CSfC with GNS3 Lab Guide

William John Holden

16 August 2019

Introduction

This informal document describes how import the GNS3 virutal machine (VM), install GNS3, start an Cisco IOSv router, and configure a very basic lab based on the National Security Agency's (NSA) Commerical Solutions for Classified (CSfC) Multi-Site Connectivity (MSC) Capability Package (CP) version 1.1. Configuration excerpts are provided as appendices. This CSfC lab uses only Cisco components and is therefore not a compliant solution (MSC-PS-6).

The purpose of this lab guide is not to develop an ideal CSfC scenario. Rather, the goal is to create a "sandbox" where one can experiment with VPN and PKI technologies in the context of CSfC.

This lab implements IKEv2 (MSC-VG-9) with AES-256-CBC (MSC-VG-10) and IPsec with AES-256-GCM (MSC-VG-12), authenticated over RSA 3072 or ECDSA with SHA-384, DH Group 20, with DH Group 20 PFS. IPsec is implemented with ESP in transport mode on red (MSC-IR-1) and tunnel mode on gray (MSC-OR-1). The gray network uses no dynamic routing protocol (MSC-OR-8). This lab does not show access rules on any interface (MSC-PF-5). No black, gray, or red firewalls are shown. A MSC network topology this simple would not require any firewalls. This lab does not show any IDS/IPS. Production MSC networks require at least two IDS/IPS devices (MSC-MR-1).

This lab uses a Cisco IOS router as the Certificate Authority (CA). Cisco IOS is not included on the Components List as an authorized CA product (MSC-PS-1). See `https://www.nsa.gov/Resources/Everyone/csfc/Components-List/` for products approved for use with CSfC.

The term "NGE" refers to Next Generation Encryption (`https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html`).

This lab provides several ideas that might be used as compensatory controls to harden an MSC deployment. In general, it is a safe and reasonable choice to make different network enclaves incompatible. For example, the use of different routing protocols, routing protocol authentication keys, GRE tunnel keys, native VLANs, user VLANs, and IP addresses across enclaves can minimize the impact of an unintended cross-domain connection. By contrast, two routers from different enclaves that operate compatible dynamic routing protocols will form an unintended peering if connected. The following configuration differences are used to intentionally break compatibility across gray and red:

1. The gray network uses the legacy `crypto map` syntax. The red netowrk uses the modern `tunnel protection profile` syntax.
2. The gray network authenticates IPsec peers by ECDSA key. The red network uses RSA 3072 keys.
3. Devices on the gray network present their fully-qualified domain names (FQDN) as their identities. Devices on the red network present their IP addresses as their identities.
4. The gray network has a standalone CA. The red network simulates an enterprise CA.
5. The gray network uses IPv6 Unique Local addresses in the range fd8a::/8 (see `https://tools.ietf.org/html/rfc4193`). The red network uses IPv4 Private IP Addresses in the range 192.168/16 (see `https://tools.ietf.org/html/rfc1918`).
6. Routers on the red network use a virtual routing and forwarding (VRF) instance to separate the management plane from the forwarding plane.

Contents

1 Install GNS3

1.1 Enable Intel VT-x/AMD-V

VT-x and AMD-V enable virtual machines to execute instructions directly on the host CPU. Without these technologies, virtualization is much slower as the hypervisor must simulate these instructions in software.

Restart your computer, enter the UEFI boot configuration, and enable VT-x/AMD-V.

1.2 Install VMware Player

In this lab we use VMware Worksation Player 14.1.7. Version 14 is not the newest version, but I have been more successful with GNS3 on version 14 than on newer releases.

Install VMware Workstation 14.1.7 Player from `https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0|PLAYER-1417|product_downloads`.

1.3 VMware VIX

VMware VIX is a an API that allows other programs to control VMware. VIX will expose functions that GNS3 needs to manage virtual machines running in VMware.

Install VMware VIX 1.17.0 API from `https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0|PLAYER-1417|drivers_tools`.

