CISCO VALIDATED DESIGN

# Intelligent WAN Public Key Infrastructure Deployment Guide

April 2017

# Table of Contents

# Deploying the Cisco Intelligent WAN

This guide is one in a series of IWAN advanced deployment guides that focus on how to deploy the advanced features of the Cisco Intelligent WAN (IWAN). These guides build on the configurations deployed in the Intelligent WAN Deployment Guide and are optional components of its base IWAN configurations.

The advanced guides are as follows:

- IWAN High Availability and Scalability Deployment Guide
- IWAN Multiple Data Center Deployment Guide
- IWAN Multiple Transports Deployment Guide
- IWAN Multiple VRF Deployment Guide
- IWAN Public Key Infrastructure Deployment Guide (this guide)
- IWAN NetFlow Monitoring Deployment Guide
- IWAN Remote Site 4G LTE Deployment Guide

For design details, see Intelligent WAN Design Summary.

For configuration details, see Intelligent WAN Configuration Files Guide.

For an automated way to deploy IWAN, use the APIC-EM IWAN Application. For more information, see the Cisco IWAN Application on APIC-EM User Guide.

If want to use TrustSec with your IWAN deployment, see "Configuring SGT Propagation" in the User-to-Data-Center Access Control Using TrustSec Deployment Guide.

## DEPLOYMENT DETAILS

### How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

# Deploying IWAN Public Key Infrastructure

Use this guide to add Public Key Infrastructure (PKI) to an existing IWAN deployment.

PROCESS

## Deploying an IOS Certificate Authority

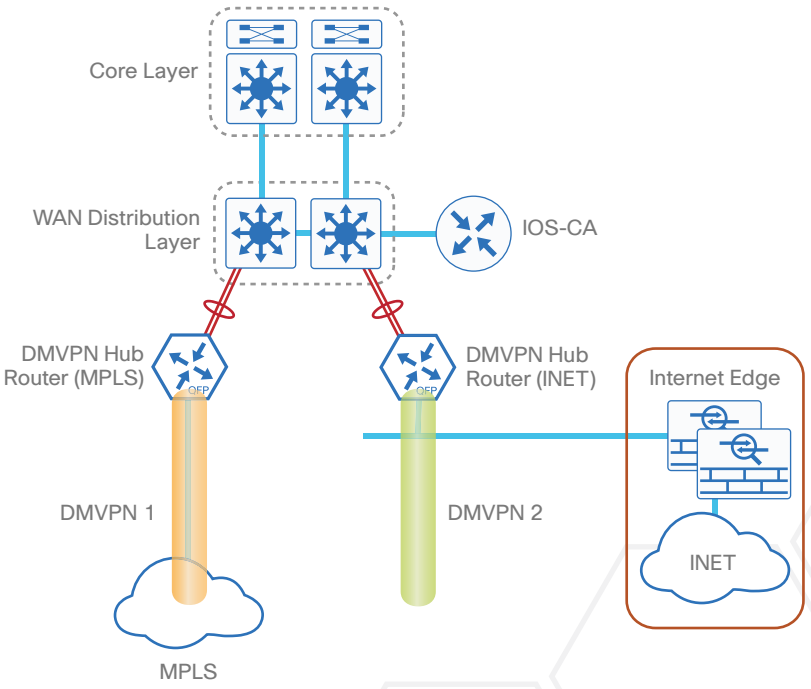
1. Configuring the IOS CA platform
2. Configuring connectivity to the network
3. Configuring the certificate authority

Use this optional process if you want to deploy an IOS Certificate Authority (IOS CA) on a router with access from the internal network. Skip this process if you plan to use a different certificate authority. You can create a more complex CA environment, but the same basic reachability principles will apply for an IWAN enabled solution.

For this process, you configure an IOS CA by using a single internal LAN interface, which allows access from the hub routers and the remote sites. The remote sites access the IOS CA for authentication and for obtaining their certificate after a DMVPN tunnel has been established with pre-shared keys.

After the remote site has obtained the PKI certificate, it can be re-configured to use PKI certificates instead of PSKs for IKEV2 authentication to build the DMVPN encrypted tunnels with the hubs and other remote sites. It no longer needs direct access to the IOS CA, except when it needs a new PKI certificate before the current PKI certificate times out (usually at least 1 year lifetime). At that point, the remote site will use the current DMVPN tunnel to access the IOS CA for the new PKI certificate.

