

ASAとルータ間のサイト間IKEv2トンネルの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[設定](#)

[ネットワーク図](#)

[背景説明](#)

[NTP](#)

[HTTP-URLベースの証明書検索](#)

[ピアIDの確認](#)

[ルータでの ISAKMP ID の選択](#)

[ルータでの ISAKMP ID の確認](#)

[ASA での ISAKMP ID の選択](#)

[ASA での ISAKMP ID の確認](#)

[相互運用性の問題](#)

[認証ペイロードのサイズ](#)

[ASAにおけるマルチコンテキストモードでのリソース割り当て](#)

[証明書失効リストの検証](#)

[証明書チェーンの検証](#)

[ASAの設定例](#)

[ルータの設定例](#)

[Cisco IOS CAの設定例](#)

[確認](#)

[フェーズ1の確認](#)

[フェーズ2の確認](#)

[トラブルシューティング](#)

[ASAでのデバッグ](#)

[ルータでのデバッグ](#)

はじめに

このドキュメントでは、Cisco ASAとCisco IOS[®]ソフトウェアを実行するルータの間にサイト間IKEv2トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インターネット キー交換バージョン 2 (IKEv2)
- 証明書と Public Key Infrastructure (PKI)
- Network Time Protocol (NTP)

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。

- ソフトウェア バージョン 9.8.4 を実行する Cisco ASA 5506 適応型セキュリティ アプライアンス
- Cisco IOS ソフトウェア バージョン 15.3(3)M1 を実行する Cisco 2900 シリーズ サービス統合型ルータ (ISR)

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。

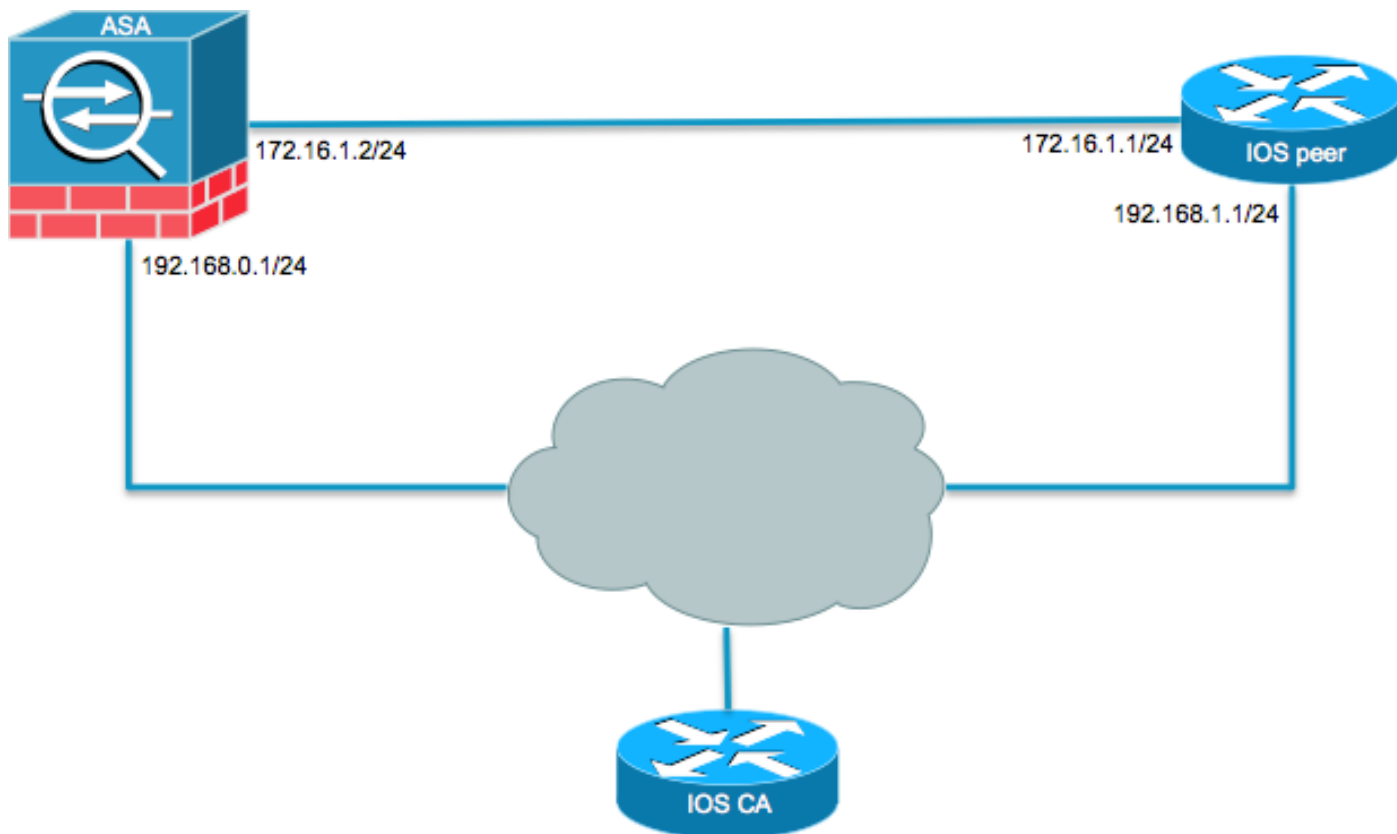
関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- ソフトウェア バージョン 8.4(1) 以降を実行する Cisco ASA
- Cisco IOS ソフトウェア バージョン 15.2(4)M 以降を実行する Cisco ISR Generation 2 (G2)
- Cisco IOS XE ソフトウェア バージョン 15.2(4)S 以降を実行する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- ソフトウェア バージョン 15.2(4)M 以降を実行する Cisco Connected Grid ルータ

