	The timeout after which the tunnel will be actively re-established after probing has failed.

### Serial Console Settings (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
<b>PPP Remote IP</b>	Enter the IP address of the client when connecting via the serial IP address.

<b>PPP Local IP</b>	Enter the IP address of the Barracuda NextGen Firewall F-Series. If this field is empty, the Box IP address is used.
<b>Require PAP</b>	Specifies if the connecting client is required to authenticate itself to the Barracuda NextGen Firewall F-Series [possible users: root or support user].

13. Click **OK**.
14. 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 **Original Source IP**.

**Rule Name:** INET-2-CC-IPv4-MGMT

**Action:** Dst NAT

**Source:** Internet  
 Ref: Any  
 NOT 10.0.0.0/8  
 NOT 172.16.0.0/12  
 NOT 192.168.0.0/16

**Service:** NGF-MGMT-Tunnel  
 TCP 692  
 UDP 692

**Destination:** HQ-ISP1-PublicIP1  
 62.99.0.40

**Redirection:**  
 Target List: 10.0.10.77  
 List of Critical Ports: 692

**Authenticated User:** Any

**Policies:**  
 IPS Policy: Default  
 Application Policy: No AppControl  
 Schedule: Always  
 QoS Band (Fwd): VOIP (ID 2)  
 QoS Band (Reply): Like-Fwd

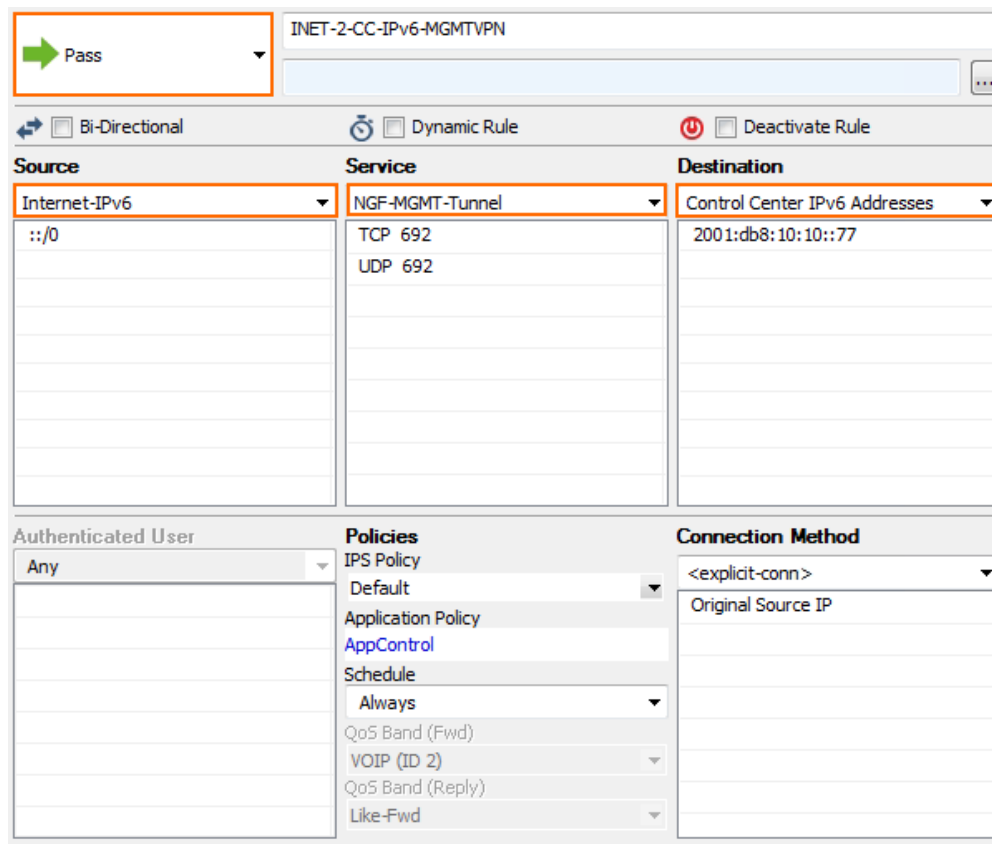
**Connection Method:** Original Source IP

## 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





INET-2-CC-IPv6-MGMTVPN

Pass

Bi-Directional Dynamic Rule Deactivate Rule

Source	Service	Destination
Internet-IPv6 ::/0	NGF-MGMT-Tunnel TCP 692 UDP 692	Control Center IPv6 Addresses 2001:db8:10:10::77

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Application Policy AppControl Schedule Always QoS Band (Fwd) VOIP (ID 2) QoS Band (Reply) Like-Fwd	<explicit-conn> Original Source IP

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

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

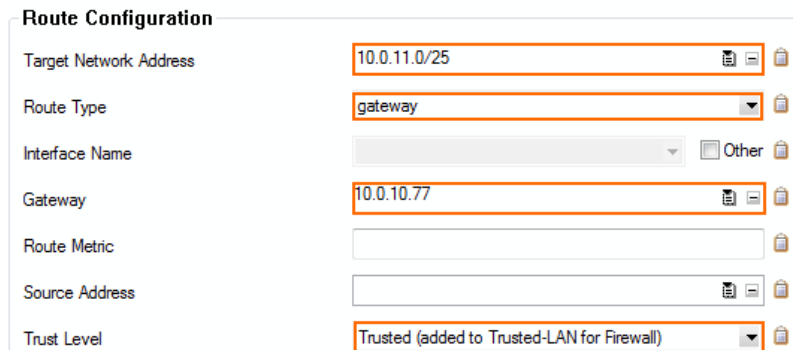
## Step 7. (optional) Create Access Rules and Routing Entries for Separate VIP Networks

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**.