1.4 Npcap

Install Npcap from `https://nmap.org/npcap/#download`. Select "Install Npcap in WinPcap API-compatible Mode" and deselect "Support loopback traffic" during installation.

1.5 GNS3 VM

Download the GNS3 VM for VMware Workstation and Fusion from `https://github.com/GNS3/gns3-gui/releases/`. Extract the OVA from this ZIP. Double-click on the OVA to import the VM into VMware.

Provision the GNS3 with as many CPU cores and as much RAM as feasible.

Open VMware Player. Right-click on the GNS3 VM and click Settings. In the Hardware tab, select Processors and enable "Virtualize Intel VT-x/EPT or AMD-V/RVI."

1.6 GNS3

Install the all-in-one package for GNS3 from `https://github.com/GNS3/gns3-gui/releases/`. Configure GNS3 to use the GNS3 VM.

2 IOSv Router

2.1 `IOSv_startup_config.img`

Download `IOSv_startup_config.img` from `https://sourceforge.net/projects/gns-3/files/Qemu%20Appliances/IOSv_startup_config.img/download`.

2.2 `vios-adventerprisek9-m.vmdk.SPA.156-2.T`

Download `vios-adventerprisek9-m.vmdk.SPA.156-2.T`.

2.3 Start the GNS3 VM

Open GNS3. You may need to enable the GNS3 VM, if it does not start automatically, by selected Edit → Preferences GNS3 VM → Enable the GNS3 VM.

2.4 Create a new project

Create a new project by clicking File → New blank project.

2.5 Import the IOSv Template

Click the Router icon (four arrows) in the palette at the left side of the screen. Click "New Template" at the bottom of the palette.

Select "Install an appliance from the GNS3 server" and click Next. Expand the triangle next to Routers and select "Cisco IOSv" and click Next.

The wizard asks for Server type, but only "Install the appliance on the GNS3 VM" should be available. Click Next. Accept the default location for the Qemu binary. For each file under "IOSv version 15.6(2)T" click Import and select the downloaded dependencies. Now the router template should be available in the palette.

3 CSfC Lab

Introduction

Import six Cisco IOSv routers into the topology. Import also one switch into the topology. R2 and R5 will be used as certificate authorities. R1, R2, and R3 are members of the gray network. R4, R5, and R6 are members of the red network.

3.1 Cables

Attach cables according to the following table:

Device	Interface	Device	Interface
R1	Gi0/1	R3	Gi0/1
R1	Gi0/2	R4	Gi0/1
R3	Gi0/2	R6	Gi0/1
R4	Gi0/0	Switch	Ethernet1
R5	Gi0/0	Switch	Ethernet2
R6	Gi0/0	Switch	Ethernet3

Device R2 is intentionally not connected to anything. Turn on all devices by selecting Control → Start/Resume all nodes. Routers may take several minutes to fully boot.

3.2 Red CA

We begin with R5, the red certificate authority (CA). The CA is responsible for issuing certificates and establishing the root of trust necessary for secure authentication.

```
ip dhcp pool RED-PROVISIONING
 network 203.0.113.0 255.255.255.128

interface GigabitEthernet0/0
 ip address 203.0.113.1 255.255.255.128
 no shutdown

no ip domain-lookup
hostname R5
ip domain-name red.local

crypto pki trustpoint CA
 revocation-check crl
 subject-name CN=r5,OU=red,O=local
 rsakeypair CA-KEY 3072 3072

ip http server

crypto pki server CA
 grant auto
 hash sha384
 issuer-name CN=r5,OU=red,O=local
 lifetime certificate 14
 lifetime ca-certificate 14
 no shutdown
```

These commands are sufficient to stand up a simple CA running on Cisco IOS.

3.3 Inner Encryption Components

3.3.1 CSR

Now enter the following commands on R4 and R6 to perform a Certificate Signing Request (CSR) over Simple Certificate Enrollment Protocol (SCEP).

