

事前共有キーを使用して Windows 8 PC と ASA の間の L2TP over IPsec を設定する

内容

[概要](#)

[前提条件](#)

[要件](#)

[制約事項](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[完全なトンネル設定](#)

[Adaptive Security Device Manager\(ASDM\)を使用したASAの設定](#)

[CLIを使用したASAの設定](#)

[Windows 8 L2TP/IPsecクライアントの設定](#)

[Split-tunnel 設定](#)

[ASAでの設定](#)

[L2TP/IPsecクライアントの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)とWindows 8ネイティブクライアント間の事前共有キーを使用して、IPsec上でレイヤ2トンネリングプロトコル(L2TP)を設定する方法について説明します。

L2TP over Internet Protocol(IPsec)セキュリティは、L2TP Virtual Private Network(VPN)ソリューションを、IPsec VPNおよびファイアウォールサービスとともに1つのプラットフォームに導入し、管理する機能を提供します。

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。

- クライアントマシンからASAへのIP接続。接続をテストするには、クライアントエンドポイントからASAのIPアドレスをpingし、クライアントエンドポイントからASAのIPアドレスをpingします

- UDPポート500および4500およびEncapsulating Security Payload(ESP)プロトコルが、接続のパス上のどこでもブロックされていないことを確認します

制約事項

- L2TP over IPsecはIKEv1のみをサポートし、IKEv2はサポートしません。
- ASA上のL2TPにより、LNSはWindows、MAC OS X、Android、およびCisco IOSなどのオペレーティングシステムに統合されたネイティブVPNクライアントと相互運用できます。IPsecを使用するL2TPのみがサポートされ、ネイティブL2TP自体はASAではサポートされません。
- WindowsクライアントでサポートされるIPsecセキュリティアソシエーションの最小ライフタイムは300秒です。ASAのライフタイムが300秒未満に設定されている場合、Windowsクライアントはそれを無視し、300秒のライフタイムに置き換えます。
- ASAは、ローカルデータベース上で、Point-to-Point Protocol(PPP)認証Password Authentication Protocol(PAP)およびMicrosoft Challenge-Handshake Authentication Protocol(CHAP)バージョン1および2のみをサポートします。Extensible Authentication Protocol(EAP)およびCHAPは、プロキシ認証サーバによって実行されます。したがって、リモートユーザがauthentication eap-proxyまたはauthentication chapコマンドで設定されたトンネルグループに属し、ASAがローカルデータベースを使用するように設定されている場合、そのユーザは接続できません。

サポートされるPPP認証タイプ

ASA上のL2TP over IPsec接続では、表に示すPPP認証タイプだけがサポートされます

AAAサーバタイプ	AAAサーバサポートとPPP認証タイプ	サポートされるPPP認証タイプ
LOCAL		PAP、MSCHAPv1、MSCHAPv2
RADIUS		PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+ [LDAP]		PAP、CHAP、MSCHAPv1
NT		PAP
Kerberos		PAP
SDI		SDI

PPP認証タイプの特性	キーワード	認証タイプ	説明
	chap	CHAP	サーバのチャレンジに回答して、クライアントは暗号化された[challenge]とセキュリティアプライアンスがPPP認証プロセスを外部RADIUS認証
	eap-proxy	EAP	
	ms-chap-v1	Microsoft CHAP、バージョン1	
	ms-chap-v2	Microsoft CHAP、バージョン、2	CHAPに似ていますが、CHAPのように、クリアテキストのパスワード
	pap	PAP	認証中にクリアテキストのユーザ名とパスワードを渡し、セキュア

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 5515シリーズASA
- L2TP/IPSecクライアント(Windows 8)

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。

関連製品

この設定は、Cisco ASA 5500 シリーズ セキュリティ アプライアンス 8.3(1) 以降にも使用できません。

表記法

ドキュメント表記の詳細は、[『シスコテクニカルティップス』の表記法](#)を参照してください

背景説明

レイヤ2トンネリングプロトコル(L2TP)は、リモートクライアントがパブリックIPネットワークを使用して企業のプライベートネットワークサーバと安全に通信できるようにするVPNトンネリングプロトコルです。L2TPはPPP over UDP (ポート1701) を使用してデータをトンネルします。

L2TPプロトコルは、クライアント/サーバモデルに基づいています。この機能は、L2TPネットワークサーバ(LNS)とL2TPアクセスコンセントレータ(LAC)の間で分割されます。LNSは通常、ASAなどのネットワークゲートウェイで動作しますが、LACはダイヤルアップネットワークアクセスサーバ(NAS)またはMicrosoft Windows、Apple iPhone、AndroidなどのバンドルされたL2TPクライアントを備えたエンドポイントデバイスです。

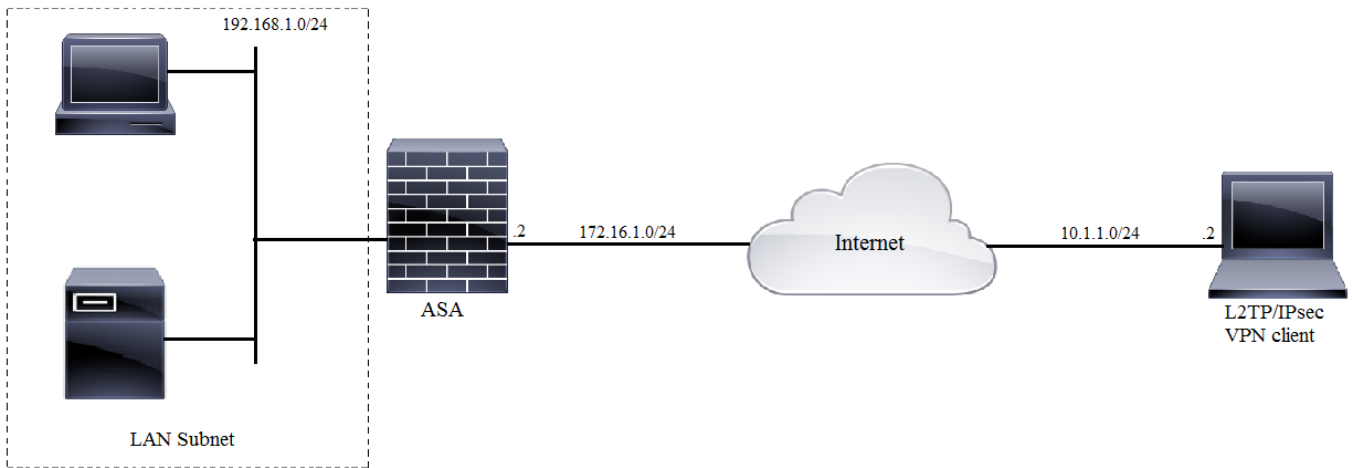
設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

注：このドキュメントで使用されているコマンドの詳細を調べるには、コマンド検索ツール（登録ユーザ専用）を使用してください。

注：この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 で使用されているアドレスであり、ラボ環境で使用されたものです。

ネットワーク図

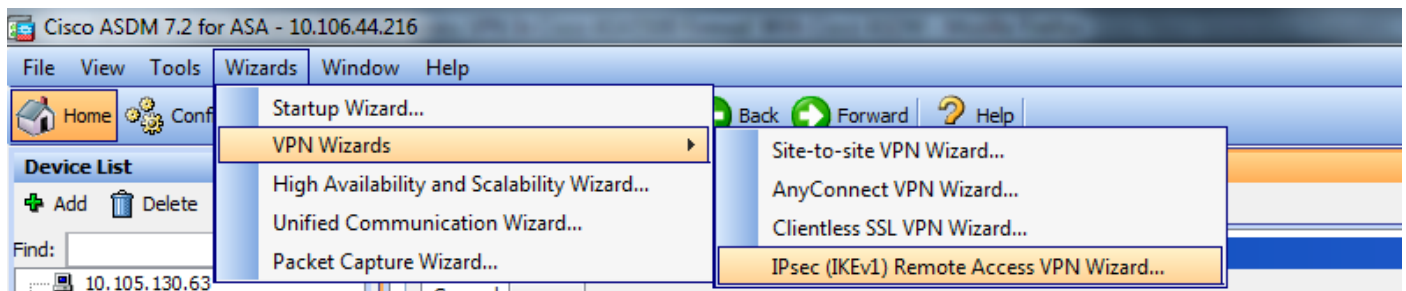


完全なトンネル設定

Adaptive Security Device Manager(ASDM)を使用したASAの設定

次のステップを実行します。

ステップ1:ASDMにログインし、[Wizards] > [VPN Wizards] > [Ipsec (IKEv1) Remote Access VPN Wizard] に移動します。




ステップ2:[Remote Access VPN setup]ウィンドウが表示されます。ドロップダウンリストから、VPNトンネルを終端するインターフェイスを選択します。この例では、外部インターフェイスはWANに接続されているため、このインターフェイスでVPNトンネルを終端します。[Enable inbound IPsec sessions to bypass interface access lists]ボックスをオンのままにします。グループポリシーとユーザごとの許可アクセスリストは、チェックされたトラフィックに適用され、クライアントが内部リソースにアクセスできるように外部インターフェイスで新しいアクセスリストを設定する必要はありません。[next] をクリックします。

VPN Wizard

VPN Wizard

IPsec IKEv1 Remote Access Wizard (Step 1 of ...)

Use this wizard to configure new new IPsec (IKEV1) remote access VPN tunnels. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.

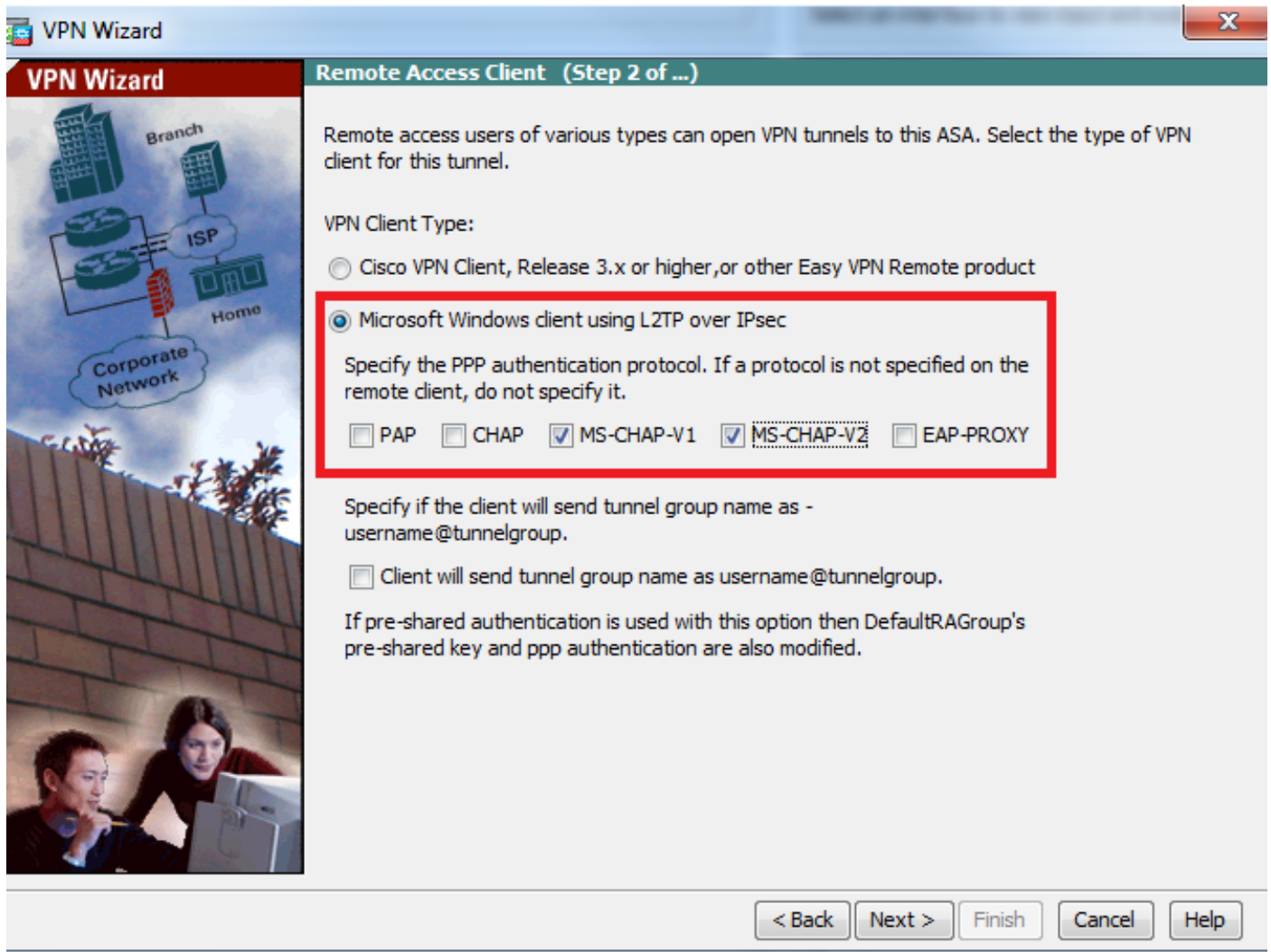


VPN Tunnel Interface: **outside**

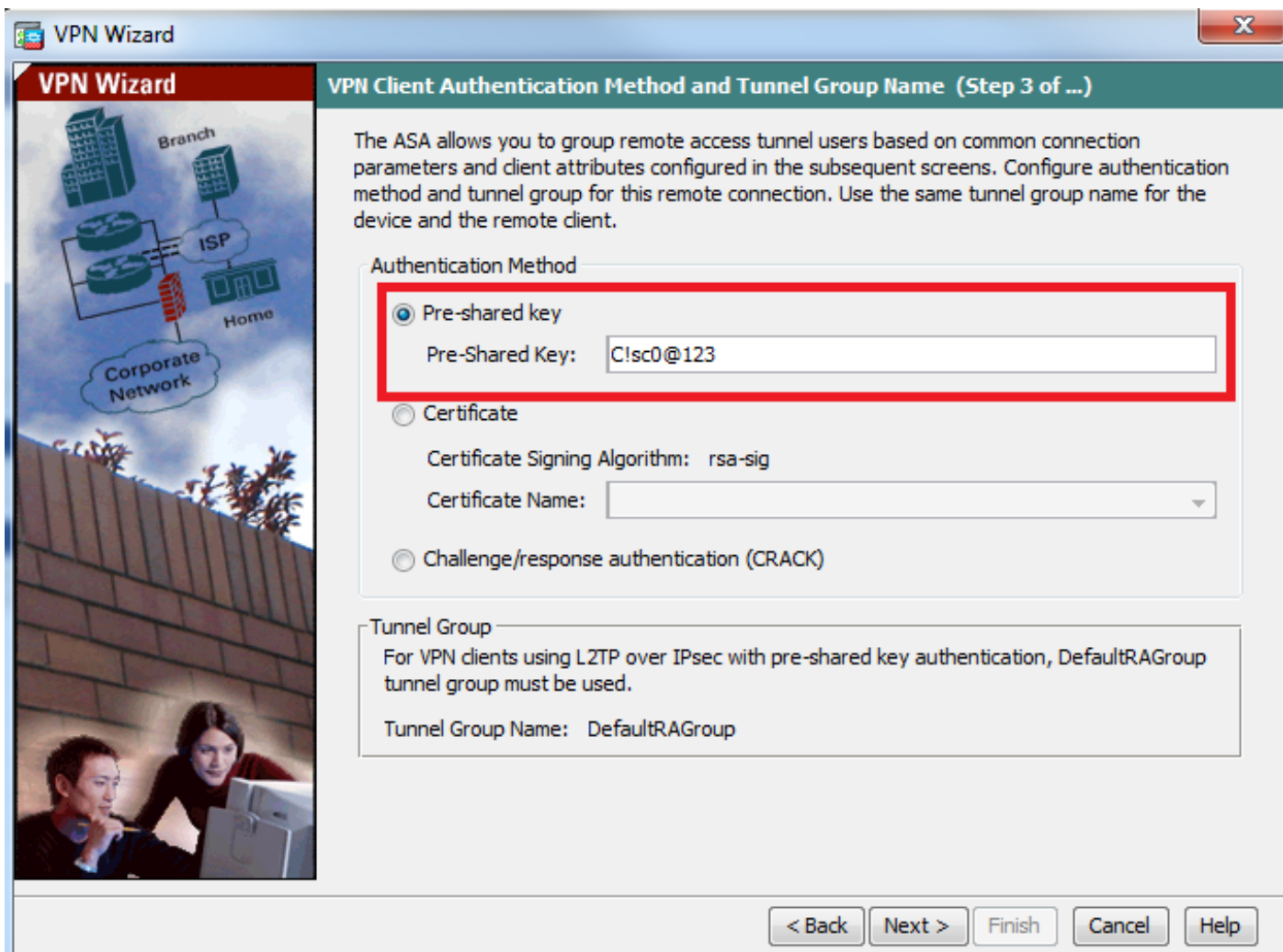
Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

