Solution Guide

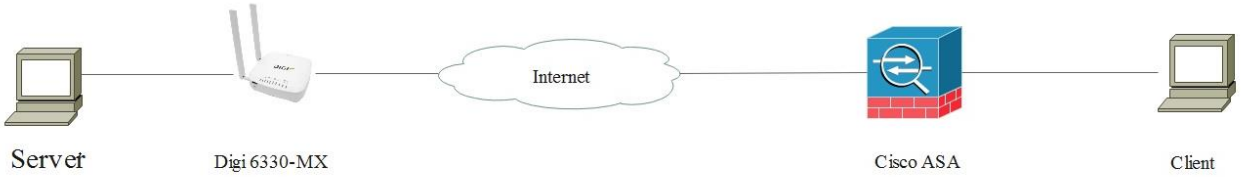
Digi 6330-MX to Cisco ASA IPSec VPN Tunnel using OpenSSL certificates.

Digi Support
September 2020

CONTENTS

1. INTRODUCTION

1.1 Outline



This document describes how to create, upload SSL certificates and configure Digi 6330-MX and Cisco routers to build an IPsec VPN tunnel.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi router.

This application note applies only to:

Model: DIGI 6330-MX running 20.5.38.58 and later

Model: Cisco ASA running 9.12 Image.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to:
tech.support@digi.com
Requests for new application notes can be sent to the same address.

2. VERSION

Version Number	Status
1.0	

3. CERTIFICATES CREATION

If you already have certificates available, you can skip to section 3.2

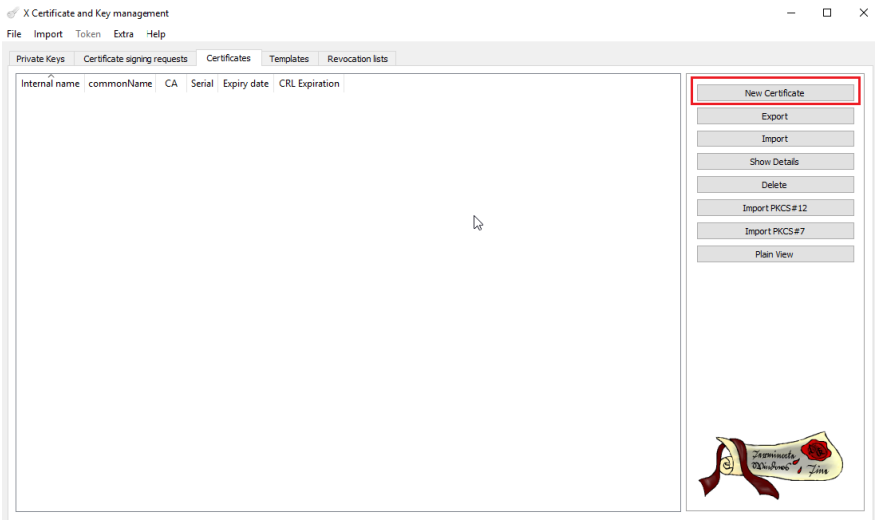
3.1 Generate Test certificates using OpenSSL and XCA

Download and install the latest release of XCA which can be found at: http://sourceforge.net/projects/xca/

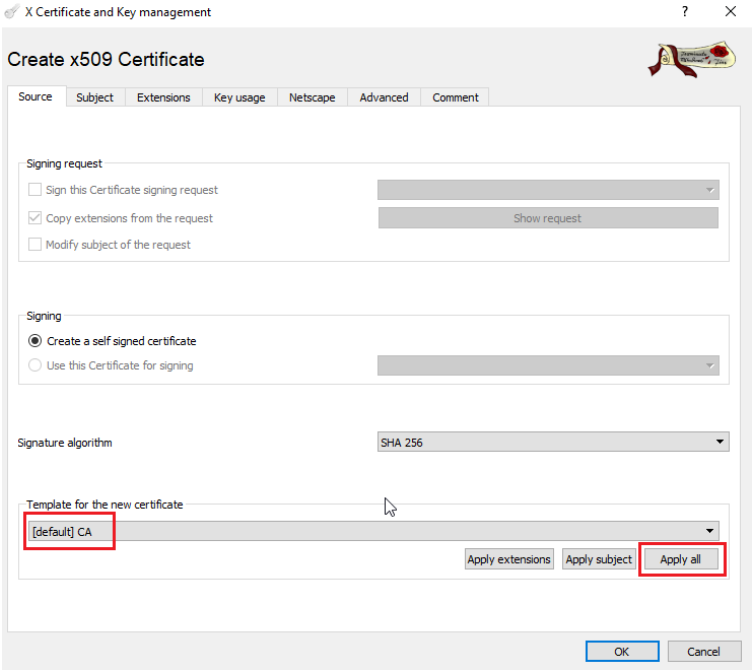
3.1.1 Create a Root CA Certificate

Open the XCA application

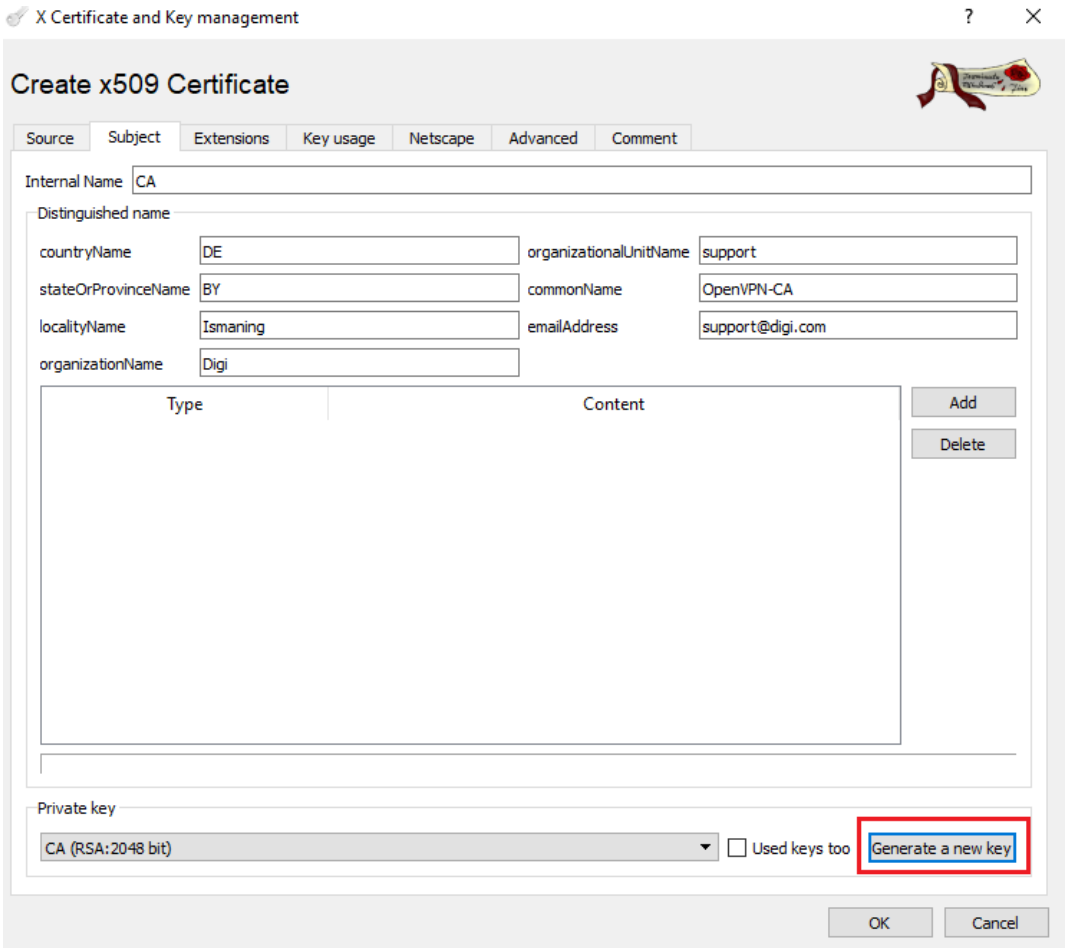
1. Click the **File** menu and select **New Database**, chose a name and click **Save.**
2. Set up a password and click **OK**
3. Click the **Certificates** tab
4. Click the **New Certificate** button



