APPLICATION NOTE 005

WeOS IPSec Authentication using Certificates

How to use IPSec Main Mode tunnels without public IP-addresses in both ends of the tunnel

Application Note Network Layout

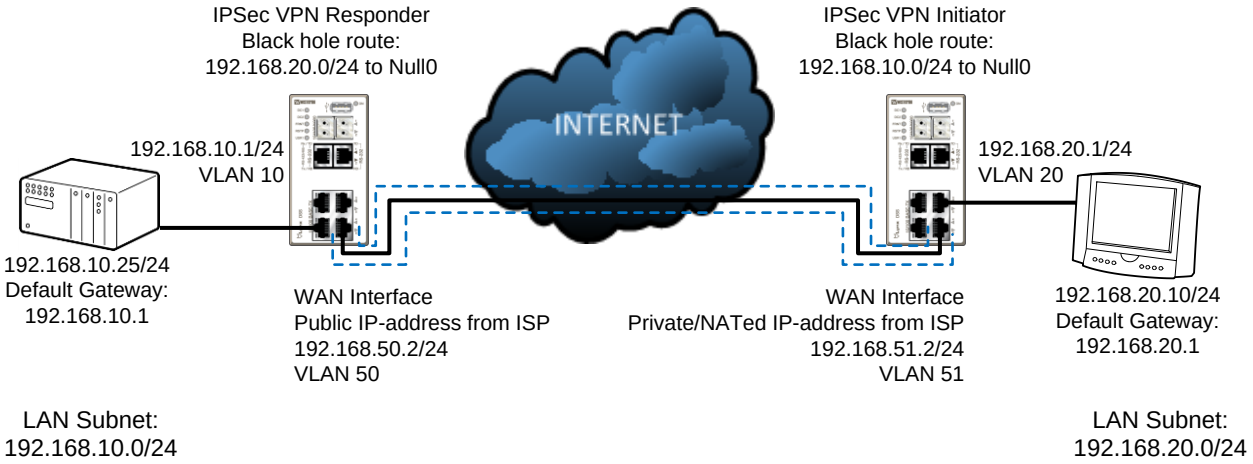
This Application Note shows how to setup a Main Mode IPSec VPN tunnel between two sites without having public IP-addresses at both ends of the tunnel.

Background

Using certificates for tunnel end point authentication has the advantage of allowing IPSec Main Mode tunnels to be used eventhough only one side of the tunnel as a public IP-address.
By using Distinguished Name authentication together with self signed certificates this is possible to accomplish.
The IPSec Main Mode tunnel is considered to be more secure than the IPSec Aggressive Mode version and to make absolutely sure that no tunnel traffic leaks out into the unsecure network the black hole route functionality in WeOS can be used. Black hole routes will prevent tunnel traffic to be forwarded out through a Default Gateway if the tunnel should for some reason go down.

Please Note! How to generate self signed certificates is explained in Tech Note 003 ver 2.0 as the certificates for IPSec VPNs differs from the SSL VPN certificates so therefore the Tech Note 003 has been updated to a version 2.0.

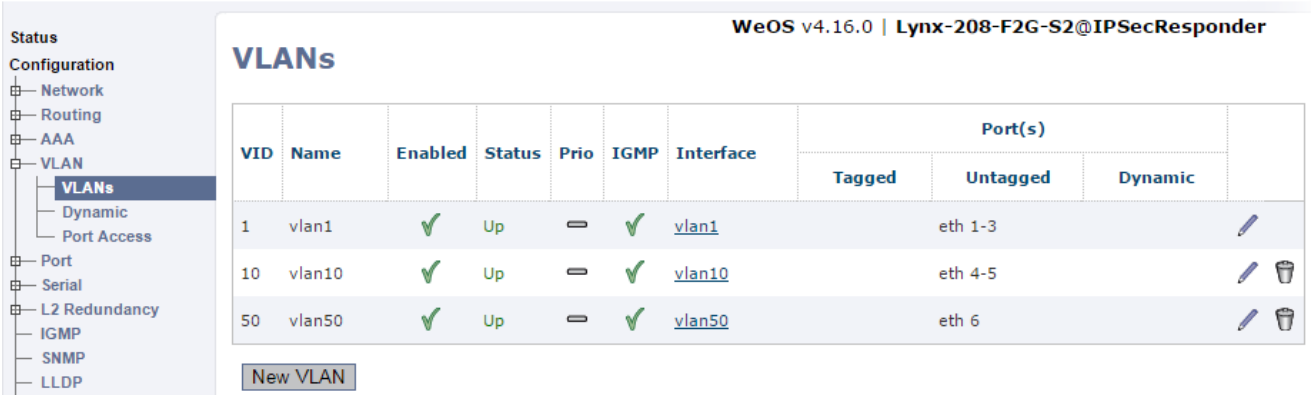
All configuration in this Application Note is done using WeOS version 4.16.0.



Configuration

Configure VLANs

Start with setting up the VLANs needed for the inside (VLAN 10) and outside network (VLAN 50) for the IPSec Responder.
Configurartion -> VLAN -> VLANs



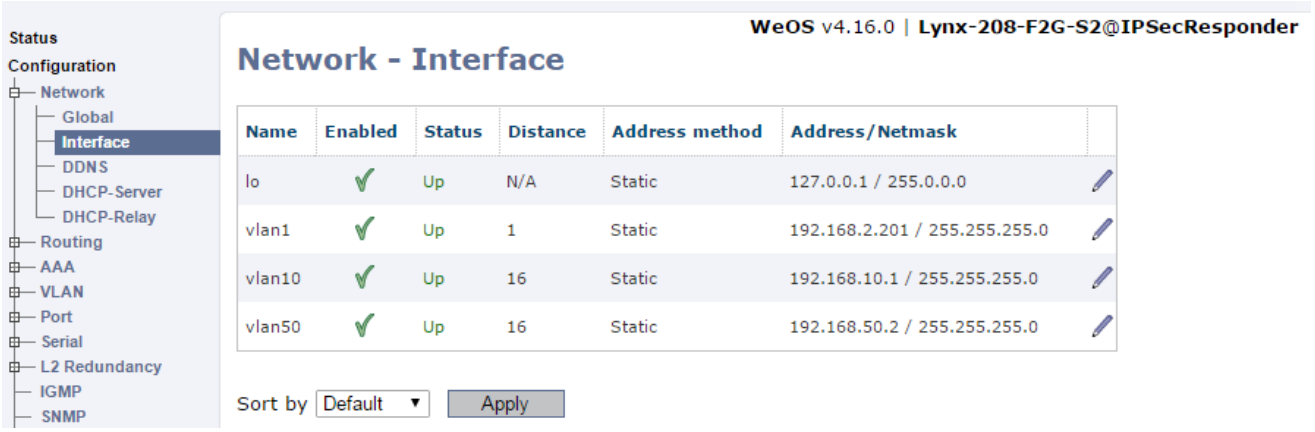
Do the same for the IPSec Initiator, inside (VLAN 20) and outside network (VLAN 51).

