

Cisco Secure PIX Firewall 6.x und Cisco VPN Client 3.5 für Windows mit Microsoft Windows 2000 und 2003 IAS RADIUS-Authentifizierung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Beispielausgabe für Debugging](#)

[Zugehörige Informationen](#)

Einführung

Diese Beispielkonfiguration zeigt, wie Cisco VPN Client Version 3.5 für Windows und die Cisco Secure PIX Firewall für die Verwendung mit dem Microsoft Windows 2000 und 2003 Internet Authentication Service (IAS) RADIUS Server konfiguriert wird. Weitere Informationen finden Sie unter [Microsoft - Checkliste: Konfiguration von IAS für Einwahl- und VPN-Zugriff](#) für weitere Informationen zu IAS.

Weitere Informationen zum gleichen Szenario in PIX/ASA 7.0 mit Cisco VPN Client 4.x finden Sie unter [PIX/ASA 7.x und Cisco VPN Client 4.x für Windows mit Microsoft Windows 2003 IAS RADIUS Authentication Configuration Example](#).

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Die Cisco Secure PIX Firewall Software 6.0 unterstützt VPN-Verbindungen vom Cisco VPN Client 3.5 für Windows.

- Bei dieser Beispielkonfiguration wird davon ausgegangen, dass das PIX bereits mit den entsprechenden Statistiken, Kanälen oder Zugriffslisten betrieben wird. Im vorliegenden Dokument werden diese grundlegenden Konzepte nicht erläutert, sondern die Anbindung an das PIX über einen Cisco VPN Client.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Firewall Software Version 6.1.1 **Hinweis:** Dies wurde mit Version 6.1.1 der PIX-Software getestet, sollte jedoch mit allen 6.x-Versionen funktionieren.
- Cisco VPN Client Version 3.5 für Windows
- Windows 2000- und 2003-Server mit IAS

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

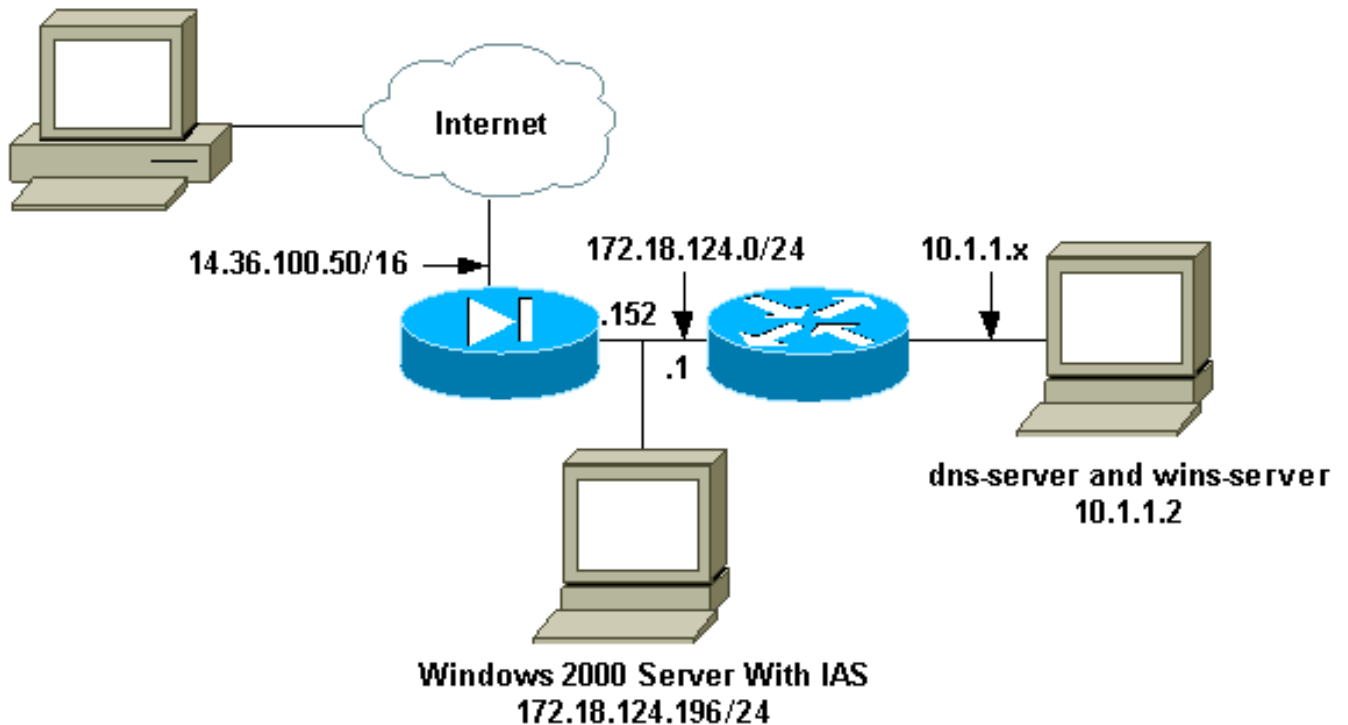
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

PC With VPN Client 3.5
14.36.100.55



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [PIX-Firewall](#)
- [Cisco VPN Client 3.5 für Windows](#)
- [Microsoft Windows 2000 Server mit IAS](#)
- [Microsoft Windows 2003 Server mit IAS](#)

PIX-Firewall

PIX-Firewall

```
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.

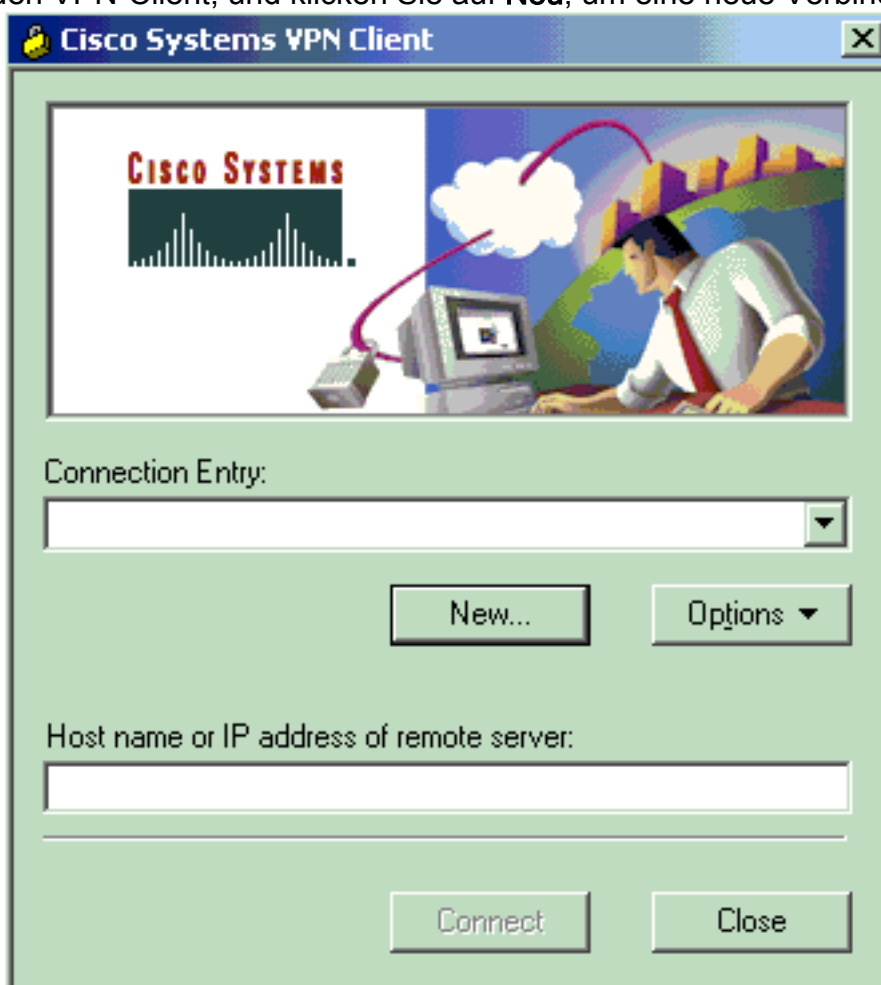
access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
    255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit 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)#
```

