PSK によるサイト間 VPN の IOS IKEv2 デバッグのトラブルシューティング テクニカルノート

目次

概要

このドキュメントでは、Cisco IOS® 上での、事前共有キー（PSK）を使用したインターネットキー交換バージョン 2（IKEv2）のデバッグについて説明します。 また、コンフィギュレーションの特定のデバッグ行の解釈方法に関する情報を提供します。

前提条件

要件

IKEv2 のパケット交換についての知識があることが推奨されます。 詳細については、『IKEv2 のパケット交換とプロトコル レベル デバッグ』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- インターネット キー交換バージョン 2（IKEv2）

- Cisco IOS 15.1(1)T 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

主な問題

IKEv2 のパケット交換は IKEv1 のパケット交換とは根本的に異なります。 IKEv1 では、6 つのパケットから成るフェーズ 1 の交換と、それに続く 3 つのパケットから成るフェーズ 2 の交換に明確に分けられていました。 IKEv2 の交換では変動します。 パケット交換の相違点と説明の詳細については、『IKEv2 のパケット交換とプロトコル レベル デバッグ』を参照してください。

ルータの設定

このセクションでは、このドキュメントで使用するコンフィギュレーションを示します。

ルータ 1

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.101 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.2
tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 policy site-pol
proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
peer peer1
address 10.0.0.2 255.255.255.0
hostname host1
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
```

```
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

ルータ 2

```
crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 keyring KEYRNG
peer peer2
address 10.0.0.1 255.255.255.0
hostname host2
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.102 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.1
tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

トラブルシューティング

ルータのデバッグ

このドキュメントで使用するデバッグ コマンドは次のとおりです。

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

ルータ 1 (発信側) のメッセージの説明	デバッグ	ルータ 2 (応答側) のメッセージの説明
ルータ 1 が暗号化 ACL と一致するピア ASA 10.0.0.2 宛のパケットを受信します。 SA の作成を開始します。	*Nov 11 20:28:34.003: IKEv2:Got a packet from dispatcher *Nov 11 20:28:34.003: IKEv2: 朴キューを離れた項目の処理 *Nov 11 19:30:34.811: IKEv2:% Getting preshared key by address 10.0.0.2 *Nov 11 19:30:34.811: IKEv2:Adding Proposal PHASE1-prop to toolkit policyle *Nov 11 19:30:34.811: IKEv2:(1): Choosing IKE profile IKEV2-SETUP *Nov 11 19:30:34.811: IKEv2:New ikev2 sa request admitted *Nov 11 19:30:34.811: IKEv2:Incrementing outgoing negotiating sa count by one *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_IKE_POLICY	
最初の 1 組のメッセージは IKE_SA_INIT 交換です。 これらのメッセージでは暗号化アルゴリズムのネゴシエーション、ナンスの交換、Diffie-Hellman 交換を行います。 **関連コンフィギュレーション** `ikev2 PHASE1-prop 3des aes-cbc-128 sha1 2 ikev2 KEYRNG peer1 10.0.0.2 255.255.255.0 host1 Cisco cisco`	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_SET_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Setting configured policies *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_CHK_AUTH4PKI *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GEN_DH_KEY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000	

(I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_CONFIG_MODE
*Nov 11 19:30:34.811: IKEv2:IKEv2 initiator - no config data to send in IKE_SA_INIT exch
*Nov 11 19:30:34.811: IKEv2:No config data to send to toolkit:
*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000
(I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_BLD_MSG
*Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: DELETE-REASON
*Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
*Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, **flags:** INITIATOR Message id: 0, length: 344
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 56
last proposal: 0x0, reserved: 0x0, length: 52
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 5 最後のトランスフォーム: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
KE Next payload: N, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0
N Next payload: VID, reserved: 0x0, length: 24
VID Next payload: VID, reserved: 0x0, length: 23
VID Next payload: NOTIFY, reserved: 0x0, length: 21
NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: NONE, reserved: 0x0, length: 28
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.814: IKEv2:Got a packet from dispatcher
*Nov 11 19:30:34.814: IKEv2:Processing an item off the pak queue
*Nov 11 19:30:34.814: IKEv2:New ikev2 sa request

発信側は IKE_INIT_SA パケットを作成します。 このパケットには、次のものが含まれています。 ISAKMP ヘッダー（SPI、バージョン、フラグ）、SAi1（IKE の発信側がサポートする暗号化アルゴリズム）、KEi（発信側の DH 公開キーの値）、N（発信側のナンス）。

応答側が IKE_INIT_SA を受信します。

admitted
*Nov 11 19:30:34.814: IKEv2:Incrementing incoming negotiating sa count by one
*Nov 11 19:30:34.814: IKEv2:Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 344
Payload contents:
 SA Next payload: KE, reserved: 0x0, length: 56
 last proposal: 0x0, reserved: 0x0, length: 52
 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 5 最後のトランスフォーム: 0x3, reserved: 0x0: length: 8
  type: 1, reserved: 0x0, id: 3DES
  last transform: 0x3, reserved: 0x0: length: 12
  type: 1, reserved: 0x0, id: AES-CBC
  last transform: 0x3, reserved: 0x0: length: 8
  type: 2, reserved: 0x0, id: SHA1
  last transform: 0x3, reserved: 0x0: length: 8
  type: 3, reserved: 0x0, id: SHA96
  last transform: 0x0, reserved: 0x0: length: 8
  type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
 KE Next payload: N, reserved: 0x0, length: 136
  DH group: 2, Reserved: 0x0
 N Next payload: VID, reserved: 0x0, length: 24

応答側がピア用の SA の作成を開始します。

*Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next payload: VID, reserved: 0x0, length: 23
*Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21
*Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28
  Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: NONE, reserved: 0x0, length: 28
  Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event: **EV_RECV_INIT**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: **EV_VERIFY_MSG**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4

応答側は IKE_INIT メッセージを確認して次の処理を行います。（1）発信側が提示した中から暗号化スイートを選択し、（2）自身の DH 秘密キーを計算し、（3）この IKE_SA

(R) MsgID = 00000000 CurState: R_INIT Event: **EV_INSERT_SA**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_INIT Event: **EV_GET_IKE_POLICY**
*Nov 11 19:30:34.814: IKEv2:Adding Proposal default to toolkit policy
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_INIT Event: **EV_PROC_MSG**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_INIT Event: EV_DETECT_NAT
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Process NAT discovery notify
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Processing nat detect src notify
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Remote address matched
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Processing nat detect dst notify
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Local address matched
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):No NAT found
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_INIT Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_SET_POLICY
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1): **Setting configured policies**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_CHK_AUTH4PKI
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_PKI_SESH_OPEN
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Opening a PKI session
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: **EV_GEN_DH_KEY**
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4

用のすべてキーの導出元となる SKEYID の値を計算します。 以降のすべてのメッセージは、ヘッダーを除いてすべて暗号化および認証されます。 暗号化および整合性の保護に使用されるキーは SKEYID から得られ、次のものがあります。 SK_e（暗号化）、SK_a（認証）、SK_d が計算され、さらに CHILD_SA のキーの材料の計算に使用されます。SK_e と SK_a は、方向ごとに別に計算されます。

関連コンフィギュレーション

