Cisco Secure PIX Firewall 6.x および Cisco VPN Client 3.5 for Windows と Microsoft Windows 2000 および 2003 の IAS RADIUS 認証

内容

概要

この設定例は、Microsoft Windows 2000 および 2003 インターネット認証サービス（IAS）RADIUS サーバで使用するために、Cisco VPN Client バージョン 3.5 for Windows と Cisco Secure PIX Firewall を設定する方法を示しています。Microsoft - Checklist:ダイヤルアップとVPNアクセスのためのIASの設定 』を参照してください。

Cisco VPN Client 4.xを使用するPIX/ASA 7.0での同じシナリオの詳細については、『Microsoft Windows 2003 IAS RADIUS認証を使用したPIX/ASA 7.xおよびCisco VPN Client 4.x for Windowsのの設定例』をを参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco Secure PIX Firewallソフトウェアリリース6.0は、Cisco VPN Client 3.5 for WindowsからのVPN接続をサポートしています。
- この設定例では、PIXがすでに適切なスタティック、コンジット、またはアクセスリストで動作していることを前提としています。このドキュメントでは、これらの基本概念を説明する

のではなく、Cisco VPN ClientからPIXへの接続を示します。

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。

- PIX Firewall ソフトウェア リリース 6.1.1**注：これは**PIXソフトウェアリリース6.1.1でテストされていますが、6.xのすべてのリリースで動作する必要があります。
- Cisco VPN Client バージョン 3.5（Windows 版）
- IASがインストールされたWindows 2000および2003 Server

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。

表記法

ドキュメント表記の詳細については、『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。

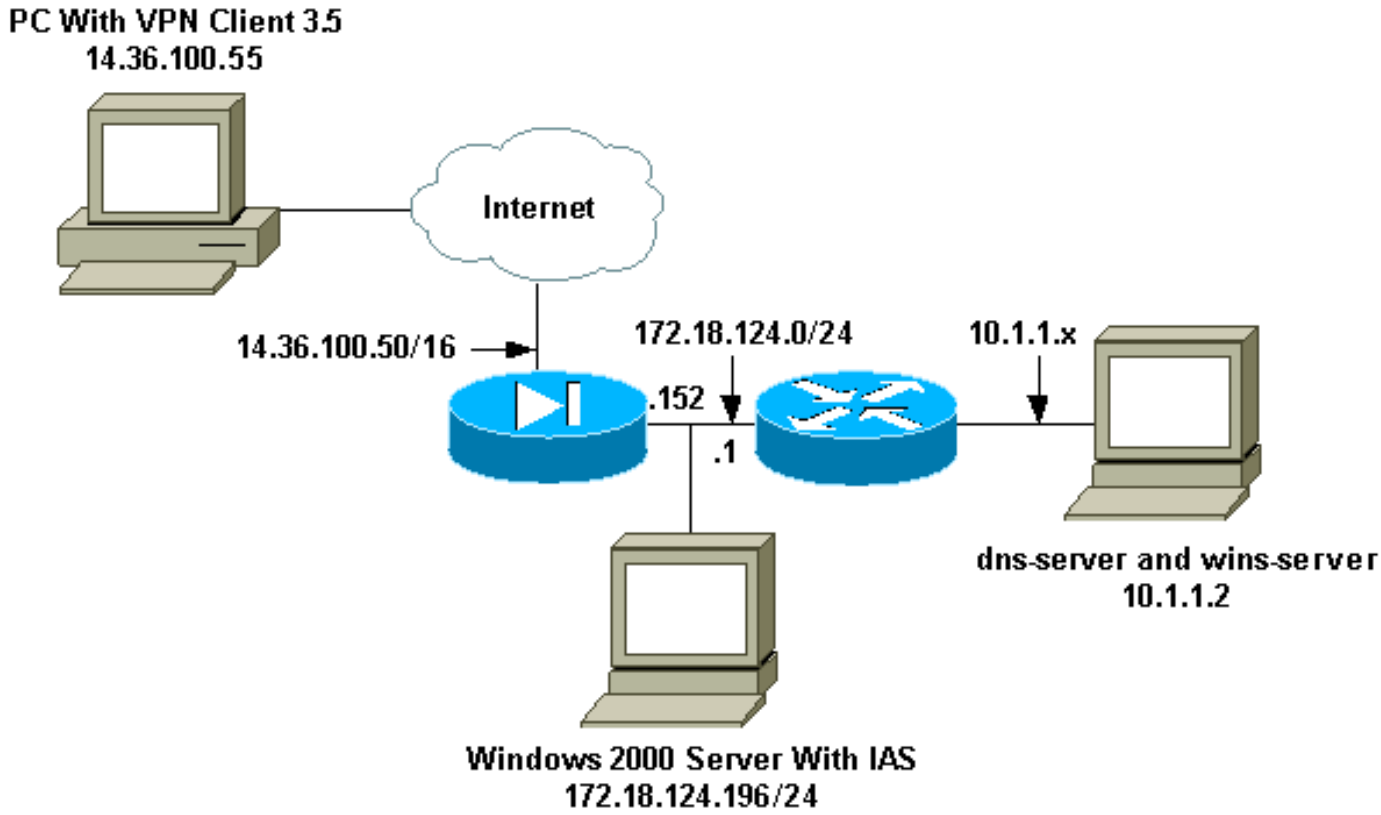
設定

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に必要な情報を提供しています。

注：このセクション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）を参照してください。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。

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 セットアップを使用します。



設定

このドキュメントでは次の設定を使用します。

- PIX ファイアウォール
- VPN Client 3.5（Windows 版）
- IAS がインストールされた Microsoft Windows 2000 サーバ
- IAS がインストールされた Microsoft Windows 2003 サーバ

PIX ファイアウォール

PIX ファイアウォール

```
pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

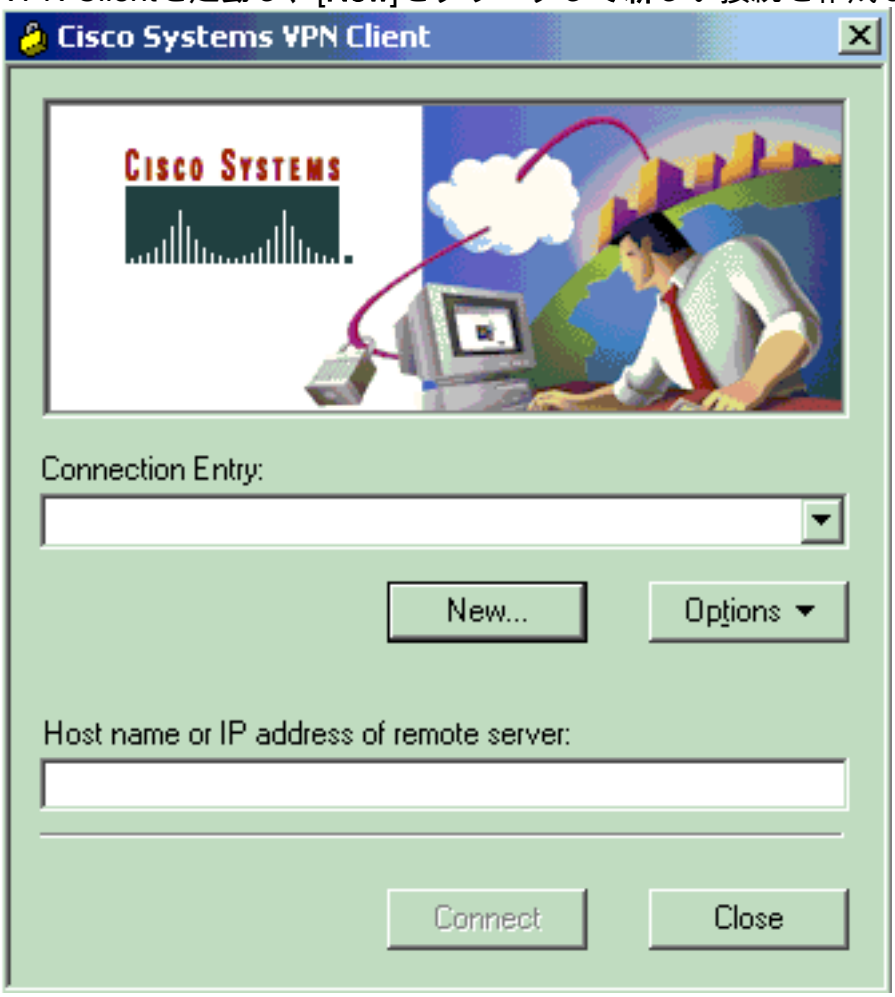
```
names
!--- Issue the access-list command to avoid !--- Network
Address Translation (NAT) on the IPsec packets.

