SDM: Konfigurationsbeispiel für ein standortübergreifendes IPsec-VPN zwischen ASA/PIX und einem IOS-Router

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für den LAN-to-LAN (Site-to-Site) IPsec-Tunnel zwischen Cisco Security Appliances (ASA/PIX) und einem Cisco IOS-Router. Zur Vereinfachung werden statische Routen verwendet.

Weitere Informationen zum Szenario, in dem die PIX/ASA Security Appliance die Softwareversion *7.x* ausführt, finden Sie unter PIX/ASA 7.x Security Appliance für einen IOS-Router, LAN-zu-LAN-IPsec-Tunnel, in Konfigurationsbeispiel.

Voraussetzungen

Anforderungen

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

- Vor Beginn dieser Konfiguration muss eine End-to-End-IP-Verbindung eingerichtet werden.
- Die Security Appliance-Lizenz muss für die DES-Verschlüsselung (Data Encryption Standard) aktiviert werden (mindestens auf Verschlüsselungsebene).

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance (ASA) ab Version 8.x
- ASDM ab Version 6.x
- Cisco 1812-Router mit Cisco IOS® Softwareversion 12.3
- Cisco Security Device Manager (SDM) Version 2.5

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Hinweis: Informationen zur Konfiguration des Routers mithilfe von SDM finden Sie unter Basic Router Configuration (Basiskonfiguration des Routers).

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.

Hinweis: Weitere Informationen finden Sie unter Configuration Professional: Site-to-Site-IPsec-VPN zwischen ASA/PIX und einem IOS-Router - Konfigurationsbeispiel für eine ähnliche Konfiguration mit Cisco Configuration Professional auf dem Router.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie PIX 500 verwendet werden, die Version 7.x und höher ausführt.

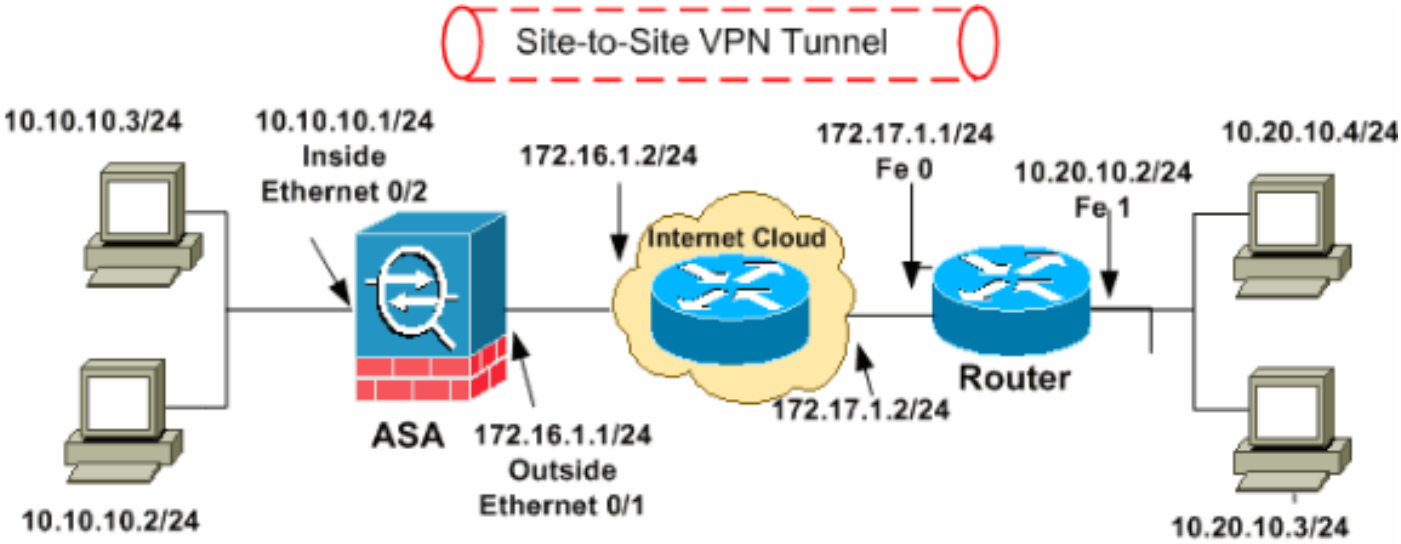
Konventionen

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

Konfiguration

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



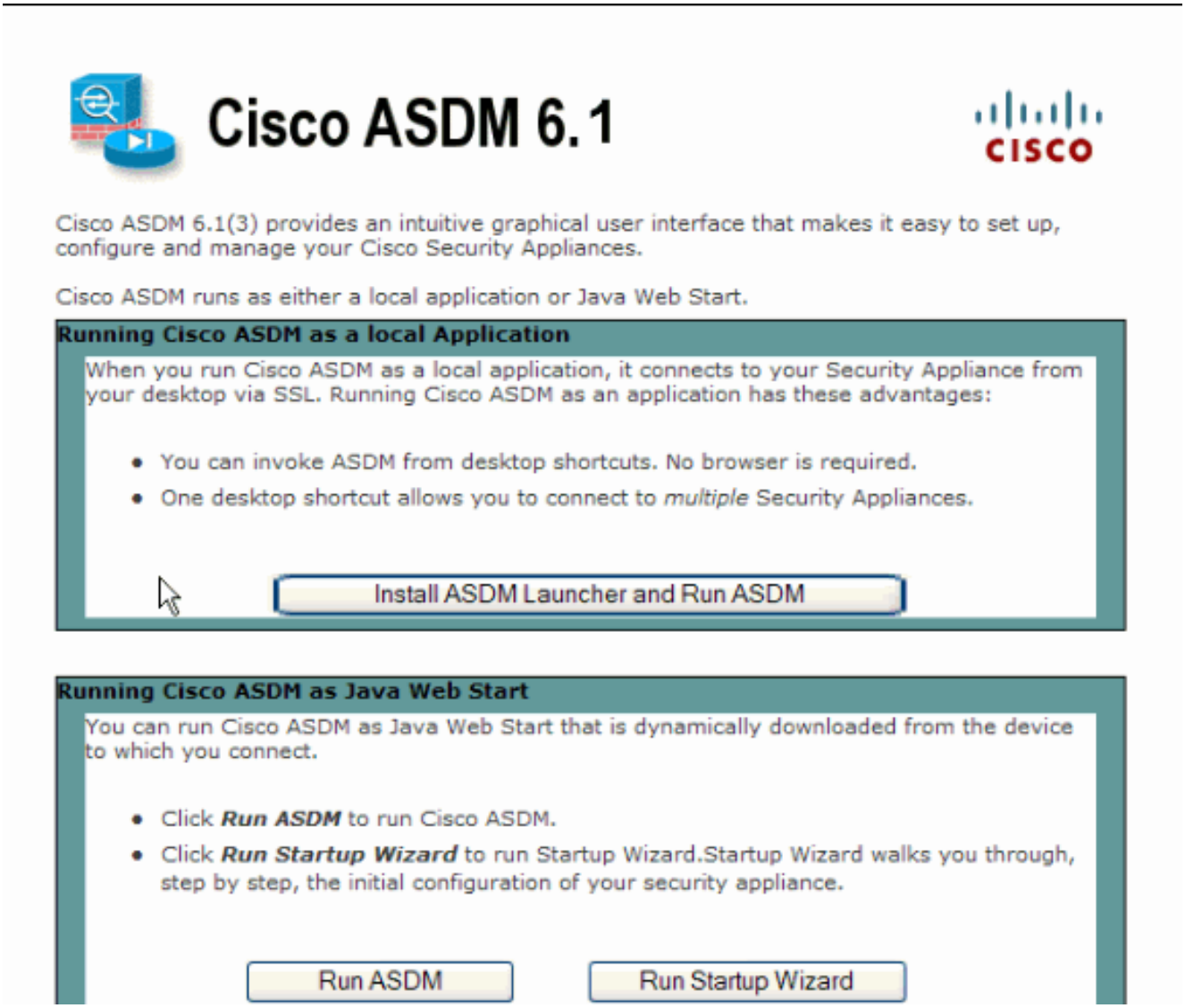
Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

- ASDM-Konfiguration für VPN-Tunnel
- Router-SDM-Konfiguration
- ASA CLI-Konfiguration
- Router-CLI-Konfiguration

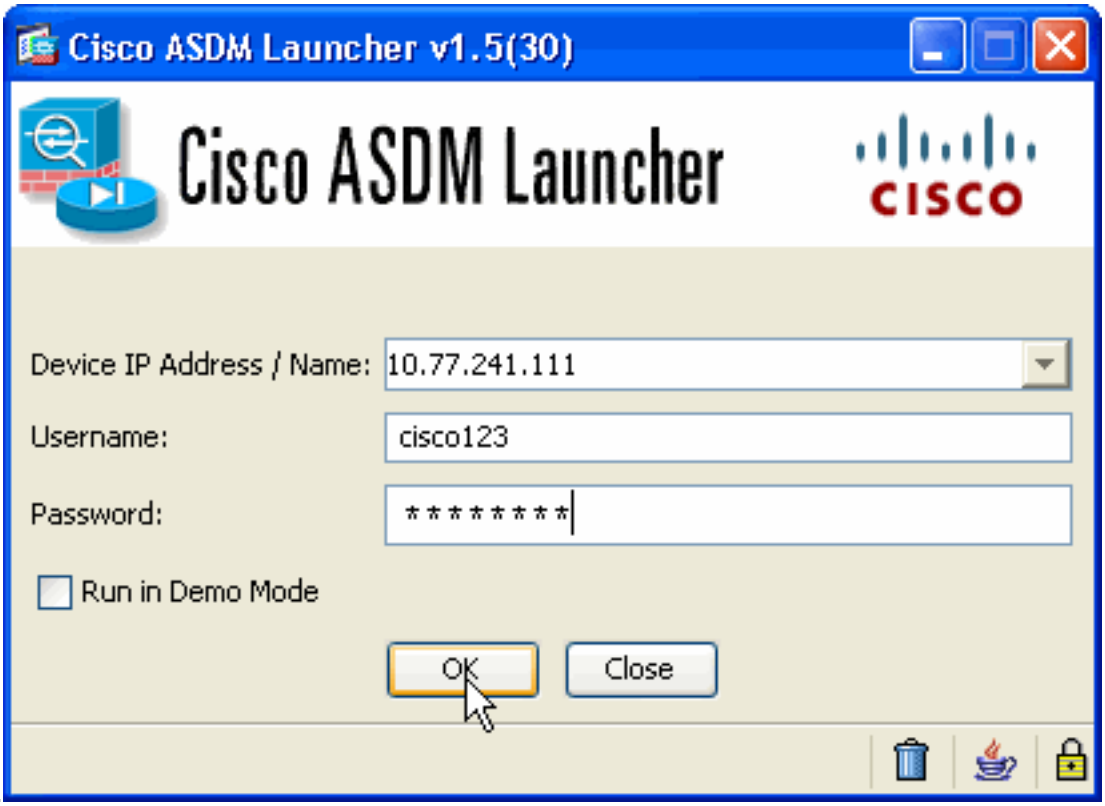
ASDM-Konfiguration für VPN-Tunnel

Gehen Sie wie folgt vor, um den VPN-Tunnel zu erstellen:

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.

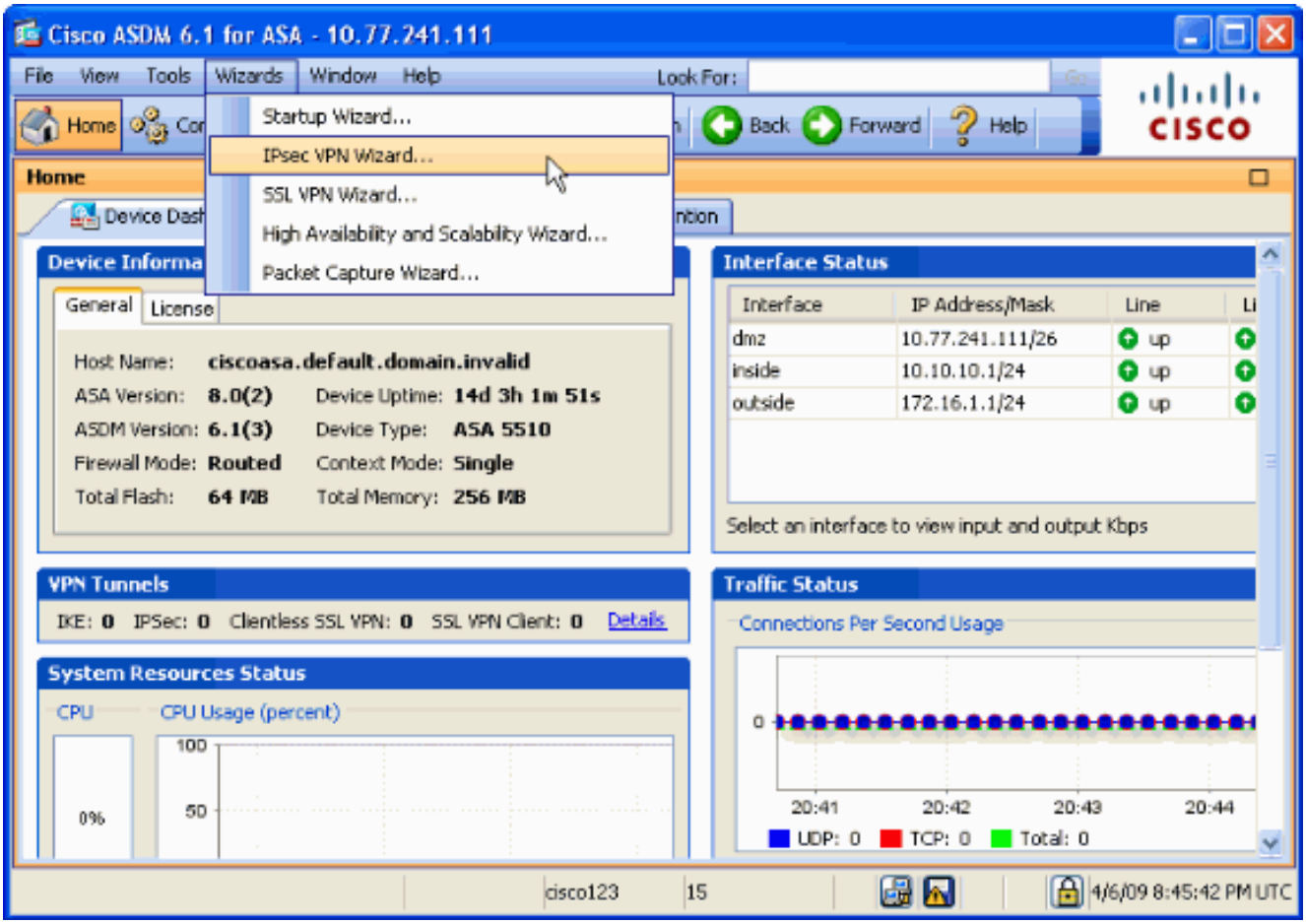


2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software und Ausführung des Cisco ASDM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