< Back Next > Finish Cancel Help

ステップ3：この図に示すように、PAPはセキュアではなく、他の認証タイプはLOCAL認証データベースでサポートされていないため、PAPをPAPとしてL2TP over IPsec、MS-CHAP-V1、MS-CHAP-CHAP-V2 [Next] をクリックします。

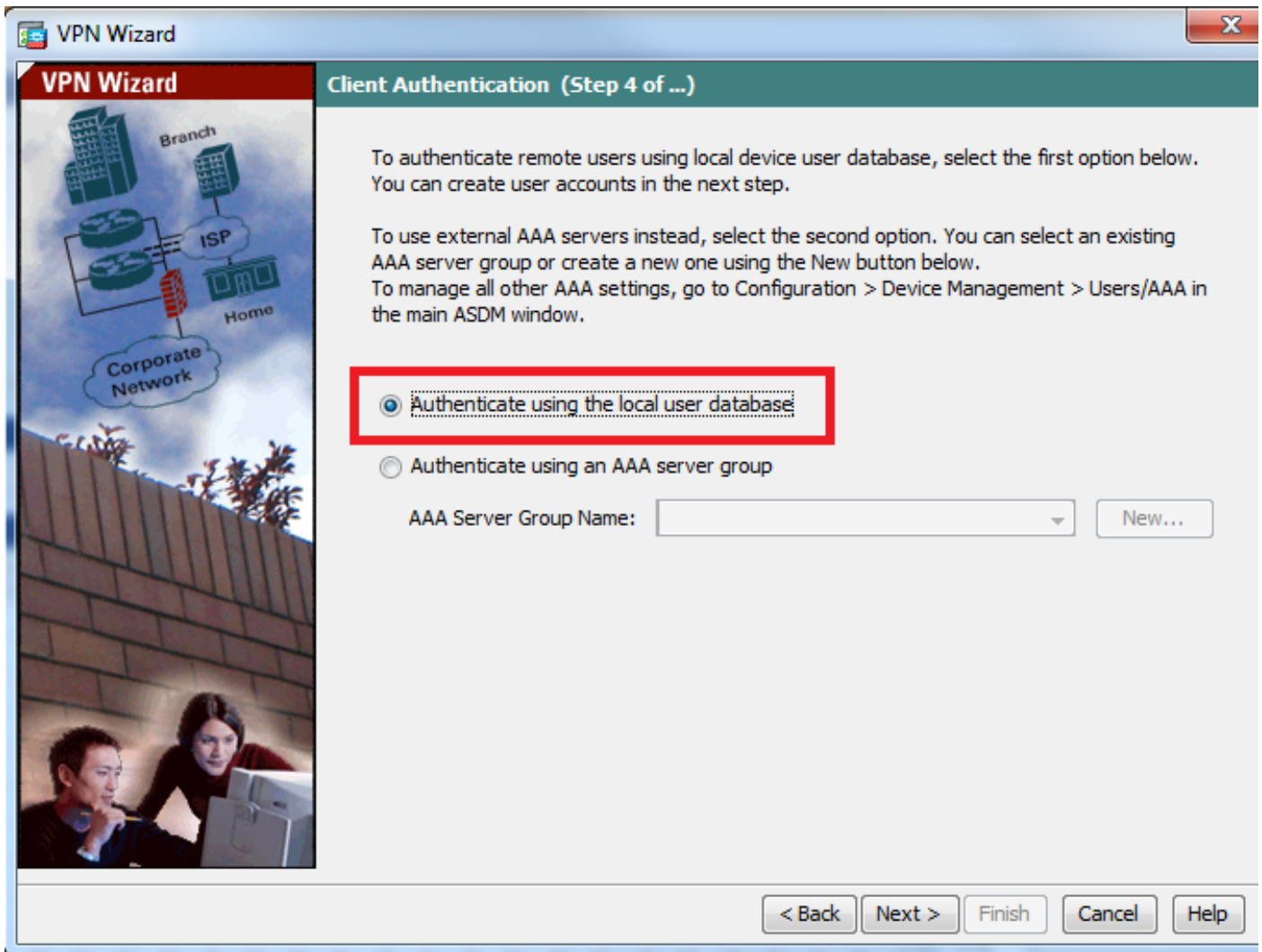


ステップ4：認証方式としてPre-shared-keyを選択して、クライアント側でも同じである必要がある事前共有キーを入力し、次の図に示すようにNextをクリックします。

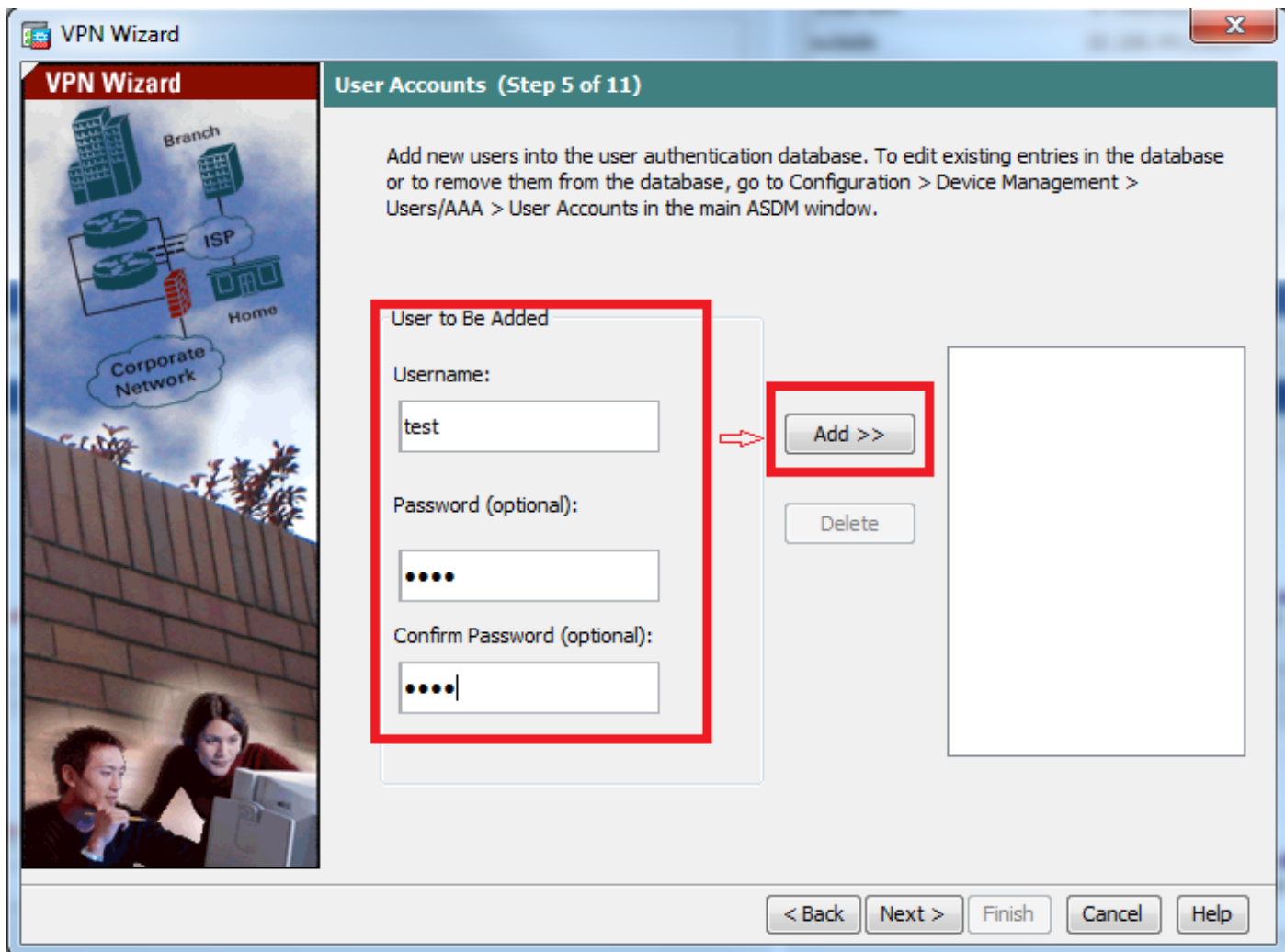


ステップ5:L2TP over IPsec接続を試行するユーザを認証する方法を指定します。外部AAA認証サーバまたは独自のローカルデータベースを使用できます。ASAのローカル・データベースに対してクライアントを認証する場合は、[Authenticate using the local user database]を選択し、[Next]をクリックします。

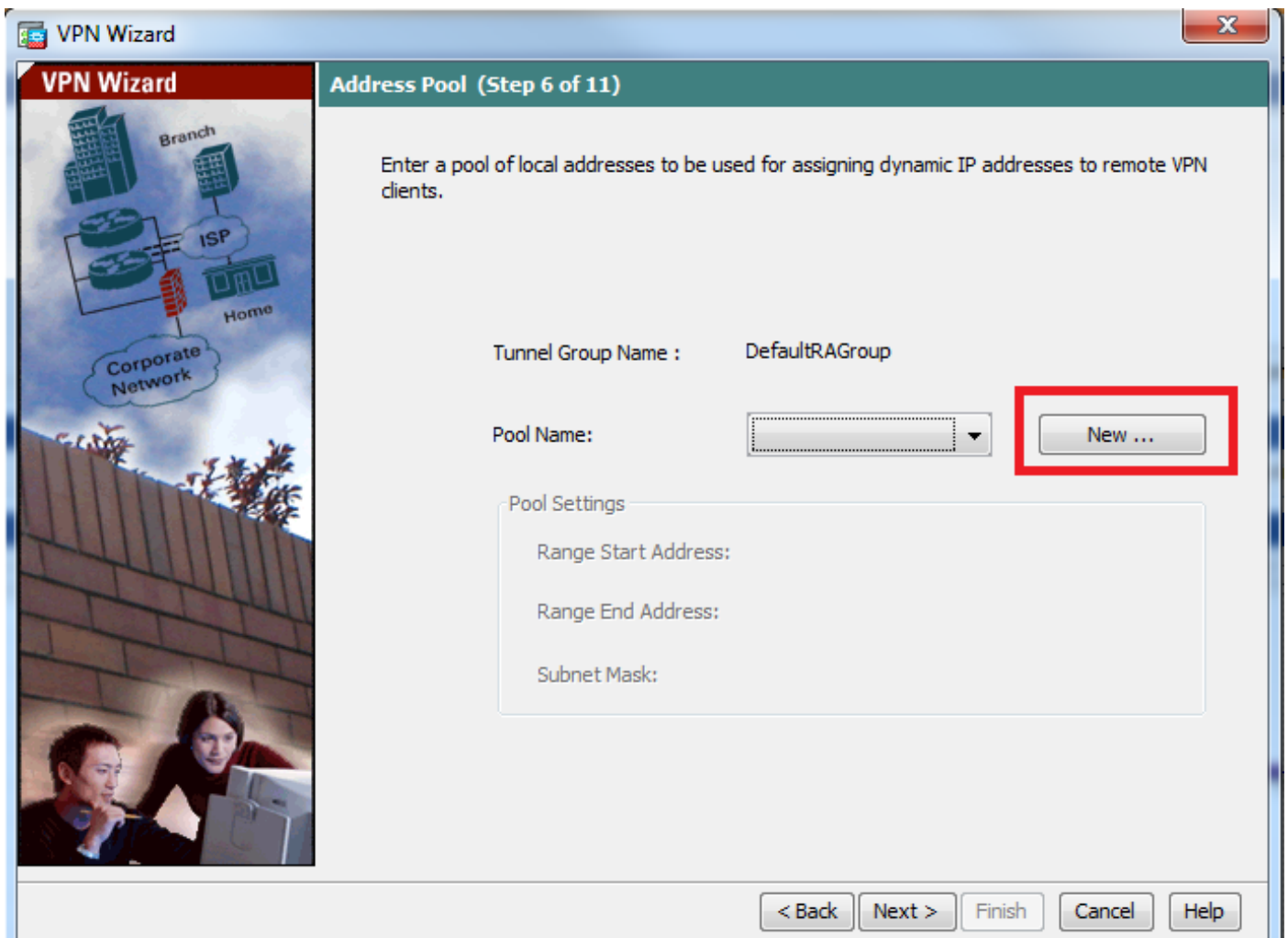
注：外部AAAサーバを使用してユーザを認証するには、[「VPNユーザのRADIUS認証の設定」](#)を参照してください。



ステップ6：ユーザ認証用にローカルデータベースに新しいユーザを追加するには、ユーザ名とパスワードを入力し、[ADD]をクリックします。それ以外の場合は、データベース内の既存のユーザアカウントを使用できます（次の図を参照）。[next] をクリックします。

