Cisco Systems

FlexVPN with Suite-B (Next Generation Encryption) Design Recommendation

Version 1.0

Authored by Arnold Ocasio – CCIE #8446

Advanced Services

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

Tables

Document Control

History

Table 1 Revision History

Version No.	Issue Date	Status	Reason for Change
1.0	11-25-2013	Initial Draft	

Review

Table 2 Revision Review

Reviewer's Details	Version No.	Date
Wade Lehrschall – Cisco Technical Lead	1.0	December 3, 2013
Justin Poole – Cisco Systems Engineer	1.0	December 2, 2013

Executive Summary

This document provides guidance for configuring a Suite-B (Next Generation Encryption) FlexVPN solution on a Cisco IOS router platform. The design was developed to create a FlexVPN solution that consists of an Elliptical Curve Cryptography (ECC) Public Key Infrastructure (PKI) to support a Suite-B solution based on the ECDH 384 set of algorithms.

A Microsoft Certificate Authority solution was used for the design presented in this document. Specifically, Windows 2012 R2 was selected to support the Suite-B PKI implementation. This PKI design is based on a two-tier PKI solution using an offline standalone root Certificate of Authority (CA), and an Enterprise Subordinate CA. The function of the subordinate CA is to issue X.509 digital certificates and provide Certificate Revocation List (CRL) to FlexVPN routers. In addition, version 3 Suite-B complaint templates are configured in the subordinate CA. The standalone CA can be a Microsoft member server or a single standalone server. In this design, the standalone CA was configured as a standalone (Workgroup) server. However, the subordinate CA was configured as part of a Microsoft domain with Active Directory services enabled. Furthermore, the subordinate CA was deployed on a router SRE module running VMware ESXi 5.1.0. However at CUSTOMERA, the subordinate CA will be deployed on a UCS E-Series server module.

Each FlexVPN router is configured with separate trustpoints containing Suite-B X.509 digital certificates, such as the certificate of authority, a subordinate CA, and an identity certificate. Unfortunately, Suite-B does not support auto-enrollment at this time. As a result a Certificate Signing Request (CSR) must be generated for each router and sent to the subordinate CA administrator to issue an X.509 digital certificate. In addition, a certificate for each trustpoint has to be manually imported into the router.

The Cisco FlexVPN design consists of two-hub routers providing the FlexVPN cloud network IP addresses for the FlexVPN client tunnel interface, and the hub routers are configured to use Dynamic Virtual Tunnel Interfaces using IP unnumbered to the loopback interface. The FlexVPN aaa authorization cert list feature is used to provide the FlexVPN client with an IP address, and the subnet IP addresses are distributed between the two hub routers. FlexVPN high availability is provided by the two hub routers in a failover configuration using features such as HSRP tracking along with ip sla monitoring a specific IP address. The failover design consists of each FlexVPN client having two FlexVPN hub peers, in which connectivity is checked to the main hub using Dead Peer Detection (DPD) messages. In the event the main hub connectivity is lost, the client clears the Security Association and builds a new connection to the backup hub. In addition, the spoke routers use Static Virtual Tunnel Interfaces (SVTI) using dynamic tunnel destinations to support the failover feature.

For the IPSec design portion, IKEv2 Phase I is based on Suite-B cbc-256 with X.509 digital certificates cryptographic key lengths of 384 ECDH, and a hash algorithm of SHA-2 384-bit (HMAC variant). The Phase II Encapsulating Security Protocol is protected by a set of Suite-B esp-gcm 256 algorithms.

Finally, EIGRP is used as the IGP routing protocol for this solution with the hub routers advertising a default route configured as stub router. The FlexVPN clients receive only a default route from the active hub.

Introduction

This document is a combined High Level Design (HLD) and Low Level Design (LLD), which contains detailed information on a Cisco FlexVPN configuration to support Suite-B X.509 digital certificates as discussed in the Executive Summary section.

Suite-B is a certificate base solution defined in RFC 6379. FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub and spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps.

Internet Key Exchange Version (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs).

It is assumed that the audience of this document has a basic knowledge of PKI, Cisco IPSec, IKEv2, routing, Windows 2012 R2, VMware, and Cisco Service Ready Module (SRE) or UCS E-Series Server modules, which includes:

- Purpose of a Certificate of Authority
- X.509 digital certificate formats (PEM, DER, etc.)
- Cisco FlexVPN (IKEv2)
- Cisco IPSec Phase I and Phase II messaging
- Cisco EIGRP Routing Protocol – Stub Feature
- Suite-B as defined in RFC 6379
- Windows 2012 R2 basic administration
- Cisco SRE operation within the ISR G2 router (vSwtich0 and vSwitch1)
- VMware ESXi vSphere 5.1.0 Hypervisor Management

FlexVPN Test Bed Diagram

Physical Topology Diagram

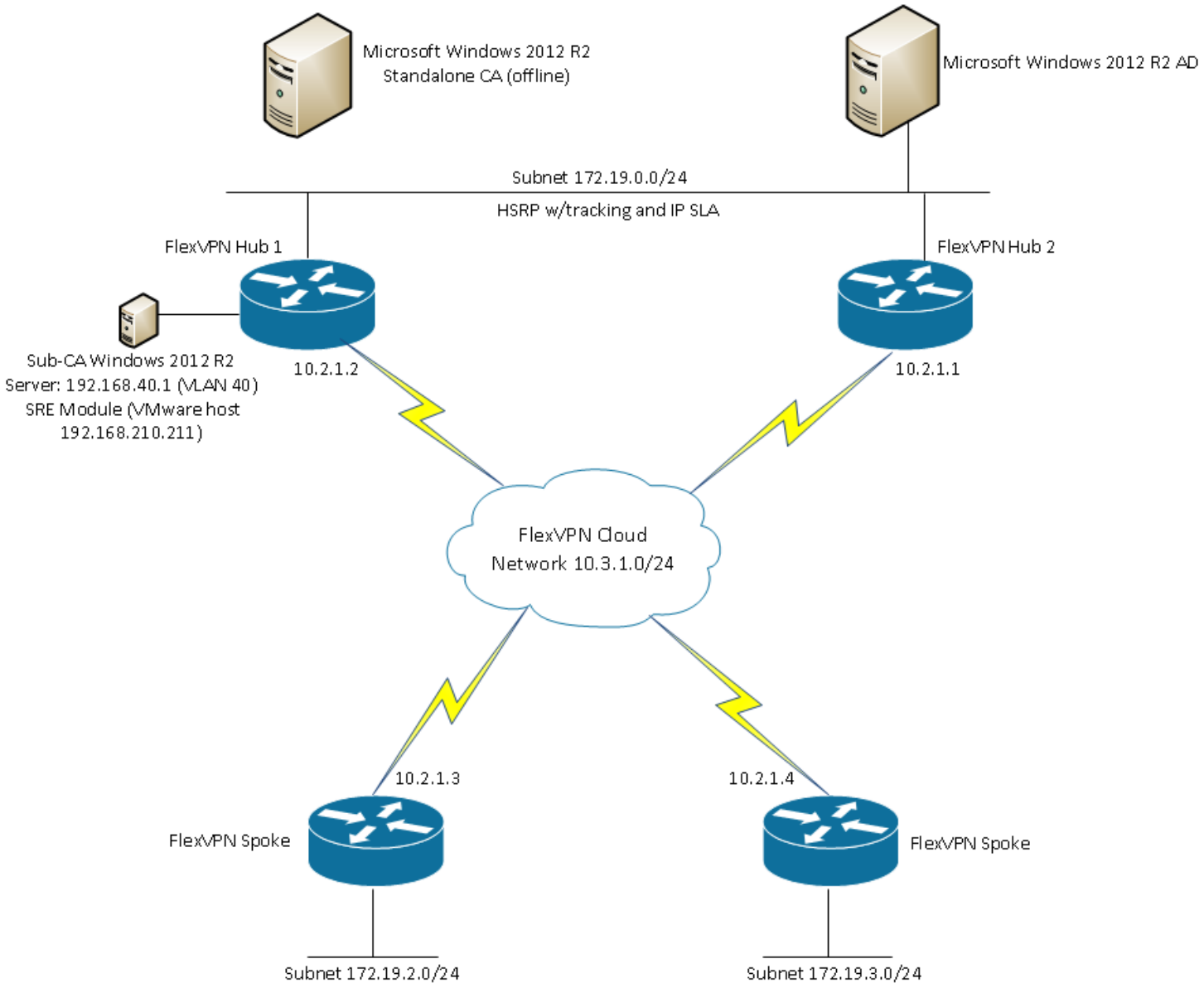


Figure 1: Physical FlexVPN RTP Lab Topology Diagram

Prerequisites

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

- Installation and configuration of Windows 2012 R2 server standalone CA server
- Windows Active Directory information (domain, forest, etc.)
- Windows user name and password with enough rights to join the subordinate CA to a domain
- Windows servers naming convention
- VMware vSphere Hypervisor ESXi 5.1.0 license
- VMware vSphere Hypervisor Latest ESXi 5.1.0 updates
- Windows 2012 R2 ISO Image
- Cisco SRE or UCS-E Series Server IP Addresses (Service Module interface and VMware machine)

Cisco SRE Module Setup

Console or SSH Connection

The Cisco SRE module can be access either through a console port or using an SSH connection to the Cisco ISR G2 routers. There is a RS-232 port with an RJ-45 connector. You can connect to the console port via a terminal program such as Windows HyperTermimal (9600,8,N,1) with a Cisco blue console cable with a DB-9 connector at one end and RJ-45 connector at the other end. Or, an SSH connection can be used to connect to the ISR G2 router.

Initial SRE Module Configuration

To access the VMware vSphere Hypervisor through the ISR G2, you must provide two IP addresses: one IP address is of the interface that connects the router to the VMware vSphere Hypervisor; and the other IP address is of the VMware vSphere Hypervisor.

Procedure

Step 1. Install the SRE Module or UCS-E Series Server into the ISR G2 router (either C2951 or C3945).

Step 2. Access the ISR G2 router and enter an IP address and a meaningful description for one of the Gigabit interfaces that will be used for the Service Ready Engine (SRE) interface:

```
H1-AA-14-3945-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
H1-AA-14-3945-A(config)#interface gigabitEthernet 0/2
H1-AA-14-3945-A(config-if)#description Windows 2012 R2 - Sub-CA
H1-AA-14-3945-A(config-if)#ip address 192.168.210.110 255.255.255.0
```

Step 3. Configure the SRE module interface *slot*/0 VMware vSphere Hypervisor (vSwitch0) and add a static route to reach the VMware ESXi host

```
H1-AA-14-3945-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
H1-AA-14-3945-A(config)#interface sm2/0
H1-AA-14-3945-A(config-if)#description ESXi 5.1.0 vSphere Hypervisor
H1-AA-14-3945-A(config-if)#ip unnumbered GigabitEthernet0/2
H1-AA-14-3945-A(config-if)# service-module ip address 192.168.210.111 255.255.255.0
H1-AA-14-3945-A(config-if)# service-module ip default-gateway 192.168.210.110
H1-AA-14-3945-A(config)#ip route 192.168.210.111 255.255.255.255 SM2/0
```

Step 4. Configure the SRE module interface *slot*/0 VMware vSphere Hypervisor (vSwitch1)

```
H1-AA-14-3945-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
H1-AA-14-3945-A(config)#interface sm2/1
H1-AA-14-3945-A(config-if)# description Internal switch interface connected to Service Module
H1-AA-14-3945-A(config-if)# switchport mode trunk
```

Step 5. Create a VLAN and an Switch Virtual Interface (SVI) to be used by the VM machine. This VLAN is the access gateway for the VMware host machine (Windows 2012 R2) to the network.

```
H1-AA-14-3945-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
H1-AA-14-3945-A(config)#vlan 40
H1-AA-14-3945-A(config-if)#name VMware_Host
H1-AA-14-3945-A(config-if)#exit
H1-AA-14-3945-A(config)# interface Vlan40
H1-AA-14-3945-A(config-if)# description Windows 2012 R2 Sub-CA
H1-AA-14-3945-A(config-if)# ip address 192.168.40.254 255.255.255.0
```

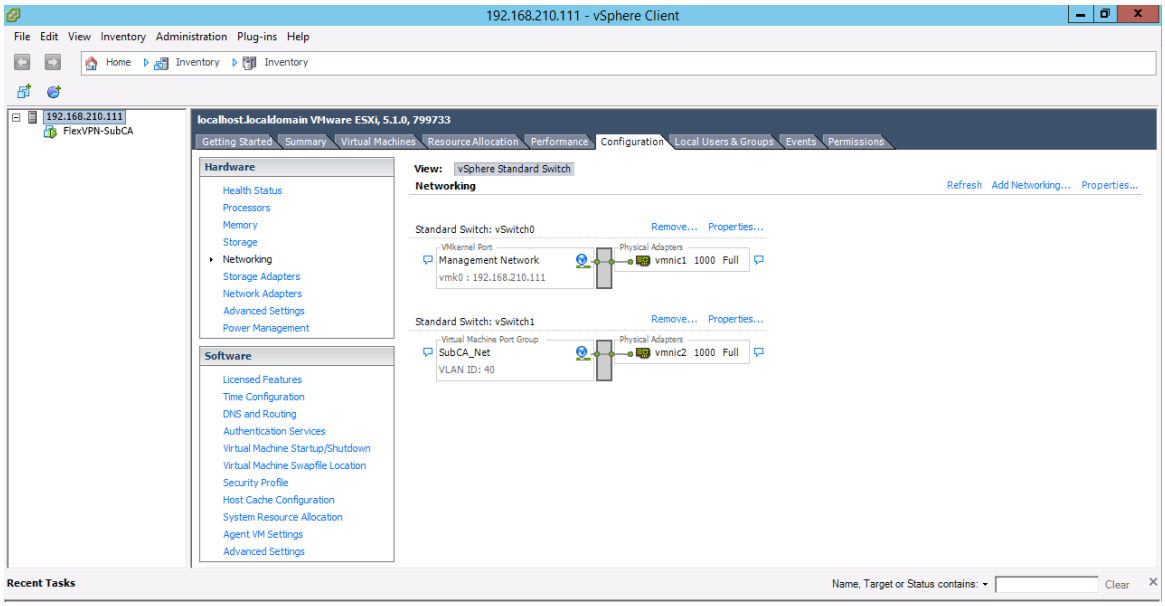
Step 6. Register and active the vSphere Hypervisor to a VMware vCenter Server

Step 7. Update the vSphere ESXi 5.1.0 with the latest VMware patches

Step 8. Install Windows 2012 R2 with a valid Activation Key

Step 9. Configure the IP addresses for the Microsoft Windows Server by using the standard Microsoft Windows network configuration setup process. In this test, the IP address of the server was set to 192.168.40.1 and a default gateway of 192.168.40.254.

Step 10. Check with the VMware administrator to make sure a vSwitch was created for the VM host machine with its relevant VLAN assigned to it. In this test, VLAN 40 was used.



Step 11. Change the server from Workgroup to a Domain Member Server and reboot

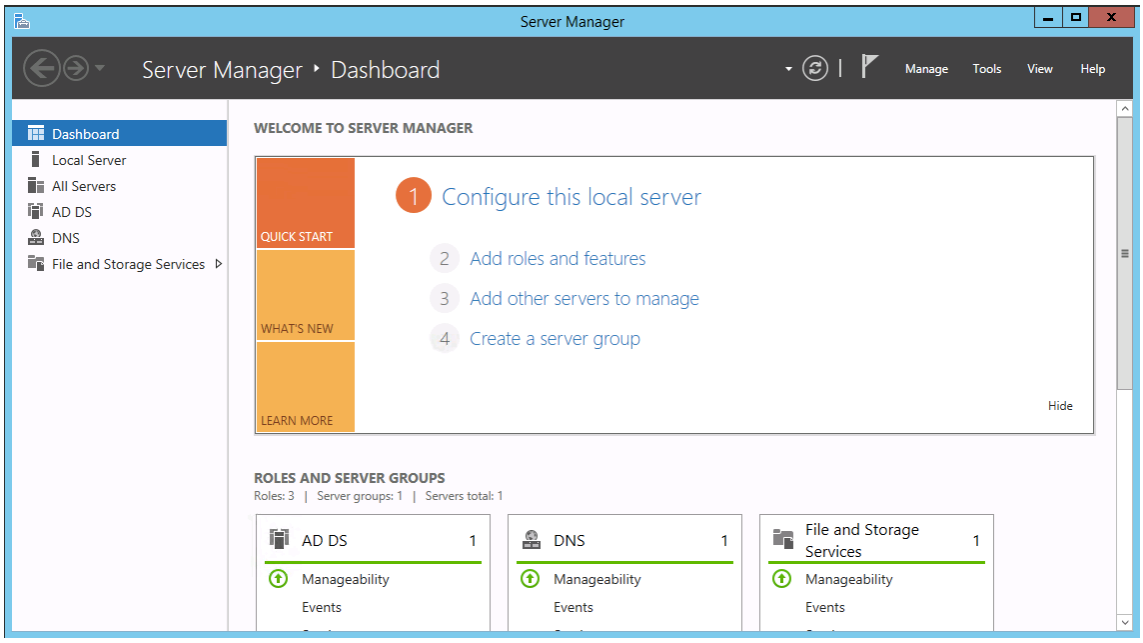
Step 12. Active the Microsoft Windows 2012 R2 license

Step 13. Install VMware tools

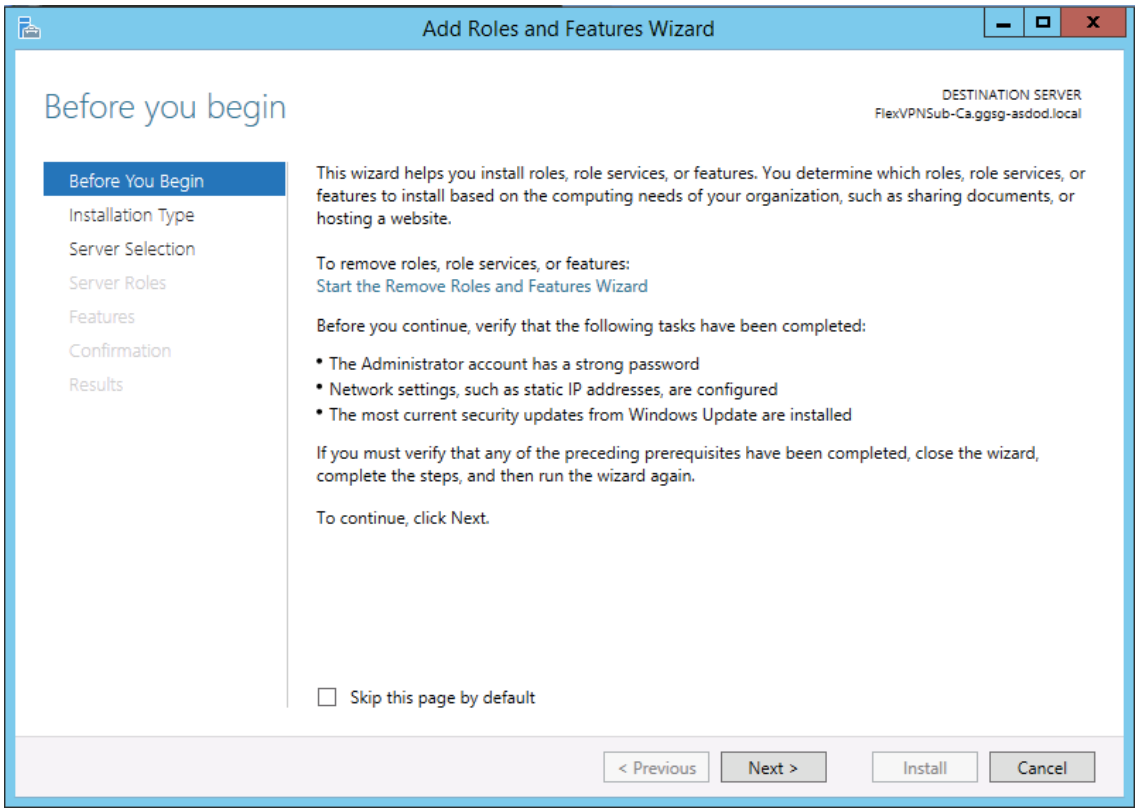
Windows 2012 R2 Subordinate CA Setup

This section covers the setup of the subordinate CA, at this point Windows 2012 R2 has already been installed, configured, and the SRE or UCS-E Series Server module has full network connectivity.