設定

ネットワーク図



背景説明

事前共有キーを使用して ASA とルータ間に IKEv2 トンネルを設定することは簡単です。ただし、証明書認証を使用する場合、留意すべき事項がいくつかあります。

NTP

証明書認証では、使用するすべてのデバイスのクロックを共通のソースと同期する必要があります。各デバイスでクロックを手動で設定できますが、これはあまり正確でなく、面倒なことになる可能性があります。すべてのデバイスのクロックを同期する最も簡単な方法は、NTP を使用することです。NTPは、分散されたタイムサーバとクライアントの間で時刻を同期します。同期化により、システム ログ作成時または時間に関するイベントの発生時に、各イベントに関連付けることができます。NTPの設定方法についての詳細は、『[Network Time Protocol: Best Practices White Paper](#)』を参照してください。

 ヒント: Cisco IOSソフトウェアのCertificate Authority (CA ; 認証局) サーバを使用する場合、一般的にはNTPサーバと同じデバイスを設定します。この例では、CA サーバが NTP サーバとしても機能します。

HTTP-URL ベースの証明書検索

HTTP URL に基づいた証明書ルックアップは、証明書の転送時に発生するフラグメンテーションを回避します。Cisco IOS ソフトウェア デバイスでは、この機能がデフォルトでイネーブルになっているため、証明書要求タイプ 12 が Cisco IOS ソフトウェアによって使用されます。

ASA で Cisco Bug ID [CSCu148246](#) の修正がないソフトウェアバージョンが使用されている場合は、[HTTP-URL ベースの検索が ASA でネゴシエートされないため、Cisco IOS ソフトウェアで認可の試行が失敗します。](#)

ASA で IKEv2 プロトコルのデバッグをイネーブルにすると、次のメッセージが表示されます。

```
IKEv2-PROTO-1: (139): Auth exchange failed
IKEv2-PROTO-1: (140): Unsupported cert encoding found or Peer requested
    HTTP URL but never sent
HTTP_LOOKUP_SUPPORTED Notification
```

この問題を回避するには、`no crypto ikev2 http-url cert` コマンドを発行して、ASAとのピア関係の確立時にルータでこの機能を無効にします。

ピア ID の確認

IKE AUTH段階のInternet Security Association and Key Management Protocol(ISAKMP)ネゴシエーション中に、ピアは互いに自身を識別する必要があります。ただし、ルータと ASA が各自のローカル ID を選択する方法には違いがあります。

ルータでの ISAKMP ID の選択

IKEv2トンネルがルータで使用される場合、ネゴシエーションで使用されるローカルIDは `identity local` IKEv2プロファイルで次のコマンドを実行します。

```
R1(config-ikev2-profile)#identity local ?
  address  address
  dn       Distinguished Name
  email    Fully qualified email string
  fqdn     Fully qualified domain name string
  key-id   key-id opaque string - proprietary types of identification
```

デフォルトでは、ルータはローカル ID としてアドレスを使用します。

ルータでの ISAKMP ID の確認

同じプロファイル内で手動で設定されたピアIDが、`match identity remote` コマンドにより、WLC CLI で明確に示されます。

```
R1(config-ikev2-profile)#match identity remote ?
  address  IP Address(es)
  any      match any peer identity
  email    Fully qualified email string [Max. 255 char(s)]
  fqdn     Fully qualified domain name string [Max. 255 char(s)]
```

key-id key-id opaque string

ASA での ISAKMP ID の選択

ASAでは、ISAKMP IDはグローバルに選択され、`crypto isakmp identity` コマンドにより、WLC CLI で明確に示されます。

```
ciscoasa/vpn(config)# crypto isakmp identity ?
configure mode commands/options:
  address  Use the IP address of the interface for the identity
  auto     Identity automatically determined by the connection type: IP
           address for preshared key and Cert DN for Cert based connections
  hostname Use the hostname of the router for the identity
  key-id   Use the specified key-id for the identity
```

デフォルトでは、このコマンド モードは auto に設定されているため、ASA 次の接続タイプに応じて ISAKMP ネゴシエーションを決定します。

- 事前共有キーの IP アドレス
- 証明書認証の証明書認定者名

 注:Cisco Bug ID [CSCul48099](https://bugzilla.cisco.com/show_bug.cgi?id=48099)は、グローバル設定ではなく、トンネルグループ単位で設定する機能の拡張要求です。

ASA での ISAKMP ID の確認

リモート ID の確認は、自動的に実行され (接続タイプによって決定される)、変更することはできません。検証は、トンネルグループ単位でイネーブルまたはディセーブルにすることができます。 `peer-id-validate` コマンドにより、WLC CLI で明確に示されます。

```
ciscoasa/vpn(config-tunnel-ipsec)# peer-id-validate ?
tunnel-group-ipsec mode commands/options:
  cert      If supported by certificate
  nocheck   Do not check
  req       Required
```

相互運用性の問題

ID の選択/確認の違いにより、次の 2 つの相互運用性の問題が発生します。

- ASA で証明書認証を使用する場合、ASA は受信した証明書で Subject Alternative Name (SAN) のピア ID を確認しようとします。ピア ID の確認をイネーブルにしている場

合や、ASA で IKEv2 プラットフォームのデバッグがイネーブルになっている場合は、次のデバッグが表示されます。


```
IKEv2-PROTO-3: (172): Getting configured policies
IKEv2-PLAT-3: attempting to find tunnel group for ID: 172.16.1.1
IKEv2-PLAT-3: mapped to tunnel group 172.16.1.1 using phase 1 ID
IKEv2-PLAT-3: (172) tg_name set to: 172.16.1.1
IKEv2-PLAT-3: (172) tunn grp type set to: L2L
IKEv2-PLAT-3: Peer ID check started, received ID type: IPv4 address
IKEv2-PLAT-2: Peer ID check: failed to retrieve IP from SAN
IKEv2-PLAT-2: Peer ID check: failed to retrieve DNS name from SAN
IKEv2-PLAT-2: Peer ID check: failed to retrieve RFC822 name from SAN
IKEv2-PLAT-1: retrieving SAN for peer ID check
IKEv2-PLAT-1: Peer ID check failed
IKEv2-PROTO-1: (172): Failed to locate an item in the database
IKEv2-PROTO-1: (172):
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
    R_SPI=F0B4D318DDDB783 (I) MsgID = 00000001 CurState: I_PROC_AUTH
    Event: EV_AUTH_FAIL
IKEv2-PROTO-3: (172): Verify auth failed
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
    R_SPI=F0B4D318DDDB783 (I) MsgID = 00000001 CurState: AUTH_DONE
    Event: EV_FAIL
IKEv2-PROTO-3: (172): Auth exchange failed
```

