

IPsec VPN—secret key

IPsec VPN Configuration
Openswan version U2.6.23/K

Existing VPN connections

Global options and policies

Start IPsec Server

Start at boot time Yes No

- Webmin Module is put Networking-> IPsec VPN configuration
- Before configuring server, must configure encryption key first

IPsec VPN—secret key

Module Index

Secret Keys

Secret for	Type	Details
Any host	RSA public key	Modulus 0x5b16b41e464fd8bfe3...

Create new shared secret key. Create new RSA key.

Return to connections list

Module Index

Edit Secret Key

Secret key details

Secret key is for Any host Hosts

Key type Shared secret RSA public key

Shared password

Save Delete

Return to secret key list | Return to connections list

- Share secret key is the most easy way for build up a VPN

Configuring IPsec VPN

Help. Module Config Search Docs.

IPsec VPN Configuration
Openswan version U2.6.23/K

Existing VPN connections

Defaults for all connections Connection host-to-host Connection net-to-net

Add a new IPsec VPN connection. Import connection from file.

Global options and policies

Server Configuration Show Public Key Secret Keys Blocked Networks
Clear Traffic Networks Encrypted or Clear Networks Clear or Encrypted Networks Encrypted Networks

Start IPsec Server Click this button to start the FreeSWAN IPsec server process. Until it is started your system will be unable to accept or establish connections.

Start at boot time Yes No Change this option to control whether the IPsec server is started at boot time or not.

Configuring IPsec VPN

IPsec VPN connection details

Connection name	Host-to-Net	At IPsec startup	Start connection
Compress data?	<input checked="" type="radio"/> Default (usually No) <input type="radio"/> Yes <input type="radio"/> No	Connection type	Tunnel (host or network)
Authentication method	Shared secret	Perfect forwarding secrecy?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default (usually Yes)
Authentication mode	ESP	Keying re-tries	<input checked="" type="radio"/> Default <input type="radio"/> []
ESP algorithm	MD5	Accept this ESP algorithm only?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Connection key lifetime	<input checked="" type="radio"/> Default <input type="radio"/> [] secs	Keying channel lifetime	<input checked="" type="radio"/> Default <input type="radio"/> [] secs

- **Authentication method:** Shared secret
- **At IPsec startup:** start connection
- All the configuration should be recorded.

Configuring IPsec VPN

Local or left system's settings

Public IP address From default route Automatic Automatic from DNS Address or hostname .. 192.168.10.1

System identifier Default IP address .. Hostname .. 192.168.10.1

Private subnet behind system None 192.168.20.1/24

System's public key None Lookup in DNS Entered below ..

Next hop to other system Default Automatic Default route IP address ..

Certificate name None

- **Public IP address/system identifier** is IP address of VPN interface (normally WAN)
- If it is an VPN route and another site want to access the internal network, **Private subnet behind system** should be configured.

Configuring IPsec VPN

Remote or right system's settings

Public IP address From default route Automatic Automatic from DNS Address or hostname .. 192.168.10.121

System identifier Default IP address .. Hostname .. 192.168.10.121

Private subnet behind system None

System's public key None Lookup in DNS Entered below ..

Next hop to other system Default Automatic Default route IP address ..

Certificate name None

Save Export Configuration .. Delete

- **Public IP address/system identifier** is the IP address of remote VPN client.

Active IPsec VPN

Existing VPN connections



Add a new IPsec VPN connection. Import connection from file.

Global options and policies



Click this button to start the FreeSWAN IPsec server process. Until it is started your system will be unable to accept or establish connections.

Yes No Change this option to control whether the IPsec server is started at boot time or not.

- If **At IPsec start** is chosen as add connection, user has to manually active the connection settings.