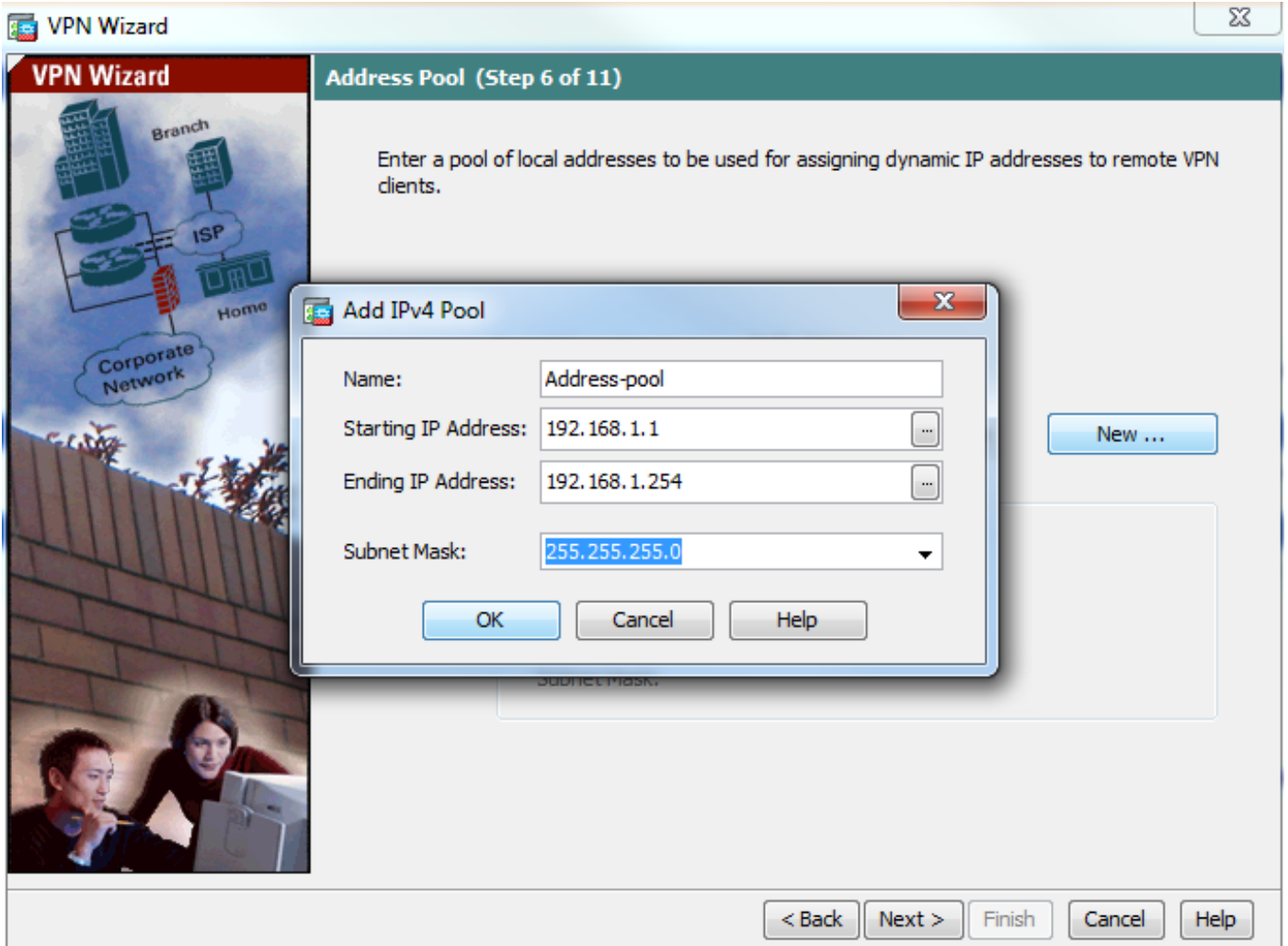


ステップ7：ドロップダウンリストから、クライアントへのIPアドレスの割り当てに使用するアドレスプールを選択します。新しいアドレスプールを作成するには、次の図に示すように[New]をクリックします。

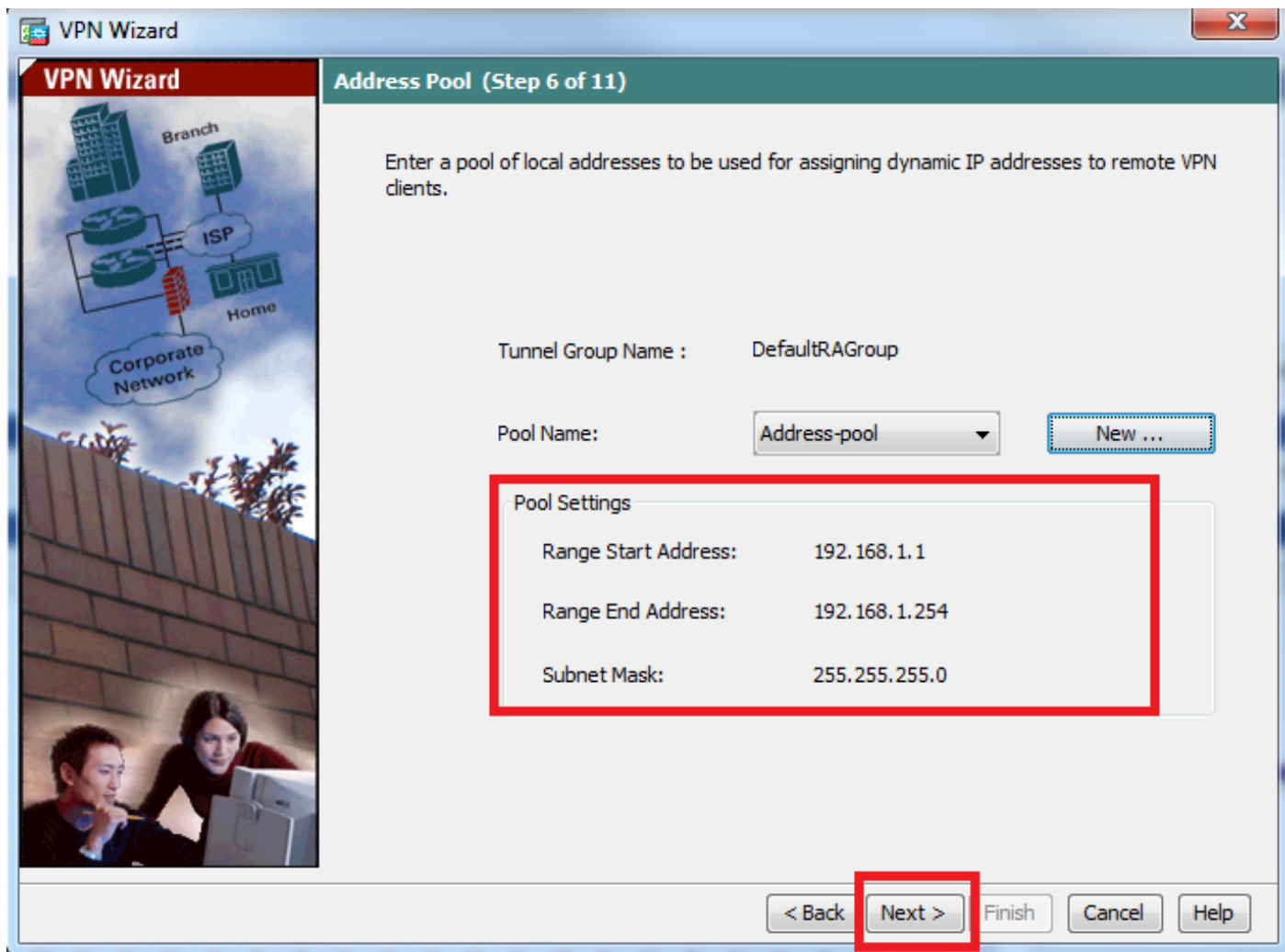


ステップ8:[Add IPv4 Pool]ダイアログボックスが表示されます。

1. 新しい IP アドレス プールの名前を入力します。
2. 最初と最後の IP アドレスを入力します。
3. サブネットマスクを入力し、 **OK**.




ステップ9 : プール設定を確認し、[Next]をクリックします。



ステップ10 : クライアントにプッシュする属性を設定するか、空のままにして[Next]をクリックします。

VPN Wizard

VPN Wizard



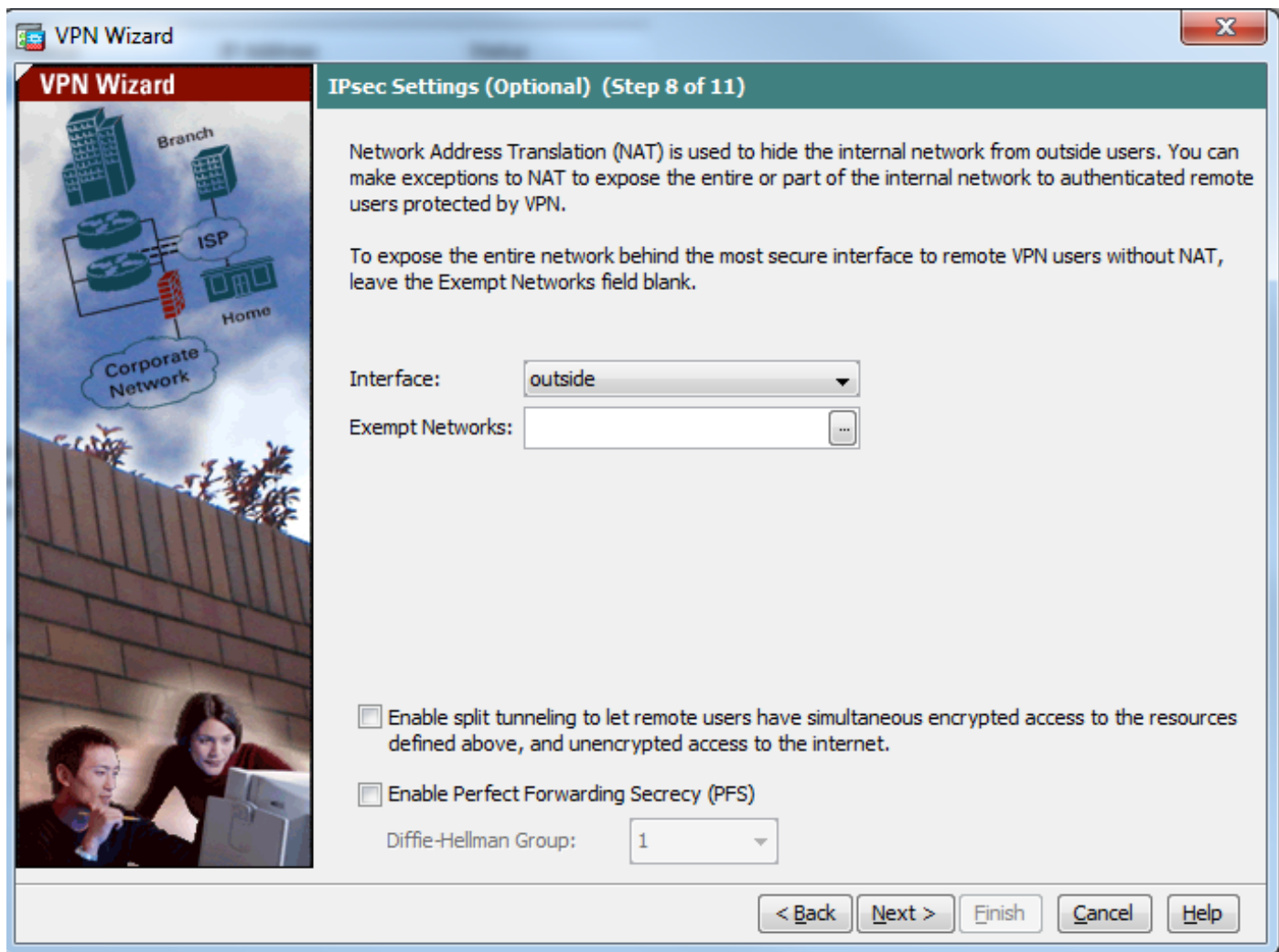
Attributes Pushed to Client (Optional) (Step 7 of 11)

Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.

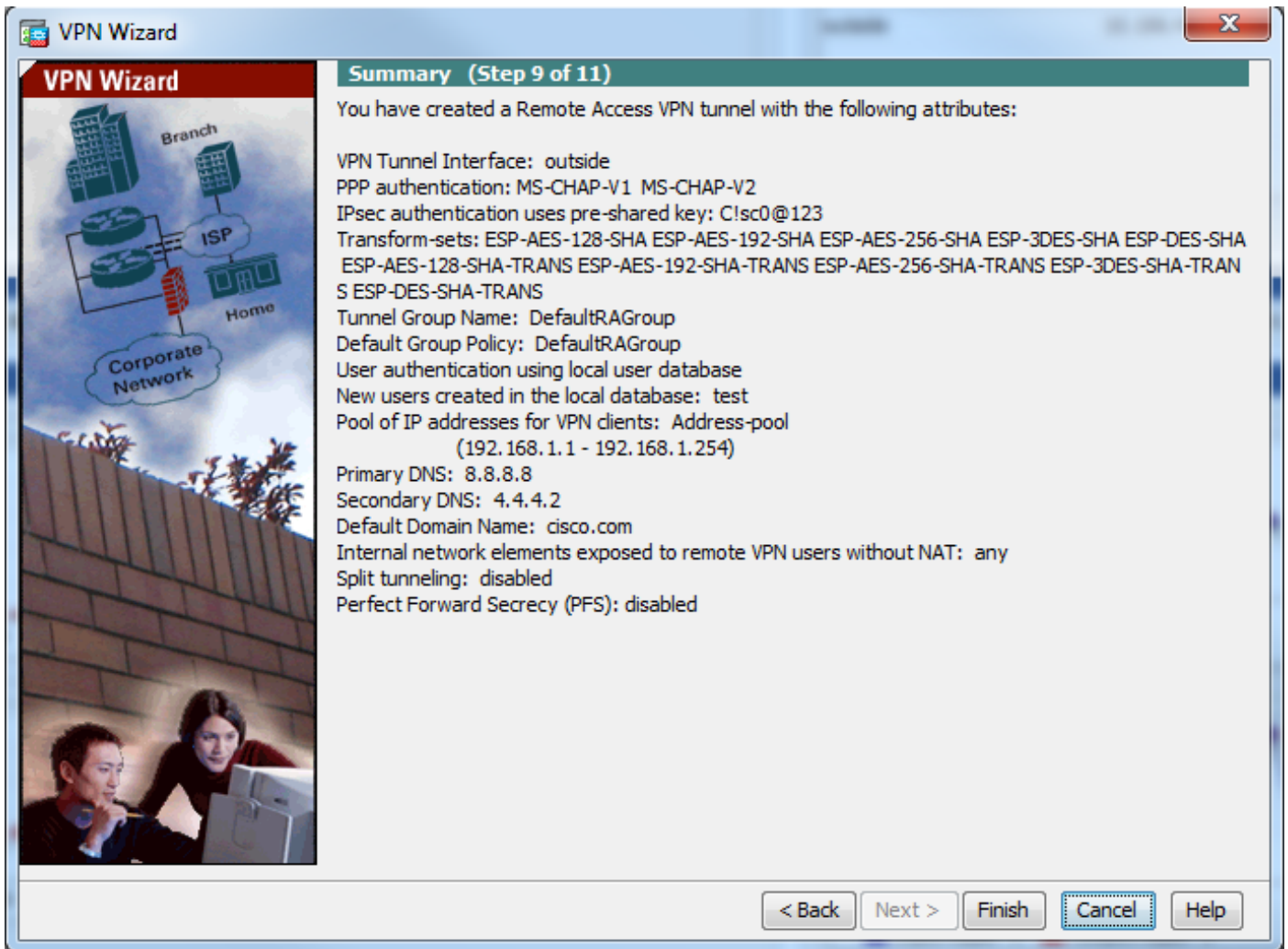
Tunnel Group:	DefaultRAGroup
Primary DNS Server:	<input type="text" value="8.8.8.8"/>
Secondary DNS Server:	<input type="text" value="4.4.4.2"/>
Primary WINS Server:	<input type="text"/>
Secondary WINS Server:	<input type="text"/>
Default Domain Name:	<input type="text" value="cisco.com"/>

