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:

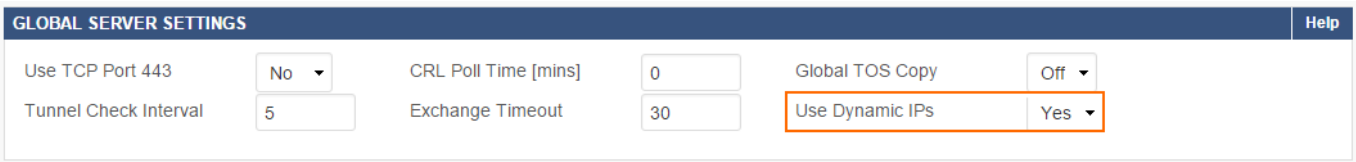
	Firewall Location 1	Firewall Location 2
Published VPN Network	172.16.0.0/24	10.0.0.0/25
Public IP Addresses	Dynamic via DHCP	62.99.0.74

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

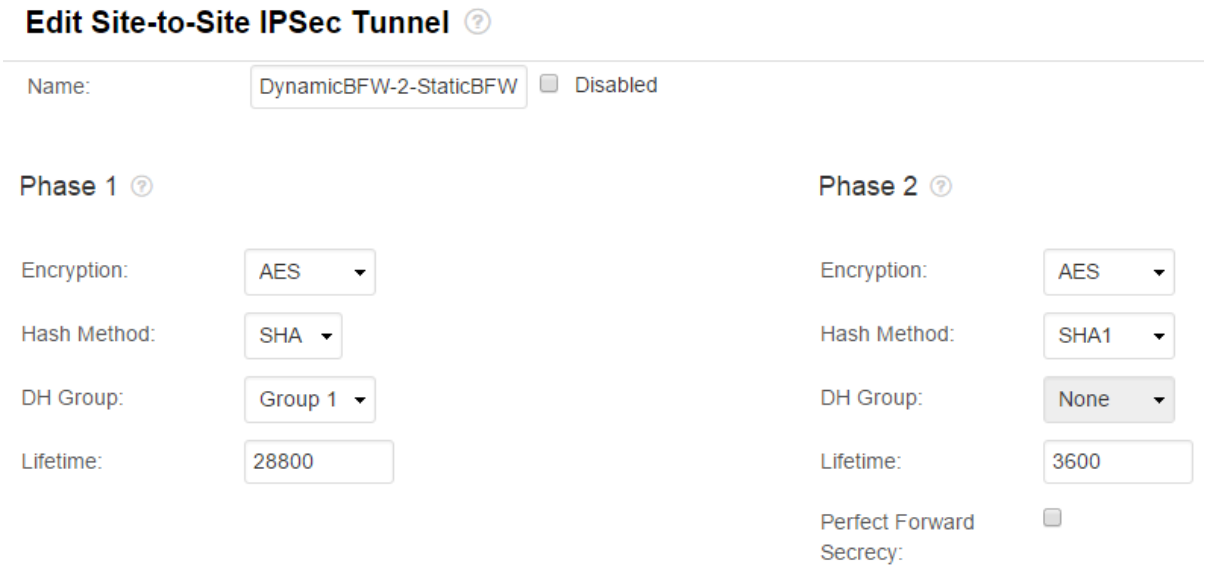
On the firewall at Location 1, enable **Use Dynamic IPs** in the **GLOBAL SERVER SETTINGS** of the **VPN > Settings** page for the VPN service to listen on all IP addresses.



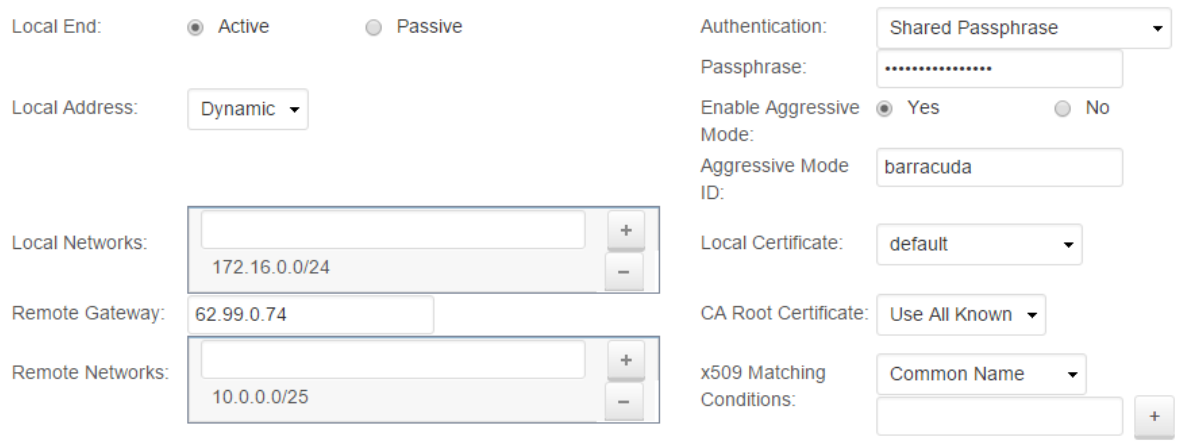
Step 2. Create the IPsec Tunnel on Location 1

