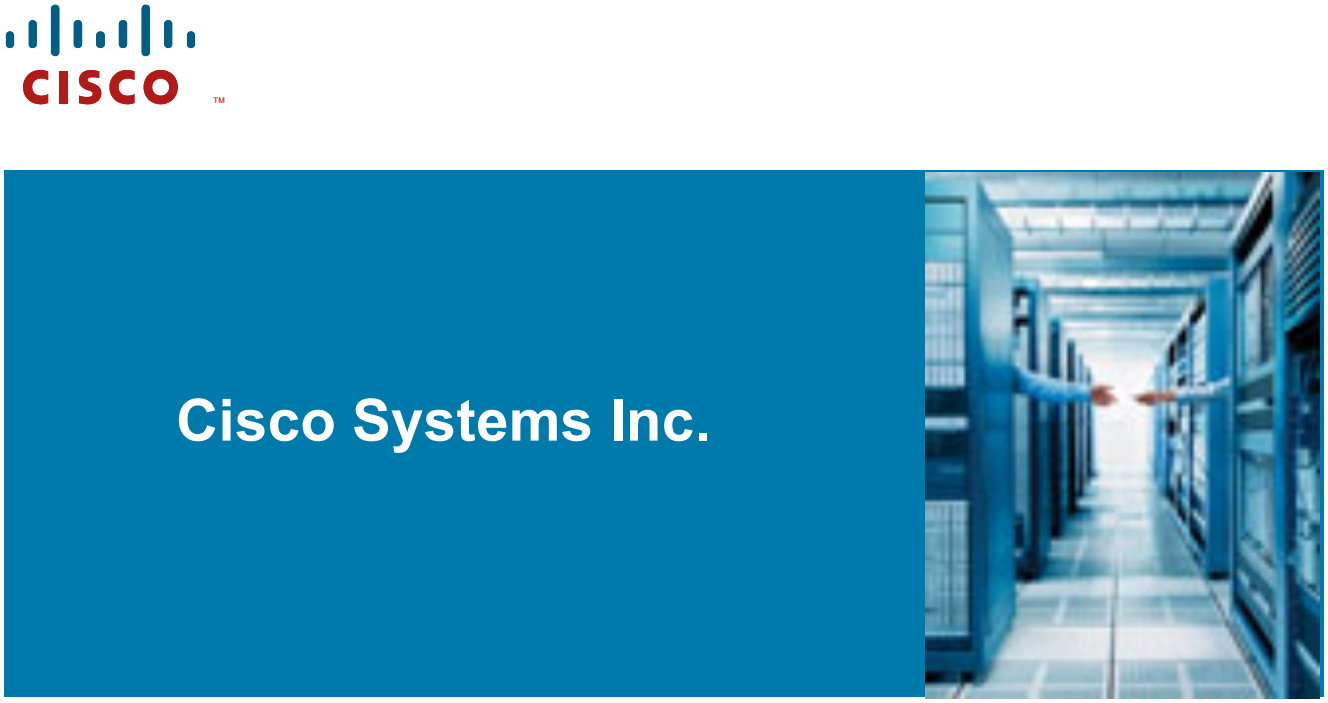


Deploying Next Generation Encryption with the AnyConnect Secure Mobility Client and the ASA 5500-X

Version 3.0

Authored by:

Justin Poole – CCIE #16224 (R&S, Sec)

Kris Swanson

Corporate Headquarters
Cisco
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Contents

Document Control

History

Table 1 Revision History

Version No.	Issue Date	Status	Reason for Change
1.0	1-30-2014	Initial Draft	
2.0	2-7-2014	First Update	
3.0	2-17-2014	2nd Update	

Review

Table 2 Revision Review

Reviewer's Details	Version No.	Date
Arnold Ocasio	1.0	2-7-2014
Andrew Benhase	1.0, 3.0	2-7-2014, 2-17-2014
Stephen Orr	1.0, 3.0	2-7-2014, 2-17-2014

Executive Summary

This document provides guidance on the implementation of a Next Generation Encryption (NGE) VPN solution utilizing the AnyConnect (AC) Secure Mobility Client and the ASA 5500-X series firewall. This design will utilize an Elliptic Curve Cryptography (ECC) Public Key Infrastructure (PKI) implementation along with cipher suites as defined in IETF RFC 6379, to create a secure VPN solution.

The ASA 5500-X series next-generation firewall will act as the head-end VPN terminating device while the clients will use the Cisco AnyConnect Secure Mobility client for VPN connectivity. X.509 Elliptic Curve (EC) certificates for authentication and security association (SA) establishment will be issued to the ASA and VPN clients by a local Certificate Authority. In this scenario, a Certificate Signing Request (CSR) will be generated for each client and the ASA, then sent to the Certificate Authority (CA) administrator to issue an X.509 digital certificate. The certificates will be manually imported into the clients and ASA.

The following protocols and cipher suites will be used for IKE and IPSec in compliance with RFC 6379 (Suite B Cryptographic Suites for IPSec):

- IKEv2
- Encryption – AES-GCM 256
- Key Exchange – ECDH 384 (Group 20)
- Digital Signature – ECDSA 384
- Integrity Hashing – SHA-2 384

A Microsoft 2012 R2 Certificate Authority (CA) solution was deployed for the PKI design presented in this document. This PKI design is based on a two-tier CA solution using an Offline Root CA and an Enterprise Subordinate CA. The Subordinate CA issues X.509 digital certificates and provides a Certificate Revocation List (CRL) to the ASA and AC VPN clients. In addition, version 3, Suite B complaint templates are configured on the Subordinate CA. The Root CA is configured as a standalone (Workgroup) server while the Subordinate CA is configured as part of a Microsoft domain with Active Directory services enabled. Appendix B of this document will cover the CA implementation in further detail.

Introduction

This document is a combined High Level Design (HLD) and Low Level Design (LLD) that contains detailed information on the setup and configuration of the Cisco AnyConnect VPN client, ASA 5500-X and Windows 2012 PKI infrastructure to enable support for an Elliptic Curve, certificate based, NGE, VPN solution as discussed in the Executive Summary section. The ASA supports IPSec, TLS and clientless TLS (known as webvpn) methods of VPN establishment. This document will focus on the IPSec Remote Access VPN use-case focusing on certificate based machine authentication only.

It is assumed that the audience of this document has a basic knowledge of the following:

- PKI and Purpose of a Certificate of Authority
- X.509 digital certificate formats (PEM, DER, etc.)
- IKEv2 concepts
- Cisco IPSec Phase I and Phase II messaging
- Suite B as defined in RFC 6379 (http://tools.ietf.org/search/rfc6379)
- ASA 5500-X Firewalls
- AnyConnect Secure Mobility Client v3.x or higher
- Windows 2012 R2 basic administration of OS and Certificate Authority

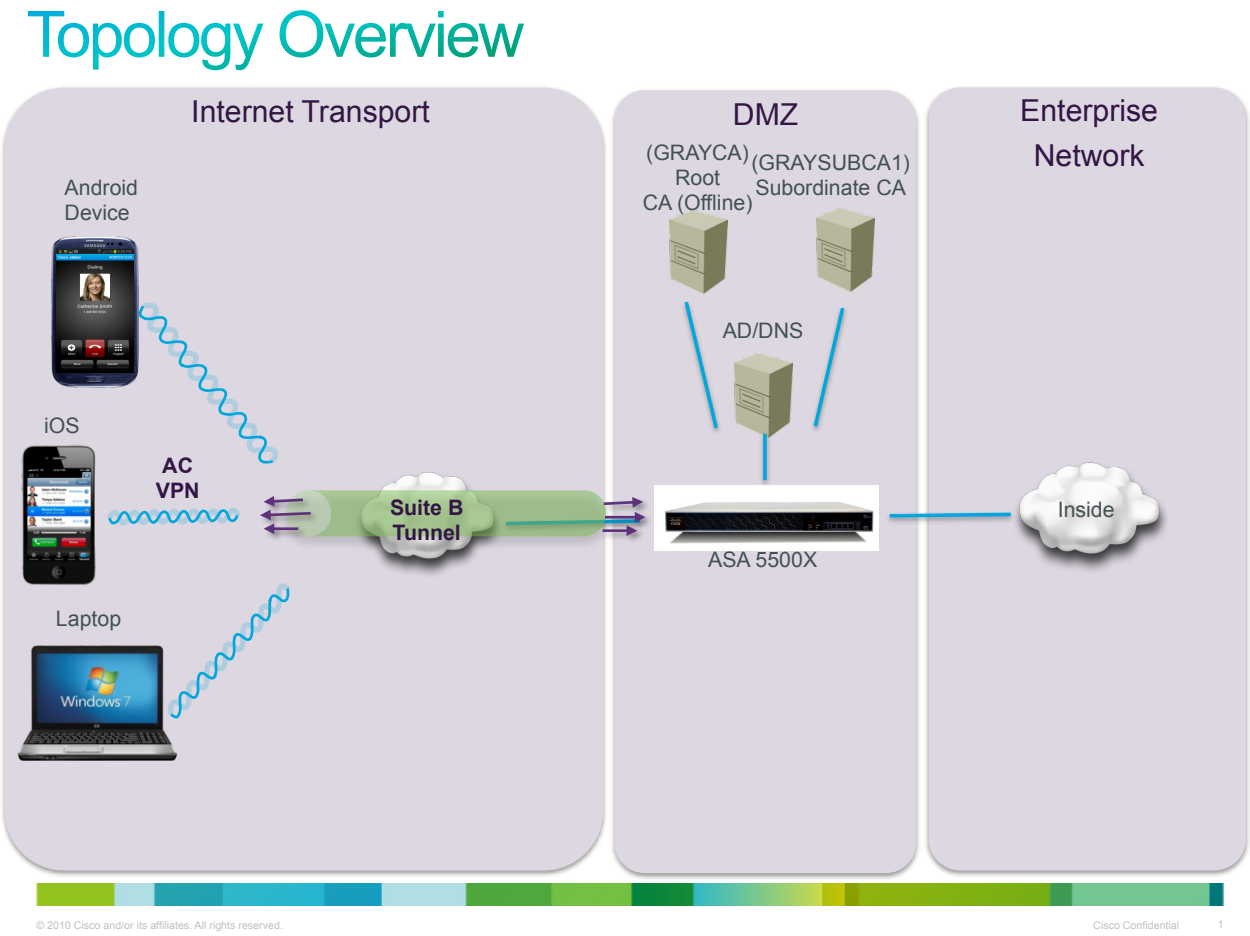
Configuration Note: The ASA supports client-services which provides the ASA with the capability to push AnyConnect profiles and software updates to the client. This capability is not used in this example. The following baseline configuration modifications are made:

1. It is assumed that AnyConnect profiles and updates are already installed on the client.
2. The AnyConnect profile and the ASA should have “auto-updates” disabled to ensure that that client-services are disabled.
3. If client-services are required, the ASA should have a standard RSA X.509 (non-EC based) digital certificate in addition to the EC-DSA based identity certificate required for NGE VPN users.

License Note: The ASA requires an AnyConnect Premium license for IKEv2 remote access connections using Suite B algorithms. Suite B algorithm usage for other connections or purposes (such as PKI) has no limitations. License checks are performed for remote access VPN connections. If you receive a message that you are attempting to use a Suite B crypto algorithm without an AnyConnect Premium license, you have the option to either install the Premium license or reconfigure the crypto settings to an appropriate level. It’s important to note that the ASA can use either AnyConnect Premium or Essentials, thus it’s important to ensure that Essentials is not enabled under the ‘webvpn’ statement in the ASA configuration. Also, if AnyConnect will be loaded on mobile devices, an **AnyConnect Mobile license** is required.

VPN Solution Diagram

Figure 1: Lab Topology Diagram



Caveats & Prerequisites

Certificate Caveats

ECDSA certificates:

1. Must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
2. Supported OS's:

   Windows Vista or later
   Mac OS X 10.6 or later

General Server Certificate Verification changes in Cisco Anyconnect 3.1:

1. ECDSA smart cards are supported only on Windows 7 or later.
2. Certificates in OS store are supported on Windows 7 or later and Vista only.
3. Certificates in the network profile (PEM encoded) supported on Windows XP/7/Vista
4. Server's ECDSA certificate chain verification is supported on Windows XP/7/Vista.
5. SSL connections being performed via FQDN no longer makes a secondary server certificate verification with the FQDN's resolved IP address for name verification if the initial verification using the FQDN fails.
6. **IPsec and TLS connections require that if a server certificate contains Key Usage, the attributes must contain DigitalSignature AND (KeyAgreement OR KeyEncipherment). If the server certificate contains an EKU, the attributes must contain serverAuth or ikeIntermediate. Note that server certificates are not required to have a KU or an EKU to be accepted.**
7. IPSec connections perform name verification on server certificates.
8. If a Subject Alternative Name (SAN) extension is present with relevant attributes, name verification is performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates and additionally include IP address attributes if the connection is being performed to an IP address.
9. If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification is performed against any Common Name attributes found in the Subject of the certificate.
10. If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.
11. Suite B profiles may require certain policy properties in the certificates; however, these requirements are enforced on the head-end and not by AnyConnect.
12. When the ASA is configured with a different server certificate for TLS and IPsec, use trusted certificates. A Posture assessment, Weblaunch, or Downloader failure can occur if using NGE (ECDSA) untrusted certificates having different IPsec and TLS certificates.

Prerequisites

The following tasks should be completed and all information collected prior to beginning the configuration:

- NTP Server configured and devices synced to same time source.
- Appropriate VLAN's and IP settings configured and established.
- DNS resolution enabled with ASA public hostname specified.
- Initial ASA configuration and connectivity established.
- ASA software updated to 9.1.x or above (9.1.3 used for this document).
- Appropriate licenses on ASA (AnyConnect Premium).
- AnyConnect software version 3.1 or above (3.1.04072 used in this document).
- AnyConnect client profiles and software installed on clients (Discussed in AC Client Section).
- Installation and initial configuration of Windows 2012 R2 domain controller, Root and Standalone CA servers must be completed.
- Windows Active Directory information (domain, forest, etc.) for CA setup and identity services.
- Windows Service Account or admin user name and password with privileges to join the Subordinate CA to a domain.
- Check the path MTU between the client and the ASA head-end. In some cases, where there are additional encryption hops (such as a VPN between intermediate network devices), an additional IPSEC wrap will exist while the data is in transit. This will force a configuration change on the ASA to lower the MTU on the 'inside' and 'outside' interfaces. This is to ensure the inner 'double-wrap' tunnel does not get fragmented.