< Back Next > Finish Cancel Help

ステップ 11：一部のクライアント・プラットフォームでこの機能がサポートされていないため、[Enable Perfect Forwarding Secrecy (PFS)]ボックスがオフになっていることを確認します。スプリットトンネリングを有効にすると、リモートユーザが上記で定義したリソースに同時に暗号化アクセスでき、インターネットボックスへの暗号化されていないアクセスはオフです。これは、クライアントマシンからのすべてのトラフィック（インターネットトラフィックを含む）がASAに送信されます。[next] をクリックします。



ステップ12 : サマリー情報を確認し、[完了]をクリックします。



CLIを使用したASAの設定

ステップ1: IKEフェーズ1ポリシーパラメータを設定します。

このポリシーは、ピア間の制御トラフィックを保護するために使用されます (つまり、事前共有キーとフェーズ2ネゴシエーションを保護します)

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

ステップ2: トランスフォームセットを設定します。

データトラフィックを保護するために使用されるIKEフェーズ2ポリシーパラメータが含まれています。Windows L2TP/IPsecクライアントはIPsecトランスポートモードを使用するため、モードをtransportに設定します。デフォルトはトンネルモードです

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

ステップ3: ダイナミックマップを設定します。

WindowsクライアントがISPまたはローカルDHCPサーバ (モデムなど) の前にダイナミックIPア

ドレスを取得すると、ASAはピアのIPアドレスを認識しないため、ASA側のスタティックピアの設定に問題が生じます。そのため、ダイナミッククリプト設定にアプローチする必要があります。クライアントからのIPSecネゴシエーションの結果として、すべてのパラメータが必ずしも定義されず、欠落しているパラメータが後で動的に学習されます。

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA
```

ステップ4: ダイナミックマップをスタティック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IKEv1を有効にします

ダイナミック暗号マップはインターフェイスに適用できないため、スタティック暗号マップにバインドします。ASAが最初に他の暗号マップを評価できるように、ダイナミック暗号セットは、暗号マップセット内で最も低い優先順位の暗号マップである必要があります (つまり、最も高いシーケンス番号が必要です)。他の (スタティック) マップエントリが一致しない場合にのみ、ダイナミッククリプトマップセットが検査されます。

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

ステップ5: IPアドレスプールの作成

IPアドレスがリモートVPNクライアントに動的に割り当てられるアドレスのプールを作成します。ASAで既存のプールを使用するには、この手順を無視します。

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

ステップ6: グループポリシーの設定

グループポリシーを内部として識別します。つまり、属性がローカルデータベースから取得されます。

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

注: L2TP/IPsec接続は、デフォルトのグループポリシー(DfltGrpPolicy)またはユーザ定義のグループポリシーで設定できます。どちらの場合も、L2TP/IPsecトンネリングプロトコルを使用するようにグループポリシーを設定する必要があります。デフォルトのグループポリシーのVPNプロトコル属性にl2tp-ipsecを設定します。このグループポリシーは、vpn-protocol属性が設定されていない場合、ユーザ定義のグループポリシーに継承されます。

vpn tunnel protocol(vpn tunnel protocol) (この例ではl2tp-ipsec)、ドメイン名、DNSおよびWINSサーバのIPアドレス、および新しいユーザアカウントなどの属性を設定します

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

AAAの使用に加えて、デバイスのユーザ名とパスワードを設定します。ユーザがMicrosoft CHAPバージョン1またはバージョン2を使用するL2TPクライアントであり、ASAがローカルデータベースに対して認証するように設定されている場合は、mschapキーワードを含める必要があります。たとえば、username <username> password <password> mschap。

```
ciscoasa(config-group-policy)# username test password test mschap
```


ステップ7:tunnel-groupの設定

tunnel-groupコマンドを使用してトンネルグループを作成し、IPアドレスをクライアントに割り当てるために使用するローカルアドレスプール名を指定します。認証方式が事前共有キーの場合、トンネルグループ名はDefaultRAGroupである必要があります。これは、クライアントにトンネルグループを指定するオプションがなく、デフォルトのトンネルグループのみに到達するためです。default-group-policyコマンドを使用して、グループポリシーをトンネルグループにバインドします

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

注：事前共有キーベースの認証が実行される場合は、デフォルトの接続プロファイル（トンネルグループ）、DefaultRAGroupを設定する必要があります。証明書ベースの認証を実行すると、証明書の識別子に基づいてユーザ定義接続プロファイルを選択できます

tunnel-group ipsec-attributesコマンドを使用して、事前共有キーを設定するためにipsec-attributeコンフィギュレーションモードに入ります。

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

tunnel group ppp-attributesモードから**authentication type**コマンドを使用して、PPP認証プロトコルを設定します。AAAサーバがローカルデータベースとして設定されている場合、CHAPはサポートされないため、デフォルトで有効になっているCHAPを無効にします。

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

ステップ8:NAT免除の設定

クライアントが内部インターフェイスに接続された内部リソースにアクセスできるように、NAT免除を設定します（この例では、内部リソースは内部インターフェイスに接続されています）。

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup
```

