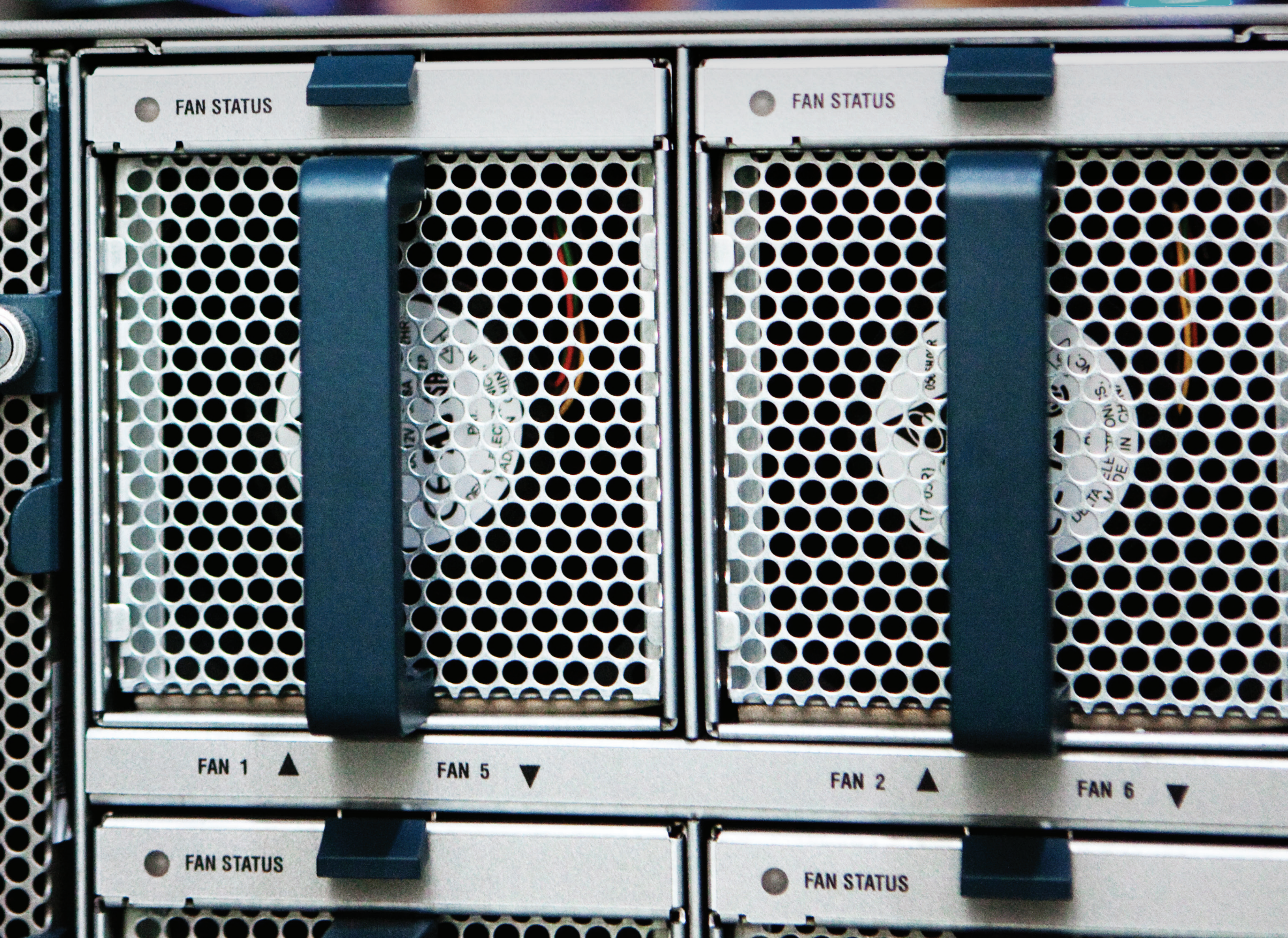
IPSec VPN Solutions Using Next Generation Encryption

Deployment Guide

Version 1.5
Authored by:
Ben Rosenblum – CCIE #21084 (R&S, SP)



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 in 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.

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.

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

COMMERCIAL IN CONFIDENCE.
A printed copy of this document is considered uncontrolled.

IPSec VPN Solutions Using Next Generation Encryption

Deployment Guide

Contents

Document Control

History

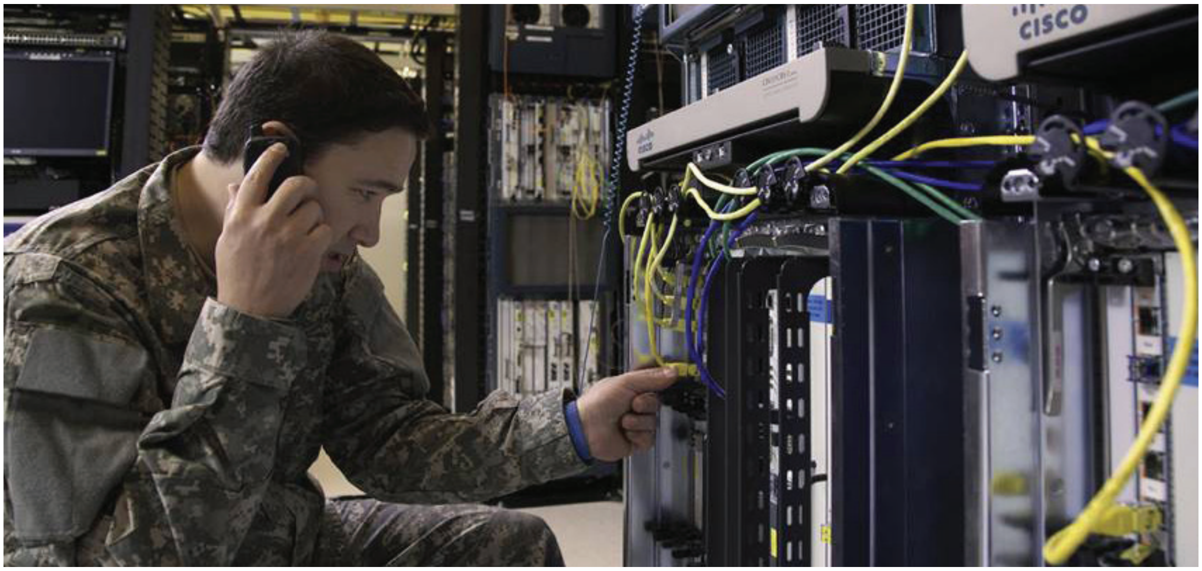
Table 1 Revision History

Version No.	Issue Date	Status	Reason for Change
1.0	4-31-2014	Initial Draft	
1.1	5-15-2014	Draft	
1.2	5-23-2014	Draft	
1.3	5-27-2014	Draft	
1.4	6-3-2014	Draft	
1.5	6-10-2014	Final	

Review

Table 2 Revision Review

Reviewer's Details	Version No.	Date
Justin Poole	1.0	May 2, 2014
Craig Hill	1.2, 1.3	May 27, 2014, June 3 2014
Andrew Benhase	1.2, 1.3	May 27, 2014, June 3 2014
Stephen Orr	1.3	June 3 2014



Executive Summary

This document provides guidance about deploying site-to-site IP Security (IPSec) VPNs using Next Generation Encryption (NGE). A subset of IPSec NGE, also known as Suite-B, is defined in RFC63791 “Suite B Cryptographic Suites for IPsec” and RFC63802 “Suite B Profile for Internet Protocol Security (IPsec)”.

RFC6380 defines two minimum levels of cryptographic security for protection of data, minLOS_128 and minLOS_192. Each of these two profiles dictates a minimum level of strength that all cryptographic algorithms must follow to be considered secure for that level of data confidentiality.

This document will describe both minLOS_128 and minLOS_192. However, all configuration examples will be done using minLOS_192. Additionally, the configuration examples will use Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) and not Advanced Encryption Standard-Galois Message Authentication Code (AES-GMAC) because AES-GMAC does not provide confidentiality of the data; only integrity.

Cisco has several platforms and operating systems that currently support NGE in both hardware and software implementations. The Cisco® Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewall, the Cisco Aggregation Services Router (ASR) 1000 Series Routers, and the Cisco Integrated Services Routers Generation 2 (ISR G2) are capable of supporting NGE in hardware and are outlined in this document. Additionally, the Cisco 5900 Series Embedded Services Routers (ESR), the Cisco Cloud Services Router (CSR) 1000v Virtual Router, and the Cisco Adaptive Security Virtual Appliance (ASAv) are capable of NGE software implementations for use in a secure cloud environment.

After a basic configuration of IPSec NGE on the platforms previously listed is discussed, this document will elaborate the multiple deployment scenarios that provide the highest level of fidelity for the data.

Introduction

This document is a combined high-level design (HLD) and low-level design (LLD) that contains detailed information on the setup and configuration of the Cisco ASA 5500-X Series, ASR1000 Series, ISR G2 Series, and 5900 Series ESR hardware platforms as well as the CSR1000v and ASAv software platforms for the deployment of a site-to-site IPSec NGE solution as described in the Executive Summary section above.

This document will also describes several secure architectures using IPSec NGE in real-world deployment scenarios. However, this document does not describe the steps required to perform device hardening. It is the responsibility of the device administrator to apply the required security configurations as dictated by their information assurance and information security teams.

Additionally, all configurations are done using static routing to illustrate that dynamic routing is not required for these deployments to function properly. However, notice that dynamic routing is fully supported in these deployments.

