|  |
| --- |
| **IPsec**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#ipsec) |

|  |
| --- |
| GRE, GRE/IPsec (or IPIP/IPsec, SIT/IPsec, or any other stateless tunnel protocol over |

|  |
| --- |
| IPsec) is the usual way to protect the traffic inside a tunnel. |

|  |
| --- |
| An advantage of this scheme is that you get a real interface with its own address, which |

makes it easier to setup static routes or use dynamic routing protocols without having to modify IPsec policies. The other advantage is that it greatly simplifies router to router communication, which can be tricky with plain IPsec because the external outgoing address of the router usually doesn’t match the IPsec policy of typical site-to-site setup and you need to add special configuration for it, or adjust the source address for outgoing traffic of your applications. GRE/IPsec has no such problem and is completely

|  |
| --- |
| transparent for the applications. |

|  |
| --- |
| GRE/IPIP/SIT and IPsec are widely accepted standards, which make this scheme easy to |

|  |
| --- |
| implement between VyOS and virtually any other router. |

|  |
| --- |
| For simplicity we’ll assume that the protocol is GRE, it’s not hard to guess what needs to |

be changed to make it work with a different protocol. We assume that IPsec will use pre-shared secret authentication and will use AES128/SHA1 for the cipher and hash. Adjust this as necessary.

|  |
| --- |
| **Note** |

|  |
| --- |
| VMware users should ensure that a VMXNET3 adapter is used. E1000 adapters have |

|  |
| --- |
| known issues with GRE processing. |

**IKE (Internet Key Exchange) Attributes**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#ike-internet-key-exchange-attributes)

IKE performs mutual authentication between two parties and establishes an IKE security

association (SA) that includes shared secret information that can be used to efficiently establish

SAs for Encapsulating Security Payload (ESP) or Authentication Header (AH) and a set of

cryptographic algorithms to be used by the SAs to protect the traffic that they

carry. <https://datatracker.ietf.org/doc/html/rfc5996>

In VyOS, IKE attributes are specified through IKE groups. Multiple proposals can be specified

in a single group.

VyOS IKE group has the next options:

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   close-action defines the action to take if the remote peer unexpectedly closes a |

CHILD\_SA:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|     | |  | | --- | |  |   none set action to none (default);   |  | | --- | |  |   hold set action to hold;   |  | | --- | |  |   restart set action to restart;   |  | | --- | |  |   dead-peer-detection controls the use of the Dead Peer Detection protocol (DPD, RFC |

3706) where R\_U\_THERE notification messages (IKEv1) or empty

INFORMATIONAL messages (IKEv2) are periodically sent in order to check the

liveliness of the IPsec peer:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|        | |  | | --- | |  |   action keep-alive failure action:   |  | | --- | |  |   hold set action to hold (default)   |  | | --- | |  |   clear set action to clear;   |  | | --- | |  |   restart set action to restart;   |  | | --- | |  |   interval keep-alive interval in seconds <2-86400> (default 30);   |  | | --- | |  |   timeout keep-alive timeout in seconds <2-86400> (default 120) IKEv1 only   |  | | --- | |  |   ikev2-reauth whether rekeying of an IKE\_SA should also reauthenticate the peer. In |

IKEv1, reauthentication is always done. Setting this parameter enables remote host

re-authentication during an IKE rekey.

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   key-exchange which protocol should be used to initialize the connection If not set |

both protocols are handled and connections will use IKEv2 when initiating, but

accept any protocol version when responding:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|     | |  | | --- | |  |   ikev1 use IKEv1 for Key Exchange;   |  | | --- | |  |   ikev2 use IKEv2 for Key Exchange;   |  | | --- | |  |   lifetime IKE lifetime in seconds <0-86400> (default 28800);   |  | | --- | |  |   disable-mobike disables MOBIKE Support. MOBIKE is only available for IKEv2 and |

enabled by default.

|  |  |  |  |
| --- | --- | --- | --- |
|   | |  | | --- | |  |   mode IKEv1 Phase 1 Mode Selection:   |  | | --- | |  |   main use Main mode for Key Exchanges in the IKEv1 Protocol (Recommended |

Default);

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   aggressive use Aggressive mode for Key Exchanges in the IKEv1 protocol aggressive |

mode is much more insecure compared to Main mode;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|    | |  | | --- | |  |   proposal the list of proposals and their parameters:   |  | | --- | |  |   dh-group dh-group;   |  | | --- | |  |   encryption encryption algorithm; |

|  |  |  |
| --- | --- | --- |
|   | |  | | --- | |  |   hash hash algorithm.  prf pseudo-random function. |

**ESP (Encapsulating Security Payload) Attributes**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#esp-encapsulating-security-payload-attributes)

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an

anti-replay service (a form of partial sequence integrity), and limited traffic flow

confidentiality. <https://datatracker.ietf.org/doc/html/rfc4303>

In VyOS, ESP attributes are specified through ESP groups. Multiple proposals can be specified

in a single group.

VyOS ESP group has the next options:

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   compression Enables the IPComp(IP Payload Compression) protocol which allows |

compressing the content of IP packets.

