Appendix: IKEv2 and Legacy VPNs

This module provides examples on how to configure IKEv2 on crypto map based configurations.

Crypto maps are considered a legacy configuration construct. It is recommended that you migrate existing crypto map based setups to use tunnel protection and virtual interfaces.

- Example: Configuring Crypto-Map-Based IKEv2 Peers Using Preshared Key Authentication Method, on page 1
- Example: Configuring Crypto Map-Based IKEv2 Peers Using Certification Authentication Method, on page 4
- Example: Configuring Crypto Map- and sVTI-Based IKEv2 Peers, on page 8
- Example: Configuring IPsec Using sVTI-Based IKEv2 Peers, on page 10
- Example: Configuring IKEv2 on DMVPN Networks, on page 13

Example: Configuring Crypto-Map-Based IKEv2 Peers Using Preshared Key Authentication Method

The following example shows how to configure crypto-map-based IKEv2 peers using the preshared key authentication method between a static crypto-map IKEv2 initiator and a dynamic crypto-map IKEv2 responder. The initiator configuration is as follows:

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
!
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
!
crypto ikev2 keyring v2-kr1
  peer abc
  address 209.165.200.231 255.255.255.224 255.255.255.224
  pre-shared-key abc
!
!```
The responder configuration is as follows:

crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
! 
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
! 
crypto ikev2 keyring v2-kr1
  peer abc
  address 209.165.200.228
  pre-shared-key abc
! 
! 
crypto ikev2 profile prof
  match fvrf any
  match identity remote fqdn smap-initiator
  identity local fqdn dmap-responder
  authentication local pre-share
  authentication remote pre-share
  keyring v2-kr1
  ivrf global
! 
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
! 
crypto dynamic-map dmap 1
  set transform-set trans
  set reverse-route tag 222
  set ikev2-profile prof
match address ikev2list
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
   ip address 209.165.200.230 255.255.255.224
!
interface Ethernet0/0
   ip address 209.165.200.231 255.255.255.224
   crypto map cmap
!
ip route 209.165.200.233 255.255.255.224 209.165.200.228
!
ip access-list extended ikev2list
   permit ip any any
!
To initiate the connection between the initiator and the responder, enter the following command at the initiator's CLI:

ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms

To display the session details, enter the following show commands:

show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
IKEv2 SA: local 209.165.200.228/500 remote 209.165.200.231/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 Active SAs: 2, origin: crypto map
show crypto ikev2 sa detail
Tunnel-id Local Remote fvrf/ivrf Status
1 209.165.200.228/500 209.165.200.231/500 (none)/(none) READY

Life/Active Time: 86400/21 sec
CE id: 1002, Session-id: 2
Status Description: Negotiation done
Local spi: 687752902752A6FD Remote spi: C9DCCFC65493D14F
Local id: smap-initiator
Remote id: dmap-responder
Local req msg id: 2 Remote req msg id: 0
Local next msg id: 2 Remote next msg id: 0
Local req queued: 2 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Example: Configuring Crypto Map-Based IKEv2 Peers Using Certification Authentication Method

The following example shows how to configure crypto-map-based IKEv2 peers using the certificate authentication method between a static crypto-map IKEv2 initiator, a dynamic crypto-map IKEv2 responder, and a CA server. The initiator configuration is as follows:

```plaintext
crypto pki trustpoint ca-server
  enrollment url http://10.1.1.3:80
  revocation-check none
!
crypto pki certificate map cmap-1 1
  subject-name eq hostname = responder
!
!
crypto pki certificate chain ca-server
  certificate 02
  `Certificate content...

Appendix: IKEv2 and Legacy VPNs

Example: Configuring Crypto Map-Based IKEv2 Peers Using Certification Authentication Method
crypto ikev2 profile prof
match fvrf any
match certificate cmap-1
identity local dn
authentication local rsa-sig
authentication remote pre-share
authentication remote rsa-sig
pki trustpoint ca-server
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
set peer 209.165.200.225
set transform-set trans
set ikev2-profile prof
match address ikev2list
!
interface Loopback0
  ip address 209.165.200.226 255.255.255.224
!
interface Ethernet0/0
  ip address 209.165.200.227 255.255.255.224
crypto map cmap
!
interface Ethernet1/0
  ip address 209.165.200.228 255.255.255.224
!
  ip route 209.165.200.229 255.255.255.224 209.265.200.231
!
  ip access-list extended ikev2list
    permit ip any any

The responder configuration is as follows:

crypto pki trustpoint ca-server
  enrollment url http://10.1.1.3:80
  revocation-check none
!
crypto pki certificate map cmap-2 1
  subject-name eq hostname = initiator
!
crypto pki certificate chain ca-server
  certificate 03
    308201AF 30820118 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
    14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
    32353231 325A170D 31313033 31303132 35323132 5A301A31 18301609 092A8648
    8F70D01 09021609 52455350 4F4E4445 5245505C 301D06 030205A0 81313A78 1F74ED3D
    669E416C A134D543 20952BC3 1A45C0B0 03AE011C 963AF523 C7C5C93 4FEB92A5
    F24B316E 4DD7D23A FA428BD1 5AFD1F72 B4007067 43C27D8A 1F74ED3D DEBE9F73
    1F515355 E77E766C AEACC03 39457991 29AB090C 99E21B5E 60DC2B48 7804479
    1FEBD462 B66C8C26 153111A2 87A4ED97 32727C
    quit

certificate ca 01
Example: Configuring Crypto Map-Based IKEv2 Peers Using Certification Authentication Method

```plaintext
crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14

crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1

crypto ikev2 profile prof
  match fvrf any
  match certificate cmap-2
  identity local dn
  authentication local rsa-sig
  authentication remote pre-share
  authentication remote rsa-sig
  pki trustpoint ca-server

crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac

crypto dynamic-map dmap 1
  set transform-set trans
  set ikev2-profile prof

crypto map cmap 1 ipsec-isakmp dynamic dmap
  interface Loopback0
    ip address 209.165.200.230 255.255.255.224

  interface Ethernet0/0
    ip address 209.165.200.231 255.255.255.224

  crypto map cmap

  interface Ethernet1/0
    ip address 209.165.200.232 255.255.255.224

  ip route 209.165.200.233 255.255.255.224 209.165.200.228

  ip access-list extended ikev2list
    permit ip host 209.165.200.231 host 209.165.200.228

The CA server configuration is as follows:

crypto pki server ca-server
```
grant auto
!
crypto pki trustpoint ca-server
revocation-check crl
rsakeypair ca-server
!
!
crypto pki certificate chain ca-server
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 63612D73 65727665 72301E17 0D033093 33303831
36333335 395A170D 31323033 30373136 33333539 5A301431 13010006 35504030
13096361 2D736572 76657230 819F500D 06092A86 4886F700 01010105 003818D
000308189 0281100 99750598 EF4AP984 823DEP7662F33BB3A3 81C2DC2F D9B4040B
99FB6020 22243DC6 B99F24C8 A543D7DB DDB3038 2E36208C D0FD4D15 EAF0DA69
C1B0302B 87CEC34B 8646593F 0185AF02 0B86A3F3 5ESC3880 A992CD44 79F13403
411CC61F 07CEB4D9 0E9C7B2 AFA0A899 5A3B6C87 73111F06 128465DA A45291F8
F82835DC 657487E7 02030100 0A363330 61300F06 3551D103 0101FF04 05030031
01FF300E 0603551D 0F0101FF 04040302 0A363330 61300F06 0603B461 CD301830 1680417B
D032B87B F3F70F1A 579B7C1E 1B42E472 5CCD6030 1D060355 1D0E0416 04178BD0
328FB7B3 F70F1A59 7B7C1E1B 42B4472C CD60000D 06092A86 4886F700 01010045
00030881 053838FA 628804EF E9F619D9 3D72E299C 90747B2C AE33A563 8AF30576
78F6E7D4 5F1E2B7B 04936FDF 78A09432 5348849D F79E17F5 70B23C92 2C1535D0
506D0C35 99335012 84B4343C 050FD3C9 6E7B1D63 41ACC2B5 2B02432D BA2CC2CF
E397DE4A 09C208AC 04BB2D8 E6488815 EB12F1E0 19072D55 D5D11A99 739144D8
279A84E ED
quit
! interface Ethernet1/0
  ip address 209.165.200.232 255.255.255.224
! ip http server

To obtain the CA and device certificates, enter the crypto pki authenticate ca-server and crypto pki enroll ca-server commands. To initiate a connection between the initiator and the responder, enter the following command at the initiator's CLI:

ping 209.165.200.230 source 209.165.200.226

The output of the command is as follows:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-SA_UP: SA UP.
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms

Enter the following show commands in the responder's CLI to display the session details:

show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 1.1.1.1 port 500
IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.227/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 209.165.200.226
Active SAs: 2, origin: dynamic crypto map
Example: Configuring Crypto Map- and dVTI-Based IKEv2 Peers

The following example shows how to configure crypto map and dVTI-based IKEv2 peers using the preshared key authentication method between a static crypto map IKEv2 initiator and a dVTI-based IKEv2 responder. The initiator configuration is as follows:

crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
!
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
!
crypto ikev2 keyring v2-kr1
  peer abc
  address 0.0.0.0 0.0.0.0
  pre-shared-key abc
!
!
crypto ikev2 profile prof
  match fvrf any
  match identity remote address 0.0.0.0
  authentication local pre-share
  authentication remote pre-share
  keyring v2-kr1
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
  set peer 206.165.200.235
  set transform-set trans
  set ikev2-profile prof
  match address ikev2list
!
interface Loopback0
  ip address 206.165.200.226 255.255.255.224
!
interface Ethernet0/0
  ip address 206.165.200.227 255.255.255.224
crypto map cmap
!
ip route 206.165.200.229 255.255.255.224 206.165.200.235
!
ip access-list extended ikev2list
   permit ip host 206.165.200.227 host 206.165.200.235
   permit ip 206.165.200.233 255.255.255.224 206.165.200.229 255.255.255.224

The responder configuration is as follows:

crypto ikev2 proposal prop-1
   encryption aes-cbc-128
   integrity sha1
   group 14
!
crypto ikev2 policy pol-1
   match fvrf any
   proposal prop-1
!
crypto ikev2 keyring v2-kr1
   peer cisco
   address 0.0.0.0 0.0.0.0
   pre-shared-key cisco
!
!
crypto ikev2 profile prof
   match fvrf any
   match identity remote address 0.0.0.0
   authentication local pre-share
   authentication remote pre-share
   keyring v2-kr1
   virtual-template 1
!
crypto ipsec transform-set set esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile vi
   set transform-set set
   set ikev2-profile prof
!
interface Loopback0
   ip address 206.165.200.230 255.255.255.224
!
interface Ethernet0/0
   ip address 206.165.200.235 255.255.255.224
!
interface Virtual-Template1 type tunnel
   ip unnumbered Ethernet0/0
   ip mtu 1000
   tunnel source Ethernet0/0
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile vi
!

To initiate a connection between the initiator and the responder, enter the following command at the initiator’s CLI:

ping 206.165.200.230 source 206.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 206.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 206.165.200.226
IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local traffic selector = Address Range: 206.165.200.226-206.165.200.226 Protocol: 1 Port Range: 0-65535;
IKEV2-5-SA_UP: SA UP

Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms

Enter the following show command in an Easy VPN server to display the session details:

```
show crypto session
Crypto session current status
Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 206.165.200.227 port 500
IKEv2 SA: local 206.165.200.235/500 remote 206.165.200.227/500 Active
IPSEC FLOW: permit ip 206.165.200.229/255.255.255.224 206.165.200.233/255.255.255.224
Active SAs: 2, origin: crypto map
```

```
show crypto ikev2 sa detail
Tunnel-id Local Remote fvrf/ivrf Status
1 206.165.200.235/500 206.165.200.227/500 (none)/(none) READY
    Life/Active Time: 86400/8 sec
    CE id: 1001, Session-id: 1
    Status Description: Negotiation done
    Local spi: 305F610F57428834 Remote spi: D9D183B5689AEDCD
    Local req msg id: 0 Remote req msg id: 2
    Local next msg id: 0 Remote next msg id: 2
    Local req queued: 0 Remote req queued: 2
    Local window: 5 Remote window: 5
    DPD configured for 0 seconds, retry 0
    NAT-T is not detected
```

```
show crypto route
VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
S - Static Map ACLs
```

```
Routes created in table GLOBAL DEFAULT
206.165.200.233/255.255.255.224 [1/0] via 206.165.200.227 tag 0
  on Virtual-Access2 RRI
```

---

**Example: Configuring IPsec Using sVTI-Based IKEv2 Peers**

The following example shows how to configure IPsec using the preshared key authentication method between an sVTI IKEv2 initiator and an sVTI IKEv2 responder. The initiator configuration is as follows:

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
!
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
!
crypto ikev2 keyring v2-kr1
  peer abc
  address 209.165.200.225
  pre-shared-key abc
```

---

**Example: Configuring IPsec Using sVTI-Based IKEv2 Peers**

The following example shows how to configure IPsec using the preshared key authentication method between an sVTI IKEv2 initiator and an sVTI IKEv2 responder. The initiator configuration is as follows:

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
!
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
!
crypto ikev2 keyring v2-kr1
  peer abc
  address 209.165.200.225
  pre-shared-key abc
```

---

**Example: Configuring IPsec Using sVTI-Based IKEv2 Peers**

The following example shows how to configure IPsec using the preshared key authentication method between an sVTI IKEv2 initiator and an sVTI IKEv2 responder. The initiator configuration is as follows:

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-128
  integrity sha1
  group 14
!
crypto ikev2 policy pol-1
  match fvrf any
  proposal prop-1
!
crypto ikev2 keyring v2-kr1
  peer abc
  address 209.165.200.225
  pre-shared-key abc
```
crypto ikev2 profile prof
    match fvrf any
    match identity remote address 209.165.200.231 255.255.255.224
    authentication local pre-share
    authentication remote pre-share
    keyring v2-kr1

crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac

crypto ipsec profile ipsecprof
    set transform-set trans
    set ikev2-profile prof

interface Loopback0
    ip address 209.165.200.226 255.255.255.224

interface Tunnel0
    ip address 10.0.0.1 255.255.255.0
    tunnel source 209.165.200.231
    tunnel mode ipsec ipv4
    tunnel destination 209.165.200.225
    tunnel protection ipsec profile ipsecprof

interface Ethernet0/0
    ip address 209.165.200.231 255.255.255.224

ip route 209.165.200.229 255.255.255.224 Tunnel0

The responder configuration is as follows:

crypto ikev2 proposal prop-1
    encryption aes-cbc-128
    integrity sha1
    group 14

crypto ikev2 policy pol-1
    match fvrf any
    proposal prop-1

crypto ikev2 keyring v2-kr1
    peer abc
    address 209.165.200.231
    pre-shared-key abc

crypto ikev2 profile prof
    match fvrf any
    match identity remote address 209.165.200.231 255.255.255.224
    authentication local pre-share
    authentication remote pre-share
    keyring v2-kr1

crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac

crypto ipsec profile ipsecprof
    set transform-set trans
    set ikev2-profile prof

crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
  ip address 209.165.200.230 255.255.255.224
!
interface Tunnel0
  ip address 10.0.0.2 255.255.255.0
  tunnel source 209.165.200.225
  tunnel mode ipsec ipv4
  tunnel destination 209.165.200.231
  tunnel protection ipsec profile ipsecprof
!
interface Ethernet0/0
  ip address 209.165.200.231 255.255.255.224
!
ip route 209.165.200.233 255.255.255.224 Tunnel0

With sVTI on IKEv2 peers, the session is initiated only when the sVTI interfaces are enabled. In other words, network traffic is not required to initiate the session. To verify the traffic between the initiator and the responder, enter the following command at the initiator's CLI:

```
ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

Enter the following `show` command in the initiator's CLI to display the session details:

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
  IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.225/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
  Active SAs: 2, origin: crypto map
show crypto ikev2 sa detailed
Tunnel-id Local Remote fvrfr/ivrf Status
1 209.165.200.231/500 209.165.200.225/500 (none)/(none) READY
  Life/Active Time: 86400/21 sec
  CE id: 1002, Session-id: 2
  Status Description: Negotiation done
  Local spi: 687752902752A6FD Remote spi: C9DCCFC65493D14F
  Local id: smap-initiator
  Remote id: dmap-responder
  Local req mag id: 2 Remote req mag id: 0
  Local next mag id: 2 Remote next mag id: 0
  Local req queued: 2 Remote req queued: 0
  Local window: 5 Remote window: 5
  DPD configured for 0 seconds, retry 0
NAT-T is not detected
```
Example: Configuring IKEv2 on DMVPN Networks

DMVPN uses a tunnel protection CLI that is identical between IKEv1 and IKEv2. The IPsec profile applied on a DMVPN tunnel only refers to an IKEv2 profile. The DMVPN Hub configuration is as follows:

crypto ikev2 keyring cisco-ikev2-keyring
peer dmvpn-node
description symmetric pre-shared key for the hub/spoke
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123
crypto ikev2 profile cisco-ikev2-profile
keyring cisco-ikev2-keyring
authentication pre-shared
match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
set transform-set cisco-ts
set ikev2-profile cisco-ikev2-profile
! interface Tunnel 0
description This is the Legacy IKEV1 facing tunnel on the hub
ip address 1.1.1.99 255.255.255.0
no ip redirects
ip nhrp map multicast dynamic
ip nhrp network-id 99
ip nhrp redirect
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec
!
interface Tunnel1
description This would be the new IKEv2 facing tunnel on the hub
ip address 2.2.2.99 255.255.255.0
no ip redirects
ip nhrp map multicast dynamic
ip nhrp network-id 100
no ip split-horizon eigrp 1
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec-ikev2

The IKEv2 configuration is as follows:

crypto ikev2 profile cisco-ikev2-profile
keyring cisco-ikev2-keyring
authentication pre-shared
match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
set transform-set cisco-ts
set ikev2-profile cisco-ikev2-profile
interface Tunnel1
ip address 2.2.2.11 255.255.255.0
no ip redirects
ip nhrp map 2.2.2.99 22.22.22.99
ip nhrp map multicast 22.22.22.99
ip nhrp network-id 100 ? Keep this same for all IKEv2 spokes for clarity
ip nhrp nhs 2.2.2.99 ? This points to the hub’s IKEv2 facing interface
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec-ikev2
Example: Configuring IKEv2 on DMVPN Networks