Configure Interfaces

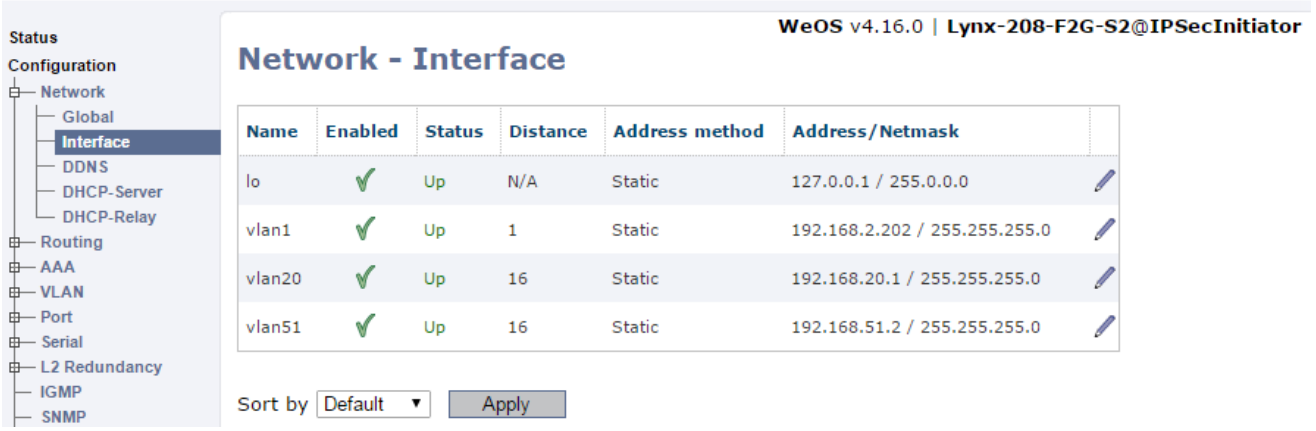
Then setup IP-addresses for the VLANs created.
Configuration -> Network -> Interface

If the WAN interfaces do not get addresses handed out via DHCP, remember to set Default Gateway and Name Server addresses manually.
Configuration -> Network -> Global

IPSec Responder:



IPSec Initiator:

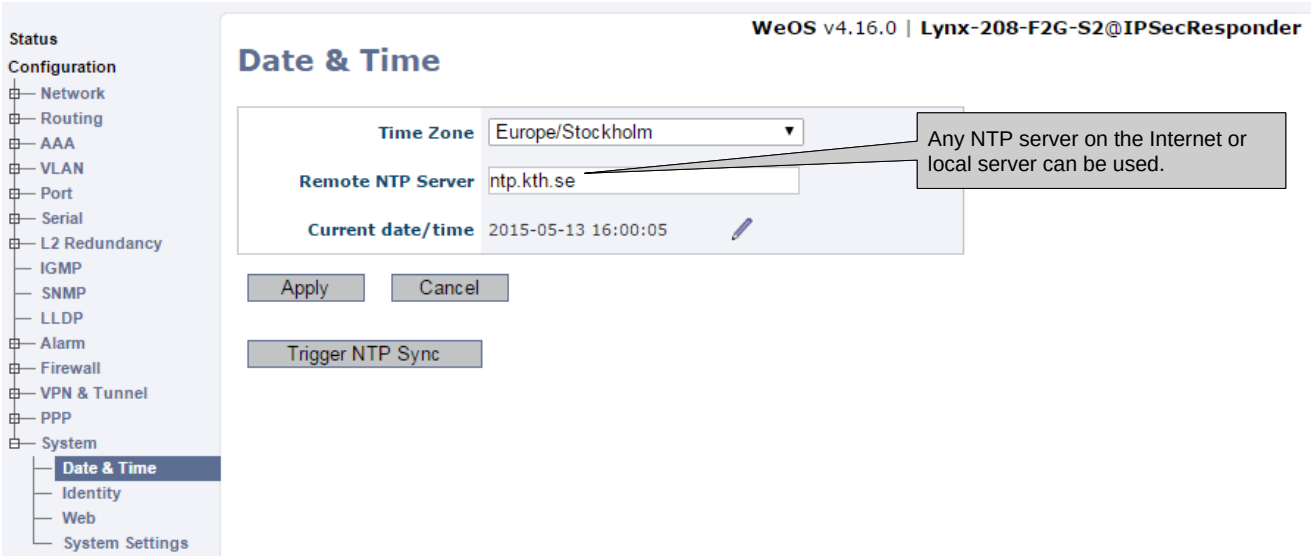


Upload Certificates

Date & Time Settings

In order for the IPSec VPN certificates to work properly the switches will have to have the correct time set. To make sure this is the case it is best to synchronize the time with a time server. If this can not be achieved make sure the time is as accurate as possible.
Configuration -> System -> Date & Time

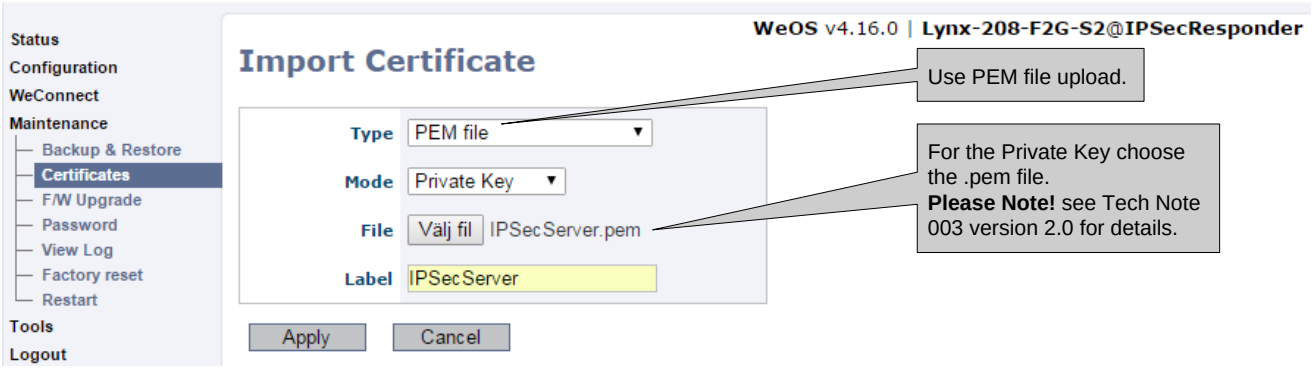
IPSec Responder and Initiator:

