

How to Configure a Site-to-Site IPsec IKEv1 VPN Tunnel

<https://campus.barracuda.com/doc/72515938/>

The firewall can establish IPsec VPN tunnels to any standard-compliant, third-party IKEv1 IPsec VPN gateway. The site-to-site IPsec VPN tunnel must be configured with identical settings on both the firewalls and the third-party IPsec gateway. The firewall supports authentication with a shared passphrase as well as X.509 certificate-based (CA-signed and self-signed) authentication. To allow traffic into the VPN tunnel, an access rule is required.



This example configuration uses the following settings:

	Firewall Location 1	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 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 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 firewall at Location 1 with the dynamic WAN IP as the active peer.

1. Log into the firewall at Location 1.
2. Go to **VPN > Site-to-Site VPN**.
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:	<input type="text" value="DynamicBFW-2-StaticBFW"/>	<input type="checkbox"/> Disabled
Phase 1 ?		Phase 2 ?
Encryption:	<input type="text" value="AES"/>	Encryption: <input type="text" value="AES"/>
Hash Method:	<input type="text" value="SHA"/>	Hash Method: <input type="text" value="SHA1"/>
DH Group:	<input type="text" value="Group 1"/>	DH Group: <input type="text" value="None"/>
Lifetime:	<input type="text" value="28800"/>	Lifetime: <input type="text" value="3600"/>
		Perfect Forward Secrecy: <input type="checkbox"/>

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

10. **Add** .

Step 3. Create the IPsec Tunnel on Location 2

Configure the 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 firewall to use dynamic WAN IP addresses.

1. Log into the firewall at Location 2.
2. Go to **VPN > Site-to-Site VPN**.
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**
8. Enable **Aggressive Mode**.
9. Define the **Aggressive Mode ID**.

Local End: Active Passive

Local Address:

Local Networks:

Remote Gateway:

Remote Networks:

Authentication:

Passphrase:

Enable Aggressive Mode: Yes No

Aggressive Mode ID:

Local Certificate:

CA Root Certificate:

x509 Matching Conditions:

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](#).

<input type="checkbox"/> VPN-Local-Networks	All locally defined networks for Site-2-Site VPN	<input type="button" value="➔"/>	10.0.0.0	25
<input type="checkbox"/> VPN-Remote-Networks	All defined remote networks for Site-2-Site VPN	<input type="button" value="➔"/>	172.16.0.0	24

Create PASS access rules on both Location 1 and Location 2 firewalls to allow traffic in and out of the VPN tunnel

1. Log into the firewall.
2. Go to **FIREWALL > Access Rules**.
3. Click **Add Access Rule**.
4. Add an access rule with the following settings:
 - o **Action** - **Pass**
 - o **Connection** - Select **Original Source IP**
 - o **Bi-directional** - Select the **Bi-directional** check box.
 - o **Service** - Select **Any**.
 - o **Source** - Select the **VPN-Local-Networks** network object.
 - o **Destination** - Select the **VPN-Remote-Networks** network object.

General
Advanced

Action: Pass

➔

*DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda NextGen Firewall.
Bi-directional - Source and destination networks are interchangeable.*

Name: VPN-SITE-2-SITE

Description:

Connection: Original Source IP

Adjust Bandwidth: Business

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

Bi-directional: Yes No

Disable: Yes No

IPS: Yes No

Application Control: Yes No

SSL Interception: Yes No

URL Filter: Yes No

Virus Scanner: Yes No

ATP: Yes No

Mail Security: Yes No

Safe Search: Yes No

Source

Any +

Ref: VPN-Local-Networks

Network Objects IP Addresses Geo Loc.

Network Services

Any-EMAIL +

Any

Destination

Any +

Ref: VPN-Remote-Networks

Network Objects IP Addresses Geo Loc.

5. At the top of the **Add Access Rule** window, click **Add**.
6. Drag the access rule above any other access rule matching this traffic.
7. 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
<div style="display: flex; justify-content: space-between; align-items: center;"> Add <div style="display: flex; gap: 10px;"> Choose a bulk action ▾ Select all Deselect all </div> </div>													
Status	Name	Local Address	Remote Gate...	Local Networks	Remote Netwo...	B/10s	Total	Idle	Start	Key	Advanced Settings	Actions	
✓	Up	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	✎ 🗑	
✓	Up												

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, ping the management IP address of the remote firewall. Go to the **NETWORK > IP Configuration** 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. ipsec_tunnel.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., 2020 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.