ASA/PIX: Remote-VPN-Server mit eingehender NAT für VPN-Client-Datenverkehr mit CLI und ASDM - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument beschreibt, wie die Cisco Adaptive Security Appliance (ASA) der Serie 5500 so konfiguriert wird, dass sie als Remote-VPN-Server mit dem Adaptive Security Device Manager (ASDM) oder CLI und NAT für den eingehenden VPN-Client-Datenverkehr fungiert. Der ASDM bietet erstklassige Sicherheitsverwaltung und -überwachung über eine intuitive, benutzerfreundliche webbasierte Verwaltungsschnittstelle. Sobald die Cisco ASA-Konfiguration abgeschlossen ist, kann sie über den Cisco VPN-Client verifiziert werden.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM oder die CLI Konfigurationsänderungen vornehmen können. Es wird auch angenommen, dass die ASA für die ausgehende NAT konfiguriert ist. Weitere Informationen zur Konfiguration der ausgehenden NAT finden Sie unter Zulassen des Zugriffs von internen Hosts auf externe Netzwerke mithilfe von PAT.

Hinweis: Weitere Informationen finden Sie unter Zulassen von HTTPS-Zugriff für ASDM oder PIX/ASA 7.x: SSH im Konfigurationsbeispiel für die Innen- und Außenschnittstelle, um die Remote-Konfiguration des Geräts durch den ASDM oder Secure Shell (SSH) zu ermöglichen.

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance Software Version 7.x oder höher
- Adaptive Security Device Manager Version 5.x und höher
- Cisco VPN Client Version 4.x oder höher

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.x oder höher verwendet werden.

Konventionen

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

Hintergrundinformationen

Konfigurationen für den Remote-Zugriff bieten sicheren Remote-Zugriff für Cisco VPN-Clients wie mobile Benutzer. Über ein Remote-Access-VPN können Remote-Benutzer sicher auf zentralisierte Netzwerkressourcen zugreifen. Der Cisco VPN Client ist mit dem IPSec-Protokoll kompatibel und wurde speziell für die Verwendung mit der Sicherheits-Appliance entwickelt. Die Sicherheits-Appliance kann jedoch IPSec-Verbindungen mit vielen protokollkonformen Clients herstellen. Weitere Informationen zu IPSec finden Sie in den ASA-Konfigurationsleitfäden.

Gruppen und Benutzer sind zentrale Konzepte für die Verwaltung der VPN-Sicherheit und die Konfiguration der Sicherheits-Appliance. Sie legen Attribute fest, die den Benutzerzugriff auf das VPN und dessen Nutzung bestimmen. Eine Gruppe ist eine Sammlung von Benutzern, die als eine Einheit behandelt werden. Benutzer erhalten ihre Attribute aus Gruppenrichtlinien. Tunnelgruppen identifizieren die Gruppenrichtlinie für bestimmte Verbindungen. Wenn Sie Benutzern keine bestimmte Gruppenrichtlinie zuweisen, gilt die Standardgruppenrichtlinie für die Verbindung.

Eine Tunnelgruppe besteht aus einer Reihe von Datensätzen, die Tunnelverbindungsrichtlinien festlegen. Diese Datensätze enthalten die Server, an die die Tunnelbenutzer authentifiziert werden, sowie ggf. die Accounting-Server, an die die Verbindungsinformationen gesendet werden. Sie identifizieren auch eine Standardgruppenrichtlinie für die Verbindungen und enthalten protokollspezifische Verbindungsparameter. Tunnelgruppen enthalten eine kleine Anzahl von Attributen, die sich auf die Erstellung des Tunnels selbst beziehen. Tunnelgruppen enthalten einen

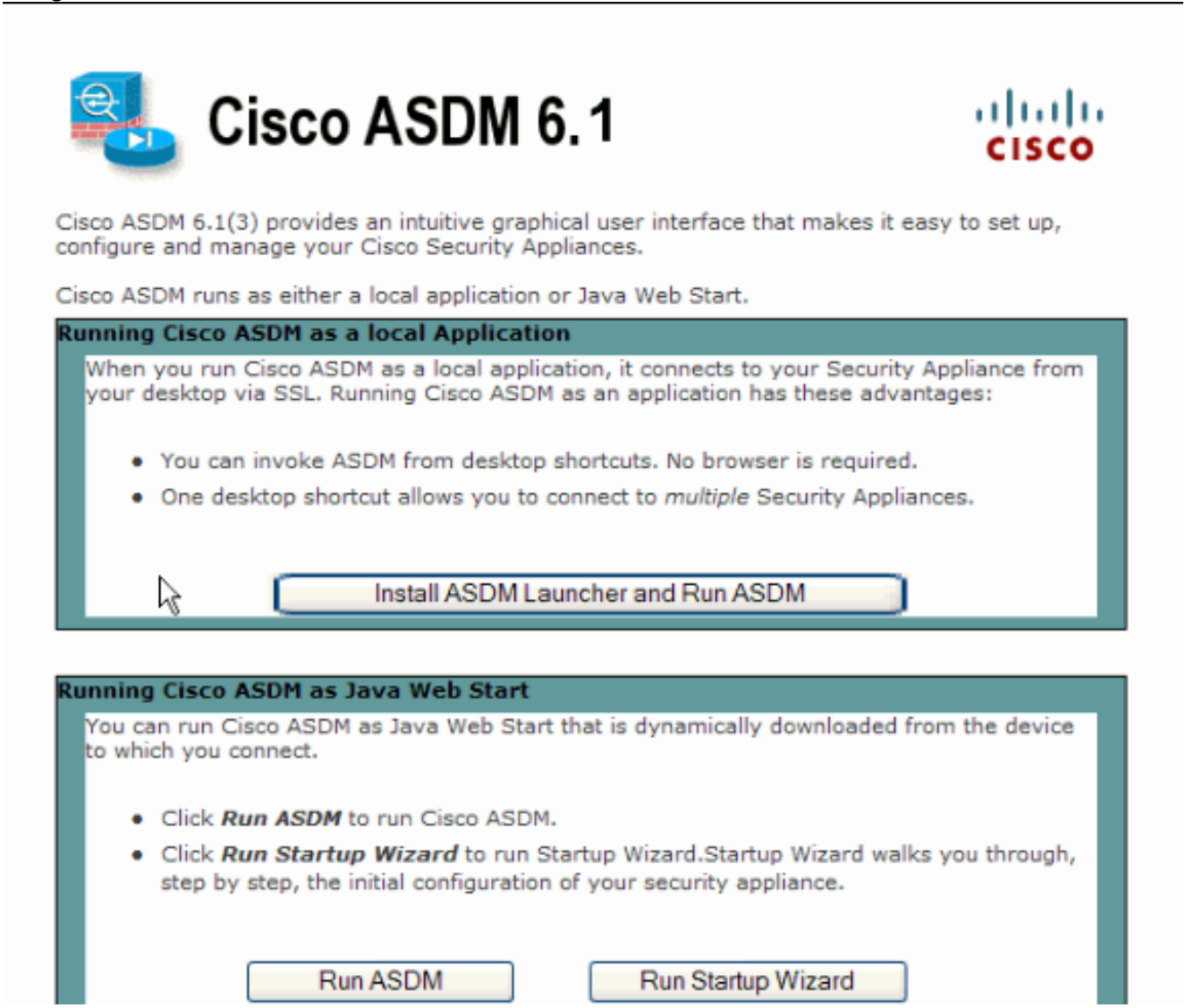
Zeiger auf eine Gruppenrichtlinie, die benutzerorientierte Attribute definiert.

Konfigurationen

ASA/PIX als Remote-VPN-Server mit ASDM konfigurieren

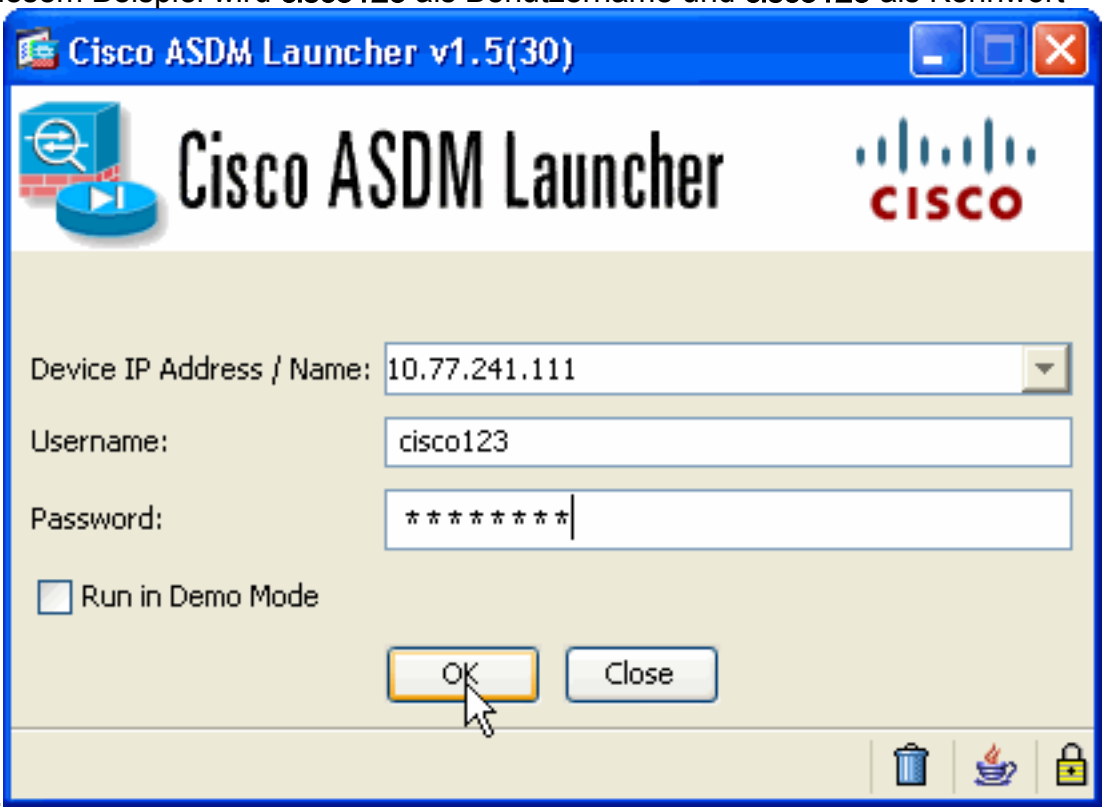
Gehen Sie wie folgt vor, um die Cisco ASA als Remote-VPN-Server mit ASDM zu konfigurieren:

1. Öffnen Sie Ihren Browser, und geben Sie **https://<IP_Adresse der ASA-Schnittstelle ein, die für ASDM Access konfiguriert wurde>**, um auf das ASDM auf der ASA zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Die ASA präsentiert dieses Fenster, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet
ausgeführt.

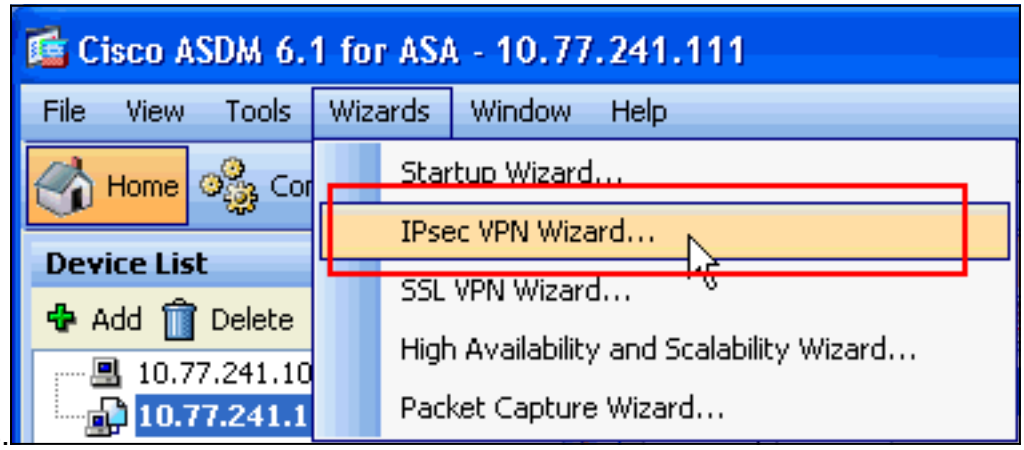


2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software und Ausführung des Cisco ASDM Launchers ausgeführt werden.

