

ASA で ASDM または CLI を使用した IKEv1 IPsec サイトツーサイト 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](#)

[ASDM VPNウィザードを使用した設定](#)

[CLIによる設定](#)

[ASAバージョン8.4以降のサイトBの設定](#)

[ASAバージョン8.2以前のサイトAの設定](#)

[グループ ポリシー](#)

[確認](#)

[ASDM](#)

[CLI](#)

[フェーズ 1](#)

[フェーズ 2](#)

[トラブルシューティング](#)

[ASA バージョン 8.4 以降](#)

[ASAバージョン8.3以前](#)

概要

このドキュメントでは、ソフトウェアバージョン9.2.xが稼働するCisco 5515-Xシリーズ適応型セキュリティアプライアンス(ASA)とソフトウェアバージョン8.2.xが稼働するCisco 5510シリーズASAの間に、インターネットキーエクステンションバージョン1(IKEv1)IPSecサイト間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。

- エンドツーエンドのIP接続を確立する必要がある
- 次のプロトコルを許可する必要があります。
 - IPSecコントロールプレーン用のユーザデータグラムプロトコル(UDP)500および4500IPsecデータプレーン用のEncapsulating Security Payload(ESP)IPプロトコル50

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8.2が稼働するCisco 5510シリーズASA
- ソフトウェアバージョン9.2が稼働するCisco 5515-X ASA

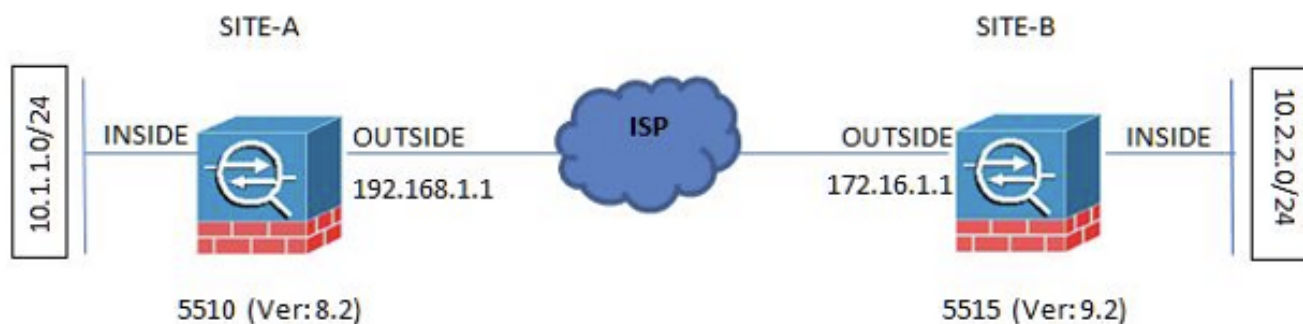
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このセクションでは、Adaptive Security Device Manager(ASDM)VPNウィザードまたはCLIを使用してサイト間VPNトンネルを設定する方法について説明します。