完全な設定例

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

```
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

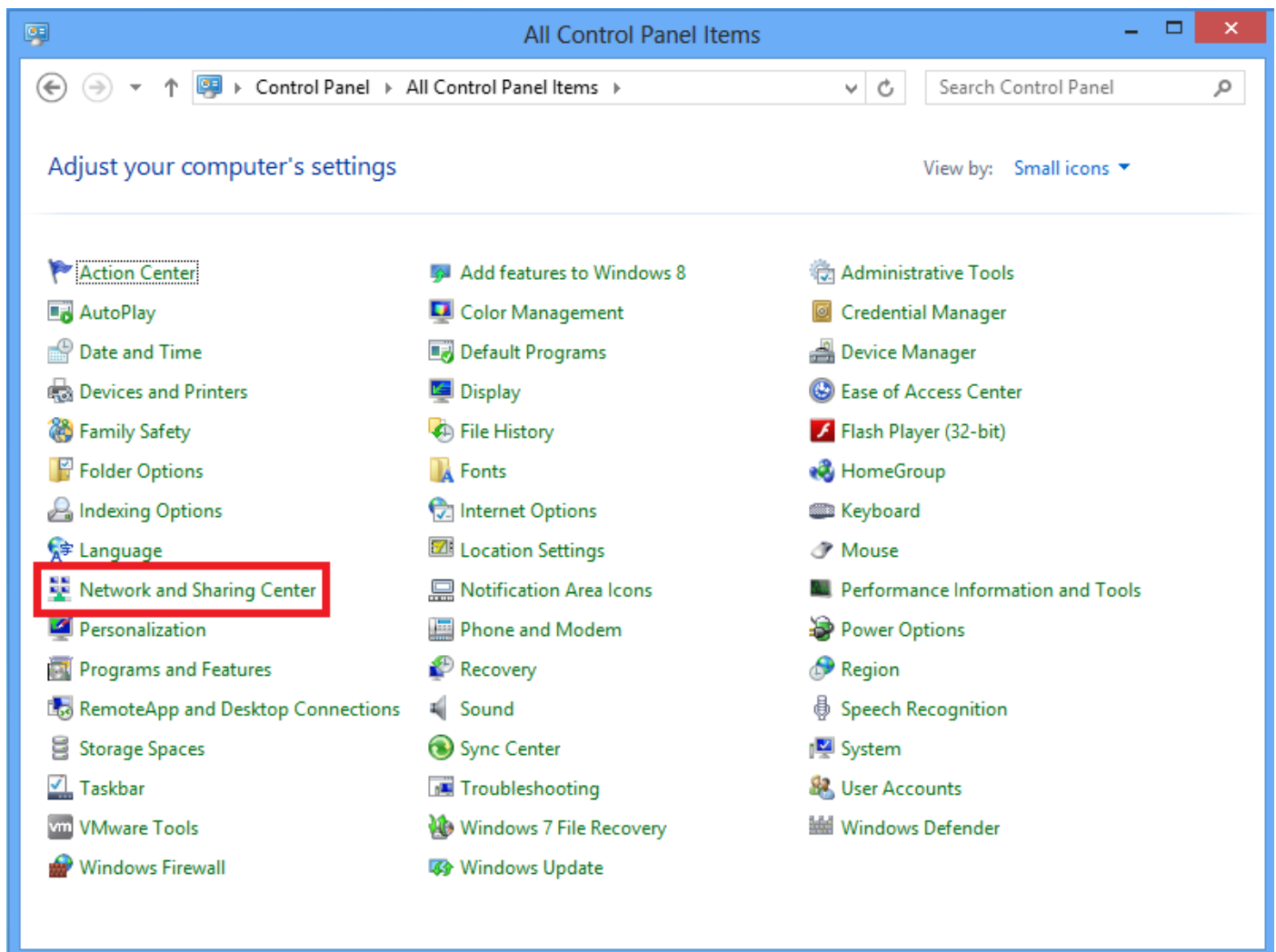
tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

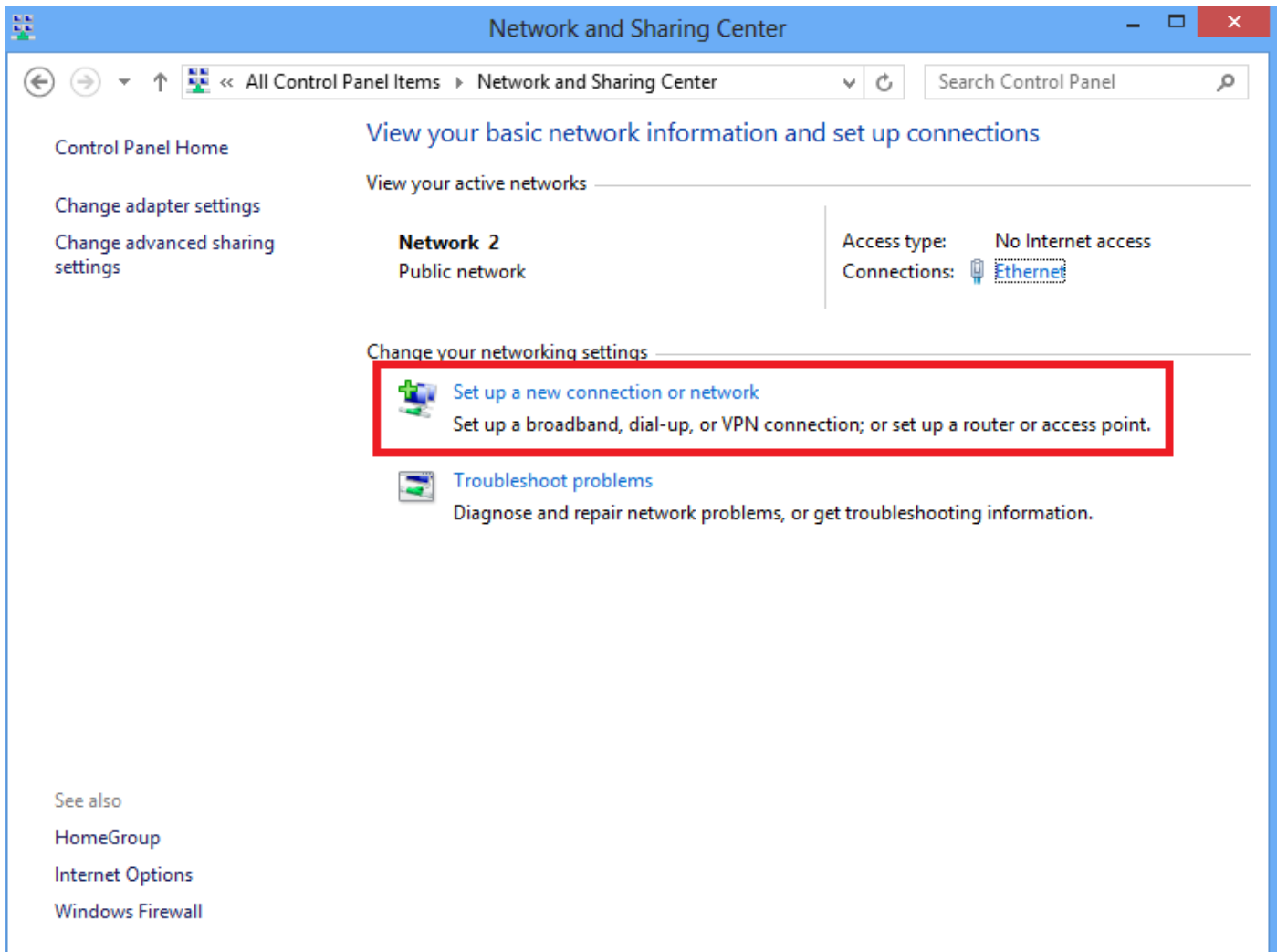
object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

Windows 8 L2TP/IPsecクライアントの設定

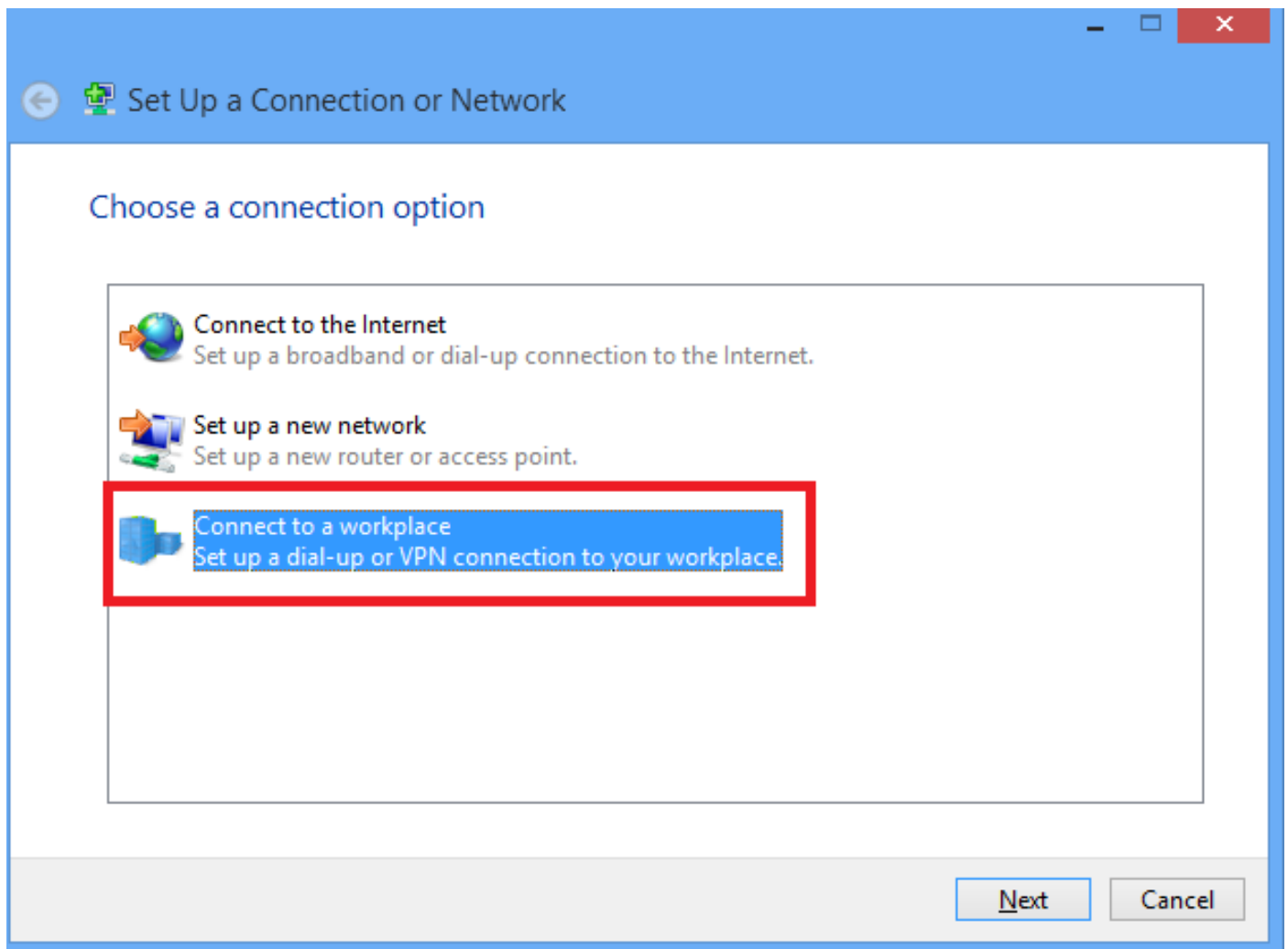
1.コントロールパネルを開き、[ネットワークと共有センター]を選択します。



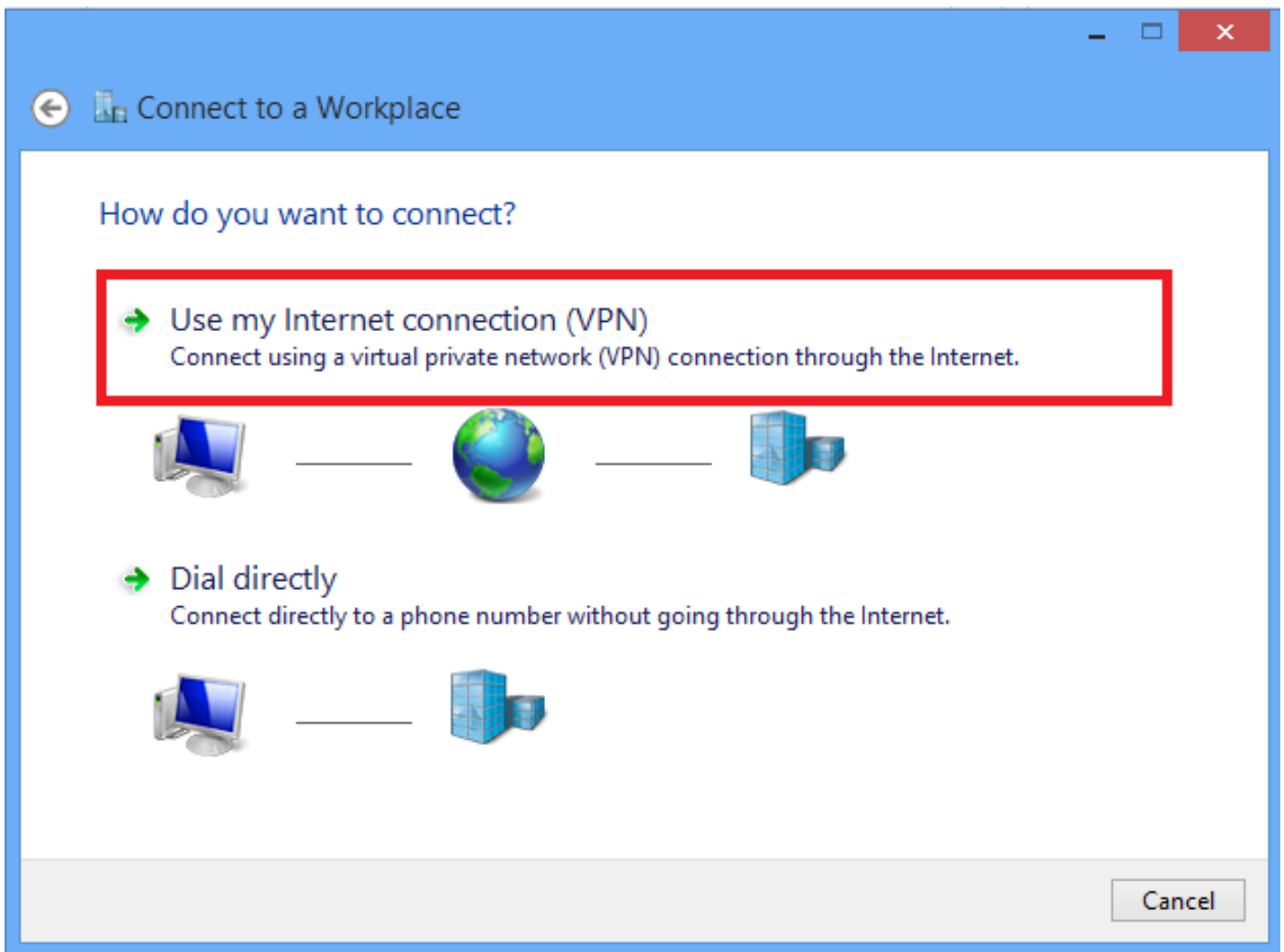
2. [新しい接続またはネットワークの設定]オプションを選択します。



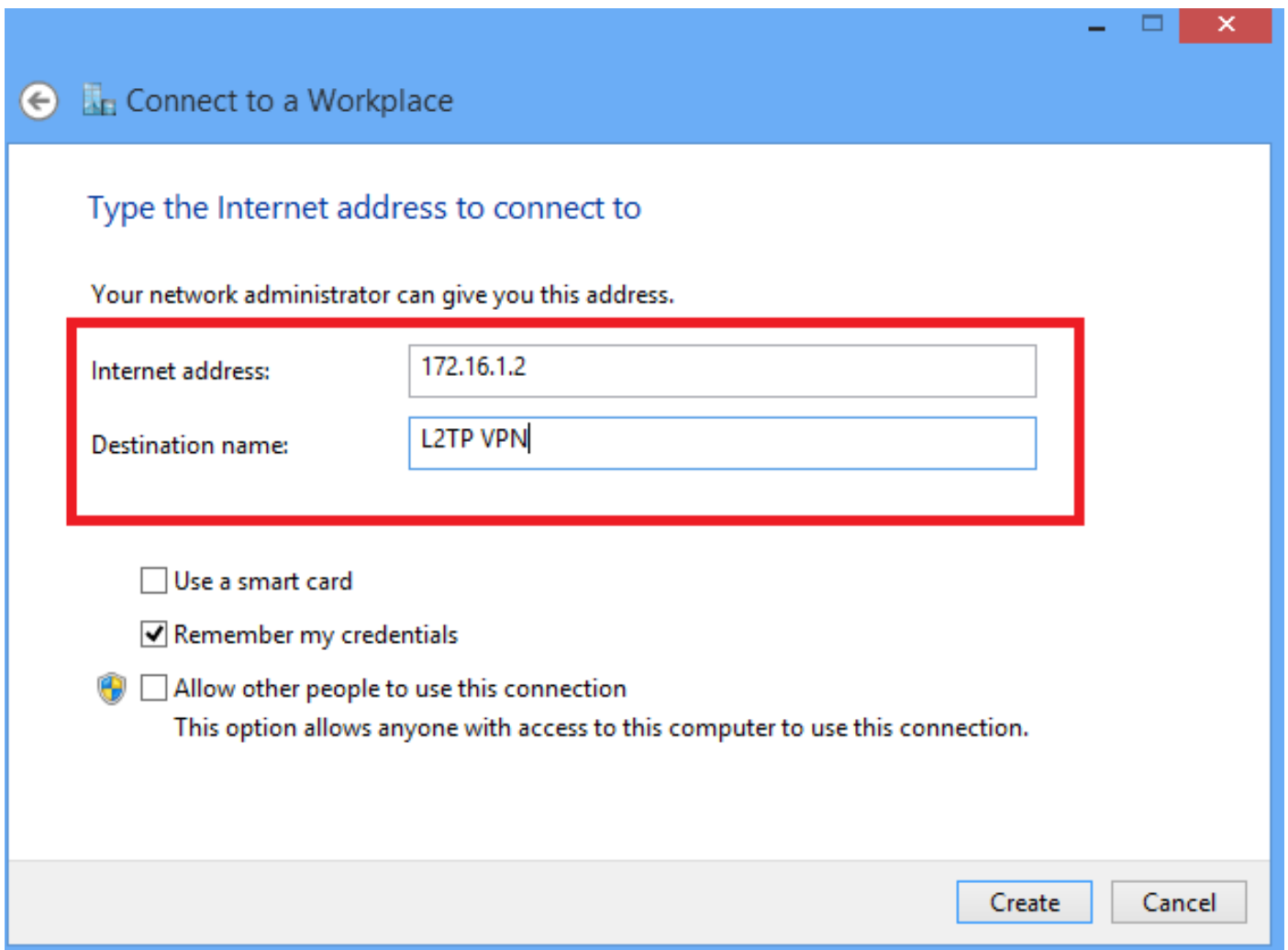
3. 「ワークプレイスに接続」オプションを選択し、「次へ」をクリックします。



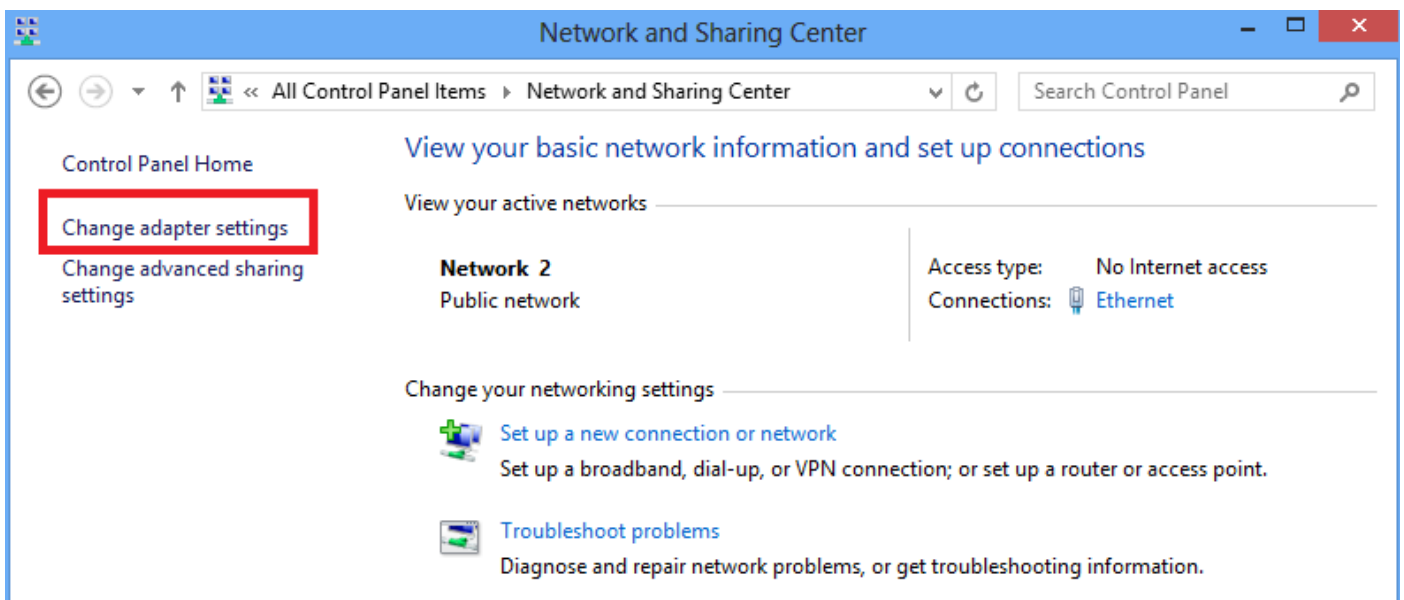
4. [Use my Internet connection (VPN)]オプションをクリックします。



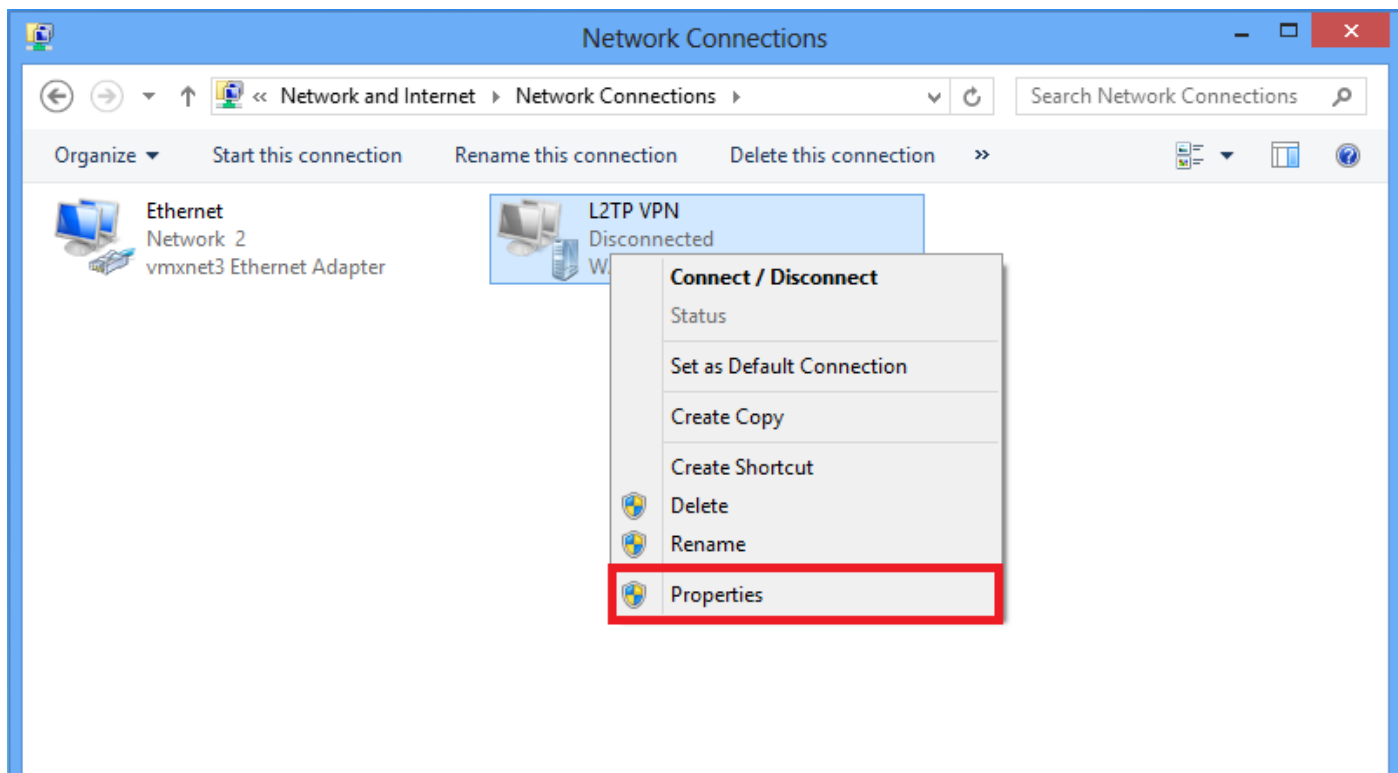
5. ASAのWANインターフェイスまたはFQDNのIPアドレスと、ローカルで有効なVPNアダプタの任意の名前を入力し、[Create]をクリックします。



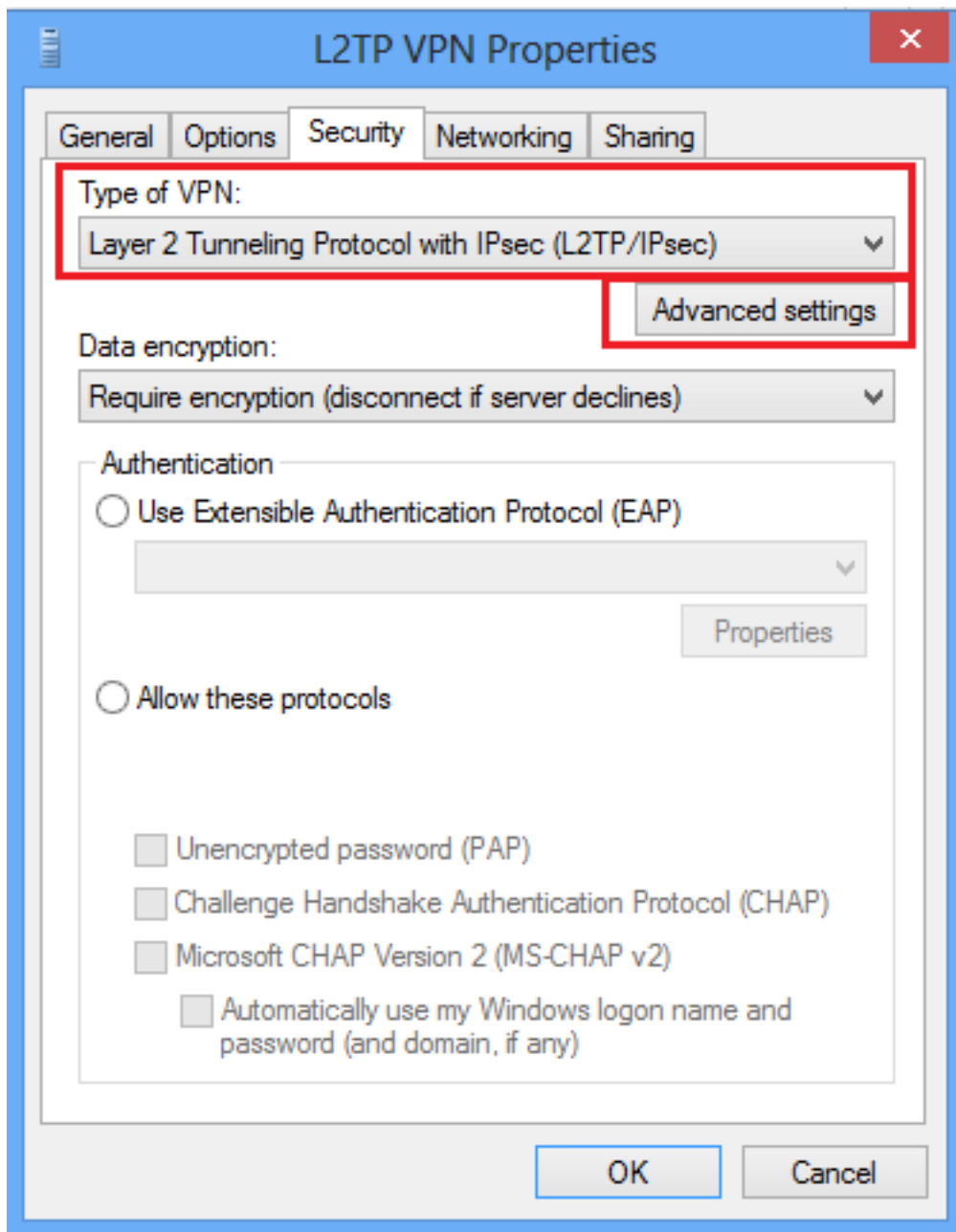
6. [ネットワークと共有センター]で、ウィンドウの左ペインにある[アダプタ設定の変更]オプションを選択します。



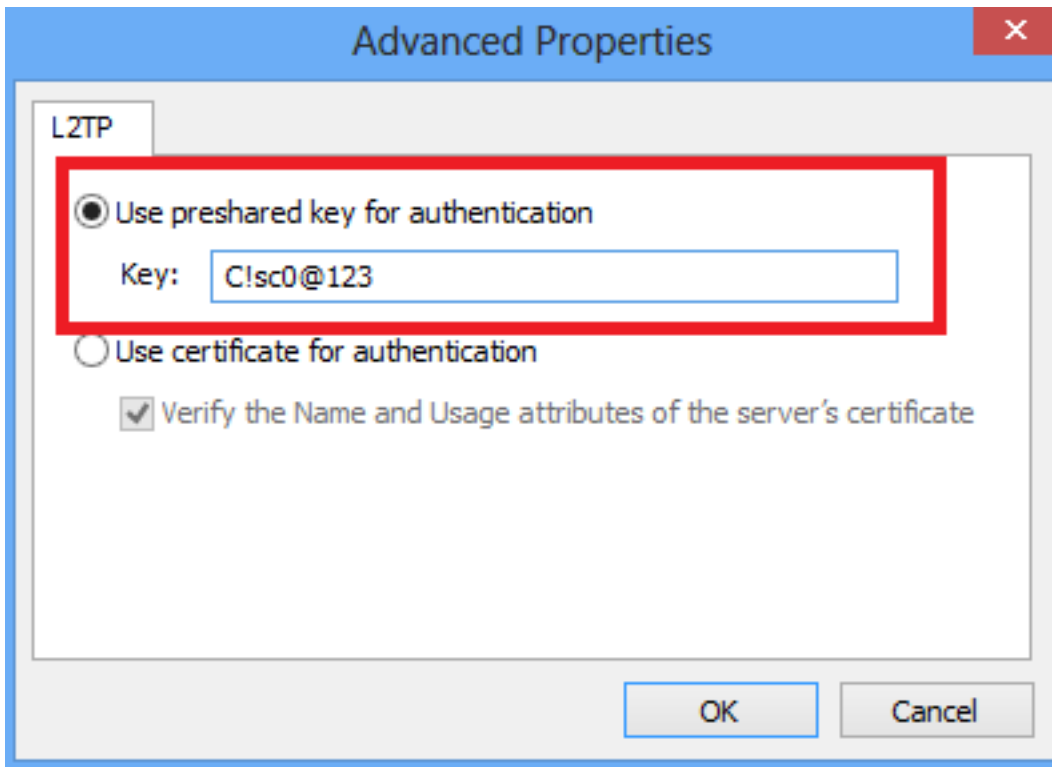
7. L2TP VPN用に最近作成したアダプタを右クリックし、[Properties]を選択します。



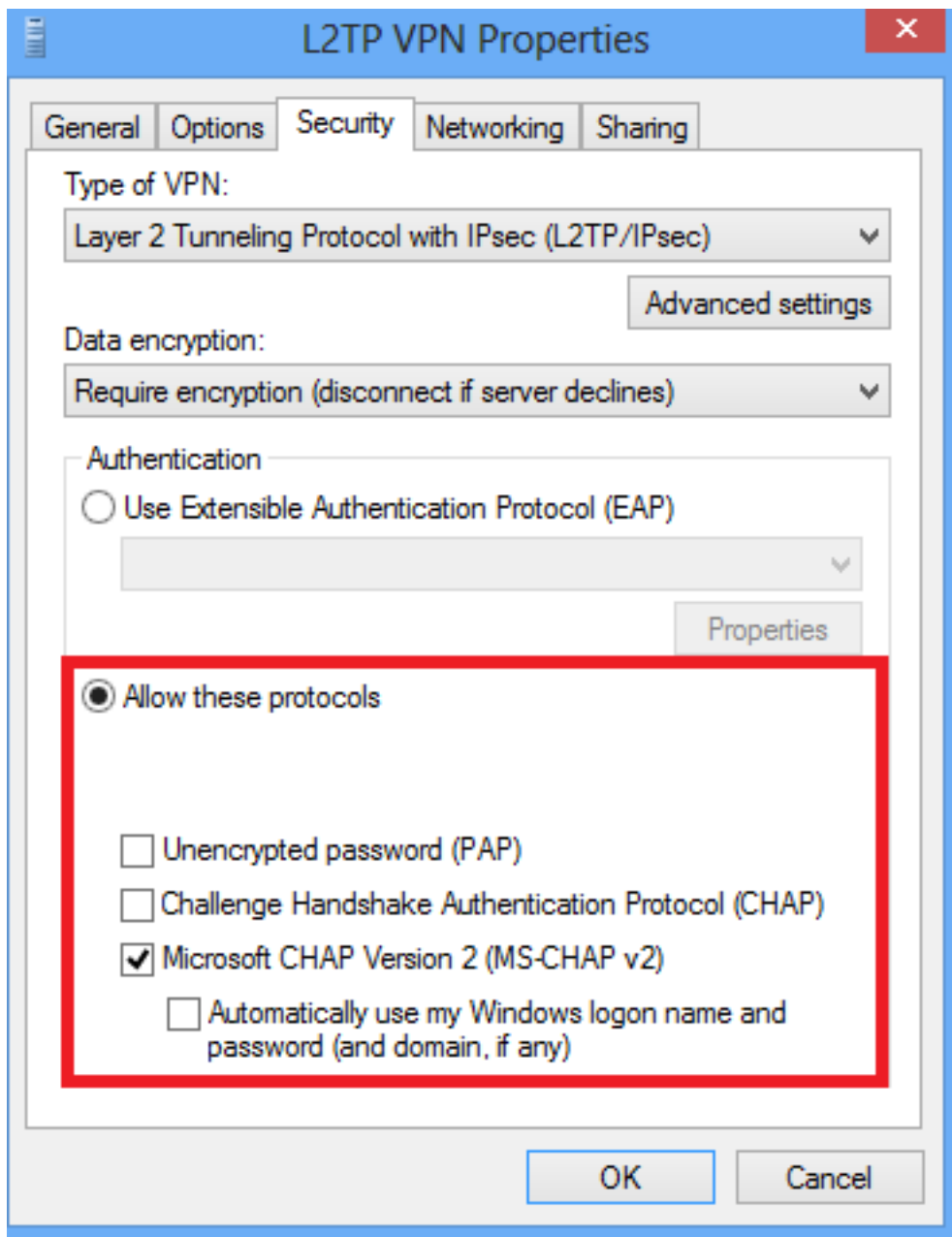