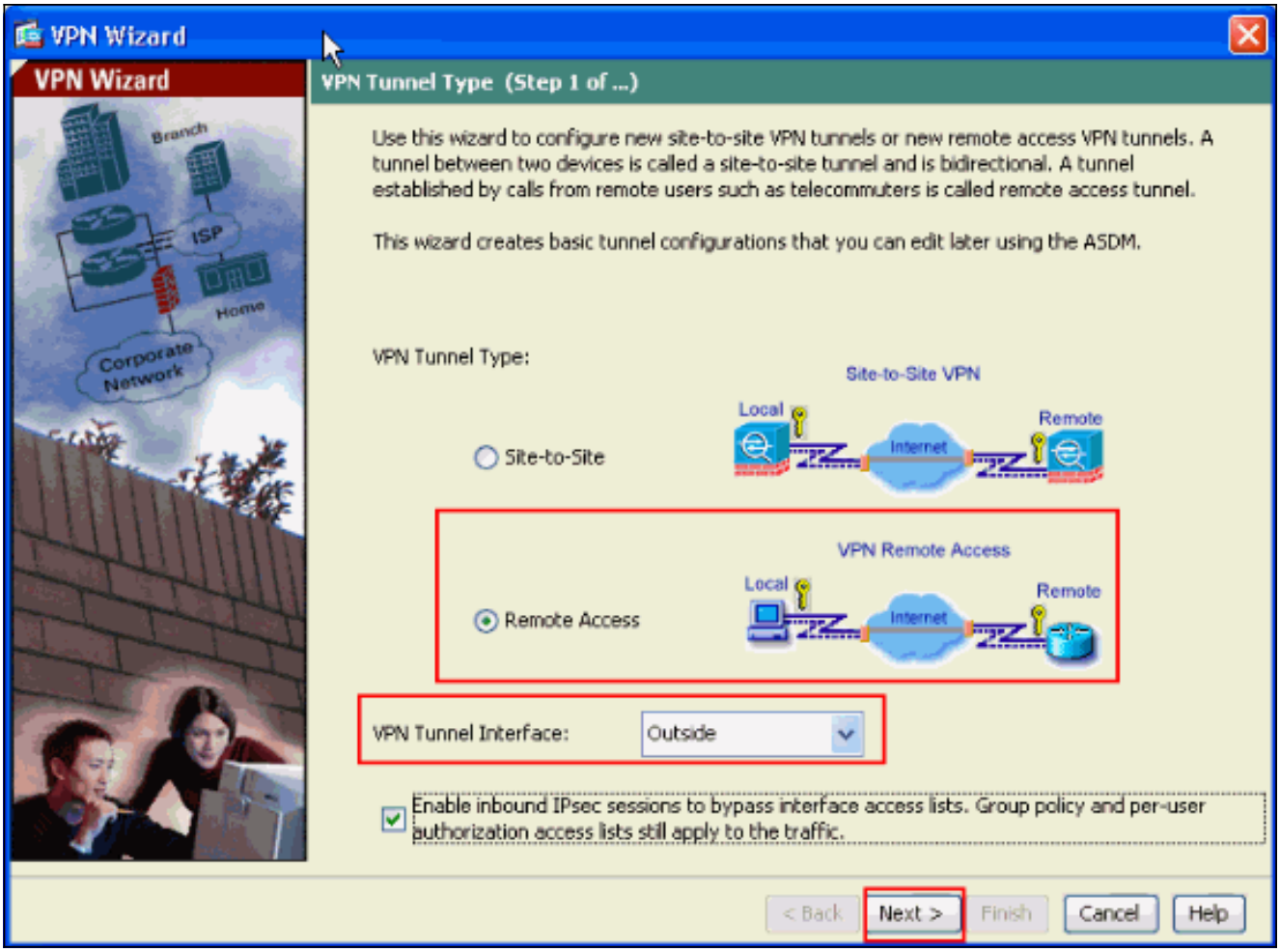
4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl **http** konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben.In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als Kennwort verwendet.



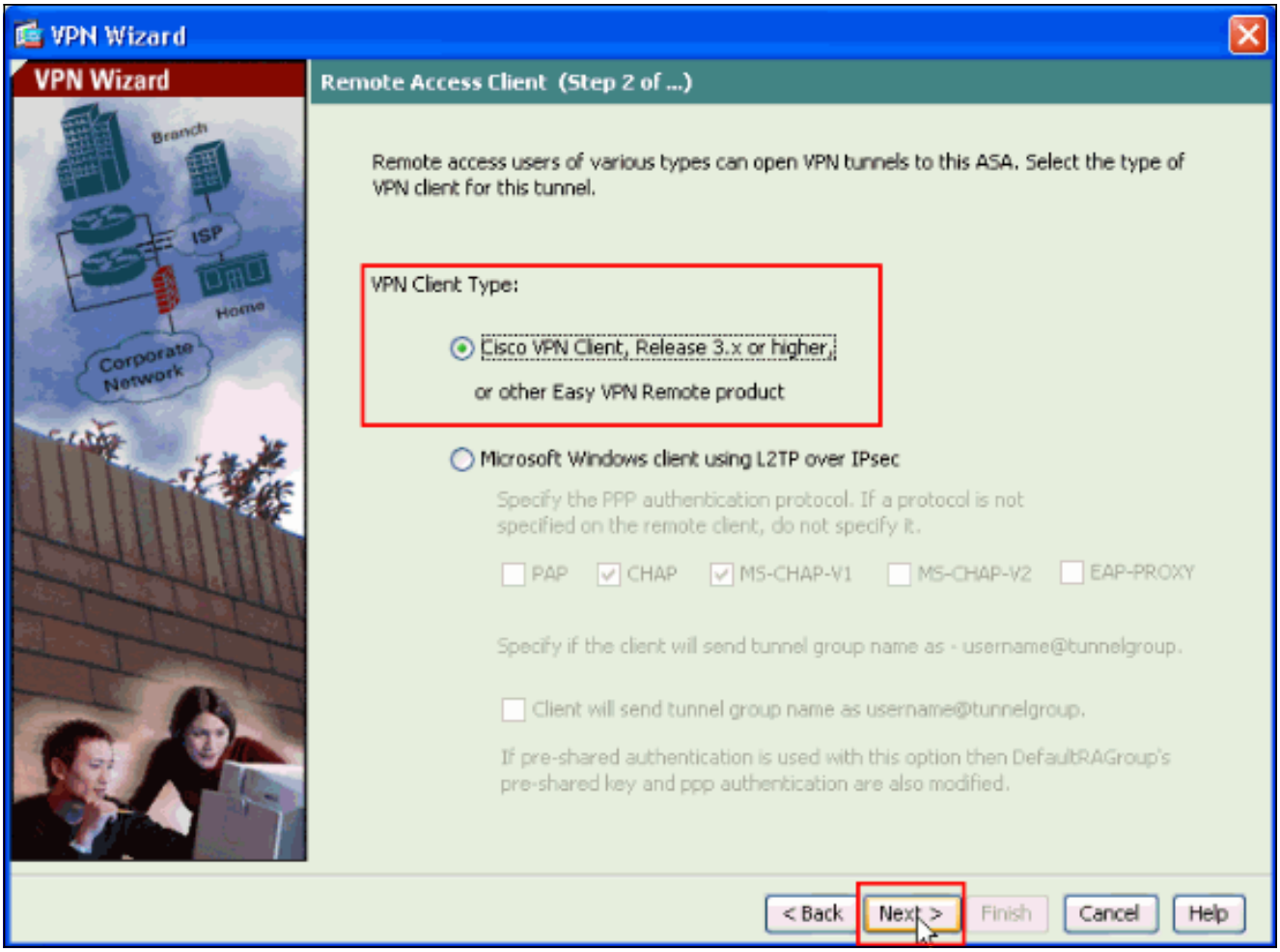
5. Wählen Sie im Home-Fenster **Wizards > IPsec VPN Wizard** aus.



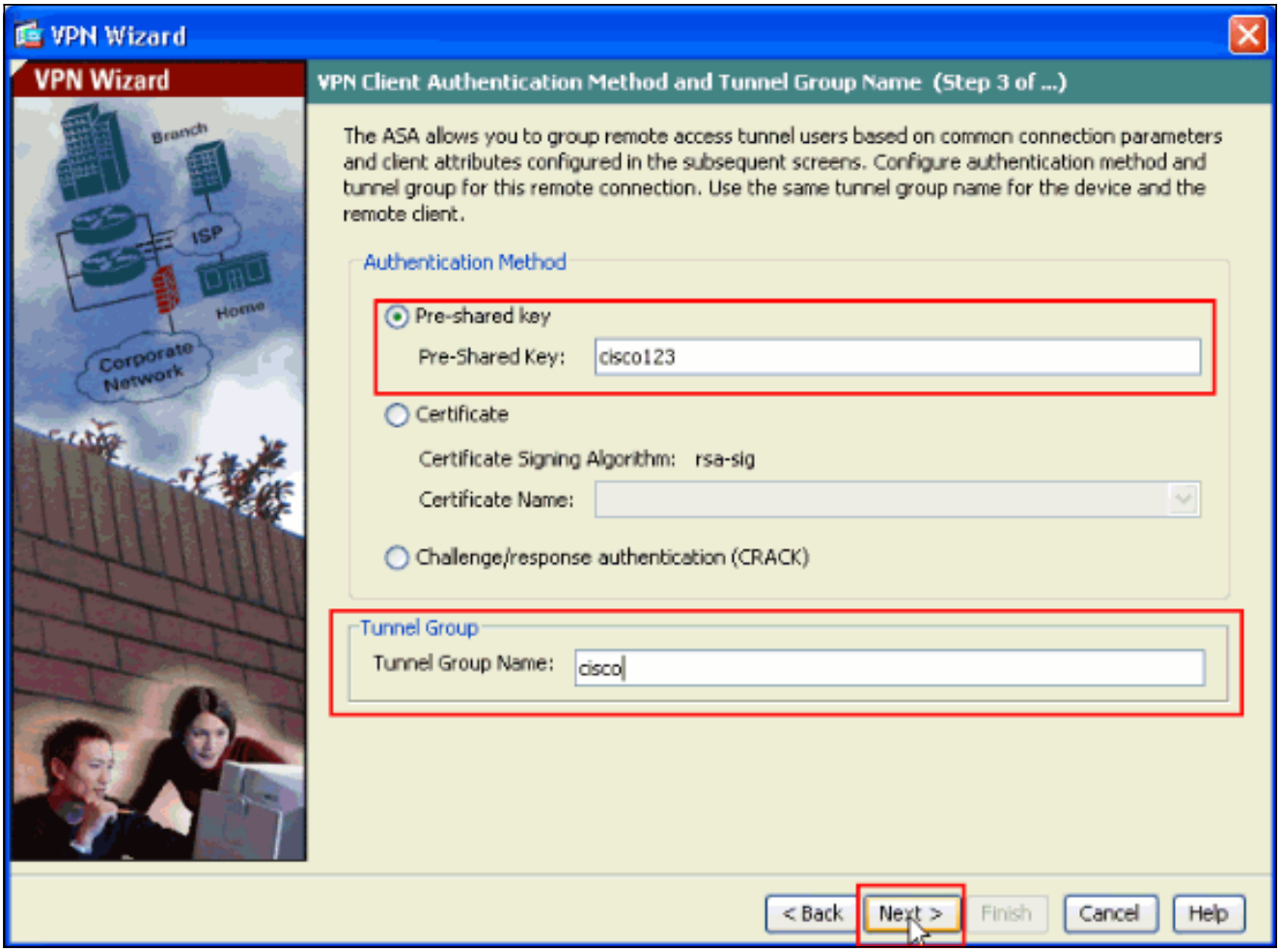
6. Wählen Sie den Tunneltyp **Remote Access** VPN aus, stellen Sie sicher, dass die VPN-Tunnel-Schnittstelle wie gewünscht eingestellt ist, und klicken Sie auf **Weiter**, wie hier gezeigt.



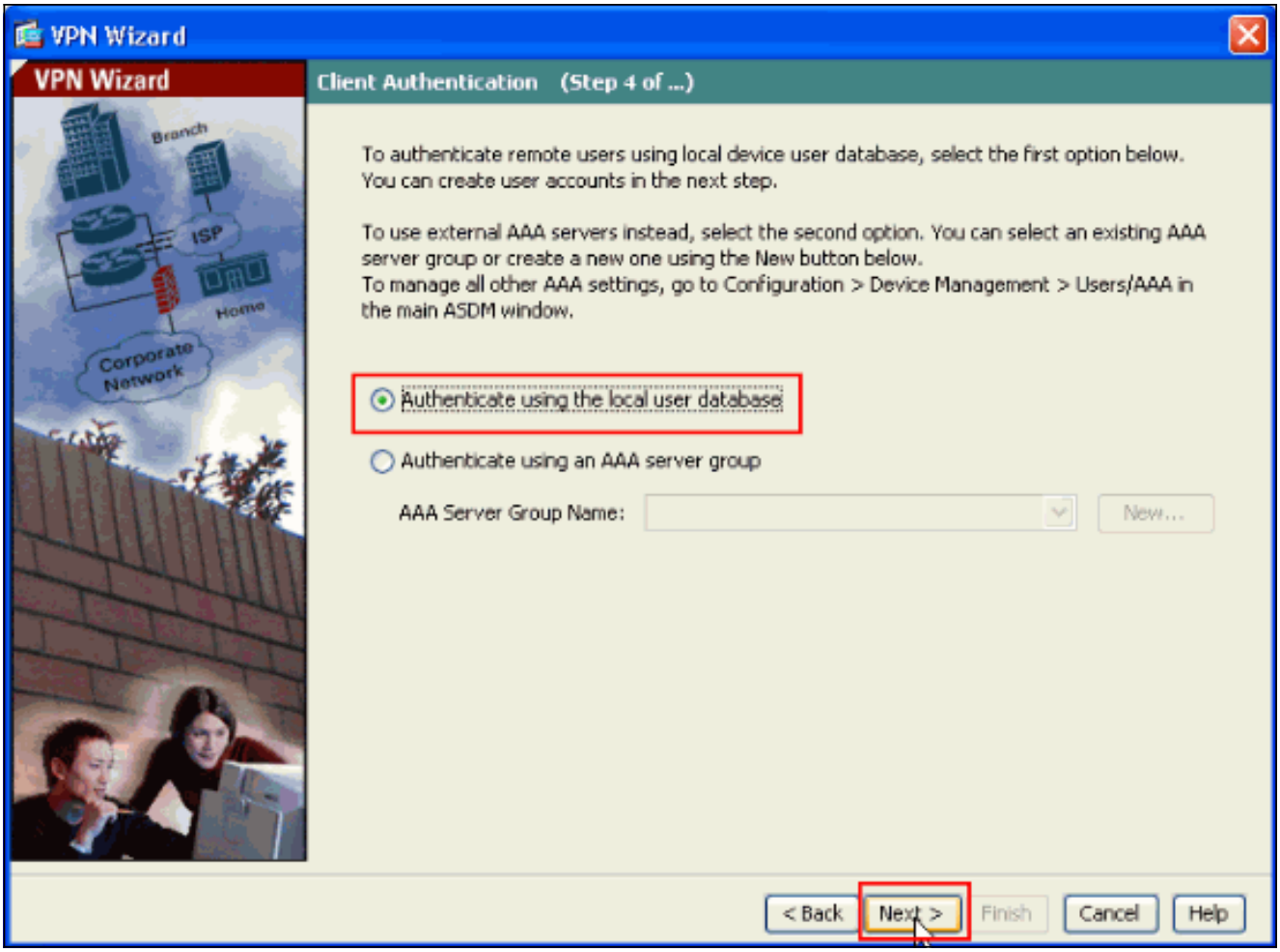
7. Der VPN-Client-Typ wird wie gezeigt ausgewählt. Hier wird **Cisco VPN Client** ausgewählt. Klicken Sie auf
Weiter.