*Figure 1* *IOS CA with internal LAN interface*



## Procedure 1 Configuring the IOS CA platform

To complete the base configuration for this router, follow the steps in "Configure the platform base features" in the IWAN Deployment Guide.

## Procedure 2 Configuring connectivity to the network

**Step 1:** The internal address is an inside address that can be accessed from the hub site or a remote site if the site is already up and running with a DMVPN tunnel.

```
interface GigabitEthernet0/0
 description Internal
 ip address 10.6.24.11 255.255.255.224
 no shutdown
```

**Step 2:** Configure IP routing using a static route.

```
ip route 0.0.0.0 0.0.0.0 10.6.24.1
```

## Procedure 3 Configuring the certificate authority

The following commands configure the CA on the router. This CA can be part of a PKI hierarchy, but only of IOS authorities, and the certificate from the root CA must be issued via SCEP.

**Step 1:** Configure the server.

```
crypto pki server IWAN-IOS-CA
 database level complete
 no database archive
 issuer-name CN=IWAN-IOS-CA.cisco.local L=SanJose St=CA C=US
```

**Step 2:** Configure the server to use SCEP for issuing certificates.

```
 grant auto
```

**Step 3:** Configure the lifetime for the issued certificates at 2 years. The time is in days.

```
 lifetime certificate 730
```

**Step 4:** Configure the lifetime for the certificate server signing certificate at 3 years. The time is in days.

```
 lifetime ca-certificate 1095
```

**Step 5:** Configure the location for certificate revocation lists.

***Tech Tip***

In order to force the parser to retain the embedded question mark within the specified location, enter CTRL+V prior to the question mark. If this action is not taken, CRL retrieval through HTTP returns an error message.

```
cdp-url http://10.6.24.11/cgi-bin/pkiclient.exe?operation=GetCRL
database url crl nvram:
```

**Step 6:** Start the server with the **no shutdown** command.

```
crypto pki server IWAN-IOS-CA
 no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: c1sco123

Re-enter password: c1sco123
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

% Certificate Server enabled.
IWAN-IOS-CA(cs-server)#
Dec 15 13:19:49.254: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

The following trustpoint and rsa keypair are automatically generated when you start the server:

```
crypto pki trustpoint IWAN-IOS-CA
 revocation-check crl
 rsakeypair IWAN-IOS-CA
```

***Reader Tip***

For more information, including options for configuring certificates, see the following document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.pdf

PROCESS

## Deploying PKI for a DMVPN border router

1. Configuring IKEv2 and IPsec with PKI

This section is for DMVPN border routers only.

The parameters in the table below are used in this section. The crypto configurations have been simplified in this version of the guide in order to minimize the variations from previous guides. Use the values in the table that represent the design you are configuring.

*Table 1 Crypto parameters*

| Parameter | Public Key Infrastructure |
|---|---|
| crypto ikev2 profile | DMVPN-PKI-IKEv2-PROFILE |
| crypto ipsec profile | DMVPN-PKI-IPSEC-PROFILE |

IPsec uses a key exchange between the routers in order to encrypt/decrypt the traffic. These keys can be exchanged using pre-shared keys or PKI certificates with a certificate authority. It is also possible to use a combination of the two, which is useful during a migration from one method to the other.

## Procedure 1 Configuring IKEv2 and IPsec with PKI

If you do not have a certificate authority in your network, you may follow the optional section "IOS Certificate Authority" to deploy an IOS certificate authority using a Cisco router.

To use a certificate authority, you will have to configure a pre-shared key on one of the hub border routers in order to allow each remote site to establish a DMVPN tunnel to the WAN aggregation site. After the first DMVPN tunnel at a remote site is established, the router will be able to authenticate to the CA and obtain a certificate. After obtaining the certificate, you can configure the remote site to use PKI.

The **crypto pki trustpoint** is the method of specifying the parameters associated with a CA. The router must authenticate to the CA first and then enroll with the CA to obtain its own identity certificate.

**Step 1:** The fingerprint command limits the responding CA. You can find this fingerprint by using **show crypto pki server** on the IOS CA.

