

事前共有鍵を使用した Windows 2000/XP PC と PIX/ASA 7.2 の間の L2TP Over IPSec 設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[Windows L2TP/IPSec クライアント設定](#)

[PIX での L2TP サーバの設定](#)

[ASDM を使用した L2TP の設定](#)

[IAS がインストールされた Microsoft Windows 2003 サーバの設定](#)

[アクティブ ディレクトリを使用した L2TP Over IPSec のための拡張認証](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[デバッグの出力例](#)

[ASDM を使用したトラブルシューティング](#)

[問題： 頻繁な切断](#)

[Windows Vista の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、事前共有鍵を使用して、リモートの Microsoft Windows 2000/2003 および XP のクライアントから PIX セキュリティ アプライアンスの企業オフィスへ、Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) over IPSec を設定する方法について説明しています。また、ユーザ認証には Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server を使用しています。参照して下さい [Microsoft -チェックリスト: ダイアル式および VPN のための IAS の設定](#) IAS のさらに詳しい詳細については [アクセスして下さい](#)。

リモート アクセスのシナリオで IP セキュリティによる L2TP を設定する主な利点は、リモート ユーザがゲートウェイや専用線を使用せずにパブリック IP ネットワークから VPN へアクセスできることです。これにより、POTS (一般電話サービス) があれば、実質的にどの場所からもリ

リモート アクセスが可能になります。もう 1 つの利点は、VPN アクセスでのクライアント側の要件が、Windows 2000 と Microsoft Dial-Up Networking (DUN; ダイアルアップ ネットワーク) を使用する点だけであることです。Cisco VPN Client ソフトウェアなどの、追加のクライアント ソフトウェアは必要ありません。

このドキュメントでは、Cisco Adaptive Security Device Manager (ASDM) を使用して、L2TP over IPsec に対応する PIX 500 シリーズ セキュリティ アプライアンスを設定する方法についても説明しています。

注: [Layer 2 Tunneling Protocol \(L2TP\) over IPsec](#) は、Cisco Secure PIX Firewall ソフトウェア リリース 6.x 以降でサポートされています。

L2TP Over IPsec を PIX 6.x と Windows 2000 との間で設定するには、『[Configuring L2TP Over IPsec Between PIX Firewall and Windows 2000 PC Using Certificates](#)』を参照してください。

暗号化方式を使用して、リモートの Microsoft Windows 2000 および XP のクライアントから企業 サイトへの L2TP over IPsec を設定するには、『[Windows 2000 またはXP のクライアントから Cisco VPN 3000 シリーズコンソントレータへの L2TP over IPsec の事前共有鍵を使用した設定](#)』を参照してください。

前提条件

要件

セキュア トンネルを確立する前に、ピア間が IP 接続されている必要があります。

接続パス上のどの場所でも、UDP ポート 1701 がブロックされていないことを確認してください。

Cisco PIX/ASA ではデフォルトのトンネル グループとデフォルトのグループ ポリシーのみを使用してください。ユーザ定義のポリシーとグループは使用できません。

注: Cisco VPN Client 3.x または Cisco VPN 3000 Client 2.5 がインストールされている場合、セキュリティ アプライアンスは Windows 2000 で L2TP/IPsec トンネルを確立しません。Windows 2000 の Services パネルで、Cisco VPN Client 3.x の Cisco VPN サービスまたは Cisco VPN 3000 クライアント 2.5 の ANetIKE サービスをディセーブルにしてください。これをするために Start > Programs > Administrative Tools > Services の順に選択し、Services パネルからの IPsec ポリシーエージェントサービスを再開し、マシンをリブートして下さい。

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くものです。

- ソフトウェア バージョン 7.2(1) 以降を搭載した PIX セキュリティ アプライアンス 515E
- Adaptive Security Device Manager 5.2(1) 以降
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional SP2
- IAS がインストールされた Windows 2003 サーバ

注: PIX 6.3 をバージョン 7.x にアップグレードする場合は、Windows XP に SP2 がインストールされていることを確認してください (L2TP クライアント) 。

注: このドキュメントの情報は、ASA セキュリティ アプライアンスにも対応しています。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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 7.2(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

L2TP over IPsec を設定するには、次の手順を実行します。

1. L2TP で IP セキュリティを有効にするため、IPsec トランスポート モードを設定します。Windows 2000 L2TP/IPsec クライアントは IPsec 転送する モードを使用します— IP ペイロードだけ暗号化され、オリジナル IP ヘッダはそのままになります。このモードの利点は、各パケットに数バイトしか追加されないことと、パブリック ネットワーク上のデバイスがパケットの最終的な発信元と宛先を確認できることです。したがって、Windows 2000 L2TP/IPsec クライアントがセキュリティ アプライアンスに接続するには、トランスフォームに IPsec トランスポート モードを設定する必要があります (「[ASDM を使用した L2TP の設定](#)」のステップ 2 を参照してください)。この機能 (トランスポート) により、IP ヘッダの情報をもとにした中間ネットワークでの特殊な処理 (たとえば QoS など) が可能になります。ただし、レイヤ 4 ヘッダが暗号化されるため、パケットの検査が制限されます。残念ながら、クリアテキストによる IP ヘッダ送信なので、トランスポート モードでは、攻撃者がなんらかのトラフィック分析を行えます。
2. Virtual Private Dial-up Network (VPDN; バーチャル プライベート ダイアルアップ ネットワーク) グループで L2TP を設定します。

IP セキュリティによる L2TP の設定では、事前共有キーや RSA 署名方式を使用した認証と、(スタティックではなく) ダイナミックな暗号マップの使用がサポートされます。事前共有鍵は L2TP over IPsec トンネルを確立する際の認証に使用されます。

設定

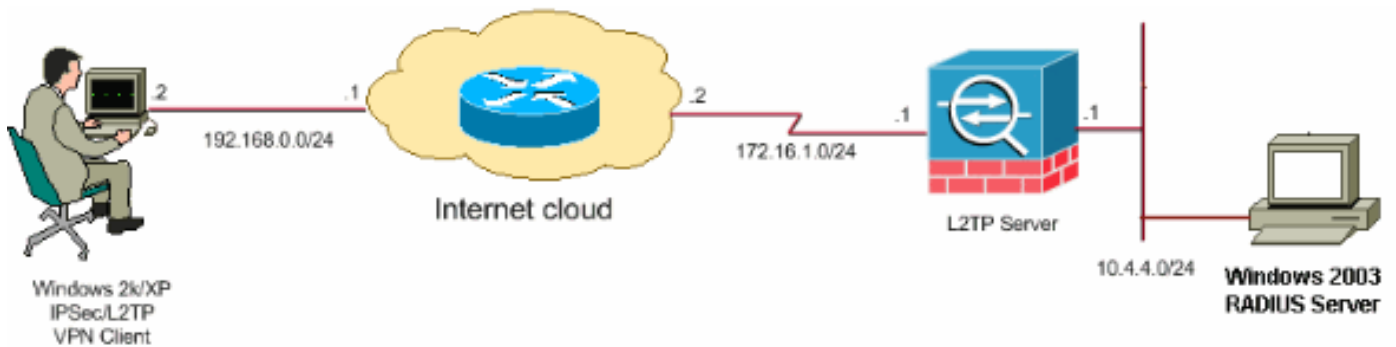
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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、[Command Lookup Tool](#) (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。これらはラボ環境で使用された RFC 1918 のアドレスです。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

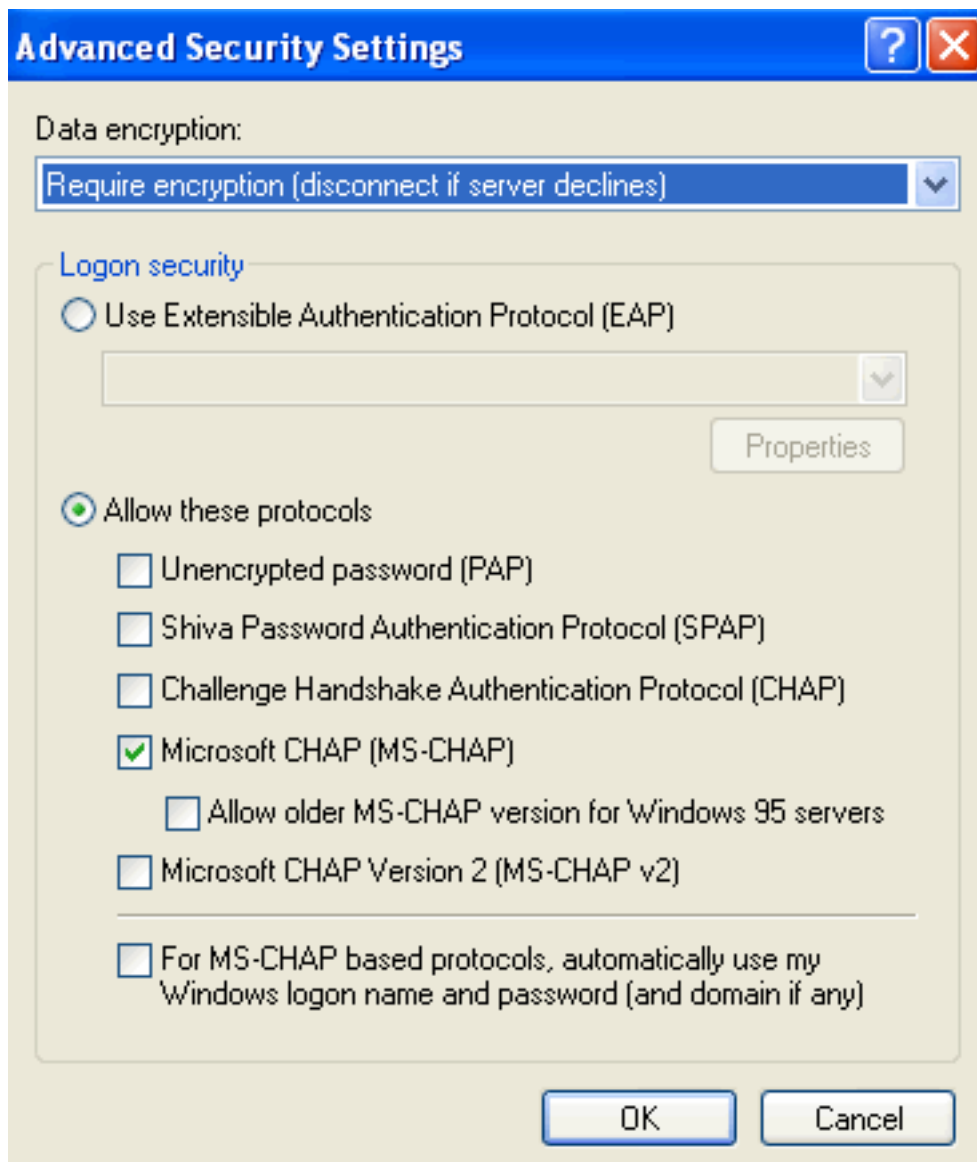
このドキュメントでは、次の設定を使用します。

- [Windows L2TP/IPSec クライアント設定](#)
- [PIX での L2TP サーバの設定](#)
- [ASDM を使用した L2TP の設定](#)
- [IAS がインストールされた Microsoft Windows 2003 サーバの設定](#)

Windows L2TP/IPSec クライアント設定

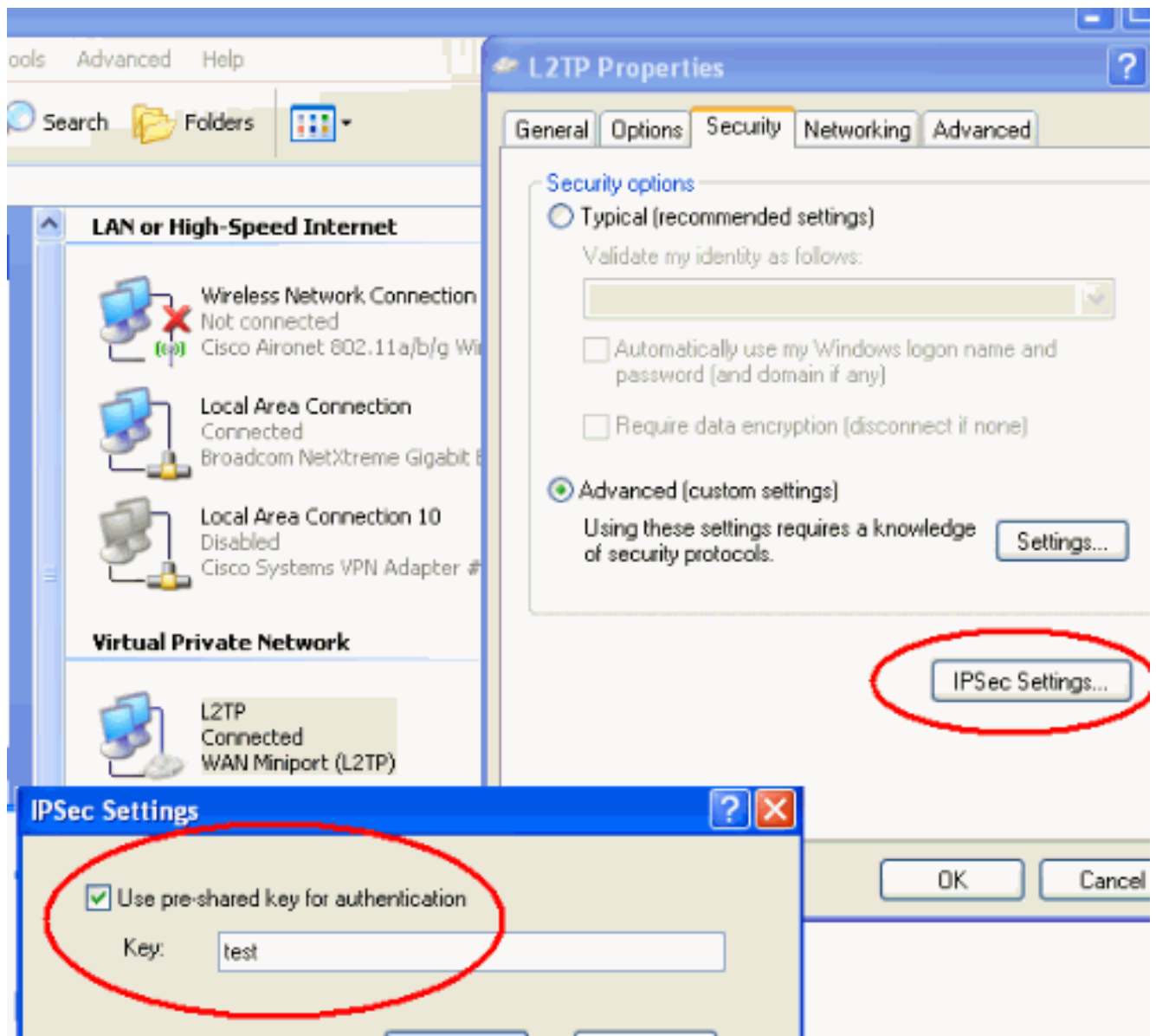
Windows 2000 に L2TP over IPSec を設定するには、次の手順を実行します。Windows XP の場合は、ステップ 1 と 2 を飛ばして、ステップ 3 から始めてください。

1. Windows 2000 マシンに、次のレジストリ値を追加します。
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
2. このキーに次のレジストリ値を追加します。Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1注: 場合によっては (Windows XP Sp2)、このキー (値の付加: XP ボックスに L2TP をネゴシエートさせると同時に 1) IPSec接続の L2TP よりもむしろだけ接続を切断するようです。このレジストリ キーと合せて IPSec ポリシーを追加することが必須になります。接続を確立することを試みるとき 800 受け取ったらキー (値を削除して下さい: はたらくために 1) 接続を得るため。注: Windows 2000/2003 XP デフォルトでは、Windows クライアントは Certificate Authority (CA; 認証局) を通じて IP セキュリティを使用するよう試みます。このレジストリ キーの設定により、それが行われなくなります。これで、PIX/ASA に使用するパラメータに合わせて、Windows ステーションに IP セキュリティ ポリシーを設定できます。Windows IPsec ポリシーのステップバイステップ設定のための[事前共有キー 認証 \(Q240262 \)](#) を使用して L2TP/IPSec 接続を設定する方法を参照して下さい。[設定を Windows XP \(の Layer 2 Tunneling Protocol 接続と併用するための事前共有キー 詳細については Q281555\)](#) 参照して下さい。
3. 接続を作成します。
4. [ネットワークとダイヤルアップ接続] で、[接続] を右クリックし、[プロパティ] を選択します。Security タブで、Advanced をクリックします。次の図のように、プロトコルを選択し



ます。

5. 注: 次の手順は、Windows XP にのみ適用できます。事前共有キーを設定するには、[IPSec Settings] をクリックし、[Use pre-shared key for authentication] にチェックマークを入れて、事前共有キーを入力します。次の例では、事前共有キーに test を使用します。



PIXでのL2TPサーバの設定

PIX 7.2

```

pixfirewall#show run PIX Version 7.2(1) ! hostname
pixfirewall domain-name default.domain.invalid enable
password 8Ry2YjIyt7RRXU24 encrypted names ! !---
Configures the outside and inside interfaces. interface
Ethernet0 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 ! interface Ethernet1 nameif
inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0 nat
(inside) 0 access-list nonat pager lines 24 logging
console debugging mtu outside 1500 mtu inside 1500 !---
Creates a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0 no failover asdm image flash:/asdm-521.bin
no asdm history enable arp timeout 14400 !--- The global
and nat command enable !--- the Port Address Translation
(PAT) using an outside interface IP !--- address for all
outgoing traffic. global (outside) 1 interface nat

```



```
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
0:05:00 absolute !--- Create the AAA server group "vpn"
and specify its protocol as RADIUS. !--- Specify the IAS
server as a member of the "vpn" group and provide its !-
-- location and key. aaa-server vpn protocol radius aaa-
server vpn host 10.4.4.2 key radiuskey !--- Identifies
the group policy as internal. group-policy
DefaultRAGroup internal !--- Instructs the security
appliance to send DNS and !--- WINS server IP addresses
to the client. group-policy DefaultRAGroup attributes
wins-server value 10.4.4.99 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPsec l2tp-
ipsec default-domain value cisco.com !--- Configure
usernames and passwords on the device !--- in addition
to using AAA. !--- If the user is an L2TP client that
uses Microsoft CHAP version 1 or !--- version 2, and the
security appliance is configured !--- to authenticate
against the local !--- database, you must include the
mschap keyword. !--- For example, username <username>
password <password> mschap. username test password
DLAUiAX3l78qgoB5c7iVNw== nt-encrypted vpn-tunnel-
protocol l2tp-ipsec http server enable http 0.0.0.0
0.0.0.0 inside no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart !--- Identifies the IPsec
encryption and hash algorithms !--- to be used by the
transform set. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac !--- Since the
Windows 2000 L2TP/IPsec client uses IPsec transport
mode, !--- set the mode to transport. !--- The default
is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport !--- Specifies the
transform sets to use in a dynamic crypto map entry.
crypto dynamic-map outside_dyn_map 20 set transform-set
TRANS_ESP_3DES_MD5 !--- Requires a given crypto map
entry to refer to a pre-existing !--- dynamic crypto
map. crypto map outside_map 20 ipsec-isakmp dynamic
outside_dyn_map !--- Applies a previously defined crypto
map set to an outside interface. crypto map outside_map
interface outside crypto isakmp enable outside crypto
isakmp nat-traversal 20 !--- Specifies the IKE Phase I
policy parameters. crypto isakmp policy 10
authentication pre-share encryption 3des hash md5 group
2 lifetime 86400 !--- Creates a tunnel group with the
tunnel-group command, and specifies the local !---
address pool name used to allocate the IP address to the
client. !--- Associate the AAA server group (VPN) with
the tunnel group. tunnel-group DefaultRAGroup general-
attributes address-pool clientVPNpool authentication-
server-group vpn !--- Link the name of the group policy
to the default tunnel !--- group from tunnel group
general-attributes mode. default-group-policy
DefaultRAGroup !--- Use the tunnel-group ipsec-
attributes command !--- in order to enter the ipsec-
attribute configuration mode. !--- Set the pre-shared
key. !--- This key should be the same as the key
configured on the Windows machine. tunnel-group
DefaultRAGroup ipsec-attributes pre-shared-key * !---
```

```

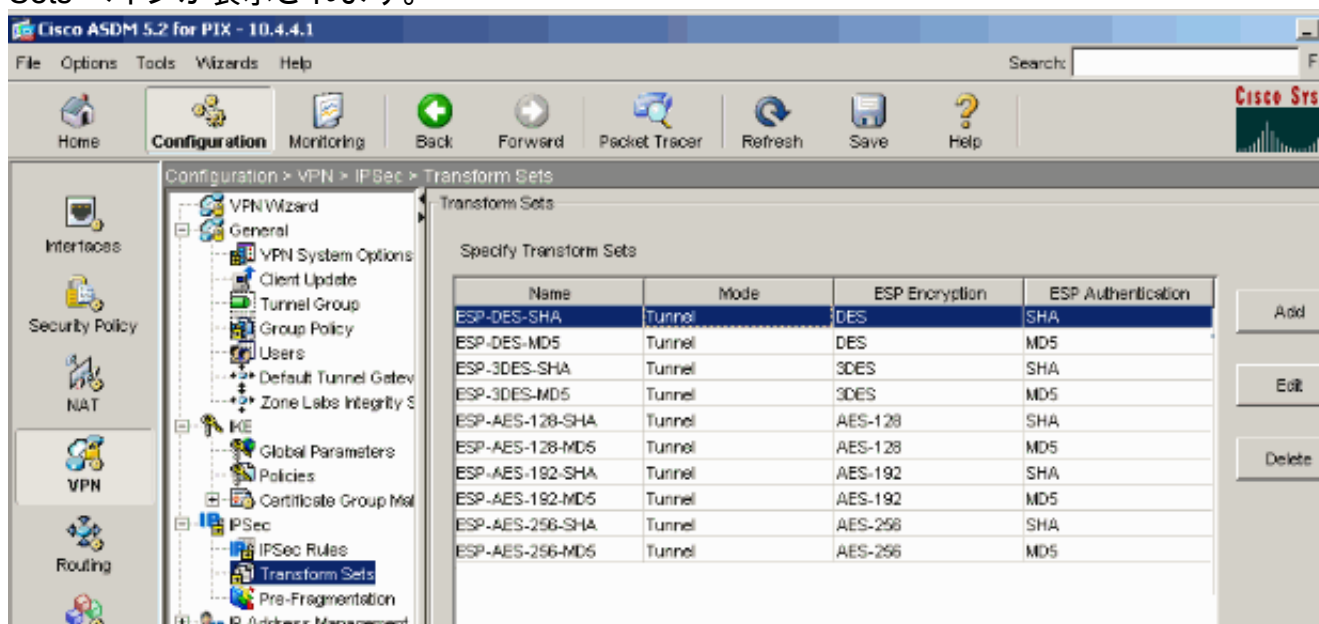
Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode. tunnel-group DefaultRAGroup ppp-
attributes no authentication chap authentication ms-
chap-v2 telnet timeout 5 ssh timeout 5 console timeout 0
! class-map inspection_default match default-inspection-
traffic !! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:ele0730fa260244caa2e2784f632accd : end

```

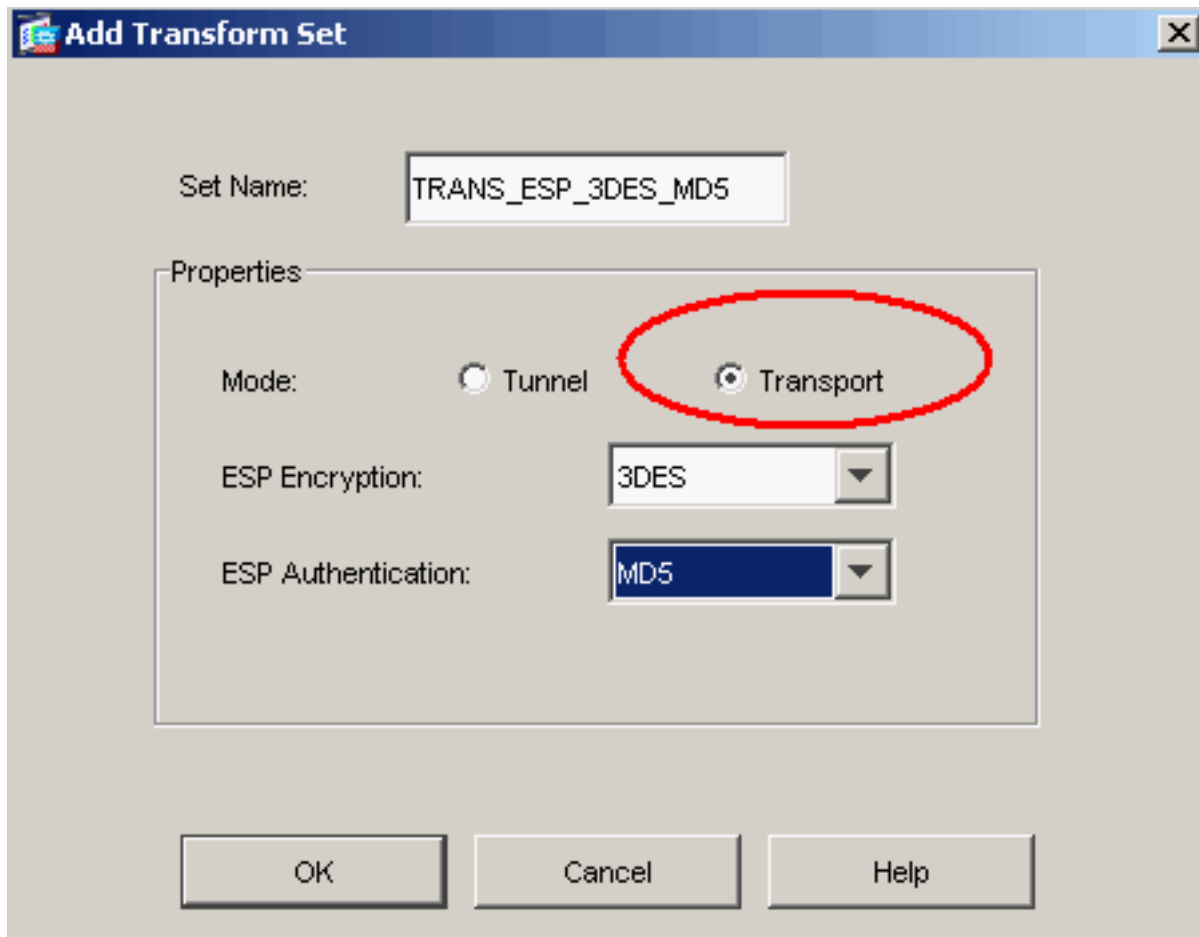
ASDM を使用した L2TP の設定

L2TP over IPSec 接続を受け入れるように、セキュリティ アプライアンスを設定するには、次の手順を実行します。

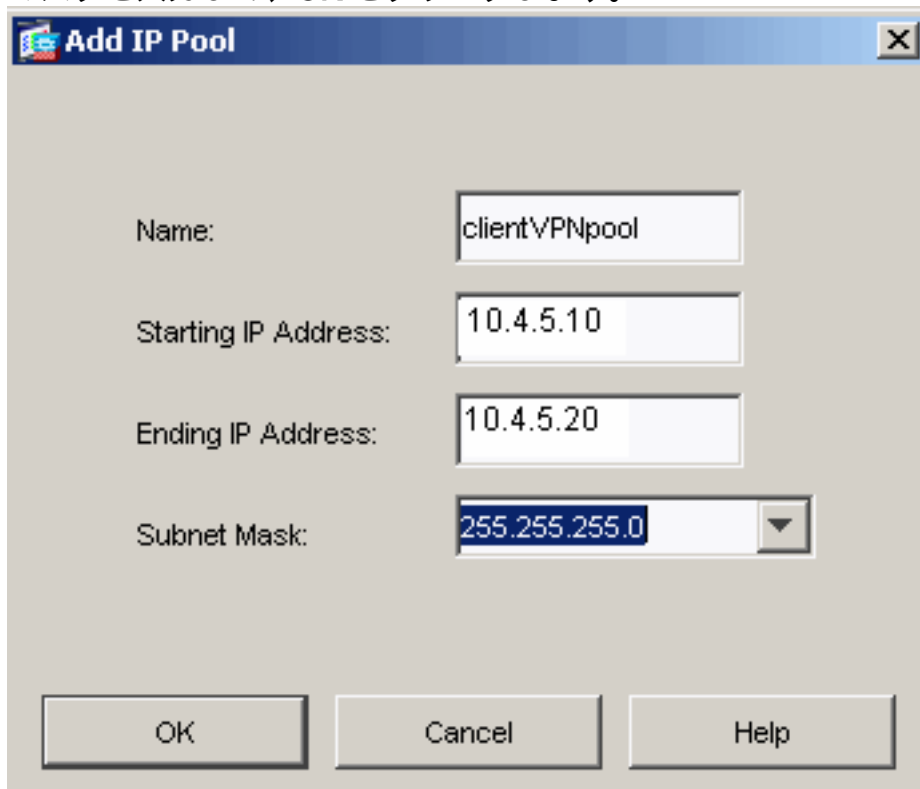
1. IPSec トランスフォーム セットを追加し、トンネル モードではなくトランスポート モードを使用するように、IPSec を指定します。これをするために、> IPSec > トランスフォーム セット Configuration > VPN の順に選択し、『Add』をクリックして下さい。Transform Sets ペインが表示されます。



2. 次の手順を実行して、トランスフォーム セットを追加します。トランスフォーム セットの名前を入力します。ESP 暗号化および ESP 認証方式を選択します。Transport モードを選択します。[OK] をクリックします。

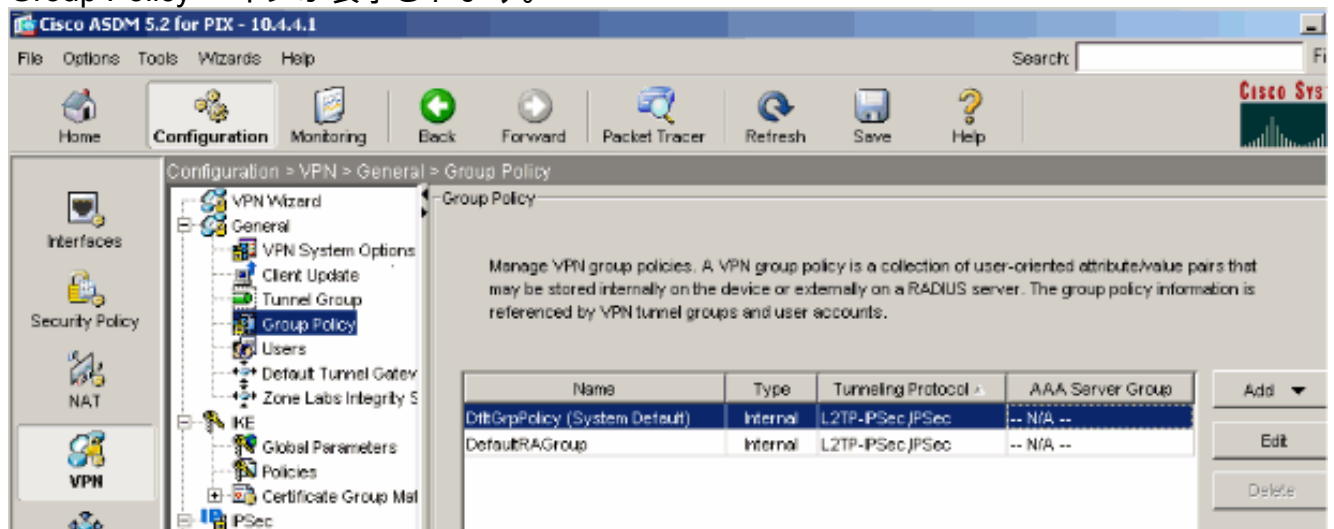


3. 次の手順を実行して、アドレス割り当ての方法を設定します。次の例では IP アドレスプールを使用します。> IPアドレス管理 > IP プール Configuration > VPN の順に選択して下さい。[Add] をクリックします。[Add IP Pool] ダイアログボックスが表示されます。新しい IP アドレスプールの名前を入力します。最初と最後の IP アドレスを入力します。サブネットマスクを入力して、OK をクリックします。

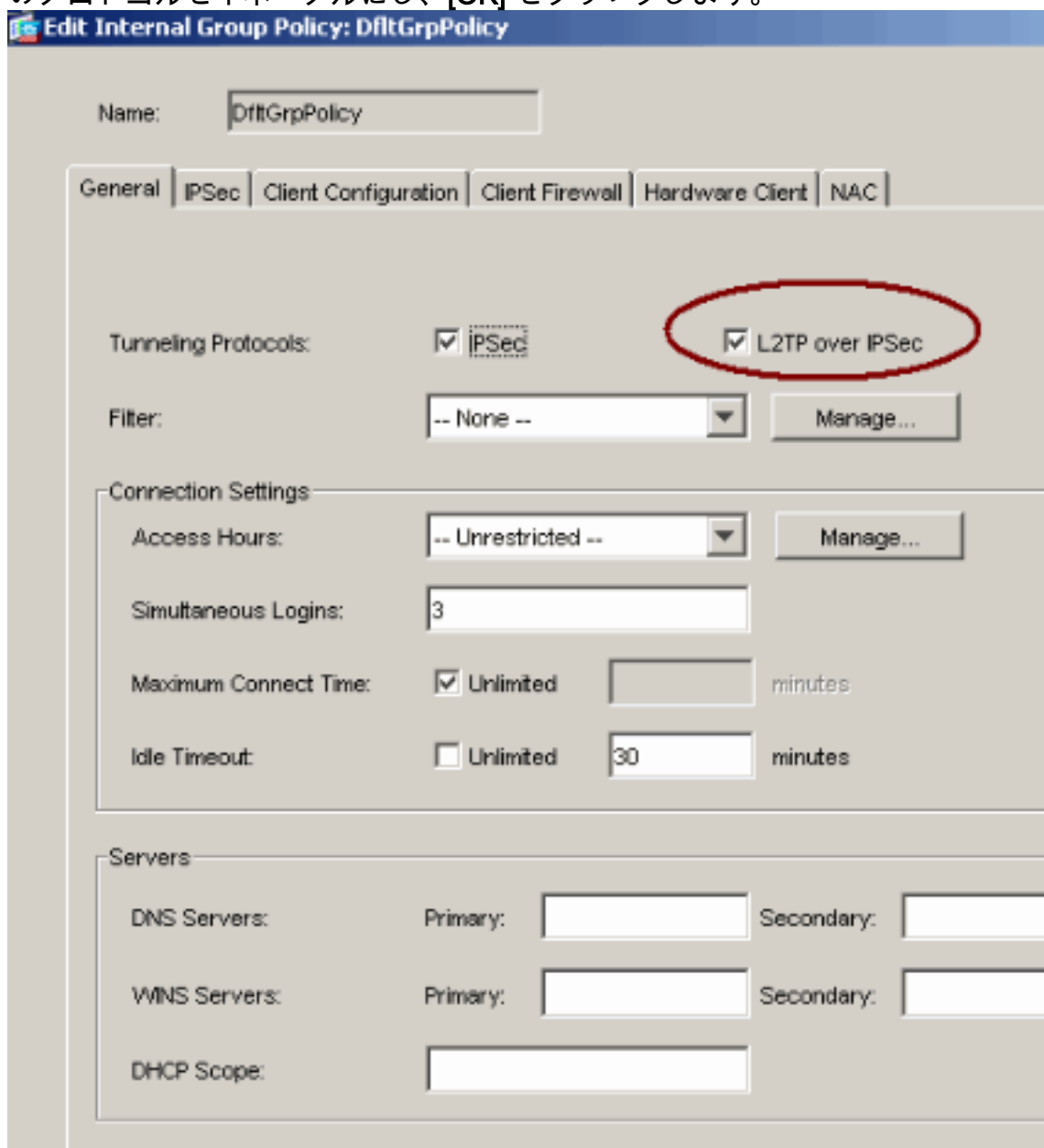


4. グループポリシーのための有効な VPN トンネリング プロトコルで L2TP Over IPsec を設定するために Configuration > VPN > General > Group Policy の順に選択して下さい。

Group Policy ペインが表示されます。

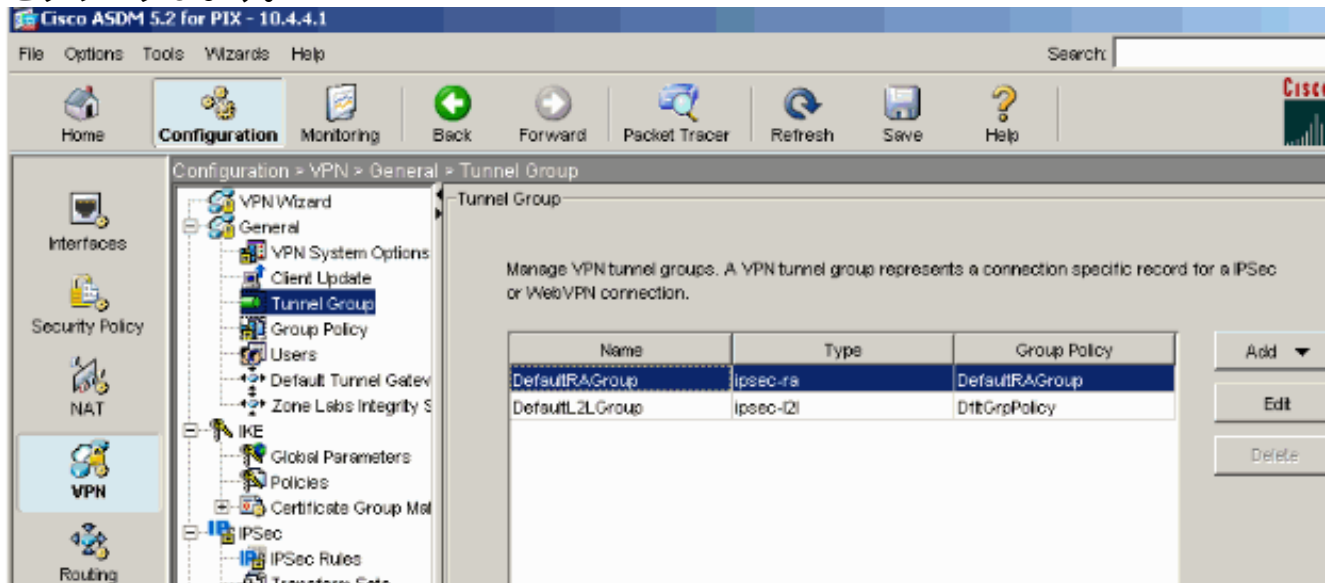


5. グループ ポリシー (DiffGrpPolicy) を選択し、Edit をクリックします。Edit Group Policy ダイアログが表示されます。L2TP over IPSec にチェックマークを入れてグループ ポリシーのプロトコルをイネーブルにし、[OK] をクリックします。

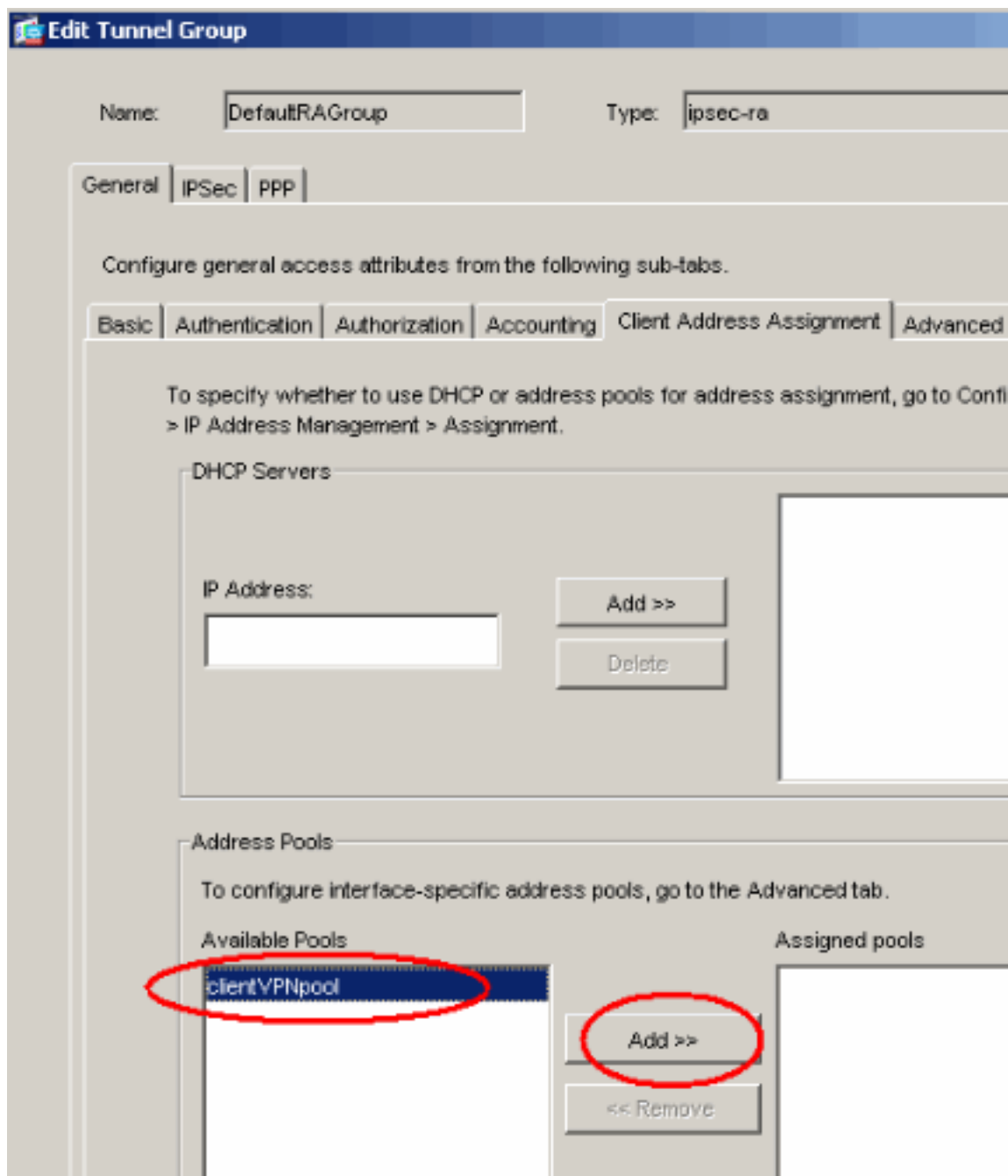


6. 次の手順を実行して、IP アドレス プールをトンネル グループに割り当てます。Configuration > VPN > General > Tunnel Group の順に選択 して下さい。Tunnel Group ペイ

ンが表示されたら、テーブルでトンネルグループ (DefaultRAGroup) を選択します。[Edit] をクリックします。



7. Edit Tunnel Group ウィンドウが表示されたら、次の手順を実行します。General タブから、Client Address Assignment タブへ移動します。Address Pools のエリアで、トンネルグループに割り当てるアドレスプールを選択します。[Add] をクリックします。Assigned Pools ボックスにアドレスプールが表示されます。



8. 事前共有キーを設定するため、[IPSec] タブへ移動し、自分の事前共有キーを入力して [OK] をクリックします。

Name: Type:

General | IPsec | **PPP**

Pre-shared Key: Trustpoint Name:

Authentication Mode: IKE Peer ID Validation:

Enable sending certificate chain

ISAKMP Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: (seconds) Retry Interval: (seconds)

Head end will never initiate keepalive monitoring

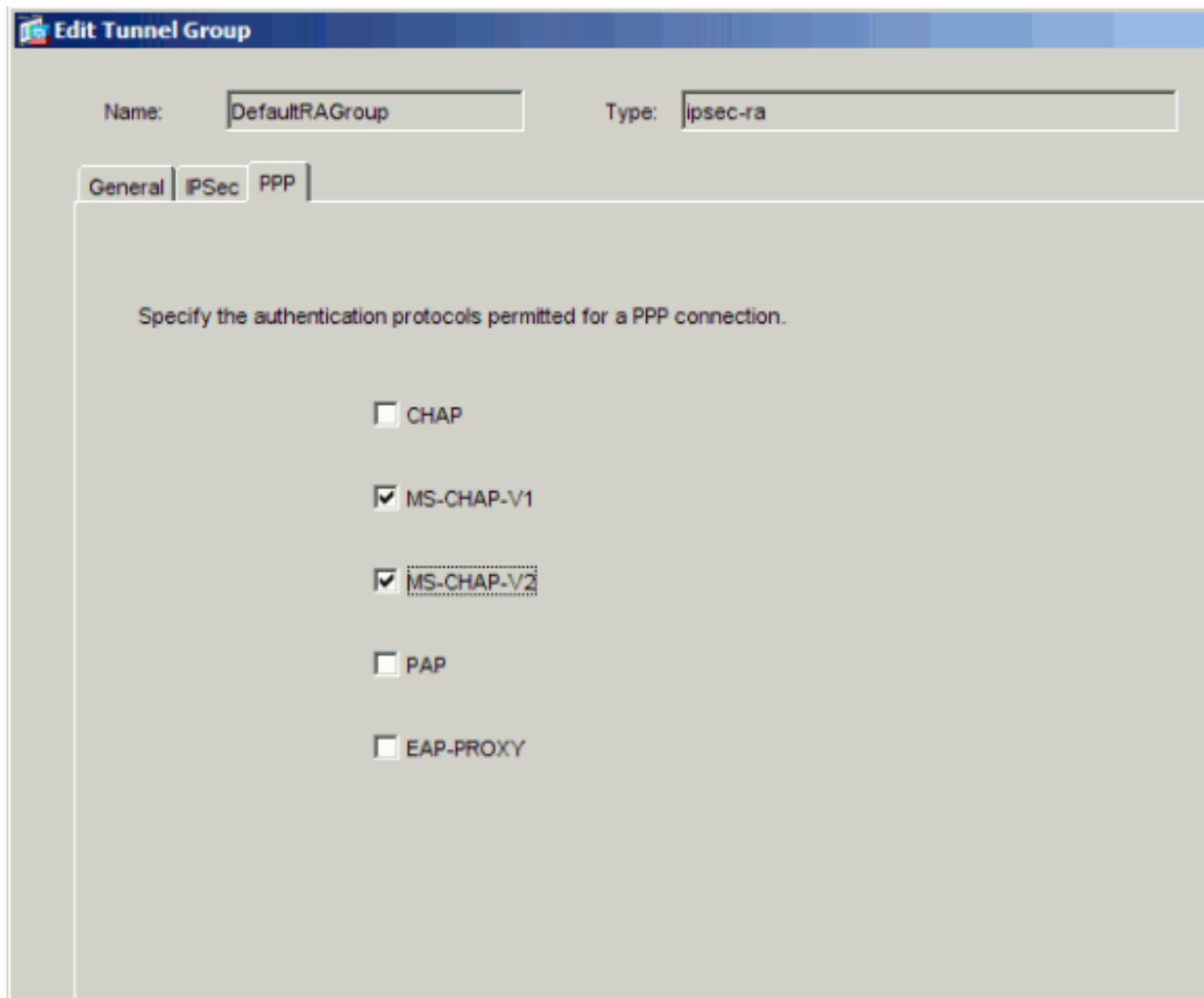
Interface-Specific Authentication Mode

Interface: Add >>

Authentication Mode: << Remove

Interface	Authentication Mode
-----------	---------------------

9. L2TP over IPsec は PPP 認証プロトコルを使用します。トンネルグループの PPP タブで、PPP 接続を許可するプロトコルを指定します。認証に **MS-CHAP-V1** プロトコルを選択します。



10. L2TP over IPsec 接続を試みるユーザの認証方法を指定します。認証サーバまたは自身のローカル データベースを使用するように、セキュリティ アプライアンスを設定できます。これを行うには、トンネル グループの Authentication へ移動します。デフォルトとして、セキュリティ アプライアンスはローカル データベースを使用します。Authentication Server Group ドロップダウン リストに LOCAL と表示されます。認証サーバを使用するには、リストから 1 つ選択します。注: PPP PAP Microsoft CHAP 1 2 EAP と CHAP は、プロキシ認証サーバで実行されます。したがって、リモート ユーザが EAP または CHAP の設定されているトンネル グループに属していて、セキュリティ アプライアンスがローカル データベースを使用するように設定されていると、そのユーザは接続できません。

注: トンネルグループにグループポリシーをリンクし、トンネルグループ切り替え (オプションの) を有効にすることができるようにトンネルグループ設定に戻るために Configuration > VPN > General > Tunnel Group の順に選択して下さい。 [Tunnel Group] ペインが表示されたら、トンネルグループを選択し、[Edit] をクリックします。注: Tunnel Group Switching L2TP over IPsec 各トンネルグループはそれぞれの AAA サーバグループと IP アドレスプールを持つため、ユーザはそのトンネルグループ特定の方法で認証を受けられます。この機能では、ユーザはユーザ名だけを送信するのではなく、ユーザ名とグループ名を username@group_name の形式で送信します。この場合、「@」は設定可能なデリミタであり、group name はセキュリティアプライアンスに設定されているトンネルグループの名前です。注: Tunnel Group Switching Strip Group VPN その後、セキュリティアプライアンスはユーザ名のユーザ部分だけを認可と認証に使用します。そうでない場合 (ディセーブルされている場合)、セキュリティアプライアンスは領域を含むユーザ名全体を送信します。Tunnel Group Switching をイネーブルにするには、**Strip the realm from username before passing it on to the AAA server** と **Strip the group from username before passing it on to the AAA server** にチェックマークを入れます。次に [OK] をクリックします。

11. 次の手順を実行して、ローカルデータベースにユーザを作成します。>Properties > デバイス Administration > ユーザアカウントを『Configuration』を選択して下さい。[Add] をクリックします。ユーザが Microsoft CHAP バージョン 1 または 2 を使用する L2TP クライアントで、セキュリティアプライアンスが認証時にローカルデータベースを照合するように設定されている場合は、MSCHAP を有効にするため [User Authenticated using MSCHAP] にチェックマークを入れる必要があります。[OK] をクリックします。

Add User Account

Identity | VPN Policy

Username: test

Password: ****

Confirm Password: ****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

12. 続くために『OK』をクリックします Configuration > VPN > IKE > Policies の順に選択し、フェーズ 1.のための IKE ポリシーを作成するために『Add』をクリックして下さい。

Add IKE Policy

Priority: 10

Authentication: pre-share

Encryption: 3des

D-H Group: 2

Hash: md5

Lifetime: Unlimited 86400 seconds

OK Cancel Help

13. (オプション) NAT デバイスの背後にある複数の L2TP クライアントが、セキュリティアプライアンスへ L2TP over IPSec 接続を試みる場合、ESP パケットが 1 つ以上の NAT デバイスをパススルーできるように、NAT トラバーサルを有効にする必要があります。これを行うには、次の手順を実行します。> IKE > グローバルなパラメータ Configuration > VPN の順に選択して下さい。ISAKMP がインタフェースで有効になって

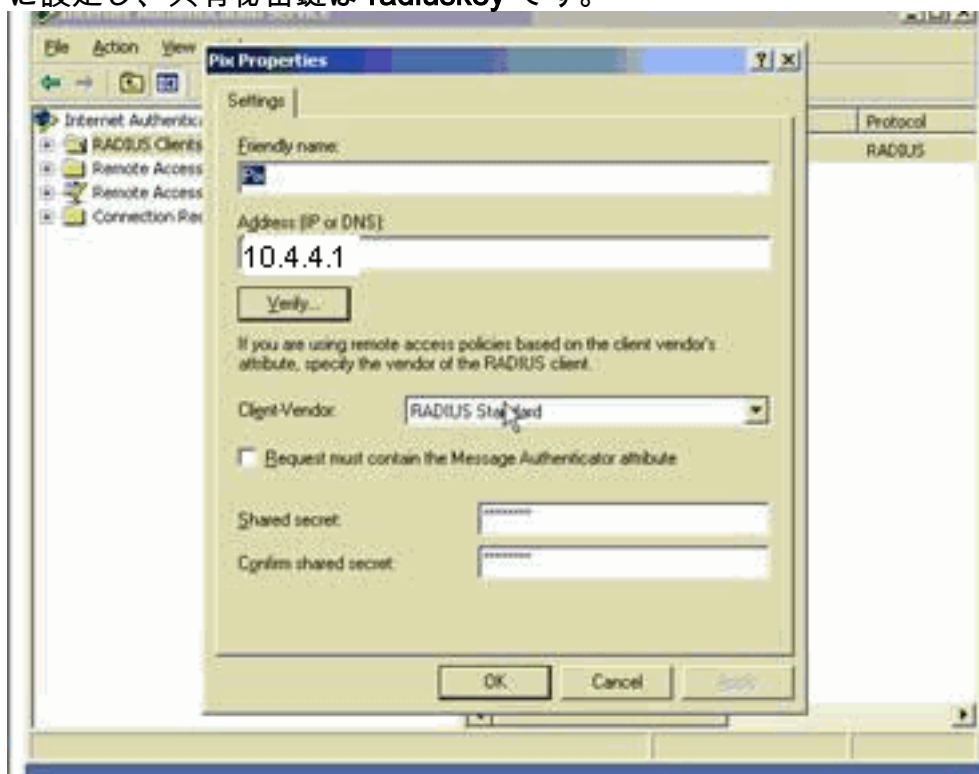
いることを確認します。[Enable IPsec over NAT-T] にチェックマークを入れます。[OK] をクリックします。

IAS がインストールされた Microsoft Windows 2003 サーバの設定

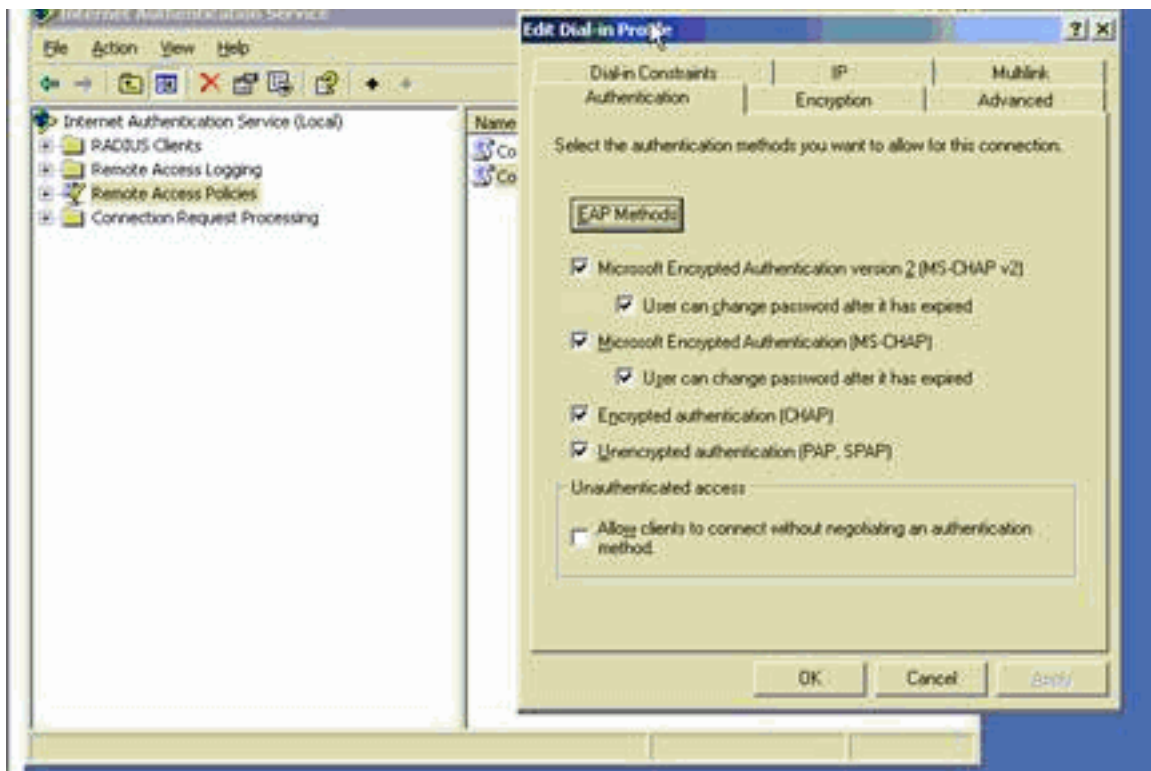
IAS がインストールされた Microsoft Windows 2003 サーバを設定するには、次の手順を実行します。

注: これらの手順では、IAS がすでにローカル マシンにインストールされていることを前提としています。まだインストールされていない場合は、**Control Panel > Add/Remove Programs** の順に選択して、IAS を追加してください。

1. 新しい RADIUSクライアントを追加するために > **RADIUSクライアントの Internet Authentication Service** および右クリック『Administrative Tools』を選択して下さい。クライアント情報を入力したら、**OK** をクリックします。この例では、IP アドレスが 10.4.4.1 で「Pix」という名前を持つクライアントを追加します。Client-Vendor は **RADIUS Standard** に設定し、共有秘密鍵は **radiuskey** です。

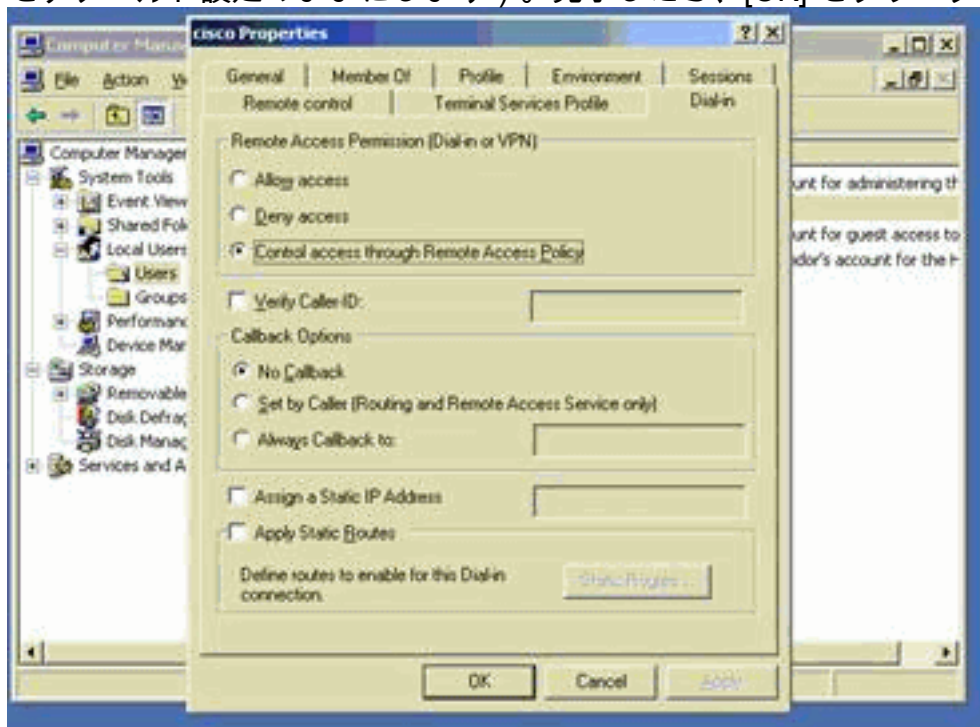


2. **Remote Access Policies** を選択して、**Connections to Other Access Servers** を右クリックし、**Properties** を選択します。
3. **[Grant Remote Access Permissions]** のオプションが選択されていることを確認します。
4. **Edit Profile** をクリックして、次の設定を確認します。Authentication タブで、**Unencrypted authentication (PAP, SPAP)** にチェックマークを入れます。Encryption タブで、**No Encryption** のオプションが選択されていることを確認します。完了したら、**[OK]** をクリッ



クします。

5. > コンピュータマネジメント > システム ツール > ローカルユーザおよびグループ 『Administrative Tools』 を選択し、ユーザを右クリックし、ローカル コンピュータ アカウントにユーザを追加するためにユーザを 『New』 を選択して下さい。
6. Cisco パスワードを password1 に設定したユーザを追加して、次のプロファイル情報を確認します。General タブで、User Must Change Password のオプションではなく、Password Never Expired のオプションが選択されていることを確認します。[Dial-in] タブで、[Allow access] のオプションを選択します (または [Control access through Remote Access Policy] をデフォルト設定のままにします)。完了したら、[OK] をクリックします。



アクティブ ディレクトリを使用した L2TP Over IPsec のための拡張認証

L2tp 接続のための認証がアクティブ ディレクトリから起こるように ASA のこの設定を使用して下さい:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)# authentication pap
```

また、L2tp クライアントで、**拡張セキュリティ設定 (カスタム)** に行き、**非暗号化パスワード (PAP)** のためのオプションだけ選択して下さい。

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto ipsec sa** — ピアですべての電流 IKE Security Association (SA) を示します。
pixfirewall#show crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1 access-list 105 permit ip host 172.16.1.1 host 192.168.0.2 local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0) remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701) current_peer: 192.168.0.2, username: test dynamic allocated peer ip: 10.4.5.15 #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23 #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 23, #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 #send errors: 0, #recv errors: 0 **local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: C16F05B8 inbound esp sas: spi: 0xEC06344D (3959829581) transform: esp-3des esp-md5-hmac in use settings = {RA, Transport, } slot: 0, conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xC16F05B8 (3245278648) transform: esp-3des esp-md5-hmac in use settings = {RA, Transport, } slot: 0, conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV size: 8 bytes replay detection support: Y
- **show crypto isakmp sa** : 現在ピアにあるすべての IKE SA を表示します。 pixfirewall#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: 192.168.0.2 Type : user Role : responder Rekey : no State : MM_ACTIVE
- **示して下さい VPNsessiondb** — L2TP Over IPSec 接続についての詳細な情報を表示するために使用できるプロトコルフィルタが含まれています。グローバル コンフィギュレーション モードからのフル コマンドは、**show vpn-sessiondb detailed remote filter protocol l2tpoveripsec** です。次の例は、単一の L2TP over IPSec 接続の詳細を示しています。
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec Session Type: Remote Detailed Username : test Index : 1 Assigned IP : 10.4.5.15 Public IP : 192.168.0.2 Protocol : L2TPOverIPSec Encryption : 3DES Hashing : MD5 Bytes Tx : 1336 Bytes Rx : 14605 Client Type : Client Ver : Group Policy : DefaultRAGroup Tunnel Group : DefaultRAGroup Login Time : 18:06:08 UTC Fri Jan 1 1993 Duration : 0h:04m:25s Filter Name : NAC Result : N/A Posture Token: IKE Sessions: 1 IPSec Sessions: 1 L2TPOverIPSec Sessions: 1 IKE: Session ID : 1 UDP Src Port : 500 UDP Dst Port : 500 IKE Neg Mode : Main Auth Mode : preSharedKeys Encryption : 3DES Hashing : MD5 Rekey Int (T): 28800 Seconds Rekey Left(T): 28536 Seconds D/H Group : 2 IPSec: Session ID : 2 Local Addr : 172.16.1.1/255.255.255.255/17/1701 Remote Addr : 192.168.0.2/255.255.255.255/17/1701 Encryption : 3DES Hashing : MD5 Encapsulation: Transport Rekey Int (T): 3600 Seconds Rekey Left(T): 3333 Seconds Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Bytes Tx : 1336 Bytes Rx : 14922 Pkts Tx : 25 Pkts Rx : 156 L2TPOverIPSec: Session ID : 3 Username : test Assigned IP : 10.4.5.15 Encryption : none Auth Mode : msCHAPv1 Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Bytes Tx : 378 Bytes Rx : 13431 Pkts Tx : 16 Pkts Rx : 146

トラブルシューティング

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。デバッグ出力例も紹介しています。

トラブルシューティングのためのコマンド

特定のコマンドは、[アウトプットインタープリタ](#) (登録ユーザ専用) でサポートされています。このツールを使用すると、`show` コマンドの出力を分析できます。▼一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。▼

注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』および『[IP Security のトラブルシューティング: debug コマンドの説明と使用](#)』を参照してください。

- `debug crypto ipsec 7` : フェーズ 2 の IPsec ネゴシエーションを表示します。
- `debug crypto isakmp 7` : フェーズ 1 の ISAKMP ネゴシエーションを表示します。

デバッグの出力例

PIX ファイアウォール

```
PIX#debug crypto isakmp 7 pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE
RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing
SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable Jan 02
18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]:
IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2,
Received Fragmentation VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID
payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V ID Jan
02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload Jan 02 18:26:44 [IKEv1
DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform # 2 acceptable Matches global IKE entry
# 2 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload Jan 02
18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID + extended capabilities
payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104 Jan 02 18:26:44 [IKEv1]: IP
= 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) +
NONE (0) total length : 184 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke
payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload Jan 02
18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload Jan 02 18:26:44 [IKEv1
DEBUG]: IP = 192.168.0.2, constructing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP =
192.168.0.2, constructing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2,
constructing Cisco Unity VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2,
constructing xauth V6 VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS Vendor ID
payload (version: 1.0.0, capabilities: 20000001) Jan 02 18:26:44 [IKEv1 DEBUG]: IP =
192.168.0.2, constructing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send
Altiga/Cisco VPN3000/Cisco ASA GW VID Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection
landed on tunnel_group DefaultRAGroup Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, Generating keys for Responder... Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2,
IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1]:
IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8)
+ NONE (0) total length : 60 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP =
192.168.0.2, processing ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP =
192.168.0.2, processing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, Computing hash for ISAKMP Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection
landed on tunnel_group DefaultRAGroup Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, Freeing previously allocated memory for authorization-dn-attributes Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing ID payload Jan
02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing hash payload
```


Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing
dpd vid payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80 **!--- Phase 1
completed successfully.** Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE
1 COMPLETED** Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection:
None Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer does not
support keep-alives (type = None) Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP =
192.168.0.2, Starting P1 rekey timer: 21600 seconds. Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2,
IKE_DECODE RECEIVED Message (msgid=elb84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NONE (0) total length : 164 Jan 02 18:26:44 [IKEv1 DEBUG]: Group =
DefaultRAGroup, IP = 192.168.0.2, processing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group
= DefaultRAGroup, IP = 192.168.0.2, processing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group
= DefaultRAGroup, IP = 192.168.0.2, processing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]:
Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload Jan 02 18:26:44 [IKEv1]: Group
= DefaultRAGroup, IP = 192.168.0.2, Received remote Proxy Host data in ID Payload: Address
192.168.0.2, Protocol 17, Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP =
192.168.0.2, processing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, Received local Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17,
Port 1701 **!--- PIX identifies the L2TP/IPsec session.** Jan 02 18:26:44 [IKEv1]: Group =
DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPsec session detected.** Jan 02 18:26:44 [IKEv1]: Group =
DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr Jan 02 18:26:44 [IKEv1]:
Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Peer configured for crypto map:
outside_dyn_map Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing IPsec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2,
IPsec S A Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 20 Jan 02
18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesting SPI! Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine:
SPI = 0xce9f6e19 **!--- Constructs Quick mode in Phase 2.** Jan 02 18:26:44 [IKEv1 DEBUG]: Group =
DefaultRAGroup, IP = 192.168.0.2, **oakley constructing quick mode** Jan 02 18:26:44 [IKEv1 DEBUG]:
Group = DefaultRAGroup, IP = 192.168.0.2, constructing blank hash payload Jan 02 18:26:44
[IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec SA payload Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec nonce
payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing
proxy ID Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmitt
ing Proxy Id: Remote host: 192.168.0.2 Protocol 17 Port 1701 Local host: 172.16.1.1 Protocol 17 Port
1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing qm
hash payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=elb
84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total
length : 144 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=el
b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 02 18:26:44 [IKEv1
DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload Jan 02 18:26:44
[IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs Jan 02 18:26:44
[IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key! Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security negotiation
complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI = 0xd08f711b Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA:
SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2,
Pitcher : received KEY_UPDATE, spi 0xce9f6e19 Jan 02 18:26:44 [IKEv1 DEBUG]: Group =
DefaultRAGroup, IP = 192.168.0.2, Starting P2 rekey timer: 3059 seconds. **!--- Phase 2 completes
successfully.** Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPLE
TED (msgid=0elb84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip
<192.168.0.2> mask <0xFFFFFFFF> port <1701> PIX#debug crypto ipsec 7 pixfirewall# IPSEC:
Deleted inbound decrypt rule, SPI 0x71933D09 Rule ID: 0x028D78D8 IPSEC: Deleted inbound permit
rule, SPI 0x71933D09 Rule ID: 0x02831838 IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
Rule ID: 0x029134D8 IPSEC: Deleted inbound VPN context, SPI 0x71933D09 VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA Rule ID: 0x028DAC90 IPSEC: Deleted outbound
permit rule, SPI 0xAF4DA5FA Rule ID: 0x02912AF8 IPSEC: Deleted outbound VPN context, SPI
0xAF4DA5FA VPN handle: 0x0048468C IPSEC: New embryonic SA created @ 0x01BF80, SCB: 0x01C262D0,
Direction: inbound SPI : 0x45C3306F Session ID: 0x0000000C VPIF num : 0x00000001 Tunnel type: ra
Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0x0283A3A8, SCB:
0x028D1B38, Direction: outbound SPI : 0x370E8DD1 Session ID: 0x0000000C VPIF num : 0x00000001
Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI

0x370E8DD1 IPSEC: Creating outbound VPN context, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: New outbound encrypt rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 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 0x370E8DD1 Rule ID: 0x02826540 IPSEC: New outbound permit rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 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: 0x370E8DD1 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: Completed host IBSA update, SPI 0x45C3306F IPSEC: Creating inbound VPN context, SPI 0x45C3306F Flags: 0x00000206 SA : 0x01BFCF80 SPI : 0x45C3306F MTU : 0 bytes VCID : 0x00000000 Peer : 0x0048C164 SCB : 0x01C262D0 Channel: 0x01693F08 IPSEC: Completed inbound VPN context, SPI 0x45C3306F VPN handle: 0x0049107C IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0049107C SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: Completed outbound inner rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 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 0x45C3306F Rule ID: 0x02831838 IPSEC: New inbound decrypt rule, SPI 0x45C3306F Src addr: 192.168.0.2 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: 0x45C3306F Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F Rule ID: 0x028DAC90 IPSEC: New inbound permit rule, SPI 0x45C3306F Src addr: 192.168.0.2 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: 0x45C3306F Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x45C3306F Rule ID: 0x02912E50

[ASDM を使用したトラブルシューティング](#)

ASDM を使用して、ロギングを有効にしてログを表示できます。

1. Configuration > Properties > Logging > Logging Setup の順に選択し、ロギングを有効にするために、『Enable Logging』を選択し、『Apply』をクリックして下さい。
2. > ロギング > ログレベルのログバッファ > 『Monitoring』を選択し、『Logging Buffer』を選択し、ログを調べるために『View』をクリックして下さい。

[問題：頻繁な切断](#)

アイドル/セッション タイムアウト

アイドル タイムアウトが 30 分 (デフォルト) に設定されている場合、これは 30 分間にわたってトンネルを通過するトラフィックがなかった場合にトンネルが廃棄されることを意味します。VPN クライアントは、アイドル タイムアウトの設定にかかわらず 30 分後に接続解除され、PEER_DELETE-IKE_DELETE_UNSPECIFIED エラー メッセージが表示されます。

トンネルが常時アップ状態で廃棄されることのないようにするには、idle timeout と session timeout を none に設定します。

ユーザのタイムアウト期間を設定するには、次のように、グループ ポリシー コンフィギュレーション モードがユーザ名コンフィギュレーション モードで `vpn-idle-timeout` コマンドを入力します。

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-
```

timeout none

次のように、グループ ポリシー コンフィギュレーション モードかユーザ名コンフィギュレーション モードで `vpn-session-timeout` コマンドにより、VPN 接続に対する最大総時間を設定します。

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-session-timeout none
```

Windows Vista のトラブルシューティング

同時ユーザ

Windows Vista の L2TP/IPSec では、複数のユーザが同時にヘッドエンド PIX/ASA に接続できないようにするという、アーキテクチャ上の変更が加えられました。この動作は、Windows 2K/XP では生じません。Cisco は、この変更に対する回避策をリリース 7.2(3) 以降で導入しています。

Vista PC で接続できない

Windows Vista を搭載したコンピュータが L2TP サーバに接続できない場合は、DefaultRAGroup の PPP アトリビュートに `mschap-v2` だけが設定されていることを確認してください。

関連情報

- [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](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス](#)
- [Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス](#)
- [Cisco PIX Firewall ソフトウェア製品サポート](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [RADIUS に関するサポート ページ](#)
- [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 \(RFC \)](#)
- [Layer Two Tunnel Protocol \(L2TP; レイヤ 2 トンネル プロトコル \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)