

Cisco Systems Inc.



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 THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment is a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

Turn the television or radio antenna until the interference stops.

Move the equipment to one side or the other of the television or radio.

Move the equipment farther away from the television or radio

Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of the UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

Xremote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PRACTICAL PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Networking Academy, the Cisco Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco, Capital, the Cisco logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R).

Please refer to http://www.cisco.com/logo/ for the latest information on Cisco logos, branding and trademarks.

INTELLECTUAL PROPERTY RIGHTS:

THIS DOCUMENT CONTAINS VALUABLE TRADE SECRETS AND CONFIDENTIAL INFORMATION OF CISCO AND IT'S SUPPLIERS, AND SHALL NOT BE DISCLOSED TO ANY PERSON, ORGANIZATION, OR ENTITY UNLESS SUCH DISCLOSURE IS SUBJECT TO THE PROVISIONS OF A WRITTEN NON-DISCLOSURE AND PROPRIETARY RIGHTS AGREEMENT OR INTELLECTUAL PROPERTY LICENSE AGREEMENT APPROVED BY CISCO THE DISTRIBUTION OF THIS DOCUMENT DOES NOT GRANT ANY LICENSE IN OR RIGHTS, IN WHOLE OR IN PART, TO THE CONTENT, THE PRODUCT(S), TECHNOLOGY OF INTELLECTUAL PROPERTY DESCRIBED HEREIN.

Proactive Software Recommendation Report Copyright © 2003, Cisco All rights reserved. COMMERCIAL IN CONFIDENCE. A PRINTED COPY OF THIS DOCUMENT IS CONSIDERED UNCONTROLLED.

Contents

Contents	
Document Control	4
History	4
Review	
Executive Summary	5
Introduction	6
VPN Solution Diagram	7
Caveats & Prerequisites	8
Certificate Caveats	8
Prerequisites	9
ASA Configuration & Enrollment with the CA	
ASA PKI Configuration and Enrollment	
ASA VPN Configuration	
AnyConnect Client Setup	
Client PKI Enrollment	
AnyConnect Client Configuration	
Appendix A – ASA Configurations	
Appendix B – CA Implementation	
Offline Root CA & Subordinate CA File Share Setup	
Enterprise Subordinate CA Setup	
Version 3 Template Configuration	
Appendix C – ASA VPN Verification Commands	

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	2 nd 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 <u>IETF RFC 6379</u>, 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. 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.
- 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

Topology Overview



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.
- 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.
- 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:

 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".

O Configu	ration > Device Setup > System Time > Clock
Configure the	ASA date and clock.
Time Zone: [(GMT-05:00)(Eastern Time) Indianapolis, Montreal, New York
Date	
Feb 10, 201	4
Time	
Clock will b	e automatically adjusted for daylight saying changes.
0.000	
Time: 10	: 06 : 18 hh:mm:ss (24-hour)
\square	Update Displayed Time

 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".

○ ○ <u>Configu</u>	ration > Dev	/ice Setup >	System Tim	<u>e > NTP</u>	
Configure NTP	servers and	define authe	ntication key	s and values.	
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add
192.168.0.14	outside	No		No	
					Edit
					Delete

 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".

$0 \odot Configuration > Dev$	vice Setup > Device Name/Password
Hostname and Domain Nar	ne
Hostname:	grayasavpn
Domain Name:	graydmz.org

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

24 February 2014

 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".

\varTheta 🔿 🔿	Install Certificate	
Trustpoint Name:	GRAYCA	
Install from a file:		Browse
Paste certificate in	PEM format:	
BEGIN CERTIFI MIIBrjCCATSgAwIBA DQYDVQQDEwZHUJ MQ&wDQYDVQQDE kdLADIde5nzM82B 61rj12EzFbq9oun9q A1UdDwQEAwIBhJA SWonOIUDFqSOSJA oZSWQJpVnFy+0eYJ MQDdMh8lak73bFC JVQ= END CERTIFIC	ICATE GIQSpTGEE/L46 IJOOTIRY3kWzAKBggq kFZQ0EwHhcNMTQwMTE2MTE1MDISW WZHUKFZQ0EwdJAQBgcqhkjOPQIBBgUr KDGMuqxzR7h34tnUOOvdk8y/geULwv TDCposTd8U6JYXJ7SI6rgQolW2Q8fiHi PBgNVHRMBAf8EBTADAQH/MB0GA1Ud QBgkrBgEEAYI3FQEEAwIBADAKBggqhkji z8yJG6vDsLdk7rAeRTMdGJ92q8rREDTY Ti/97uFW4oShLrnKk0/U8EunRPbVq+QF CATE	hkjOPQQDAzARMQ8w hcNMTkwMTE2MTIwMDI5WjAR gQQAIgNiAAQH49gLYqJG Cwt6CEnsQNYbCJVgQdI Wc5skGjUTBPMAsG DgQWBBQanO0cU0d1i56v OPQQDAwNoADBIAjAx UAXNNnsb5Cr7OUgC INox+Y/IR8AYjuiIDJ7
Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
He	lp Cancel	More Options

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".

