Beispiel für eine Stick-Konfiguration: PIX/ASA und VPN-Client für Public Internet VPN

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine ASA Security Appliance 7.2 oder höher einrichten, um IPsec auf einem Stick auszuführen. Diese Konfiguration gilt für einen bestimmten Fall, in dem ASA kein Split-Tunneling zulässt und Benutzer eine direkte Verbindung mit der ASA herstellen, bevor sie das Internet nutzen dürfen.

Hinweis: In PIX/ASA Version 7.2 und höher ermöglicht das *Intra-Interface*-Schlüsselwort den gesamten Datenverkehr, dieselbe Schnittstelle einzugeben und zu verlassen, und nicht nur den IPsec-Datenverkehr.

Weitere Informationen zum Abschluss einer ähnlichen Konfiguration auf einem Router an einem zentralen Standort finden Sie unter Router und VPN-Client für das öffentliche Internet in einem Stick-Konfigurationsbeispiel.

Unter Konfigurationsbeispiel für PIX/ASA 7.x Enhanced Spoke-to-Client VPN mit TACACS+-Authentifizierung erfahren Sie mehr über das Szenario, in dem der Hub PIX den Datenverkehr vom VPN-Client an den Spoke-PIX umleitet.

Hinweis: Um eine Überschneidung von IP-Adressen im Netzwerk zu vermeiden, weisen Sie dem

VPN-Client einen völlig anderen Pool von IP-Adressen zu (z. B. 10.x.x.x, 172.16.x.x und 192.168.x.x). Dieses IP-Adressierungsschema ist hilfreich bei der Fehlerbehebung in Ihrem Netzwerk.

Voraussetzungen

Anforderungen

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

- Die Hub-PIX/ASA Security Appliance muss Version 7.2 oder höher ausführen
- Cisco VPN Client Version 5.x

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der PIX- oder ASA Security Appliance Version 8.0.2 und dem Cisco VPN Client Version 5.0.

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX Security Appliance Version 7.2 oder höher verwendet werden.

Konventionen

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

Hintergrundinformationen

Hairpinning oder U-Turn

Diese Funktion ist nützlich für VPN-Datenverkehr, der in eine Schnittstelle eintritt, aber dann über diese Schnittstelle weitergeleitet wird. Wenn Sie beispielsweise über ein Hub-and-Spoke-VPN-Netzwerk verfügen, in dem die Sicherheits-Appliance der Hub ist und die Remote-VPN-Netzwerke Spokes bilden, muss der Datenverkehr zur Sicherheits-Appliance und dann wieder zum anderen Spoke übertragen werden.

Verwenden Sie den Befehl **für den gleichen Sicherheitsdatenverkehr**, damit der Datenverkehr dieselbe Schnittstelle betritt und verlässt.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

Hinweis: Hairpinning oder U-Turn ist auch für die Kommunikation zwischen VPN-Client und VPN-Client geeignet.

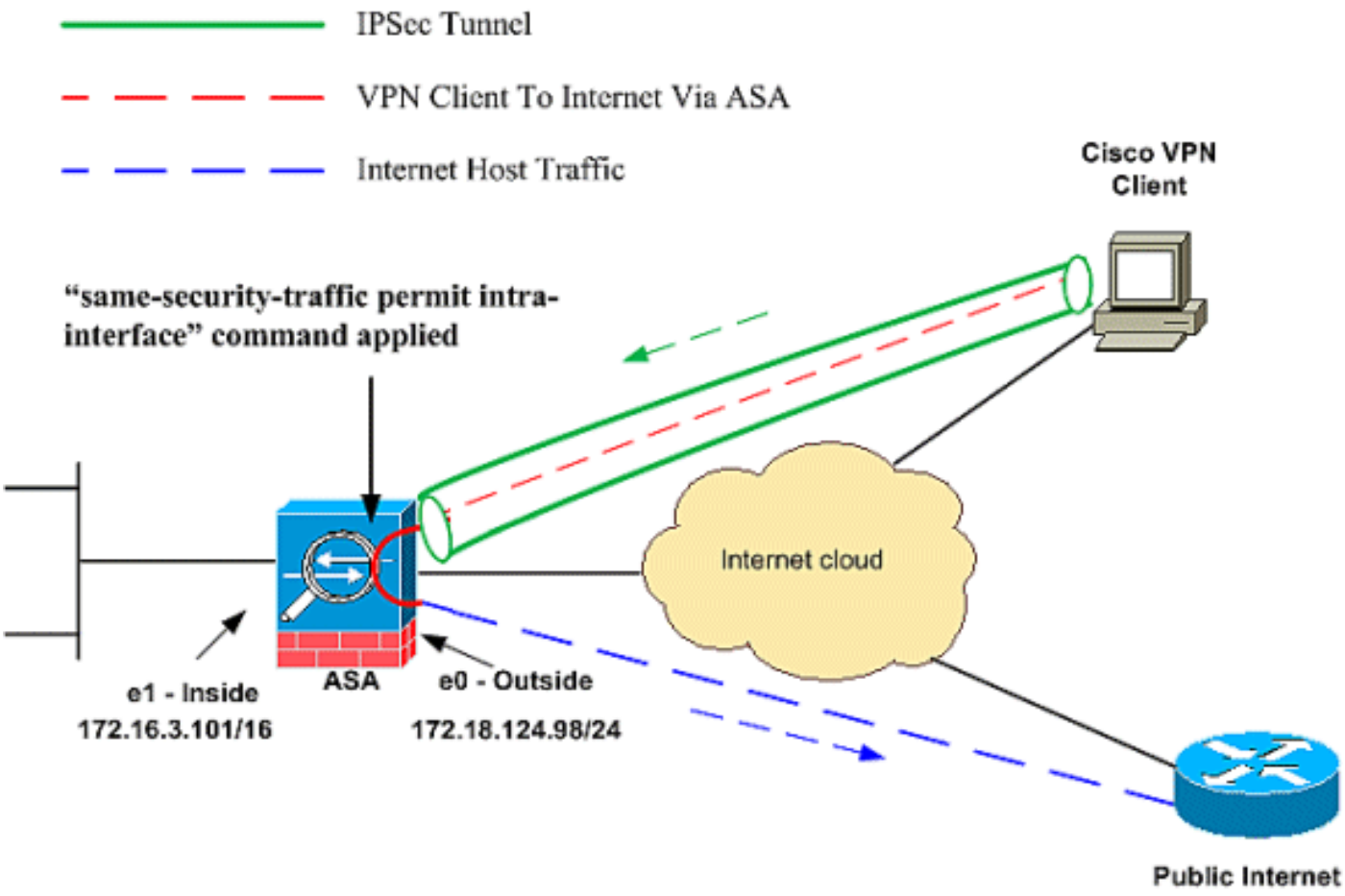
Konfigurationen

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:



CLI-Konfiguration von PIX/ASA

- PIX/ASA

Konfiguration auf PIX/ASA ausführen

`PIX Version 8.0(2)`
`names`
`!`

```
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500

ip local pool vpnpool
   192.168.10.1-192.168.10.254 mask 255.255.255.0

no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control!--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.

global (outside) 1 172.18.124.166
```