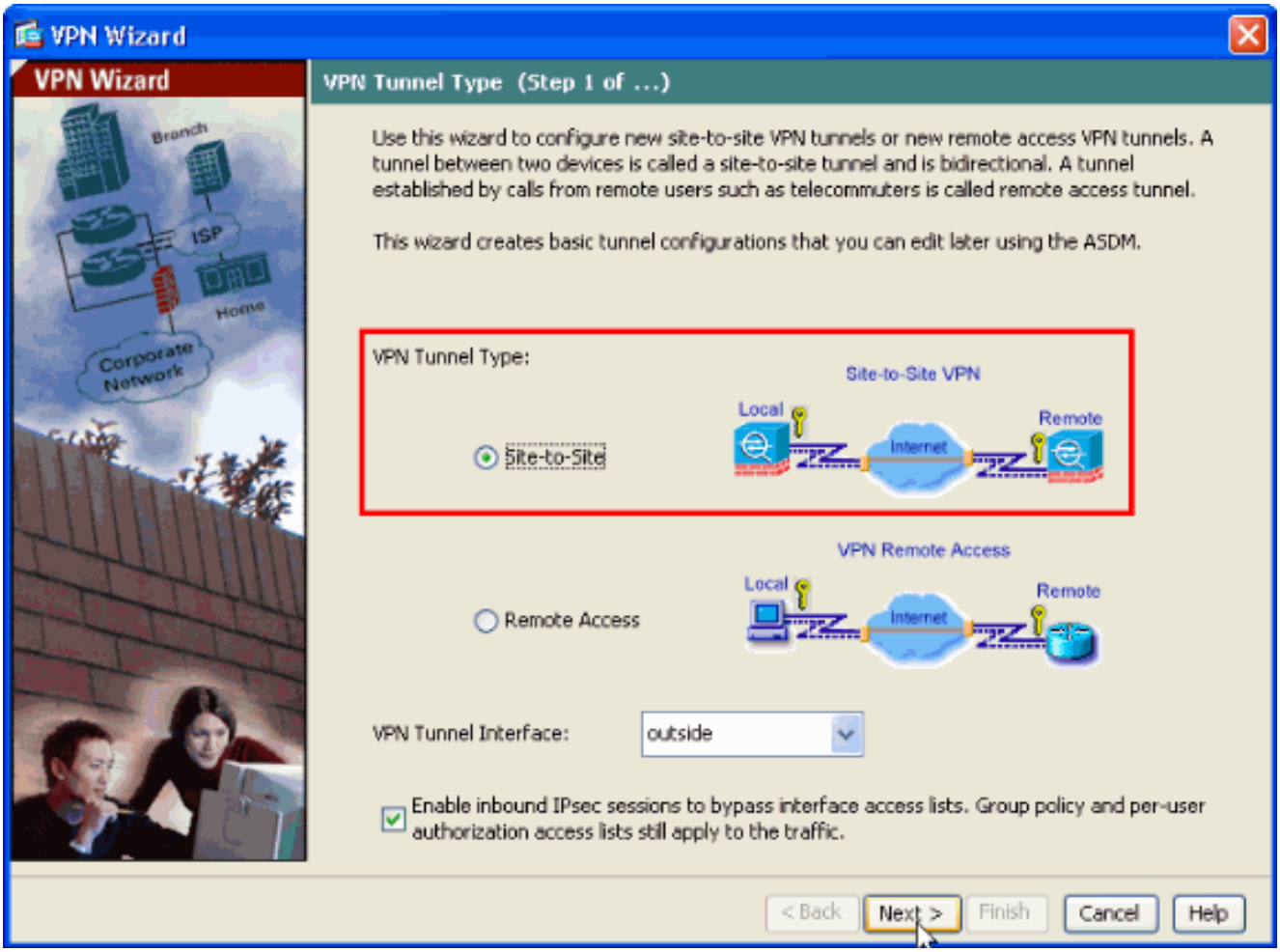


verwendet.

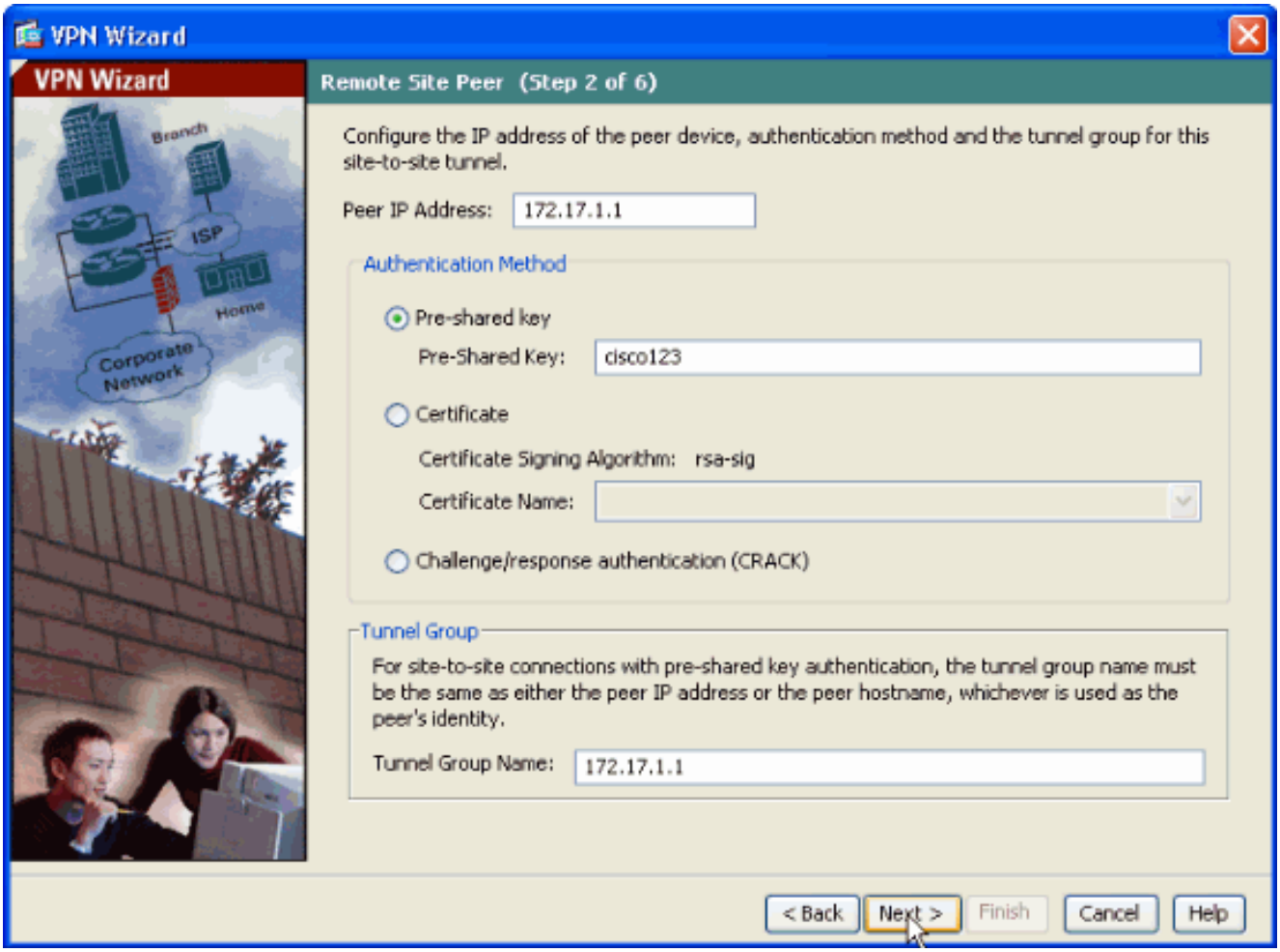
5. Führen Sie den **IPsec VPN Wizard** aus, sobald die ASDM-Anwendung eine Verbindung mit der ASA
herstellt.



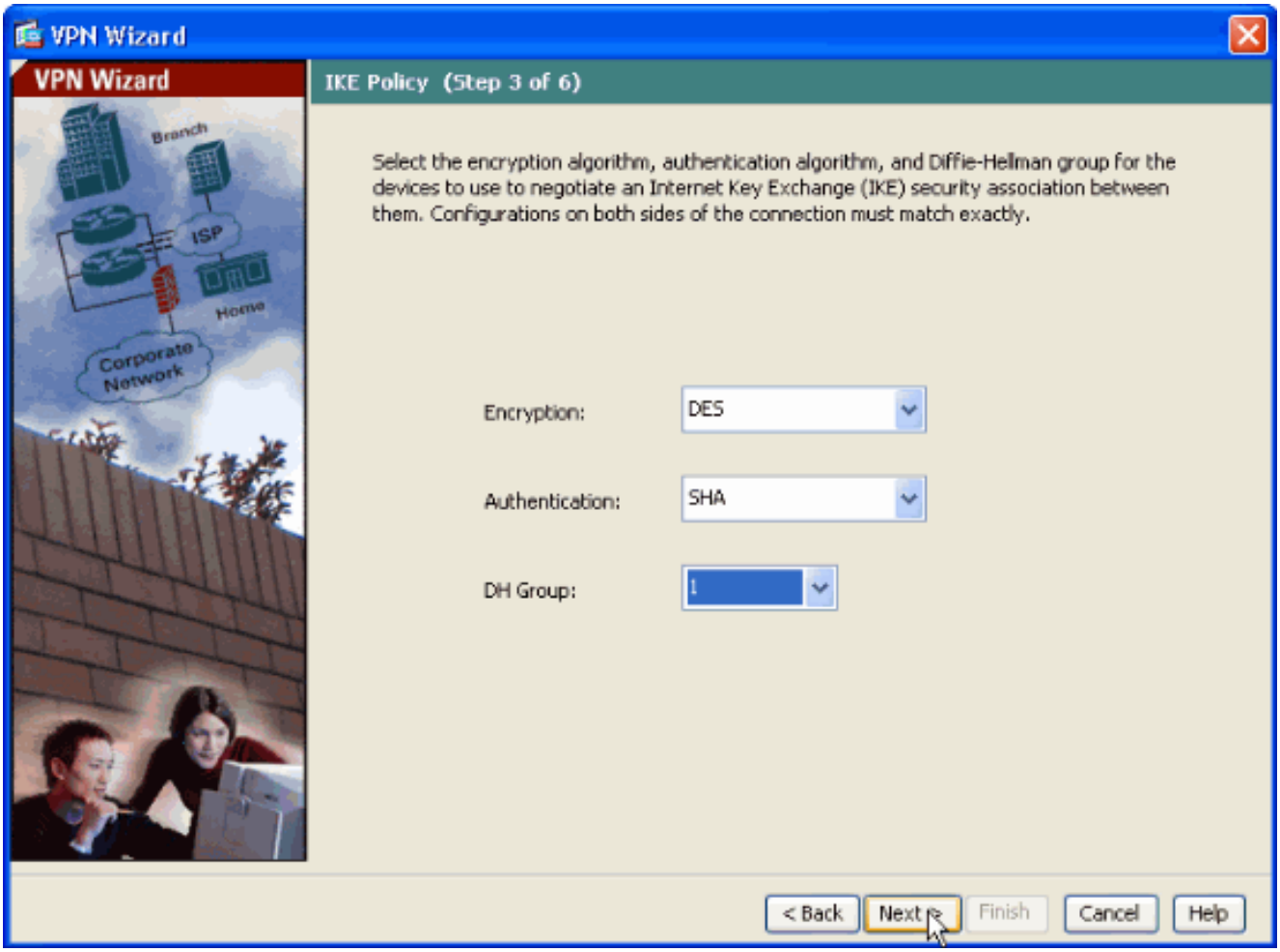
6. Wählen Sie den **Site-to-Site-**IPsec VPN-Tunneltyp aus, und klicken Sie auf **Weiter**, wie hier gezeigt.



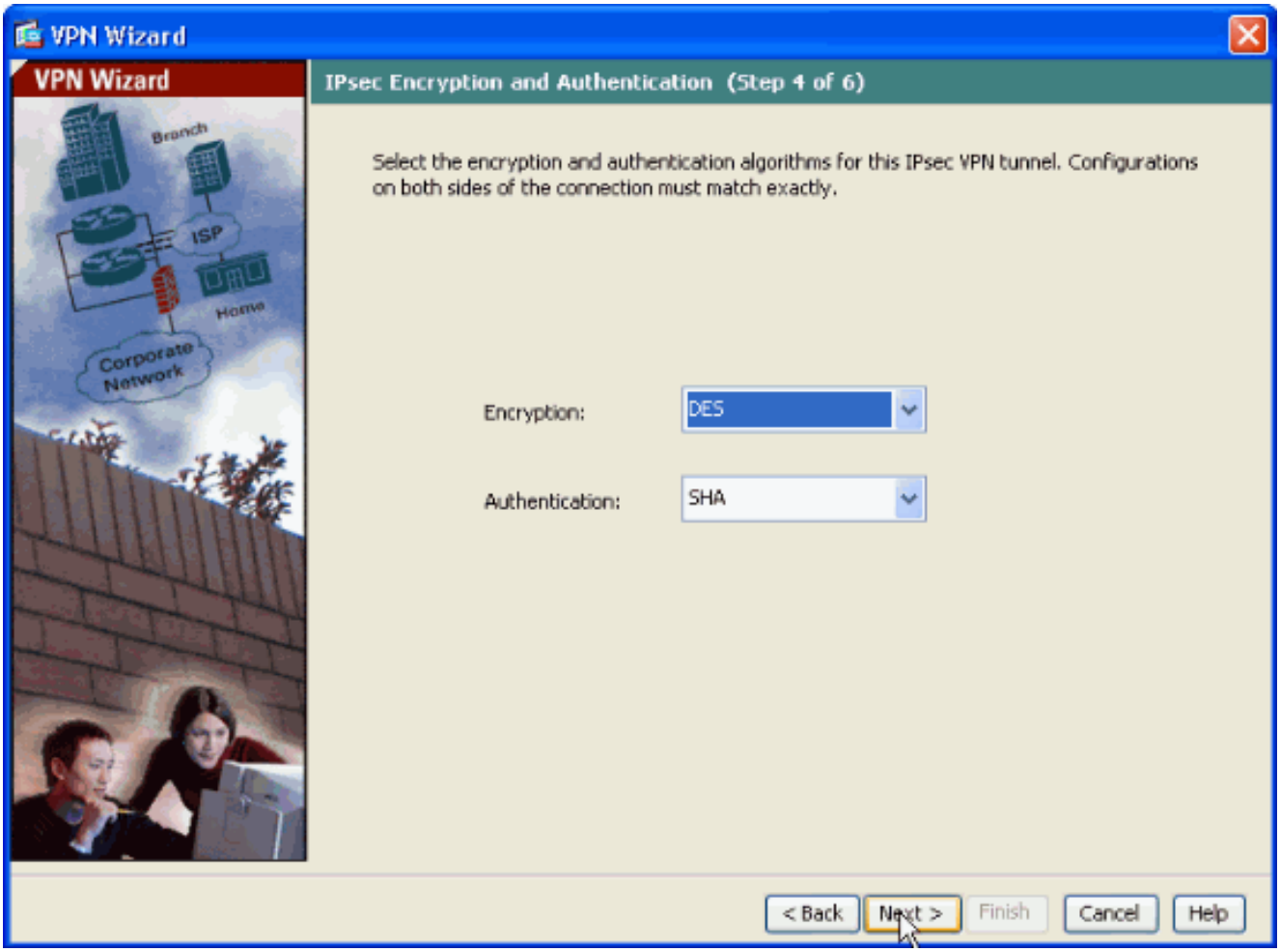
7. Geben Sie die externe IP-Adresse des Remote-Peers an. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den vorinstallierten Schlüssel in diesem Beispiel. Der in diesem Beispiel verwendete vorinstallierte Schlüssel ist **cisco123**. Der **Tunnelgruppenname** ist standardmäßig Ihre externe IP-Adresse, wenn Sie L2L VPN konfigurieren. Klicken Sie auf **Weiter**.



