付録：IKEv2 およびレガシー VPN

このモジュールでは、暗号マップ ベースの設定で IKEv2 を設定する例を示します。

（注） 暗号マップは、レガシー設定の構造と見なされます。既存の暗号マップ ベースの設定を移行して、トンネル保護および仮想インターフェイスを使用することをお勧めします。

例：事前共有キー認証方式を使用する暗号マップベースの IKEv2 ピアの設定

次の例に、スタティック暗号マップ IKEv2 発信側とダイナミック暗号マップ IKEv2 応答側との間で事前共有キー認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
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
  pre-shared-key abc
 !
```

```
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote fqdn dmap-responder
 identity local fqdn smap-initiator
 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 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
!
ip route 209.165.200.229 255.255.255.224 209.165.200.225
!
ip access-list extended ikev2list
 permit ip any any
!
```

応答側の設定は次のとおりです。

```
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
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
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-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
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
```

セッションの詳細を表示するには、次の **show** コマンドを入力します。

```
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
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify:
 PSK
      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
```

例：証明書認証方式を使用する暗号マップベースの IKEv2 ピアの設定

次の例は、スタティック暗号マップ IKEv2 発信側、ダイナミック暗号マップ IKEv2 応答側、および CA サーバーの間で証明書認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
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
  308201AF 30820118 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32353132 355A170D 31313033 31303132 35313235 5A301A31 18301606 092A8648
  86F70D01 09021609 494E4954 4941544F 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100A47E 8C58BA89 8CCDC5A4 5A63BD29 C331A2A5 393F4616
  6B43FD2E 5ED4C81A 913E3B13 33A9B2DC CFC30391 24BB0DC8 B28FD6F1 C008D101
  34C10062 30F88CF7 9D630203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 E77C74E7 183AB530 83DC531B 1DE3DA1D 914A925D
  300D0609 2A864886 F70D0101 04050003 81810042 21934B77 7E485E6F EE717D75
  6407B361 45190CEF E1A29CF2 6FA29E9A 5ECC1CEE B273533D 1453F6CE 1FDDA747
  7E701B4B 2A2AE53F D67C2345 952325BA 30950435 0706C5EE A7A8B414 CFEEB7A2
  9CD46F8F 3F663268 A20C4CCF E75D61EF 03FBA85D EDD6B26E 63653F09 F97DAFA6
  6C76E44E C9CA3FDC 6CD85D30 169A1D9E 4E870B
        quit
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
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-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
!
```

応答側の設定は次のとおりです。

```
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 18301606 092A8648
  86F70D01 09021609 52455350 4F4E4445 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100B517 EB8E64E1 B58CB014 07B3A6AF E6B69577 87486367
  9471B1DA BC66B847 DFA5073A 82121332 E787EA2D 3C433514 39033074 4095E7C7
  67A387A1 EBD24692 A76F0203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 DFF2401C 53276D96 89DE8C0A 786CCA71 C9EA792B
  300D0609 2A864886 F70D0101 04050003 8181002C 6E334273 CB832A95 3DDC6293
  669E416C A134D543 20952BC3 14A5C0B0 03AE011C 963AF523 C7C5C935 4FE9B2A5
  F24B3161 4D0D723A FA428BD1 85ADF172 B4007067 43C27D8A 1F74ED3D DEBE9F73
  1F515355 E77E766C AEACC303 39457991 29AB090C 99E21B5B 60DCB2C8 780B4479
  3EB3D46B B66C8C26 15311A7A B7A4ED97 32727C
        quit
```

```
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
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
```

CA サーバーの設定は次のとおりです。

```
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 0D303930 33303831
  36333335 395A170D 31323033 30373136 33333539 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 99750598 EF4AF8B4 823DEF66 2F3BBA31 81C2DC5F D9B4040B
  99FB6020 22243CD6 B9F24C84 A543D7DB DD0B3018 2E36208C D0FD4015 EAF0DA69
  C1B0302B 87CEC34B 8646593F 0185AF02 0B86A3F3 5E5C3880 A992CD4A 79F13403
  411CC61F 07CEB4D9 0E967CB2 FAE0A899 5A3B6C87 73111F06 128465DA A45291F8
  F828C5DC 657487E7 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 1680147B
  D032BFB7 B3F70F1A 597B7C1E 1B42E472 5CCD6030 1D060355 1D0E0416 04147BD0
  32BFB7B3 F70F1A59 7B7C1E1B 42E4725C CD60300D 06092A86 4886F70D 01010405
  00038181 003838FA 628804EF E9FF69D9 3D5E299C 29074B2C AE33A563 8AF75976
  78FB68D4 5EF1E27B 04936FDF 78A09432 5348849D F79E17F5 70B233C9 2C1535D0
  506F0C35 99335012 84BBA3DC 050FD3C9 6E7B1D63 41ACC2B5 2B02432D BA2CC2CF
  E379DEA0 A9C208AC 0BEBB2D8 E6488815 EB12F1E0 19072D55 D5D11A49 739144D8
  271A842E ED
        quit
!
interface Ethernet1/0
 ip address 209.165.200.232 255.255.255.224
!
ip http server
```

CA およびデバイス証明書を取得するには、**crypto pki authenticate ca-server** コマンドおよび **crypto pki enroll ca-server** コマンドを入力します。発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
```

コマンドの出力は次のようになります。

```
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-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
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
```

セッションの詳細を表示するには、応答側の CLI に次の **show** コマンドを入力します。

```
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
show crypto ikev2 sa detailed
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         209.165.200.231/500 209.165.200.227/500  (none)/(none)                  READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA, Auth verify:
 RSA
      Life/Active Time: 86400/846 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: F79756E978ED41C7       Remote spi: 188FB9A119516D34
      Local id: hostname=RESPONDER
      Remote id: hostname=INITIATOR
      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
```

例：暗号マップ ベースおよび dVTI ベースの IKEv2 ピアの設定

次の例は、スタティック クリプト マップ IKEv2 発信側と dVTI に基づく IKEv2 応答側との間に事前共有キー認証方式を使用し、クリプト マップと dVTI ベースの IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
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
```

応答側の設定は次のとおりです。

```
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
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
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; remote traffic selector = Address Range: 206.165.200.230-206.165.200.230
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
```

次の **show** コマンドを Easy VPN サーバーに入力すると、セッションの詳細が表示されます。

```
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
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/8 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 305F610F57428834       Remote spi: D9D183B5689AEDCD
      Local id: 206.165.200.235
      Remote id: 206.165.200.227
      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
```

例： sVTI ベース IKEv2 ピアを使用した IPSec の設定

次の例は、sVTI IKEv2 発信側と sVTI IKEv2 応答側との間に事前共有キー認証方式を使用する IPsec の設定方法を示します。発信側の設定は次のとおりです。

```
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
!
```

応答側の設定は次のとおりです。

```
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
```

IKEv2 ピアの sVTI では、セッションは sVTI インターフェイスが有効なときにだけ開始されます。つまり、セッションの開始のためにネットワーク トラフィックは必要ありません。発信側と応答側との間のトラフィックを確認するには、発信側の CLI で次のコマンドを入力します。

```
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-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.23 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
```

次の **show** コマンドを発信側の CLI に入力すると、セッションの詳細が表示されます。

```
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                fvrf/ivrf            Status
1   209.165.200.231/500  209.165.200.225/500           (none)/(none)        READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      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
```

例：DMVPN ネットワークでの IKEv2 の設定

DMVPN は、IKEv1 と IKEv2 の間で同一のトンネル保護 CLI を使用します。DMVPN トンネルに適用される IPSec プロファイルは、IKEv2 プロファイルのみを参照します。DMVPN ハブの設定は次のとおりです。

```
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
```

IKEv2 の設定は次のとおりです。

```
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
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。