```
IWAN-IOS-CA#show crypto pki server
Certificate Server IWAN-IOS-CA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=IWAN-IOS-CA.cisco.local L=SanJose St=CA C=US
    CA cert fingerprint: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
    Granting mode is: auto
    Last certificate issued serial number (hex): 59
    CA certificate expiration timer: 13:19:42 PST Dec 24 2017
    CRL NextUpdate timer: 14:55:59 PDT Sep 12 2016
    Current primary storage dir: nvram:
    Current storage dir for .crl files: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
```

**Step 2:** Configure the PKI trust point.

```
crypto pki trustpoint [name]
 enrollment url [URL of IOS CA]
 serial-number none
 fqdn [fully qualified domain name of this router]
 ip-address [Loopback IP address of this router]
 fingerprint [fingerprint from IOS CA]
 revocation-check crl none
 rsakeypair [name] 2048 2048
```

### *Tech Tip*

With the **revocation-check crl none** command, the router will do a CRL check as long as the CA server is reachable. If the CA server is not reachable, then the router checks the signature.

### Example: Hybrid hub border router– HY-INET1-ASR1002X-2

This example is from the secondary WAN hub router in the hybrid design model. It can reach the IOS CA through the internal network at 10.6.24.11 using the default VRF.

```
crypto pki trustpoint IWAN-CA
 enrollment url http://10.6.24.11:80
 serial-number none
 fqdn HY-INET1-ASR1002X-2.cisco.local
 ip-address 10.6.32.242
 fingerprint 75BEF6259A9876CF6F341FE586D4A5D8
 revocation-check crl none
 rsakeypair IWAN-CA-KEYS 2048 2048
```

**Step 3:** Authenticate to the CA and obtain the CA's certificate

Exit the trustpoint configuration mode on the hub router and issue the following command to authenticate to the CA and get its certificate.

```
(config)# crypto pki authenticate IWAN-CA
Certificate has the following attributes:
       Fingerprint MD5: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
      Fingerprint SHA1: 9C14D6F4 D1F08023 17A85669 52922632 C6B02928
Trustpoint Fingerprint: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
Certificate validated - fingerprints matched.
```

**Step 4:** When the trustpoint CA certificate is accepted, enroll with the CA, enter a password for key retrieval, and obtain a certificate for this hub router.

```
(config)# crypto pki enroll IWAN-CA

% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: c1sco123
Re-enter password: c1sco123

% The subject name in the certificate will include: HY-INET1-ASR1002X-2.cisco.
local
% The IP address in the certificate is 10.6.32.242
```

```
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose IWAN-CA' command will show the finger-
print.
```

**Step 5:** Configure the IKEv2 proposal.

The user-defined IKEv2 proposal includes only the following:

- Encryption with AES cipher and a 256-bit key
- Pseudo-random function with SHA and a 512-bit digest
- Diffie-Hellman group: 19

```
crypto ikev2 proposal [proposal name]
 encryption [encryption algorithm]
 prf [pseudo-random function algorithm]
 group [Diffie-Hellman group]
```

### Example

```
crypto ikev2 proposal AES/GCM/256
 encryption aes-gcm-256
 prf sha512
 group 19
```

The default IKEv2 proposal is also used.

A **show crypto ikev2 proposal** displays the details of the two proposals.

```
show crypto ikev2 proposal
 IKEv2 proposal: AES/GCM/256
      Encryption : AES-GCM-256
      Integrity  : none
      PRF        : SHA512
      DH Group   : DH_GROUP_256_ECP/Group 19
 IKEv2 proposal: default
      Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
      Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
      PRF        : SHA512 SHA384 SHA256 SHA1 MD5
      DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

**Step 6:** Configure the IKEv2 policy.

The crypto policy includes the proposal you created in the previous step. This policy will match any FVRF defined on the router.

```
crypto ikev2 policy [policy name]
 match fvrf any
 proposal [proposal name]
```

### Example

```
crypto ikev2 policy AES/GCM/256
 match fvrf any
 proposal AES/GCM/256
```

The default IKEv2 policy is also used.