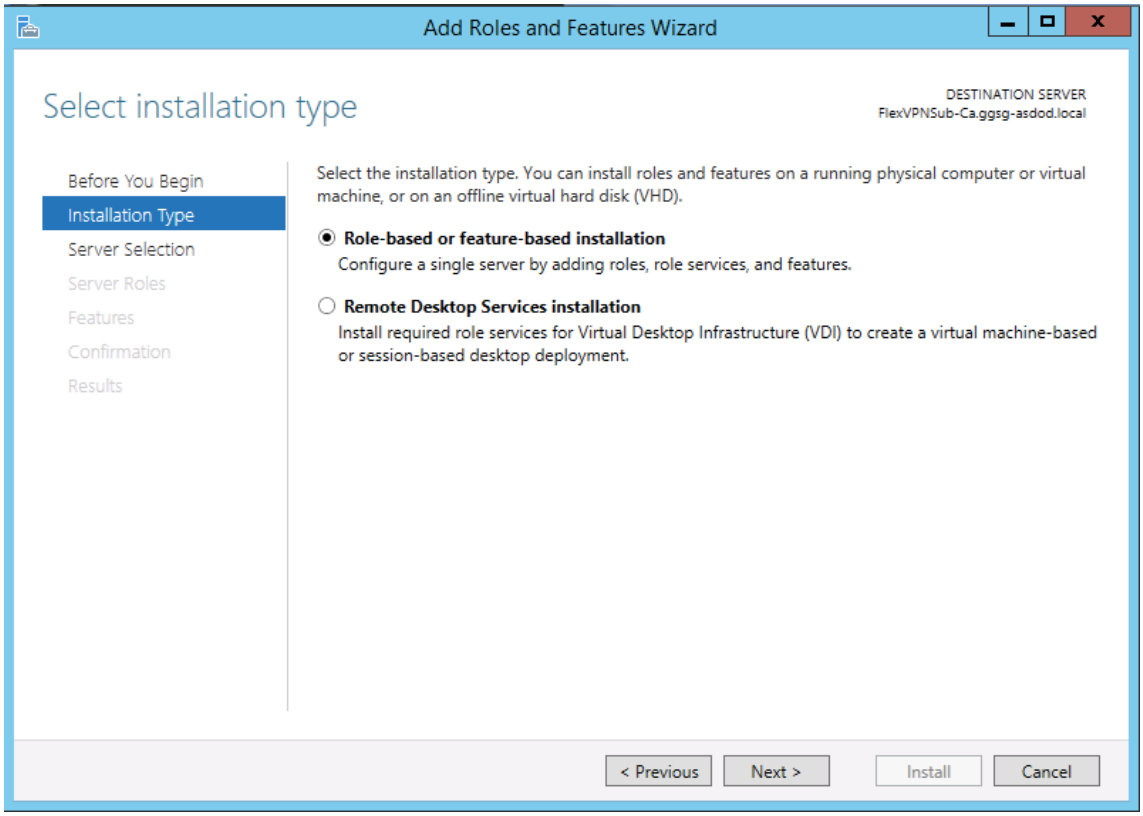
Step 1. Log into the Windows 2012 R2 Server and open the Server Manager. Select Add Roles and features



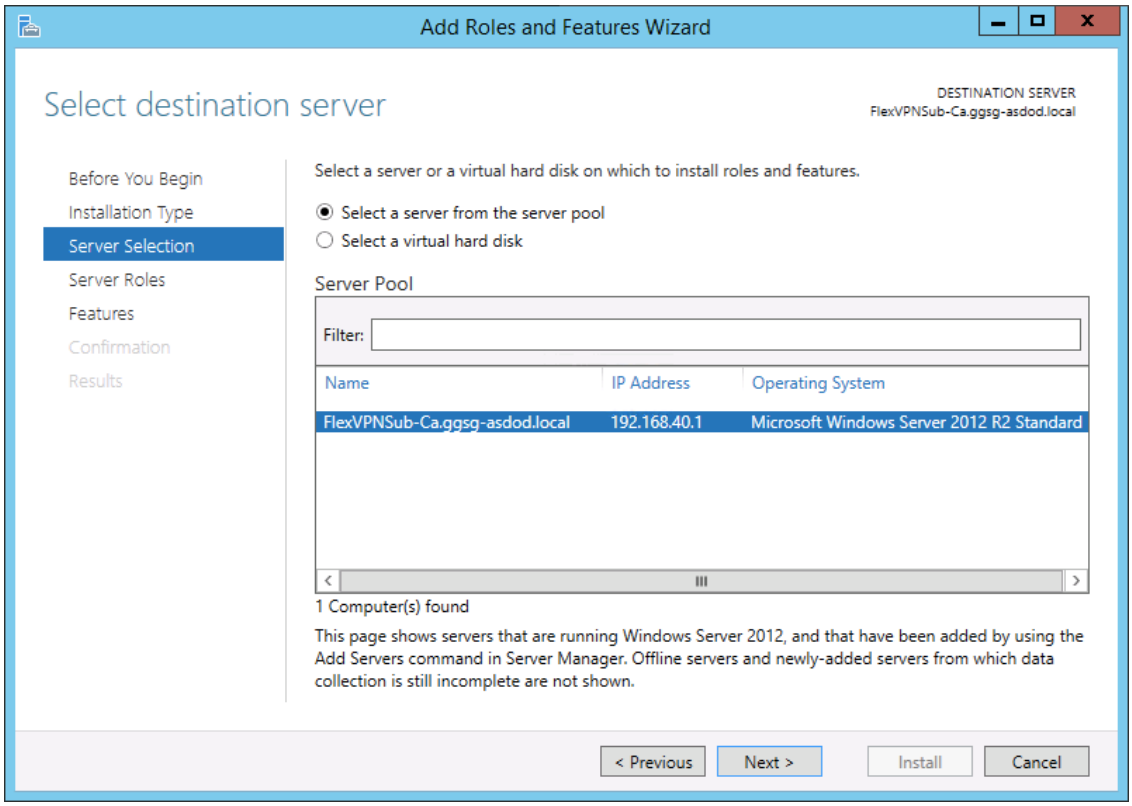
Step 2. The Add Roles and Features Wizard appears; select Next.



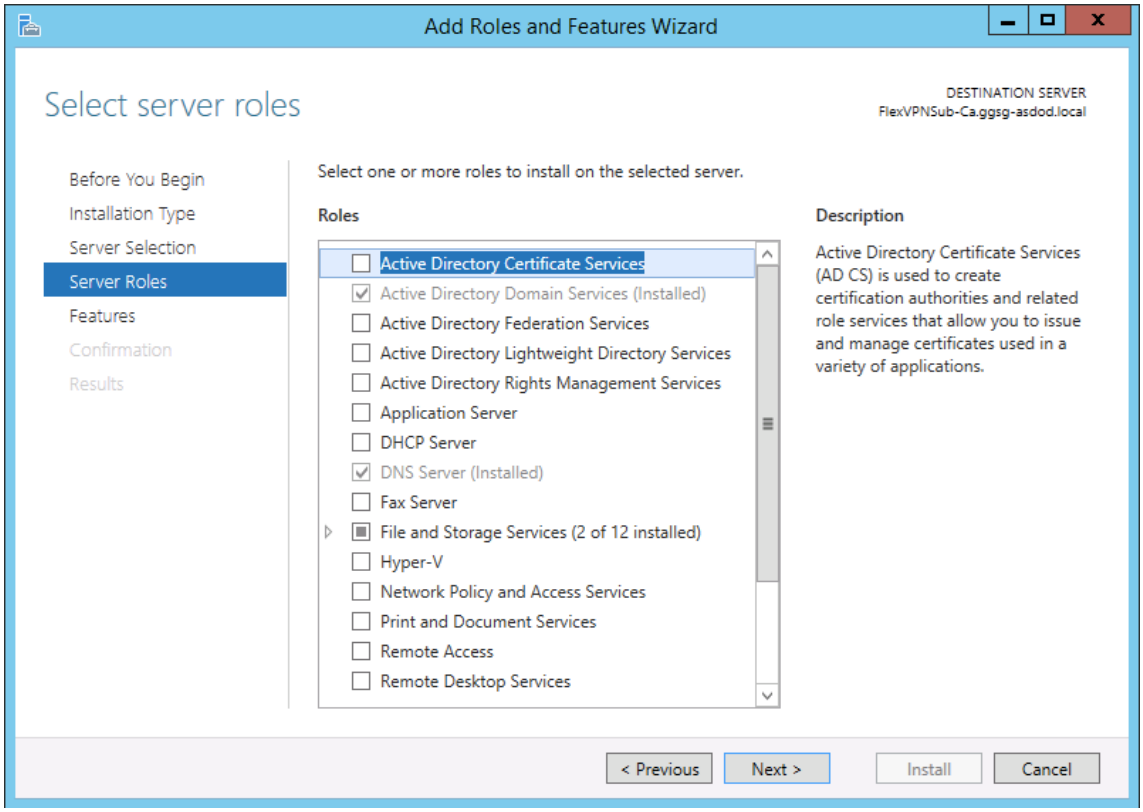
Step 3. Accept the defaults selected on this page and press Next



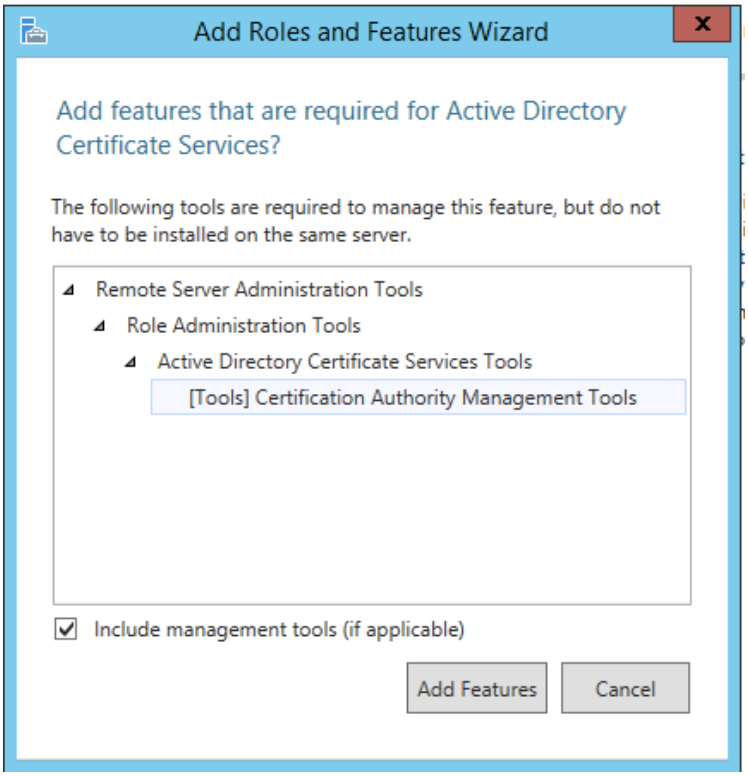
Step 4. Accept the selected Server and press Next



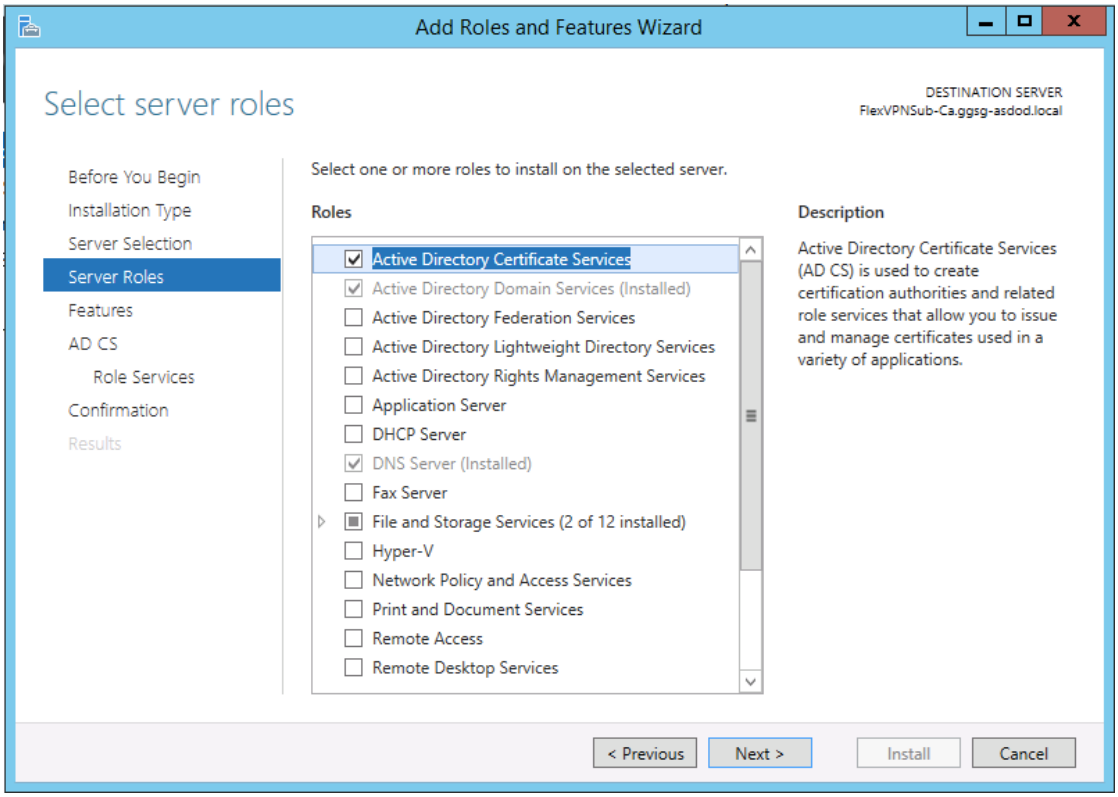
Step 5. Select Active Directory Certificate Services, and a pop-window will appear.



