IPsec IKEv1 Tunnel Settings

https://campus.barracuda.com/doc/73719169/

The following IKEv1 IPsec tunnel settings can be configured:

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.
IPv6	Enable to use IPv6 addresses for the VPN tunnel envelope

Basics

In 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. The Barracuda CloudGen Firewall supports **Group1** to **Group18**.
Lifetime [sec]	The re-keying time in seconds that the server offers to the partner.
Min. Lifetime [sec]	The minimum re-keying time in seconds that the server accepts from its partner.
Max. Lifetime [sec]	The maximum re-keying time in seconds that the server accepts from its partner.
Enable Perfect Forward Secrecy	Toggle to enable or disable PFS. The remote gateway mus also support PFS.

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 rulesets and specify bandwidth assignment to transports as a whole. Multiple transports can 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 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. Set to `-1` to disable Replay Protection. • 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** page to open the **Transport Details** window (attribute: transport_replayWindow).

Advanced

Setting	Description
DPD intervals [s]	Enter the number of seconds between sending IKE notify checks if the peer is still available. Default 5 sec.
HW Accel.	Specifies the preferred encryption engine. This allows for load balancing between the CPU and an optional cryptocard with more than one tunnel in use. You can select one of the following options: • **Use Acceleration Card – If a cryptographic 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 Settings.
VPN Next Hop Routing	Enter the IP address of the remote VPN tunnel interface that is reachable via the **vpnr** interface using the index entered as the **Interface Index**.
NAT-T Autodetect	Attempt to detect the UDP NAT-T type supported by the remote VPN gateway.

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)** **Active** also implies that incoming VPN connection attempts are accepted.
Local IKE Gateway	The IP address of the local IKE gateway. If you are using dynamic IP addresses, enter `0.0.0.0/0`
ID-type	• **IPV4_ADDR (auto)** – Automatically chosen IP address. • **IPV4_ADDR (explicit)** – Enter a single IP address. • **IPV4_ADDR_SUBNET (auto)** – Automatically chosen network. • **IPV4_ADDR_SUBNET (explicit)** – Explicit network. E.g., 62.99.0.0/24

Identify

Setting	Description
Identification Type	• **Shared Secret** • **X509 Certificate (CA signed)** • **X509 Certificate (explicit)** • **Box SCEP Certificate (CA signed)** X509 certificates must have the SubAltName field populated with at least one entry.
Mode	• **Main Mode** – By default, the firewall uses main mode. Main mode is considered more secure than aggressive mode. • **Aggressive Mode** – Aggressive mode is required if the remote IP address is unknown and shared key authentication is used.

Remote Networks

Setting	Description
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) hostname 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.

Setting	Description
Shared Secret	Enter the shared passphrase used to authenticate. Passphrases using the hash (#) character are not accepted.
CA Root	Select the root certificate used to validate the certificate.
X509 Condition	Enter the certificate key patterns the certificate is required to match when X.509 certificate authentication is used.
Explicit X509	Import an explicit certificate for X.509 certificate authentication. X509 certificates must have the SubAltName field populated with at least one entry.