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   life-bytes ESP life in bytes <1024-26843545600000>. Number of bytes transmitted |

over an IPsec SA before it expires;

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   life-packets ESP life in packets <1000-26843545600000>. Number of packets |

transmitted over an IPsec SA before it expires;

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   lifetime ESP lifetime in seconds <30-86400> (default 3600). How long a particular |

instance of a connection (a set of encryption/authentication keys for user packets)

should last, from successful negotiation to expiry;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|     | |  | | --- | |  |   mode the type of the connection:   |  | | --- | |  |   tunnel tunnel mode (default);   |  | | --- | |  |   transport transport mode;   |  | | --- | |  |   pfs whether Perfect Forward Secrecy of keys is desired on the connection’s keying |

channel and defines a Diffie-Hellman group for PFS:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|       | |  | | --- | |  |   enable Inherit Diffie-Hellman group from IKE group (default);   |  | | --- | |  |   disable Disable PFS;   |  | | --- | |  |   < dh-group > defines a Diffie-Hellman group for PFS;   |  | | --- | |  |   proposal ESP-group proposal with number <1-65535>:   |  | | --- | |  |   encryption encryption algorithm (default 128 bit AES-CBC);  hash hash algorithm (default sha1). |

**Options (Global IPsec settings) Attributes**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#options-global-ipsec-settings-attributes)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|    | |  | | --- | | options |  |  | | --- | |  |   disable-route-autoinstall Do not automatically install routes to remote networks;   |  | | --- | |  |   flexvpn Allows FlexVPN vendor ID payload (IKEv2 only). Send the Cisco FlexVPN |

vendor ID payload (IKEv2 only), which is required in order to make Cisco brand devices allow negotiating a local traffic selector (from strongSwan’s point of view) that is not the assigned virtual IP address if such an address is requested by   
strongSwan. Sending the Cisco FlexVPN vendor ID prevents the peer from narrowing the initiator’s local traffic selector and allows it to e.g. negotiate a TS of 0.0.0.0/0 == 0.0.0.0/0 instead. This has been tested with a “tunnel mode ipsec ipv4” Cisco template but should also work for GRE encapsulation;

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   interface Interface Name to use. The name of the interface on which virtual IP |

addresses should be installed. If not specified the addresses will be installed on the outbound interface;

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | |  |   virtual-ip Allows to install virtual-ip addresses. Comma separated list of virtual IPs to |

request in IKEv2 configuration payloads or IKEv1 Mode Config. The wildcard addresses 0.0.0.0 and :: request an arbitrary address, specific addresses may be defined. The responder may return a different address, though, or none at all. Define the virtual-address option to configure the IP address in site-to-site hierarchy.

**IPsec policy matching GRE**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#ipsec-policy-matching-gre)

The first and arguably cleaner option is to make your IPsec policy match GRE packets between external addresses of your routers. This is the best option if both routers have static external addresses.

Suppose the LEFT router has external address 192.0.2.10 on its eth0 interface, and the RIGHT router is 203.0.113.45

On the LEFT:

|  |
| --- |
| # GRE tunnel  set interfaces tunnel tun0 encapsulation gre  set interfaces tunnel tun0 source-address 192.0.2.10 set interfaces tunnel tun0 remote 203.0.113.45  set interfaces tunnel tun0 address 10.10.10.1/30 |

|  |
| --- |
| ## IPsec  set vpn ipsec interface eth0 |

|  |
| --- |
| # Pre-shared-secret  set vpn ipsec authentication psk vyos id 192.0.2.10 |

|  |
| --- |
| set vpn ipsec authentication psk vyos id 203.0.113.45 set vpn ipsec authentication psk vyos secret MYSECRETKEY |

|  |
| --- |
| # IKE group  set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group '2'  set vpn ipsec ike-group MyIKEGroup proposal 1 encryption 'aes128' set vpn ipsec ike-group MyIKEGroup proposal 1 hash 'sha1' |

|  |
| --- |
| # ESP group  set vpn ipsec esp-group MyESPGroup proposal 1 encryption 'aes128' set vpn ipsec esp-group MyESPGroup proposal 1 hash 'sha1' |

|  |
| --- |
| # IPsec tunnel  set vpn ipsec site-to-site peer right authentication mode pre-shared-secret set vpn ipsec site-to-site peer right authentication remote-id 203.0.113.45 |

|  |
| --- |
| set vpn ipsec site-to-site peer right ike-group MyIKEGroup  set vpn ipsec site-to-site peer right default-esp-group MyESPGroup |

|  |
| --- |
| set vpn ipsec site-to-site peer right local-address 192.0.2.10 set vpn ipsec site-to-site peer right remote-address 203.0.113.45 |

|  |
| --- |
| # This will match all GRE traffic to the peer  set vpn ipsec site-to-site peer right tunnel 1 protocol gre |

On the RIGHT, setup by analogy and swap local and remote addresses.

**Source tunnel from loopbacks**[](https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html#source-tunnel-from-loopbacks)

The scheme above doesn’t work when one of the routers has a dynamic external address though. The classic workaround for this is to setup an address on a loopback interface and use it as a source address for the GRE tunnel, then setup an IPsec policy to match those loopback   
addresses.