この問題では、証明書のIPアドレスをピア証明書に含めるか、ピアIDの検証をASAで無効にする必要があります。

- 同様に、ASA はデフォルトでローカル ID を自動的に選択するため、証明書認証を使用する場合、ID として認定者名 (DN) を送信します。ルータがリモート ID としてアドレスを受信するように設定されている場合、ルータでピア ID 確認が失敗します。IKEv2 デバッグがルータでイネーブルになっている場合、次のデバッグが表示されます。

```
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):SM Trace-> SA:
    I_SPI=E9E4B7FD0A336C97 R_SPI=F2CF438COCCA281C (R) MsgID = 1 CurState:
    R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):Searching policy
    based on peer's identity 'hostname=asa.cisco.com' of type 'DER ASN1 DN'
Nov 30 22:49:14.464: IKEv2:%Profile could not be found by peer certificate.
Nov 30 22:49:14.468: IKEv2:% IKEv2 profile not found
Nov 30 22:49:14.468: IKEv2:(SESSION ID = 172,SA ID = 1):: Failed to
    locate an item in the database
```

この問題には、完全修飾ドメイン名 (FQDN) を確認するようにルータを設定するか、ISAKMP ID としてアドレスを使用するように ASA を設定します。

 注：ルータでは、IKEv2プロファイルに接続された証明書マップを設定して、DNを認識する必要があります。この設定方法については、Ciscoドキュメント『[IPSec VPN用のインターネットキー交換\(IKE\)コンフィギュレーションガイド](#)、Cisco IOS XEリリース3S』の「証明書とISAKMPプロファイルのマッピング」セクションを参照してください。

認証ペイロードのサイズ

認証に証明書（事前共有キーではなく）が使用される場合、認証ペイロードは非常に大きくなります。通常、これにより、フラグメンテーションが発生し、フラグメントがパスで失われたり、ドロップされたりした場合には、認証が失敗します。認証ペイロードのサイズが原因でトンネルがアップ状態にならない場合、一般的な原因は次のとおりです。

- Control Plane Policing パケットをブロックする可能性があります。
- 誤った最大伝送ユニット(MTU)ネゴシエーション。これは、`crypto ikev2 fragmentation mtu size` コマンドを使用して、アップグレードを実行します。

ASA におけるマルチコンテキスト モードでのリソース割り当て

ASA バージョン 9.0 では、ASA はマルチコンテキスト モードで VPN をサポートします。ただし、マルチコンテキストモードでVPNを設定する場合は、VPNが設定されているシステムに適切なリソースを割り当ててください。

詳細については、『[CLIブック1:Cisco ASAシリーズの一般的な操作に関するCLIコンフィギュレーションガイド](#)、9.8』の「[リソース管理に関する情報](#)」セクションを参照してください。

証明書失効リストの検証

証明書失効リスト(CRL)は、特定のCAによって発行され、その後i撤回された、失効した証明書のリストです。証明書はi次のようないくつかの理由で無効にすることができます。

- 特定の証明書を使用するデバイスの障害または改ざん。
- 証明書によって使用されるキーペアの改i善。
- 不正なIDや名前の変更にi対応する必要性など、発行された証明書iート内のエラー。

証明書失効に使用されるメカニズムはiCAによって異なります。取り消された証明書iは、CRL内でシリアル番号で表されます。ネットワークデバイスは、証明書の有効性を確認しようとする場合i、現在のCRLをダウンロードして、提示された証明書のシリアル番号をスキャンします。このため、どちらか一方のピアでCRLの確認iネータブルになっている場合は、ID証明書の有効性を確認できるように適切なCRLのURLも設定する必要があります。

CRLの詳細については、『[公開キー インフラストラクチャ コンフィギュレーション ガイド](#)、Cisco IOS XE リリース 3S』の「[CRLとは](#)」の項を参照してください。

証明書チェーンの検証

ASAが中間CAを持つ証明書で設定され、そのピアが同じ中間CAを持たない場合、完全な証明書チェーンをルータに送信するようにASAを明示的に設定する必要があります。ルータはデフォルトでこれを実行します。これを行うには、暗号マップ下でトラストポイントを定義するときに、次のように、chain キーワードを追加します。

```
crypto map outside-map 1 set trustpoint ios-ca chain
```

これが行われない場合、ASAが応答側である限り、トンネルはネゴシエートされます。発信側の場合、トンネルネゴシエーションが失敗し、ルータのPKIおよびIKEv2デバッグに次のように表示されます。

```
2328304: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
Get peer's authentication method  
2328305: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
Peer's authentication method is 'RSA'  
2328306: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1  
  CurState: R_VERIFY_AUTH Event: EV_CHK_CERT_ENC  
2328307: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1  
  CurState: R_VERIFY_AUTH Event: EV_VERIFY_X509_CERTS  
2328308: Jun  8 19:14:38.051 GMT: CRYPTO_PKI: (A16A8) Adding peer certificate  
2328309: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Added x509 peer certificate -(1359) bytes  
2328310: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: ip-ext-val: IP extension validation  
  not required  
2328311: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: create new ca_req_context type  
  PKI_VERIFY_CHAIN_CONTEXT,ident 4177  
2328312: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8)validation path has 1 certs  
2328313: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Check for identical certs  
2328314: Jun  8 19:14:38.055 GMT: CRYPTO_PKI : (A16A8) Validating non-trusted cert  
2328315: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Create a list of suitable  
  trustpoints  
2328316: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Unable to locate cert record by  
  issuername  
2328317: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: No trust point for cert issuer,  
  looking up cert chain  
2328318: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) No suitable trustpoints found  
2328319: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):: Platform  
  errors  
2328320: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):SM Trace-> SA:  
  I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:  
  R_VERIFY_AUTH Event: EV_CERT_FAIL  
2328321: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):Verify cert  
  failed  
2328322: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:  
  R_VERIFY_AUTH Event: EV_AUTH_FAIL  
2328323: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68)  
:Verification of peer's authentication data FAILED
```


ASA の設定例

```
domain-name cisco.com
!
interface outside
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
interface CA
 nameif CA
 security-level 50
 ip address 192.168.0.1 255.255.255.0
!
! acl which defines crypto domains, must be mirror images on both peers
!
access-list cryacl extended permit ip 192.168.0.0 255.255.255.0 172.16.2.0
 255.255.255.0
pager lines 24
logging console debugging
mtu outside 1500
mtu CA 1500
mtu backbone 1500
route outside 172.16.2.0 255.255.255.0 172.16.1.1 1
route CA 192.168.254.254 255.255.255.255 192.168.0.254 1
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside-map 1 match address cryacl
crypto map outside-map 1 set pfs
crypto map outside-map 1 set peer 172.16.1.1
crypto map outside-map 1 set ikev2 ipsec-proposal DES AES256
crypto map outside-map 1 set trustpoint ios-ca chain
crypto map outside-map interface outside
crypto ca trustpoint ios-ca
 enrollment url http://192.168.254.254:80
 fqdn asa.cisco.com
 keypair ios-ca
 crl configure
crypto ca certificate chain ios-ca
certificate ca 01
 3082020f 30820178 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
 1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
 31333131 31353231 33353533 5a170d31 33313231 35323133 3535335a 301b3119
 30170603 55040313 10696f73 2d63612e 63697363 6f2e636f 6d30819f 300d0609
 2a864886 f70d0101 01050003 818d0030 81890281 81009ebb 48957c44 c940236f
 a1cda758 aa930e8c 91390734 b8ef814d 0bf7aec9 7ec40379 7749d3c6 154f6a32
 00738655 33b20207 037a9e15 3229fa72 478424fb 409f518d b13d328d e761be08
 8023b4ff f410054b 4423156d 66c99788 69ab5956 966d5e1b 4d1c1120 a05ad08c
 f036a134 3b2fc425 e4a2524f 36e0a129 2c8f6cee 971d0203 010001a3 63306130
 0f060355 1d130101 ff040530 030101ff 300e0603 551d0f01 01ff0404 03020186
 301f0603 551d2304 18301680 14082896 b9f4af20 75514321 d072f161 d09d2ec8
 aa301d06 03551d0e 04160414 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
 300d0609 2a864886 f70d0101 04050003 81810087 a06d354a f7423e0e 64a7c5ec
 6006fbde 914d7bfd f86ada50 b1a00d17 0bf06ec1 5423d514 fbeb0a76 986eb63f
```

```
f7fce99a 81c4b112 61fd69ce a2ce750e b1b3a6f9 84e92490 8f213613 451dd9a8
3fc3406a 854b20ed 27e4ddd8 62f6dea5 dd8b4396 1879b3e7 651cb9d1 3dd46b8b
32796963 9f6854f1 389f0060 aa0d1b8d f83e09
```

quit

certificate 08

```
3082028e 308201f7 a0030201 02020108 300d0609 2a864886 f70d0101 04050030
1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
31333131 31383136 31383130 5a170d31 33313132 38313631 3831305a 301e311c
301a0609 2a864886 f70d0109 02160d61 73612e63 6973636f 2e636f6d 30819f30
0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c38ee5 75215237
2728cffd 3519cd15 ebcaab2c 48d63b92 7562d2fc f7db60bc ecb03b2c 4e4dff07
47ad5122 80899055 37f346d7 d10962e9 1e5edb06 8985ee7e 8a6da977 2460f82e
53679457 ed10372a 9ff2946e 449214e4 9be95cab 51d7681c 2db0382b 048fe807
1d1bb9b0 e4bd9de6 c99cafea c279e943 1e1f5d1b d1e6010c b7020301 0001a381
de3081db 30310603 551d2504 2a302806 082b0601 05050703 0106082b 06010505
07030506 082b0601 05050703 0606082b 06010505 07030730 3c060355 1d1f0435
30333031 a02fa02d 862b6874 74703a2f 2f313932 2e313638 2e323534 2e323534
2f696f73 2d636163 64702e69 6f732d63 612e6372 6c301806 03551d11 0411300f
820d6173 612e6369 73636f2e 636f6d30 0e060355 1d0f0101 ff040403 0205a030
1f060355 1d230418 30168014 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
301d0603 551d0e04 1604145b 76de9ef0 d3255efe f4bc551b 69cd8398 d1596c30
0d06092a 864886f7 0d010104 05000381 81003fb0 ec7719cd 4f6162b2 90727db4
da5606f2 61441dc6 094fb3a6 defe62ef 5ff8f140 3bc3448c e0b42d26 07647607
fd7518cb 034139d3 e3648fd2 9d93b5e4 db3b828b 16d50dd5 3e18cdd6 74855de4
88a159d6 6ef51718 cf6cc4e4 53c2aca3 36442ff0 bb4b8493 22f0e632 a8b32b36
f287801f 8d47637f e4e9ee6a b4555094 c092
```

quit

```
!
! manually select the ISAKMP identity to use address on the ASA
```

```
crypto isakmp identity address
```

```
crypto ikev2 policy 1
```

```
encryption aes-256
```

```
integrity sha
```

```
group 14 5 2
```

```
prf sha
```

```
lifetime seconds 86400
```

```
crypto ikev2 policy 10
```

```
encryption aes-192
```

```
integrity sha256 sha
```

```
group 14 5 2
```

```
prf sha
```

```
lifetime seconds 86400
```

```
crypto ikev2 policy 30
```

```
encryption 3des
```

```
integrity sha
```

```
group 5 2
```

```
prf sha
```

```
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

```
!
```

```
! to allow pings from the CA interface that will bring up the tunnel during testing.
```

```
!
```

```
management-access CA
```

```
!
```

```
group-policy GroupPolicy2 internal
```

```
group-policy GroupPolicy2 attributes
```

```
vpn-idle-timeout 30
```

```
vpn-tunnel-protocol ikev1 ikev2
```

```
tunnel-group 172.16.1.1 type ipsec-l2l
```

```
tunnel-group 172.16.1.1 general-attributes
```

```
default-group-policy GroupPolicy2
```

```
tunnel-group 172.16.1.1 ipsec-attributes
!
! disable peer-id validation
!
peer-id-validate nocheck
ikev2 remote-authentication certificate
ikev2 local-authentication certificate ios-ca
: end
! NTP configuration
ntp trusted-key 1
ntp server 192.168.254.254
```

ルータの設定例

```
ip domain name cisco.com
!
crypto pki trustpoint tp_ikev2
enrollment url http://192.168.254.254:80
usage ike
fqdn R1.cisco.com
!
! necessary only in this example as no crl has been configured on the IOS CA.
! On the ASA this is enabled by default. When using proper 3rd party
! certificates this is not necessary.
!
revocation-check none
rsa-keypair ikev2_cert
eku request server-auth
!
crypto pki certificate chain tp_ikev2
certificate 0B
308202F4 3082025D A0030201 0202010B 300D0609 2A864886 F70D0101 05050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 32353233 35363537 5A170D31 33313230 35323335 3635375A 301D311B
30190609 2A864886 F70D0109 02160C52 312E6369 73636F2E 636F6D30 82012230
0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A1032A61
A3F14539 87816C22 8C66A170 3A9661EA 4AF6F063 3FC305B8 E525B84D AA74A9CE
666B1BF5 3C7DF025 31FEB161 CE49845F 3EC2DE7B D3FCC685 D6F80C8C 0AA12772
1B4AB15C 90C04446 068A0DBA 7BFA4E40 E978364F A2B07F7C 02C691A8 921A5481
A4AF07B4 BA0C9DBA D35F4566 6CB70553 DAF09A45 F2948C5A 1621E5D2 98508D49
A2EF61D3 AAF3A9DB 87F2D763 89AD0BBE 916A6CF8 1B59C426 7960013B 061AA0A5
F6870319 87A35ABA 8C1B5CF5 42976739 B8C936D3 24276E56 F59E3CFD 9B9B4A0D
2E5294AB C4470376 5D96915F 275CBC78 586D6755 F45C7592 62DCA916 CEC1A450
3FF090A9 15088CD2 13B90391 B0795263 071C7002 8CBF98F2 89788A0B 02030100
01A381C1 3081BE30 3C060355 1D1F0435 30333031 A02FA02D 862B6874 74703A2F
2F313932 2E313638 2E323534 2E323534 2F696F73 2D636163 64702E69 6F732D63
612E6372 6C303106 03551D25 042A3028 06082B06 01050507 03010608 2B060105
05070305 06082B06 01050507 03060608 2B060105 05070307 300B0603 551D0F04
04030205 A0301F06 03551D23 04183016 80140828 96B9F4AF 20755143 21D072F1
61D09D2E C8AA301D 0603551D 0E041604 14C63949 4CA10DBB 2BBB6F98 BAFF0EE2
B3716CEE 3B300D06 092A8648 86F70D01 01050500 03818100 3080FEF6 9160357B
6F28ED60 428BA6CE 203706F6 F91DA273 AF6E81D3 46539E13 B4C89A9A 19E1F0BC
A631A418 C30DFC8E 0585039D EB07D35D E719F5FE A4EE47B5 CED31B12 745C9EE8
5B6B0F17 67C3B965 C927B379 C674933F 84E7A1F7 851A6CF0 8775B1C5 3A033D90
75965DCA 86E4A842 E2C35AC0 6BFA8144 699B1582 C094BF35
quit
certificate ca 01
```

```
3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
```

quit

```
!
crypto ikev2 proposal aes-cbc-256-proposal
 encryption aes-cbc-256
 integrity sha1
 group 5 2 14
!
crypto ikev2 policy policy1
 match address local 172.16.1.1
 proposal aes-cbc-256-proposal
!
crypto ikev2 profile profile1
 description IKEv2 profile
!
! router configured to use address as the remote identity. By default local
  identity is address
!
 match address local 172.16.1.1
 match identity remote address 172.16.1.2 255.255.255.255
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint tp_ikev2
!
! disable http-url based cert lookup
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set ESP-AES-SHA
 set pfs group2
 set ikev2-profile profile1
 match address 103
!
interface Loopback0
 ip address 172.16.2.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
```

```

!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip route 192.168.0.0 255.255.255.0 172.16.1.2
ip route 192.168.254.254 255.255.255.255 192.168.1.254
!
! access list that defines crypto domains, must be mirror images on both peers.
!
access-list 103 permit ip 172.16.2.0 0.0.0.255 192.168.0.0 0.0.0.255
!
! ntp configuration
!
ntp trusted-key 1
ntp server 192.168.254.254
!
end

```

Cisco IOS CAの設定例

```

ip domain name cisco.com
!
! CA server configuration
!
crypto pki server ios-ca
 database archive pkcs12 password 7 02050D4808095E731F
 issuer-name CN=ios-ca.cisco.com
 grant auto
 lifetime certificate 10
 lifetime ca-certificate 30
 cdp-url http://192.168.254.254/ios-cacdp.ios-ca.crl
 eku server-auth ipsec-end-system ipsec-tunnel ipsec-user
!
! this trustpoint is generated automatically when the CA server is enabled.
!
crypto pki trustpoint ios-ca
 revocation-check crl
 rsa-keypair ios-ca
!
!
crypto pki certificate chain ios-ca
 certificate ca 01
 3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
 31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
 30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
 2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
 A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
 00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
 8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
 F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
 301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
 AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
 300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC

```

```
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
quit
voice-card 0
!
!
interface Loopback0
 ip address 192.168.254.254 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 duplex auto
 speed auto
!
! http-server needs to be enabled for SCEP
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.122.162.129
ip route 172.18.108.26 255.255.255.255 10.122.162.129
!
! ntp configuration
!
ntp trusted-key 1
ntp master 1
!
end
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。


次のコマンドは、ASA とルータの両方で動作します。

- `show crypto ikev2 sa` – フェーズ1セキュリティアソシエーション(SA)の状態を表示します。
- `show crypto ipsec sa` – フェーズ2 SAの状態を表示します。



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 Perfect Forwarding Secrecy(PFS)Diffie-Hellman(DH)グループ値が「PFS (Y/N): N, DH group: none」と表示されます。キー再生成が発生すると、正しい値が表示されます。これはバグではなく、正常な動作です。

IKEv2 では、IKEv1 と IKEv2 の違いは、子 SA が認証交換自体の一部として作成される点です。クリプト マップに設定された 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ための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。

フェーズ 1 の確認

次の手順では、フェーズ 1 のアクティビティを確認します。

1. config コマンドを入力します `show crypto ikev2 sa` コマンドをルータで入力します。

```
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.1/500 172.16.1.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/53 sec
IPv6 Crypto IKEv2 SA
```

2. config コマンドを入力します `show crypto ikev2 sa` ASAで次のコマンドを実行します。

```
ciscoasa/vpn(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
45926289 172.16.1.2/500 172.16.1.1/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/4 sec
Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
remote selector 172.16.2.0/0 - 172.16.2.255/65535
ESP spi in/out: 0xa84caabb/0xf18dce57
```

フェーズ 2 の確認

次の手順では、Security Parameter Index (SPI) が 2 のピアで正常にネゴシエートされたかどうかを確認する方法について説明します。

1. config コマンドを入力します `show crypto ipsec sa | i spi` コマンドをルータで入力します。

```
R1#show crypto ipsec sa | i spi
current outbound spi: 0xA84CAABB(2823596731)
spi: 0xF18DCE57(4052602455)
spi: 0xA84CAABB(2823596731)
```

2. config コマンドを入力します `show crypto ipsec sa | i spi` ASAで次のコマンドを実行します。

```
ciscoasa/vpn(config)# show crypto ipsec sa | i spi
current outbound spi: F18DCE57
current inbound spi : A84CAABB
spi: 0xA84CAABB (2823596731)
spi: 0xF18DCE57 (4052602455)
```

次の手順では、トラフィックがトンネルを通過するかどうかを確認する方法について説明します。

1. config コマンドを入力します `show crypto ipsec sa | i pkts` コマンドをルータで入力します。


```
R1#show crypto ipsec sa | i pkts
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

2. config コマンドを入力します `show crypto ipsec sa | i pkts` ASAで次のコマンドを実行します。


```
ciscoasa/vpn(config)# show crypto ipsec sa | i pkts
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp
failed: 0
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

 注：使用する前に、『[debugコマンドの重要な情報](#)』を参照してください debug コマンドを発行します。

ASA でのデバッグ

 注意:ASAでは、さまざまなデバッグレベルを設定できます。デフォルトでは、レベル1が使用されます。デバッグレベルを変更すると、デバッグの冗長性が増す場合があります。特に実稼働環境では、注意して変更してください。

トンネル ネゴシエーションの ASA のデバッグは次のとおりです。

- `debug crypto ikev2 protocol`
- `debug crypto ikev2 platform`

証明書認証に関する ASA のデバッグは次のとおりです。

- `debug crypto ca`

ルータのデバッグ

トンネル ネゴシエーションのルータのデバッグは次のとおりです。

- `debug crypto ikev2`
- `debug crypto ikev2 error`
- `debug crypto ikev2 internal`

証明書認証のルータのデバッグは次のとおりです。

- `debug cry pki validation`
- `debug cry pki transaction`
- `debug cry pki messages`

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。