ネットワーク図

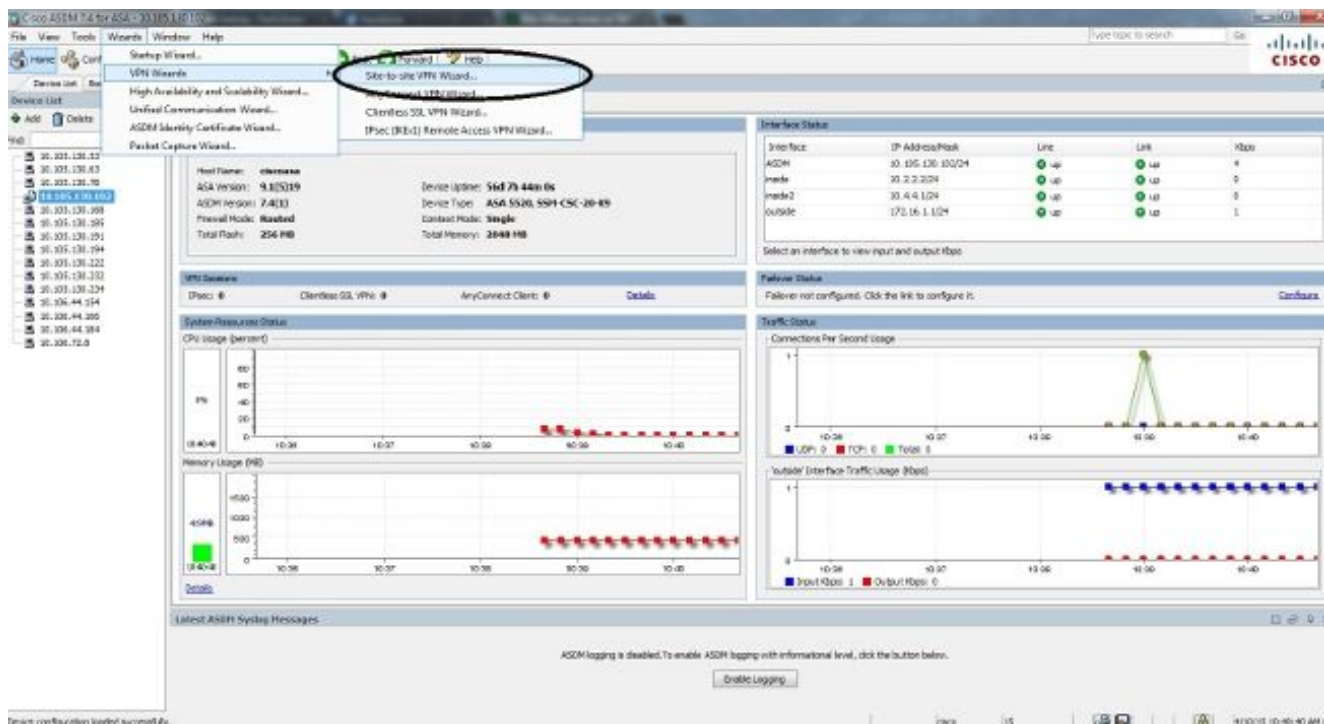
このドキュメント全体の例では、次のトポロジを使用します。



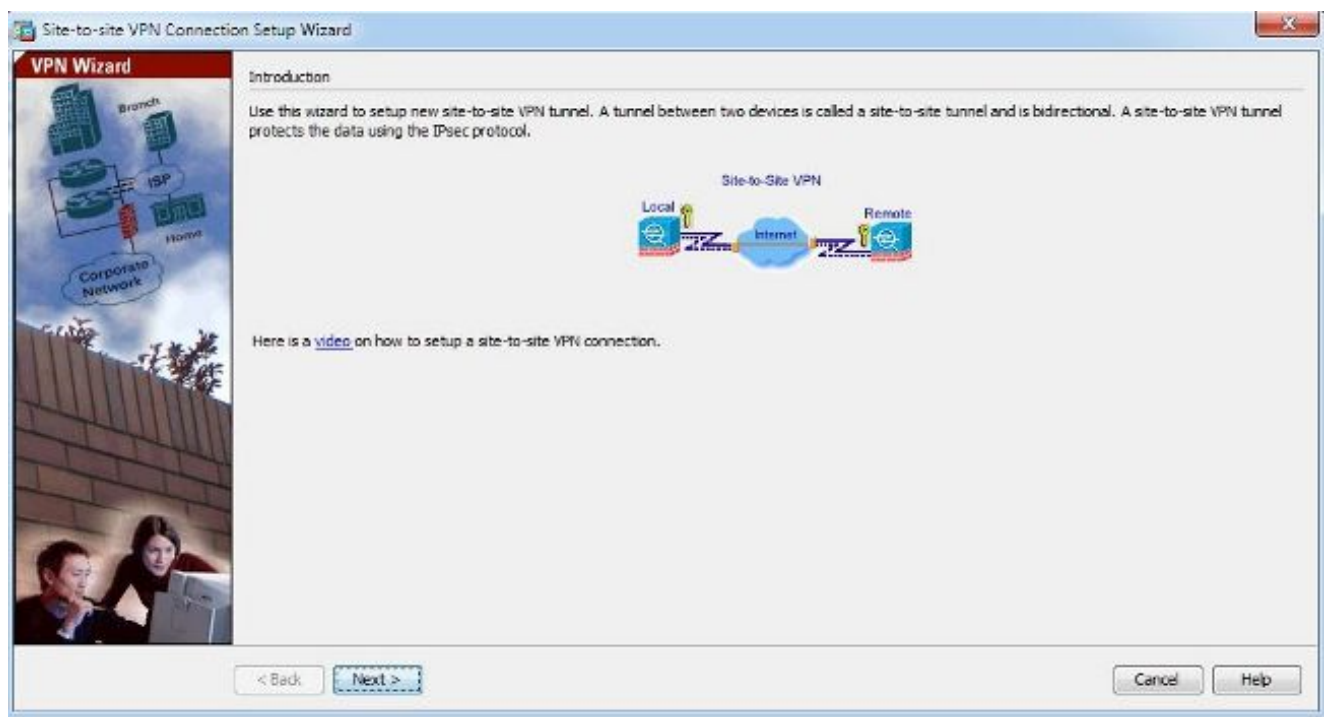
ASDM VPNウィザードを使用した設定

ASDMウィザードを使用してサイト間VPNトンネルを設定するには、次の手順を実行します。

1. ASDMを開き、 Wizards > VPN Wizards > Site-to-site VPN Wizard.

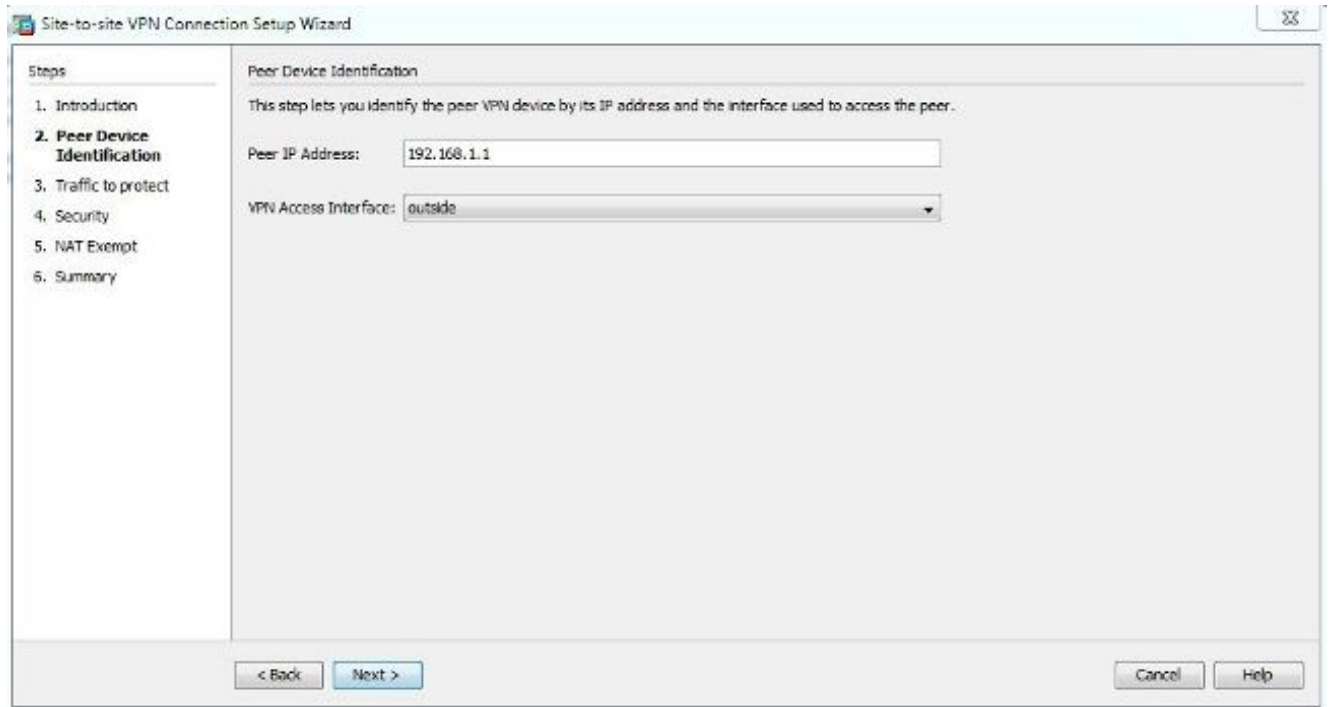