A **show crypto ikev2 policy** displays the details of the two policies.

```
show crypto ikev2 policy
 IKEv2 policy : AES/GCM/256
      Match fvrf : any
      Match address local : any
      Proposal    : AES/GCM/256

 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
```

**Step 7:** Configure the IKEv2 profile.

The IKEv2 profile creates an association between an identity address and a VRF. A wildcard address within a VRF is referenced with 0.0.0.0. The **identity local address** must match the crypto pki trustpoint's **ip-address** value from the step above.

***Tech Tip***

Use the **identity local address** in the ikev2 profile in order to avoid repeated CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH warning messages on the router.

The profile also defines what method of key sharing will be used on this router with **authentication local** and what methods will be accepted from remote locations with **authentication remote**. The **rsa-sig** keyword is used when certificates contain the encryption key.

```
crypto ikev2 profile [profile name]
 description [profile description]
 match fvrf [vrf name]
 match identity remote address [IP address]
 identity local address [Loopback IP address of this router]
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint [trustpoint name]
```

### Example: Hybrid hub border router– HY-INET1-ASR1002X-2

```
crypto ikev2 profile DMVPN-PKI-IKEv2-PROFILE
 description PKI Profile
 match fvrf any
 match identity remote address 0.0.0.0
 identity local address 10.6.32.242
 authentication remote rsa-sig
 authentication local rsa-sig
```

**Step 8:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit GCM encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [transform set] esp-gcm 256
 mode transport
```

### Example

```
crypto ipsec transform-set AES256/GCM/TRANSPORT esp-gcm 256
 mode transport
```

**Step 9:** Configure the IPsec profile.

The IPsec profile creates an association between an IKEv2 profile and an IPsec transform-set.

```
crypto ipsec profile [profile name]
 set transform-set [transform set]
 set ikev2-profile [ikev2 profile name]
```

**Example**

```
crypto ipsec profile DMVPN-PKI-IPSEC-PROFILE
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-PKI-IKEv2-PROFILE
```

**Step 10:** Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size [value]
```

**Example**

```
crypto ipsec security-association replay window-size 1024
```

***Tech Tip***

QoS queuing delays can cause anti-replay packet drops, so it is important to extend the window size to prevent the drops from occurring.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the maximum window size in order to minimize future anti-replay problems. On the Cisco ASR1K, ISR 4K and ISR G2 router platforms, the maximum replay window size is 1024.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI and in the log:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

A **show crypto ipsec sa** displays the transform and anti-replay window size.

```
show crypto ipsec sa
interface: Tunnel11
    Crypto map tag: Tunnel11-head-0, local addr 192.168.146.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.146.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.19.98.108/255.255.255.255/47/0)
   current_peer 172.19.98.108 port 4500
```

```
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 88955556, #pkts encrypt: 88955556, #pkts digest: 88955556
     #pkts decaps: 118171922, #pkts decrypt: 118171922, #pkts verify: 118171922
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

      local crypto endpt.: 192.168.146.10, remote crypto endpt.: 172.19.98.108
      plaintext mtu 1358, path mtu 1400, ip mtu 1400, ip mtu idb Tunnel21
      current outbound spi: 0x3B1610D2(991301842)
      PFS (Y/N): N, DH group: none

      inbound esp sas:
       spi: 0xF47FC338(4102013752)
         transform: esp-gcm 256 ,
         in use settings ={Transport UDP-Encaps, }
         conn id: 16489, flow_id: HW:14489, sibling_flags FFFFFFFF80000008, crypto
map: Tunnel11-head-0
         sa timing: remaining key lifetime (k/sec): (4582843/385)
         IV size: 8 bytes
         replay detection support: Y  replay window size: 1024
         Status: ACTIVE(ACTIVE)
```

PROCESS

## Deploying PKI for a remote site router

1. Configuring with a certificate authority

This section is for remote site routers only.

The parameters in the table below are used in this section. The crypto configurations have been simplified in this version of the guide in order to minimize the variations from previous guides. Use the values in the table that represent the design you are configuring.