Θ \odot Θ	Install Certificate	
Trustpoint Name:	GRAYSUBCA1	
 Install from a file: 		Browse
 Paste certificate in 	PEM format:	
BEGIN CERTII MIIFsDCCASigAwlB MQswCQYDVQQGE ZC4xKjAoBgNVBAs Fw0wNDEyMJAWMJ SSB5b290IENIEnRpp AA0CAg8AMIICCgJ SyzbCUNsiZ5qyNU ijHyl3SJCRImHJ7K2 D2oTMJPRYfi61dd, TBnsZfZrxQWh7kc Quse SCEP:	FICATE HaglQFc192Udcr71XAF7kBtK8nTANBgkqh wJUV2EjMCEGA1UECgwaQ2h1bmdod25 MIWVQ50kgUm9ydCBD2XJ0aW2pY2F0al MxMjdaFw02NDEYMJAwMJMMMJdaMF4, zmJjYXRpb24g0XV0aC9yaXR5MIICIJANB xCAgEA4SUP703biDN1282tH306Tm2d0 D9WBpJ8zvluQf5/dqIjG2LBXy4P4AakP/ RKiITza6We/CKBk49ZCt0XvI/T29de1Sh 4 s5029wCG2h1NIDivq0x4UXCKXBCDUS T1rMhJSQQCtkk07q+RBNGMD+XPNJ12	kiG9w0BAQUFADBe gvGvsZWNvbSBDby4sIEx0 V9ulEF1dGhvcmloeTAe ZzAJBgNVBAYTAIRXMSMw gkqhkiG9w0BAQEF ysU82N0ywEhajfqhFAH h2XGfRF8p0xtInAh JCWH2YWEtgvM3X H3ET00h17ISM2XgY11 *u02jjK95XDrkb5wdj
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Options
Сне	elp Cancel	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".

\varTheta 🔿 🔘	Add Identity Certificate	
Trustpoint Name:	ASDM_TrustPoint0	
 Import the identity certified 	cate from a file (PKCS12 format with Ce	rtificate(s)+Private Key):
Decryption Passphrase:		
File to Import From:		Browse
💿 Add a new identity certifi	cate:	
Key Pair:	<default-rsa-key></default-rsa-key>	Show New
Certificate Subject DN:	CN=grayasavpn.graydmz.org	Select
Generate self-signed	certificate	
Act as local certif	icate authority and issue dynamic certif	icates to TLS-Proxy
		Advanced
Hel	p Cancel Ac	dd Certificate

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

0	$\bigcirc \bigcirc$	Add Key Pair
	Key Type:	○ RSA
	Name:	 Use default key pair name Enter new key pair name: ecdsa-384
	Size:	384
	\subset	Help Cancel 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".

l	Certificate Parameters	Enrollment Mode	SCEP Challenge Password
QDN:	grayasavpn.graydmz.or	rg	
-mail:			
P Address:	192.168.0.1		
🗌 Include	serial number of the dev	vice	

6. Return to the "Add Identity Certificate" page, select "Add Certificate".

$\Theta \bigcirc \bigcirc$	Add Identity Certificate				
Trustpoint Name:	ASDM_TrustPoint0				
Import the identity certification	icate from a file (PKCS12 format with Certificate(s)+Private Key):				
Decryption Passphrase:					
File to Import From:	Browse				
💿 Add a new identity certifi	cate:				
Key Pair:	<default-rsa-key> Show New</default-rsa-key>				
Certificate Subject DN:	CN=grayasavpn.graydmz.org Select				
Generate self-signed certificate					
Act as local certif	Act as local certificate authority and issue dynamic certificates to TLS–Proxy				
	Advanced				
Hel	p Cancel Add Certificate				

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

0	$\bigcirc \bigcirc$	Identity Certificate Request			
	To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.				
	You will then need the Install button	to install the certificate that is returned from the CA by clicking in the Identity Certificates panel.			
	Save CSR to File:	Browse			
		Help Cancel 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".

