

# ASA 間、動的静的間 IKEv1/IPsec の設定例

## 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 の設定](#)

[中央 ASA \(スタティックピア\)](#)

[リモート ASA \(ダイナミックピア\)](#)

[CLI での設定](#)

[中央 ASA \(スタティックピア\) の設定](#)

[リモート ASA \(ダイナミックピア\)](#)

[確認](#)

[中央 ASA](#)

[リモート ASA](#)

[トラブルシューティング](#)

[リモート ASA \(イニシエータ\)](#)

[中央 ASA \(レスポンド\)](#)

[関連情報](#)

## 概要

このドキュメントでは、適応型セキュリティ アプライアンス (ASA) が任意のダイナミックピア (このケースでは ASA) からのダイナミック IPsec サイト間 VPN 接続を受け入れるようにする方法について説明します。このドキュメントのネットワーク図に示されているように、IPsec トンネルは、トンネルがリモート ASA 側から開始される場合にのみ確立されます。中央 ASA は、ダイナミック IPsec 設定のために VPN トンネルを開始できません。リモート ASA の IP アドレスは不明です。

ワイルドカード IP アドレス (0.0.0.0/0) とワイルドカード事前共有キーからの接続を動的に受け入れるように中央 ASA を設定します。その後、リモート ASA は、暗号アクセスリストでの指定に従ってローカルサブネットから中央 ASA サブネットへのトラフィックを暗号化するように設定されます。どちら側でも、IPsec トラフィックのネットワークアドレス変換 (NAT) をバイパスするために NAT 除外が実行されます。

## 前提条件

## 要件

このドキュメントに特有の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、Cisco ASA ( 5510 および 5520 ) ファイアウォール ソフトウェア リリース 9.x 以降に基づくものです。

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、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

注：このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \( 登録ユーザ専用 \)](#) を使用してください。

## ネットワーク図

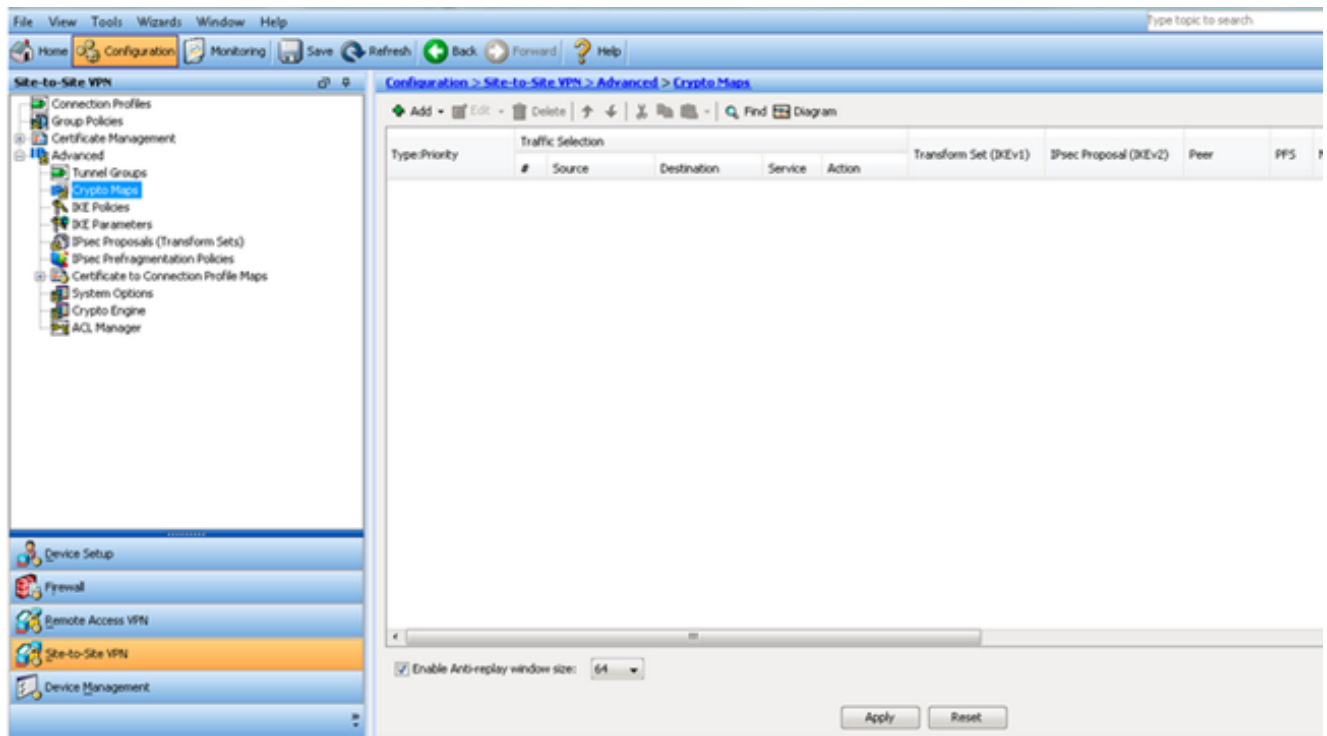


## ASDM の設定

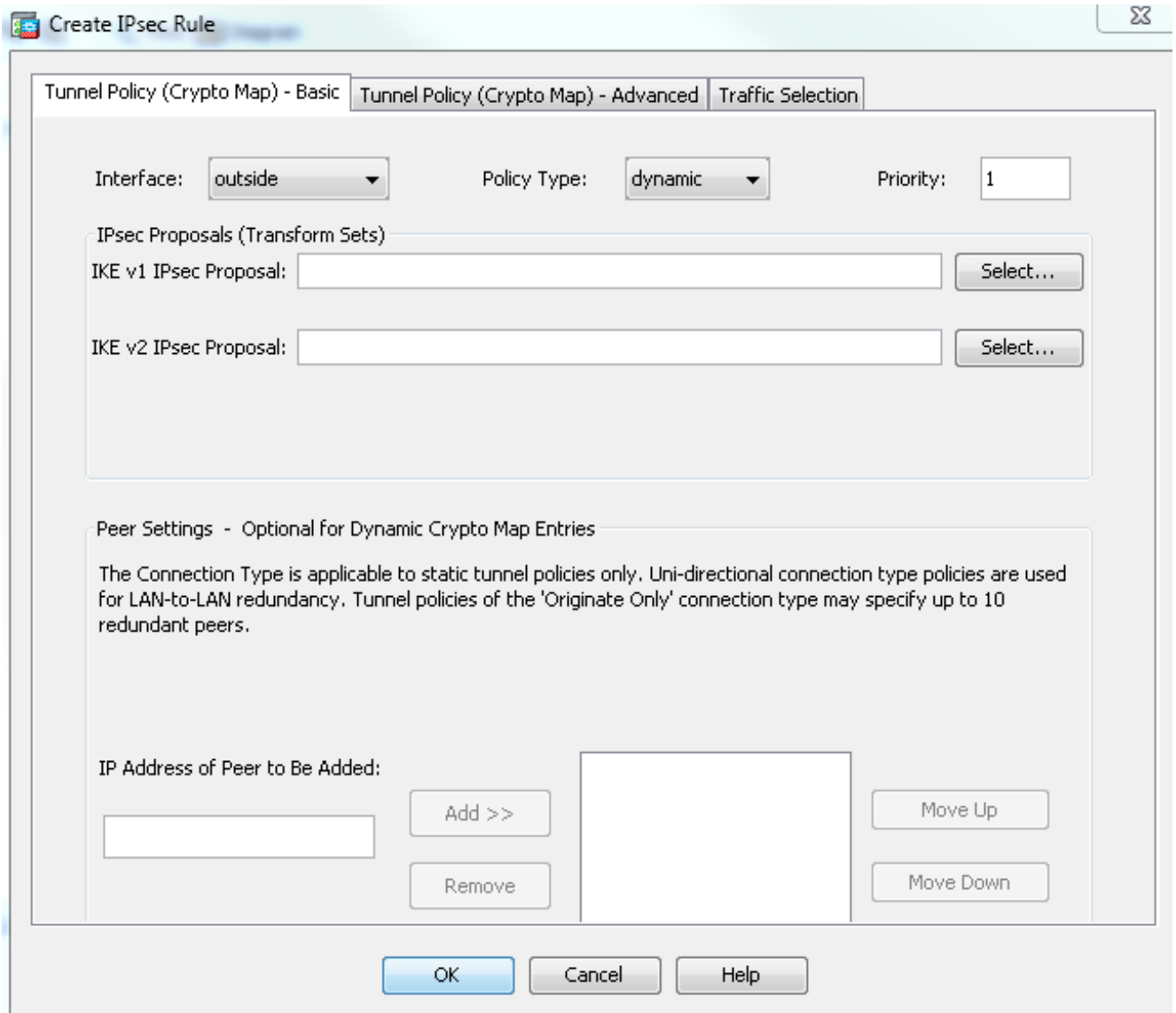
### 中央 ASA ( スタティック ピア )