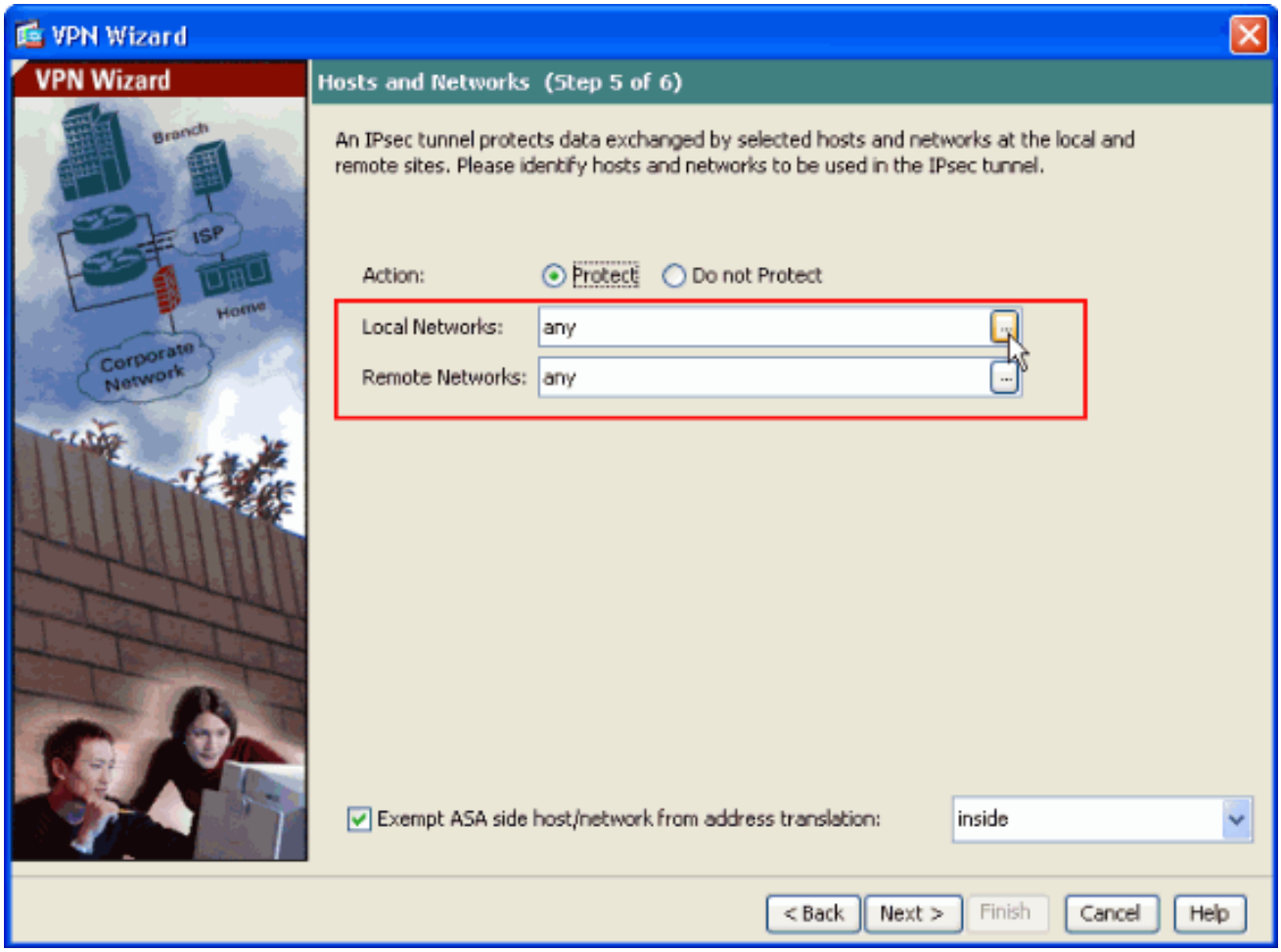
8. Geben Sie die Attribute für IKE an, die auch als Phase 1 bezeichnet werden. Diese Attribute müssen auf dem ASA-Router und dem IOS-Router identisch sein. Klicken Sie auf **Weiter**.



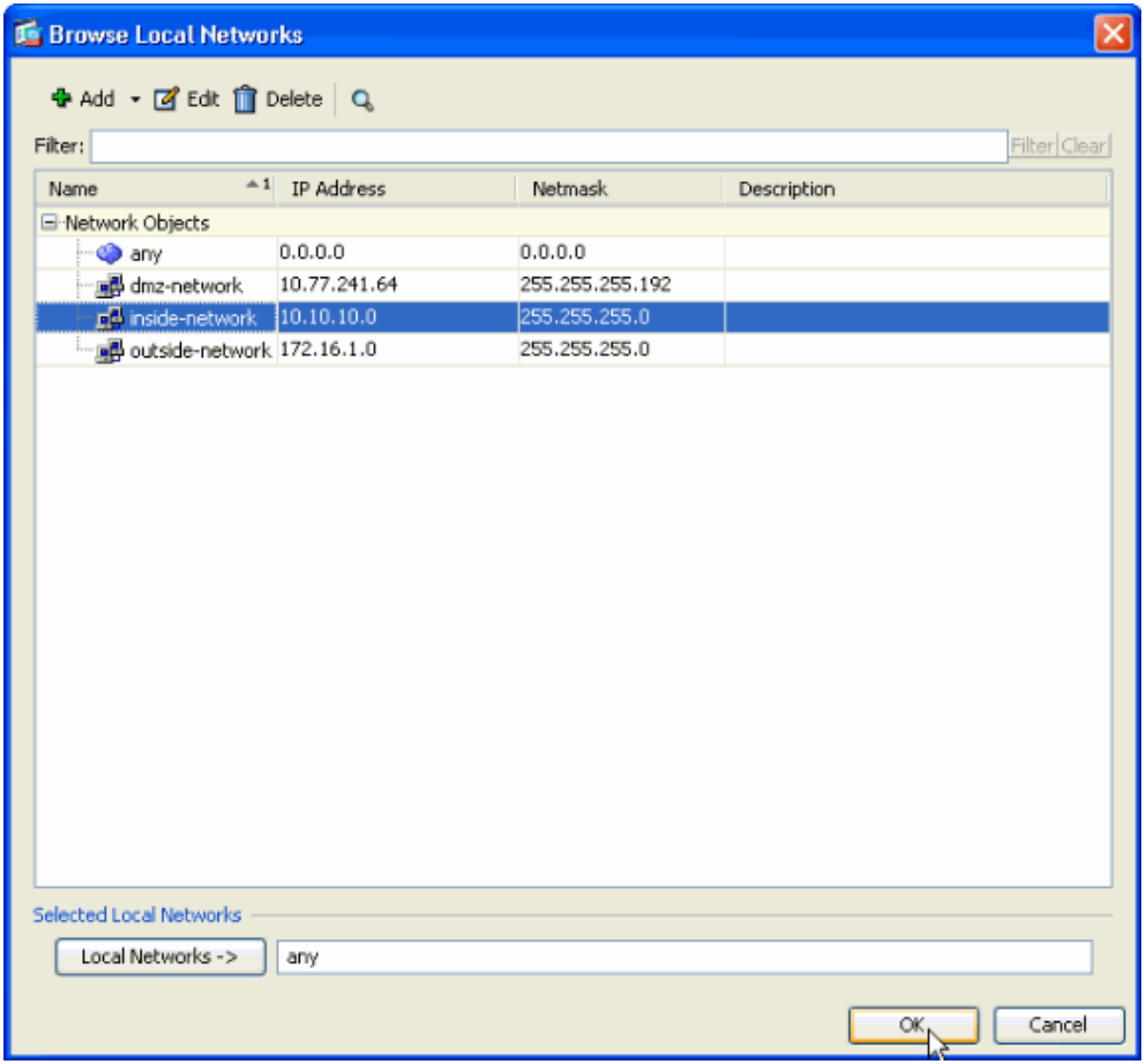
9. Geben Sie die Attribute an, die für IPsec verwendet werden sollen, auch als Phase 2 bezeichnet. Diese Attribute müssen auf dem ASA- und dem IOS-Router übereinstimmen. Klicken Sie auf
Weiter.



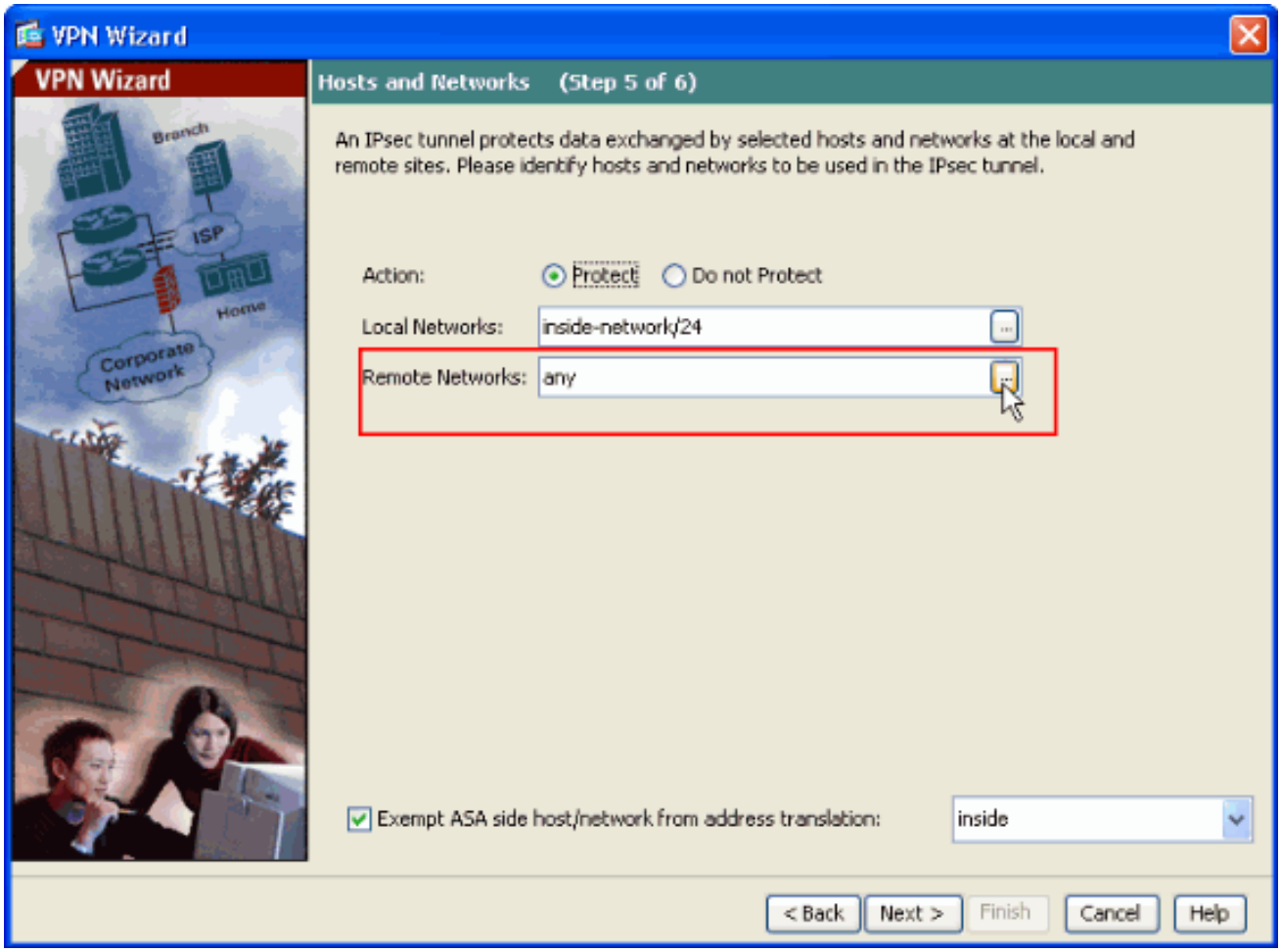
10. Geben Sie die Hosts an, deren Datenverkehr den VPN-Tunnel passieren darf. In diesem Schritt müssen Sie die **lokalen** und **Remote-Netzwerke** für den VPN-Tunnel bereitstellen. Klicken Sie auf die Schaltfläche neben **Lokale Netzwerke** wie hier gezeigt, um die lokale Netzwerkadresse aus der Dropdown-Liste auszuwählen.