0	O Configuratio	on > Remote A	ccess VPN > Certi	ficate Management >	Identity Certifi	<u>cates</u>	
	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
	[grayasavpn.gr	Not Available	Pending	ASDM_TrustPoint0	Unknown	ECDSA (384 DIIS)	Show Details
							Delete
							Export
							Install

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

0 0	Install Identity certificate	
Identity Certificate		
O Install from a file:		Browse
Paste the certificate	data in base-64 format:	
vL8jcITbkj2yx3gCAV MCcGCSsGAQQBgjcV zj0EAwMDaAAwZQJ b1N4atMkTy4IgF/06 jYJPjDvAt4BOeEBRh END CERTIFIC	VQCAQMwHQYDVR0IBBYwFAYIKwYBBQUH /CgQaMBgwCgYIKwYBBQUHAwEwCgYIKwY ‹AKVyAPTKUI92q1X2aFsRi8IZIMqMYEmUk Qlwl/rAmFD7vO4HR+Oq7b3vPhdLmnI4j; Oc ATE	AwEGCCsGAQUFCAIC /BBQUIAgIwCgYIKoZI FY2KktG7KnsFiNZ 7tYLFi6bTRjRfYJ
Н	elp Cancel	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="" base64="" ca="" certificate="" from="" offline="" paste="" the=""></copy>			
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			
!			

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="" base64="" ca="" certificate="" from="" paste="" sub="" the=""></copy>				
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:

% The IP address in the certificate is 192.168.0.1
% The serial number in the certificate will be: FCH1744J8L7
% Include the device serial number in the subject name? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: grayasavpn.graydmz.org
% The subject name in the certificate will be: CN=grayasavpn.graydmz.org
crypto ca enroll GRAYSUBCA1

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.
- 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	

 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.

	O Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles						
Ad	The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options. Access Interfaces						
		SSL Access		IPsec (IKEv2) Access]	
	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate	
	outside			. ✓		Device certificate	
	dmz					(Port Settings)	

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.

\varTheta 🔿 😋	Specify Device Certificate			
Device certificate is a digital certificate t	hat identifies this ASA to the clients.			
Certificate with RSA key				
Use the same device certificate for S	SL and IPsec IKEv2			
Device Certificate for SSL Connection:	None 🗘			
Device Certificate for IPsec Connection:	None 🗘			
	Manage Certificates			
Certificate with ECDSA key (for IPsec connection only)				
Device Certificate: GRAYSUBCA1:cn=g	rayasavpn.graydmz.org:cn=GRAYSUBCA1 🛟 Manage			
Help	Cancel 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.

$\Theta \bigcirc \bigcirc$	Add IKE v2 Policy(Proposal)	
Priority:	1	
Encryption:	aes-gcm-256	
D-H Group:	20	
Integrity Hash:	null	
Pseudo Random Function	RF) Hash: sha384	
Lifetime:	Unlimited 86400 seconds	•
	elp Cancel OK	

 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.

\varTheta 🔿 🕙 🛛 Add	I IPsec Proposa	al
Name:	NGE-AES-GC	M-256
Encryption:	aes-gcm-256	•
Integrity Hash:	null	
Help	Cancel	ОК

 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.

٥	Create IPsec Rule
Tunnel f	olicy (Crypto Map) – Basic Tunnel Policy (Crypto Map) – Advanced Traffic Selection
Interface: outside	Policy Type: dy Priority: 1
IPsec Proposals (Trans	form Sets)
IKE v1 IPsec Proposal:	Select
IKE v2 IPsec Proposal:	NGE-AES-GCM-256 Select
IP Address of Peer to E	e Add Add >> Remove Move Up Move Down
Diffie-Hellman G	arding Se
	(Help) (Cancel) OK

 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.

○ ○ Configuration	> Remote Access VPN	> Network (Client) Access > Address As	signment > Address Pools	
Configure named IP Address Pools. The IP Address Pools can be used in either a VPN <u>IPsec(IKEv1) Connection Profiles</u> , <u>AnyConnect Connection Profiles</u> , <u>Group Policies</u> configuration				
🕈 Add 🔻 🗹 Ed	lit <u>Î</u> Delete			
Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length	
VPNUSERS	192.168.10.1	192.168.10.253	255.255.255.0	
Pool Name VPNUSERS	Starting Address 192.168.10.1	Ending Address/Number of Addresses 192.168.10.253	Subnet Mask/Prefix Length 255.255.255.0	

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.

