

## IPsec Tunnel Settings

<https://campus.barracuda.com/doc/42048397/>

The following IPsec tunnel settings can be configured

### General

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

### Basics

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

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

### TI - VPN Envelope Policy

Setting	Description
---------	-------------

<b>TOS Policy</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Copy TOS From Payload to Envelope</b> - 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.</li> <li>• <b>Fixed Envelope TOS</b> - The ToS information is masked by enveloping it without consideration. In the <b>Envelope TOS Value</b> field, enter the fixed ToS value. The same ToS information is then assigned to all packets. For example:</li> </ul> <table border="1" data-bbox="284 667 831 1099"> <thead> <tr> <th>DSCP</th> <th>Precedence</th> <th>Purpose</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>For more information about precedence values, see <a href="http://www.bogpeople.com/networking/dscp.shtml">http://www.bogpeople.com/networking/dscp.shtml</a> and <a href="http://www.tucny.com/Home/dscp-tos">http://www.tucny.com/Home/dscp-tos</a>.</p>	DSCP	Precedence	Purpose	0	0	Best effort	8	1	Class 1	16	2	Class 2	24	3	Class 3	32	4	Class 4	40	5	Express forwarding	48	6	Control	56	7	Control
DSCP	Precedence	Purpose																										
0	0	Best effort																										
8	1	Class 1																										
16	2	Class 2																										
24	3	Class 3																										
32	4	Class 4																										
40	5	Express forwarding																										
48	6	Control																										
56	7	Control																										
<b>Band Policy</b>	<p>For band policy settings to apply, you must configure traffic shaping. For more information, see <a href="#">Traffic Shaping</a>. Band policy settings work independently from bandwidth protection settings.</p> <p>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 can share a single band if they are processed by the same interface.</p> <p>You can select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Use Band According to Rule Set</b> - Use the band from the firewall rule, allowing traffic between the tunnel endpoints.</li> <li>• <b>Copy Band From Payload To Envelope</b> - 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.</li> <li>• <b>Fixed Envelope Band</b> - Use a static band. From the <b>Envelope Band Value</b> list, select one of the available bands (<b>System, Band A to Band G</b>).</li> </ul>																											

<b>Replay Window Size</b>	<p>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 can 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.</p> <ul style="list-style-type: none"> <li>• To view or edit the global replay window size, see the <a href="#">VPN server settings</a>.</li> <li>• To view the replay window size for a tunnel, double-click the tunnel on the <a href="#">VPN Tab</a> to open the <b>Transport Details</b> window (attribute: transport_replayWindow).</li> </ul>
---------------------------	--

## Advanced

Setting	Description
<b>DPD Interval (s)</b>	Sets the time interval in seconds to perform Dead Peer Detection.
<b>VPN Next Hop Routing</b>	Enter the IP address of the remote VPN next hop interface. See <a href="#">How to Configure BGP Routing over IPsec VPN</a> for a configuration example.
<b>HW Accel.</b>	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: <ul style="list-style-type: none"> <li>• <b>Use Acceleration Card</b> - If a crypto accelerator hardware board is in use, select this option.</li> <li>• <b>Use CPU</b> - Use CPU acceleration.</li> </ul>
<b>Encaps. Mode Auto Detec.</b>	Automatically determines the IPsec encapsulation mode when NAT-T is used.
<b>Interface Index</b>	By default, the tunnel is fed through <b>vpn0</b> . To use another VPN interface, enter it in this field. Before using this option, you must first create the indexed VPN interface in the <a href="#">VPN server settings</a> .

## 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](http://www.openbsd.org/cgi-bin/man.cgi).

## Local Networks

Setting	Description
<b>Initiates Tunnel</b>	Specifies whether the tunnel is active or passive. You can select one of the following options: <ul style="list-style-type: none"> <li>• <b>Yes (passive IKE)</b></li> <li>• <b>No (active IKE)</b></li> </ul> <b>Active</b> also implies that incoming VPN connection attempts are accepted.
<b>Local IKE Gateway</b>	The IP address of the local IKE gateway. If you are using dynamic IP addresses, enter <code>0.0.0.0/0</code>

## 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
<b>Remote IKE Gateway</b>	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) hostname of the gateway.
<b>Network Address</b>	To add the network address of the VPN partner, enter it in this field and then click <b>Add</b> .

## 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](#).

© Barracuda Networks Inc., 2019 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.