[Cisco VPN Client 3.5 für Windows](#)

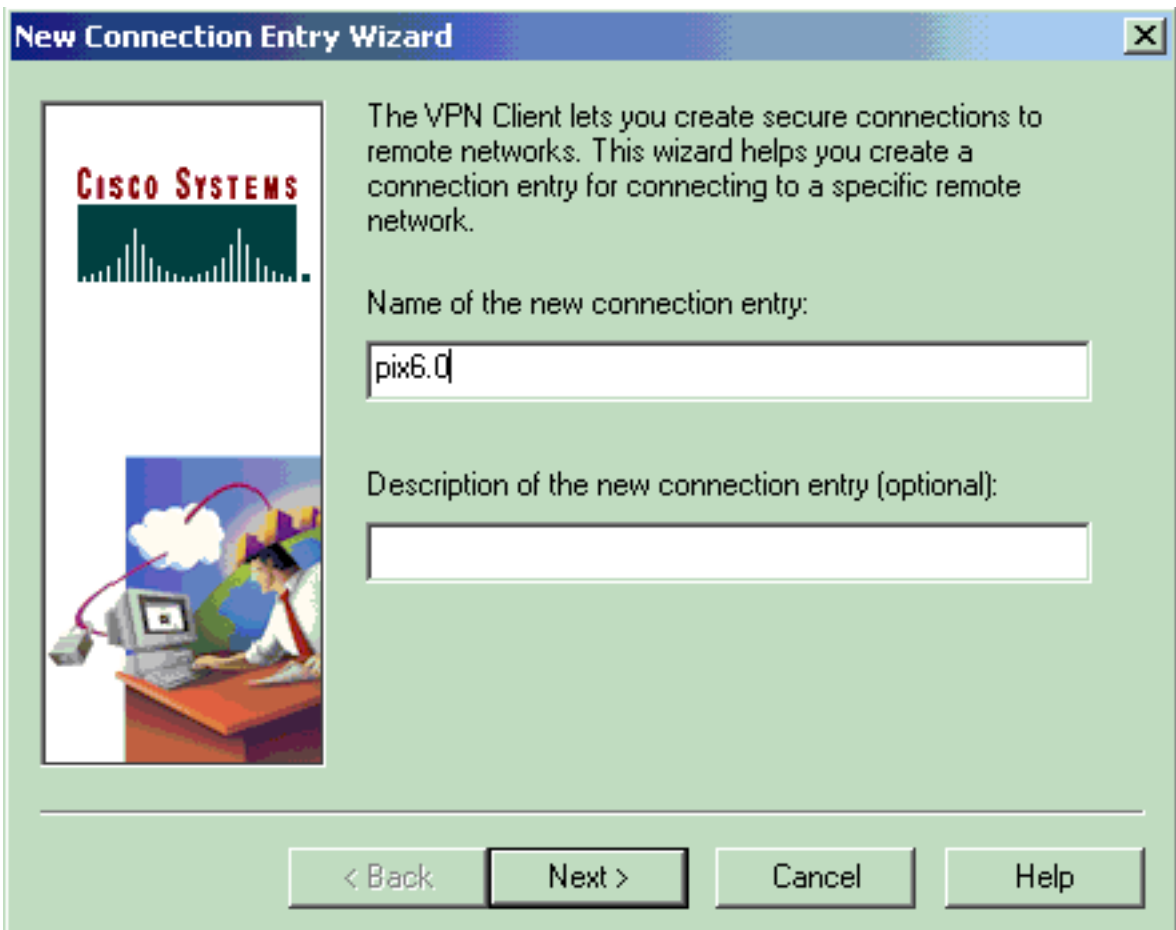
In diesem Abschnitt wird erläutert, wie der Cisco VPN Client 3.5 für Windows konfiguriert wird.

1. Starten Sie den VPN-Client, und klicken Sie auf **Neu**, um eine neue Verbindung



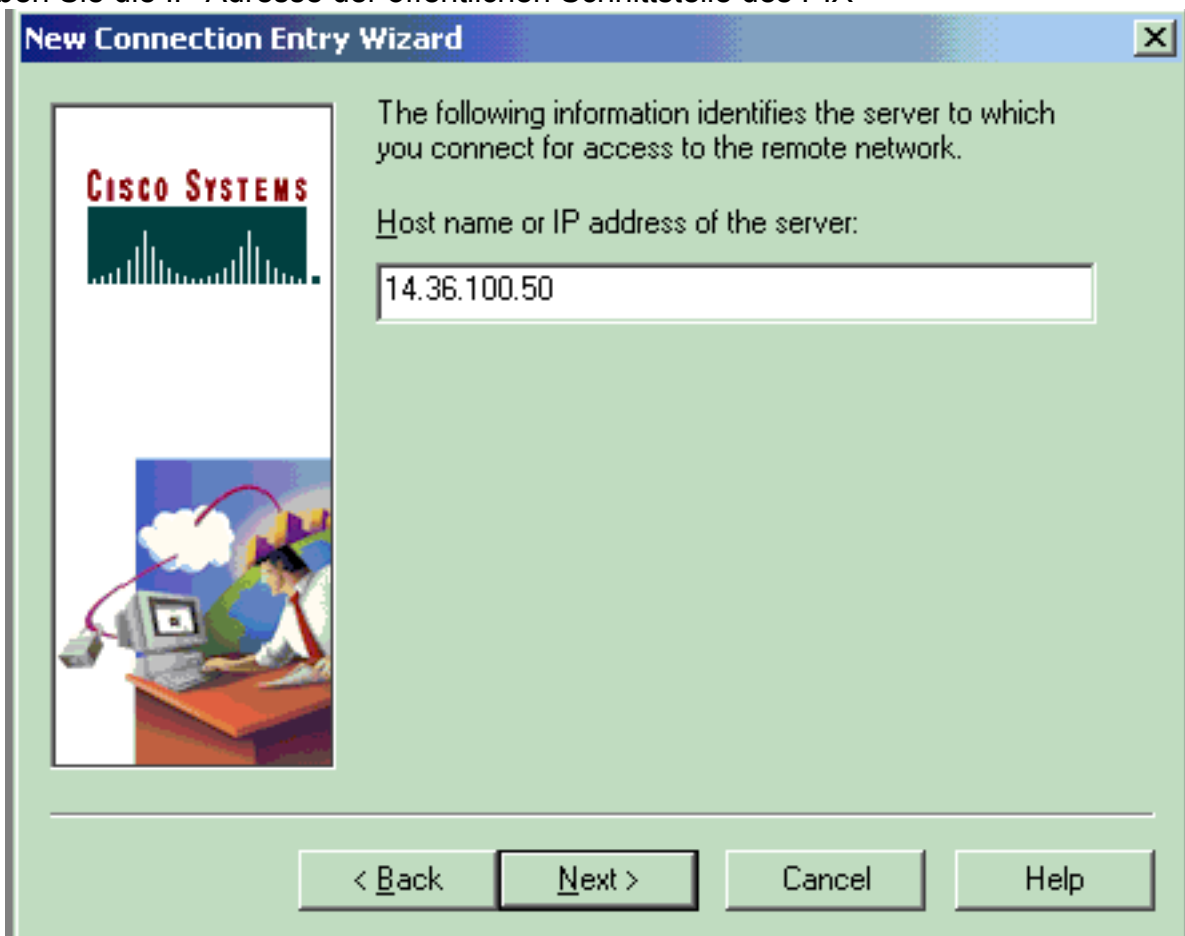
herzustellen.

2. Weisen Sie Ihrem Eintrag im Feld **Verbindungseintrag** einen Namen



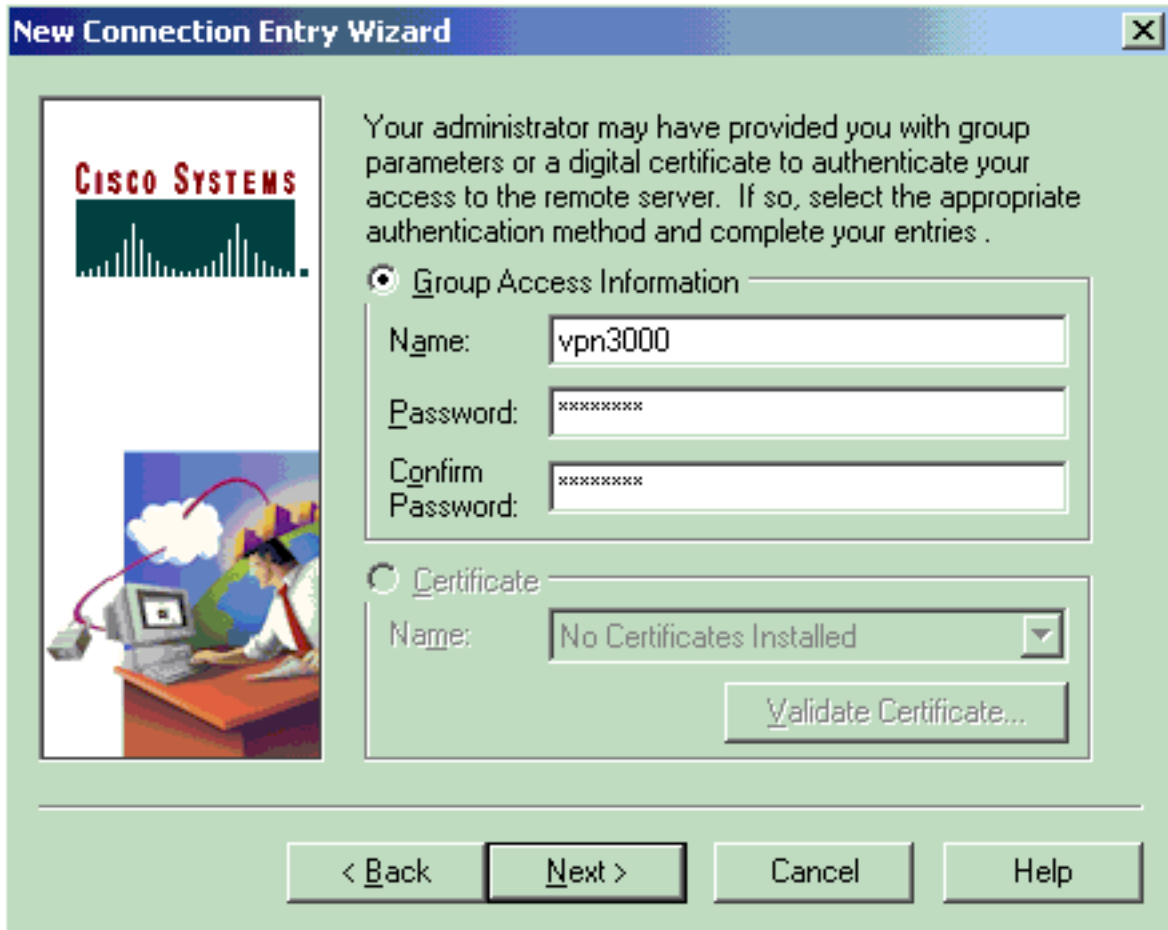
zu.

3. Geben Sie die IP-Adresse der öffentlichen Schnittstelle des PIX



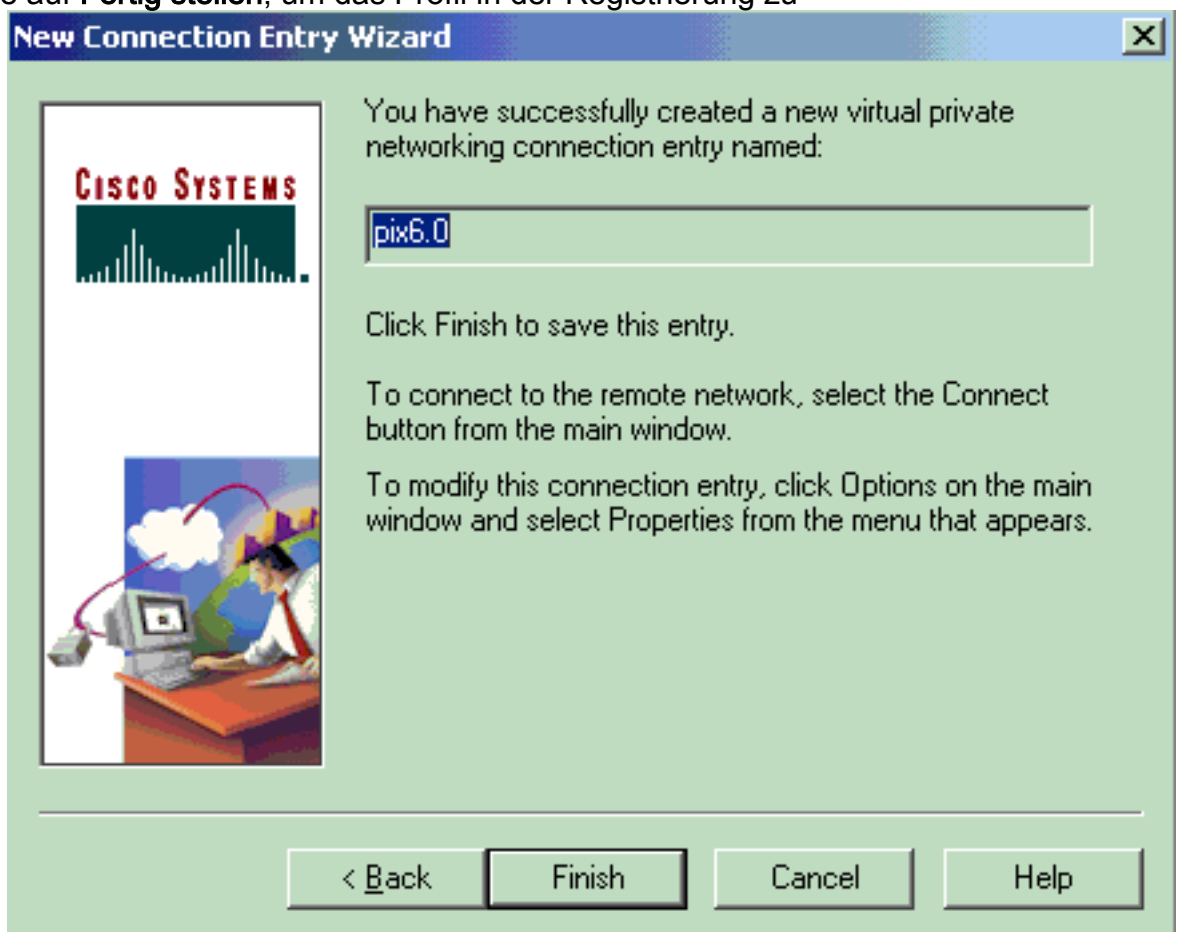
ein.

4. Geben Sie unter **Gruppenzugriffsinformationen** den Gruppennamen und das Gruppenkennwort



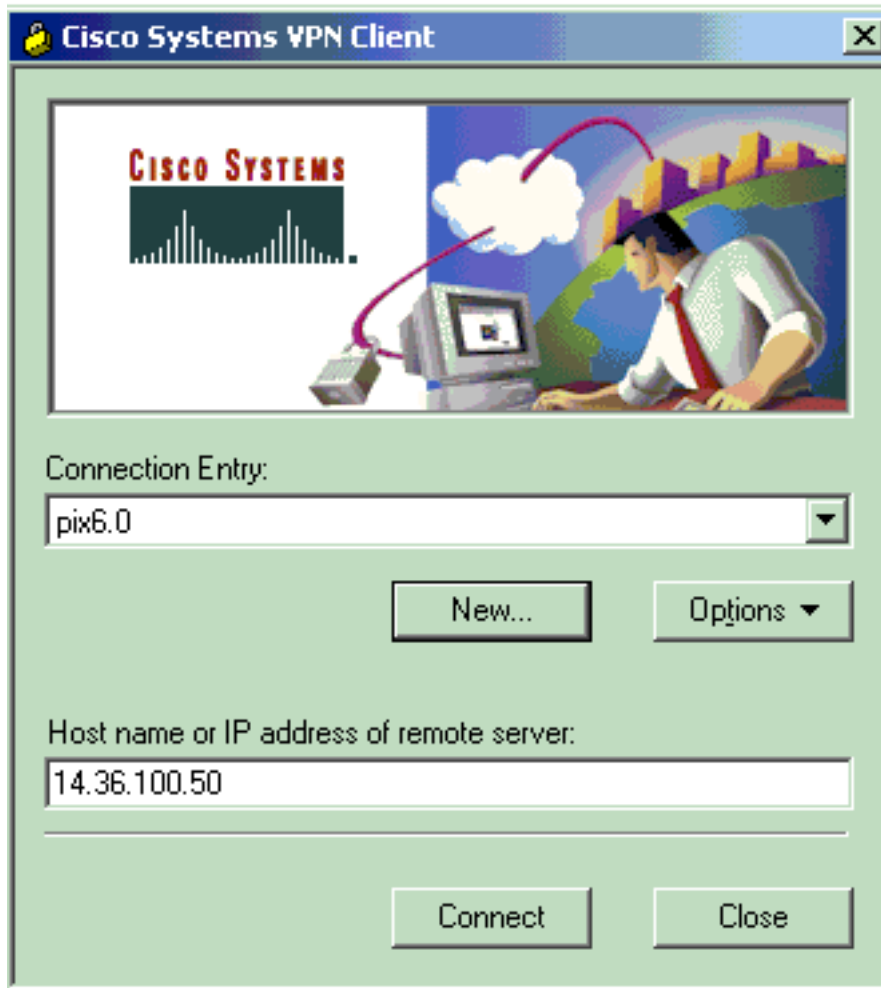
ein.

5. Klicken Sie auf **Fertig stellen**, um das Profil in der Registrierung zu



speichern.

6. Klicken Sie auf **Verbinden**, um eine Verbindung zum PIX



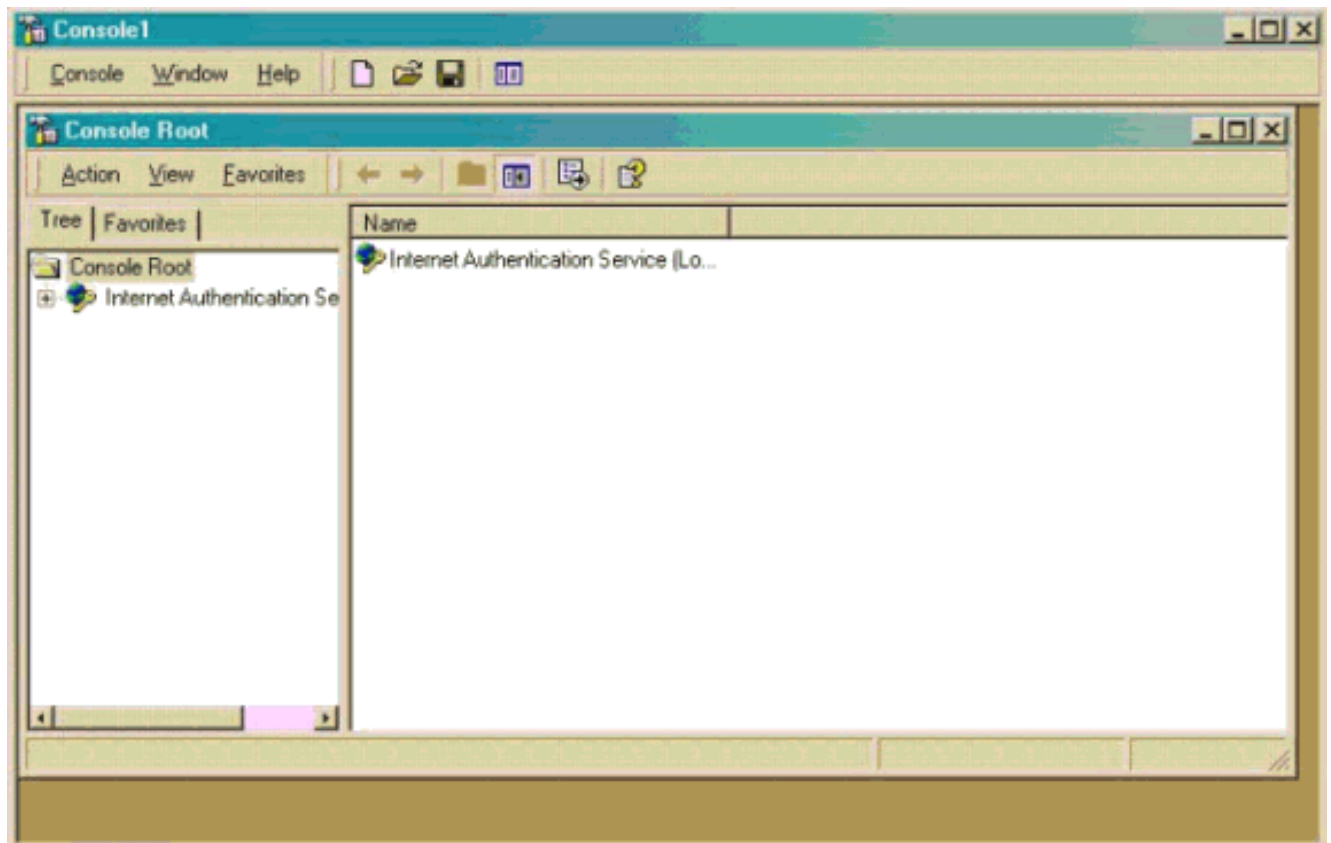
herzustellen.

[Microsoft Windows 2000 Server mit IAS](#)

Führen Sie diese Schritte aus, um den Microsoft Windows 2000-Server mit IAS zu konfigurieren. Dies ist eine sehr einfache Konfiguration zur Verwendung eines Windows 2000 IAS-Servers für die RADIUS-Authentifizierung von VPN-Benutzern. Wenn Sie ein komplexeres Design benötigen, wenden Sie sich an Microsoft, um Unterstützung zu erhalten.

Hinweis: Bei diesen Schritten wird davon ausgegangen, dass IAS bereits auf dem lokalen Computer installiert wurde. Falls nicht, fügen Sie dies über **Systemsteuerung > Software hinzu**.

1. Starten Sie die Microsoft Management Console. Wählen Sie **Start > Ausführen**, und geben Sie **mmc ein**. Klicken Sie anschließend auf **OK**.
2. Wählen Sie **Konsole > Snap-In entfernen aus....** um den IAS-Dienst dieser Konsole hinzuzufügen.
3. Klicken Sie auf **Hinzufügen**, um ein neues Fenster mit allen verfügbaren eigenständigen Snap-Ins zu öffnen. Klicken Sie auf **Internet Authentication Service (IAS)** und dann auf **Add**.
4. Vergewissern Sie sich, dass **Lokaler Computer** ausgewählt ist, und klicken Sie auf **Fertig stellen**. Klicken Sie anschließend auf **Schließen**.
5. Beachten Sie, dass IAS jetzt hinzugefügt wird. Klicken Sie auf **OK**, um anzuzeigen, dass der Console Root hinzugefügt wurde.



6. Erweitern Sie den **Internet Authentication Service**, und klicken Sie mit der rechten Maustaste auf **Clients**. Klicken Sie auf **Neuer Client**, und geben Sie einen Namen ein. Die Wahl des Namens spielt wirklich keine Rolle. wird es das sein, was Sie in dieser Ansicht sehen. Wählen Sie **RADIUS aus**, und klicken Sie auf **Weiter**.
7. Geben Sie die **Client-Adresse** mit der PIX-Schnittstellenadresse ein, mit der der IAS-Server verbunden ist. Wählen Sie den **RADIUS Standard** aus, und fügen Sie den geheimen Schlüssel hinzu, um dem auf dem PIX eingegebenen Befehl zu entsprechen:

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

Hinweis: In diesem Beispiel ist "cisco123" der gemeinsame geheime Schlüssel.

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
172.18.124.152 Verify...

Client-Vendor:
RADIUS Standard

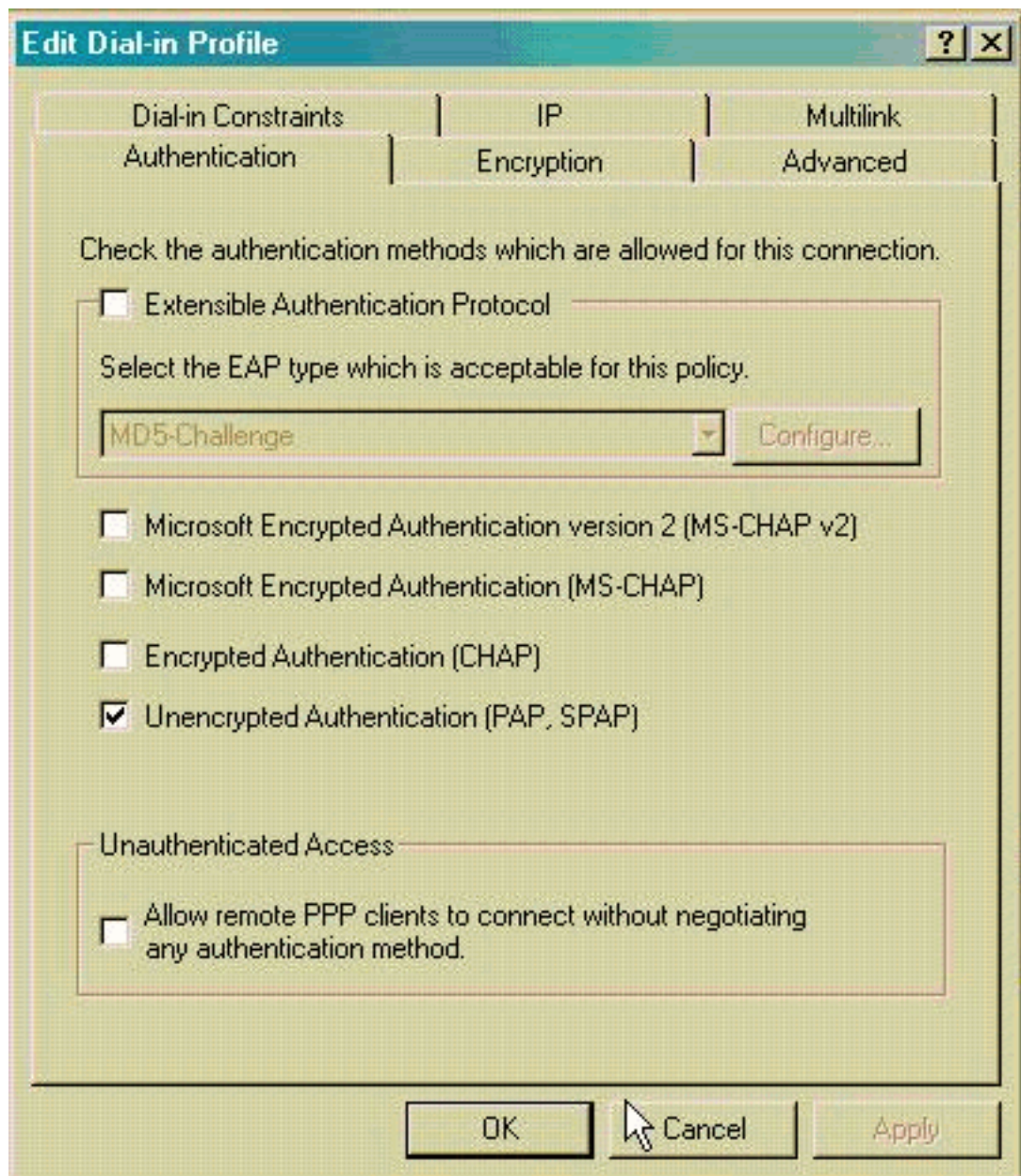
Client must always send the signature attribute in the request

Shared secret: xxxxxxxx

Confirm shared secret: xxxxxxxx

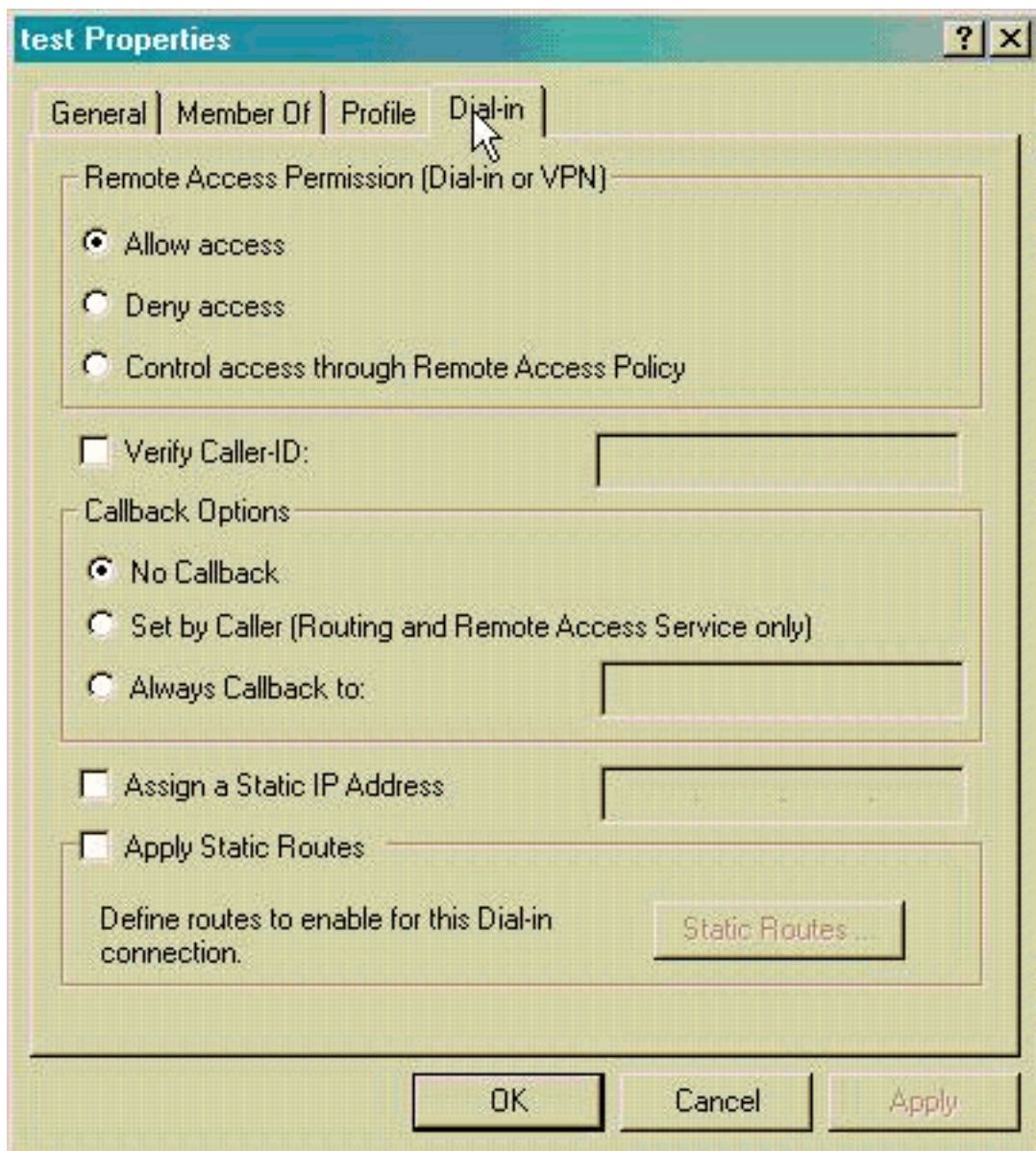
< Back Finish Cancel

8. Klicken Sie auf **Fertig stellen**, um zur Konsolenstamm zurückzukehren.
9. Klicken Sie im linken Bereich auf **Remote Access Policies (Remote-Zugriffsrichtlinien)**, und doppelklicken Sie auf die Richtlinie mit der Bezeichnung **Allow access (Zugriff zulassen)**, wenn die **Einwahlberechtigung aktiviert ist**.
10. Klicken Sie auf **Profil bearbeiten**, und wechseln Sie zur Registerkarte Authentifizierung. Stellen Sie sicher, dass unter **Authentifizierungsmethoden** nur **Uncrypted Authentication (PAP, SPAP)** aktiviert ist. **Hinweis:** Der VPN-Client kann diese Methode nur für die Authentifizierung



verwenden.

11. Klicken Sie auf **Übernehmen** und **OK** zweimal.
12. Um die Benutzer so zu ändern, dass eine Verbindung zulässig ist, wählen Sie **Konsole > Snap-In hinzufügen/entfernen aus**. Klicken Sie auf **Hinzufügen** und wählen Sie dann das **Snap-In Lokale Benutzer und Gruppen aus**. Klicken Sie auf **Hinzufügen**. Wählen Sie **Lokaler Computer aus** und klicken Sie auf **Fertig stellen**. Klicken Sie auf **OK**.
13. Erweitern Sie **Lokale Benutzer und Gruppen**, und klicken Sie im linken Bereich auf den Ordner **Benutzer**. Doppelklicken Sie im rechten Teilfenster auf den Benutzer, dem der Zugriff gewährt werden soll.
14. Klicken Sie auf die Registerkarte Dial-in (Einwählen), und wählen Sie **Allow Access** (Zugriff zulassen) unter **Remote-Zugriffsberechtigung (Einwahl oder VPN)**



aus.