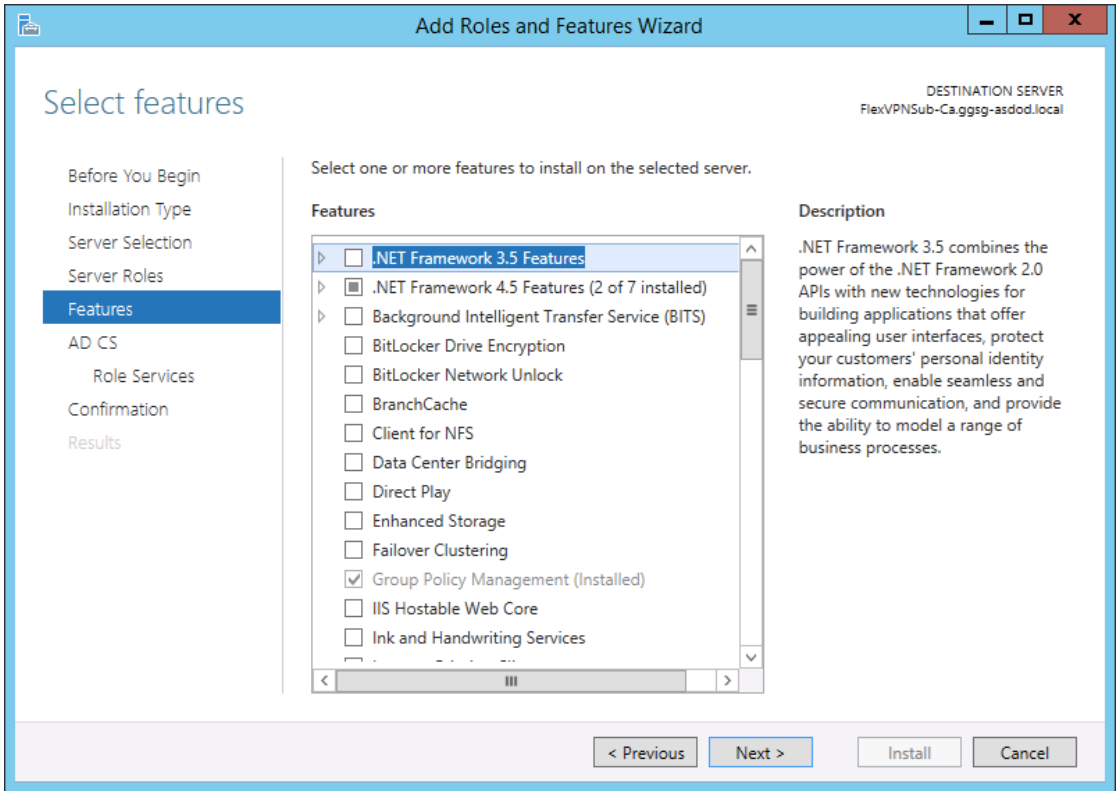
Step 6. Select Add Features



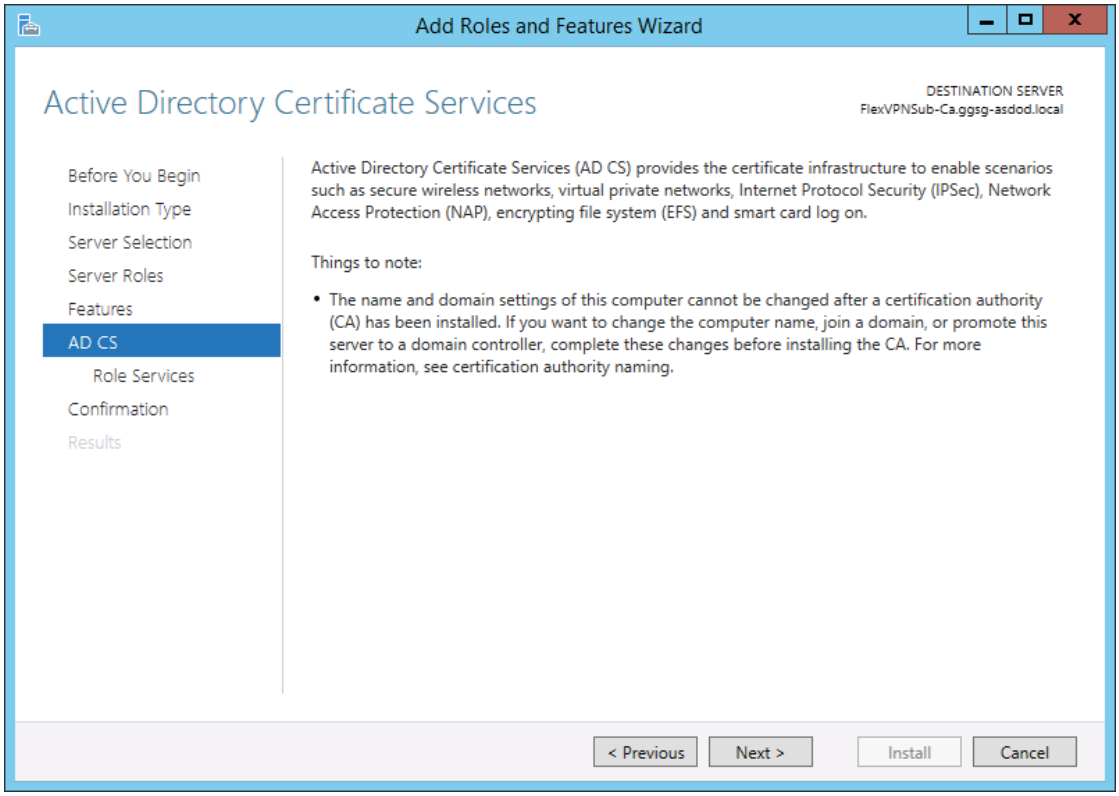
Step 7. Press on Next



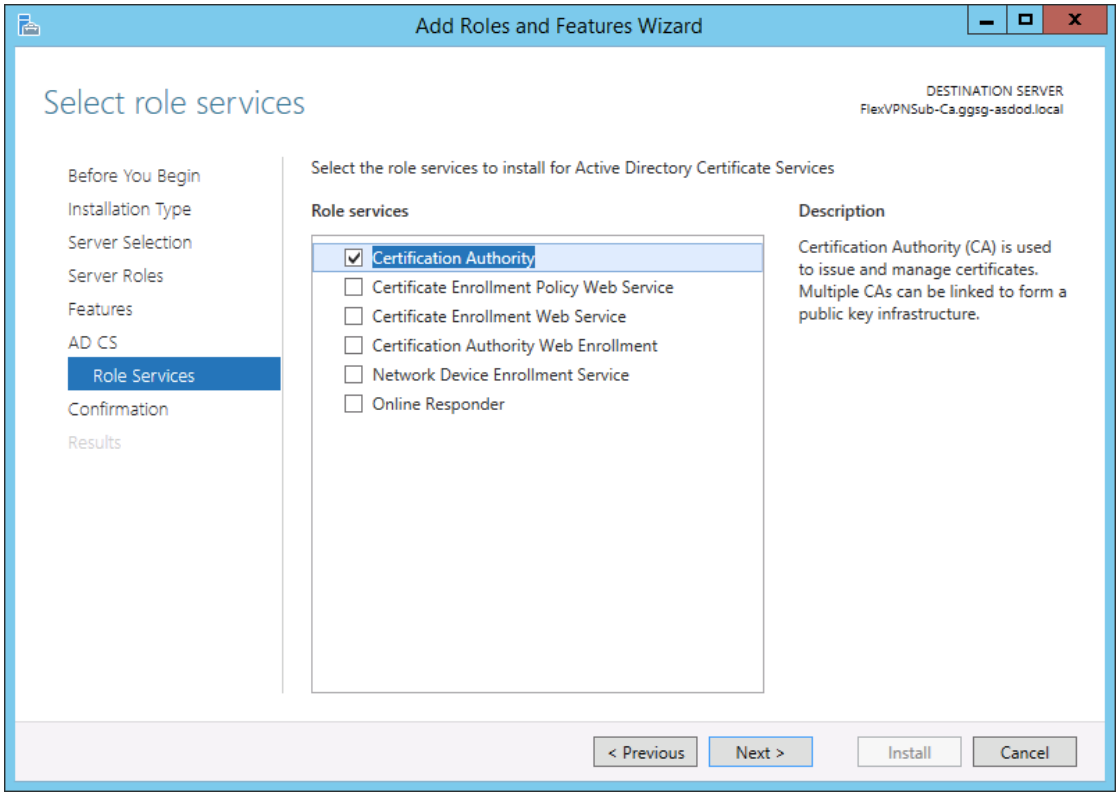
Step 8. Press on Next



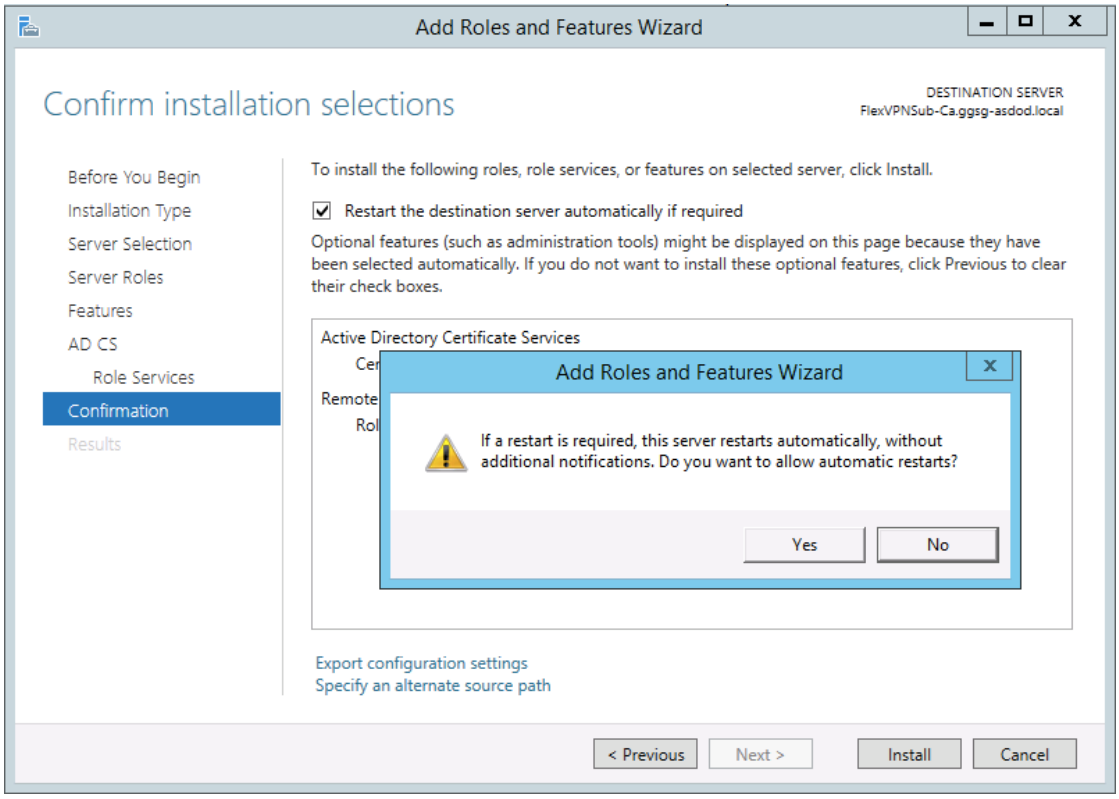
Step 9. Press on Next



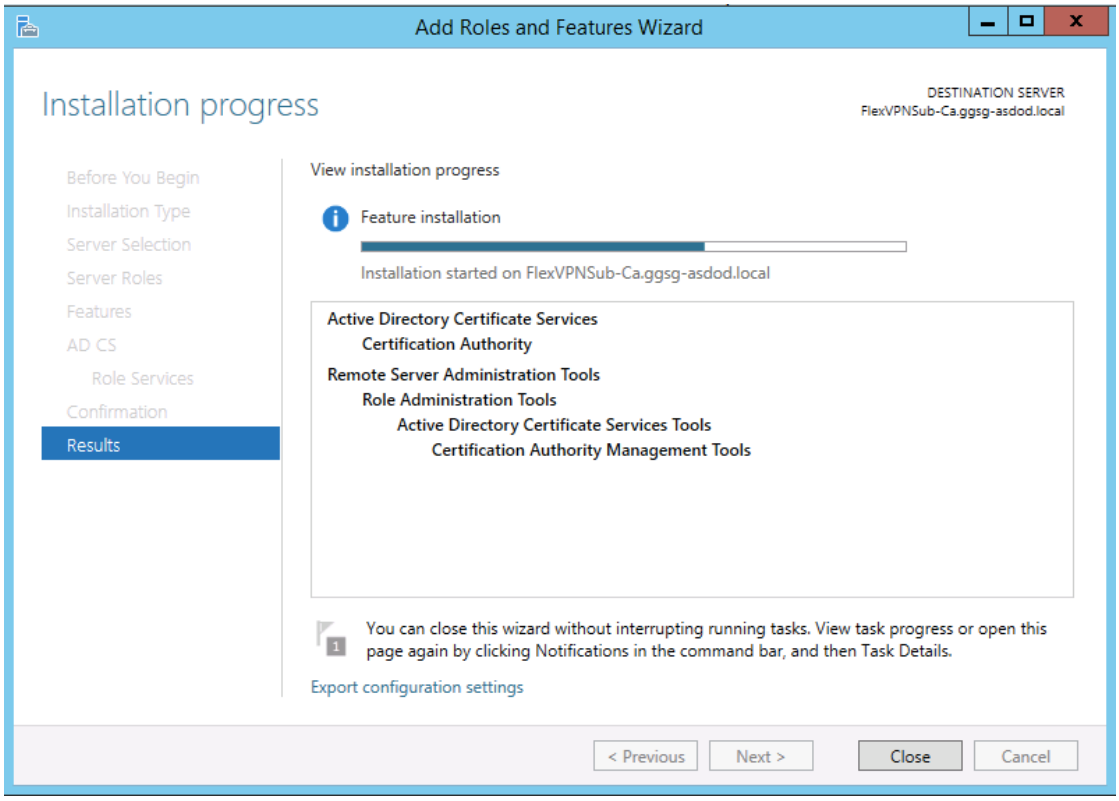
Step 10. Select Certification Authority and press Next



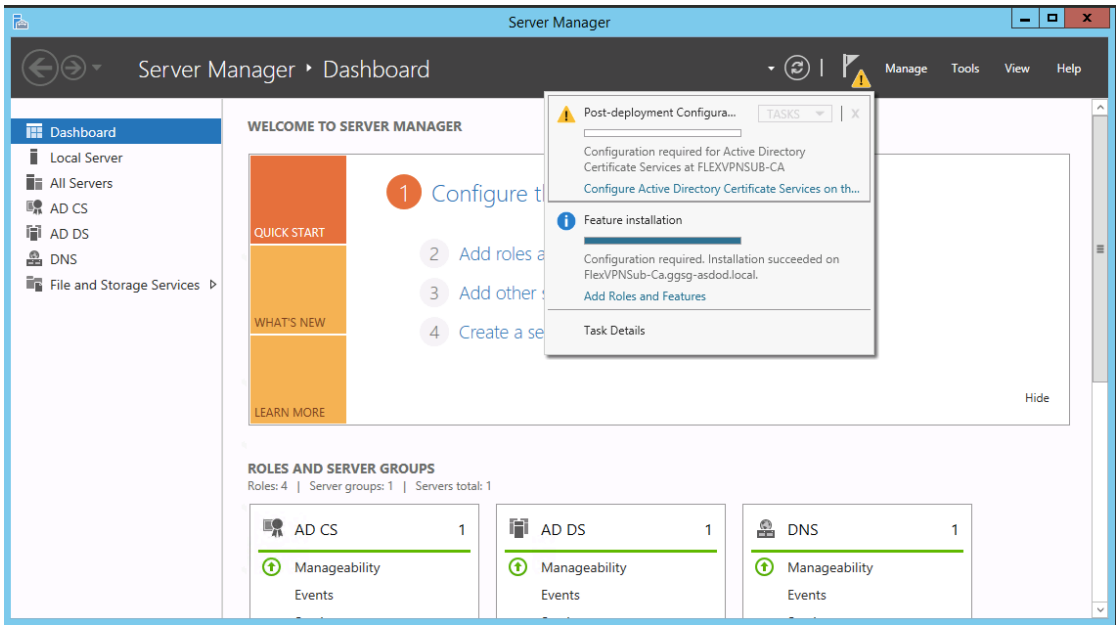
Step 11. Select 'Restart the destination server automatically, if required. Press Yes and then Install



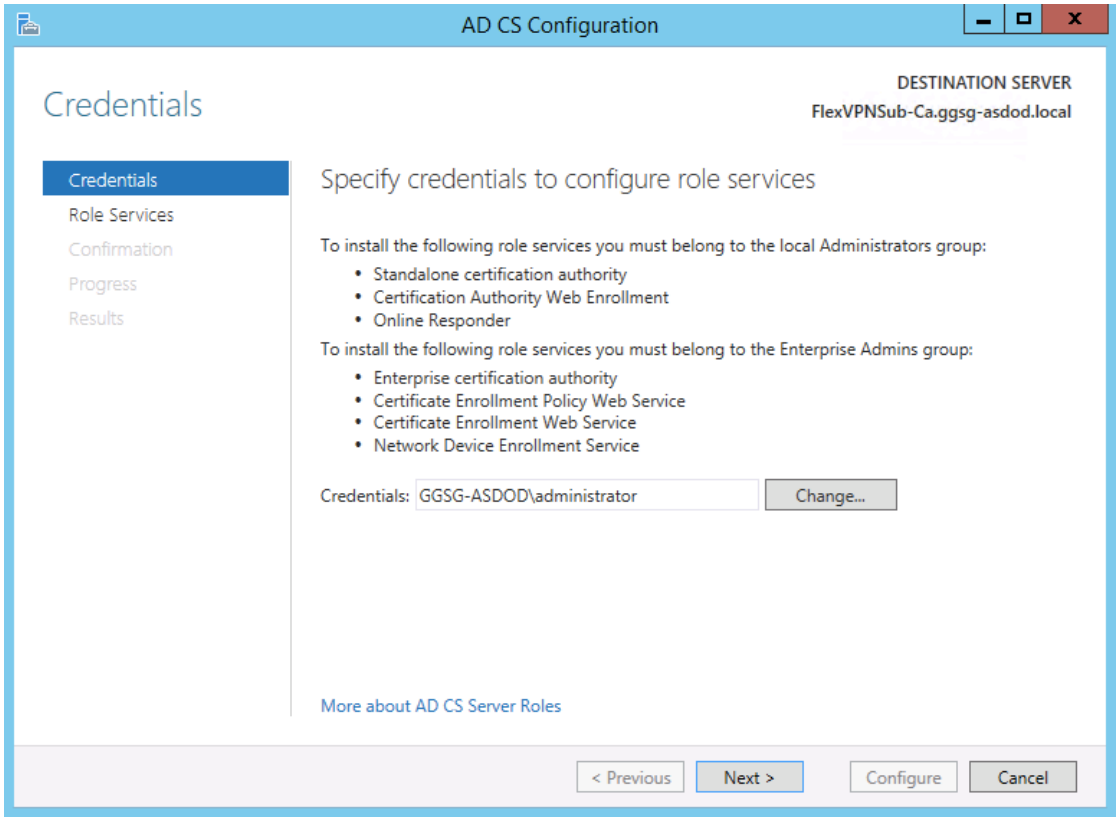
Step 12. The installation process is display after the installation button is pressed



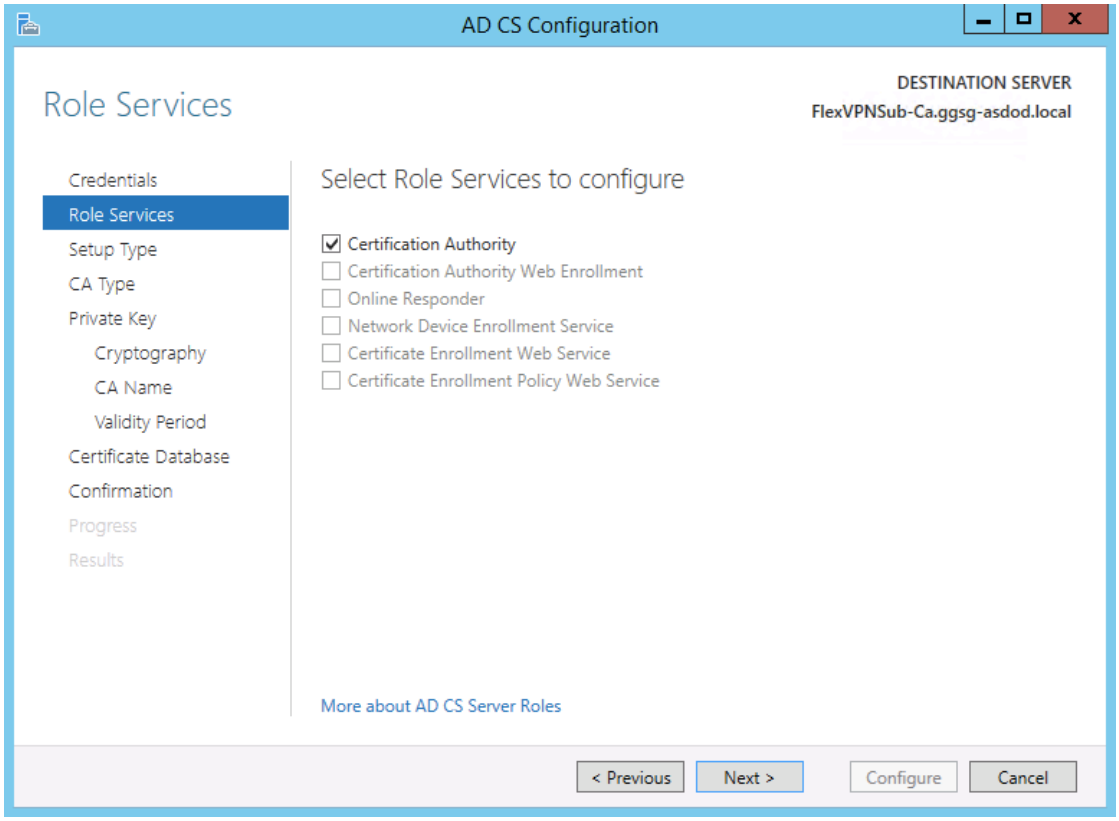
Step 13. Under Server Manager select the yellow triangle. From the dropdown menu, select Configure Active Directory Certificate Services.



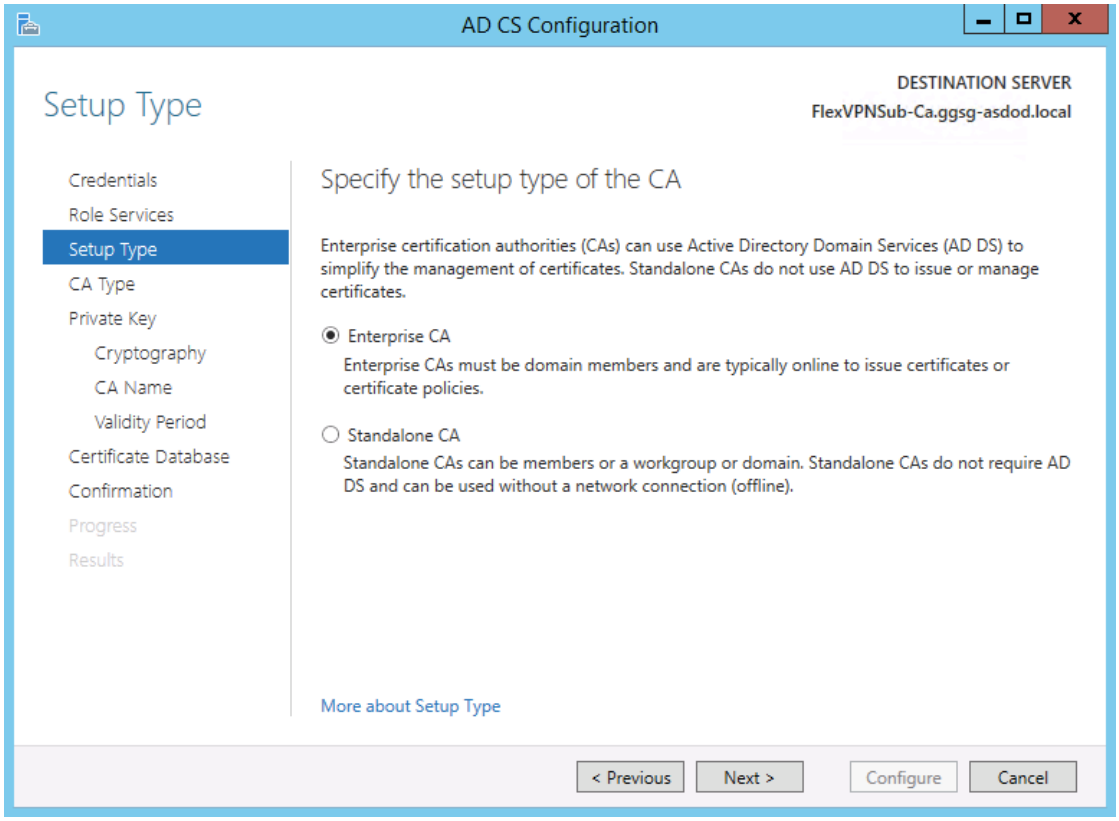
Step 14. Press on Next



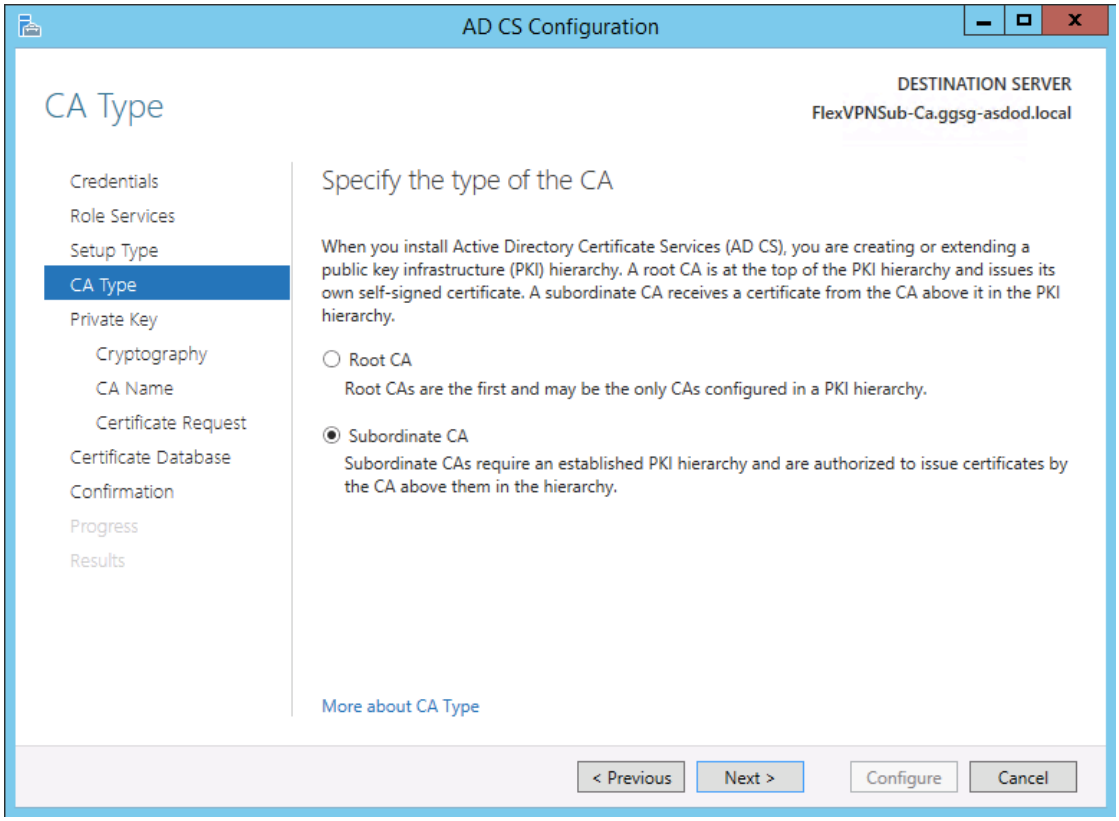
Step 15. Select Certification Authority, and press Next



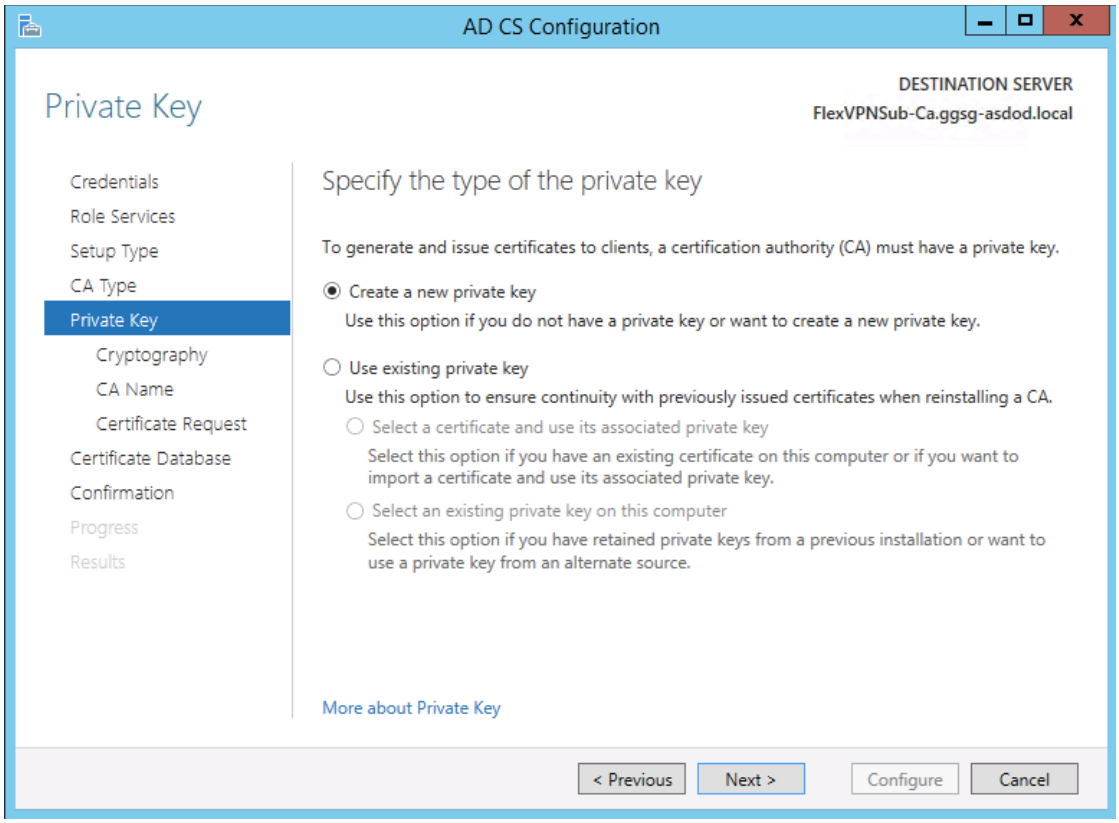
Step 16. At the setup type leave the default "Enterprise CA," and press Next



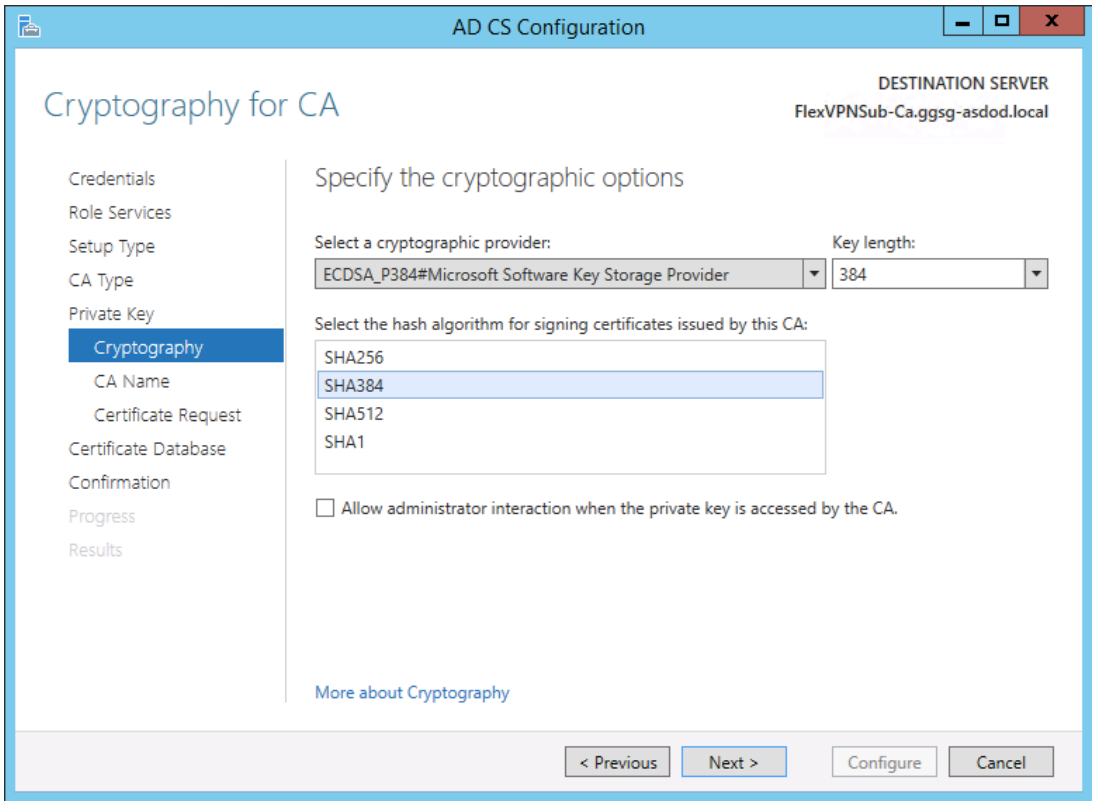
Step 17. From the CA Type, select “Subordinate CA,” and press Next



