How to: Get up and running with VyOS 1.4 with IPsec and GRE

Erfi Anugrah

2024-05-24

Table of contents

0.1 Firewall

0.1.1 Global Options

```
set firewall global-options all-ping 'enable'
set firewall global-options broadcast-ping 'disable'
set firewall global-options ip-src-route 'disable'
set firewall global-options ipv6-receive-redirects 'disable'
set firewall global-options ipv6-src-route 'disable'
set firewall global-options log-martians 'enable'
set firewall global-options receive-redirects 'disable'
set firewall global-options send-redirects 'enable'
set firewall global-options source-validation 'disable'
set firewall global-options syn-cookies 'enable'
```

0.1.2 Network Groups

In this case, I used Cloudflare's IP Ranges:

```
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/29'
set firewall group ipv6-network-group cf-ipv6 network 'xxxx:xxxx::/32'
set firewall group network-group cf-ipv4 network 'xxx.xxx.48.0/20'
set firewall group network-group cf-ipv4 network 'xxx.xxx.244.0/22'
set firewall group network-group cf-ipv4 network 'xxx.xxx.200.0/22'
set firewall group network-group cf-ipv4 network 'xxx.xxx.4.0/22'
set firewall group network-group cf-ipv4 network 'xxx.xxx.64.0/18'
set firewall group network-group cf-ipv4 network 'xxx.xxx.192.0/18'
set firewall group network-group cf-ipv4 network 'xxx.xxx.240.0/20'
set firewall group network-group cf-ipv4 network 'xxx.xxx.96.0/20'
set firewall group network-group cf-ipv4 network 'xxx.xxx.240.0/22'
set firewall group network-group cf-ipv4 network 'xxx.xxx.128.0/17'
set firewall group network-group cf-ipv4 network 'xxx.xxx.0.0/15'
set firewall group network-group cf-ipv4 network 'xxx.xxx.0.0/13'
set firewall group network-group cf-ipv4 network 'xxx.xxx.0.0/14'
set firewall group network-group cf-ipv4 network 'xxx.xxx.0.0/13'
set firewall group network-group cf-ipv4 network 'xxx.xxx.72.0/22'
```

0.1.3 Jump Filters

This is based on the Netfilter project.

Input filter is for the WAN, destination being the router which is on the prerouting stage. Forward filter is for the inbound-interfaces, which is into the postrouting and egress stages.

```
set firewall ipv4 forward filter default-action 'accept'
set firewall ipv4 forward filter rule 5 action 'jump'
set firewall ipv4 forward filter rule 5 inbound-interface name 'pppoe0'
set firewall ipv4 forward filter rule 5 jump-target 'EXTERNAL-IN'
set firewall ipv4 forward filter rule 10 action 'jump'
set firewall ipv4 forward filter rule 10 inbound-interface name 'eth1'
set firewall ipv4 forward filter rule 10 jump-target 'INTERNAL1'
set firewall ipv4 forward filter rule 20 action 'jump'
set firewall ipv4 forward filter rule 20 inbound-interface name 'eth1'
set firewall ipv4 forward filter rule 20 jump-target 'INTERNAL2'
set firewall ipv4 input filter default-action 'accept'
set firewall ipv4 input filter rule 5 action 'jump'
set firewall ipv4 input filter rule 5 inbound-interface name 'pppoe0'
set firewall ipv4 input filter rule 5 jump-target 'EXTERNAL-LOCAL'
```