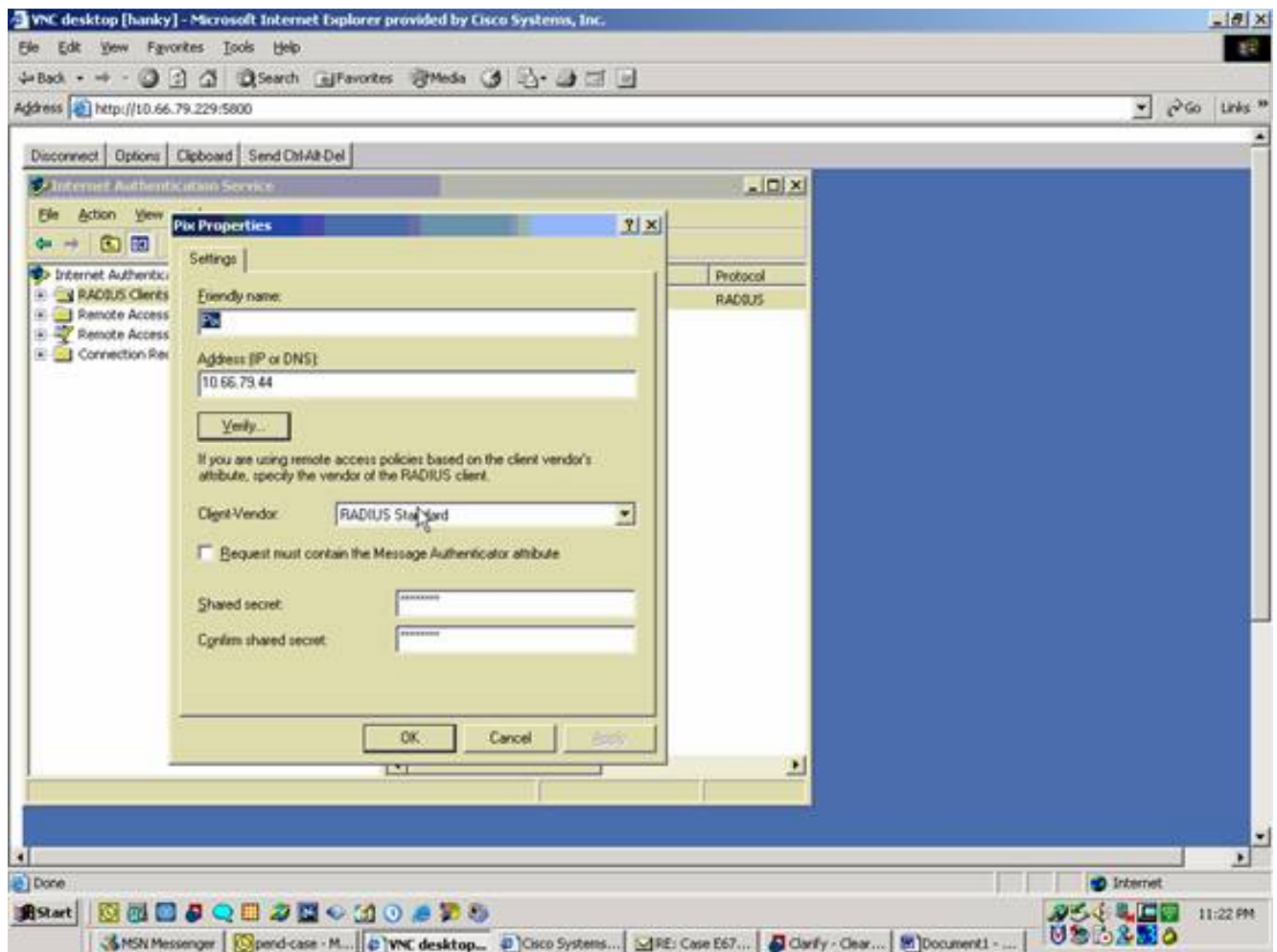
15. Klicken Sie auf **Übernehmen** und **OK**, um den Vorgang abzuschließen. Sie können den Bildschirm **Konsolenverwaltung** schließen und die Sitzung gegebenenfalls speichern.
16. Die von Ihnen geänderten Benutzer sollten nun über den VPN Client 3.5 auf das PIX zugreifen können. Beachten Sie, dass der IAS-Server nur die Benutzerinformationen authentifiziert. Der PIX führt weiterhin die Gruppenauthentifizierung durch.

[Microsoft Windows 2003 Server mit IAS](#)

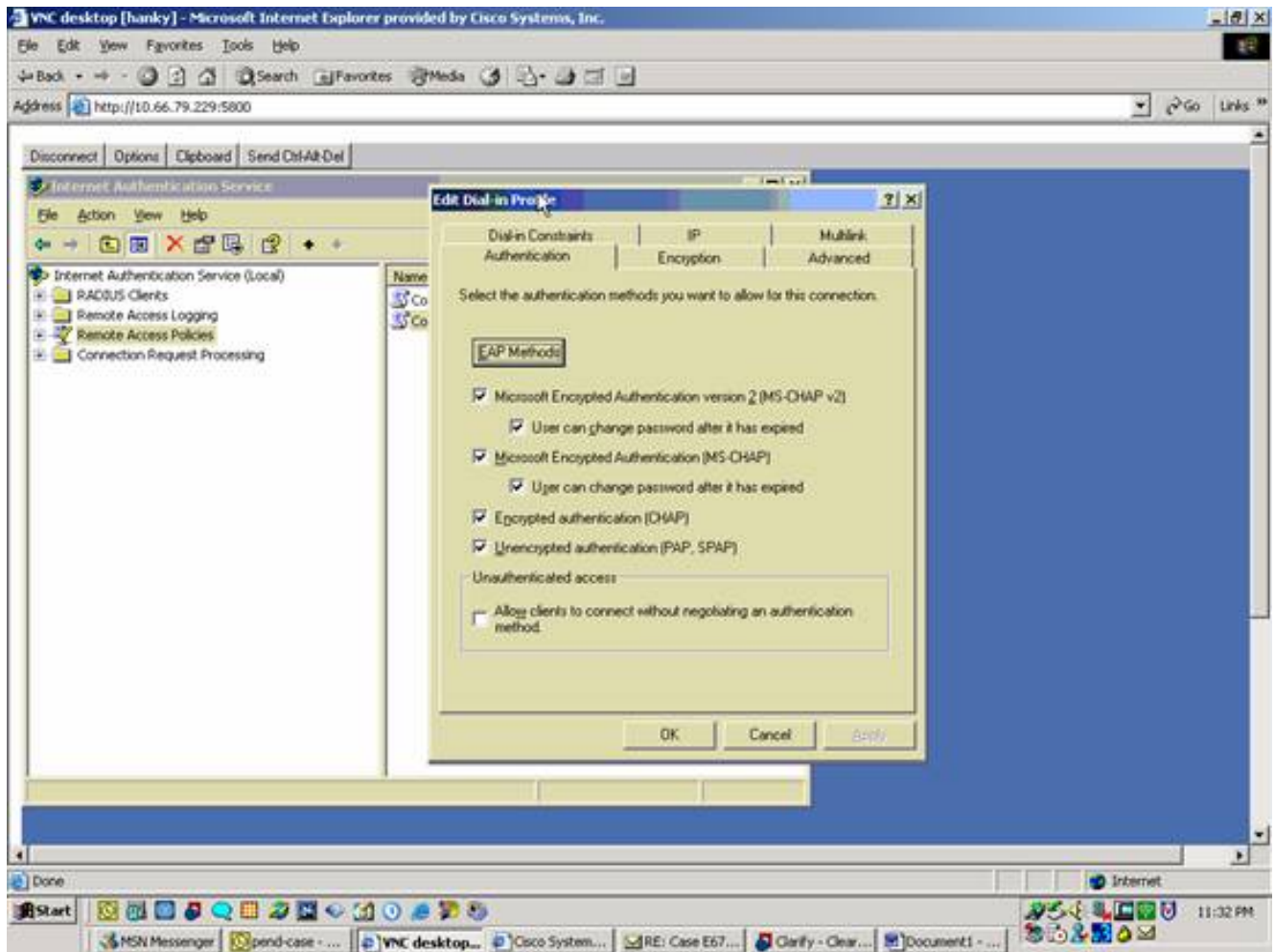
Führen Sie diese Schritte aus, um den Microsoft Windows 2003-Server mit IAS zu konfigurieren.

Hinweis: Bei diesen Schritten wird davon ausgegangen, dass IAS bereits auf dem lokalen Computer installiert wurde. Falls nicht, fügen Sie dies über **Systemsteuerung > Software** hinzu.