スタティック IP アドレスを持つ ASA で、不明なピアからのダイナミック接続を受け入れる一方で IKEv1 事前共有キーを使用してピアを認証するように VPN をセットアップします。

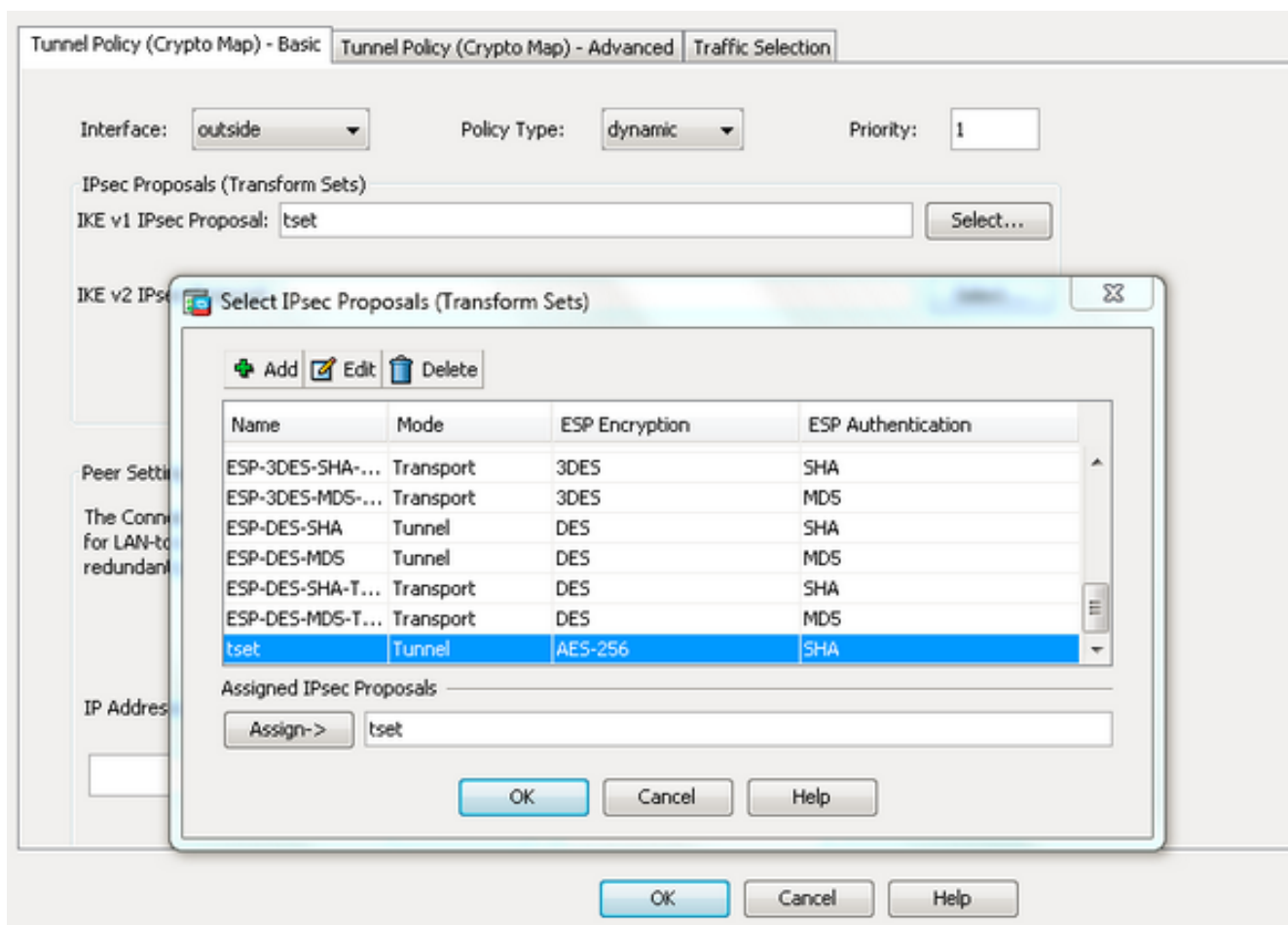
1. [Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] の順に選択します。このウィンドウには、すでに存在する暗号マップ エントリのリストが表示されます ( 存在する場合 )。ASA にはピアの IP アドレスが不明であるため、ASA が接続を受け入れるために、一致するトランスフォームセット ( IPsec プロポーザル ) を使用してダイナミック マップを設定します。[Add] をクリックします。



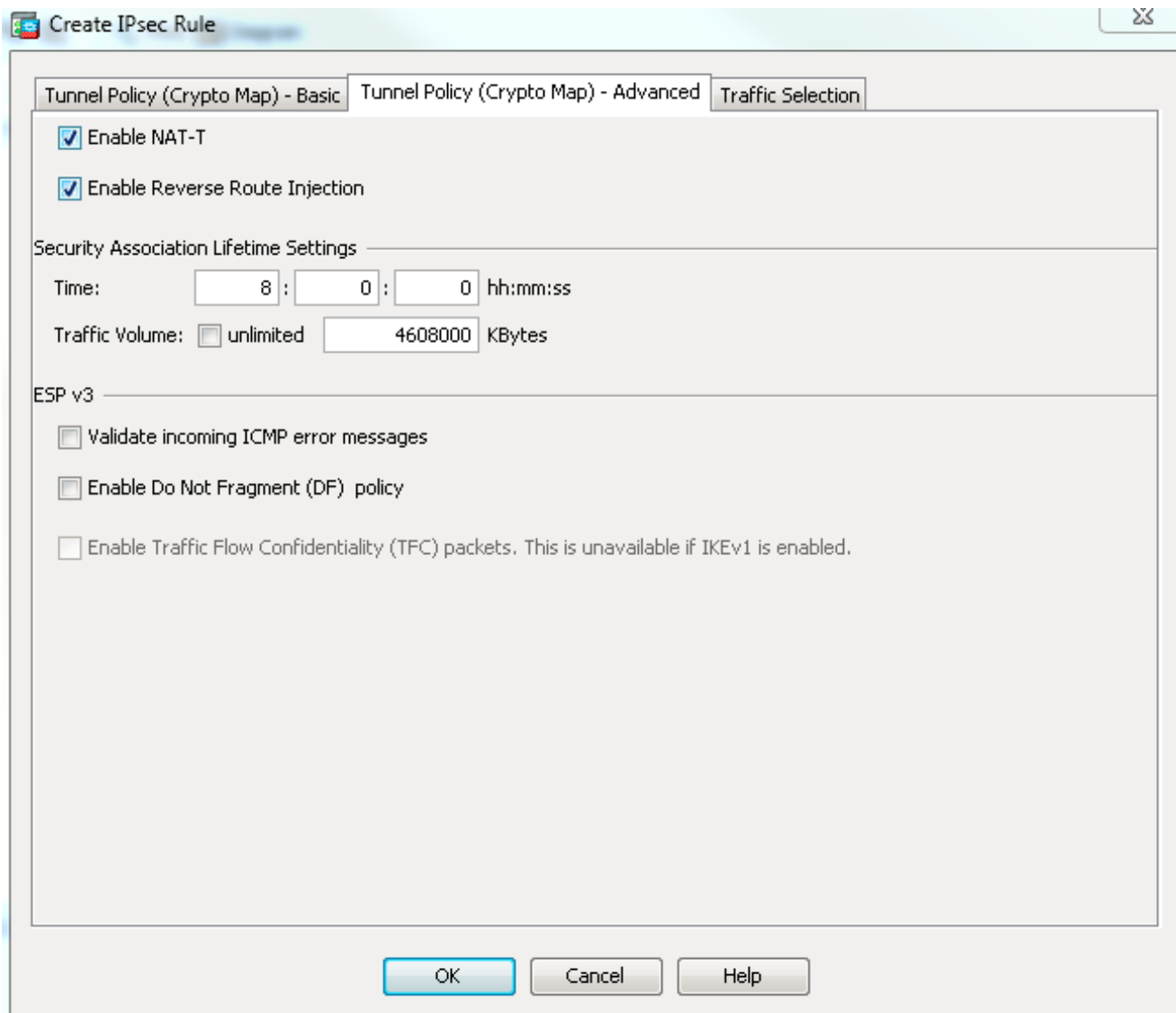
2. [Create IPsec Rule] ウィンドウの [Tunnel Policy (Crypto Map) - Basic] タブで、[Interface] ドロップダウンリストから [outside] を選択し、[Policy Type] ドロップダウンリストから [dynamic] を選択します。[Priority] フィールドで、ダイナミック マップに複数のエントリがある場合のこのエントリの優先順位を割り当てます。次に、[IKE v1 IPsec Proposal] フィールドの横にある [Select] をクリックして、IPsec プロポーザルを選択します。