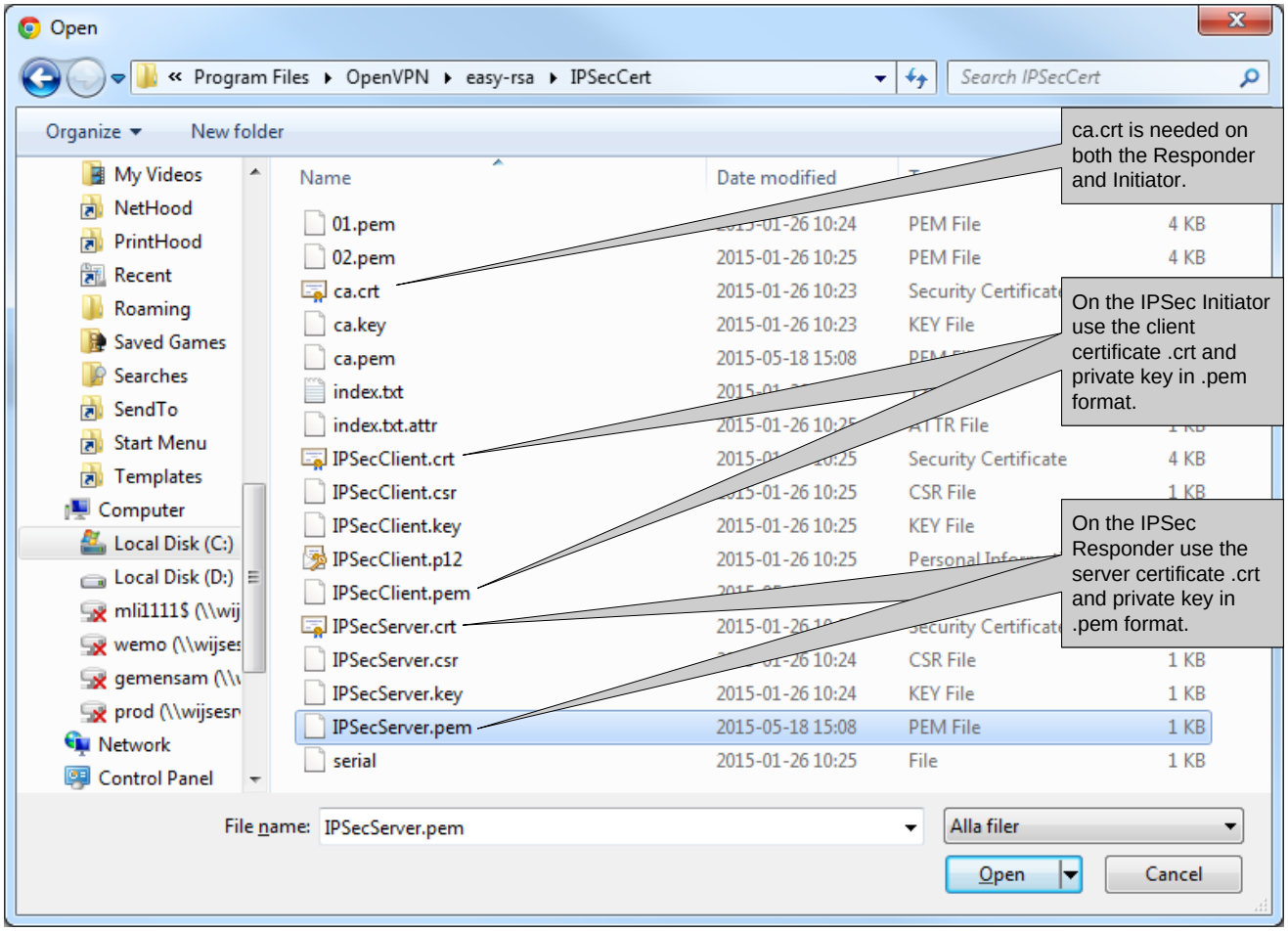


Certificates Import

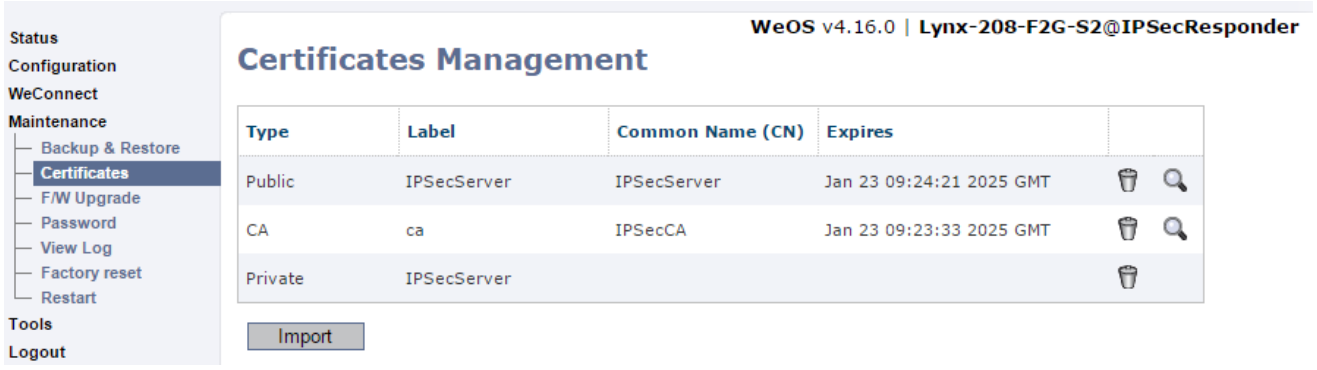
Import the certificates for the IPSec Responder and IPSec Initiator.
How to generate certificates for IPSec VPN Tunnels is described in Tech Note 003 Self Signed Certificates version 2.0.
Maintenance -> Certificates

IPSec Responder and Initiator:

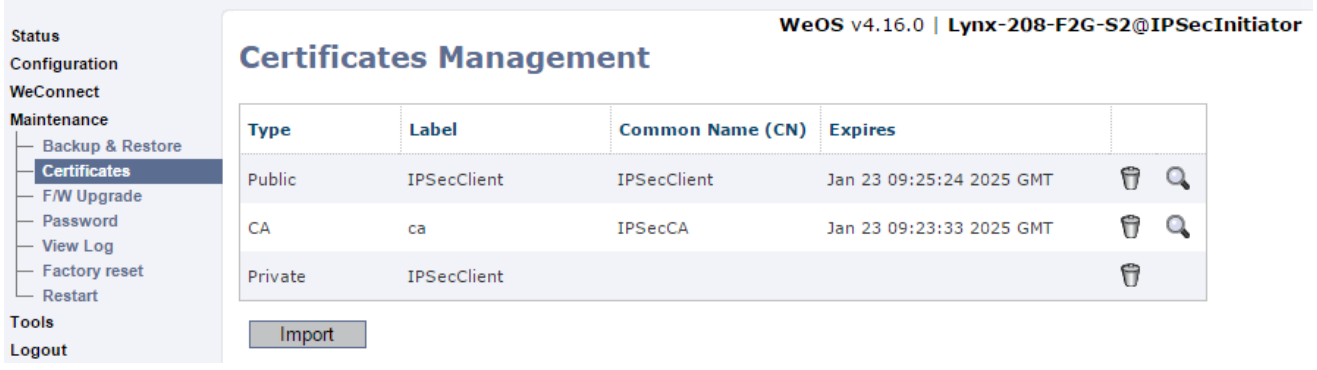




IPSec Responder:



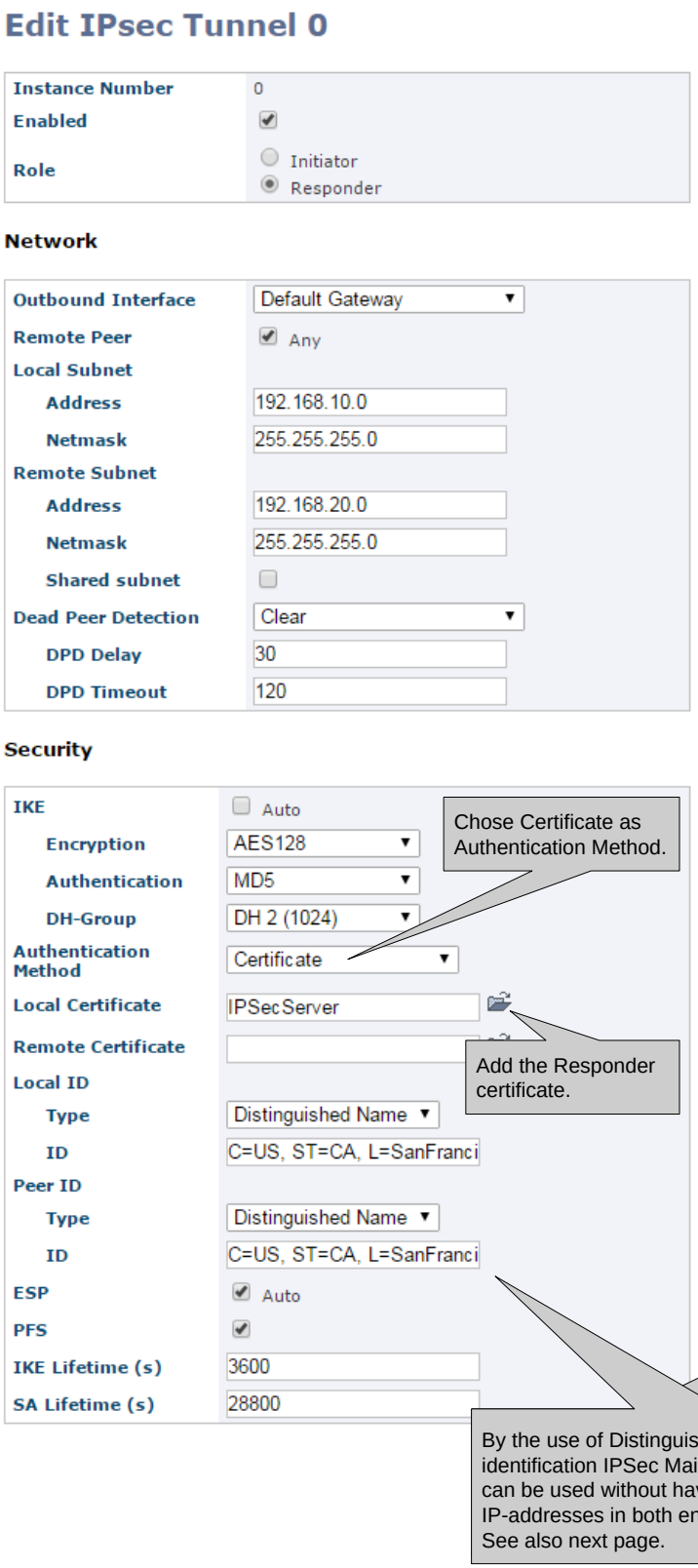
IPSec Initiator:



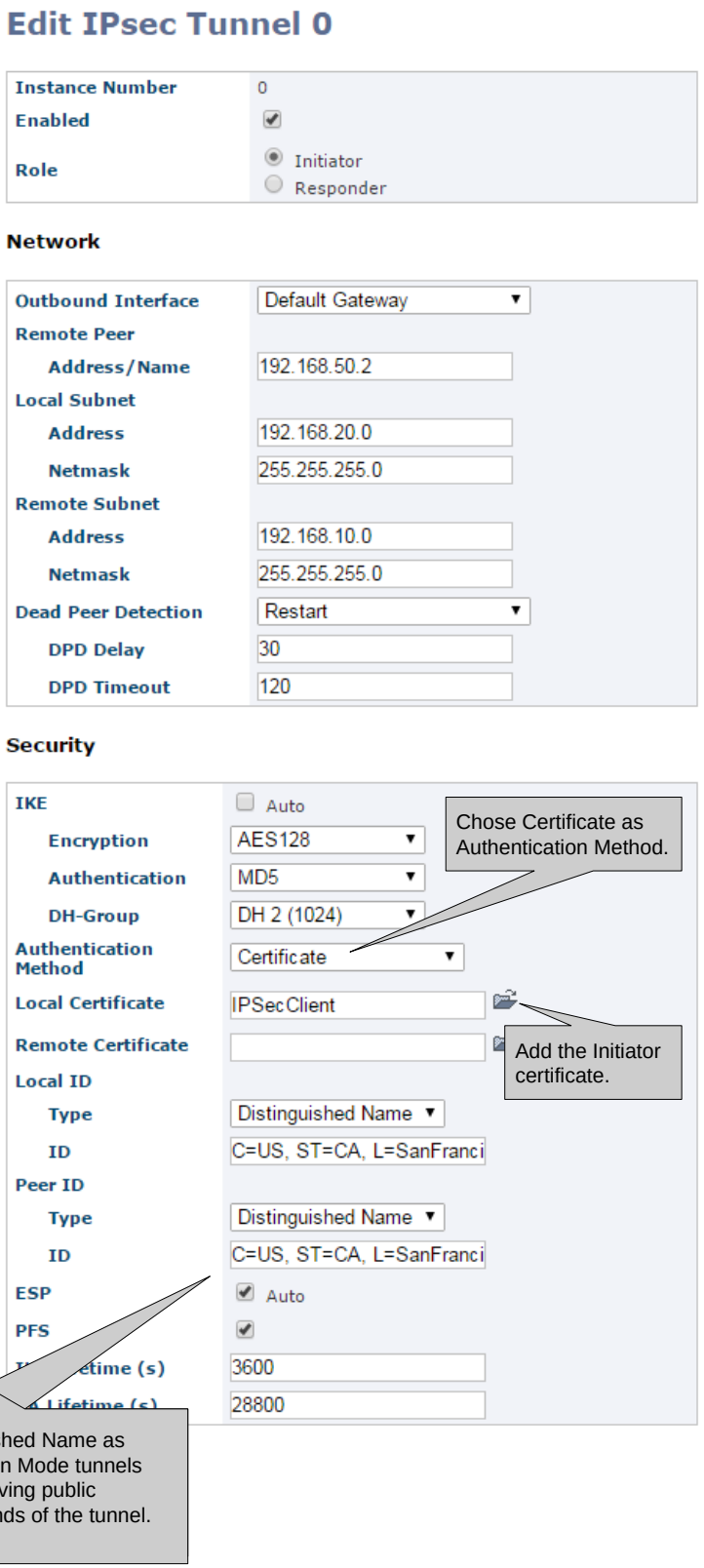
Configure the IPSec Tunnel

After the certificates have been uploaded configure the IPSec VPN tunnel.

IPSec Responder:



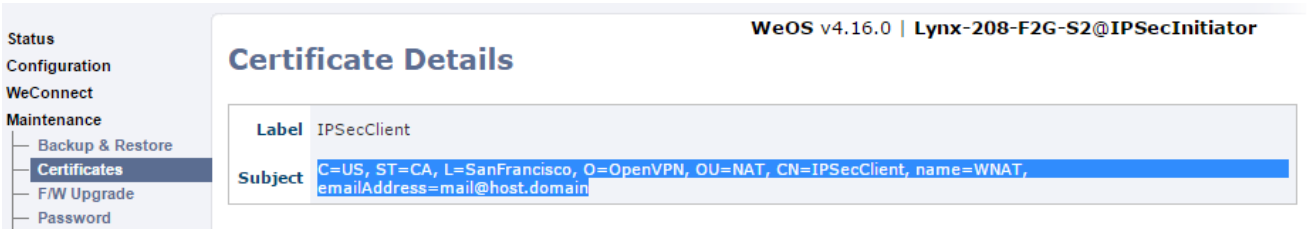
IPSec Initiator:



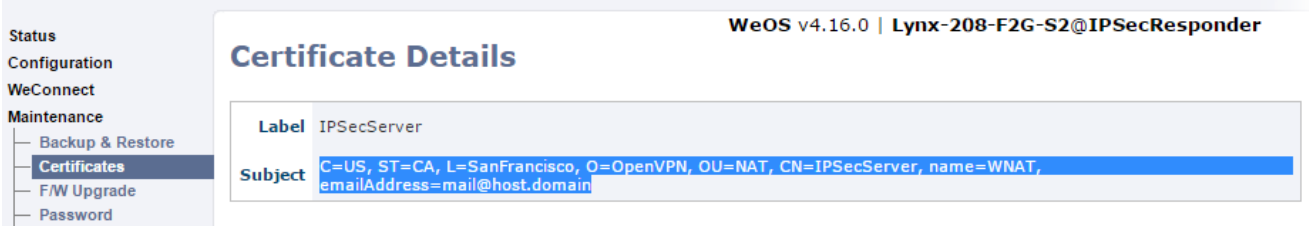
By the use of Distinguished Name as identification IPSec Main Mode tunnels can be used without having public IP-addresses in both ends of the tunnel. See also next page.

Distinguished Name Authentication

The distinguished name consists of the subject settings in the public certificates, almost. In the examples used in this Application Note the subjects from the client and the server certificates can be seen under Maintenace -> Certificates -> Click the magnifying class.



C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, **name**=WNAT, **emailAddress**=mail@host.domain



C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, **name**=WNAT, **emailAddress**=mail@host.domain

However the IPSec implemetation identifies using a strings looking like this:
C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, **N**=WNAT, **E**=mail@host.domain

C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, **N**=WNAT, **E**=mail@host.domain

As these strings are not exactly the same the IPSec authentication will fail. This can be seen in the log of the WeOS unit and by using the exact same string displayed in the log in the tunnel configuration the distinguished name will be correct. See the previous page.

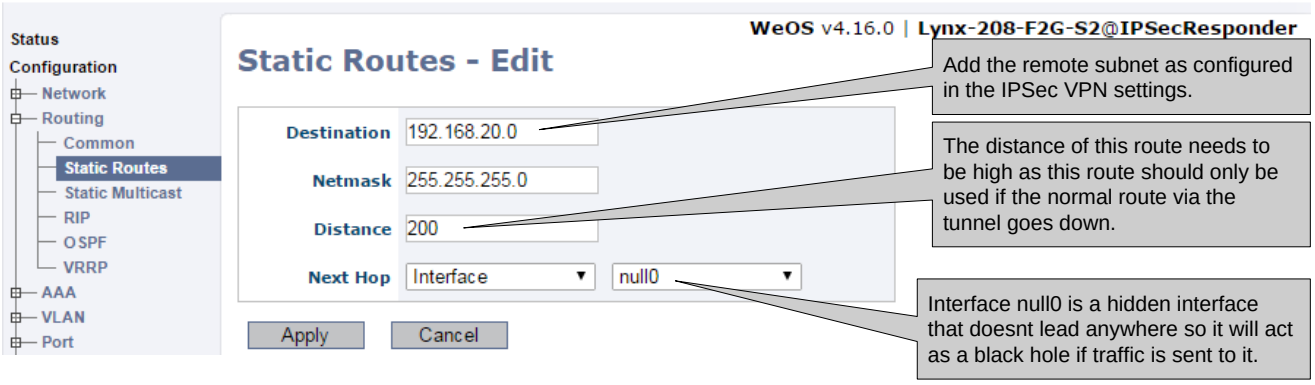
Log from the IPSec Responder:

May 6 15:25:05 default pluto[622]: bad right --id: unknown OID in ID_DER_ASN1_DN (ignored)
May 6 15:25:05 default pluto[622]: added connection description "ipsec0"
May 6 15:25:06 default pluto[622]: packet from 192.168.51.2:500: ignoring unknown Vendor ID payload []
May 6 15:25:06 default pluto[622]: packet from 192.168.51.2:500: received Vendor ID payload [Dead Peer Detection]
May 6 15:25:06 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: responding to Main Mode from unknown peer 192.168.51.2
May 6 15:25:06 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
May 6 15:25:06 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: STATE_MAIN_R1: sent MR1, expecting MI2
May 6 15:25:07 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
May 6 15:25:07 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: STATE_MAIN_R2: sent MR2, expecting MI3
May 6 15:25:07 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: Main mode peer ID is ID_DER_ASN1_DN: '**C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, N=WNAT, E=mail@host.domain**'
May 6 15:25:07 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: no crl from issuer "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecCA, N=WNAT, E=mail@host.domain" found (strict=no)
May 6 15:25:07 default pluto[622]: "ipsec0"[1] 192.168.51.2 #1: switched from "ipsec0" to "ipsec0"
May 6 15:25:07 default pluto[622]: "ipsec0"[2] 192.168.51.2 #1: deleting connection "ipsec0" instance with peer 192.168.51.2 {isakmp=#0/ipsec=#0}

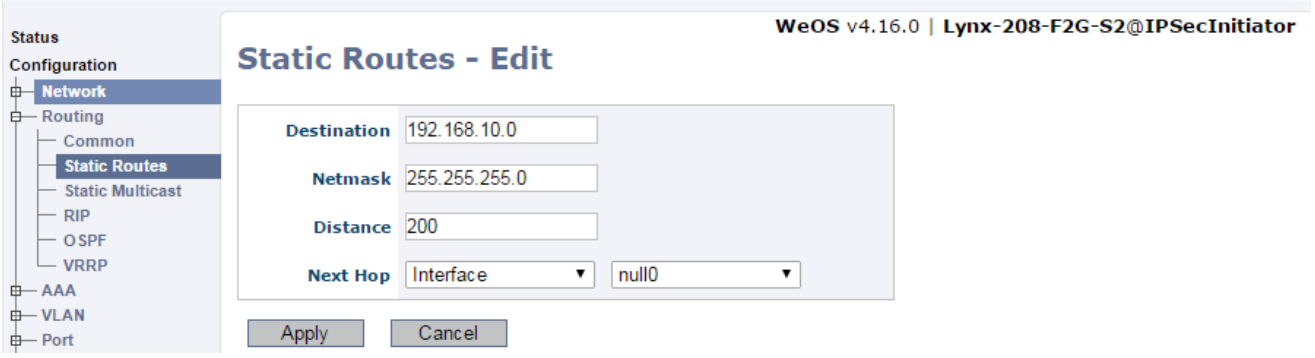
Black Hole Routes

Configure black hole routes via the Null0 interface to prevent tunnel traffic to leak out unencrypted through the Default Gateway and into the unsecure network if the tunnel goes down.
Configuration -> Routing -> Static Routes.

IPSec Responder:



IPSec Initiator:

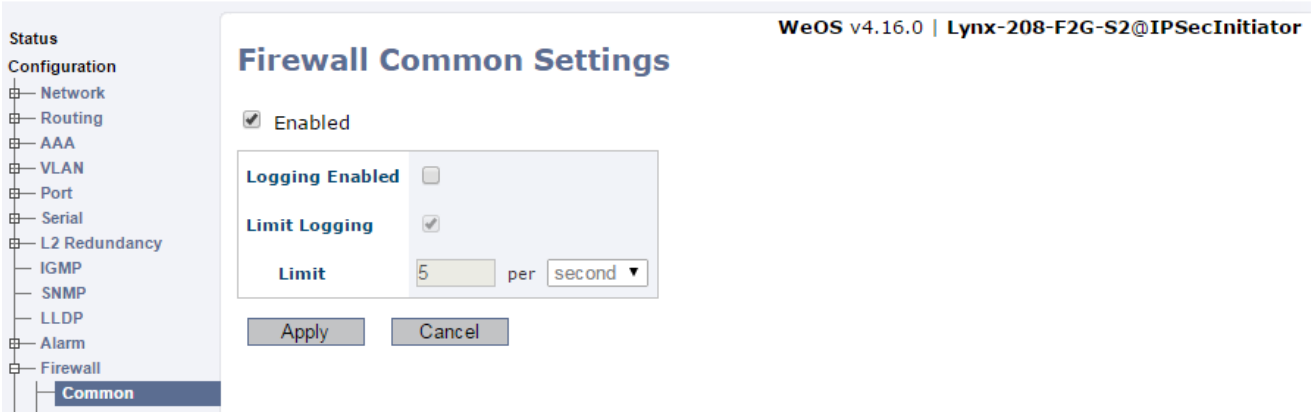


Firewall

Finally enable the Firewall to protect the WAN interfaces and to add NAPT functionality if needed. No rules needs to be configured to allow the IPSec tunnel through the Firewall this is automatically generated when the tunnel is configured.
Configuration -> Firewall

IPSec Responder:

IPSec Initiator:



IPSec Responder Configuration

```
# \\/ Westermo WeOS v4.16.0, CLI Format v1.16
# Lynx L208-F2G-S2, art.no. 3643-0205-005 ser.no. 21559

aaa
        username admin hash $1$r6mXNVvD$JaDxe9xNk/MI7Ebdk7B0q.
        end

system
        hostname Lynx-208-F2G-S2
        location "IPSecResponder"
        timezone Europe/Stockholm
        end

fdb
        mac 01:00:5e:00:00:01 port cpu, all
        mac 01:00:5e:00:00:02 port cpu, all
        mac 01:00:5e:00:00:04 port cpu, all
        mac 01:00:5e:00:00:05 port cpu, all
        mac 01:00:5e:00:00:06 port cpu, all
        mac 01:00:5e:00:00:09 port cpu, all
        mac 01:00:5e:00:00:0a port cpu, all
        mac 01:00:5e:00:00:0d port cpu, all
        mac 01:00:5e:00:00:0e port cpu, all
        mac 01:00:5e:00:00:12 port cpu, all
        mac 01:00:5e:00:00:18 port cpu, all
        mac 01:00:5e:00:00:66 port cpu, all
        mac 01:00:5e:00:00:6b port cpu, all
        mac 01:00:5e:00:00:fb port cpu, all
        end

alarm
        trigger 1 frnt
                ring 1
                severity active warning inactive notice
                condition high
                action 1
                end
        action 1
                target snmp log led digout
                end
        end

port ALL
        speed-duplex auto
        end

port serial 1
        no enable
        end
port serial 2
        enable
        end

no spanning-tree

vlan 1
        name vlan1
        untagged 1-3
        end

vlan 10
        name vlan10
        untagged 4-5
        end

vlan 50
        name vlan50
        untagged 6
        end
```

```
iface vlan1 inet static
        distance 1
        primary
        management ssh http https ipconfig snmp
        address 192.168.2.201/24
        end

iface vlan10 inet static
        distance 16
        management ssh http https ipconfig snmp
        address 192.168.10.1/24
        end

iface vlan50 inet static
        distance 16
        management ssh http https ipconfig snmp
        address 192.168.50.2/24
        end

ip
        route default 192.168.50.1
        firewall
                policy input DROP
                policy forward DROP
                filter allow in lo proto icmp
                filter allow in vlan1 proto icmp
                filter allow in vlan10 proto icmp
                nat type napt in vlan10 out vlan50 addfilter
                enable
                no log
                end
        end

tunnel
        ipsec 0
                enable
                no initiator
                no aggressive
                pfs
                ike crypto AES128 auth MD5 dh 1024
                no esp
                no peer
                no outbound
                local-id dn "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, N=WNAT, E=mail@host.domain"
                remote-id dn "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, N=WNAT, E=mail@host.domain"
                local-subnet 192.168.10.0/24
                remote-subnet 192.168.20.0/24
                method Cert
                local-cert IPSecServer
                dpd-action clear
                dpd-delay 30
                dpd-timeout 120
                sa-lifetime 28800
                ike-lifetime 3600
                end
        end

snmp-server
        rocommunity public
        no rwcommunity
        trapcommunity trap
        end

sntp
        server ntp.kth.se
        end

ntp
        end
```

