

How to Configure a Site-to-Site VPN with IPsec

<https://campus.barracuda.com/doc/8650760/>

The Barracuda NextGen Firewall X-Series can establish IPsec VPN tunnels to any other appliance supporting the IPsec VPN protocol, including another X-Series Firewall. To set up the IPsec VPN tunnel, you must create it on the X-Series Firewall and its remote appliance. For a successful IPsec tunnel, configure identical Phase 1 and Phase 2 settings on both VPN gateways. The X-Series Firewall supports authentication with a shared passphrase as well as X.509 certificate-based (CA-signed as well as self-signed) authentication. You must also configure a firewall rule to allow traffic between both networks.

Step 1. Create the IPsec Tunnel on the X-Series Firewall and on the Remote Appliance

To create the IPsec tunnel on the X-Series Firewall:

1. Go to the **VPN > Site-to-Site VPN** page.
2. In the **Site-to-Site IPsec Tunnels** section, click **Add**.
3. On the **Add Site-to-Site IPsec Tunnels** page, configure the settings. The Phase 1 and Phase 2 settings must be identical on both VPN gateways.
4. After configuring the tunnel settings, click **Save**.
5. Configure the IPsec tunnel on the remote appliance.

Step 2. Configure the X-Series Firewall VPN Server

The VPN server that runs on the X-Series Firewall must listen on the appropriate IP address for its peer. Depending on whether the X-Series Firewall is connected to the Internet through an ISP that statically or dynamically assigns the WAN IP address, complete the steps in the following [Static WAN IP Address](#) or [Dynamic WAN IP Address](#) section.

Static WAN IP Address

If the X-Series Firewall is connected to the Internet through an ISP that statically assigns the WAN IP address:

1. Go to the **NETWORK > IP Configuration** page.
2. In the **Static Interface Configuration** section, verify that the **VPN Server** check box is selected for the interface or for any **Secondary IP Address** of the management IP address.

Dynamic WAN IP Address

If your X-Series Firewall is connected to the Internet through an ISP that dynamically assigns the WAN IP address, see [How to Allow VPN Access via a Dynamic WAN IP Address](#).

Step 3. Create the Access Rule for VPN Traffic

Create a firewall rule to allow network traffic between the two networks. If the tunnel is to be established between two X-Series Firewalls, create the same rule on *both* appliances.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Add a firewall rule with the following settings:

Action	Connection	Bi-directional	Service	Source	Destination
Allow	No SNAT (the original source IP address is used)	Select the Bi-directional check box.	Any	The LAN 1 address.	The LAN 2 address.

3. At the top of the **Add Access Rule** window, click **Add**.



Step 4. Verify the Order of the Access Rules

New rules are created at the bottom of the firewall rule set. Because rules are processed from top to bottom in the rule set, ensure that you arrange your rules in the correct order. Take special care to place your rule above the BLOCKALL rule. Otherwise, the rule will never match and all traffic is blocked. If you are configuring a tunnel between two X-Series Firewalls, verify the order of the firewall rules in the rule sets for both appliances.

After adjusting the order of rules in the rule set, 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 Tunnels** page. Verify that green check marks are displayed in the **Status** column of the VPN tunnel.

SITE-TO-SITE IPSEC TUNNELS													
<div>Add</div> <div> Choose a bulk action ▼ <div>Select all</div> <div>Deselect all</div> </div>													
	Status	Name	Local Address	Remote Gateway	Local Networks	Remote Networks	bps10	Total	Idle	Start	Key	Advanced Settings	Actions
<input checked="" type="checkbox"/>	✓ Up	IPsecS2STunnel	Dynamic	62.99.0.221								Traffic Control	 
<input type="checkbox"/>	✓ Up				172.16.0.0/24	10.0.11.0/24	0 B	0 K	4 m	4 m	17 s		

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** 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 firewall rule.

Figures

1. S2S-VPN01.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.