8. [Security] タブに移動し、[Type of VPN]で[Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)]を選択して、[Advanced settings]をクリックします。



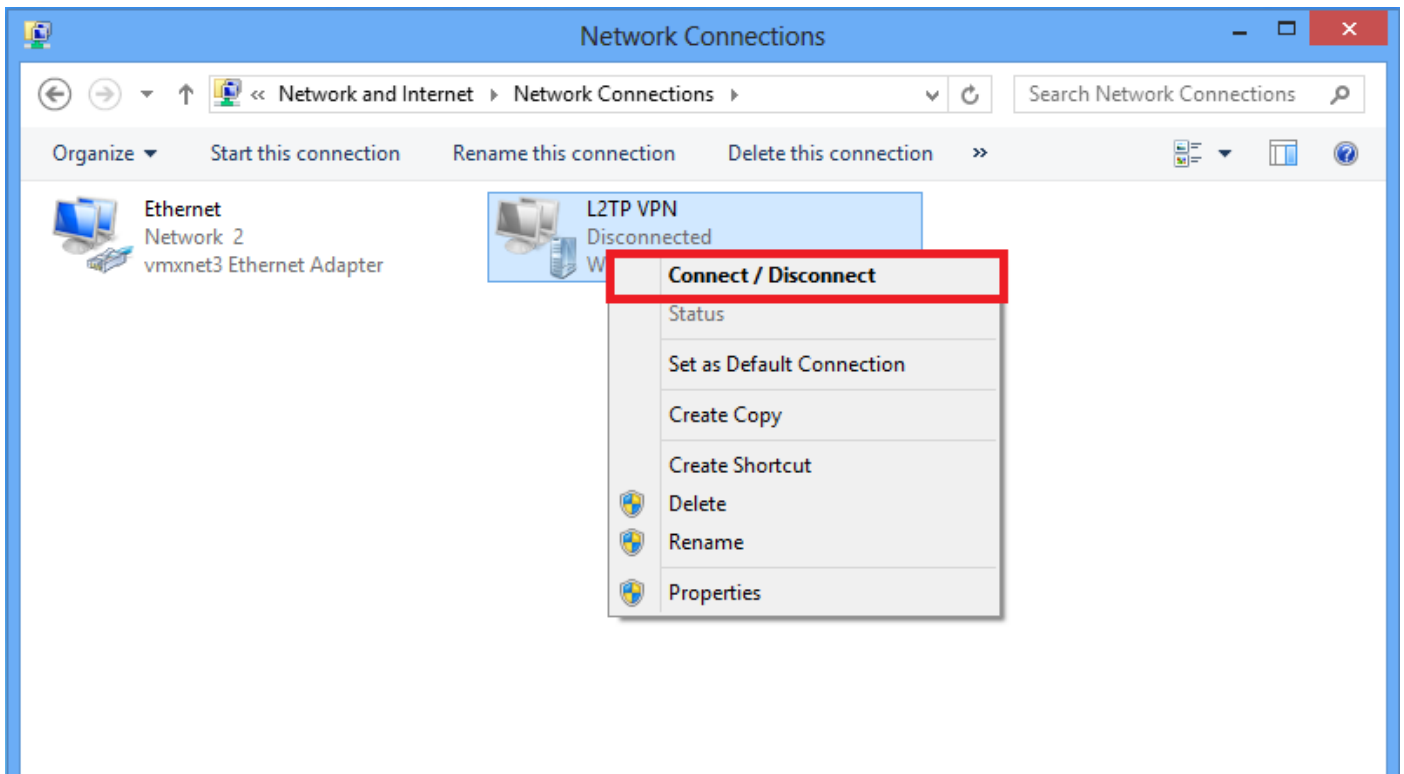
9. tunnel-group **DefaultRAGroup**で指定した事前共有キーを入力し、[OK]をクリックします。この例では、事前共有キーとしてC!sc0@123が使用されています。



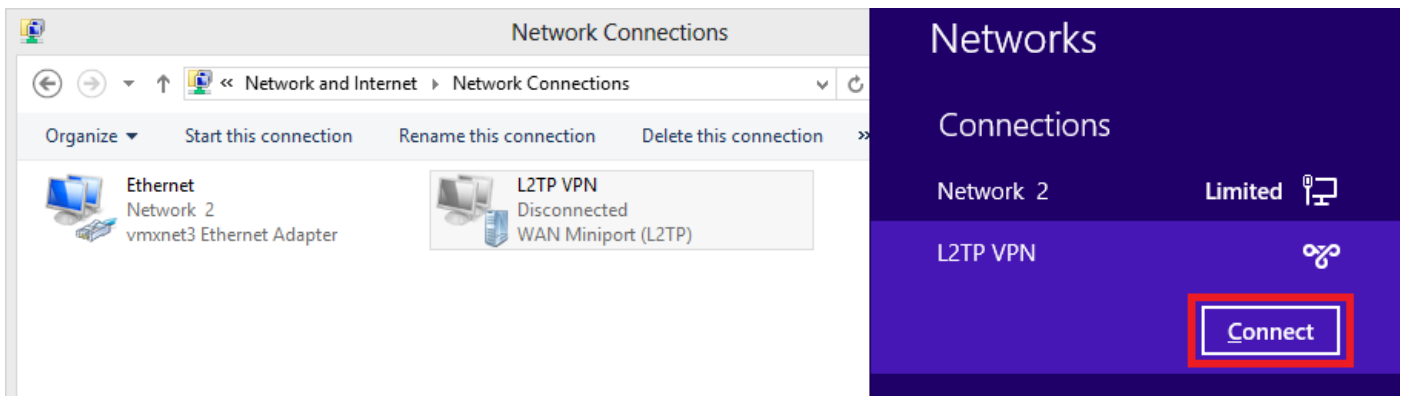
10. [Allow these protocols]で認証方式を選択し、[Microsoft CHAP Version 2 (MS-CHAP v2)]チェックボックスだけがオンになっていることを確認し、[OK]をクリックします。



11. [Network Connections]で、[L2TP VPN adapter]を右クリックし、[Connect/Disconnect]を選択します。



12. [Networks]アイコンがポップアップし、[L2TP VPN connection]をクリックします。



13.ユーザーの資格証明を入力し、「OK」をクリックします。

← Networks

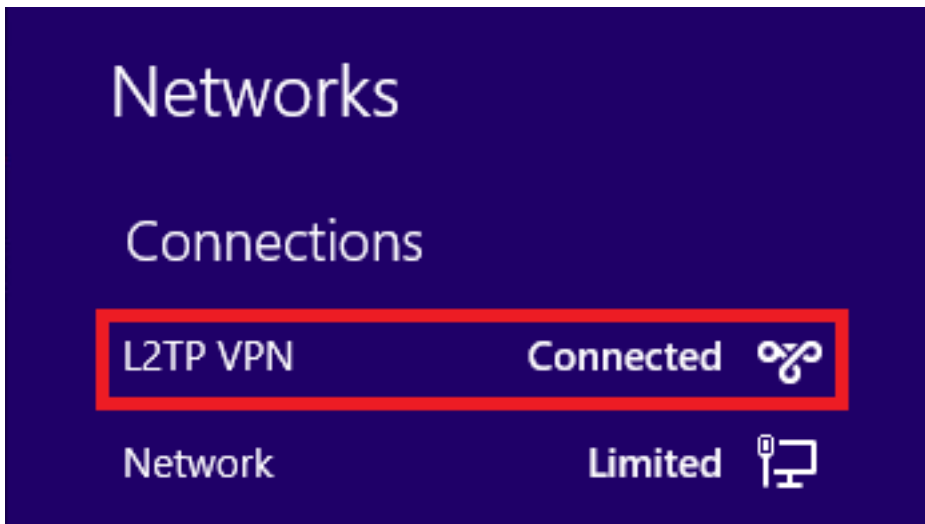
Connecting to 172.16.1.2

Network Authentication



Domain:

必要なパラメータが両端で一致すると、L2TP/IPsec接続が確立されます。



Split-tunnel 設定

スプリットトンネリングは、暗号化する必要があるサブネットまたはホストのトラフィックを定義するために使用できる機能です。これには、この機能に関連付けられたアクセスコントロールリスト(ACL)の設定が含まれます。このACLで定義されたサブネットまたはホストのトラフィックは、クライアントエンドからのトンネルを介して暗号化され、これらのサブネットのルートがPCルーティングテーブルにインストールされます。ASAはクライアントからのDHCPINFORMメッセージを代行受信し、サブネットマスク、ドメイン名、クラスレススタティックルートで応答します。

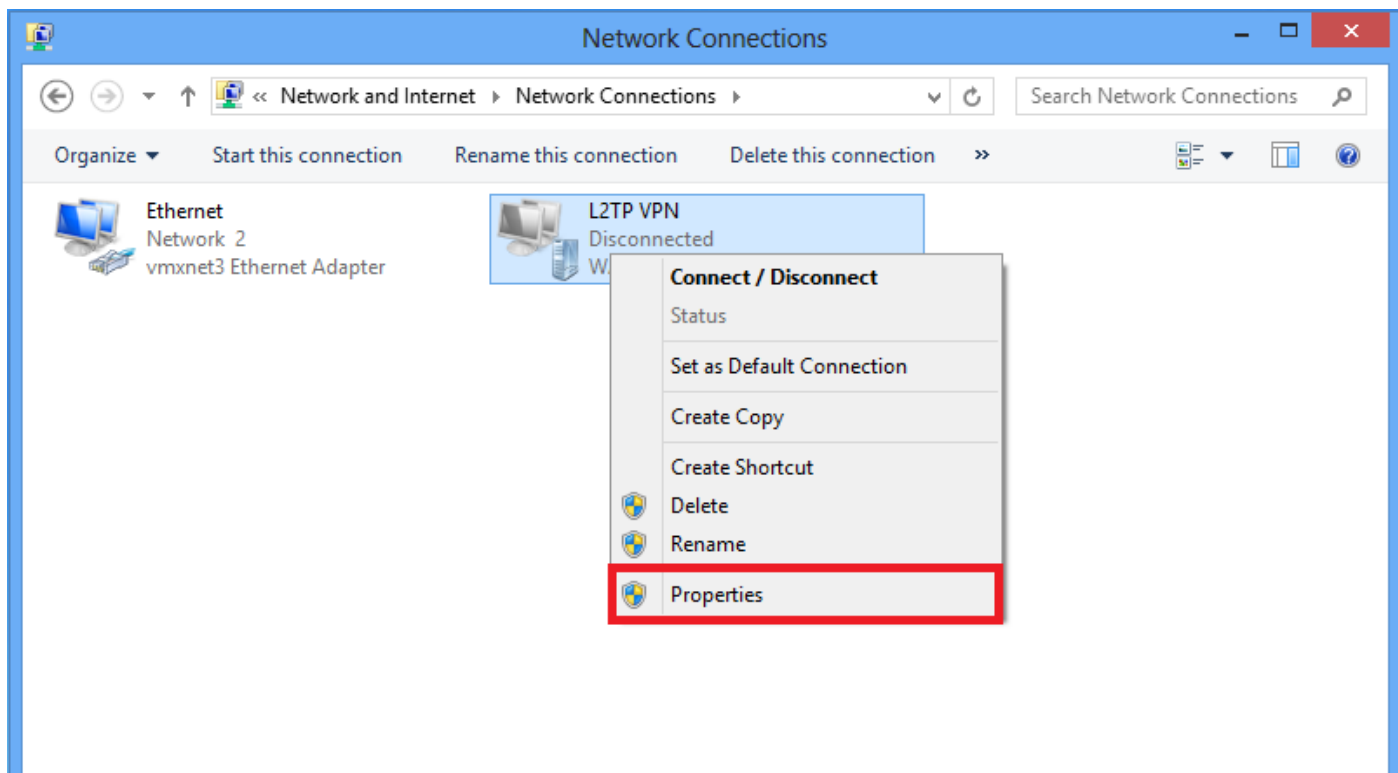
ASAでの設定