```
ikev2 PHASE1-prop 3des aes-cbc-128 sha1 2 ikev2 KEYRNG peer2 10.0.0.1 255.255.255.0 host2 Cisco cisco
```

(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: **EV_OK_RECD_DH_PUBKEY_RESP**
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: **EV_GEN_DH_SECRET**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT
*Nov 11 19:30:34.822: IKEv2:% Getting preshared key by address 10.0.0.1
*Nov 11 19:30:34.822: IKEv2:Adding Proposal default to toolkit policy
*Nov 11 19:30:34.822: IKEv2:(2): Choosing IKE profile IKEV2-SETUP
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: **EV_GEN_SKEYID**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1): **Generate skeyid**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_GET_CONFIG_MODE
*Nov 11 19:30:34.822: IKEv2:IKEv2 responder - no config data to send in IKE_SA_INIT exch
*Nov 11 19:30:34.822: IKEv2:No config data to send to toolkit:
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_BLD_MSG
*Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: DELETE-REASON
*Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
*Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP

*Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, **flags: 応答側 MSG-RESPONSE** メッセージID: 0, length: 449
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 48
last proposal: 0x0, reserved: 0x0, length: 44
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 最後のトランスフォーム: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
KE Next payload: N, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0
N Next payload: VID, reserved: 0x0, length: 24
VID Next payload: VID, reserved: 0x0, length: 23
VID Next payload: NOTIFY, reserved: 0x0, length: 21
NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: CERTREQ, reserved: 0x0, length: 28
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
CERTREQ Next payload: NOTIFY, reserved: 0x0, length: 105
Cert encoding Hash and URL of PKIX
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Next payload: NONE, reserved: 0x0, length: 8
Security protocol id: IKE, spi size: 0, type: HTTP_CERT_LOOKUP_SUPPORTED

ルータ 2 は、ASA1 が受け取る IKE_SA_INIT 交換の応答側メッセージを作成します。このパケットには次が含まれます。ISAKMP ヘッダー（SPI、バージョン、フラグ）、SAr1（IKE の応答側が選択した暗号化アルゴリズム）、KEr（応答側の DH 公開キーの値）、応答側のナンス。

*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Cisco DeleteReason Notify is enabled
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_CHK4_ROLE
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event: **EV_START_TMR**

ルータ 2 は、ルータ 1 に応答側のメッセージを送信します。

*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_WAIT_AUTH Event: EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2: **New ikev2 sa request admitted** *Nov 11 19:30:34.822: IKEv2: **1 つによる発信ネゴシエート sa 数を増分すること** *Nov 11 19:30:34.823: IKEv2:Got a packet from dispatcher	
ルータ 1 は、ルータ 2 からの IKE_SA_INIT 応答パケットを受信します。	*Nov 11 19:30:34.823: IKEv2:Got a packet from dispatcher	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event: **EV_START_TMR** 応答側は認証プロセスのタイマーを開始します。
	*Nov 11 19:30:34.823: IKEv2:Processing an item off the pak queue *Nov 11 19:30:34.823: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: **応答側 MSG-RESPONSE** メッセージID: 0, length: 449 Payload contents: **SA** Next payload: KE, reserved: 0x0, length: 48 last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 最後のトランスフォーム: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **KE** Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 **N** Next payload: VID, reserved: 0x0, length: 24	
ルータ 1 は応答を確認して次の処理を行います。（1）発信側の DH 秘密キーを計算し、（2）発信側の SKEYID を生成します。	*Nov 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next payload: VID, reserved: 0x0, length: 23 *Nov 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21 *Nov 11 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP	

*Nov 11 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: CERTREQ, reserved: 0x0, length: 28
   Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
 CERTREQ Next payload: NOTIFY, reserved: 0x0, length: 105
   Cert encoding Hash and URL of PKIX

*Nov 11 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: IKE, spi size: 0, type: HTTP_CERT_LOOKUP_SUPPORTED
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_WAIT_INIT Event: EV_RECV_INIT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK4_NOTIFY
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_VERIFY_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_PROC_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_DETECT_NAT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Process NAT discovery notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing nat detect src notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Remote address matched