The image shows a 'Route Configuration' form with the following fields and values:

Field	Value
Target Network Address	10.0.11.0/25
Route Type	gateway
Interface Name	(empty)
Gateway	10.0.10.77
Route Metric	(empty)
Source Address	(empty)
Trust Level	Trusted (added to Trusted-LAN for Firewall)

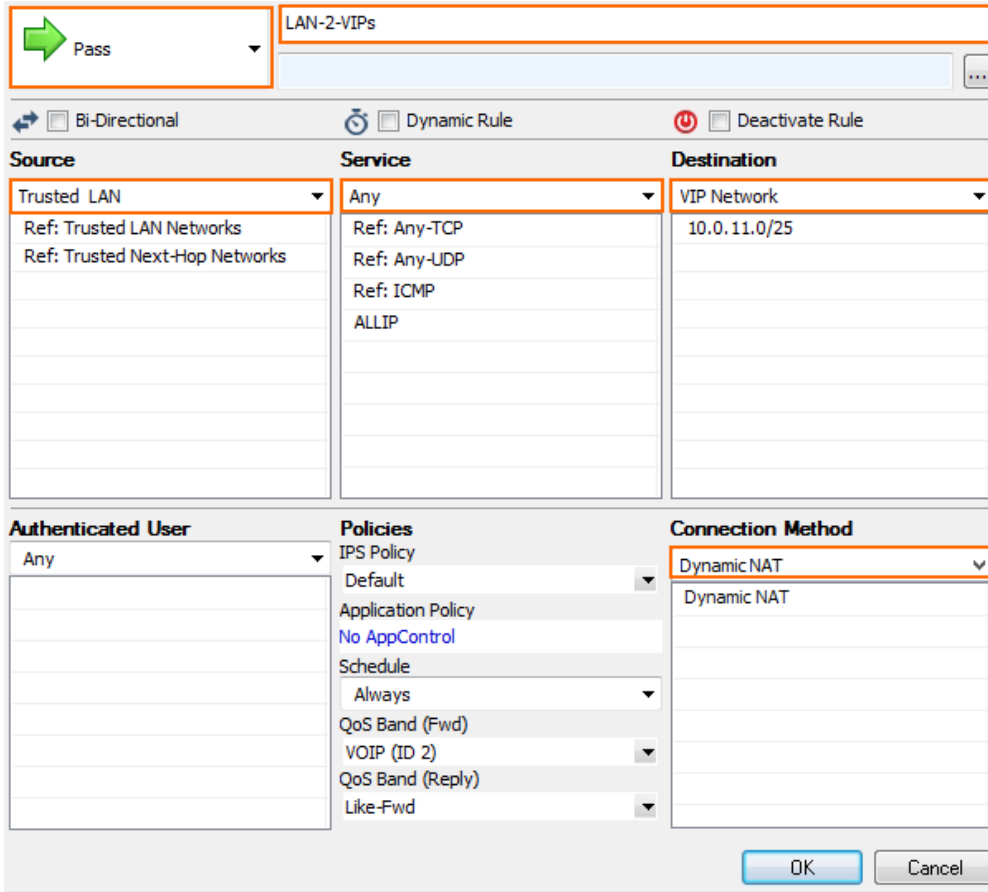
5. Click **OK**.
6. Click **Send Changes** and **Activate**.
7. Activate the network changes on the **Box** page (**CONTROL > Box**).

#### 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 NextGen Firewall F-Series, 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**.



Pass

LAN-2-VIPs

Bi-Directional

Dynamic Rule

Deactivate Rule

**Source**

Trusted LAN

Ref: Trusted LAN Networks

Ref: Trusted Next-Hop Networks

**Service**

Any

Ref: Any-TCP

Ref: Any-UDP

Ref: ICMP

ALLIP

**Destination**

VIP Network

10.0.11.0/25

**Authenticated User**

Any

**Policies**

IPS Policy

Default

Application Policy

No AppControl

Schedule

Always

QoS Band (Fwd)

VOIP (ID 2)

QoS Band (Reply)