3. [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開いたら、現在の IPsec プロポーザルの中から選択するか、[Add] をクリックし、新しいプロポーザルを作成して使用します。完了したら、[OK] をクリックします。



4. [Tunnel Policy (Crypto Map)-Advanced] タブで、[Enable NAT-T] チェックボックス (ピアが NAT デバイスの背後にある場合に必要) と [Enable Reverse Route Injection] チェックボックスをオンにします。ダイナミックピアに対してVPNトンネルが稼働状態になると、ASAは、VPNインターフェイスを指すネゴシエートされたリモートVPNネットワークのダイナミックルートをインストールします。



必要に応じて、[Traffic Selection] タブで、ダイナミック ピアの関心のある VPN トラフィックを定義し、[OK] をクリックすることもできます。

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | **Traffic Selection**

Action:  Protect  Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

**More Options**

Enable Rule

Source Service: (TCP or UDP service only) ⓘ

Time Range:

OK

Cancel

Help

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

+ Add ▾ Edit ▾ Delete | ↑ ↓ | ✂ | Find Diagram

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
[-] interface: outside						
dynamic: 65535.1	1	any4	any4	IP ip	Protect	tset

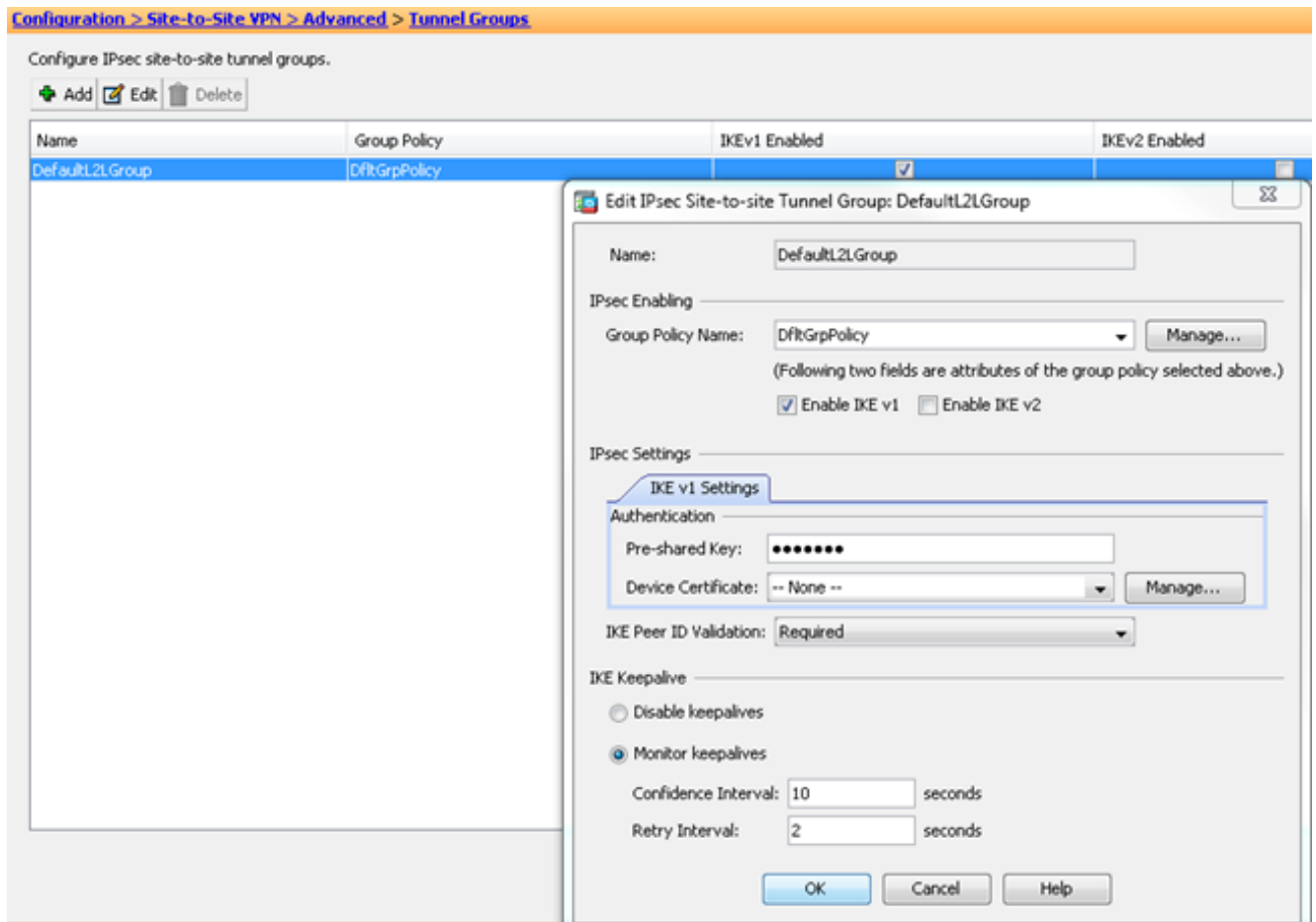
Enable Anti-replay window size: 64 ▾

Apply Reset

前述のように、ASA にはリモート ダイナミック ピアの IP アドレスに関する情報がいないため、不明な接続要求は、デフォルトで、ASA 上に存在する DefaultL2LGroup に到達します。認証に成功するには、リモート ピアで設定された事前共有キー（この例では cisco123）が DefaultL2LGroup にあるものと一致する必要があります。

5. [Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel Groups] の順に選択して、[DefaultL2LGroup] を選択し、[Edit] をクリックして必要な事前共有キーを設定します。完了したら、[OK] をクリックします。





