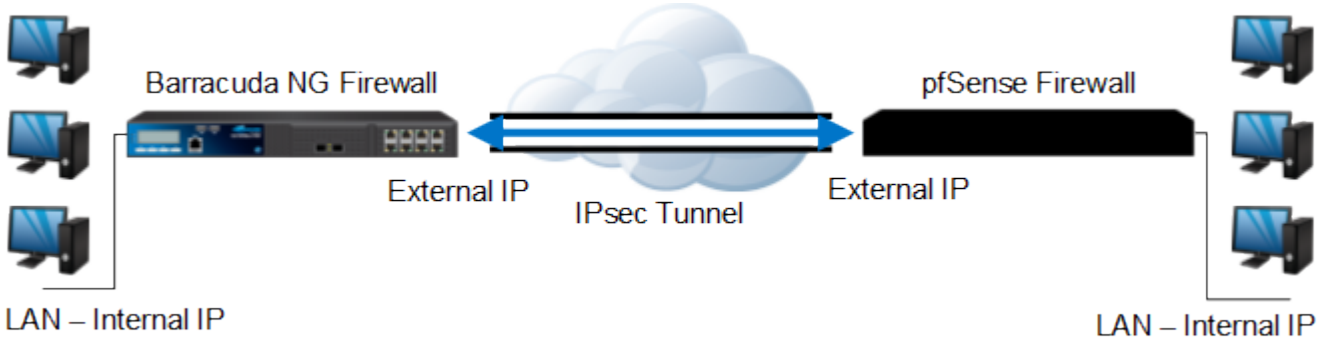
How to Create an IPsec VPN Tunnel between the Barracuda NG Firewall and a pfSense Firewall

https://campus.barracuda.com/doc/43846991/

Before configuring an IPsec VPN Tunnel between a Barracuda NG Firewall and a pfSense Firewall, make sure that the VPN and Firewall services have been created on the Barracuda NG Firewall. For more information, see How to Configure Services.



The following article provides information and steps for configuring the IPsec VPN tunnel. It also provides an overview of the settings for creating the tunnel on the Barracuda NG Firewall.

In this article:

Configuration Overview and Recommendations

When creating IPsec tunnels between Barracuda NG Firewall and third party gateways, consider the following recommendations:

- Do not use "Supernetting." It is not supported.
- Configure lifetimes (i.e. tunnel rekeying times) as time (seconds only) and not as KB-values. The **Phase 1** and **Phase 2** lifetime should never have the same value.
- Tunnel partners must be active at one end and passive at the other end.
- Encryption and DH-Group settings must be identical on both tunnel ends. Thereby, the Perfect Forward Security (PFS) configuration matches the **DH-Group** / **Phase 2** configuration on Barracuda NG Firewall systems.
- Lifetimes in **Phase 1** must be greater than lifetimes in **Phase 2**.
- The local and remote network must not contain single IP addresses; they must be at least a network with mask /30.
- Do not use IPsec-SA bundling.

- The Barracuda NG Firewall ISAKMPD supports Dead Peer Detection (DPD). If the remote IPsec gateway does not support DPD, you must disable it in the advanced VPN server settings by entering *0* in the **Dead Peer Detection Interval (s)** field.
- Do not set the **Tunnel Check Interval (s)** to *0* seconds. The default value is 5 seconds. Specifying an interval that is less than 5 seconds will generate too much traffic.
- The Barracuda NG Firewall ISAKMPD implementation uses the *IPv4_net* and not *IPv4_address* as ID-Type.
- Only net announcements from the *IPv4_net* type is supported. Other announcement methods may generate "Supernetting" errors.
- Do not use identical or overlapping remote networks in different configured IPSec tunnels, the remote network is used for authentication.

For successful negotiations, the settings for Phase 1 and Phase 2 must meet the requirements of the remote peer. The IPsec specification allows two possible values for the local and remote network settings if the local or the remote network consists of only a single IP address.

Most of the IPsec implementations represent a single IP address as a network address in combination with a subnet mask (*255.255.255.255*). The IKE protocol is difficult to debug. Therefore, Barracuda NG Admin displays a warning message if IPsec networks contain single IP addresses. It may happen that an IPsec connection cannot be established and the following error is displayed: *no compatible proposals chosen.*

In this case, you should first verify whether both IPsec peers are using the same IPsec settings (e.g. encryption, hash method, etc.). If all settings are identical but the tunnel still fails to be established, you may try to use network addresses (using netmask *255.255.255.252*) for the local and remote network settings.

If the tunnel can then properly be established, it means that the IPsec implementation is not compatible with the use of single IP addresses. In this case, a whole network range for the IPsec tunnel must be reserved.