We assume that the LEFT router has static 192.0.2.10 address on eth0, and the RIGHT router has a dynamic address on eth0.

The peer names RIGHT and LEFT are used as informational text.

**Setting up the GRE tunnel**

On the LEFT:

|  |
| --- |
| set interfaces loopback lo address 192.168.99.1/32 |

|  |
| --- |
| set interfaces tunnel tun0 encapsulation gre  set interfaces tunnel tun0 address 10.10.10.1/30  set interfaces tunnel tun0 source-address 192.168.99.1 set interfaces tunnel tun0 remote 192.168.99.2 |

On the RIGHT:

|  |
| --- |
| set interfaces loopback lo address 192.168.99.2/32 |

|  |
| --- |
| set interfaces tunnel tun0 encapsulation gre  set interfaces tunnel tun0 address 10.10.10.2/30  set interfaces tunnel tun0 source-address 192.168.99.2 set interfaces tunnel tun0 remote 192.168.99.1 |

**Setting up IPSec**

However, now you need to make IPsec work with dynamic address on one side. The tricky part is that pre-shared secret authentication doesn’t work with dynamic address, so we’ll have to use RSA keys.

First, on both routers run the operational command “generate pki key-pair install <key-pair name>”. You may choose different length than 2048 of course.

|  |
| --- |
| vyos@left# run generate pki key-pair install ipsec-LEFT  Enter private key type: [rsa, dsa, ec] (Default: rsa)  Enter private key bits: (Default: 2048)  Note: If you plan to use the generated key on this router, do not encrypt the private key.  Do you want to encrypt the private key with a passphrase? [y/N] N Configure mode commands to install key pair:  Do you want to install the public key? [Y/n] Y  set pki key-pair ipsec-LEFT public key 'MIIBIjANBgkqh...'  Do you want to install the private key? [Y/n] Y  set pki key-pair ipsec-LEFT private key 'MIIEvgIBADAN...'  [edit] |

Configuration commands for the private and public key will be displayed on the screen which needs to be set on the router first. Note the command with the public key (set pki key-pair ipsec-LEFT public key ‘MIIBIjANBgkqh…’). Then do the same on the opposite router:

|  |
| --- |
| vyos@left# run generate pki key-pair install ipsec-RIGHT |

Note the command with the public key (set pki key-pair ipsec-RIGHT public key ‘FAAOCAQ8AMII…’).

Now the noted public keys should be entered on the opposite routers.

On the LEFT:

|  |
| --- |
| set pki key-pair ipsec-RIGHT public key 'FAAOCAQ8AMII...' |

On the RIGHT:

|  |
| --- |
| set pki key-pair ipsec-LEFT public key 'MIIBIjANBgkqh...' |

Now you are ready to setup IPsec. You’ll need to use an ID instead of address for the peer.

On the LEFT (static address):

set vpn ipsec interface eth0

|  |
| --- |
| set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128 set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2  set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128 set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec site-to-site peer RIGHT authentication local-id LEFT  set vpn ipsec site-to-site peer RIGHT authentication mode rsa  set vpn ipsec site-to-site peer RIGHT authentication rsa local-key ipsec-LEFT  set vpn ipsec site-to-site peer RIGHT authentication rsa remote-key ipsec-RIGHT  set vpn ipsec site-to-site peer RIGHT authentication remote-id RIGHT  set vpn ipsec site-to-site peer RIGHT default-esp-group MyESPGroup  set vpn ipsec site-to-site peer RIGHT ike-group MyIKEGroup  set vpn ipsec site-to-site peer RIGHT local-address 192.0.2.10  set vpn ipsec site-to-site peer RIGHT connection-type respond  set vpn ipsec site-to-site peer RIGHT tunnel 1 local prefix 192.168.99.1/32 # Additional loopback address on the local  set vpn ipsec site-to-site peer RIGHT tunnel 1 remote prefix 192.168.99.2/32 # Additional loopback address on the remote |

On the RIGHT (dynamic address):

set vpn ipsec interface eth0

|  |
| --- |
| set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128 set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2  set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128 set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec site-to-site peer LEFT authentication local-id RIGHT  set vpn ipsec site-to-site peer LEFT authentication mode rsa  set vpn ipsec site-to-site peer LEFT authentication rsa local-key ipsec-RIGHT  set vpn ipsec site-to-site peer LEFT authentication rsa remote-key ipsec-LEFT  set vpn ipsec site-to-site peer LEFT authentication remote-id LEFT  set vpn ipsec site-to-site peer LEFT connection-type initiate  set vpn ipsec site-to-site peer LEFT default-esp-group MyESPGroup  set vpn ipsec site-to-site peer LEFT ike-group MyIKEGroup  set vpn ipsec site-to-site peer LEFT local-address any  set vpn ipsec site-to-site peer LEFT remote-address 192.0.2.10  set vpn ipsec site-to-site peer LEFT tunnel 1 local prefix 192.168.99.2/32 # Additional loopback address on the local  set vpn ipsec site-to-site peer LEFT tunnel 1 remote prefix 192.168.99.1/32 # Additional loopback address on the remote |