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

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント
- 表記法

背景説明

主な問題

ルータの設定

トラブルシュート

- ルータのデバッグ
- CHILD_SA のデバッグ

トンネルの確認

- ISAKMP
- IPSec

関連情報

はじめに

このドキュメントでは、非共有キー(PSK)が使用される場合のCisco IOS®でのインターネットキーエクスチェンジバージョン2(IKEv2)のデバッグについて説明します。

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いています。

- 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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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。

背景説明

このドキュメントでは、特定のデバッグ行を設定に変換する方法について説明します。

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個のパケットで構成されるフェーズ1交換と、その後のフェーズ2交換で3個のパケットで構成されるフェーズ2交換が明確に区別されていました。IKEv2交換は可変です。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
```

トラブルシュート

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:Processing an item off the pak queue *Nov 11 19:30:34.811: IKEv2:% Getting preshared key by address 10.0.0.2 *11月11日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：新しいikev2 sa要求が許可されました *Nov 11 19:30:34.811: IKEv2：発信negotiating sa countを1増やす	
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	*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 *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 *11月11日19:30:34.811:IKEv2:(SA ID = 1)：設定済みポリシーの設定 *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:	

ギュレーション crypto ikev2 proposal PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key local cisco pre-shared-key remote cisco	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イベント：EV_OK_RECD_DH_pubkey応答 *Nov 11 19:30:34.811:IKEv2:(SA ID = 1)：アクション：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 - IKE_SA_INIT交換で送信する構成データなし *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	
発信側はIKE_INIT_SAパケットを作成します。これには、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公開キー値）、およびN（発信側のナンス）が含まれます。	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1)：次のペイロード：SA、バージョン： 2.0交換タイプ：IKE_SA_INIT、フラグ：INITIATORメッセージID:0、長さ：344 Payload contents: SA：次のペイロード：KE、予約済み：0x0、長さ：56 最終提案：0x0、予約済み：0x0、長さ：52 プロポーザル：1、プロトコルID:IKE、SPIサイズ：0、#trans:5最後の変換：0x3、予約済み：0x0：長さ：8 タイプ：1、予約済み：0x0、id:3DES 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 KE 次のペイロード：N、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 N次のペイロード：VID、予約済み：0x0、長さ：24 VID次のペイロード：VID、予約済み：0x0、長さ：23 VID Nextペイロード：NOTIFY、予約済み：0x0、長さ：21	

	NOTIFY(NAT_DETECTION_SOURCE_IP)次のペイロード ：NOTIFY、予約済み：0x0、長さ：28 　セキュリティプロトコルID: IKE、spiサイズ： 0、種類： NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)次のペイロード：なし、予約済み：0x0、長さ：28 　セキュリティプロトコルID: IKE、spiサイズ： 0、種類： NAT_DETECTION_DESTINATION_IP	
----------発信側が IKE_INIT_SA を送信 ---------->		
	*Nov 11 19:30:34.814: IKEv2:Got a packet from dispatcher *11月11日19:30:34.814:IKEv2:Processing an item off the pak queue *Nov 11 19:30:34.814: IKEv2：新しいikev2 sa要求が認められた *Nov 11 19:30:34.814: IKEv2:Incrementing incoming negotiating sa count by one	応答側が IKE_INIT_SA を受信します。
	*Nov 11 19:30:34.814: IKEv2：次のペイロード： SA、バージョン：2.0交換タイプ： IKE_SA_INIT、フラグ： INITIATORメッセージID: 0、長さ： 344 Payload contents: SA次ペイロード：KE、予約済み：0x0、長さ：56 最終提案：0x0、予約済み：0x0、長さ：52 プロポーザル：1、プロトコルID:IKE、SPIサイズ：0、#trans:5最後の変換：0x3、予約済み：0x0：長さ：8 タイプ：1、予約済み：0x0、id:3DES 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 KE次ペイロード：N、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 N次のペイロード：VID、予約済み：0x0、長さ：24 *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	応答側がピア用の SA の作成を開始します。

	NOTIFY(NAT_DETECTION_SOURCE_IP)次のペイロード： NOTIFY，予約済み： 0x0，長さ： 28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)次のペイロード：なし、予約済み：0x0、長さ：28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： 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_RECCV初期化 *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 メッセージ(_M) *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_INSERT SA_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_EV ike_IKE_ポリシー *11月11日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 メッセージ(_M) *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_DETECT NATを使用する *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)：リモートアドレスの一致 *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)：ローカルアドレスの一致 *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):NATが見つかりません *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA:	応答側はIKE_INITメッセージを確認して処理します。(1)発信側が提供する暗号スイートを選択し、(2)独自のDH秘密キーを計算し、(3)skeyid値を計算します。この値から、このIKE_SA用のすべてのキーを取得できます。以降に送信されるすべてのメッセージのヘッダーを除くすべてのメッセージが暗号化され、認証されます。暗号化と整合性の保護に使用されるキーはSKEYIDから取得され、SK_e（暗号化）、SK_a（認証）、SK_dが取得され、