Create the IPsec VPN Tunnel on the Barracuda NG Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click the **IPSEC Tunnels** tab.
3. Click **Lock**.
4. Right-click the table and select **New IPSec tunnel**. The **IPsec Tunnel** window opens.
5. In the **Name** field, enter your tunnel name. For example, *HQ2PFSense*.
6. Configure the local network settings. Click the **Local Networks** tab and specify the following settings:
    - **Local IKE Gateway –** The external IP address of the Barracuda NG Firewall.

- **Network Address –** The external network IP address. Enter the address and then click **Add**. For example, *192.168.9.0/24*.

7. Configure the remote network settings. Click the **Remote Networks** tab and specify the following settings:
   - **Remote IKE Gateway –** The external IP address of the pfSense unit.
   - **Network Address –** The external network IP address of the pfSense unit. Enter the address and then click **Add**. *For example, 10.10.110.0/24.*
8. Specify the shared passphrase. Click the **Peer Identification** tab and then enter the shared passphrase in the **Passphrase** field. For example, *secret*.
9. Configure the encryption settings. Click the **Basics** tab and then select the following **Phase 1** and **Phase 2** settings:

Phase 1	
Setting	**Value**
Encryption	3DES
Hash. Meth.	MD5
DH-Group	Group2
Lifetime [sec]	28800
Min. Lifetime [sec]	25200
Max. Lifetime [sec]	32400

Phase 2	
Setting	**Value**
Encryption	3DES
Hash. Meth.	MD5
DH-Group	Group1
Lifetime [sec]	3600
Min. Lifetime [sec]	1200
Max. Lifetime [sec]	4800

10. Click the **Advanced** tab. In the **DPD interval (s)** field, enter `0`.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

For more information on the settings in the **IPSec Tunnel** configuration window, see the following IPSec Tunnel Settings section in this article.

Create the IPsec VPN Tunnel on the pfSense Firewall

1. On the pfSense unit, select the **VPN** menu and choose **IPSEC**.
2. Select the **Enable IPsec** check box.
3. Click the **+** icon to add a tunnel.

4. Configure the network settings. Specify the following settings:
    1. **remote subnet –** The remote subnet address. For example, `192.168.9.0/24`
    2. **Remote Gateway –** The external IP address of the pfSense unit. For example,`192.168.100.1`
5. Configure the settings in the **Phase 1 proposal** (Authentication) section.
    1. Select the following settings:

Setting	Value
Encryption algorithm	3DES
Hash algorithm	MD5
DH key group	2
Lifetime	28800
Authentication method	Pre-shared key

    2. In the **Pre-Shared Key** field, enter the key. For example, `secret`.
6. Configure the settings in the **Phase 2 proposal** (SA/Key Exchange) section. Select the following settings:

Setting	Value
Hash algorithms	MD5
PFS key group	1
Lifetime	3600

7. Click **Save**.
8. Click **Apply changes**. You should now see the tunnel entry.

Create Firewall Rules for VPN Access

You must create firewall rules on the Barracuda NG Firewall and the pfSense Firewall to allow VPN traffic between them. On the Barracuda NG Firewall, the connection for the VPN rules must be set as *Client\Std Client (same port)*. For more information on creating firewall rules, see Firewall Access Rules.

IPSec Tunnel Settings

For more information on the settings in the **IPSec Tunnel** configuration window, expand the following section:

In the **IPSec Tunnel** window, you can configure settings from the following tabs:

General

Setting	Description
Name	The tunnel name. You can enter a maximum of 26 characters.
Disabled	To manually disable the tunnel, select this check box.

Basics

From this tab, you can edit the following **Phase 1** and **Phase 2** settings.

Setting	Description
Encryption	The data encryption algorithm.
Hash Meth.	The hash algorithm.
DH-Group	The Diffie-Hellman Group that specifies the type of key exchange. You can select one of the following options: • **Group1 –** Default; 768-bit modulus. • **Group2 –** 1024-bit modulus. • **Group5 –** 1536-bit modulus. • None
Lifetime [sec]	The rekeying time in seconds that the server offers to the partner.
Min. Lifetime [sec]	The minimum rekeying time in seconds that the server accepts from its partner.
Max. Lifetime [sec]	The maximum rekeying time in seconds that the server accepts from its partner.

