

Example - Configuring a Site-to-Site IPsec VPN Tunnel

<https://campus.barracuda.com/doc/14320455/>

To configure a Site-to-Site VPN connection between two Barracuda NextGen X-Series Firewalls, in which one unit (Location 1) has a dynamic Internet connection and the peer unit (Location 2) has a static public IP address, create an IPsec tunnel on both units. In this setup, Location 1 acts as the active peer. You will need to add an access rule to allow VPN traffic. Because the WAN IP address of Location 1 is chosen dynamically via DHCP, the remote gateway on Location 2 must use 0.0.0.0/0 so that any incoming IP address is accepted. Using 0.0.0.0/0 as the remote gateway is supported only for site-to-site tunnels in Aggressive mode. This setup does not require third-party DNS services such as DynDNS.



This example configuration uses the following settings:

	X-Series Firewall Location 1	X-Series Firewall Location 2
Published VPN Network	172.16.0.0/24	10.0.0.0/25
Public IP Addresses	dynamic via DHCP	62.99.0.74

Before you Begin

On the **VPN > Settings** page of both X-Series Firewalls, verify that you selected a valid VPN certificate. For more information, see [Certificate Manager](#).

Step 1. Enable VPN Listener on the Dynamic IP Address of the Active Peer

On the X-Series Firewall at Location 1, enable **Use Dynamic IPs** in the **GLOBAL SERVER SETTINGS** of the **VPN > Settings** page for the VPN service to listen on all IP addresses.

GLOBAL SERVER SETTINGS				Help	
Use TCP Port 443	No ▾	CRL Poll Time [mins]	0	Global TOS Copy	Off ▾
Tunnel Check Interval	5	Exchange Timeout	30	Use Dynamic IPs	Yes ▾

Step 2. Create the IPsec Tunnel on Location 1

Configure the X-Series Firewall at Location 1 with the dynamic WAN IP as the active peer.

1. Log into the X-Series Firewall at Location 1.
2. Go to the **VPN > Site-to-Site VPN** page.
3. In the **Site-to-Site IPsec Tunnels** section, click **Add**.
4. Enter a **Name** for the VPN tunnel.
5. Configure the settings for **Phase 1** and **Phase 2**.

Edit Site-to-Site IPsec Tunnel ?

Name: ☐ Disabled

Phase 1 ?

Encryption: ▾
Hash Method: ▾
DH Group: ▾
Lifetime:

Phase 2 ?

Encryption: ▾
Hash Method: ▾
DH Group: ▾
Lifetime:
Perfect Forward Secrecy: ☐

6. Specify the network settings:
 - **Local End** - Select **Active**.
 - **Local Address** - Select **Dynamic**.
 - **Local Networks** - Enter 172.16.0.0/24 (the network address for the locally configured LAN), and click +.
 - **Remote Gateway** - Enter 62.99.0.74 (the WAN IP address of Location 2).
 - **Remote Networks** - Enter 10.0.0.0/25 (the remote LAN), and click +.
7. Specify the authentication settings:

- **Authentication** – Select **Shared Passphrase**.
 - **Passphrase** – Enter the shared secret.
8. Enable **Aggressive Mode**.
 9. Define the **Aggressive Mode ID**.

Local End:	<input checked="" type="radio"/> Active <input type="radio"/> Passive	Authentication:	<input type="text" value="Shared Passphrase"/>
Local Address:	<input type="text" value="Dynamic"/>	Passphrase:	<input type="text" value="....."/>
Local Networks:	<div><input type="text" value="172.16.0.0/24"/> + -</div>	Enable Aggressive Mode:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Remote Gateway:	<input type="text" value="62.99.0.74"/>	Aggressive Mode ID:	<input type="text" value="barracuda"/>
Remote Networks:	<div><input type="text" value="10.0.0.0/25"/> + -</div>	Local Certificate:	<input type="text" value="default"/>
		CA Root Certificate:	<input type="text" value="Use All Known"/>
		x509 Matching Conditions:	<input type="text" value="Common Name"/> +

10. Click **Add**.

Step 3. Create the IPsec Tunnel on Location 2

Configure the X-Series Firewall at Location 2, with the static WAN IP as the passive peer. Use 0.0.0.0/0 as the IP address for the remote gateway to allow the Location 1 unit to use dynamic WAN IP addresses.

1. Log into the X-Series Firewall at Location 2.
2. Go to the **VPN > Site-to-Site VPN** page.
3. In the **Site-to-Site IPsec Tunnels** section, click **Add**.
4. Enter a **Name** for the VPN tunnel.
5. Configure the same settings for **Phase 1** and **Phase 2** as for Location 1.
6. Specify the network settings:
 - **Local End** – Select **Passive**.
 - **Local Address** – Select 62.99.0.74 (the WAN IP address of Location 2).
 - **Local Networks** – Enter 10.0.0.0/25 (the network address for the locally configured LAN), and click +.
 - **Remote Gateway** – Enter 0.0.0.0/0 because the WAN IP address of location 1 is chosen dynamically via DHCP.
 - **Remote Networks** – Enter 172.16.0.0/24. (the remote LAN), and click +.
7. Specify the authentication settings:
 - **Authentication** – Select **Shared Passphrase**.
 - **Passphrase** – Enter the shared secret.
8. Enable **Aggressive Mode**.
9. Define the **Aggressive Mode ID**.

Local End:	<input type="radio"/> Active <input checked="" type="radio"/> Passive	Authentication:	<input type="text" value="Shared Passphrase"/>
Local Address:	<input type="text" value="62.99.0.74"/>	Passphrase:	<input type="text" value="....."/>
Local Networks:	<input type="text" value="10.0.0.0/25"/> <input type="button" value="+"/> <input type="button" value="-"/>	Enable Aggressive Mode:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Remote Gateway:	<input type="text" value="0.0.0.0/0"/>	Aggressive Mode ID:	<input type="text" value="barracuda"/>
Remote Networks:	<input type="text" value="172.16.0.0/24"/> <input type="button" value="+"/> <input type="button" value="-"/>	Local Certificate:	<input type="text" value="default"/>
		CA Root Certificate:	<input type="text" value="Use All Known"/>
		x509 Matching Conditions:	<input type="text" value="Common Name"/> <input type="button" value="+"/>

10. Click **Add**.

Step 4. Configure the Access Rule for VPN Traffic

Remote and local subnets are automatically added to the **VPN-Local-Networks** and **VPN-Remote-Networks** network objects when saving the Site-to-Site VPN configuration. If not present, go to **FIREWALL > Network Objects** and create these network objects. For more information, see [Network Objects](#).

VPN-Local-Networks	All locally defined networks for Site-2-Site VPN	→ 10.0.0.0	25
VPN-Remote-Networks	All defined remote networks for Site-2-Site VPN	→ 172.16.0.0	24

Create PASS access rules on both Location 1 and Location 2 X-Series Firewalls to allow traffic in and out of the VPN tunnel.

1. Log into the X-Series Firewall.
2. Go to **FIREWALL > Firewall Rules** page.
3. Add an access rule with the following settings:
 - **Action** – **Allow**
 - **Connection** – Select **No SNAT**
 - **Bi-directional** – Select the **Bi-directional** checkbox.
 - **Service** – Select **Any**. All types of network traffic are allowed between the remote and local network.
 - **Source** – Select the **VPN-Local-Networks** network object.
 - **Destination** – Select the **VPN-Remote-Networks** network object.

General

Advanced

Action:

Allow

Name:

VPN-SITE-2-SITE

Bi-directional:

☐ Yes
 ☒ No

Disable:

☐ Yes
 ☒ No

IPS:

☒ Yes
 ☐ No

Application Control:

☒ Yes
 ☐ No

URL Filter:

☐ Yes
 ☒ No

Safe Search:

☐ Yes
 ☒ No

Virus Protection:

☐ Yes
 ☒ No

SSL Inspection:

☐ Yes
 ☒ No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Description:

Connection:

No SNAT

Adjust Bandwidth:

Business

The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.

Source

Any

+

Ref: VPN-Local-Networks

-

Network Objects

IP Address

Geo Loc.

Network Services

Any

+

Any

-

Destination

Any

+

Ref: VPN-Remote-Networks

-

Network Objects


IP Address

Geo Loc.

DNAT (port forwarding) - Redirect traffic to a specific IP address.

Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.



Bi-directional - Source and destination networks are interchangeable.



- At the top of the **Add Access Rule** window, click **Add**.
- Use drag and drop to place the access rule above any other access rule matching this traffic.
- Click **Save**.

Step 5. Verify Successful VPN Tunnel Initiation and Traffic Flow

To verify that the VPN tunnel was initiated successfully and traffic is flowing, go to the **VPN > Site-to-Site VPN** page. Verify that green check marks are displayed in the **Status** column of the VPN tunnel.

SITE-TO-SITE IPSEC TUNNELS														Help
Add														
Choose a bulk action ▾														
Select all Deselect all														
Status		Name	Local Address	Remote Gate...	Local Networks	Remote Netwo...	B/10s	Total	Idle	Start	Key	Advanced Settings	Actions	
<input checked="" type="checkbox"/>	Up	Dynami...	62.99.0.74	0.0.0.0/0	10.0.0.0/25	172.16.0.0/24	0 B	5 K	3 h	4 h	19 m	Traffic Control		
<input checked="" type="checkbox"/>	Up													

Use ping to verify that network traffic is passing the VPN tunnel. Open the console of your operating system and ping a host within the remote network. If no host is available, you can ping the management IP address of the remote X-Series Firewall. Go to the **NETWORK > IP Configuration**

[Example - Configuring a Site-to-Site IPsec VPN Tunnel](#)

5 / 7

page and ensure that **Services to Allow: Ping** is enabled for the management IP address of the remote firewall.

If network traffic is not passing the VPN tunnel, go to the **BASIC > Recent Connections** page and ensure that network traffic is not blocked by any other access rule.

Figures

1. s_to_s_dynamic.png
2. s2s_dynamic_ips.png
3. s2s_ipsec_settings01.png
4. s2s_ipsec_settings02.png
5. s2s_ipsec_settings04.png
6. s2s_net_objects.png
7. s2s_access_rule.png
8. s2s_ipsec_tunnels.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.