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: EV_CHK CONFIG_MODE（設定モード） *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: ポリシーの設定 *11月11日19:30:34.814:IKEv2:(SA ID = 1):設定済みポリシーの設定 *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: 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: PKI_SESH_OPEN *11月11日19:30:34.814:IKEv2:(SA ID = 1):PKIセッションのオープン *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_キー *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: イベントなし *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)：アクション： 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: イベントなし *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（提案書のデフォルトをツールキットのポリシーに追加） *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: OK_RECD_DH_秘密_応答 *Nov 11 19:30:34.822: IKEv2:(SA ID = 1)：アクション： Action_Null *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)	CHILD_SAのキー関連情報の取得に使用されます。また、方向ごとに個別のSK_eとSK_aが計算されます。 関連コンフィギュレーション `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`

	MsgID = 00000000 CurState: R_BLD_INIT Event: ev_GEN_SKEYID *11月11日19:30:34.822:IKEv2:(SA ID = 1):skeyidを生成 *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: GET_CONFIG_MODEコマンドを発行します。 *Nov 11 19:30:34.822: IKEv2:IKEv2レスポンダ – IKE_SA_INIT交換で送信する構成データがありません *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: BLDメッセージ *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)：次のペイロード： SA、バージョン： 2.0交換の種類： IKE_SA_INIT、フラグ： RESPONDER MSG-RESPONSEメッセージID: 0、長さ： 449 Payload contents: SA：次のペイロード：KE、予約済み：0x0、長さ：48 最終提案：0x0、予約済み：0x0、長さ：44 プロポーザル：1、プロトコルID:IKE、SPIサイズ：0、#trans:4最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 KE 次のペイロード：N、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 N次のペイロード：VID、予約済み：0x0、長さ：24 VID次のペイロード：VID、予約済み：0x0、長さ：23 VID Nextペイロード：NOTIFY、予約済み：0x0、長さ：21 NOTIFY(NAT_DETECTION_SOURCE_IP)次のペイロード	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、ISAKMPヘッダー（SPI//バージョン/フラグ）、SAr1（IKEレスポンダが選択する暗号化アルゴリズム）、KEr（レスポンダのDH公開キー値）、およびレスポンダのナンスが含まれます

	：NOTIFY、予約済み：0x0、長さ：28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)ネクストペイロード：CERTREQ、予約済み：0x0、長さ：28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：NAT_DETECTION_DESTINATION_IP CERTREQ次のペイロード：NOTIFY、予約済み：0x0、長さ：105 Cert encoding Hash and URL of PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)次のペイロード：なし、予約済み：0x0、長さ：8 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：HTTP_CERT_LOOKUP_SUPPORTED		。
	*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イベント： EV_DONE *Nov 11 19:30:34.822:IKEv2:(SA ID = 1):Cisco DeleteReason Notifyが有効 *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_CHK 4_ロール *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_EV開始_TMR *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_SIP イベントなし *Nov 11 19:30:34.822: IKEv2:New ikev2 sa request admitted *Nov 11 19:30:34.822: IKEv2:Incrementing outgoing negotiating sa count by one		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。
<---------- 応答側が IKE_INIT_SA を送信----------			
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 *Nov 11 19:30:34.823: IKEv2:Got a packet from dispatcher *11月11日 19:30:34.823:IKEv2:Processing an item off the pak queue	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。

ルータ1は応答を確認して処理します。 (1)発信側のDH秘密キーが計算され、 (2)発信側のSKEYIDも生成されます。	*Nov 11 19:30:34.823: IKEv2:(SA ID = 1)：次のペイロード： SA、バージョン： 2.0交換タイプ： IKE_SA_INIT、フラグ： RESPONDER MSG-RESPONSEメッセージID: 0、長さ： 449 Payload contents: SA：次のペイロード：KE、予約済み：0x0、長さ：48 最終提案：0x0、予約済み：0x0、長さ：44 プロポーザル：1、プロトコルID:IKE、SPIサイズ：0、#trans:4最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 KE 次のペイロード：N、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 N次のペイロード：VID、予約済み：0x0、長さ：24 *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)次のペイロード： NOTIFY，予約済み： 0x0，長さ： 28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)次のペイロード： CERTREQ、予約済み： 0x0、長さ： 28 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： NAT_DETECTION_DESTINATION_IP CERTREQ次のペイロード：NOTIFY、予約済み：0x0、長さ：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)次のペイロード：なし、予約： 0x0、長さ： 8
セキュリティプロトコルID: IKE、spiサイズ： 0、種類： 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_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: 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: verify_MSG（確認メッセージ）
*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: 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:検出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)：リモートアドレスの一致
*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)：ローカルアドレスの一致
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):NATが見つかりません
*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: 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: chk_CONFIG_MODEを設定します。
*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_EV gen_DH_シークレット
*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 イベント

	*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イベント： EV_OK RECD_DH_SECRET_RESP（デフォルト） *Nov 11 19:30:34.831: IKEv2:(SA ID = 1)：アクション： 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_EV gen_SKEYID *11月11日19:30:34.831:IKEv2:(SA ID = 1):skeyidを生成 *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イベント： EV_DONE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Cisco DeleteReason Notifyが有効 *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_CHK 4_ロール *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_EV: GET_CONFIG_MODEコマンドを発行します。 *11月11日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_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、ISAKMPヘッダー（SPI/バージョン/フラグ）、IDi（発信側ID）、AUTHペイロード、SAi2（IKEv1でのフェーズ2トランスフォームセット交換	*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_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_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_EV: SEND_AUTH（送信の認証） *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	

に類似したSAを開始）、TSiおよびTSr（発信側および応答側のトラフィックセレクタ）が含まれます。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 `crypto ipsec transform-set`	*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次ペイロード：IDi、予約済み：0x0、長さ：20 IDi：次のペイロード：AUTH、予約済み：0x0、長さ：12 Idタイプ：IPv4アドレス、予約済み：0x0 0x0 AUTH Next payload:CFG、予約済み：0x0、長さ：28 認証方法PSK、予約済み： 0x0、予約済み0x0 CFG：次のペイロード：SA、予約済み：0x0、長さ：309 cfgタイプ：CFG_REQUEST、予約済み：0x0、予約済み：0x0 *Nov 11 19:30:34.831: SA次のペイロード： TSi、予約済み：0x0、長さ：40 最終提案：0x0、予約済み：0x0、長さ：36 プロポーザル：1、プロトコルID:ESP、SPIサイズ：4、#trans:3最後の変換：0x3、予約済み：0x0：長さ：8 タイプ：1、予約済み：0x0、id:3DES 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：5、予約済み：0x0、ID:ESNを使用しない TSi次のペイロード：TSr、予約済み：0x0、長さ：24 TS数：1、予約済み0x0、予約済み0x0 TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16 開始ポート：0、終了ポート：65535 開始アドレス： 0.0.0.0、終了アドレス： 255.255.255.255 TSr次のペイロード：NOTIFY、予約済み：0x0、長さ：24 TS数：1、予約済み0x0、予約済み0x0 TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16 開始ポート：0、終了ポート：65535 開始アドレス： 0.0.0.0、終了アドレス： 255.255.255.255 NOTIFY(INITIAL_CONTACT)次のペイロード：NOTIFY、予約済み：0x0、長さ：8 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE)次のペイロード： NOTIFY，予約済み： 0x0，長さ： 12 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT)次のペイロード：NOTIFY、予約済み：0x0、長さ：8 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：ESP_TFC_NO_SUPPORT	

TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP	NOTIFY(NON_FIRST_FRAGS)次のペイロード：なし、予約済み：0x0、長さ：8 セキュリティプロトコルID: IKE、spiサイズ： 0、種類：NON_FIRST_FRAGS *Nov 11 19:30:34.832: IKEv2:(SA ID = 1)：次のペイロード：ENCR、バージョン： 2.0交換タイプ： IKE_AUTH、フラグ：発信側メッセージID: 1、長さ： 556 Payload contents: ENCR次ペイロード：VID、予約済み：0x0、長さ：528 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000001CurState: i_WAIT_AUTHイベント： EV_NO_EVENT	
----------発信側が IKE_AUTH を送信 ---------->		
	*Nov 11 19:30:34.832: IKEv2:Got a packet from dispatcher *11月11日19:30:34.832:IKEv2:Processing an item off the pak queue *Nov 11 19:30:34.832: IKEv2:(SA ID = 1)：要求にmess_id 1があります。予期される値は1 ~ 1です。 *Nov 11 19:30:34.832: IKEv2:(SA ID = 1)：次のペイロード：ENCR、バージョン： 2.0交換タイプ： IKE_AUTH、フラグ：INITIATORメッセージID: 1、長さ： 556 Payload contents: *Nov 11 19:30:34.832: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0, length: 20 IDi：次のペイロード：AUTH、予約済み：0x0、長さ：12 Idタイプ：IPv4アドレス、予約済み：0x0 0x0 AUTH Next payload:CFG、予約済み：0x0、長さ：28 認証方法PSK、予約済み： 0x0、予約済み0x0 CFG次のペイロード：SA、予約済み：0x0、長さ：309 cfgタイプ：CFG_REQUEST、予約済み：0x0、予約済み：0x0 *11月11日19:30:34.832: attrib type: internal IP4 DNS, length: 0 *11月11日19:30:34.832: attrib type: internal IP4 DNS, length: 0 *11月11日19:30:34.832:attribタイプ：内部IP4 NBNS、長さ：0 *11月11日19:30:34.832:attribタイプ：内部IP4 NBNS、長さ：0 *11月11日19:30:34.832:attribタイプ：内部IP4サブネット、長さ：0 *11月11日19:30:34.832:attribタイプ：アプリケーションバージョン、長さ：257 属性タイプ：不明 – 28675、長さ： 0 *Nov 11 19:30:34.832: attrib type: Unknown - 28672, length: 0 *Nov 11 19:30:34.832: attrib type: Unknown - 28692, length: 0 *Nov 11 19:30:34.832: attrib type: Unknown - 28681, length: 0 *Nov 11 19:30:34.832: attrib type: Unknown - 28674, length: 0 *Nov 11 19:30:34.832: SA次のペイロード：TSi、予約済み：0x0、	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： crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5

	長さ：40 最終提案：0x0、予約済み：0x0、長さ：36 プロポーザル：1、プロトコルID:ESP、SPIサイズ：4、#trans:3最後の変換：0x3、予約済み：0x0：長さ：8 タイプ：1、予約済み：0x0、id:3DES 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：5、予約済み：0x0、ID:ESNを使用しない TSi次のペイロード：TSr、予約済み：0x0、長さ：24 TS数：1、予約済み0x0、予約済み0x0 TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16 開始ポート：0、終了ポート：65535 開始アドレス： 0.0.0.0、終了アドレス： 255.255.255.255 TSr次のペイロード：NOTIFY、予約済み：0x0、長さ：24 TS数：1、予約済み0x0、予約済み0x0 TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16 開始ポート：0、終了ポート：65535 開始アドレス： 0.0.0.0、終了アドレス： 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_SIP 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_SIP 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_SIP proc_ID *Nov 11 19:30:34.832: IKEv2:(SA ID = 1)：プロセスIDで有効なパラメータを受信しました *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_SIP chk_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_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_SIP 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	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、ISAKMPヘッダー（SPI//バージョン/フラグ）、IDr（レスポンダID）、AUTHペイロード、SAr2（IKEv1でのフェーズ2トランスフォームセット交換に類似したSAを開始）、TSiおよびTSr（イニシエータおよびレスポンダトラフィックセレ

	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（提案書のデフォルトをツールキットのポリシーに追加） *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):IKEv2プロファイル「IKEV2-SETUP」の使用 *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_SIP set_POLICY（ポリシーの設定） *Nov 11 19:30:34.833:IKEv2:(SA ID = 1)：設定済みポリシーの設定 *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_SIP verify_POLICY_BY_PEERID（ポリシーごとの検証） *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_SIP chk_AUTH4EAPを使用します。 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_SIP 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: chk_AUTH_タイプ *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: 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: verify_AUTH（認証の検証） *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: 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: chk_REDIRECT *Nov 11 19:30:34.833: IKEv2:(SA ID = 1)：リダイレクトチェックは不要です。スキップします。	クタ）が含まれます。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。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: notify_AUTH_DONE（認証完了） *Nov 11 19:30:34.833:IKEv2:AAAグループ許可が設定されていない *Nov 11 19:30:34.833:IKEv2:AAAユーザ許可が設定されていない *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: chk_CONFIG_MODEを設定します。 *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: set_RECD_CONFIG_モード *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: 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:取得_設定_モード *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_EV: MY_AUTH_メソッド *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_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_EV:認証の生成(_A) *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_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_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_EV: SEND_AUTH（送信の認証）	

	*11月11日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)：次のペイロード：ENCR、バージョン： 2.0交換の種類：IKE_AUTH、フラグ：RESPONDER MSG-RESPONSEメッセージID: 1、長さ： 252 Payload contents: ENCR次ペイロード：VID、予約済み：0x0、長さ：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イベント： EV_OK *Nov 11 19:30:34.833: IKEv2:(SA ID = 1)：アクション： 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閉じる(_S) *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):PKIセッションの終了 *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イベント： 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_EV挿入IKE *Nov 11 19:30:34.834: IKEv2:Store mib index ikev2 1、プラットフォーム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イベント： EV_GEN ロードIPSEC *Nov 11 19:30:34.834: IKEv2:(SA ID = 1)：非同期要求キュー *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イベント： イベントなし		応答側は IKE_AUTH の応答を送信します。
<---------- 応答側が IKE_AUTH を送信----------			
発信側が応答側からの応答	*Nov 11 19:30:34.834: IKEv2:Got	*Nov 11 19:30:34.840:	応答側はエントリを SAD に

を受信します。	a packet from dispatcher *11月11日 19:30:34.834:IKEv2:Processing an item off the pak queue	IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONEイベント： EV_OK RECD_LOAD_IPSEC *11月11日 19:30:34.840:IKEv2:(SA ID = 1)：アクション：Action_Null *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イベント： EV_START アカウント *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イベント： EV_CHECK重複 *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イベント： EV_CHK 4_ロール	追加します。
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:(SA ID = 1)：次のペイロード：ENCR、バージョン： 2.0交換の種類： IKE_AUTH、フラグ：RESPONDER MSG-RESPONSEメッセージID: 1、長さ： 252 Payload contents: *Nov 11 19:30:34.834: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDr., reserved: 0x0, length: 20 IDr：次のペイロード：AUTH、予約済み：0x0、長さ：12 Idタイプ：IPv4アドレス、予約済み：0x0 0x0 AUTH：次のペイロード：SA、予約済み：0x0、長さ：28 認証方法PSK、予約済み： 0x0、予約済み0x0 SA：次のペイロード：TSi、予約済み：0x0、長さ：40 最終提案：0x0、予約済み：0x0、長さ：36 プロポーザル：1、プロトコルID:ESP、SPIサイズ：4、#trans:3最		

後の変換：0x3、予約済み：0x0：長さ：8
タイプ：1、予約済み：0x0、id:3DES
最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8
タイプ：3、予約済み：0x0、id:SHA96
最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8
タイプ：5、予約済み：0x0、ID:ESNを使用しない
TSi次のペイロード：TSr、予約済み：0x0、長さ：24
TS数：1、予約済み0x0、予約済み0x0
TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16
開始ポート：0、終了ポート：65535
開始アドレス： 0.0.0.0、終了アドレス： 255.255.255.255
TSr次のペイロード：NOTIFY、予約済み：0x0、長さ：24
TS数：1、予約済み0x0、予約済み0x0
TSタイプ：TS_IPV4_ADDR_RANGE、プロトコルID:0、長さ：16
開始ポート：0、終了ポート：65535
開始アドレス： 0.0.0.0、終了アドレス： 255.255.255.255

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload:
SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)次のpayload:
NOTIFY, reserved: 0x0, length: 12
セキュリティプロトコルID: IKE、spiサイズ： 0、種類：
SET_WINDOW_SIZE

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload:
ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT)次の
ペイロード： NOTIFY，予約済み： 0x0，長さ： 8
セキュリティプロトコルID: IKE、spiサイズ： 0、種類：
ESP_TFC_NO_SUPPORT

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload:
NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS)次のpayload:
NONE, reserved: 0x0, length: 8
セキュリティプロトコルID: IKE、spiサイズ： 0、種類：
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 auth_RECV_認証
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1)：アクション： 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: 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 MSG_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: 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: get_POLICY_BY_PEERID
*11月11日19:30:34.834:IKEv2:Adding Proposal PHASE1-prop to toolkit policy
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):IKEv2プロファイル「IKEV2-SETUP」の使用
*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: verify_POLICY_BY_PEERID（ポリシーごとの検証）
*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: chk_AUTH_タイプ
*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: 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認証の確認
*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: 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 AUTH_NOTIFY_AUTH_完了
*Nov 11 19:30:34.835:IKEv2:AAAグループ許可が設定されていない
*Nov 11 19:30:34.835:IKEv2:AAAユーザ許可が設定されていない
*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: chk_CONFIG_MODEを設定します。
*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: 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: 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: 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イベント： EV_OK
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1)：アクション： 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閉じる(_S)
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):PKIセッションの終了
*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イベント： 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イベント： EV_INSERT アイク
*Nov 11 19:30:34.835: IKEv2:Store mib index ikev2 1、プラットフォーム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イベント： EV_GEN ロード IPSEC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1)：非同期要求キュー

*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 イベント
*11月11日19:30:34.835:IKEv2:KMIメッセージ8が使用されました。No action taken.
*11月11日19:30:34.835:IKEv2:KMIメッセージ12が使用されました。No action taken.
*Nov 11 19:30:34.835: IKEv2:No data to send in mode config set.（モード設定で送信するデータがありません）
*Nov 11 19:30:34.841: IKEv2：セッション8のSPI 0x9506D414に関連付けられたIDENTハンドル0x80000002の追加

*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イベント： EV_OK RECD_LOAD_IPSEC
*Nov 11 19:30:34.841: IKEv2:(SA ID = 1)：アクション： 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イベント： EV_START アカウント *Nov 11 19:30:34.841: IKEv2:(SA ID = 1)：アカウンティングは不要 *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イベント： EV_CHECK重複 *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イベント： _CHK4_ロール		
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 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	*Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READYイベント： EV_A了解 (_O) *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	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。

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、IKE_SAのどちらの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 の CHILD_SA メッ 説明
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):CHILD_SAが初期交換の一部として作成される場合、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	*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 ID = 2):Request has mess_id 3; expected 3 ~ 7 *Nov 11 19:31:35.873: IKEv2:(SA ID	

• KEi(Key-optional):CREATE_CHILD_SA要求には、CHILD_SAの転送秘密をより強固に保証するために、追加のDH交換のKEペイロードをオプションで含めることができます。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。推測が正しくない場合、CREATE_CHILD_SA交換は失敗し、別のKEiで再試行できます • 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）、INFORMATIONAL交換 (IKE要求以外のエラーを報告する) 、またはその他のメッセージに表示され、送信者の能力を示したり、要求の意味を変更したりできます。このCREATE_CHILD_SA交換がIKE_SA以外の既存のSAのキーの再生成を行う場合、タイプREKEYのSAをであることをします。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。	= 2)：次のペイロード： ENCR、バージョン： 2.0交換タイプ：CREATE_CHILD_SA、フラグ：イニシエータメッセージID: 3、長さ：396 Payload contents: SA：次のペイロード：N、予約済み：0x0、長さ：152 最終提案：0x0、予約済み：0x0、長さ：148 プロポーザル：1、プロトコルID:IKE、SPIサイズ：8、#trans:15最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA512 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA384 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA256 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:MD5 最後のトランスフォーム： 0x3、	

	予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA512 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA384 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA256 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:MD596 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、id:DH_GROUP_1536_MODP/Group 5 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 N次のペイロード：KE、予約済み：0x0、長さ：24 KE次ペイロード：NOTIFY、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)次のpayload: NONE, reserved: 0x0, length: 12 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： 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子 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2)：アクション： 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子 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2)：アクション： 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_CC タイプ *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_IKE esa *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_GET_IKE_POLICY 0.9599994 *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（提案のフェーズ1プロップをツールキットのポリシーに追加） *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):IKEv2プロファイル「IKEV2-SETUP」の使用 *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 *11月11日19:31:35.874:IKEv2:(SA ID = 2):設定済みポリシーの設定 *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イベント：EV_GEN_GEN dh_キー *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イベント：EV_NO_MSG イベント	

	*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イベント： EV_OK_OK recd_DH_PUBKEY_RESP *Nov 11 19:31:35.874: IKEv2:(SA ID = 2)：アクション： 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イベント： EV_NO_MSG イベント *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イベント： EV_OK_OK recd_DH_SECRET_RESP (デフォルト) *Nov 11 19:31:35.882: IKEv2:(SA ID = 2)：アクション： 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イベント： EV_BLD メッセージ *Nov 11 19:31:35.882: IKEv2:ConstructNotify Payload: SET_WINDOW_SIZE	

	Payload contents: SA：次のペイロード：N、予約済み：0x0、長さ：56 最終提案：0x0、予約済み：0x0、長さ：52 プロポーザル：1、プロトコルID:IKE、SPIサイズ：8、#trans:4最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 N次のペイロード：KE、予約済み：0x0、長さ：24 KE次ペイロード：NOTIFY、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 NOTIFY(SET_WINDOW_SIZE)次のペイロード：なし、予約済み：0x0、長さ：12 セキュリティプロトコルID:IKE、spiサイズ： 0、種類：SET_WINDOW_SIZE	
	*Nov 11 19:31:35.869: IKEv2:(SA ID = 2)：次のペイロード： ENCR、バージョン： 2.0交換タイプ：CREATE_CHILD_SA、フラグ：INITIATORメッセージID: 2、長さ：460 Payload contents: ENCR次ペイロード：SA、予約済み：0x0、長さ：432	このパケットをルータ 2 が受 す。

	*Nov 11 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE Payload contents: SA：次のペイロード：N、予約済み：0x0、長さ：152 最終提案：0x0、予約済み：0x0、長さ：148 プロポーザル：1、プロトコルID:IKE、SPIサイズ：8、#trans:15最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA512 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA384 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA256 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:MD5 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、	

	id:SHA512 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA384 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA256 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:MD596 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、id:DH_GROUP_1536_MODP/Group 5 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 N次のペイロード：KE、予約済み：0x0、長さ：24 KE 次ペイロード：NOTIFY、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 NOTIFY(SET_WINDOW_SIZE)次のペイロード：なし、予約済み：0x0、長さ：12 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： SET_WINDOW_SIZE	
	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2)：次のペイロード： ENCR、バージョン： 2.0交換の種類： CREATE_CHILD_SA、フラグ： RESPONDER MSG-RESPONSEメッセージID: 3、長さ： 300	ルータ 2 は CHILD_SA 交換 作成します。これは CREATE_CHILD_SA 応答で CHILD_SA パケットには一 が含まれます。 • SA HDR (バージョン

	Payload contents: SA：次のペイロード：N、予約済み：0x0、長さ：56 最終提案：0x0、予約済み：0x0、長さ：52 プロポーザル：1、プロトコルID:IKE、SPIサイズ：8、#trans:4最後の変換：0x3、予約済み：0x0：長さ：12 タイプ：1、予約済み：0x0、id:AES-CBC 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：2、予約済み：0x0、id:SHA1 最後のトランスフォーム： 0x3、予約済み： 0x0：長さ： 8 タイプ：3、予約済み：0x0、id:SHA96 最後のトランスフォーム： 0x0、予約済み： 0x0：長さ： 8 タイプ：4、予約済み：0x0、ID:DH_GROUP_1024_MODP/Group 2 N次のペイロード：KE、予約済み：0x0、長さ：24 KE 次ペイロード：NOTIFY、予約済み：0x0、長さ：136 DHグループ：2、予約済み：0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)次のpayload: NONE, reserved: 0x0, length: 12 セキュリティプロトコルID: IKE、spiサイズ： 0、種類： SET_WINDOW_SIZE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState:	、交換タイプ） • ナンスNi（オプション）:CHILD_SAが初期交として作成される場合のKEペイロードとナンされません。 • SA ペイロード • KEi(Key-optional):CREATE_CH求には、CHILD_SAのをより強固に保証する追加のDH交換のKEペをオプションで含めるきます。SA が別の DHプを含めることを提案、KEi は、発信側が応け入れを期待するグル素である必要がありまに失敗した場合、CREATE_CHILD_SA失敗し、別の KEi を使試行を行う必要があり • N(Notify payload-optional):Notifyペイロエラー状態や状態遷移報データをIKEピアに通ために使用されます。イロードは、応答メッ（通常は、要求が拒否由を示す）、情報交換求以外のエラーを報告またはその他の任意のジに含まれ、送信者のしたり、要求の意味をりするために使用されの CREATE_CHILD_Sが IKE_SA 以外の既存キーの再生成を行う場REKEY_SA タイプの先ペイロードによってキ成する SA を特定するります。CREATE_CHの交換が既存の SA の生成を行わない場合、ードは省略する必要が

	CHILD_I_WAITイベント： EV_RECV作成_子 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2)：アクション： 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イベント： EV_CHK4通知(_N) *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 0.9599994 *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:	。 ルータ 2 は応答を送信し、 CHILD SA のアクティブ化を す。

	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_RECD dh_SECRET_RESP *Nov 11 19:31:35.890: IKEv2:(SA ID = 2)：アクション： 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 キー再生成 *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):skeyidを生成する *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONEイベント： EV_ACTIVATE _新規_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_DONE統計 *Nov 11 19:31:35.890:IKEv2：新しいikev2 sa要求がアクティブ化されました *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イベント： EV_CHK_PENDING *Nov 11 19:31:35.890: IKEv2:(SA ID = 2)：メッセージID 3の処理済み応答。要求は4 ～ 8の範囲で送信可能 *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Event: イベントなし	
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)：次のペイロード： ENCR、バージョン： 2.0交換の種類： CREATE_CHILD_SA、フラグ： RESPONDER MSG-RESPONSEメッセージID: 3、長さ： 300 Payload contents: ENCR次ペイロード：SA、予約済み：0x0、長さ：272 *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_CHMSG K_IKE_キー再生成 *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イベント：EV_GEN_GEN スキーID *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):skeyidを生成する *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(_S) *Nov 11 19:31:35.882: IKEv2:Store mib index 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_DONE統計 *Nov 11 19:31:35.882: IKEv2：新しいikev2 sa要求がアクティブ化されました *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イベント：EV_CHECK_ED重複 *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_DONE g_TMR *Nov 11 19:31:35.882: IKEv2:(SA ID = 2)：アクション： 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イベント： EV_CHK_PENDING *Nov 11 19:31:35.882: IKEv2:(SA ID = 2)：メッセージID 3で応答を送信、要求は4 ~ 8の範囲で受け入れ可能 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Event: イベントなし	

トンネルの確認

ISAKMP

コマンド

<#root>

show crypto ikev2 sa detailed

ルータ 1 の出力

<#root>

```
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
```

ルータ 2 の出力

<#root>

```
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

<#root>

show crypto ipsec sa

> 注：この出力では、IKEv1の場合とは異なり、最初のトンネルネゴシエーション時にPFS DHグループの値が「PFS (Y/N): N, DH group: none」と表示されますが、キー再生成が発生すると、正しい値が表示されます。この動作はCisco Bug ID CSCug67056に記述されていますが、これはバグではありません（シスコの内部ツールや情報にアクセスできるのは、登録ユーザのみです）。
> IKEv1とIKEv2の違いは、後者では子SAがAUTH交換の一部として作成される点です。暗号マップで設定されたDHグループは、キー再生成時にのみ使用されます。したがって、最初のキー再生成まで、「PFS (Y/N): N, DH group: none」と表示されます。
> IKEv1では、クイックモード時に子SAの作成が発生し、CREATE_CHILD_SAメッセージに鍵交換ペイロードを伝送するプロビジョニングがあり、これによって新しい共有秘密を取得するDHパラメータが指定されるため、異なる動作であることがわかります。

ルータ 1 の出力

<#root>

```
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:
```

ルータ 2 の出力

<#root>

```
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コマンドの出力を調べることもできます。この出力には、トンネルセッションのステータスがUP-ACTIVEと表示されています。

```
<#root>

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
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。