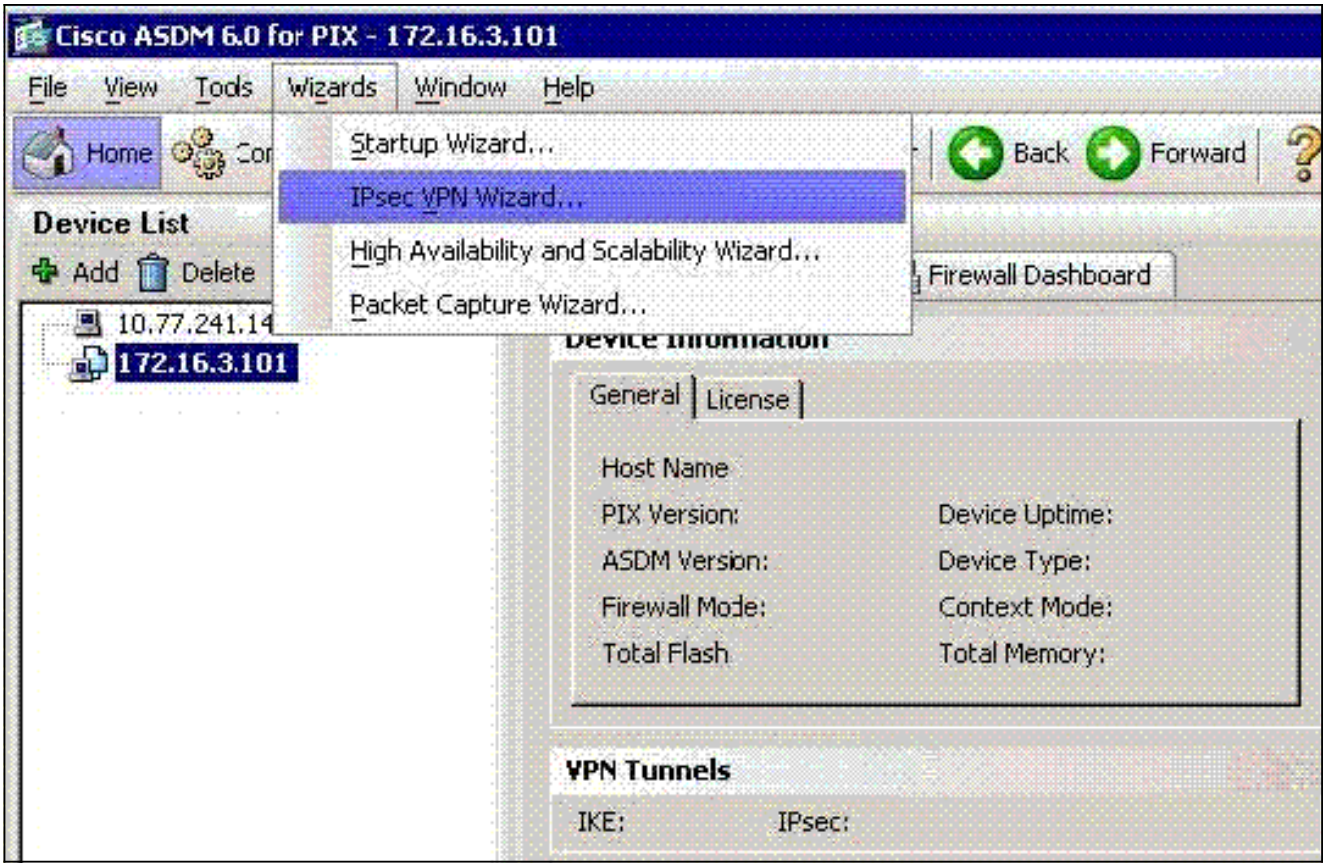
```
!--- The NAT statement to define what to encrypt (the
addresses from the vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.3.102 172.16.3.102
   netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.124.98 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20

!--- Forces VPN Clients over the tunnel for Internet
access. split-tunnel-policy tunnelall


no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac

!--- Crypto map configuration for VPN Clients that
connect to this PIX. crypto dynamic-map rtpdynmap 20 set
transform-set myset

!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

!--- Crypto map applied to the outside interface. crypto
map mymap interface outside

!--- Enable ISAKMP on the outside interface. isakmp
identity address
isakmp enable outside

!--- Configuration of ISAKMP policy. isakmp policy 10
authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Configuration of tunnel-group with group
```

```
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra

!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool

!--- Disable user authentication. authentication-server-
group none


!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 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
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