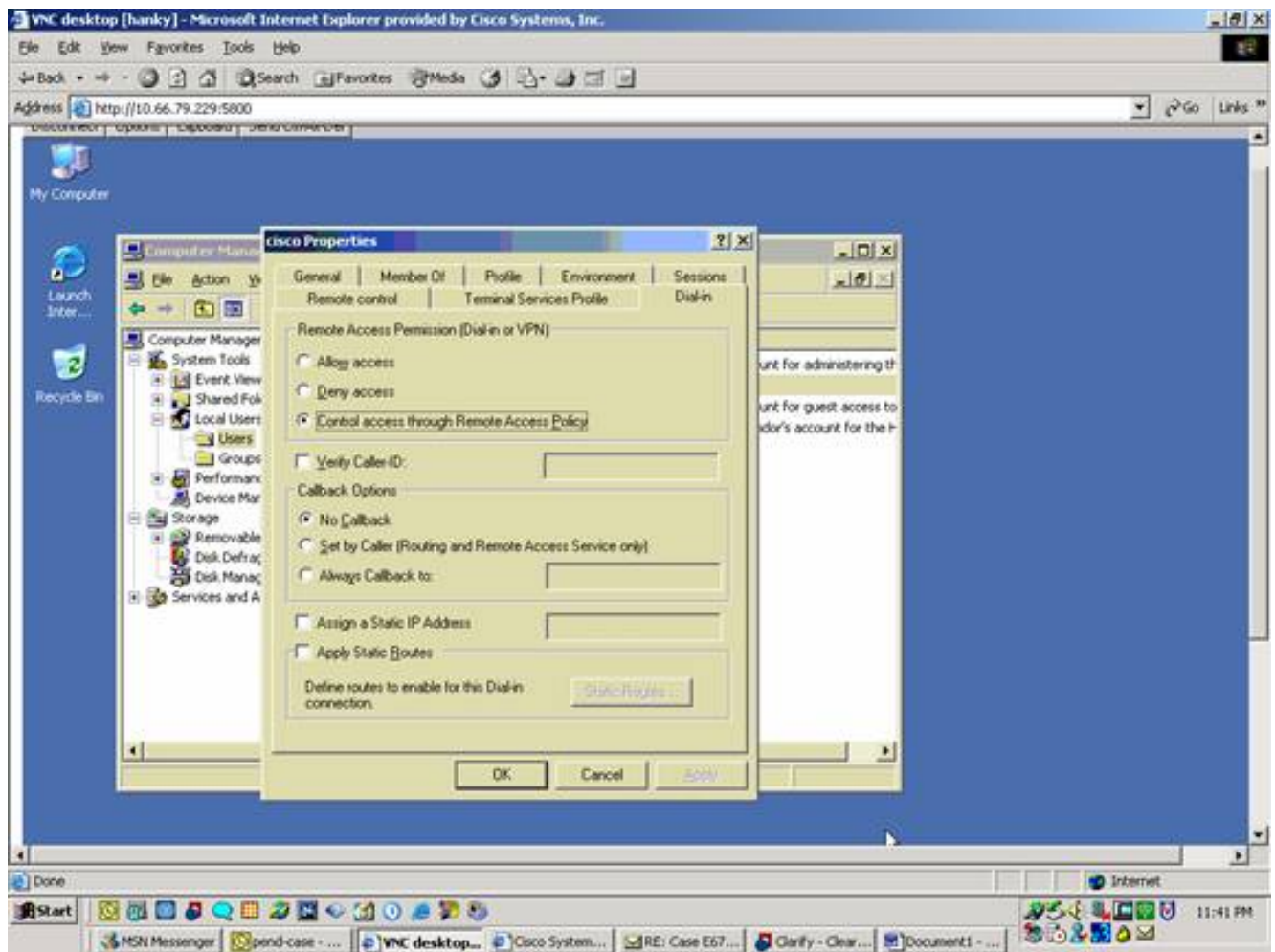
1. Wählen Sie **Verwaltung > Internet Authentication Service** und klicken Sie mit der rechten Maustaste auf **RADIUS Client**, um einen neuen RADIUS-Client hinzuzufügen. Nachdem Sie die Clientinformationen eingegeben haben, klicken Sie auf **OK**. Dieses Beispiel zeigt einen Client mit dem Namen "Pix" und einer IP-Adresse von 10.66.79.44. Der Client-Anbieter ist auf RADIUS Standard und der geheime Schlüssel auf "cisco123" gesetzt.



2. Gehen Sie zu **Remotezugriffsrichtlinien**, klicken Sie mit der rechten Maustaste auf **Verbindungen zu anderen Zugriffsservern**, und wählen Sie **Eigenschaften** aus.
3. Stellen Sie sicher, dass die Option "Remote-Zugriffsberechtigungen gewähren" ausgewählt ist.
4. Klicken Sie auf **Profil bearbeiten**, und überprüfen Sie diese Einstellungen. Aktivieren Sie auf der Registerkarte Authentifizierung die Option **Uncrypted Authentication (PAP, SPAP)**. Stellen Sie sicher, dass auf der Registerkarte Verschlüsselung die Option Keine Verschlüsselung ausgewählt ist. Klicken Sie abschließend auf **OK**.



5. Fügen Sie dem lokalen Computerkonto einen Benutzer hinzu. Wählen Sie dazu **Verwaltung > Computerverwaltung > Systemprogramme > Lokale Benutzer und Gruppen**.. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und wählen Sie **Neue Benutzer aus**.
6. Fügen Sie einen Benutzer mit dem Cisco Kennwort "cisco123" hinzu, und überprüfen Sie diese Profilinformationen. Stellen Sie auf der Registerkarte Allgemein sicher, dass die Option **Kennwort nie abgelaufen** anstelle der Option Kennwort ändern muss aktiviert ist. Wählen Sie auf der Registerkarte Dial-in (Einwählen) die Option **Allow access (Zugriff zulassen)** (oder belassen Sie die Standardeinstellung Control Access (Zugriffssteuerung über Remote-Zugriffsrichtlinie)). Klicken Sie abschließend auf **OK**.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe** des Befehls **show** anzuzeigen.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa**: Zeigt die von aktuellen Sicherheitszuordnungen verwendeten Einstellungen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration. Weitere Informationen finden Sie unter [Fehlerbehebung bei PIX zum Übergeben von Datenverkehr an einen etablierten IPSec-Tunnel](#).

Befehle zur Fehlerbehebung

Bestimmte Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **Ausgabe** von **show** Command anzeigen können.

Hinweis: Lesen Sie die [wichtigen Informationen über Debug-Befehle](#), bevor Sie **Debugbefehle** verwenden, und lesen Sie [IP-Sicherheitsfehlerbehebung - Verständnis und Verwenden von Debugbefehlen](#).

- **debug crypto ipsec** - Zeigen Sie die IPSec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp** - Zeigen Sie die ISAKMP-Verhandlungen für Phase 1 an.
- **debug crypto engine** - Zeigen Sie den verschlüsselten Datenverkehr an.

[Beispielausgabe für Debugging](#)

- [PIX-Firewall](#)
- [VPN Client 3.5 für Windows](#)

[PIX-Firewall](#)

```
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
    OIPSEC(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
```

```
ISAKMP (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 für 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

[Zugehörige Informationen](#)

- [PIX-Support-Seite](#)
- [PIX-Befehlsreferenzen](#)
- [RADIUS-Support-Seite](#)
- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [Cisco VPN Client Support-Seite der Serie 3000](#)
- [Support-Seite für IPsec-Aushandlung/IKE-Protokoll](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support - Cisco Systems](#)