Template:Networking rut9xx manual vpn ipsec

□

Contents

IPsec

To create a new IPsec instance, go to the *Services → VPN → IPsec* section, enter a custom name and click "Add". An IPsec instance with the given name will appear in the "IPsec Configuration" list.

To begin configuration, click the 'Edit' button located next to the instance.

IPsec configuration

The **IPsec configuration** section is used to configure the main parameters of an IPsec connection. Refer to the figure and table below for information on the configuration fields located in the general settings section.

Field	Value	Description
Enable	yes | no; default: **no**	Turns the IPsec instance on or off.
IKE version	IKEv1 | IKEv2; default: **IKEv1**	Internet Key Exchange (IKE) version used for key exchange. • **IKEv1** - more commonly used but contains known issues, for example, dealing with NAT. • **IKEv2** - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).

Mode	Main | Aggressive; default: **Main**	Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode. • **Main** - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages). • **Aggressive** - performs fewer exchanges than main mode (a total of 6 messages) by storing most data into the first exchange. In aggressive mode, the information is exchanged before there is a secure channel, making it less secure but faster than main mode.
Type	Tunnel | Transport; default: **Tunnel**	Type of connection. • **Tunnel** - protects internal routing information by encapsulating the entire IP packet (IP header and payload); commonly used in site-to-site VPN connections; supports NAT traversal. • **Transport** - only encapsulates IP payload data; used in client-to-site VPN connections; does not support NAT traversal; usually implemented with other tunneling protocols (for example, L2TP).
On startup	Ignore | Add | Route | Start; default: **Start**	Defines how the instance should act on router startup. • **Ignore** - does not start the tunnel. • **Add** - loads a connection without starting it. • **Route** - starts the tunnel only if there is traffic. • **Start** - starts the tunnel on router startup.
My identifier	ip | string; default: **none**	Defines how the user (IPsec instance) will be identified during authentication.
Tunnel: Local IP address/Subnet mask	ip/netmask | default: **none**	Local IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. If left empty, IP address will be selected automatically.
Left firewall	off | on; default: **on**	Adds neccessary firewall rules to allow traffic of this IPsec instance on this router.
Force encapsulation	yes | no; default: **no**	Forces UDP encapsulation for ESP packets even if a "no NAT" situation is detected.
Dead Peer Detection	yes | no; default: **no**	A function used during Internet Key Exchange (IKE) to detect a "dead" peer. It used to reduce traffic by minimizing the number of messages when the opposite peer in unavailable and as failover mechanism.
Dead Peer Detection: Delay (sec)	integer; default: **none**	The frequency of checking whether a peer is still availaible or not.
Dead Peer Detection: Timeout (sec)	integer; default: **none**	Time limit after which the IPsec instance will stop checking the availability of a peer and determine it to be "dead" if no response is received.
Authentification type	Pre-shared key | X.509; default: **Pre-shared key**	Here you can choose authentification type accordingly to your IPSec configuration
Certificate file	.crt file; default: **none**	Uploads a certificate file.
Key file	.key file; default: **none**	Uploads a key file.

CA certificate	.crt file; default: **none**	Uploads a Certificate authority (CA) file.
Remote participant's certificate	.crt file; default: **none**	Remote participant's certificate certificate is used to authenticate remote peer
Use additional xauth authentification	yes | no; default: **no**	Adds additional xauth authentification options.
Xauth: Xauth password	string; default: **none**	Password for additional peer authentification.
Remote VPN endpoint	host | ip; default: **none**	IP address or hostname of the remote IPsec instance.
Remote identifier	ip | string; default: **none**	Defines remote IPsec instance identification.
Tunnel: Remote IP address/subnet mask	ip/netmask; default: **none**	Remote network IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. This value must differ from the device's LAN IP.
Right firewall	yes | no; default: **yes**	Adds neccessary firewall rules to allow traffic of from the opposite IPsec instance on this router.
Transport: Use with DMVPN	yes | no; default: **no**	Adds several necessary options to make DMVPN work.
Passthrough networks	None | LAN | Wired | WiFi | Mobile | custom; default: **none**	Select networks which should be passthrough and excluded from routing through tunnel
Enable keepalive	yes | no; default: **no**	When enabled, the instance sends ICMP packets to the specified host at the specified frequency. If no response is received, the router will attempt to restart the connection.
Host	host | ip; default: **none**	Hostname or IP address to which keepalive ICMP packets will be sent to.
Ping period (sec)	integer [0..9999999]; default: **none**	The frequency at which keepalive ICMP packets will be sent to the specified host or IP address.
Allow WebUI access	yes | no; default: **no**	Allows WebUI access for hosts in the VPN network.
Custom options	ipsec options; default: **none**	Provides the possibility to further customize the connection by adding extra IPsec options.

Additional notes:

- Some configuration fields become available only when certain other parameters are selected. Different color codes are used for different parameters:
  - Orange for Type: Xauth
  - Red for Type: Tunnel
  - Purple for Type: Transport
  - Blue for Dead Peer Detection: Enabled
- After changing any of the parameters, don't forget to click the **Save** button located at the bottom-right side of the page.

Phase settings

IKE (Internet Key Exchange) is a protocol used to set up security associations (SAs) for the IPsec connection. This process is required before the IPsec tunnel can be established. It is done in two phases:

Phase	Mode	
Phase 1 • Establishes a secure channel between peers • Authenticates peers • Negotiates SA policy • Shares secret keys • Establishes secure tunnel for phase 2 **Phase 2** • Sets up matching IPsec SAs • Periodically renegotiates IPsec SAs	Main mode (figure 1) • 6 packets exchanged • Identity protected during exchange Quick mode • 3 packets exchanged • IPsec SA parameters (ESP/AH, SHA/MD5) established • SA lifetime set	Aggressive mode (figure 2) • 3 packets exchanged • Identity information exchanged before a secure channel is established

Figure 1
[[File:{{{file_ipsec_main_mode}}}]]

Figure 2
[[File:{{{file_ipsec_aggressive_mode}}}]]

[[File:{{{file_ipsec_phase}}}]]

Field	Value	Description
Encryption algorithm	DES | 3DES | AES128 | AES192 | AES256; default: **3DES**	Algorithm used for data encryption.
Authentication/Hash algorithm	MD5 | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	Algorithm used for exchanging authentication and hash information.
DH group/PFS group	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096; default: **MODP1536**	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key.
Lifetime	integer; default: **8 hours**	Defines a time period after which the phase will re-initiate its exchange of information.

Pre-shared keys

A **pre-shared key** is a secret password used for authentication between IPsec peers before a secure tunnel is established. During authentication device will try to check if connection matches any **Secret's ID selector** and then the **pre-shared key** from the first match will be used.

To create a new key, click the 'Add' button.

The figure below is an example of the Pre-shared keys section and the table below provides information on configuration fields contained in that section:

[[File:{{{file_ipsec_psk}}}]]

Field	Value	Description
Pre-shared key	string; default: **none**	A shared password used for authentication between IPsec peers before a secure channel is established.

Secret's ID selector	string; default: **none**	Each secret can be preceded by a list of optional ID selectors. A selector is an IP address, a Fully Qualified Domain Name, user@FQDN or %any. **NOTE**: IKEv1 only supports IP address ID selector.