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

- Public Key Infrastructure (PKI) and X.509 digital certificate formats including Elliptical Curve Digital Signature Algorithm (ECDSA) and Certificate Revocation Lists (CRLs)
- Internet Key Exchange v2 (IKEv2) concepts including Elliptical Curve Diffie-Hellman (ECDH)
- IPSec Phase I and Phase II
- Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) Encryption
- Cisco ASA 5500-X Series and ASAv Next-Generation Firewalls
- Cisco ASR 1000 Series and CSR 1000v Series IOS-XE Based Routers
- Cisco ISR G2 Series IOS Routers
- LAN-to-LAN VPN connections on Cisco ASA Firewalls
- Point-to-Point Generic Routing Encapsulation (GRE) and Multipoint GRE (Dynamic Multipoint VPN [DMVPN]) tunnels on IOS Routers

It is also assumed that a PKI infrastructure capable of supporting ECDSA-signed X.509 certificates are available.

This document is not about the deployment of the PKI environment itself. However, it does enumerate requirements that the infrastructure must provide for the solution to operate correctly. Instructions on how to deploy an ECDSA PKI infrastructure based on the Microsoft Windows Server 2012 platform can be found at: cisco.com/web/strategy/docs/gov/next_generation_encryption.pdf

Document Conventions

Historically, we have always looked at data that is encrypted as two types: cipher text (CT) and plain text (PT). For purposes of this document we define them as the following:

- Plain Text (PT) – Data-in-the-Clear (No Encryption)
- Cipher Text (CT) – Encrypted data of any kind and depth
- Single-Layer Cipher Text (SLCT) – PT that has been encrypted once
- Double-Layer Cipher Text (DLCT) – PT that has been encrypted twice

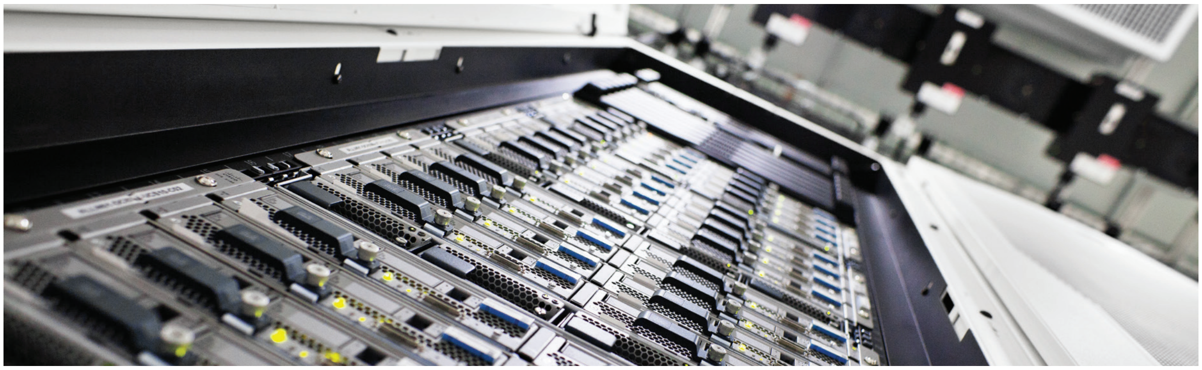
RFC6380 - Suite B Profile for Internet Protocol Security (IPsec)

As mentioned in the Executive Summary, RFC6380 dictates two minimum levels of cryptographic security for protection of data: minLOS_128 and minLOS_192. Table 1 describes the necessary minimum cryptographic algorithm strength to meet each level.

Table 1 – Minimum Cryptographic Algorithm Strength

Algorithm	minLOS_128	minLOS_192
Confidentiality (Encryption)	AES-GCM-128	AES-GCM-192
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384
Key Exchange/ Establishment	ECDH over the curve P-256 (DH Group 19)	ECDH over the curve P-384 (DH Group 20)
Integrity (Hashing)	SHA-256	SHA-384

Note: Performance testing on both the hardware and software based devices mentioned in this document show at most, a 2.5 percent performance difference when encrypting and decrypting at 128, 192, and 256 bits. Because this gap is very low, it is recommended to use 256-bit encryption instead of the 128-bit or 192-bit profiles to help ensure that the highest level of security is deployed. As mentioned in the Executive Summary, for consistency with RFC6380 all configurations will demonstrate minLOS_192.



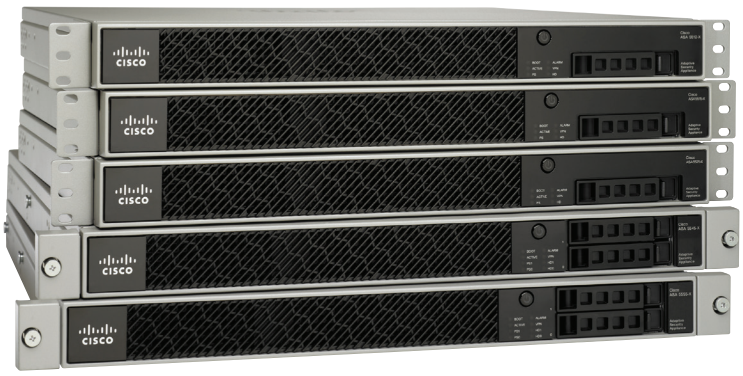
Cisco ASA Configuration

Because the ASA 5500-X Series and ASAv share a common command-line interface (CLI), the configuration for IPSec NGE is identical on both platforms. Functionally, the Cisco ASA 5500-X Series firewall has a hardware accelerator that provides for higher throughput than the software-based Cisco ASAv. The following configuration below dictates how each side should be setup so that a LAN-to-LAN IPSEC NGE VPN is created. LAN-to-LAN simply means that traffic coming from one set of IP addresses (LAN A) going to another set of IP addresses (LAN B) should be encrypted. Configuration for both sides is identical with the exception of the IP addressing being reversed.

Step 1. Define IP addressing, routing and time

```
interface GigabitEthernet0/0
  nameif CT
  security-level 0
  ip address <External-IP-Address> <External-Subnet-Mask>
!
interface GigabitEthernet0/1
nameif PT
security-level 100
ip address <Internal-IP-Address> <Internal-Subnet-Mask>
!
! A static /32 route is recommended instead of a 0.0.0.0/0 as added security
!
route CT <Remote-External-IP-Address> 255.255.255.255 <External-Default-GW> 1
route CT <CRL-Location-IP-Address> 255.255.255.255 <External-Default-GW> 1
!
! NTP is highly recommended. The clock on the ASA must be synced for the PKI
! infrastructure to work properly.
!
ntp server <NTP-Server>
```

Cisco ASA 5500-X Family



Step 2. Configure the PKI infrastructure

```
! Generate ECDSA Private Key
crypto key generate ecdsa label <Hostname>-ec elliptic-curve 384
! Root Certificate Authority
crypto ca trustpoint ROOT-CA
  revocation-check crl
  enrollment terminal
  crl configure
! Subordinate Certificate Authority
crypto ca trustpoint SUB-CA
  revocation-check crl
  enrollment terminal
  fqdn <FQDN-of-Local-ASA>
  subject-name CN=<FQDN-of-Local-ASA>
  serial-number
  ip-address <External-IP-Address>
  keypair <Hostname>-ec
  crl configure
!
! CAs must be configured to issue the id-kp-clientAuth 1.3.6.1.5.5.7.3.2 EKU
! as part of the signing request.  That EKU must be present in both the local and
! remote certificate to be utilized.
! If that EKU is not included in the certificate, you may set the ASA to ignore
! by adding the “ignore-ipsec-keyusage” command to both of the CA configurations
!
```

Step 3. Authenticate the PKI infrastructure

```
! Import the Root CA Public Key
crypto ca authenticate ROOT-CA
! ASA will reply with:
Enter the base 64 encoded CA certificate.
End with the word “quit” on a line by itself
! Paste Base-64 Encoded Certificate as follows:
-----BEGIN CERTIFICATE-----
CERTIFICATE DATA
-----END CERTIFICATE-----
quit
! ASA will reply with:
INFO: Certificate has the following attributes:
Fingerprint:     aa121d87 b020c7e8 3b1cfbb6 4bc6a181
Do you accept this certificate? [yes/no]:
! Validate that the fingerprint is correct.
! If the fingerprint is valid, type “yes” and hit enter
! Import the Subordinate CA Public Key with the same process
! NOTE: When importing the Subordinate CA, you should not be asked to
! validate the fingerprint.  This is because it is validated against the Root
! CA as a valid signed certificate.
```

Step 4. Enroll in the PKI infrastructure

```
crypto ca enroll SUB-CA
! ASA will reply with:
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=<FQDN-of-Local-ASA>

% The fully-qualified domain name in the certificate will be: <FQDN-of-Local-ASA>

% The serial number in the certificate will be: <ASA-Serial-Number>

% The IP address in the certificate is <External-IP-Address>

Display Certificate Request to terminal? [yes/no]:
! Enter “yes” at the prompt and hit enter.
! ASA will reply with:
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
CERTIFICATE SIGNING REQUEST DATA
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]:
! Enter “no” and hit enter
! Using the CSR information above, sign the certificate with the SUB-CA
! Export the signed certificate from the SUB-CA as a Base-64 encoded text file
```

Step 5. Import the signed certificate

```
crypto ca import CFUN-LWR-SBCA-2 certificate
! ASA will reply with:
% The fully-qualified domain name in the certificate will be: <FQDN-of-Local-ASA>

% The IP address in the certificate is <External-IP-Address>


Enter the base 64 encoded certificate.
End with the word “quit” on a line by itself
! Paste Base-64 Encoded Certificate as follows:
-----BEGIN CERTIFICATE-----
CERTIFICATE DATA
-----END CERTIFICATE-----
quit
! ASA will reply with:
INFO: Certificate successfully imported
```