5. Under “Template for the new certificate”, select **default CA** and click **Apply all**



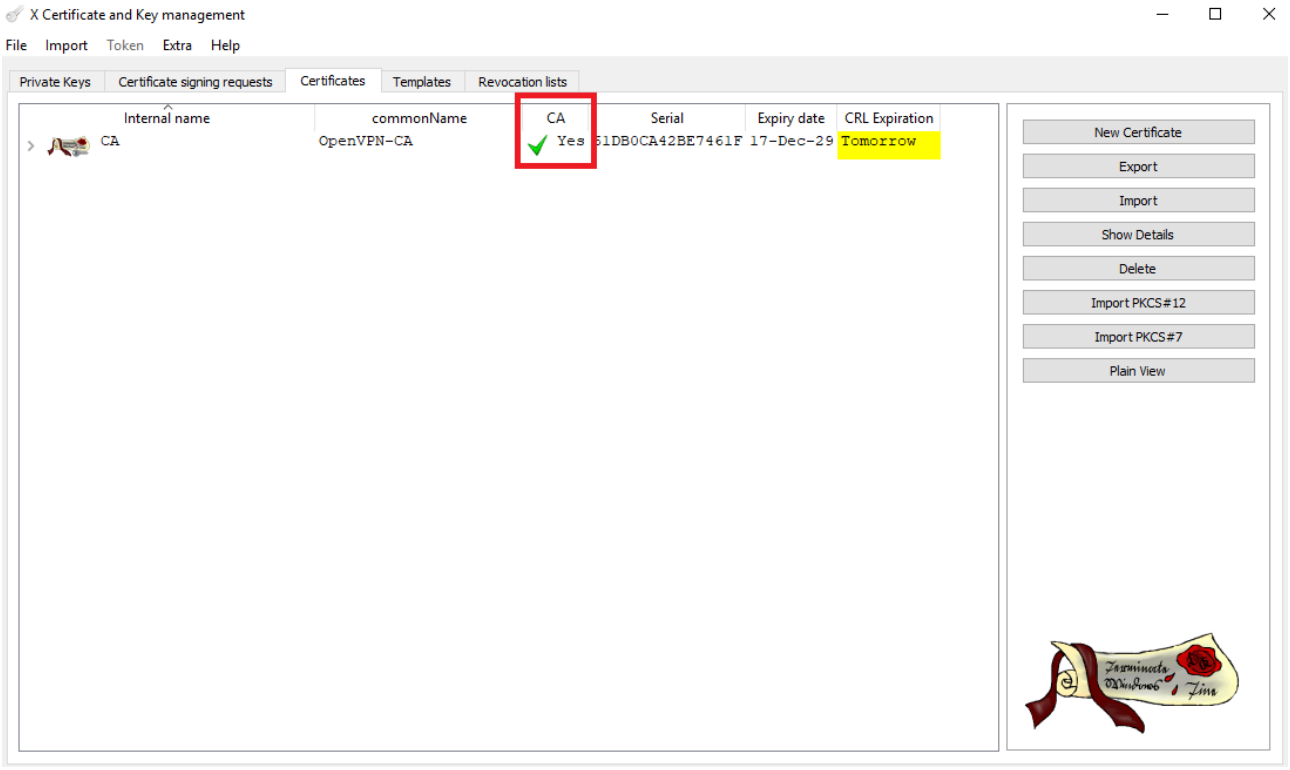
6. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Paris
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: Digi
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.

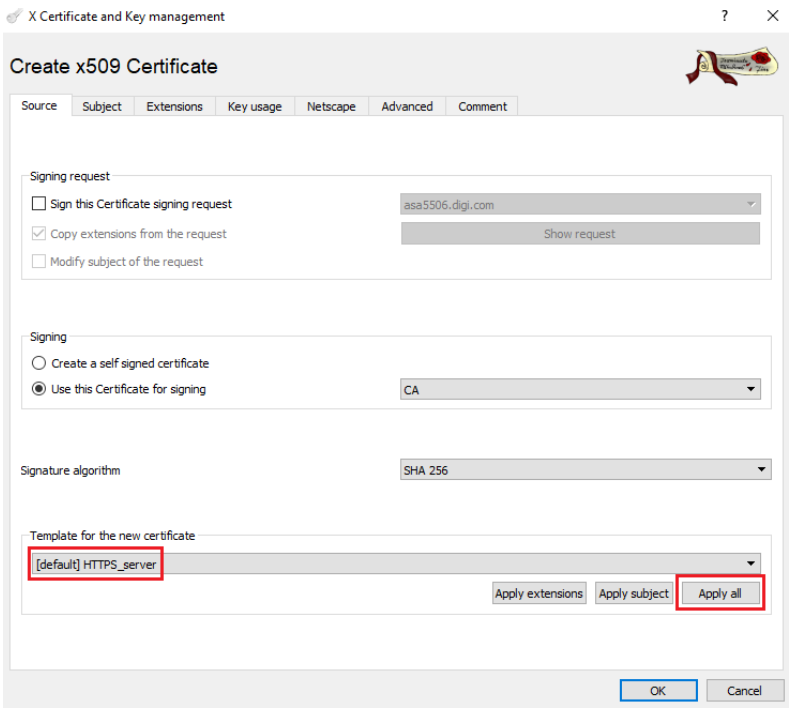
Common Name	In this example DigiCA will be used.
Email Address	Enter your organization general email address. In this example certteam@digi.com

7. The certificate should now appear in the window with the **CA : YES** confirmation. If it does not say **CA: YES,** verify that you selected CA in the template and clicked Apply All.

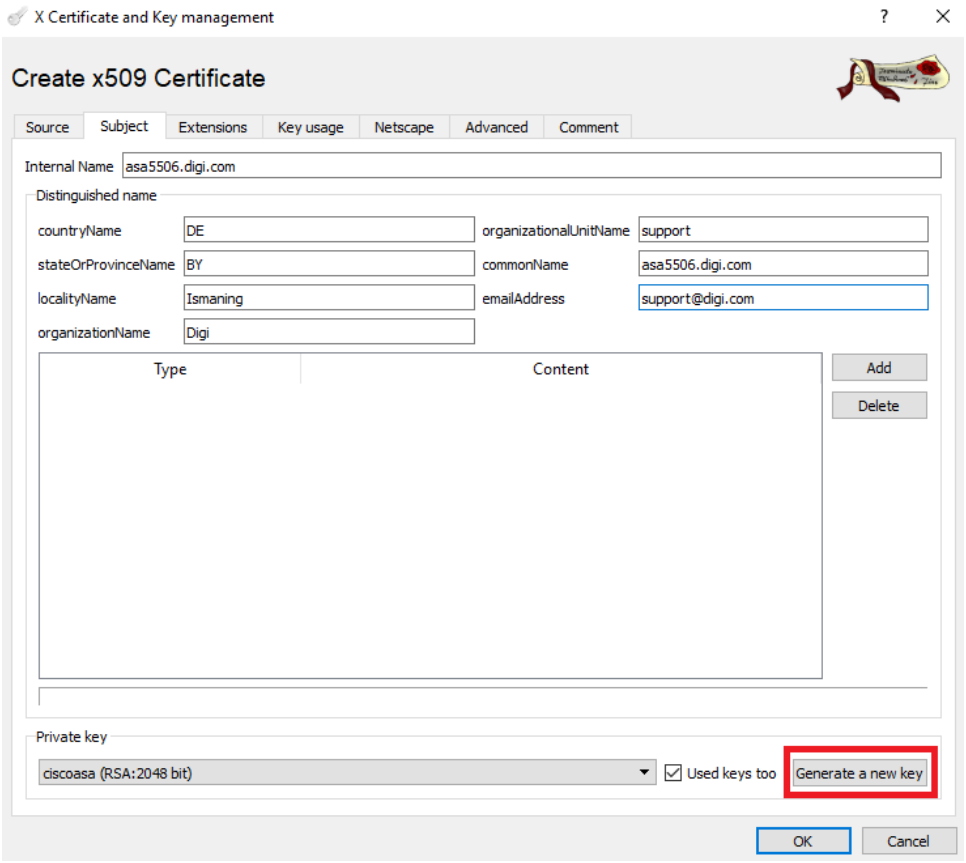


3.1.2 Create a CA-Signed Host Certificate (Cisco ASA, Responder)

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_server** and click **Apply all**

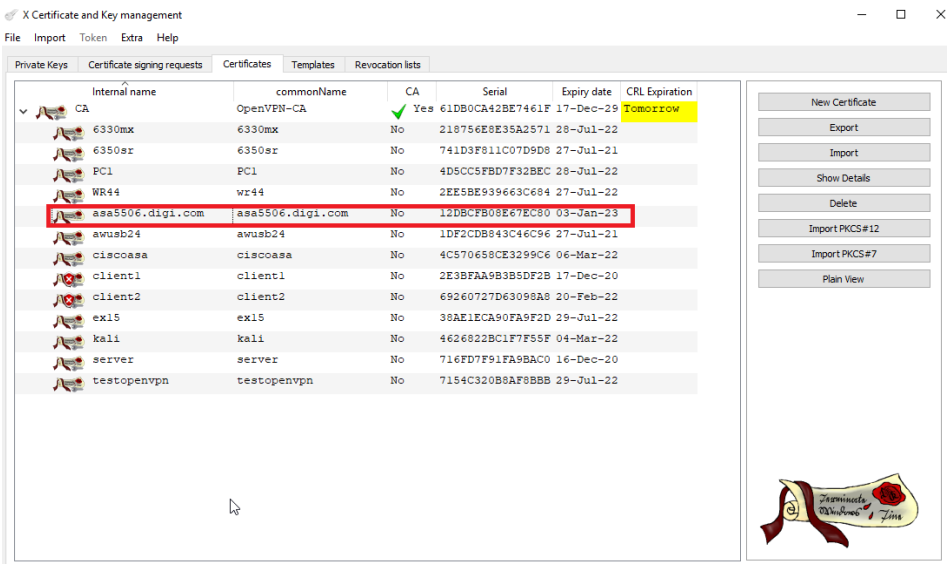


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



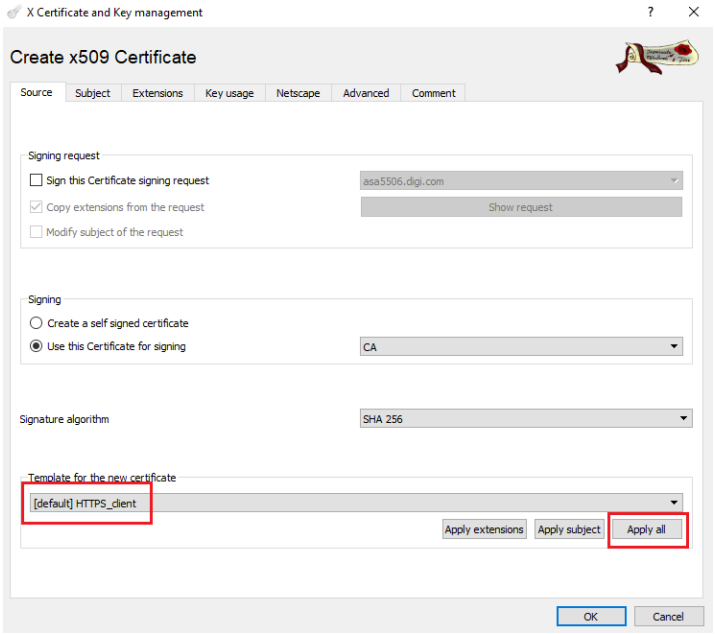
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **6330mx** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