*Table 2 Crypto parameters*

| Parameter | Public Key Infrastructure |
|---|---|
| crypto ikev2 profile | DMVPN-PKI-IKEv2-PROFILE |
| crypto ipsec profile | DMVPN-PKI-IPSEC-PROFILE |

IPsec uses a key exchange between the routers in order to encrypt/decrypt the traffic. These keys can be exchanged using pre-shared keys or PKI certificates with a certificate authority. It is also possible to use a combination of the two, which is useful during a migration from one method to the other.

### Procedure 1 Configuring with a certificate authority

If you do not have a certificate authority in your network, you may follow the optional section "IOS Certificate Authority" to deploy an IOS certificate authority using a Cisco router.

To use a certificate authority, you will have to configure a pre-shared key on one of the hub border routers in order to allow each remote site to establish a DMVPN tunnel to the WAN aggregation site. After the first DMVPN tunnel at a remote site is established, the router will be able to authenticate to the CA and obtain a certificate. After obtaining the certificate, you can configure the remote site to use PKI.

The **crypto pki trustpoint** is the method of specifying the parameters associated with a CA. The router must authenticate to the CA first and then enroll with the CA in order to obtain its own identity certificate.

**Step 1:** The fingerprint command limits the responding CA. You can find this fingerprint by using **show crypto pki server** on the IOS CA.

```
IWAN-IOS-CA#show crypto pki server
Certificate Server IWAN-IOS-CA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=IWAN-IOS-CA.cisco.local L=SanJose St=CA C=US
    CA cert fingerprint: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
    Granting mode is: auto
    Last certificate issued serial number (hex): 59
    CA certificate expiration timer: 13:19:42 PST Dec 24 2017
    CRL NextUpdate timer: 14:55:59 PDT Sep 12 2016
    Current primary storage dir: nvram:
    Current storage dir for .crl files: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
```

**Step 2:** Configure the PKI trust point.

```
crypto pki trustpoint [name]
 enrollment url [URL of IOS CA]
 serial-number none
 fqdn [fully qualified domain name of this router]
 ip-address [loopback IP address of this router]
 fingerprint [fingerprint from IOS CA]
 revocation-check crl none
 rsakeypair [name] 2048 2048
```

### Example: Second router of dual-router site for hybrid—RS14-2921-2

This example is from the primary WAN remote site router in the hybrid design model. After the DMVPN tunnel is established with pre-shared keys, it can reach the IOS CA through the internal network at 10.6.24.11 using the default VRF.

```
crypto pki trustpoint IWAN-CA
 enrollment url http://10.6.24.11:80
 serial-number none
 fqdn RS14-2921-2.cisco.local
 ip-address 10.255.247.14
 fingerprint 75BEF6259A9876CF6F341FE586D4A5D8
 revocation-check crl none
 rsakeypair IWAN-CA-KEYS 2048 2048
```

#### *Tech Tip*

With the **revocation-check crl none** command, the router will do a CRL check as long as the CA server is reachable. If the CA server is not reachable, then the router checks the signature.

**Step 3:** Authenticate to the CA and obtain the CA's certificate

Exit the trustpoint configuration mode on the hub router and issue the following command to authenticate to the CA and get its certificate.

```
(config)# crypto pki authenticate IWAN-CA
Certificate has the following attributes:
       Fingerprint MD5: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
      Fingerprint SHA1: 9C14D6F4 D1F08023 17A85669 52922632 C6B02928
Trustpoint Fingerprint: 75BEF625 9A9876CF 6F341FE5 86D4A5D8
Certificate validated - fingerprints matched.
```

**Step 4:** When the trustpoint CA certificate is accepted, enroll with the CA, enter a password for key retrieval, and obtain a certificate for this hub router.

```
(config)# crypto pki enroll IWAN-CA
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: c1sco123
Re-enter password: c1sco123

% The subject name in the certificate will include: RS14-2921-2.cisco.local
% The IP address in the certificate is 10.255.247.14

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose IWAN-CA' command will show the finger-
print.
```

**Step 5:** Configure the IKEv2 proposal.

The user-defined IKEv2 proposal includes only the following:

- Encryption with AES cipher and a 256-bit key
- Pseudo-random function with SHA and a 512-bit digest
- Diffie-Hellman group: 19

```
crypto ikev2 proposal [proposal name]
 encryption [encryption algorithm]
 prf [pseudo-random function algorithm]
 group [Diffie-Hellman group]
```

### Example

```
crypto ikev2 proposal AES/GCM/256
 encryption aes-gcm-256
 prf sha512
 group 19
```

The default IKEv2 proposal is also used.