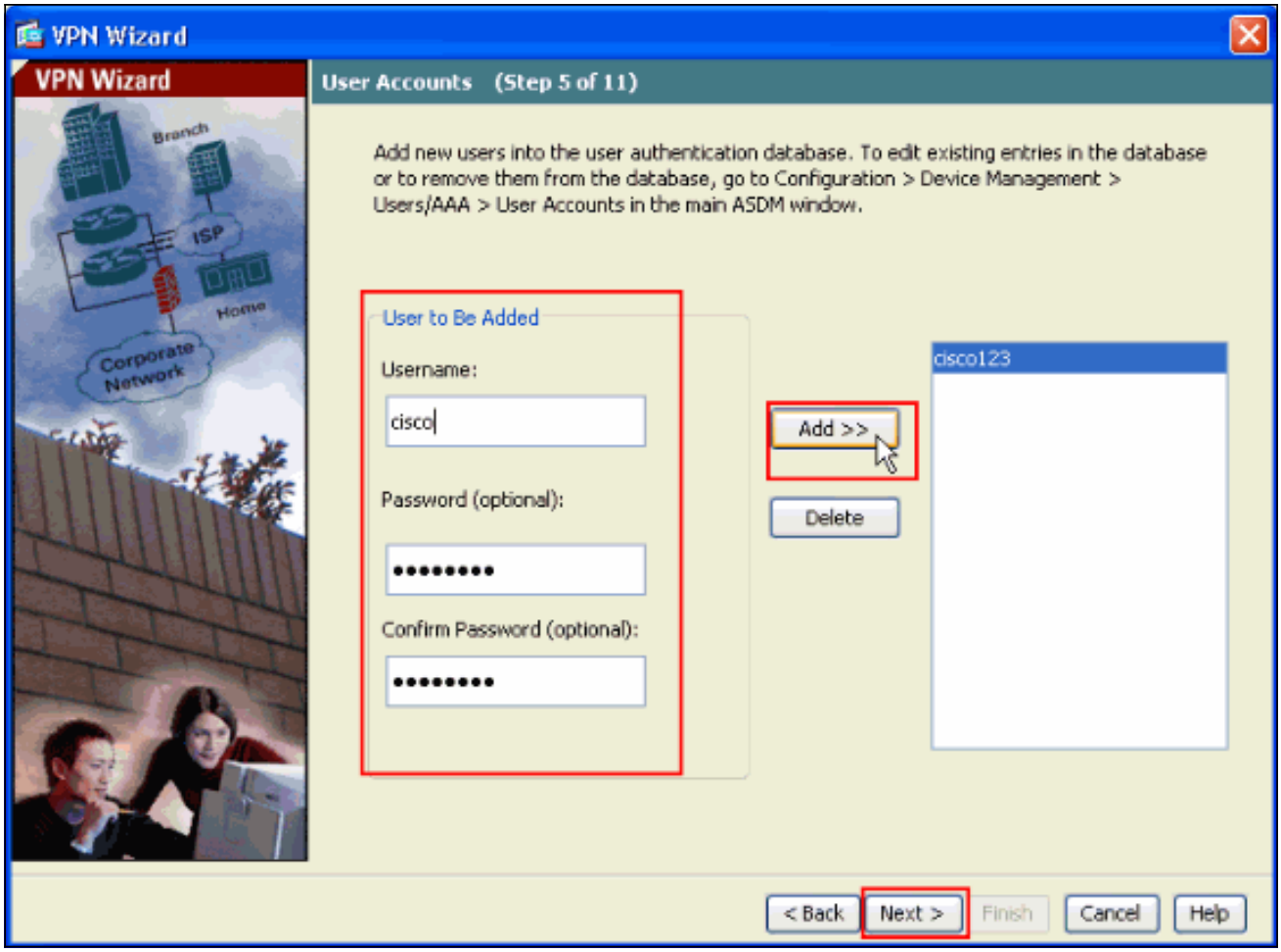
8. Geben Sie einen Namen für den **Tunnelgruppennamen ein**. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den **vorinstallierten Schlüssel** in diesem Beispiel. Der in diesem Beispiel verwendete vorinstallierte Schlüssel ist **cisco123**. Der in diesem Beispiel verwendete Tunnel-Gruppenname lautet **cisco**. Klicken Sie auf **Weiter**.



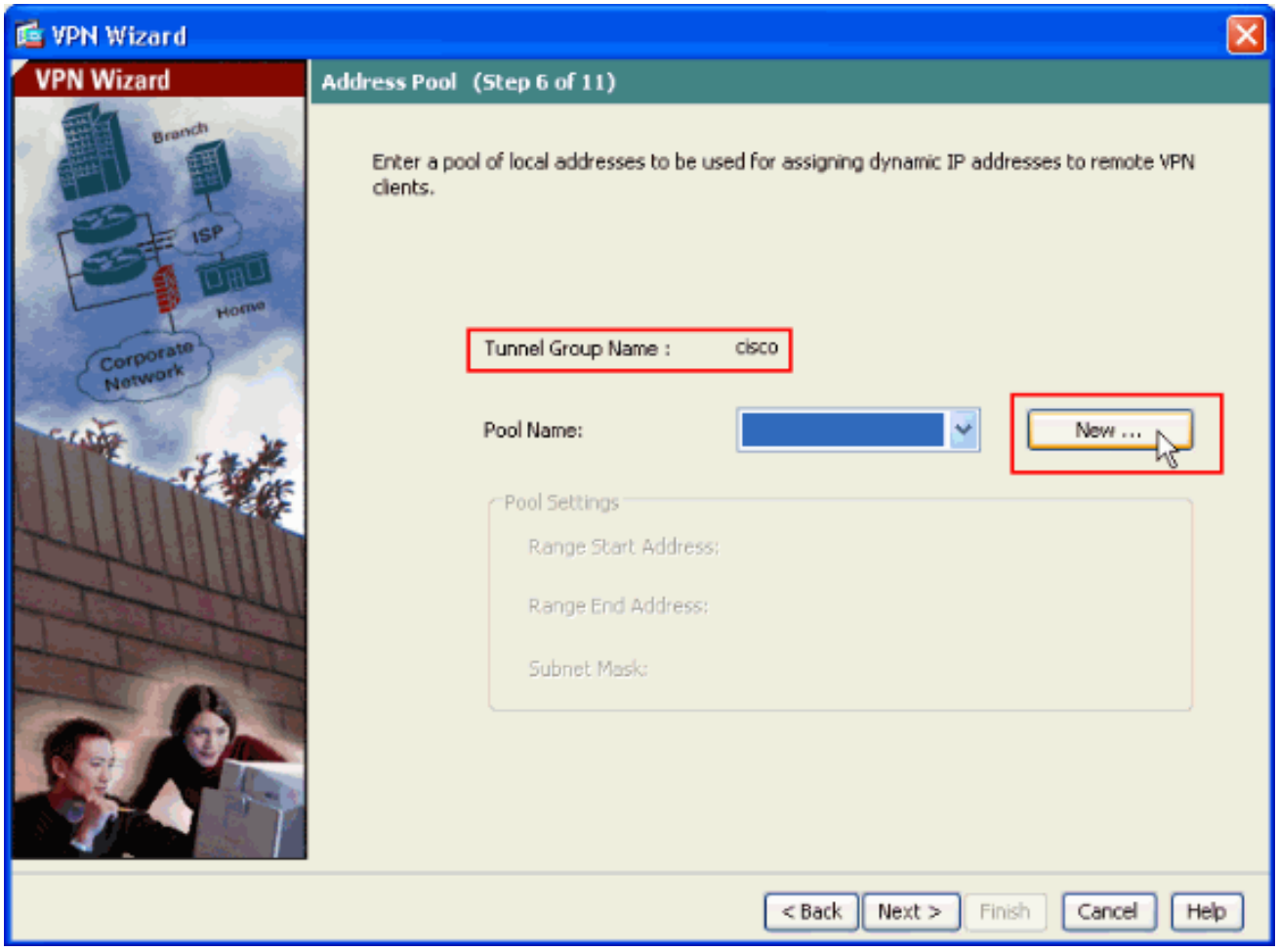
9. Wählen Sie aus, ob Remote-Benutzer in der lokalen Benutzerdatenbank oder in einer externen AAA-Servergruppe authentifiziert werden sollen.**Hinweis:** Sie fügen der lokalen Benutzerdatenbank in Schritt 10 Benutzer hinzu.**Hinweis:** Informationen zur Konfiguration einer externen AAA-Servergruppe mit ASDM finden Sie unter PIX/ASA 7.x Authentication and Authorization Server Groups für VPN-Benutzer unter ASDM Configuration Example (Konfigurationsbeispiel für
ASDM).



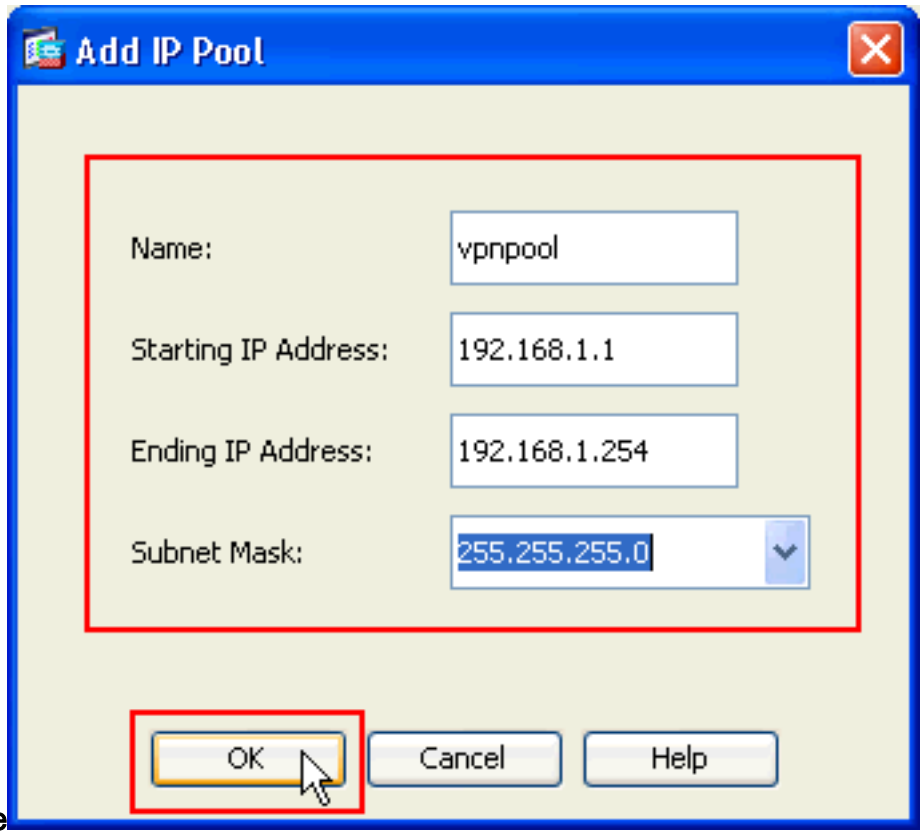
10. Geben Sie einen **Benutzernamen** und ein optionales **Kennwort ein,** und klicken Sie auf **Hinzufügen**, um der Benutzerauthentifizierungsdatenbank neue Benutzer hinzuzufügen. Klicken Sie auf **Weiter**.**Hinweis:** Entfernen Sie keine vorhandenen Benutzer aus diesem Fenster. Wählen Sie im ASDM-Hauptfenster **Konfiguration > Gerätemanagement > Benutzer/AAA > Benutzerkonten** aus, um vorhandene Datenbankeinträge zu bearbeiten oder aus der Datenbank zu
entfernen.



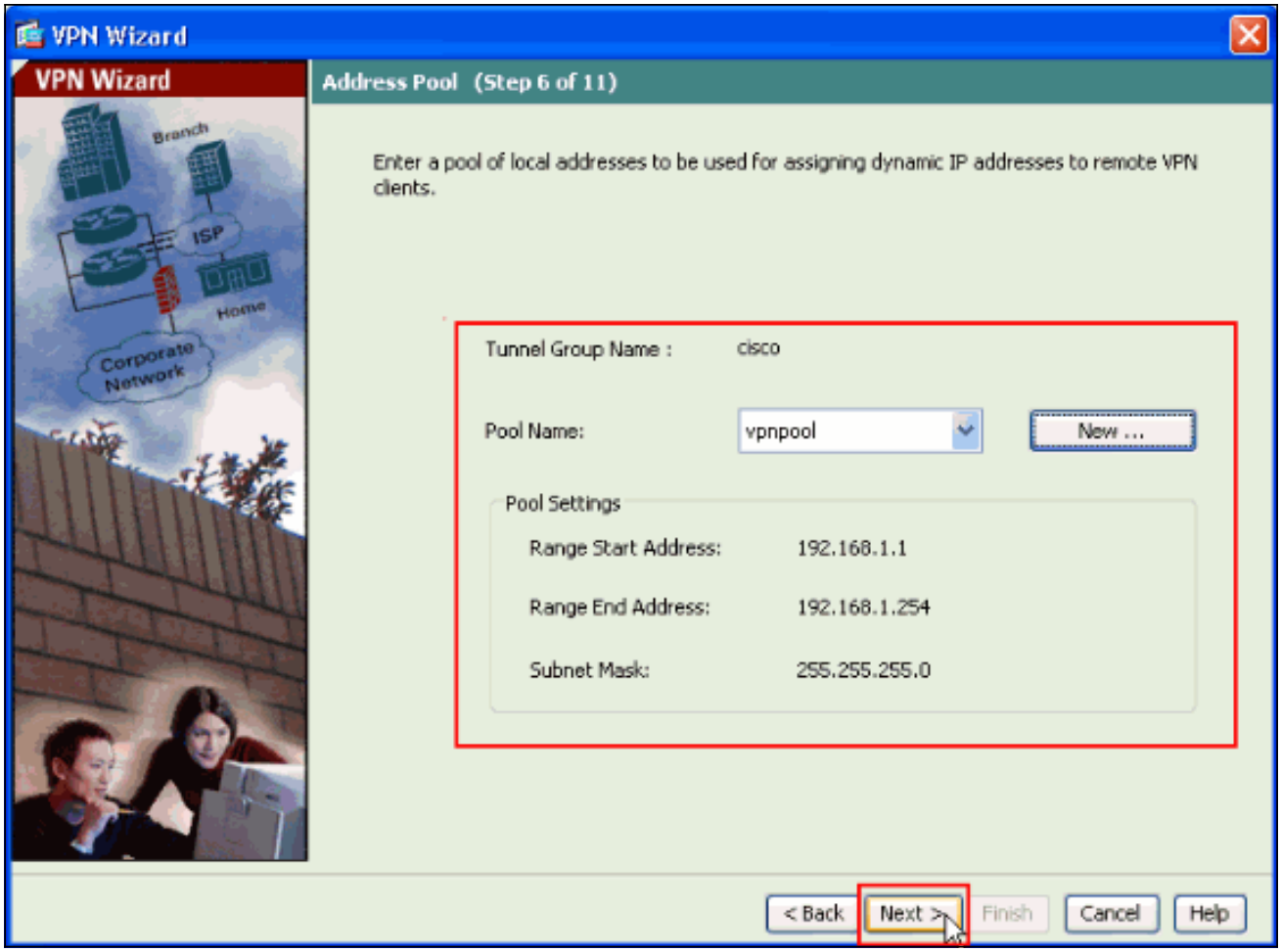
11. Um einen Pool lokaler Adressen zu definieren, die Remote-VPN-Clients dynamisch zugewiesen werden sollen, klicken Sie auf **Neu**, um einen neuen **IP-Pool** zu erstellen.



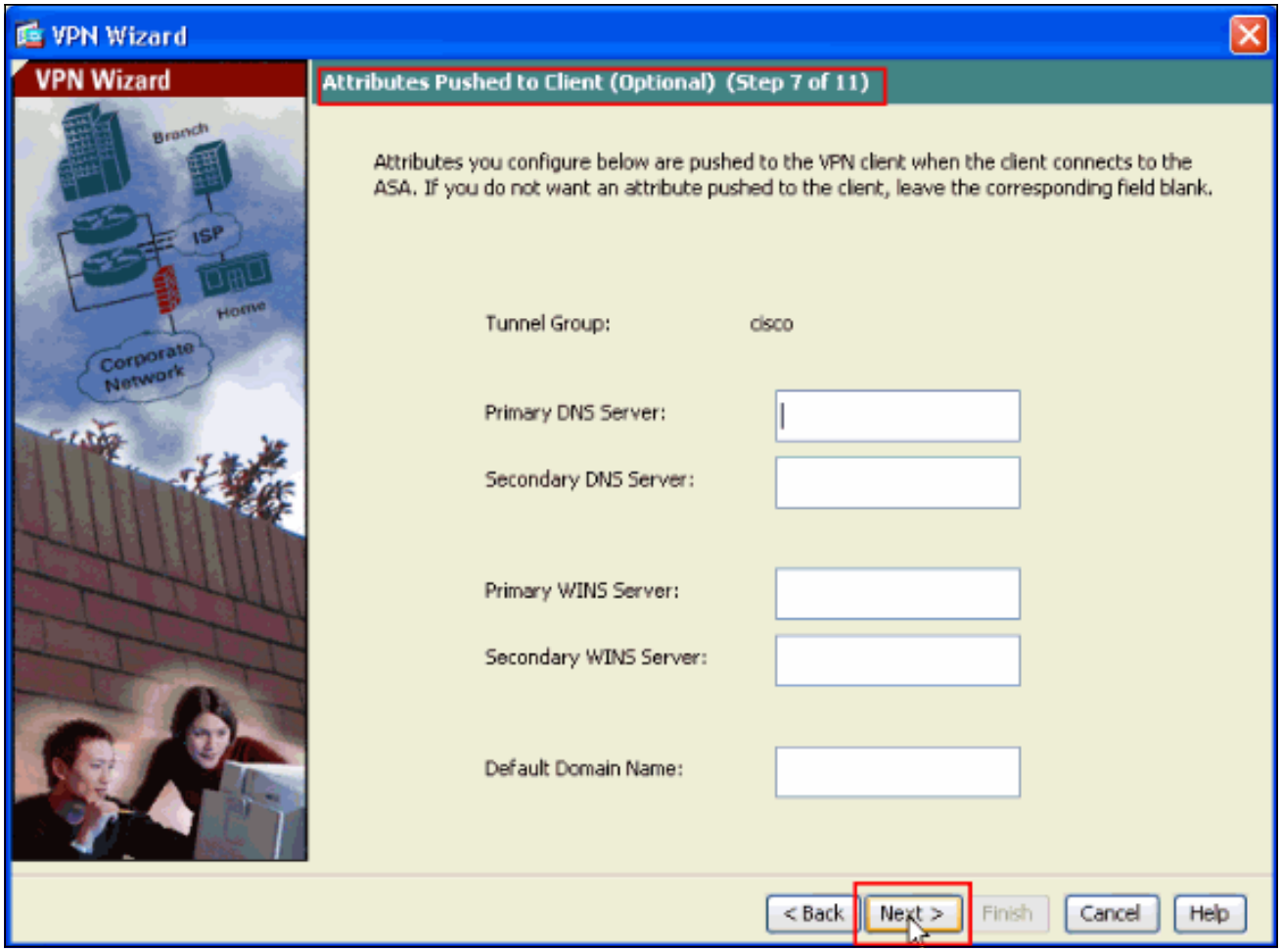
12. Geben Sie im neuen Fenster **Add IP Pool (IP-Pool hinzufügen)** diese Informationen an, und klicken Sie auf **OK**.**Name des IP-PoolsStart-IP-AdresseEnd-IP-AdresseSubnetzmaske**



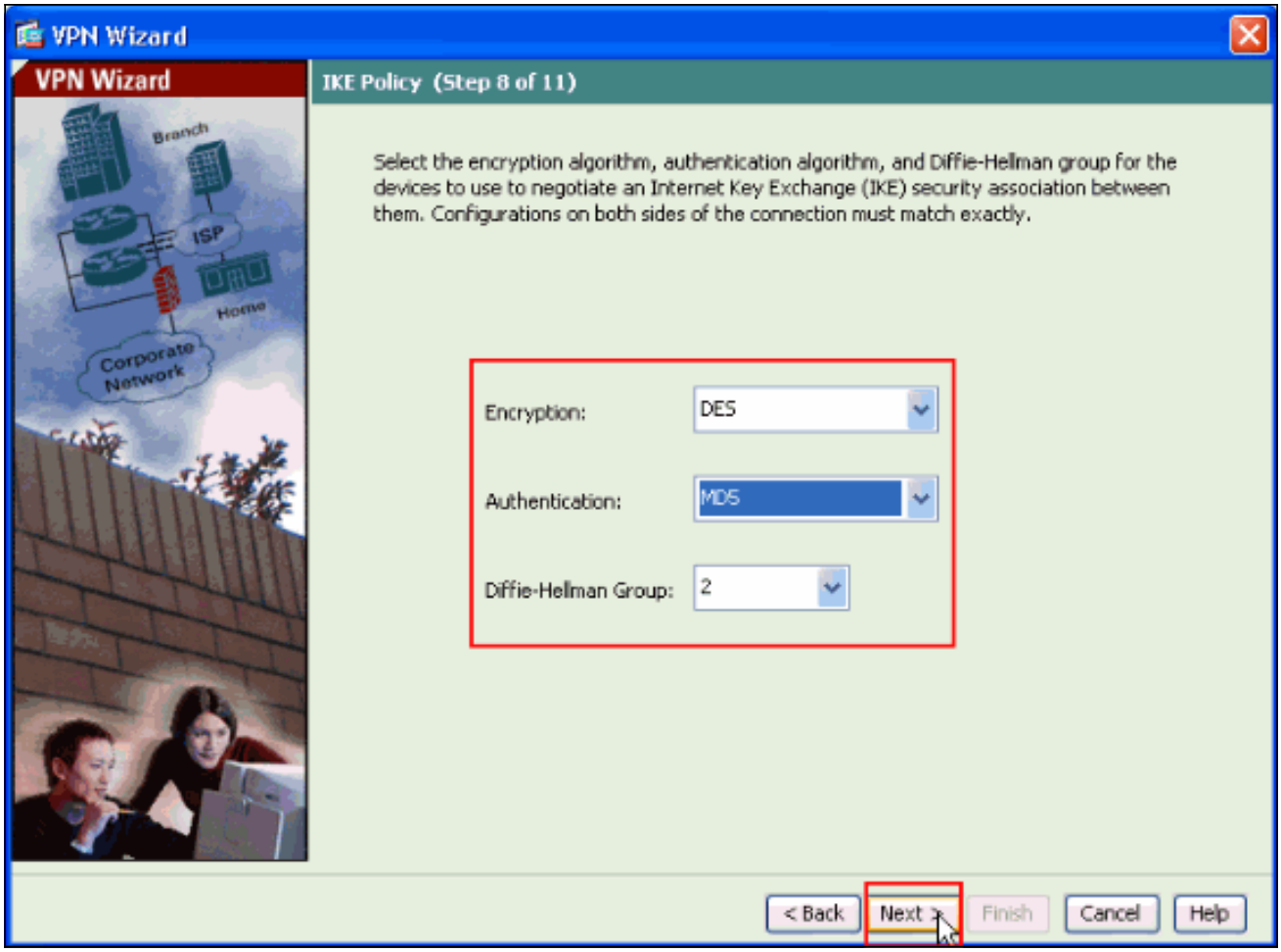
13. Nachdem Sie den Pool der lokalen Adressen definiert haben, die Remote-VPN-Clients beim Herstellen einer Verbindung dynamisch zugewiesen werden sollen, klicken Sie auf **Weiter.**



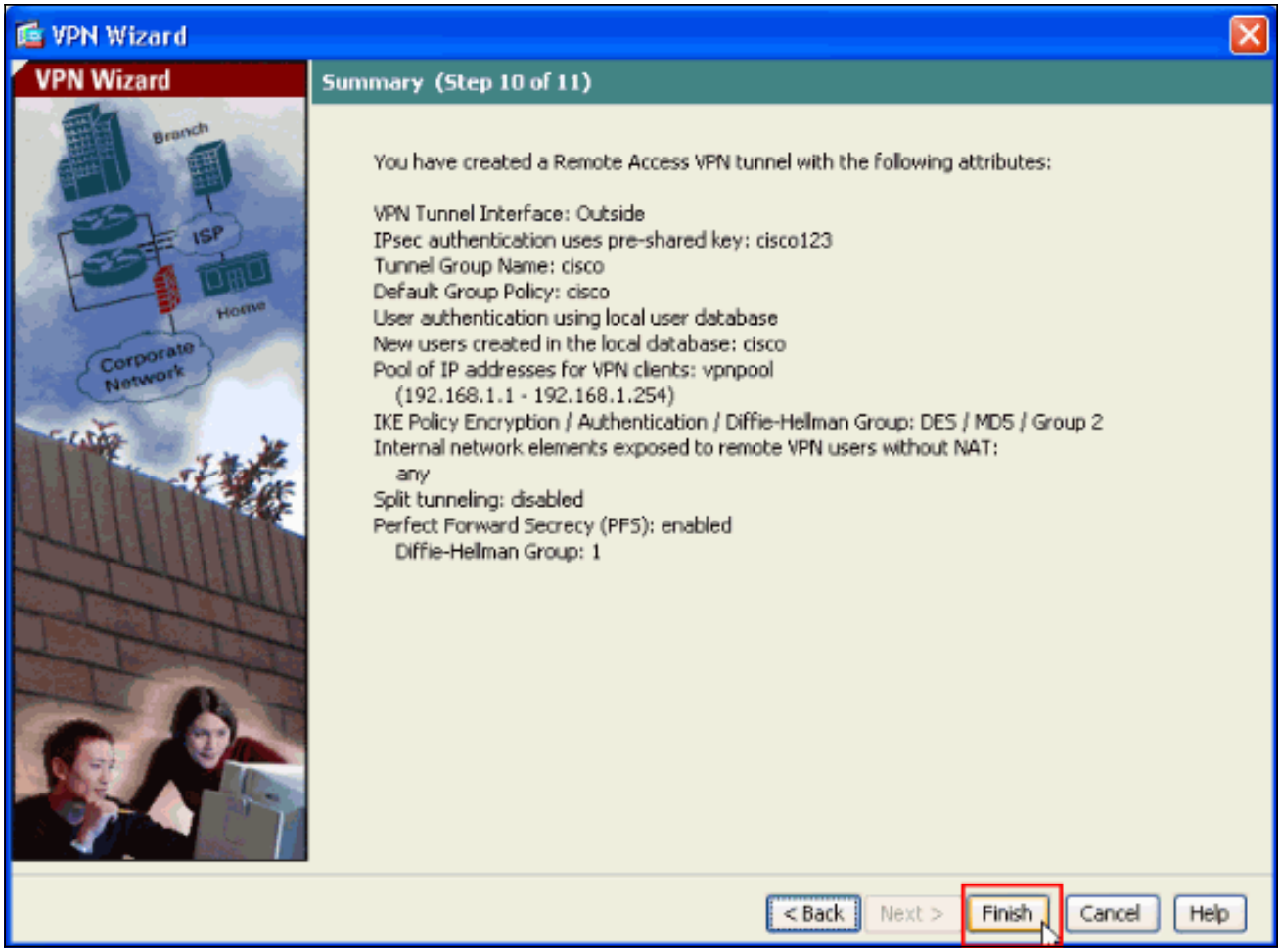
14. *Optional:* Geben Sie die DNS- und WINS-Serverinformationen und einen Standard-Domänennamen an, der an Remote-VPN-Clients übertragen werden soll.



