リモート アクセス VPN の ASA IKEv2 デバッグのトラブルシューティング

目次

概要

このドキュメントでは、Internet Key Exchange Version 2（IKEv2）を Cisco AnyConnect モビリティ クライアントで使用している場合に、Cisco 適応型セキュリティ アプライアンス（ASA）でのデバッグをどのように理解するかについて説明します。 また、特定のデバッグ行を ASA 設定に変換する方法に関する情報も提供します。

このドキュメントでは、ASA に VPN トンネルが確立された後にトラフィックをどのように受け渡すかについては説明せず、IPSec や IKE の基本概念も含まれていません。

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 適応型セキュリティ アプライアンス（ASA）バージョン 8.4 以降

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

主な問題

Cisco Technical Assistance Center（TAC）では、IPsec VPN トンネルの確立に問題があっても、コマンドが暗号化できる場合を把握するために、IKE や IPSec のデバッグコマンドを頻繁に使用しています。

シナリオ

debug コマンド

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

ASA の設定

この ASA 設定では基本中の基本であり、外部サーバを使用しません。

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure

crypto ikev2 policy 10
 encryption aes-192
```

```
 integrity sha
 group 2
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
 anyconnect modules value dart
 anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

XML ファイル

```
<ServerList>
       <HostEntry>
              <HostName>Anu-IKEV2</HostName>
              <HostAddress>10.0.0.1</HostAddress>
              <UserGroup>ASA-IKEV2</UserGroup>
              <PrimaryProtocol>IPsec</PrimaryProtocol>
       </HostEntry>
</ServerList>
```

注: XML のクライアント プロファイルの UserGroup の名前は、ASA のトンネル グループの名前と同じである必要があります。 同じでない場合は、「Invalid Host Entry. Please re-enter」というエラー メッセージが AnyConnect クライアントに表示されます。

デバッグ ログと説明

注: Diagnostic and Reporting Tool（DART）からのログは些細な内容である場合が多く、この例では無意味であるため、特定の DART のログは省略しています。

サーバ メッセージの説明

ASA がクライアントから IKE_SA_INIT メッセージを受信します。

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ネゴ
クライアントから受信した IKE_SA_INIT メッセージには次のフィールドが含まれています。

1. **ISAKMP ヘッダー** - SPI//バージョン/フラグ
2. **SAi1** - IKE の発信側がサポートする暗号化アルゴリズム
3. **KEi** - 発信側の DH 公開キーの値
4. **N** - 発信側のナンス

ASA は
IKE_INIT メッセージを確認し、処理します。 ASA は次を実行します。

1. 暗号スイートを発信側が
   提供したものから選択します。
2. 自身の DH 秘密キーを計算します。
3. この IKE_SA 用のすべてのキーを
   導出することができる SKEYID 値
   を計算します。 後続のすべての
   メッセージのヘッダーが
   暗号化され、認証されます。 その
   暗号化に使用されたキーおよび
   完全性の保護は、SKEYID から
   導出され、次のように知られています。

   SK_e - 暗号化**SK_a** - 認証**SK_d** - CHILD_SAs
   の詳細なキー関連情報の
   導出のために
   導出し、使用SK_e と SK_a は
   方向ごとに個々に計算されます。

関連コンフィギュレーション

```
crypto ikev2 policy 10
 encryption aes-192 integrity
sha group 2  prf sha lifetime
seconds 86400
crypto ikev2 enable outside
```

ASA は IKE_SA_INIT 交換の応答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。

1. **ISAKMP ヘッダー** - SPI//バージョン/フラグ
2. **SAr1** - IKE の応答側が選択する暗号化アルゴリズム
3. **KEr** - 応答側の DH 公開キーの値
4. **N** - 応答側のナンス

ASA が IKE_SA_INIT 交換の応答メッセージを送信します。 これで IKE_SA_INIT 交換が完了しました。

この認証は、EAP を使用して行われます。 EAP のメッセージ交換では、単一の EAP 認証方式だけが許す。

クライアントに IDi ペイロードが含まれていても
AUTH ペイロードが含まれていない場合は、
クライアントは ID を宣言たものの証明されて
いないことを示します。 デバッグでは、AUTH
ペイロードはクライアントから送信される
IKE_AUTH パケットにはありません。 クライアントの除外は、
EAP 交換が正常に行われた後にのみ、
AUTH ペイロードを送信します。 ASA が
拡張認証方式を使用
する場合は、EAP ペイロードを
メッセージ 4 に配置し、送信側の
認証が後続の IKE_AUTH 交換で
完了するまで、SAr2、TSi、および
TSr の送信を延期します。
IKE_AUTH の発信側パケットには、次が含まれています。

1. **ISAKMP ヘッダー** -
   SPI//バージョン/フラグ

2. **IDi** - クライアントが接続したい
   トンネル グループの名前は、
   IKE_AUTH 交換の最初の
   メッセージのタイプ ID_KEY_ID の
   IDi ペイロードで提供される場合が
   あります。 これは、
   クライアント プロファイル* が
   グループ名で事前に設定されているか、
   前回の正常な認証後に、
   クライアントが優先順位ファイルの
   グループ名をキャッシュしている場合に
   発生します。 ASA は
   トンネル グループ名と IKE IDi
   ペイロードの内容を一致させようと
   します。 最初に成功した
   IPsec VPN が確立された後、
   クライアントはユーザが認証された
   グループ名 (グループ エイリアス) を
   キャッシュします。 このグループ
   名は、ユーザが希望した
   予測グループを示すために、
   次の接続試行の
   IDi ペイロードで提供
   されます。 EAP 認証がクライアント プロファイル
   で指定または示唆されていて、
   プロファイルに <IKEIdentity> 要素
   が含まれていない場合は、
   クライアントは固定文字列
   $AnyConnectClient$ を
   含んだ ID_GROUP タイプの
   IDi ペイロードを送信します。
3. **CERTREQ** - クライアントは、
   優先度の高い証明書の
   ASA を要求しています。 証明書
   要求ペイロードは、送信側が
   受信側の証明書を入手する
   必要がある場合に、交換の際に
   含められる場合があります。 証明書要求
   ペイロードは、プロセッサに
   この種の証明書があるか
   どうかを特定するため、
   [Cert encodindg] フィールドの検査
   により処理されます。 この場合、
   指定した証明機関のいずれか
   で検証できる証明書がプロセッサ
   にあるかかどうかを特定するために、
   [Certification Authority]

フィールドが検査
されます。 これは、証明書のチェーンである場合があります。
指定できます。

4. CFG - CFG_REQUEST/
   CFG_REPLY では、IKE
   エンドポイントを使用して、ピア
   の情報を要求できます。 CFG_REQUEST 設定
   ペイロードの属性がゼロ長でない
   場合は、その属性
   についての推奨として
   考えることができます。CFG_REPLY
   設定ペイロードがその値、または
   新しい値を返すことがあります。 また、
   新しい属性を追加して、
   要求したものを含めない場合があります。
   要求側は、認識しない
   属性が返された場合は
   それらを無視します。 このようなデバッグでは、
   クライアントが CFG_REQUEST
   でトンネル設定を要求
   します。 ASA は
   EAP 交換が成功した後にだけ、
   これに応答し、トンネル設定
   属性を送信します。
5. SAi2 - SAi2 は、IKEv1 の
   フェーズ 2 のトランスフォーム セットの
   交換に類似した SA を開始します。
6. TSi および TSr - 発信側と
   応答側のトラフィック セレクタには、
   暗号化されたトラフィックを転送
   および受信するために、発信側と
   応答側の送信元と宛先の
   アドレスがそれぞれ含まれて
   います。 アドレス範囲は、
   その範囲を対象とするすべてのトラフィック
   がトンネリングされることを指定します。 If the
   が応答側に受け入れられる場合は、
   同じ TS ペイロードを送り返し
   ます。

クライアントがグループ認証用に提供する
必要がある属性は AnyConnect
プロファイル ファイルに保存されています。
**関連プロファイル設定:

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
```

```
</HostAddress>
 <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

ASA は IKE_AUTH メッセージへの応答を生成し、クライアントに対して自身を認証するための準備を行

ASA はクライアントからユーザ クレデンシャルを要求するために、AUTH ペイロードを送信します。 A
アントに送信することになます。これにより、クライアントは ASA サーバを認証できます。
ASA には拡張性認証方式の使用を希望しているため、EAP ペイロードをメッセージ 4 に配置し、発信側
信を延期します。 したがって、これらの 3 種類のペイロードはデバッグにありません。
EAP パケットには次が含まれています。

1. **Code (コード) ： request** - このコードはオーセンティケータによってピアに送信されます。
2. **id: 1** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は、EAP 交換の最初のパケット
   になります。 これは ASA からクライアントに送信され、EAP 交換が開始されます。
3. **Length: 150** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

フラグメンテーションは、証明書が大きいか、証明書チェーンが含まれている場合に発生する可能性があ
ンを引き起こす可能性がある大きいキーが含まれている場合がありす。

クライアントは、応答という形で EAP 要求に応答します。
EAP パケットには次が含まれています。

1. **Code (コード) ： response** - このコードは、EAP 要求への応答としてピアがオーセンティケータ
2. **id: 1** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は 1 です。これは、ASA (オー
   。 この EAP 応答は「config autht」タイプが「init」になります。 クライアントが EAP 交換を初期
3. **Length: 252** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

ASA はこの応答を復号化し、クライアントは前のパケット (および証明書) で AUTH ペイロードを受信
init」EAP 応答パケットに含まれているものです。

これは、ASA がクライアントに送信した 2 番目の要求です。
EAP パケットには次が含まれています。

1. **Code (コード) ： request** - このコードはオーセンティケータによってピアに送信されます。
2. **id: 2** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は、EAP 交換の 2 番目のパケッ
   request」になります。 ASA は、クライアントがユーザ認証クレデンシャルを送信するように要求
3. **Length: 457** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

ENCR ペイロード:
このペイロードは復号化され、そのコンテンツは追加ペイロードとして解析されます。

クライアントが EAP のペイロードがある別の IKE_AUTH 発信側メッセージを送信します。
EAP パケットには次が含まれています。

1. **Code (コード) ： response** - このコードは、EAP 要求への応答としてピアがオーセンティケータ
2. **id: 2** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は 2 です。これは、ASA (オー
   。
3. **Length: 420** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

ASA がこの応答を処理します。 クライアントは、ユーザがクレデンシャルを入力するように要求してい
このパケットにはユーザが入力したクレデンシャルが含まれています。

ASA は交換で 3 番目の EAP 要求を作成します。
EAP パケットには次が含まれています。

1. **Code (コード) ： request** - このコードはオーセンティケータによってピアに送信されます。
2. **id: 3** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は EAP 交換の 3 番目のパケット
   complete」になります。 ASA は応答を受信し、EAP 交換が完了します。
3. **Length: 4235** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

ENCR ペイロード:
このペイロードは復号化され、そのコンテンツは追加ペイロードとして解析されます。

クライアントは EAP ペイロードを含む発信側パケットを送信します。
EAP パケットには次が含まれています。

1. **Code (コード) ： response** - このコードは、EAP 要求への応答としてピアがオーセンティケータ
2. **id: 3** - ID は、要求への EAP 応答の照合に役立ちます。 ここで、値は 3 です。これは、ASA (オー
   。 これで、ASA はクライアントから応答パケットを受信します。この「config-auth」タイプは「a
   受領を確認します。
3. **Length: 173** - EAP パケットの長さには、コード、ID、長さ、EAP データが含まれます。
4. **EAP データ**

ASA がこのパケットを処理します。 その
AUTH ペイロードを送信します。 ASA は
次のパケットでトンネル グループを送信
する準備を行います。これは、クライアント
が以前 IDi ペイロードで要求
しています。 ASA はクライアントから
応答パケットを受信します。この

「config-aut」タイプは「ack」です。 これは、
この応答で、ASA が前に送信
した EAP 「complete」メッセージの
受信を確認します。
関連コンフィギュレーション

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
 <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

これで EAP 交換が成功しました。
EAP パケットには次が含まれています。

1. Code: success - このコードは
   EAP 認証方式の完了後に
   オーセンティケータがピアに送信します。
   認証方式を設定します。 これは、
   ピアがオーセンティケータに
   正常に認証されたことを
   示します。
2. id: 3 - ID は、EAP 応答の
   要求との照合に役立ちます。
   ここで、値は 3 です。これは、
   ASA（オーセンティケータ）が以前送信
   した要求への応答であることを
   示します。 交換の 3 セット
   目のパケットが成功し、
   EAP 交換が成功
   しました。
3. Length: 4 - EAP パケットの
   長さには、コード、ID、長さ、
   EAP データが含まれます。
4. EAP データ

EAP 交換が成功したため、クライアントは AUTH ペイロードを含む IKE_AUTH 発信側パケットを送信し

EAP 認証が指定されている、または
クライアント プロファイルで示唆されており、
プロファイルに <IKEIdentity> 要素が
含まれていない場合は、クライアントは
固定文字列 *$AnyConnectClient$*
を含む ID_GROUP タイプの IDi ペイロードを送信します。
ASA がこのメッセージを処理します。

関連コンフィギュレーション

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
 <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

ASA は、SA、TSi、および TSr のペイロードを含む IKE_AUTH 応答メッセージを作成します。
IKE_AUTH の応答側パケットには、次が含まれています。

1. **ISAKMP ヘッダー** - SPI//バージョン/フラグ
2. **AUTH ペイロード** - 選択した認証方式が含まれる
3. **CFG** - CFG_REQUEST/CFG_REPLY により、IKE エンドポイントがピアの情報を要求できます。
   の推奨として考えることができます。 CFG_REPLY 設定ペイロードは、その値、または新しい値を
   ない場合もあります。 要求側は、認識しない属性が返された場合は、それを無視します。 ASA は、
4. **SAr2** - SAr2 が 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 を開始します。
5. **TSi** と **TSr** - 発信側と応答側のトラフィックのセレクタには、暗号化されたトラフィックを転送およ
   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
   答側は同一の TS ペイロードを送り返します。

ENCR ペイロード:
このペイロードは復号化され、そのコンテンツは追加ペイロードとして解析されます。

ASA は、9 個のパケットに断片化されたこの IKE_AUTH 応答メッセージを送信します。 IKE_AUTH 交換

接続はセキュリティ アソシエーション (SA) データベースへ入り、ステータスは REGISTERED になり
の有無など、いくつかの検査を行い、デッド ピア検出 (DPD) などの値を設定します。

トンネルの確認

AnyConnect

show vpn-sessiondb detail anyconnect コマンドの出力例を次に示します。

```
Session Type: AnyConnect Detailed

Username     : Anu                    Index        : 2
Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 11192
Pkts Tx      : 0                      Pkts Rx      : 171
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
Login Time   : 22:06:24 UTC Mon Apr 22 2013
Duration     : 0h:02m:26s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.1
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Client Type  : AnyConnect
Client Ver   : 3.0.1047
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 25171                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES192                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86254 Seconds
  PRF          : SHA1                   D/H Group    : 1
  Filter Name  :
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
```

```
  Remote Addr  : 10.2.2.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 11192
  Pkts Tx      : 0                      Pkts Rx      : 171
 NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 146 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
Redirect URL :
```

ISAKMP

show crypto ikev2 sa コマンドの出力例を次に示します。

```
Session Type: AnyConnect Detailed

Username     : Anu                    Index        : 2
Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 11192
Pkts Tx      : 0                      Pkts Rx      : 171
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
Login Time   : 22:06:24 UTC Mon Apr 22 2013
Duration     : 0h:02m:26s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.1
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Client Type  : AnyConnect
Client Ver   : 3.0.1047
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 25171                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES192                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86254 Seconds
  PRF          : SHA1                   D/H Group    : 1
  Filter Name  :
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.2.2.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
```

```
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 11192
  Pkts Tx      : 0                      Pkts Rx      : 171
 NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 146 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
Redirect URL :
```

show crypto ikev2 sa detail コマンドの出力例を次に示します。

```
ASA-IKEV2# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
      Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/98 sec
      Session-id: 2
      Status Description: Negotiation done
      Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
      Local id: hostname=ASA-IKEV2
      Remote id: *$AnyConnectClient$*
      Local req mess id: 0              Remote req mess id: 9
      Local next mess id: 0             Remote next mess id: 9
      Local req queued: 0               Remote req queued: 9       Local window:
1                  Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

show crypto ipsec sa コマンドの出力例を次に示します。

```
ASA-IKEV2# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
      Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/98 sec
      Session-id: 2
      Status Description: Negotiation done
```

```
      Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
      Local id: hostname=ASA-IKEV2
      Remote id: *$AnyConnectClient$*
      Local req mess id: 0              Remote req mess id: 9
      Local next mess id: 0             Remote next mess id: 9
      Local req queued: 0               Remote req queued: 9       Local window:
1                 Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

関連情報

- RFC 4306、Internet Key Exchange（IKEv2）プロトコル
- RFC 3748、拡張可能認証プロトコル（EAP）
- RFC 5996、Internet Key Exchange Protocol Version 2（IKEv2）
- テクニカル サポートとドキュメント – Cisco Systems