Step 6. Validate the PKI infrastructure

```
show crypto key mypubkey ecdsa
! ASA will reply with:
Key pair was generated at: 16:32:33 EST Feb 20 2014
Key name: <Hostname>-ec
  Usage: General Purpose Key
  EC Size (bits): 384
  Key Data:

PUBLIC KEY DATA
!
show crypto ca cert
! ASA will reply with:
Certificate
  Status: Available
  Certificate Serial Number: <Local ASA Certificate Serial Number>
  Certificate Usage: Signature
  Public Key Type: ECDSA (384 bits)
  Signature Algorithm: SHA384 with ECDSA Encryption
  Issuer Name:
    cn=<SUB-CA-Hostname>
    dc=<Domain-Name>
  Subject Name:
    cn=<FQDN-of-Local-ASA>
  CRL Distribution Points:
    [1]  <SUB-CA-CRL-Location>
  Validity Date:
    start date: 12:23:57 EDT Apr 28 2014
    end   date: 12:23:57 EDT Apr 27 2016
  Associated Trustpoints: SUB-CA

CA Certificate
  Status: Available
  Certificate Serial Number: <SUB-CA Certificate Serial Number>
  Certificate Usage: Signature
  Public Key Type: ECDSA (384 bits)
  Signature Algorithm: SHA384 with ECDSA Encryption
  Issuer Name:
    cn=<ROOT-CA-Hostname>
  Subject Name:
    cn=<SUB-CA-Hostname>
    dc=<Domain-Name>
  CRL Distribution Points:
    [1]  <ROOT-CA-CRL-Location>
  Validity Date:
    start date: 15:05:19 EST Jan 27 2014
    end   date: 15:15:19 EST Jan 27 2024
  Associated Trustpoints: SUB-CA

CA Certificate
  Status: Available
  Certificate Serial Number: <ROOT-CA Certificate Serial Number>
  Certificate Usage: Signature
  Public Key Type: ECDSA (384 bits)
  Signature Algorithm: SHA384 with ECDSA Encryption
  Issuer Name:
    cn=<ROOT-CA-Hostname>
  Subject Name:
    cn=<ROOT-CA-Hostname>
  Validity Date:
    start date: 11:46:02 EST Jan 3 2014
    end   date: 11:56:02 EST Jan 3 2044
  Associated Trustpoints: ROOT-CA
```

Step 7. Configure crypto maps

```
!
!
access-list OUTER_CRYPTO_MAP_ACL extended permit ip <Internal-IP-Subnet> <Internal-Subnet-Mask> <Remote-
Internal-Subnet> <Remote-Internal-Subnet-Mask>
crypto ipsec ikev2 ipsec-proposal NGE-AES-GCM-192
  protocol esp encryption aes-gcm-192
  protocol esp integrity null
crypto map OUTER_CRYPTO_MAP 1 match address OUTER_CRYPTO_MAP_ACL
crypto map OUTER_CRYPTO_MAP 1 set peer <Remote-External-IP-Address>
crypto map OUTER_CRYPTO_MAP 1 set ikev2 ipsec-proposal NGE-AES-GCM-192
crypto map OUTER_CRYPTO_MAP 1 set trustpoint SUB-CA chain
crypto map OUTER_CRYPTO_MAP interface PT
crypto ikev2 policy 1
  encryption aes-gcm-192
  integrity null
  group 20
  prf sha384
  lifetime seconds 86400
crypto ikev2 enable PT
crypto ikev2 remote-access trustpoint SUB-CA
group-policy OUTER_CRYPTO_MAP_GPOLICY internal
group-policy OUTER_CRYPTO_MAP_GPOLICY attributes
  vpn-tunnel-protocol ikev2
tunnel-group <Remote-External-IP-Address> type ipsec-l2l
tunnel-group <Remote-External-IP-Address> general-attributes
  default-group-policy OUTER_CRYPTO_MAP_GPOLICY
tunnel-group <Remote-External-IP-Address> ipsec-attributes
  peer-id-validate nocheck
  chain
  ikev2 remote-authentication certificate
  ikev2 local-authentication certificate CFUN-LWR-SBCA-2
!
! NOTE: MTU and MSS must also be configured on the ASA. This will be discussed later in the
!     document.
!
```

Step 8. Validate crypto connectivity

```
show crypto ikev2 sa detail
! ASA will reply with:

IKEv2 SAs:

Session-id:10, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote      Status         Role
247828377    <External-IP-Address>/500    <Remote-External-IP-Address>/500       READY     INITIATOR
        Encr: AES-GCM, keysize: 192, Hash: N/A, DH Grp:20, Auth sign: ECDSA, Auth verify: ECDSA
        Life/Active Time: 86400/67 sec
        Session-id: 10
        Status Description: Negotiation done
        Local spi: 34AD6C56E1A79A8A       Remote spi: 4BF9405F181C6EA1
        Local id: <External-IP-Address>
        Remote id: <Remote-External-IP-Address>
        Local req mess id: 3              Remote req mess id: 1
        Local next mess id: 3             Remote next mess id: 1
        Local req queued: 3               Remote req queued: 1
        Local window: 1                   Remote window: 1
        DPD configured for 10 seconds, retry 2
        NAT-T is not detected
Child sa: local selector  <Internal-IP-Subnet>/0 - <End-Internal-IP-Subnet>/65535
        remote selector <Remote-Internal-Subnet>/0 - <End-Remote-Internal-Subnet>/65535
        ESP spi in/out: 0x6838b843/0x2ba7ba8d
        AH spi in/out: 0x0/0x0
        CPI in/out: 0x0/0x0
        Encr: AES-GCM, keysize: 192, esp_hmac: N/A
        ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

show crypto ipsec sa detail
! ASA will reply with:

interface: CT
    Crypto map tag: OUTER_CRYPTO_MAP, seq num: 1, local addr: <External-IP-Address>

    access-list OUTER_CRYPTO_MAP_ACL extended permit ip <Internal-IP-Subnet> <Internal-Subnet-Mask>
    <Remote-Internal-Subnet> <Remote-Internal-Subnet-Mask>
    local ident (addr/mask/prot/port): (<Internal-IP-Subnet>/<Internal-Subnet-Mask>/0/0)
    remote ident (addr/mask/prot/port): (<Remote-Internal-Subnet>/<Remote-Internal-Subnet-Mask>/0/0)
    current_peer: <Remote-External-IP-Address>


    #pkts encaps: 1020, #pkts encrypt: 1020, #pkts digest: 1020
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 1020, #pkts comp failed: 0, #pkts decomp failed: 0
```

Step 8. Validate crypto connectivity (cont.)

```
  #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
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts invalid pad (rcv): 0,
  #pkts invalid ip version (rcv): 0,
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: <External-IP-Address>/500, remote crypto endpt.: <Remote-External-IP-Address>/500
  path mtu 1500, ipsec overhead 55(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: 2BA7BA8D
  current inbound spi : 6838B843

  inbound esp sas:
    spi: 0x6838B843 (1748547651)
      transform: esp-aes-gcm-192 esp-null-hmac no compression
      in use settings ={L2L, Tunnel, IKEv2, }
      slot: 0, conn_id: 512000, crypto-map: OUTER_CRYPTO_MAP
      sa timing: remaining key lifetime (kB/sec): (4193280/28776)
      IV size: 8 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
  outbound esp sas:
    spi: 0x2BA7BA8D (732412557)
      transform: esp-aes-gcm-192 esp-null-hmac no compression
      in use settings ={L2L, Tunnel, IKEv2, }
      slot: 0, conn_id: 512000, crypto-map: OUTER_CRYPTO_MAP
      sa timing: remaining key lifetime (kB/sec): (4239260/28776)
      IV size: 8 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
!
! NOTE: Crypto will only establish on demand.  It may be necessary to send a ping through from the
! Internal-IP-Subnet to the Remote-Internal-IP-Subnet for the session to come up.
!
```

Cisco IOS and IOS-XE Configuration

Because Cisco IOS and IOS-XE Software share a common CLI, configuration for IPSec NGE is identical on both operating systems. This configuration covers all Cisco IOS and IOS-XE platforms including the Cisco ASR 1000 Series, Cisco CSR 1000v, Cisco 5900 Series ESR, and Cisco ISR G2. The following configuration determines how each side should is set up to establish both a point-to-point and Multipoint (DMVPN) IPSec NGE GRE Tunnel. PKI configuration is the same for both deployments. For the point-to-point configuration, both sides are identical with the exception of the IP addressing being reversed. For the multipoint configuration, the hub and spoke will have different configuration.