It is noteworthy that the clocks of IOSv devices automatically synchronize to the host operating system. This was not true of older equipment. Clock synchronization is usually a consideration for all public key infrastructure (PKI) operations. **It is generally not safe to assume clocks are synchronized from a cold start**.

```
vrf definition MANAGEMENT
 address-family ipv4

interface GigabitEthernet0/0
 vrf forwarding MANAGEMENT
 ip address dhcp
 no shutdown

interface Loopback0
 ip address 192.168.4.4 255.255.255.255
 ip ospf 1 area 4

no ip domain-lookup
hostname R4
ip domain-name red.local

crypto pki trustpoint Red-CA
 auto-enroll 50 regenerate
 revocation-check crl
 rsakeypair CSFC-KEY 3072 3072
 enrollment url http://203.0.113.1
 subject-name CN=r4,OU=red,O=local
 ip-address 192.168.4.4
 serial-number
 vrf MANAGEMENT
```

On R6 set the IP address of interface Loopback0 to 192.168.6.6/32 and the OSPF area to 6. Change the hostname to R6 and update the `crypto pki trustpoint` configuration.

Install the CA's root certificate and perform the CSR over SCEP.

```
crypto pki authenticate Red-CA

crypto pki enroll Red-CA
```

Now that each inner encryption component has a certificate we move our attention to creating a tunnel. This lab provides a simple GRE tunnel with an IPsec protection profile running OSPF. The underlay (gray) network will use IPv6.

3.3.2 IKEv2 and IPsec Configuration

The following configuration provides Internet Key Exchange (IKE) and Internet Protocol Security (IPsec).

```
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
```

```
 group 20

crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL

no crypto ikev2 policy default

crypto ikev2 profile IKEV2-PROFILE
 match identity remote address 192.168.6.6 255.255.255.255
 identity local address 192.168.4.4
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint Red-CA

crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode transport

crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE

no crypto ipsec profile default
```

3.3.3 Tunnel over gray

Finally, the inner encryption components must establish tunnels to one another. For R4:

```
ipv6 unicast-routing

ipv6 route ::/0 FD8A:1::1

interface GigabitEthernet0/1
 ipv6 address FD8A:1::4/64
 no shutdown

interface Tunnel46
 ip address 192.168.4.1 255.255.255.0
 ip ospf 1 area 0
 tunnel source GigabitEthernet0/1
 tunnel mode gre ipv6
 tunnel destination FD8A:2::6
 tunnel protection ipsec profile NGE-PROFILE
```

For R6:

```
ipv6 unicast-routing

ipv6 route ::/0 FD8A:2::3

interface GigabitEthernet0/1
 ipv6 address FD8A:2::6/64
 no shutdown

interface Tunnel64
```

```
 ip address 192.168.6.1 255.255.255.0
 ip ospf 1 area 0
 tunnel source GigabitEthernet0/1
 tunnel mode gre ipv6
 tunnel destination FD8A:1::4
 tunnel protection ipsec profile NGE-PROFILE
```

3.4 Gray CA

The gray CA will not be attached to the network. Rather, the CA will be a standalone device. All CSRs will occur out-of-band through manual enrollment.

```
no ip domain-lookup
hostname R2
ip domain-name gray.local

crypto pki trustpoint CA
 revocation-check none
 rsakeypair CA-KEY 3072 3072
 enrollment terminal
 subject-name CN=r2,OU=gray,O=local

crypto pki server CA
 grant auto
 hash sha384
 issuer-name CN=r2,OU=gray,O=local
 lifetime certificate 14
 lifetime ca-certificate 14
 no shutdown
```

The configuration of the standalone gray CA is now complete.

3.5 Outer Encryption Components

3.5.1 CSR

We will perform manual CSRs for the gray devices. Begin the CSR with the following configuration and enrollment request:

```
no ip domain-lookup
hostname R1
ip domain-name gray.local

crypto pki trustpoint Gray-CA
 enrollment terminal
 serial-number
 subject-name CN=r1,OU=gray,O=local
 revocation-check none
 rsakeypair CSFC-KEY 3072 3072

crypto pki enroll Gray-CA
```

The command `crypto pki enroll` will display the text of the CSR. Copy this text into the gray CA's command `crypto pki server CA request pkcs10 terminal base64` to grant the CSR.