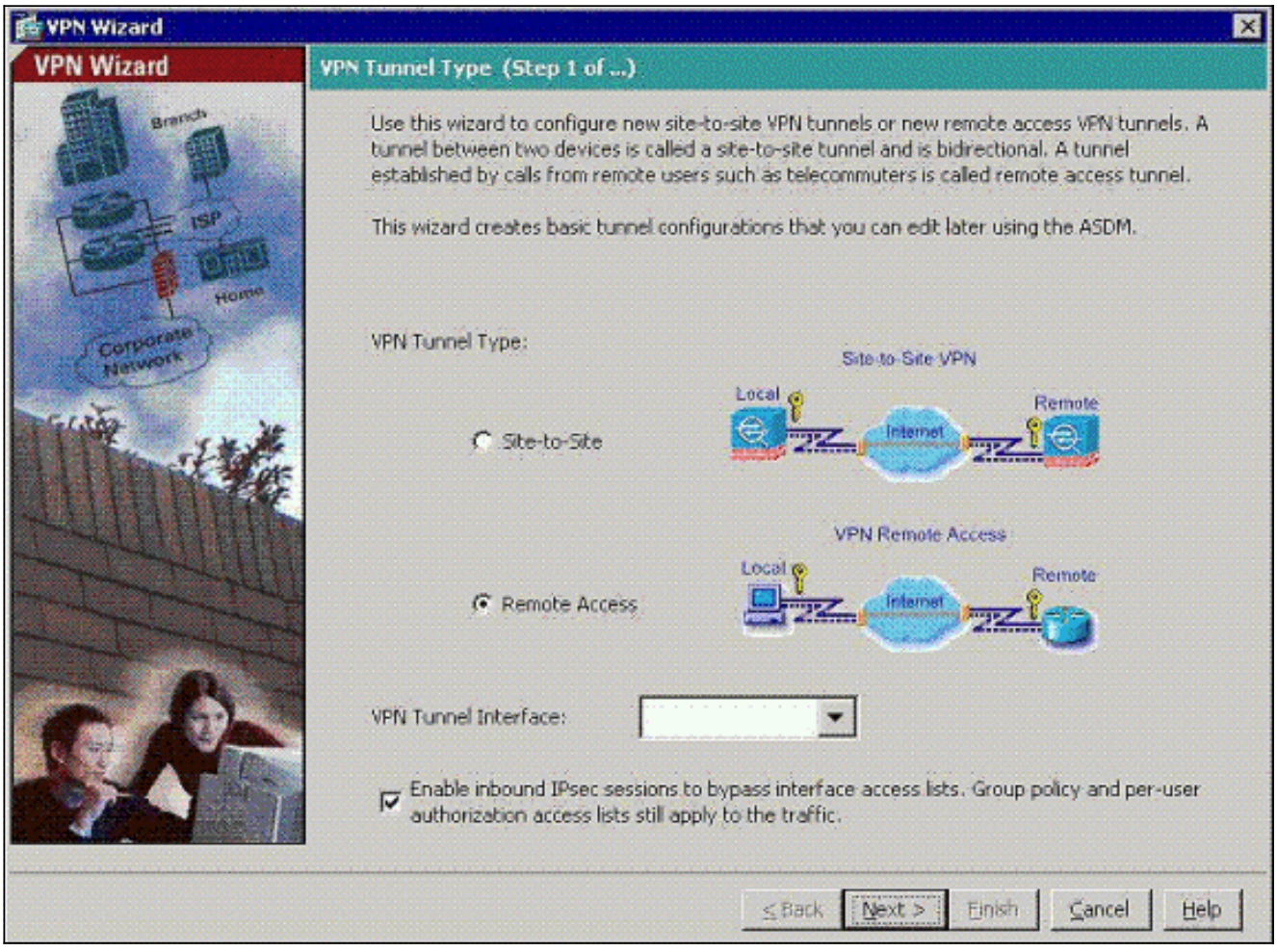
Konfigurieren von ASA/PIX mit ASDM

Gehen Sie wie folgt vor, um die Cisco ASA als Remote-VPN-Server mit ASDM zu konfigurieren:

1. Wählen Sie im Hauptfenster **Wizards > IPsec VPN Wizard** aus.

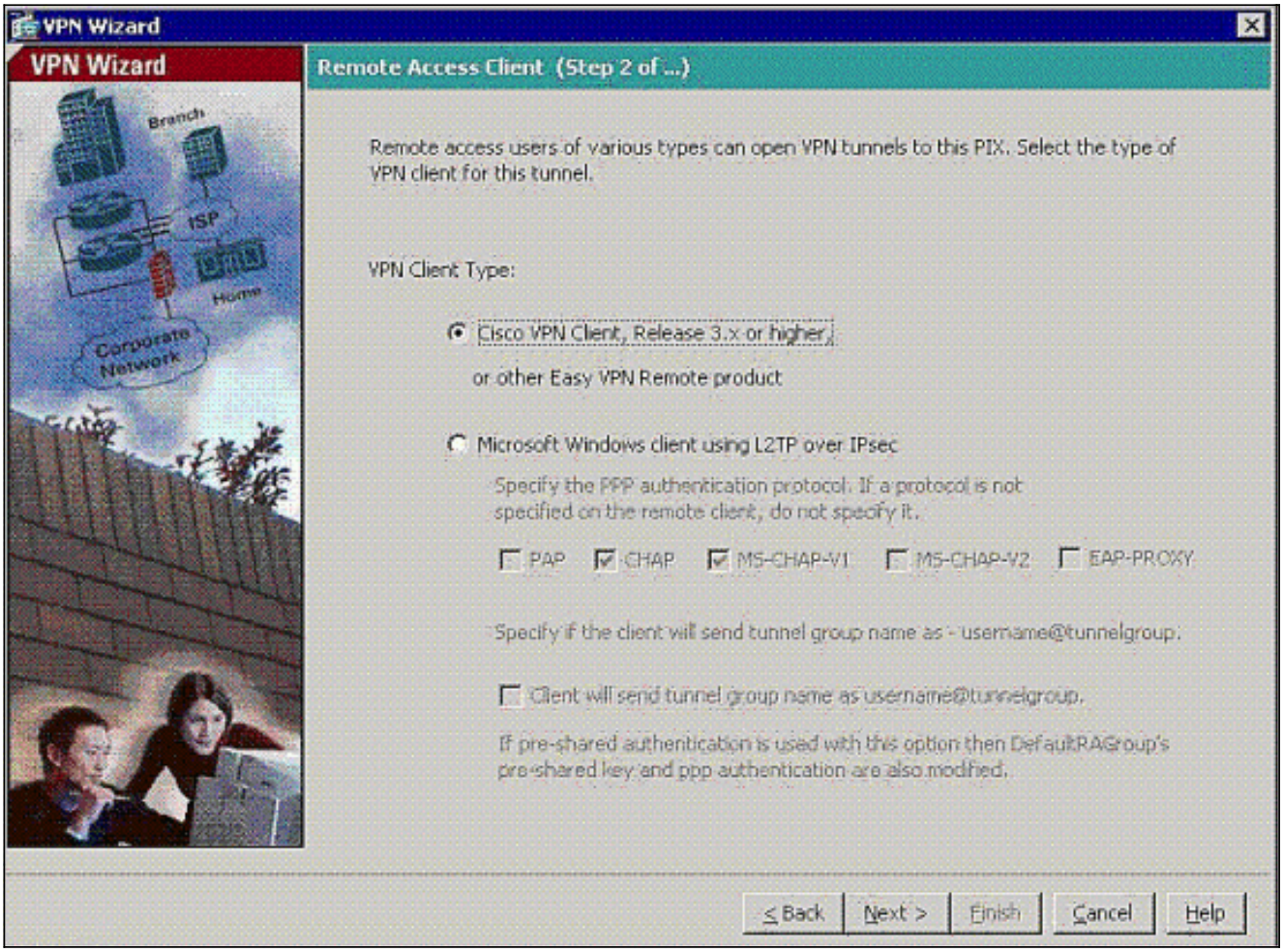


2. Wählen Sie den Tunneltyp **Remote Access** VPN aus, und stellen Sie sicher, dass die VPN-Tunnel-Schnittstelle wie gewünscht eingestellt
ist.

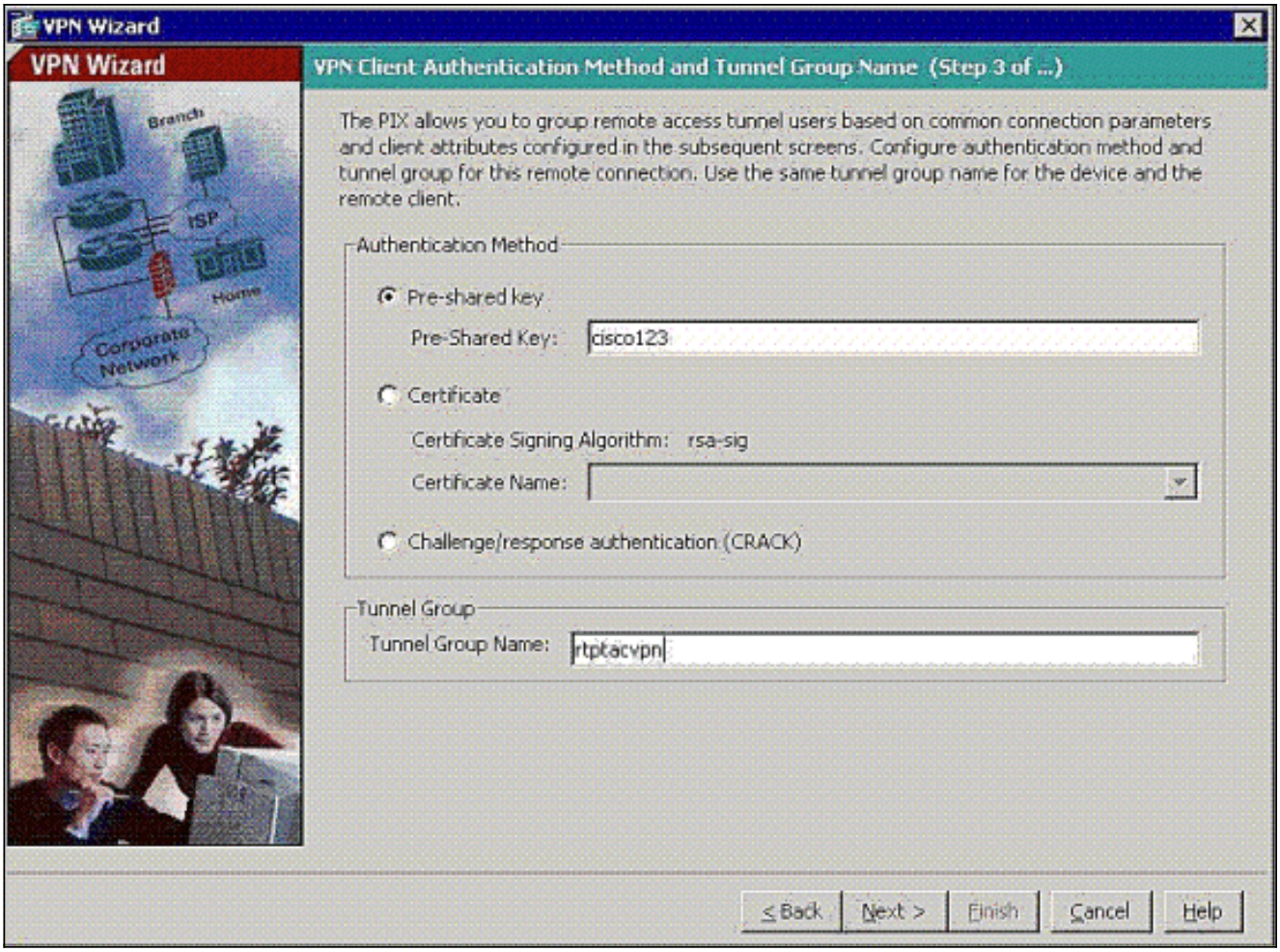


3. Der einzige verfügbare VPN-Client-Typ ist bereits ausgewählt. Klicken Sie auf

Weiter.

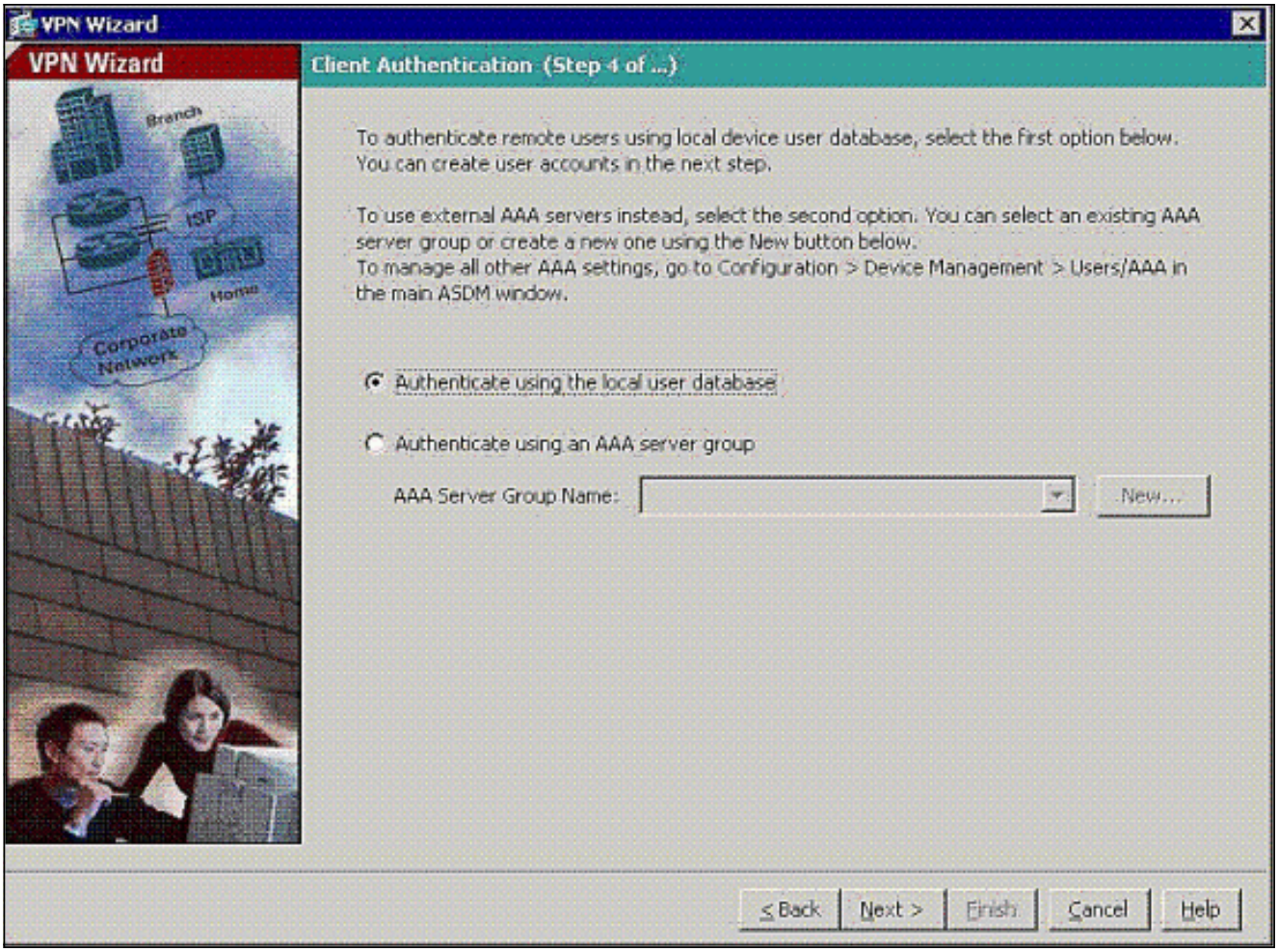


4. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie die zu verwendenden Authentifizierungsinformationen an.**Vorinstallierter Schlüssel** wird in diesem Beispiel ausgewählt.

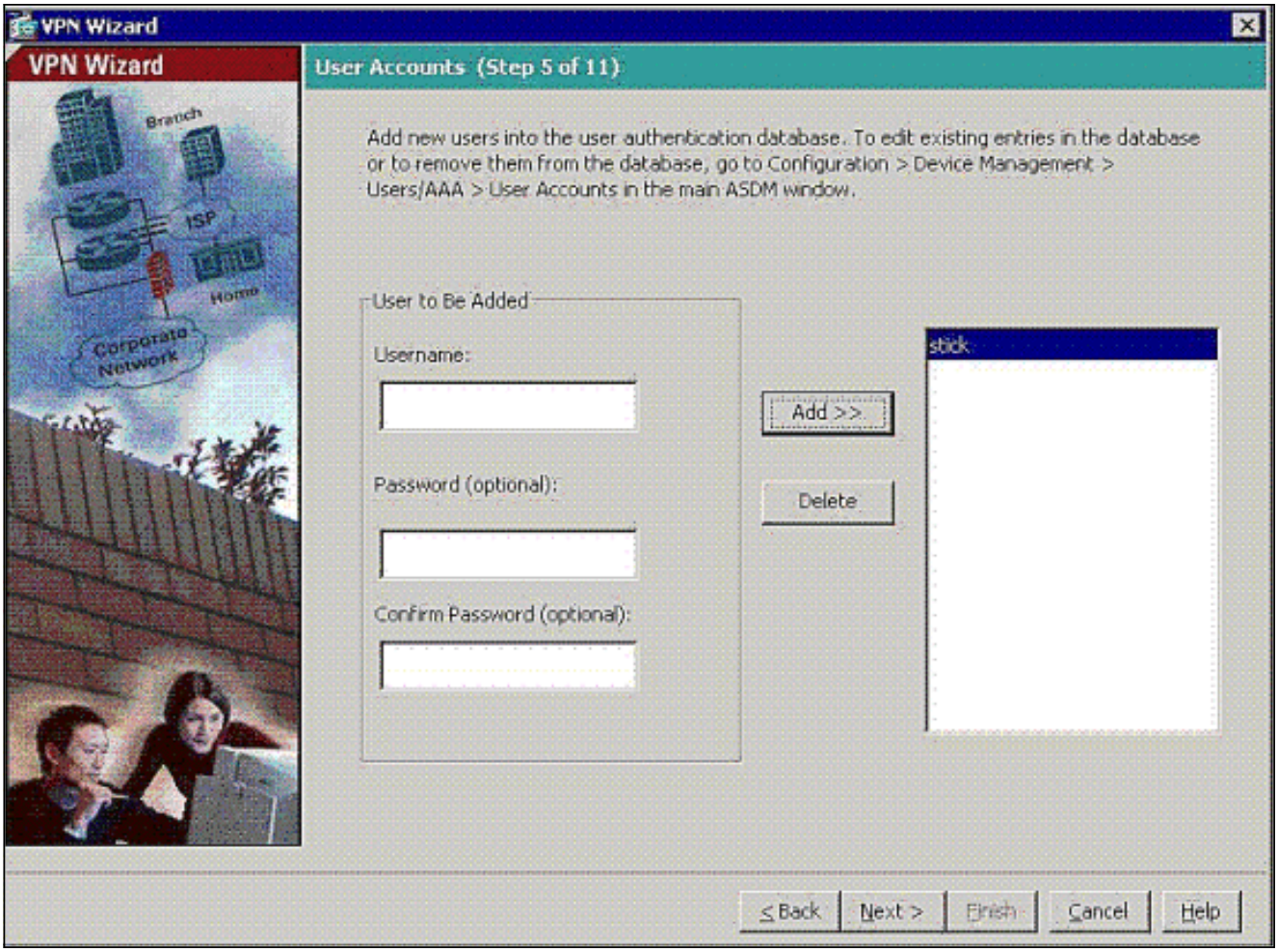


Hinweis: Es gibt keine Möglichkeit, den Pre-Shared Key auf dem ASDM auszublenden/zu verschlüsseln. Der Grund hierfür ist, dass das ASDM nur von Personen verwendet werden darf, die die ASA konfigurieren, oder von Personen, die den Kunden bei dieser Konfiguration unterstützen.

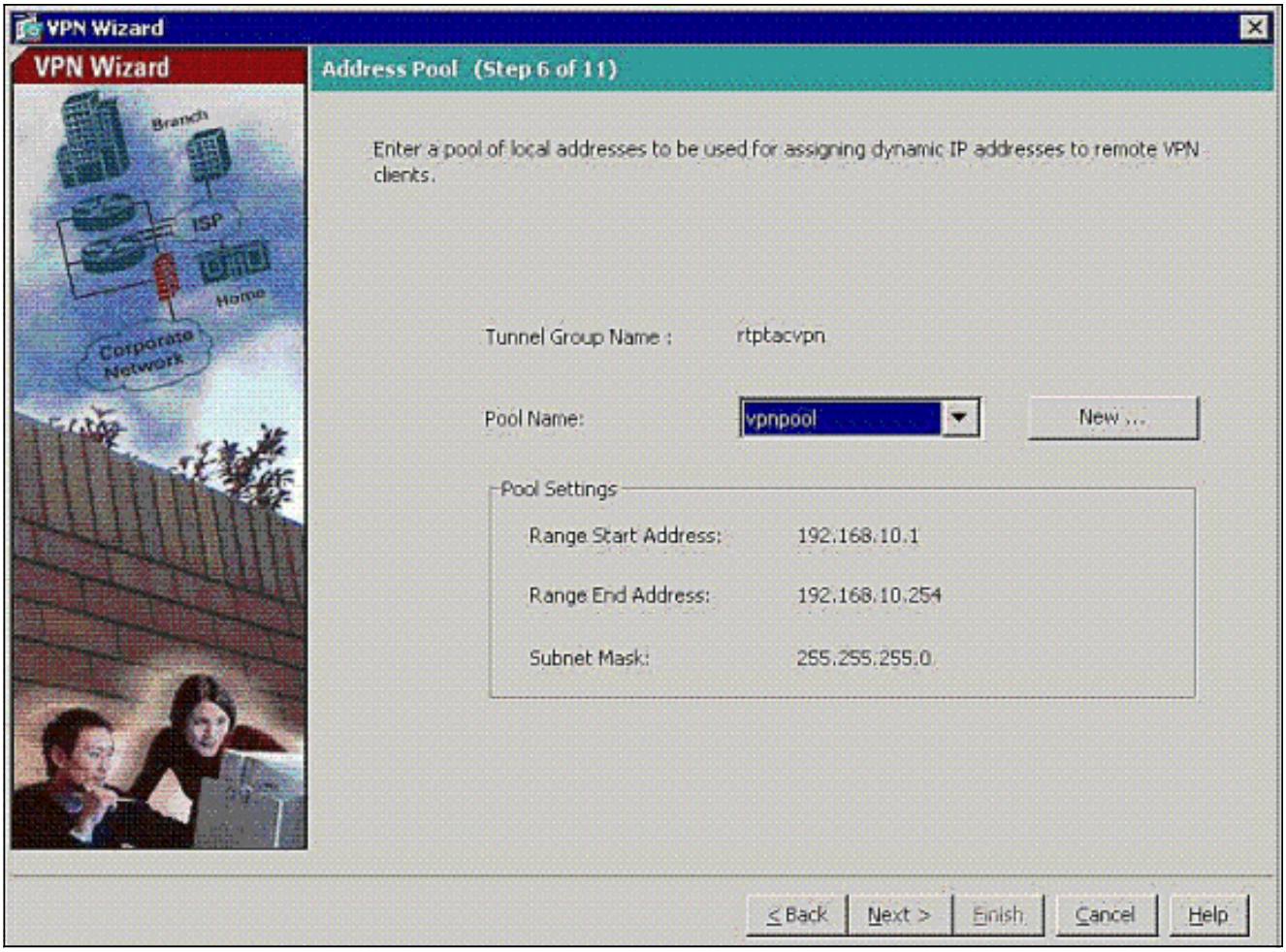
5. Wählen Sie aus, ob Remote-Benutzer in der lokalen Benutzerdatenbank oder in einer externen AAA-Servergruppe authentifiziert werden sollen.**Hinweis:** Sie fügen der lokalen Benutzerdatenbank in Schritt 6 Benutzer hinzu.