Basic Router and PKI Configuration

Step 1. Define virtual routing and forwarding (VRFs), IP addressing, routing and time

```
vrf definition CT
  rd 2:1
  !
  address-family ipv4
  exit-address-family
  !
!
vrf definition PT
  rd 1:1
  !
  address-family ipv4
  exit-address-family
  !
!
interface GigabitEthernet0/0/0
  description PT
  vrf forwarding PT
  ip address <External-IP-Address> <External-Subnet-Mask>
  negotiation auto
!
interface GigabitEthernet0/0/1
  description CT
  vrf forwarding CT
  ip address <Internal-IP-Address> <Internal-Subnet-Mask>
  negotiation auto
!
!
! A static /32 route is recommended instead of a 0.0.0.0/0 as added security
!
ip route vrf CT <Remote-External-IP-Address> 255.255.255.255 <External-Default-GW>
ip route vrf CT <CRL-Location-IP-Address> 255.255.255.255 <External-Default-GW>
!
! If the IOS device is used as the inner layer, an additional static route must be added
! for the remote side PT subnet.
!
ip route vrf PT <Remote-Internal-IP-Subnet> <Remote-Internal-Subnet-Mask> <Remote-Tunnel-IP-Address>
!
! If the IOS device is used as the outer layer, an additional static route must be added
! for the remote side inner layer IP addresses.
!
ip route vrf PT <Remote-Inner-IP-Address> 255.255.255.255 <Remote-Tunnel-IP-Address>
!
! NTP is highly recommended.  The clock on the router must be synced for the PKI
! infrastructure to work properly.
!
ntp server vrf PT <NTP-Server>
```

Step 2. Configure the PKI infrastructure

```
crypto key generate ec keysize 384 label <Hostname>-ec
!
crypto pki trustpoint ROOT-CA
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint SUB-CA
  enrollment terminal
  serial-number none
  ip-address none
  subject-name CN=<FQDN-of-Local-Router>
  vrf PT
  revocation-check crl
  eckeypair <Hostname>-ec
!
ip host vrf PT <CRL-Location> <CRL-Location-IP-Address>
!
```

Step 3. Authenticate the PKI infrastructure

```
crypto pki authenticate ROOT-CA
! Router will reply with:

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

! Paste Base-64 Encoded Certificate as follows:
-----BEGIN CERTIFICATE-----
CERTIFICATE DATA
-----END CERTIFICATE-----
quit
! Router will reply with:
Certificate has the following attributes:
    Fingerprint MD5: CDF658B7 68598060 B4AC374E 120D91CB
    Fingerprint SHA1: 3C1059CE E3159BBB BF315EE8 E9FE25D7 40E74CE8

% Do you accept this certificate? [yes/no]:
! Validate that the fingerprint is correct.
! If the fingerprint is valid, type "yes" and hit enter
! Import the Subordinate CA Public Key with the same process
! NOTE: When importing the Subordinate CA, you should not be asked to
! validate the fingerprint.  This is because it is validated against the Root
! CA as a valid signed certificate.  It will instead say:
! "Certificate validated - Signed by existing trustpoint CA certificate."

! Router will reply with:
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Step 4. Enroll in the PKI infrastructure

```
crypto pki enroll SUB-CA
! Router will reply with:
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=<FQDN-of-Local-Router>
% The subject name in the certificate will include: <FQDN-of-Local-Router>
Display Certificate Request to terminal? [yes/no]:
! Enter “yes” at the prompt and hit enter.
! Router will reply with:

Certificate Request follows:

CERTIFICATE SIGNING REQUEST DATA

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
! Enter “no” and hit enter
! Using the CSR information above, sign the certificate with the SUB-CA
! Export the signed certificate from the SUB-CA as a Base-64 encoded text file
```

Step 5. Import the signed certificate

```
crypto pki import SUB-CA certificate
! Router will reply with:

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
! Paste Base-64 Encoded Certificate as follows:

-----BEGIN CERTIFICATE-----
CERTIFICATE DATA
-----END CERTIFICATE-----
quit

! Router will reply with:
% Router Certificate successfully imported
```

Step 6. Validate the PKI infrastructure

```
show crypto key mypubkey ec
! Router will reply with:

% Key pair was generated at: 04:23:48 EST Jan 27 2014
Key name: <Hostname>-ec
Key type: EC KEYS
    Storage Device: private-config
    Usage: Signature Key
    Key is not exportable. Redundancy enabled.
    Key Data:
        PUBLIC KEY DATA

show crypto pki certificates verbose
! Router will reply with:

Certificate
    Status: Available
    Version: 3
    Certificate Serial Number (hex): <Local Router Certificate Serial Number>
    Certificate Usage: Signature
    Issuer:
        cn=<SUB-CA-Hostname>
        dc=<Domain-Name>
    Subject:
        Name: <FQDN-of-Local-Router>
        cn=<FQDN-of-Local-Router>
    CRL Distribution Points:
        <SUB-CA-CRL-Location>
    Validity Date:
        start date: 20:29:20 EDT Apr 28 2014
        end   date: 20:29:20 EDT Apr 27 2016
    Subject Key Info:
        Public Key Algorithm: rsaEncryption
        EC Public Key:  (384 bit)
    Signature Algorithm: SHA384 with ECDSA
    Fingerprint MD5: 0EBBD652 80A34954 E6459D78 A792BA0B
    Fingerprint SHA1: EA140FDA CD8ADCCE 2B0930E3 8F914FBB 7B00CB53
    X509v3 extensions:
        X509v3 Key Usage: 88000000
            Digital Signature
            Key Agreement
    X509v3 Subject Key ID: 4DA43928 AED7A775 352306F3 0F60AE68 A0EFFE26
    X509v3 Authority Key ID: 5DACCDD7 9BE1CDBA 82A641A2 4D794FD6 81E9056E
    Authority Info Access:
    Extended Key Usage:
        1.3.6.1.5.5.8.2.2
        Server Auth
        IPSEC Tunnel
        IPSEC User
        IPSEC End System
        Client Auth
    Associated Trustpoints: SUB-CA
    Storage: nvram:SUB-CA#1.cer
```

Step 6. Validate the PKI infrastructure (cont.)

```
Key Label: <Hostname>-ec
Key storage device: private config

CA Certificate
  Statust: Available
  Version: 3
  Certificate Serial Number (hex): <SUB-CA Certificate Serial Number>
  Certificate Usage: Signature
  Issuer:
    cn=<ROOT-CA-Hostname>
  Subject:
    cn=<SUB-CA-Hostname>
    dc=<Domain-Name>
  CRL Distribution Points:
    <SUB-CA-CRL-Location>
  Validity Date:
    start date: 10:28:54 EST Jan 27 2014
    end   date: 10:38:54 EST Jan 27 2024
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    EC Public Key:  (384 bit)
  Signature Algorithm: SHA384 with ECDSA
  Fingerprint MD5: C397A221 36E589BE 7B6C2655 A08CFDB5
  Fingerprint SHA1: 0F6DB06B ABDF0ADE E240F8B2 55DC3866 6BF3F0DC
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 5DACCDD7 9BE1CDBA 82A641A2 4D794FD6 81E9056E
    X509v3 Basic Constraints:
      CA: TRUE
    X509v3 Authority Key ID: B727A753 22D629B9 DC664AA3 D67C9961 37CC70EF
  Authority Info Access:
  Associated Trustpoints: SUB-CA
  Storage: nvram:SUB-CA#2CA.cer

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): <ROOT-CA Certificate Serial Number>
  Certificate Usage: Signature
  Issuer:
    cn=<ROOT-CA-Hostname>
  Subject:
    cn=<ROOT-CA-Hostname>
  Validity Date:
    start date: 11:46:02 EST Jan 3 2014
    end   date: 05:27:46 EST Nov 28 1907
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    EC Public Key:  (384 bit)
  Signature Algorithm: SHA384 with ECDSA
  Fingerprint MD5: CDF658B7 68598060 B4AC374E 120D91CB
  Fingerprint SHA1: 3C1059CE E3159BBB BF315EE8 E9FE25D7 40E74CE8
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: B727A753 22D629B9 DC664AA3 D67C9961 37CC70EF
    X509v3 Basic Constraints:
      CA: TRUE
  Authority Info Access:
Associated Trustpoints: ROOT-CA
Storage: nvram:ROOT-CA#D426CA.cer
```

Step 7. Configure crypto

```
crypto ikev2 proposal NGC-IKEv2
   encryption aes-cbc-192
   integrity sha384
   group 20
!
crypto ikev2 policy NGC-IKEv2-Policy
   match fvrf CT
   proposal NGC-IKEv2
!
!
crypto ikev2 profile NGC-IKE2-Profile
   match fvrf CT
   match identity remote address 0.0.0.0
   authentication remote ecdsa-sig
   authentication local ecdsa-sig
   pki trustpoint SUB-CA
!
crypto ipsec transform-set NGC-IPSEC esp-gcm 192
   mode transport
!
crypto ipsec profile NGC-PROFILE
   set transform-set NGC-IPSEC
   set ikev2-profile NGC-IKE2-Profile
!
```

Point-to-Point Tunnel Configuration

Step 1. Configure the tunnel

```
interface Tunnel101
   description PT to CT Point-to-Point
   vrf forwarding PT
   ip address <Tunnel-IP-Address> <Tunnel-Subnet-Mask>
   tunnel source GigabitEthernet0/0/0
   tunnel destination <Remote-External-IP-Address>
   tunnel mode gre
   tunnel key 101
   tunnel vrf CT
   tunnel protection ipsec profile NGC-PROFILE shared
!
! NOTE: MTU and MSS must also be configured on the tunnel. This will be discussed later in the
!       document.
!
ip route vrf PT <Remote-Internal-Subnet> <Remote-Internal-Subnet-Mask> <Remote-Tunnel-IP-Address>
!
```

Multipoint Tunnel Configuration

Step 1. Configure the hub