00			Edit	t Internal Group Policy: NGE-VPN-GP	
General Servers	Name:	NGE-VPN-GP			
▶ Advanced	Banner:	🗹 Inherit			
	SCEP forwarding URL:	🗹 Inherit]
	Address Pools:	Inherit VP	NUSERS		Select
	IPv6 Address Pools:	🗹 Inherit			Select
	More Ontions				\$
	Tunneling Protocols:		🗌 Inherit	□ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 🗹 IPsec IKEv2 □ L2TP/IPsec	
	Filter:		🗹 Inherit	(Manage
	NAC Policy:		🗹 Inherit	\$	Manage
~	Access Hours:		🗹 Inherit	\$	Manage
	Simultaneous Logins	:	🗹 Inherit		
	Restrict access to VL	AN:	🗹 Inherit	\$	
	Connection Profile (T	unnel Group) Lock	a 🗹 Inherit	(4)	
	Maximum Connect T	ime:	🗹 Inherit	Unlimited minutes	
	Idle Timeout:		🗹 Inherit	None minutes	
	On smart card remov	al:	🗹 Inherit	○ Disconnect ○ Keep the connection	

 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.

0		Edit Any	Connect Connection Profile: NGE-RAS-VPN
	<mark>Basic</mark> ▶ Advanced	Name:	NGE-RAS-VPN
		Aliases:	
		Authentication	
		Method:	🔾 AAA 💿 Certificate 🔾 Both
		AAA Server Group:	LOCAL \$ Manage
			Use LOCAL if Server Group fails
		Client Address Assignment	
		DHCP Servers:	
			None ○ DHCP Link ○ DHCP Subnet
		Client Address Pools:	Select
		Client IPv6 Address Pools:	Select
		Default Group Policy	
		Group Policy:	NGE-VPN-GP Manage
		(Following field is an attrib	ute of the group policy selected above.)
		Enable SSL VPN clien	t protocol
		🗹 Enable IPsec(IKEv2) c	lient protocol
		DNS Servers: 10.32.	32.5
		WINS Servers:	
		Domain Name: graydn	nz.org

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**.

0	O O Add Cer	tificate Matchi	ng Rule
	Configure a certificate matchin profile. The rule priority unique and assigns a priority to the ru Rules that are not mapped will	g rule and ass ly identifies th le with lower v be ignored.	ociate it with a connection ne certificate matching rule alues having greater priority.
	Map:	💽 Existing	DefaultCertificateMap 🛟
		O New	
	Priority:	10	
	Mapped to Connection Profile:	NGE-RAS-\	/PN 🗧
	Help	Cancel	ОК

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**.

0 0		Add Certifica	te Matching	Rule Criterion			
Configure a	a certificate m	atching rule criterion					
Rule Priorit Mapped to	y: Connection Pr	10 ofile: NGE-RAS-VPN					
Field Issuer	•	Component Common Name (CN)	•	Operator Contains	•	Value gravsubca1	
		Help	Cancel	ОК			

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 ipsecproposal 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

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 2100000002ce552a1b3388eae100000000002
308202a5 3082022b a0030201 02021321 00000002 ce552a1b 3388eae1 00000000
quit

certificate 5c00000037b5a1afb01899c7f00000000000

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**.
- 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.
- 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.

- 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.

- 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

 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.
- 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.

- 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.
- 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"



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.

.	Certificate	Templates Conso	le	_ D X
File Action View Help				
🗢 🌳 🔲 🗎 🗟 🖬				
Certificate Templates (FlexVPNS)	Template Display Name	Schema Version	Versi Inten	Actions
	Administrator	1	4.1	Certificate Templates (Elev\/P
	Authenticated Session	1	3.1	Mars Artises
	Basic EFS	1	3.1	More Actions
	🗷 CA Exchange	2	106.0 Privat	IPSec (Offline request)
	CEP Encryption	1	4.1	More Actions
	🐵 Code Signing	1	3.1	More Actions
	🐵 Computer	1	5.1	
	Cross Certification Authority	2	105.0	
	Directory Email Replication	2	115.0 Direct	
	Domain Controller	1	4.1	
	Domain Controller Authentication	2	110.0 Client	
	I EFS Recovery Agent	1	6.1	
	Enrollment Agent	1	4.1	
	Enrollment Agent (Computer)	1	5.1	
	🗵 Exchange Enrollment Agent (Offline requ	. 1	4.1	
	Exchange Signature Only	1	6.1	
	Exchange User	1	7.1	
	IPSec	1	8.1	
	IPSec (Offline request)	1	D. F. I. T. I.I.	
	Kerberos Authentication	2	Duplicate Template	
	Key Recovery Agent	2	All Tasks	•
	OCSP Response Signing	3	Properties	
	RAS and IAS Server	2	Usta	
	Root Certification Authority	1	нер	
	Router (Offline request)	1	4.1	
	Smartcard Logon	1	6.1	
	Smartcard User	1	11.1	-
	Subordinate Certification Authority	1	5.1	
	Regional Trust List Signing	1	3.1	
	🚇 User	1	3.1	
< III >	< 111		>	
Opens the properties dialog box for th	he current selection.			

 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.

Subject Name Server Issuance Requirements Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Certification Authority Image: Version Server 2012 R2 V Windows 7 / Server 2008 R2 V	Properties of New Template							
Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Compatibility Settings Image: Compatibility Settings Certification Authority Image: Vertificate recipient Image: Vertificate recipient Windows 7 / Server 2008 R2 ✓ Image: Vertificate recipient	Subject Name Server Issuance Requirements							
Compatibility General Request Handling Coptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Compatibility Settings Compatibility Settings Certification Authority Windows Server 2012 R2 ✓ Certificate recipient Image: Vertificate recipient	Superseded Templa	ates	Exte	ensions	Security			
The template options available are based on the earliest operating system versions set in Compatibility Settings. ✓ Show resulting changes Compatibility Settings Certification Authority Windows Server 2012 R2 Certificate recipient Windows 7 / Server 2008 R2 ✓	Compatibility General	Request	Handling	Cryptography	Key Attestation			
Show resulting changes Compatibility Settings Certification Authority Windows Server 2012 R2 Certificate recipient Windows 7 / Server 2008 R2	The template options available are based on the earliest operating system versions set in Compatibility Settings.							
Compatibility Settings Certification Authority Windows Server 2012 R2 v Certificate recipient Windows 7 / Server 2008 R2 v	Show resulting char	nges						
Lettrication Automy Windows Server 2012 R2 Cettricate recipient Windows 7 / Server 2008 R2	Compatibility Settings							
Windows Server 2012 R2 V Cettificate recipient Windows 7 / Server 2008 R2 V	Certification Authority	у						
Certificate recipient Windows 7 / Server 2008 R2 v	Windows Server 20)12 R2		~				
Windows 7 / Server 2008 R2 V	Certificate recipient							
	Windows 7 / Server 2008 R2 V							
These settings may not prevent earlier operating systems from using this template.								

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.

Properties of New Template						
Subject Name	Server	Issu	uance Re	quirements		
Superseded Temp	lates	Extensions		Security		
Compatibility General	Request Han	dling Crypto	graphy	Key Attestation		
Template display name						
NGEASA	·.					
Machon						
Template name:						
NGEASA						
NGE/G/						
Validity period:	R	enewal period:				
2 vears	v	6 weeks	~			
Publish certificate i	n Active Directo	iry				
Do not automat	ically reenroll if a	a duplicate cer	rtificate ex	dists in Active		
Directory						
OK	C		la a bi	Ush		
OK	Cano	P	(ppiy	нер		

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

Properties of New Template								
Subject Name Server Issuance Requirements								
Superseded Templa	tes	es Extensions			Security			
Compatibility General	ompatibility General Request Handling Cryptography Key Attestation							
Purpose: Signature and encryption Delete revoked or expired certificates (do not archive)								
	bive eubie	et's energy	ntion private	e ev				
Authorize additional service accounts to access the private key (*) Key Permissions Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created								
Do the following when the subject is enrolled and when the private key associated with this certificate is used:								
Enroll subject without requiring any user input								
O Prompt the user during enrollment								
\bigcirc Prompt the user during enrollment and require user input when the private key is used								
* Control is disabled due	* Control is disabled due to <u>compatibility settings.</u>							
ОК	(Cancel	Apply		Help			

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.

Properties of New Template ×						
Subject Name	Server	Issuance R	equirements			
Superseded Templates	Ext	ensions	Security			
Compatibility General Re	quest Handling	Cryptography	Key Attestation			
Provider Category:	Key Storage	Provider	~			
Algorithm name:	ECDH P384		~			
Minimum key size:	384					
Choose which cryptographi	c providers can	be used for requ	ests			
Requests can use any p	provider availab	le on the subject'	s computer			
 Requests must use one 	of the following	providers:				
Providers:						
Microsoft Software Key Microsoft Smart Card Ke	Storage Provide sy Storage Provi	er der				
			₽			
Request hash:	SHA384		~			
Use alternate signature	format					
ОК	Cancel	Apply	Help			

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**.