A **show crypto ikev2 proposal** displays the details of the two proposals.

```
show crypto ikev2 proposal
 IKEv2 proposal: AES/GCM/256
      Encryption : AES-GCM-256
      Integrity  : none
      PRF        : SHA512
      DH Group   : DH_GROUP_256_ECP/Group 19
 IKEv2 proposal: default
      Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
      Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
      PRF        : SHA512 SHA384 SHA256 SHA1 MD5
      DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

**Step 6:** Configure the IKEv2 policy.

The crypto policy includes the proposal you created in the previous step. This policy will match any FVRF defined on the router.

```
crypto ikev2 policy [policy name]
 match fvrf any
 proposal [proposal name]
```

### Example

```
crypto ikev2 policy AES/GCM/256
 match fvrf any
 proposal AES/GCM/256
```

The default IKEv2 policy is also used.

A **show crypto ikev2 policy** displays the details of the two policies.

```
show crypto ikev2 policy
 IKEv2 policy : AES/GCM/256
      Match fvrf : any
      Match address local : any
      Proposal    : AES/GCM/256

 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
```

**Step 7:** Configure the IKEv2 profile.

The IKEv2 profile creates an association between an identity address and a VRF. A wildcard address within a VRF is referenced with 0.0.0.0. The **identity local address** must match the crypto pki trustpoint's **ip-address** value from the step above.

***Tech Tip***

Use the **identity local address** in the ikev2 profile in order to avoid repeated CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH warning messages on the router.

The profile also defines what method of key sharing will be used on this router with **authentication local** and what methods will be accepted from remote locations with **authentication remote**. The **rsa-sig** keyword is used when certificates contain the encryption key.

DPD is essential in order to facilitate fast reconvergence and for spoke registration to function properly in case a DMVPN hub is restarted. The IWAN design recommends you set the remote site DPD timer to 40 seconds with a 5 second retry.

```
crypto ikev2 profile [profile name]
 description [profile description]
 match fvrf [vrf name]
 match identity remote address [IP address]
 identity local address [Loopback IP address of this router]
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint [trustpoint name]
 dpd [interval in seconds] [retry interval] on-demand
```

**Example: Second router of dual-router site for hybrid–RS14-2921-2**

```
crypto ikev2 profile DMVPN-PKI-IKEv2-PROFILE
 description PKI Profile
 match fvrf any
 match identity remote address 0.0.0.0
 identity local address 10.255.247.14
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint IWAN-CA
 dpd 40 5 on-demand
```

**Step 8:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit GCM encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [transform set] esp-gcm 256
 mode transport
```

**Example**

```
crypto ipsec transform-set AES256/GCM/TRANSPORT esp-gcm 256
 mode transport
```

**Step 9:** Configure the IPsec profile.

The IPsec profile creates an association between an IKEv2 profile and an IPsec transform-set.

```
crypto ipsec profile [profile name]
 set transform-set [transform set]
 set ikev2-profile [ikev2 profile name]
```

**Example**

```
crypto ipsec profile DMVPN-PKI-IPSEC-PROFILE
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-PKI-IKEv2-PROFILE
```

**Step 10:** Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size [value]
```

**Example**

```
crypto ipsec security-association replay window-size 1024
```

### *Tech Tip*

QoS queuing delays can cause anti-replay packet drops, so it is important to extend the window size in order to prevent the drops from occurring.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the maximum window size in order to minimize future anti-replay problems. On the Cisco ASR 1K, ISR 4K and ISR G2 router platforms, the maximum replay window size is 1024.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI and in the log:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

# Appendix A: Product List

To view the full list of IWAN-supported routers for this version of the CVD, see Supported Cisco Platforms and Software Releases.

# Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- Public Key Infrastructure updates:
  - Changed the revocation-check to crl none
- Guide updates:
  - This new guide is one in a series of IWAN advanced deployment guides.

Please use the feedback form to send comments and suggestions about this guide.


**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.