

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[主な問題](#)

[ルータの設定](#)

[トラブルシューティング](#)

[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](#)

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

ルータ 2

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。

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。

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

```
*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

*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_REC'D_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

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
```

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)。

```
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
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
*Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific
```

応答側が
IKE_INIT_SA を受
信します。

応答側がピア用の
SA の作成を開始し
ます。

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
 (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

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 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

*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: peer2 10.0.0.1
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 255.255.255.0
(R) MsgID = 00000000 CurState: R_BLD_INIT Event: host2 Cisco cisco
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_REC'D_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_REC'D_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:

```

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。

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
*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

*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

*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

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。

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:Processing an item off
the pak queue

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:(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

応答側は認証プロ
セスのタイマーを
開始します。

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

*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_REC'D_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 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

*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:
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

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

*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

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

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,
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: ルータ 2 はルータ
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 1 から受信した
(R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: IKE_AUTH パケッ
トの応答を作成し

*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 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

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。

(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
*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**
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

応答側は
IKE_AUTH の応答
を送信します。

*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

*?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_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
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

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

応答側はエントリを SAD に追加します。

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

*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
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

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_F
OR_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_REC'D_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
*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_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 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

```

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。

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

ルータ 1 が
CHILD_SA 交換を
開始します。これ
は
CREATE_CHILD_S
A 要求です。
CHILD_SA パケッ

```

*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

```

ルータ 2

CHILD_SA メッセージ概要

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

*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

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=0C33DB40DBAAAE6

KEi を使用して再試行を行う必要がありません。

- 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ず。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 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

```

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
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_REC'D_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_REC'D_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

```

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。

このパケットをルータ 2 が受信します。

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
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

ルータ 2 は
CHILD_SA 交換の
返信を作成します
。これは
CREATE_CHILD_S
A 応答です。

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=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: CHILD_I_WAIT イベント
: EV_RECV_CREATE_CHILD

*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:

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 ペイロードとナンズは送信されません。
- 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

I_SPI=0C33DB40DBAAADE6
 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
 CurState: CHILD_I_PROC Event:
 EV_OK_REC'D_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 keyid
 *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
 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

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)、INFORMATIONAL 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
ありません。

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。

*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:
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

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):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 ペイロードを送信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](#)