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing nat detect dst notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Local address matched
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):No NAT found
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK_NAT_T

*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: **EV_GEN_DH_SECRET**
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_NO_EVENT
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: **EV_GEN_SKEYID**
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1): **Generate skeyid**
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Cisco DeleteReason Notify is enabled
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_CHK4_ROLE
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_GET_CONFIG_MODE
*Nov 11 19:30:34.831: IKEv2:Sending config data to toolkit
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_EAP

発信側は IKE_AUTH 交換を開始し、認証ペイロードを生成します。 IKE_AUTH パケットには次が含まれます。 ISAKMP ヘッダー（SPI、バージョン、フラグ）、IDi（発信側の

*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: **EV_GEN_AUTH**
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event:

ID）、AUTH ペイロード、SAi2（IKEv1 のフェーズ 2 トランスフォーム セット交換と同様の SA の開始）、TSi と TSr（発信側と応答側のトラフィック セレクタ）。これらには、暗号化されたトラフィックを送受信するための発信側と応答側の送信元アドレスと宛先アドレスがそれぞれ含まれています。このアドレス範囲は、宛先および送信元がこの範囲内であるすべてのトラフィックをトンネルすることを指定します。提案が応答側で受け入れ可能な場合、応答側は同一の TS ペイロードを送り返します。トリガー パケットと一致する proxy_ID ペア用に最初の CHILD_SA が作成されます。

関連コンフィギュレーション `IPSec TS esp-3des esp-sha-hmac IPSec phse2-prof transform-set TS ikev2-profile IKEV2-SETUP`

EV_OK_AUTH_GEN
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_SEND_AUTH
*Nov 11 19:30:34.831: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE
*Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT
*Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE
*Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT
*Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS
Payload contents:
VID Next payload: IDi, reserved: 0x0, length: 20
IDi Next payload: AUTH, reserved: 0x0, length: 12
Id type: IPv4 address, Reserved: 0x0 0x0
AUTH Next payload: CFG, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
CFG Next payload: SA, reserved: 0x0, length: 309
cfg type: CFG_REQUEST, reserved: 0x0, reserved: 0x0
*Nov 11 19:30:34.831: **SA** Next payload: TSi, reserved: 0x0, length: 40
last proposal: 0x0, reserved: 0x0, length: 36
Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 最後のトランスフォーム: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
NOTIFY(INITIAL_CONTACT) Next payload: NOTIFY, reserved: 0x0, length: 8
Security protocol id: IKE, spi size: 0, type: INITIAL_CONTACT
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: IKE, spi size: 0, type:
ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE,
reserved: 0x0, length: 8
Security protocol id: IKE, spi size: 0, type:
NON_FIRST_FRAGS

*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Next payload:
ENCR, version: 2.0 Exchange type: IKE_AUTH,
flags: INITIATOR Message id: 1, **length**: 556
Payload contents:
ENCR Next payload: VID, reserved: 0x0, length: 528

*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(I) MsgID = 00000001 **CurState: I_WAIT_AUTH** Event:
EV_NO_EVENT
*Nov 11 19:30:34.832: IKEv2:Got a packet from dispatcher
*Nov 11 19:30:34.832: IKEv2:Processing an item off the
pak queue
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Request has
mess_id 1; expected 1 through 1
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Next payload:
ENCR, version: 2.0 Exchange type: IKE_AUTH,
flags: INITIATOR Message id: 1, **length**: 556
Payload contents:
*Nov 11 19:30:34.832: IKEv2:Parse Vendor Specific
Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0,
length: 20
IDi Next payload: AUTH, reserved: 0x0, length: 12
Id type: IPv4 address, Reserved: 0x0 0x0
AUTH Next payload: CFG, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
CFG Next payload: SA, reserved: 0x0, length: 309
cfg type: CFG_REQUEST, reserved: 0x0, reserved: 0x0
*Nov 11 19:30:34.832: attrib type: internal IP4 DNS,
length: 0
*Nov 11 19:30:34.832: attrib type: internal IP4 DNS,
length: 0
*Nov 11 19:30:34.832: attrib type: internal IP4 NBNS,
length: 0
*Nov 11 19:30:34.832: attrib type: internal IP4 NBNS,
length: 0
*Nov 11 19:30:34.832: attrib type: internal IP4 subnet,
length: 0
*Nov 11 19:30:34.832: attrib type: application version,
length: 257
attrib type: Unknown - 28675, length: 0
*Nov 11 19:30:34.832: attrib type: Unknown - 28672,
length: 0
*Nov 11 19:30:34.832: attrib type: 未知- 28692、長さ: 0
*Nov 11 19:30:34.832: attrib type: 未知- 28681、長さ: 0
*Nov 11 19:30:34.832: attrib type: Unknown - 28674,

ルータ 2 はルータ 1 から受信した認証データを確認します。

関連コンフィギュレーション `ipsec ikev2 ipsec AES256 aes-256 sha-1 md5`

```
length: 0
*Nov 11 19:30:34.832:   SA  Next payload: TSi, reserved:
0x0, length: 40
  last proposal: 0x0, reserved: 0x0, length: 36
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 最後
のトランスフォーム: 0x3, reserved: 0x0: length: 8
    type: 1, reserved: 0x0, id: 3DES
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
    last transform: 0x0, reserved: 0x0: length: 8
    type: 5, reserved: 0x0, id: Don't use ESN
 TSi Next payload: TSr, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 0.0.0.0, end addr: 255.255.255.255
 TSr Next payload: NOTIFY, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 0.0.0.0, end addr: 255.255.255.255
 *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_RECV_AUTH
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_NAT_T
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_PROC_ID
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Received valid
parameteres in process id
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_F
OR_PROF_SEL
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.833: IKEv2:(1): Choosing IKE profile
IKEV2-SETUP
*Nov 11 19:30:34.833: IKEv2:% Getting preshared key by
address 10.0.0.1
*Nov 11 19:30:34.833: IKEv2:% Getting preshared key by
address 10.0.0.1
*Nov 11 19:30:34.833: IKEv2:Adding Proposal default to
toolkit policy
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Using IKEv2
```

ルータ 2 はルータ 1 から受信した IKE_AUTH パケットの応答を作成します。 この応答パケットには次が含まれます。 ISAKMP ヘッダー（SPI、バージョン、フラグ）、IDr（応答側の ID）、AUTH ペイロード、SAr2（IKEv1 のフェーズ 2 トランスフォーム セット交換と同様の SA の開始）、TSi と TSr（発信側と応答側のトラフィック セレクタ）。 これらには、暗号化されたトラフィックを送受信するための発信側と応答側の送信元アドレスと宛先アドレスがそれぞれ含まれています。 このアドレス範囲は、宛先および送信元がこの範囲内であるす

```
profile 'IKEV2-SETUP'
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_SET_POLICY
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Setting
configured policies
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_AUTH4EAP
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_POLREQEAP
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_VERIFY_AUTH
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_CHK4_IC
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_CHK_REDIRECT
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Redirect check is
not needed, skipping it
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_NOTIFY_AUTH_DONE
*Nov 11 19:30:34.833: IKEv2:AAA group authorization is
not configured
*Nov 11 19:30:34.833: IKEv2:AAA user authorization is not
configured
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4
(R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:
EV_CHK_CONFIG_MODE
```

べてのトラフィックをトンネルすることを指定します。これらのパラメータは ASA1 が受信したパラメータと同一です。

*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_SET_RECD_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:Received config data from toolkit:
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_PROC_SA_TS
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_GET_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:Error constructing config reply
*Nov 11 19:30:34.833: IKEv2:No config data to send to toolkit:
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_MY_AUTH_METHOD
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GEN_AUTH
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_CHK4_SIGN
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_OK_AUTH_GEN
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_SEND_AUTH
*Nov 11 19:30:34.833: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE
*Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE
*Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT
*Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, **flags: 応答側 MSG-RESPONSE** メッセージID: 1, **length**: 252

応答側は IKE_AUTH の応答を送信します。

Payload contents:
ENCR Next payload: VID, reserved: 0x0, length: 224
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Closing the PKI session
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: **EV_INSERT_IKE**
*Nov 11 19:30:34.834: IKEv2:Store mib index ikev2 1, platform 60
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_GEN_LOAD_IPSEC
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Asynchronous request queued
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **AUTH_DONE** Event: EV_NO_EVENT

発信側が応答側からの応答を受信します。	*Nov 11 19:30:34.834: IKEv2:Got a packet from dispatcher *Nov 11 19:30:34.834: IKEv2:Processing an item off the pak queue	***?Nov 11 19:30:34.840:** IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK_RECD_LOAD_IPSEC ***?Nov 11 19:30:34.840:** IKEv2:(SA ID = 1):Action: Action_Null ***?Nov 11 19:30:34.840:** IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B	応答側はエントリを SAD に追加します。

R_SPI=F94020DD8CB4B9C
4 (R) MsgID = 00000001
CurState: AUTH_DONE
Event: EV_START_ACCT
***?Nov 11 19:30:34.840:**
IKEv2:(SA ID = 1):SM Trace-
> SA:
I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C
4 (R) MsgID = 00000001
CurState: AUTH_DONE
Event: EV_CHECK_DUPE
***?Nov 11 19:30:34.840:**
IKEv2:(SA ID = 1):SM Trace-
> SA:
I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C
4 (R) MsgID = 00000001
CurState: AUTH_DONE
Event: EV_CHK4_ROLE

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, **flags: 応答側 MSG-RESPONSE** メッセージID: 1, **length**: 252
Payload contents:

*Nov 11 19:30:34.834: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDr, reserved: 0x0, length: 20
IDr Next payload: AUTH, reserved: 0x0, length: 12
Id type: IPv4 address, Reserved: 0x0 0x0
AUTH Next payload: SA, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
SA Next payload: TSi, reserved: 0x0, length: 40
last proposal: 0x0, reserved: 0x0, length: 36
Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 最後のトランスフォーム: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255

ルータ 1 はこのパケットの認証データを確認して処理します。 その後、ルータ 1 はこの SA を SAD に追加します。

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload:

SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
   Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
   Security protocol id: IKE, spi size: 0, type: ESP_TFC_NO_SUPPORT

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: IKE, spi size: 0, type: NON_FIRST_FRAGS

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Event: EV_RECV_AUTH
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_NOTIFY
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_MSG
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:Adding Proposal PHASE1-prop to toolkit policy
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Using IKEv2 profile 'IKEV2-SETUP'
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_AUTH_TYPE

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_VERIFY_AUTH
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_EAP
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_NOTIFY_AUTH_DONE
*Nov 11 19:30:34.835: IKEv2:AAA group authorization is not configured
*Nov 11 19:30:34.835: IKEv2:AAA user authorization is not configured
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_SA_TS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Closing the PKI session
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_INSERT_IKE *Nov 11 19:30:34.835: IKEv2:Store mib index ikev2 1, platform 60 *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_GEN_LOAD_IPSEC *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Asynchronous request queued *Nov 11 19:30:34.835: IKEv2:(SA ID = 1): *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_EVENT *Nov 11 19:30:34.835: IKEv2:KMI message 8 consumed. No action taken. *Nov 11 19:30:34.835: 消費される IKEv2:KMI メッセージ 12。 No action taken. *Nov 11 19:30:34.835: IKEv2:No data to send in mode config set. *Nov 11 19:30:34.841: IKEv2:Adding ident handle 0x80000002 associated with SPI 0x9506D414 for session 8 *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK_RECD_LOAD_IPSEC *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_START_ACCT *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):Accounting not required *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **AUTH_DONE** Event: EV_CHK4_ROLE	
発信側でトンネルがアップし、ステータスに [READY] と表示されます。	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001	***?Nov 11 19:30:34.840:** IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
		応答側でトンネルがアップします。応答側のトンネルは通常発信側よりも先に開始されます。

CurState: **READYEvent**: EV_CHK_IKE_ONLY *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READY Event: EV_I_OK	CurState: READY Event: EV_R_OK ***?Nov 11 19:30:34.840:** IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY Event: EV_NO_EVENT

CHILD_SA のデバッグ

この交換は 1 組の要求と応答から成り、IKEv1 ではフェーズ 2 の交換と呼ばれていました。 最初の交換が完了した後に、IKE_SA のどちら側からでも開始できます。

ルータ 1 の CHILD_SA メッセージの説明	デバッグ	ルータ 2 CHILD_SA メッセージ 概要
ルータ 1 が CHILD_SA 交換を開始します。 これは CREATE_CHILD_SA 要求です。 CHILD_SA パケットには一般的に次が含まれます。 • SA HDR (バージョン、フラグ、交換タイプ) • ナンス Ni (オプション)。 最初の交換の際に CHILD_SA が作成されている場合は 2 番目の KE ペイロードとナンスは送信されません。 • SA ペイロード • KEi (キー、オプション)。 CREATE_CHILD_SA 要求には追加の DH 交	*Nov 11 19:31:35.873: IKEv2:Got a packet from dispatcher *Nov 11 19:31:35.873: IKEv2:Processing an item off the pak queue *Nov 11 19:31:35.873: IKEv2:(SA に ID = 2):Request mess_id 3 があります; expected 3 through 7 *Nov 11 19:31:35.873: IKEv2:(**SA ID = 2**):Next payload: ENCR, version: 2.0 Exchange type: **CREATE_CHILD_SA**、フラグ: INITIATOR Message id: **3,** length: 396 Payload contents: **SA** Next payload: N, reserved: 0x0, length: 152 last proposal: 0x0, reserved: 0x0, length: 148 Proposal: 1, Protocol id: IKE, SPI size: 8、#trans: 15 最後のトランスフォーム: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA512 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA384 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA256 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: MD5 last transform: 0x3, reserved: 0x0: length: 8	

換のための KE ペイロードをオプションで含めることができ、これにより CHILD_SA の転送秘密の保証をより強力にできます。SA が別の DH グループを含めることを提案する場合、KEi は、発信側が応答側の受け入れを期待するグループの要素である必要があります。 推測に失敗した場合、CREATE_CHILD_SA の交換は失敗し、別の KEi を使用して再試行を行う必要があります。

- N（Notify ペイロード、オプション）。Notify ペイロードは、エラー状態や状態遷移などの情報データを IKE ピアに送信するために使用されます。 呼出 ペイロードは応答メッセージに（通常要求がなぜ拒否されたか規定 する）、情報 Exchange

```
    type: 3, reserved: 0x0, id: SHA512
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA384
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA256
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: MD596
    last transform: 0x3, reserved: 0x0: length: 8
    type: 4, reserved: 0x0, id:
DH_GROUP_1536_MODP/Group 5
    last transform: 0x0, reserved: 0x0: length: 8
    type: 4, reserved: 0x0, id:
DH_GROUP_1024_MODP/Group 2
  N  Next payload: KE, reserved: 0x0, length: 24
 KE  Next payload: NOTIFY, reserved: 0x0, length: 136
    DH group: 2, Reserved: 0x0

*Nov 11 19:31:35.874: IKEv2:Parse Notify Payload:
SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next
payload: NONE, reserved: 0x0, length: 12
    Security protocol id: IKE, spi size: 0, type:
SET_WINDOW_SIZE

*Nov 11 19:31:35.874: IKEv2:（SA ID = 2):SM Trace->
SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: READY Event: EV_RECV_CREATE_CHILD
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action:
Action_Null
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_INIT Event:
EV_RECV_CREATE_CHILD
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action:
Action_Null
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_INIT Event: EV_VERIFY_MSG
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_INIT Event: EV_CHK_CC_TYPE
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_IKE Event: EV_REKEY_IKESA
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
```

に（IKE 要求のエラーをない報告するため）、または送信側機能を示すか、または要求の意味を修正する他のどのメッセージに現われるかもしれません。この CREATE_CHILD_SA の交換が IKE_SA 以外の既存の SA のキーの再生成を行う場合、REKEY_SA タイプの先行する N ペイロードによってキーを再生成する SA を特定する必要があります。CREATE_CHILD_SA の交換が既存の SA のキーの再生成を行わない場合、N ペイロードは省略する必要があります。

CurState: CHILD_R_IKE Event: EV_GET_IKE_POLICY
*Nov 11 19:31:35.874: IKEv2:% Getting preshared key by address 10.0.0.2
*Nov 11 19:31:35.874: IKEv2:% Getting preshared key by address 10.0.0.2
*Nov 11 19:31:35.874: IKEv2:Adding Proposal PHASE1-prop to toolkit policy
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Using IKEv2 プロファイル 'IKEV2-SETUP
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_IKE Event: EV_PROC_MSG
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_IKE Event: EV_SET_POLICY
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2) : **Setting configured policies**
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_GEN_DH_KEY
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_PUBKEY_RESP
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: **EV_GEN_DH_SECRET**
*Nov 11 19:31:35.881: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003

CurState: CHILD_R_BLD_MSG Event: EV_BLD_MSG
*Nov 11 19:31:35.882: IKEv2:Construct Notify Payload:
SET_WINDOW_SIZE
Payload contents:
 SA Next payload: N, reserved: 0x0, length: 56
 last proposal: 0x0, reserved: 0x0, length: 52
 Proposal: 1, Protocol id: IKE, SPI size: 8、#trans: 4 最後
のトランスフォーム: 0x3, reserved: 0x0: length: 12
  type: 1, reserved: 0x0, id: AES-CBC
  last transform: 0x3, reserved: 0x0: length: 8
  type: 2, reserved: 0x0, id: SHA1
  last transform: 0x3, reserved: 0x0: length: 8
  type: 3, reserved: 0x0, id: SHA96
  last transform: 0x0, reserved: 0x0: length: 8
  type: 4, reserved: 0x0, id:
DH_GROUP_1024_MODP/Group 2
 N Next payload: KE, reserved: 0x0, length: 24
KE Next payload: NOTIFY, reserved: 0x0, length: 136
  DH group: 2, Reserved: 0x0
 NOTIFY(SET_WINDOW_SIZE) Next payload: NONE,
reserved: 0x0, length: 12
  Security protocol id: IKE, spi size: 0, type:
SET_WINDOW_SIZE
*Nov 11 19:31:35.869: IKEv2:（SA ID = 2):Next ペイロー
ド: ENCR, version: 2.0 Exchange
type: CREATE_CHILD_SA、フラグ: INITIATOR Message
id: 2, length: 460
Payload contents:
ENCR Next payload: SA, reserved: 0x0, length: 432
*Nov 11 19:31:35.873: IKEv2:Construct Notify Payload:
SET_WINDOW_SIZE
Payload contents:
 SA Next payload: N, reserved: 0x0, length: 152
last proposal: 0x0, reserved: 0x0, length: 148
Proposal: 1, Protocol id: IKE, SPI size: 8、#trans: 15 最後
のトランスフォーム: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: MD5
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA512

このパケットをルータ 2 が受信します。

last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: MD596
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id:
DH_GROUP_1536_MODP/Group 5
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id:
DH_GROUP_1024_MODP/Group 2
N Next payload: KE, reserved: 0x0, length: 24
KE Next payload: NOTIFY, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0
NOTIFY(SET_WINDOW_SIZE) Next payload: NONE,
reserved: 0x0, length: 12
Security protocol id: IKE, spi size: 0, type:
SET_WINDOW_SIZE
*Nov 11 19:31:35.882: IKEv2:（**SA ID = 2):Next** ペイロード: ENCR, version: 2.0 Exchange
type: **CREATE_CHILD_SA**、フラグ: **応答側 MSG-RESPONSE** メッセージID: **3,** length: 300
Payload contents:
SA Next payload: N, reserved: 0x0, length: 56
last proposal: 0x0, reserved: 0x0, length: 52
Proposal: 1, Protocol id: IKE, SPI size: 8、#trans: 4 最後のトランスフォーム: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id:
DH_GROUP_1024_MODP/Group 2
N Next payload: KE, reserved: 0x0, length: 24
KE Next payload: NOTIFY, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0

*Nov 11 19:31:35.882: IKEv2:Parse Notify Payload:
SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Next
payload: NONE, reserved: 0x0, length: 12
Security protocol id: IKE, spi size: 0, type:
SET_WINDOW_SIZE

*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: **CHILD_I_WAIT** イベント
: **EV_RECV_CREATE_CHILD**

ルータ 2 は CHILD_SA 交換の返信を作成します。 これは CREATE_CHILD_SA 応答です。 CHILD_SA パケットには一般的に次が含まれます。

- SA HDR（バージョン、フラグ、交換タイプ）
- 臨時 Ni（optional）：最初の交換の際に CHILD_SA が作成されている場合は 2 番目の KE ペイロードとナンスは送信されません。
- SA ペイロード
- KEi（キー、オプション）。 CREATE_CHILD_SA 要求には追加の DH 交

*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK4_NOTIFY
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: **EV_VERIFY_MSG**
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_PROC_MSG
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK4_PFS
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_DH_SECRET
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_NO_EVENT
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK_IKE_REKEY
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_SKEYID
*Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Generate skeyid
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: **EV_ACTIVATE_NEW_SA**
*Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_UPDATE_CAC_STATS
*Nov 11 19:31:35.890: IKEv2:New ikev2 sa request

換のための KE ペイロードをオプションで含めることができ、これにより CHILD_SA の転送秘密の保証をより強力にできます。 SA が別の DH グループを含めることを提案する場合、KEi は、発信側が応答側の受け入れを期待するグループの要素である必要があります。 推測に失敗した場合、CREATE_CHILD_SA の交換は失敗し、別の KEi を使用して再試行を行う必要があります。

- N（Notify ペイロード、オプション）。 Notify ペイロードは、エラー状態や状態遷移などの情報データを IKE ピアに送信するために使用されます。 Notify ペイロードは、応答メッセージ（通常は要求が拒否された理由を示す）、INFORMATIO

	activated *Nov 11 19:31:35.890: IKEv2:Failed to decrement count for outgoing negotiating *Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_CHECK_DUPE *Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_OK *Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Processed response with message id 3, Requests can be sent from range 4 to 8 *Nov 11 19:31:35.890: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 **CurState: EXIT** Event: EV_NO_EVENT	NAL 交換（IKE 要求以外のエラーの報告）、またはその他の任意のメッセージに含まれ、送信側の機能を示したり要求の意味を変更したりするために使用されます。 この CREATE_CHILD_SA の交換が IKE_SA 以外の既存の SA のキーの再生成を行う場合、REKEY_SA タイプの先行する N ペイロードによってキーを再生成する SA を特定する必要があります。 CREATE_CHILD_SA の交換が既存の SA のキーの再生成を行わない場合、N ペイロードは省略する必要があります。
ルータ 1 は、ルータ 2 から応答パケットを受信し、CHILD SA のアクティブ化を実行します。	*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):Next payload: ENCR, version: 2.0 Exchange type: **CREATE_CHILD_SA**、フラグ: **応答側 MSG-RESPONSE** メッセージID: **3,** length: 300 Payload contents: ENCR Next payload: SA, reserved: 0x0, length: 272 *Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:	ルータ 2 は応答を送信し、新しい CHILD SA のアクティブ化を実行します。

I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event:
EV_CHK_IKE_REKEY
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_BLD_MSG Event: EV_GEN_SKEYID
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2) : **Generate skeyid**
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE Event:
EV_ACTIVATE_NEW_SA
*Nov 11 19:31:35.882: IKEv2:Store MIB インデックス ikev2 3、プラットフォーム 62
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE Event:
EV_UPDATE_CAC_STATS
*Nov 11 19:31:35.882: IKEv2:New ikev2 sa request activated
*Nov 11 19:31:35.882: IKEv2:Failed to decrement count for incoming negotiating
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE Event: EV_CHECK_DUPE
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE Event: EV_OK
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE Event:
EV_START_DEL_NEG_TMR
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action:
Action_Null
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: EXIT Event: EV_CHK_PENDING
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Sent response with message id 3, Requests can be accepted from range 4 to 8
*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 **CurState: EXIT** Event: EV_NO_EVENT

トンネルの確認

ISAKMP

コマンド

show crypto ikev2 sa detailed

ルータ 1 の出力

```
Router1#show crypto ikev2 sa  detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.0.1/500 10.0.0.2/500 none/none READY
Encr: AES-CBC, keysize: 128,
Hash: SHA96, DH Grp:2,
Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/10 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: E58F925107F8B73F Remote spi: AFD098F4147869DA
Local id: 10.0.0.1
Remote id: 10.0.0.2
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
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

出力されるルータ 2

```
Router2#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.0.2/500 10.0.0.1/500 none/none READY
Encr: AES-CBC, keysize: 128, Hash: SHA96,
DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/37 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: AFD098F4147869DA Remote spi: E58F925107F8B73F
Local id: 10.0.0.2
Remote id: 10.0.0.1
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
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

IPSec

コマンド

show crypto ipsec sa

注: IKEv1 のとは違ってこの出力では、PFS DH グループ値は「PFS として現われます（Y/N）: N, DH group: キーの再生成が発生した後最初のトンネルネゴシエーションの間のどれも」、しかし、右の値現われません。 これは動作が Cisco バグ ID CSCug67056 に説明があるのに、不具合ではないです。

IKEv1 と IKEv2 の違いは、後者で、子 SA が AUTH 交換自体の一部として作成されることです。 クリプト マップの下で設定された DH グループはキーの再生成の間にだけ使用されます。 それ故に、「PFS を見ます（Y/N）: N, DH group: none」が表示されます。

IKEv1 を使うと、子 SA 作成が Quick Mode の間に起こり、CREATE_CHILD_SA メッセージに新しい共有秘密を得るために DH パラメータを規定 する 鍵交換 ペイロードを伝送するプロビジョニングするがあるので、異なる動作を見ます。

ルータ 1 の出力

```
Router1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt:
10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt:
10, #pkts verify: 10
#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.: 10.0.0.1,
remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xF6083ADD(4127734493)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec):
(4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

出力されるルータ 2

```
Router2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#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.: 10.0.0.2,
remote crypto endpt.: 10.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x6B74CB79(1802816377)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime
(k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

両方のルータで **show crypto session** コマンドの出力を確認することもできます。 次の出力では、トンネルのセッション ステータスに [UP-ACTIVE] と表示されています。

```
Router1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 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

Router2#show cry session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 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
```

関連情報

- IKEv2 パケット交換とプロトコル レベルのデバッグ
- テクニカルサポートとドキュメント - Cisco Systems