IPSec Initiator Configuration

```
# \\/ Westermo WeOS v4.16.0, CLI Format v1.16
# Lynx L208-F2G-S2, art.no. 3643-0205-005 ser.no. 21560

aaa
        username admin hash $1$r6mXNVvD$JaDxe9xNk/MI7Ebdk7B0q.
        end

system
        hostname Lynx-208-F2G-S2
        location "IPSecInitiator"
        timezone Europe/Stockholm
        end

fdb
        mac 01:00:5e:00:00:01 port cpu, all
        mac 01:00:5e:00:00:02 port cpu, all
        mac 01:00:5e:00:00:04 port cpu, all
        mac 01:00:5e:00:00:05 port cpu, all
        mac 01:00:5e:00:00:06 port cpu, all
        mac 01:00:5e:00:00:09 port cpu, all
        mac 01:00:5e:00:00:0a port cpu, all
        mac 01:00:5e:00:00:0d port cpu, all
        mac 01:00:5e:00:00:0e port cpu, all
        mac 01:00:5e:00:00:12 port cpu, all
        mac 01:00:5e:00:00:18 port cpu, all
        mac 01:00:5e:00:00:66 port cpu, all
        mac 01:00:5e:00:00:6b port cpu, all
        mac 01:00:5e:00:00:fb port cpu, all
        end

alarm
        trigger 1 frnt
                ring 1
                severity active warning inactive notice
                condition high
                action 1
                end
        action 1
                target snmp log led digout
                end
        end

port ALL
        speed-duplex auto
        end

port serial 1
        no enable
        end
port serial 2
        enable
        end

no spanning-tree

vlan 1
        name vlan1
        untagged 1-3
        end

vlan 20
        name vlan20
        untagged 4-5
        end

vlan 51
        name vlan51
        untagged 6
        end
```

```
iface vlan1 inet static
        distance 1
        primary
        management ssh http https ipconfig snmp
        address 192.168.2.202/24
        end

iface vlan20 inet static
        distance 16
        management ssh http https ipconfig snmp
        address 192.168.20.1/24
        end

iface vlan51 inet static
        distance 16
        management ssh http https ipconfig snmp
        address 192.168.51.2/24
        end

ip
        route default 192.168.51.1
        firewall
                policy input DROP
                policy forward DROP
                filter allow in lo proto icmp
                filter allow in vlan1 proto icmp
                filter allow in vlan20 proto icmp
                nat type napt in vlan20 out vlan51 addfilter
                enable
                no log
                end
        end

tunnel
        ipsec 0
                enable
                initiator
                no aggressive
                pfs
                ike crypto AES128 auth MD5 dh 1024
                no esp
                peer 192.168.50.2
                no outbound
                local-id dn "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, N=WNAT, E=mail@host.domain"
                remote-id dn "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, N=WNAT, E=mail@host.domain"
                local-subnet 192.168.20.0/24
                remote-subnet 192.168.10.0/24
                method Cert
                local-cert IPSecClient
                dpd-action restart
                dpd-delay 30
                dpd-timeout 120
                sa-lifetime 28800
                ike-lifetime 3600
                end
        end

snmp-server
        rocommunity public
        no rwcommunity
        trapcommunity trap
        end

sntp
        server ntp.kth.se
        end

ntp
        end
```