2. クリック Next ウィザードのホームページにアクセスします。

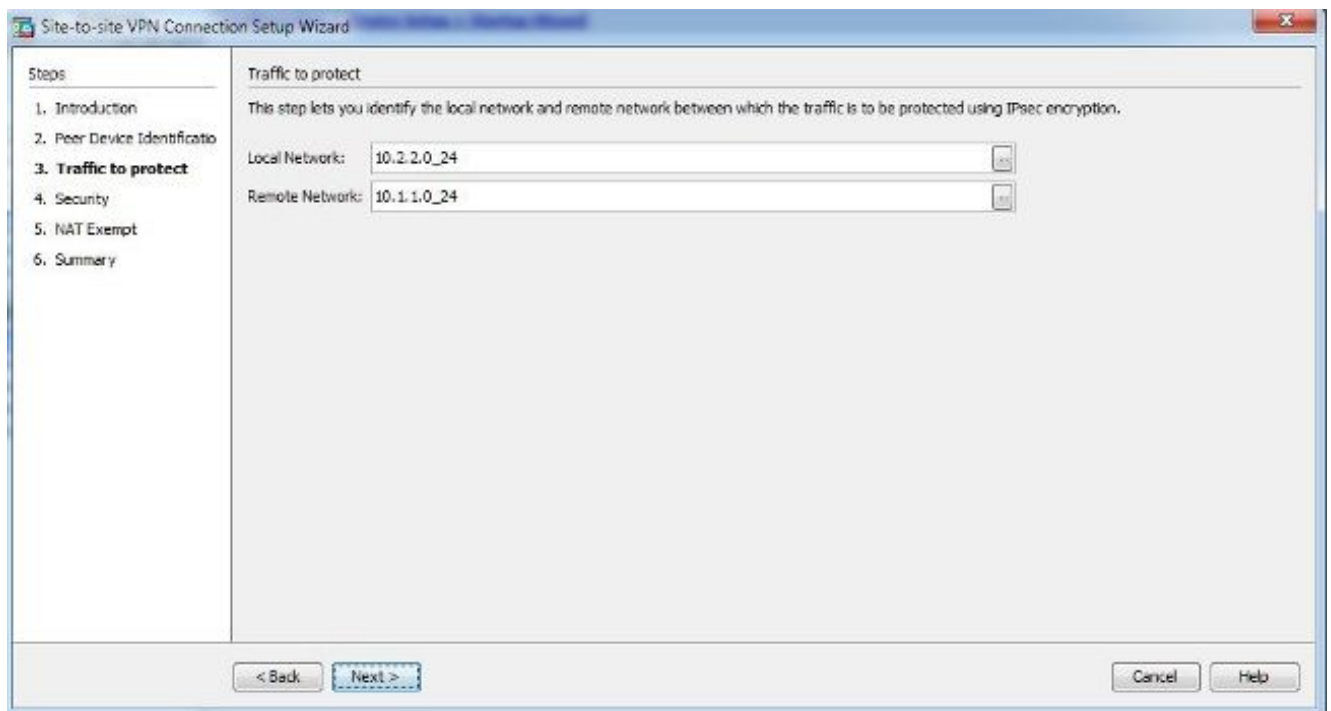


注：最新のASDMバージョンには、この設定を説明するビデオへのリンクがあります。

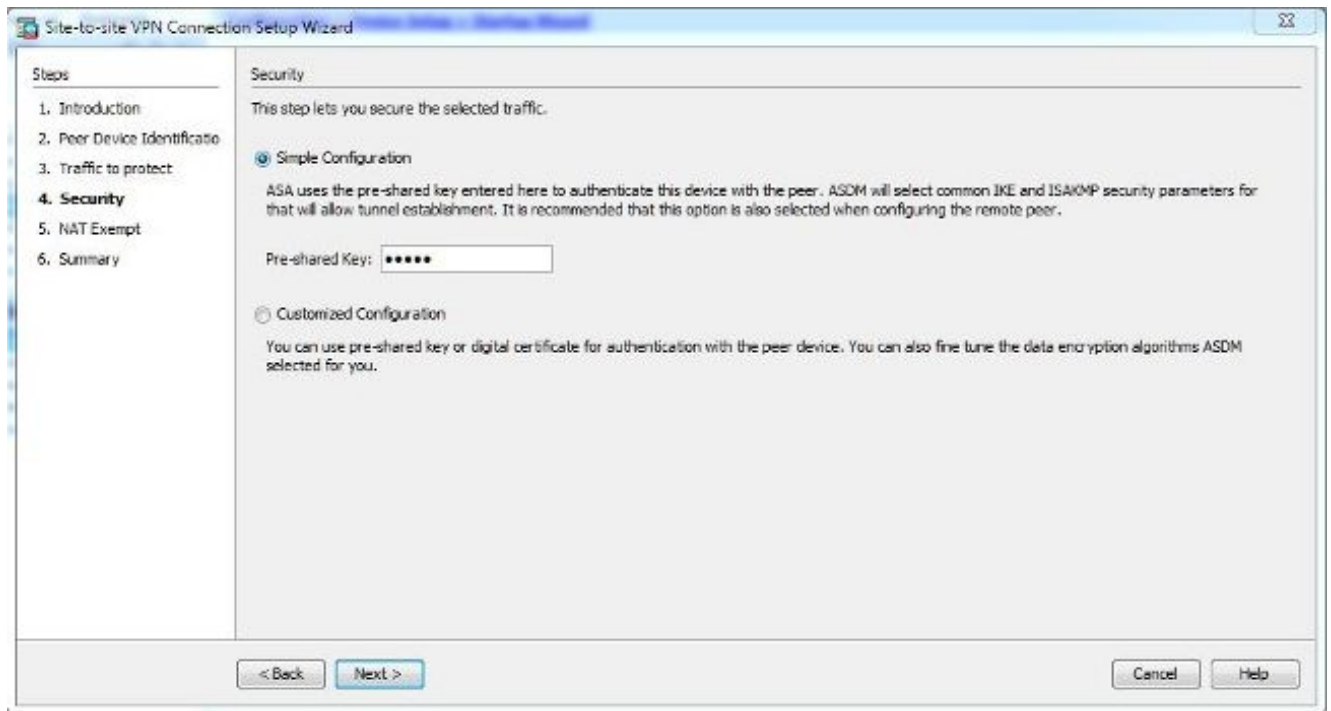
3. ピアのIPアドレスを設定します。この例では、ピアのIPアドレスはサイトBで192.168.1.1に設定されています。サイトAでピアのIPアドレスを設定する場合は、172.16.1.1に変更する必要があります。リモートエンドに到達できるインターフェイスも指定されます。クリック Next 完了したら、