ASA Configuration & Enrollment with the CA

In the coming sections, the relevant ASA VPN and ECC PKI configurations will be discussed along with the ASA PKI enrollment process with a Certificate Authority. The ASA must be enrolled with the ECC CA and appropriately configured to allow for proper IKE and IPSec negotiation with VPN users. A detailed ASA configuration is provided in Appendix A of this document. Appendix C will also provide ASA commands that can be entered to verify VPN connectivity.

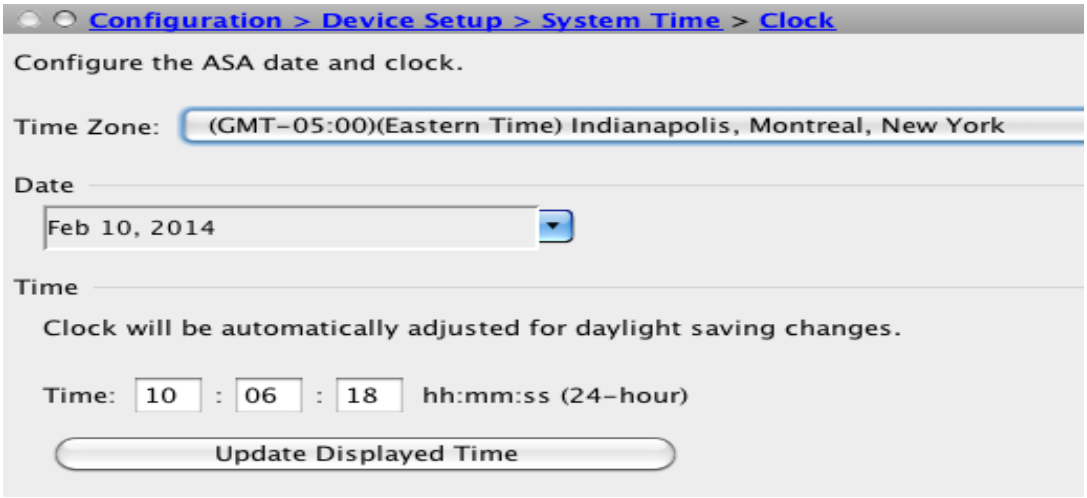
ASA PKI Configuration and Enrollment

In this section, specific ASA PKI configurations along with the enrollment process will be discussed. Since neither Simple Certificate Enrollment Protocol (SCEP) nor domain Auto-Enrollment is an option for the ASA, an offline, manual enrollment process must be followed. In this scenario, both the Offline Root CA (GRAYCA) certificate and the Enterprise Subordinate CA (GRAYSUBCA1) certificate must be installed and trusted to ensure a trusted certificate chain is established. During this process, the previously created "**NGEASA**" template (see Appendix B for more details) and the "**certreq**" command line utility will be used on the Subordinate CA to enroll the ASA and obtain an identity certificate.

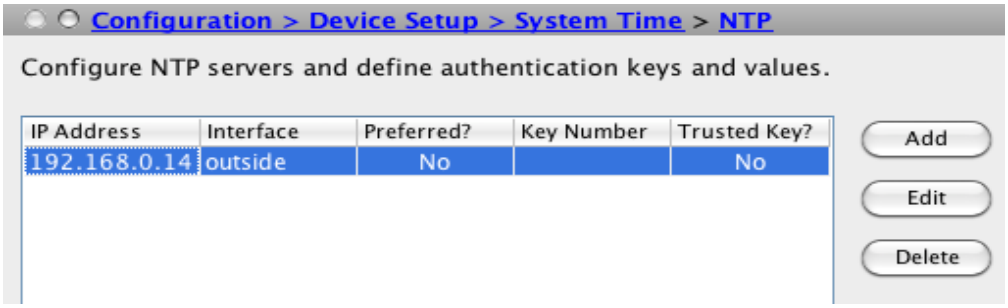
Throughout the document, the ASDM configuration steps will be discussed. The equivalent command line (CLI) configuration steps will also be referenced to ensure both configuration methods are documented. However, the administrator should use either ASDM or CLI depending on preference.

At this point, it is assumed that the basic ASA configuration is completed and connectivity is established to the network. To begin the configuration process on the ASA, follow the configuration steps below:

1. Configure the time zone information and date. In ASDM, go to Configuration > Device Setup > System Time > Clock and enter the appropriate information for the local network and then select "Apply".



2. Configure an NTP source. In ASDM, go to Configuration > Device Setup > System Time > NTP > Add and enter the appropriate information for the local network and then select “Apply”.



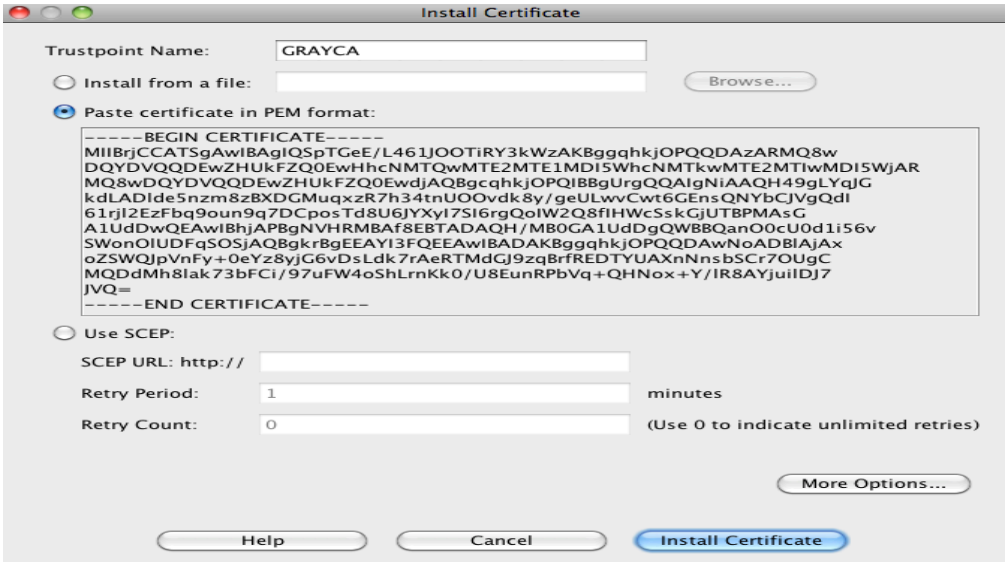
3. Configure the hostname and domain name. In ASDM go to, Configuration > Device Setup > Device Name/Password and enter the appropriate information for the local network and then select “Apply”.

ASA CLI configuration example:

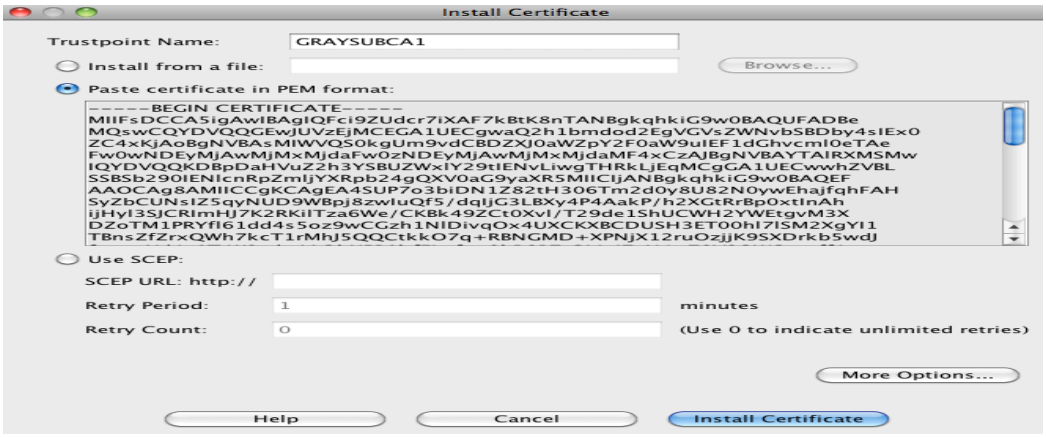
```
hostname grayasavpn

domain-name
graydmz.org
```

The ASA administrator must obtain the CA certificates from the PKI admin and import the certificates to the ASA. In this scenario, both the Root CA and Subordinate CA certificates must be imported. The ASA admin can open the CA certificates with NotePad to copy and paste

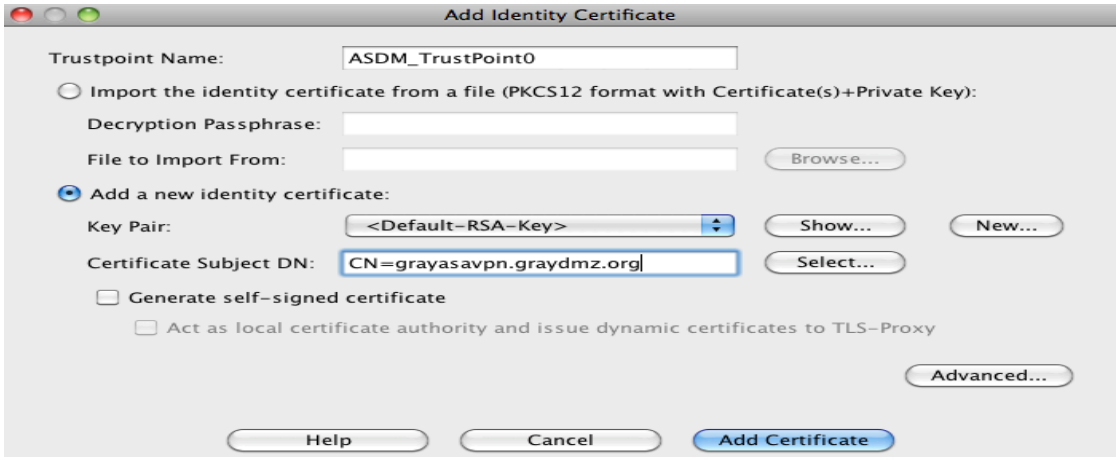
1. In ASDM, go to Configuration > Device Management > Certificate Management > CA Certificates and select “Add”. Enter the Trustpoint Name (GRAYCA), open the certificate file with WordPad, copy the certificate and then paste the PEM formatted certificate (or browse to file). Then select “ Install Certificate”.



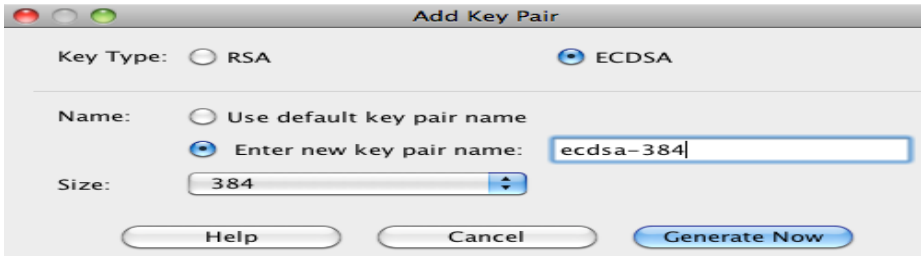
2. Follow the previous steps again for the Subordinate CA. In ASDM, go to Configuration > Device Management > Certificate Management > CA Certificates and select “Add”. Enter the Trustpoint Name (GRAYSUBCA1), open the certificate file with WordPad, copy the certificate and then paste the PEM formatted certificate (or browse to file). Then select “ Install Certificate”.



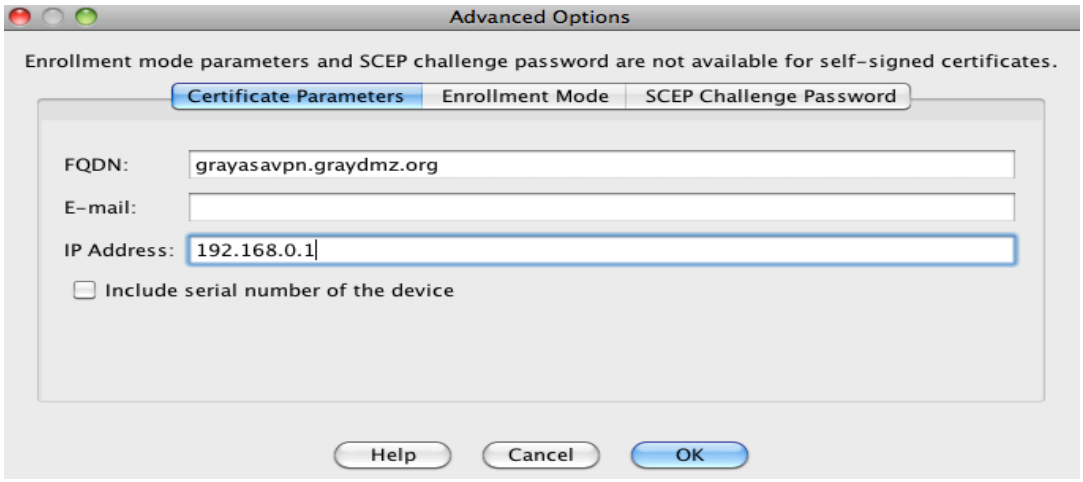
3. Generate a key pair. To stay consistent with the previously chosen algorithms in the templates, generate an ECDSA 384-bit key called “**ecdsa-384**”. In ASDM, go to Configuration > Device Management > Certificate Management > Identity Certificates and select “Add”. The “Add Identity Certificate” window appears. Select “Add New Identity Certificate” and enter the CN. Then, next to “Key Pair”, select “New”.



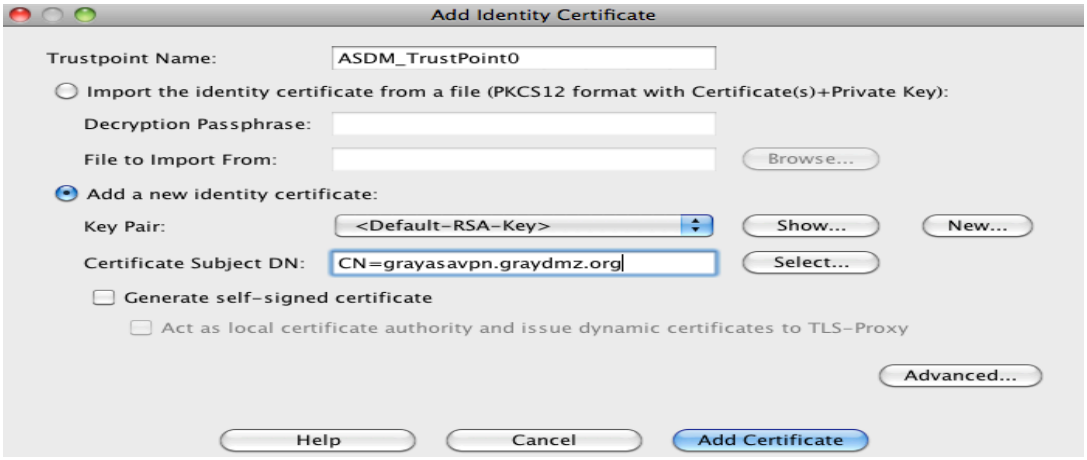
4. Select “ECDSA”, then select “Enter new key pair name” and add the name. Ensure the size is “384” and select “Generate Now”.



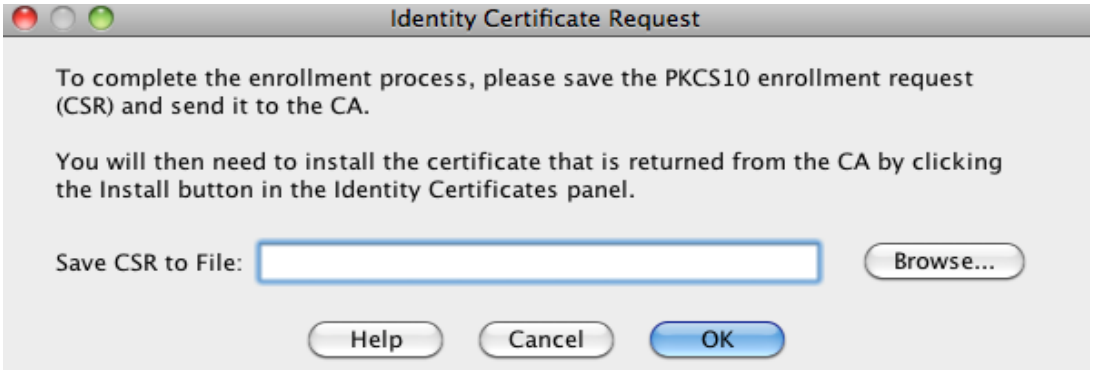
5. Return to the “Add Identity Certificate” page, select “Advanced” and enter the FQDN and IP address information under “Certificate Parameter” and select “Ok”.



6. Return to the “Add Identity Certificate” page, select “Add Certificate”.



7. The Certificate Signing Request (CSR) dialogue box appears. Save the CSR to a location and select “OK”.

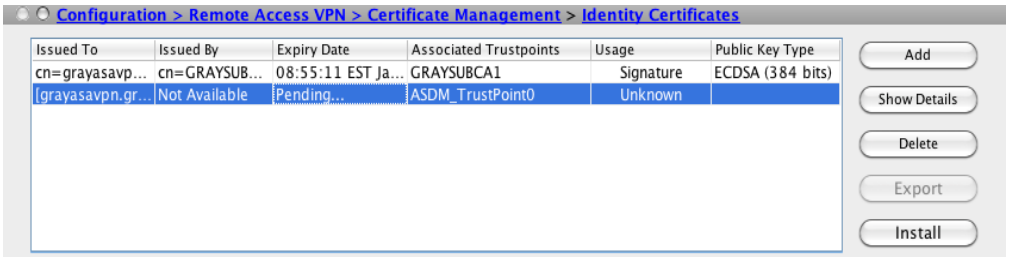


Configuration note: The CSR will now need to be sent to the CA administrator and processed to obtain the ASA identity certificate. On the CA, open a command prompt and enter the command below (notice the previously created “**NGEASA**” template is referenced):

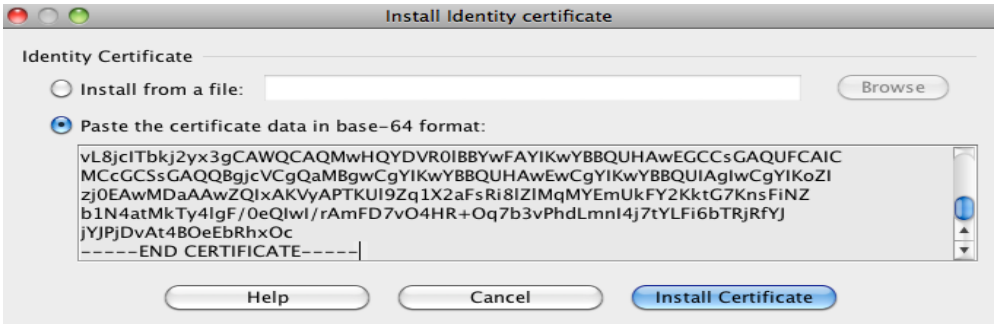
```
certreq –submit –attrib
“certificatetemplate:NGEASA”
```

Upon hitting return, you will be prompted for the CSR file. Select the CSR “**.req**” file, in this case “**asa-csr.req**”, then ensure the CA is selected, then save the certificate to a location on the CA.

8. Retrieve the identity certificate from the CA admin and install on the ASA. In ASDM, go to Configuration > Device Management > Certificate Management > Identity Certificates and select the “Pending” request and select “Install”.



9. Open the ID certificate in NotePad and Paste the certificate in (or browse to file). Then select “Install Certificate”.



ASA CLI configuration example:

```
crypto key generate ecdsa label ecdsa-384 elliptic-
curve 384

!

crypto ca trustpoint GRAYCA

enrollment terminal

exit

!

crypto ca authenticate GRAYCA

Enter the base 64 encoded CA certificate.

End with the word "quit" on a line by itself

<Copy and Paste the base64 certificate from the
Offline CA>

quit

INFO: Certificate has the following attributes:

Fingerprint:     70ef6c46 90f61fef ee48e5f3

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

!

crypto ca trustpoint GRAYSUBCA1
```

```
enrollment terminal

subject-name CN= grayasavpn.graydmz.org

fqdn grayasavpn.graydmz.org

ip-address 192.168.0.1

keypair ecdsa-384

!

crypto ca authenticate GRAYSUBCA1

!

Enter the base 64 encoded CA certificate.

End with the word "quit" on a line by itself

<Copy and Paste the base64 certificate from the Sub CA>

quit

INFO: Certificate has the following attributes:

Fingerprint:     70ef6c46 90f61fef ee48e5f3 b3726fd8

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Enroll the ASA with the Subordinate CA, a certificate-signing request must be generated and manually exported to the CA.

Enter the following commands to generate a CSR:

```
crypto ca enroll GRAYSUBCA1

% The subject name in the certificate will be:
CN=grayasavpn.graydmz.org

% The fully-qualified domain name in the certificate will be:
grayasavpn.graydmz.org

% Include the device serial number in the subject name? [yes/no]: yes

% The serial number in the certificate will be: FCH1744J8L7

% The IP address in the certificate is 192.168.0.1
```

```
Display Certificate Request to terminal? [yes/no]: yes

<CSR DATA DISPLAYED>
```

Configuration Note: The CSR data will appear on the ASA console in Base-64 format. Perform the following steps:

1. Select all of the text in the CSR and copy it to a text file using a program like WordPad.
2. Save the file but ensure you select "**All Files**" as the type and add the "**.req**" file extension. In this example, the text file was saved as "**asa-csr.req**" and placed in a location that is accessible from the Subordinate CA.
3. On the CA, open a command prompt and enter the command below (notice the previously created "**NGEASA**" template is referenced):

```
certreq –submit –attrib
"certificatetemplate:NGEASA"
```

4. Upon hitting return, you will be prompted for the CSR file. Select the CSR "**.req**" file, in this case "**asa-csr.req**", then ensure the CA is selected, then save the file to a location on the CA.

Now, the PEM formatted ASA identity certificate must be imported to the ASA under the Subordinate CA trustpoint.

1. Open the ASA certificate with WordPad and copy the certificate.
2. Import the certificate with the following commands:

```
grayasavpn(config)# crypto ca import GRAYSUBCA1
certificate

% The fully-qualified domain name in the certificate will be:
grayasavpn.graydmz.org

% The IP address in the certificate is 192.168.0.1

Enter the base 64 encoded certificate.

End with the word "quit" on a line by itself

<PASTE the CERTIFICATE>

quit

INFO: Certificate successfully imported
```

At this point, the ASA has an identity certificate and the CA certificates are installed. In the next section, the ASA must be configured for VPN access to include the necessary NGE algorithms and policies.

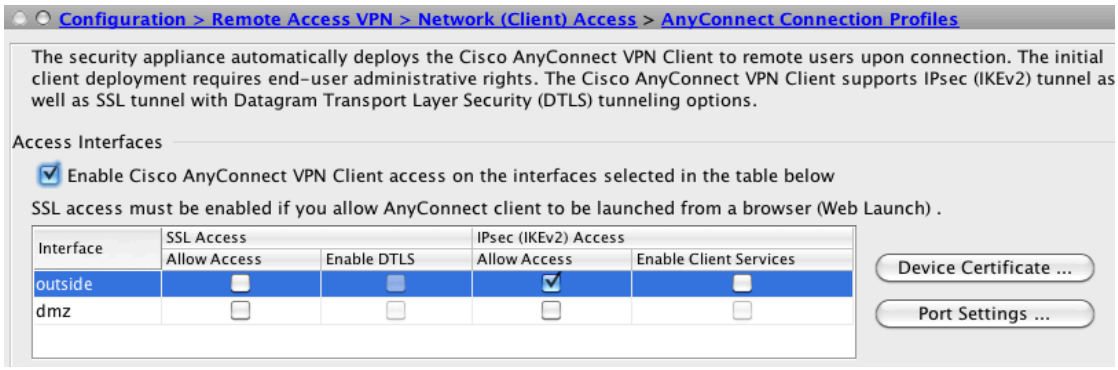
ASA VPN Configuration

In this section, the relevant NGE IKE, IPSec and AnyConnect VPN user settings that are required on the ASA will be discussed. At this point, the ASA should be enrolled with the PKI infrastructure creating a trusted certificate chain.

1. To start, **disable AnyConnect Essentials** from the command line. This ensures the Premium licenses are enabled for IKEv2. Enter the below in configuration mode.

```
Webvpn

 no anyconnect-
essentials
```

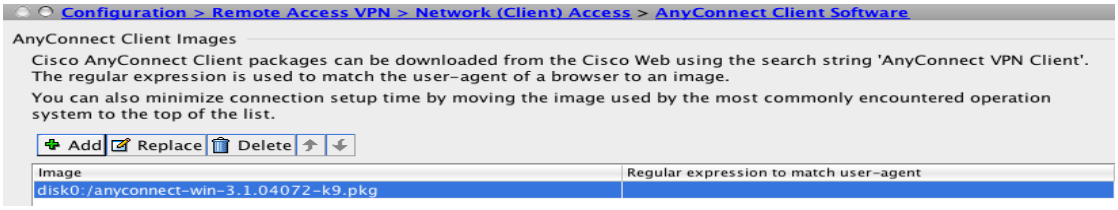
2. Enable AnyConnect and IKEv2 on the ASA. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles and select **Enable Cisco AnyConnect**… and **Allow Access** under IKEv2. Ensure **Enable Client Services** is **NOT** checked.



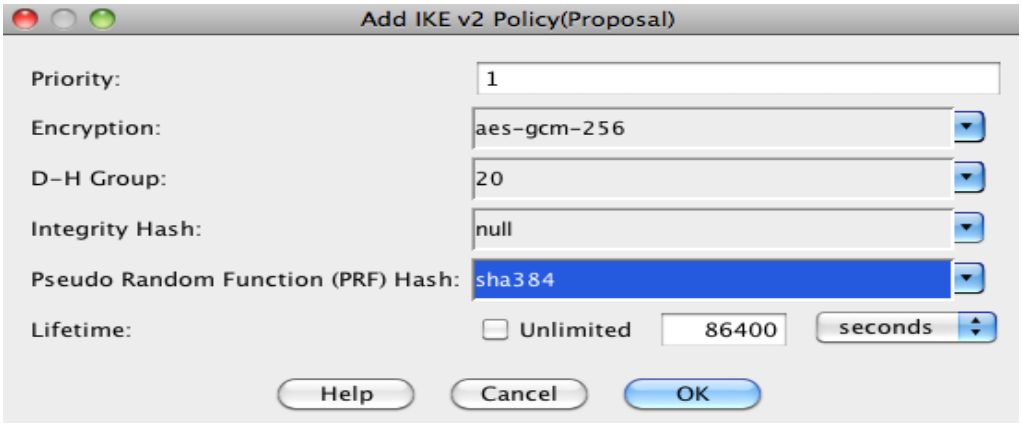
3. On the **AnyConnect Connection Profiles** page mentioned above, select **Device Certificate**. Ensure **Use the same device certificate**… is **NOT** checked and select the EC ID certificate under the ECDSA device certificate. Then select **Ok**.

4. It is assumed that an AnyConnect image is already loaded on to the ASA flash. This example used AC for Windows version (3.1.04072). If Linux or MAC-OS is used, then those images should be loaded, as well. The NGE algorithms are supported across platforms in the 3.1 releases. In ASDM, go to Configuration > Remote Access VPN >

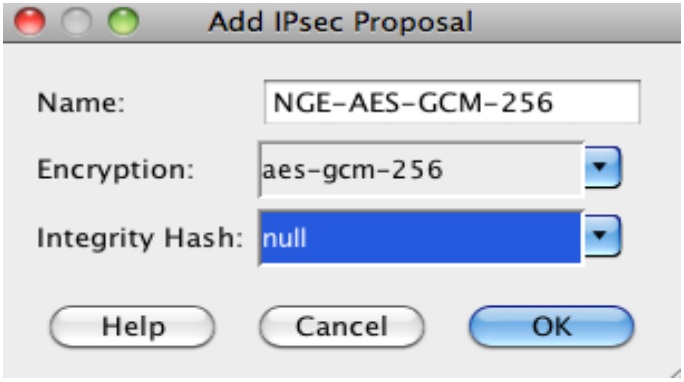
Network (Client) Access > AnyConnect Client Software, then **Add** and an AC image. Then select **Ok**.



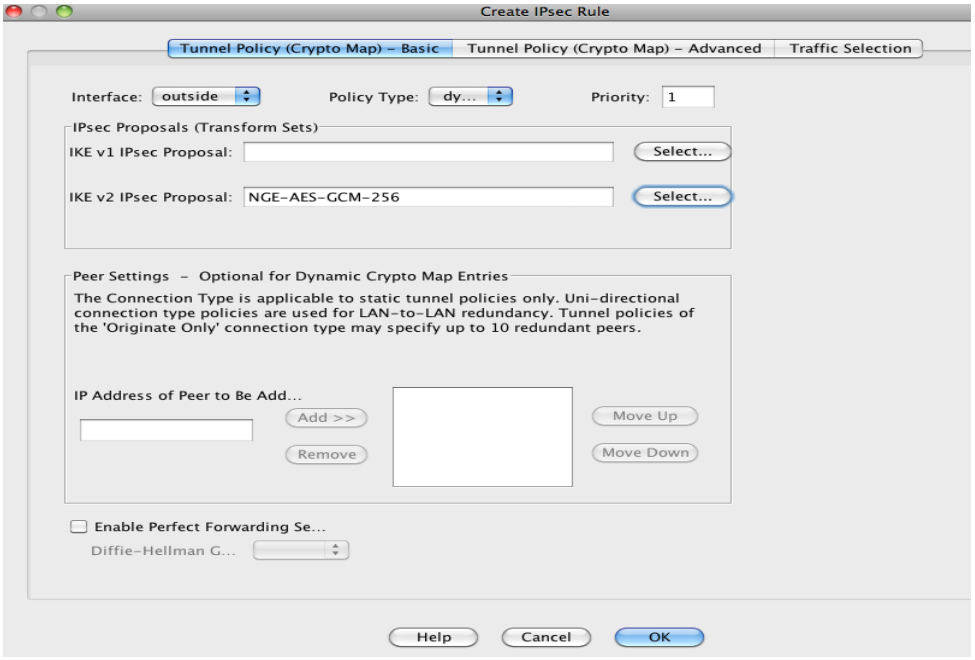
5. An IKEv2 crypto policy **1** needs to be created utilizing the Suite B desired algorithms. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies and add an IKEv2 policy. Select **Add** and configure the highest priority (1) to use AES Galois Counter Mode (AES-GCM) 256-bit encryption. When GCM is selected, it precludes the need to select an integrity algorithm. This is because the authenticity capabilities are built into GCM, unlike CBC (Cipher-Block Chaining). Diffie-Hellman Group 20 is also selected, then select **Ok**.



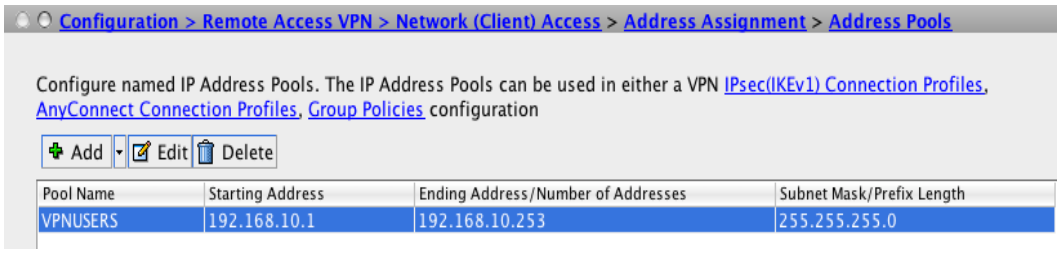
6. Create an IPSEC proposal **NGE-AES-GCM-256**. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Proposals (Transform Sets) and add an IKEv2 IPSec Proposal. Select **AES-GCM-256** for encryption and **Null** for the Integrity Hash, then select **Ok**.



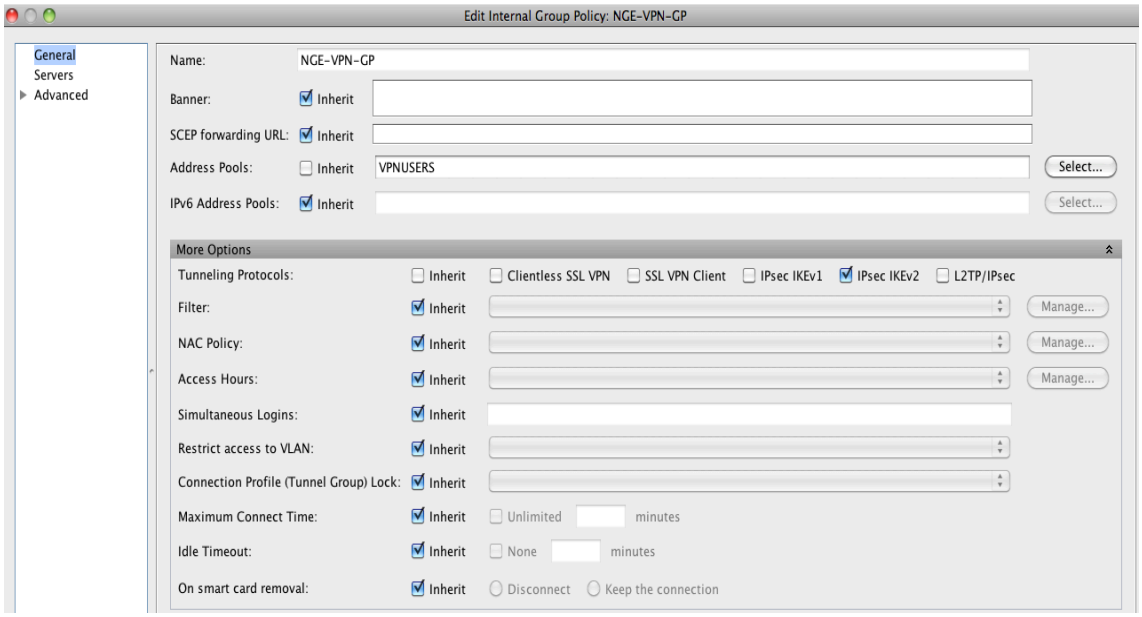
7. Create a dynamic crypto map, select the IPSec proposal and apply to the outside interface. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps. Select **Add**, select the **outside** interface and the **IKEv2** proposal and then select **Ok**.



8. Create an IP address pool **VPNUSERS** that will be assigned to VPN users. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools and add an IP pool and then select **Ok**.

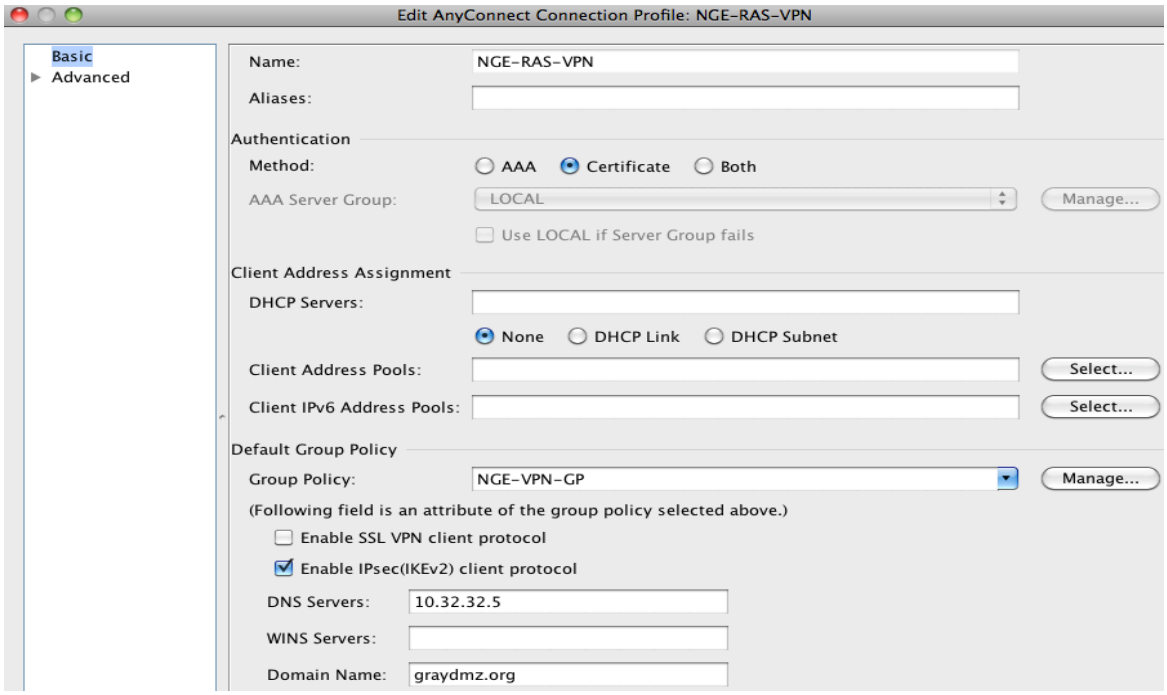


9. Add a group policy **NGE-VPN-GP** that will apply the desired settings to the VPN users. Ensure the VPN tunnel protocol is set to **IKEv2** and the IP pool created above is referenced in the policy by de-selecting the **Inherit** check box and selecting the appropriate setting. Relevant DNS, WINS and domain names can also be added in the policy in the **Servers** section. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Group Polices and **Add** an internal group policy and then select **Ok**.



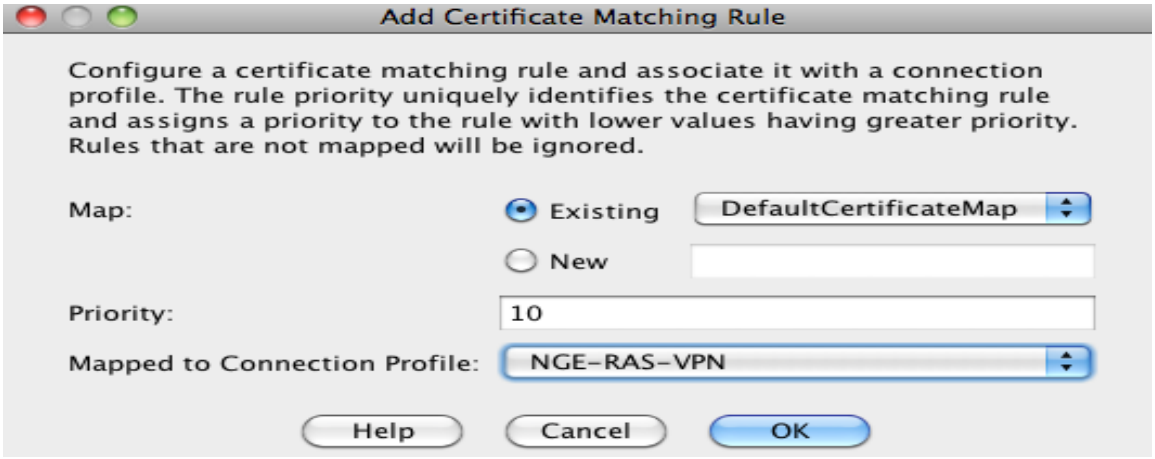
10. Create a tunnel group **NGE-VPN-RAS** for NGE remote-access and define general and webvpn attributes. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. At the bottom of the page under **Connection Profiles**, select **Add**. The configuration references **Certificate** authentication, the associated group policy **NGE-VPN-GP** and **Enable IPSec (IKEv2)**. Once completed, select **Ok**.

    Configuration note: DNS and domain name can also be added here. Also, to ensure only IPSec is used, **Enable SSL VPN Client Protocol** is not enabled.



11. Create a certificate map, mapping the NGE VPN users to the VPN tunnel group that was previously created. The certificate map will be applied to the AC users under the **Webvpn** configuration. In this scenario, the Subordinate CA common name was matched to ensure any user coming in with an EC certificate issued from the Subordinate CA will be mapped to the appropriate tunnel group that was previously created. VPN users that are not issued a certificate from the EC CA will fall back to the default tunnel groups and fail authentication and will be denied access.

    In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under **Certificate to Connection Profile Maps** select **Add**. Choose the existing **DefaultCertificateMap** with a priority of **10** and reference the **NGE-RAS-VPN** tunnel group. Then select **Ok**.



    In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under **Mapping Criteria** select **Add**. Select **Issuer** for field, **Common Name (CN)** for component, **Contains** for Operator and **CANAME** for value and then select **Ok**.

    Ensure to select **APPLY** on the main page and **SAVE** the configuration.

ASA configuration example:

```
Webvpn

    anyconnect image disk0:/anyconnect-win-3.1.04072-
k9.pkg 1

    anyconnect enable

    no anyconnect-essentials



crypto ikev2 remote-access trustpoint GRAYSUBCA1

crypto ikev2 enable outside
```

Note, if the below error is received; disable AC Essentials to ensure Premium licenses are used.

```
crypto ikev2 remote-assess trustpoint
GRAYSUBCA1

WARNING: ECDSA trustpoint for
IKEv2 remote access cannot be used
due to license restrictions. An
AnyConnect Premium license must be
installed to use this trustpoint with
IKEv2 remote access.

!

webvpn

    no anyconnect-essentials
```

ASA configuration example continued:

```
crypto ikev2 policy 1

    encryption aes-gcm-
256

    integrity null

    group 20

    prf sha384
```

```
lifetime seconds 86400
```

```
crypto ipsec ikev2 ipsec-proposal NGE-AES-GCM-256
    protocol esp encryption aes-gcm-256
    protocol esp integrity null
```

```
crypto dynamic-map NGE-DYNAMIC-VPN 1 set ikev2 ipsec-proposal NGE-AES-GCM-256

crypto map NGE-VPN 1 ipsec-isakmp dynamic NGE-DYNAMIC-VPN

crypto map NGE-VPN interface outside
```

```
ip local pool VPNUSERS 192.168.10.1-192.168.10.253 mask 255.255.255.0

group-policy NGE-VPN-GP internal

group-policy NGE-VPN-GP attributes

 wins-server none

 dns-server value <X.X.X.X>

 vpn-tunnel-protocol ikev2

 default-domain value graydmz.org

 address-pools value VPNUSERS
```

```
tunnel-group NGE-RAS-VPN type remote-access

tunnel-group NGE-RAS-VPN general-attributes

 default-group-policy NGE-VPN-GP

tunnel-group NGE-RAS-VPN webvpn-attributes

 authentication certificate
```

```
crypto ca certificate map DefaultCertificateMap 10

  issuer-name attr cn co graysubca1

webvpn
```

```
certificate-group-map DefaultCertificateMap 10 NGE-RAS-VPN
```

AnyConnect Client Setup

Client PKI Enrollment

It is assumed that the client has already imported and trusted each CA into the trusted certificate store and the machine has an identity certificate issued from the PKI admin that references the "**NGECOMPUTER**" template created on the CA (see Appendix B for more details). The Microsoft "**MMC**" Certificate snap-in tool should be used to both import the CA certificates and enroll the machine with the PKI infrastructure. More information on using MMC can be found here:

http://technet.microsoft.com/en-us/library/dd632619.aspx

The machine will be manually enrolled with the CA. The following site describes the process to complete a manual CSR on a Windows machine that must be submitted to the Subordinate CA:

http://technet.microsoft.com/en-us/library/cc730929.aspx

AnyConnect Client Configuration

In this section, the AnyConnect client specific configuration and setup will be discussed. It is assumed that all client software and profile pushes are done manually to adhere to strict security guidelines. The AnyConnect profile can be configured using the AnyConnect Profile Editor GUI or via the manual editing of the XML file. To use the profile editor, follow the instructions found below:

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/administration/guide/ac02asaconfig.html - wp1620141

The AnyConnect XML profile is located at the following location on a Windows 7 machine:

```
%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\name.xml
```

In the following example, "**Certificate Store Override**" is set to "**true**" in order to access the clients' machine certificate store for non-administrative users. Under the "**Server List**" portion of the AnyConnect profile, an **accurate host name and address MUST** match the name presented in the certificate. **ENSURE** the "**Primary Protocol**" is set to "**IPSec**".

```
<ClientInitialization>

		<UseStartBeforeLogon
UserControllable="true">false</UseStartBeforeLogon>

		<AutomaticCertSelection
UserControllable="true">false</AutomaticCertSelection>

		<ShowPreConnectMessage>false</ShowPreConnectMessage>

		<CertificateStore>Machine</CertificateStore>

		<CertificateStoreOverride>true</CertificateStoreOverride>

<ServerList>

		<HostEntry>

			<HostName>grayasavpn.graydmz.org</HostName>

			<HostAddress> grayasavpn.graydmz.org </HostAddress>

			<PrimaryProtocol>IPsec</PrimaryProtocol>

		</HostEntry>

</ServerList>
```

Appendix A – ASA Configurations

```
grayasavpn# sh run

ASA Version 9.1(3)2

!

hostname grayasavpn

domain-name graydmz.org

ip local pool VPNUSERS 192.168.10.1-192.168.10.253 mask 255.255.255.0

!

interface GigabitEthernet0/0

 nameif outside

 security-level 0

 ip address 192.168.0.1 255.255.255.252

!

interface GigabitEthernet0/2

 description graydmz

 nameif dmz

 security-level 80

 ip address 10.32.32.1 255.255.255.0

!

boot system disk0:/asa913-2-smp-k8.bin

clock timezone EST -5

dns server-group DefaultDNS

 domain-name graydmz.org

access-list outside extended permit ip any any

dynamic-access-policy-record DfltAccessPolicy
```

```
crypto ipsec ikev2 ipsec-proposal NGE-AES-GCM-256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map NGE-DYNAMIC-VPN 1 set ikev2 ipsec-proposal NGE-AES-GCM-256
crypto map NGE-VPN 1 ipsec-isakmp dynamic NGE-DYNAMIC-VPN
crypto map NGE-VPN interface outside
crypto ca trustpoint GRAYSUBCA1
 revocation-check crl none
 enrollment terminal
 fqdn grayasavpn.graydmz.org
 subject-name CN=grayasavpn.graydmz.org
 serial-number
 ip-address 192.168.0.1
 keypair ecdsa-384
 crl configure
crypto ca trustpoint GRAYCA
 enrollment terminal
 crl configure
crypto ca trustpool policy
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr cn co graysubca1
crypto ca certificate chain GRAYSUBCA1
 certificate ca 2100000002ce552a1b3388eae1000000000002
    308202a5 3082022b a0030201 02021321 00000002 ce552a1b 3388eae1 00000000
quit
```

```
 certificate 5c000000037b5a1afb01899c7f000000000003
    3082033b 308202c1 a0030201 0202135c 00000003 7b5a1afb 01899c7f 00000000


  quit
crypto ca certificate chain GRAYCA
 certificate ca 4a94c6784fcbe3ad4938e4e2458de45b
    308201ae 30820134 a0030201 0202104a 94c6784f cbe3ad49 38e4e245 8de45b30
quit
crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 group 20
 prf sha384
 lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev2 remote-access trustpoint GRAYSUBCA1
webvpn
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.04072-k9.pkg 1
 anyconnect enable
 certificate-group-map DefaultCertificateMap 10 NGE-RAS-VPN
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev2
group-policy NGE-VPN-GP internal
group-policy NGE-VPN-GP attributes
 wins-server none
 dns-server value 10.32.32.5
```

```
 vpn-tunnel-protocol ikev2
 default-domain value graydmz.org
 address-pools value VPNUSERS
tunnel-group NGE-RAS-VPN type remote-access
tunnel-group NGE-RAS-VPN general-attributes
 default-group-policy NGE-VPN-GP
tunnel-group NGE-RAS-VPN webvpn-attributes
 authentication certificate
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sip
!
service-policy global_policy global
: end
```

Appendix B – CA Implementation

In this design, there are three Windows 2012 R2 Servers setup and configured in a two-tier PKI Hierarchy. There is a Domain Controller with Active Directory Domain Services (AD DS) and DNS services enabled, along with the Offline Standalone Root CA and a separate the Enterprise Subordinate CA. The Offline Root CA will not be part of the domain and will remain in a workgroup. The AD DC and Enterprise Subordinate CA will be in the same domain. It is assumed that basic configuration of the servers is complete and the Directory Services are configured as required per Microsoft guidance. The following guides can be referenced for initial server setup and configuration:

http://technet.microsoft.com/en-us/library/hh831348.aspx

http://technet.microsoft.com/en-us/library/ff829847%28v=ws.10%29.aspx

Offline Root CA & Subordinate CA File Share Setup

This section covers the setup of the offline Root CA along with the various tasks that need to be completed to setup the Subordinate CA file share and distribution points to support the end PKI solution. At this point, it is assumed that Windows 2012 R2 has already been installed, configured, and the servers have full network connectivity. The Subordinate CA should already be part of the AD domain per the guidance specified in the Technet links mentioned in the previous section.

We will start by configuring the **CAPolicy.inf** file on the RootCA.

1. Open Windows PowerShell, type **notepad c:\Windows\CAPolicy.inf** and press ENTER.
2. When prompted to create a new file, click **Yes**.
3. Enter the following as the contents of the file:

```
[Version]

Signature= "$Windows NT$"

[Certsrv_Server]

LoadDefaultTemplates = False
```

4. Click **Save As**. Ensure the following:

   File name is set to **CAPolicy.inf**

   Save as type is set to **All Files**

Encoding is **ANSI**

Next, we will install AD Certificate Services on the Offline Root CA.

1. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. On the **Before you begin** screen, click **Next**.
3. On the **Select installation type** screen, ensure the default selection of **Role-based or feature-based installation** is selected. Click **Next**.
4. On the **Select destination server** screen, ensure that **RootCA** is selected and then click **Next**.
5. On the **Select server roles** screen, select the **Active Directory Certificate Services** role.
6. When prompted to install Remote Server Administration Tools click **Add Features**. Click **Next**.
7. On the **Select features** screen, click **Next**.
8. On the **Active Directory Certificate Services** screen, click **Next**.
9. On the **Select role services** screen, the **Certification Authority** role is selected by default. Click **Next**.
10. On the **Confirm installation selections** screen, verify the information and then click **Install**.
11. Wait for the installation to complete. The installation progress screen is displayed while the binary files for the CA are installed. When the binary file installation is complete, click the **Configure Active Directory Certificate Services on the destination server** link.
12. On the **Credentials** screen, you should see that the **RootCA\Administrator** is displayed in the **Credentials** box. (Ensure the user account is an admin on server). Click **Next**.
13. On the **Role Services** screen, select **Certification Authority**. This is the only available selection when only the binary files for the certification authority role are installed on the server. Click **Next**.
14. The only selection available on the **Setup Type** screen is **Standalone CA**. This is because the account used to install is a member of the local Administrators group and the server is not a member of an Active Directory Domain Services (AD DS) domain. Click **Next**.
15. On the **CA Type** screen, **Root CA** is selected by default. Click **Next**.
16. On the **Private Key** screen, leave the default selection to **Create a new private key** selected. Click **Next**.
17. On the **Cryptography for CA** screen, ensure that the following are selected:

    - From the dropdown menu, select "**ECDSA_P384#Microsoft Software Key Store Provider**," a key length of **384**, and **SHA384**.

18. Then click **Next**.
19. On **Specify the name of the CA,** ensure you specify the CN and DN suffix required for your design.
20. On the **Validity Period** screen, enter **5** for the number of years for the certificate to be valid.
21. On the **CA Database** screen, leave the default locations for the database and database log files. Click **Next**.
22. On the **Confirmation** screen, click **Configure**.
23. The **Progress** screen is displayed during the configuration processing, then the **Results** screen appears. Click **Close**. If the **Installation progress** screen is still open, click **Close** on that screen as well.

Detailed Certificate Authority configuration is out of scope of this document. However, the CA CRL CDP and AIA settings should be updated to reference the CRL CDP URL for revocation checking and publication. Notice below how the URL referenced is the **www.domain.org/pki**,

this URL will be referenced for CRL publishing and checking and should be changed to match your domain.

1. In Server Manager, click **Tools** and then click **Certification Authority**.
2. In the Certification Authority console tree, expand **RootCA**. Right-click **Revoked Certificates** and then click **Properties**.
3. On the **CRL Publishing Parameters** tab, ensure that **Publish Delta CRLs** is cleared (not selected). Click **OK**.
4. In the Certification Authority console tree, right-click **RootCA** and then click **Properties**.
5. Click the **Extensions** tab. Ensure that **Select extensions** is set to **CRL Distribution Point (CDP)** and in the **Specify locations from which users can obtain a certificate revocation list (CRL)**, review the default settings.
6. Change **Select extension** to **Authority Information Access (AIA)** and review the default settings. Click **OK**. If you are prompted to restart Active Directory Certificate Services, click **No**. You will restart the service after modifying the default paths in the next step.
7. From Windows PowerShell run the following commands (Ensure you change domain name):

```
certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\system32\CertSrv\CertEnroll\%3%8.crl\n2:http://www.domain.org/pki/%3%8.crl"

certutil –setreg CA\CACertPublicationURLs "2:http://www.domain.org/pki/%1_%3%4.crt"

Certutil -setreg CA\CRLOverlapPeriodUnits 12

Certutil -setreg CA\CRLOverlapPeriod "Hours"

Certutil -setreg CA\ValidityPeriodUnits 10

Certutil -setreg CA\ValidityPeriod "Years"

certutil -setreg CA\DSConfigDN “CN=Configuration,DC=domain,DC=org”

restart-service certsvc

certutil -crl
```

At this point, the RootCA X.509 identity certificate and CRL should be copied/exported off the server to a file system, such as the SubCA C: drive for later use. This can be done via the CLI.

1. From Windows PowerShell, run the command **dir C:\Windows\system32\certsrv\certenroll*.cr***, which displays the certificates and CRLs in the default certificate store.
2. Copy the CA certificate file and CRL to a local or remote file share. For example, if you were running commands to copy the certificate and CRL to the C: drive (C:), you would run the following commands and then move the files to the SubCA:

```
copy
C:\Windows\system32\certsrv\certenroll\*.
cr* C:\
```

Next, the RootCA certificate and the CRL should be distributed to the SubCA. Also, the local DNS domain needs an “A” record configured for “**WWW**” pointing to the SubCA location where the CRL and CA certificate will be stored.

1. On SubCA, sign in using the User1 account, which is a member of both **Domain Admins** and **Enterprise Admins**. Open Windows PowerShell as administrator. To do so, right-click the Windows PowerShell icon and then click **Run as administrator**. When prompted by User Account Control, click **Yes**.
2. From Windows PowerShell change to the drive where the files were copied using the cd command (as in run **cd c:** to change to the root of drive C).
3. From the Windows PowerShell, run the following commands on SubCA:

```
certutil –dspublish –f RootCA.crt RootCA

certutil –addstore –f root RootCA.crt

certutil –addstore –f root RootCA.crl
```

4 . Coordinate with DNS admin to create a DNS A record for **WWW** pointing to the IP of SubCA.

In the extensions of the root CA, it was stated that the CRL from the root CA would be available via http://www.domain.org/pki. Currently, there is not a PKI virtual directory on SubCA, so one must be created.

1. Ensure that you sign in using the User1 account. Run Windows PowerShell as Administrator and then run the following commands:

```
New-item -path c:\pki –type directory

write-output "Example CPS statement" | out-file c:\pki\cps.txt

new-smbshare -name pki c:\pki -FullAccess SYSTEM,"DOMAIN\Domain Admins"
-ChangeAccess "DOMAIN\Cert Publishers"
```

2. Open the IIS console. In Server Manager, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In the Internet Information Services (IIS) Manager console tree, expand **SubCA**. If you are invited to get started with Microsoft Web Platform, click **Cancel**.
4. Expand **Sites** and then right-click the **Default Web Site** and then click **Add Virtual Directory**.
5. In **Alias**, type **pki** and then in physical path type **C:\pki**, then click **OK**.
6. Enable Anonymous access to the pki virtual directory. To do so:

    - In the **Connections** pane, expand **Default Web Site**, ensure that **pki** is selected.
    - On **pki Home** click **Authentication**.
    - In the **Actions** pane, click **Edit Permissions**.
    - On the **Security** tab, click **Edit**
    - On the **Permissions for pki** dialog box, click **Add**.
    - On **Select Users, Computers, Service Accounts, or Groups**, type **Cert Publishers** and then click **Check Names**.
    - On **Select Users, Computers, Service Accounts, or Groups**, click **Object Types**.
    - On **Object Types**, select **Service Accounts** and then click **OK**.
    - On **Select Users, Computers, Service Accounts, or Groups**, click **Locations**.

- On **Locations**, click **SubCA** and then click **OK**.
- On **Select Users, Computers, Service Accounts, or Groups** after **Cert Publishers**, type "**;IIS AppPool\DefaultAppPool"** and then click **Check Names**. Click **OK**.
- On **Permissions for pki** select **Cert Publishers (DOMAIN\Cert Publishers)**. Under **Permissions for Cert Publishers**, select the **Modify** checkbox in the **Allow** column and then click **OK** twice.

1. In the **pki Home** pane, double-click **Request Filtering**.
2. The **File Name Extensions** tab is selected by default in the **Request Filtering** pane. In the **Actions** pane, click **Edit Feature Settings**.
3. In **Edit Request Filtering Settings**, select **Allow double escaping** and then click **OK**. Close Internet Information Services (IIS) Manager.
4. Run Windows PowerShell as an administrator. From Windows PowerShell, run the command **iisreset**

Enterprise Subordinate CA Setup

This section covers the setup of the Enterprise Subordinate CA. At this point, Windows 2012 R2 has already been installed, configured, and the server has full network connectivity. The CA should be part of the AD domain or have AD DS installed locally. In this design, the SubCA is part of the existing domain.

To start, we will configure the **CAPolicy.inf** file.

1. Open Windows PowerShell, type **notepad c:\Windows\CAPolicy.inf** and press ENTER.
2. When prompted to create a new file, click **Yes**.
3. Enter the following as the contents of the file:

```
[Version]

Signature= "$Windows NT$"

[Certsrv_Server]

LoadDefaultTemplates = False
```

4. Click **Save As**. Ensure the following:

   File name is set to **CAPolicy.inf**

   Save as type is set to **All Files**

   Encoding is **ANSI**

Next, we will install AD Certificate Services on the Subordinate CA.

1. On **SubCA**, as User1, run Windows PowerShell as Administrator, and then run the following command **gpupdate /force**. This action ensures that the GPO for the trusted root certification authority is applied to **SubCA**.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.

3. On the **Before you begin**, click **Next**.
4. On the **Select installation type** screen, ensure the default selection of **Role or Feature Based Install** is selected. Click **Next**.
5. On the **Select destination server** screen, ensure that **SubCA** is selected and then click **Next**.
6. On the **Select server roles** screen, select the **Active Directory Certificate Services** role.
7. When prompted to install **Remote Server Administration Tools** click **Add Features**. Click **Next**.
8. On the **Select features** screen, click **Next**.
9. On the **Active Directory Certificate Services** screen, click **Next**.
10. On the **Select role services** screen, ensure **Certification Authority** is selected and then click **Next**.
11. On the **Confirm installation selections** screen, verify the information and then click **Install**.
12. Wait for the installation to complete. The installation progress screen is displayed while the binary files for the CA are installed. When the binary file installation is complete, click the **Configure Active Directory Certificate Services on the destination server** link.
13. On the **Credentials** screen, the credentials for User1 appear. (Ensure the user is part of the Enterprise Admin Group). Click **Next**.
14. On the **Role Services** screen, select **Certification Authority**.
15. On the **Setup Type** screen, ensure that **Enterprise CA** is selected and then click **Next**.
16. On the **CA Type** screen, select **Subordinate CA** to install an Enterprise Subordinate CA. Click **Next**.
17. On the **Private Key** screen, ensure the **Create a new private key** option is selected and then click **Next**.
18. On the **Cryptography for CA** screen, ensure that the following are selected:

    - From the dropdown menu, select "**ECDSA_P384#Microsoft Software Key Store Provider**," a key length of **384**, and **SHA384**.

19. Then click **Next**.
20. On the **CA Name** screen, in **Common name for this CA**, type **CA-NAME**. You will see that the distinguished name changes to **CN=CA-NAME,DC=domain,DC=com**. Click **Next**.
21. On the **Certificate Request** screen, notice that **Save a certificate request to file on the target machine** is selected. This is the correct option because we are using an offline parent CA (the root CA) in this configuration. Leave the default and click **Next**.
22. On the **CA Database** screen, leave the default database and log locations and then click **Next**.
23. On the **Confirmation** screen, click **Configure**.
24. On the **Results** screen, you see that you must take the certificate request to the RootCA in order to complete the configuration. Click **Close.**

Next, the Certificate Signing Request (CSR) (.req file) must be submitted to the RootCA so that an X.509 identity certificate can be issued to the subordinate CA. This file should be in the folder indicated in Step 21 above, typically this file is on the root of the C: drive.

1. Once the .req file is moved to the RootCA, on RootCA, from Windows PowerShell, submit the request using the following command (assuming that C:\ is your media drive letter):
   certreq -submit C:\SubCA.domain.req
2. On **Certification Authority List**, ensure that **RootCA (Kerberos)** CA is selected and then click **OK**. You see that the certificate request is pending and the request identification number. Ensure that you note the request ID number.
3. On **RootCA**, the admin must approve the request. You can do this using Server Manager or by using **certutil** from the command line.

4. To use Server Manager, click **Tools**, and then click **Certification Authority**. Expand the **RootCA** object and then click **Pending Requests**.

   - Right-click the Request ID that corresponds with the one in the previous step.

   - Click **All Tasks** and then click **Issue**.

   - Click **Issued Certificates** and see the issued certificate in the **Details** pane.

5. To use certutil, enter **Certutil resubmit <*RequestId*>**, replace the actual request number for <RequestId>. For example, if the Request ID is 2, you would enter **Certutil resubmit 2**
6. From the command prompt on **RootCA**, retrieve the issued certificate by running the command
   certreq –retrieve <*RequestId*> **C**:**\SubCA.crt**.
   - Substitute the actual number of the request when it was submitted for <RequestId> and the actual drive letter of the removable media for <drive>. For example, if the request ID where 2 and the removable media was drive C:, then the request would be: **certreq –retrieve 2 C:\SubCA.crt**.
7. When prompted to select the CA, ensure that RootCA is selected and then click **OK**.

At this point, ensure the RootCA X.509 identity certificate, the CRL and the SubCA X.509 identity certificate are exported to the SubCA **C:\pki** folder for installation. We must install the certificate on the SubCA to start the AD CA services. Note, the RootCA certificate should be installed, via the MMC.exe certificate snap-in tool, into the SubCA machine account as a trusted root CA.

1. After the RootCA administrator processes the SubCA request and a valid certificate has been issued, open the **Server Manager**, then select **Tools** and select **Certification Authority**.
2. Right click on the CA server and select **All Tasks** -> **Install CA Certificate** and browse to the directory where the SubCA certificate is stored.
3. Select the SubCA certificate issued by the RootCA, make sure that *cer, *crt is selected, and press **Open.**
4. Select **OK** to install the certificate on the local trusted store.
5. Right click on the CA server and select **All Tasks** -> **Start Service** to start the CA Server. If the CA certificate was processed and installed correctly, then the server will start without any errors. A green check mark shows beside the server indicating that is functioning.
6. Next, copy appropriate files to the PKI location by using the command:

```
copy c:\Windows\system32\certsrv\certenroll\*.cr* c:\pki\
```

Next, the CDP and AIA settings need to be configured on SubCA.

1. On SubCA, as User1, right-click Windows PowerShell, click **Run as Administrator**. Click **Yes** to confirm that you want to run Windows PowerShell as an Administrator.
2. From Windows PowerShell run the following commands (Ensure you reference your domain):

```
certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\system32\CertSrv\CertEnroll\%3%8.crl\n2:http://www.domain.org/pki/%3%8.crl"


certutil -setreg CA\CACertPublicationURLs
"2:http://www.domain.org/pki/%1_%3%4.crt\n1:file://\\SubCA.domain.org\pki\%1_%3%4.crt"
```

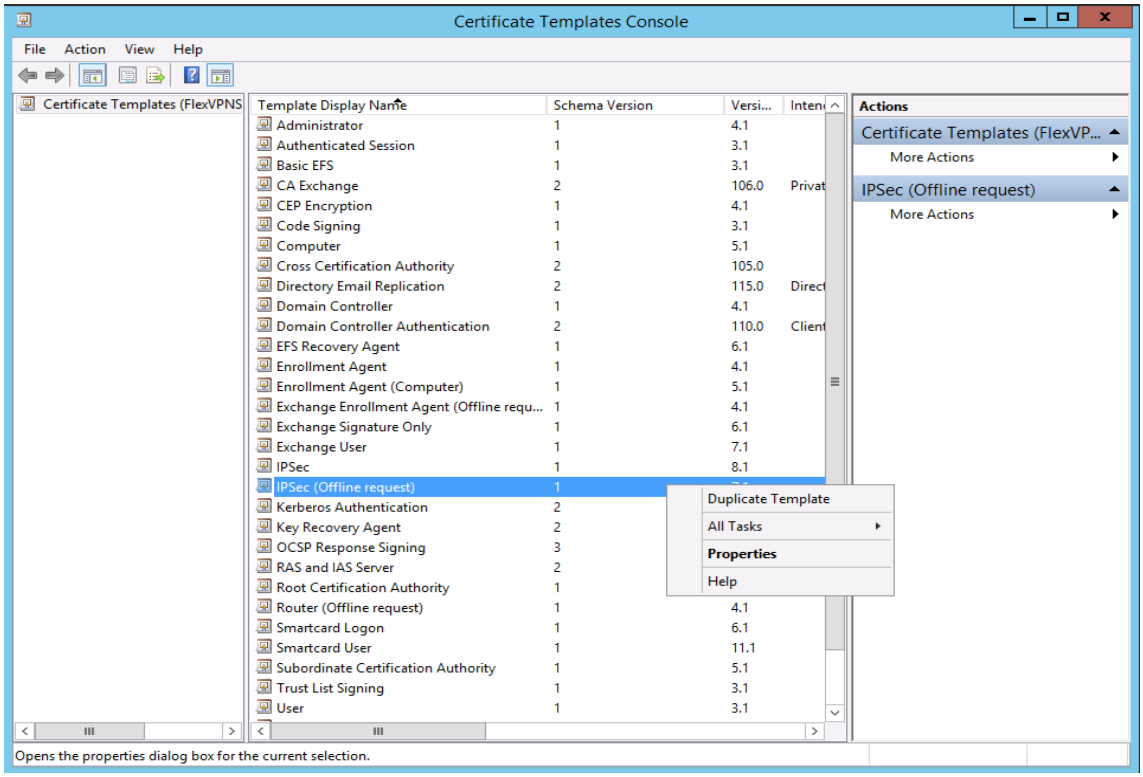
```
Certutil -setreg CA\CRLPeriodUnits 2

Certutil -setreg CA\CRLPeriod "Weeks"

Certutil -setreg CA\CRLDeltaPeriodUnits 1

Certutil -setreg CA\CRLDeltaPeriod "Days"

Certutil -setreg CA\CRLOverlapPeriodUnits 12

Certutil -setreg CA\CRLOverlapPeriod "Hours"

Certutil -setreg CA\ValidityPeriodUnits 5

Certutil -setreg CA\ValidityPeriod "Years"

restart-service certsvc

certutil -crl
```

Finally, the RootCA can be removed from the network and stored in a secure location. The remaining configurations, certificate request, templates etc. will all be processed via the SubCA. Next, we must configure the certificate templates to support Suite B.

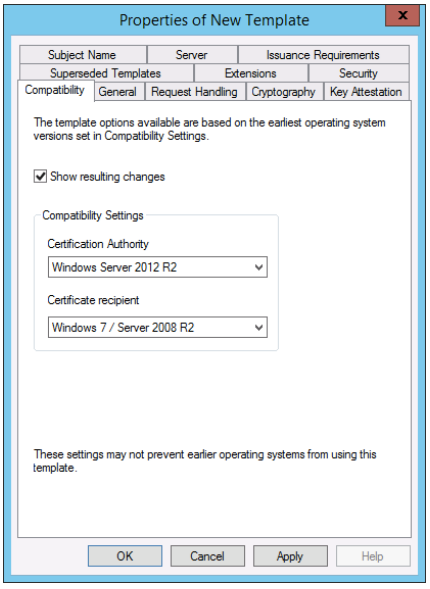
Version 3 Template Configuration

After completing the setup and configuration of the root CA and subordinate CA, version 3 templates must be configured to issue EC/Suite B certificates to the ASA and user machines. The certificate templates need to specify the certificate issuance policies for those devices. Microsoft Certificate Services has preconfigured templates that are installed as part of the CA installation process. In Windows 2012, these default templates do not contain the newer Suite B algorithms that were implemented in Windows 2008 R2 and beyond and need to be modified. It is also necessary to ensure the templates have the correct Suite B algorithms specified along with the appropriate Key Usage (KU) and Enhanced Key Usage (EKU) values to ensure the issued certificate follow the Suite B guidelines and support device authentication per the guidelines in the caveats section. In this design, two templates will be created. One will be used for ASA enrollment and the other for client devices.

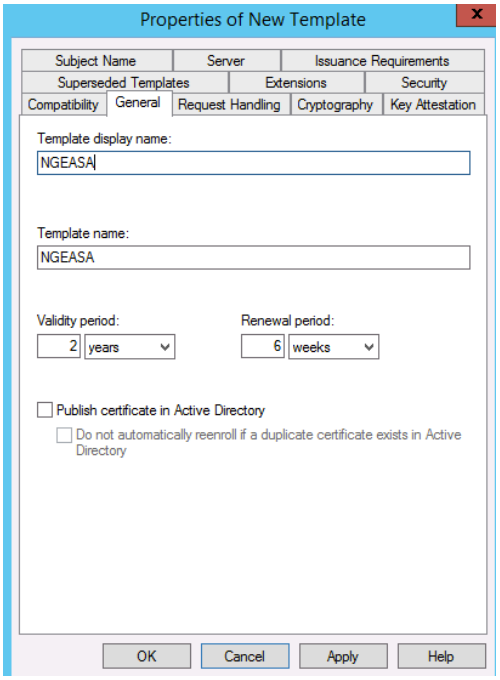
1. Open **Administrative Tools** and select **Certification Authority**
2. Right click **Certificate Templates** and select **Manage**.
3. Right click on **IPSec (Offline request)** template and select **Duplicate Template**.



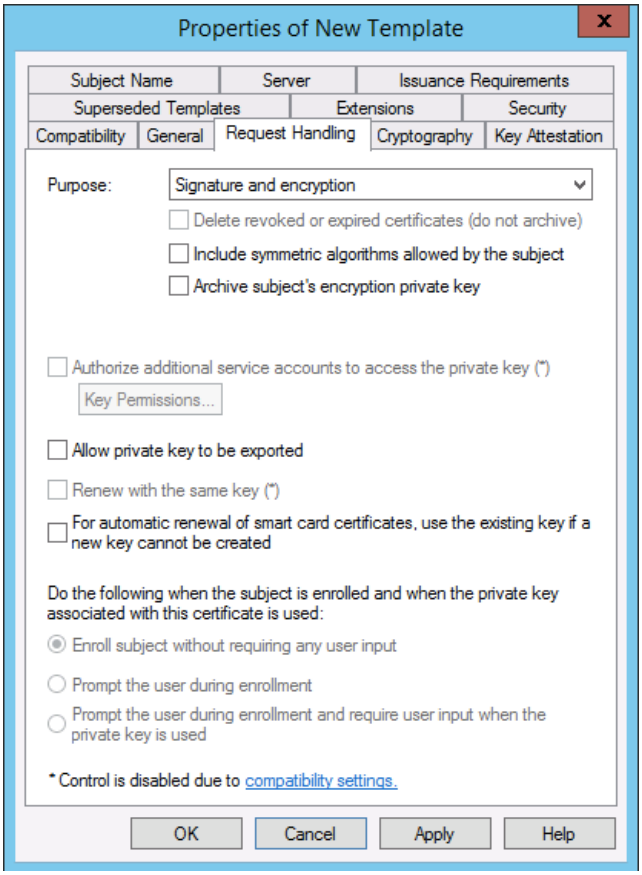
4. A new template appears on the **Compatibility** section. Under the Certification Authority dropdown menu, select **Windows Server 2012 R2,** then click **OK** for resulting changes. Under the **Certificate recipient** dropdown, select **Windows 7/Server 2008 R2**, then click **OK** for resulting changes.



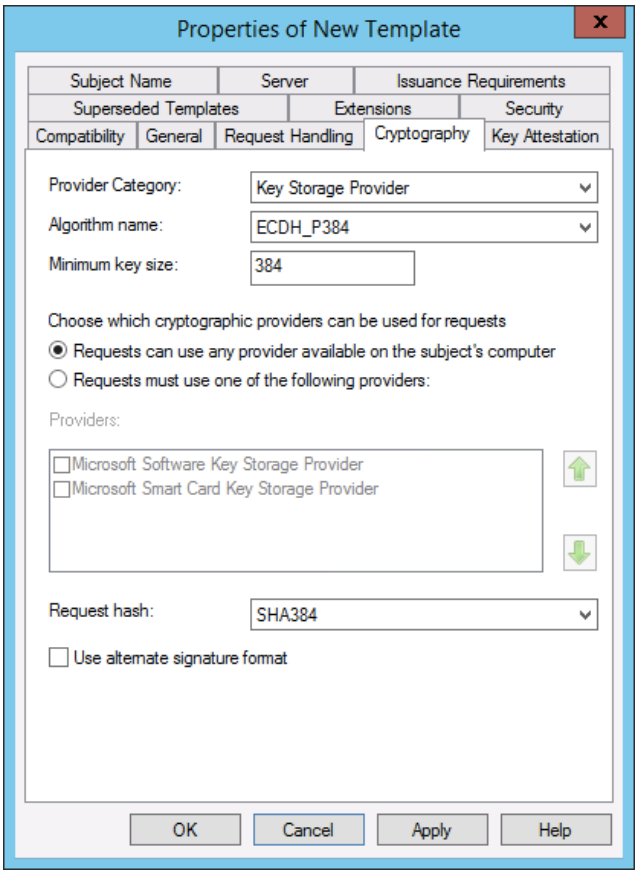
5. Under the **General** tab, in **Template display name** enter **NGEASA** with a validity period of 2 years, and a renewal period of 6 weeks.



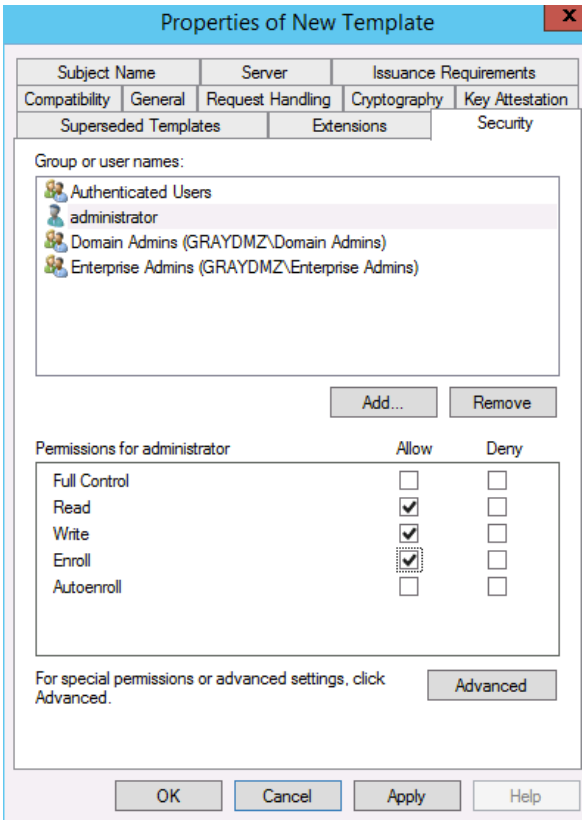
6. Under the **Request Handling** tab, select **Purpose**, make sure that **Signature and Encryption** is selected.



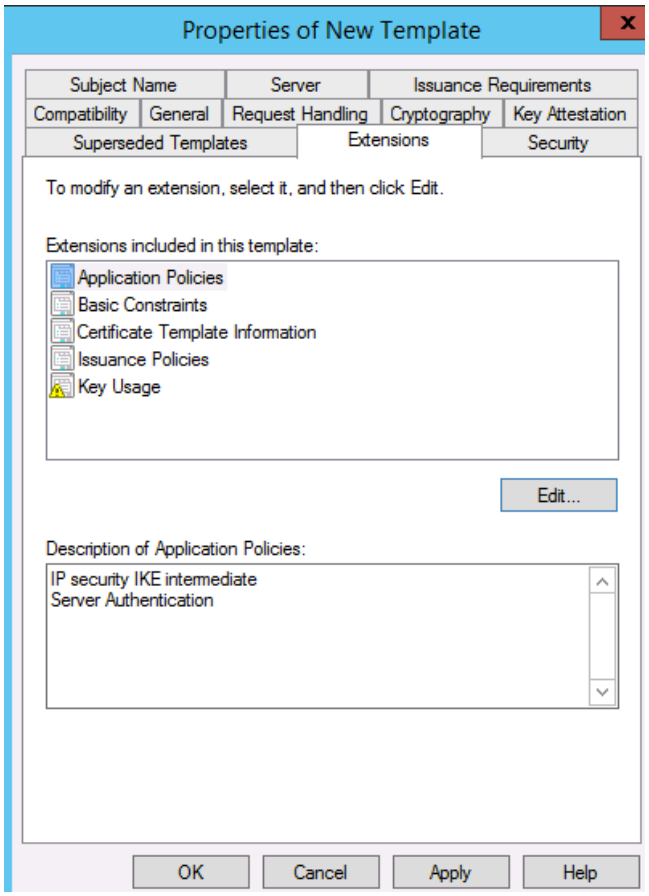
7. Under the **Cryptography** tab, select the Provider category **Key Storage Provider**, Algorithm name **ECDH_P384**, Minimum key size **384**, and the request hash **SHA384**. Leave everything else at default.



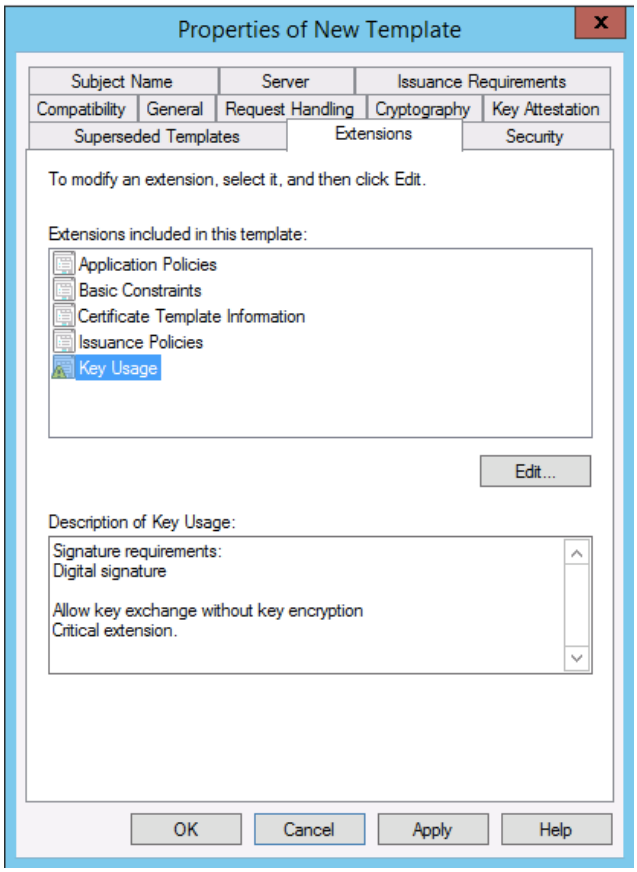
8. Next click the **Security** tab. The purpose of this template is to be used this for manual enrollment while logged on as an administrator. Therefore, ensure the appropriate permissions are selected: **Read, Write, and Enroll**.



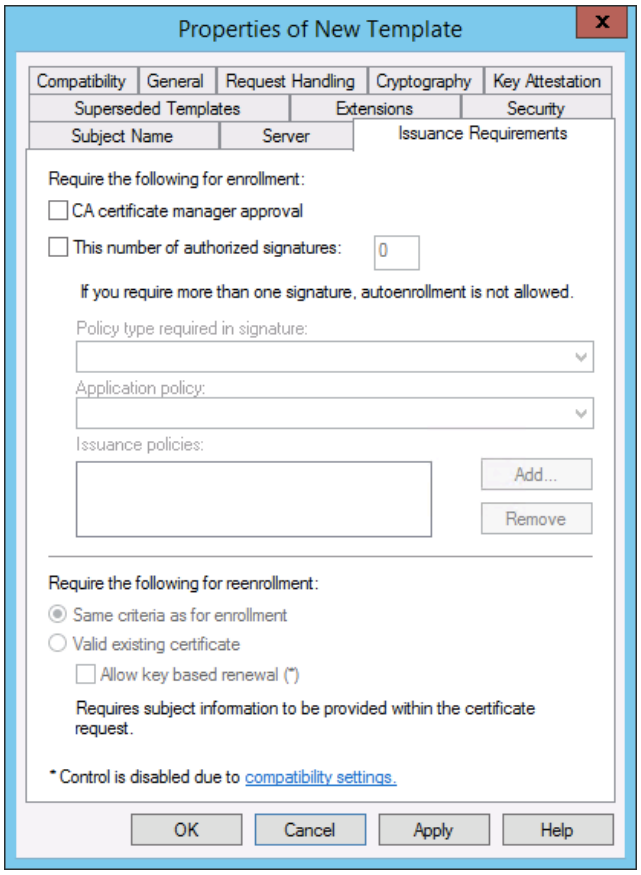
9. Select the **Extensions** tab. Under **Application Policies** (EKU), **Description of Key Usage**, **IP Security IKE intermediate** is already present. We need to add **Server Authentication** to the EKU field. Select **Edit,** then Add **Server Authentication**, then click **OK**. Make sure **Server Authentication** and **IP Security IKE intermediate** are displayed in the **Description of Key Usage box**.



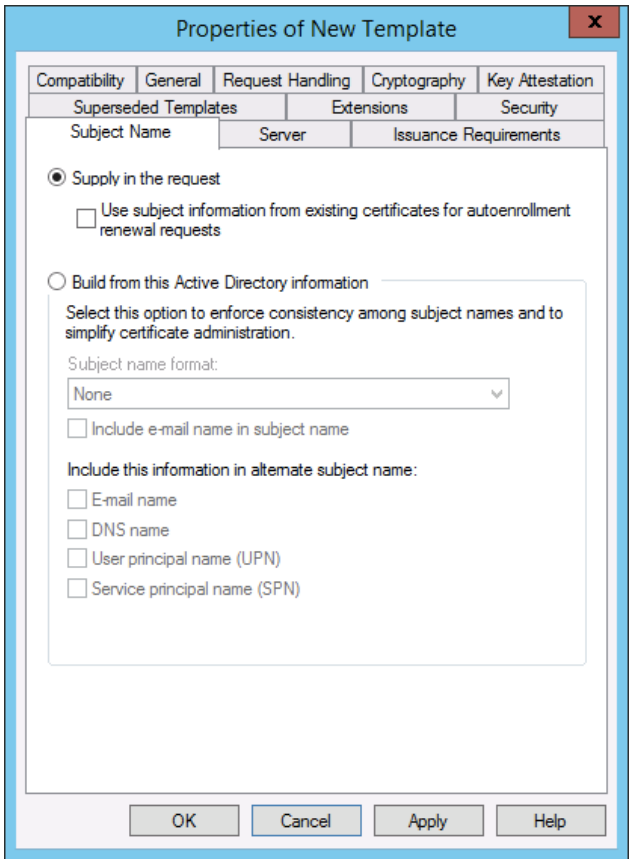
10. Under **Key Usage, Description of Key Usage** box, make sure **Digital signature, Allow key exchange without key encryption** and **Critical extension** are shown. As mentioned in the caveats section, these fields must be present in the ASA's certificate along with the EKU value for either IKE Intermediate and/or Server Authentication. If the ASA's certificate does not have these field populated, the AnyConnect client will not trust the ASA's certificate.



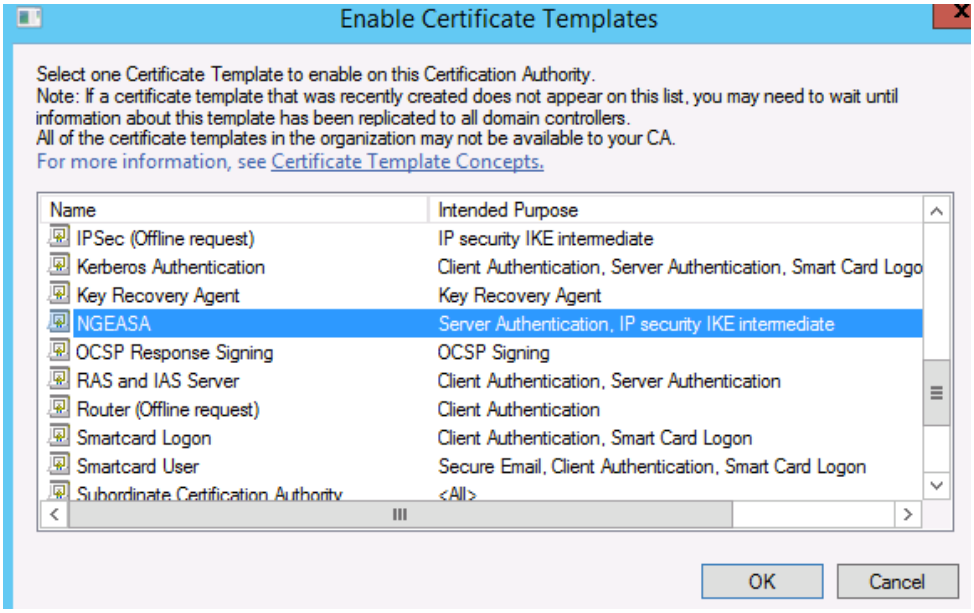
11. Select **Issuance Requirements** tab. If it is desired to have the CA admin approve request, the **CA certificate manager approval** box should be checked. However, for this design, ensure that **CA certificate manager approval** is not selected.



12. Next, click on the **Subject Name** tab. The Common Name (CN) from the ASA will be used for the CSR. We want this information to be supplied in the request. Therefore, we need to make sure that **Supply in the request** is selected (default). Select **OK**.

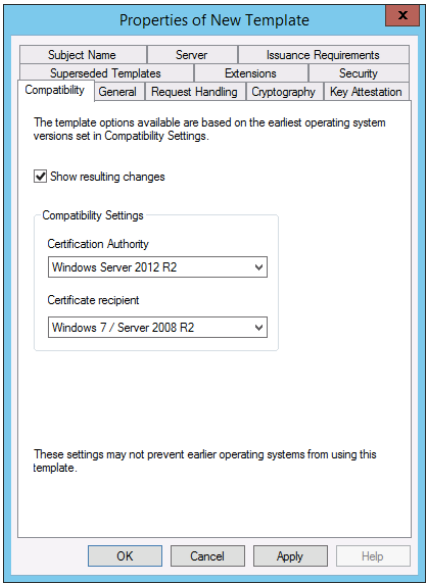


13. After configuring the **NGEASA** certificate template, we must ensure the template is available for use by the CA. Right click **Certificate Template,** select **New** and **Certificate Template to Issue**. Select the previously created **NGEASA** certificate template, then press **OK.**

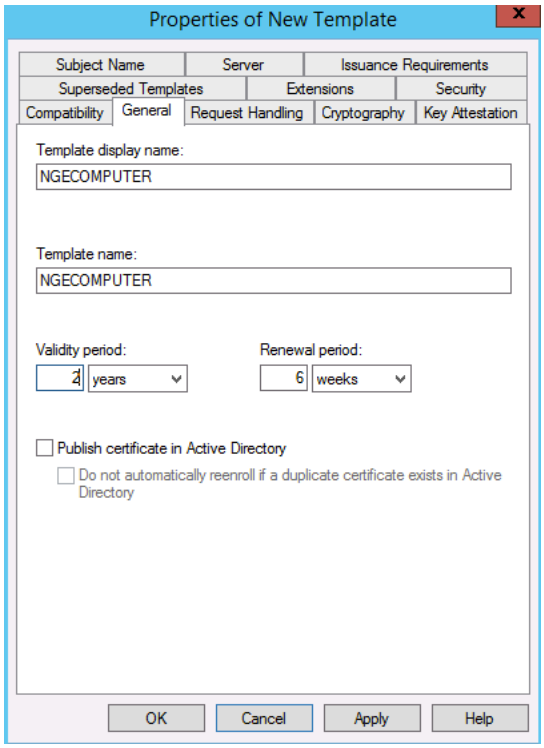


After completing the NGEASA template, we need to also configure a template for client certificates.

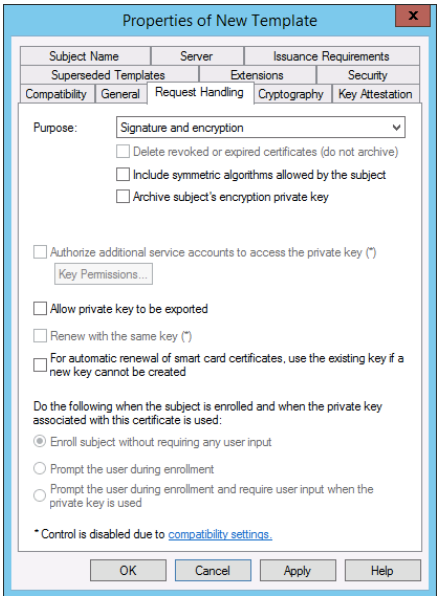
1. Return to **Certificate Templates** by going to the **Certificate Templates** folder on the **Certificate Authority** console, right-click **Certificate Templates** and select **Manage**.
2. Find the template for **Computer**, right-click on it and select **Duplicate Template**.
3. A new template appears on the **Compatibility** section. Under the Certification Authority dropdown menu, select **Windows Server 2012 R2,** then click **OK** for resulting changes. Under the **Certificate recipient** dropdown, select **Windows 7/Server 2008 R2**, then click **OK** for resulting changes.



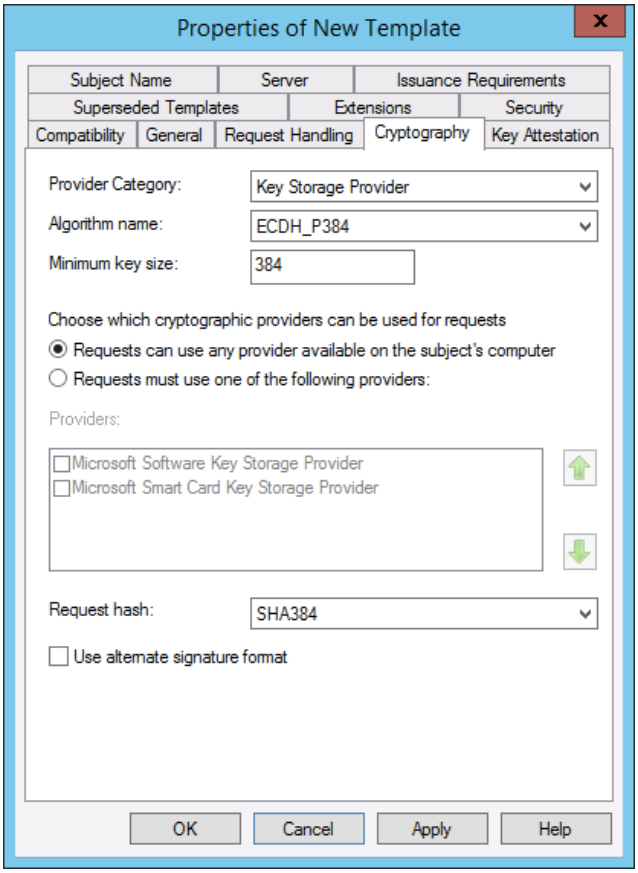
4. Under the **General** tab, in **Template display name** enter **NGECOMPUTER** with a validity period of 2 years, and a renewal period of 6 weeks.



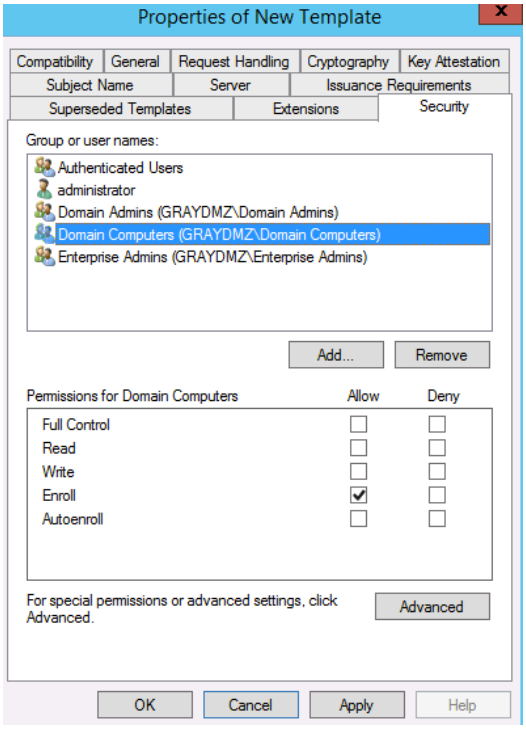
5. Under the **Request Handling** tab, select **Purpose**, make sure that **Signature and Encryption** is selected.



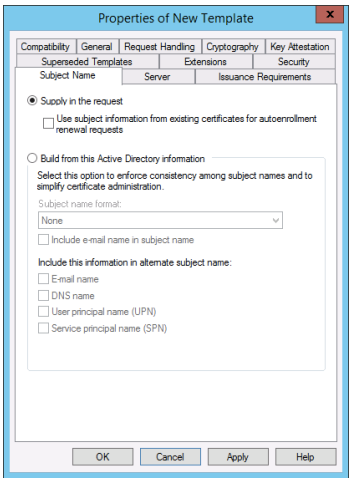
6. Under the **Cryptography** tab, select the Provider category **Key Storage Provider**, Algorithm name **ECDH_P384**, Minimum key size **384**, and the request hash **SHA384**. Leave everything else at default.



7. Next, click the **Security** tab. The purpose of this template is to be used this for manual enrollment by the computer. Therefore, ensure the appropriate permissions are selected: **Enroll**.

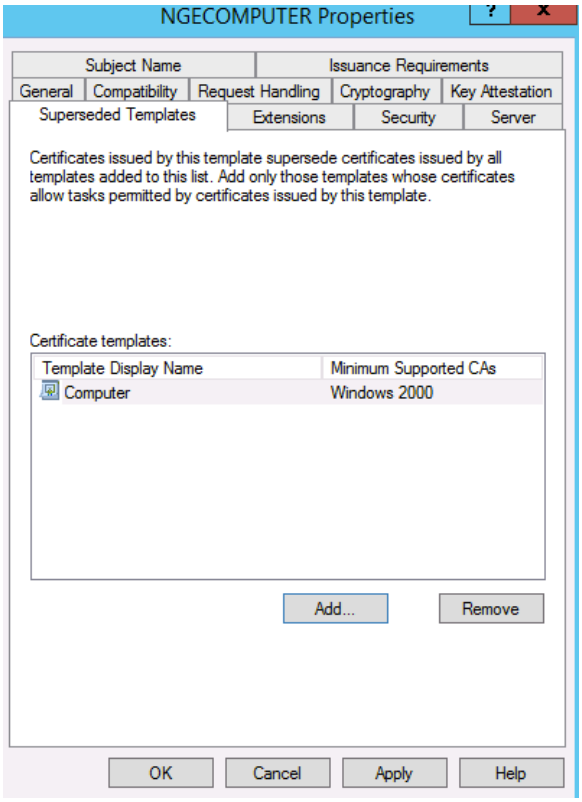


8. Next, click on the **Subject Name** tab. The Common Name (CN) from the client will be used for the CSR. We want this information to be supplied in the request. Therefore, we need to make sure that **Supply in the request** is selected (default). Select **OK**.



This template will obsolete the original **Computer** Template that we modified. Since it is not desirable to issue certificates under the previous **Computer** template, this needs to be specified under the **Superseded Templates** tab.

9. Under this tab, click **Add**, select the **Computer** Template, and then click **OK**. Click **Apply**, for the template changes to take effect.



10. After configuring the **NGECOMPUTER** certificate template, we must ensure the template is available for use by the CA. Right click **Certificate Template,** select **New** and **Certificate Template to Issue**. Select the previously created **NGECOMPUTER** certificate template, then click **OK.**

Appendix C – ASA VPN Verification Commands

Note, important data to verify is highlighted in yellow below.

```
grayasavpn# sh crypto isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id        Local            Remote      Status        Role

 4711049     192.168.0.1/4500     10.40.40.7/53509     READY
RESPONDER

     Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign:
ECDSA, Auth

verify: EAP

     Life/Active Time: 86400/388 sec

Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535

          remote selector 192.168.10.1/0 - 192.168.10.1/65535

          ESP spi in/out: 0x54d56e/0xd0cf1c23



grayasavpn# sh crypto ipsec sa

interface: outside

    Crypto map tag: NGE-DYNAMIC-VPN, seq num: 1, local addr:
192.168.0.1



     local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

     remote ident (addr/mask/prot/port):
(192.168.10.1/255.255.255.255/0/0)
```

```
current_peer: 10.40.40.7, username: ngeuser

dynamic allocated peer ip: 192.168.10.1



#pkts encaps: 33, #pkts encrypt: 33, #pkts digest: 33

#pkts decaps: 338, #pkts decrypt: 338, #pkts verify: 338

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 33, #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.: 192.168.0.1/4500, remote crypto endpt.:
10.40.40.7/53

path mtu 1464, ipsec overhead 66(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: D0CF1C23

current inbound spi : 0054D56E



 inbound esp sas:

spi: 0x0054D56E (5559662)

   transform: esp-aes-gcm-256 esp-null-hmac no compression

   in use settings ={RA, Tunnel,  NAT-T-Encaps, IKEv2, }

   slot: 0, conn_id: 4096, crypto-map: NGE-DYNAMIC-VPN

   sa timing: remaining key lifetime (sec): 26309
```

```
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD0CF1C23 (3503234083)
        transform: esp-aes-gcm-256 esp-null-hmac no compression
        in use settings ={RA, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 4096, crypto-map: NGE-DYNAMIC-VPN
        sa timing: remaining key lifetime (sec): 26309
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001


grayasavpn# sh vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                          Active : Cumulative : Peak Concur : Inactive
                        ----------------------------------------------
AnyConnect Client          :      1 :          1 :          1 :        0
  IKEv2 IPsec              :      1 :          1 :          1 :        0
--------------------------------------------------------------------------
Total Active and Inactive    :      1          Total Cumulative :      1
Device Total VPN Capacity    :    250
Device Load                  :     0%
```

```
--------------------------------------------------------------------------------



--------------------------------------------------------------------------------

Tunnels Summary

--------------------------------------------------------------------------------

                            Active : Cumulative : Peak Concurrent

                          ------------------------------------------

IKEv2                     :      1 :          1 :               1

IPsecOverNatT             :      1 :          1 :               1

AnyConnect-Parent         :      1 :          1 :               1

--------------------------------------------------------------------------------

Totals                    :      3 :          3

--------------------------------------------------------------------------------
```