access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
  255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
pdm history enable
arp timeout 14400
global (outside) 1 14.36.100.51
!--- Binding access list 101 to the NAT statement to
avoid !--- NAT on the IPsec packets. nat (inside) 0
access-list 101
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
route inside 10.1.1.0 255.255.255.0 172.18.124.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
   rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
!--- Enable access to the RADIUS protocol.
aaa-server RADIUS protocol radius
!--- Associate the partnerauth protocol to RADIUS. aaa-
server partnerauth protocol radius
aaa-server partnerauth (inside) host 172.18.124.196
cisco123
   timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Tell PIX to implicitly permit IPsec traffic. sysopt
connection permit-ipsec
no sysopt route dnat
!--- Configure a transform set that defines how the
traffic is protected. crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- Create a dynamic crypto map and specify which !---
transform sets are allowed for this dynamic crypto map
entry. crypto dynamic-map dynmap 10 set transform-set
myset
!--- Add the dynamic crypto map set into a static crypto
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- Enable the PIX to launch the Xauth application on
the VPN Client. crypto map mymap client authentication
partnerauth
!--- Apply the crypto map to the outside interface.
crypto map mymap interface outside
!--- IKE Policy Configuration. isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
```

```
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
: end
[OK]
pixfirewall(config)#
```

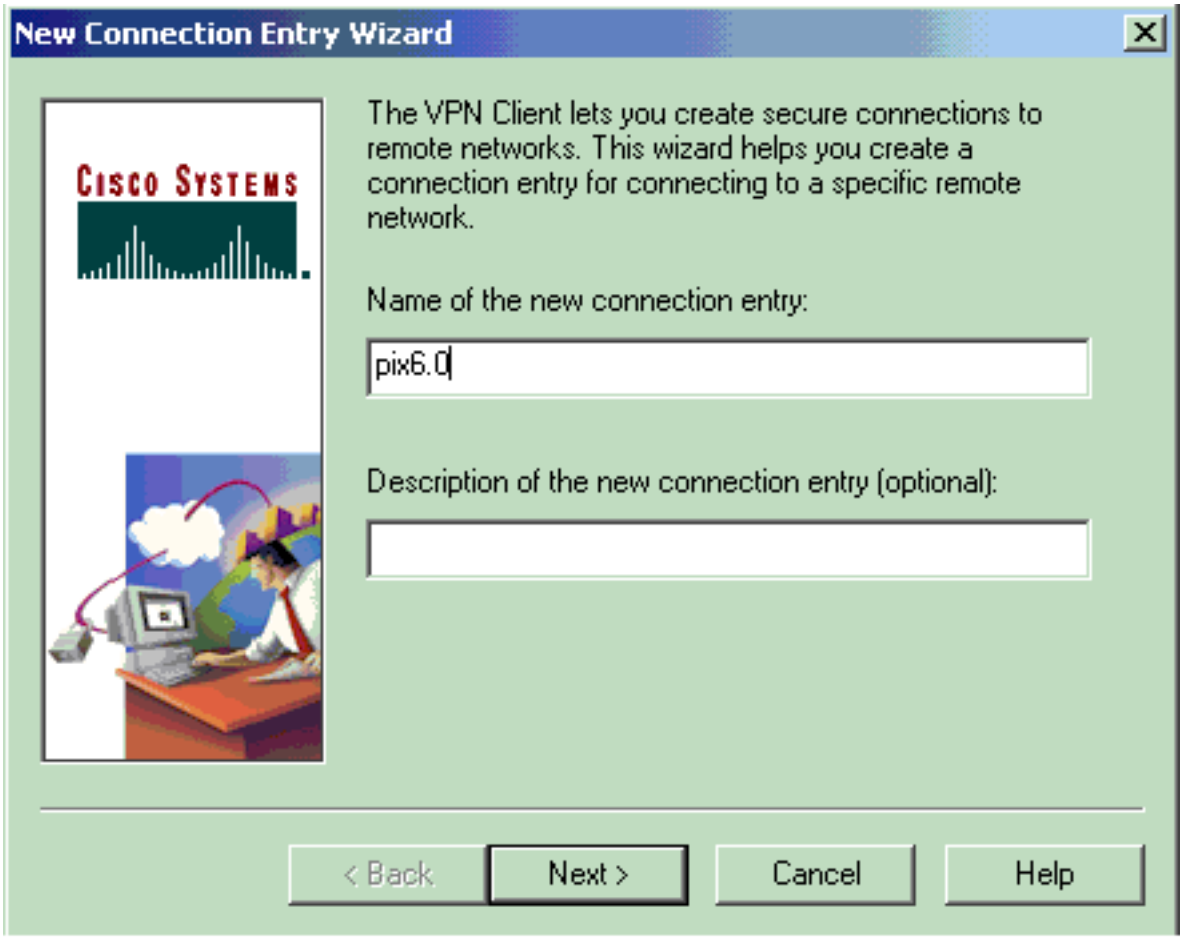
VPN Client 3.5 (Windows 版)

このセクションでは、Cisco VPN Client 3.5 for Windowsの設定方法について説明します。

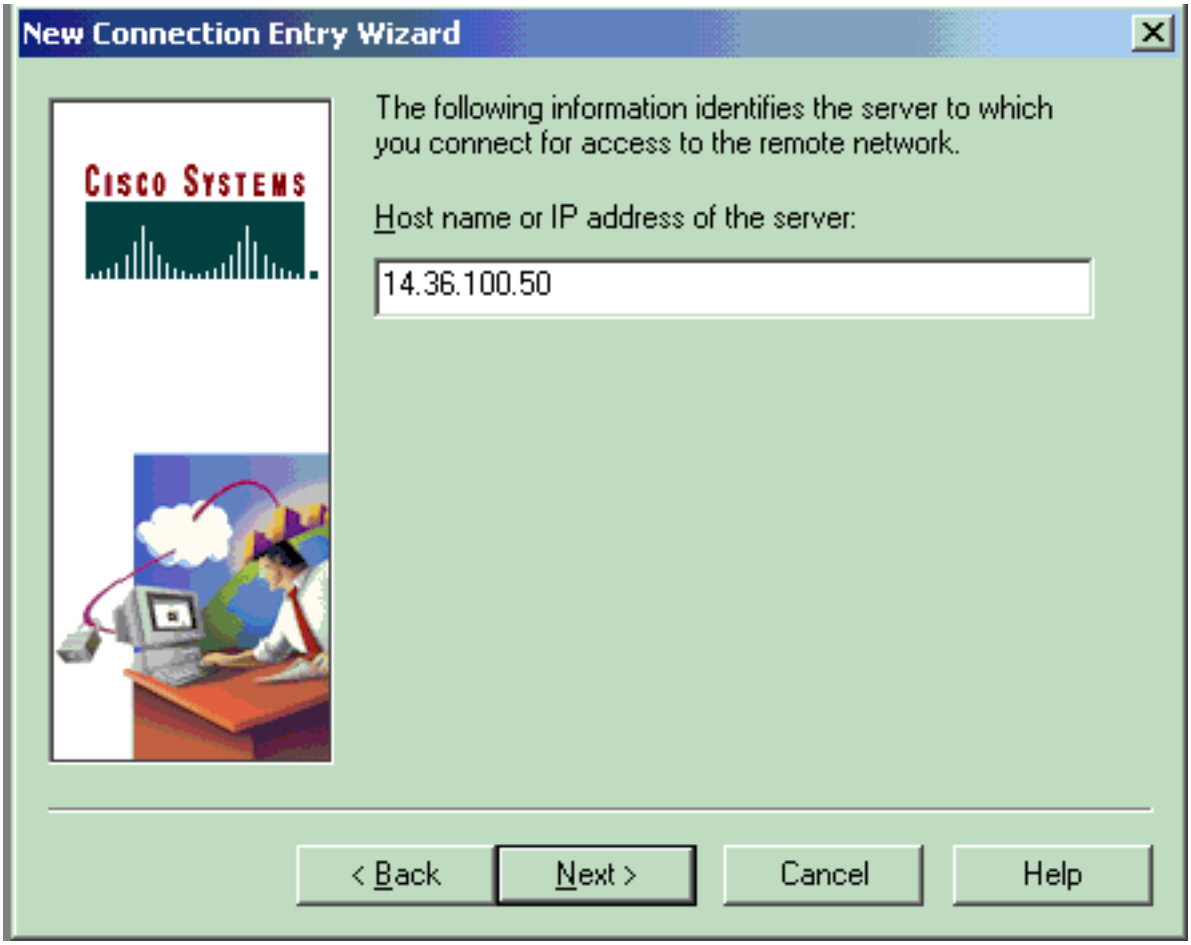
1. VPN Clientを起動し、[New]をクリックして新しい接続を作成します。



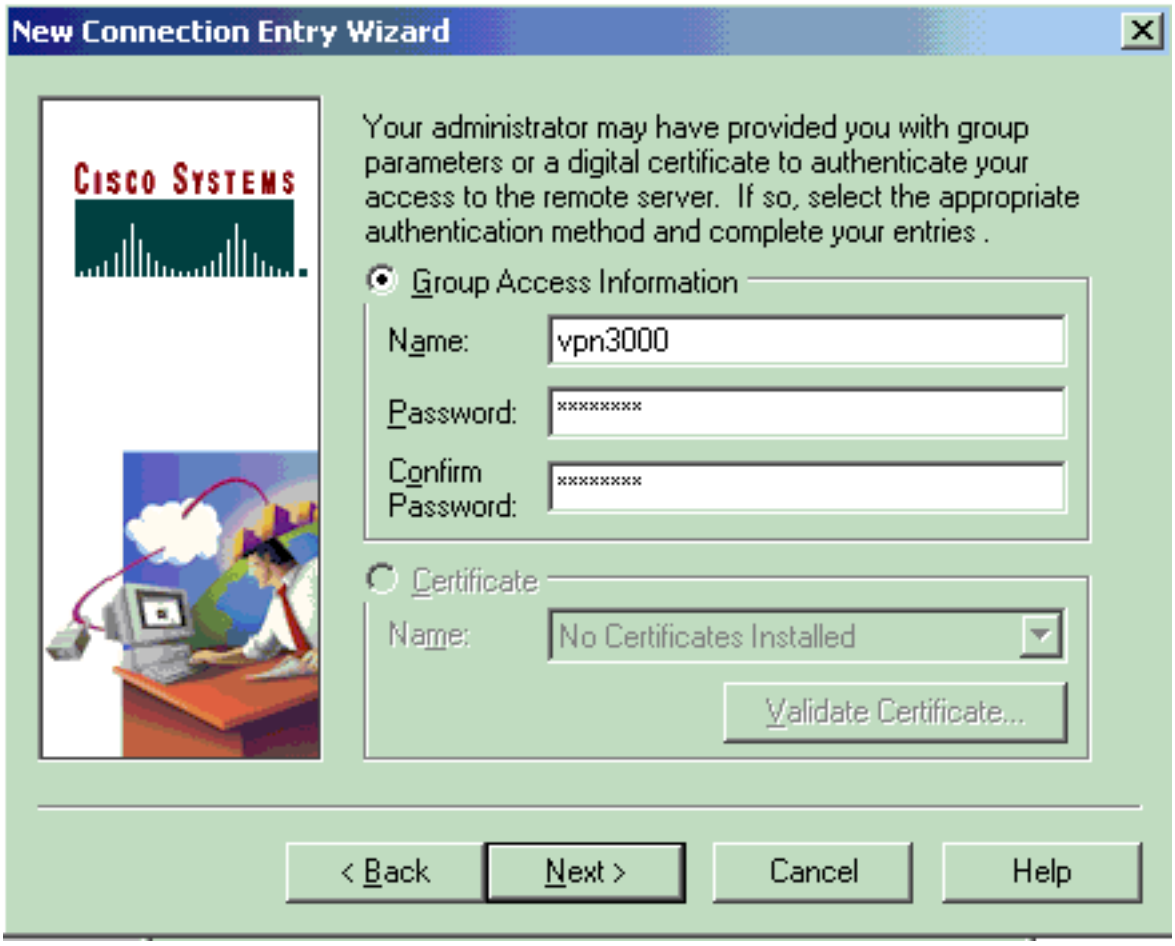
2. Connection Entry ボックスで、エントリに名前を割り当てます。



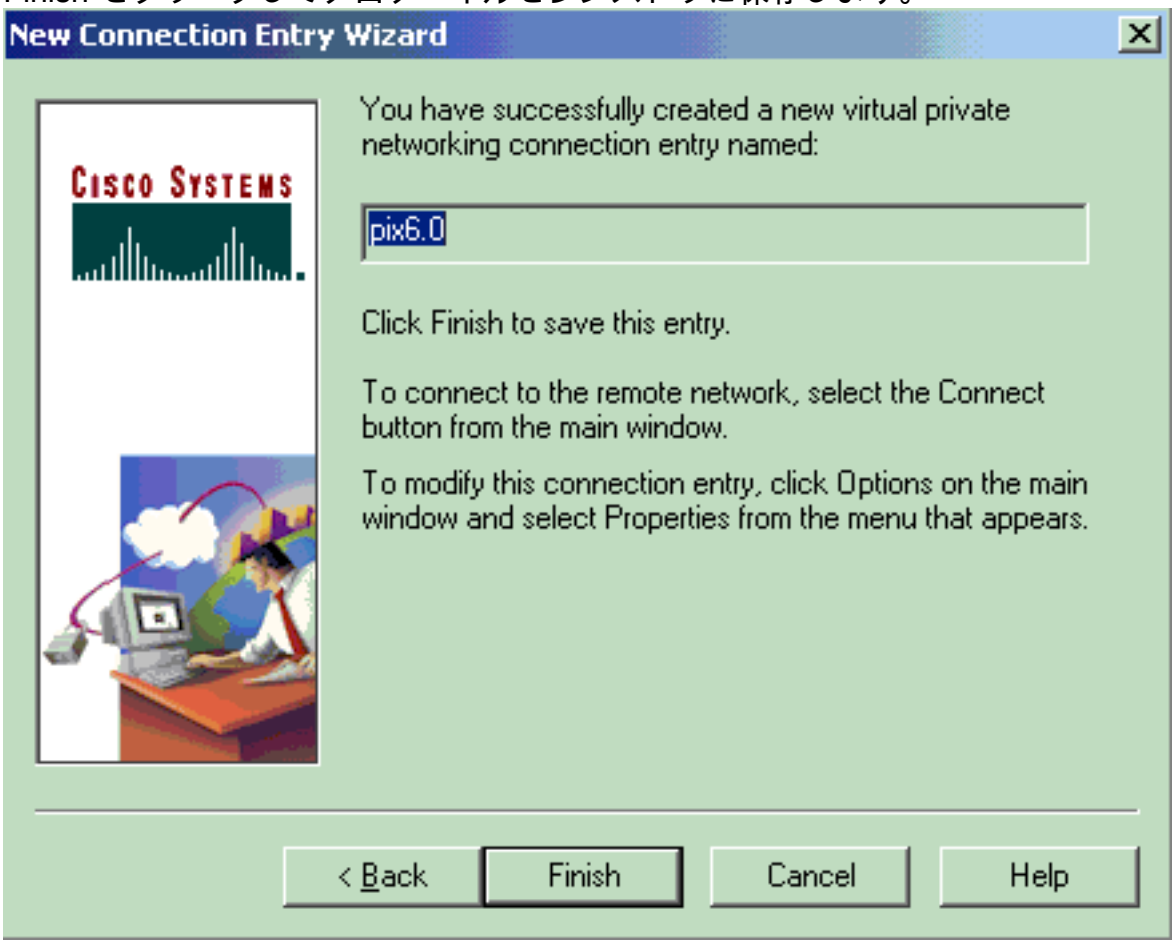
3. PIXのパブリックインターフェイスのIPアドレスを入力します。



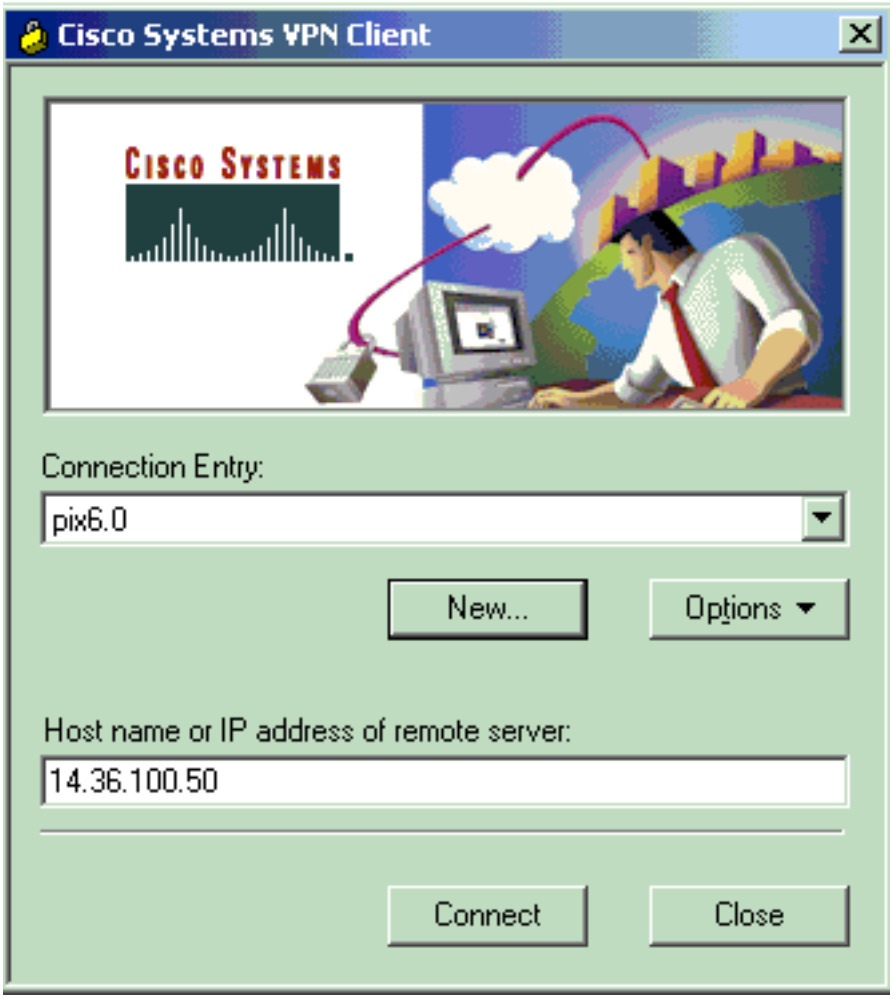
4. [Group Access Information] で、グループ名とグループパスワードを入力します。



5. Finish をクリックしてプロファイルをレジストリに保存します。



6. Connect をクリックして PIX に接続します。

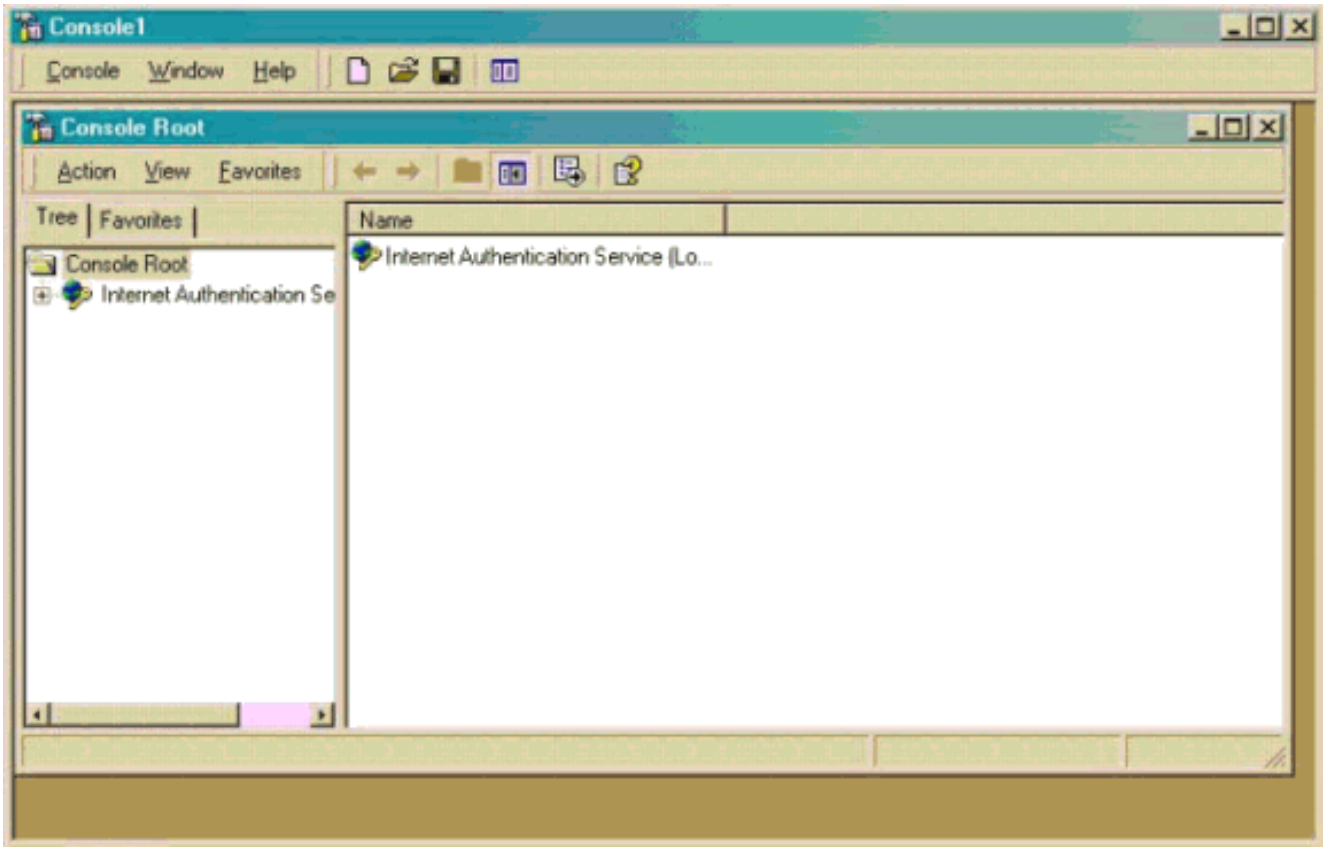


IAS がインストールされた Microsoft Windows 2000 サーバ

IAS がインストール Microsoft Windows 2000 サーバを設定するには、次の手順を実行します。これは、VPNユーザのRADIUS認証にWindows 2000 IASサーバを使用するための非常に基本的な設定です。より複雑な設計が必要な場合は、Microsoftにお問い合わせください。