Working Log from IPSec Responder

11:29:13 default pluto[1428]: OCF support for IKE [disabled]
May 18 11:29:13 default pluto[1428]: Setting NAT-Traversal port-4500 floating to off
May 18 11:29:13 default pluto[1428]: port floating activation criteria nat_t=0/port_float=1
May 18 11:29:13 default pluto[1428]: NAT-Traversal support [disabled]
May 18 11:29:13 default pluto[1428]: using /dev/urandom as source of random entropy
May 18 11:29:13 default pluto[1428]: starting up 1 cryptographic helpers
May 18 11:29:13 default pluto[1428]: started helper pid=1429 (fd:5)
May 18 11:29:13 default pluto[1428]: Using Linux 2.6 IPsec interface code on 3.0.101-lw4160 (experimental code)
May 18 11:29:13 default pluto[1429]: using /dev/urandom as source of random entropy
May 18 11:29:17 default pluto[1428]: loaded CA cert file 'ca.pem' (1322 bytes)
May 18 11:29:17 default pluto[1428]: adding interface vlan50/vlan50 192.168.50.2:500
May 18 11:29:17 default pluto[1428]: adding interface vlan10/vlan10 192.168.10.1:500
May 18 11:29:17 default pluto[1428]: adding interface vlan1/vlan1 192.168.2.201:500
May 18 11:29:17 default pluto[1428]: adding interface lo/lo 127.0.0.1:500
May 18 11:29:17 default pluto[1428]: loading secrets from "/etc/ipsec.secrets"
May 18 11:29:17 default pluto[1428]: loaded private key file '/crt/private/IPSecServer.key' (887 bytes)
May 18 11:29:17 default pluto[1428]: loaded private key for keyid: PPK_RSA:AwEAAdQ7L
May 18 11:29:17 default pluto[1428]: loading secrets from "/etc/ipsec.secrets"
May 18 11:29:17 default pluto[1428]: loaded private key file '/crt/private/IPSecServer.key' (887 bytes)
May 18 11:29:17 default pluto[1428]: loaded private key for keyid: PPK_RSA:AwEAAdQ7L
May 18 11:29:17 default pluto[1428]: loaded CA cert file 'ca.pem' (1322 bytes)
May 18 11:29:18 default pluto[1428]: loading certificate from IPSecServer.pem
May 18 11:29:18 default pluto[1428]: loaded host cert file '/crt/certs/IPSecServer.pem' (1460 bytes)
May 18 11:29:18 default pluto[1428]: added connection description "ipsec0"
May 18 11:29:18 default pluto[1428]: terminating all conns with alias='l2tp0'
May 18 11:29:27 default pluto[1428]: packet from 192.168.51.2:500: ignoring unknown Vendor ID payload []
May 18 11:29:27 default pluto[1428]: packet from 192.168.51.2:500: received Vendor ID payload [Dead Peer Detection]
May 18 11:29:27 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: responding to Main Mode from unknown peer 192.168.51.2
May 18 11:29:27 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
May 18 11:29:27 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: STATE_MAIN_R1: sent MR1, expecting MI2
May 18 11:29:27 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
May 18 11:29:27 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: STATE_MAIN_R2: sent MR2, expecting MI3
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: Main mode peer ID is ID_DER_ASN1_DN: 'C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, N=WNAT, E=mail@host.domain'
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: no crl from issuer "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecCA, N=WNAT, E=mail@host.domain" found (strict=no)
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: I am sending my cert
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG cipher=aes_128 prf=oakley_md5 group=modp1024}
May 18 11:29:28 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: Dead Peer Detection (RFC 3706): enabled
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #1: the peer proposed: 192.168.10.0/24:0/0 -> 192.168.20.0/24:0/0
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: responding to Quick Mode proposal {msgid:2ab8a6c6}
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: us: 192.168.10.0/24===192.168.50.2[C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, N=WNAT, E=mail@host.domain]
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: them: 192.168.51.2[C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecClient, N=WNAT, E=mail@host.domain]===192.168.20.0/24
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: transition from state STATE_QUICK_R0 to state STATE_QUICK_R1
May 18 11:29:29 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: STATE_QUICK_R1: sent QR1, inbound IPsec SA installed, expecting QI2
May 18 11:29:30 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: Dead Peer Detection (RFC 3706): enabled
May 18 11:29:30 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: transition from state STATE_QUICK_R1 to state STATE_QUICK_R2
May 18 11:29:30 default pluto[1428]: "ipsec0"[1] 192.168.51.2 #2: STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x24051fbd <0x518364f9 xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=enabled}

Working Log from IPSec Initiator

May 18 11:29:13 default pluto[1447]: OCF support for IKE [disabled]
May 18 11:29:13 default pluto[1447]: Setting NAT-Traversal port-4500 floating to off
May 18 11:29:13 default pluto[1447]: port floating activation criteria nat_t=0/port_float=1
May 18 11:29:13 default pluto[1447]: NAT-Traversal support [disabled]
May 18 11:29:13 default pluto[1447]: using /dev/urandom as source of random entropy
May 18 11:29:13 default pluto[1447]: starting up 1 cryptographic helpers
May 18 11:29:13 default pluto[1447]: started helper pid=1448 (fd:5)
May 18 11:29:13 default pluto[1447]: Using Linux 2.6 IPsec interface code on 3.0.101-lw4160 (experimental code)
May 18 11:29:13 default pluto[1448]: using /dev/urandom as source of random entropy
May 18 11:29:16 default pluto[1447]: loaded CA cert file 'ca.pem' (1322 bytes)
May 18 11:29:17 default pluto[1447]: adding interface vlan51/vlan51 192.168.51.2:500
May 18 11:29:17 default pluto[1447]: adding interface vlan20/vlan20 192.168.20.1:500
May 18 11:29:17 default pluto[1447]: adding interface vlan1/vlan1 192.168.2.202:500
May 18 11:29:17 default pluto[1447]: adding interface lo/lo 127.0.0.1:500
May 18 11:29:17 default pluto[1447]: loading secrets from "/etc/ipsec.secrets"
May 18 11:29:17 default pluto[1447]: loaded private key file '/crt/private/IPSecClient.key' (891 bytes)
May 18 11:29:17 default pluto[1447]: loaded private key for keyid: PPK_RSA:AwEAAcwlb
May 18 11:29:17 default pluto[1447]: loading secrets from "/etc/ipsec.secrets"
May 18 11:29:17 default pluto[1447]: loaded private key file '/crt/private/IPSecClient.key' (891 bytes)
May 18 11:29:17 default pluto[1447]: loaded private key for keyid: PPK_RSA:AwEAAcwlb
May 18 11:29:17 default pluto[1447]: loaded CA cert file 'ca.pem' (1322 bytes)
May 18 11:29:17 default pluto[1447]: loading certificate from IPSecClient.pem
May 18 11:29:17 default pluto[1447]: loaded host cert file '/crt/certs/IPSecClient.pem' (1424 bytes)
May 18 11:29:17 default pluto[1447]: added connection description "ipsec0"
May 18 11:29:17 default pluto[1447]: "ipsec0" #1: initiating Main Mode
May 18 11:29:18 default pluto[1447]: terminating all conns with alias='l2tp0'
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: received Vendor ID payload [Openswan (this version) 2.6.38]
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: received Vendor ID payload [Dead Peer Detection]
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: STATE_MAIN_I2: sent MI2, expecting MR2
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: I am sending my cert
May 18 11:29:27 default pluto[1447]: "ipsec0" #1: I am sending a certificate request
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: STATE_MAIN_I3: sent MI3, expecting MR3
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: received Vendor ID payload [CAN-IKEv2]
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: Main mode peer ID is ID_DER_ASN1_DN: 'C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecServer, N=WNAT, E=mail@host.domain'
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: no crl from issuer "C=US, ST=CA, L=SanFrancisco, O=OpenVPN, OU=NAT, CN=IPSecCA, N=WNAT, E=mail@host.domain" found (strict=no)
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG cipher=aes_128 prf=oakley_md5 group=modp1024}
May 18 11:29:28 default pluto[1447]: "ipsec0" #1: Dead Peer Detection (RFC 3706): enabled
May 18 11:29:29 default pluto[1447]: "ipsec0" #2: initiating Quick Mode RSASIG+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+SAREFTRACK {using isakmp#1 msgid:2ab8a6c6 proposal=defaults pfsgroup=OAKLEY_GROUP_MODP1024}
May 18 11:29:30 default pluto[1447]: "ipsec0" #2: Dead Peer Detection (RFC 3706): enabled
May 18 11:29:30 default pluto[1447]: "ipsec0" #2: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2
May 18 11:29:30 default pluto[1447]: "ipsec0" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0x518364f9 <0x24051fbd xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=enabled}

Revision history for version 1.0

Revision	Rev by	Revision note	Date
00	ML	First version	150526
01			
02			
03			
04			
05			
06			
07			

HEAD OFFICE

Sweden
Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units

Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.