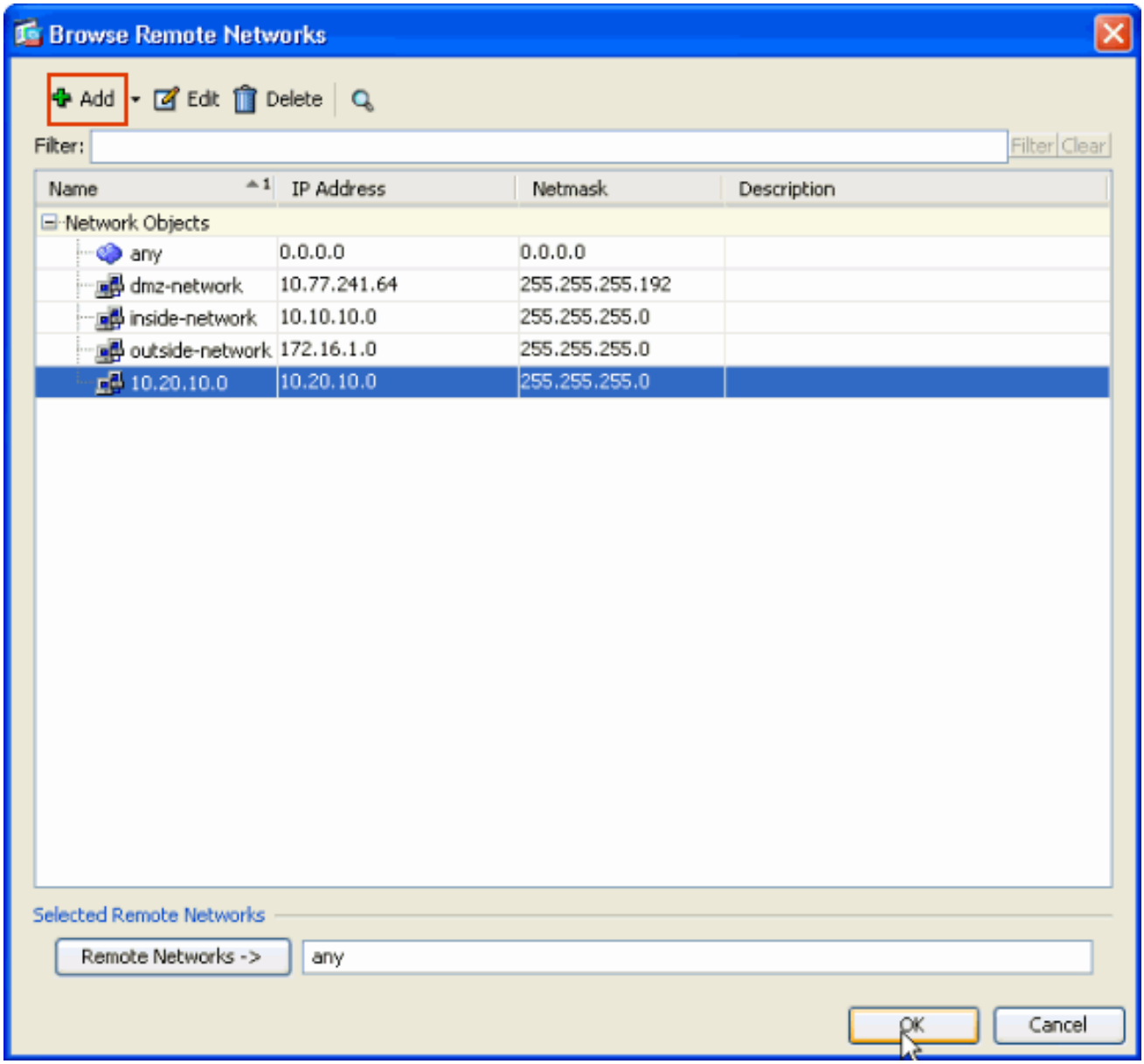
11. Wählen Sie die Adresse des **lokalen Netzwerks aus**, und klicken Sie dann auf **OK**, wie hier gezeigt.



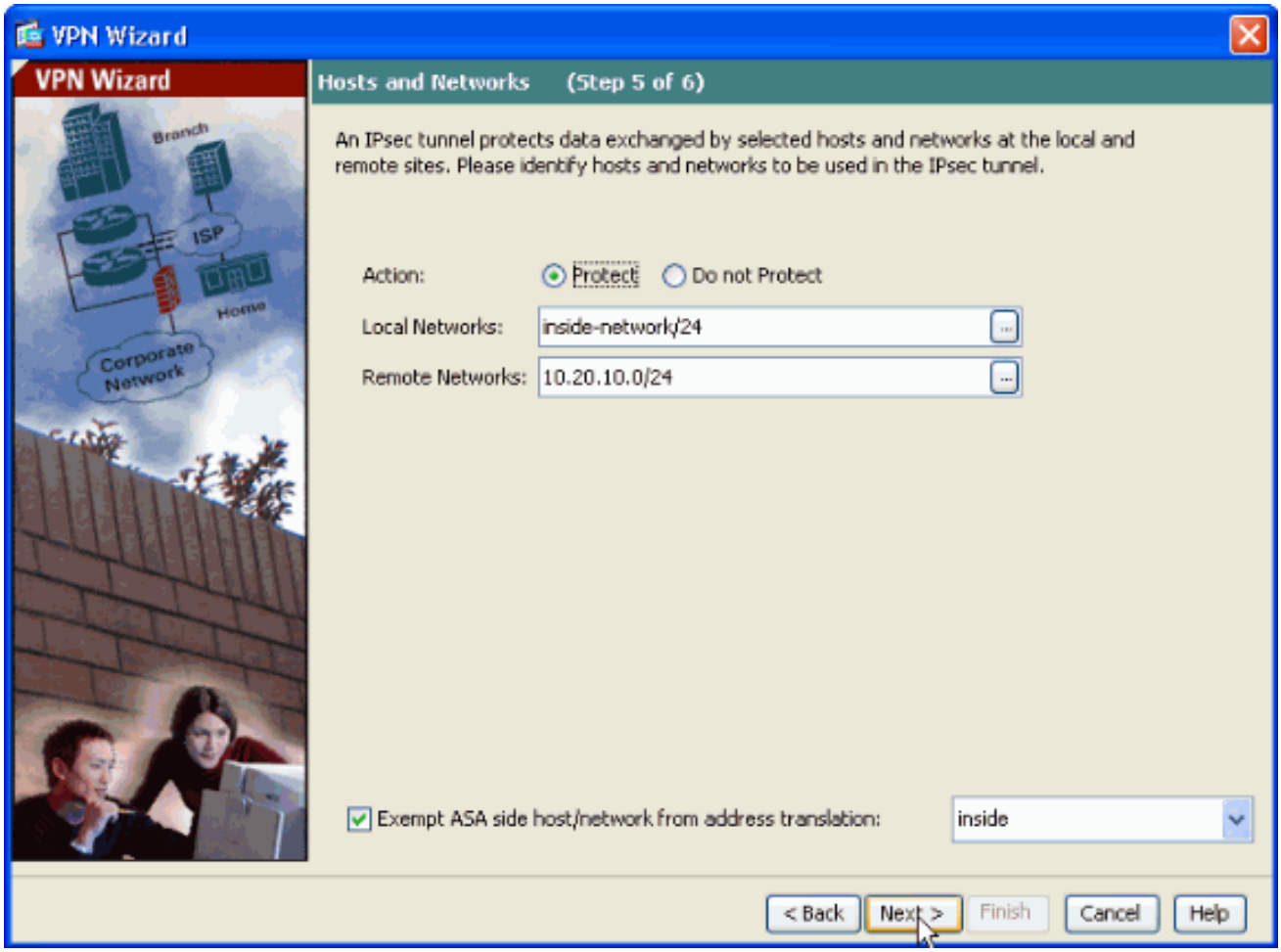
12. Klicken Sie auf die Schaltfläche neben **Remote Networks (Remote-Netzwerke)** wie hier gezeigt, um die Remote-Netzwerkadresse aus der Dropdown-Liste auszuwählen.



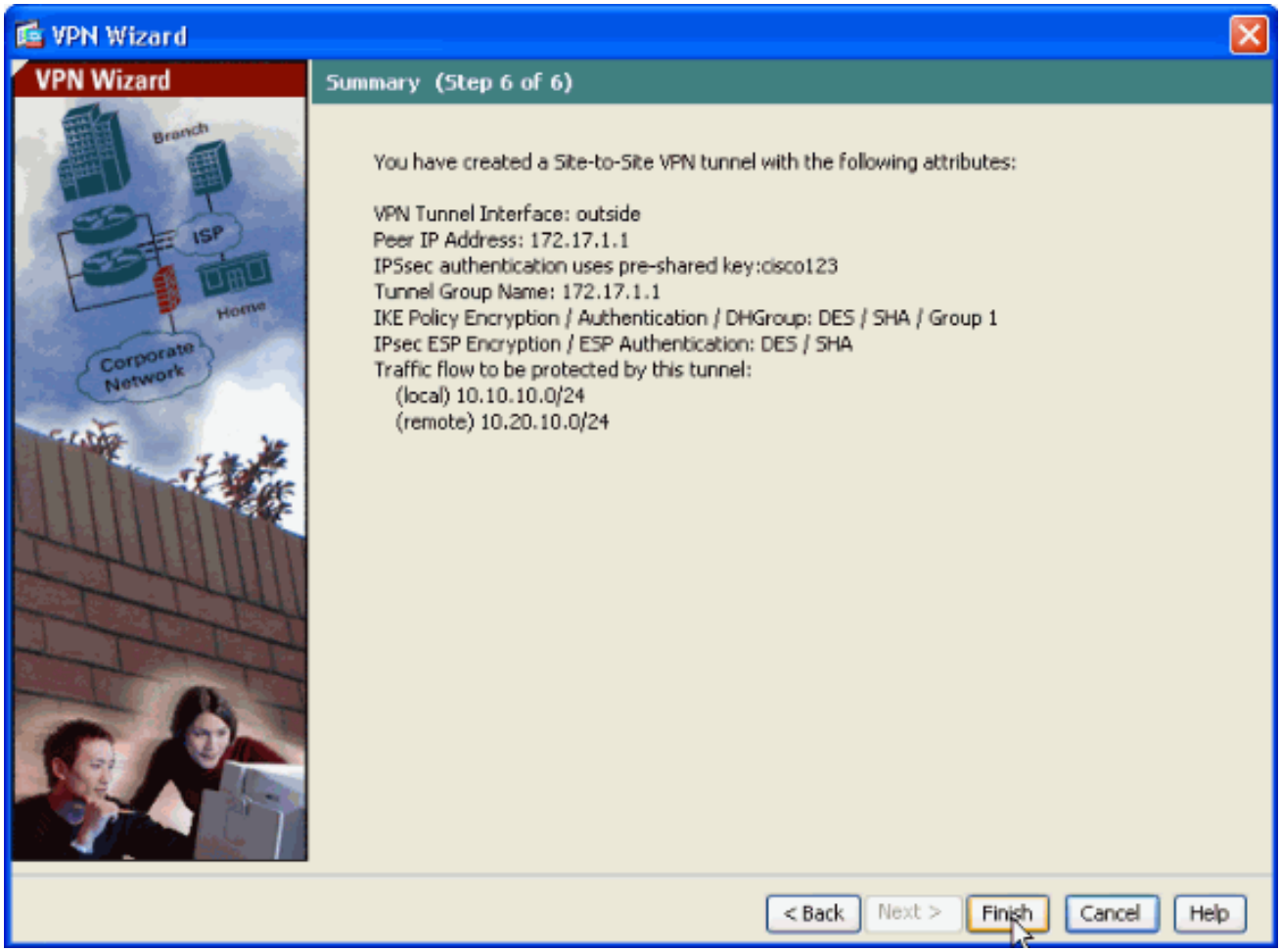
13. Wählen Sie die **Remote Network**-Adresse aus, und klicken Sie dann auf **OK**, wie hier gezeigt.**Hinweis:** Wenn das Remote-Netzwerk nicht in der Liste enthalten ist, muss das Netzwerk der Liste durch Klicken auf **Hinzufügen** hinzugefügt werden.



14. Aktivieren Sie das Kontrollkästchen **ASA-seitigen Host/Netzwerk von Adressenumwandlung ausnehmen**, um zu verhindern, dass der Tunnelverkehr **Network Address Translation** durchläuft. Klicken Sie anschließend auf **Weiter**.



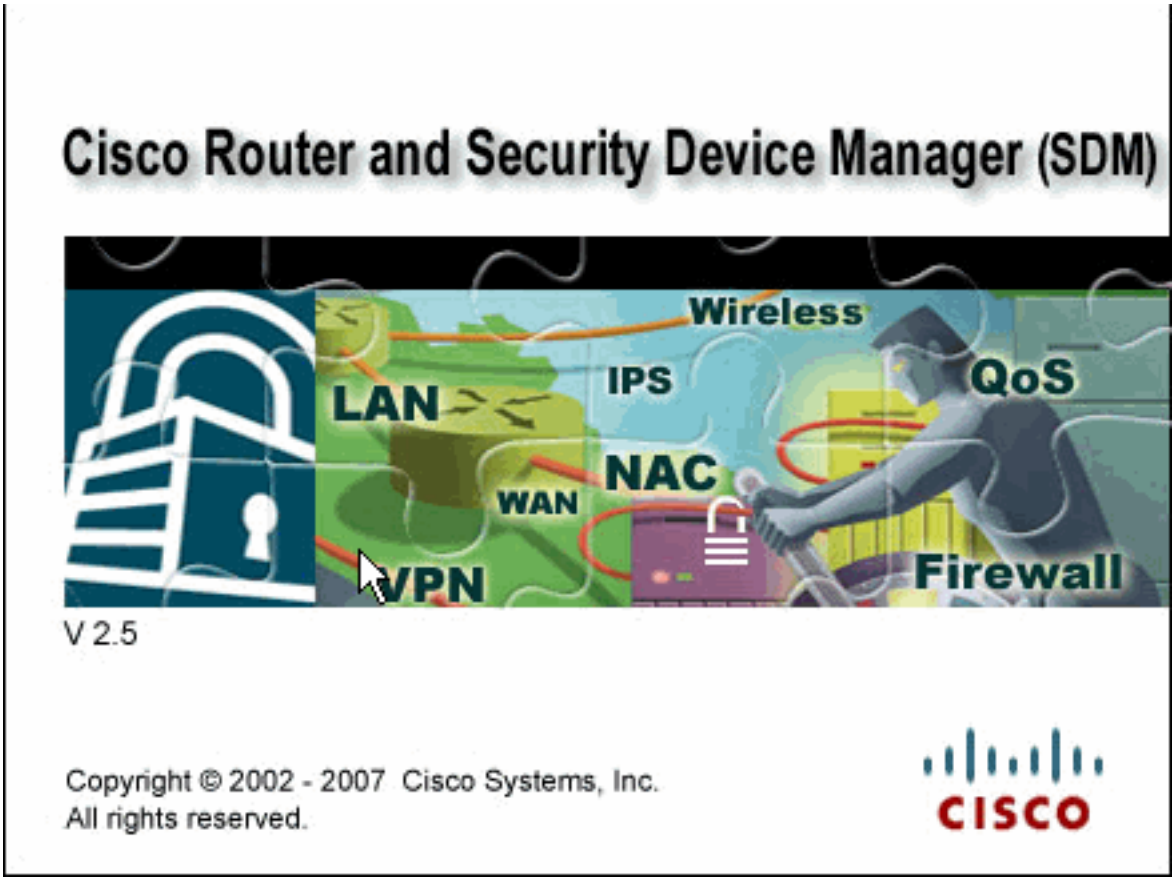
15. Die vom VPN-Assistenten definierten Attribute werden in dieser Zusammenfassung angezeigt. Überprüfen Sie die Konfiguration erneut, und klicken Sie auf **Fertig stellen**, wenn die Einstellungen korrekt
sind.