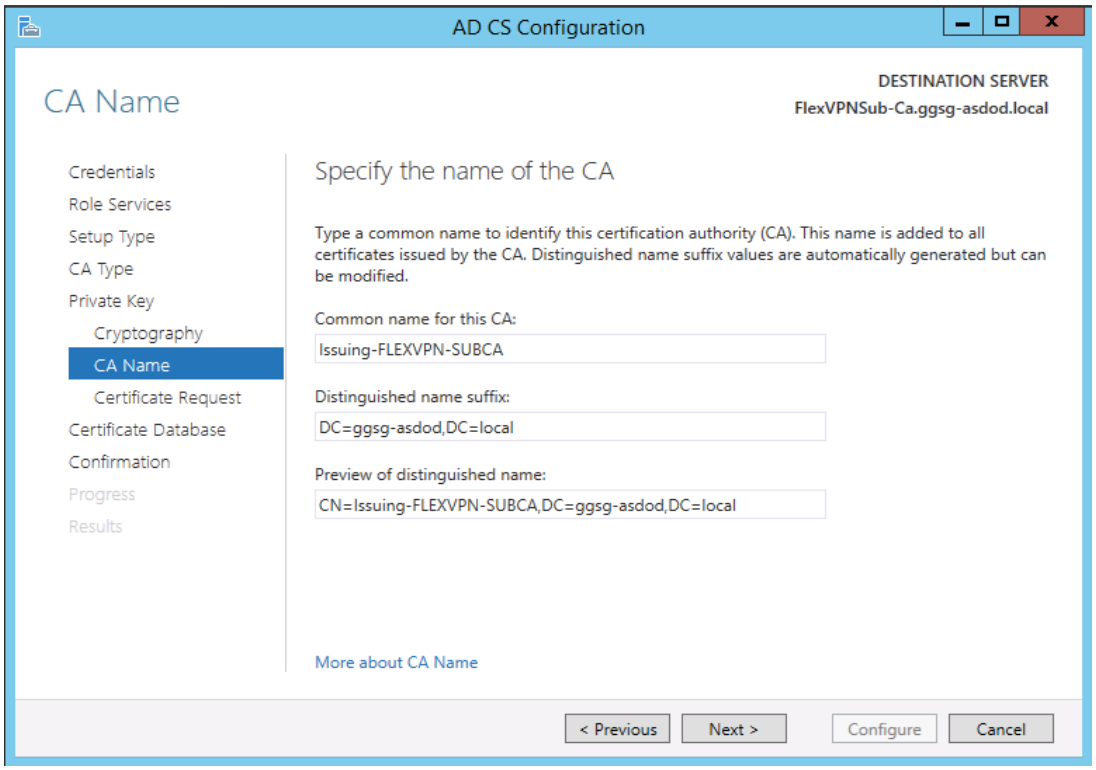
Step 18. Leave the default “Create a new private key” selected, and press Next



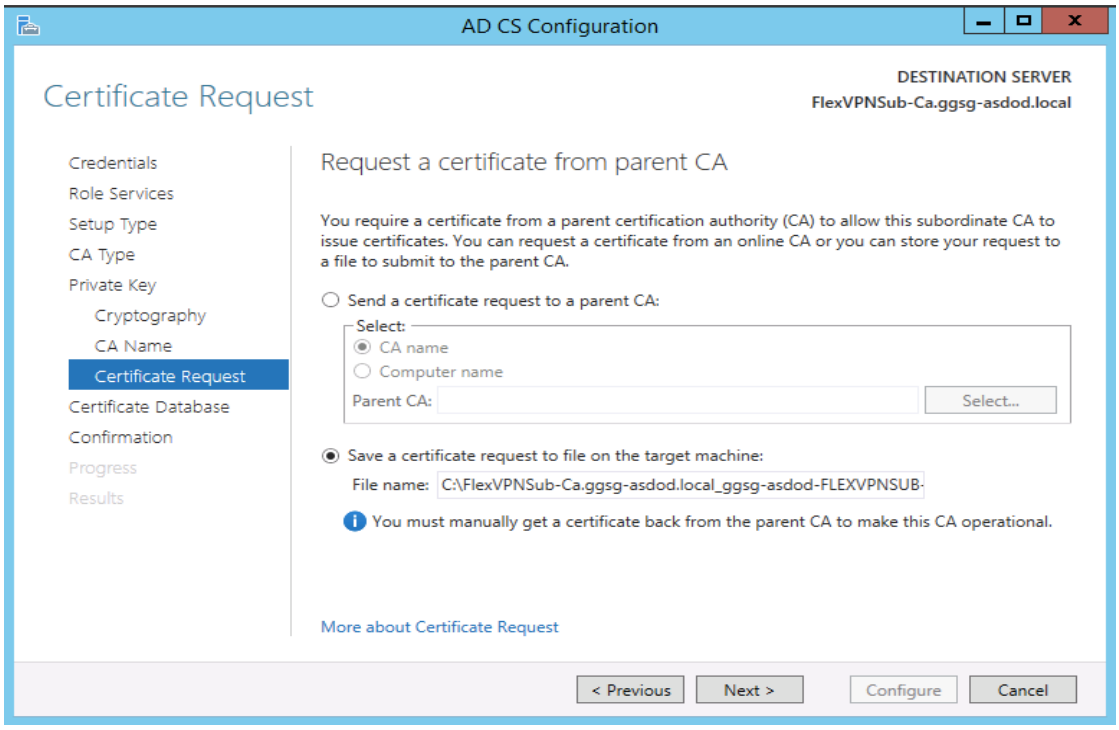
Step 19. In order for the subordinate CA to be Suite-B complaint, a set of algorithms supported by Suite-B must be selected. From the dropdown menu, select “ECDSA_P384#Microsoft Software Key Store Provider,” a key length of 384, and SHA384. Press Next.



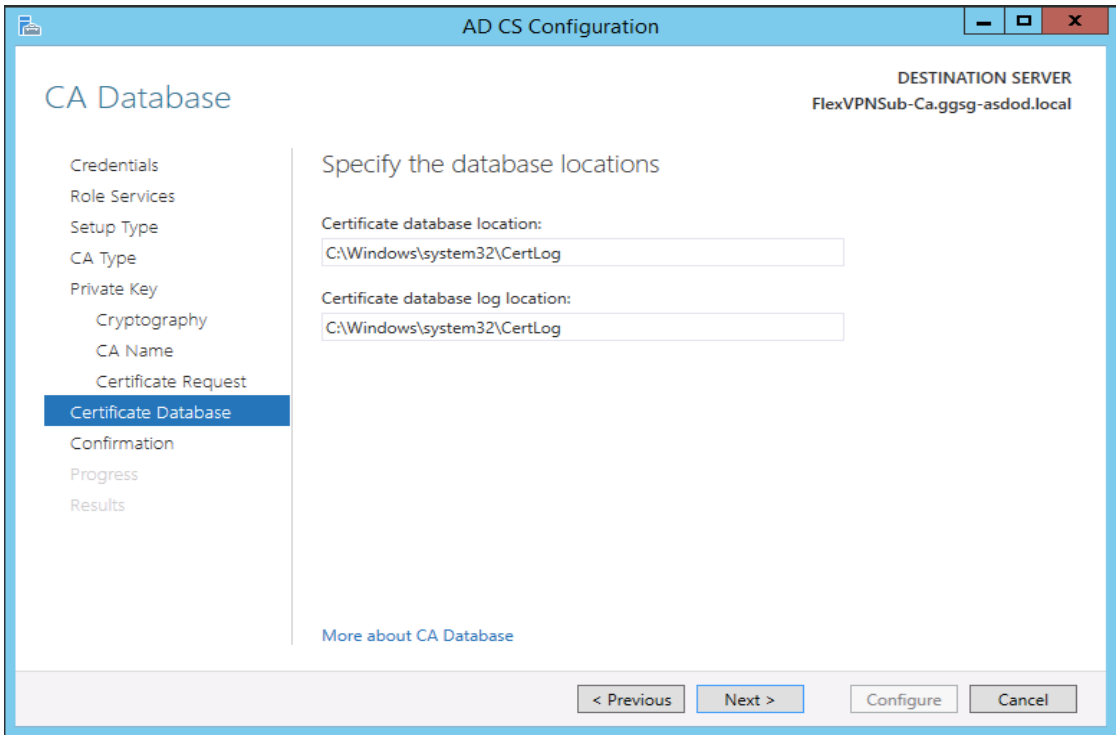
Step 20. For the CA common name type: Issuing-FLEXVPN-SUBCA, and leave the remaining entries at default and press Next



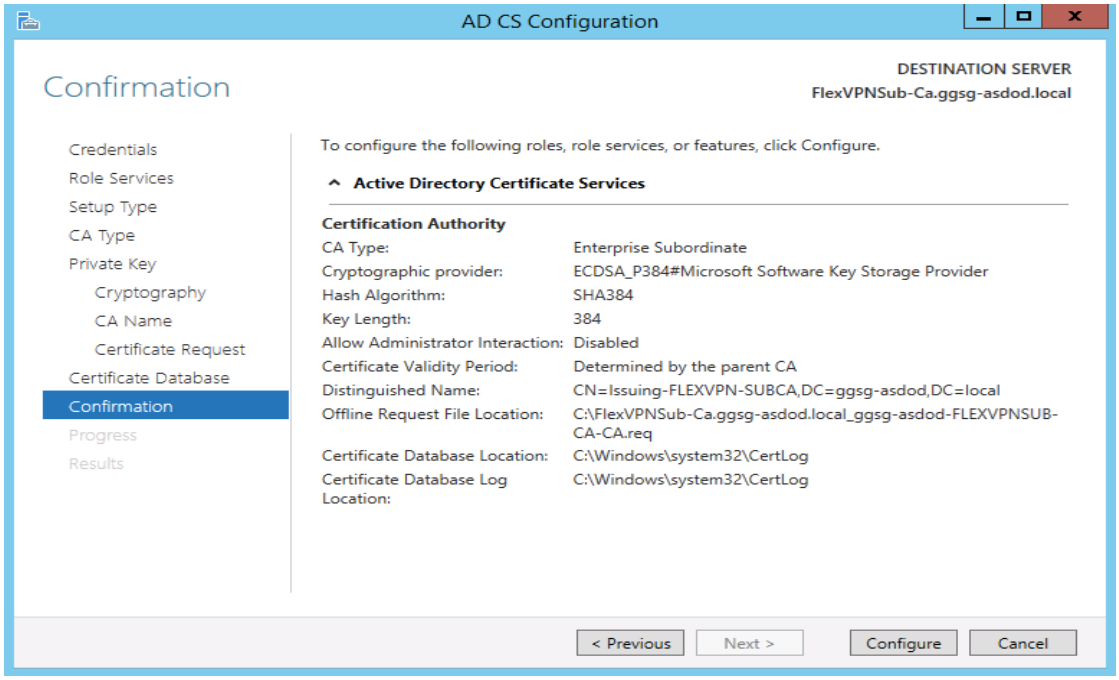
Step 21. Since the CA is supposed to be offline, we will need to send a Certificate Signing Request (CSR) to the CA. Leave the selected defaults and press Next.



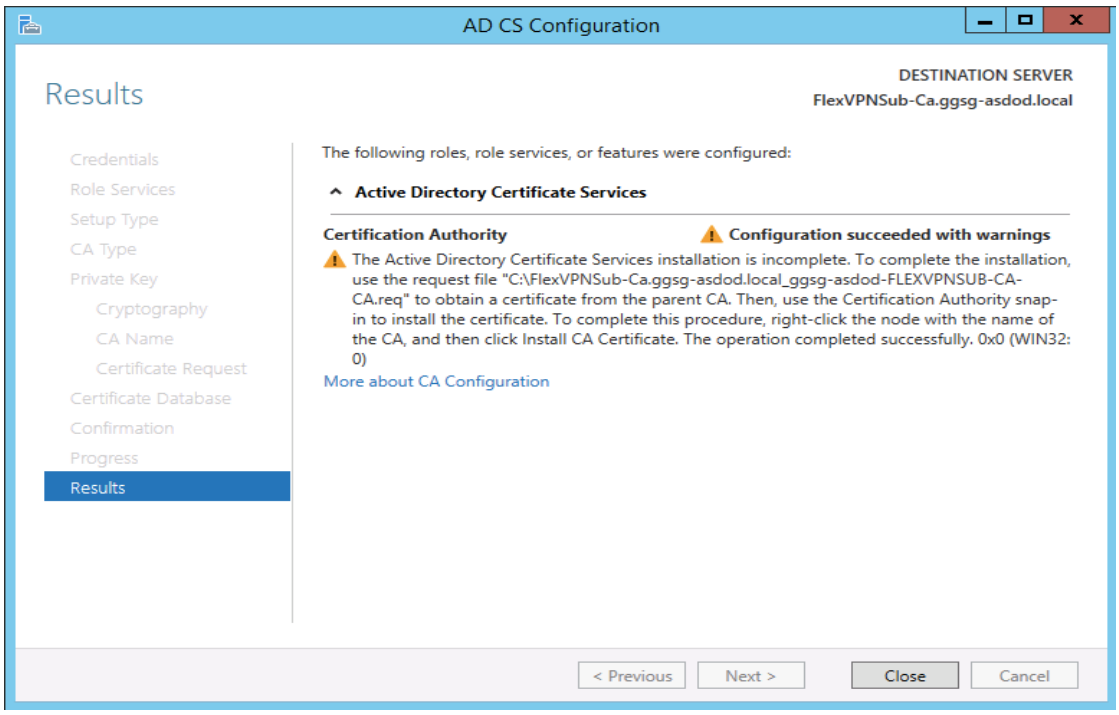
Step 22. Accept the default and press Next



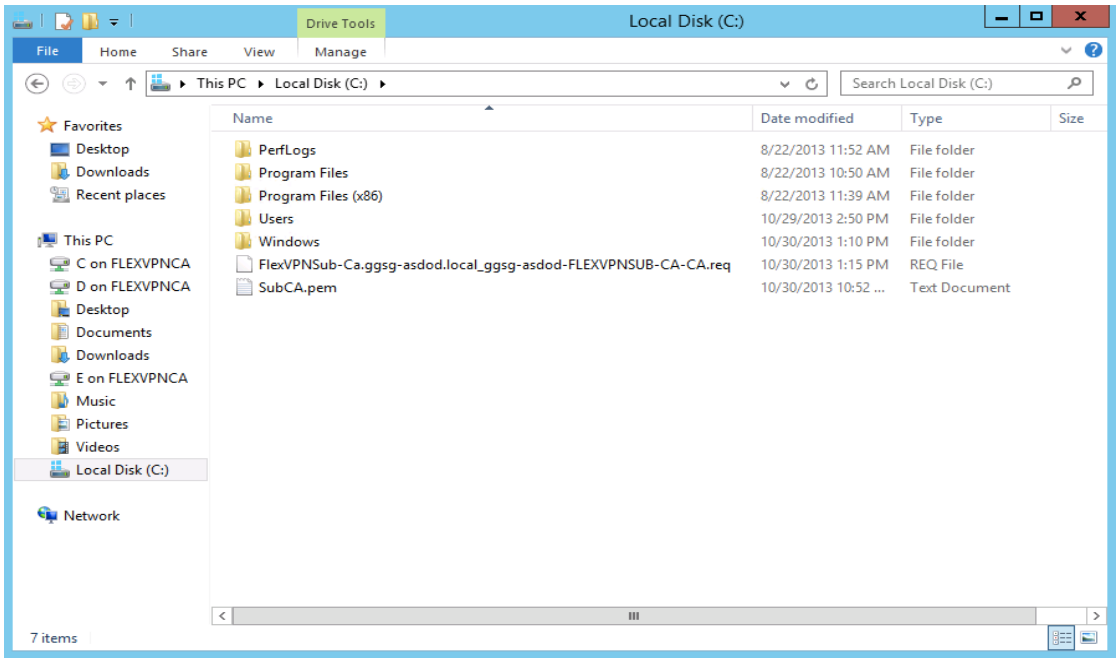
Step 23. Review the parameters entered, and press Configure



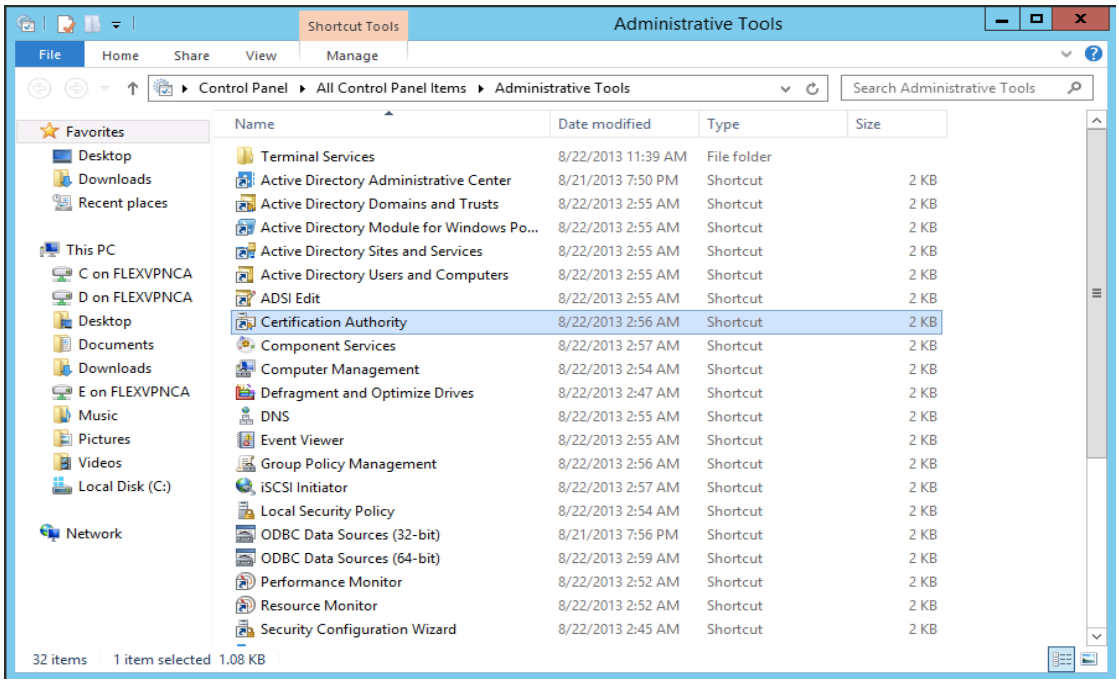
Step 24. There should be no errors on the results page; however, a Warning is display reminding you to obtain a certificate from the parent CA and install it in the local store.



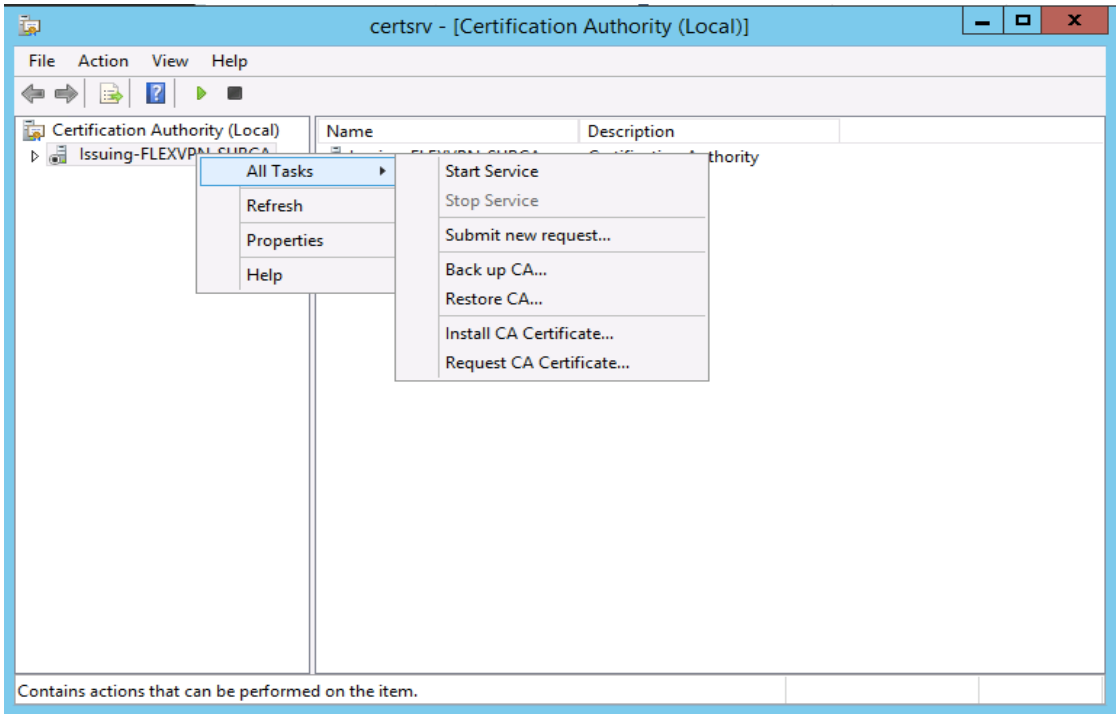
Step 25. Before the SubCA becomes operational, the Certificate Signing Request (CSR) with an extension of .req, will need to be submitted to the CA for registration and issuing of a valid certificate



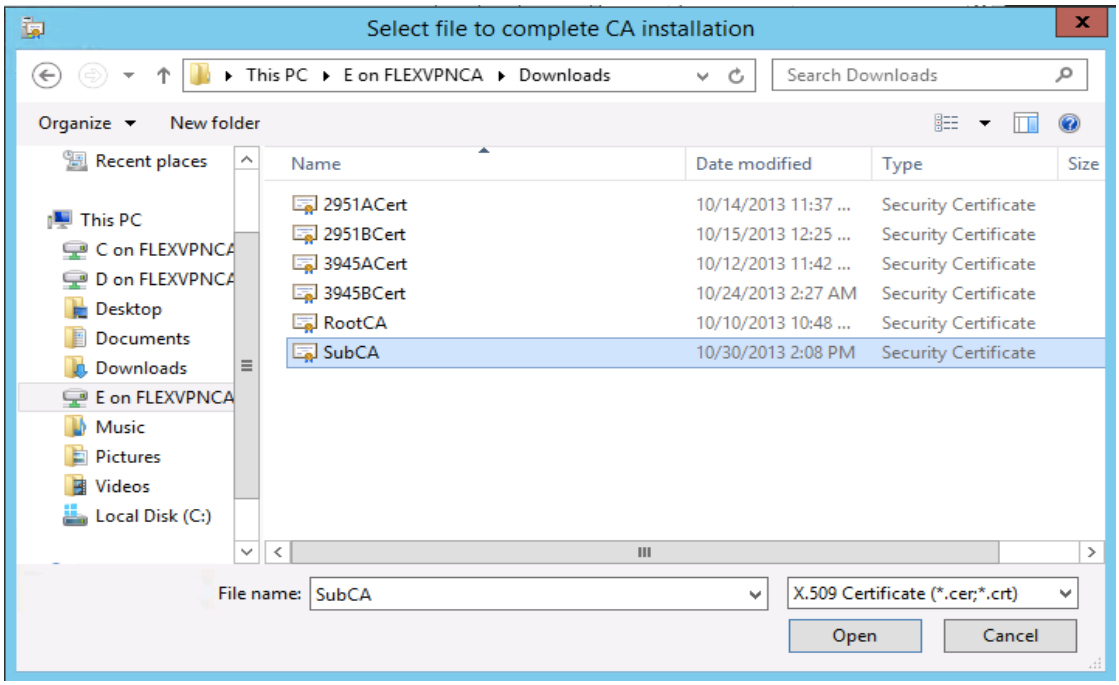
Step 26. After the RootCA administrator process the SubCA and a valid certificate has been issued, open the Administrative Tools and select Certification Authority



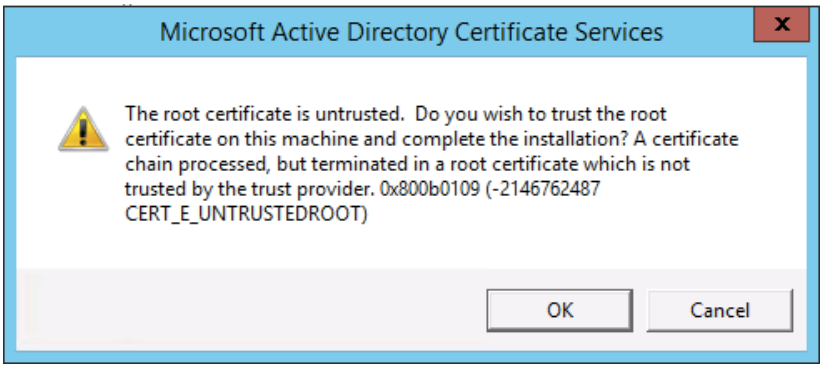
Step 27. Right click on the CA server and select All Tasks -> Install CA Certificate…



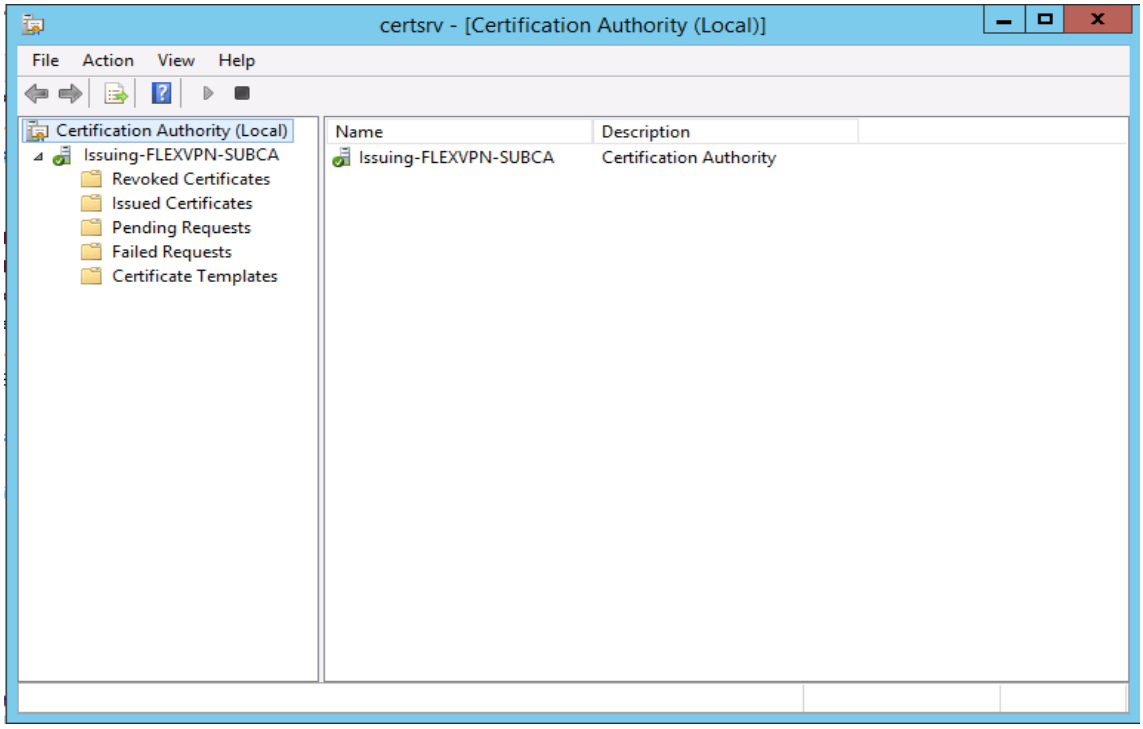
Step 28. Select the SubCA certificate issued by the RootCA, make sure that *cer, *crt is selected, and press Open



Step 29. Select OK to install the root certificate on the local trusted store.



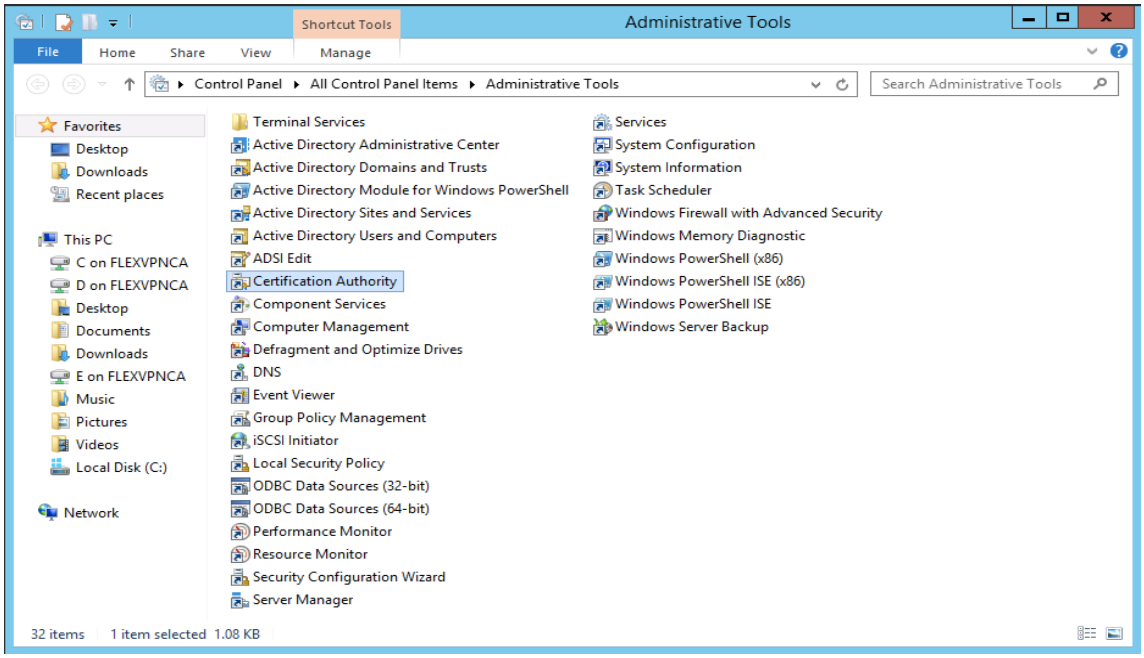
Step 30. Start the CA Server. If the CA certificate was processed and installed correctly, then the server will start without any errors. A green check mark shows beside the server indicating that is functioning.



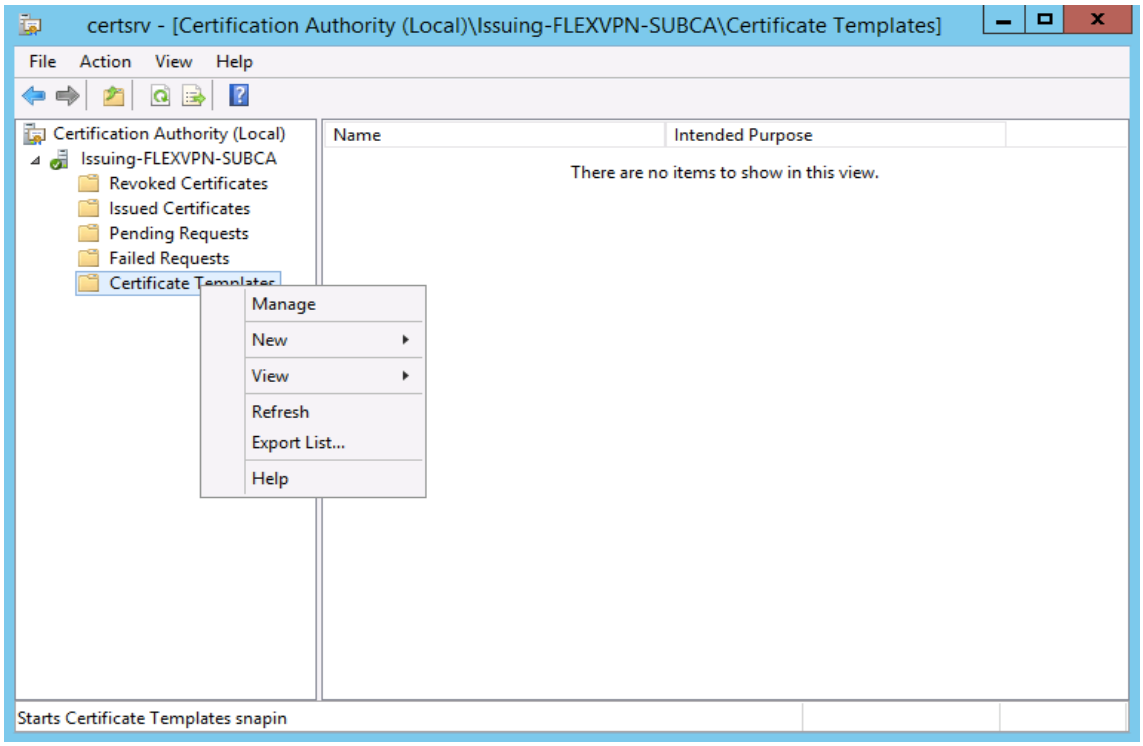
Suite-B Version 3 Template Configuration

After completing the subordinate CA, a Suite-B version 3 template must be configured to issue certificates to the FlexVPN routers.

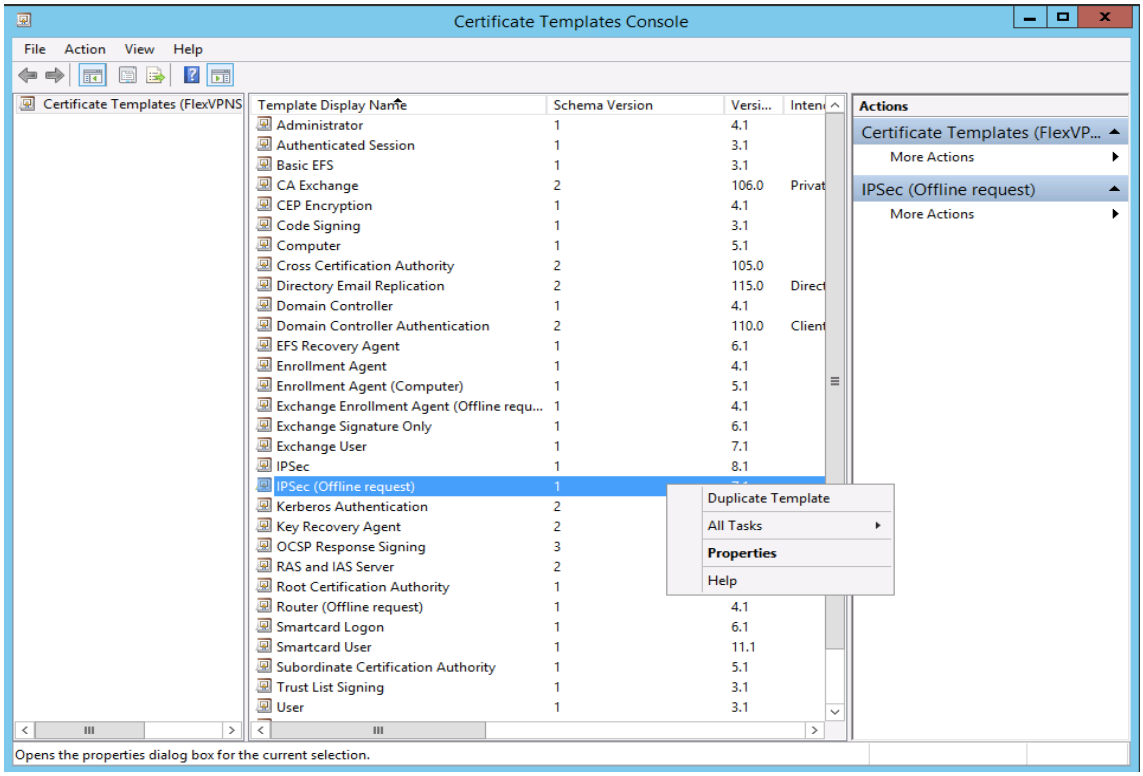
Step 1. Open Administrative Tools and select Certification Authority



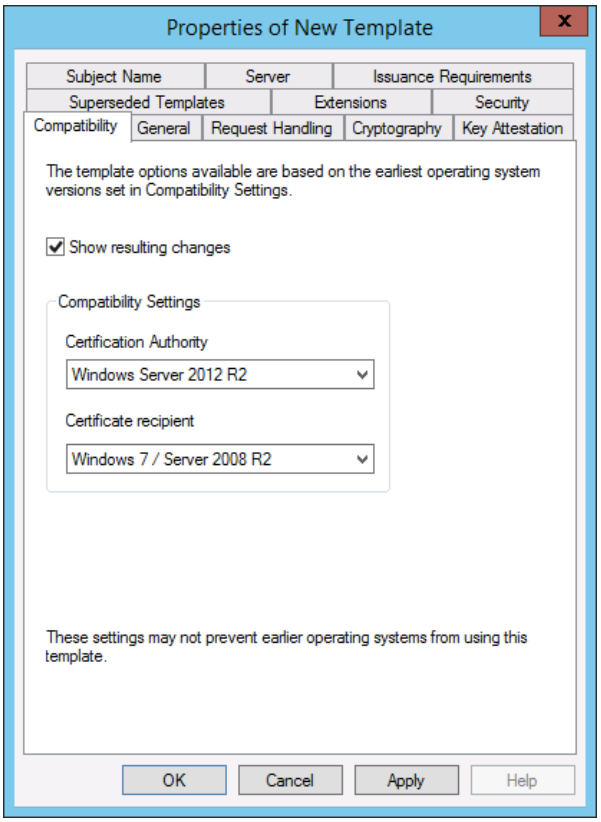
Step 2. Right click Certificate Templates and select Manage.



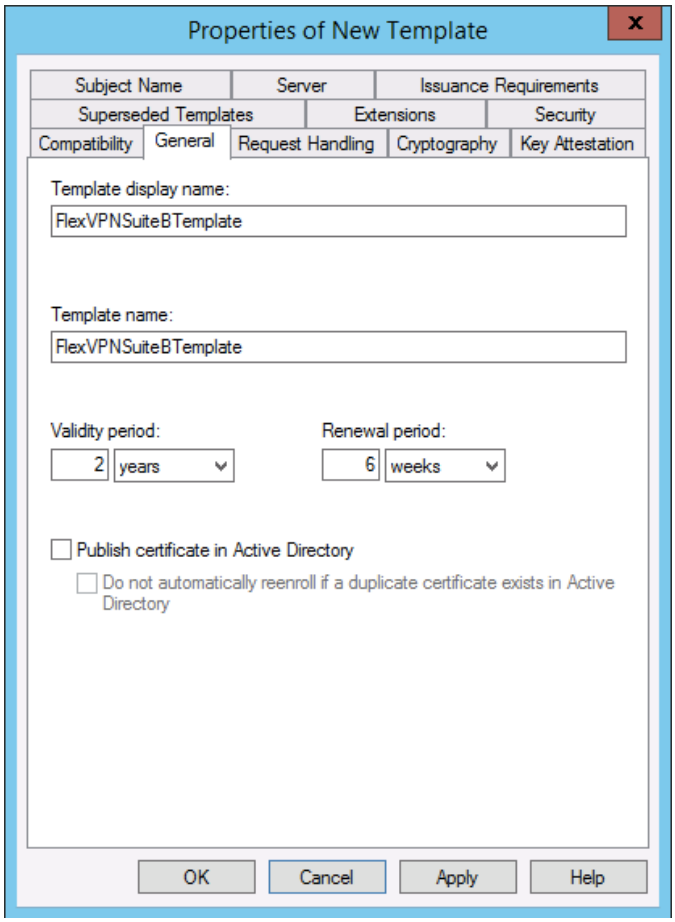
Step 3. Right click on IPSec (Offline request) template and select Duplicate Template.



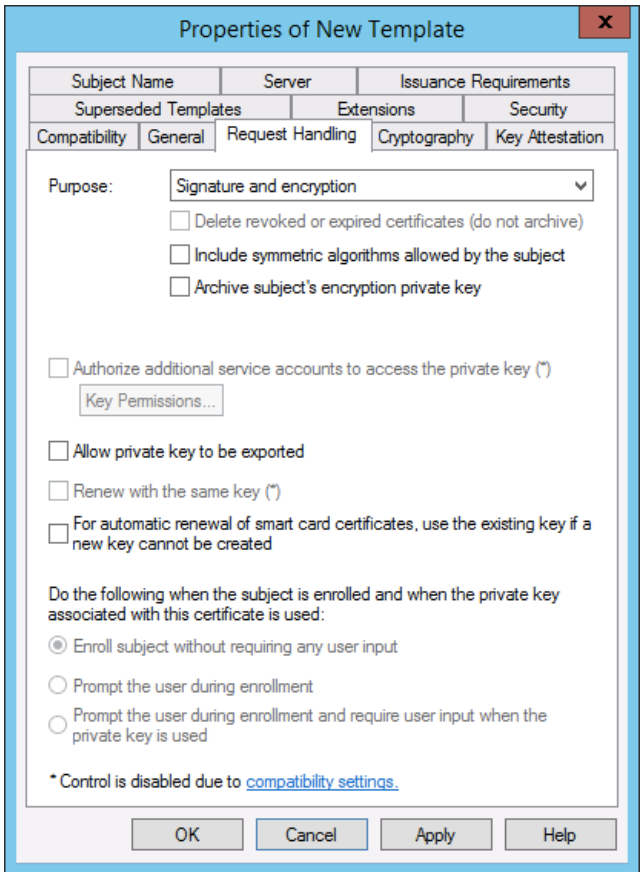
Step 4. A new template appears. Under the Certification Authority dropdown menu, select 'Windows Server 2012 R2.' And under 'Certificate recipient' dropdown menu select Windows 7/Server 2008 R2. Select the General tab.



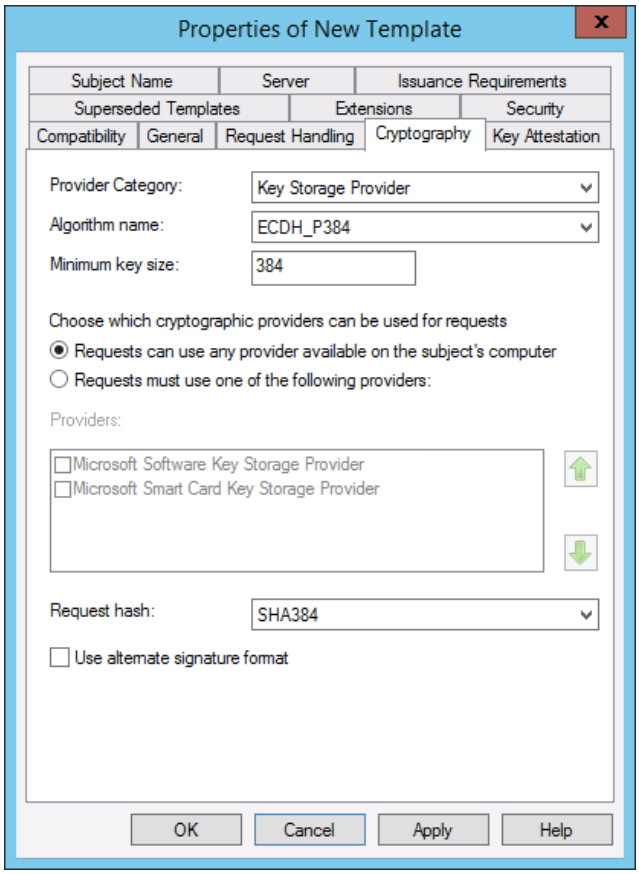
Step 5. Under the General tab 'Template display name' enter 'FlexVPNSuiteBTemplate' with a validity period of 2 years, and a renewal period of 6 weeks. Select 'Request Handling' tab.



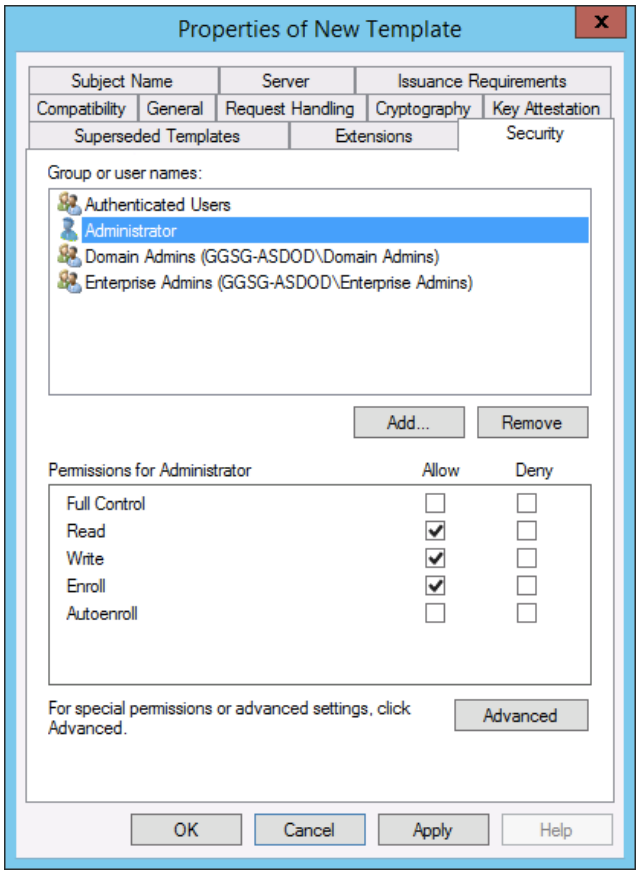
Step 6. Under 'Purpose', make sure that 'Signature and Encryption' is selected. Select 'Cryptography.'



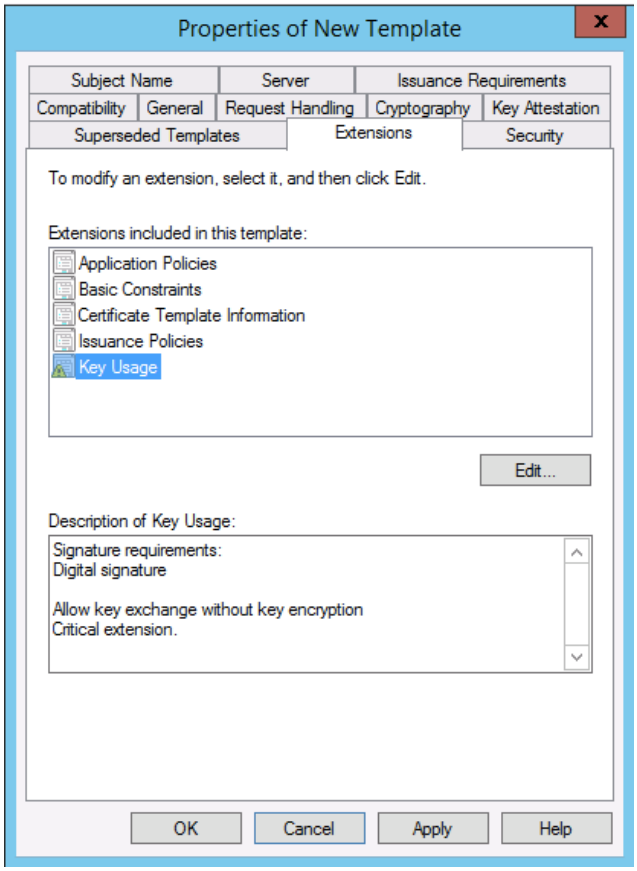
Step 7. Under the 'Cryptography' tab, select the Provider category (Key Storage Provider), Algorithm name (ECDH_P384), Minimum key size (384), and the hash (SHA384). Leave everything else at default. Select the 'Security tab'



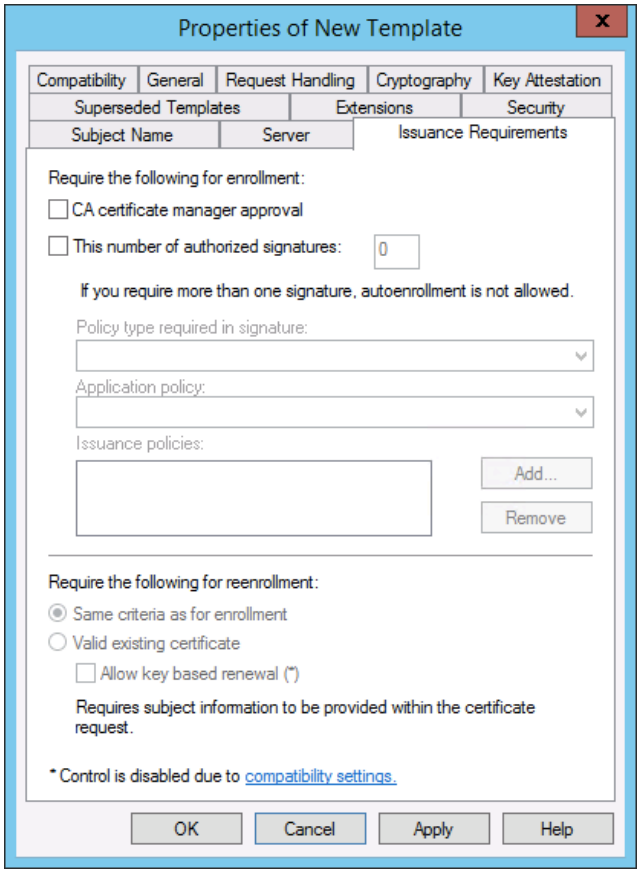
Step 8. The purpose of this template is to be used this for manual enrollment while logged on as an administrator; therefore, ensure the appropriate permissions are selected: Read, Write, and Enroll. Select the 'Extensions' tab



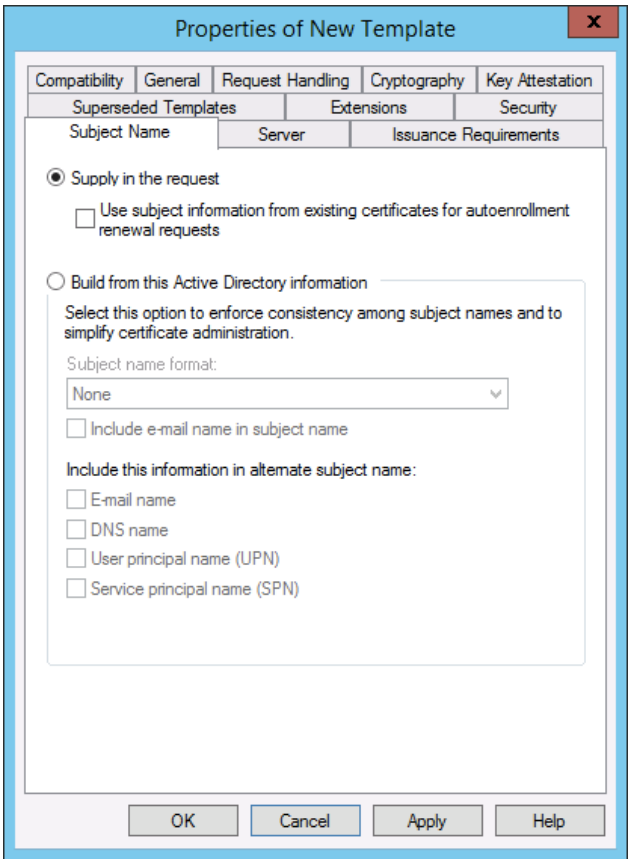
Step 9. Under 'Key Usage,' 'Description of Key Usage box,' make sure 'Digital signature,' 'Allow key exchange without key encryption,' and 'Critical extension' are shown. Select 'Issuance Requirements' tab.



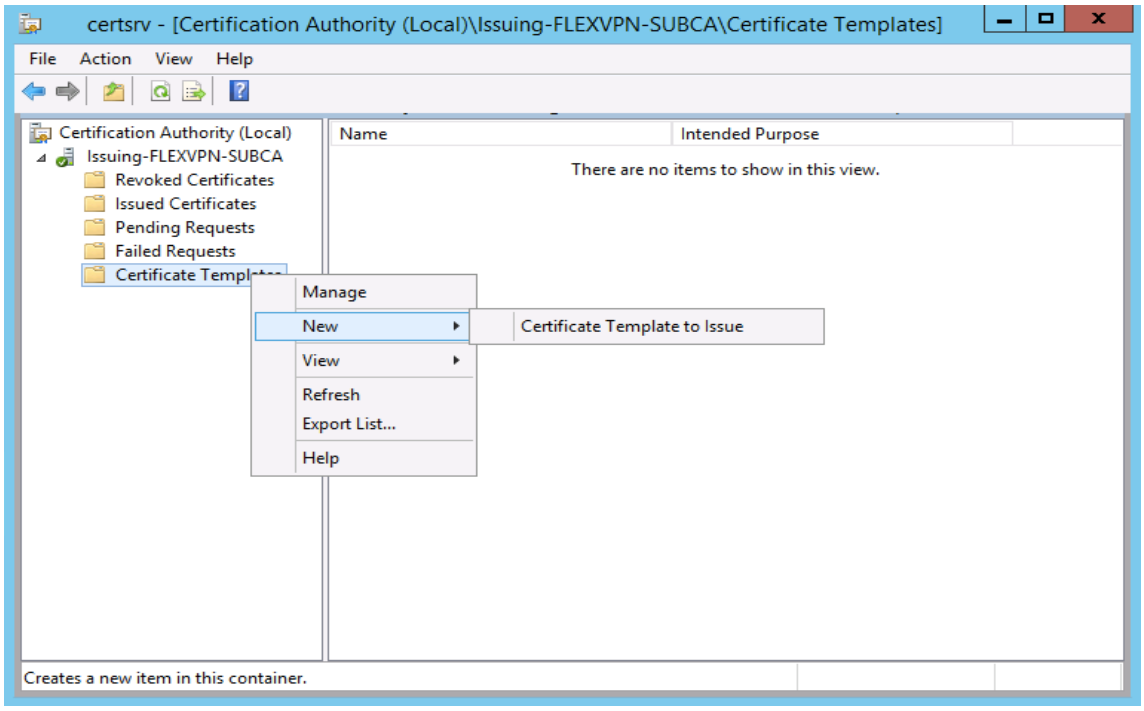
Step 10. Ensure that 'CA certificate manager approval' is not selected. Select 'Subject Name' tab.



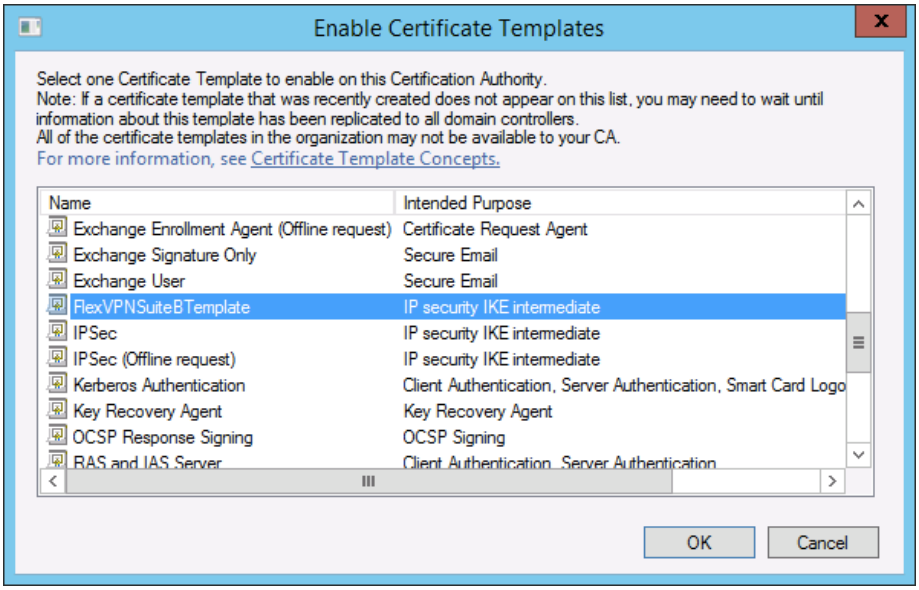
Step 11. The Common Name (CN) from the routers will be used for the CSR. We want this information to be supplied in the request. This is specified under the 'Subject Name' tab. Therefore, we need to make sure that 'Supply in the request' is selected (default). Select OK.



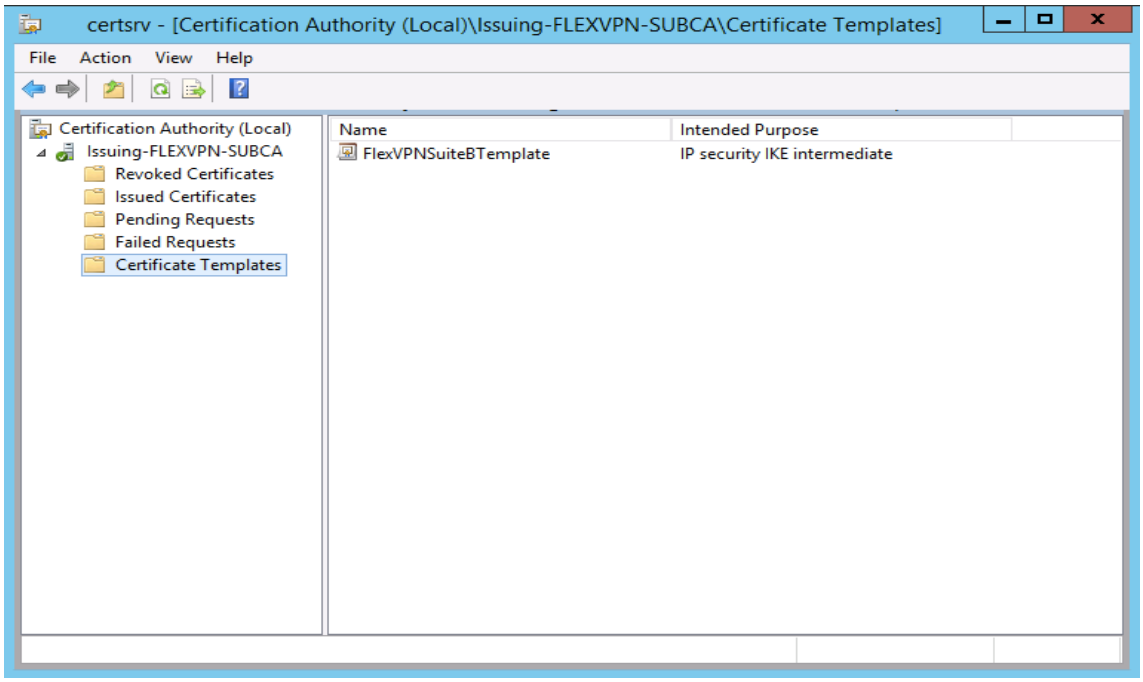
Step 12. After configuring the Suite-B complaint certificate template, right click 'Certificate Template' select new and 'Certificate Template to Issue.'



Step 13. Select the previous created certificate template 'FlexVPNSuiteBTemplate'; press OK



Step 14. The newly configured version 3 Suite-B certificate to be used for FlexVPN now appear under the certificate templates.



FlexVPN Routers Certificate Configuration

Since ECC Suite-B currently does not support auto-enrollment, all the certificates in the CA Chain must be manually imported. Trustpoints are created in the router to import the trusted certificate chain.

In a Public Key Infrastructure (PKI), a trustpoint is essentially where a trusted certificate of authority certificate is store. For the hub and spoke routers, there are two Trustpoints: one for the CA, and the other for the Sub-CA and the router Identity certificate.

The following steps describe what needs to be done in the router to import the CA, Sub-CA and the router identity certificate.

Step 1. Generate a non-exportable ECC key-pair:

```
H1-AA-14-2951-A(config)#cry key generate ec keysize 384
The name for the keys will be: H1-AA-14-2951-A.nge-customera.local
EC key pair created successfully
Check the ECC key pair:
H1-AA-14-2951-A#sh cry key mypub ec
% Key pair was generated at: 08:10:55 EDT Nov 1 2013
Key name: H1-AA-14-2951-A.nge-customera.local
Key type: EC KEYS
Storage Device: private-config
Usage: Signature Key
Key is not exportable.
Key Data:
30763010 06072A86 48CE3D02 0106052B 81040022 03620004 543A4923 D7BB8A47   91D0A8D2
77B46C5B FEF94A43 F2DD259C 74575086 CFFF7435 188C717C 22B64D9B   A79BC3FC 66DB2E2F
```

Note: Make sure the clock in the router is sync with an NTP server before generating the EC keys, and that the correct time zone is being used

Step 2. Create a Certificate of Authority Trustpoint. Notice that the enrolment process is going to use the console for the import of the certificates.

```
H1-AA-14-2951-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
H1-AA-14-2951-A(config)#crypto pki trustpoint CUSTOMERARootCA
H1-AA-14-2951-A(ca-trustpoint)# enrollment terminal
H1-AA-14-2951-A(ca-trustpoint)# revocation-check none
H1-AA-14-2951-A(ca-trustpoint)# hash sha384
```

Step 3. A valid CA certificate must be authenticated and then imported into the previously created Trustpoint. The CA and Sub-CA certificates will be provided by the PKI administrator in a PEM format, and then, copy and pasted into each appropriate Trustpoint, as shown in the following steps.

```
H1-AA-14-2951-A(config)#cry pki authenticate CUSTOMERARootCA
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

-----BEGIN CERTIFICATE-----
MIICTjCCAdSgAwIBAgIQUMos5Lcu7rNNNtSA17K3pzAKBggqhkjOPQQDAzBVMRUw
EwYKCZImiZPyLGQBGRYFbG9jYWwxGjAYBgoJkiaJk/IsZAEZFgpnZ3NnLWFzZG9k
MSAwHgYDVQQDExdnZ3NnLWFzZG9kLUZMRVhWUE5DQS1DQTAeFw0xMzEwMDcxNjMy
MzFaFw0xNTEwMDcxNjQyMzFaMFUxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEaMBgG
-----END CERTIFICATE-----

quit <- Make sure that the keyword ‘quit’ is entered after the “END CERTIFICATE”

Certificate has the following attributes:

Fingerprint MD5: 7D41C925 B14A9614 74B8DF71 A1E7CBA0

Fingerprint SHA1: 61ADB3B1 2AD1B0ED DA8B9DEA 2165B487 AEEDBACA

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

Trustpoint CA certificate accepted.

% Certificate successfully imported

Step 4. Following the installation of the CA certificate, another trustpoint is created where the Sub-CA and the router identity certificate would be imported. In addition, the eckeypair previously generated is tied to this trustpoint and that’s for the IPSec Phase I authentication process.

H1-AA-14-2951-A(config)#crypto pki trustpoint CUSTOMERAFlexSubCa

H1-AA-14-2951-A(ca-trustpoint)#enrollment terminal

H1-AA-14-2951-A(ca-trustpoint)#subject-name CN=H1-AA-14-2951-A.nge-customera.local, OU=Cisco, O=NGE, ST=NC

H1-AA-14-2951-A(ca-trustpoint)#revocation-check none

H1-AA-14-2951-A(ca-trustpoint)# hash sha384

H1-AA-14-2951-A(ca-trustpoint)#eckeypair H1-AA-14-2951-A.nge-customera.local

Step 5. This Trustpoint needs to be authenticated and the Sub-CA certificate copy and pasted into this Trustpoint.

H1-AA-14-2951-A(config)#cry pki authenticate CUSTOMERAFlexSubCa

Enter the base 64 encoded CA certificate.

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

-----BEGIN CERTIFICATE-----
MIIEJjCCA62gAwIBAgITdgAAAAd0KnxfH/EUoAAAAAAABzAKBggqhkjOPQQDAzBV
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGjAYBgoJkiaJk/IsZAEZFgpnZ3NnLWFz
ZG9kMSAwHgYDVQQDExdnZ3NnLWFzZG9kLUZMRVhWUE5DQS1DQTAeFw0xMzEwMzAx
NzU3NDRaFw0xNDEwMzAxODA3NDRaMFMxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEa
MBgGCgmSJomT8ixkARkWCmdnc2ctYXNkb2QxHjAcBgNVBAMTFUlzc3VpbmctRkxF
WFZQTi1TVUJDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABECbbKrzsC72wCffK4fv
izLgcRBgy4AarztzlZck0Ddr/WMlpawvkPKzFB7PyahnV3dZw6mjgyU4AlCo0HpD
4NNHQhPsKF56fRo/TKIqCgBndwHPn141+PTTj/lFa4KqIKOCAj8wggI7MBAGCSsG
AQQBgjcVAQQDAgEAMB0GA1UdDgQWBBSgpJUm65x0cY36ZsknOYrQkix8YjAZBgkr
BgEEAYI3FAIEDB4KAFMAdQBiAEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUw
AwEB/zAfBgNVHSMEGDAWgBQ4wfAgUztZF1kNlSp07skq3ouQejCB3AYDVR0fBIHU
Z3VyYXRpb24sREM9Z2dzZy1hc2RvZCxEQz1sb2NhbD9jQUNlcnRpZmljYXRlP2Jh
c2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTAKBggqhkjOPQQD
AwNnADBkAjAe4MpIyAQLF/wDXINgymwmoJOMnPMbNvk8oPN/SKwiblXyx24gA3v1
yzk/cc2qGkICMCO8RgK25GPbZ96h5/BFEunwUh3y/BLFtrxNZKBYiMhlgmF6JisB S9ZHQciTlPF7kQ==
-----END CERTIFICATE-----

quit

```
Certificate has the following attributes:
        Fingerprint MD5: 6D7FFFDA FED81748 C55E4DB5 ECBF115B
        Fingerprint SHA1: 17350521 19DE1E80 E8F145F6 5AB69B0D ACFE60A7
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
% Certificate successfully imported
H1-AA-14-2951-A(config)#
```

Step 6. Check the certificates to make sure that the CA and Sub-CA certificates shows in the router certificate store.

```
H1-AA-14-2951-A#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 7600000007742A7C5F1FF114A0000000000007
  Certificate Usage: Signature
  Issuer:
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Subject:
    cn=Issuing-FLEXVPN-SUBCA
    dc=nge-customera
    dc=local
  CRL Distribution Points:
    ldap:///CN=nge-customera-FLEXVPNCA-
CA,CN=FlexVPNCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nge-
customera,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Validity Date:
    start date: 13:57:44 EDT Oct 30 2013
    end   date: 14:07:44 EDT Oct 30 2014
  Associated Trustpoints: CUSTOMERAFlexSubCa
  Storage: nvram:nge-customera-F#7CA.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 50CA2CE4B72EEEB34D36D480D7B2B7A7
  Certificate Usage: Signature
  Issuer:
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Subject:
```

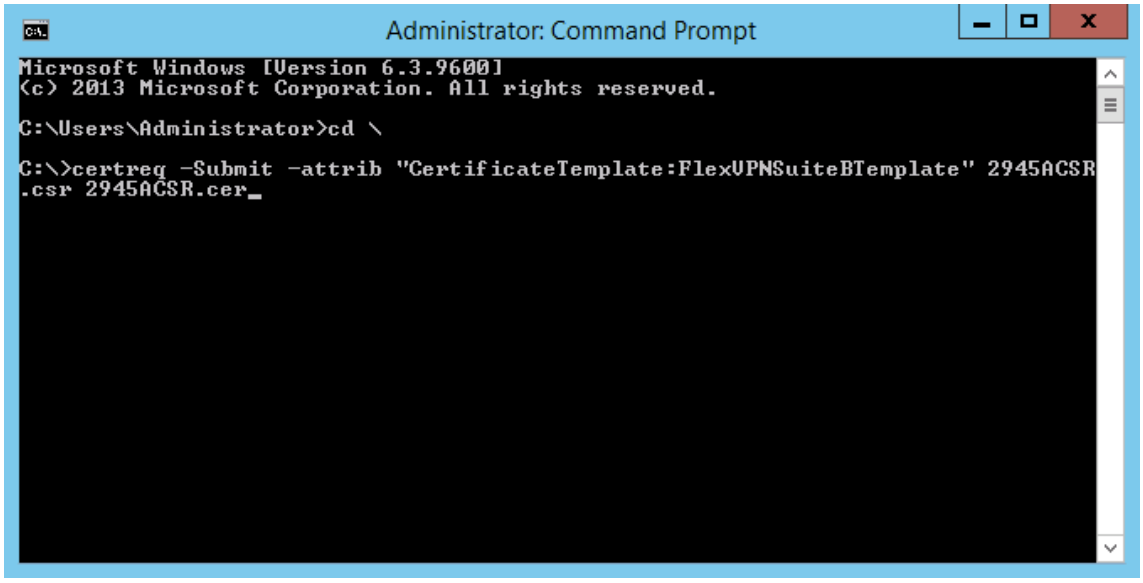
```
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Validity Date:
    start date: 12:32:31 EDT Oct 7 2013
    end   date: 12:42:31 EDT Oct 7 2015
  Associated Trustpoints: CUSTOMERARootCA
  Storage: nvram:nge-customera-F#B7A7CA.cer
```

Step 7. The final step for the certificate process is to generate a router Certificate Signing Request (CSR), which is processed by the PKI administrator to issue a certificate. That certificate is then imported into the Sub-CA Trustpoint.

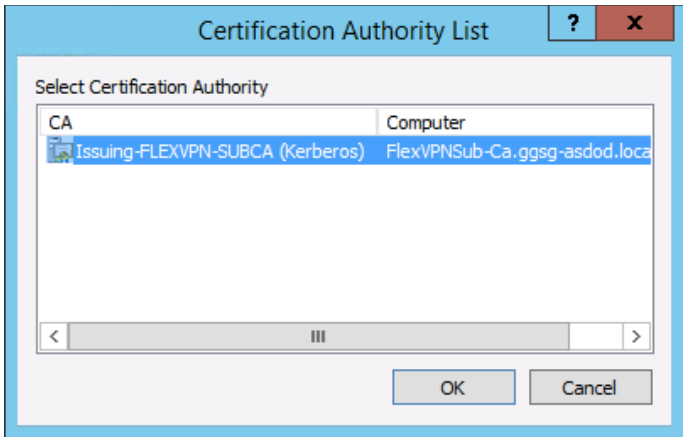
```
H1-AA-14-2951-A(config)#cry pki enroll CUSTOMERAFlexSubCa
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=H1-AA-14-2951-A.nge-customera.local, OU=Cisco, O=NGE, ST=NC
% The subject name in the certificate will include: H1-AA-14-2951-A.nge-customera.local
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
MIIBozCCASkCAQAwgYgxCzAJBgNVBAgTAk5DMQ0wCwYDVQQKEwRHR1NHMQ4wDAYDVQQLEw
VDaXNjbzEpMCcGA1UEAxMgSDEtQUEtMTQtMjk1MS1BLmdnc2ctYXNkb2QubG9jYWwxLzAtBgkqhkiG
9w0BCQIWIEgxLUFBLTE0LTI5NTEtQS5nZ3NnLWFzZG9kLmxvY2FsMHYwEAYHKoZIzj0CAQYFK4EE
ACIDYgAEVDpJI9e7ikeR0KjSd7RsW/75SkPy3SWcdFdQhs//dDUYjHF8IrZNm6ebw/xm2y4vfy/VSfN+WE
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:no
```

Step 8. Copy and paste the CSR into an ASCI text file, save it with a *.csr extension and submit the CSR to the PKI administrator for process. The PKI administrator will execute the following command to issue a certificate for the router.

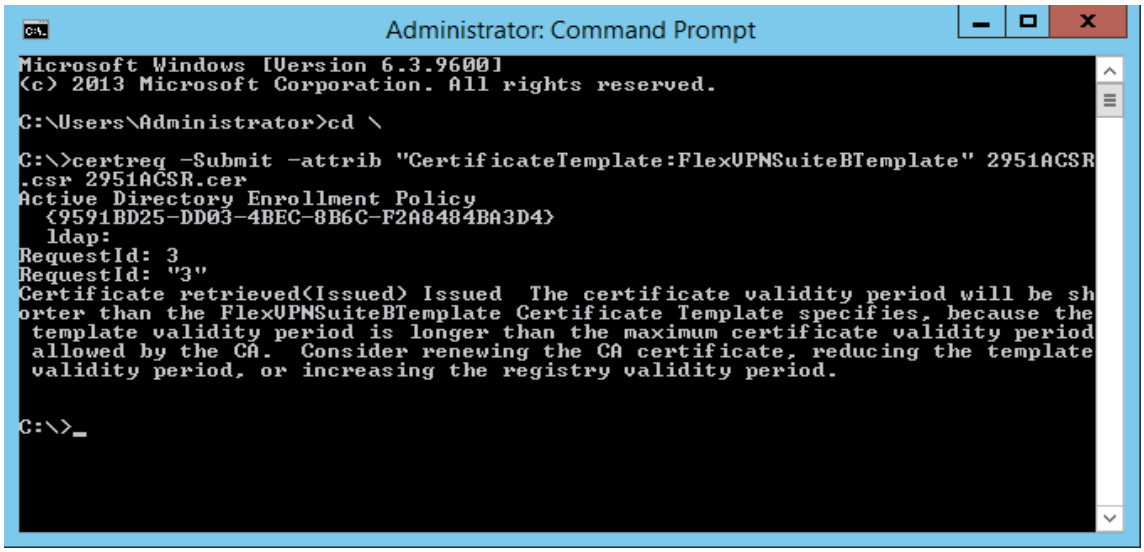
```
certreq -Submit -attrib "CertificateTemplate:FlexVPNSuiteBTemplate" 2945ACSR.csr 2945ACSR.cer
```



Step 9. After the command is executed, the following pop-up window appears. Press OK and notice below the certificate issued by the Sub-CA.

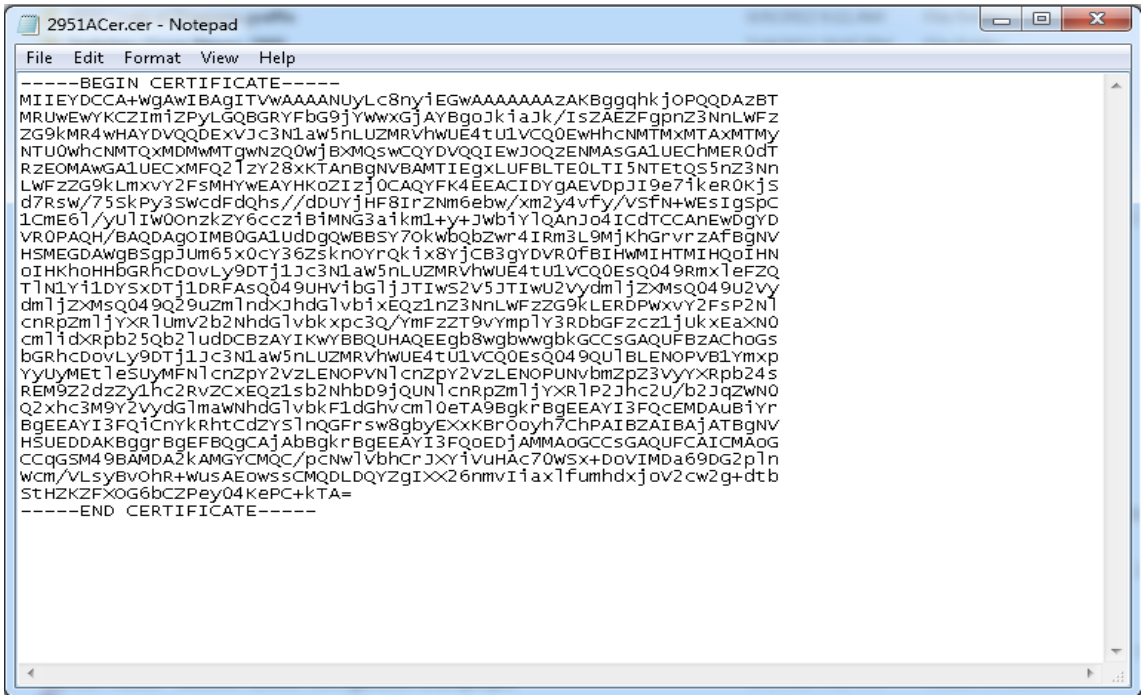


Step 10. After the router certificate is issued, the PKI administrator provides the certificate through a secured method, such as SFTP. On a side note, the certificate must be provided in PEM format or the router will reject the certificate.



Note: A copy of the issued certificate is created on the Sub-CA root directory. This certificate can then be moved to an SFTP server for retrieval by the network staff.

Step 11. Follow the following procedure to import the certificate into the router: Open the certificate with notepad and copy it.



Import the certificate into the Sub-Ca trustpoint

H1-AA-14-2951-A(config)#cry pki import CUSTOMERAFlexSubCa certificate

Enter the base 64 encoded certificate.

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

-----BEGIN CERTIFICATE-----

MIIEYDCCA+WgAwIBAgITVwAAAANUyLc8nyiEGwAAAAAAAzAKBggqhkjOPQQDAzBTMRUwEwYKCZI
miZPyLGQBGRYFbG9jYWwxGjAYBgoJkiaJk/IsZAEZFgpnZ3NnLWFzZG9kMR4wHAYDVQQDExVJc3N
1aW5nLUZMRVhWUE4tU1VCQ0EwHhcNMTMxMTAxMTMyNTU0WhcNMTQxMDMwMTgwNzQ0WjBX
MQswCQYDVQQIEwJOQzENMAsGA1UEChMER0dTRzEOMAwGA1UECxMFQ2lzY28xKTAnBgNVBAM
TIEgxLUFBLTE0LTI5NTEtQS5nZ3NnLWFzZG9kLmxvY2FsMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE
VDpJI9e7ikeR0KjSd7RsW/75SkPy3SWcdFdQhs//dDUYjHF8IrZNm6ebw/xm2y4vfy/VSfN+WEsIgSpC1C
mE6l/yUIIW0OnzkZY6ccziBiMNG3aikm1+y+JWbiYlQAnJo4ICdTCCAnEwDgYDVR0PAQH/BAQDAgOIM
B0GA1UdDgQWBBSY7OkWbQbZwr4IRm3L9MjKhGrvrzAfBgNVHSMEGDAWgBSgpJUm65x0cY36Zskn
OYrQkix8YjCB3gYDVR0fBIHWMIHTMIHQoIHNoIHKhoHHbGRhcDovLy9DTj1Jc3N1aW5nLUZMRVhWU
+dtbStHZKZFXOG6bCZPey04KePC+kTA=

-----END CERTIFICATE-----

quit

% Router Certificate successfully imported

Step 12. After the router identity certificate has been imported, check the router certificate store to make sure that the complete CA chain shows. There should be three certificates, as display below.

```
H1-AA-14-2951-A#sh cry pki certificates
Certificate (This is the Router Identity Certificate)
  Status: Available
  Certificate Serial Number (hex): 570000000354C8B73C9F28841B000000000003
  Certificate Usage: Signature
  Issuer:
    cn=Issuing-FLEXVPN-SUBCA
    dc=nge-customera
    dc=local
  Subject:
    Name: H1-AA-14-2951-A.nge-customera.local
    cn=H1-AA-14-2951-A.nge-customera.local
    ou=Cisco
    o=NGE
    st=NC
  CRL Distribution Points:
    ldap:///CN=Issuing-FLEXVPN-SUBCA,CN=FlexVPNSub-
Ca,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nge-
customera,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Validity Date:
    start date: 09:25:54 EDT Nov 1 2013
    end   date: 14:07:44 EDT Oct 30 2014
  Associated Trustpoints: CUSTOMERAFlexSubCa
  Storage: nvram:Issuing-FLEX#3.cer
CA Certificate (This is the Sub-CA Certificate)
  Status: Available
```

```
  Certificate Serial Number (hex): 7600000007742A7C5F1FF114A0000000000007
  Certificate Usage: Signature
  Issuer:
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Subject:
    cn=Issuing-FLEXVPN-SUBCA
    dc=nge-customera
    dc=local
  CRL Distribution Points:
    ldap:///CN=nge-customera-FLEXVPNCA-
CA,CN=FlexVPNCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nge-
customera,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Validity Date:
    start date: 13:57:44 EDT Oct 30 2013
    end   date: 14:07:44 EDT Oct 30 2014
  Associated Trustpoints: CUSTOMERAFlexSubCa
  Storage: nvram:nge-customera-F#7CA.cer
CA Certificate (This is the Root CA Certificate)
  Status: Available
  Certificate Serial Number (hex): 50CA2CE4B72EEEB34D36D480D7B2B7A7
  Certificate Usage: Signature
  Issuer:
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Subject:
    cn=nge-customera-FLEXVPNCA-CA
    dc=nge-customera
    dc=local
  Validity Date:
    start date: 12:32:31 EDT Oct 7 2013
    end   date: 12:42:31 EDT Oct 7 2015
  Associated Trustpoints: CUSTOMERARootCA
  Storage: nvram:nge-customera-F#B7A7CA.cer
```

The process presented above will be the same for the hubs and spoke routers; except, the Container Name (CN) will change for each router, which is the router name.

FlexVPN Hub Configuration Recommendation

The following configuration covers FlexVPN IKEv2 Phase I, and IPSec Phase II required to support Suite-B complaint set of algorithms in the hub routers. In addition, this configuration covers HSRP tracking and EIGRP default route advertisement.

Step 1. Configure a pool of IP address that will be issued to the FlexVPN clients

```
H1-AA-14-3945-A(config)#ip local pool FlexVPNSpokes 10.3.1.1 10.3.1.100
```

Step 2. Configure an AAA to authorize the provisioning of IP address for the FlexVPN clients

```
H1-AA-14-3945-A(config)#aaa authorization network IPPool local
```

Step 3. As part of IKEv2 phase I, define an authorization policy mapping the IP pool with their subnet masks, and advertise a dynamic static route to the spoke router that points to the hub virtual interface

```
H1-AA-14-3945-A(config)#crypto ikev2 authorization policy CUSTOMERAPool
H1-AA-14-3945-A(config-ikev2-author-policy)#pool FlexVPNSpokes
H1-AA-14-3945-A(config-ikev2-author-policy)#netmask 255.255.255.0
H1-AA-14-3945-A(config-ikev2-author-policy)# route set interface
```

Step 4. An IKEv2 Phase I proposal is configure to provide the Elliptic Curve aes encryption size, the SHA key value, and a 384-bit Elliptic Diffie Hellman group (group 20).

```
H1-AA-14-3945-A(config)#crypto ikev2 proposal CUSTOMERAFlexVPN
H1-AA-14-3945-A(config-ikev2-proposal)#encryption aes-cbc-256
H1-AA-14-3945-A(config-ikev2-proposal)#integrity sha384
H1-AA-14-3945-A(config-ikev2-proposal)#group 20
```

Step 5. Configure an IKEv2 policy that will be used between peers phase I handshake

```
H1-AA-14-3945-A(config)#crypto ikev2 policy CUSTOMERAFlexVPNPolicy
H1-AA-14-3945-A(config-ikev2-policy)#proposal CUSTOMERAFlexVPN
```

Step 6. As part of IKEv2 Phase I, an IKEv2 profile must also be configured with the type of authentication method (ECDSA-SIG), the FQDN as the authentication to present to the next router, the trustpoint to be used, the aaa authorization point for the FlexVPN hub to issue a DHCP IP address to the FlexVPN clients, and the virtual template to use for connectivity.

```
H1-AA-14-3945-A(config)#crypto ikev2 profile CUSTOMERAFlexVPNProfile
H1-AA-14-3945-A(config-ikev2-profile)#match identity remote fqdn domain nge-customera.local
H1-AA-14-3945-A(config-ikev2-profile)#identity local fqdn H1-AA-14-3945-B.nge-customera.local
H1-AA-14-3945-A(config-ikev2-profile)#authentication remote ecdsa-sig
H1-AA-14-3945-A(config-ikev2-profile)#authentication local ecdsa-sig
H1-AA-14-3945-A(config-ikev2-profile)#pki trustpoint CUSTOMERAFlexSubCa
H1-AA-14-3945-A(config-ikev2-profile)#aaa authorization group cert list IPPool CUSTOMERAPool
H1-AA-14-3945-A(config-ikev2-profile)#virtual-template 1
```

Note: The router ip domain-name command FQDN must match your organization domain.

Step 7. Configure IPSec (ESP) Phase II Suite-B set of algorithms. This proposal must be the same on both peers.

```
H1-AA-14-3945-A(config)#crypto ipsec transform-set CUSTOMERASuiteB esp-gcm 256
H1-AA-14-3945-A(cfg-crypto-trans)#mode transport
```

Step 8. Configure an IPSec profile that specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires, and the number of seconds a security association will live. The transform previously created is tied to the IPSec and the IKEv2 profiles. This information will be used between the FlexVPN hubs and spokes to established Phase I and II. In addition, noticed the hub cannot initiate a connection to the spokes and that's the purpose of the command *responder-only*.

```
H1-AA-14-3945-A(config)#crypto ipsec profile FlexVPNHub
H1-AA-14-3945-A(ipsec-profile)#set security-association lifetime kilobytes 4294967295
H1-AA-14-3945-A(ipsec-profile)#set security-association lifetime seconds 86400
H1-AA-14-3945-A(ipsec-profile)#set transform-set CUSTOMERASuiteB
H1-AA-14-3945-A(ipsec-profile)#set ikev2-profile CUSTOMERAFlexVPNProfile
H1-AA-14-3945-A(ipsec-profile)#responder-only
```

Step 9. Configure a Dynamic Virtual Tunnel Interface (DTVI) to use an unnumbered IP address to a loopback, and use the WAN interface as the tunnel source. In addition, map the Phase I and Phase II IPSec profile to the DVTI.

```
H1-AA-14-3945-A(config)#interface Virtual-Template1 type tunnel
H1-AA-14-3945-A(config-if)#description FlexVPN Hub Router
H1-AA-14-3945-A(config-if)#ip unnumbered Loopback0
H1-AA-14-3945-A(config-if)#tunnel source GigabitEthernet0/1
H1-AA-14-3945-A(config-if)#tunnel mode ipsec ipv4
H1-AA-14-3945-A(config-if)#tunnel protection ipsec profile FlexVPNHub
```

Step 10. Configure HSRP tracking and IP SLA on the active HSRP FlexVPN hub that monitors the status of the WAN interface and also ping an upstream host. This configuration might be modified to reflect CUSTOMERA implementation of tracking and/or IP SLA.

```
H1-AA-14-3945-A(config)#track 10 interface GigabitEthernet0/1 line-protocol
H1-AA-14-3945-A(config)#ip sla 100
H1-AA-14-3945-A(config-ip-sla)#icmp-echo 10.2.1.4
H1-AA-14-3945-A(config-ip-sla)#frequency 120
H1-AA-14-3945-A(config)#ip sla schedule 100 life forever start-time now
H1-AA-14-3945-A(config)# track 69 ip sla 100
```

Step 11. Add the tracking objects to the LAN interface HSRP configuration with a value high enough that will make the decrement of the active HSRP router priority lower than the standby HSRP router.

```
H1-AA-14-3945-A(config)#interface GigabitEthernet0/0
H1-AA-14-3945-A(config-if)#ip address 172.19.0.2 255.255.255.0
H1-AA-14-3945-A(config-if)#standby 19 ip 172.19.0.254
H1-AA-14-3945-A(config-if)#standby 19 priority 125
H1-AA-14-3945-A(config-if)#standby 19 preempt
```

```
H1-AA-14-3945-A(config-if)#standby 19 track 10 decrement 35
H1-AA-14-3945-A(config-if)#standby 19 track 69 decrement 35
```

Step 12. Advertise a default route to the FlexVPN clients using the EIGRP routing protocol. In this example, a standard access list was used. However, a prefix list with a route-map could be used as well. Ultimately, it is up to CUSTOMERA to decide which method to use.

```
H1-AA-14-3945-A(config)#ip access-list standard EIGRP_Default
H1-AA-14-3945-A(config-std-nacl)#permit 0.0.0.0
H1-AA-14-3945-A(config)#router eigrp 69
H1-AA-14-3945-A(config-router)#distribute-list EIGRP_Default out Virtual-Template1
H1-AA-14-3945-A(config-router)#network 10.3.1.0 0.0.0.255
H1-AA-14-3945-A(config-router)#network 10.3.2.0 0.0.0.255
H1-AA-14-3945-A(config-router)#network 172.19.0.0 0.0.0.255
H1-AA-14-3945-A(config-router)#network 192.168.40.0
H1-AA-14-3945-A(config-router)#network 192.168.210.0
H1-AA-14-3945-A(config)#ip route 0.0.0.0 0.0.0.0 192.168.210.1
```

FlexVPN Client Configuration Recommendation

The following configuration covers FlexVPN IKEv2 Phase I, and IPSec Phase II required to support Suite-B complaint set of algorithms in the spoke routers.

Step 1. As part of IKEv2 phase I, configure an authorization policy to inject a static route to point to the next hop IP unnumbered virtual interface.

```
H1-AA-14-2951-B(config)#crypto ikev2 authorization policy CUSTOMERA
H1-AA-14-2951-B(config-ikev2-author-policy)#route set interface
```

Step 2. Configure an IKEv2 Phase I proposal to provide the Elliptic Curve aes encryption size, the SHA key value, and a 384-bit Elliptic Diffie Hellman group (group 20) that will be negotiated between the spoke and hub.

```
H1-AA-14-2951-B(config)#crypto ikev2 proposal CUSTOMERAFlexVPN
H1-AA-14-2951-B(config-ikev2-proposal)#encryption aes-cbc-256
H1-AA-14-2951-B(config-ikev2-proposal)#integrity sha384
H1-AA-14-2951-B(config-ikev2-proposal)#group 20
```

Step 3. Define an IKEv2 policy that will be used between peers phase I handshake

```
H1-AA-14-2951-B(config)#crypto ikev2 policy CUSTOMERAFlexVPNPolicy
H1-AA-14-2951-B(config-ikev2-policy)#proposal CUSTOMERAFlexVPN
```

Step 4. As part of IKEv2 Phase I, an IKEv2 profile must also be configured with the type of authentication method (ECDSA-SIG), the FQDN as the authentication to present to the next hub router, the trustpoint to be used, the aaa authorization point to obtain an IP address and set a static route, and the Dead Peer Detection (DPD) to periodically monitor connectivity with the hub router.

```
H1-AA-14-2951-B(config)#crypto ikev2 profile CUSTOMERAFlexVPNProfile
H1-AA-14-2951-B(config-ikev2-profile)#match identity remote fqdn domain nge-customera.local
H1-AA-14-2951-B(config-ikev2-profile)#identity local fqdn H1-AA-14-2951-B.nge-customera.local
H1-AA-14-2951-B(config-ikev2-profile)#authentication remote ecdsa-sig
H1-AA-14-2951-B(config-ikev2-profile)#authentication local ecdsa-sig
H1-AA-14-2951-B(config-ikev2-profile)#pki trustpoint CUSTOMERAFlexSubCa
H1-AA-14-2951-B(config-ikev2-profile)#dpd 10 3 periodic
H1-AA-14-2951-B(config-ikev2-profile)#aaa authorization group cert list default CUSTOMERA
```

Step 5. DPD monitors the connectivity status between the FlexVPN client and the FlexVPN hub; in the event a connectivity failure occurs, the FlexVPN client clears its IPSec Security Association (SA) and automatically initiates a connection to its backup peer. This configuration accomplishes this task.

```
H1-AA-14-2951-B(config)#crypto ikev2 client flexvpn CUSTOMERAFlexVPNClient
H1-AA-14-2951-B(config-ikev2-flexvpn)#peer 1 10.2.1.2
H1-AA-14-2951-B(config-ikev2-flexvpn)#peer 2 10.2.1.1
H1-AA-14-2951-B(config-ikev2-flexvpn)#client connect Tunnel0
```

Step 6. Configure an IPSec (ESP) Phase II Suite-B set of algorithms. This proposal must be the same on both peers.

```
H1-AA-14-2951-B(config)#crypto ipsec transform-set CUSTOMERASuiteB esp-gcm 256
H1-AA-14-2951-B(cfg-crypto-trans)#mode transport
```

Step 7. Configure an IPSec profile that specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires, and the number of seconds a security association will live. The transform previously created is tied to the IPSec and the IKEv2 profiles. This information will be used between the FlexVPN hubs and spokes to established Phase I and II.

```
H1-AA-14-2951-B(config)#crypto ipsec profile FlexVPNSpoke
H1-AA-14-2951-B(ipsec-profile)#set security-association lifetime kilobytes 4294967295
H1-AA-14-2951-B(ipsec-profile)#set security-association lifetime seconds 86400
H1-AA-14-2951-B(ipsec-profile)#set transform-set CUSTOMERASuiteB
H1-AA-14-2951-B(ipsec-profile)#set ikev2-profile CUSTOMERAFlexVPNProfile
```

Step 8. Configure the FlexVPN tunnel interface to obtain an IP address from the active FlexVPN hub. Make sure the tunnel destination is configured as *dynamic* and not to the next hop HSRP VIP address. This is done so the FlexVPN client can negotiate an IPSec tunnel to its backup FlexVPN hub, and that is if connectivity to the primary is lost.

```
H1-AA-14-2951-B(config)#interface Tunnel0
H1-AA-14-2951-B(config-if)#description SVTI to HUB Router
H1-AA-14-2951-B(config-if)#ip address negotiated
H1-AA-14-2951-B(config-if)#ip mtu 1400
H1-AA-14-2951-B(config-if)#ip tcp adjust-mss 1360
H1-AA-14-2951-B(config-if)#tunnel source GigabitEthernet0/1
H1-AA-14-2951-B(config-if)#tunnel mode ipsec ipv4
H1-AA-14-2951-B(config-if)#tunnel destination dynamic
H1-AA-14-2951-B(config-if)#tunnel path-mtu-discovery
H1-AA-14-2951-B(config-if)#tunnel protection ipsec profile FlexVPNSpoke
```

Step 9. Add the FlexVPN cloud network to the EIGRP routing process, which in this testing was 10.3.1.0/24. In addition, it is highly recommended that the FlexVPN clients be configured as EIGRP stub routers.

Appendix – FlexVPN Configurations

FlexVPN Hub Router

```
H1-AA-14-3945-A#sh run
Building configuration...

Current configuration : 12276 bytes
!
! Last configuration change at 12:16:03 EDT Fri Nov 1 2013
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname H1-AA-14-3945-A
!
boot-start-marker
boot system flash0:c3900-universalk9-mz.SPA.152-4.M4.bin
boot-end-marker
!
!
! card type command needed for slot/vwic-slot 0/1
logging buffered 64000
no logging monitor
enable secret 4 U5mYUdmuzQBVcsX8hgoh7dHXvImCY6NOkWHSgHL.m46
!
aaa new-model
!
aaa authentication login default none
aaa authorization network IPPool local
!
aaa session-id common
clock timezone EST -5 0
clock summer-time EDT recurring
no network-clock-participate wic 0
!
!
crypto pki trustpoint CUSTOMERARootCA
 enrollment terminal
 revocation-check none
  hash sha384

!
crypto pki trustpoint CUSTOMERAFlexSubCa
 enrollment terminal
 subject-name CN=H1-AA-14-3945-A.nge-customera.local, OU=Cisco, O=NGE, ST=NC
 revocation-check none
  hash sha384

 eckeypair H1-AA-14-3945-A.nge-customera.local
!
!
crypto pki certificate chain CUSTOMERARootCA
```

```
 certificate ca 50CA2CE4B72EEEB34D36D480D7B2B7A7
  3082024E 308201D4 A0030201 02021050 CA2CE4B7 2EEEB34D 36D480D7 B2B7A730
  0A06082A 8648CE3D 04030330 55311530 13060A09 92268993 F22C6401 1916056C
  6F63616C 311A3018 060A0992 268993F2 2C640119 160A6767 73672D61 73646F64
  3120301E 06035504 03131767 6773672D 6173646F 642D464C 45585650 4E43412D
A6CBDF94 C3E01B8E F48F0972 17F5CCD7 6993
      quit
crypto pki certificate chain CUSTOMERAFlexSubCa
 certificate 6A0000000A64F38245D87198D300000000000A
  30820462 308203E7 A0030201 0202136A 0000000A 64F38245 D87198D3 00000000
  000A300A 06082A86 48CE3D04 03033053 31153013 060A0992 268993F2 2C640119
  16056C6F 63616C31 1A301806 0A099226 8993F22C 64011916 0A676773 672D6173
  646F6431 1E301C06 03550403 13154973 7375696E 672D464C 45585650 4E2D5355
  42434130 1E170D31 33313031 33303333 3235345A 170D3134 31303037 31373134
  30345A30 57310B30 09060355 04081302 4E43310D 300B0603 55040A13 04474753
  47310E30 0C060355 040B1305 43697363 6F312930 27060355 04031320 48312D41
  412D3134 2D333934 352D412E 67677367 2D617364 6F642E6C 6F63616C 30763010
  06072A86 48CE3D02 0106052B 81040022 03620004 6254C002 8169FDFE D69DB6AC
  FF9EE446 F2E2D9C5 3E6149BF E223459B 935261FA 85F517D4 E1A04E30 4032219A
  98742F6E B8056B6C CB27C900 9194AB29 1276D094 21CB8879 BE655834 FF04ED1A
  63103316 13528864 69464303 65ED220D 99F2FB20 A3820277 30820273 300E0603
C2DD17D2 F20B
      quit
 certificate ca 760000000225FD1779F5337B4F000000000002
  30820427 308203AD A0030201 02021376 00000002 25FD1779 F5337B4F 00000000
  0002300A 06082A86 48CE3D04 03033055 31153013 060A0992 268993F2 2C640119
  16056C6F 63616C31 1A301806 0A099226 8993F22C 64011916 0A676773 672D6173
  646F6431 20301E06 03550403 13176767 73672D61 73646F64 2D464C45 5856504E
  43412D43 41301E17 0D313331 30303731 37303430 345A170D 31343130 30373137
  31343034 5A305331 15301306 0A099226 8993F22C 64011916 056C6F63 616C311A
  3018060A 09922689 93F22C64 0119160A 67677367 2D617364 6F64311E 301C0603
  55040313 15497373 75696E67 2D464C45 5856504E 2D535542 43413076 30100607
  2A8648CE 3D020106 052B8104 00220362 000469A4 B32A0F91 85DC686F E601A1F8
  41198E7E DAF44D33 DE9206B6 4AEDC337 5CAA7E64 82518BBD 4C0E55FE 41D7CAE0
  51D628EB F9606958 3FC28E46 07D7D97E 95C2AA0A E111E676 EEC74BC2 76BF5499
  C8B50B0F BC767B55 CB9F67E0 944B03BA 37C7A382 023F3082 023B3010 06092B06
 2F008DD6 22C29741 8D750B
      quit
ip cef
!
ip domain name nge-customera.local
no ipv6 cef
!
license udi pid C3900-SPE150/K9 sn FOC162569SJ
license boot module c3900 technology-package securityk9
hw-module ism 0
!
redundancy
!
crypto ikev2 authorization policy CUSTOMERAPool
 pool FlexVPNSpokes
 netmask 255.255.255.0
 route set interface
!
crypto ikev2 proposal CUSTOMERAFlexVPN
 encryption aes-cbc-256
 integrity sha384
 group 20
!
```

```
crypto ikev2 policy CUSTOMERAFlexVPNPolicy
 proposal CUSTOMERAFlexVPN
!
!
crypto ikev2 profile CUSTOMERAFlexVPNProfile
 match identity remote fqdn domain nge-customera.local
 identity local fqdn H1-AA-14-3945-A.nge-customera.local
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint CUSTOMERAFlexSubCa
 aaa authorization group cert list IPPool CUSTOMERAPool
 virtual-template 1
!
track 10 interface GigabitEthernet0/1 line-protocol
!
track 69 ip sla 100
!
crypto ipsec transform-set CUSTOMERASuiteB esp-gcm 256
 mode transport
!
crypto ipsec profile FlexVPNHub
 set security-association lifetime kilobytes 4294967295
 set security-association lifetime seconds 86400
 set transform-set CUSTOMERASuiteB
 set ikev2-profile CUSTOMERAFlexVPNProfile
 responder-only
!
crypto ipsec profile FlexVPNSpoke
 set security-association lifetime seconds 86400
!
!
interface Loopback0
 ip address 10.3.2.110 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 172.19.0.2 255.255.255.0
 standby 19 ip 172.19.0.254
 standby 19 priority 125
 standby 19 preempt
 standby 19 track 10 decrement 35
 standby 19 track 69 decrement 35
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description WAN Interface
 ip address 10.2.1.2 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description Windows 2008 R2 Server
 ip address 192.168.210.110 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
```

```
 duplex auto
 speed auto
!
!
interface GigabitEthernet1/0
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet1/1
 description Internal switch interface connected to Service Module
 switchport mode trunk
 no ip address
!
interface SM2/0
 description Windows 2012 R2
 ip unnumbered GigabitEthernet0/2
 service-module ip address 192.168.210.111 255.255.255.0
 service-module ip default-gateway 192.168.210.110
!
interface SM2/1
 description Internal switch interface connected to Service Module
 switchport mode trunk
 no ip address
!
interface Virtual-Template1 type tunnel
 description FlexVPN Hub Router
 ip unnumbered Loopback0
 tunnel source GigabitEthernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FlexVPNHub
!
interface Vlan1
 no ip address
!
interface Vlan40
 description Windows 2012 R2 Sub-CA
 ip address 192.168.40.254 255.255.255.0
!
router eigrp 69
 distribute-list EIGRP_Default out Virtual-Template1
 network 10.3.1.0 0.0.0.255
 network 10.3.2.0 0.0.0.255
 network 172.19.0.0 0.0.0.255
 network 192.168.40.0
 network 192.168.210.0
!
ip local pool FlexVPNSpokes 10.3.1.1 10.3.1.100
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.210.1
ip route 192.168.210.111 255.255.255.255 SM2/0
!
ip access-list standard EIGRP_Default
 permit 0.0.0.0
!
ip sla auto discovery
ip sla 100
```

```
 icmp-echo 10.2.1.4
 frequency 120
ip sla schedule 100 life forever start-time now
```

FlexVPN Client Router

```
H1-AA-14-2951-B#sh run
Building configuration...

Current configuration : 11223 bytes
!
! Last configuration change at 12:28:38 EDT Fri Nov 1 2013
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname H1-AA-14-2951-B
!
boot-start-marker
boot system flash0:c2951-universalk9-mz.SPA.152-4.M4.bin
boot-end-marker
!
! card type command needed for slot/vwic-slot 0/1
enable secret 4 U5mYUdmuzQBVcsX8hgoh7dHXvImCY6NOkWHSgHL.m46
!
no aaa new-model
clock timezone EST -5 0
clock summer-time EDT recurring
no network-clock-participate wic 0
!
!
crypto pki trustpoint CUSTOMERARootCA
 enrollment terminal
 revocation-check none
 hash sha384


!
crypto pki trustpoint CUSTOMERAFlexSubCa
 enrollment terminal
 subject-name CN=H1-AA-14-2951-B.nge-customera.local, OU=Cisco, O=NGE, ST=NC
 revocation-check none
 hash sha384

 eckeypair H1-AA-14-2951-B.nge-customera.local
!
!
crypto pki certificate chain CUSTOMERARootCA
 certificate ca 50CA2CE4B72EEEB34D36D480D7B2B7A7
  3082024E 308201D4 A0030201 02021050 CA2CE4B7 2EEEB34D 36D480D7 B2B7A730
  0A06082A 8648CE3D 04030330 55311530 13060A09 92268993 F22C6401 1916056C
  6F63616C 311A3018 060A0992 268993F2 2C640119 160A6767 73672D61 73646F64
  3120301E 06035504 03131767 6773672D 6173646F 642D464C 45585650 4E43412D
  4341301E 170D3133 31303037 31363332 33315A17 0D313531 30303731 36343233
  315A3055 31153013 060A0992 268993F2 2C640119 16056C6F 63616C31 1A301806
  0A099226 8993F22C 64011916 0A676773 672D6173 646F6431 20301E06 03550403
  13176767 73672D61 73646F64 2D464C45 5856504E 43412D43 41307630 1006072A
  8648CE3D 02010605 2B810400 22036200 0432D735 D3D8D59D F25A06E1 393735C5
```

```
 CA2339C3 098CF088 8A3D4B05 FDA18E66 00C522A2 699E2034 37A4D291 DBB38B43
 85D3F5C2 8F4C1D1E 7FA43140 0211F312 964C5F78 6B1C60B0 B2B5DC81 60501629
 21AD350E 2667C43B EA64D3F0 4572F736 8FA36930 67301306 092B0601 04018237
 A6CBDF94 C3E01B8E F48F0972 17F5CCD7 6993
      quit
crypto pki certificate chain CUSTOMERAFlexSubCa
 certificate 6A0000000C6AB6338EA090BAA500000000000C
  30820461 308203E7 A0030201 0202136A 0000000C 6AB6338E A090BAA5 00000000
  000C300A 06082A86 48CE3D04 03033053 31153013 060A0992 268993F2 2C640119
  16056C6F 63616C31 1A301806 0A099226 8993F22C 64011916 0A676773 672D6173
  646F6431 1E301C06 03550403 13154973 7375696E 672D464C 45585650 4E2D5355
  42434130 1E170D31 33313031 35303431 3532315A 170D3134 31303037 31373134
  30345A30 57310B30 09060355 04081302 4E43310D 300B0603 55040A13 04474753
  47310E30 0C060355 040B1305 43697363 6F312930 27060355 04031320 48312D41
  412D3134 2D323935 312D422E 67677367 2D617364 6F642E6C 6F63616C 30763010
  06072A86 48CE3D02 0106052B 81040022 03620004 3EE26ABD 53A67A13 E42DC882
  B3B7D6BD B3B5DD38 61BC2B74 233DB63A 2CF27B3B 3AA1A48E 08F799F5 2D83EE97
  71E35FD0 1B27A4C6 D906DB9F 861402D0 03B5E890 D211A47C CA8CC49F 5A542446
  3D973035 3783A26D 559D5382 14B43E27 AD4C5E78 A3820277 30820273 300E0603
  551D0F01 01FF0404 03020388 301D0603 551D0E04 160414E3 86F63E6D D4EC9B1C
  A35D52DD C497390D E419F630 1F060355 1D230418 30168014 1DFB7B39 53240FB5
  96E0C25A 867CF479 308FFC4A 3081E006 03551D1F 0481D830 81D53081 D2A081CF
  A081CC86 81C96C64 61703A2F 2F2F434E 3D497373 75696E67 2D464C45 5856504E
  2D535542 43412C43 4E3D466C 65785650 4E2D5375 62434144 432C434E 3D434450
  2C434E3D 5075626C 69632532 304B6579 25323053 65727669 6365732C 434E3D53
  03551D25 040C300A 06082B06 01050508 0202301B 06092B06 01040182 37150A04
  0E300C30 0A06082B 06010505 08020230 0A06082A 8648CE3D 04030303 68003065
  023049C7 4B63B016 34F7AEE0 C8DFA77B DCC02293 F797E432 E49DF025 9F2E4A4C
  5F717497 6C8B2B40 66F3DECF 1ED198F5 533F0231 00DF5FE4 763585B7 E8CD60FF
  E3805E79 2DA7B5E0 955EB231 D98659E8 3C8E9096 F69E6379 410A54E9 D2004037
  503116DA 3F
      quit
 certificate ca 760000000225FD1779F5337B4F000000000002
  30820427 308203AD A0030201 02021376 00000002 25FD1779 F5337B4F 00000000
  0002300A 06082A86 48CE3D04 03033055 31153013 060A0992 268993F2 2C640119
  16056C6F 63616C31 1A301806 0A099226 8993F22C 64011916 0A676773 672D6173
  646F6431 20301E06 03550403 13176767 73672D61 73646F64 2D464C45 5856504E
  43412D43 41301E17 0D313331 30303731 37303430 345A170D 31343130 30373137
  31343034 5A305331 15301306 0A099226 8993F22C 64011916 056C6F63 616C311A
  3018060A 09922689 93F22C64 0119160A 67677367 2D617364 6F64311E 301C0603
  55040313 15497373 75696E67 2D464C45 5856504E 2D535542 43413076 30100607
  2A8648CE 3D020106 052B8104 00220362 000469A4 B32A0F91 85DC686F E601A1F8
  41198E7E DAF44D33 DE9206B6 4AEDC337 5CAA7E64 82518BBD 4C0E55FE 41D7CAE0
 436F6E66 69677572 6174696F 6E2C4443 3D676773 672D6173 646F642C 44433D6C
 25323053 65727669 6365732C 434E3D53 65727669 6365732C 434E3D43 6F6E6669
  67757261 74696F6E 2C44433D 67677367 2D617364 6F642C44 433D6C6F 63616C3F
  63414365 72746966 69636174 653F6261 73653F6F 626A6563 74436C61 73733D63
  65727469 66696361 74696F6E 41757468 6F726974 79300A06 082A8648 CE3D0403
  03036800 30650230 093C9D34 C80940FB 52737957 A34AE4E4 AE5E21AA 6816AC1C
  A31C13F9 04F08827 4F03F21D 35CCC6EB B8649B87 40CA920C 023100C9 3F44028E
  1A44F250 2CEC87D6 46607C79 3723749B D54F99C1 26BD00F2 257289B7 FE38F84E
  2F008DD6 22C29741 8D750B
      quit
ip cef
!
crypto ikev2 authorization policy CUSTOMERA
route set interface
!
crypto ikev2 proposal CUSTOMERAFlexVPN
```

```
encryption aes-cbc-256
integrity sha384
group 20
!
crypto ikev2 policy CUSTOMERAFlexVPNPolicy
proposal CUSTOMERAFlexVPN
!
!
crypto ikev2 profile CUSTOMERAFlexVPNProfile
match identity remote fqdn domain nge-customera.local
dentity local fqdn H1-AA-14-2951-B.nge-customera.local
authentication remote ecdsa-sig
authentication local ecdsa-sig
pki trustpoint CUSTOMERAFlexSubCa
dpd 10 3 periodic
aaa authorization group cert list default CUSTOMERA
!
crypto ikev2 client flexvpn CUSTOMERAFlexVPNClient
peer 1 10.2.1.2
peer 2 10.2.1.1
client connect Tunnel0
!
!
crypto ipsec transform-set CUSTOMERASuiteB esp-gcm 256
mode transport
!
crypto ipsec profile FlexVPNSpoke
set security-association lifetime kilobytes 4294967295
set security-association lifetime seconds 86400
set transform-set CUSTOMERASuiteB
set ikev2-profile CUSTOMERAFlexVPNProfile
!
!
!
interface Loopback0
 ip address 10.3.2.1 255.255.255.255
!
interface Tunnel0
description SVTI to HUB Router
ip address negotiated
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/1
tunnel mode ipsec ipv4
tunnel destination dynamic
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPNSpoke
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 172.19.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description WAN Interface
```

```
 ip address 10.2.1.4 255.255.255.248
 duplex auto
 speed auto
!
!
router eigrp 69
 network 10.3.1.0 0.0.0.255
 network 10.3.2.0 0.0.0.255
 network 172.19.3.0 0.0.0.255
 eigrp stub connected
```