Like-Fwd

**Connection Method**

Dynamic NAT

Dynamic NAT

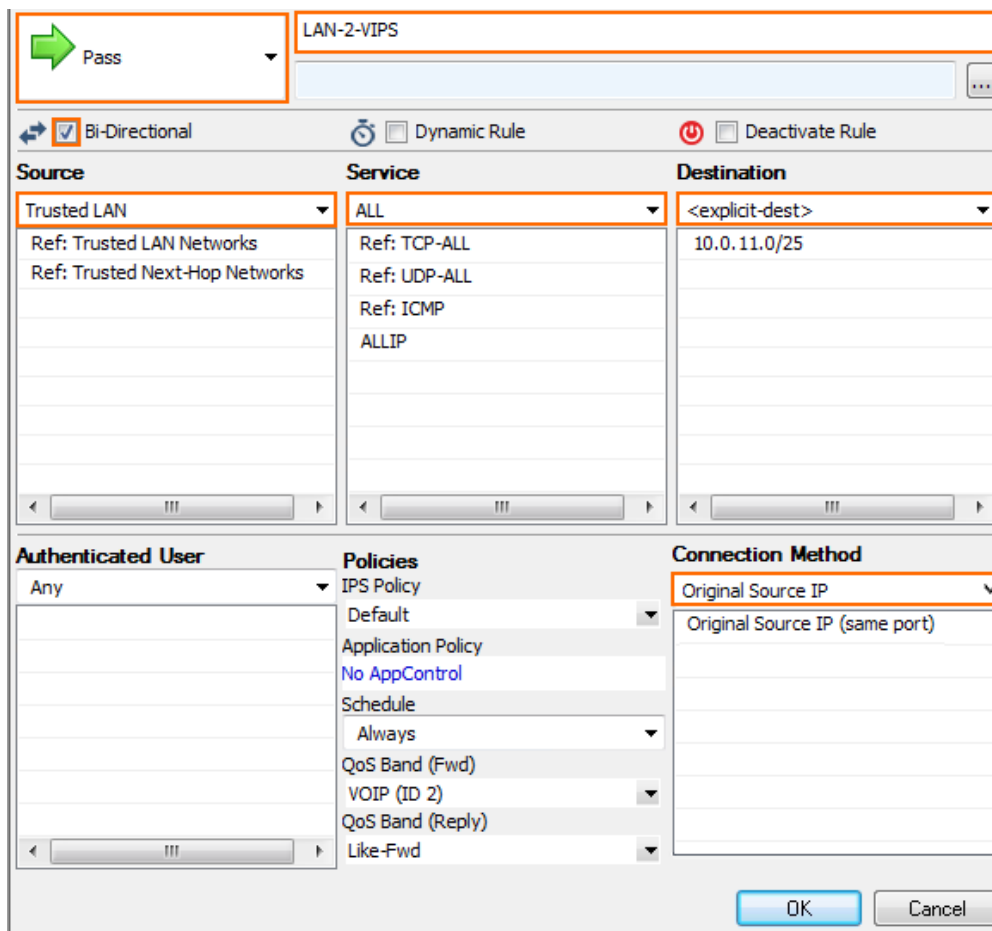
OK

Cancel

### 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 > 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 **Original Source IP**.



Pass  
 LAN-2-VIPS

☒ Bi-Directional
 ☐ Dynamic Rule
 ☐ Deactivate Rule

Source	Service	Destination
Trusted LAN	ALL	<explicit-dest>
Ref: Trusted LAN Networks	Ref: TCP-ALL	10.0.11.0/25
Ref: Trusted Next-Hop Networks	Ref: UDP-ALL	
	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
Any	IPS Policy	Original Source IP
	Default	Original Source IP (same port)
	Application Policy	
	No AppControl	
	Schedule	
	Always	
	QoS Band (Fwd)	
	VOIP (ID 2)	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

- Click **OK**.
- 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.

Site-to-Site

Client-to-Site

Status

Filter

Name	Tunnel	Type	Group	Local	Peer	Virtual IP	Info	Transport	Encryption
Barracuda Group (2)									
BOX-BO1-NG4_BranchOffice1-2_1	PGRP		box	2001.db8:10:10:...	2001.db8:20:1	10.0.11.19	SM:Auth-BOX-BO1-NG4_BranchOffice1-2_1.PS...	TCP	AES 256
BOX-BO2-NG1_BranchOffice1-2_1	PGRP		box	10.0.10.77	213.47.0.13	10.0.11.94	SM:Auth-BOX-BO2-NG1_BranchOffice1-2_1.PS...	TCP	AES 256

## Figures

1. cc\_remote\_mgmt\_tunnel\_01.png
2. cc\_remote\_mgmt\_tunnel\_02.png
3. ipv6\_listener\_ccvpn.png
4. mgmt\_tunnel\_network\_settings.png
5. mgmt\_tunnel\_ipv4\_rule.png
6. mgmt\_tunnel\_ipv6\_rule.png
7. MGMT\_Tunnel\_BorderFW\_Route.png
8. MGMT\_Tunnel\_BorderFW\_PASS.png
9. MGMT\_Tunnel\_CC\_FW\_PASS.png
10. mgmt\_tunnel\_CC\_VPN.png

© Barracuda Networks Inc., 2024 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.