```
interface Tunnel101
    description PT to CT DMVPN HUB
    vrf forwarding PT
    ip address <Tunnel-IP-Address> <Tunnel-Subnet-Mask>
    no ip redirects
    ip nhrp map multicast dynamic
    ip nhrp network-id 101
    ip nhrp holdtime 500
    ip tcp adjust-mss 1360
    tunnel source GigabitEthernet0/0/0
    tunnel mode gre multipoint
    tunnel key 101
    tunnel vrf CT
    tunnel protection ipsec profile NGC-PROFILE
!
! NOTE: MTU and MSS must also be configured on the tunnel. This will be discussed later in the
!           document.
!
ip route vrf PT <Remote-Internal-Subnet> <Remote-Internal-Subnet-Mask> <Remote-Tunnel-IP-Address>
!
```

Step 2. Configure the spoke

```
interface Tunnel101
    description PT to CT DMVPN HUB
    vrf forwarding PT
    ip address <Tunnel-IP-Address> <Tunnel-Subnet-Mask>
    no ip redirects
    ip mtu 1400
    ip nhrp map multicast <Hub-External-IP-Address>
    ip nhrp map <Hub-Tunnel-IP-Address> <Hub-External-IP-Address>
    ip nhrp network-id 101
    ip nhrp nhs <Hub-Tunnel-IP-Address>
    ip nhrp server-only
    ip nhrp registration no-unique
    ip nhrp shortcut
    ip nhrp redirect
    ip tcp adjust-mss 1360
    tunnel source GigabitEthernet0/0/0
    tunnel mode gre multipoint
    tunnel key 101
    tunnel vrf CT
    tunnel protection ipsec profile NGC-PROFILE
!
! NOTE: MTU and MSS must also be configured on the tunnel. This will be discussed later in the
!           document.
!
ip route vrf PT <Remote-Internal-Subnet> <Remote-Internal-Subnet-Mask> <Hub-Tunnel-IP-Address>
!
```

Deployment Scenarios

In most real-world scenarios, it is impossible to ensure data fidelity to any degree of certainty when a single point of failure exists. We can eliminate this single point of failure by adding a second layer of encryption to the data as it moves through the network. This creates three separate security zones as opposed to the traditional two. Traditionally, we have the plain text (PT) and cipher text (CT) sides of the device. In these scenarios, we modify that to be plain text (PT), single-layer cipher text (SLCT), and double-layer cipher text (DLCT).

As the possibility of vulnerabilities existing in any operating system is high, it is recommended that each layer be generated by a separate operating system. This creates a higher statistical probability that if any vulnerability is discovered that impacts one layer of the encryption, then the second layer should still remains secure.

To accomplish this, a mixture of Cisco ASA firewalls and devices based on Cisco IOS/IOS-XE Software is recommended. It is, however, not recommended to mix the devices inside the same layer. Doing so would increases the risk of a potential breach because that layer can be compromised by any vulnerability in either side. In each of the following scenarios below, it is assumed that there are other devices between the outer VPN device within the network to handle such tasks as Border Gateway Protocol (BGP) and Internet peerings, switching, firewalling, intrusion prevention system (IPS) and intrusion detection system (IDS), etc. These devices are not depicted in the diagrams to reduce complexity.

When deploying in a high-speed environment such as within a campus network, and only the most basic connectivity is required, the Cisco ASA or the Cisco IOS/IOS-XE device can be used as the inner or outer device interchangeably. Both can provide the necessary basic routing and encryption to satisfy the needs of this document as established in the previous configurations.

At times, there may be a need to tunnel the secure traffic over GRE. Multicast is a common example of this requirement. In these use cases, the Cisco IOS/IOS-XE device is better suited as the inner device with the Cisco ASA providing the outer layer of encryption.

In use case scenarios where the outer device is also acting as a WAN router, or in environments where subrate interfaces may be present, the Cisco IOS/IOS-XE device is better suited as the outer layer device.

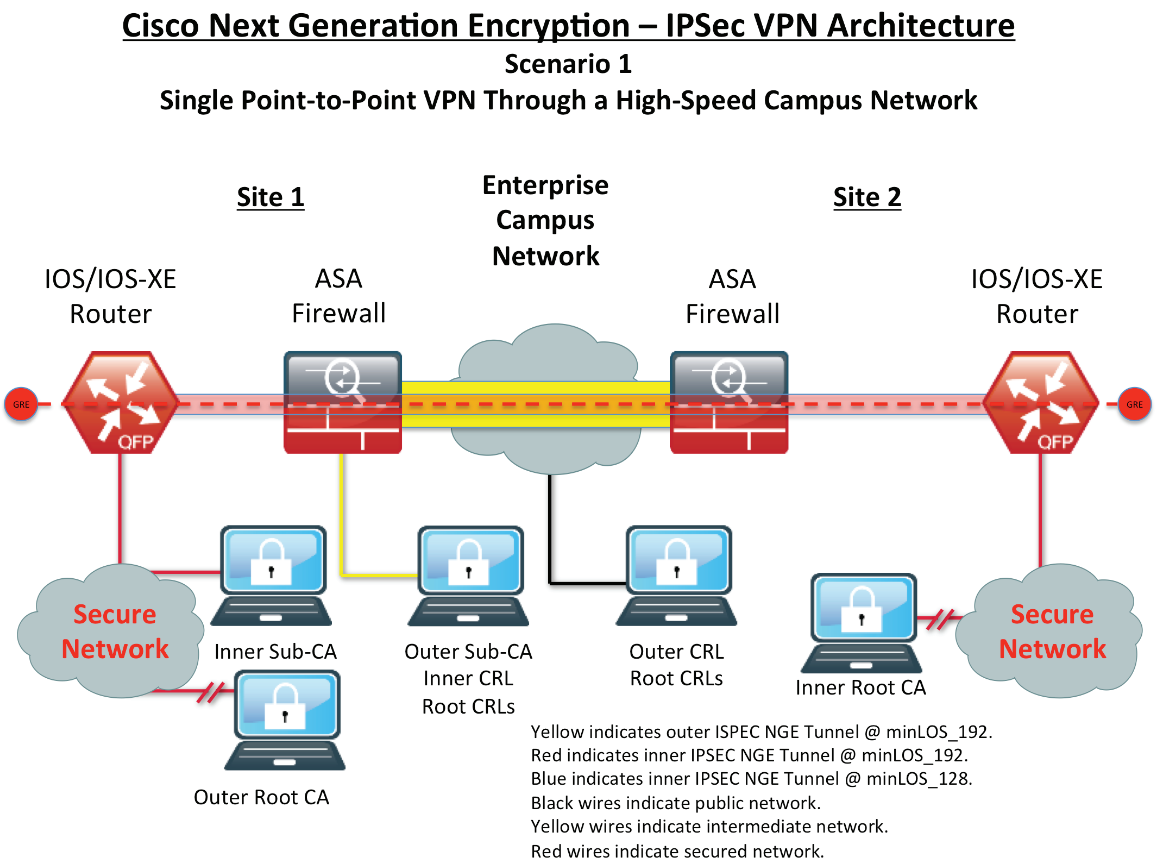
As you can see from the previous examples provided above, it is critically important to understand the anticipated traffic flows as well as the path between the two outer devices before selecting the inner and outer device types.

Cisco ASR 1000 Family

Scenario 1: Cisco IOS/IOS-XE Inner Layer and Cisco ASA Outer Layer

In many cases, the Cisco IOS feature set provides capabilities required by the secure plain text network. To facilitate this requirement, we can use the Cisco IOS/IOS-XE based devices as the inner encryption layer and the Cisco ASA based devices as the outer encryption layer as shown in figure 1.

Figure 1. Single Point-to-Point VPN Through a High-Speed Campus Network



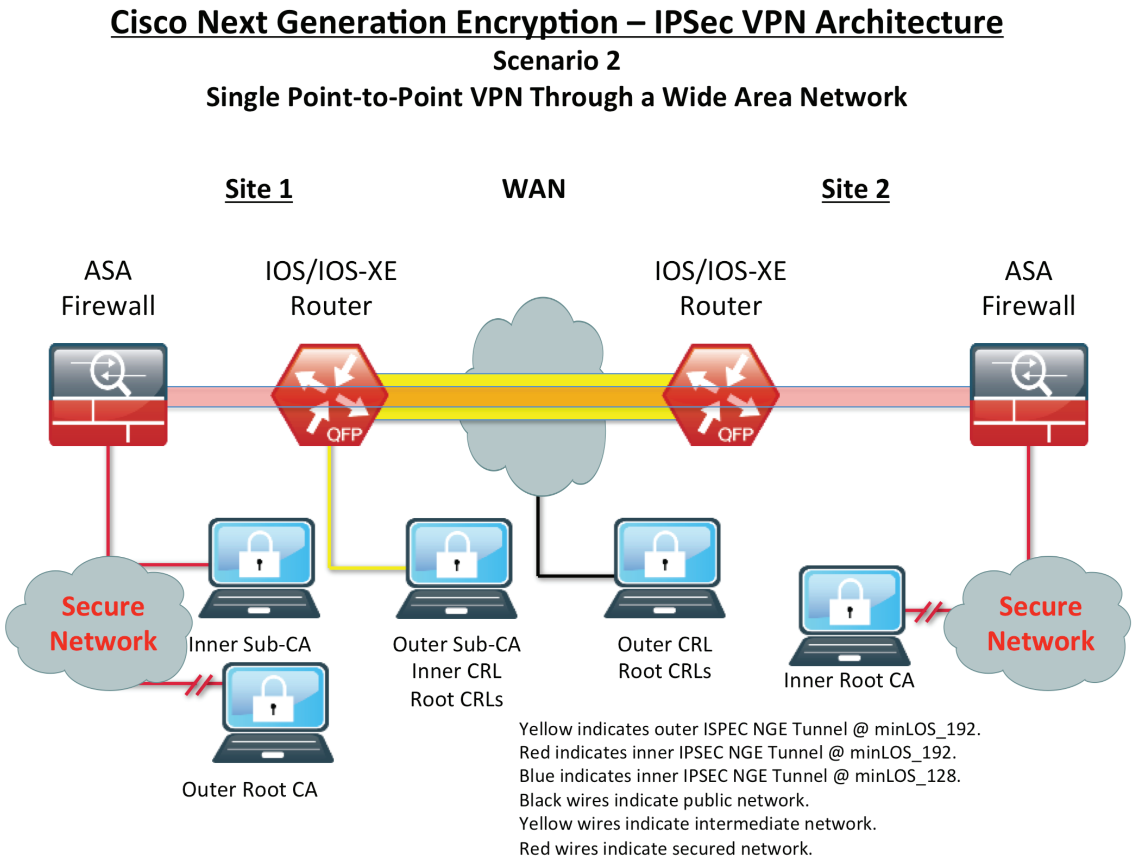
Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.