**Hinweis:** Informationen zur Konfiguration einer externen AAA-Servergruppe über ASDM finden Sie unter PIX/ASA 7.x Authentication and Authorization Server Groups für VPN-Benutzer unter ASDM Configuration Example (Beispiel für die ASDM-Konfiguration).



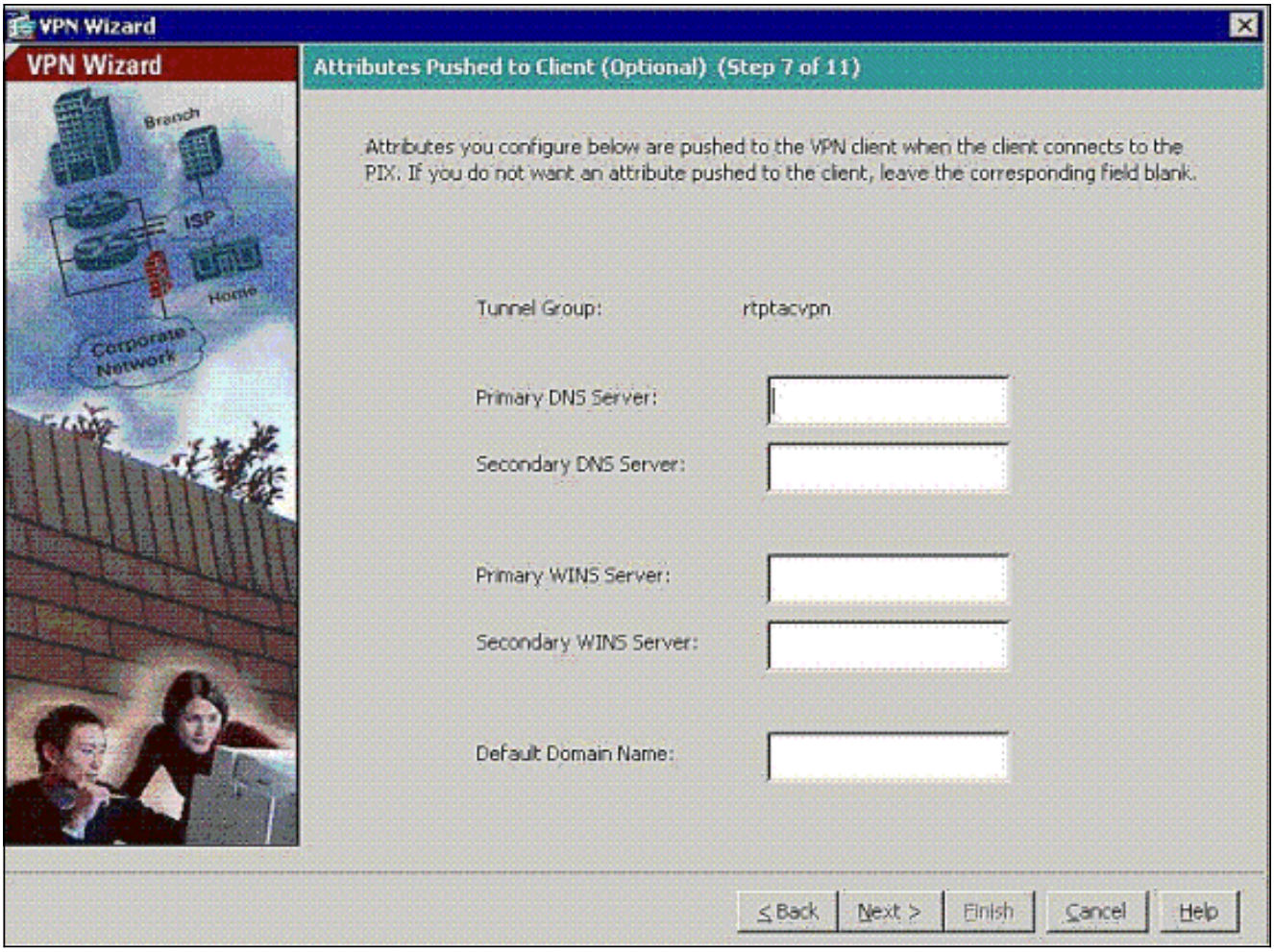
6. Fügen Sie bei Bedarf Benutzer zur lokalen Datenbank hinzu.**Hinweis:** Entfernen Sie aktuelle Benutzer nicht aus diesem Fenster. Wählen Sie **im ASDM-Hauptfenster** die Optionen **Konfiguration > Geräteverwaltung > Verwaltung > Benutzerkonten aus**, um vorhandene Datenbankeinträge zu bearbeiten oder aus der Datenbank zu entfernen.



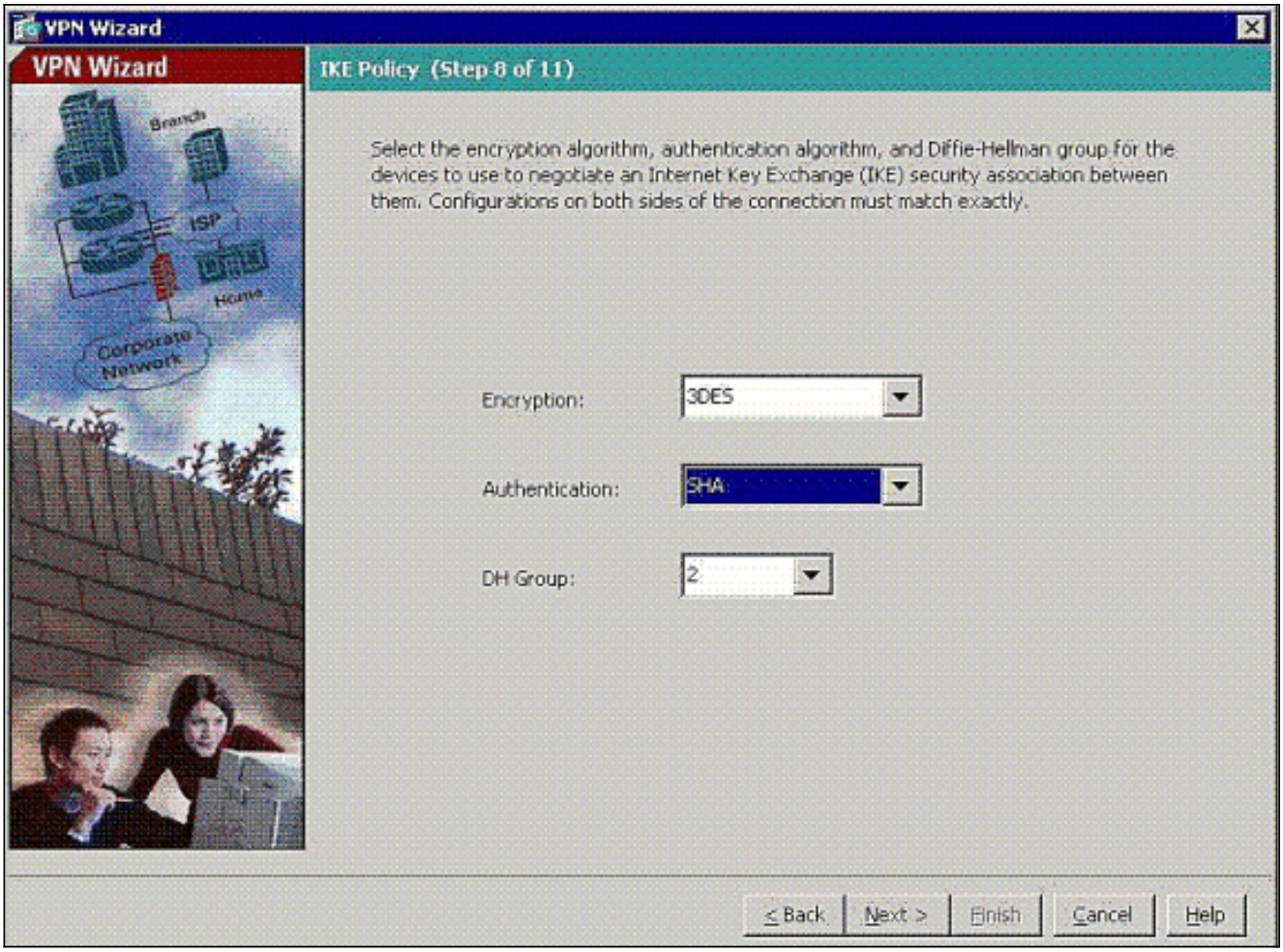
7. Definieren Sie einen Pool lokaler Adressen, der Remote-VPN-Clients bei der Verbindung dynamisch zugewiesen
   wird.



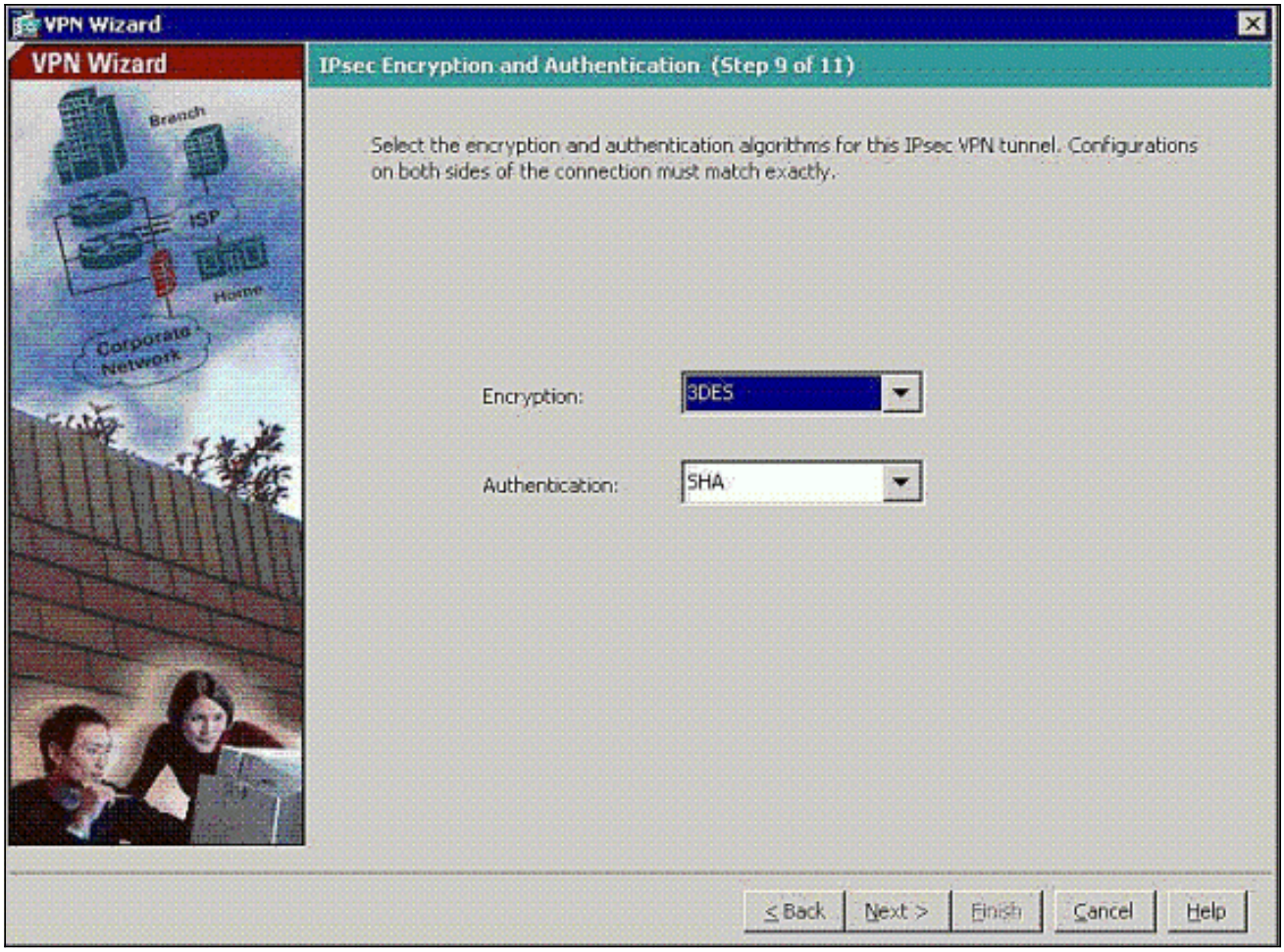
8. *Optional:* Geben Sie die DNS- und WINS-Serverinformationen und einen Standard-Domänennamen an, der an Remote-VPN-Clients übertragen werden soll.



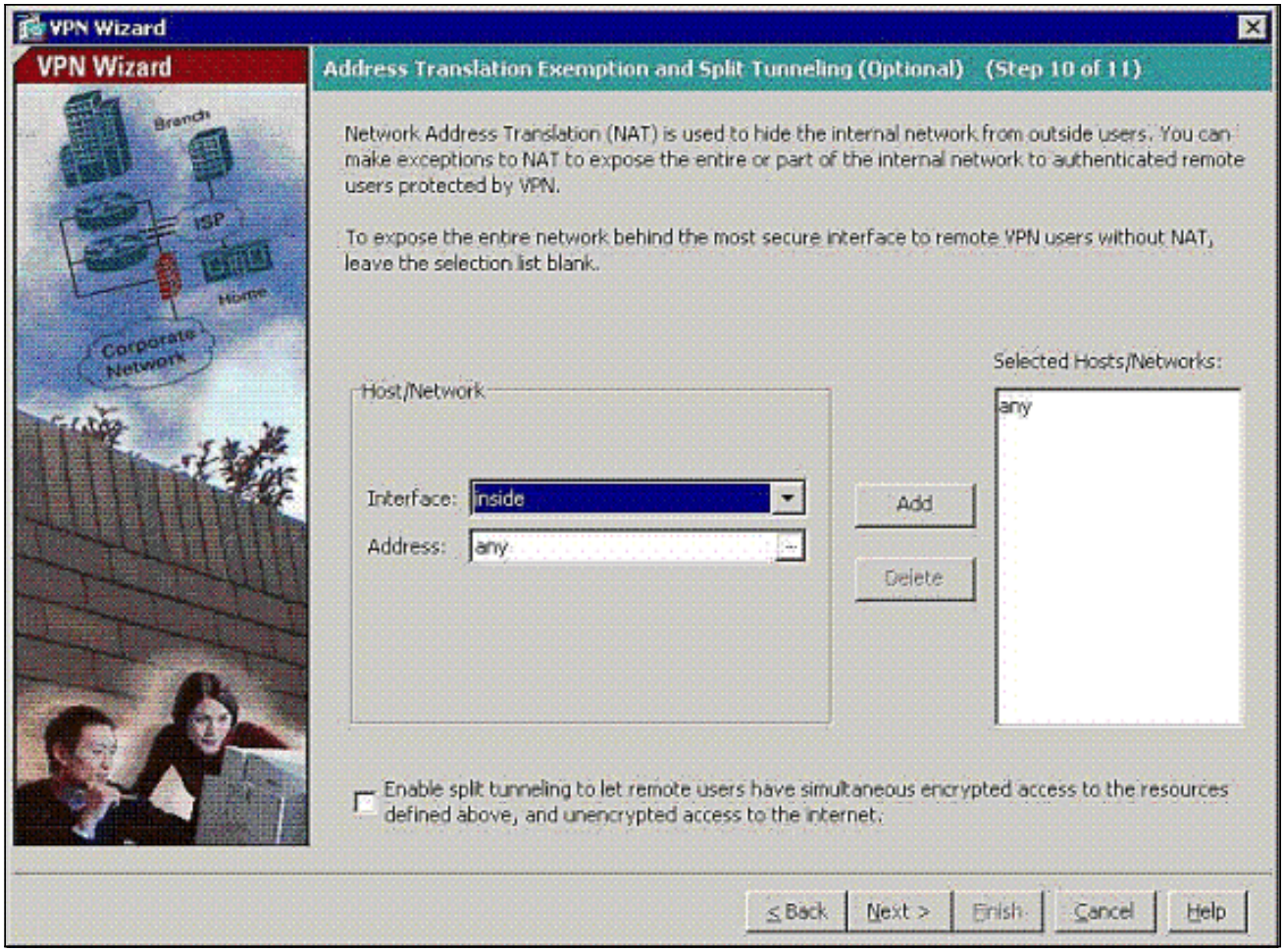
9. Geben Sie die Parameter für IKE an, auch als IKE-Phase 1 bezeichnet.Konfigurationen auf beiden Seiten des Tunnels müssen genau übereinstimmen, aber der Cisco VPN Client wählt automatisch die richtige Konfiguration für sich aus. Auf dem Client-PC ist keine IKE-Konfiguration
erforderlich.