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



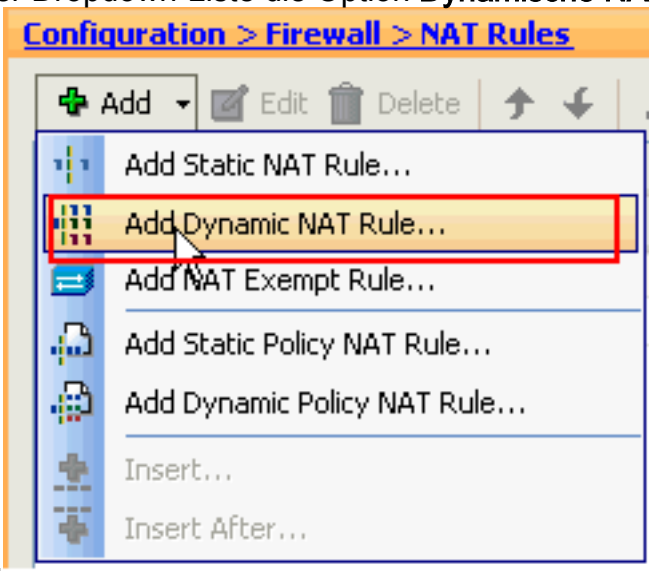
16. In diesem Fenster wird eine Zusammenfassung der von Ihnen ergriffenen Maßnahmen angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie mit Ihrer Konfiguration zufrieden sind.



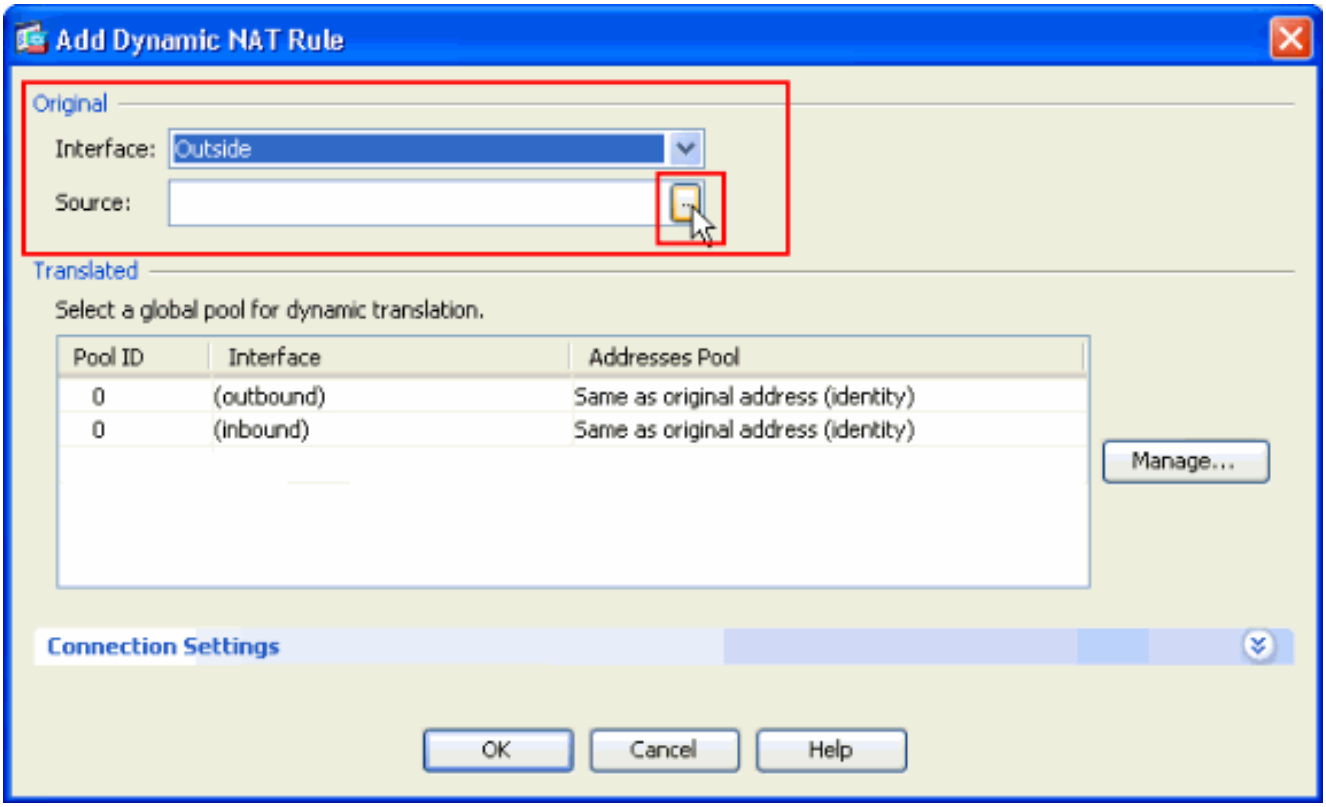
Konfigurieren des ASA/PIX für eingehenden VPN-Client-Datenverkehr von NAT mit ASDM

Gehen Sie wie folgt vor, um den Datenverkehr des Cisco ASA-to-NAT-eingehenden VPN-Clients mit ASDM zu konfigurieren:

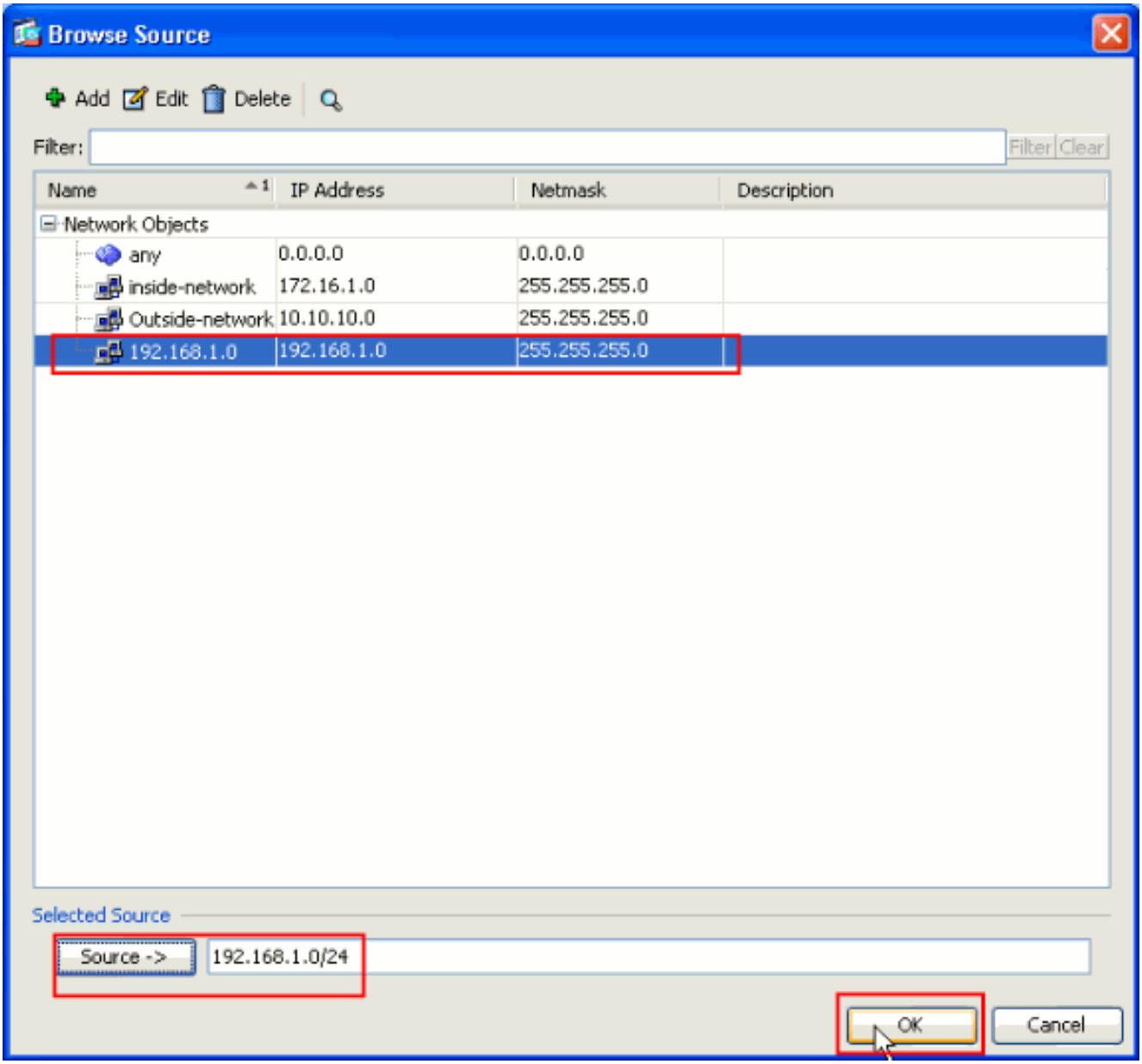
1. Wählen Sie **Konfiguration > Firewall > NAT Rules aus**, und klicken Sie auf **Add**. Wählen Sie in der Dropdown-Liste die Option **Dynamische NAT-Regel hinzufügen aus**.



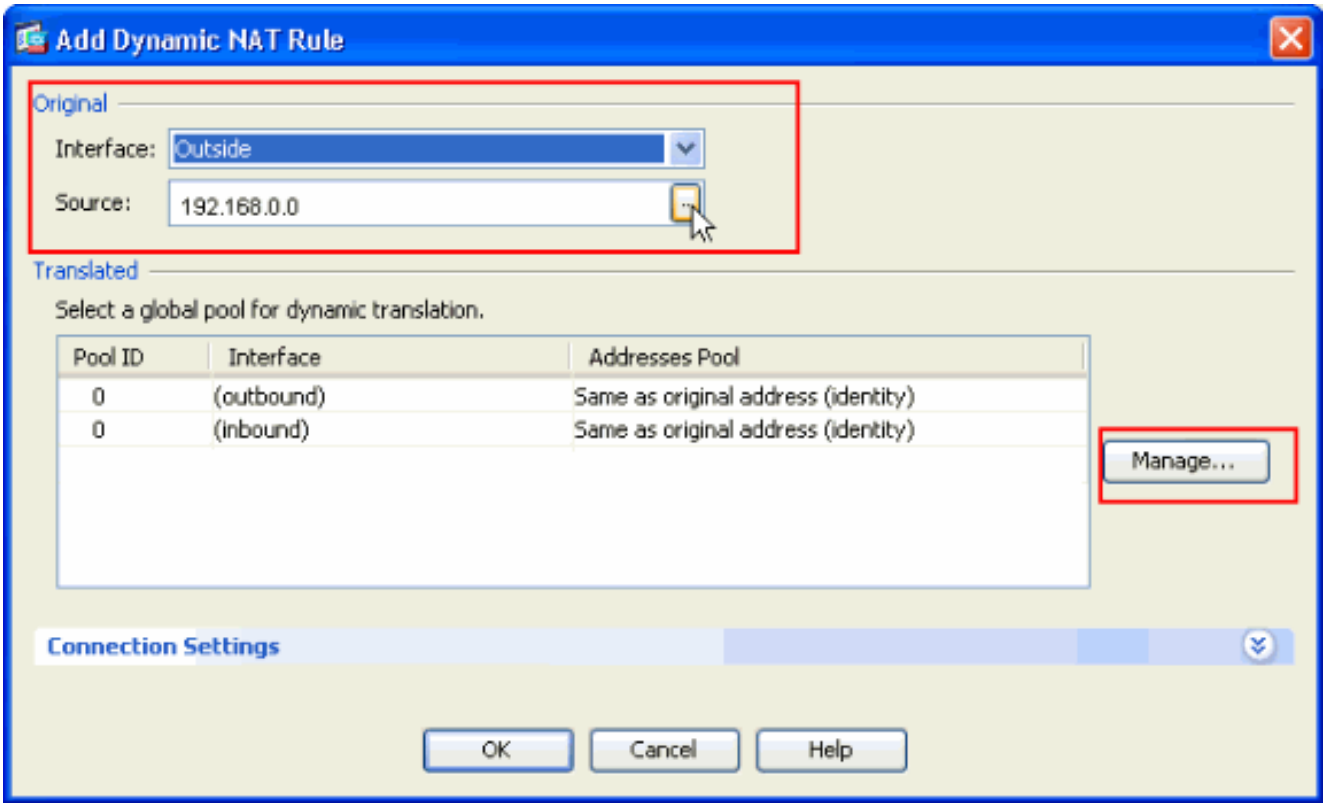
2. Wählen Sie im Fenster **Dynamische NAT-Regel hinzufügen** die Option **Außerhalb** als Schnittstelle aus, und klicken Sie auf die Schaltfläche Durchsuchen neben dem Feld **Quelle**.



