

## IPsec Settings

<https://campus.barracuda.com/doc/17325/>

Navigate to the following window on path **CONFIGURATION > Configuration Tree > your box > Assigned Services > VPN Service > VPN Settings > IPsec.**

Use IPsec dynamic IPs

### IKEv1

Timeout	<input type="text" value="30"/>
Tunnel check interval [s]	<input type="text" value="5"/>
Dead Peer Detection Interval [s]	<input type="text" value="5"/>
IKEv1 Log Class	<input type="text" value="ALL"/>
IKEv1 Log Level	<input type="text" value="0"/>
Pre-shared key (PSK)	<input type="text"/>

### IKEv2

Start IKEv2	<input checked="" type="checkbox"/>
IKEv2 Make Before Break	<input type="checkbox"/>
IKEv2 Log Class	<input type="text" value="ALL"/>
IKEv2 Log Level	<input type="text" value="0"/>
IKEv2 Suppress Network Change Events	<input type="checkbox"/>

Setting	Value(s) *= default	Description
<b>Use IPsec dynamic IPs</b>	Selected Unselected*	Select the checkbox if the service is connected to the Internet via a dynamic link (dynamic IP address). The server IP address is not yet known at configuration time and IKE then listens to all local IP addresses.

### IKEv1

Setting	Value(s) *=default	Description
<b>Timeout</b>	30	The maximum period to wait until the request for IPsec tunnel connection establishment must be approved by the remote peer.

<b>Tunnel check interval [s]</b>	30	The interval between queries for a valid exchange that is assignable to an IPsec tunnel.
<b>Dead Peer Detection Interval [s]</b>	5	Tunnels can be configured to be <i>Active</i> or <i>Passive</i> . An active tunnel is capable of establishing a connection while a passive tunnel is waiting for a connection request. This parameter sets the interval between keep-alive checks on the remote peer.
<b>IKEv1 Log Class</b>	ALL*	The debug log class of IKEv2. Do not select a log class different than ALL if the log is not required for solving issues.
<b>IKEv1 Log Level</b>	0*	The debug log level of IKE. The debug log may be very “noisy.” Do not select a log level greater than 0 if the log is not required for solving an issue.
<b>Pre-shared key (PSK)</b>	-	Holds the pre-shared IKE key.

#### IKEv2

<b>Setting</b>	<b>Value(s) *=default</b>	<b>Description</b>
<b>Start IKEv2</b>	Selected* Deselected	If selected, IKEv2 will be used. If deselected, IKEv2 will be disabled and some additional memory will be saved.
<b>IKEv2 Make Before Break</b>	Selected Deselected	Selecting this option creates a duplicate of the IKE and all IPsec SAs, and the deletes the old ones. This setting requires that both peers can handle overlapping SAs.
<b>IKEv2 Log Class</b>	All*	The debug log class of IKEv2. Do not select a log class different than ALL if the log is not required for solving issues.
<b>IKEv2 Log Level</b>	0	The debug log level of IKEv2. Do not select a log level greater than 0 if the log is not required for solving an issue.
<b>IKEv2 Suppress Network Change Events</b>	Selected Deselected*	This is an advanced setting. If selected, network interface/address/route changes which may cause an automatic reconnect of the VPN tunnel will be ignored. This parameter becomes active after a restart of the IKEv2 daemon. Restart the VPN service or execute <code>ipsec restart</code> in a shell.

## Figures

1. vpn\_settings\_ipsec.png

© Barracuda Networks Inc., 2026 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.