Subject Name Server Issuance Requirements Compatibility General Request Handling Cryptography Key Attesta Superseded Templates Extensions Security Group or user names: Authenticated Users administrator Authenticated Users administrator Bomain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Madd Remove Permissions for administrator Aldow Deny Full Control Image: Ima	Pro	perties	of New	Template			
Compatibility General Request Handling Cryptography Key Attesta Superseded Templates Extensions Security Group or user names: Authenticated Users administrator Security & Domain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Enterprise Administrator Aldout Remove Permissions for administrator Allow Deny Full Control Image: Control Image: Control Read Image: Control Image: Control Autoenroll Image: Control Image: Control For special permissions or advanced settings, click Advanced	Subject Name	Ser	ver	Issuance F	Requirements		
Superseded Templates Extensions Security Group or user names: Authenticated Users administrator Domain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Add Remove Permissions for administrator Allow Deny Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced. Advanced	Compatibility General	Request	Handling	Cryptography	Key Attestation		
Group or user names: Authenticated Users administrator Domain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Add Remove Permissions for administrator Add Remove Permissions for administrator Add Remove Permissions for administrator Add Permissions for administrator Add Permissions for administrator Add Permissions or advanced settings, click Advanced.	Superseded Templates Extensions Security						
Authenticated Users administrator Domain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Add Remove Permissions for administrator Allow Deny Full Control	Group or user names:						
Image: Second stress Advanced Image: Second stress Advanced Image: Second stress Advanced	& Authenticated Use	ers					
Bomain Admins (GRAYDMZ\Domain Admins) Enterprise Admins (GRAYDMZ\Enterprise Admins) Add Remove Permissions for administrator Allow For special permissions or advanced settings, click Advanced	👗 administrator						
Add Remove Permissions for administrator Allow Deny Full Control Image: Control Image: Control Read Image: Control Image: Control Write Image: Control Image: Control Enroll Image: Control Image: Control Autoenroll Image: Control Image: Control For special permissions or advanced settings, click Advanced	& Domain Admins (G	RAYDMZ	\Domain /	Admins)			
Add Remove Pemissions for administrator Allow Deny Full Control Read Write Enroll Autoenroll For special pemissions or advanced settings, click Advanced Advanced							
Add Remove Permissions for administrator Allow Deny Full Control							
Permissions for administrator Allow Deny Full Control				Add	Remove		
Full Control Image: Control Cont	Permissions for adminis	trator		Allow	Deny		
Read Image: Constraint of the second settings, click Write Image: Constraint of the second settings, click For special permissions or advanced settings, click Advanced	Full Control						
Write Image: Constraint of the second settings, click Autoenroll Image: Constraint of the second settings, click Advanced. Advanced	Read			\checkmark			
Enroll Autoenroll For special pemissions or advanced settings, click Advanced.	Write			\checkmark			
Autoenroll	Enroll						
For special pemissions or advanced settings, click Advanced	Autoenroll						
For special permissions or advanced settings, click Advanced							
For special permissions or advanced settings, click Advanced							
Advanced.	For special permissions	or advanc	ed setting	s click			
	Advanced.		iou ootang	e, sion	Advanced		
OK Cancel Apply Help	OK		Cancel	Apply	Help		

 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.

Properties of New Template							
Subject Name Server Issuance Requirements							
Compatibility General	Request	Handling	Key Attestation				
Superseded Templates Extensions Security							
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Extensions Constraints Certificate Template Information Issuance Policies Key Usage							
Description of Application	on Policie:	s.		Edit			
Description of Application Policies:							
ОК	(Cancel	Apply	Help			

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.

	Properties of New Template						
Subject Name Server Issuance Requirements							
Compatibility	General	Request	Handling	Cryptography	Key Attesta	tion	
Supersed	led Templa	ites	Ext	ensions	Security		
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage							
Description of	of Key Usag	je:			Edit		
Description of Key Usage: Signature requirements: Digital signature Allow key exchange without key encryption Critical extension.							
[ОК		Cancel	Apply	Help		

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.

Properties of New Template X						
Compatibility General	Request I	Handling	Cryptography	Key Attestation		
Superseded Templa	ates	Exte	ensions	Security		
Subject Name	Serv	er	Issuance R	equirements		
Require the following fo	or enrollmen	t:				
CA certificate mana	ger approva	al				
This number of auth	orized signa	atures:	0			
If you require more	than one si	ignature, a	autoenrollment is	not allowed.		
Policy type required	l in signatur	e:				
				~		
Application policy:						
				~		
Issuance policies:						
				Add		
				Remove		
				Nemove		
Require the following fo	or reenrollme	ent:				
Same criteria as for	enrollment					
O Valid existing certific	ate					
Allow key based	renewal (")				
Requires subject in request.	formation to	be provid	ded within the ce	rtificate		
* Control is disabled du	e to <u>compa</u>	tibility setti	ings.			
ОК	С	ancel	Apply	Help		

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**.