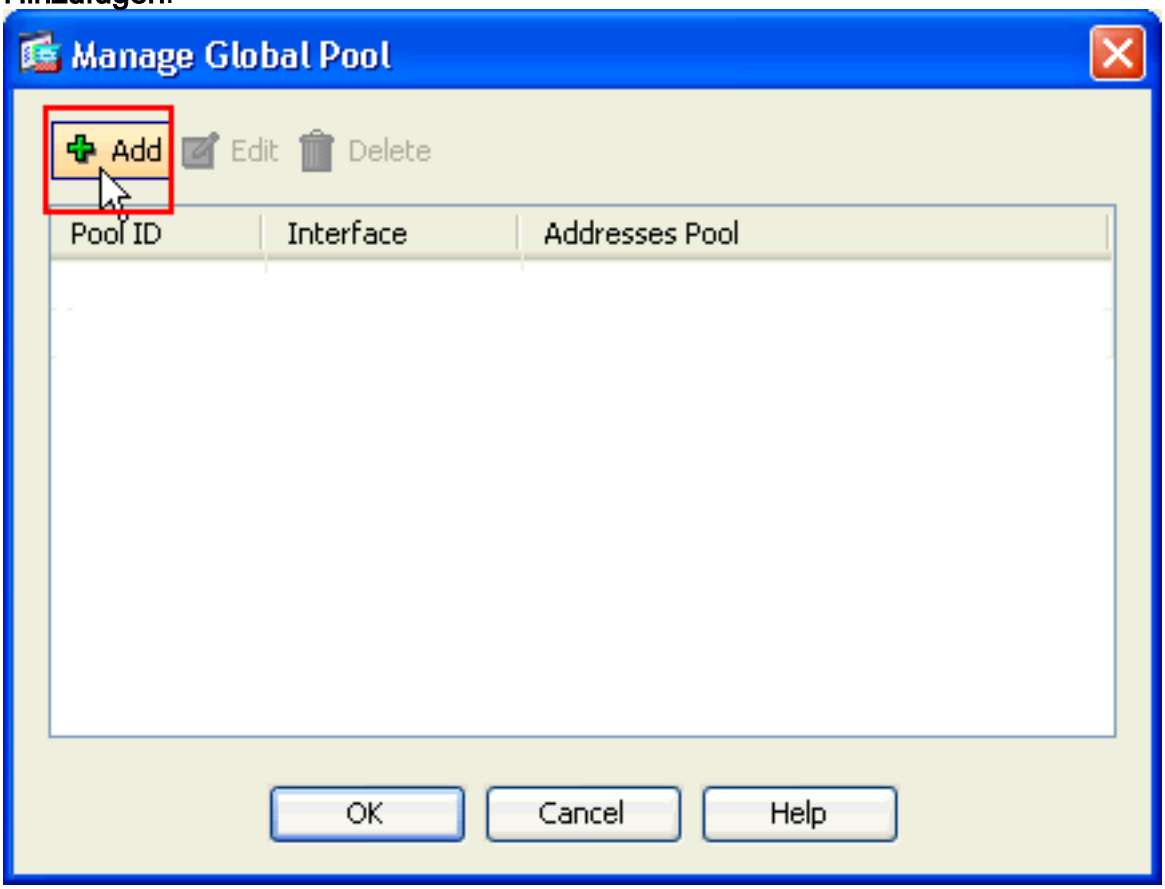
3. Wählen Sie im Fenster Quelle durchsuchen die richtigen Netzwerkobjekte aus, wählen Sie im Abschnitt Ausgewählte Quelle auch die **Quelle aus**, und klicken Sie auf **OK**. Hier wird das Netzwerkobjekt 192.168.1.0
ausgewählt.



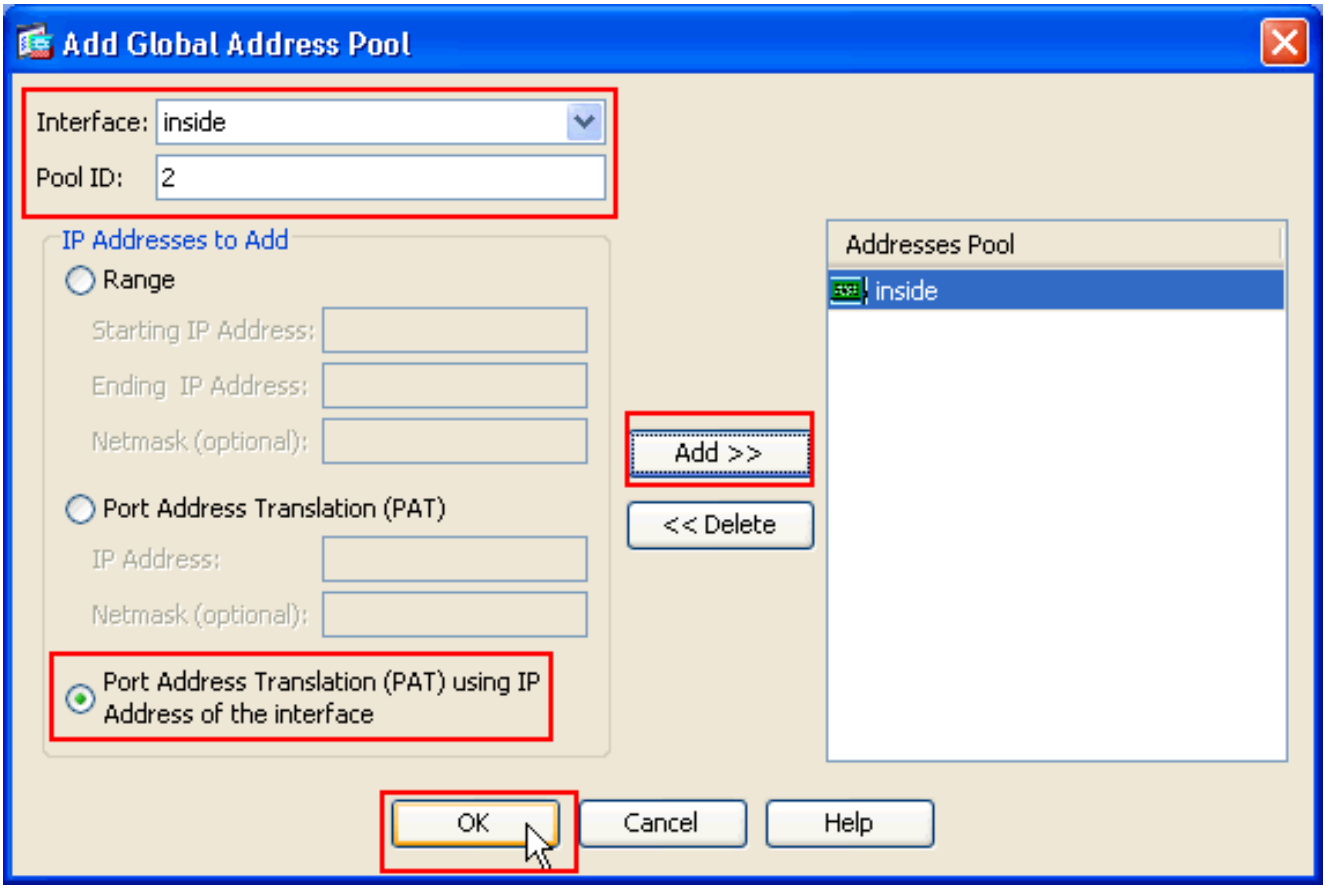
4. Klicken Sie auf **Verwalten**.



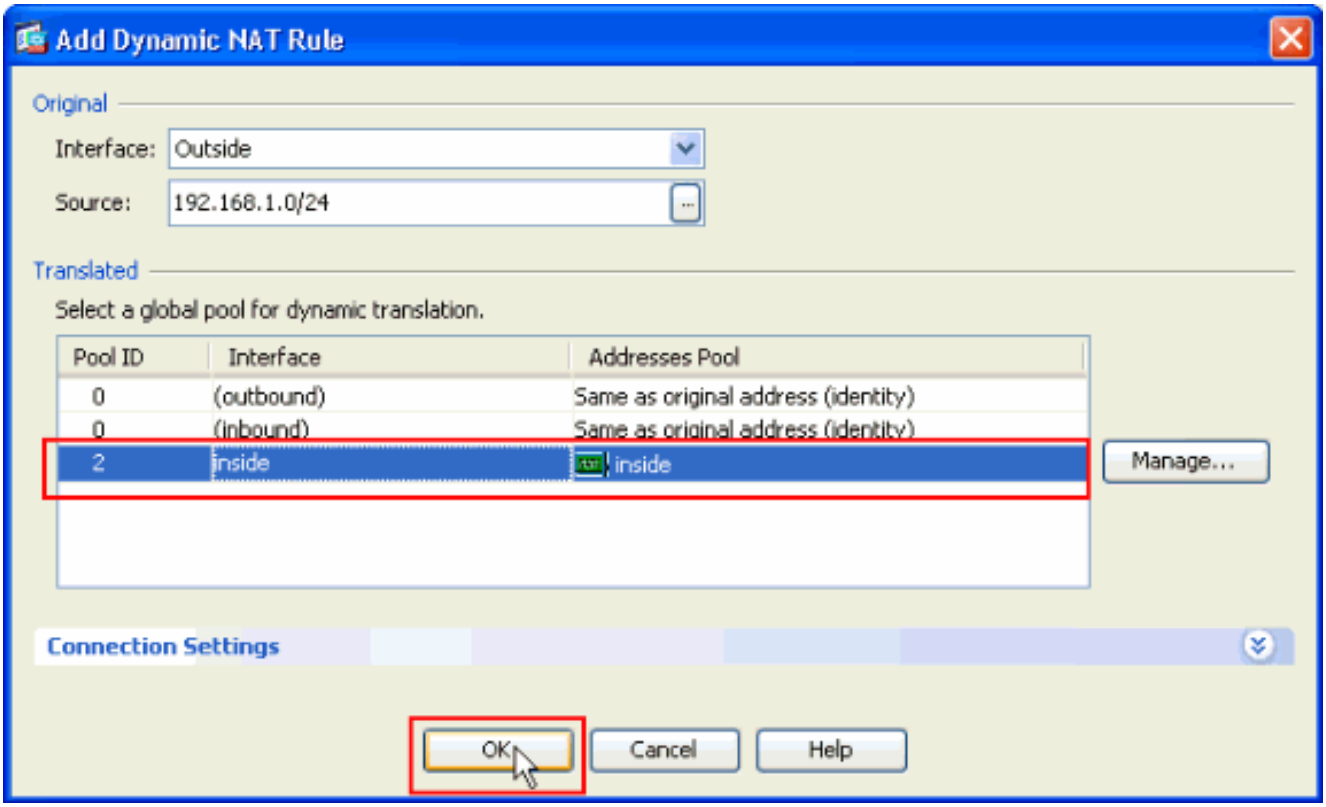
5. Klicken Sie im Fenster Globalen Pool verwalten auf **Hinzufügen**.



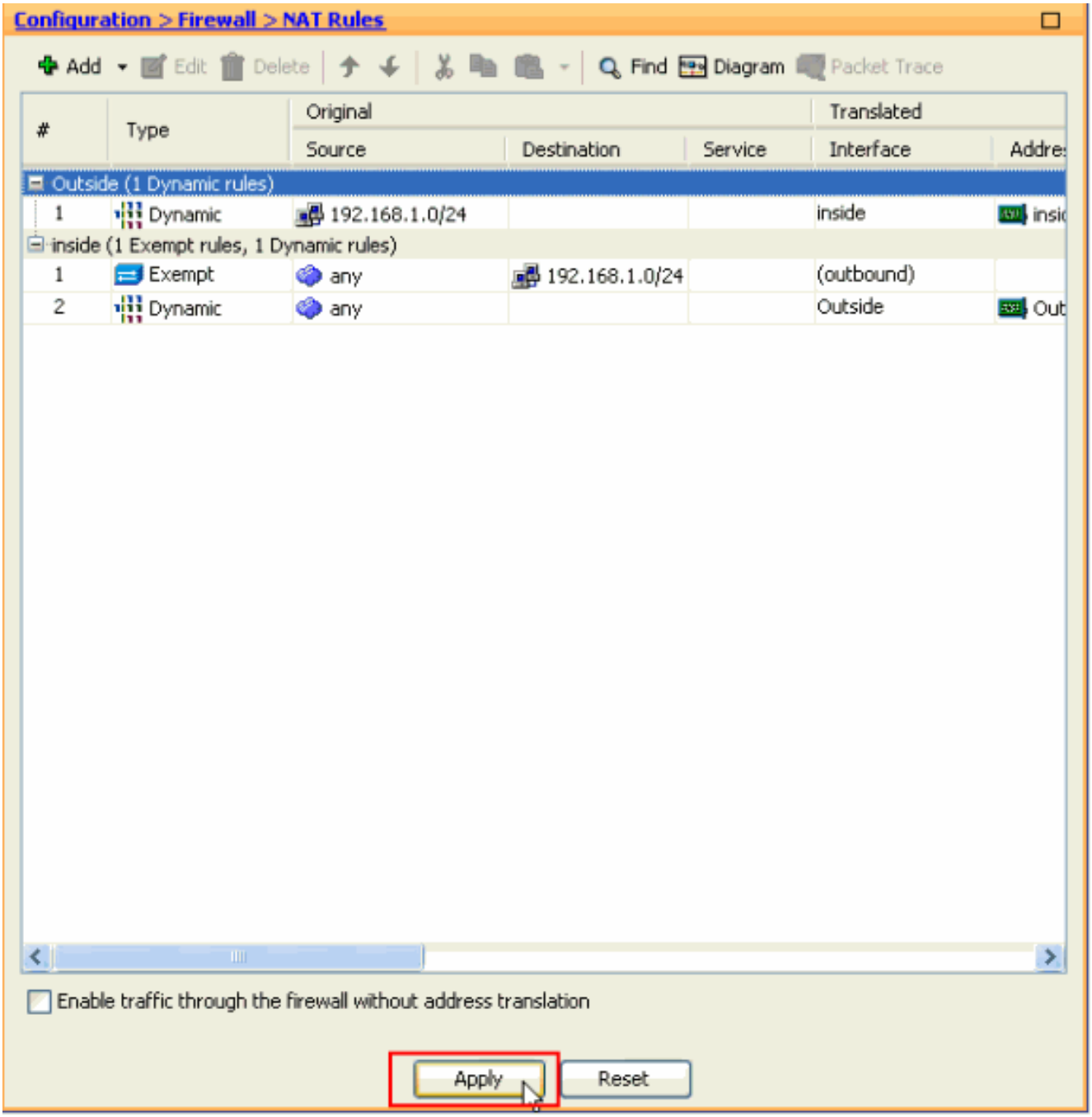
6. Wählen Sie im Fenster Globalen Adresspool hinzufügen die Option **Inside** als Schnittstelle und **2** als **Pool-ID aus**. Stellen Sie außerdem sicher, dass das Optionsfeld neben **PAT unter Verwendung der IP-Adresse der Schnittstelle** aktiviert ist. Klicken Sie auf **Hinzufügen>>** und dann auf **OK**.