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**.



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**.

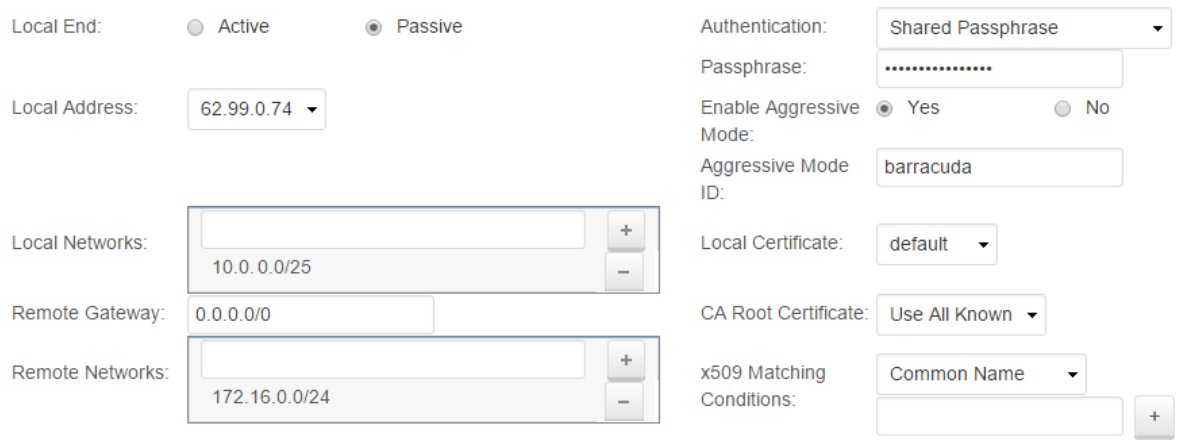


10. **Add** .

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.

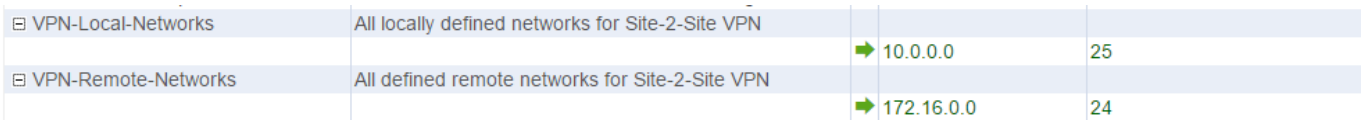
1. Log into the firewall at Location 2.
2. Go to **VPN > Site-to-Site VPN**.
3. In the **Site-to-Site IPSec Tunnels** section, click **Add**
4. Enter a **Name** for the VPN tunnel.
5. Configure the same settings for **Phase 1** and **Phase 2** as for Location 1.
6. Specify the network settings:
   - **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**.



10. Click **Add**.

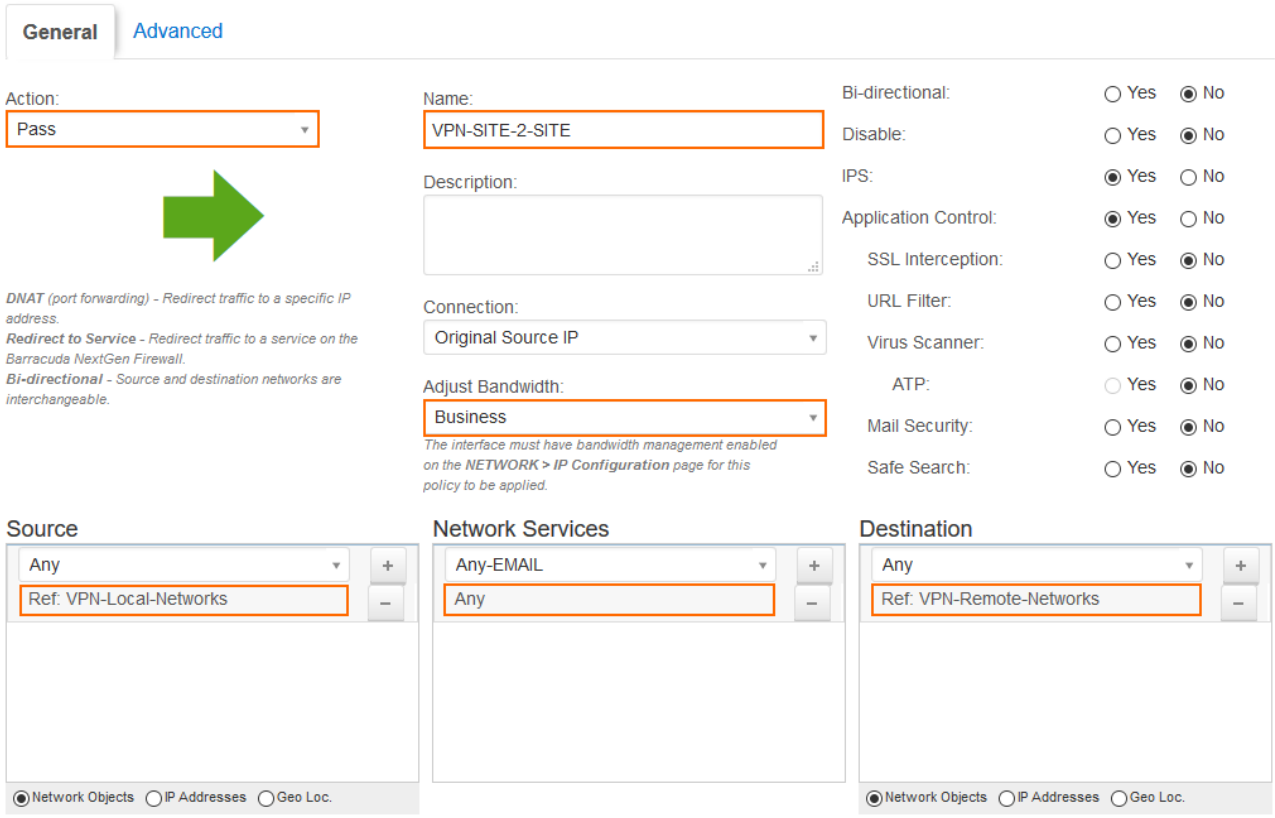
Step 4. Configure the Access Rule for VPN Traffic

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.



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

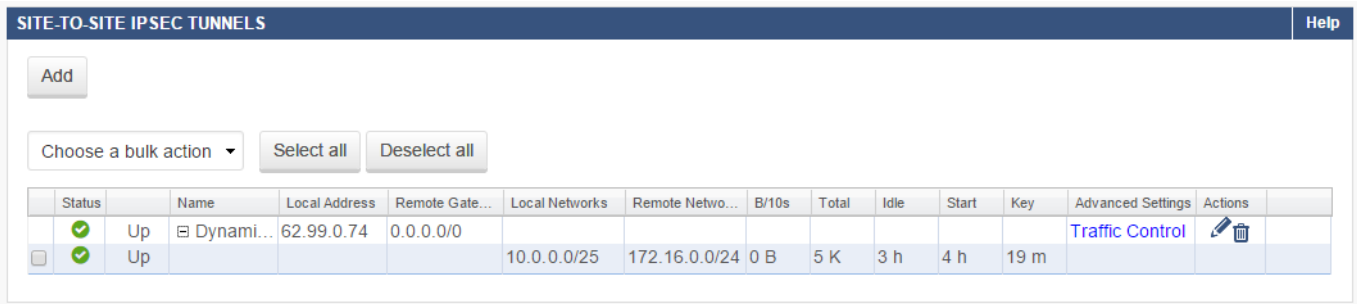
1. Log into the firewall.
2. Go to **FIREWALL > Access Rules**.
3. Click **Add Access Rule**.
4. Add an access rule with the following settings:
   - **Action** – **Pass**
   - **Connection** – Select **Original Source IP**
   - **Bi-directional** – Select the **Bi-directional** check box.
   - **Service**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



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.



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