Before we paste the CA's response into the router we must authenticate the CA. Obtain the CA's signing certificate with the command `crypto pki export CA pem terminal`. Authenticate the CA at the router

with the command `crypto pki authenticate Gray-CA`. Finally, install the signed certificate at the router with the command `crypto pki import Gray-CA certificate`.

The order of operations is flexible. The following sequence of commands can also work:

1. (CA) `crypto pki export CA pem terminal` (copy output)
2. (Router) `crypto pki authenticate Gray-CA` (paste input)
3. (Router) `crypto pki enroll Gray-CA` (copy output)
4. (CA) `crypto pki server CA request pkcs10 terminal base64` (paste input, copy output)
5. (Router) `crypto pki import Gray-CA certificate` (paste input)

3.5.2 IKEv2 and IPsec Configuration

There are several minor differences in the IKEv2 profile given below. Foremost, trust is anchored at the gray CA, not the red. Second, routers present their fully-qualified domain names (FQDN) as their identities instead of IP addresses. Third, notice that this configuration uses Elliptical Curve Digital Signature Algorithm (ECDSA) instead of Rivest-Shamir-Adleman (RSA).

On R1:

```
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
 group 20

crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL

no crypto ikev2 policy default

crypto ikev2 profile IKEV2-PROFILE
 match identity remote fqdn R3.gray.local
 identity local fqdn R1.gray.local
 authentication local ecdsa-sig
 authentication remote ecdsa-sig
 pki trustpoint Gray-CA

no crypto ikev2 http-url cert

crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode tunnel

crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE

no crypto ipsec profile default
```

On R3, switch the text of R1 and R3 in the `crypto ikev2 profile` section. Observe that these fully-qualified domain names are case-sensitive.

3.5.3 Tunnel over black

This MSC network uses a generic "black" network between the two gray outer encryption components. If there black network were the public Internet, then a black firewall would be required.

Configure interfaces on R1:

```
ipv6 unicast-routing

interface GigabitEthernet0/1
 ip address 198.51.100.0 255.255.255.254
 no shutdown

interface GigabitEthernet0/2
 ipv6 address FD8A:1::1/64
 no shutdown

interface Tunnel13
 no ip address
 ipv6 address FD8A:13::/64 eui-64
 cdp enable
 tunnel source GigabitEthernet0/1
 tunnel destination 198.51.100.1

ipv6 route FD8A:2::/64 Tunnel13
```

Configure interfaces on R3:

```
ipv6 unicast-routing

interface GigabitEthernet0/1
 ip address 198.51.100.1 255.255.255.254
 no shutdown

interface GigabitEthernet0/2
 ipv6 address FD8A:2::3/64
 no shutdown

interface Tunnel31
 no ip address
 ipv6 address FD8A:13::/64 eui-64
 cdp enable
 tunnel source GigabitEthernet0/1
 tunnel destination 198.51.100.0

ipv6 route FD8A:1::/64 Tunnel31
```

Observe that the tunnel interfaces do not use the `tunnel protection ipsec profile` statement. We will use the legacy `crypto map` syntax to protect this traffic instead.

3.5.4 `crypto map`

The `crypto map` statement matches which packets should be encapsulated with IPsec, determines cryptographic parameters, and specifies the peer to which encapsulated packets should be forwarded.