Prop	perties	of New	Template	x			
Compatibility General	Request	Handling	Cryptography	Key Attestation			
Superseded Templa	tes	Ext	ensions	Security			
Subject Name	Ser	ver	Issuance	Requirements			
Supply in the request Use subject infor	t mation fro	om existin <u>o</u>	g certificates for	autoenrollment			
 Build from this Active Select this option to e simplify certificate adr 	» Directory Inforce co ministration	y information nsistency n.	on among subject	names and to			
Subject name format							
None				\sim			
Include e-mail nar	ne in subj on in alten	ect name nate subje	ct name:				
DNS name							
User principal nan	ne (UPN)						
Service principal name (SPN)							
ОК		Cancel	Apply	Help			

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.

•	Enable Certificate Templates					
Select one Certificate Template to enable on this Certification Authority. Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers. All of the certificate templates in the organization may not be available to your CA. For more information, see <u>Certificate Template Concepts</u> .						
Name		Intended Purpose	~			
IPSec (Offline re	equest)	IP security IKE intermediate				
Rerberos Auther	ntication	Client Authentication, Server Authenti	cation, Smart Card Logo			
🗷 Key Recovery A	lgent	Key Recovery Agent				
R NGEASA		Server Authentication, IP security IKE	intermediate			
Response	e Signing	OCSP Signing				
RAS and IAS Se	erver	Client Authentication, Server Authenti	cation _			
🗷 Router (Offline re	equest)	Client Authentication	=			
🗷 Smartcard Logo	n	Client Authentication, Smart Card Log	on			
🗷 Smartcard User		Secure Email, Client Authentication, S	Smart Card Logon			
R Subordinate Cer	tification Authority	<all></all>	Y			
<			>			
			OK Cancel			

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**.
- 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.

Subject i	lame	Ser	ver	Issuance Requirements		
Supersec	ded Templa	ites	Exte	insions	Security	
Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Template dis	nlav name					
NGECOMP						
NULCOM	UTEN					
Template pa	me:					
INGECOMP	UTER					
Validity perio	d:		Renewa	l period:		
2 4		1			1	
4 900	10 T			wooke M		
			0	weeks V		
			0	weeks ∨		
Publish c	ertificate in	Active Dir	rectory	weeks V		
Publish c	ertificate in	Active Dir	rectory	cate certificate	exists in Active	
Publish c	ertificate in ot automatic	Active Dir cally reenro	rectory	cate certificate	exists in Active	
Publish c Do no Direct	ertificate in ot automatic tory	Active Dir cally reenro	rectory oll if a dupli	veeks V	exists in Active	
Publish c Do no Direct	ertificate in ot automatic	Active Dir	rectory oll if a dupli	veeks V	exists in Active	
Publish c	ertificate in ot automatio	Active Dir cally reenro	rectory oll if a dupli	veeks V	exists in Active	
Publish c	ertificate in automatio	Active Dir cally reenro	rectory	weeks V	exists in Active	
Publish c Do nc Direct	ertificate in ot automatio	J Active Dir cally reenro	rectory	weeks V	exists in Active	
Publish c Do nc Direct	ertificate in ot automation ory	Active Dir	rectory oll if a dupli	weeks V	exists in Active	
Publish c Do no Direct	ertificate in ot automatic tory	L Active Di	rectory	weeks V	exists in Active	

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

	Prop	perties	of New	Template	x				
Subject N	lame	Ser	ver	Issuance R	equirements				
Supersec	led Templa	tes	Exte	insions	Security				
Compatibility	General	Request	Handling	Cryptography	Key Attestation				
Purpose:	Signal	ture and e	ncryption		~				
	Delete revoked or expired certificates (do not archive)								
	Include symmetric algorithms allowed by the subject								
	Arc	hive subje	ect's encryp	tion private key					
Authorize Key Per	additional missions	service ad	ccounts to	access the priva	ite key (*)				
Allow priv	rate key to	be export	ed						
Renew w	ith the sam	e key (*)							
For auton new key	natic renew cannot be	al of smar created	t card certi	ficates, use the	existing key if a				
Do the follow associated w	ving when t vith this cer	he subjec tificate is u	t is enrolled used:	l and when the j	orivate key				
Enroll sub	ject withou	t requiring	any user i	nput					
O Prompt th	ie user duri	ng enrollm	ent						
O Prompt the private keep	ie user duri ey is used	ng enrollm	ient and re	quire user input v	when the				
* Control is d	isabled due	e to <u>comp</u>	atibility sett	ings.					
[ОК		Cancel	Apply	Help				

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.

	Prop	erties o	of New	Temp	olate		x
Subject Na	Subject Name		er	Issuance Requirement			nts
Supersede	ed Template	es	Exte	ensions Security			rity
Compatibility	General	Request I	Handling	Crypto	ography	Key Att	estation
Provider Cate	Provider Category: Key Storage Provider						
Algorithm nam	ne:	ECD	H_P384				~
Minimum key	size:	384					
Requests Requests Requests Providers: Microsoft:	can use an must use of Software Ke Smart Card	ne of the ne of the ey Storage Key Stora	aers can r r available following p e Provider age Provid	e used on the provider er	subject's	ests e compute	er
Request hash	1:	SHA	384				~
Use altem	ate signatu	re format					
	ОК	C	ancel	J	Apply	H	Help

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**.

Pro	perties	of New	Template	
Compatibility General	Request	Handling	Cryptography	Key Attestation
Subject Name	Ser	Server		lequirements
Superseded Templ	ates	Exte	ensions	Security
Group or user names:				
& Authenticated Us	ers			
👗 administrator				
🍇 Domain Admins (0	GRAYDMZ	\Domain A	Admins)	
Bomain Compute	rs (GRAYD	MZ\Doma	in Computers)	
용 Enterprise Admins	GRAYDI	MZ\Enterpr	ise Admins)	
		Γ	Add	Remove
Permissions for Domain	n Computer	5	Allow	Deny
Full Control				
Read				
Write				
Enroll			~	
Autoenroll				
For special permissions	s or advance	ced setting	s, click	Advanced
Auvanceu.				

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**.

Proj	perties	of New	Template	x
Compatibility General	Request	Handling	Cryptography	Key Attestation
Superseded Templa	tes	Exte	ensions	Security
Subject Name	Ser	ver	Issuance R	equirements
Supply in the request Use subject information of the request of	t mation fro s	om existing	certificates for a	utoenrollment
O Build from this Active	Directory	rinformatio	n	
Select this option to e simplify certificate ad	nforce co ministration	nsistency n.	among subject n	ames and to
Subject name format				
None				v
Include e-mail nar	ne in subj	ect name		
Include this informati	on in alter	nate subier	ct name:	
E-mail name				
DNS name				
User principal par	ne (UPN)			
Service principal	no (or ri)	ND		
	iame (or	n)		
ОК		Cancel	Apply	Help

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.

	NGECC	OMP	UTER P	rop	erties	y x
Su	ubject Name			Issua	ance Require	ements
General (Compatibility Req	uest	Handling	Cryptography		Key Attestation
Supersec	ded Templates	E	xtensions		Security	Server
Certificate: templates allow task:	s issued by this tem added to this list. A s permitted by certi	nplate dd or ficate	supersed nly those to s issued b	e cer empli y this	tificates issu ates whose o s template.	ed by all certificates
Certificate	templates:			Minir		ed CAs
	outer			Wind	Hows 2000	eu cha
			Ad	ld		Remove
	ОК	C	Cancel		Apply	Help

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	I, CHILD o	count:1
Tunnel-id	Local	Remote	Status	Role
4711049 RESPONDE	192.168.0.1/4500 R	10.40.40.7	7/53509	READY
Encr: AE	S-GCM, keysize: 256	, Hash: N/A	<mark>, DH Grp</mark> :	20, Auth sign:
ECDSA, Autr	<u>1</u>			
verify: EAP				
Life/Activ	e Time: 86400/388 se	ec		
Child sa: loca	al selector 0.0.0.0/0 -	255.255.2	55.255/65	535
remote	e selector 192.168.10	.1/0 - 192.1	68.10.1/6	5535
ESP sp	oi in/out: 0x54d56e/0	xd0cf1c23		
grayasavpn#	sh crypto ipsec sa			
interface: out	side			
Crypto ma	p tag: NGE-DYNAMI	<mark>C-VPN, sec</mark>	<mark>ן num: 1, l</mark>	ocal addr:
192.100.U.I				
local iden	it (addr/mask/prot/poi	rt): (0.0.0.0/	0.0.0/0/	0)
remote id	ent (addr/mask/prot/p 1/255 255 255 255/0/	port): (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:
0xFFFFFFF 0xFFFFFFF
outbound esp sas:
spi: 0xD0CF1C23 (3503234083)
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={RA, Tunnel, NAT-T-Encaps, <mark>IKEv2</mark> , }
slot: 0, conn_id: 4096, <mark>crypto-map: NGE-DYNAMIC-VPN</mark>
sa timing: remaining key lifetime (sec): 26309
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x0000000 0x0000001
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							
-	Activ	/e : C	umula	tive : Pea	ak Co	oncurren	ıt
IKEv2	:	1:	1	:	1		
IPsecOverNatT		:	1:	1:		1	
AnyConnect-Parer	ıt	:	1:	1:		1	
Totals	:	3 :	3				