IPsec Site-to-Site VPN

Yuriy Andamasov - 2018-10-13 - 0 Comments - in IPSec

Introduction

In addition to being used with other protocols (such as L2TP) in a server-client VPN setup, another common use for IPsec is the creation of site-to-site VPNs.

Basic Configuration

For this example, we'll be using the following two network topologies:

For `central-office-net`:

- Public address of `203.0.113.2` on interface `eth1`
- Local private network of `10.1.1.0/24`
- A VyOS router called `central-office-rtr`

For `remote-office-net`:

- Public address of `192.51.100.2` on interface `eth1`
- Local private network of `10.2.2.0/24`
- A VyOS router called `remote-office-rtr`

For simplicity, we will be using pre-shared secret authentication for IPsec, although one may also use an RSA key or X.509 certificates, depending on existing infrastructure. The pre-shared key will be `not-so-secret`.

Note: These configurations are run from the `vpn ipsec` tree. The `edit vpn ipsec` is issued in the first line to change the current configuration path. It is displayed as `[edit vpn ipsec]` in the command line, and as a comment here (prefixed by `#`).

Configuration of central-office-rtr:

```
edit vpn ipsec
#[edit vpn ipsec]
set esp-group central-rtr-esp compression 'disable'
set esp-group central-rtr-esp lifetime '1800'
set esp-group central-rtr-esp mode 'tunnel'
set esp-group central-rtr-esp pfs 'enable'
set esp-group central-rtr-esp proposal 1 encryption 'aes256'
set esp-group central-rtr-esp proposal 1 hash 'sha256'
```

```
set ike-group central-rtr-ike ikev2-reauth 'no'
set ike-group central-rtr-ike key-exchange 'ikev1'
set ike-group central-rtr-ike lifetime '3600'
set ike-group central-rtr-ike proposal 1 encryption 'aes256'
set ike-group central-rtr-ike proposal 1 hash 'sha256'
set ipsec-interfaces interface 'eth1'
set site-to-site peer 192.51.100.2 authentication mode 'pre-shared-
secret'
set site-to-site peer 192.51.100.2 authentication pre-shared-secret
'not-so-secret'
set site-to-site peer 192.51.100.2 ike-group 'central-rtr-ike'
set site-to-site peer 192.51.100.2 local-address '203.0.113.2'
set site-to-site peer 192.51.100.2 tunnel 0 allow-nat-networks
'disable'
set site-to-site peer 192.51.100.2 tunnel 0 allow-public-networks
'disable'
set site-to-site peer 192.15.100.2 tunnel 0 esp-group 'central-rtr-
esp'
set site-to-site peer 192.51.100.2 tunnel 0 local prefix
'10.1.1.0/24'
set site-to-site peer 192.51.100.2 tunnel 0 remote prefix
'10.2.2.0/24'
```

Configuration of remote-office-rtr:

```
edit vpn ipsec
#[edit vpn ipsec]
set esp-group remote-rtr-esp compression 'disable'
set esp-group remote-rtr-esp lifetime '1800'
set esp-group remote-rtr-esp mode 'tunnel'
set esp-group remote-rtr-esp pfs 'enable'
set esp-group remote-rtr-esp proposal 1 encryption 'aes256'
set esp-group remote-rtr-esp proposal 1 hash 'sha256'
set ike-group remote-rtr-ike ikev2-reauth 'no'
set ike-group remote-rtr-ike key-exchange 'ikev1'
set ike-group remote-rtr-ike lifetime '3600'
set ike-group remote-rtr-ike proposal 1 encryption 'aes256'
set ike-group remote-rtr-ike proposal 1 hash 'sha256'
set ipsec-interfaces interface 'eth1'
set site-to-site peer 203.0.113.2 authentication mode 'pre-shared-
secret'
set site-to-site peer 203.0.113.2 authentication pre-shared-secret
```

```
'not-so-secret'
set site-to-site peer 203.0.113.2 ike-group 'remote-rtr-ike'
set site-to-site peer 203.0.113.2 local-address '192.51.100.2'
set site-to-site peer 203.0.113.2 tunnel 0 allow-nat-networks
'disable'
set site-to-site peer 203.0.113.2 tunnel 0 allow-public-networks
'disable'
set site-to-site peer 203.0.113.2 tunnel 0 esp-group 'remote-rtr-esp'
set site-to-site peer 203.0.113.2 tunnel 0 local prefix '10.2.2.0/24'
set site-to-site peer 203.0.113.2 tunnel 0 remote prefix
'10.1.1.0/24'
```

At this point, there should be a working tunnel between `central-office-net` and `remote-office-net`. This can be verified on each router:

```
vyos@central-office-rtr:~$ show vpn ipsec sa #show security
associations
Peer ID / IP                            Local ID / IP
------------                            -------------
192.51.100.2                            203.0.113.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-
Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ---
---  -----
    0       up     0.0/0.0        aes256   sha256  no     1145
1800    all

vyos@central-office-rtr:~$ show vpn ipsec status #show status of
IPsec tunnels/process
IPSec Process Running PID: 4058

1 Active IPsec Tunnels

IPsec Interfaces :
        eth1    (203.0.113.2)

vyos@central-office-rtr:~$ show vpn ipsec state #not displayed, but
shows the in-kernel crypto state.
```

The same commands may be performed on `remote-office-rtr` as well.

Additional Configuration

SNAT

If you have source NAT rules on the outbound interface, exceptions need to be added on each router:

```
edit nat source rule 10
# [edit nat source rule 10]
set destination address 10.2.2.0/24
set exclude
set outbound-interface eth1
set source address 10.1.1.0/24
```

And similarly for `remote-office-rtr`:

```
edit nat source rule 10
# [edit nat source rule 10]
set destination address 10.1.1.0/24
set exclude
set outbound-interface eth1
set source address 10.2.2.0/24
```

Firewall Rules

If either or both router has existing firewall rules that prevent non-local LAN traffic from being sent/accepted, the appropriate firewall exceptions need to be made on each router for the other network, for example:

For `central-office-rtr`:

```
set firewall name REMOTE-LOCAL rule 32 action accept
set firewall name REMOTE-LOCAL rule 32 source address 10.2.2.0/24
```

and `remote-office-rtr`:

```
set firewall name CENTRAL-LOCAL rule 32 action accept
set firewall name CENTRAL-LOCAL rule 32 source address 10.1.1.0/24
```