7. Klicken Sie auf **OK**, nachdem Sie den globalen Pool mit der im vorherigen Schritt konfigurierten **Pool-ID 2** ausgewählt haben.



8. Klicken Sie jetzt auf **Apply**, um die Konfiguration auf die ASA anzuwenden.Damit ist die Konfiguration abgeschlossen.



Konfigurieren von ASA/PIX als Remote-VPN-Server und für eingehende NAT mit der CLI

Ausführen der Konfiguration auf dem ASA-Gerät
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0

```
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa803-k8.bin
ftp mode passive
access-list inside_nat0_outbound extended permit ip any
192.168.1.0 255.255.255
0
pager lines 24
logging enable
mtu Outside 1500
mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
asdm history enable
arp timeout 14400
nat-control
global (Outside) 1 interface
global (inside) 2 interface
nat (Outside) 2 192.168.1.0 255.255.255.0 outside
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
no snmp-server location
no snmp-server contact

!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-DES-
SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-
hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
transform-set ESP-DES-SH
 ESP-DES-MD5
crypto map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Outside_map interface Outside
crypto isakmp enable Outside

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
```

```
used during an IKE negotiation. Encryption and !---
Policy details are hidden as the default values are
chosen. crypto isakmp policy 10
authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
 vpn-tunnel-protocol IPSec

!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0

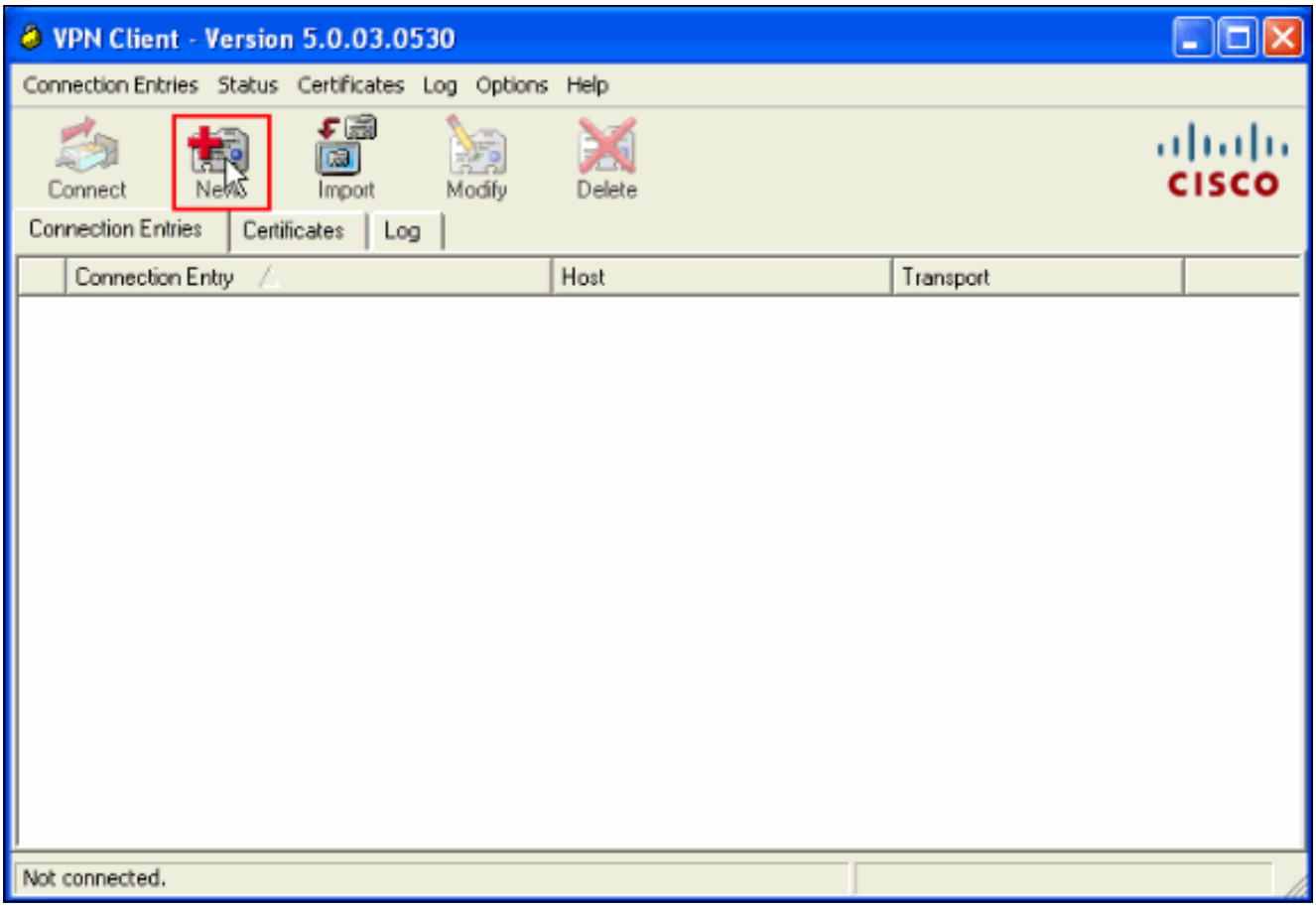
username cisco attributes
 vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
 address-pool vpnpool
 default-group-policy cisco

!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
```

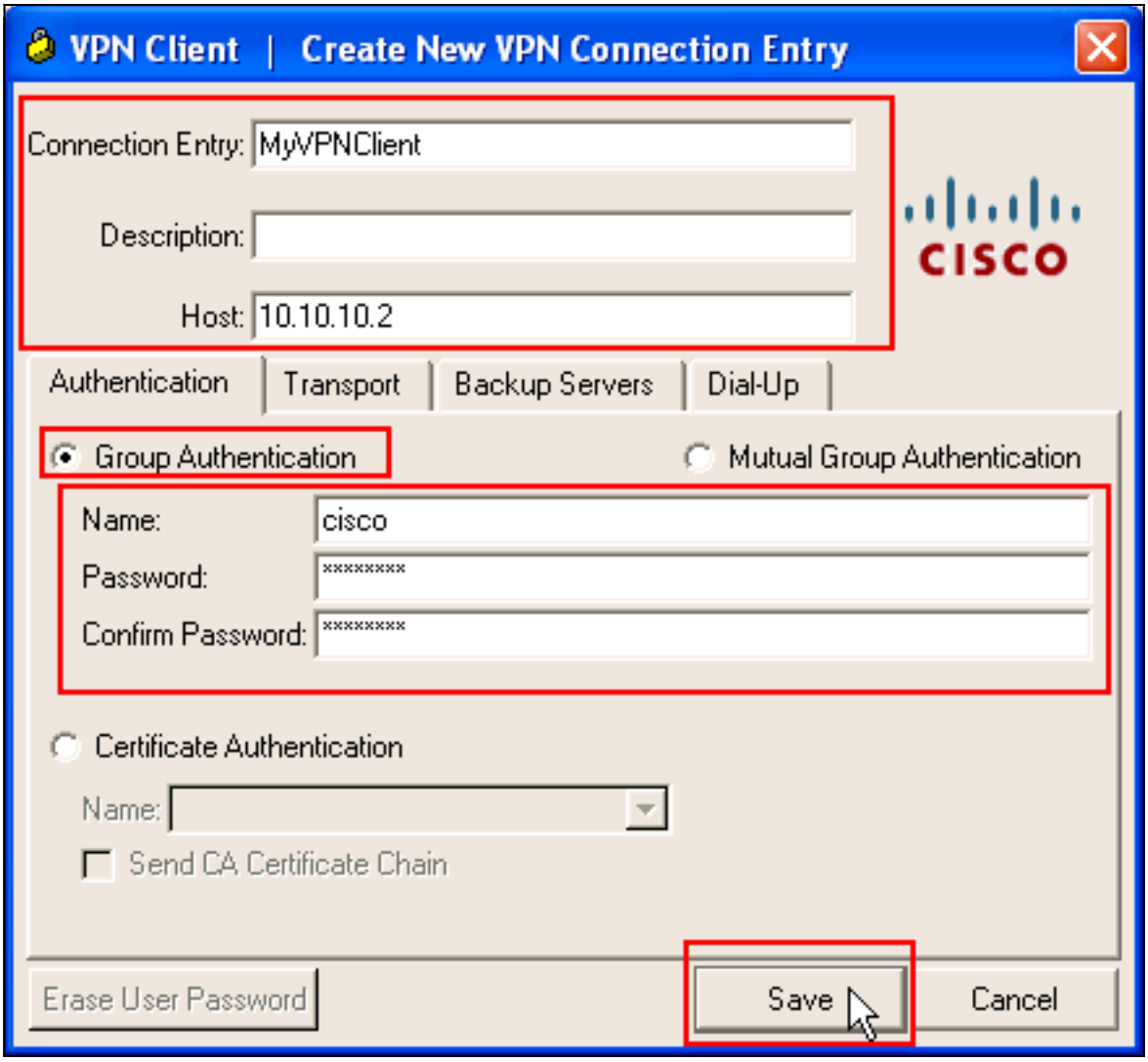
```
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

Überprüfen

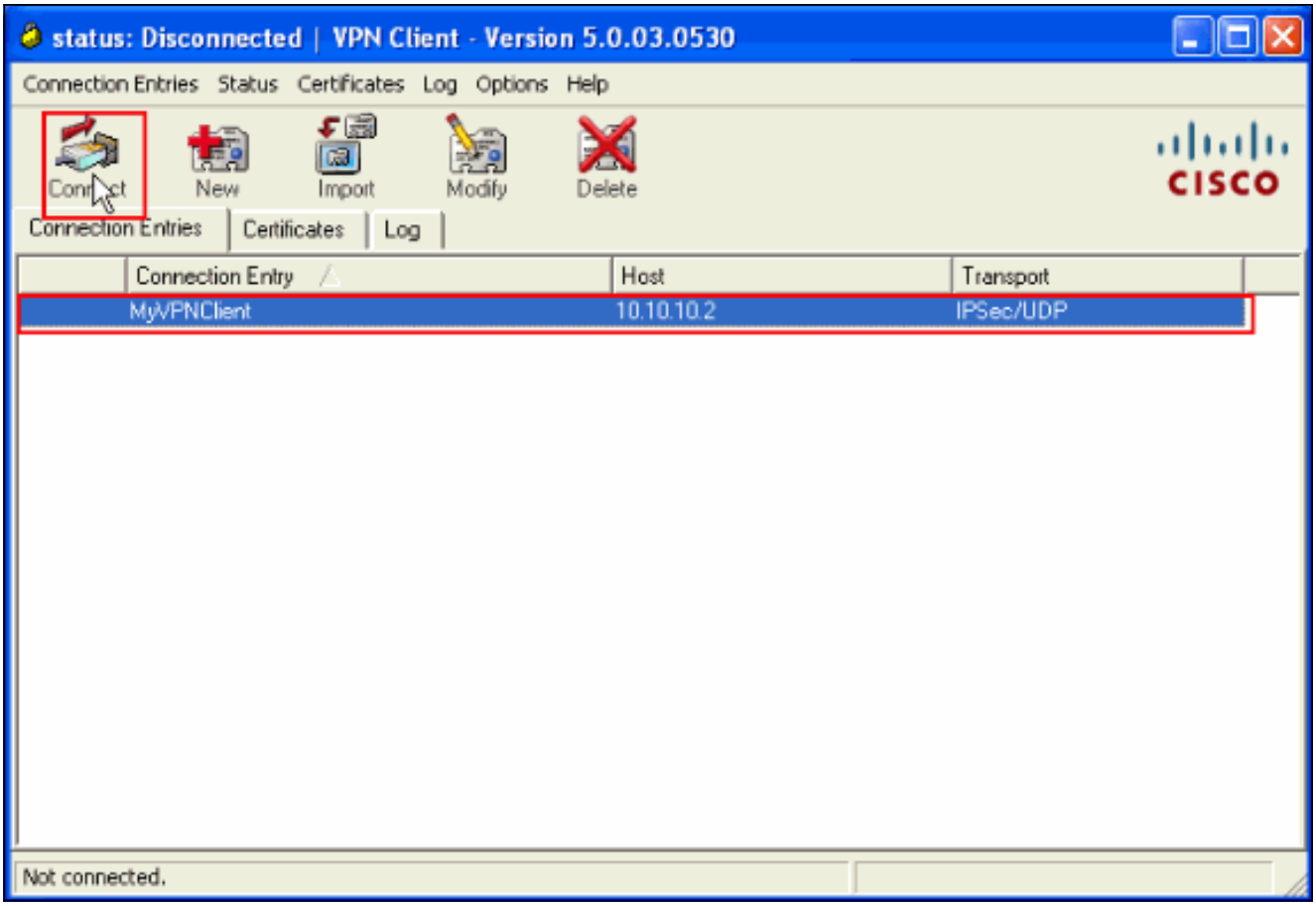
Versuchen Sie, über den Cisco VPN-Client eine Verbindung zur Cisco ASA herzustellen, um zu überprüfen, ob die ASA erfolgreich konfiguriert wurde.

1. Klicken Sie auf
   Neu.


2. Füllen Sie die Details Ihrer neuen Verbindung aus.Das Host-Feld muss die IP-Adresse oder den Hostnamen der zuvor konfigurierten Cisco ASA enthalten. Die Informationen zur Gruppenauthentifizierung müssen mit denen in **Schritt 4** übereinstimmen. Klicken Sie abschließend auf
   Speichern.

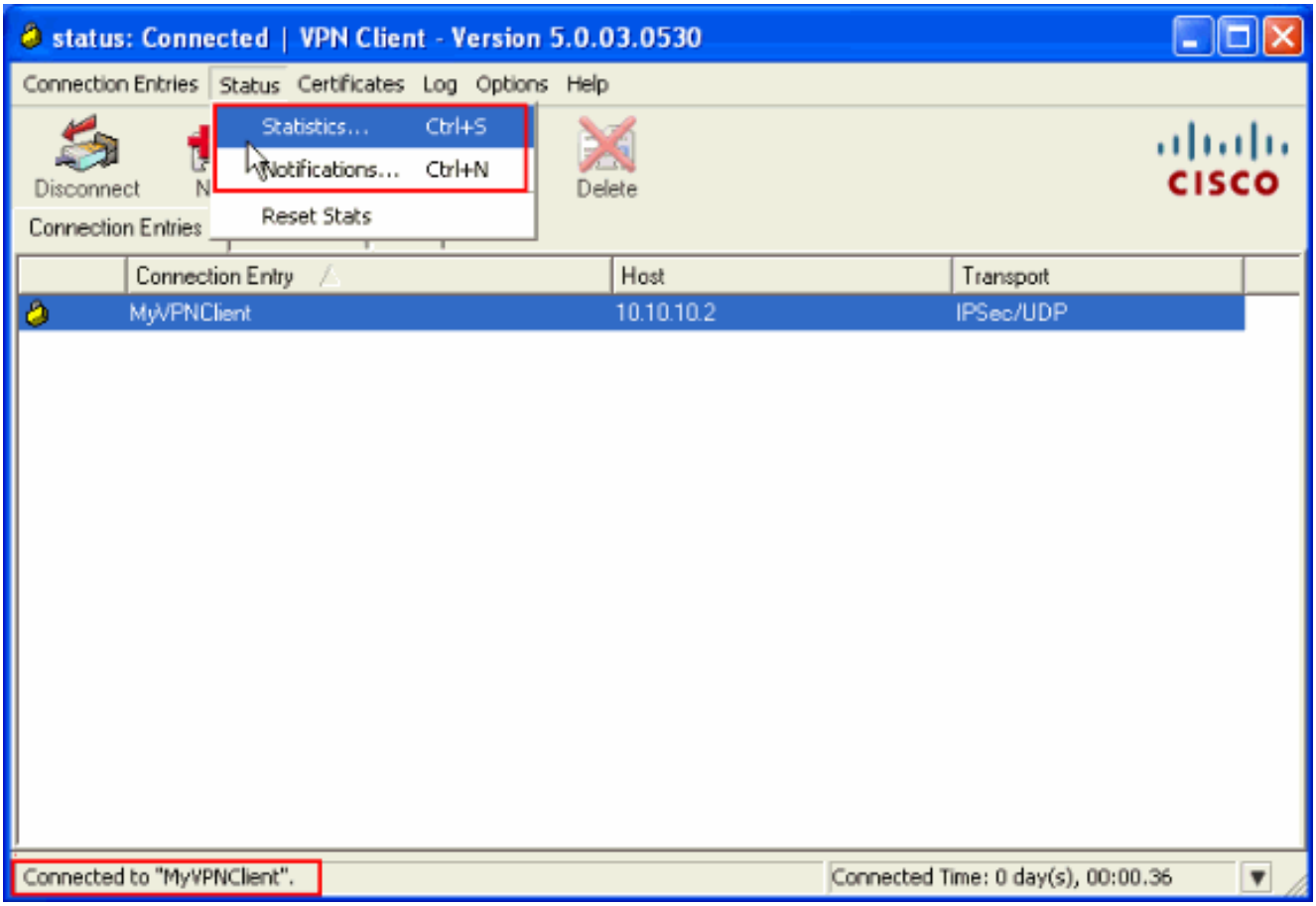


3. Wählen Sie die neu erstellte Verbindung aus, und klicken Sie auf **Verbinden**.

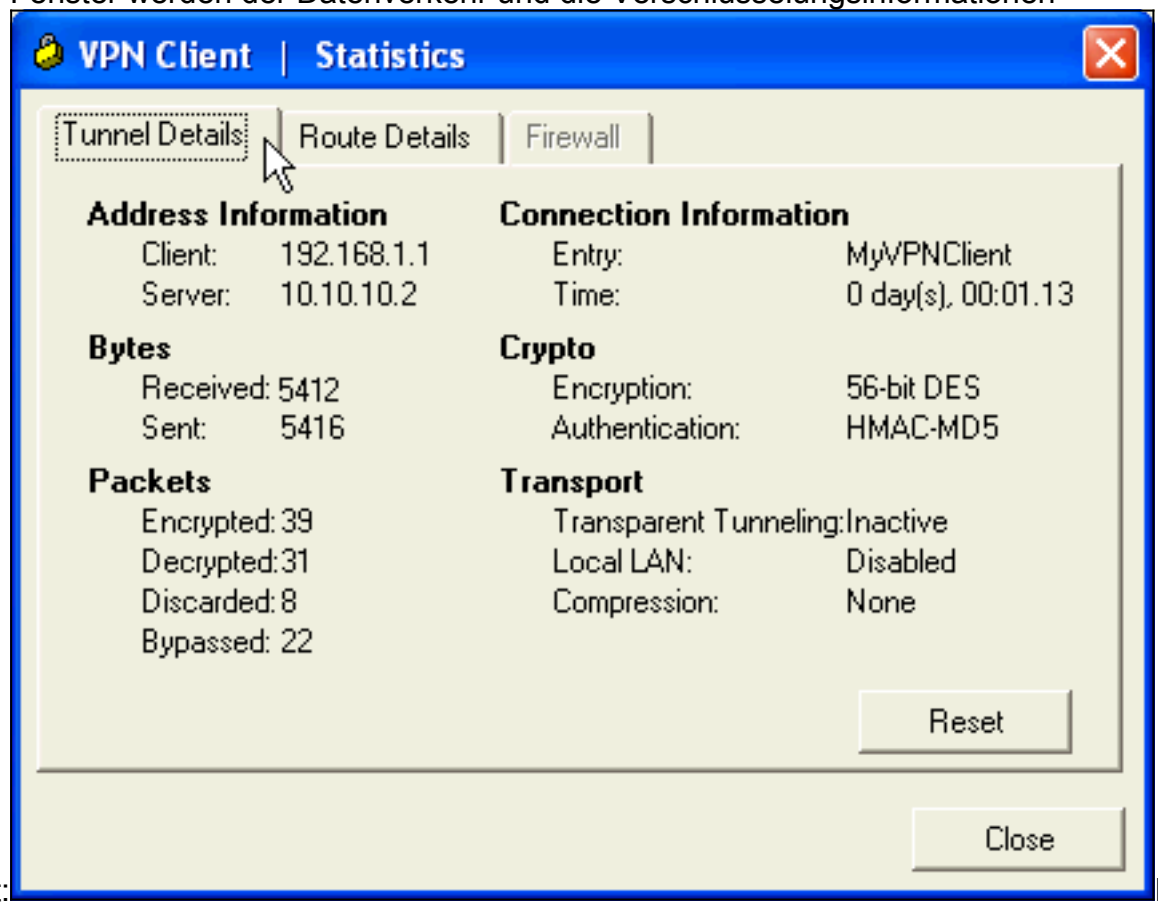


4. Geben Sie einen Benutzernamen und ein Kennwort für die erweiterte Authentifizierung ein. Diese Informationen müssen mit den in den **Schritten 5 und 6** angegebenen übereinstimmen.

5. Wenn die Verbindung erfolgreich hergestellt wurde, wählen Sie im Menü Status die Option **Statistik**, um die Details des Tunnels zu überprüfen.

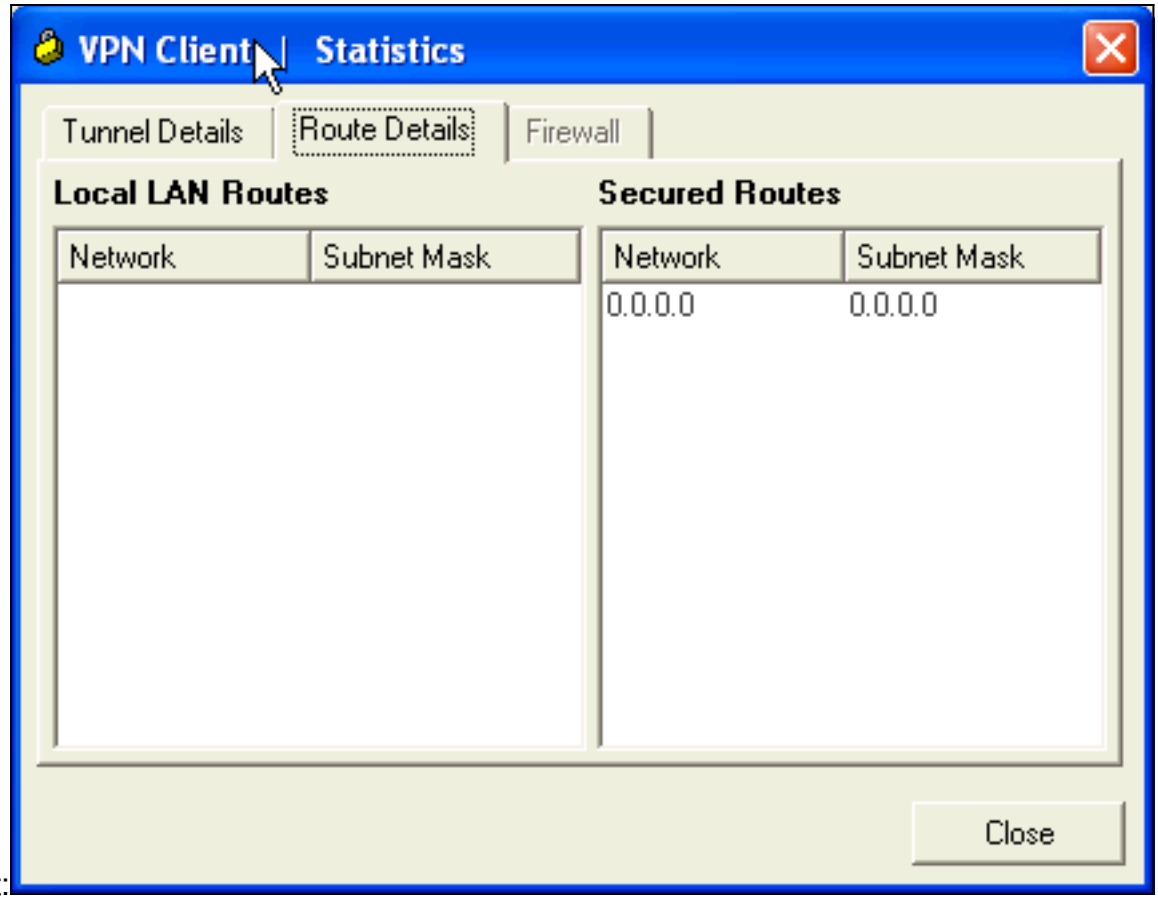


In diesem Fenster werden der Datenverkehr und die Verschlüsselungsinformationen angezeigt:



In diesem Fenster werden Split-Tunneling-Informationen

angezeigt:



ASA/PIX Security Appliance - Befehle anzeigen

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
ASA#show crypto isakmp sa

      Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.10.10.1
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
```

- **show crypto ipsec sa** - Zeigt alle aktuellen IPsec-SAs in einem Peer an.

```
ASA#show crypto ipsec sa
interface: Outside
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
.10.2

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
      current_peer: 10.10.10.1, username: cisco123
      dynamic allocated peer ip: 192.168.1.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
      #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C

    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
```

- ```
  ciscoasa(config)#debug icmp trace
  !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
  translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
  2
  !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
  untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
  len=32
  ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
  2
  ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
  ```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

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**.

Weitere Informationen zur Fehlerbehebung bei Site-Site-VPNs finden Sie unter Häufigste L2L- und Remote Access IPSec VPN-Problemlösung.

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Fehlerbehebung und Warnmeldungen
- Technischer Support und Dokumentation - Cisco Systems
  ```