On R1:

```
ip access-list extended VPN-ACL
 permit ip 198.51.100.0 0.0.0.1 198.51.100.0 0.0.0.1
```

```
crypto map l2l 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
 match address VPN-ACL

interface GigabitEthernet0/1
 crypto map l2l
```

On R3:

```
ip access-list extended VPN-ACL
 permit ip 198.51.100.0 0.0.0.1 198.51.100.0 0.0.0.1

crypto map l2l 10 ipsec-isakmp
 set peer 198.51.100.0
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
 match address VPN-ACL

interface GigabitEthernet0/1
 crypto map l2l
```

A Reference Configuration

A.1 R1

```
hostname R1
!
no ip domain lookup
ip domain name gray.local
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto pki trustpoint Gray-CA
 enrollment terminal
 serial-number
 subject-name CN=r1,OU=gray,O=local
 revocation-check none
 rsakeypair CSFC-KEY 3072 3072
!
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
 group 20
!
crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL
```

```
no crypto ikev2 policy default
!
crypto ikev2 profile IKEV2-PROFILE
 match identity remote fqdn R3.gray.local
 identity local fqdn R1.gray.local
 authentication local ecdsa-sig
 authentication remote ecdsa-sig
 pki trustpoint Gray-CA
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode tunnel
!
crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
!
no crypto ipsec profile default
!
crypto map l2l 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
 match address VPN-ACL
!
interface Tunnel13
 no ip address
 ipv6 address FD8A:13::/64 eui-64
 cdp enable
 tunnel source GigabitEthernet0/1
 tunnel destination 198.51.100.1
!
interface GigabitEthernet0/1
 ip address 198.51.100.0 255.255.255.254
 crypto map l2l
!
interface GigabitEthernet0/2
 ipv6 address FD8A:1::1/64
!
ip access-list extended VPN-ACL
 permit ip 198.51.100.0 0.0.0.1 198.51.100.0 0.0.0.1
!
ipv6 route FD8A:2::/64 Tunnel13
```

A.2 R2

```
hostname R2
!
no ip domain lookup
ip domain name gray.local
```

```
!
crypto pki server CA
 no database archive
 issuer-name CN=r2,OU=gray,O=local
 grant auto
 hash sha384
 lifetime certificate 14
 lifetime ca-certificate 14
!
crypto pki trustpoint CA
 enrollment terminal
 subject-name CN=r2,OU=gray,O=local
 revocation-check none
 rsakeypair CA-KEY 3072 3072
```

A.3 R3

```
hostname R3
!
no ip domain lookup
ip domain name gray.local
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto pki trustpoint Gray-CA
 enrollment terminal
 serial-number
 subject-name CN=r3,OU=gray,O=local
 revocation-check none
 rsakeypair CSFC-KEY 3072 3072
!
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
 group 20
!
crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL
no crypto ikev2 policy default
!
crypto ikev2 profile IKEV2-PROFILE
 match identity remote fqdn R1.gray.local
 identity local fqdn R3.gray.local
 authentication local ecdsa-sig
 authentication remote ecdsa-sig
 pki trustpoint Gray-CA
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode tunnel
```

```
!
crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
!
no crypto ipsec profile default
!
crypto map l2l 10 ipsec-isakmp
 set peer 198.51.100.0
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
 match address VPN-ACL
!
interface Tunnel31
 no ip address
 ipv6 address FD8A:13::/64 eui-64
 cdp enable
 tunnel source GigabitEthernet0/1
 tunnel destination 198.51.100.0
!
interface GigabitEthernet0/1
 ip address 198.51.100.1 255.255.255.254
 crypto map l2l
!
interface GigabitEthernet0/2
 ipv6 address FD8A:2::3/64
!
ip access-list extended VPN-ACL
 permit ip 198.51.100.0 0.0.0.1 198.51.100.0 0.0.0.1
!
ipv6 route FD8A:1::/64 Tunnel31
```