```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0
```

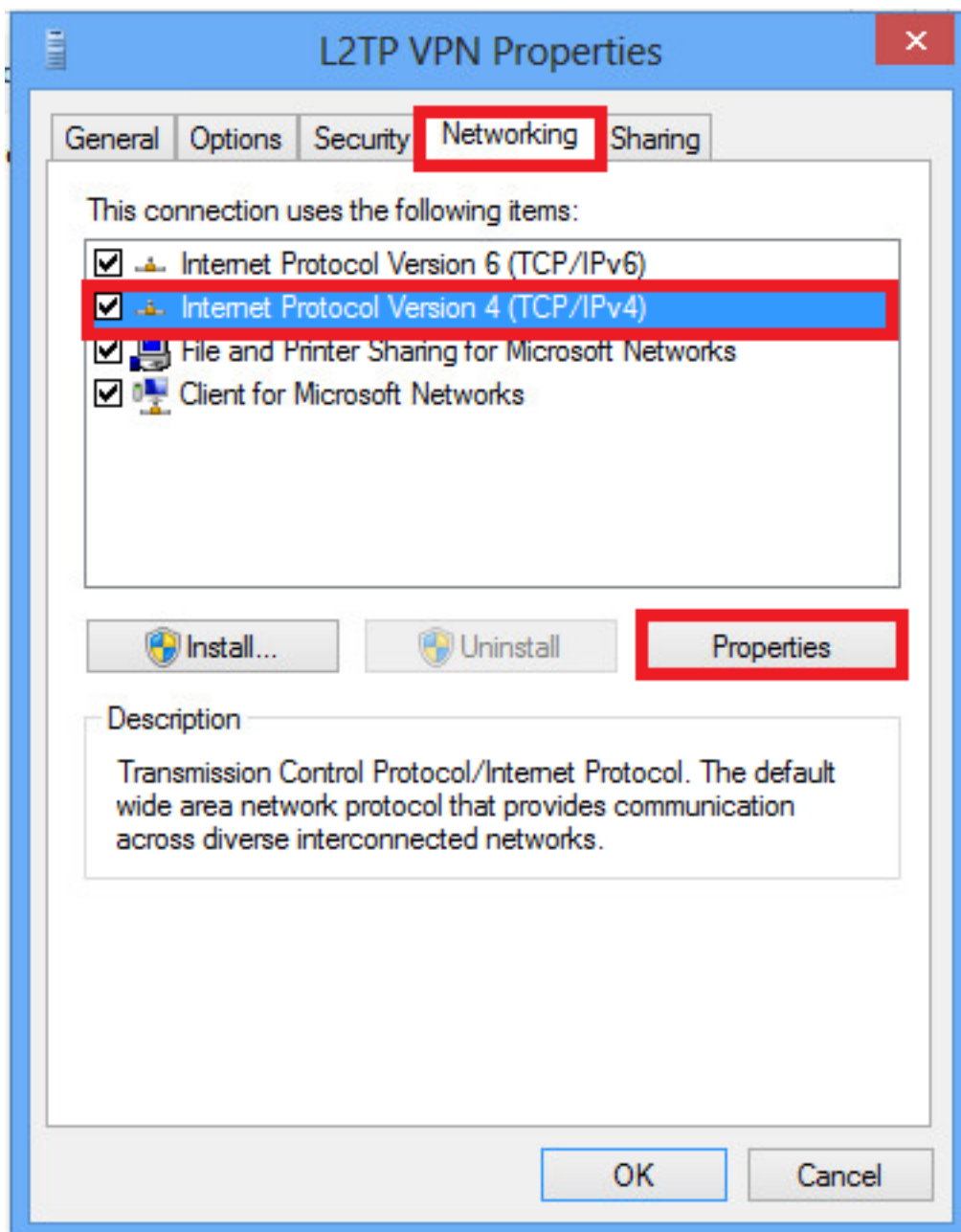
```
ciscoasa(config)# group-policy DefaultRAGroup attributes  
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified  
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT  
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

L2TP/IPsecクライアントの設定

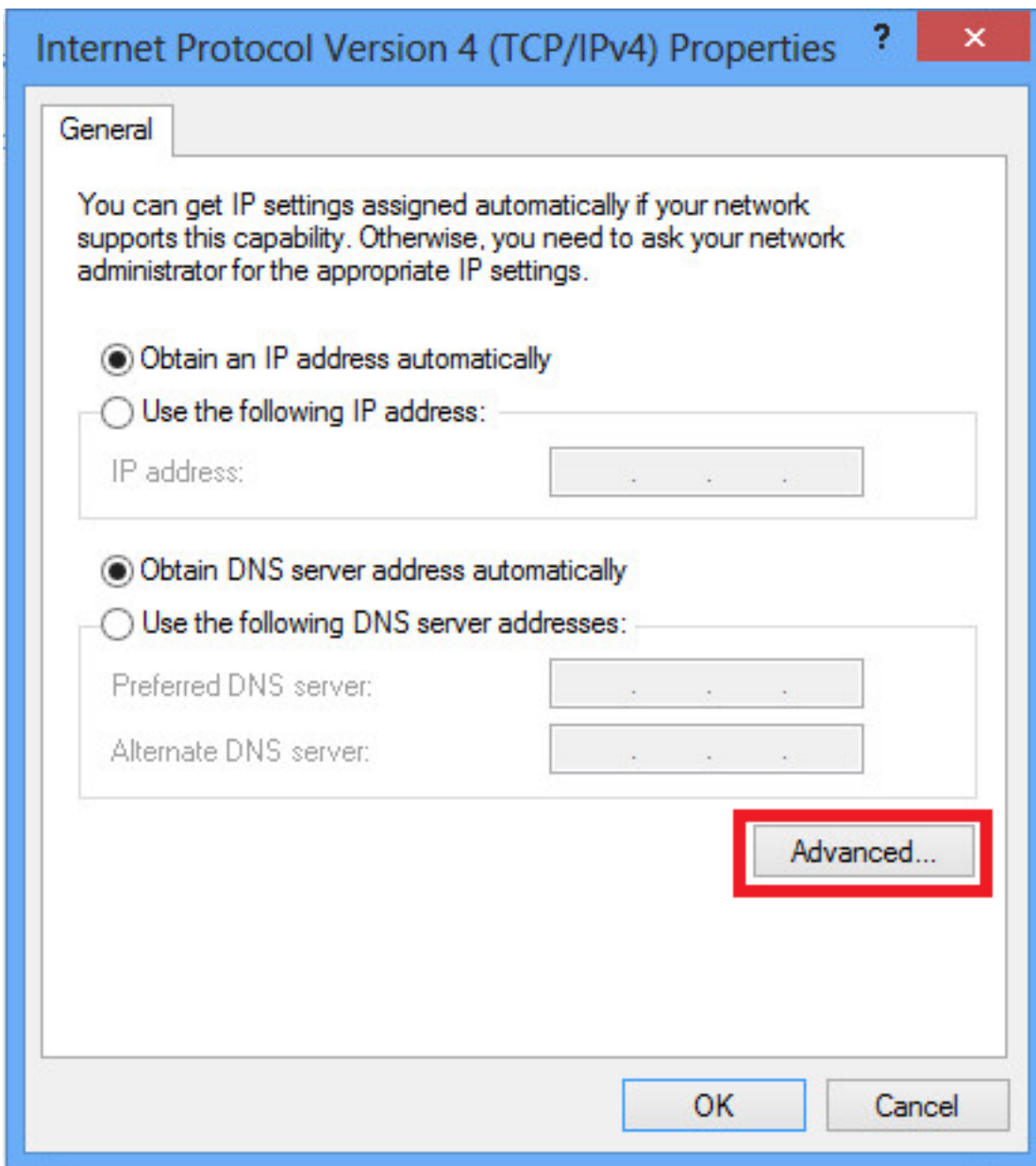
1. L2TP VPNアダプタを右クリックし、[Properties]を選択します。



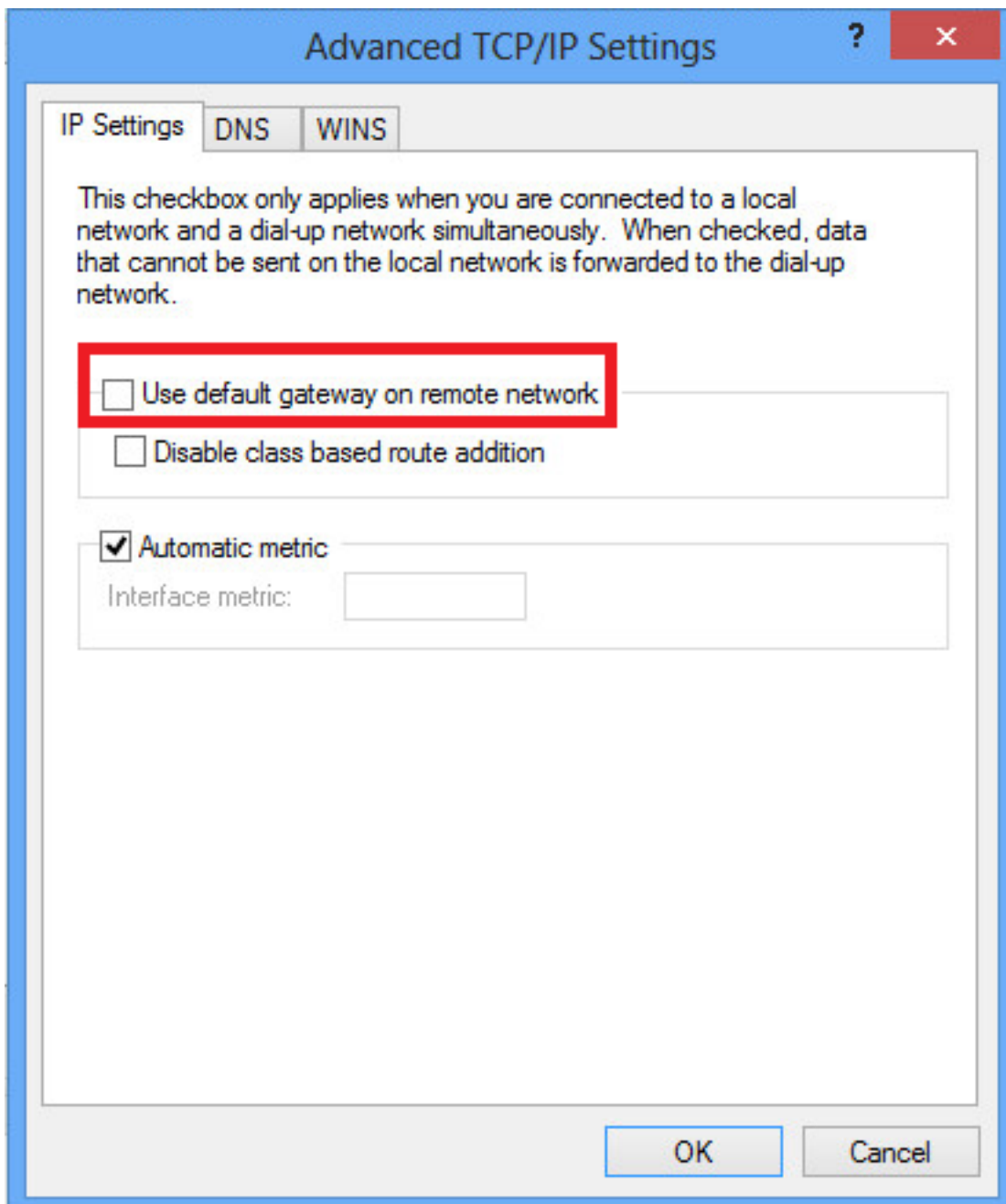
2. [Networking]タブに移動し、[Internet Protocol Version 4 (TCP/IPv4)]を選択して[Properties]をクリックします。



3. 「詳細」 オプションをクリックします。



4. [Use default gateway on remote network]オプションのチェックを外し、[OK]をクリックします。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

注：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 ikev1 sa` : ピアにおける現在のIKE SAをすべて表示します。

```
ciscoasa# show crypto ikev1 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:

10.1.1.2

Type : user Role : responder
Rekey : no

State : MM_ACTIVE

- show crypto ipsec sa : 現在ピアにあるすべての IPsec SA を表示します。

```
ciscoasa# show crypto ipsec sa
interface: outside
Crypto map tag:
```

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)
remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-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.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
path mtu 1500, ipsec overhead 58(36), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: E8AF927A
current inbound spi : 71F346AB
```

```
inbound esp sas:
spi: 0x71F346AB (1911768747)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000003
```

```
outbound esp sas:
spi: 0xE8AF927A (3903820410)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

- show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec - L2TP over IPsec接続の詳細情報を表示します。

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec
```

Session Type: IKEv1 IPsec Detailed

Username : test

Index : 1

Assigned IP : 192.168.1.1 Public IP : 10.1.1.2

```
Protocol : IKEv1 IPsec L2TPOverIPsec
License : Other VPN
Encryption : IKEv1: (1)3DES IPsec: (1)3DES L2TPOverIPsec: (1)none
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1 L2TPOverIPsec: (1)none
Bytes Tx : 1574                                      Bytes Rx : 12752
Pkts Tx : 29                                              Pkts Rx : 118
Pkts Tx Drop : 0                                      Pkts Rx Drop : 0
```

Group Policy : L2TP-VPN Tunnel Group : DefaultRAGroup

Login Time : 23:32:48 UTC Sat May 16 2015

Duration : 0h:04m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1

IKEv1:

Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Main Auth Mode : preSharedKeys
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 28800 Seconds Rekey Left(T): 28555 Seconds
D/H Group : 2
Filter Name :

IPsec:

Tunnel ID : 1.2
Local Addr : 172.16.1.2/255.255.255.255/17/1701
Remote Addr : 10.1.1.2/255.255.255.255/17/1701
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport
Rekey Int (T): 3600 Seconds Rekey Left(T): 3576 Seconds
Rekey Int (D): 250000 K-Bytes Rekey Left(D): 250000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 1574 Bytes Rx : 12752
Pkts Tx : 29 Pkts Rx : 118

L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

Assigned IP : 192.168.1.1

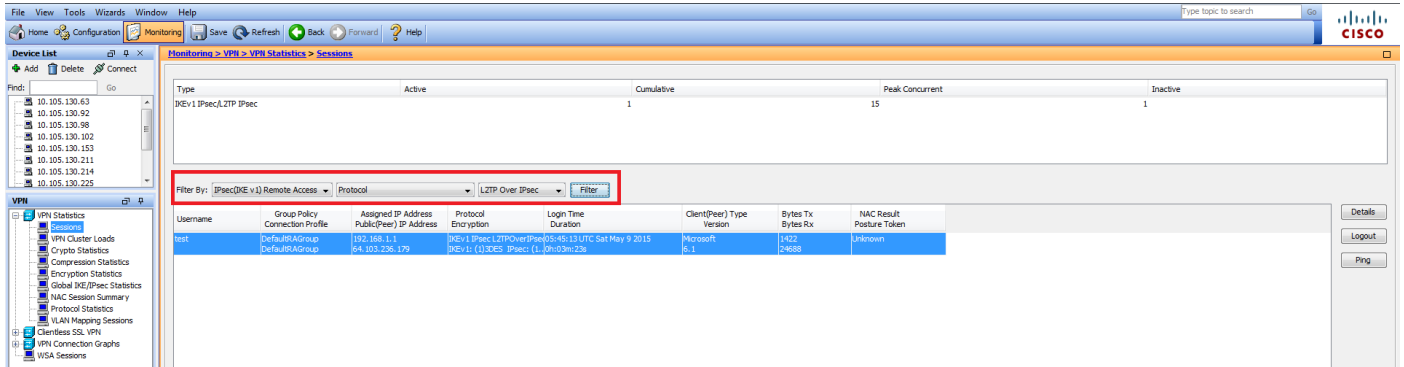
Public IP : 10.1.1.2

Encryption : none Hashing : none

Auth Mode : msCHAPV2

Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Microsoft
Client OS Ver: 6.2
Bytes Tx : 475 Bytes Rx : 9093
Pkts Tx : 18 Pkts Rx : 105

ASDMで、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]の下に、VPNセッションに関する一般情報が表示されます。L2TP over IPsecセッションは、IPsec (IKEv1) Remote Access > Protocol > L2TP Over IPsecでフィルタリングできます。



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。

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。

注意： ASA では、さまざまなデバッグレベルを設定できます。デフォルトでは、レベル1が使用されます。デバッグレベルを変更すると、デバッグの冗長性が高くなる場合があります。特に実稼働環境では、注意して変更してください。

VPNトンネルに関する問題をトラブルシューティングするには、次のdebugコマンドを注意して使用してください

- debug crypto ikev1:IKEに関するデバッグ情報を表示します
- debug crypto ipsec:IPSecに関するデバッグ情報を表示します

正常なL2TP over IPsec接続のデバッグ出力を次に示します。

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
```

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

Connection landed on tunnel_group DefaultRAGroup

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, 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
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR

+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPsec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

IPsec SA Proposal # 2, Transform # 1 acceptable

Matches global IPsec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007ffffe13ab260,
SCB: 0xE1C00540,
Direction: inbound
SPI : 0x7AD72E0D
Session ID: 0x00001000
VPIF num : 0x00000002
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:
SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constructing quick mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!

IPSEC: New embryonic SA created @ 0x00007ffffelc75c00,

SCB: 0xE13ABD20,
Direction: outbound
SPI : 0x8C14FD70
Session ID: 0x00001000
VPIF num : 0x00000002
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds

IPSEC: Completed host OBSA update, SPI 0x8C14FD70

IPSEC: Creating outbound VPN context, SPI 0x8C14FD70

Flags: 0x00000205
SA : 0x00007ffffelc75c00
SPI : 0x8C14FD70
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0AC609F9
Channel: 0x00007ffffed817200

IPSEC: Completed outbound VPN context, SPI 0x8C14FD70

VPN handle: 0x000000000000028d4

IPSEC: New outbound encrypt rule, SPI 0x8C14FD70

Src addr: 172.16.1.2
Src mask: 255.255.255.255
Dst addr: 10.1.1.2
Dst mask: 255.255.255.255

Src ports

Upper: 1701

Lower: 1701

Op : equal

Dst ports

Upper: 1701

Lower: 1701

Op : equal

Protocol: 17

```
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
Src addr: 172.16.1.2
Src mask: 255.255.255.255
Dst addr: 10.1.1.2
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: 0x8C14FD70
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007ffffel3ab260,
SCB: 0xE1C00540,
Direction: inbound
SPI       : 0x7AD72E0D
Session ID: 0x00001000
VPIF num  : 0x00000002
Tunnel type: ra
Protocol   : esp
Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
Flags: 0x00000206
SA    : 0x00007ffffel3ab260
SPI   : 0x7AD72E0D
MTU   : 0 bytes
VCID  : 0x00000000
Peer  : 0x000028D4
SCB   : 0x0AC5BD5B
Channel: 0x00007ffffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
Flags: 0x00000205
SA    : 0x00007ffffelc75c00
SPI   : 0x8C14FD70
MTU   : 1500 bytes
VCID  : 0x00000000
Peer  : 0x00004174
```

SCB : 0x0AC609F9
Channel: 0x00007ffffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
Dst mask: 255.255.255.255
Src ports
Upper: 1701
Lower: 1701
Op : equal
Dst ports
Upper: 1701
Lower: 1701
Op : equal
Protocol: 17
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
Rule ID: 0x00007ffffel3aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
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: 0x7AD72E0D
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
Rule ID: 0x00007ffffelc77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
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: 0x7AD72E0D
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D

```
Rule ID: 0x00007ffffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

```
(msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

Windowsクライアントで一般的に発生するVPN関連のエラーの一部を次の表に示します

エラー
コード

考えられる解決策

691	入力したユーザ名とパスワードが正しいことを確認します
789,835	クライアントマシンに設定されている事前共有キーがASAと同じであることを確認します
800	1. VPNタイプが[Layer 2 Tunneling Protocol (L2TP)]に設定されていることを確認します 2. 事前共有キーが正しく設定されていることを確認します
809	UDPポート500、4500 (クライアントまたはサーバのいずれかがNATデバイスの背後にある場合)

関連情報

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [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](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)