Portal > Knowledgebase > VPN > IPSec > VTI with Palo Alto

VTI with Palo Alto

Santiago Lorente - 2020-03-30 - 0 Comments - in IPSec

Palo Alto Networks is a network security equipment manufacturer.

In this example we setup IPsec with VTI between a Palo Alto firewall and VyOS.

Palo Alto side

```
set network interface tunnel units tunnel.<unit> ip <pa-tunnel-address/netmask>
set network interface tunnel units tunnel.<unit> interface-management-profile <allow ping>

set vsys vsys1 zone vyos-pa-zone network layer3 tunnel.<unit>

set network ike crypto-profiles ike-crypto-profiles vyos-pa-ike encryption aes256
set network ike crypto-profiles ike-crypto-profiles vyos-pa-ike hash sha256
set network ike crypto-profiles ike-crypto-profiles vyos-pa-ike dh-group group14
set network ike crypto-profiles ike-crypto-profiles vyos-pa-ike lifetime hours 24
set network ike crypto-profiles ipsec-crypto-profiles vyos-pa-ipsec esp encryption aes256
set network ike crypto-profiles ipsec-crypto-profiles vyos-pa-ipsec esp authentication sha1
set network ike crypto-profiles ipsec-crypto-profiles vyos-pa-ipsec dh-group group14
set network ike crypto-profiles ipsec-crypto-profiles vyos-pa-ipsec lifetime hours 1

set network ike gateway vyos-pa protocol ikev1 dpd enable yes
set network ike gateway vyos-pa protocol ikev1 ike-crypto-profile vyos-pa-ike
set network ike gateway vyos-pa protocol ikev1 exchange-mode auto
set network ike gateway vyos-pa local-address ip <pa-wan-address>
set network ike gateway vyos-pa local-address interface <pa-wan-interface>
set network ike gateway vyos-pa authentication pre-shared-key key <pre-shared-key>
set network ike gateway vyos-pa protocol-common passive-mode yes
set network ike gateway vyos-pa peer-address ip <vyos-wan-address>
set network ike gateway vyos-pa peer-id id <vyos-wan-address>
set network ike gateway vyos-pa peer-id type ipaddr
set network ike gateway vyos-pa local-id id <pa-wan-address>
set network ike gateway vyos-pa local-id type ipaddr

set network tunnel ipsec vyos-pa auto-key ike-gateway vyos-pa-ike
set network tunnel ipsec vyos-pa auto-key ipsec-crypto-profile vyos-pa-ipsec
set network tunnel ipsec vyos-pa tunnel-interface tunnel.<unit>
set network tunnel ipsec vyos-pa anti-replay yes

set network virtual-router <virtual-router> routing-table ip static-route vyos-pa-vpn nexthop ip-address <vyos-tunnel-address>
set network virtual-router <virtual-router> routing-table ip static-route vyos-pa-vpn interface tunnel.<unit>
set network virtual-router <virtual-router> routing-table ip static-route vyos-pa-vpn destination <vyos-lan-network/netmask>

set vsys vsys1 rulebase security rules vyos-pa-vpn from <pa-wan-zone>
set vsys vsys1 rulebase security rules vyos-pa-vpn to <pa-wan-zone>
set vsys vsys1 rulebase security rules vyos-pa-vpn source [ <pa-wan-address> <vyos-wan-address> ]
set vsys vsys1 rulebase security rules vyos-pa-vpn destination [ <pa-wan-address> <vyos-wan-address> ]
set vsys vsys1 rulebase security rules vyos-pa-vpn application [ ciscovpn dtls ipsec ssl ]
set vsys vsys1 rulebase security rules vyos-pa-vpn service application-default
set vsys vsys1 rulebase security rules vyos-pa-vpn action allow
set vsys vsys1 rulebase security rules vyos-pa-vpn log-start yes
```

VyOS side

```
set system offload ipsec enable
set vpn ipsec esp-group vyos-pa-esp lifetime 3600
set vpn ipsec esp-group vyos-pa-esp mode tunnel
set vpn ipsec esp-group vyos-pa-esp pfs dh-group 14
set vpn ipsec esp-group vyos-pa-esp proposal 1 encryption aes256
set vpn ipsec esp-group vyos-pa-esp proposal 1 hash sha1
set vpn ipsec ike-group vyos-pa-ike key-exchange ikev1
set vpn ipsec ike-group vyos-pa-ike lifetime 86400
set vpn ipsec ike-group vyos-pa-ike proposal 1 dh-group 14
set vpn ipsec ike-group vyos-pa-ike proposal 1 encryption aes256
set vpn ipsec ike-group vyos-pa-ike proposal 1 hash sha256
set vpn ipsec ipsec-interfaces interface <vyos-wan-interface>
set vpn ipsec logging log-modes all
set vpn ipsec site-to-site peer <pa-wan-address> authentication id
<vyos-wan-address>
set vpn ipsec site-to-site peer <pa-wan-address> authentication mode
pre-shared-secret
set vpn ipsec site-to-site peer <pa-wan-address> authentication pre-
shared-secret <pre-shared-key>
set vpn ipsec site-to-site peer <pa-wan-address> authentication
remote-id <pa-wan-address>
set vpn ipsec site-to-site peer <pa-wan-address> connection-type
initiate
set vpn ipsec site-to-site peer <pa-wan-address> default-esp-group
vyos-pa
set vpn ipsec site-to-site peer <pa-wan-address> ike-group vyos-pa
set vpn ipsec site-to-site peer <pa-wan-address> local-address <vyos-
wan-address>
set vpn ipsec site-to-site peer <pa-wan-address> vti bind vti0
set vpn ipsec site-to-site peer <pa-wan-address> vti esp-group vyos-
pa

set interfaces vti vti0 address <vyos-tunnel-ip/netmask>

set protocols static route <pa-lan-network/netmask> next-hop <pa-
tunnel-address>

set firewall name <vyos-wan-interface-to-local-ruleset> rule 20
action accept
set firewall name <vyos-wan-interface-to-local-ruleset> rule 20
destination group address-group ADDRv4_<vyos-wan-interface>
set firewall name <vyos-wan-interface-to-local-ruleset> rule 20 log
```

```
enable
set firewall name <vyos-wan-interface-to-local-ruleset> rule 20 protocol esp
set firewall name <vyos-wan-interface-to-local-ruleset> rule 20 source address <pa-wan-address>
```

Tags

VTI