7. The certificate should now appear in the window under the CA certificate.

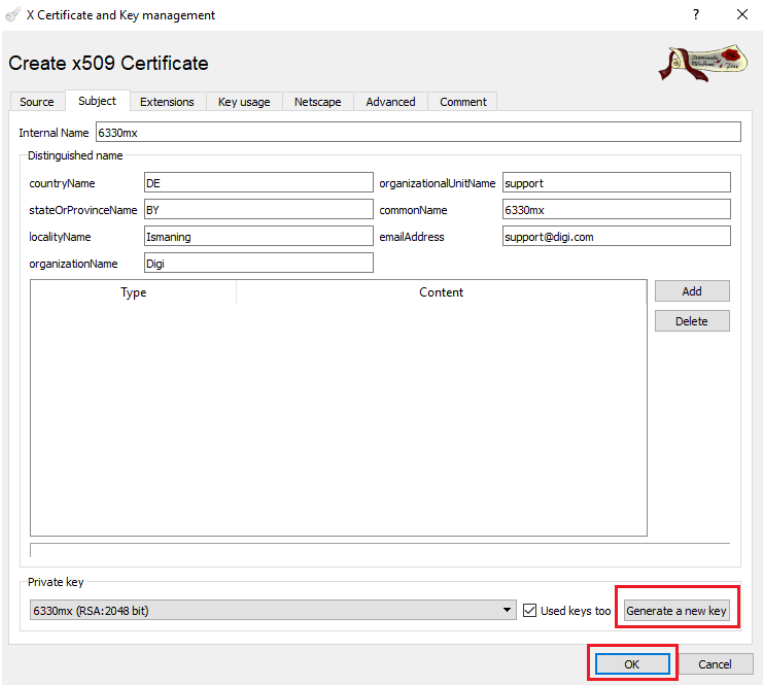


3.1.3 Create a CA-Signed Client Certificate (Digi 6330-MX, initiator)

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_client** and click **Apply all**

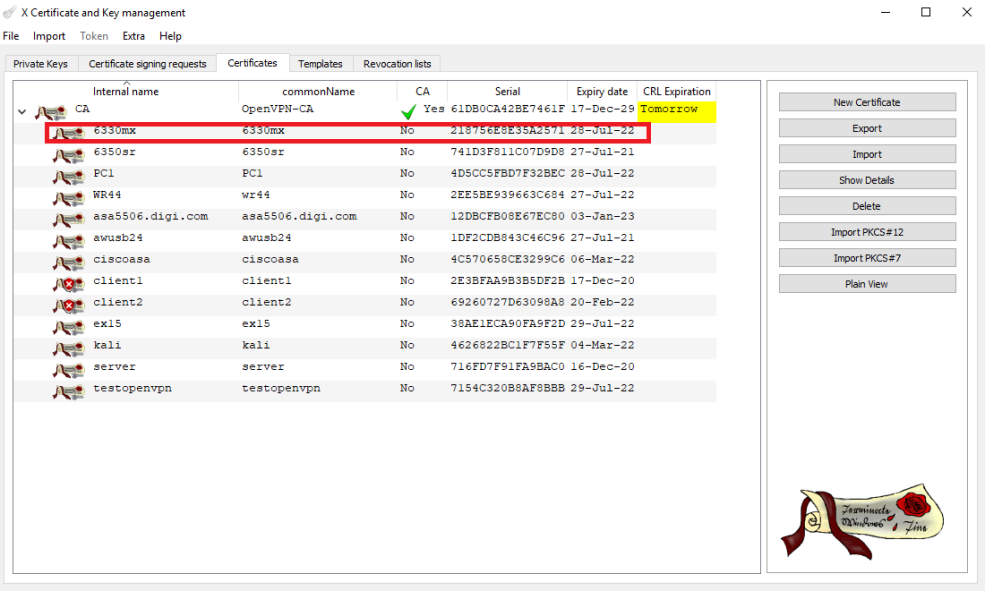


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



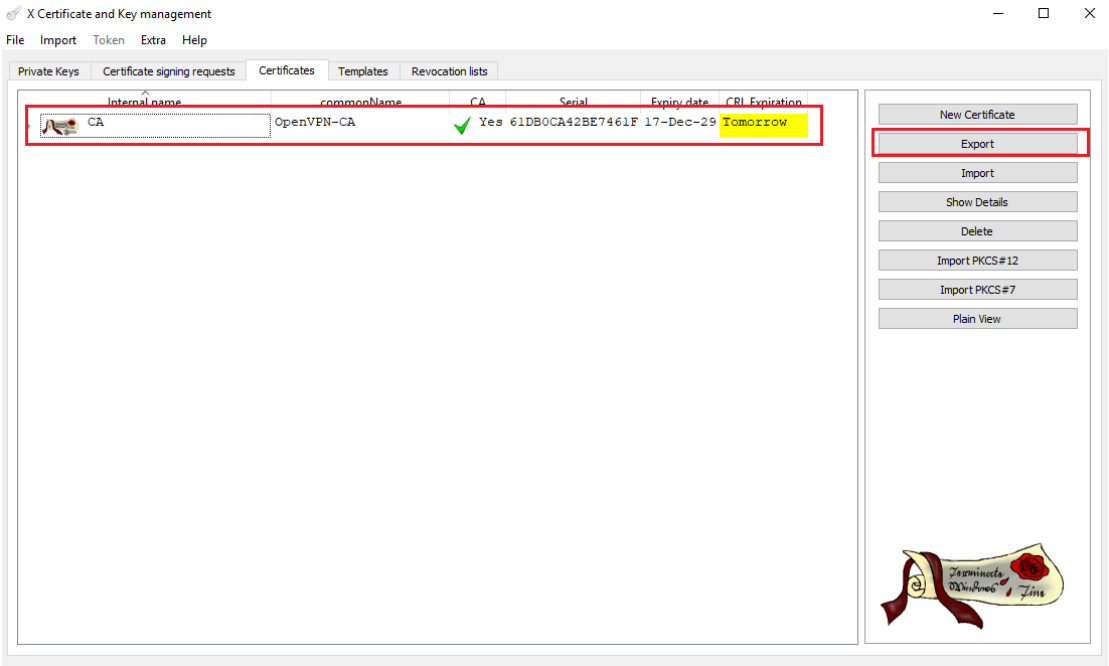
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **wrdigide** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

1. The certificate should now appear in the window under the CA certificate.

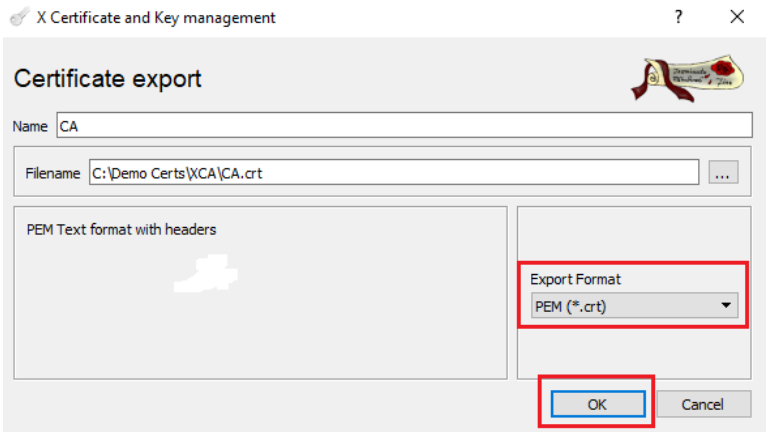


3.1.4 Export the certificates and keys in .PEM format

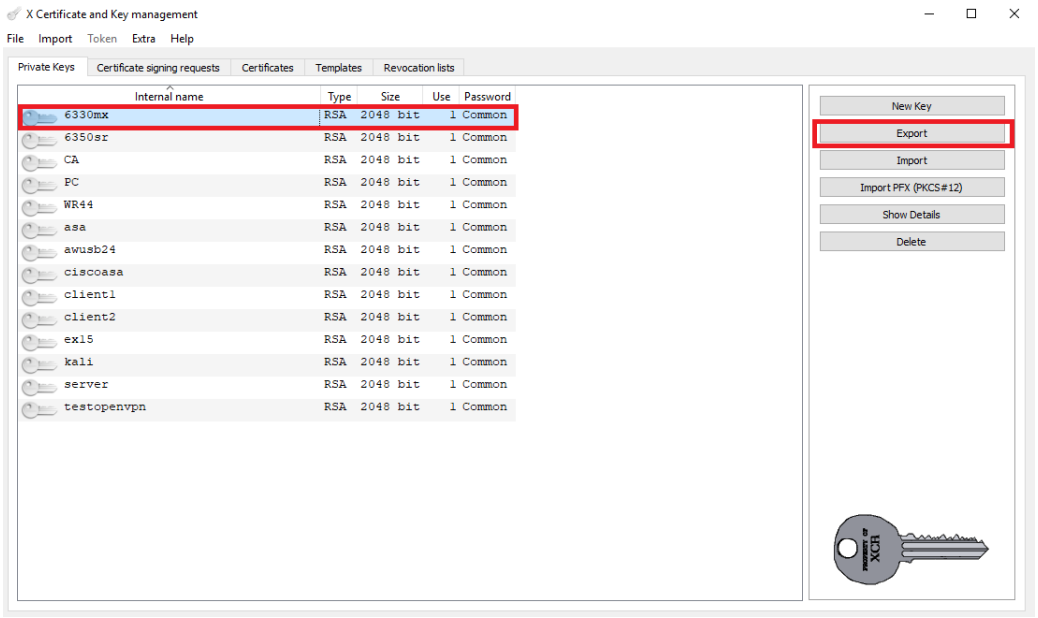
1. Select the **Certificates** Tab.
2. Highlight the CA certificate and click the **Export** button



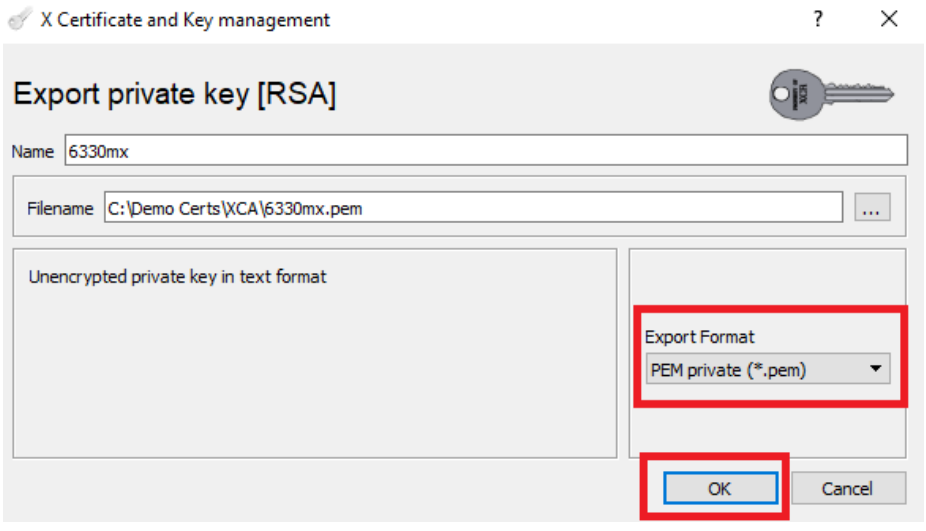
3. In the Certificate export window, select **PEM** as the export format and click **OK**



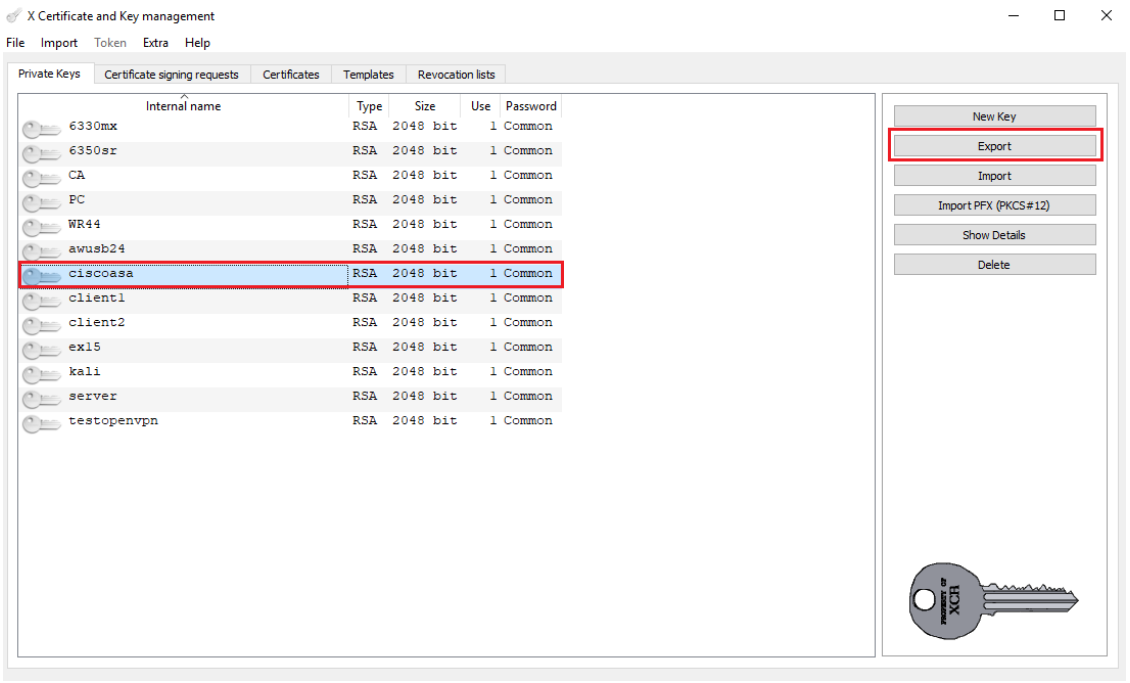
4. Repeat the previous step for the Digi router certificate.
5. Select the **Private Keys** tab.
6. Highlight the Digi 6330-MX certificate and click the **Export** button

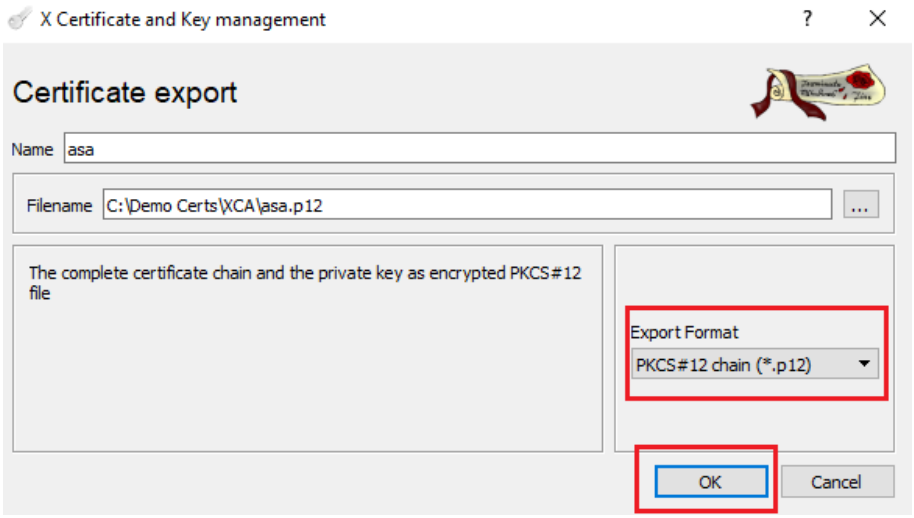


In the Key export window, select **PEM** as the export format and click **OK**



7. Repeat the previous step for the Cisco ASA certificate.
   Please note: Cisco ASA firewall requires the certificate to be concatenated with encrypted key in format PKCS#12. Make sure to check the export format as encrypted PKCS#12.





The following files should now be available:

- CA.crt : CA root certificate
- asa.p12 : Cisco ASA (responder) certificate with encrypted private key
- 6330mx.crt : Digi 6330-MX (initiator) certificate
- 6330mx.pem : Digi 6330-MX (initiator) private key

4. DIGI 6330-MX CONFIGURATION

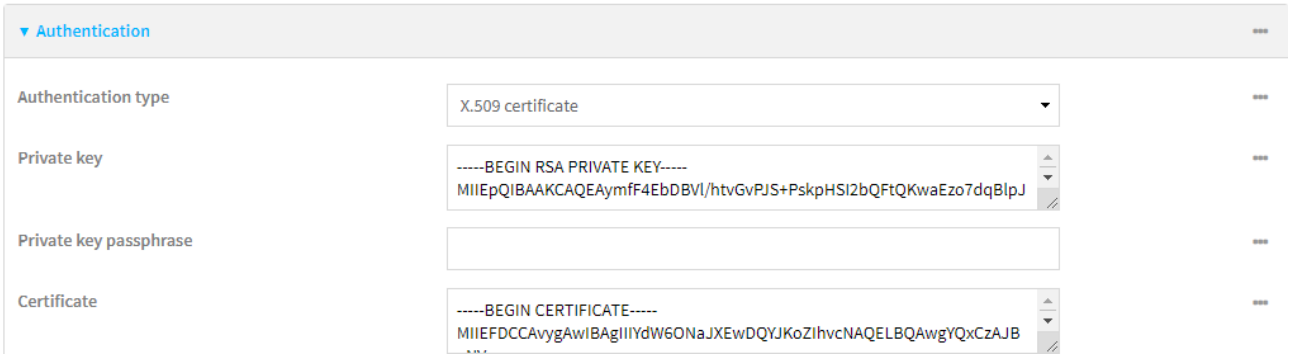
4.1 Upload SSL certificate to the Digi 6330-MX (initiator)

4.1.1 Upload the certificates via the Web GUI

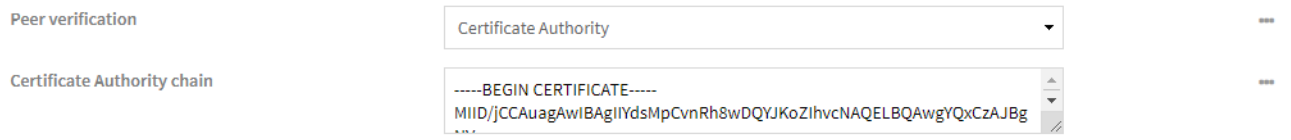
Open a web browser to the IP address of the Digi router 6330-MX (initiator)

System > Configuration > VPN > IPSec > Tunnels > Tunnel name > Authentication

Click on the drop down menu **Authentication type** and select X.509 certificate option.
Then open Certificate and Private key files (6330mx.crt, 6330mx.pem) with any text editor and copy/paste all content of the files to the corresponding configuration fields.



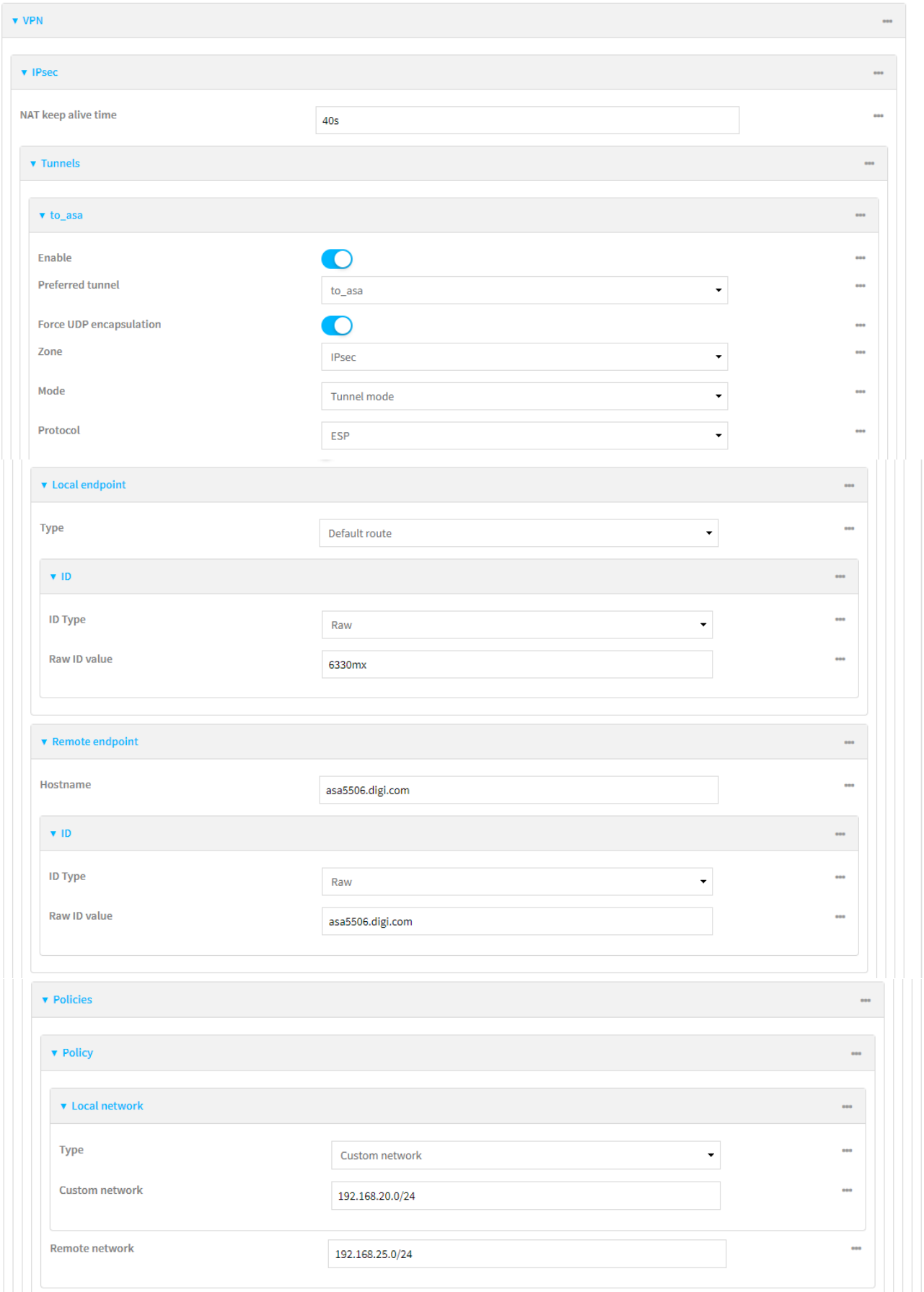
Click on the drop down menu **Peer verification** and select **Certificate Authority** option.
Then copy and paste content of the file CA.crt to the Certificate Authority chain field.

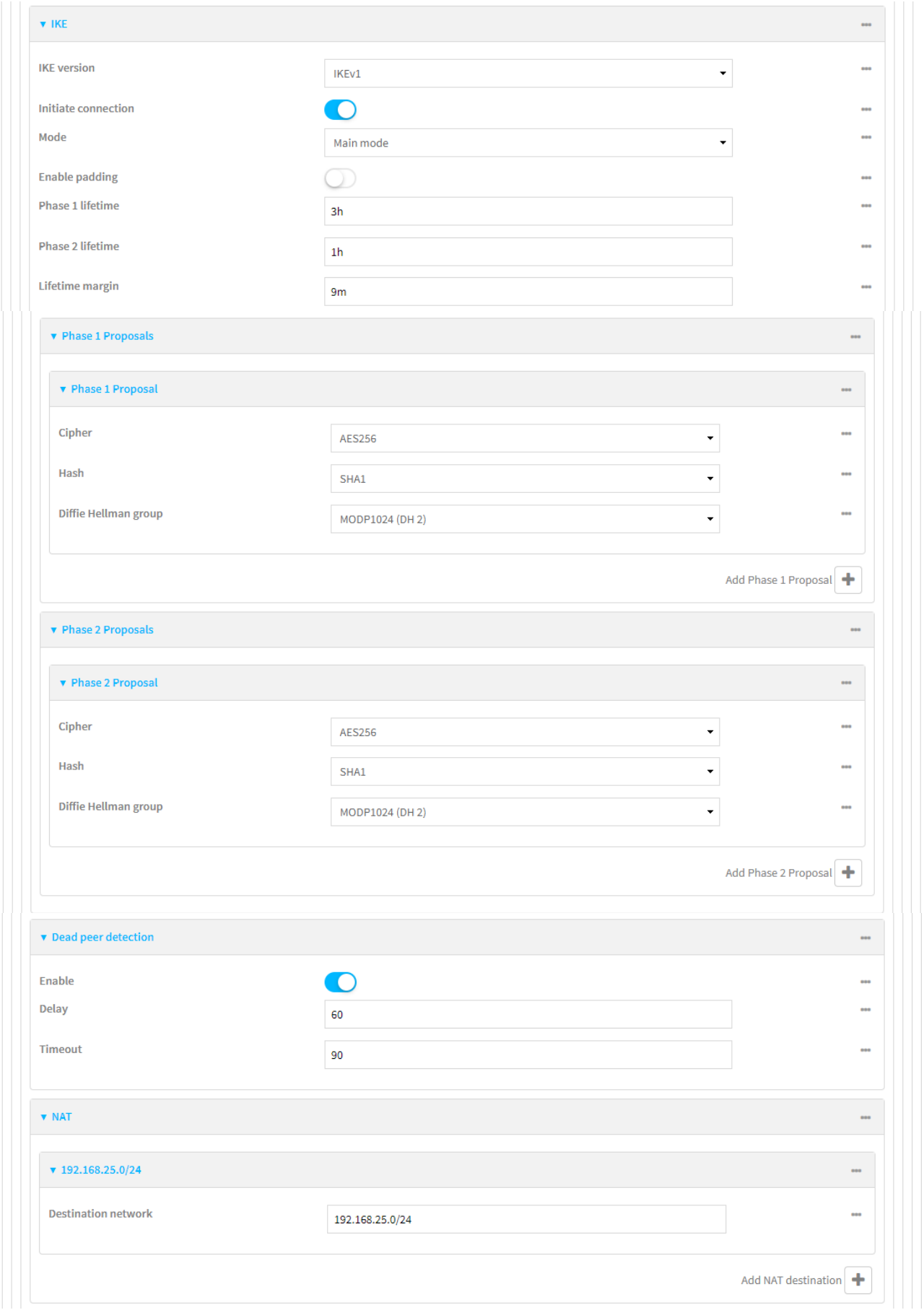


4.2 Configure the VPN Tunnel settings on the Digi 6330-MX (Initiator).

Follow the Web UI interface path:
System > Configuration > VPN > IPSec > Tunnels
Add a new IPSec tunnel with the appropriate configuration as indicated on the screenshot below:

To avoid a problem with network address translation, when cellular provider does not allocate a public IP addresses to the clients, an UDP encapsulation was enforced in the settings.


▾ VPN
▾ IPsec
NAT keep alive time
40s
▾ Tunnels
▾ to_asa
Enable
Preferred tunnel
to_asa
Force UDP encapsulation
Zone
IPsec
Mode
Tunnel mode
Protocol
ESP
▾ Local endpoint
Type
Default route
▾ ID
ID Type
Raw
Raw ID value
6330mx
▾ Remote endpoint
Hostname
asa5506.digi.com
▾ ID
ID Type
Raw
Raw ID value
asa5506.digi.com
▾ Policies
▾ Policy
▾ Local network
Type
Custom network
Custom network
192.168.20.0/24
Remote network
192.168.25.0/24


▾ IKE
IKE version
IKEv1
Initiate connection
Mode
Main mode
Enable padding
Phase 1 lifetime
3h
Phase 2 lifetime
1h
Lifetime margin
9m
▾ Phase 1 Proposals
▾ Phase 1 Proposal
Cipher
AES256
Hash
SHA1
Diffie Hellman group
MODP1024 (DH 2)
Add Phase 1 Proposal
▾ Phase 2 Proposals
▾ Phase 2 Proposal
Cipher
AES256
Hash
SHA1
Diffie Hellman group
MODP1024 (DH 2)
Add Phase 2 Proposal
▾ Dead peer detection
Enable
Delay
60
Timeout
90
▾ NAT
▾ 192.168.25.0/24
Destination network
192.168.25.0/24
Add NAT destination

Parameter	Setting	Description
Description	to_asa	Description of the IPsec tunnel
Remote endpoint IP Address / Hostname	asa5506.digi.com	IP Address or hostname of the remote endpoint router (responder)
Local Network	192.168.20.0/24	Local Lan IP address
Remote Network	192.168.25.0/24	Remote Lan IP address
Local endpoint Type	Default route	The method of determining the local network interface that is used to communicate with the peer
ID Type	Raw	The type of identifier to be used
Local endpoint ID value	6330mx	ID that is matching the CN of the certificate in the Digi router (initiator)
Local network Type	Custom network	The method for determining the local network
Remote endpoint ID value	asa5506.digi.com	Remote ID that is matching the CN in the Cisco ASA firewall certificate (responder)
Phase 1 lifetime	3 hours	The period of time after a successful negotiation that the IKE security association expires and must be reauthenticated
Phase 2 lifetime	1 hour	The period of time after a successful negotiation that the IPSec security association expires and must be rekeyed
Lifetime margin	9 minutes	The amount of time before the end of the Phase 1 and Phase 2 lifetimes that renegotiation may be initiated
IKE version	1	IKE protocol version used to setup the tunnel
Enable padding	disabled	Enable padding of IKE packets to 4 bytes
Initiate connection	enable	Initiate the key exchange, rather than waiting for an incoming request
Mode	Main mode	The IKE Phase 1 mode determines how to establish a secure channel between the peers for the further negotiation
NAT Destination network	192.168.25.0/24	The destination network that requires source NAT
Dead peer detection	enable	Dead peer detection uses periodic IKE transmissions to the remote endpoint to detect whether tunnel communications have failed

Parameter	Setting	Description
Phase 1 Cipher	AES (256 bit)	Encryption settings used on the Phase 1
Phase 2 Cipher	AES (256 bit)	Encryption settings used on the Phase 2
Phase 1 Hash	SHA1	The Hash to use for checking communication integrity on Phase 1
Phase 1 Hash	SHA1	The Hash to use for checking communication integrity on Phase 2
MODP Group for Phase 1	2 (1024)	DH Phase 1
MODP Group for Phase 2	2 (1024)	DH Phase 2

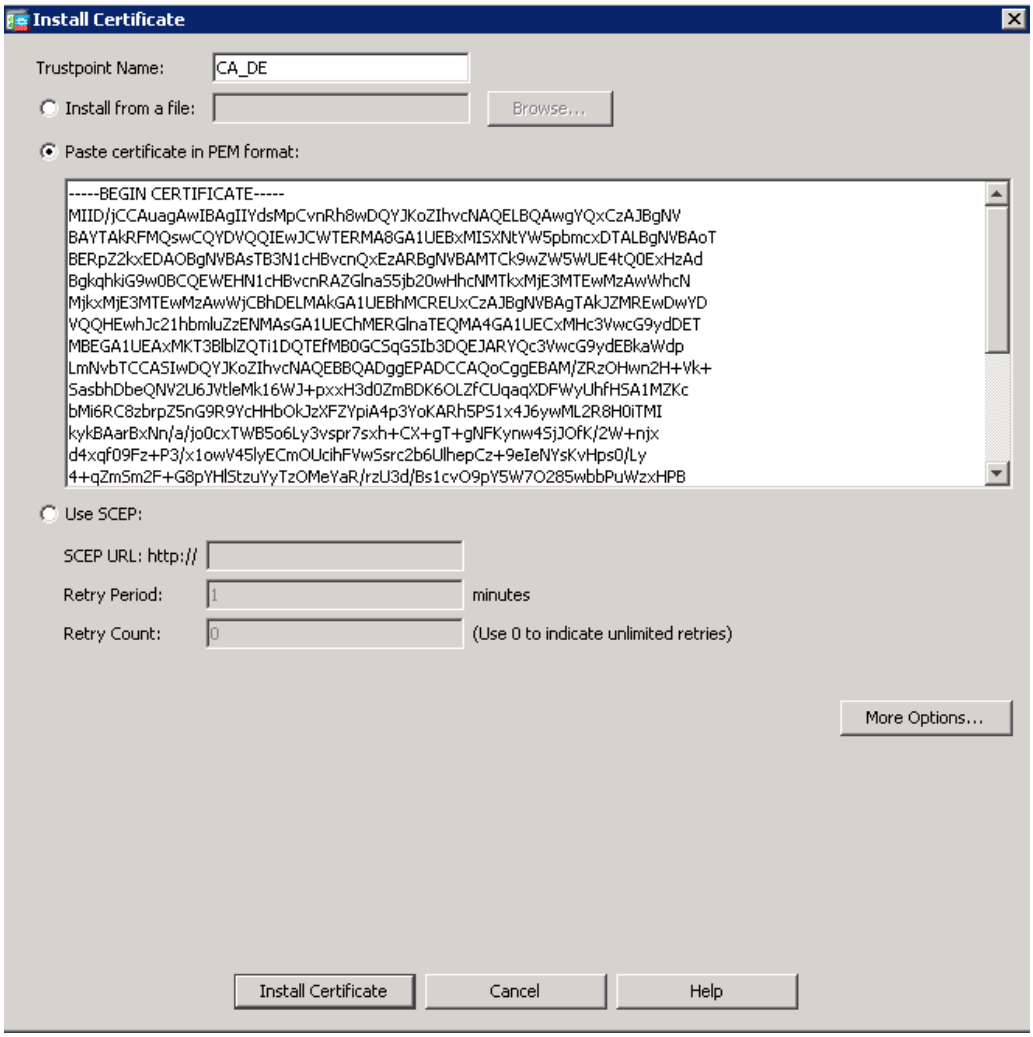
Click **Apply** to save the settings.

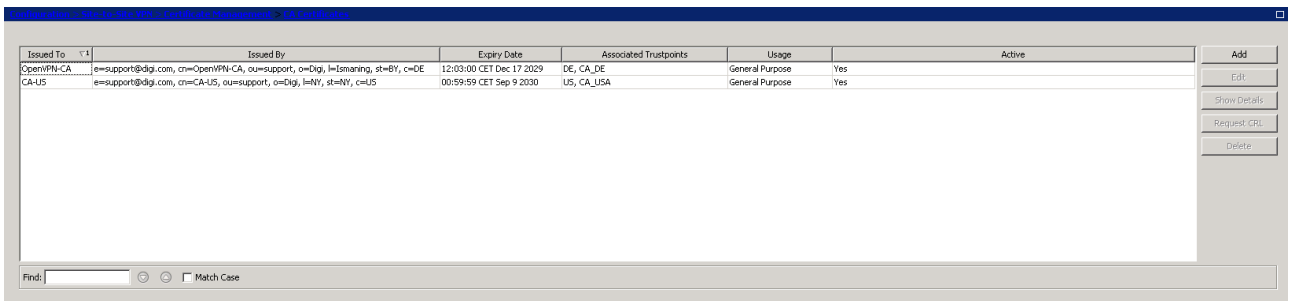
5. CISCO ASA CONFIGURATION

The values for Date, Time, and Time Zone must be accurate in order for the proper certificate validation to occur.

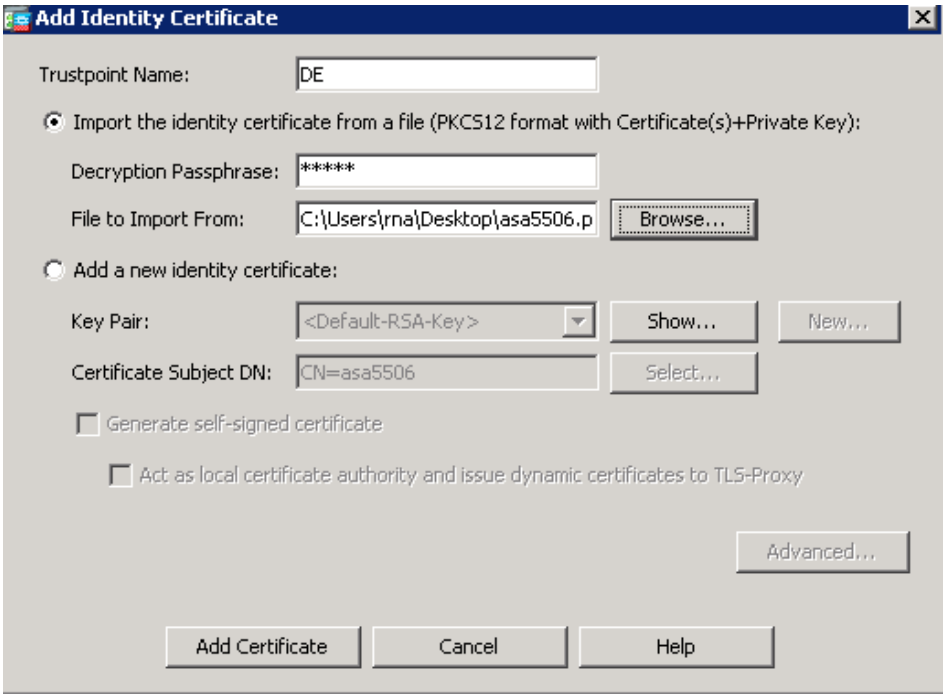
5.1 Import the certificates and private key

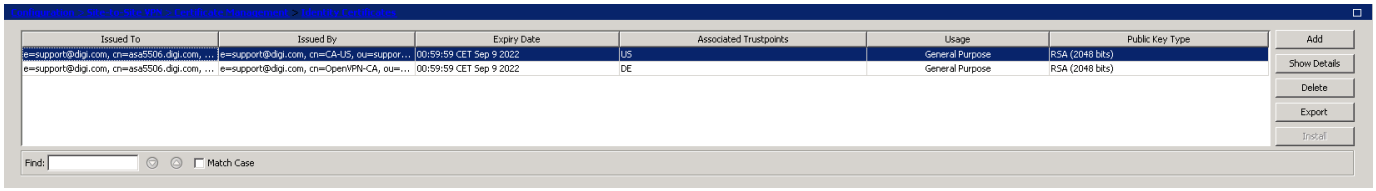
5.1.1 Create a Trustpoint for the CA root certificate via ASDM and import the CA root certificate in the created Trustpoint with copy and paste





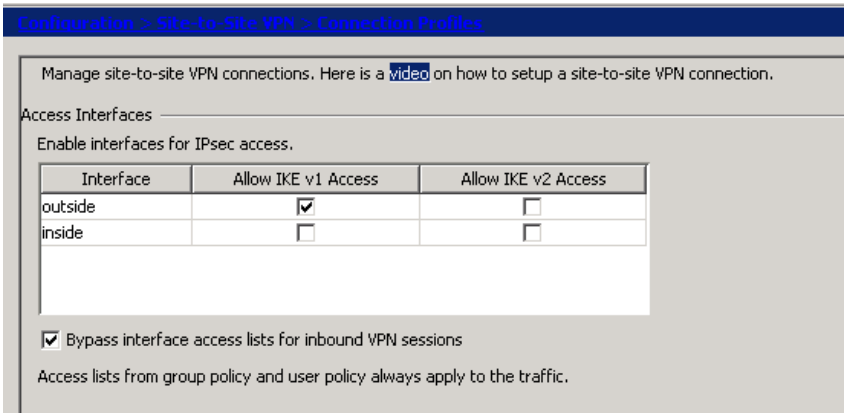
5.1.2 Create a Trustpoint for the identity certificate and import the public certificate and the private key in the created Trustpoint with a PKCS#12 file.



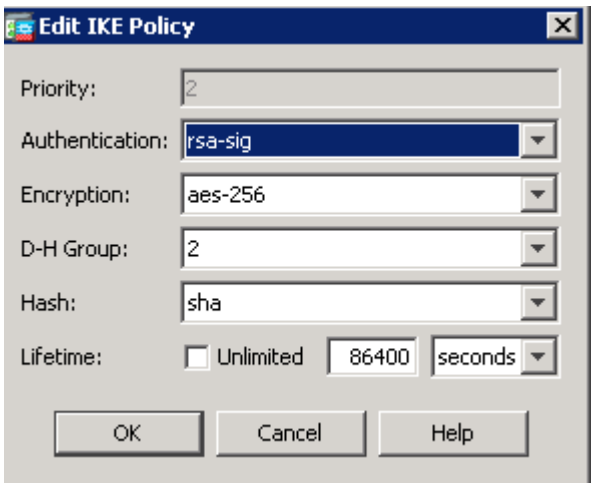


5.2 Configure the tunnel

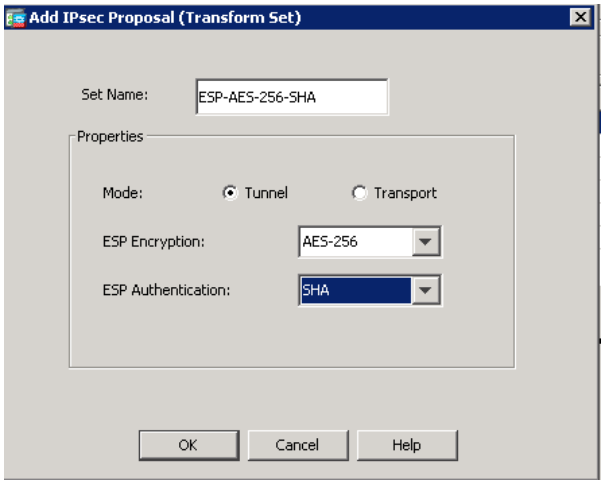
Enable outside interface for IPSec access:



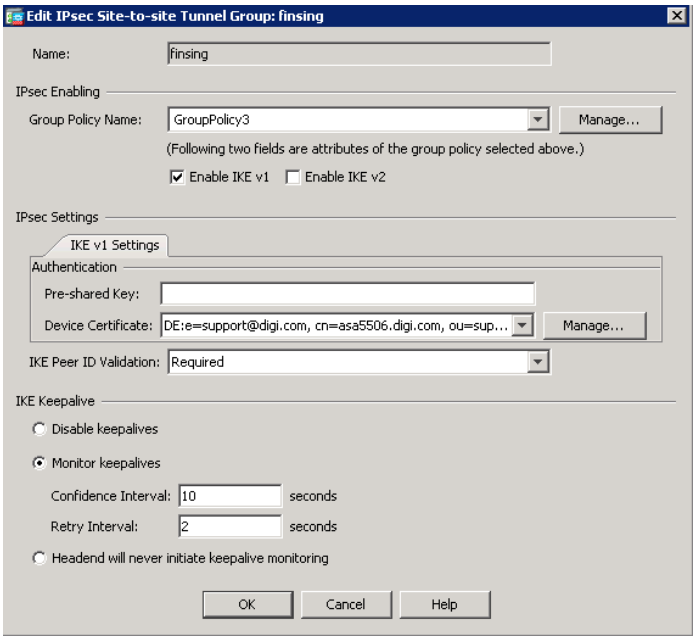
Create an IKEv1 policy



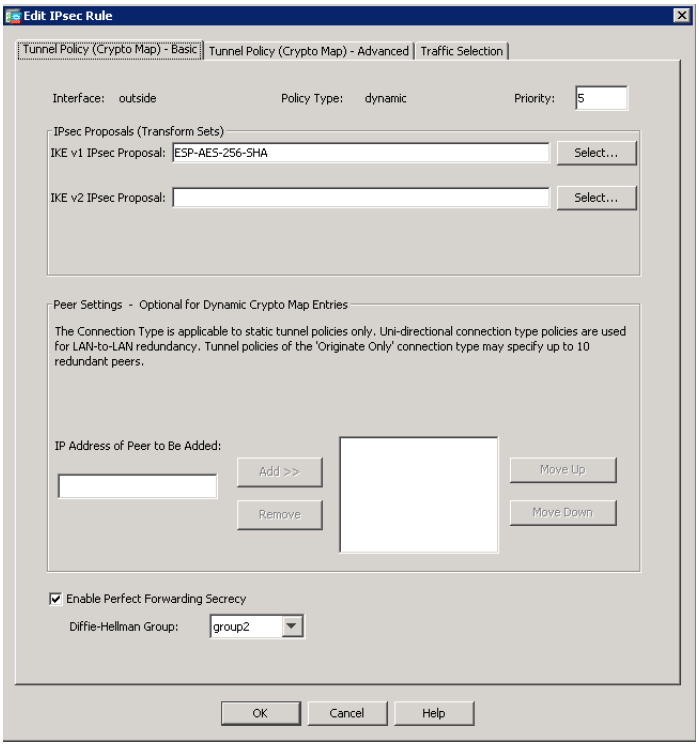
Create IKEv1 IPSec proposal:

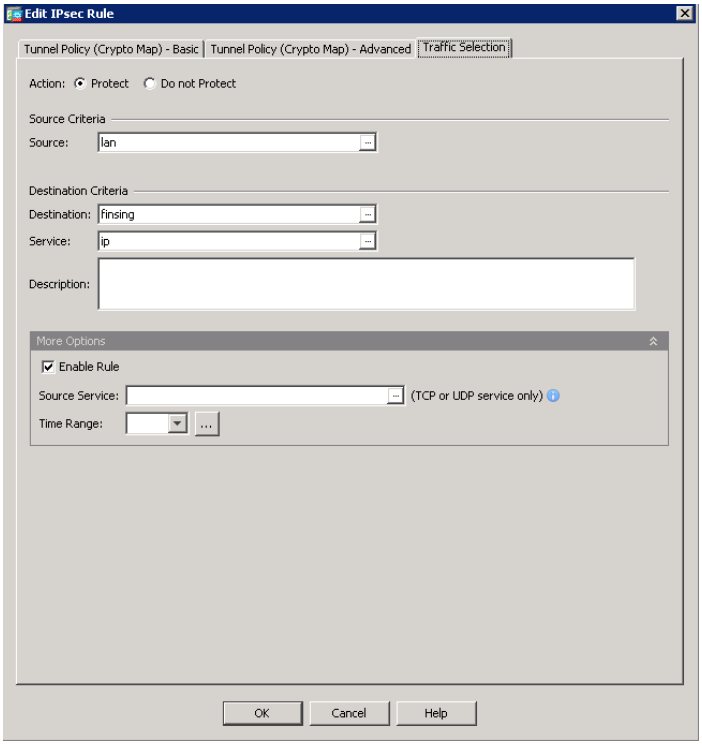


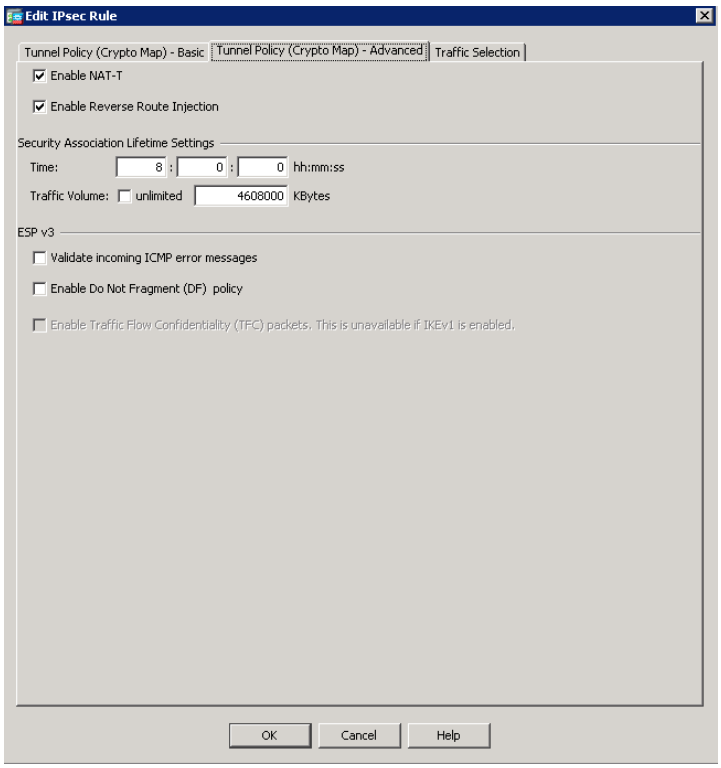
Configure IPSec Site-to-Site Tunnel group:



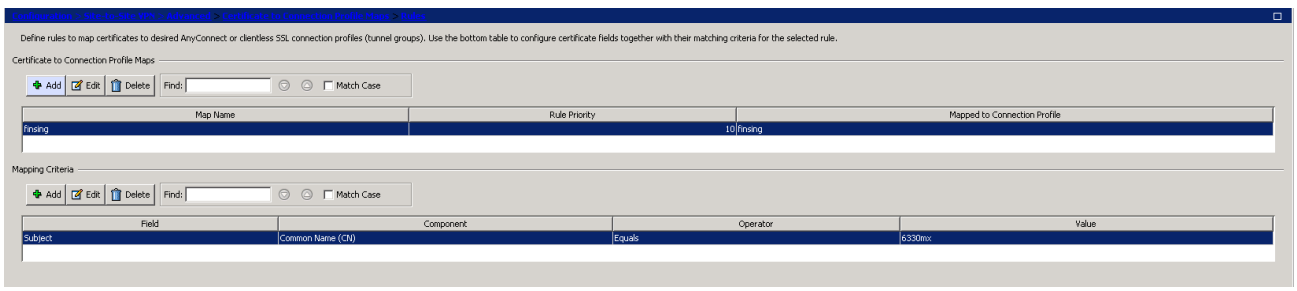
Configure Crypto Map:


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Interface: outside
Policy Type: dynamic
Priority: 5
IPsec Proposals (Transform Sets)
IKE v1 IPsec Proposal: ESP-AES-256-SHA
Select...
IKE v2 IPsec Proposal:
Select...
Peer Settings - Optional for Dynamic Crypto Map Entries
The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.
IP Address of Peer to Be Added:
Add >>
Remove
Move Up
Move Down
Enable Perfect Forwarding Secrecy
Diffie-Hellman Group: group2
OK
Cancel
Help


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Action: Protect
Do not Protect
Source Criteria
Source: lan
Destination Criteria
Destination: finsing
Service: ip
Description:
More Options
Enable Rule
Source Service:
(TCP or UDP service only)
Time Range:
OK
Cancel
Help



Create certificate to Connection profile maps rule:



The Cisco ASA is now configured and the tunnel should come up.

6. TESTING

This section will show that the IPSec tunnel has been established.

Cisco ASA

```
asa5506# sh crypto isa sa detail

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 95.115.25.102
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : aes-256         Hash    : SHA
    Auth    : rsa             Lifetime: 10800
    Lifetime Remaining: 9552

There are no IKEv2 SAs


asa5506# sh crypto ipsec sa peer 95.115.25.102
peer address: 95.115.25.102
    Crypto map tag: finsing, seq num: 5, local addr: 37.81.85.5

      access-list outside_cryptomap extended permit ip 192.168.25.0 255.255.255.0 192.168.20.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.25.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
      current_peer: 95.115.25.102


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 37.81.85.5/4500, remote crypto endpt.: 95.115.25.102/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CE754E6D
      current inbound spi : 0BF0F91E

    inbound esp sas:
      spi: 0x0BF0F91E (200341790)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, PFS Group 2, IKEv1, }
         slot: 0, conn_id: 2331, crypto-map: finsing
         sa timing: remaining key lifetime (kB/sec): (3915000/2320)
         IV size: 16 bytes
         replay detection support: Y
```

```
        Anti replay bitmap:
         0x00000000 0x00000001
    outbound esp sas:
      spi: 0xCE754E6D (3463794285)
        SA State: active
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, PFS Group 2, IKEv1, }
        slot: 0, conn_id: 2331, crypto-map: finsing
        sa timing: remaining key lifetime (kB/sec): (3915000/2320)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Digi 6330-MX

```
# ipsec status
Shunted Connections:
Bypass LAN 127.0.0.0/8:  127.0.0.0/8 === 127.0.0.0/8 PASS
Bypass LAN 192.168.1.0/24:  192.168.1.0/24 === 192.168.1.0/24 PASS
Bypass LAN 192.168.1.1/32:  192.168.1.1/32 === 192.168.1.1/32 PASS
Bypass LAN fe80::ce32:e5ff:fe59:f2a9/128:  fe80::ce32:e5ff:fe59:f2a9/128 === fe80::ce32:e5ff:fe59:f2a9/128
PASS
Bypass LAN fe80::/64:  fe80::/64 === fe80::/64 PASS
Bypass LAN 169.254.0.0/16:  169.254.0.0/16 === 169.254.0.0/16 PASS
Bypass LAN 192.168.20.0/24:  192.168.20.0/24 === 192.168.20.0/24 PASS
Bypass LAN 192.168.210.0/24:  192.168.210.0/24 === 192.168.210.0/24 PASS
Bypass LAN fd00:2704::/64:  fd00:2704::/64 === fd00:2704::/64 PASS
Security Associations (1 up, 0 connecting):
 to_asa_1of1[155]: ESTABLISHED 17 minutes ago, 192.168.1.119[6330mx]...37.81.85.5[asa5506.digi.com]
 to_asa_1of1{128}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: ce754e6d_i 0bf0f91e_o
 to_asa_1of1{128}:   192.168.20.0/24 === 192.168.25.0/24


# ip -s xfrm state
src 192.168.1.119 dst 37.81.85.5
        proto esp spi 0x0bf0f91e(200341790) reqid 1(0x00000001) mode tunnel
        replay-window 0 seq 0x00000000 flag af-unspec (0x00100000)
        auth-trunc hmac(sha1) 0xa69f3c0555d8f899e7124297ca6e3f2746509fc5 (160 bits) 96
        enc cbc(aes) 0xdff342216a6143a80f63bfa24f61b3eab1b223619dbeb8b15507051506055335 (256 bits)
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
          expire add: soft 2954(sec), hard 3600(sec)
          expire use: soft 0(sec), hard 0(sec)
        lifetime current:
          0(bytes), 0(packets)
          add 2020-09-10 17:20:03 use -
        stats:
          replay-window 0 replay 0 failed 0
src 37.81.85.5 dst 192.168.1.119
        proto esp spi 0xce754e6d(3463794285) reqid 1(0x00000001) mode tunnel
        replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
        auth-trunc hmac(sha1) 0x766a9dccbfa77a94d1c150a7c84620c835430871 (160 bits) 96
        enc cbc(aes) 0x1b2cfb289992da38288f3e86af505256bc66824f15e333b425c1ba8641c5c2b5 (256 bits)
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
```

```
  expire add: soft 2935(sec), hard 3600(sec)
  expire use: soft 0(sec), hard 0(sec)
lifetime current:
  0(bytes), 0(packets)
  add 2020-09-10 17:20:03 use -
stats:
  replay-window 0 replay 0 failed 0
```

6.1 Confirm Traffic Traverses the IPSec Tunnels

This section will show traffic passing across the tunnel. To test this easily, an ICMP Echo Request/Reply (or PING) will pass from the Digi router 6330-MX lan (initiator) to Cisco ASA firewall Ethernet interface side (responder)

```
#  ping 192.168.25.1
PING 192.168.25.1 (192.168.25.1) 56(84) bytes of data.
64 bytes from 192.168.25.1: icmp_seq=1 ttl=255 time=118 ms
64 bytes from 192.168.25.1: icmp_seq=2 ttl=255 time=76.6 ms
64 bytes from 192.168.25.1: icmp_seq=3 ttl=255 time=125 ms
64 bytes from 192.168.25.1: icmp_seq=4 ttl=255 time=72.9 ms
64 bytes from 192.168.25.1: icmp_seq=5 ttl=255 time=111 ms
64 bytes from 192.168.25.1: icmp_seq=6 ttl=255 time=79.0 ms
^C
--- 192.168.25.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 72.912/97.127/125.054/21.414 ms
```

```
asa5506# ping inside 192.168.20.1 repeat 5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/82/110 ms
```

7. CONFIGURATION FILES

Digi 6330-MX

```
auth group admin acl shell enable "true"
auth idle_timeout ""
network interface lan ipv4 address "192.168.20.1/24"
add service dns host end
service dns host 0 address "37.81.85.5"
service dns host 0 name "asa5506.digi.com"
add vpn ipsec tunnel to_asa
vpn ipsec tunnel to_asa auth cert "-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----"
vpn ipsec tunnel to_asa auth peer_ca "-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----"
vpn ipsec tunnel to_asa auth peer_verify "ca"
vpn ipsec tunnel to_asa auth private_key "-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----"
vpn ipsec tunnel to_asa auth type "x509"
vpn ipsec tunnel to_asa force_udp_encap "true"
add vpn ipsec tunnel to_asa ike phase1_proposal end
vpn ipsec tunnel to_asa ike phase1_proposal 0 cipher "aes256"
vpn ipsec tunnel to_asa ike phase1_proposal 0 dh_group "modp1024"
add vpn ipsec tunnel to_asa ike phase2_proposal end
vpn ipsec tunnel to_asa ike phase2_proposal 0 cipher "aes256"
vpn ipsec tunnel to_asa ike phase2_proposal 0 dh_group "modp1024"
vpn ipsec tunnel to_asa ipsec_failover "to_asa"
vpn ipsec tunnel to_asa local id raw_id "6330mx"
vpn ipsec tunnel to_asa local id type "raw"
add vpn ipsec tunnel to_asa nat end
vpn ipsec tunnel to_asa nat 0 dst "192.168.25.0/24"
add vpn ipsec tunnel to_asa policy end
vpn ipsec tunnel to_asa policy 0 local custom "192.168.20.0/24"
vpn ipsec tunnel to_asa policy 0 local type "custom"
vpn ipsec tunnel to_asa policy 0 remote network "192.168.25.0/24"
vpn ipsec tunnel to_asa remote hostname "asa5506.digi.com"
vpn ipsec tunnel to_asa remote id raw_id "asa5506.digi.com"
vpn ipsec tunnel to_asa remote id type "raw"
```

Cisco ASA

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map finsing 5 match address outside_cryptomap
crypto dynamic-map finsing 5 set pfs
crypto dynamic-map finsing 5 set ikev1 transform-set ESP-AES-256-SHA
crypto dynamic-map finsing 5 set reverse-route
crypto map outside_map 5 ipsec-isakmp dynamic finsing
crypto map outside_map interface outside
crypto ca trustpoint CA_DE
 enrollment terminal
 crl configure
crypto ca trustpoint DE
 keypair DE
 no validation-usage
 crl configure
crypto ca trustpool policy
crypto ca certificate map finsing 10
 subject-name attr cn eq 6330mx
```

```
crypto ca certificate chain CA_DE
 certificate ca 61db0ca42be7461f

  quit
crypto ca certificate chain DE
 certificate 0c22bf3f170cab4c

  quit
 certificate ca 61db0ca42be7461f

  quit
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication rsa-sig
 encryption aes
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 2
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```