0.1.4 Firewall rules for the input filter

Since we only care about the tunnels in this case, we will be focusing on the input filter rules here:

```
set firewall ipv4 name EXTERNAL-LOCAL default-action 'drop'
set firewall ipv4 name EXTERNAL-LOCAL default-log
set firewall ipv4 name EXTERNAL-LOCAL rule 10 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 10 log
set firewall ipv4 name EXTERNAL-LOCAL rule 10 state 'established'
set firewall ipv4 name EXTERNAL-LOCAL rule 10 state 'related'
set firewall ipv4 name EXTERNAL-LOCAL rule 20 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 20 log
set firewall ipv4 name EXTERNAL-LOCAL rule 20 protocol 'icmp'
set firewall ipv4 name EXTERNAL-LOCAL rule 40 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 40 description 'magic-wan'
set firewall ipv4 name EXTERNAL-LOCAL rule 40 log
set firewall ipv4 name EXTERNAL-LOCAL rule 40 protocol 'gre'
set firewall ipv4 name EXTERNAL-LOCAL rule 40 source group network-group 'cf-ipv4'
set firewall ipv4 name EXTERNAL-LOCAL rule 50 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 50 description 'magic-wan-ipsec'
set firewall ipv4 name EXTERNAL-LOCAL rule 50 log
set firewall ipv4 name EXTERNAL-LOCAL rule 50 protocol 'esp'
set firewall ipv4 name EXTERNAL-LOCAL rule 50 source group network-group 'cf-ipv4'
set firewall ipv4 name EXTERNAL-LOCAL rule 51 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 51 description 'magic-wan-ipsec'
set firewall ipv4 name EXTERNAL-LOCAL rule 51 destination port '500'
set firewall ipv4 name EXTERNAL-LOCAL rule 51 log
set firewall ipv4 name EXTERNAL-LOCAL rule 51 protocol 'udp'
set firewall ipv4 name EXTERNAL-LOCAL rule 51 source group network-group 'cf-ipv4'
set firewall ipv4 name EXTERNAL-LOCAL rule 52 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 52 description 'magic-wan-ipsec'
set firewall ipv4 name EXTERNAL-LOCAL rule 52 destination port '4500'
set firewall ipv4 name EXTERNAL-LOCAL rule 52 log
set firewall ipv4 name EXTERNAL-LOCAL rule 52 protocol 'udp'
set firewall ipv4 name EXTERNAL-LOCAL rule 52 source group network-group 'cf-ipv4'
set firewall ipv4 name EXTERNAL-LOCAL rule 61 action 'accept'
set firewall ipv4 name EXTERNAL-LOCAL rule 61 description 'sflow'
set firewall ipv4 name EXTERNAL-LOCAL rule 61 destination port '6343'
set firewall ipv4 name EXTERNAL-LOCAL rule 61 log
set firewall ipv4 name EXTERNAL-LOCAL rule 61 protocol 'tcp_udp'
set firewall ipv4 name EXTERNAL-LOCAL rule 61 source group network-group 'cf-ipv4'
```

0.2 WAN

In my case since it is a PPPoE connection to the ISP, I will set a VLAN tag on the ethernet interface that I designated for WAN:

```
set interfaces ethernet eth0 description 'EXTERNAL'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 hw-id 'xx:xx:xx:xx:xx:71'
set interfaces ethernet eth0 ip disable-arp-filter
set interfaces ethernet eth0 offload gro
set interfaces ethernet eth0 offload gso
set interfaces ethernet eth0 offload rps
set interfaces ethernet eth0 offload sg
set interfaces ethernet eth0 offload tso
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth0 vif 6 ip disable-arp-filter
```

This would then be used to create the PPPoE interface, do note the TCP clamping (if) required by your ISP:

```
set interfaces pppoe pppoe0 authentication password xxxxxx
set interfaces pppoe pppoe0 authentication username xxxxxx
set interfaces pppoe pppoe0 description 'kpn'
set interfaces pppoe pppoe0 ip adjust-mss 'clamp-mss-to-pmtu'
set interfaces pppoe pppoe0 no-peer-dns
set interfaces pppoe pppoe0 source-interface 'eth0.6'
```

0.3 NAT

Since we are focusing on the tunnels, we are just gonna set the masquerade rules (later on you can setup the other ethernet interfaces:

```
set nat source rule 20 description 'pppoe'
set nat source rule 20 log
set nat source rule 20 outbound-interface name 'pppoe0'
set nat source rule 20 source address 'xxx.xxx.0.0/16'
set nat source rule 20 translation address 'masquerade'
```

0.4 GRE

`tun0` interface, not the MSS clamping from the GRE overhead:

```
set interfaces tunnel tun0 address 'xxx.xxx.99.20/31'
set interfaces tunnel tun0 description 'magic-wan'
set interfaces tunnel tun0 encapsulation 'gre'
set interfaces tunnel tun0 ip adjust-mss '1436'
set interfaces tunnel tun0 ip disable-arp-filter
set interfaces tunnel tun0 remote 'xxx.xxx.66.5' # Cloudflare's endpoint
set interfaces tunnel tun0 source-address 'xxx.xxx.81.4.2' # Your IP
```

0.5 IPsec

`vti0` interface, note the MSS clamping from the IPsec overhead:

```
set interfaces vti vti0 address 'xxx.xxx.100.20/31'
set interfaces vti vti0 description 'magic-wan-ipsec'
set interfaces vti vti0 ip adjust-mss '1350'
set interfaces vti vti0 ip disable-arp-filter
```

0.5.1 VPN

This is the site-to-site VPN setup that will be using the `vti0` we have initially setup to initiate the IPsec tunnels to Cloudflare:

```
set vpn ipsec authentication psk cf-ipsec id 'xxx.xxx.242.5' # Cloudflare's endpoint
set vpn ipsec authentication psk cf-ipsec secret xxxxxx # Secret token that you generated for use or randomly via the Tunnel creation with Cloudflare
set vpn ipsec esp-group vyos-nl-esp lifetime '14400'
set vpn ipsec esp-group vyos-nl-esp mode 'tunnel'
set vpn ipsec esp-group vyos-nl-esp pfs 'enable'
set vpn ipsec esp-group vyos-nl-esp proposal 1 encryption 'aes256gcm128'
set vpn ipsec esp-group vyos-nl-esp proposal 1 hash 'sha512'
set vpn ipsec ike-group vyos-nl-ike close-action 'start'
set vpn ipsec ike-group vyos-nl-ike dead-peer-detection action 'restart'
set vpn ipsec ike-group vyos-nl-ike dead-peer-detection interval '30'
set vpn ipsec ike-group vyos-nl-ike dead-peer-detection timeout '120'
set vpn ipsec ike-group vyos-nl-ike disable-mobike
set vpn ipsec ike-group vyos-nl-ike key-exchange 'ikev2'
set vpn ipsec ike-group vyos-nl-ike lifetime '14400'
set vpn ipsec ike-group vyos-nl-ike proposal 1 dh-group '14'
set vpn ipsec ike-group vyos-nl-ike proposal 1 encryption 'aes256gcm128'
set vpn ipsec ike-group vyos-nl-ike proposal 1 hash 'sha512'
set vpn ipsec interface 'pppoe0'
set vpn ipsec log level '2'
set vpn ipsec log subsystem 'any'
set vpn ipsec options disable-route-autoinstall
set vpn ipsec site-to-site peer magic-wan-ipsec authentication local-id 'ID' # The authentication ID you can get from the API
set vpn ipsec site-to-site peer magic-wan-ipsec authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer magic-wan-ipsec authentication remote-id 'xxx.xxx.242.5' # Cloudflare's endpoint
set vpn ipsec site-to-site peer magic-wan-ipsec connection-type 'initiate'
set vpn ipsec site-to-site peer magic-wan-ipsec ike-group 'vyos-nl-ike'
set vpn ipsec site-to-site peer magic-wan-ipsec ikev2-reauth 'yes'
set vpn ipsec site-to-site peer magic-wan-ipsec local-address 'xxx.xxx.81.42' # The IP assigned by your ISP
set vpn ipsec site-to-site peer magic-wan-ipsec remote-address 'xxx.xxx.242.5' # Cloudflare's endpoint
set vpn ipsec site-to-site peer magic-wan-ipsec vti bind 'vti0'
set vpn ipsec site-to-site peer magic-wan-ipsec vti esp-group 'vyos-nl-esp'
```

0.5.2 Replay Window

Refer to the docs when deciding to set it to `0` or not:

```
set vpn ipsec site-to-site peer magic-wan-ipsec replay-window '0'
```

0.5.3 Strongswan

The configuration above essentially updates a script that generates the Strongwan config below, this can be found in `/etc/swanctl/swanctl.conf`:

```
connections {
    magic-wan-ipsec {
        proposals = aes256gcm128-sha512-modp2048
        version = 2
        local_addrs = xxx.xxx.xxx.42 # Your IP address
        remote_addrs = xxx.xxx.xxx.5 # Cloudflare's endpoint
        dpd_timeout = 120
        dpd_delay = 30
        rekey_time = 14400s
        mobike = no
        keyingtries = 0
        local {
            id = "ID" # From Cloudfare IPsec Tunnel API
            auth = psk
        }
        remote {
            id = "x.x.242.5"
            auth = psk
        }
        children {
            magic-wan-ipsec-vti {
                esp_proposals = aes256gcm128-sha512-modp2048
                life_time = 14400s
                local_ts = 0.0.0.0/0,::/0
                remote_ts = 0.0.0.0/0,::/0
                updown = "/etc/ipsec.d/vti-up-down vti0"
                if_id_in = 1
                if_id_out = 1
                ipcomp = no
                mode = tunnel
                start_action = start
                dpd_action = restart
                close_action = start
                replay_window = 0
            }
        }
    }

}

pools {
}

secrets {
    ike-cf-ipsec {
        # ID's from auth psk <tag> id xxx
```

```
        id-xxxxxxx = "x.x.242.5" # Cloudflare's endpoint
        secret = "SECRET" # Secret used to create tunnel
    }

}
```

0.5.4 Bidirectional Health-checks

As mentioned above, without replay-window being zero, you can't get health-checks working unless you select the option when creating the tunnel on Cloudflare.

0.6 Policy Based Routing

We set the routing tables:

```
set protocols static table 10 route xxx.xxx.0.0/0 interface tun0
set protocols static table 20 route xxx.xxx.0.0/0 interface vti0
```

And in this case, I choose to route selectively via the PBRs below:

0.6.1 GRE

```
set policy route magic-wan-gre-rasp rule 5 description 'magic-wan-gre-rasp'
set policy route magic-wan-gre-rasp-tcp-udp rule 5 protocol 'tcp_udp'
set policy route magic-wan-gre-rasp rule 5 log
set policy route magic-wan-gre-rasp rule 5 set table '10'
set policy route magic-wan-gre-rasp rule 5 source address 'xxx.xxx.69.7'
```

0.6.2 IPsec

```
set policy route magic-wan-ipsec-rasp-tcp-udp rule 5 log
set policy route magic-wan-ipsec-rasp rule 5 description 'magic-wan-ipsec-rasp'
set policy route magic-wan-ipsec-rasp-tcp-udp rule 5 protocol 'tcp_udp'
set policy route magic-wan-ipsec-rasp-tcp-udp rule 5 set table '20'
set policy route magic-wan-ipsec-rasp-tcp-udp rule 5 source address 'xxx.xxx.69.7'
```

0.7 NFT Rulesets

The configuration rules above just create `nft` rules and if you did decide to, it's best to create your own ruleset, as the config will override.

Run `sudo nft list ruleset` to see the current rules, this would include firewall, NAT, PBRs etc.

0.8 Sysctl

If required the following might need to be set:

```
set system sysctl parameter net.core.rmem_max value '2500000'
set system sysctl parameter net.core.wmem_max value '2500000'
set system sysctl parameter net.ipv4.conf.all.accept_local value '1'
set system sysctl parameter net.ipv4.conf.all.accept_redirects value '0'
set system sysctl parameter net.ipv4.conf.all.arp_filter value '0'
set system sysctl parameter net.ipv4.conf.all.rp_filter value '0'
set system sysctl parameter net.ipv4.conf.all.send_redirects value '0'
set system sysctl parameter net.ipv4.conf.default.arp_filter value '0'
set system sysctl parameter net.ipv4.conf.default.rp_filter value '0'
```

This has to do with `reverse path` filtering, `ip forwarding` and `rmem` and `wmem` for QUIC tunnels should you choose to set up Cloudflare Tunnels on the same machine. Take a look at the definitions on sysctl-explorer.