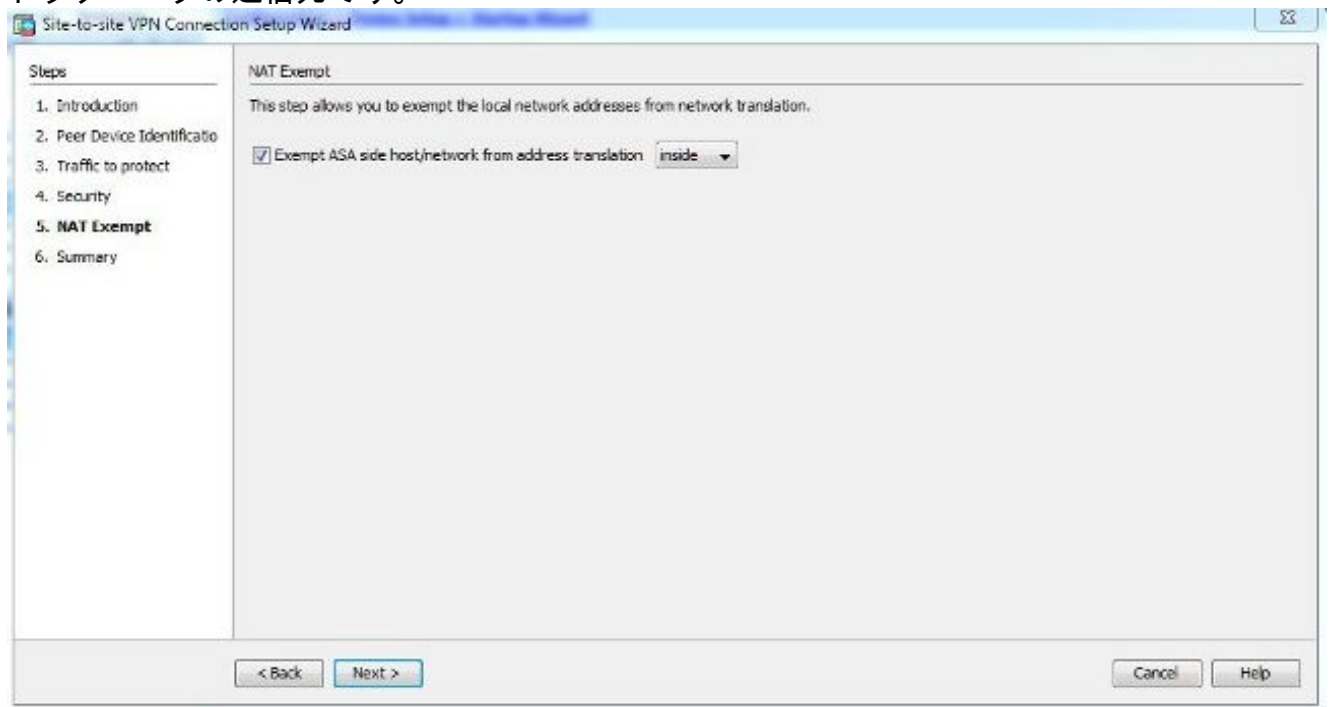
4. ローカルネットワークとリモートネットワーク（トラフィックの送信元と宛先）を設定します。次の図に、サイトBの設定を示します（逆の設定はサイトAに適用されます）。



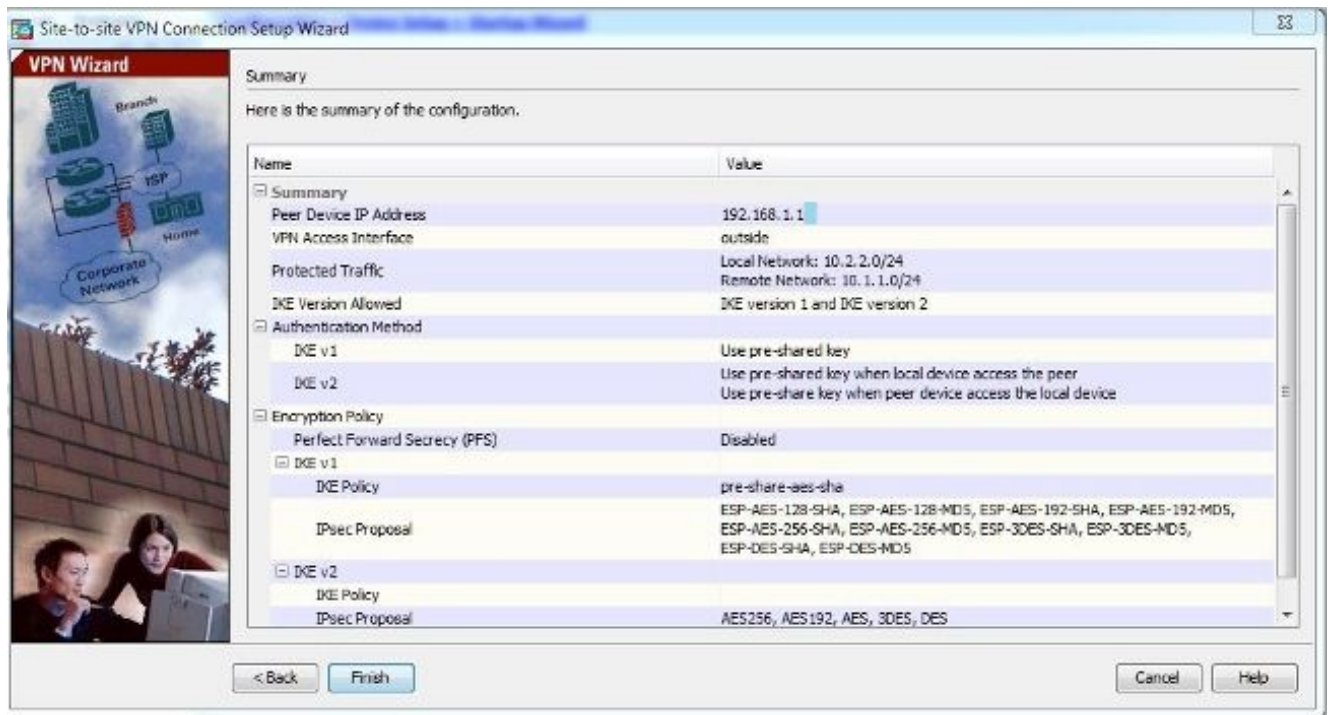
5. [Security]ページで、事前共有キーを設定します（両端で一致する必要があります）。クリック Next 完了したら、



6. ASA上のトラフィックの送信元インターフェイスを設定します。ASDMはASAバージョンに基づいてネットワークアドレス変換(NAT)ルールを自動的に作成し、最後のステップで残りの設定とともに適用します。注：このドキュメントで使用されている例では、「inside」がトラフィックの送信元です。



7. このウィザードでは、ASAにプッシュされる設定の概要が表示されます。設定を確認して確認し、 Finish.



CLIによる設定

このセクションでは、CLIを使用してIKEv1 IPsecサイト間トンネルを設定する方法について説明します。

ASAバージョン8.4以降のサイトBの設定

ASAバージョン8.4以降では、IKEv1とインターネットキーエクスチェンジバージョン2(IKEv2)の両方のサポートが導入されました。

ヒント：この2つのバージョンの違いについての詳細は、『ASA 8.4コードでのIKEv1からIKEv2 L2Lトンネル設定への迅速な移行Cisco』ドキュメントの「[IKEv2に移行する理由](#)」セクションを参照してください。

ヒント:ASAを使用したIKEv2の設定例については、シスコのドキュメント『[ASAとルータ間のサイト間IKEv2トンネルの設定例](#)』を参照してください。

フェーズ1(IKEv1)

フェーズ1の設定では、次の手順を実行します。

1. CLIに次のコマンドを入力して、外部インターフェイスでIKEv1を有効にします。

```
crypto ikev1 enable outside
```

2. ハッシュ、認証、Diffie-Hellmanグループ、ライフタイム、および暗号化に使用するアルゴリズム/方式を定義するIKEv1ポリシーを作成します。

```
crypto ikev1 policy 1
```

```
!The 1 in the above command refers to the Policy suite priority
(1 highest, 65535 lowest)
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. IPsec属性の下にトンネルグループを作成し、ピアIPアドレスとトンネル事前共有キーを設定します。

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

フェーズ2(IPsec)

フェーズ2の設定では、次の手順を実行します。

1. 暗号化およびトンネリングするトラフィックを定義するアクセスリストを作成します。この例では、対象のトラフィックは、10.2.2.0サブネットから10.1.1.0に送信されたトンネルからのトラフィックです。サイト間に複数のサブネットが関係する場合は、複数のエントリを含めることができます。

バージョン8.4以降では、ネットワーク、サブネット、ホストIPアドレス、または複数のオブジェクトのコンテナとして機能するオブジェクトまたはオブジェクトグループを作成できます。ローカルサブネットとリモートサブネットを持つ2つのオブジェクトを作成し、それらを暗号アクセスコントロールリスト(ACL)とNAT文の両方に使用します。

```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

2. キーワードを含むトランスフォームセット(TS)を設定します。IKEv1.リモートエンドでも同じTSを作成する必要があります。

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

3. 次のコンポーネントを含むクリプトマップを設定します。
ピアIPアドレス対象のトラフィックを含む定義済みのアクセスリストTSオプションのPerfect Forward Secrecy(PFS)設定。データを保護するために使用されるDiffie-Hellmanキーの新しいペアを作成します (フェーズ2が起動する前に、両側でPFSが有効になっている必要があります)。

4. 外部インターフェイスにクリプトマップを適用します。

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
```



```
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT免除

VPNトラフィックが他のNATルールに従っていないことを確認します。使用されるNATルールを次に示します。

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

注：複数のサブネットを使用する場合は、すべての送信元および宛先サブネットを含むオブジェクトグループを作成し、NATルールで使用する必要があります。

```
object-group network 10.x.x.x_SOURCE
network-object 10.4.4.0 255.255.255.0
network-object 10.2.2.0 255.255.255.0
```

```
object network 10.x.x.x_DESTINATION
network-object 10.3.3.0 255.255.255.0
network-object 10.1.1.0 255.255.255.0
```

```
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination
static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

完全な設定例

サイトBの完全な設定を次に示します。

crypto ikev1 enable outside

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

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
!Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```



```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

ASAバージョン8.2以前のサイトAの設定

このセクションでは、ASAバージョン8.2以前のサイトAを設定する方法について説明します。

フェーズ1(ISAKMP)

フェーズ1の設定では、次の手順を実行します。

1. OutsideインターフェイスでInternet Security Association and Key Management Protocol(ISAKMP)を有効にするには、CLIに次のコマンドを入力します。

```
crypto isakmp enable outside
```

注：複数のバージョンのIKE (IKEv1とIKEv2) はサポートされなくなったため、ISAKMPを使用してフェーズ1を参照します。

2. フェーズ1を構築するために使用するアルゴリズム/メソッドを定義するISAKMPポリシーを作成します。

注：この設定例では、キーワード IKEv1 バージョン9.x以降は、 ISAKMP.

```
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. 事前共有キーを使用して、ピアIPアドレス (外部IPアドレス5515) のトンネルグループを作成します。

```
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
```

フェーズ2(IPsec)

フェーズ2の設定では、次の手順を実行します。

1. バージョン9.xの設定と同様に、対象のトラフィックを定義するために拡張アクセスリストを作成する必要があります。

```
access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
```

2. 使用可能なすべての暗号化およびハッシュアルゴリズムを含むTSを定義します (提供され

た問題には疑問符が付きます)。反対側で設定されているものと同一であることを確認します。

```
crypto ipsec transform-set myset esp-aes esp-sha-hmac
```

3. 次のコンポーネントを含むクリプトマップを設定します。

ピアIPアドレス対象のトラフィックを含む定義済みのアクセスリストTSオプションのPFS設定。データを保護するために使用されるDiffie-Hellmanキーの新しいペアを作成します(フェーズ2が起動するように、両側でPFSを有効にする必要があります)。

4. 外部インターフェイスにクリプトマップを適用します。

```
crypto map outside_map 20 set peer 172.16.1.1
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT免除

NATチェックから除外するトラフィックを定義するアクセスリストを作成します。このバージョンでは、対象のトラフィックに対して定義したアクセスリストに似ています。

```
access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
```

複数のサブネットを使用する場合は、同じアクセスリストに別の行を追加します。

```
access-list nonat line 1 extended permit ip 10.3.3.0 255.255.255.0
10.4.4.0 255.255.255.0
```

次に示すように、NATではアクセスリストが使用されます。

```
nat (inside) 0 access-list nonat
```

注：ここでの「内部」は、アクセスリストに一致するトラフィックをASAが受信する内部インターフェイスの名前を示します。

完全な設定例

サイトAの完全な設定を次に示します。

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

```

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat

```

グループ ポリシー

グループポリシーは、トンネルに適用される特定の設定を定義するために使用されます。これらのポリシーは、トンネルグループと組み合わせて使用されます。

グループポリシーは、内部 (ASAで定義されている属性から属性が取得される) と、外部 (外部サーバから属性が照会される) として定義できます。グループポリシーを定義するために使用するコマンドを次に示します。

```
group-policy SITE_A internal
```

注：グループポリシーでは複数の属性を定義できます。考えられるすべての属性のリストについては、『Cisco ASA 5500シリーズバージョン5.2用に選択したASDM VPN設定手順』の「[グループポリシーの設定](#)」セクションを参照してください。

グループポリシーのオプション属性

「 vpn-tunnel-protocol 属性は、これらの設定を適用する必要があるトンネルタイプを決定します。この例では、IPsecが使用されます。

```

vpn-tunnel-protocol ?
group-policy mode commands/options:
IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
svc SSL VPN Client
webvpn WebVPN

vpn-tunnel-protocol ipsec - Versions 8.2 and prior
vpn-tunnel-protocol ikev1 - Version 8.4 and later

```

トンネルを設定して、アイドル状態 (トラフィックなし) を維持し、ダウンを防ぐことができます。このオプションを設定するには、 vpn-idle-timeout 属性値は分を使用する必要があります。または、値をに設定できます。 noneこれは、トンネルがダウンしないことを意味します。

以下が一例です。

```
group-policy SITE_A attributes
vpn-idle-timeout ?
group-policy mode commands/options:
<1-35791394> Number of minutes
none IPsec VPN: Disable timeout and allow an unlimited idle period;
```

「 default-group-policy コマンドをトンネルグループのgeneral attributesの下に設定すると、確立されたトンネルの特定のポリシー設定をプッシュするために使用されるグループポリシーが定義されます。グループポリシーで定義しなかったオプションのデフォルト設定は、グローバルなデフォルトのグループポリシーから取得されます。

```
tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE_A
```

確認

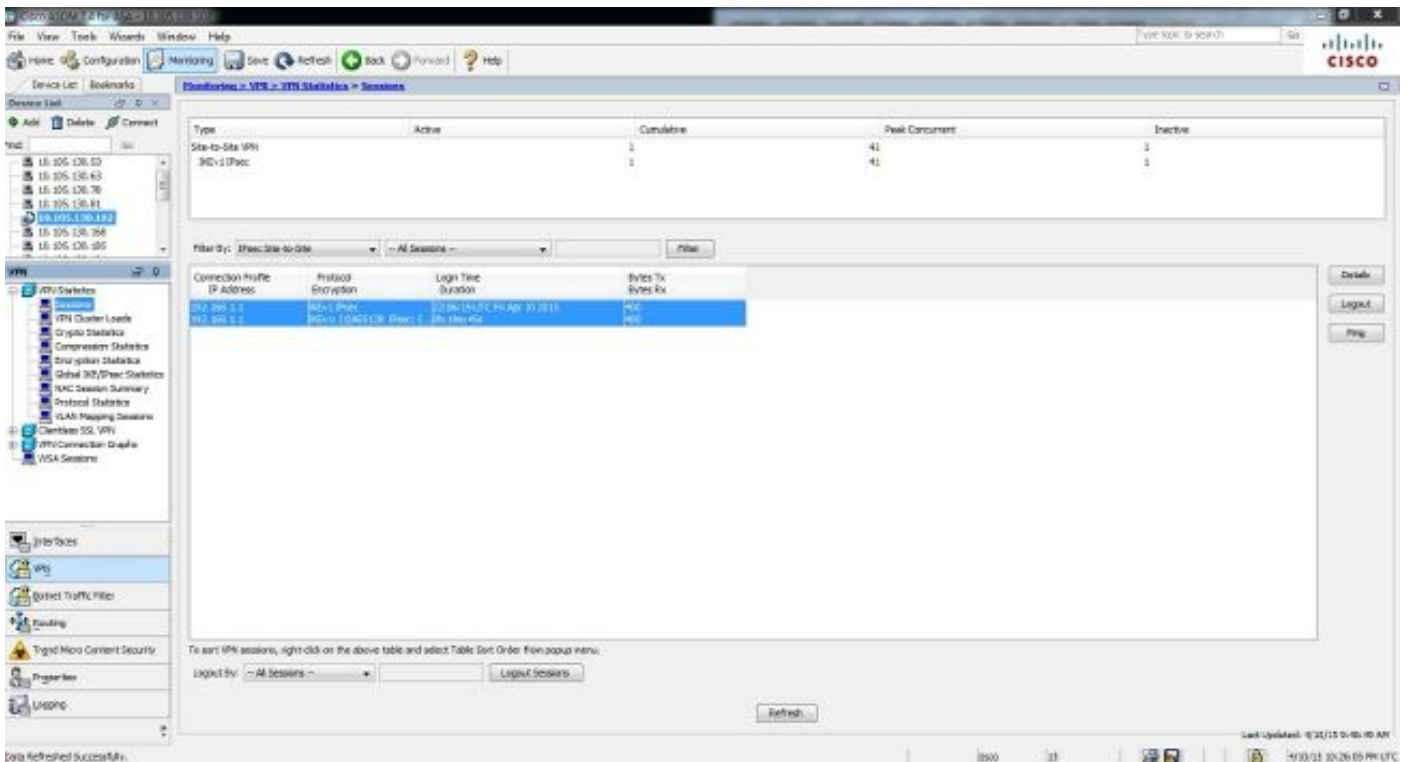
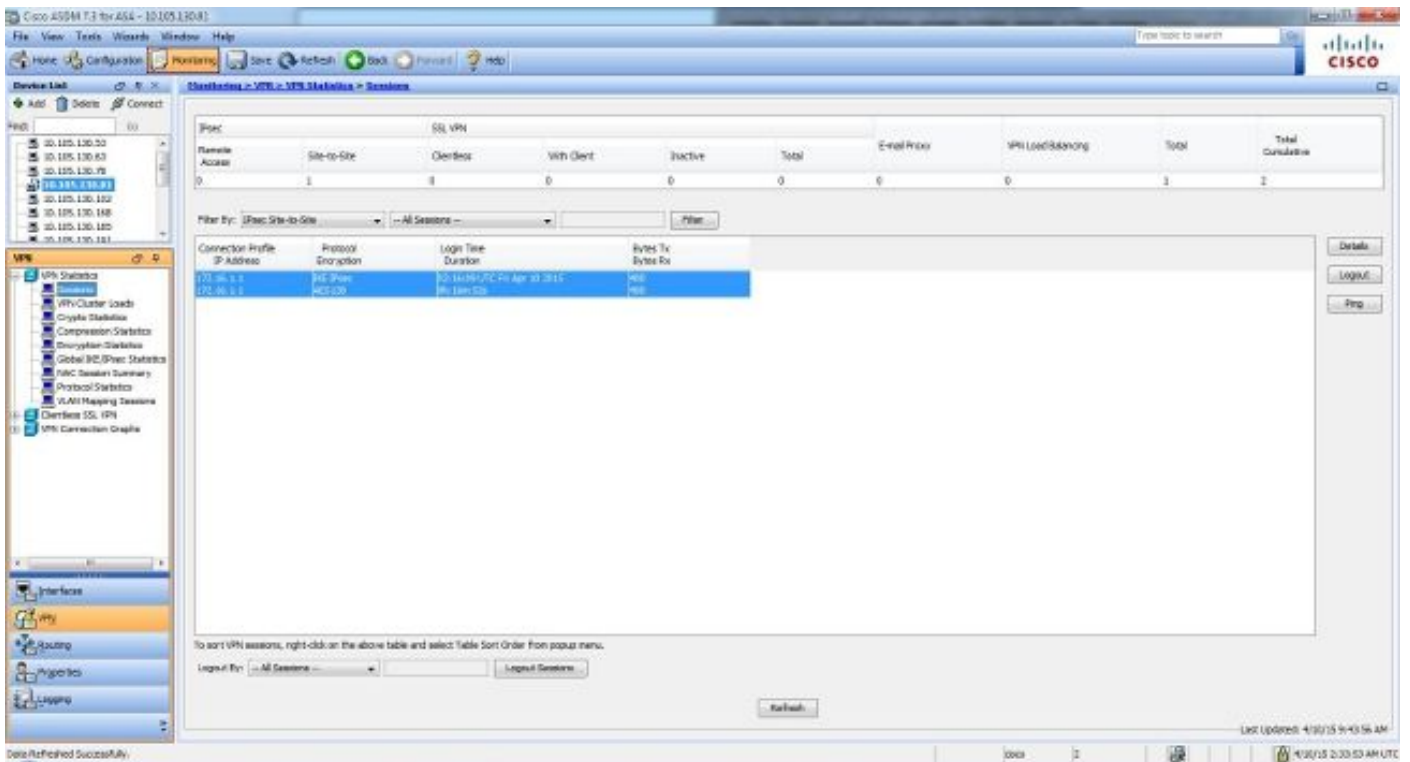
このセクションに記載されている情報を使用して、設定が適切に機能するか確認します。

ASDM

ASDMからトンネルステータスを表示するには、 [Monitoring > VPN](#). 次の情報が表示されます。

- ピアIPアドレス
- トンネルを構築するために使用されるプロトコル
- 使用される暗号化アルゴリズム
- トンネルがアップした時刻とアップ時間
- 受信および転送されたパケットの数

ヒント： クリック [Refresh](#) 最新の値を表示するには、データはリアルタイムで更新されません。



CLI

このセクションでは、CLIを使用して設定を確認する方法について説明します。

フェーズ 1

サイトB(5515)側でフェーズ1の設定を確認するには、CLIに次のコマンドを入力します。

```
show crypto ikev1 sa
```

```
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: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

サイトA(5510)側でフェーズ1の設定を確認するには、CLIに次のコマンドを入力します。

```
show crypto isakmp sa
```

```
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: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

フェーズ2

「 show crypto ipsec sa コマンドは、ピア間に構築されたIPsec SAを表示します。ネットワーク10.1.1.0と10.2.2.0の間を流れるトラフィック用に、IPアドレス192.168.1.1と172.16.1.1の間に暗号化トンネルが構築されます。着信および発信トラフィック用に構築された2つのESP SAを確認できます。AH SAがないため、認証ヘッダー(AH)は使用されません。

サイトB(5515)側でフェーズ2の設定を確認するには、CLIに次のコマンドを入力します。

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
  local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
```

```
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
    transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

サイトA(5510)側でフェーズ2の設定を確認するには、次のコマンドをCLIに入力します。

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
    local ident (addr/mask/prot/port): (10.1.1.0/255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
    transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
    transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

トラブルシューティング

設定の問題のトラブルシューティングを行うには、この項で説明する情報を使用します。

ASA バージョン 8.4 以降

次のdebugコマンドを入力して、トンネル障害の場所を特定します。

- debug crypto ikev1 127 (フェーズ 1)
- debug crypto ipsec 127 (フェーズ 2)

デバッグ出力の完全な例を次に示します。

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
```

(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco
VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
!
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, **Connection landed on tunnel_group
192.168.1.1**
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating
keys for Initiator...
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing
ID payload
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing
hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive
payload: proposal=32767/32767 sec.
!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing dpd vid payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
**Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT
Detection Status: Remote end is NOT behind a NAT device This end is NOT behind
a NAT device**
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing
ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR ID received 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received

DPD VID

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group
192.168.1.1

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley
begin quick mode

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE
Initiator starting QM: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1
rekey timer: 73440 seconds.

IPSEC: New embryonic SA created @ 0x75298588,

SCB: 0x75C34F18,

Direction: inbound

SPI : 0x03FC9DB7

Session ID: 0x00004000

VPIF num : 0x00000002

Tunnel type: 121

Protocol : esp

Lifetime : 240 seconds

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

IKE got SPI from key engine: SPI = 0x03fc9db7

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

oakley constructing quick mode

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

constructing blank hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

constructing IPSec SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

constructing IPSec nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

constructing proxy ID

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

Transmitting Proxy Id:

Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0

Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,

IKE Initiator sending Initial Contact

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1,

IP = 192.168.1.1, constructing qm hash payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1,

IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)

with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +

NOTIFY (11) + NONE (0) total length : 200

Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500

from 192.168.1.1:500

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21)

with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)

total length : 172

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,

ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,

ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
loading all IPSEC SAs
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
NP encrypt rule look up for crypto map outside_map 20 matching ACL
100: returned cs_id=6ef246d0; encrypt_rule=752972d0;
tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x6f0e03f0,
SCB: 0x75B6DD00,
Direction: outbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: 121
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C
IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: New outbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50

Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7, Outbound SPI = 0x1ba0c55c
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing final quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 3rd QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 76
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD msg for SA: SPI = 0x1ba0c55c
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F614
SCB : 0x0B4707C7
Channel: 0x6ef0a5c0
IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x00011f6c
IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00011F6C
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore

```
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

ASAバージョン8.3以前

次のdebugコマンドを入力して、トンネル障害の場所を特定します。

- debug crypto isakmp 127 (フェーズ 1)

- debug crypto ipsec 127 (フェーズ 2)

デバッグ出力の完全な例を次に示します。

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: True
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 1
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver
02 payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA_KE payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor
ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
```


Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys
for Responder...
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR
ID received 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing
hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection
Status: Remote end is NOT behind a NAT device This end is NOT behind
a NAT device**
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing ID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
Computing hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing dpd vid payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1
rekey timer: 82080 seconds.
Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id =
4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NOTIFY (11) + NONE (0) total length : 200
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP
Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,

processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP
Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
notify payload
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa
not found by addr
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, checking map = outside_map, seq = 20...
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, map outside_map, seq = 20 is a successful match**
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer
configured for crypto map: outside_map**
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
IPSec SA payload
**Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA
Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20**
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0xAB5C63A8,
SCB: 0xABD54E98,
Direction: inbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI
from key engine: SPI = 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley
constucting quick mode
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
blank hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
proxy ID
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting
Proxy Id:
Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
qm hash payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder
sending 2nd QM pkt: msg id = 4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all
IPSEC SAs
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt
rule look up for crypto map outside_map 20 matching ACL 100: returned
cs_id=ab9302f0; rule=ab9309b0

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0xAB570B58,
SCB: 0xABD55378,
Direction: outbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: 121
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: New outbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c, Outbound SPI = 0x03fc9db7

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a KEY_ADD msg for SA: SPI = 0x03fc9db7

IPSEC: Completed host IBSA update, SPI 0x1BA0C55C

IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C

Flags: 0x00000006

SA : 0xAB5C63A8

SPI : 0x1BA0C55C

MTU : 0 bytes

VCID : 0x00000000

Peer : 0x0000F99C

SCB : 0x0150B419

Channel: 0xA7A98400

IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C

VPN handle: 0x0001169C

IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7

Flags: 0x00000005

SA : 0xAB570B58

SPI : 0x03FC9DB7

MTU : 1500 bytes

VCID : 0x00000000

Peer : 0x0001169C

SCB : 0x01512E71

Channel: 0xA7A98400

IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7

VPN handle: 0x0000F99C

IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7

Rule ID: 0xABD557B0

IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7

Rule ID: 0xABD55848

IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C

Src addr: 10.2.2.0

Src mask: 255.255.255.0

Dst addr: 10.1.1.0

Dst mask: 255.255.255.0

Src ports

Upper: 0

Lower: 0

Op : ignore

Dst ports

Upper: 0

Lower: 0

Op : ignore

Protocol: 0

Use protocol: false

SPI: 0x00000000

Use SPI: false

IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C

Rule ID: 0xAB8D98A8

IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C

Src addr: 172.16.1.1

Src mask: 255.255.255.255

Dst addr: 192.168.1.1

Dst mask: 255.255.255.255

Src ports

Upper: 0

Lower: 0

Op : ignore

Dst ports

Upper: 0

Lower: 0

Op : ignore

Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C
Rule ID: 0xABD55CB0
IPSEC: New inbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C
Rule ID: 0xABD55D48
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received
KEY_UPDATE, spi 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey
timer: 27360 seconds.
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED
(msgid=4c073b21)**

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。