TI - VPN Envelope Policy

Setting	Description

<table>
<tr>
<td>TOS Policy</td>
<td>This policy setting specifies how Type of Service (ToS) information contained within a packet’s IP header is handled. In networks, the ToS may be used to define the handling of the datagram during transport. If the ToS is enveloped, this information is lost. You can select one of the following options:
• Copy TOS From Payload to Envelope – Use this option with non-TCP transports. The packet’s original ToS information is copied onto the envelope, so that it stays available for use.
• Fixed Envelope TOS – The ToS information is masked by enveloping it without consideration. In the Envelope TOS Value field, enter the fixed ToS value. The same ToS information is then assigned to all packets. For example:
<table>
<tr><th>DSCP</th><th>Precedence</th><th>Purpose</th></tr>
<tr><td>0</td><td>0</td><td>Best effort</td></tr>
<tr><td>8</td><td>1</td><td>Class 1</td></tr>
<tr><td>16</td><td>2</td><td>Class 2</td></tr>
<tr><td>24</td><td>3</td><td>Class 3</td></tr>
<tr><td>32</td><td>4</td><td>Class 4</td></tr>
<tr><td>40</td><td>5</td><td>Express forwarding</td></tr>
<tr><td>48</td><td>6</td><td>Control</td></tr>
<tr><td>56</td><td>7</td><td>Control</td></tr>
</table>
For more information about precedence values, see http://www.bogpeople.com/networking/dscp.shtml and http://www.tucny.com/Home/dscp-tos.</td>
</tr>
<tr>
<td>Band Policy</td>
<td>For band policy settings to apply, you must configure traffic shaping. For more information, see Traffic Shaping. Band policy settings work independently from bandwidth protection settings.
The Band Policy settings rely on connection objects that are assigned to bands in the firewall rule sets and specify bandwidth assignment to transports as a whole. Multiple transports may share a single band if they are processed by the same interface.
You can select one of the following options:
• Use Band According to Rule Set – Use the band from the firewall rule, allowing traffic between the tunnel endpoints.
• Copy Band From Payload To Envelope – Use the band from the firewall rule, redirecting traffic to the VPN tunnel entry point. The band setting for the rule that configures traffic between the tunnel endpoints is then ignored.
• Fixed Envelope Band – Use a static band. From the Envelope Band Value list, select one of the available bands (System, Band A to Band G).</td>
</tr>
</table>

Replay Window Size	If ToS policies assigned to VPN tunnels or transports packets are not forwarded instantly according to their sequence number, you can configure the replay window size for sequence integrity assurance and to avoid IP packet "replaying." The window size specifies a maximum number of IP packets that may be on hold, until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. Individual window size settings are configurable per tunnel and transport, overriding any global policy settings. • To view or edit the global replay window size, see the VPN server settings. • To view the replay window size for a tunnel, double-click the tunnel on the VPN Tab to open the **Transport Details** window (attribute: transport_replayWindow).

Advanced

Setting	Description
HW Accel.	Specifies the preferred encryption engine. This allows for load balancing between the CPU and an optional crypto card with more than one tunnel in use. You can select one of the following options: • **Use Acceleration Card –** If a crypto accelerator hardware board is in use, select this option. • **Use CPU –** Use CPU acceleration.
Interface Index	By default, the tunnel is fed through **vpn0**. To use another VPN interface, enter it in this field. Before using this option, you must first create the indexed VPN interface in the VPN server settings.

RAW IPSec

In this section, you can add optional parameters for establishing IPsec tunnels. When appending a parameter, first specify the section that the parameter is assigned to. Then specify the new parameter itself in the next line. Enter one single value per line. For example:

```
[Section]
key=value
```

The new sections are added to the end of the `isakmpd.conf` file. New parameters are added to the top of the specified section.

For more information on the syntax to be used in this field, see the `isakmpd.conf` man page at www.openbsd.org/cgi-bin/man.cgi.

Local Networks

Setting	Description

Initiates Tunnel	Specifies whether the tunnel is active or passive. You can select one of the following options: • **Yes (passive IKE)** • **No (active IKE)** The active direction implies accepting (passive) too.
Local IKE Gateway	The IP address of the local IKE gateway. If you are using dynamic IP addresses, enter `0.0.0.0/0`

Identify

From the **Identification Type** list, you can select one of the following options:

- **Shared Secret**
- **X509 Certificate (CA signed)**
- **X509 Certificate (explicit)**
- **Box SCEP Certificate (CA signed)**

Remote Networks

Setting	Description
Remote IKE Gateway	The IP address of the remote IKE gateway. The IP address of the remote IKE gateway. If the remote IPsec gateway is connected to the Internet with a dynamic IP address, enter the DDNS (Dynamic Domain Name System) host name of the gateway.
Network Address	To add the network address of the VPN partner, enter it in this field and then click **Add**.

Peer Identification

Depending on which identification type is selected, different fields are unlocked in the **Peer Identification** section. For more information on the different authentication options, see Site-to-Site VPN Encryption and Authentication.

Additional Information

- For general information about IPsec, see www.netbsd.org/Documentation/network/ipsec/.

Figures

1. ipsec_tunnel.png