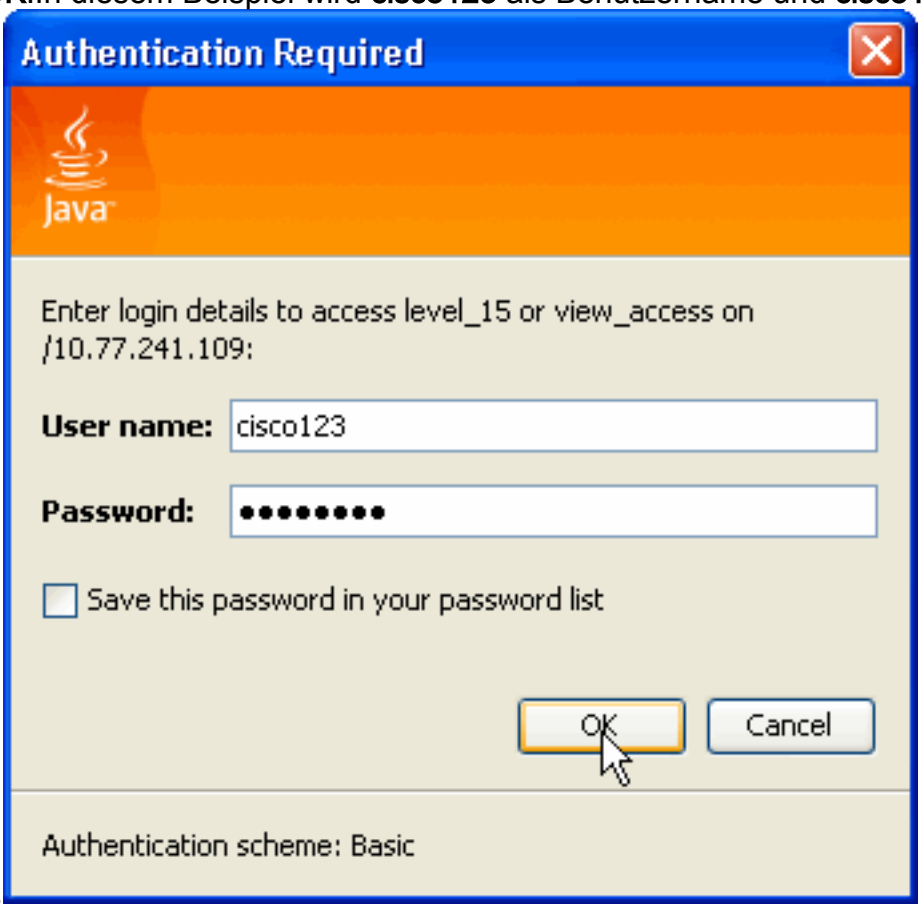
Router-SDM-Konfiguration

Gehen Sie wie folgt vor, um den Site-to-Site-VPN-Tunnel auf dem Cisco IOS-Router zu konfigurieren:

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

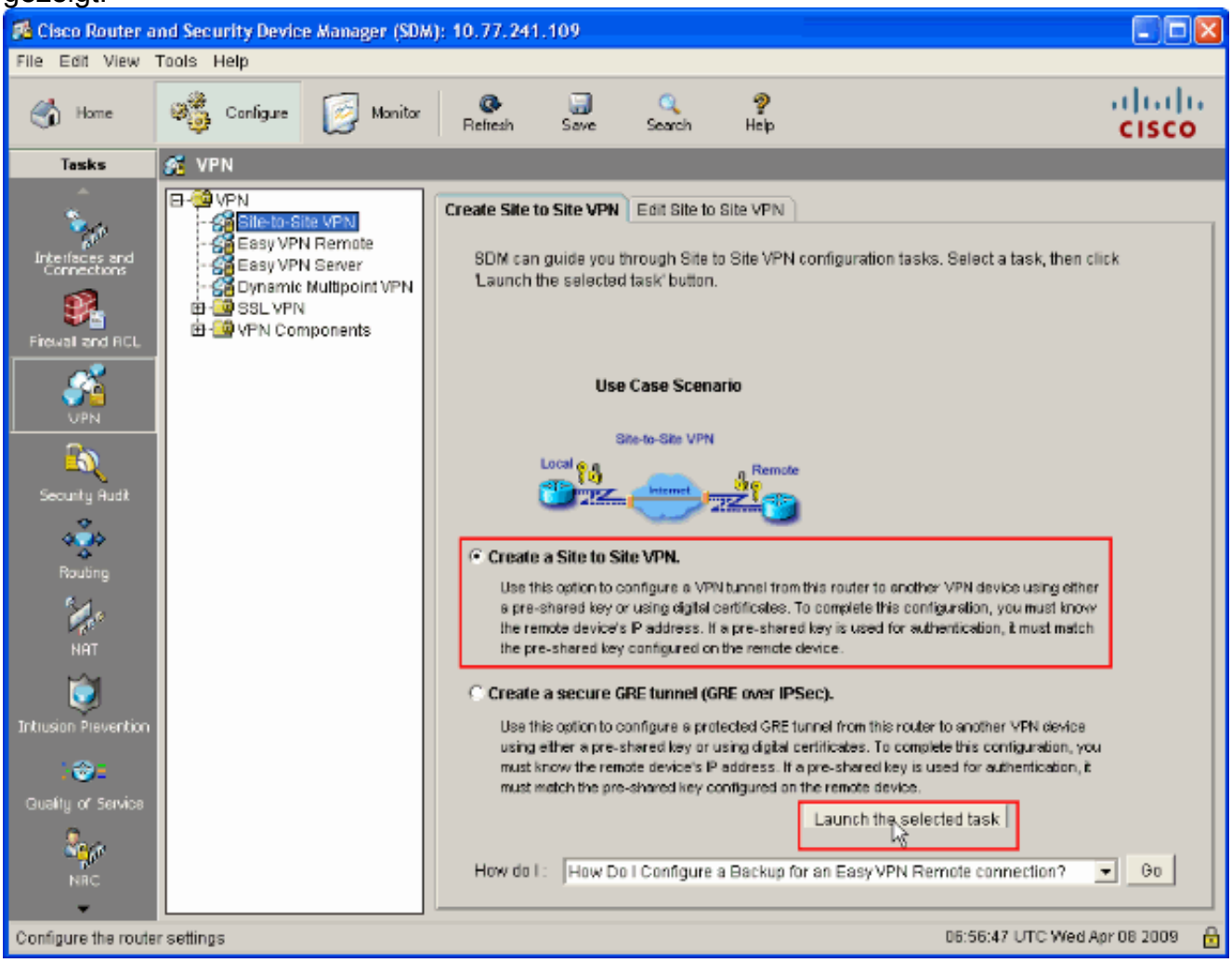


2. Der SDM-Download beginnt jetzt. Wenn der SDM-Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen angewiesen werden, um die Software zu installieren und den Cisco SDM Launcher auszuführen.
3. Geben Sie den **Benutzernamen** und das **Passwort ein**, wenn Sie diesen eingegeben haben, und klicken Sie auf **OK**.In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als Kennwort verwendet.

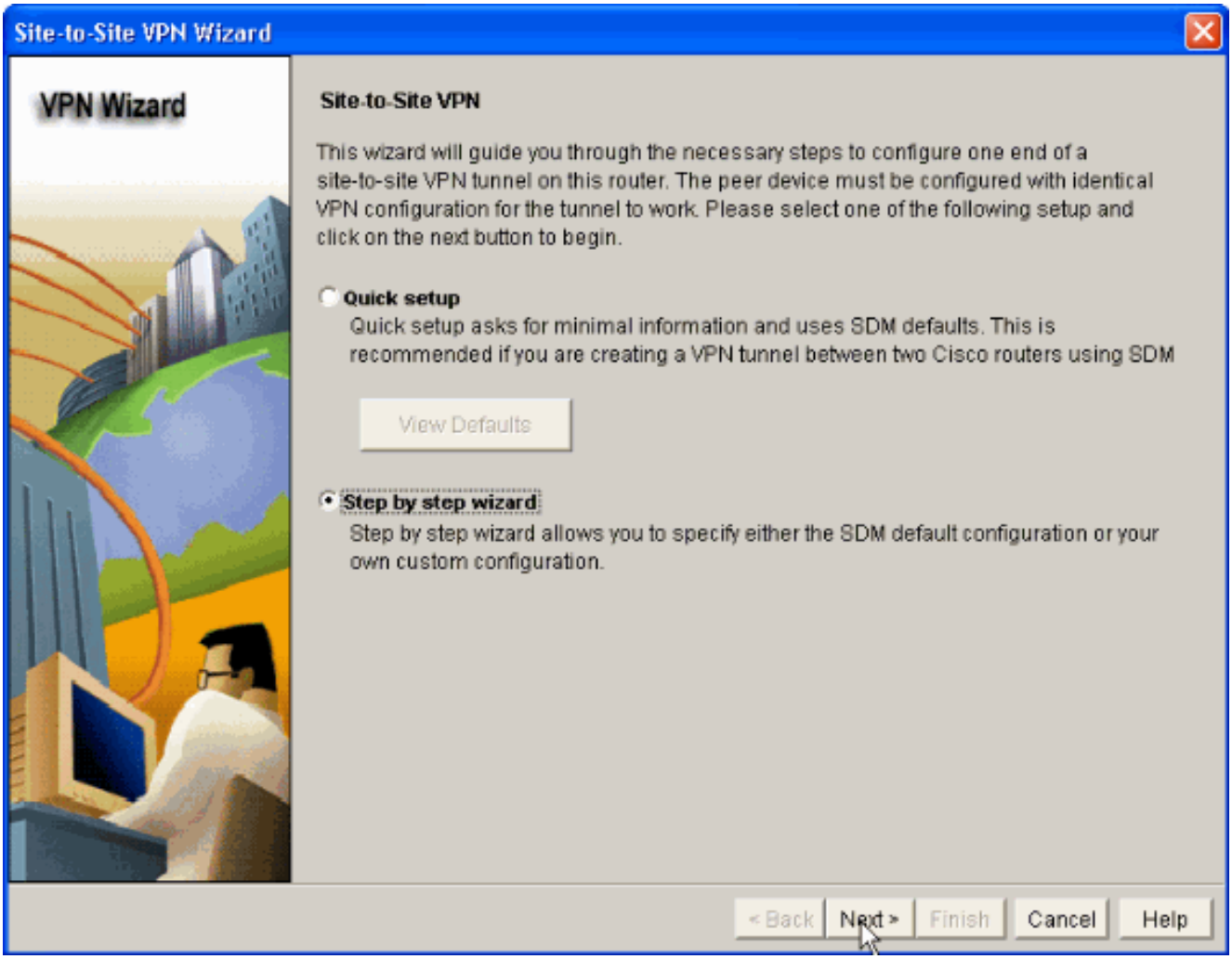


4. Wählen Sie **Konfiguration > VPN > Site-to-Site VPN**, und klicken Sie auf das Optionsfeld

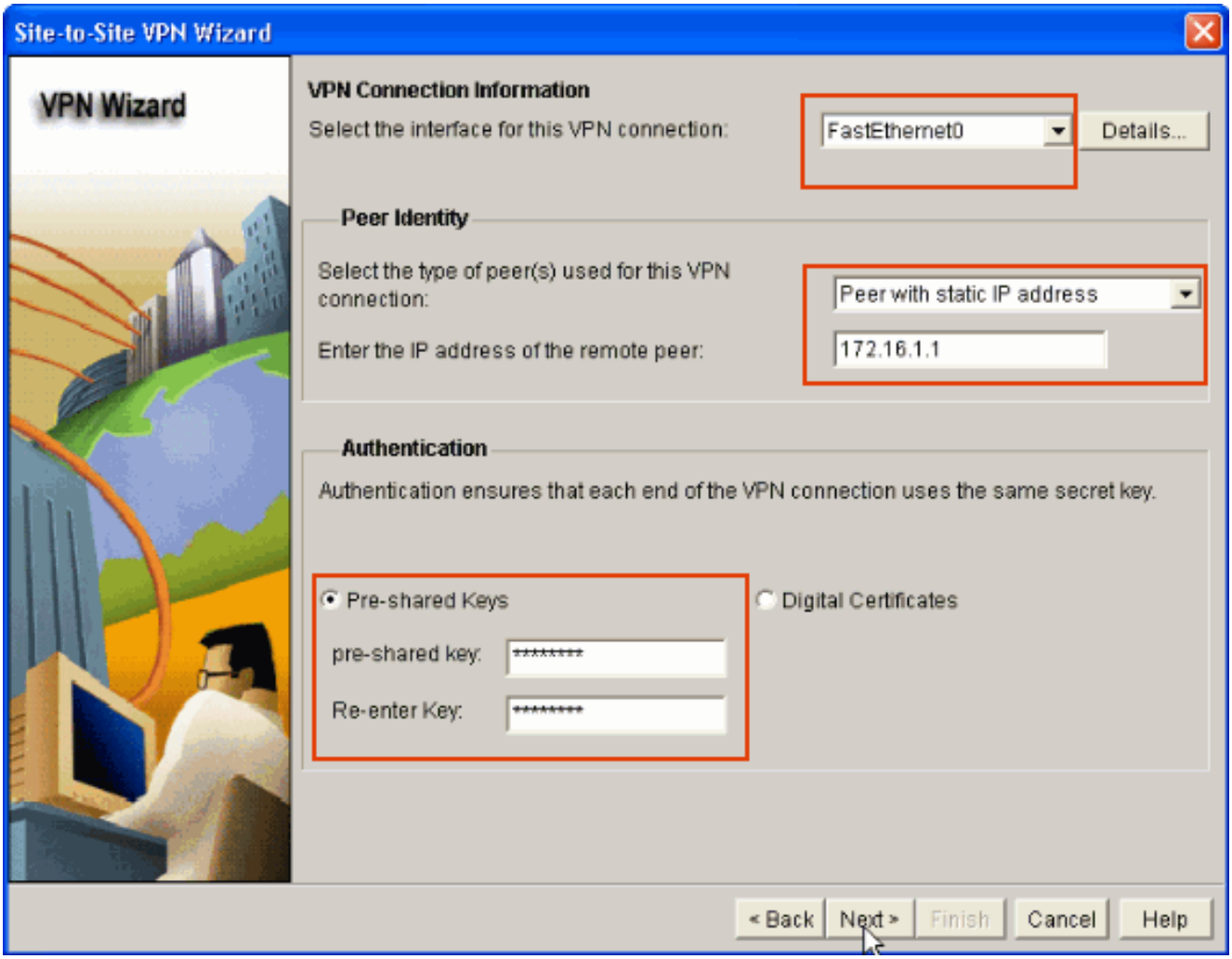
neben **Create a Site-to-Site VPN (Site-to-Site-VPN erstellen) auf** der SDM-Startseite. Klicken Sie anschließend auf **Ausgewählten Task starten**, wie hier gezeigt:



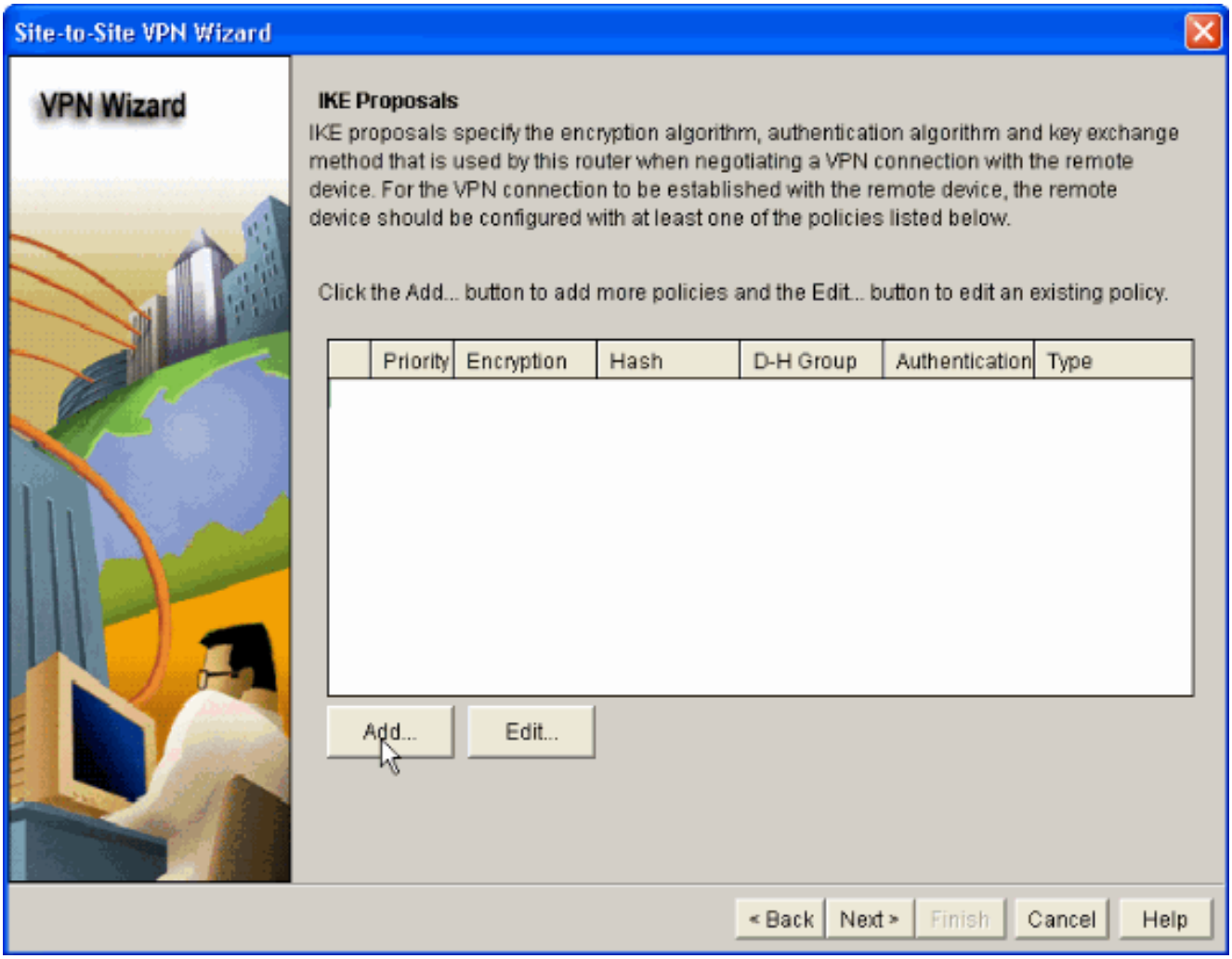
5. Wählen Sie **Schritt-für-Schritt-Assistent**, um mit der Konfiguration fortzufahren:



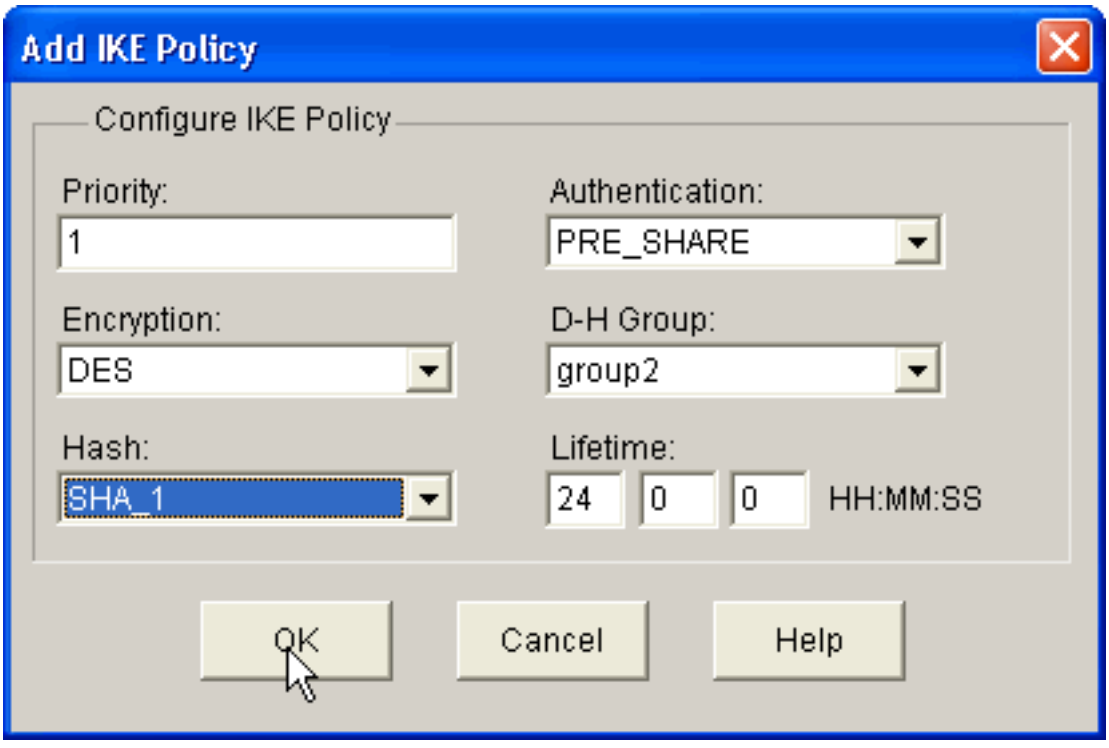
6. Geben Sie im nächsten Fenster die **VPN-Verbindungsinformationen** in den entsprechenden Räumen an. Wählen Sie die Schnittstelle des VPN-Tunnels aus der Dropdown-Liste aus. Hier wird **FastEthernet0** ausgewählt. Wählen Sie im Abschnitt **Peer Identity (Peer-Identität)** die Option **Peer with static IP address (Peer mit statischer IP-Adresse)** aus, und geben Sie die IP-Adresse des Remote-Peers an. Geben Sie dann den **Pre-shared Key** (**cisco123** in diesem Beispiel) im Authentifizierungsbereich wie gezeigt ein. Klicken Sie anschließend auf **Weiter**.



7. Klicken Sie auf **Hinzufügen**, um IKE-Vorschläge hinzuzufügen, die den **Verschlüsselungsalgorithmus, den Authentifizierungsalgorithmus** und die **Key Exchange-Methode**
angeben.

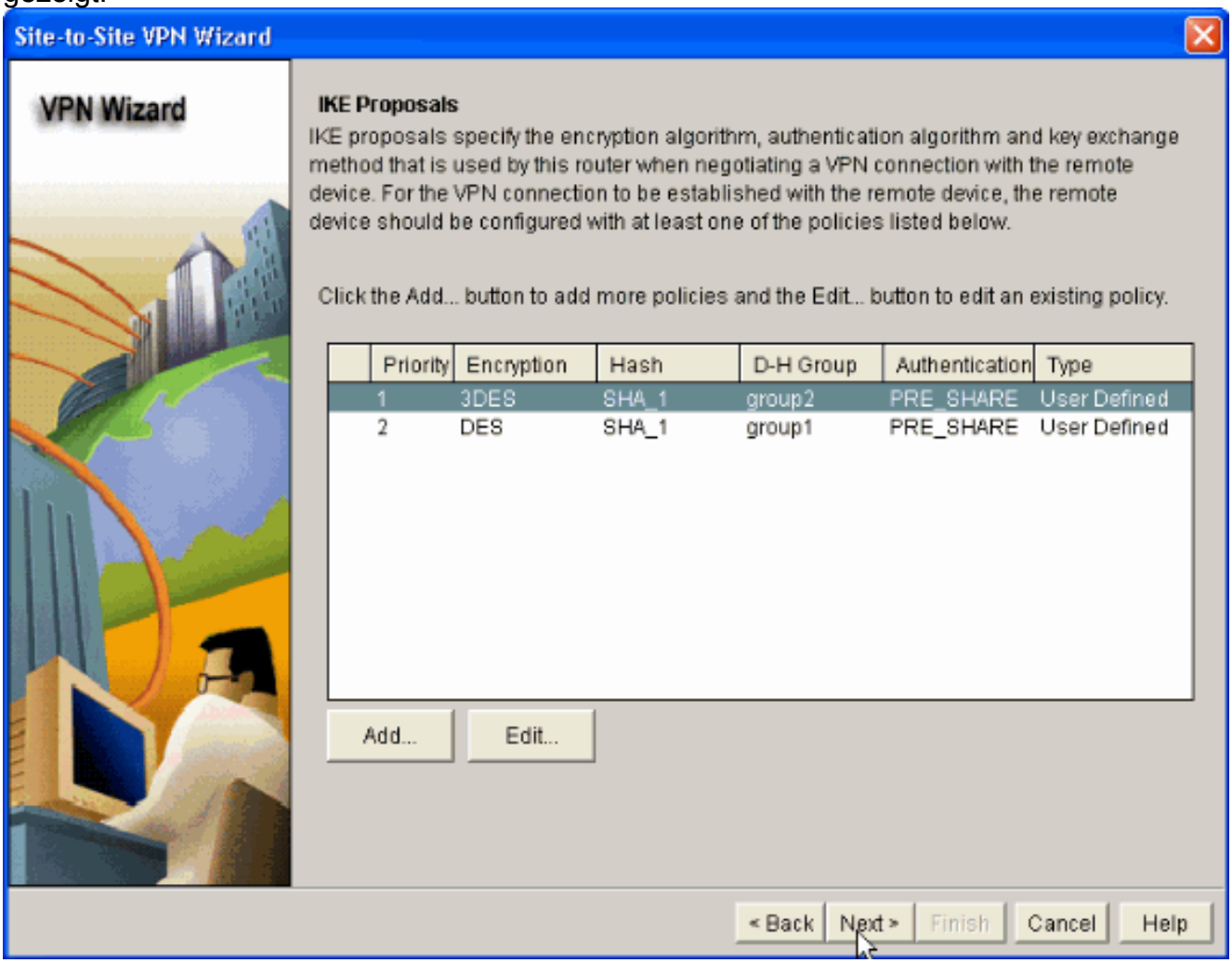


8. Stellen Sie **Verschlüsselungsalgorithmus**, **Authentifizierungsalgorithmus** und die **Exchange-Methode** wie hier gezeigt bereit, und klicken Sie dann auf **OK**. Die Werte **Encryption Algorithm**, **Authentication Algorithm** und **Key Exchange** sollten mit den in der ASA bereitgestellten Daten übereinstimmen.