In this scenario, it is also possible to deploy a mulitpoint network by adding additional Cisco ASA firewalls. Each Cisco ASA firwall must be configured to establish secure sessions to all other Cisco ASA firewalls in a full mesh configuration. After they are established, the Cisco IOS/IOS-XE based devices will establish connections through DMVPN/IPSec to each other router. Notice that both the point-to-point and multipoint architectures are supported.

Scenario 2: Cisco ASA Inner Layer and Cisco IOS/IOS-XE Outer Layer

In an environment where the IP addressing of the outer devices can be dynamic, or where one side may be behind a layer of obscurity such as Network Address Translation (NAT), it may be preferable for the Cisco IOS/IOS-XE based devices to be on the outside (Figure 2). As long as there is one side with a known static IP address, DMVPN may be used to establish the peering. Refer to the multipoint tunnel configuration above for instructions on how to configure this outer layer.

Figure 2. Single Point-to-Point VPN Through a Wide Area Network



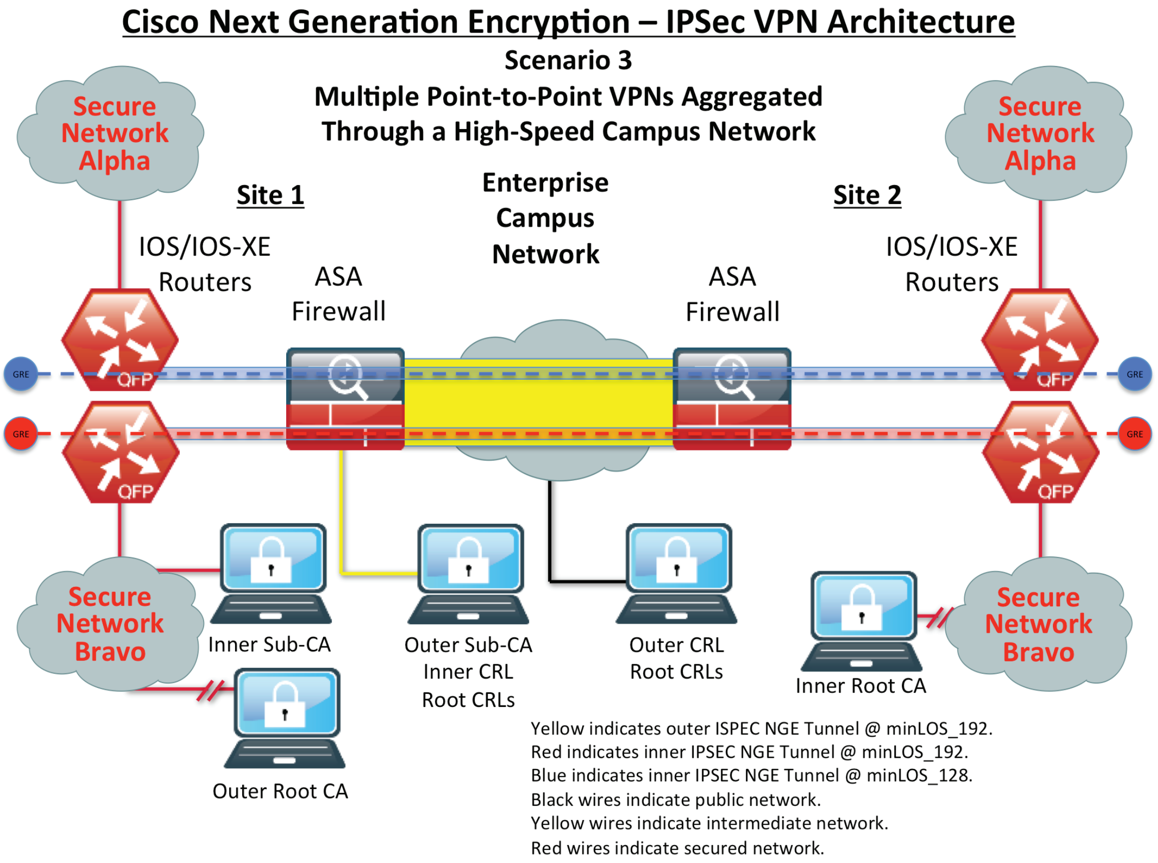
Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.

After the peering is established between the two Cisco IOS/IOS-XE routers, the Cisco ASAs can establish a peering through the known private IP addressing, which is now available through those tunnels.

Scenario 3: Cisco IOS/IOS-XE Inner Layer and Cisco ASA Outer Layer with Multiple Inner Encryption Levels

In some instances, it may be necessary to have multiple separate secure networks located at the same physical site talk to similar secure networks at a remote site. It also may be necessary for those secure networks to communicate with each other using different encryption levels. To accomplish this, both inner security layers can be tunneled through the same outer layer as long as the outer layer provides the security of the highest inner encryption level (Figure 3).

Figure 3. Multiple Point-to-Point VPNs Aggregated Through a High-Speed Campus Network



Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.

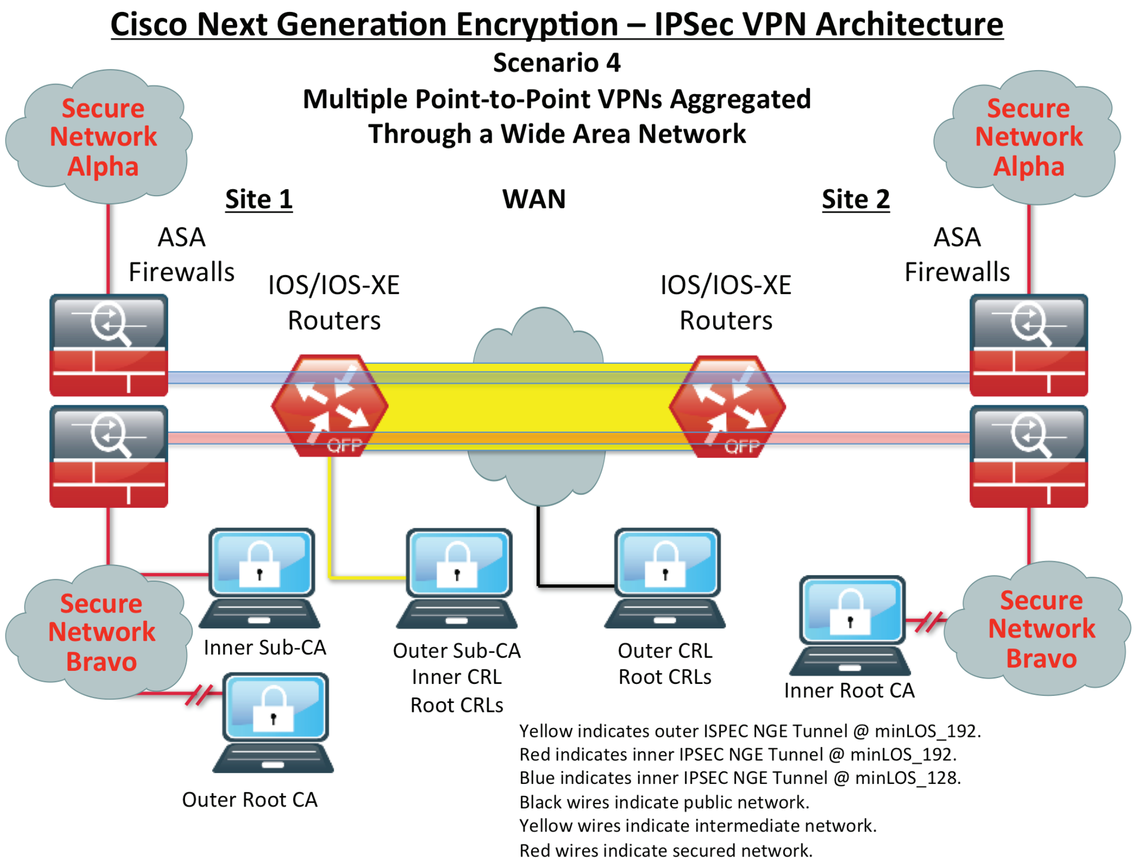
In this scenario above, the secure networks at the top of the figure require minLOS_128 and the secure networks at the bottom of the diagram require minLOS_192. To accommadate both layers, the outer tunnel is secured using minLOS_192. There are two differences in configuration on the Cisco ASA. First, an additional physical interface must be added. Second, an additional line on the OUTER_CRYPTO_MAP_ACL entry must be added to include the second inner layer. With those exceptions, configurations on both layers are identical. For added security, a third certificate authority hierarchy may be deployed to support the second inner layer so that each inner layer has it's own certificate authority hierarchy.

Scenario 4: Cisco ASA Inner Layer and Cisco IOS/IOS-XE Outer Layer with Multiple Inner Encryption Levels

Similar to Scenario 2, (with single inner Cisco ASA and single outer Cisco IOS), it may be necessary to deploy scenario 4 with multiple Cisco ASAs on the inside and a single Cisco IOS/IOS-XE platform on the outside acting as the aggregate crypto egress device.

There are two configuration changes shown in Figure 4. First, an additional interface needs to be added on the Cisco IOS/IOS-XE device. Secondly, an additional static route must be added so that the additional tunnel traffic is sent through the outer tunnel interface. With those two exceptions, all configurations are the same.

Figure 4. Multiple Point-to-Point VPNs Aggregated Through a Wide Area Newtork



Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.

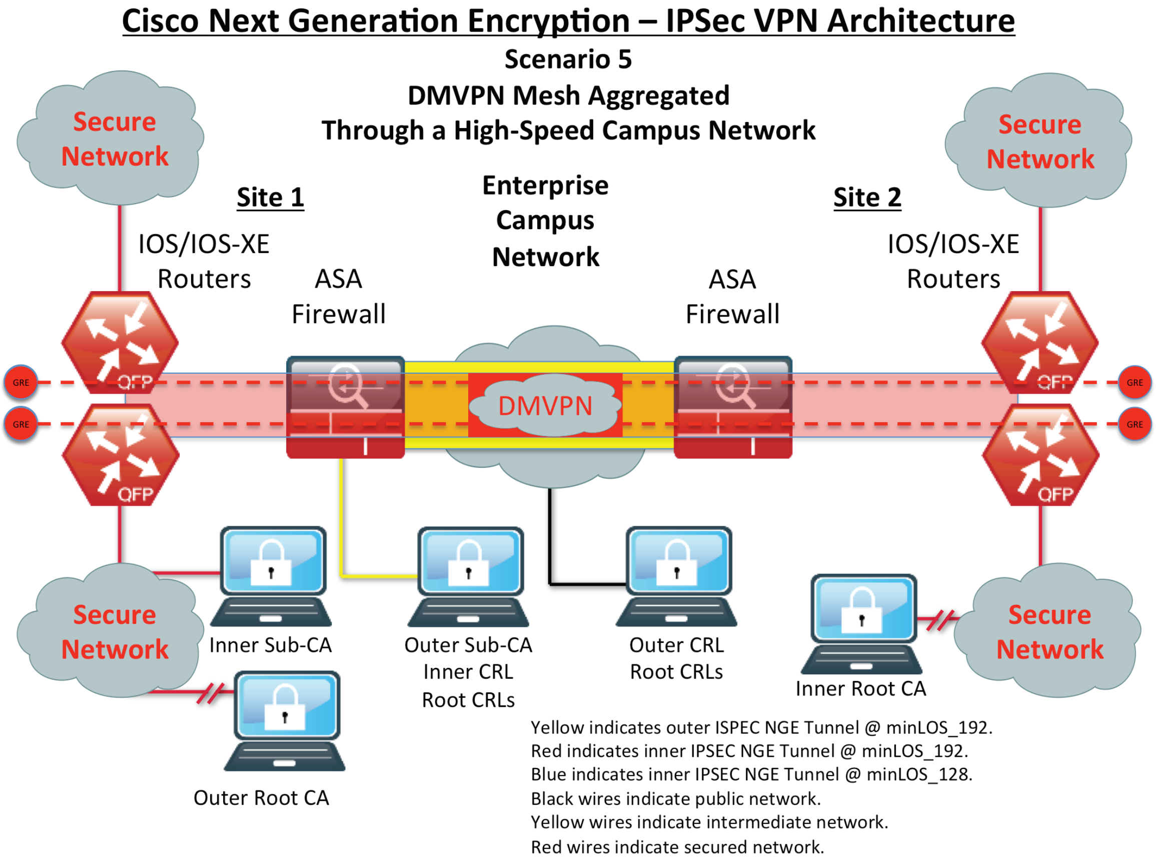
Scenario 5: Cisco IOS/IOS-XE Inner Layer and Cisco ASA Outer Layer with Multiple Inner Secure Networks at the Same Encryption Level

In scenario 5, multiple secure networks are in the same physical location, operating at the same level of encryption, but they may need to talk to each other in addition to the secure networks on the remote side.

This capability can be easily accomplished using similar methodology and configuration to the previous scenarios. Because these inner networks all exist behind the first layer of encryption, it is acceptable to only require only a single layer of encryption between the two when in the same physical location.

Configuration for the additional inner peers can be done as point-to-point or multipoint depending on the requirements of the deployment (Figure 5). As with scenarios 3 and 4, the only other additional configurations are the additional physical interface on the Cisco ASA and additions to the access control list (ACL) to accomodate the additional traffic paths.

Figure 5. DMVPN Mesh Aggregated Through a High-Speed Campus Network



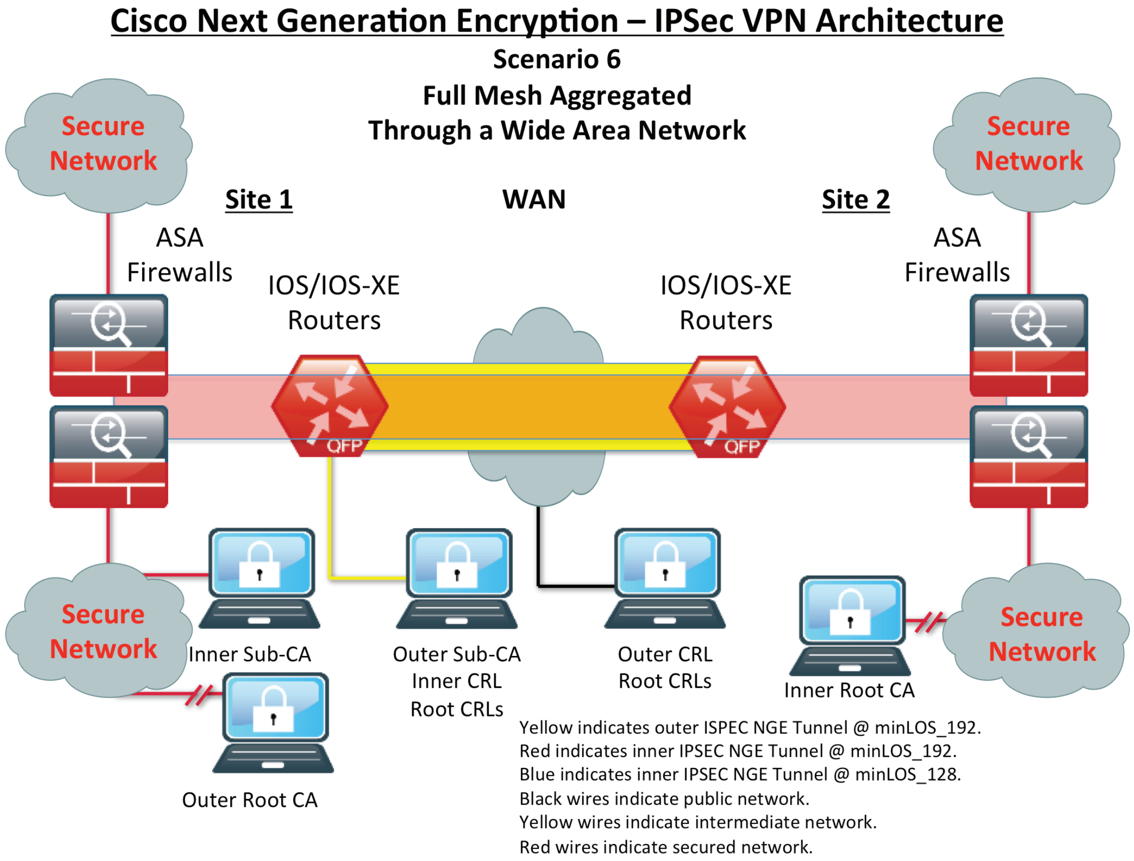
Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.

Note: Because there is a need for both on-site and remote communications, when calculating maximum transmission unit (MTU) for the inner layer always assume that the overhead for the outer layer is required. This prevents any fragmentation issues.