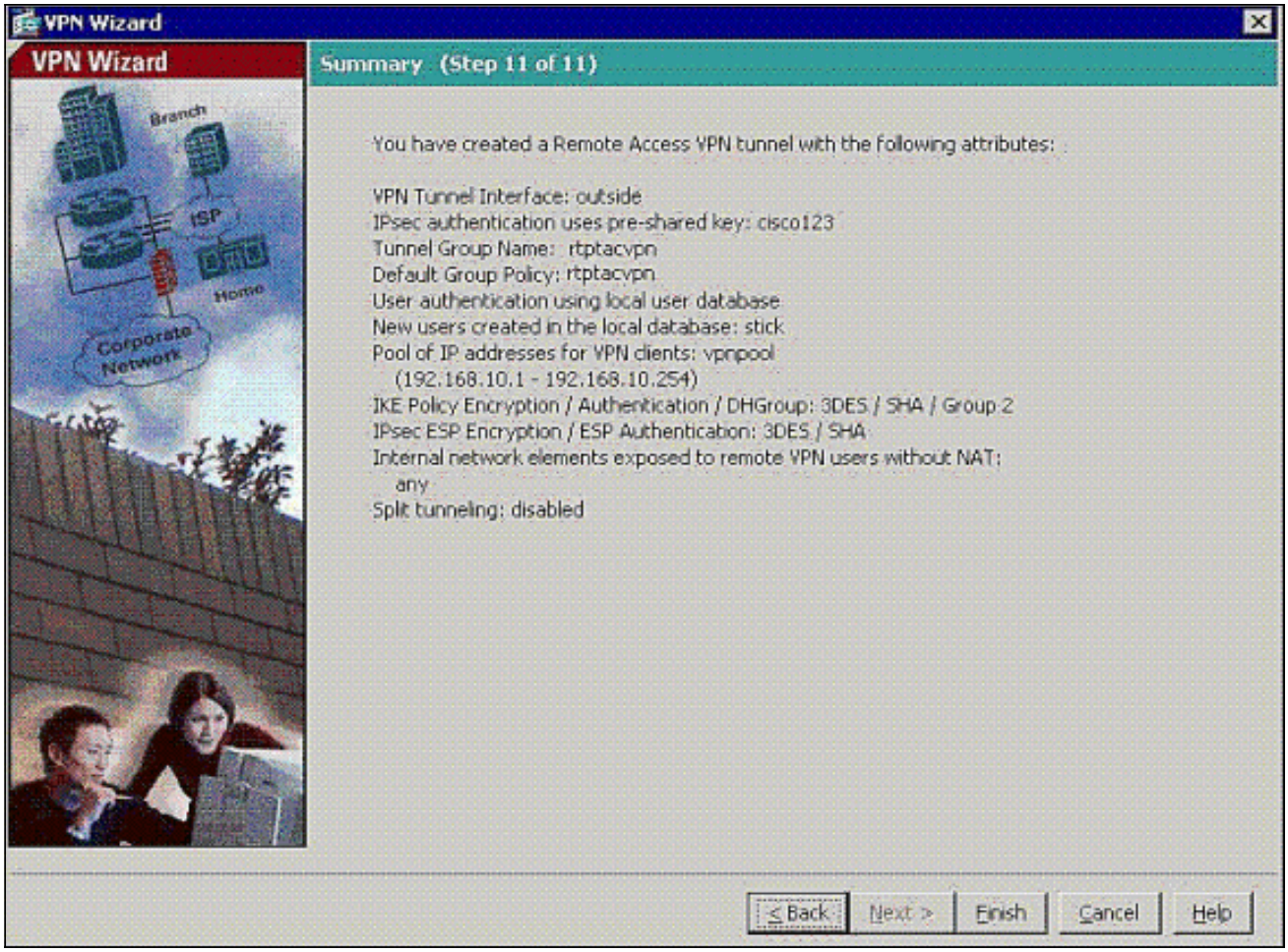
10. Geben Sie die Parameter für IPSec an, auch als IKE-Phase 2 bezeichnet.Konfigurationen auf beiden Seiten des Tunnels müssen genau übereinstimmen, aber der Cisco VPN Client wählt automatisch die richtige Konfiguration für sich aus. Auf dem Client-PC ist keine IKE-Konfiguration
erforderlich.



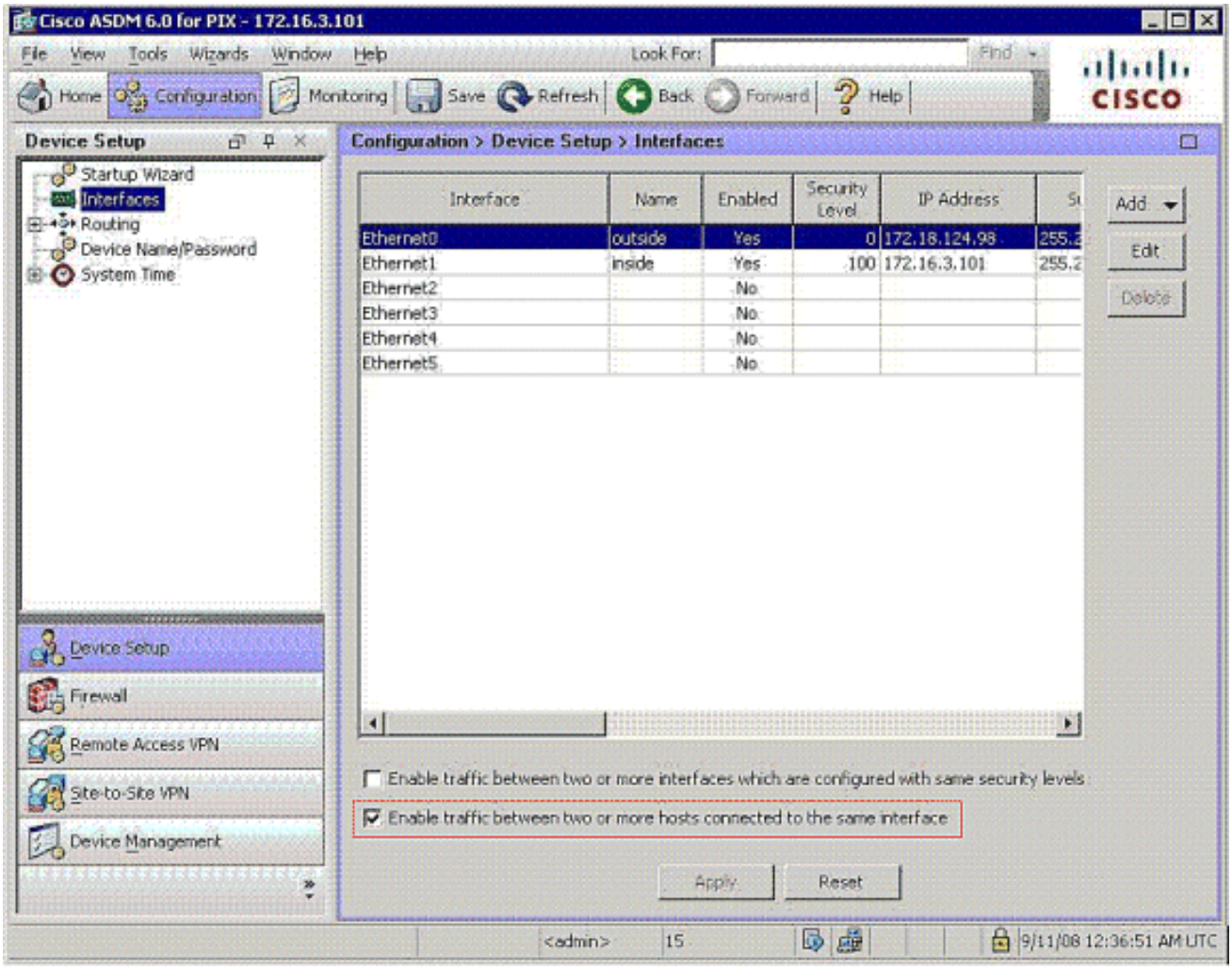
11. Geben Sie an, welche internen Hosts oder Netzwerke Remote-VPN-Benutzern ausgesetzt werden können, falls vorhanden.Wenn Sie diese Liste leer lassen, können Remote-VPN-Benutzer auf das gesamte interne Netzwerk der ASA zugreifen.In diesem Fenster können Sie auch Split-Tunneling aktivieren. Split-Tunneling verschlüsselt den Datenverkehr mit den zuvor in diesem Verfahren definierten Ressourcen und bietet im Allgemeinen unverschlüsselten Zugriff auf das Internet, indem dieser Datenverkehr nicht getunnelt wird. Wenn Split-Tunneling *nicht* aktiviert ist, wird der gesamte Datenverkehr von Remote-VPN-Benutzern an die ASA getunnelt. Je nach Konfiguration kann dies zu einer sehr hohen Bandbreite und einem hohen Prozessor
führen.



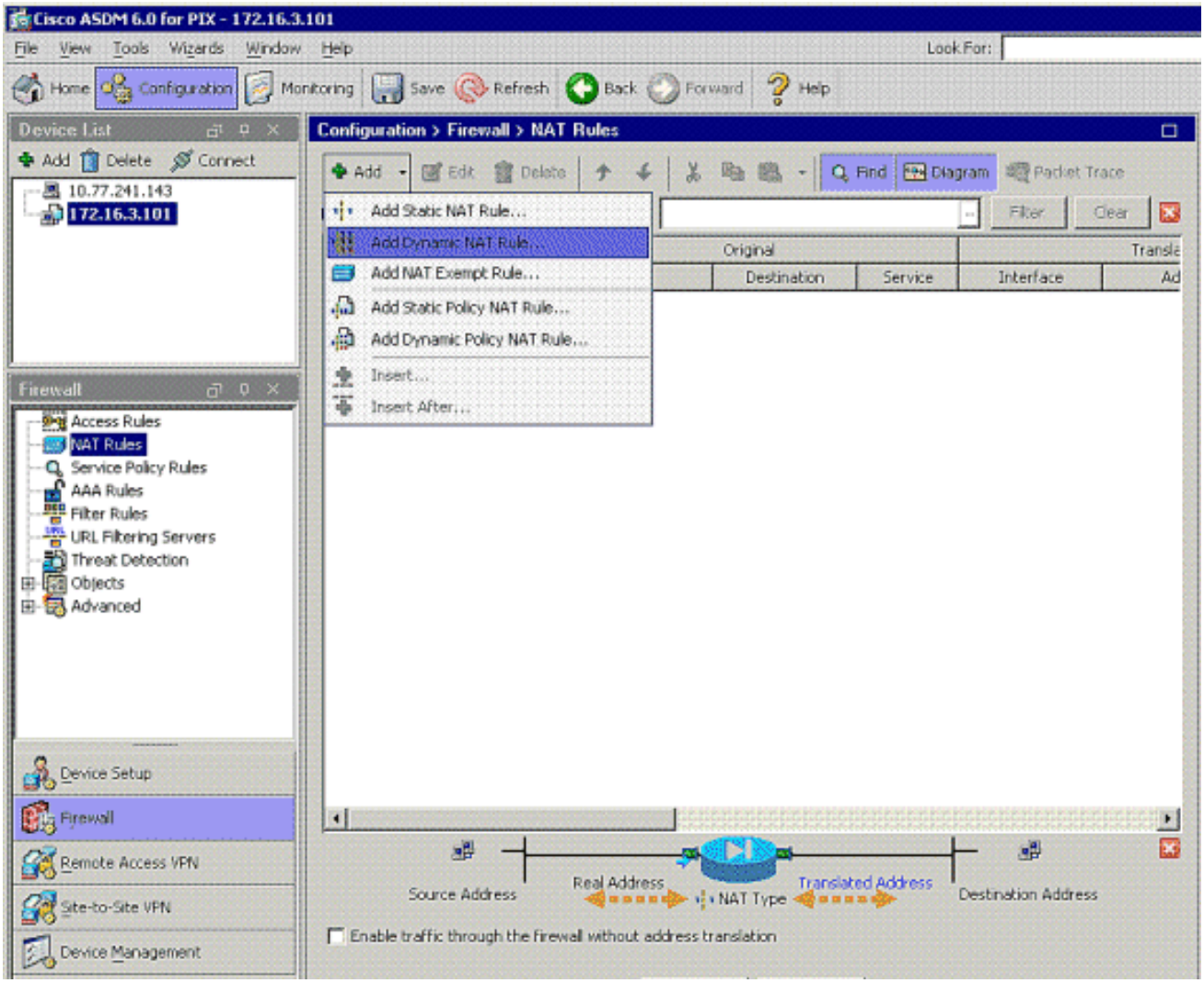
12. In diesem Fenster wird eine Zusammenfassung der von Ihnen ergriffenen Maßnahmen angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie mit Ihrer Konfiguration zufrieden sind.