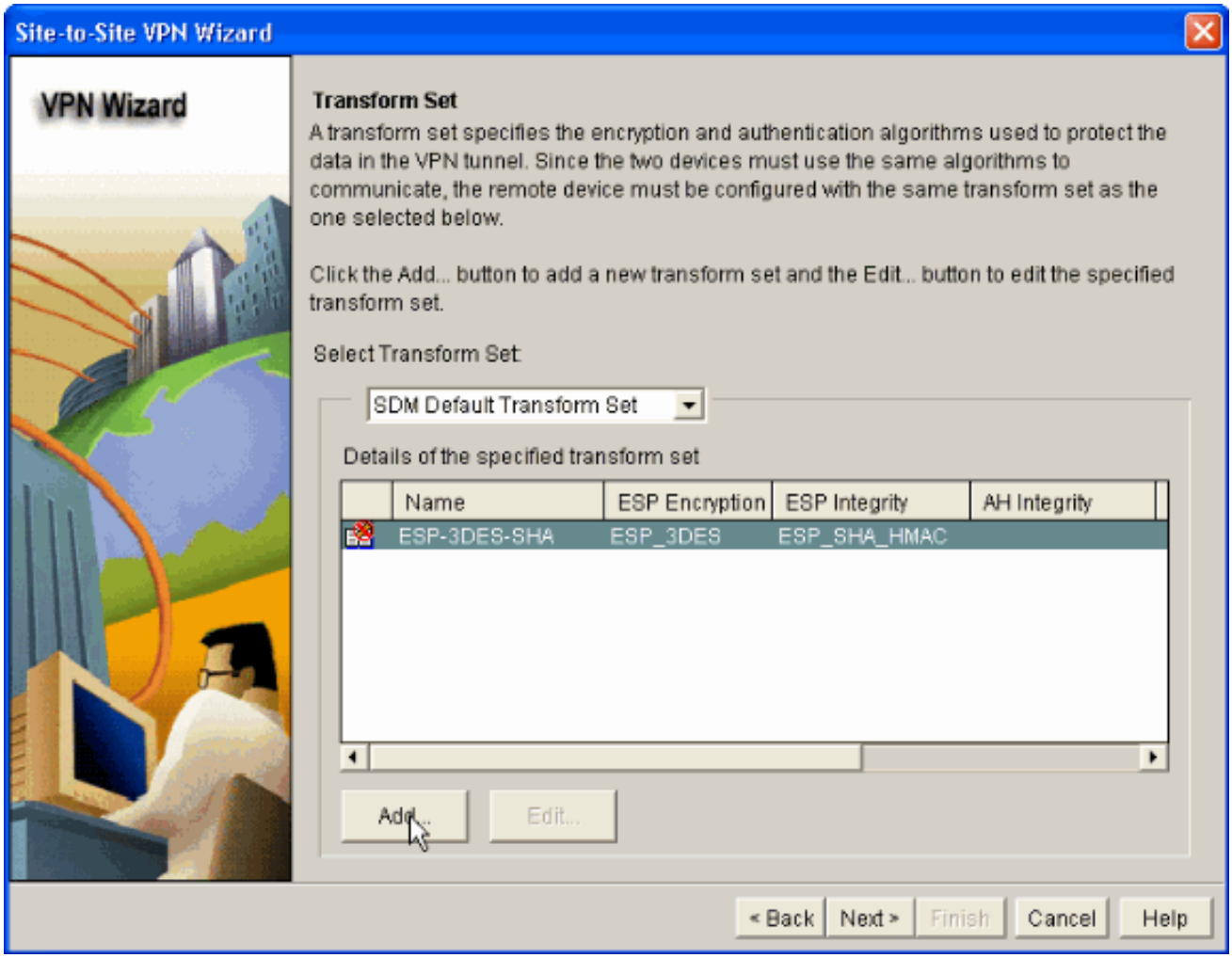


9. Klicken Sie auf **Weiter**, wie hier

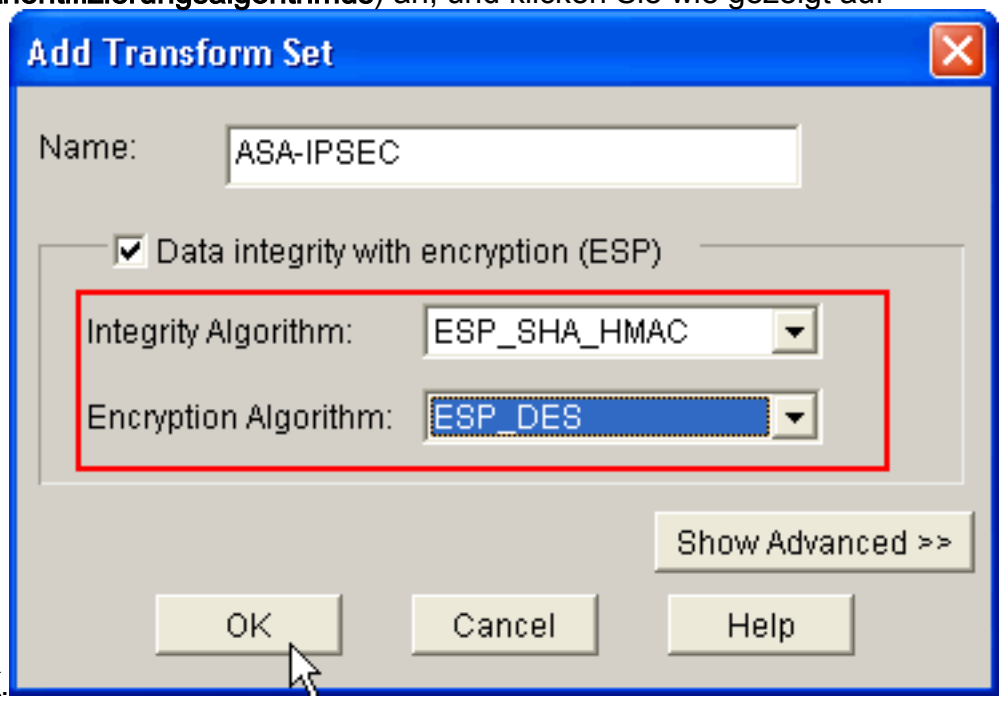
gezeigt.



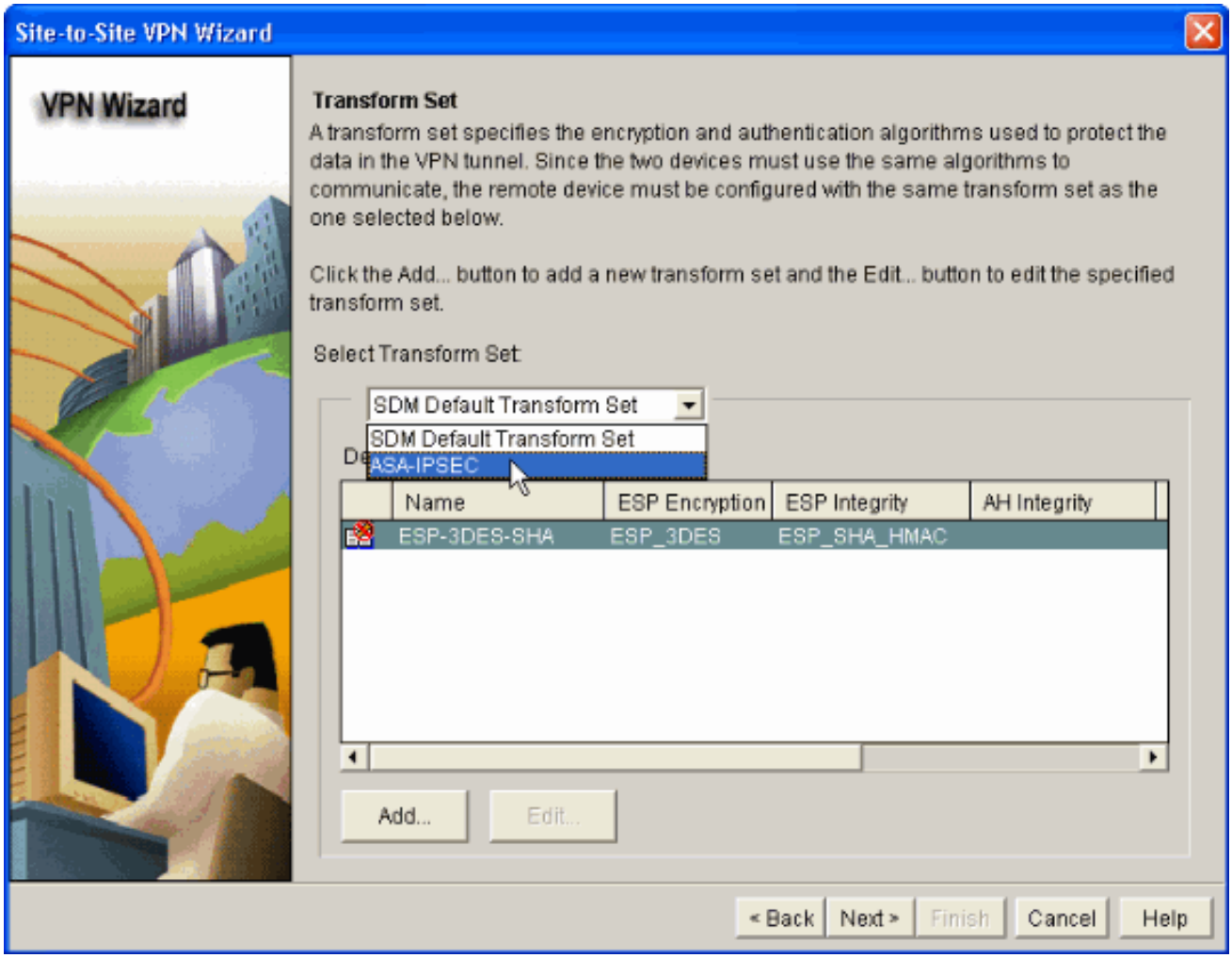
10. In diesem neuen Fenster sollten die Details zum **Konfigurationssatz** angegeben werden. Das Transform Set legt die **Verschlüsselungs**- und **Authentifizierungsalgorithmen** fest, die zum Schutz **von Daten im VPN-Tunnel** verwendet werden. Klicken Sie anschließend auf **Hinzufügen**, um diese Details anzugeben. Sie können nach Bedarf eine beliebige Anzahl Transform Sets hinzufügen, indem Sie auf **Hinzufügen** klicken und die Details angeben.



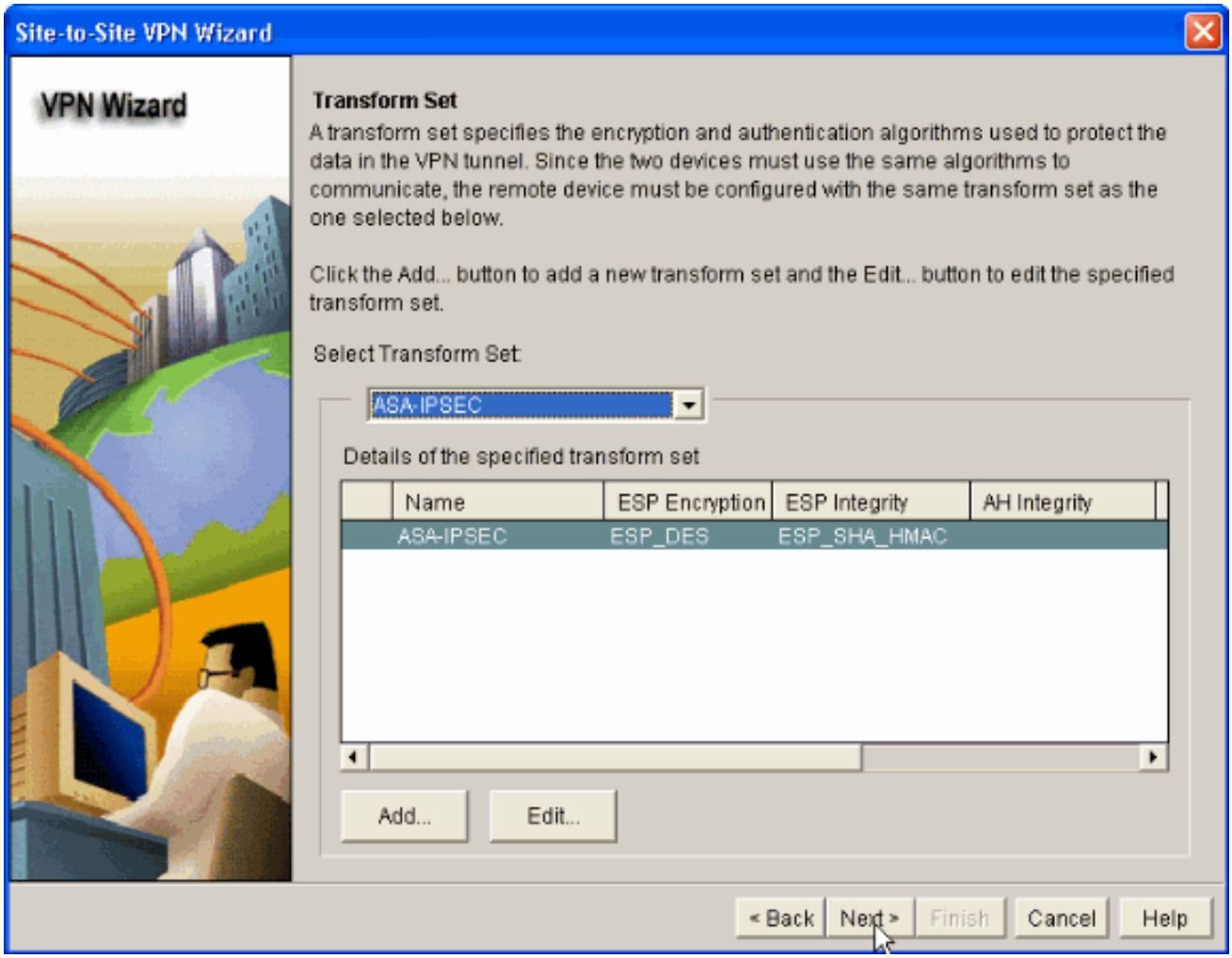
11. Geben Sie die Details zum **Transform Set** (**Verschlüsselungs- und Authentifizierungsalgorithmus**) an, und klicken Sie wie gezeigt auf **OK**.



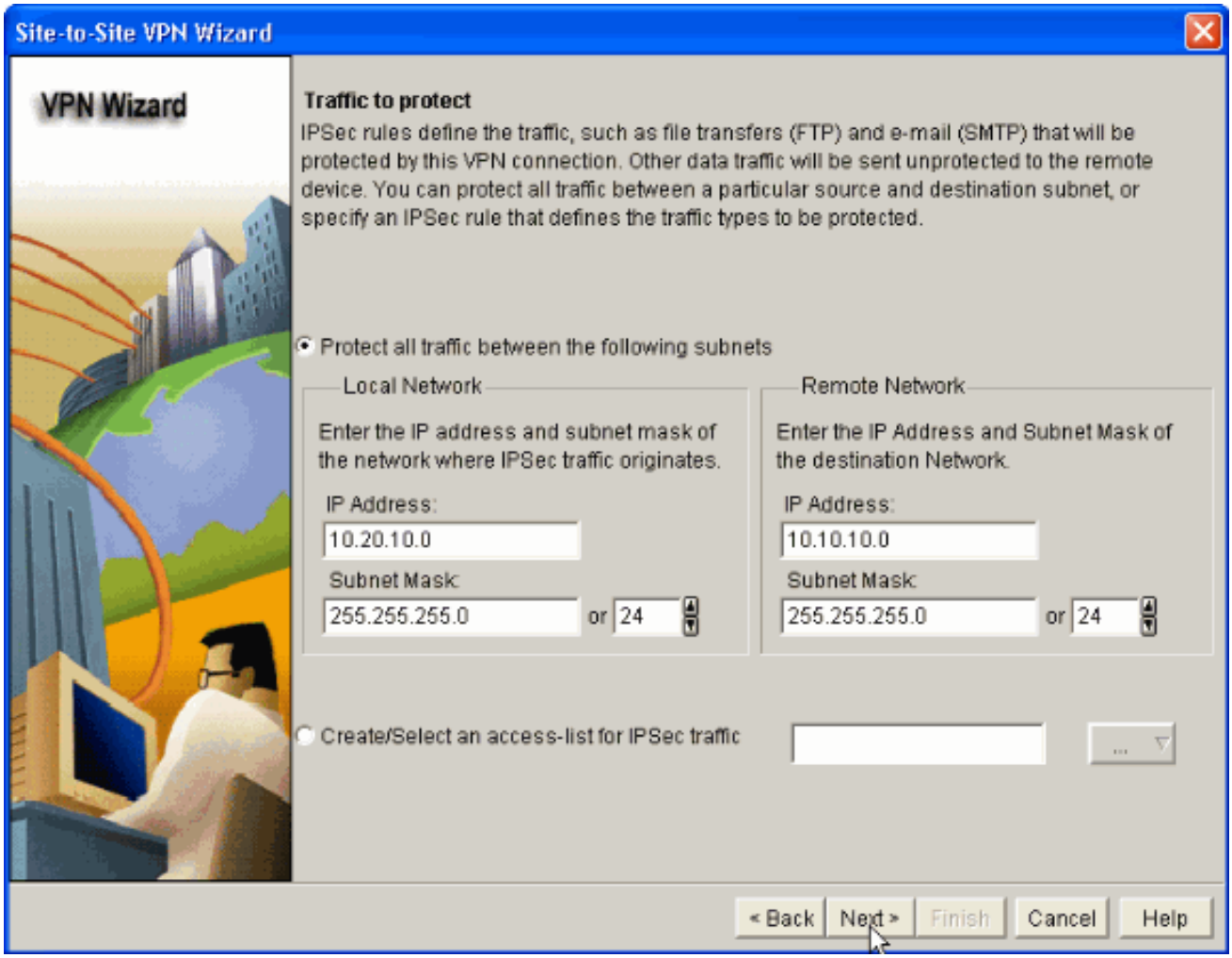
12. Wählen Sie den erforderlichen **Transform Set** aus der Dropdown-Liste aus, wie gezeigt.



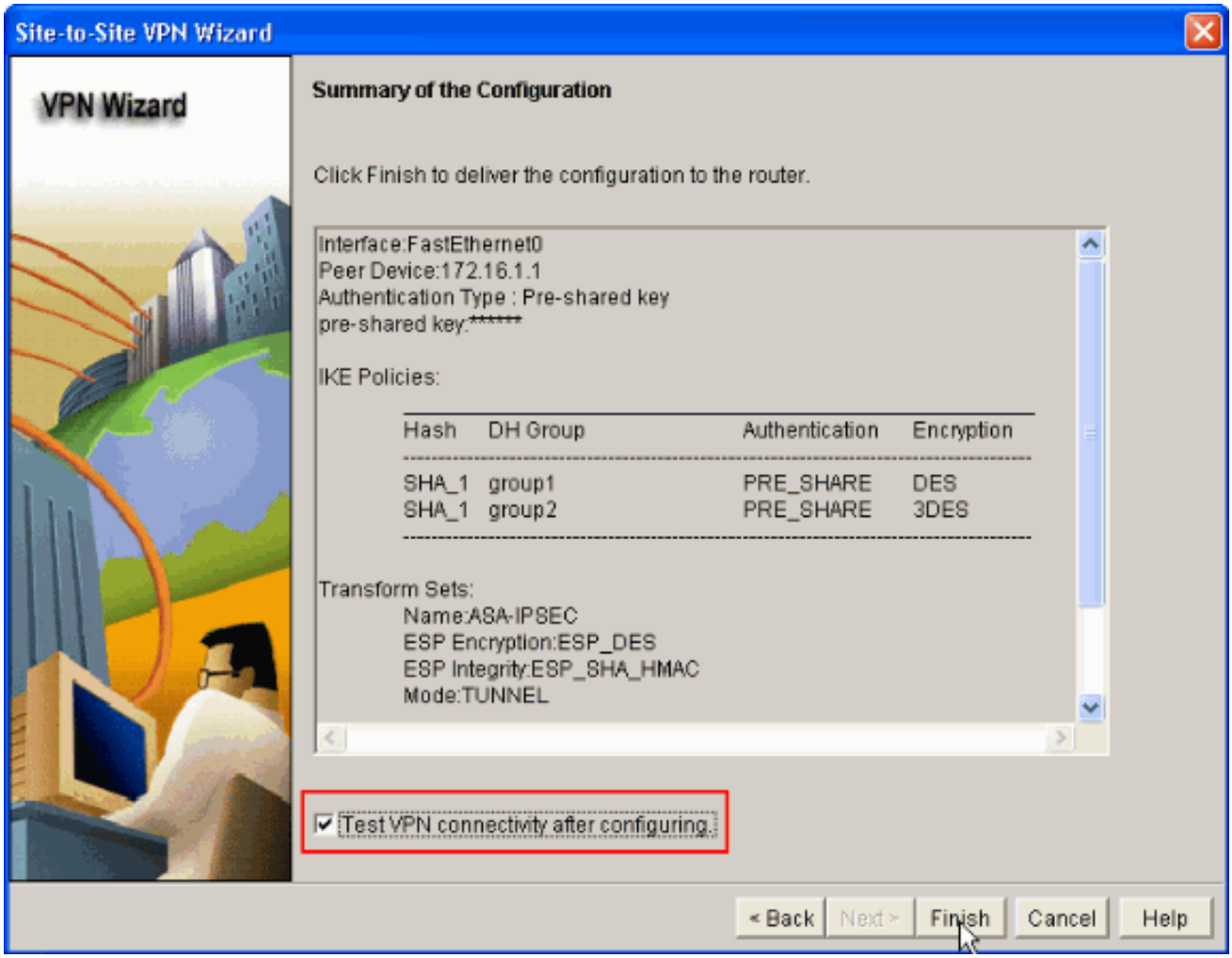
13. Klicken Sie auf **Weiter**.



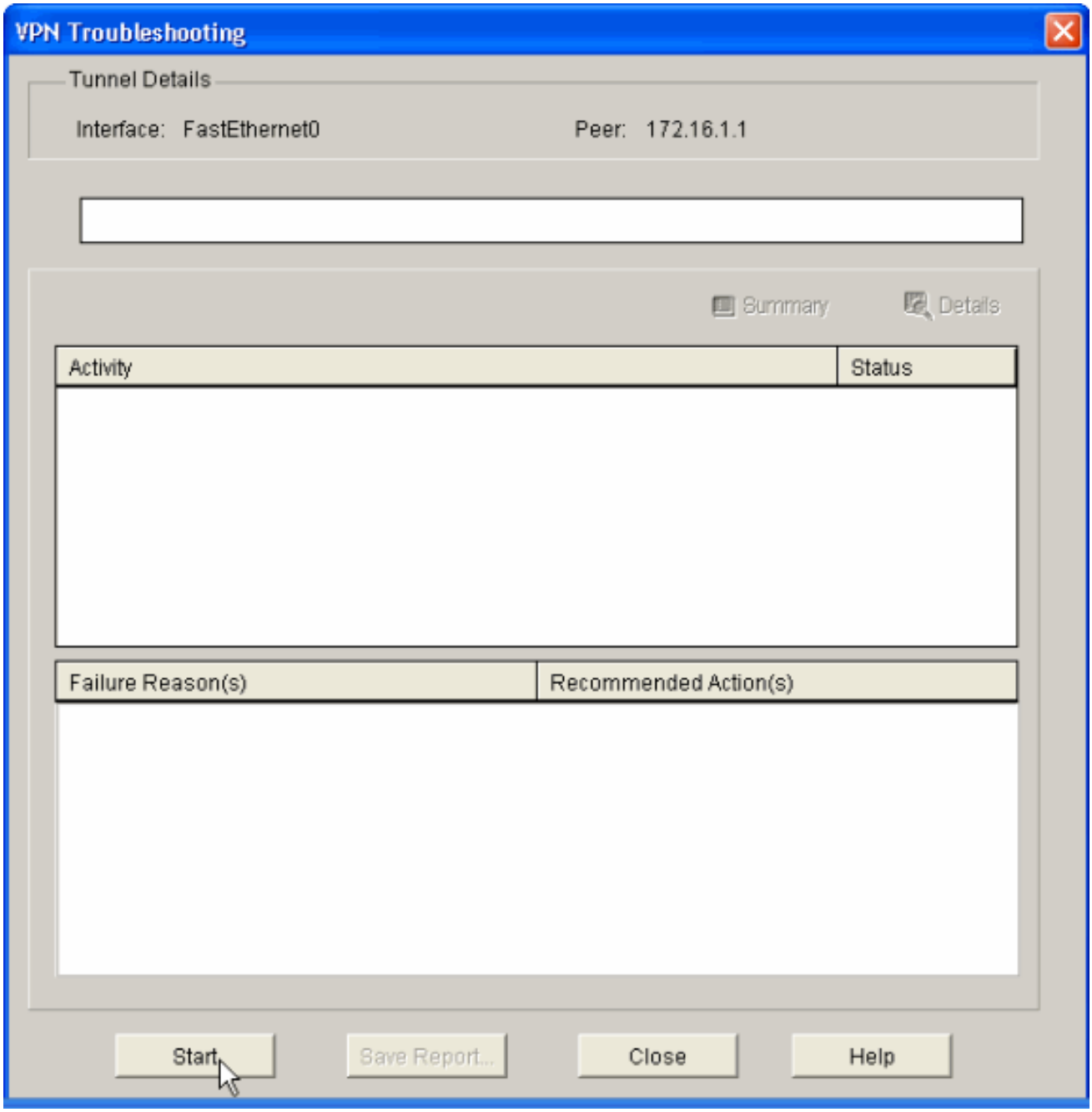
14. Geben Sie im folgenden Fenster die Details zum **Datenverkehr an, der** über den VPN-Tunnel **geschützt werden soll**. Geben Sie die **Quell- und Zielnetzwerke** des zu schützenden Datenverkehrs an, sodass der Datenverkehr zwischen den angegebenen Quell- und Zielnetzwerken geschützt ist. In diesem Beispiel ist das Quellnetzwerk 10.20.10.0 und das Zielnetzwerk 10.10.10.0. Klicken Sie anschließend auf **Weiter**.



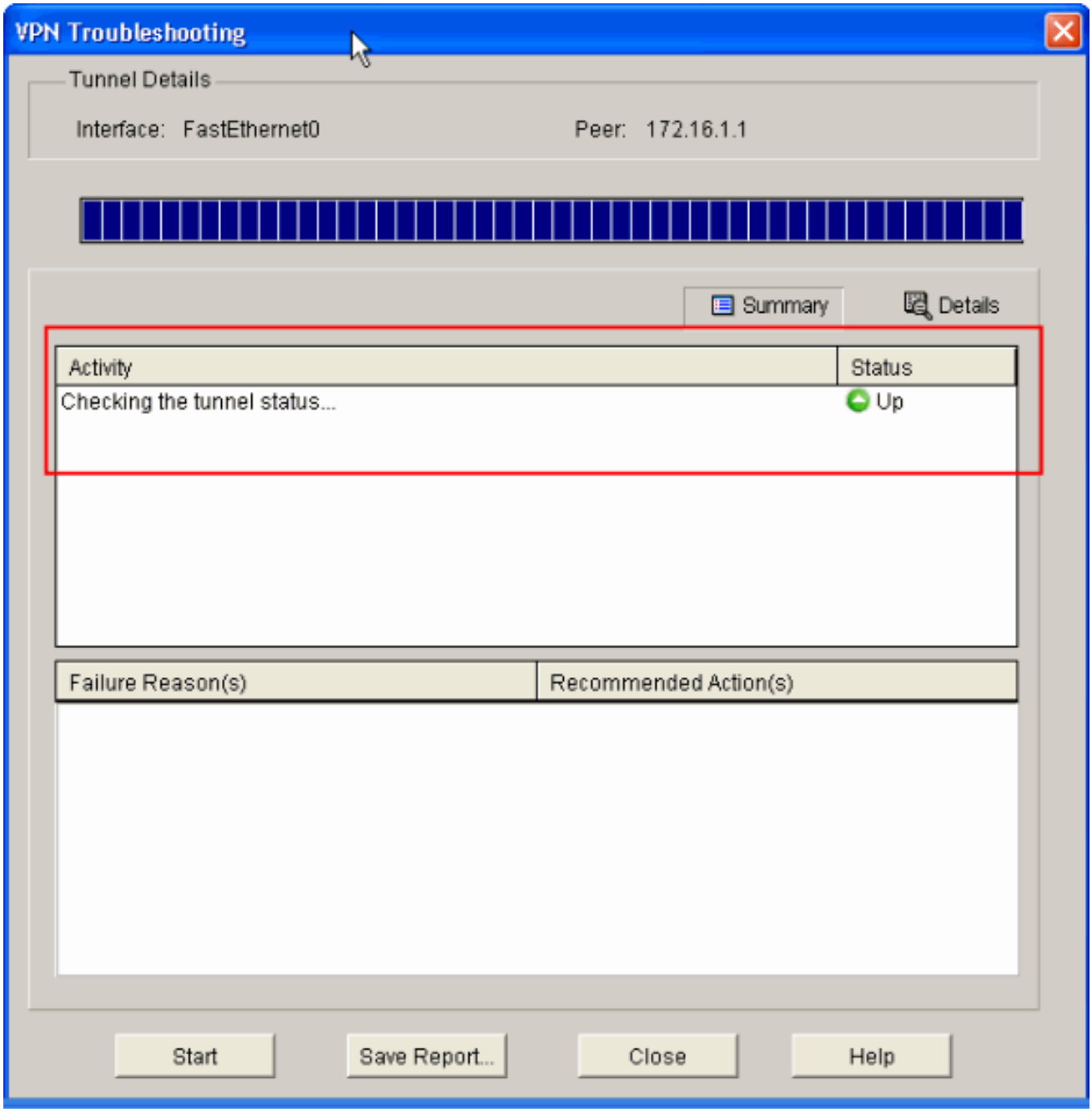
15. In diesem Fenster wird die Zusammenfassung der fertig gestellten Site-to-Site-VPN-Konfiguration angezeigt. Aktivieren Sie das Kontrollkästchen **VPN-Verbindung testen nach der Konfiguration**, wenn Sie die VPN-Verbindung testen möchten. Hier ist das Kontrollkästchen aktiviert, da die Verbindung aktiviert werden muss. Klicken Sie anschließend auf **Fertig stellen**.



16. Klicken Sie auf **Start**, um die VPN-Verbindung zu überprüfen.



17. Im nächsten Fenster wird das Ergebnis des **VPN-Verbindungstests** bereitgestellt. Hier können Sie sehen, ob der Tunnel **oben** oder **unten** ist. In dieser Beispielkonfiguration ist der Tunnel **nach oben** wie in grün dargestellt.



Damit ist die Konfiguration auf dem Cisco IOS-Router abgeschlossen.

ASA CLI-Konfiguration

ASA

```
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside interface. ! interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list 100
extended permit ip any any access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (inside_nat0_outbound) is used !--
- with the nat zero command. This prevents traffic which
!--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_1_cryptomap extended permit ip
10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (outside_cryptomap) is used !---
with the crypto map outside_map !--- to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound
!--- NAT 0 prevents NAT for networks specified in !---
the ACL inside_nat0_outbound.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 dmz
no snmp-server location
no snmp-server contact

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac
!--- Define the transform set for Phase 2. crypto map
outside_map 1 match address outside_1_cryptomap
!--- Define which traffic should be sent to the IPsec
peer. crypto map outside_map 1 set peer 172.17.1.1
!--- Sets the IPsec peer crypto map outside_map 1 set
```

```
transform-set ESP-DES-SHA
!--- Sets the IPsec transform set "ESP-AES-256-SHA" !---
to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 type ipsec-l2l
!--- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 172.17.1.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
!-- Output suppressed! username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Router-CLI-Konfiguration

Router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- 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 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- 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 ASA-IPSEC
esp-des esp-sha-hmac
!

!--- !--- Indicates that IKE is used to establish !---
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- !--- Sets the IP address of the remote end. set
peer 172.16.1.1

!--- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

!--- !--- Specifies the interesting traffic to be
encrypted. match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

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**.

- PIX Security Appliance - **show** Commands
- Remote-IOS-Router - **Anzeigen von** Befehlen

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: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

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

```
ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Remote-IOS-Router - Anzeigen von Befehlen

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

```
Router#show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

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

```
Router#show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto engine connections active** - Zeigt aktuelle Verbindungen und Informationen über verschlüsselte und entschlüsselte Pakete (nur Router).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0        172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0        172.17.1.1      set    DES+SHA                  59        0
```

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**.

Hinweis: Lesen Sie die wichtigen Informationen zu Debug-Befehlen und IP-Sicherheitsfehlerbehebung - Verwenden von Debugbefehlen, bevor Sie **Debug-**Befehle verwenden.

- **debug crypto ipsec 7**: Zeigt die IPsec-Aushandlungen für Phase 2 an.**debug crypto isakmp 7**: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.
- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.**debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.

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

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Configuration Professional: Konfigurationsbeispiel für ein standortübergreifendes IPsec-VPN zwischen ASA/PIX und einem IOS-Router
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Cisco Router- und Security Device Manager
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems