# IKEv2マルチキー交換を使用して2つのASA間にサイト間IKEv2トンネルを設定する

## 内容



## はじめに

このドキュメントでは、IKEv2マルチキーエクスチェンジ(MKEY)を使用して2つのCisco ASA間のサイト間IKEv2 VPN接続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。

- Cisco Adaptive Security Appliance（ASA）
- IKEv2の一般的な概念

### 使用するコンポーネント

このドキュメントの情報は、9.20.1を実行するCisco ASAに基づくものです。

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。

### 制限事項

IKEv2 Multiple Key Exchange(MKEY)には次の制限があります。

- ASA CLIでのみサポート
- マルチコンテキストおよびHAデバイスでサポート
- クラスタ化されたデバイスではサポートされない

### ライセンス

ライセンス要件は、ASAでのサイト間VPNの場合と同じです。

## 背景説明

### 追加のキー交換の必要性

大きな量子コンピュータの登場は、特に公開鍵暗号法を使用するセキュリティシステムに大きなリスクをもたらします。通常の計算機では難しいと思われていた暗号法は、量子計算機では簡単に破れる。そのため、ポスト量子暗号(PQC)アルゴリズムとも呼ばれる、新しい量子耐性のある方法に切り替える必要性が生じています。複数のキー交換を使用することで、IPSec通信のセキュリティを強化することを目的としています。これには、従来の鍵交換と量子化後の鍵交換を組み合わせることが含まれます。このアプローチにより、結果として得られる交換は従来の鍵交換と少なくとも同等の強度があり、セキュリティの層が追加されます。

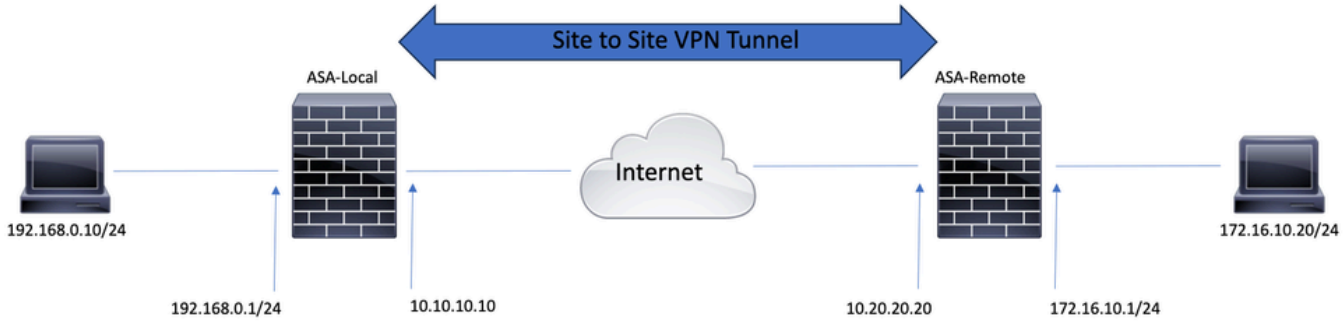
計画では、複数のキー交換のサポートを追加して、IKEv2を改善します。これらの特別なキー交換は、量子の脅威から安全なアルゴリズムを処理できます。これらの追加キーに関する情報を交換するために、Intermediate Exchangeという新しいメッセージタイプが導入されました。これらのキー交換は、SAペイロードを介して、通常のIKEv2方式を使用してネゴシエートされます。

## 設定

このセクションでは、ASAの設定について説明します。

### ネットワーク図

このドキュメントの情報は、次のネットワーク設定を使用します。

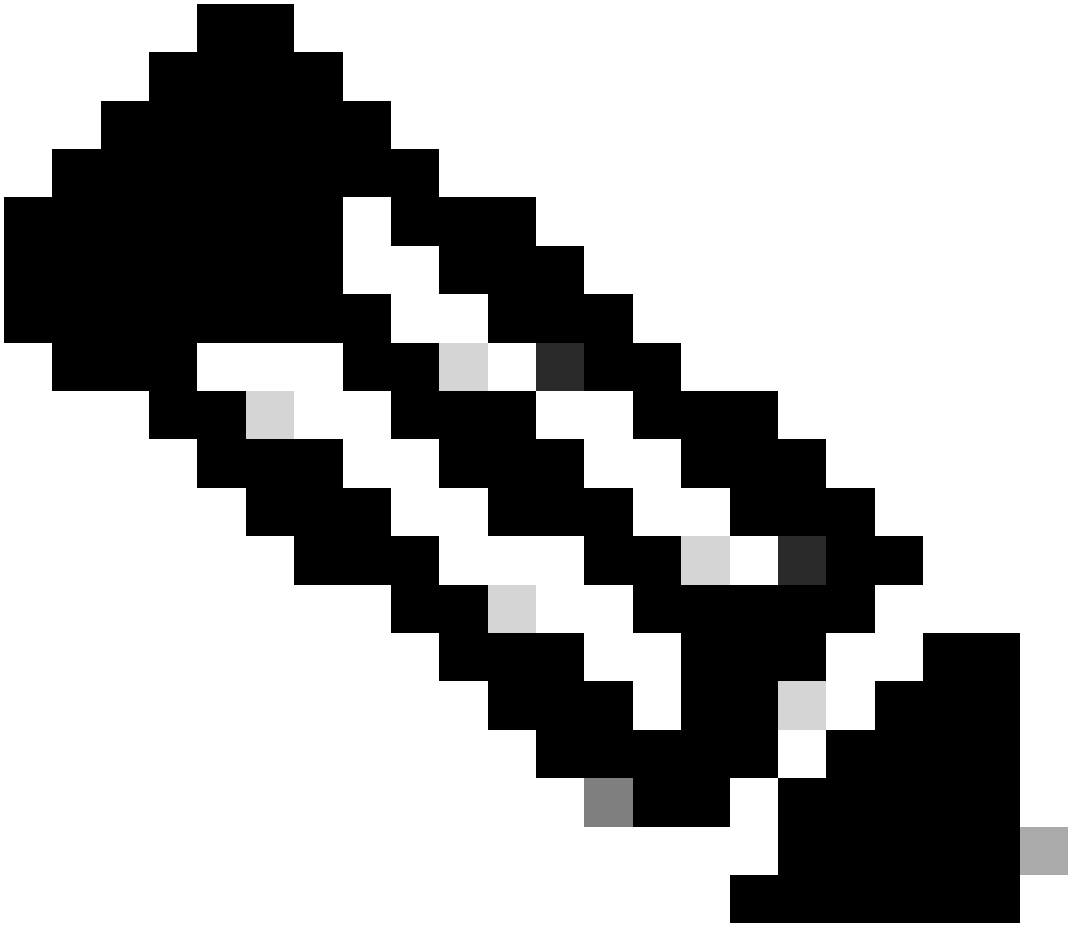



## ASA の設定

### ASA インターフェイスの設定

ASAインターフェイスが設定されていない場合、少なくともIPアドレス、インターフェイス名、およびセキュリティレベルを設定してください。

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```



注：内部ネットワークと外部ネットワークの両方に接続できることを確認してください。特に、サイト間VPNトンネルを確立するために使用されるリモートピアに接続できることを確認してください。基本的な接続を確認するには、ping を使用できます。

複数のキー交換を使用したIKEv2ポリシーの設定と外部インターフェイスでのIKEv2の有効化

これらの接続のIKEv2ポリシーを設定するには、次のコマンドを入力します。

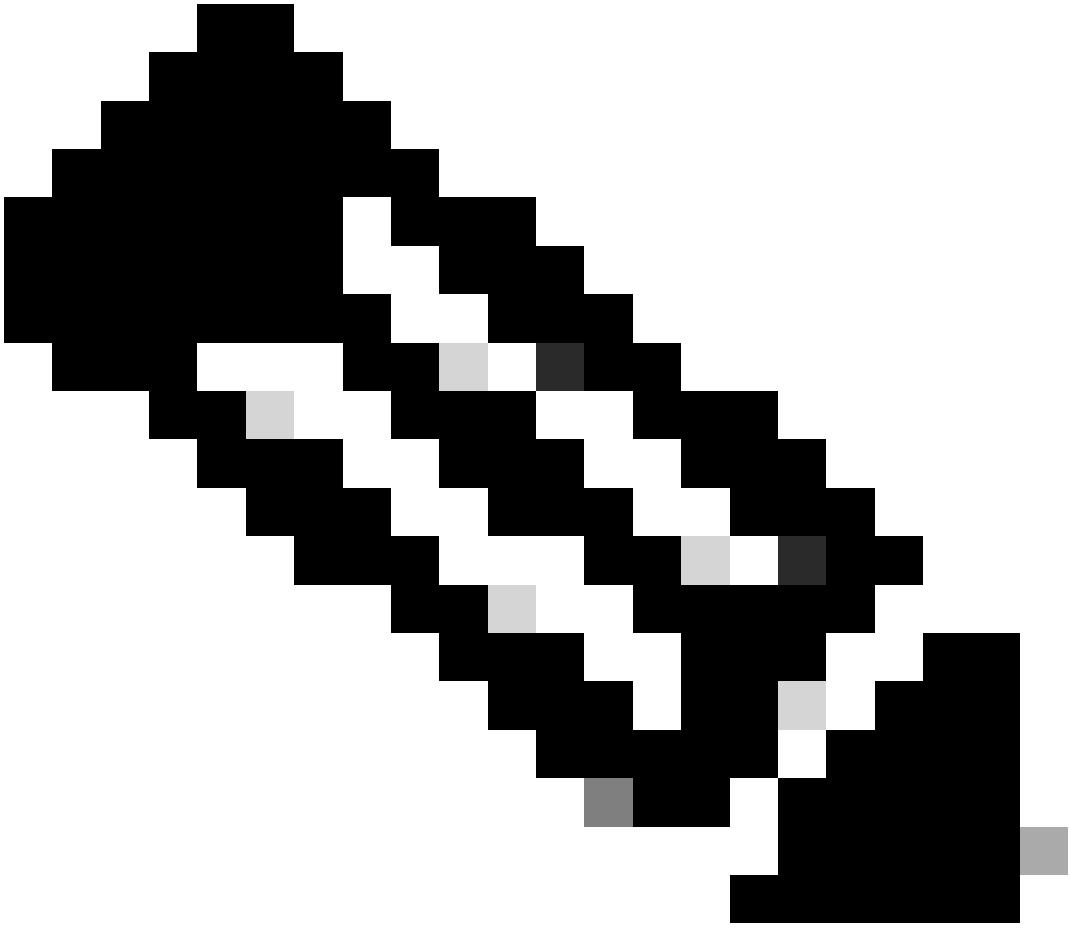
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

その他のキー交換トランスフォームは、additional-key-exchangeコマンドを使用してcrypto ikev2 policyで設定できます。さらに合計7つのExchangeトランスフォームを設定できます。この例では、2つの追加の交換トランスフォームが設定されています（DHグループ21および31を使用）。

```
additional-key-exchange 1 key-exchange-method 21 additional-key-exchange 2 key-exchange-method 31
```

最終的なIKEv2ポリシーは次のようになります。

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



**注：**IKEv2ポリシーの一致が存在するのは、2つのピアからの両方のポリシーに同じ認証、暗号化、ハッシュ、Diffie-Hellmanパラメータ、および追加のキー交換パラメータ値が含まれている場合です。

---

VPNトンネルを終端するインターフェイスでIKEv2を有効にする必要があります。通常、これは外部（またはインターネット）インターフェイスです。IKEv2を有効にするには、グローバルコンフィギュレーションモードでcrypto ikev2 enable outsideコマンドを入力します。

トンネルグループの設定

サイト間トンネルの接続プロファイルタイプはIPSec-l2lです。IKEv2事前共有キーを設定するには、次のコマンドを入力します。

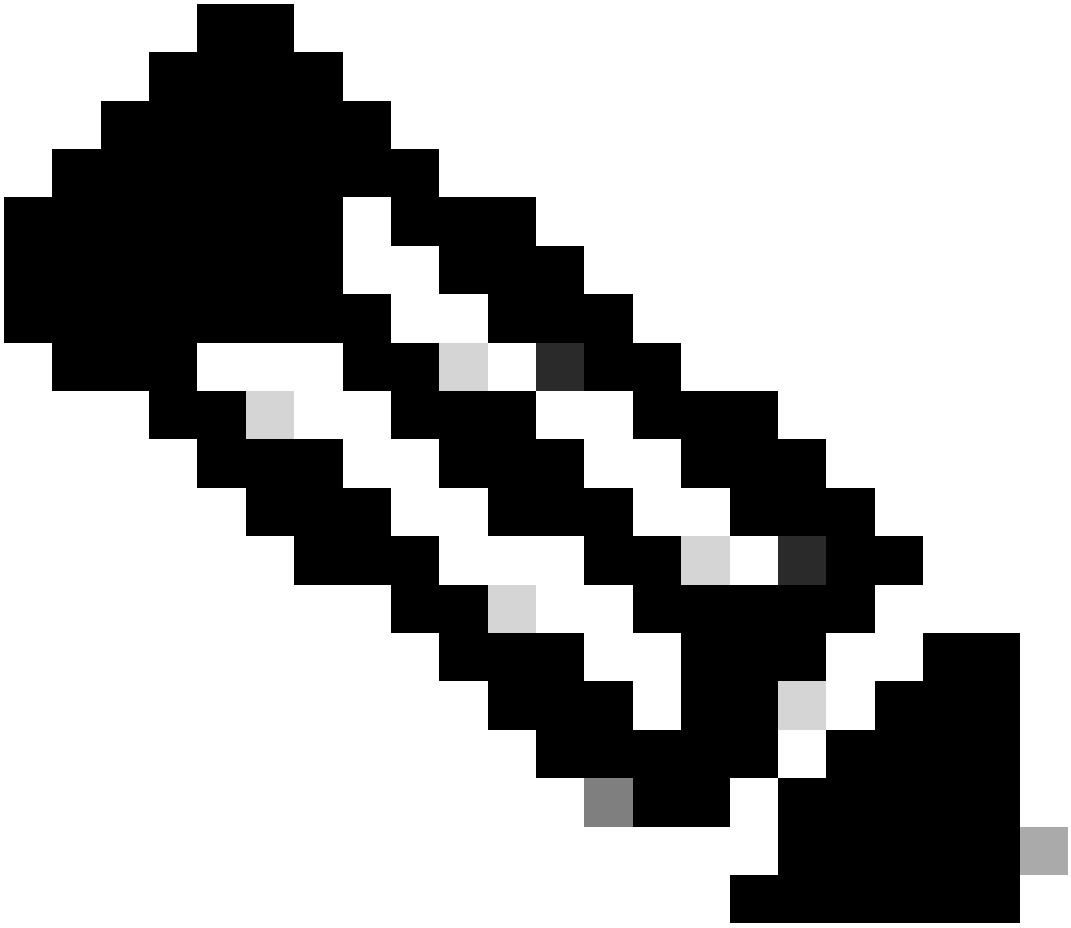
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

対象トラフィックとクリプトACLの設定

ASAは、アクセスコントロールリスト(ACL)を使用して、IPSec暗号化で保護する必要があるトラフィックと保護を必要としないトラフィックを区別します。これは、許可 Application Control Engine（ACE）に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが確実に保護されるようにします。

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
```

```
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```



**注**:VPNピアには、ミラー形式の同じACLが必要です。

---

アイデンティティNATの設定（オプション）

通常、対象トラフィックがダイナミックNATにヒットしないようにするには、アイデンティティNATが必要です。この場合に設定されるアイデンティティNATは次のとおりです。

nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup

IKEv2 IPSecプロポーザルの設定

IKEv2 IPSecプロポーザルは、データトラフィックを保護するための暗号化および整合性アルゴリズムのセットを定義するために使用されます。IPSec SAを正常に構築するには、このプロポーザルが両方のVPNピアと一致している必要があります。この場合に使用するコマンドは次のとおりです。

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

暗号マップの設定とインターフェイスへのバインド

暗号マップは、必要なすべての設定を組み合わせたものであり、必ず次のものを含む必要があります。

- 暗号化する必要があるトラフィックに一致するアクセスリスト（一般にクリプトACLと呼ばれる）
- ピア ID
- 1つ以上のIKEv2 IPSecプロポーザル

ここで使用する設定は次のとおりです。

crypto map outside_map 1 match address asa-vpn crypto map outside_map 1 set peer 10.20.20.20 crypto map outside_map 1 set ikev2 ipsec-proposal IKEV

最後に、crypto map outside_map interface outsideコマンドを使用して、この暗号マップを外部（パブリック）インターフェイスに適用します。

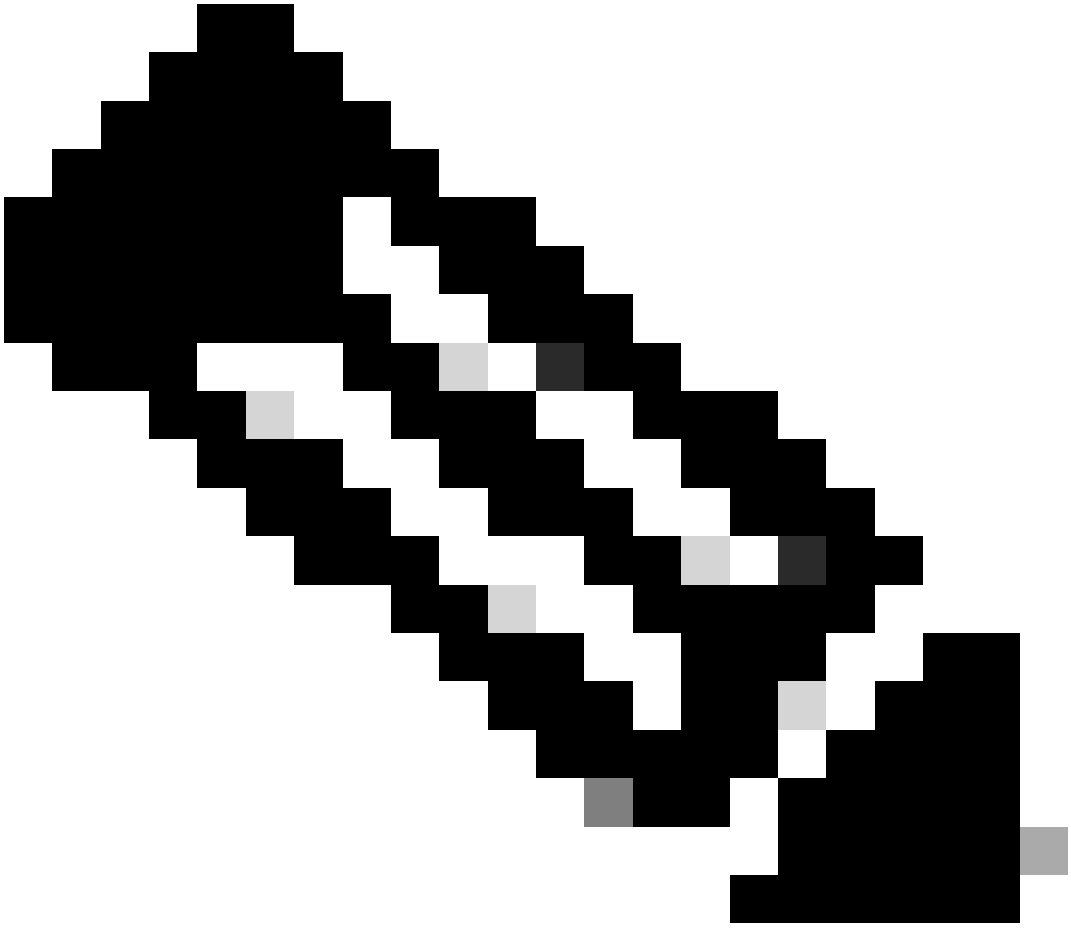
ローカルASAの最終設定

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
```

```
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
!
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
!
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

リモートASAの最終設定

```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```

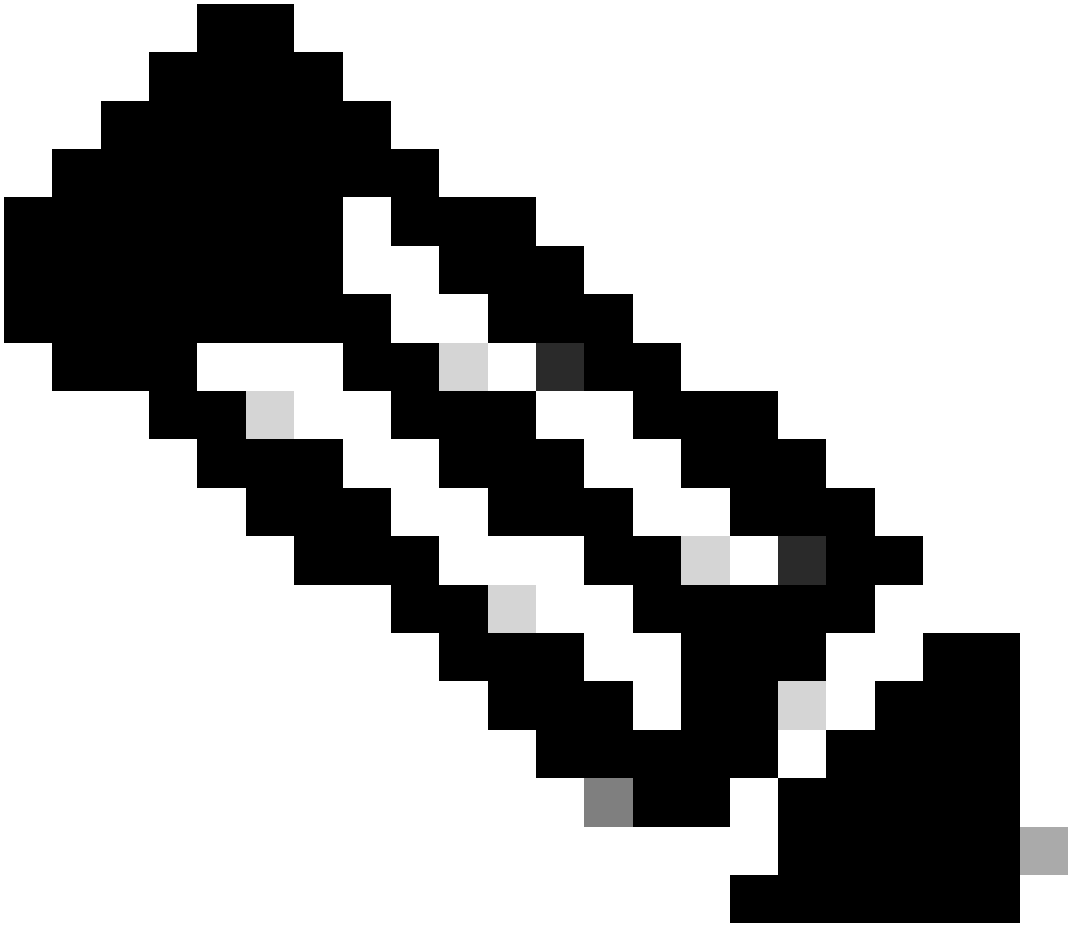


**注**:ACLはミラー形式であり、事前共有キーは両端で同じです。

---

## 確認

トンネルがアップ状態でトラフィックを通過させているかどうかを確認する前に、対象トラフィックがASAに送信されていることを確認する必要があります。



**注**：パケットトレーサはトラフィックフローをシミュレートするために使用しました。これを行うには、packet-tracerコマンドを使用します。packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11については、ローカルASAで詳しく説明されています。

---

追加のキー交換を検証するには、show crypto ikev2 saコマンドを使用できます。出力に示されているように、選択した交換アルゴリズムを検証するためにAKEパラメータを確認できます。

<#root>

Local-ASA# show crypto ikev2 sa IKEv2 SAs: Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status R

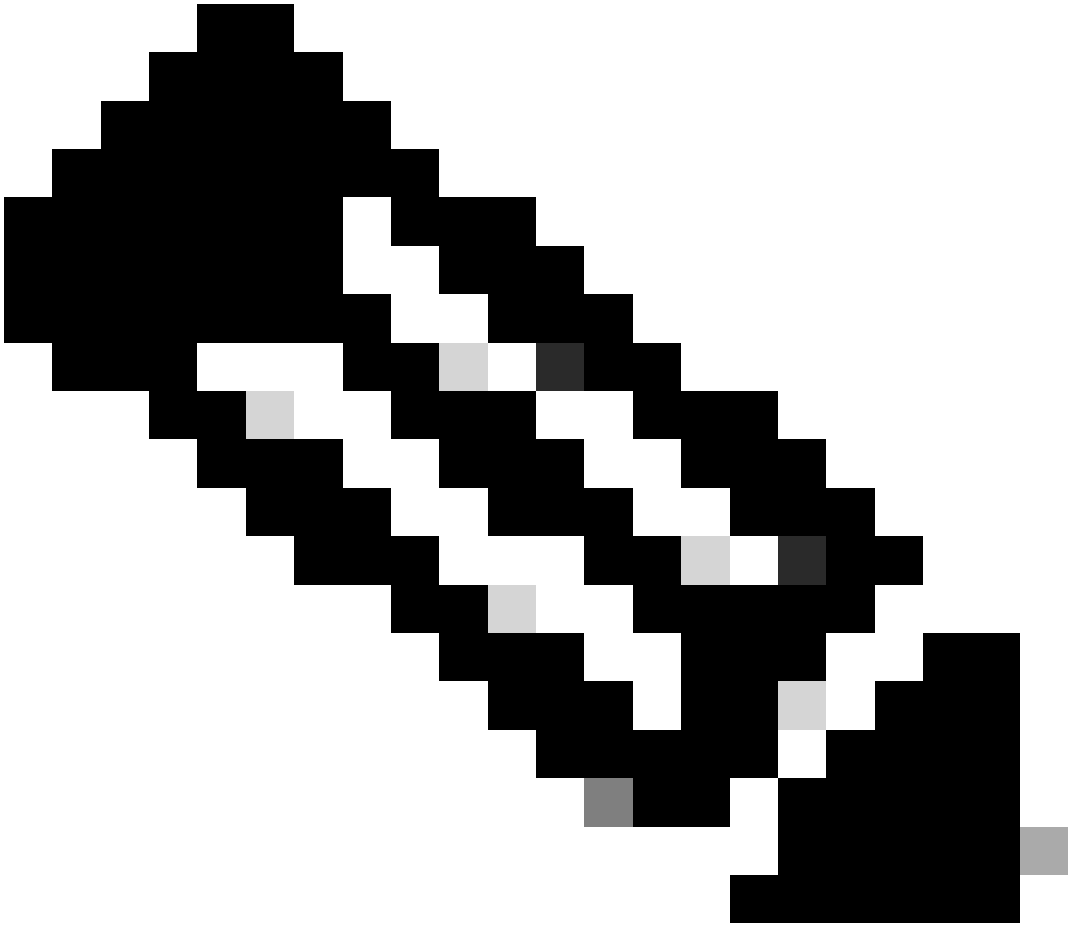
**AKE1: 21 AKE2: 31**

```
 Life/Active Time: 86400/7 sec Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535 remote sele
```

トラブルシュート

上記のデバッグは、IKEv2トンネルのトラブルシューティングに使用できます。

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```



**注：**1つのトンネルだけをトラブルシューティングする場合（デバイスが実稼働環境にある場合に必要）、debug crypto condition peer X.X.X.Xコマンドを使用して、デバッグを条件付きで有効にする必要があります。

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。