A.4 R4

```
hostname R4
!
vrf definition MANAGEMENT
 !
 address-family ipv4
 exit-address-family
!
no ip domain lookup
ip domain name red.local
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto pki trustpoint Red-CA
 enrollment url http://203.0.113.1:80
 serial-number
 ip-address 192.168.4.4
```

```
 subject-name CN=r4,OU=red,O=local
 vrf MANAGEMENT
 revocation-check crl
 rsakeypair CSFC-KEY 3072 3072
!
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
 group 20
!
crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL
no crypto ikev2 policy default
!
crypto ikev2 profile IKEV2-PROFILE
 match identity remote address 192.168.6.6 255.255.255.255
 identity local address 192.168.4.4
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint Red-CA
!
crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode transport
!
no crypto ipsec profile default
!
crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
!
interface Loopback0
 ip address 192.168.4.4 255.255.255.255
 ip ospf 1 area 4
!
interface Tunnel46
 ip address 192.0.2.1 255.255.255.252
 ip ospf 1 area 0
 tunnel source GigabitEthernet0/1
 tunnel mode gre ipv6
 tunnel destination FD8A:2::6
 tunnel protection ipsec profile NGE-PROFILE
!
interface GigabitEthernet0/0
 vrf forwarding MANAGEMENT
 ip address dhcp
!
interface GigabitEthernet0/1
 ipv6 address FD8A:1::4/64
!
router ospf 1
!
ipv6 route ::/0 FD8A:1::1
```

A.5 R5

```
hostname R5
!
ip dhcp pool RED-PROVISIONING
 network 203.0.113.0 255.255.255.128
!
no ip domain lookup
ip domain name red.local
ip cef
no ipv6 cef
!
crypto pki server CA
 no database archive
 issuer-name CN=r5,OU=red,O=local
 grant auto
 hash sha384
 lifetime certificate 14
 lifetime ca-certificate 14
!
crypto pki trustpoint CA
 subject-name CN=r5,OU=red,O=local
 revocation-check crl
 rsakeypair CA-KEY 3072 3072
!
interface GigabitEthernet0/0
 ip address 203.0.113.1 255.255.255.128
!
ip http server
```

A.6 R6

```
hostname R6
!
vrf definition MANAGEMENT
 !
 address-family ipv4
 exit-address-family
!
no ip domain lookup
ip domain name red.local
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto pki trustpoint Red-CA
 enrollment url http://203.0.113.1:80
 serial-number
 ip-address 192.168.6.6
 subject-name CN=r6,OU=red,O=local
 vrf MANAGEMENT
 revocation-check crl
 rsakeypair CSFC-KEY 3072 3072
```

```
!
crypto ikev2 proposal IKEV2-PROPOSAL
 encryption aes-cbc-256
 prf sha512
 integrity sha384
 group 20
!
crypto ikev2 policy IKEV2-POLICY
 proposal IKEV2-PROPOSAL
no crypto ikev2 policy default
!
crypto ikev2 profile IKEV2-PROFILE
 match identity remote address 192.168.4.4 255.255.255.255
 identity local address 192.168.6.6
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint Red-CA
!
crypto ipsec transform-set NGE-TRANSFORM-SET esp-gcm 256
 mode transport
!
crypto ipsec profile NGE-PROFILE
 set transform-set NGE-TRANSFORM-SET
 set pfs group20
 set ikev2-profile IKEV2-PROFILE
!
no crypto ipsec profile default
!
interface Loopback0
 ip address 192.168.6.6 255.255.255.255
 ip ospf 1 area 6
!
interface Tunnel64
 ip address 192.0.2.2 255.255.255.252
 ip ospf 1 area 0
 tunnel source GigabitEthernet0/1
 tunnel mode gre ipv6
 tunnel destination FD8A:1::4
 tunnel protection ipsec profile NGE-PROFILE
!
interface GigabitEthernet0/0
 vrf forwarding MANAGEMENT
 ip address dhcp
!
interface GigabitEthernet0/1
 ipv6 address FD8A:2::6/64
!
router ospf 1
!
ipv6 route ::/0 FD8A:2::3
```

B Useful Troubleshooting Commands

- `debug crypto pki transactions`
- `show crypto pki server`
- `show ip http server status`
- `show crypto pki certificates`
- `debug crypto ikev2`
- `show crypto ikev2 policy`
- `show crypto ikev2 profile`
- `show crypto ikev2 sa`
- `show crypto ipsec profile`
- `show crypto ipsec sa`
- `show interface tunnel`
- `show crypto map`