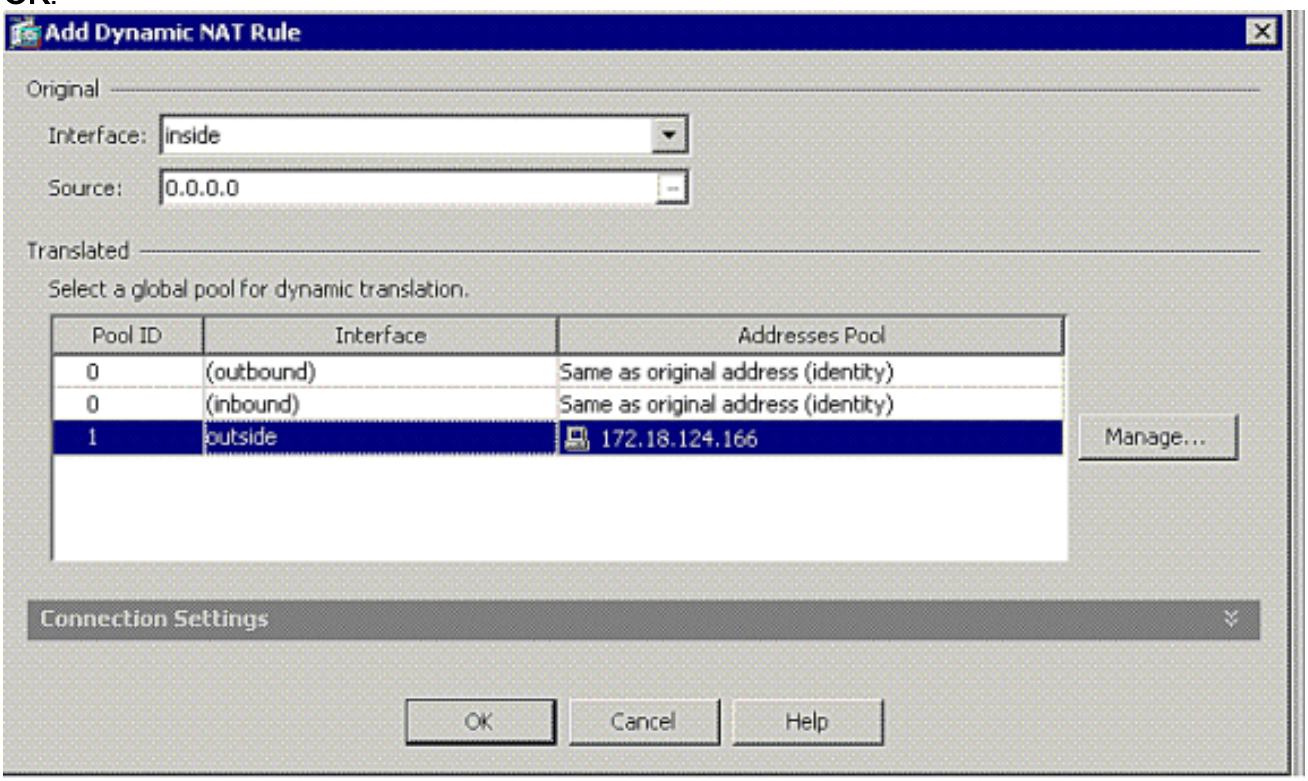
13. Konfigurieren Sie den Befehl **same** Sicherheit-**Verkehr**, um den Datenverkehr zwischen zwei oder mehr Hosts zu aktivieren, die mit derselben Schnittstelle verbunden sind, wenn Sie auf das Kontrollkästchen wie gezeigt
klicken:



14. Wählen Sie **Configuration > Firewall >NAT Rules**, und klicken Sie auf **Add Dynamic NAT Rule (Dynamische NAT-Regel hinzufügen)**, um diese dynamische Übersetzung mit ASDM zu
erstellen.

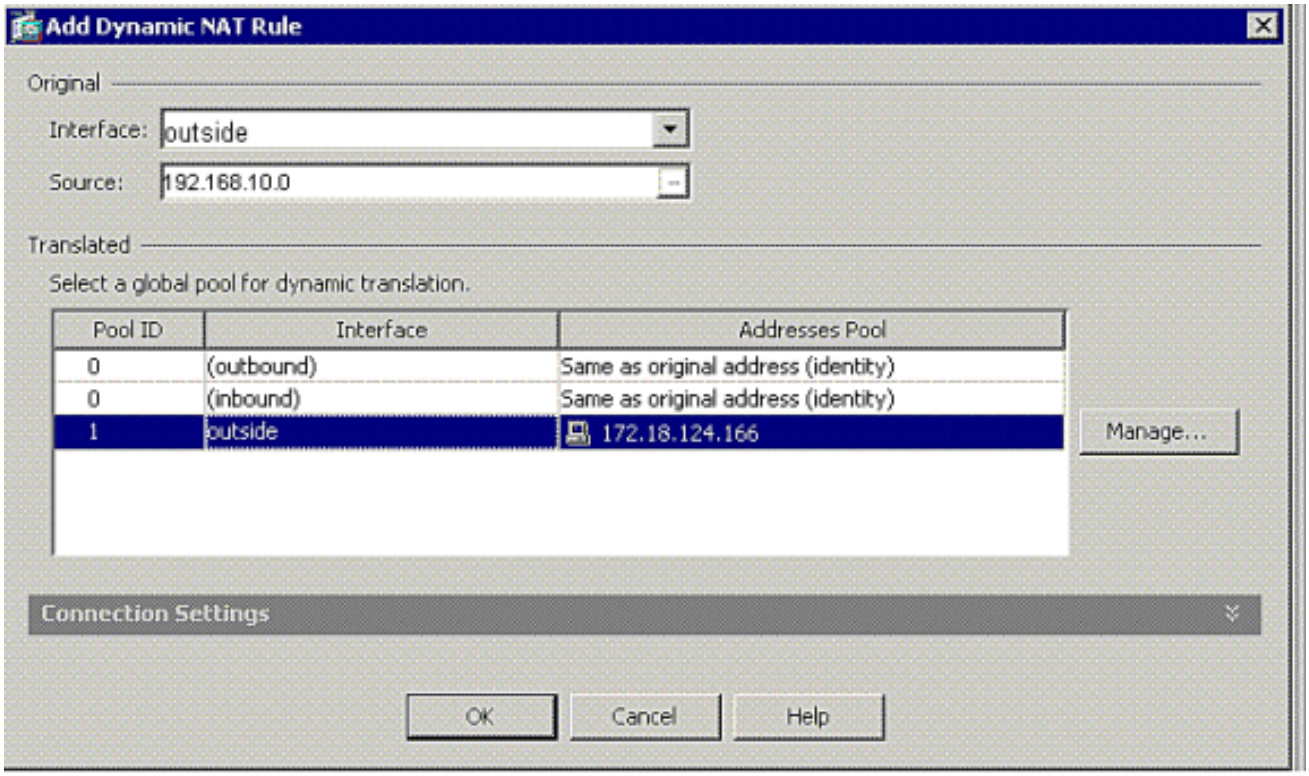


15. Wählen Sie **innen** als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten. Wählen Sie als Übersetzen der Adresse auf der Schnittstelle die Option **Außen** aus, und klicken Sie auf **OK**.

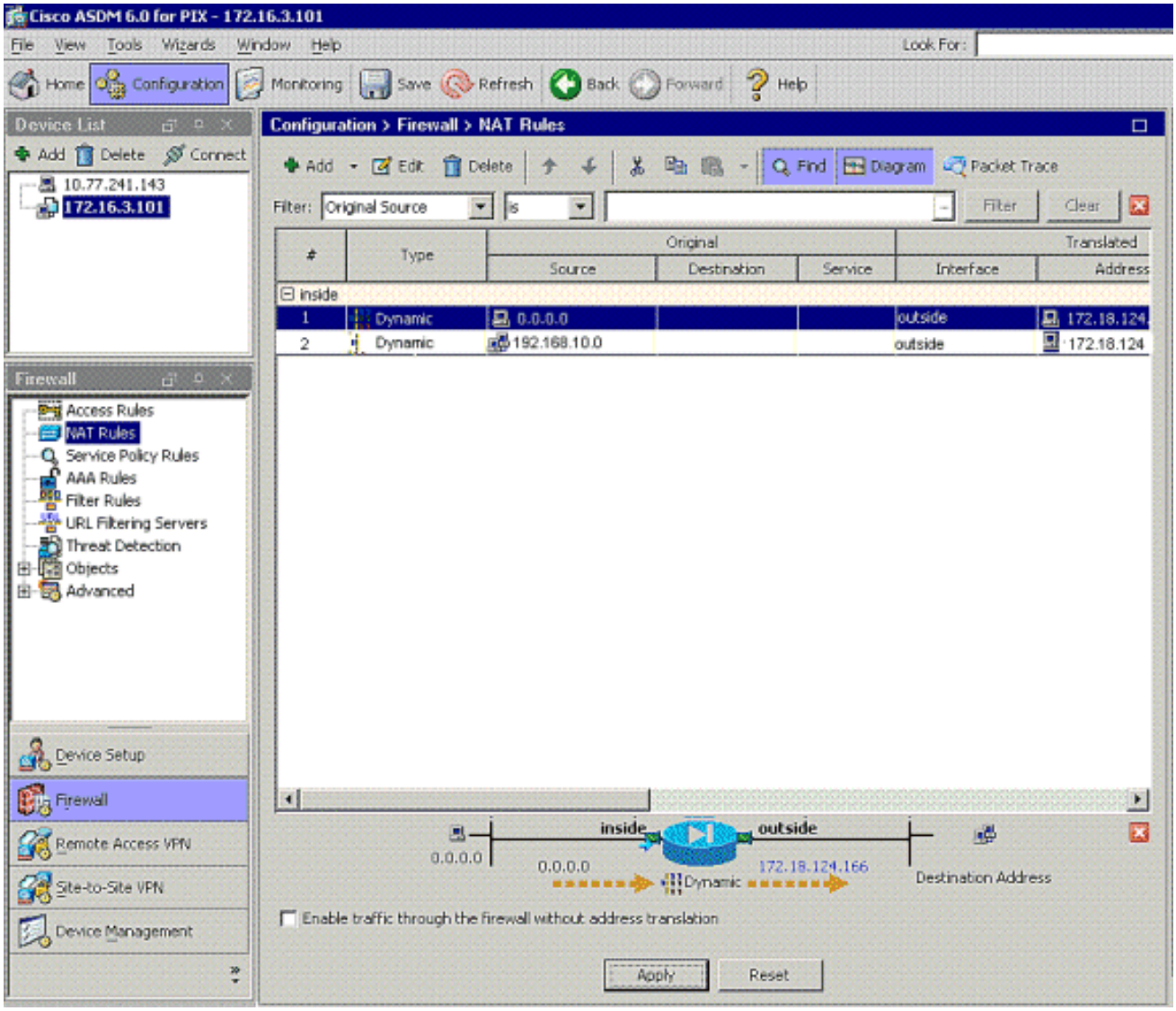


16. Wählen Sie **außen** als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT

hinzufügen möchten. Wählen Sie als Übersetzen der Adresse auf der Schnittstelle die Option **Außen** aus, und klicken Sie auf **OK**.



17. Die Übersetzung wird unter Übersetzungsregeln unter **Konfiguration > Firewall >NAT Rules angezeigt**.



Anmerkung 1: Der **Befehl** sysopt connection permit-vpn muss konfiguriert werden. Der **Befehl** show running-config sysopt überprüft, ob die Konfiguration vorgenommen wurde.

Anmerkung 2: Fügen Sie diese Ausgabe für den optionalen UDP-Transport hinzu:

```
group-policy clientgroup attributes vpn-idle-timeout 20
ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

Anmerkung 3: Konfigurieren Sie diesen Befehl in der globalen Konfiguration der PIX-Appliance, damit VPN-Clients über IPsec über TCP eine Verbindung herstellen können:

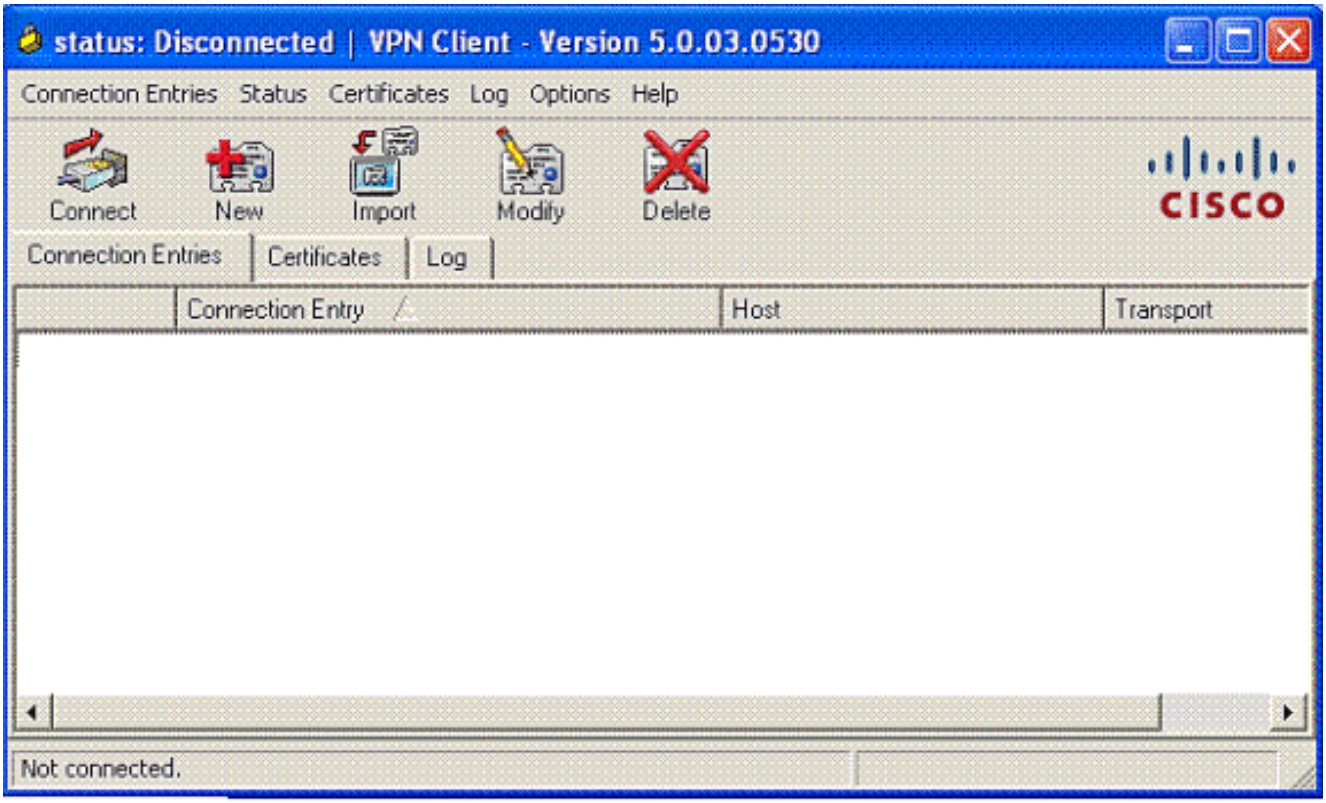
```
isakmp ipsec-over-tcp port 10000
```

Hinweis: Weitere Informationen zu den verschiedenen Szenarien, in denen Haarpinning verwendet werden kann, finden Sie im Video Hair Pinning auf Cisco ASA .

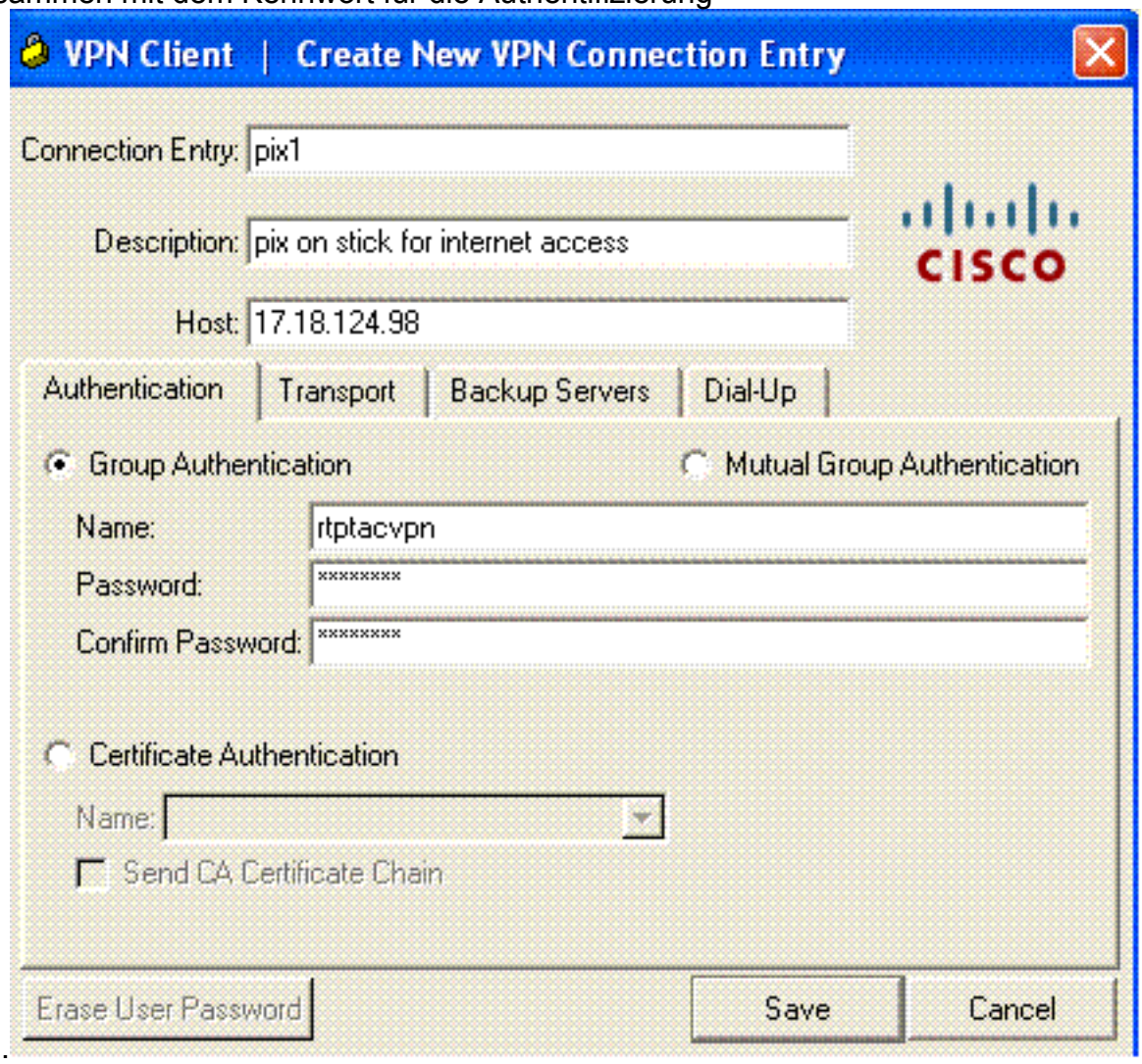
VPN-Client-Konfiguration

Gehen Sie wie folgt vor, um den VPN-Client zu konfigurieren:

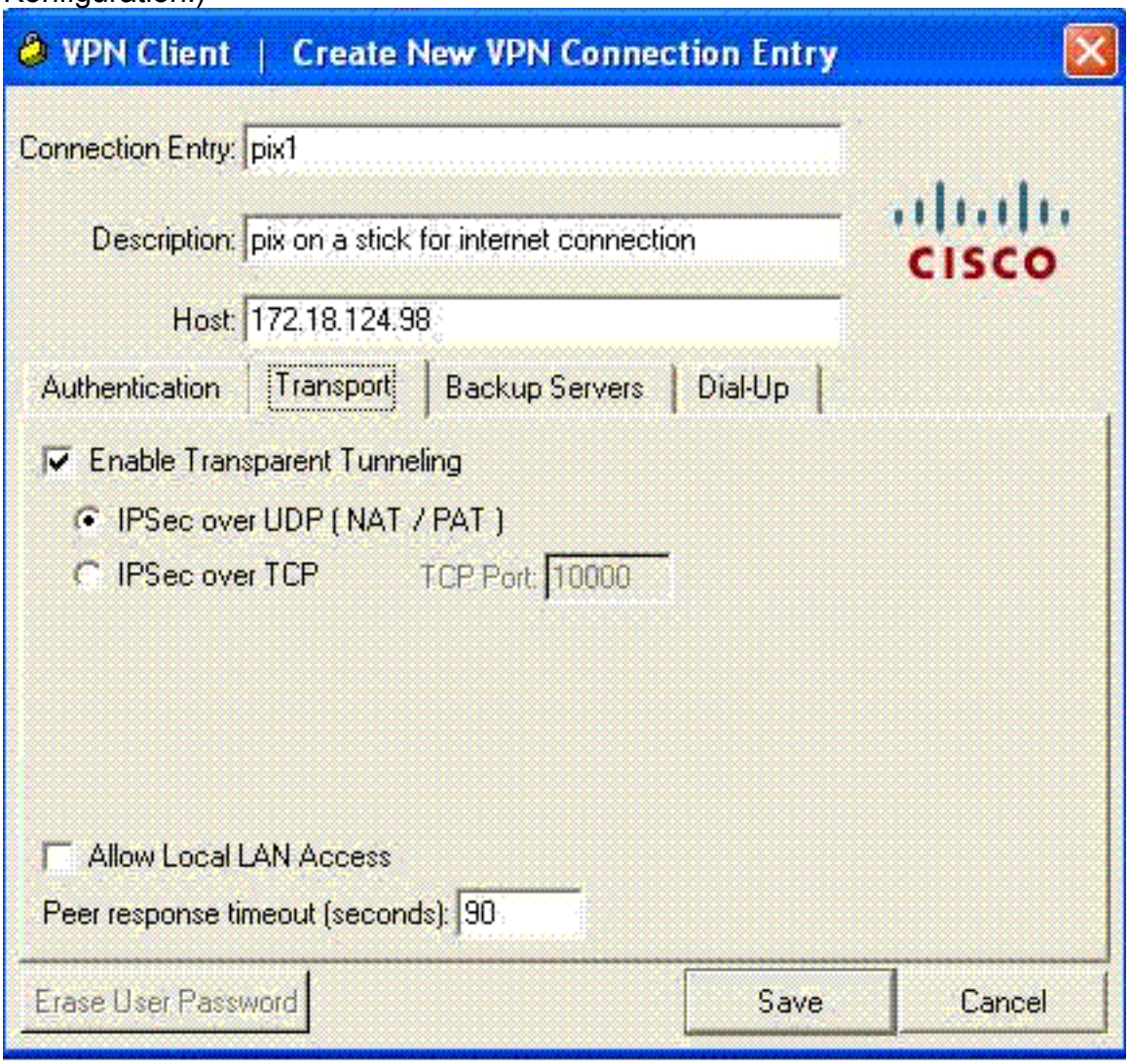
1. Wählen Sie
   Neu.



2. Geben Sie die IP-Adresse der externen PIX-Schnittstelle und den Namen der Tunnelgruppe zusammen mit dem Kennwort für die Authentifizierung ein.



3. (*Optional*) Klicken Sie auf der Registerkarte Transport auf **Transparentes Tunneling aktivieren**. (Dies ist optional und erfordert die in Hinweis 2 erwähnte zusätzliche PIX/ASA-Konfiguration.)



4. Profil speichern

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 alle aktuellen SAs an. Suchen Sie nach verschlüsselten und entschlüsselten Paketen auf dem SA, die den VPN-Client-Datenverkehr definieren.

Versuchen Sie, vom Client aus einen Ping zu senden oder eine öffentliche IP-Adresse anzuzeigen (z. B. www.cisco.com).

Hinweis: Die interne Schnittstelle des PIX kann nur dann für die Erstellung eines Tunnels gepingt werden, wenn der Befehl **Management-Access** im globalen Bestätigungsmodus konfiguriert ist.

```
PIX1(config)#management-access inside
PIX1(config)#show management-access

management-access inside
```

VPN-Client-Verifizierung

Führen Sie diese Schritte aus, um den VPN-Client zu überprüfen.

1. Klicken Sie mit der rechten Maustaste auf das im Systembereich angezeigte VPN Client-Sperrsymbol nach erfolgreicher Verbindung, und wählen Sie die Option für **Statistiken** zum Anzeigen von Verschlüsselungen und Entschlüsseln aus.
2. Klicken Sie auf die Registerkarte Route Details (Routendetails), um die Liste "Kein Split-Tunnel" zu überprüfen, die von der Appliance weitergeleitet wurde.

Fehlerbehebung

Hinweis: Weitere Informationen zur Fehlerbehebung bei VPN-Problemen finden Sie unter VPN-Fehlerbehebungslösungen.

Zugehörige Informationen

- Erweiterte Spoke-to-Client-VPN-Konfiguration Beispiel für PIX Security Appliance Version 7.0
- Cisco VPN-Client
- IPsec-Aushandlung/IKE-Protokolle
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Hair Pinning auf Cisco ASA
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems