

ASA と Cisco IOS ルータの間におけるサイト間 IPSec IKEv1 トンネルの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ASA の設定](#)

[ASA インターフェイスの設定](#)

[IKEv1 ポリシーを設定し、外部インターフェイスの IKEv1 を有効にする](#)

[トンネルグループ \(LAN-to-LAN 接続プロファイル \) の設定](#)

[対象の VPN トラフィックの ACL の設定](#)

[NAT 適用除外の設定](#)

[IKEv1 トランスフォーム セットの設定](#)

[暗号マップの設定とインターフェイスへの適用](#)

[ASA の最終設定](#)

[Cisco IOSルータのCLI設定](#)

[インターフェイスの設定](#)

[ISAKMP \(IKEv1 \) ポリシーの設定](#)

[暗号 ISAKMP キーの設定](#)

[対象の VPN トラフィックの ACL 設定](#)

[NAT 適用除外の設定](#)

[トランスフォーム セットの設定](#)

[暗号マップの設定とインターフェイスへの適用](#)

[Cisco IOSの最終設定](#)

[確認](#)

[フェーズ 1 の確認](#)

[フェーズ 2 の確認](#)

[フェーズ 1 および 2 の確認](#)

[トラブルシューティング](#)

[IPSec LAN-to-LAN チェッカー ツール](#)

[ASA のデバッグ](#)

[Cisco IOSルータのデバッグ](#)

[参考資料](#)

概要

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間のCLIを使用して、サイト間(LAN-to-LAN)IKEv1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。

- Cisco IOS
- Cisco Adaptive Security Appliance (ASA)
- 一般的な IPsec の概念

使用するコンポーネント

このドキュメントの情報は、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 9.4(1) が稼働する Cisco 5512-X シリーズ ASA
- Cisco IOS ソフトウェアバージョン 15.4(3)M2 が稼働する Cisco 1941 シリーズ サービス統合型ルータ (ISR)

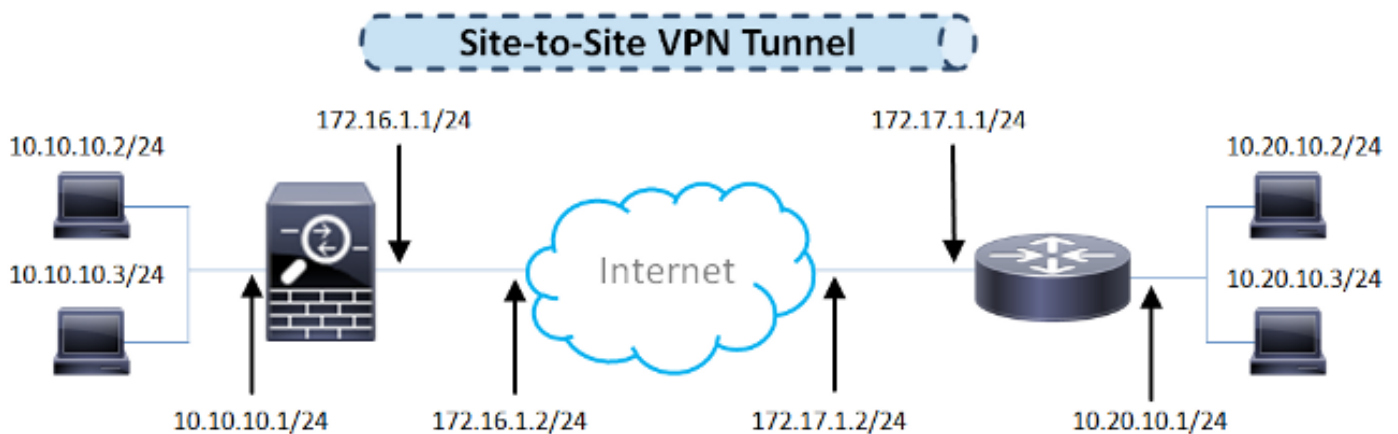
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このセクションでは、ASAおよびCisco IOSルータのCLI設定を完了する方法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は、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 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

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ます。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ます。基本的な接続を確認するには、ping を使用できます。

IKEv1 ポリシーを設定し、外部インターフェイスの IKEv1 を有効にする

IPSec Internet Key Exchange Version 1(IKEv1)接続に対してInternet Security Association and Key Management Protocol(ISAKMP)ポリシーを設定するには、`crypto ikev1 policy` コマンドにより、WLC CLI で明確に示されます。

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

注：IKEv1ポリシーの一致は、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、およびDiffie-Hellmanパラメータ値が含まれている場合に発生します。IKEv1 では、リモートピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが等しくない場合、ASA は短い方のライフタイムを使用します。

注：特定のポリシーパラメータの値を指定しない場合は、デフォルト値が適用されます。

VPN トンネルを終端するインターフェイスでは、IKEv1 をイネーブルにする必要があります。通常は外部（つまり、パブリック）インターフェイスです。IKEv1を有効にするには、`crypto ikev1 enable` グローバルコンフィギュレーションモードで次のコマンドを実行します。

```
crypto ikev1 enable outside
```

トンネルグループ (LAN-to-LAN 接続プロファイル) の設定

LAN-to-LANトンネルの場合、接続プロファイルタイプは ipsec-l2l IKEv1事前共有キーを設定するには、 tunnel-group ipsec-attributes ip inspect コマンドを使用して、一連の:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

対象のVPNトラフィックの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を、保護を必要としないトラフィックと区別します。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 10.10.10.0 255.255.255.0
object-group network remote-network
network-object 10.20.10.0 255.255.255.0
```

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

注：VPNトラフィックのACLは、ネットワークアドレス変換(NAT)後に送信元と宛先のIPアドレスを使用します。

注：VPNトラフィックのACLは、両方のVPNピアでミラーリングする必要があります。

注：保護されたトラフィックに新しいサブネットを追加する必要がある場合は、それぞれのオブジェクトグループにサブネット/ホストを追加し、リモートVPNピアでミラーの変更を完了するだけです。

NAT 適用除外の設定

注：このセクションで説明する設定はオプションです。

通常、VPNトラフィックに対して実行されるNATはありません。そのトラフィックを除外するには、アイデンティティ NAT ルールを作成する必要があります。アイデンティティ NAT ルールは、あるアドレスを同じアドレスに変換するだけです。

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

IKEv1 トランスフォーム セットの設定

IKEv1 トランスフォーム セットとは、ASA のデータ保護方法を定義したセキュリティ プロトコルとアルゴリズムの組み合わせのことです。ピアは、IPsec セキュリティ アソシエーション (SA) のネゴシエーション中に、両方のピアで同一であるトランスフォーム セットまたはプロポーザルを識別する必要があります。次に ASA はこの一致しているトランスフォーム セットまたはプロポーザルを適用して SA を作成し、この SA によって暗号マップに対するアクセス リストのデータ フローが保護されます。

IKEv1 トランスフォーム セットを設定するには、`crypto ipsec ikev1 transform-set` コマンドにより、WLC CLI で明確に示されます。

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

暗号マップの設定とインターフェイスへの適用

暗号マップは IPsec SA でネゴシエートされる IPsec ポリシーを定義し、以下を含みます。

- IPsec 接続が許可および保護するパケットを識別するためのアクセス リスト
- ピア ID
- IPsec トラフィックのローカル アドレス
- IKEv1 トランスフォーム セット

以下が一例です。

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

ここで、インターフェイスに暗号マップを適用できます。

```
crypto map outside_map interface outside
```

ASA の最終設定

ASA の最終的な設定を次に示します。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
```

```
security-level 100
ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
network-object 10.10.10.0 255.255.255.0
object-group network remote-network
network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-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 ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

Cisco IOSルータのCLI設定

インターフェイスの設定

Cisco IOSルータインターフェイスがまだ設定されていない場合は、少なくともLANおよびWANインターフェイスを設定する必要があります。以下が一例です。

```
interface GigabitEthernet0/0
ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
ip address 10.20.10.1 255.255.255.0
no shutdown
```

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ます。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ます。基本的な接続を確認するには、pingを使用できます。

ISAKMP (IKEv1) ポリシーの設定

IKEv1接続のISAKMPポリシーを設定するには、`crypto isakmp policy` コマンドを使用します。以下が一例です。

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
```

注：IPSecに参加する各ピアに複数のIKEポリシーを設定できます。IKE ネゴシエーションが開始されると、リモートピアに指定された最高プライオリティのポリシーから順に、両

方のピアに設定された共通のポリシーの検索が試行されます。

暗号 ISAKMP キーの設定

事前共有認証キーを設定するには、`crypto isakmp key` グローバルコンフィギュレーションモードで次のコマンドを実行します。

```
crypto isakmp key cisco123 address 172.16.1.1
```

対象の VPN トラフィックの ACL 設定

暗号化によって保護する必要があるトラフィックを指定するには、拡張アクセスリストまたは名前付きアクセスリストを使用します。以下が一例です。

```
access-list 110 remark Interesting traffic access-list  
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

注：VPNトラフィックのACLは、NATの後に送信元と宛先のIPアドレスを使用します。

注：VPNトラフィックのACLは、両方のVPNピアでミラーリングする必要があります。

NAT 適用除外の設定

注：このセクションで説明する設定はオプションです。

通常、VPNトラフィックに対して実行されるNATはありません。NATオーバーロードを使用する場合、対象のVPNトラフィックを変換から除外するために、ルートマップを使用する必要があります。ルートマップで使用されるアクセスリストでは、対象のVPNトラフィックを拒否する必要がありますことに注意してください。

```
access-list 111 remark NAT exemption access-list  
access-list 111 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255  
access-list 111 permit ip 10.20.10.0 0.0.0.255 any  
  
route-map nonat permit 10  
match ip address 111  
  
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

トランスフォーム セットの設定

IPSecトランスフォームセット (セキュリティプロトコルとアルゴリズムの許容可能な組み合わせ)

せ)を定義するには、`crypto ipsec transform-set` コマンドを使用します。以下が一例です。

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

暗号マップの設定とインターフェイスへの適用

暗号マップ エントリを作成または変更し、暗号マップ コンフィギュレーション モードを開始するには、`crypto map` グローバル設定コマンドを入力します。暗号マップ エントリを完了するには、最低限定義する必要がある次のようないくつかの項目があります。

- 保護されたトラフィックを転送する IPSec ピアを定義する必要があります。これらは、SA を確立できるピアです。暗号マップ エントリで IPSec ピアを指定するには、`set peer` コマンドが表示されない場合もあります。
- 保護されたトラフィックで使用が受け入れられるトランスフォーム セットを定義する必要があります。暗号マップ エントリで使用できるトランスフォームセットを指定するには、`set transform-set` コマンドが表示されない場合もあります。
- 保護する必要があるトラフィックを定義する必要があります。暗号マップ エントリの拡張アクセスリストを指定するには、`match address` コマンドが表示されない場合もあります。

以下が一例です。

```
crypto map outside_map 10 ipsec-isakmp
set peer 172.16.1.1
set transform-set ESP-AES-SHA
match address 110
```

最後の手順は、前にインターフェイスに対して定義した暗号マップを適用することです。これを適用するには、`crypto map` インターフェイス設定コマンド：

```
interface GigabitEthernet0/0
crypto map outside_map
```

Cisco IOSの最終設定

最終的なCisco IOSルータのCLI設定を次に示します。

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```



```
mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set ESP-AES-SHA
  match address 110
!
interface GigabitEthernet0/0
  ip address 172.17.1.1 255.255.255.0
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  speed auto
  crypto map outside_map
!
interface GigabitEthernet0/1
  ip address 10.20.10.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  duplex auto
  speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
  match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

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、対象のトラフィックがASAまたはCisco IOSルータのいずれかに向けて送信されていることを確認する必要があります。

注：ASAでは、対象のトラフィックに一致するパケットトレーサツールを使用して、IPSecトンネルを開始できます(たとえば、`packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed` 例えは)。

フェーズ 1 の確認

IKEv1フェーズ1がASAでアップしているかどうかを確認するには、`show crypto isakmp sa` コマンドを入力します。予想される出力は、`MM_ACTIVE state`:

```
ciscoasa# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
```

```
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

```
Total IKE SA: 1
```

```
1 IKE Peer: 172.17.1.1
  Type      : L2L                Role      : responder
  Rekey     : no                 State     : MM_ACTIVE
```

```
There are no IKEv2 SAs
ciscoasa#
```

IKEv1フェーズ1がCisco IOSでアップしているかどうかを確認するには、`show crypto isakmp sa` コマンドが表示されない場合もあります。予想される出力は、ACTIVE state:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.1.1   172.17.1.1   QM_IDLE       1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

フェーズ 2 の確認

IKEv1フェーズ2がASAでアップしているかどうかを確認するには、`show crypto ipsec sa` コマンドが表示されない場合もあります。正常な出力は、着信および発信のセキュリティ パラメータ インデックス (SPI) が表示されます。トラフィックがトンネルを通過する場合は、encaps/decapsカウンタが増加していることを確認する必要があります。

注：各ACLエントリに対して、個別のインバウンド/アウトバウンドSAが作成され、結果として長くなる可能性があります show crypto ipsec sa コマンド出力 (クリプトACL内のACEエントリ数に依存)。

以下が一例です。

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
  Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
  local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  current_peer: 172.17.1.1

#pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
#pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1005, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
```

```
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8A9FE619
current inbound spi : D8639BD0
```

inbound esp sas:

```
spi: 0xD8639BD0 (3630406608)
transform: esp-aes esp-sha-hmac no compression
in use settings =(L2L, Tunnel, IKEv1, )
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914900/3519)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF
```

outbound esp sas:

```
spi: 0x8A9FE619 (2325734937)
transform: esp-aes esp-sha-hmac no compression
in use settings =(L2L, Tunnel, IKEv1, )
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914901/3519)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ciscoasa#

Cisco IOSでIKEv1フェーズ2がアップしているかどうかを確認するには、`show crypto ipsec sa` コマンドが表示されない場合もあります。正常な出力は、着信および発信のSPIが表示されます。トラフィックがトンネルを通過する場合は、`encaps/decaps`カウンタが増加していることを確認する必要があります。

以下が一例です。

```
Router#show crypto ipsec sa peer 172.16.1.1
```

```
interface: GigabitEthernet0/0
Crypto map tag: outside_map, local addr 172.17.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
#pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 26, #recv errors 0

local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xD8639BD0(3630406608)
```

PFS (Y/N): N, DH group: none

inbound esp sas:

```
spi: 0x8A9FE619(2325734937)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4449870/3455)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xD8639BD0(3630406608)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4449868/3455)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Router#

フェーズ 1 および 2 の確認

このセクションでは、フェーズ1と2の両方の詳細を確認するためにASAまたはCisco IOSで使用できるコマンドについて説明します。

次を入力します。 show vpn-sessiondb 確認のためのASAでのコマンド :

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1
```

Session Type: LAN-to-LAN Detailed

```
Connection   : 172.17.1.1
Index        : 2                               IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128 IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx     : 100500                           Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1
```

IKEv1:

```
Tunnel ID    : 2.1
UDP Src Port : 500                               UDP Dst Port : 500
```

```
IKE Neg Mode : Main                Auth Mode      : preSharedKeys
Encryption   : AES128              Hashing        : SHA1
Rekey Int (T): 86400 Seconds       Rekey Left(T): 86093 Seconds
D/H Group    : 2
Filter Name  :
```

IPsec:

```
Tunnel ID    : 2.2
Local Addr   : 10.10.10.0/255.255.255.0/0/0
Remote Addr  : 10.20.10.0/255.255.255.0/0/0
Encryption   : AES128              Hashing        : SHA1
Encapsulation: Tunnel
Rekey Int (T): 3600 Seconds        Rekey Left(T): 3293 Seconds
Rekey Int (D): 4608000 K-Bytes     Rekey Left(D): 4607901 K-Bytes
Idle Time Out: 30 Minutes          Idle TO Left  : 26 Minutes
Bytes Tx     : 100500              Bytes Rx      : 101400
Pkts Tx     : 1005                Pkts Rx      : 1014
```

NAC:

```
Reval Int (T): 0 Seconds           Reval Left(T): 0 Seconds
SQ Int (T)   : 0 Seconds           EoU Age(T)    : 309 Seconds
Hold Left (T): 0 Seconds          Posture Token:
Redirect URL :
```

ciscoasa#

次を入力します。 show crypto session 確認のためのCisco IOSコマンドは次のとおりです。

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
  Phase1_id: 172.16.1.1
  Desc: (none)
  IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
    Capabilities:(none) connid:1005 lifetime:23:56:23
  IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
    Active SAs: 2, origin: crypto map
    Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
    Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383
```

Router#

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

注: 使用する前に、シスコのドキュメント『[debugコマンドの重要な情報](#)』および『[IP Securityのトラブルシューティング - debugコマンドの理解と使用](#)』を参照してください

debug コマンドを発行します。

IPSec LAN-to-LAN チェッカー ツール

ASAとCisco IOSの間のIPSec LAN-to-LAN設定が有効かどうかを自動的に確認するには、[IPSec LAN-to-LANhecker](#)ツールを使用できます。このツールは、次のものを受け入れるように設計されています。 show tech または show running-config コマンドを発行します。設定を調べ、暗号マップページのLAN-to-LAN IPSecトンネルが設定されているかどうかを検出しようとします。これを設定すると、設定のマルチポイント チェックを行い、ネゴシエートされたトンネルの設定エラーや設定をハイライトします。

ASA のデバッグ

ASAファイアウォールでIPSec IKEv1トンネルネゴシエーションをトラブルシューティングするには、次のコマンドを使用できます debug コマンド：

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

注：ASA上のVPNトンネルの数が著しい場合は、 debug crypto condition peer A.B.C.D デバッグ出力に指定したピアだけが含まれるように制限するには、デバッグを有効にする前にコマンドを使用する必要があります。

Cisco IOSルータのデバッグ

Cisco IOSルータでIPSec IKEv1トンネルネゴシエーションをトラブルシューティングするには、次のdebugコマンドを使用できます。

```
debug crypto ipsec
debug crypto isakmp
```

注：Cisco IOS上のVPNトンネルの数が著しい場合は、 debug crypto condition peer ipv4 A.B.C.D デバッグ出力に指定したピアだけが含まれるように制限するには、デバッグを有効にする前に使用する必要があります。

ヒント：サイト間VPNのトラブルシューティング方法についての詳細は、シスコのドキュメント『[一般的なL2LおよびリモートアクセスIPSec VPNのトラブルシューティング方法について](#)』を参照してください。

参考資料

- [デバッグ コマンドに関する重要な情報](#)
- [IIP Security のトラブルシューティング：debug コマンドの説明と使用](#)
- [一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について](#)

- [IPSec LAN-to-LAN チェッカー](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

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。