注：これにより、スタティックピア（中央-ASA）にワイルドカード事前共有キーが作成されます。この事前共有キーおよびその一致するプロポーザルを認識しているデバイス/ピアは、VPN トンネルを確立し、VPN 経路でリソースにアクセスすることができます。この事前共有キーが不明なエンティティと共有されていないことと容易に推測できないことを確認してください。

6. [Configuration] > [Site-to-Site VPN] > [Group Policies]を選択し、選択したグループポリシー（この場合はデフォルトのグループポリシー）を選択します。[Edit] をクリックし、[Edit Internal Group Policy]ダイアログボックスでグループポリシーを編集します。完了したら、[OK] をクリックします。

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. Policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

**Edit Internal Group Policy: DfltGrpPolicy**

Name:

Tunneling Protocols:
  Clientless SSL VPN
  SSL VPN Client
  IPsec IKEv1
  IPsec IKEv2
  L2TP/IPsec

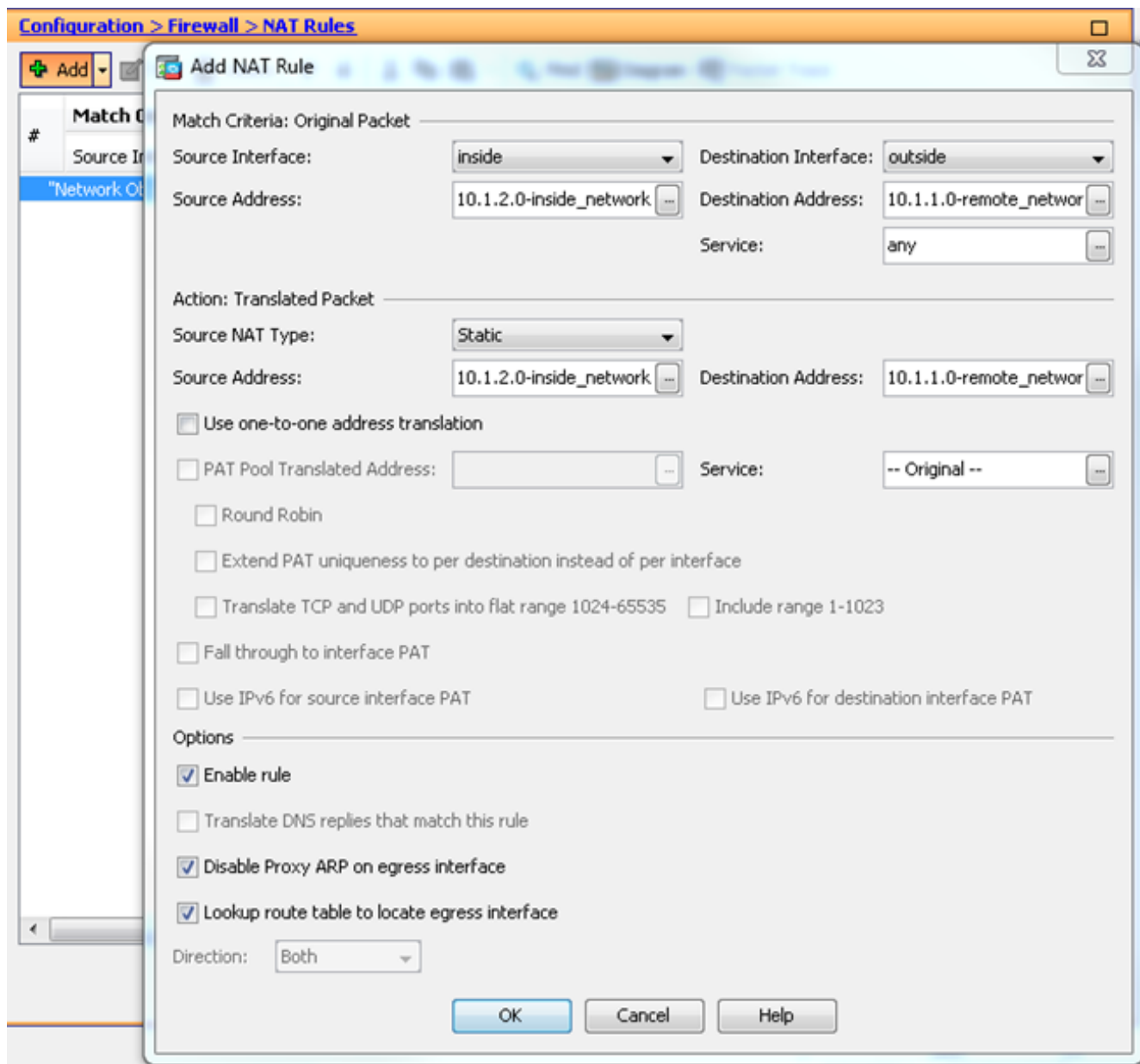
Filter:

Idle Timeout:
  Unlimited
  minutes

Maximum Connect Time:
  Unlimited
  minutes

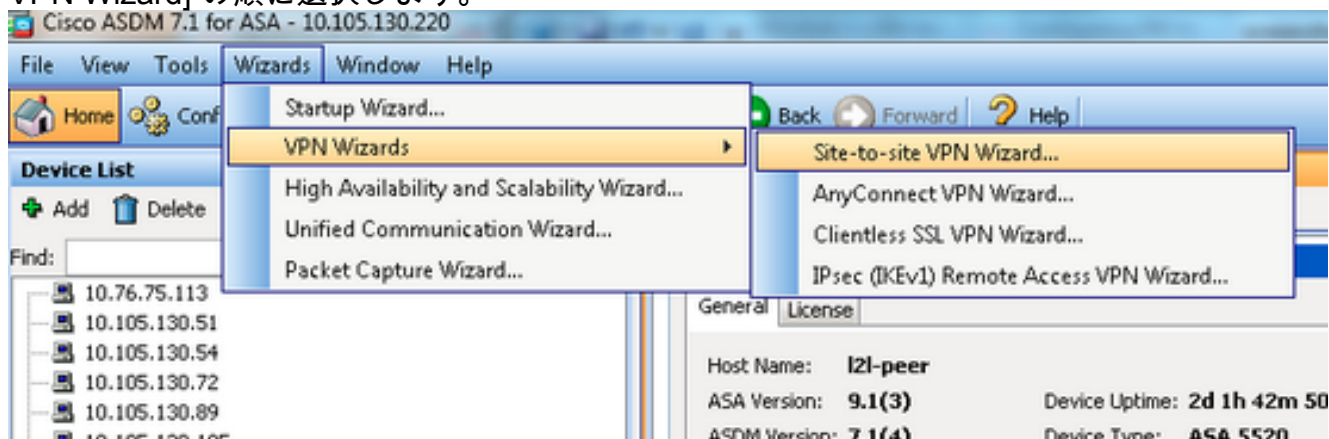
Find:     Match Case

7. [Configuration] > [Firewall] > [NAT Rules] の順に選択し、[Add Nat Rule] ウィンドウで VPN トラフィックの no nat ( NAT-EXEMPT ) ルールを設定します。完了したら、[OK] をクリックします。



## リモート ASA (ダイナミックピア)


1. ASDM アプリケーションが ASA に接続したら、[Wizards] > [VPN Wizards] > [Site-to-site VPN Wizard] の順に選択します。



2. [next] をクリックします。

Site-to-site VPN Connection Setup Wizard

### VPN Wizard



**Introduction**

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional protects the data using the IPsec protocol.

Here is a [video](#) on how to setup a site-to-site VPN connection.

< Back   Next >

3. [VPN Access Interface] ドロップダウンリストから [outside] を選択し、リモートピアの外部 IP アドレスを指定します。暗号マップを適用するインターフェイス (WAN) を選択してください。[next] をクリックします。

Site-to-site VPN Connection Setup Wizard

### Steps

1. Introduction
2. **Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

### Peer Device Identification

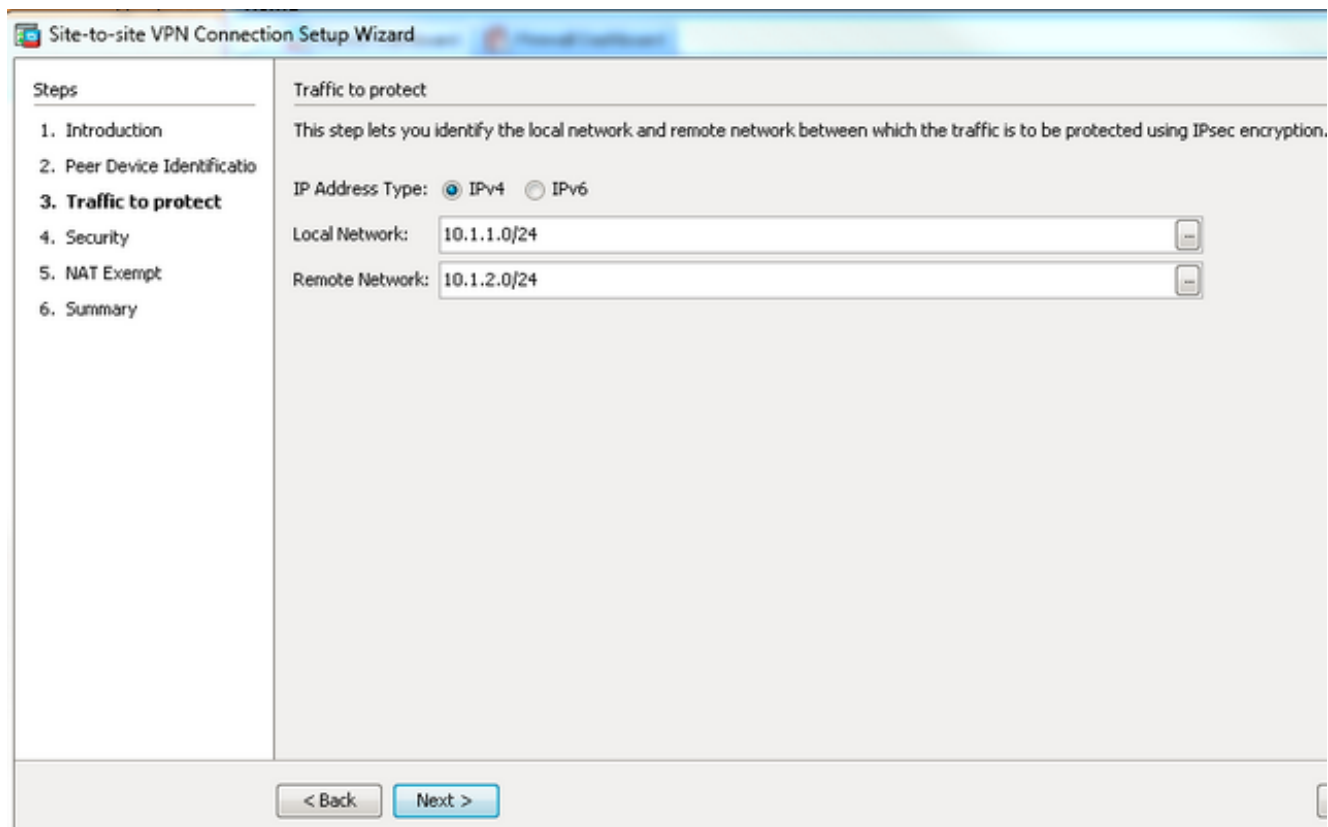
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address:

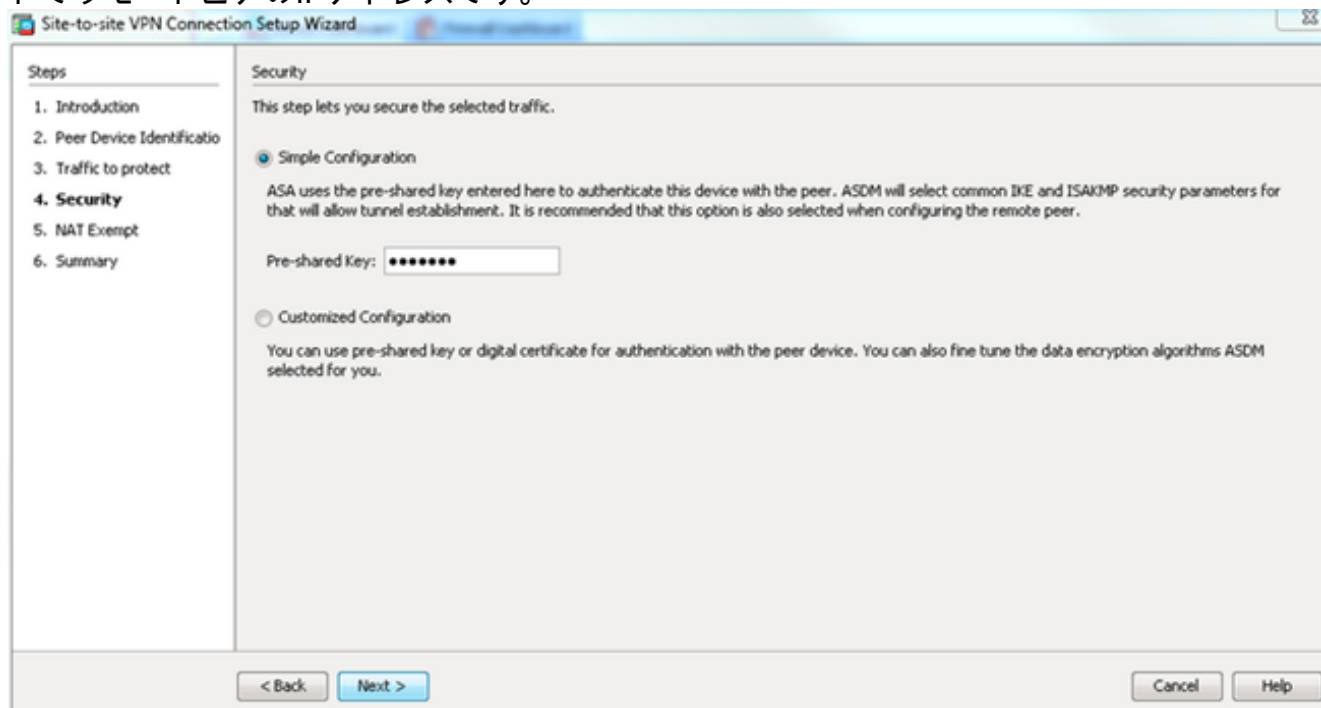
VPN Access Interface:

< Back   Next >

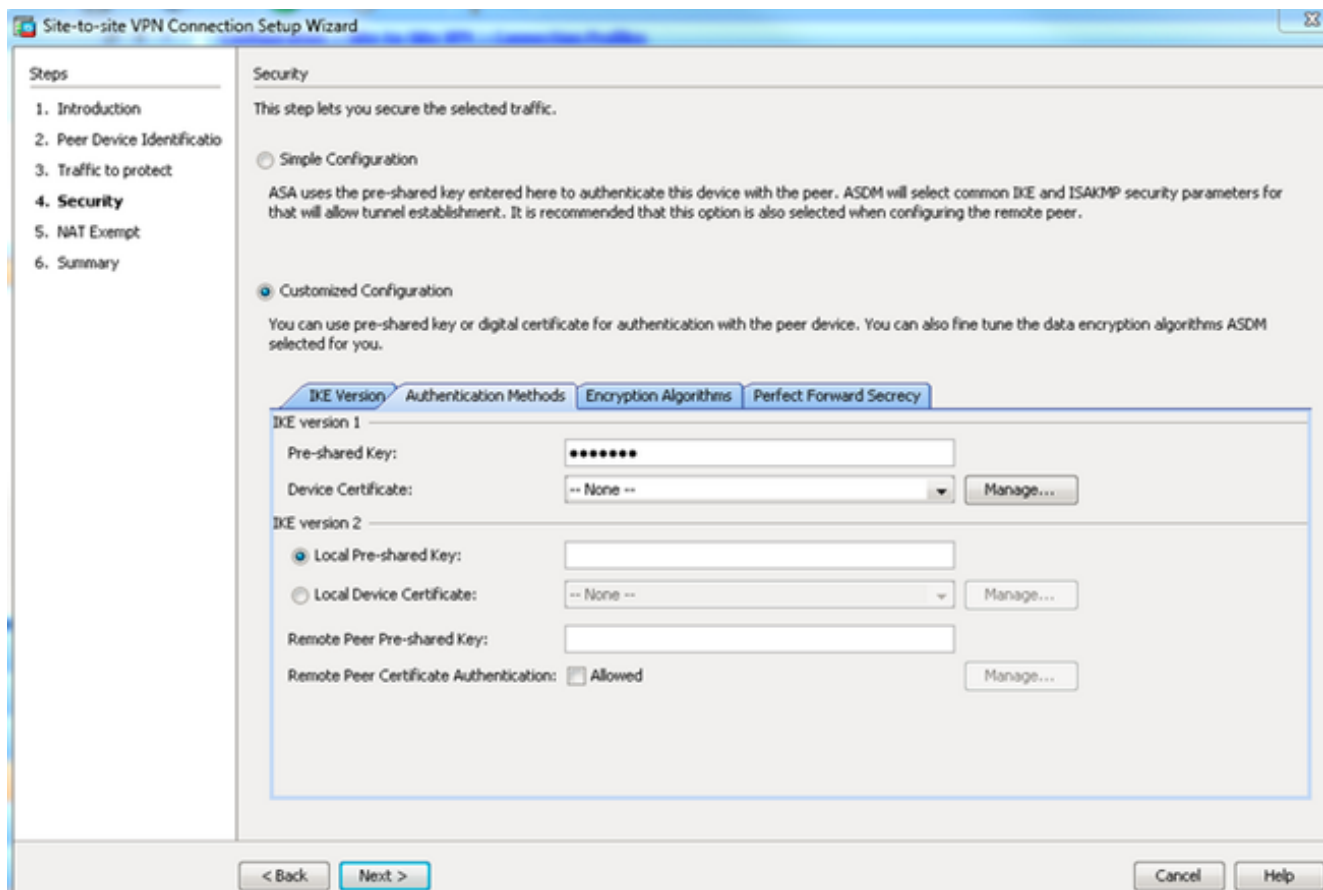
4. VPN トンネルの通過を許可する必要のあるホスト/ネットワークを指定します。このステップでは、VPN トンネルの [Local Networks] と [Remote Networks] を指定します。必要に応じて、[Local Network] フィールドと [Remote Network] フィールドの横にあるボタンをクリックしてアドレスを選択します。完了したら、[Next] をクリックします。



5. 使用する認証情報（この例では事前共有キー）を入力します。この例で使用する事前共有キーはcisco123です。LAN-to-LAN(L2L)VPNを設定する場合、トンネルグループ名はデフォルトでリモートピアのIPアドレスです。

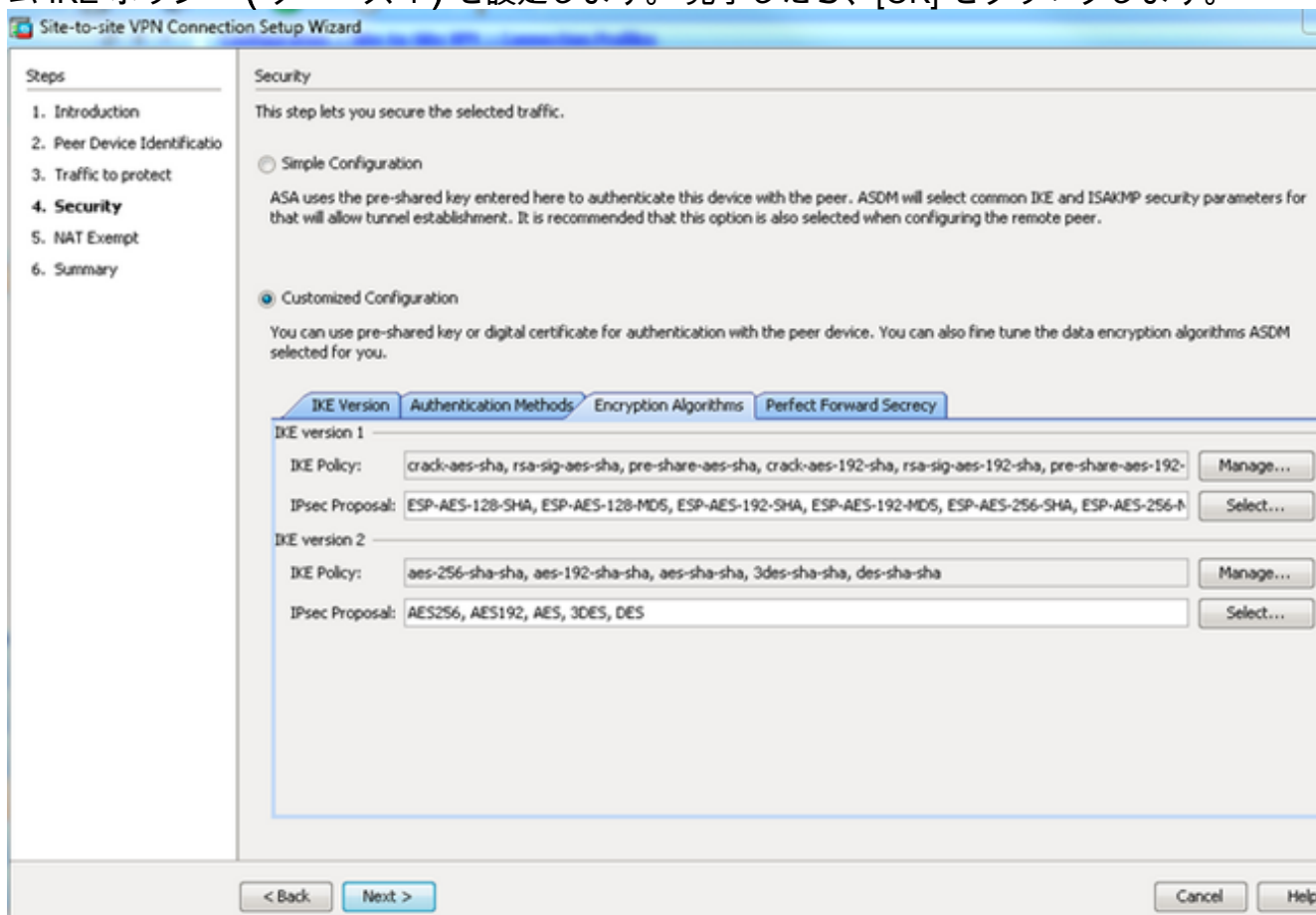


または任意の IKE および IPsec ポリシーを含むように設定をカスタマイズできます。ピア間には少なくとも 1 つの一致するポリシーがある必要があります。[Authentication Methods] タブで、[Pre-shared Key] フィールドに IKE バージョン 1 の事前共有キーを入力します。この例では、cisco123 です。



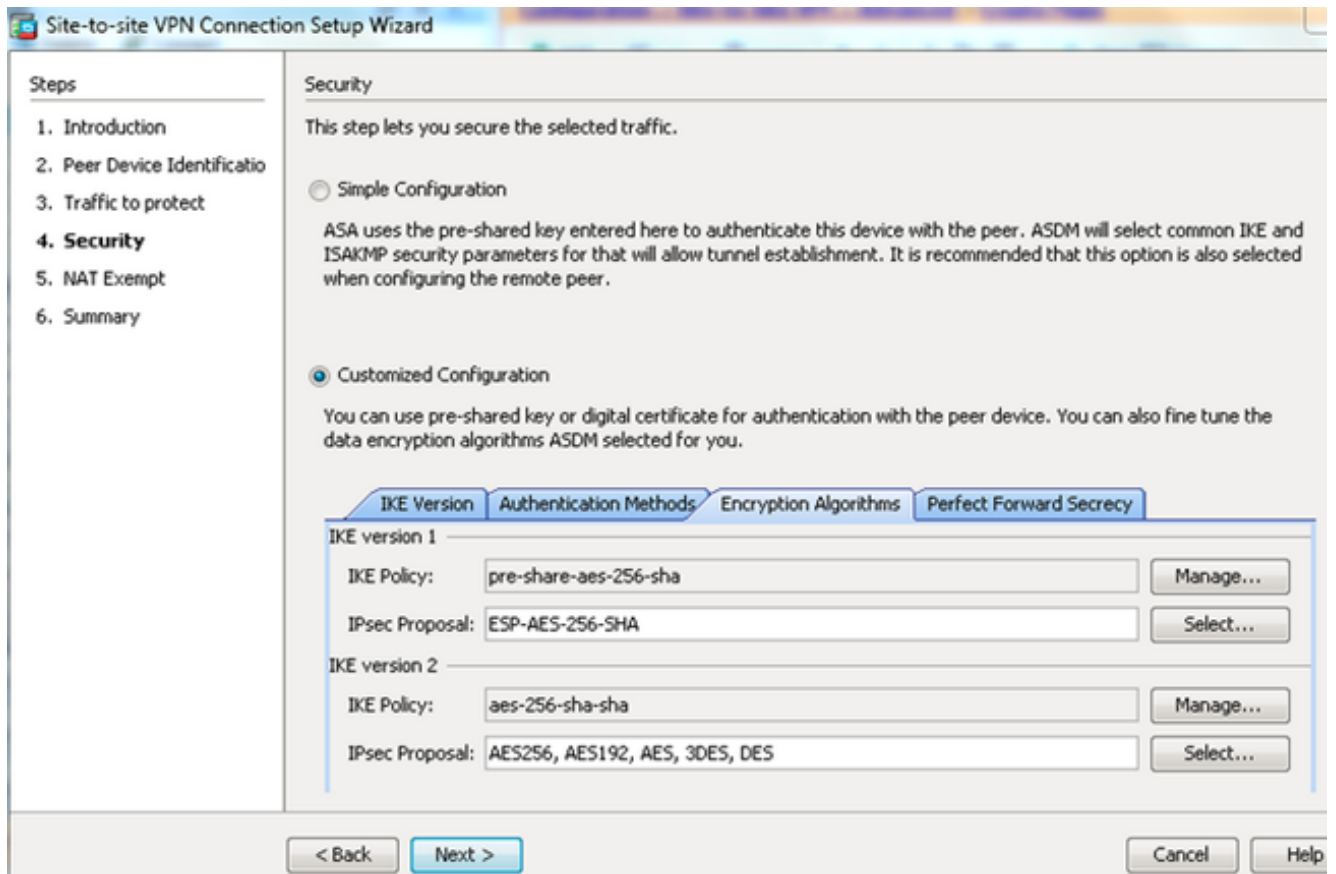
[Encryption Algorithms] タブをクリックします。

6. [IKE Policy] フィールドの横にある [Manage] をクリックし、[Add] をクリックして、カスタム IKE ポリシー ( フェーズ 1 ) を設定します。完了したら、[OK] をクリックします。

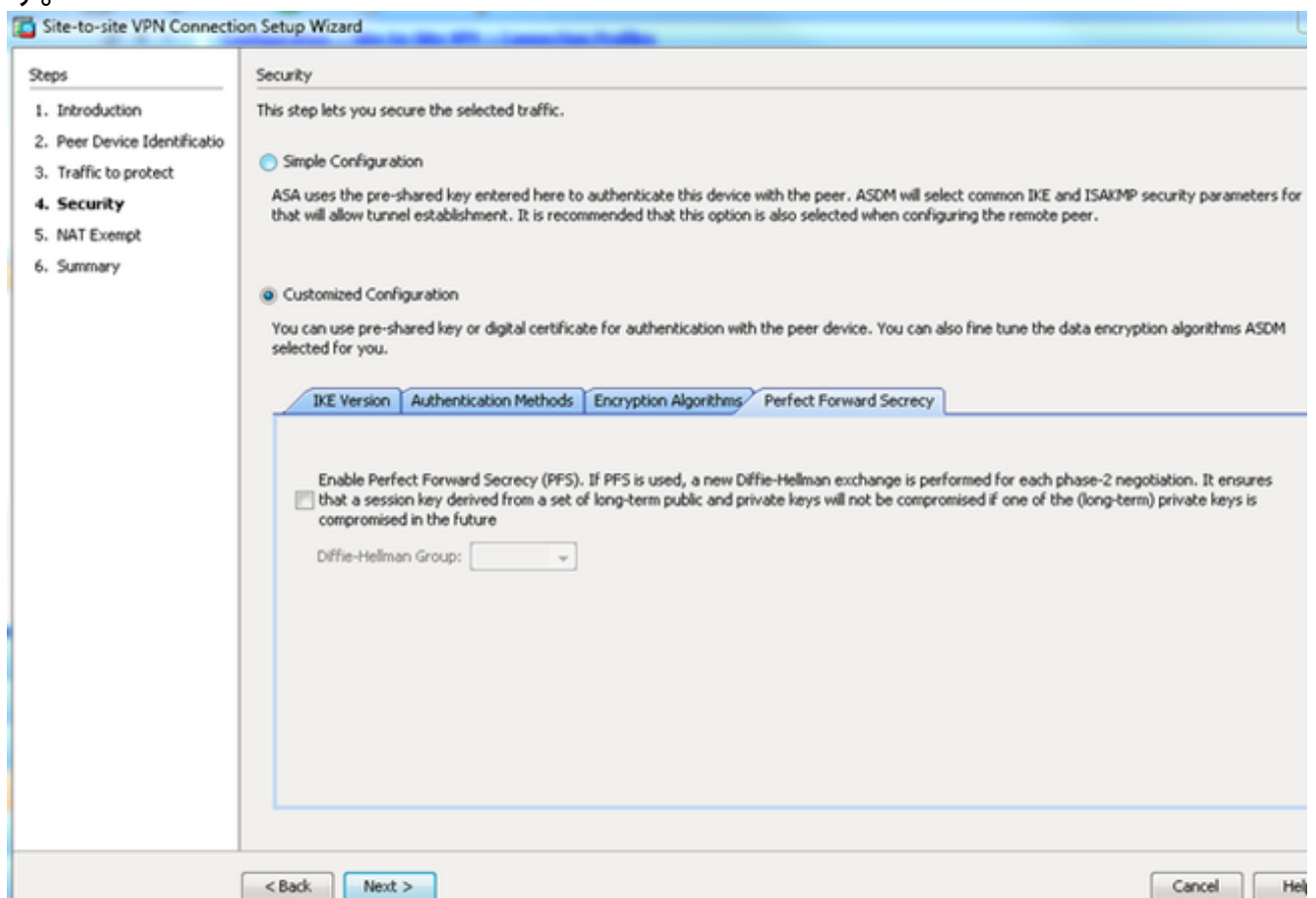


7. [IPsec Proposal] フィールドの横にある [Select] をクリックして、必要な IPsec プロポーザルを選択します。完了したら、[Next] をクリックします。





必要に応じて、[Perfect Forward Security] タブに移動し、[Enable Perfect Forward Security (PFS)] チェックボックスをオンにすることができます。完了したら、[Next] をクリックします。



8. [Exempt ASA side host/network from address translation] チェックボックスをオンにして、トンネルトラフィックのネットワークアドレス変換が開始されないようにします。ドロップダウンリストから [local] または [inside] を選択してローカルネットワークに到達可能なイ

インターフェイスを設定します。[next] をクリックします。

The screenshot shows the 'NAT Exempt' step of the VPN setup wizard. On the left, a 'Steps' sidebar lists: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. Security, 5. NAT Exempt (highlighted), and 6. Summary. The main area is titled 'NAT Exempt' and contains the text: 'This step allows you to exempt the local network addresses from network translation.' Below this, there is a checked checkbox labeled 'Exempt ASA side host/network from address translation' and a dropdown menu currently set to 'inside'. At the bottom, there are '< Back' and 'Next >' buttons.

9. 設定した VPN の概要が表示されます。確認して、[Finish] をクリックします。

The screenshot shows the 'Summary' screen of the VPN setup wizard. On the left, there is a 'VPN Wizard' graphic with a network diagram showing 'Branch', 'ISP', 'Home', and 'Corporate Network' connected. The main area is titled 'Summary' and contains the text: 'Here is the summary of the configuration.' Below this is a table with two columns: 'Name' and 'Value'. The table lists various configuration parameters and their values. At the bottom, there are '< Back', 'Finish', 'Cancel', and 'Help' buttons.

Name	Value
Summary	
Peer Device IP Address	172.16.2.1
VPN Access Interface	outside
Protected Traffic	Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	pre-share-aes-256-sha
IPsec Proposal	ESP-AES-256-SHA
IKE v2	
IKE Policy	aes-256-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Network Address Translation	The protected traffic is not subjected to network address translation



## CLI での設定

### 中央 ASA ( スタティックピア ) の設定

1. 次の例のように、VPN トラフィックのNO-NAT/NAT-EXEMPT ルールを設定します。

```
object network 10.1.1.0-remote_network
 subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
 destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
 no-proxy-arp route-lookup
```

2. 任意のリモート ダイナミック L2L ピアを認証するために、DefaultL2LGroup で事前共有キーを設定します。

```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```

3. フェーズ 2/ISAKMP ポリシーを定義します。

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

4. フェーズ 2 トランスフォーム セット/IPsec ポリシーを定義します。

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. 次のパラメータを使用してダイナミック マップを設定します。必要なトランスフォーム セットリバースルート インジェクションの有効化：接続されたクライアントのルーティング情報をセキュリティ アプライアンスが学習することを可能にする (任意)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
 crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. ダイナミック マップを暗号マップにバインドし、暗号マップを適用して、外部インターフェイスで ISAKMP/IKEv1 を有効にします。

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
```

```
crypto map outside_map interface outside
 crypto ikev1 enable outside
```

### リモート ASA ( ダイナミックピア )

1. VPN トラフィックの NAT 除外ルールを設定します。

```
object network 10.1.1.0-inside_network
 subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-remote_network
 subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
 destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
 no-proxy-arp route-lookup
```

2. スタティック VPN ピアおよび事前共有キーのトンネル グループを設定します。

```
tunnel-group 172.16.2.1 type ipsec-l2l
 tunnel-group 172.16.2.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

### 3. フェーズ 1/ISAKMP ポリシーを定義します。

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

### 4. フェーズ 2 トランスフォーム セット/IPsec ポリシーを定義します。

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

### 5. 関心のある VPN トラフィック/ネットワークを定義するアクセス リストを設定します。

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

### 6. 次のパラメータを使用してスタティック暗号マップを設定します。暗号/VPN アクセス リストリモート IPsec ピアの IP アドレス必要なトランスフォーム セット

```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```

### 7. 暗号マップを適用して、外部インターフェイスで ISAKMP/IKEv1 を有効にします。

```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

## 確認

ここでは、設定が正常に動作することを確認します。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

- **show crypto isakmp sa** : ピアにおける現在の IKE セキュリティ アソシエーション (SA) をすべて表示します。
- **show crypto ipsec sa** : 現在の IPsec SA をすべて表示します。

ここでは、2 つの ASA の検証出力の例を示します。

## 中央 ASA

```
Central-ASA#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: 172.16.1.1
```

```
Type      : L2L           Role       : responder
```

```
Rekey     : no           State      : MM_ACTIVE
```

```
Central-ASA# show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1
```

```
local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
```

```
current_peer: 172.16.1.1
```

```
#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
#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.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
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: 30D071C0
current inbound spi : 38DA6E51
```

inbound esp sas:

```
spi: 0x38DA6E51 (953839185)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
```

outbound esp sas:

```
spi: 0x30D071C0 (818966976)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## リモート ASA

Remote-ASA#**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: 172.16.2.1
Type      : L2L           Role      : initiator
Rekey     : no           State     : MM_ACTIVE
```

Remote-ASA#**show crypto ipsec sa**

interface: outside

Crypto map tag: **outside\_map**, seq num: 1, local addr: 172.16.1.1

```
access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
```

```
current_peer: 172.16.2.1
```

```
#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
#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.: 172.16.2.1/0
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: 38DA6E51
current inbound spi : 30D071C0
```

#### **inbound esp sas:**

**spi: 0x30D071C0 (818966976)**

```
transform: esp-aes-256 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): (4373999/28676)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
```

#### **outbound esp sas:**

**spi: 0x38DA6E51 (953839185)**

```
transform: esp-aes-256 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): (4373999/28676)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## 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。

アウトプット インタープリタ ツール ( 登録ユーザ専用 ) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

注 : debug コマンドを使用する前に、[「デバッグコマンドの重要な情報」](#)を参照してください。

次のようなコマンドを使用します。

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

**注意 :** clear crypto isakmp sa コマンドは、アクティブな VPN トンネルをすべてクリアするため、動作の中断をとまいません。

PIX/ASA ソフトウェア リリース 8.0(3) 以降では、clear crypto isakmp sa <peer ip address> コマ

ンドを使用して IKE SA を個別にクリアできます。8.0(3) より前のソフトウェア リリースでは、[vpn-sessiondb logoff tunnel-group <tunnel-group-name> コマンドを使用して、1つのトンネルの IKE および IPsec SA をクリアします。](#)

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

```
clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

デバッグの使用 :

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

## リモート ASA ( イニシエータ )

次の packet-tracer コマンドを入力してトンネルを開始します。

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [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=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
```

```
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED

Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

## 中央 ASA (レスポンス)

```
Jan 20 12:42:35 [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  
:  
.  
Jan 20 12:42:35 [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  
Jan 20 12:42:35 [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 (20) + NAT-D (20) + NONE (0) total length : 304  
:  
.  
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, **Connection landed on tunnel\_group**  
**DefaultL2LGroup**  
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,  
Generating keys for Responder...  
Jan 20 12:42:35 [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 (20) + NAT-D (20) +  
NONE (0) total length : 304  
Jan 20 12:42:35 [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  
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,  
**ID\_IPV4\_ADDR ID received172.16.1.1**  
:  
.  
Jan 20 12:42:35 [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  
Jan 20 12:42:35 [IKEv1]Group = **DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**  
:  
.  
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM:**  
msg id = c45c7b30  
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE\_DECODE  
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +  
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200  
:  
.  
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote**  
**IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,**  
**Protocol 0, Port 0:**  
.  
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,  
IP = 172.16.1.1, **Received local**  
**IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,**  
**Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,  
IP = 172.16.1.1, processing notify payload  
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM  
IsRekeyed old sa not found by addr  
Jan 20 12:42:35 [IKEv1]Group = **DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map**  
**check, map outside\_dyn\_map, seq = 1 is a successful match**  
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE  
Remote Peer configured for crypto map: outside\_dyn\_map  
:  
.  
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,  
**Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0**  
**Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:**  
.  
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=c45c7b30)  
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE

```
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

## 関連情報

- [Cisco ASA シリーズ コマンド リファレンス](#)
- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)