# IPsec over PPPoE

Oleksandr Fedorov - 2021-08-20 - 0 Comments - in IPSec

IPsec (IP Security) is an IETF (Internet Engineering Task Force) standard suite of protocols between two communication points across the IP network that provides data authentication, integrity and confidentiality. It defines TCP/IP packet encryption, decryption and authentication. IPsec is a widely accepted standard, which makes it easy to setup between VyOS and virtually any other router. Let's review simple setup. We assume that IPsec will be using pre-shared secret authentication and AES256 and SHA1 for the cipher and the hash respectively. Adjust this as necessary.

First, we need to create and setup ESP (Encapsulating Security Payload) and IKE (Internet Key Exchange) groups in IPSec profile

```
set vpn ipsec esp-group example-esp compression 'disable'
set vpn ipsec esp-group example-esp lifetime '1800'
set vpn ipsec esp-group example-esp mode 'tunnel'
set vpn ipsec esp-group example-esp pfs 'enable'
set vpn ipsec esp-group example-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group example-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group example-ike ikev2-reauth 'no'
set vpn ipsec ike-group example-ike key-exchange 'ikev1'
set vpn ipsec ike-group example-ike lifetime '3600'
set vpn ipsec ike-group example-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group example-ike proposal 1 hash 'sha1'
```

We see here that IP payload compression is disabled and the lifetime is 1800 seconds. IPSec is in "tunnel" mode with the PFS (Perfect Forward Secrecy) feature enabled.

Next we see IKE and ESP types of encryption and hash. The lifetime of IKE means that the key comparison keep-alive time is 3600 seconds and after that it has to renew.

Finally, the key exchange here would be via the IKEv1 mode and reauthorization via IKEv2 is denied.

Now we need to specify which interface should be used for IPsec.

```
set vpn ipsec ipsec-interfaces interface 'eth1'
```

It's time to setup the peer address. We need to specify the destination router's IP address and the authentication type. It can be pre-shared key (PSK) or certificate-based authentication. In this example, we will use pre-shared key.

```
set vpn ipsec site-to-site peer 203.0.113.2 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 203.0.113.2 authentication pre-shared-secret 'SomePreSharedKey'
```

Next we specify which group will be used for exchanging keys and the local IP address of the source router.

```
set vpn ipsec site-to-site peer 203.0.113.2 ike-group 'example-ike'
set vpn ipsec site-to-site peer 203.0.113.2 local-address '198.51.100.3'
```

Last step — configuration of the tunnel, its properties and the encapsulation group. The local prefix means that LAN should have access to the peer LAN (remote prefix).

```
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 esp-group 'example-esp'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 local prefix '192.168.0.0/24'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 remote prefix '10.0.0.0/21'
```

Let's look at the second router. IKE and ESP configuration remains the same.

```
set vpn ipsec esp-group example-esp compression 'disable'
set vpn ipsec esp-group example-esp lifetime '1800'
set vpn ipsec esp-group example-esp mode 'tunnel'
set vpn ipsec esp-group example-esp pfs 'enable'
set vpn ipsec esp-group example-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group example-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group example-ike ikev2-reauth 'no'
set vpn ipsec ike-group example-ike key-exchange 'ikev1'
set vpn ipsec ike-group example-ike lifetime '3600'
set vpn ipsec ike-group example-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group example-ike proposal 1 hash 'sha1'
```

Peer configuration has to be setup vice versa. Now the destination peer is the IP address of the first router.

```
set vpn ipsec site-to-site peer 198.51.100.3 authentication mode
'pre-shared-secret'
set vpn ipsec site-to-site peer 198.51.100.3 authentication pre-
shared-secret 'SomePreSharedKey'
set vpn ipsec site-to-site peer 198.51.100.3 ike-group 'example-ike'
set vpn ipsec site-to-site peer 198.51.100.3 local-address
'203.0.113.2'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-nat-
networks 'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-public-
networks 'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 esp-group
'example-esp'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 local prefix
'10.0.0.0/21'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 remote prefix
'192.168.0.0/24'
```

This configuration looks fine. But what if one of the routers has a PPPoE connection? In this case, it doesn't have a constant IP address. The solution is to give this router an ID.

```
set vpn ipsec ipsec-interfaces interface 'pppoe0'
set vpn ipsec site-to-site peer 203.0.113.2 authentication id @Test
set vpn ipsec site-to-site peer 203.0.113.2 authentication mode 'pre-
shared-secret'
set vpn ipsec site-to-site peer 203.0.113.2 authentication pre-
shared-secret 'SomePreSharedKey'
set vpn ipsec site-to-site peer 203.0.113.2 ike-group 'example-ike'
set vpn ipsec site-to-site peer 203.0.113.2 connection-type initiate
set vpn ipsec site-to-site peer 203.0.113.2 local-address any
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-nat-
networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-public-
networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 esp-group
'example-esp'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 local prefix
'192.168.0.0/24'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 remote prefix
'10.0.0.0/21'
```

Note that the outbound interface is 'pppoe0' now. Also, as you can see here, it has the connection type of 'initiate' now. The destination side has the 'respond' type. As the router

doesn't have a constant IP address, we're specifying that so that the address can be local.

On the destination side the configuration looks like this:

```
set vpn ipsec site-to-site peer @Test authentication mode 'pre-
shared-secret'
set vpn ipsec site-to-site peer @Test authentication pre-shared-
secret 'SomePreSharedKey'
set vpn ipsec site-to-site peer @Test ike-group 'example-ike'
set vpn ipsec site-to-site peer @Test connection-type respond
set vpn ipsec site-to-site peer @Test authentication remote-id @Test
set vpn ipsec site-to-site peer @Test local-address '203.0.113.2'
set vpn ipsec site-to-site peer @Test tunnel 0 allow-nat-networks
'disable'
set vpn ipsec site-to-site peer @Test tunnel 0 allow-public-networks
'disable'
set vpn ipsec site-to-site peer @Test tunnel 0 esp-group 'example-
esp'
set vpn ipsec site-to-site peer @Test tunnel 0 local prefix
'10.0.0.0/21'
set vpn ipsec site-to-site peer @Test tunnel 0 remote prefix
'192.168.0.0/24'
```

Now the second router is connecting to the ID we assigned to the first router.