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。

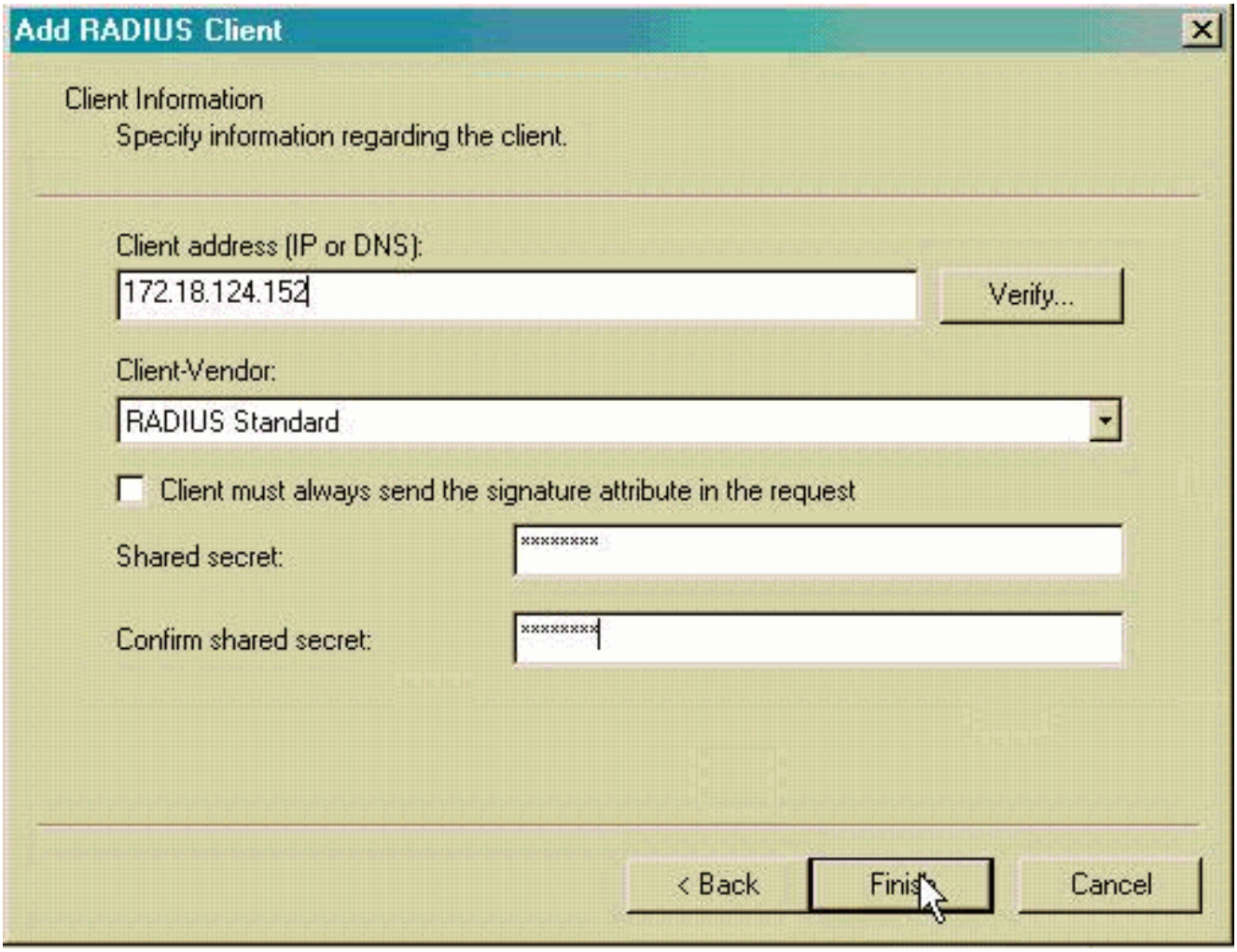
1. Microsoft管理コンソールを起動します。**Start > Run**の順に選択**し、**mmcと入力**します。**次に [OK] をクリックします。
2. [コン**ソール] > [スナップインの削除...]を選択します。**.IASサービスをこのコンソールに追加します。
3. [Add]をクリックして、使用可能なすべてのスタンドアロンスナップインを含む新しいウィンドウを起動します。[Internet Authentication Service (IAS)]**をクリックし、**[Add]をクリック**します。**
4. [ローカルコンピュー**タ]が選択され**ていることを確認し、[完了]をク**リックします。**次に、[閉じる]を**クリックします。**
5. IASが追加されました。[OK]をクリックして、コンソールルートに追加されたことを確認します。



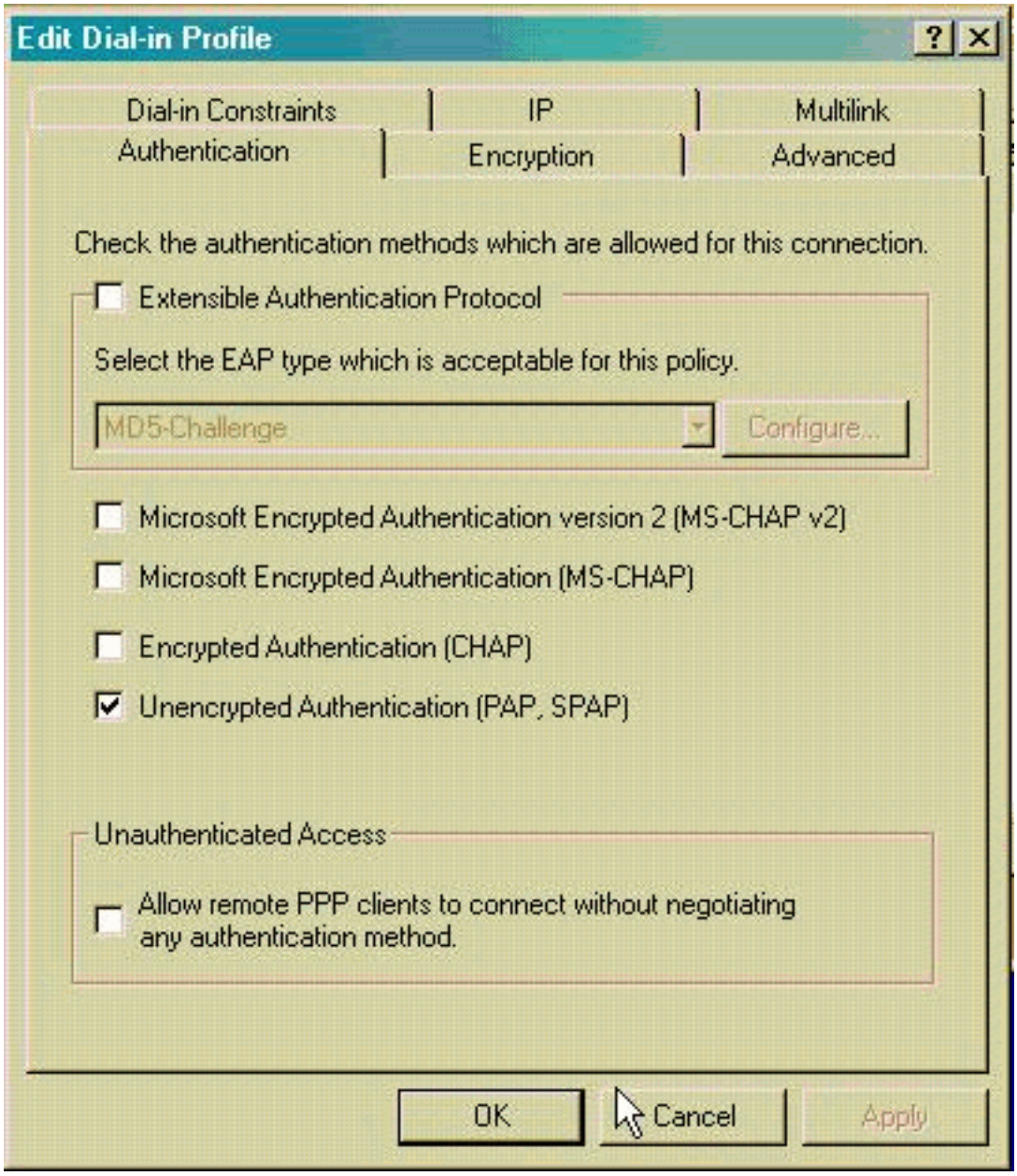
6. [Internet Authentication Service]を展開し、[Clients]を右クリックします。「新規クライアント」をクリックし、名前を入力します。名前の選択は重要ではありません。このビューで表示されるものです。必ず[RADIUS]を選択し、[Next]をクリックしてください。
7. IASサーバが接続されているPIXインターフェースのアドレスをクライアントアドレスに入力します。RADIUS Standardを選択し、PIXで入力したコマンドに一致する共有秘密を追加します。

```
aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
```

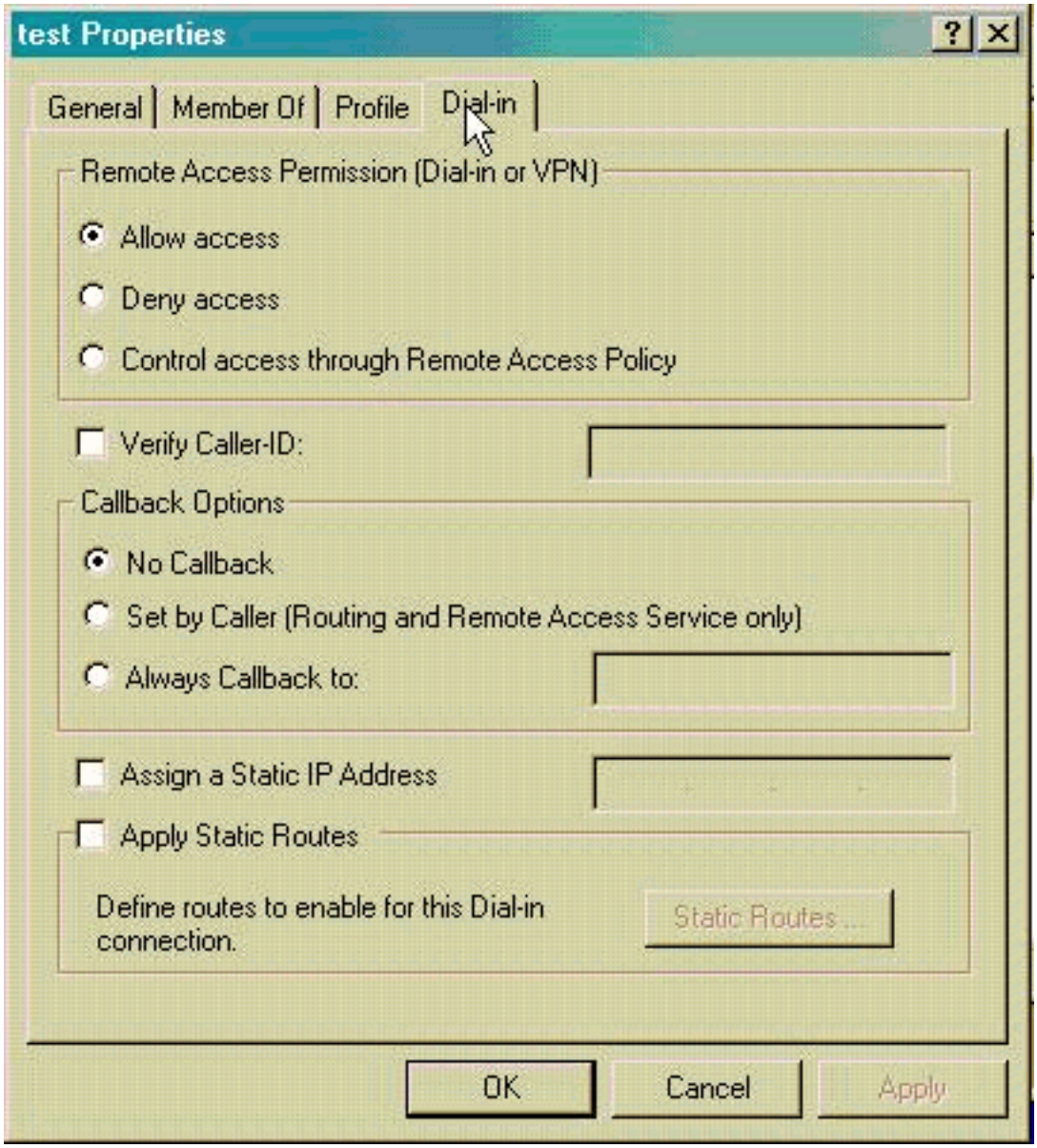
注：この例では、「cisco123」は共有秘密です。



8. [Finish]をクリックして、コンソールルートに戻ります。
9. 左側のペインで[Remote Access Policies]をクリックし、[Allow access if dial-in permission is enabled]というポリシーをダブルクリックします。
10. [Edit Profile]をクリックし、[Authentication]タブに移動します。[Authentication Methods]で、[Unencrypted Authentication (PAP, SPAP)]だけがオンになっていることを確認します。
    注：VPN Clientは、認証にこの方式のみを使用できます。



11. [Apply]をクリックし、[OK]を2回クリックします。
12. 接続を許可するようにユーザを変更するには、[Console] > [Add/Remove Snap-in]を選択します。[Add]をクリックし、[Local Users and Groups]スナップインを選択します。[Add] をクリックします。必ず[ローカルコンピュータ]を選択し、[完了]をクリックしてください。[OK] をクリックします。
13. [ローカルユーザーとグループ]を展開し、左側のペインの[ユーザー]フォルダをクリックします。右側のペインで、アクセスを許可するユーザをダブルクリックします。
14. [Dial-in]タブをクリックし、[Remote Access Permission (Dial-inまたはVPN)]の下の[Allow Access]を選択します。



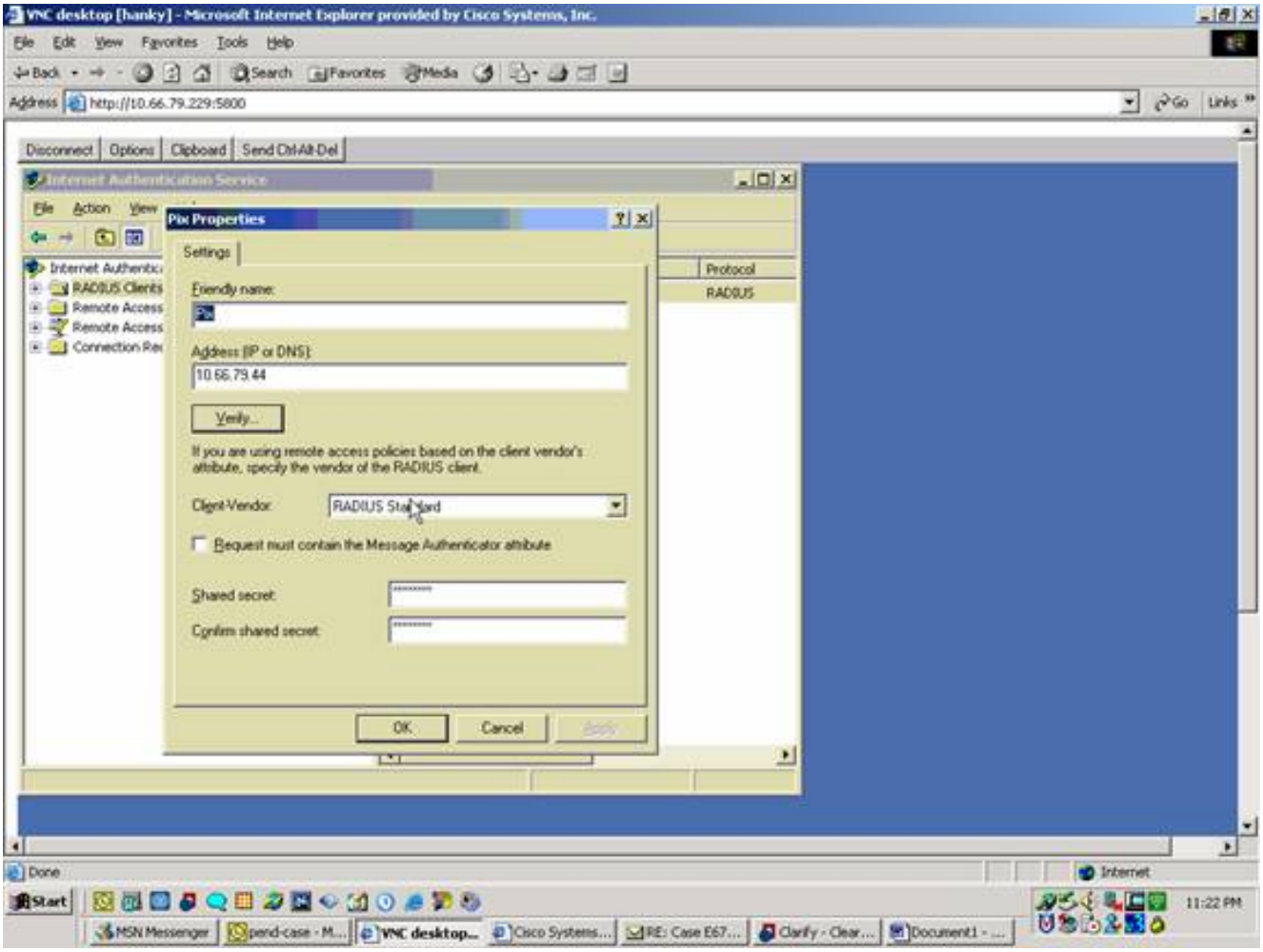
15. [Apply]をクリックし、**[OK]をクリック**してアクションを完了します。必要に応じて、[コンソール管理]画面を閉じてセッションを保存できます。
16. 変更したユーザは、VPN Client 3.5を使用してPIXにアクセスできます。IASサーバがユーザ情報を認証するだけであることに注意してください。PIXはグループ認証を行います。

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

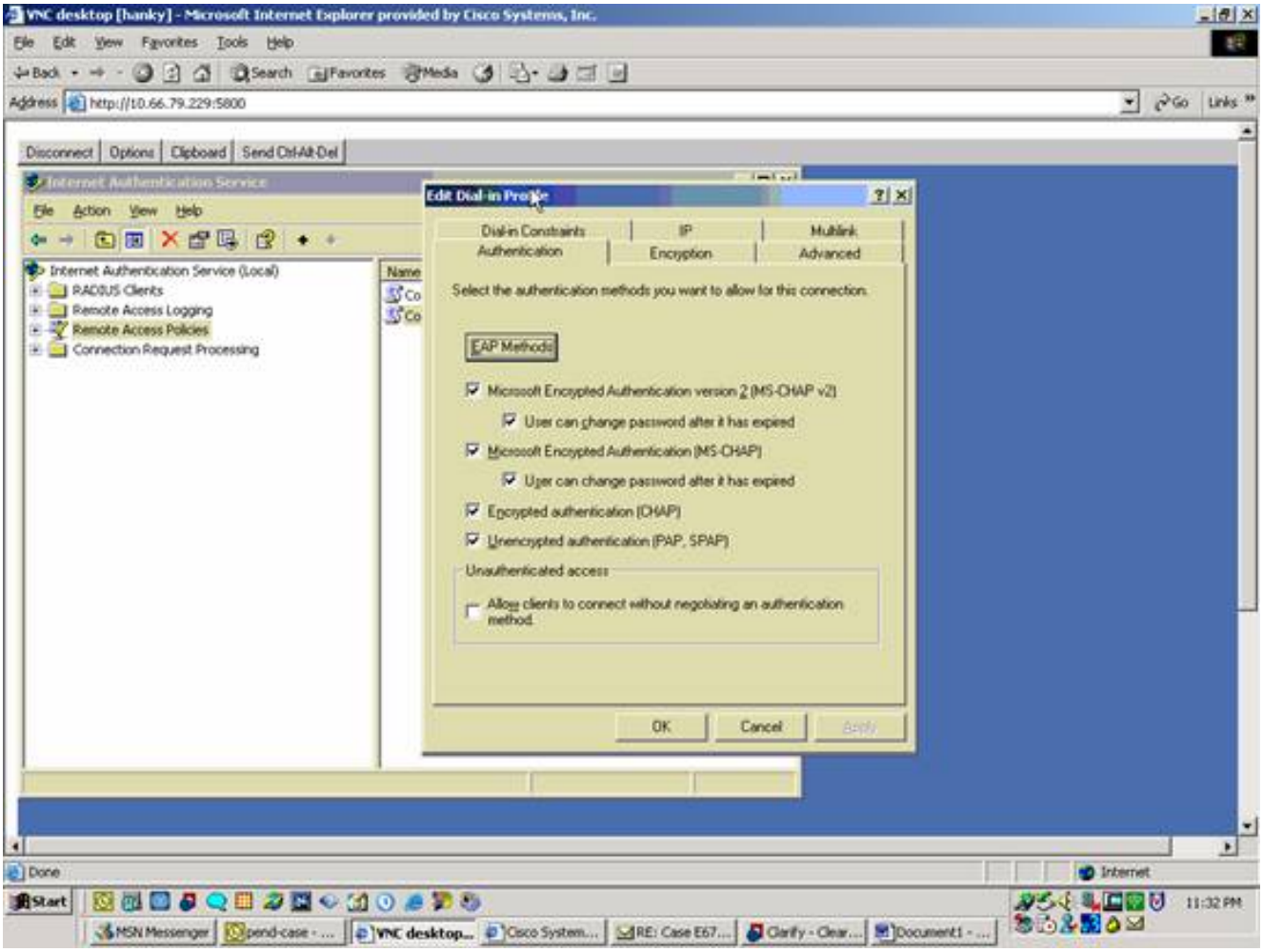
IAS がインストール Microsoft Windows 2003 サーバを設定するには、次の手順を実行します。

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。

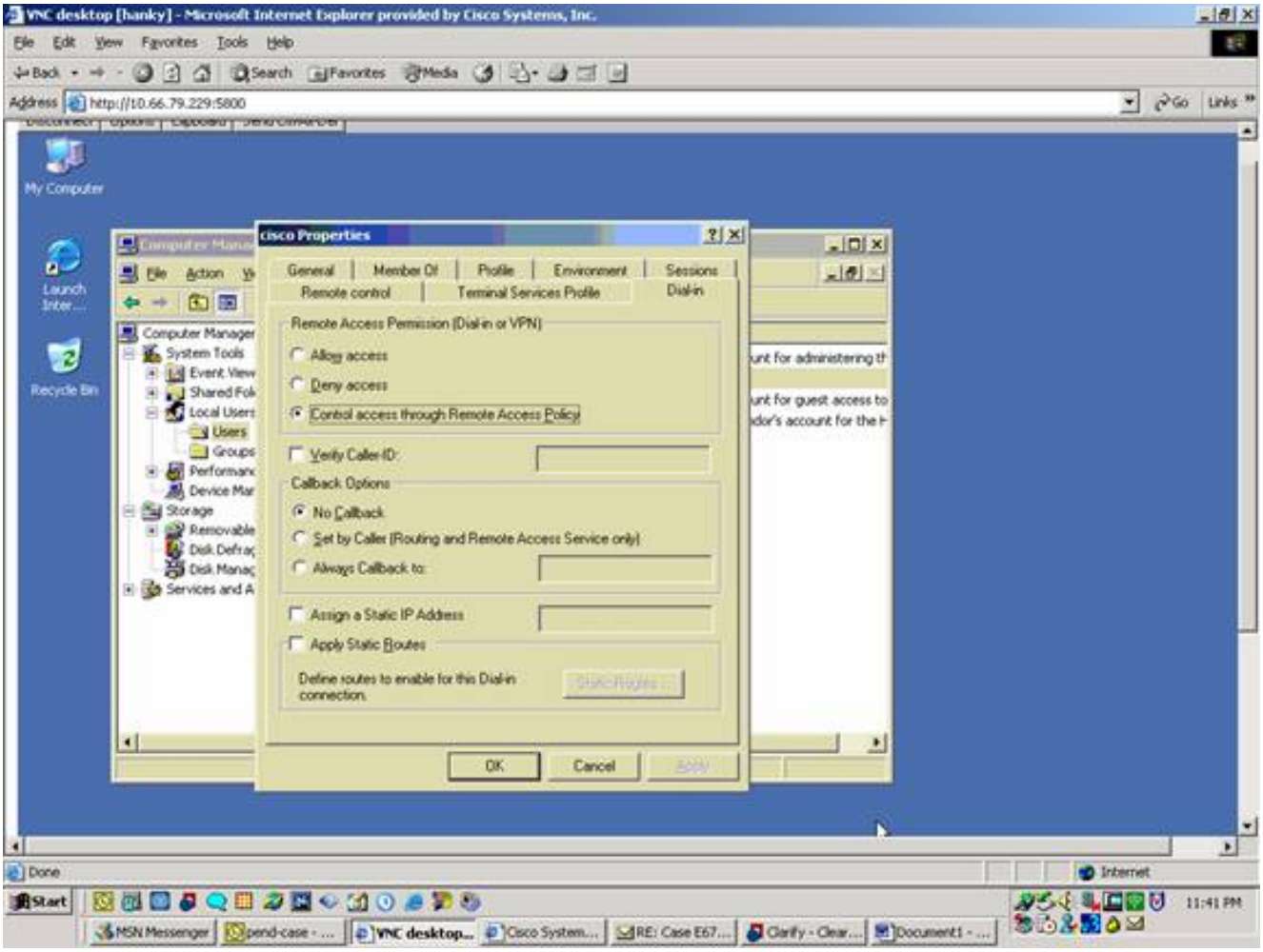
1. **Administrative Tools > Internet Authentication Serviceの順に選択**し、**RADIUS Clientを右クリック**して、新しいRADIUSクライアントを追加します。クライアント情報を入力したら、**OK** をクリックします。次の例は、IPアドレスが10.66.79.44の「Pix」という名前のクライアントを示しています。Client-VendorはRADIUS Standardに、共有秘密は「cisco123」に設定されています。



2. [Remote Access Policies] に移動して、[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. [プロファイルの編集]をクリックし、これら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. ローカルコンピュータアカウントにユーザを追加します。これを行うには、[Administrative Tools] > [**Computer Management] > [System Tools] > [Local Users and Groups]の順に選択します。**[Users]を右クリックし、[**New** Users]を選択**します。**
6. シスコパスワード「cisco123」のユーザを追加し、こ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。[ダイヤルイン]タブで、[アクセスを許可する]オプションを選択します(**または、既定の設定**の[リモートアクセスポリシーによるコントロールアクセス]のままにします)。完了したら、[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。

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

- **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**：現在のセキュリティアソシエーションで使用されている設定を表示します。

トラブルシュート

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。詳細は、『確立されたIPSecトンネルでデータトラフィックを渡すためのPIXのトラブルシューティング』を参照してください。

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は、『debugコマンドの重要な情報』を参照して、『IP Securityのトラブルシューティング：debugコマンドの理解と使用』を参照してください。

- **debug crypto ipsec：フェーズ 2 の IPSec ネゴシエーションを表示します。**
- **debug crypto isakmp**：フェーズ1のISAKMPネゴシエーションを表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。

デバッグの出力例

- PIX ファイアウォール
- VPN Client 3.5 for Windows

PIX ファイアウォール

```
pixfirewall(config)#
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
   Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
```

```
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 14.36.100.55
ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
   a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
   (0xe6b4ec14)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
   (0xd755b422)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
```

```
   message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
        Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
        Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
        Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
        Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
        Unsupported Attr: 28680
ISAKMP: attribute    UNKNOWN (28677)
        Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 14.36.100.55.
   ID = 3979868003
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1527320241

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (2)
```

```
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (6)
ISAKMP : Checking IPSec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
   proposal part #1,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1),
    src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
ISAKMP (0): processing NONCE payload. message ID = 1527320241

ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
   0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
        from    14.36.100.55 to    14.36.100.50 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3487980779

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to    14.36.100.50)
        has spi 4087095831 and conn_id 1 and flags 4
        lifetime of 2147483 seconds
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy    14.36.100.50 to        10.1.2.1)
        has spi 1929305241 and conn_id 2 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to         0.0.0.0)
        has spi 1791135440 and conn_id 3 and flags 4
        lifetime of 2147483 seconds
```

```
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy         0.0.0.0 to        10.1.2.1)
        has spi 173725574 and conn_id 4 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 3443334051
ISAMKP (0): received DPD_R_U_THERE from peer 14.36.100.55
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
```

VPN Client 3.5 for Windows

```
193    19:00:56.073  01/24/02  Sev=Info/6       DIALER/0x63300002
Initiating connection.

194    19:00:56.073  01/24/02  Sev=Info/4       CM/0x63100002
Begin connection process

195    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100004
Establish secure connection using Ethernet

196    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100026
Attempt connection with server "14.36.100.50"

197    19:00:56.083  01/24/02  Sev=Info/6       IKE/0x6300003B
Attempting to establish a connection with 14.36.100.50.

198    19:00:56.124  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 14.36.100.50

199    19:00:56.774  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

200    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

201    19:00:59.539  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
from 14.36.100.50

202    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
```

```
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

203    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer is a Cisco-Unity compliant peer

204    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

205    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer supports DPD

206    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

207    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 14.36.100.50

208    19:00:59.569  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

209    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

210    19:00:59.569  01/24/02  Sev=Info/4       CM/0x63100015
Launch xAuth application

211    19:01:04.236  01/24/02  Sev=Info/4       CM/0x63100017
xAuth application returned

212    19:01:04.236  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

213    19:01:04.496  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

214    19:01:04.496  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

215    19:01:04.496  01/24/02  Sev=Info/4       CM/0x6310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

216    19:01:04.506  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

217    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005D
Client sending a firewall request to concentrator

218    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Policy Push).

219    19:01:04.516  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

220    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

221    19:01:04.586  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

222    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
value = 10.1.2.1
```

```
223    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): ,
value = 10.1.1.2

224    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS)
: , value = 10.1.1.2

225    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: ,
value = cisco.com

226    19:01:04.586  01/24/02  Sev=Info/4       CM/0x63100019
Mode Config data received

227    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 14.36.100.50,
GW IP = 14.36.100.50

228    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

229    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 14.36.100.50

230    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

231    19:01:04.786  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

232    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

233    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

234    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

235    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

236    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

237    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI =
0xF39C2217 INBOUND SPI = 0x72FEDC99)

238    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xF39C2217

239    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x72FEDC99

240    19:01:05.948  01/24/02  Sev=Info/4       CM/0x6310001A
One secure connection established

241    19:01:05.988  01/24/02  Sev=Info/6       DIALER/0x63300003
Connection established.
```

```
242    19:01:06.078  01/24/02  Sev=Info/6       DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

243    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

244    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

245    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

246    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

247    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

248    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI =
0x6AC28ED0 INBOUND SPI = 0x0A5AD786)

249    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x6AC28ED0

250    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0A5AD786

251    19:01:06.118  01/24/02  Sev=Info/4       CM/0x63100022
Additional Phase 2 SA established.

252    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

253    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x17229cf3 into key list

254    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

255    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x99dcfe72 into key list

256    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

257    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0xd08ec26a into key list

258    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

259    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x86d75a0a into key list

260    19:01:15.032  01/24/02  Sev=Info/6       IKE/0x6300003D
Sending DPD request to 14.36.100.50, seq# = 152233542

261    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 14.36.100.50
```

```
262    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

263    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)
from 14.36.100.50

264    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300003F
Received DPD ACK from 14.36.100.50, seq# received = 152233542,
seq# expected = 152233542
```

関連情報

- PIX に関するサポート ページ
- PIX コマンド リファレンス
- RADIUS に関するサポート ページ
- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート 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 (RFCs)
- テクニカルサポート - Cisco Systems