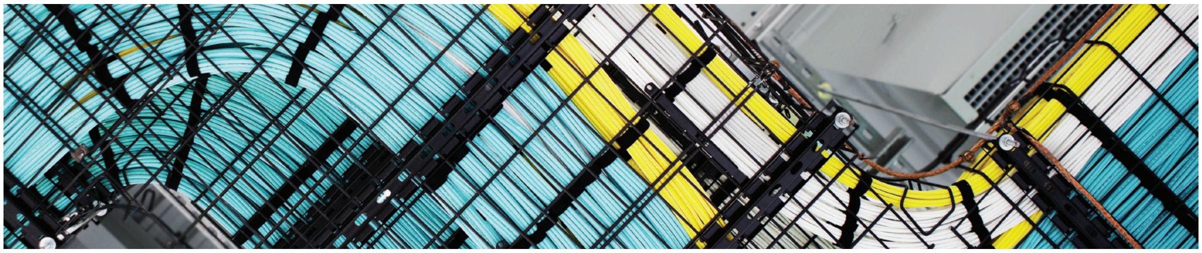
Scenario 6: Cisco ASA Inner Layer and Cisco IOS/IOS-XE Outer Layer with Multiple Inner Secure Networks at the Same Encryption Level

In scenario 6 as shown in Figure 6, similar to scenarios 2 and 4, the Cisco ASA devices are used as the inner layer. And as with scenario 5, the only additional configurations required are the additional inner peer configuration and the additional physical interface and static routes on the outer layer device.

Figure 6. Full Mesh Aggregated Through a Wide Area Network



Yellow indicates outer ISPEC NGE Tunnel @ minLOS_192.
Red indicates inner IPSEC NGE Tunnel @ minLOS_192.
Blue indicates inner IPSEC NGE Tunnel @ minLOS_128.
Black wires indicate public network.
Yellow wires indicate intermediate network.
Red wires indicate secured network.



Design Notes

Payload Maximum Transmission Unit (MTU) and TCP Maximum Segment Size (MSS)

Due to the additional packet overhead added by introducing layers of encryption, care must be taken to prevent fragmentation. If the devices are required to perform fragmentation, performance will decline rapidly. However, limiting the maximum packet size that is allowed to go through the system can prevent the potential performance decline. For the purposes of these examples, we are assuming standard 1500-byte Ethernet packets and transport mode for the IPSec profile as configured above. However, additional care must be taken if any links in the path have a lower MTU.

Scenarios 1, 3, and 5 – Cisco IOS/IOS-XE Inner Layer and Cisco ASA Outer Layer

In these scenarios, we start with the packet flow entering through the inner tunnel first. From the 1500 bytes we subtract 20 for the IP header. Another 4 bytes are then subtracted for the GRE header and 4 bytes for the GRE tunnel key. This brings us to 1472 bytes. The encapsulating security payload (ESP) header for an AES-GCM packet consists of a 4-byte Security Parameters Index (SPI), a 4-byte sequence number (SEQ), an 8-byte initialization vector (IV), a 16-byte integrity check value (ICV), and 4 bytes for the pad, pad length and next header fields. This brings the total for the ESP header is now 36 bytes. If we subtract that from the 1476 bytes previously calculated, we are left with 1436 bytes of usable payload space in the inner layer. If we apply the same math to the outer layer except starting with 1436 instead of 1500, and remove the 8 bytes we previously subtracted for the GRE headers, 1380 bytes remain (1436 – 20 – 36 = 1380).

Scenario 2, 4, and 6 – Cisco ASA Inner Layer and Cisco IOS/IOS-XE Outer Layer

The math for scenarios 2, 4 and 6 is almost identical to their pair scenarios above. Each layer still has the 20 bytes for the IP header and 36 bytes for the ESP header. The only difference is that the 8 bytes of GRE is on the outer tunnel instead of the inner tunnel. Starting at 1500 again for our inner tunnel, 1444 bytes remain (1500 – 20 – 36 = 1444). If we then apply the math with the GRE headers to the outer tunnel, 1380 bytes remain (1444 – 20 – 36 – 8 = 1380) as we expect.

Additional Overhead

It is rare to know the exact available MTU size in the path when going through a public domain. Some service providers may encapsulate traffic through their networks with technologies such as Multiprotocol Label Switching (MPLS). It is also possible that there are additional protocols enabled on the inner tunnel device that may require additional overhead space. To accommodate an average amount of overhead, we recommend reducing the available MTU from the previous 1380 bytes. The AES cipher operates most efficiently in 40-byte increments. With traditional single-tunnel GRE deployments, it is recommended to reduce the MTU from 1436 to 1400. Because 1380 sits halfway between the 1400-byte and 1360-byte efficiency boundaries, it is recommended to reduce the available MTU to 1360 bytes. This provides 20 bytes of space for any additional protocol overhead. To note, this assumes a clean 1500-byte path between the devices. If additional overhead is required, the next safe boundary that can be used is 1320 bytes.

TCP Maximum Segment Size (MSS)

After the overall available payload is calculated, we must calculate the available space to fit the original packet. This packet includes its own IP and TCP headers. To account for this, we must subtract 20 bytes for the IP header and 20 bytes for the TCP header (assuming no TCP options are in use). Using the previous recommendation of 1360 bytes, that would align the maximum segment size to 1320 bytes. If TCP options are in use, we must reduce the MSS to account for that.

Device Configuration

The MTU configuration is best applied on the inner tunnel device. Setting the limit on the inner tunnel device forces all traffic through the tunnel to maintain that size. The following examples use the previous recommendations of a 1360-byte MTU and 1320-byte MSS.

Scenarios 1, 3, and 5 - Cisco IOS/IOS-XE Inner Layer and Cisco ASA Outer Layer

```
! Added configuration on IOS/IOS-XE inner device(s)
interface Tunnel101
   ip mtu 1360
   ip tcp adjust-mss 1320
!
```

Scenarios 2, 4, and 6 - Cisco ASA Inner Layer and Cisco IOS/IOS-XE Outer Layer

```
! Added configuration on ASA inner device(s)
mtu PT 1360
sysopt connection tcpmss 1320
!
```

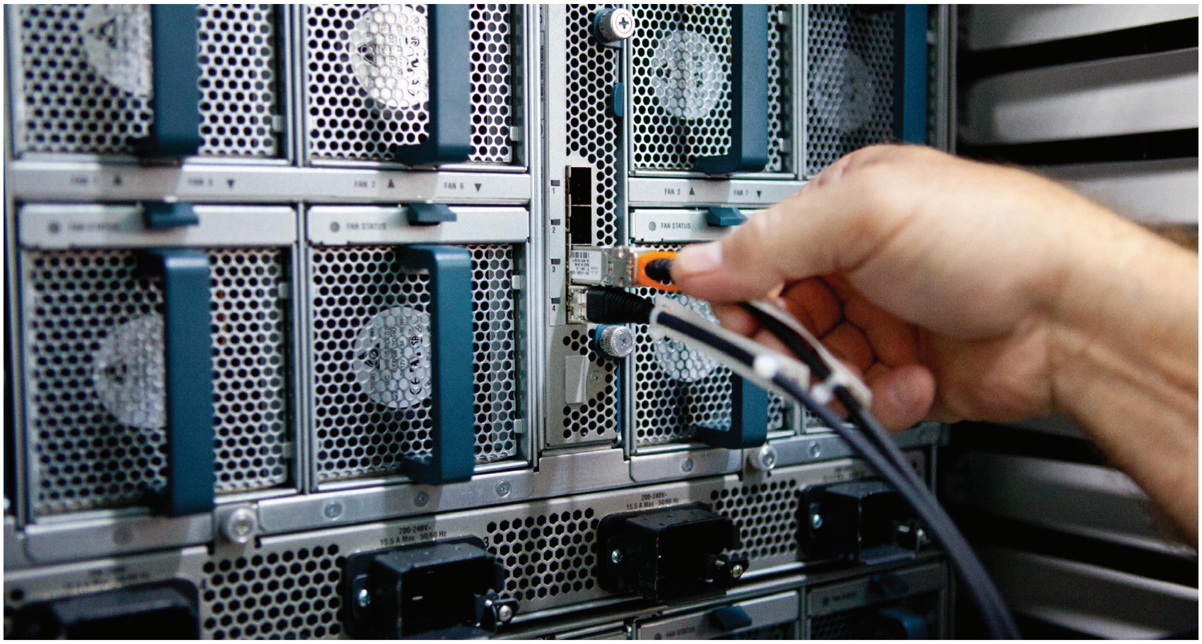
Certificate Authority Architecture

It should be noted that a properly functioning certificate authority along with the proper placement are critical elements for this architecture.

It is also recommended to have a hierarchical certificate infrastructure in place for each layer. As with all PKI infrastructures, the root is the most critical device to protect. It is critical that the root be both offline and kept physically in a high-security environment. Additionally, it is recommended that each tunnel layer have a separate subordinate certificate authority signed by the root for that layer. Using the proper configuration as shown in the scenarios prevents outer and inner devices from establishing a connection with each other.

Certificate revocation checking is also a critical component that can be deployed to help ensure that only valid devices are allowed to use VPN to reach the enclave. To help ensure that each side is able to validate the other as well as the infrastructure itself, they must be able to access the most recent copies of the CRL.

The easiest way to do this is to have the CRL for each layer published on the CT side of that layer. This approach helps ensure that both sides of the session are able to read from the same CRL and validate each other. Both scenario diagrams above depict this. For simplicity, the diagrams show both the certificate authorities and CRLs on the same device. In practice, these can and should be on different devices to reduce exposure of the certificate authority. Also note that only the CRL itself needs to live outside the secured network. The root and subordinate certificate authorities should always remain inside the secured area. As a result, a manual distribution of the CRL to the publishing point is required to help ensure that the most recent CRL is available. Additionally, when configuring the certificate authorities, the CRL URLs need to be included in the certificates themselves so that they are always published to the devices.



Virtualized Cloud Solutions

With the increase of data center services that are moved onto cloud-based solutions, security between a data center and the end-user devices must be assured.

Using the Cisco CSR1000v and the Cisco ASAv, the same level of fidelity of the data as it moves between the cloud-based services and the user can be established. Both the Cisco CSR1000v and Cisco ASAv support the complete feature set required to support all of the necessary next-generation encryption and integrity protocols as shown in the previous examples.

As always, physical security of the data needs to be ensured while it is in the clear text state. More information about secure datacenters can be found at:

cisco.com/c/en/us/solutions/enterprise-networks/secure-data-center-solution/

References

[1] Suite B Cryptographic Suites for IPsec: http://www.ietf.org/rfc/rfc6379.txt

[2] Suite B Profile for Internet Protocol Security (IPsec) http://www.ietf.org/rfc/rfc6380.txt

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**