Dynamischer IPsec-Tunnel zwischen einer statisch adressierten ASA und einem dynamisch adressierten Cisco IOS-Router, der ein Konfigurationsbeispiel für CCP verwendet

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, wie die PIX/ASA Security Appliance so konfiguriert wird, dass sie dynamische IPsec-Verbindungen vom Cisco IOS® Router akzeptiert. In diesem Szenario wird der IPsec-Tunnel erstellt, wenn der Tunnel nur vom Routerende aus initiiert wird. ASA konnte wegen der dynamischen IPsec-Konfiguration keinen VPN-Tunnel initiieren.

Diese Konfiguration ermöglicht der PIX Security Appliance die Erstellung eines dynamischen IPsec LAN-to-LAN (L2L)-Tunnels mit einem Remote-VPN-Router. Dieser Router erhält dynamisch seine externe öffentliche IP-Adresse von seinem Internetdienstanbieter. Dynamic Host Configuration Protocol (DHCP) stellt diesen Mechanismus bereit, um IP-Adressen dynamisch vom Anbieter zuzuweisen. Dadurch können IP-Adressen wiederverwendet werden, wenn Hosts sie nicht mehr benötigen.

Die Konfiguration auf dem Router erfolgt mithilfe des Cisco Configuration Professional (CCP). CCP ist ein GUI-basiertes Gerätemanagement-Tool, mit dem Sie Cisco IOS-basierte Router konfigurieren können. Unter Grundlegende Routerkonfiguration mit Cisco Configuration Professional finden Sie weitere Informationen zum Konfigurieren eines Routers mit CCP.

Weitere Informationen und Konfigurationsbeispiele zur Einrichtung von IPsec-Tunneln, die ASA- und Cisco IOS-Routern verwenden, finden Sie unter Site-to-Site-VPN (L2L) mit ASA.

Unter Site-to-Site-VPN (L2L) mit IOS finden Sie weitere Informationen und ein Konfigurationsbeispiel für die dynamische Einrichtung von IPSec-Tunneln unter Verwendung von PIX und Cisco IOS-Routern.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass ASA und Router über eine Internetverbindung verfügen, um den IPSEC-Tunnel einzurichten.

Verwendete Komponenten

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

- Cisco IOS Router1812, der Cisco IOS Software Release 12.4 ausführt
- Cisco ASA 5510 Softwareversion 8.0.3

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).

Hintergrundinformationen

In diesem Szenario liegt das Netzwerk 192.168.100.0 hinter der ASA, und das Netzwerk 192.168.200.0 befindet sich hinter dem Cisco IOS-Router. Es wird davon ausgegangen, dass der Router seine öffentliche Adresse über DHCP vom ISP erhält. Da dies ein Problem bei der Konfiguration eines statischen Peers am ASA-Ende darstellt, müssen Sie sich der Methode der dynamischen Verschlüsselungskonfiguration nähern, um einen Site-to-Site-Tunnel zwischen ASA und dem Cisco IOS-Router einzurichten.

Die Internetbenutzer am ASA-Ende werden in die IP-Adresse der externen Schnittstelle übersetzt. Es wird davon ausgegangen, dass NAT nicht auf dem Cisco IOS-Router-Ende konfiguriert ist.

Dies sind die wichtigsten Schritte, die am ASA-Ende konfiguriert werden müssen, um einen dynamischen Tunnel einzurichten:

1. ISAKMP-bezogene Konfiguration Phase 1
2. Konfiguration der NAT-Freistellung
3. Dynamische Konfiguration der Crypto Map

Für den Cisco IOS-Router ist eine statische Crypto Map konfiguriert, da angenommen wird, dass die ASA über eine statische öffentliche IP-Adresse verfügt. Dies ist die Liste der wichtigsten Schritte, die auf dem Cisco IOS-Router-Ende konfiguriert werden müssen, um einen dynamischen IPSEC-Tunnel einzurichten.

1. ISAKMP-bezogene Konfiguration Phase 1
2. Statische Kryptozuordnungskonfiguration

Diese Schritte werden in diesen Konfigurationen ausführlich beschrieben.

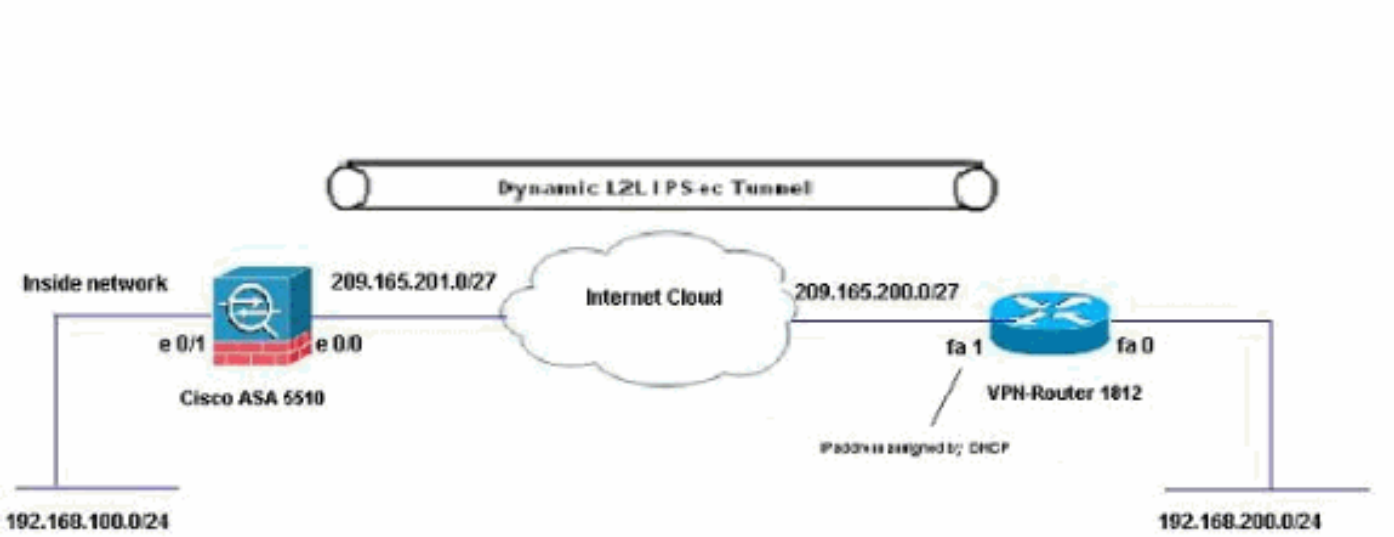
Konfigurieren

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

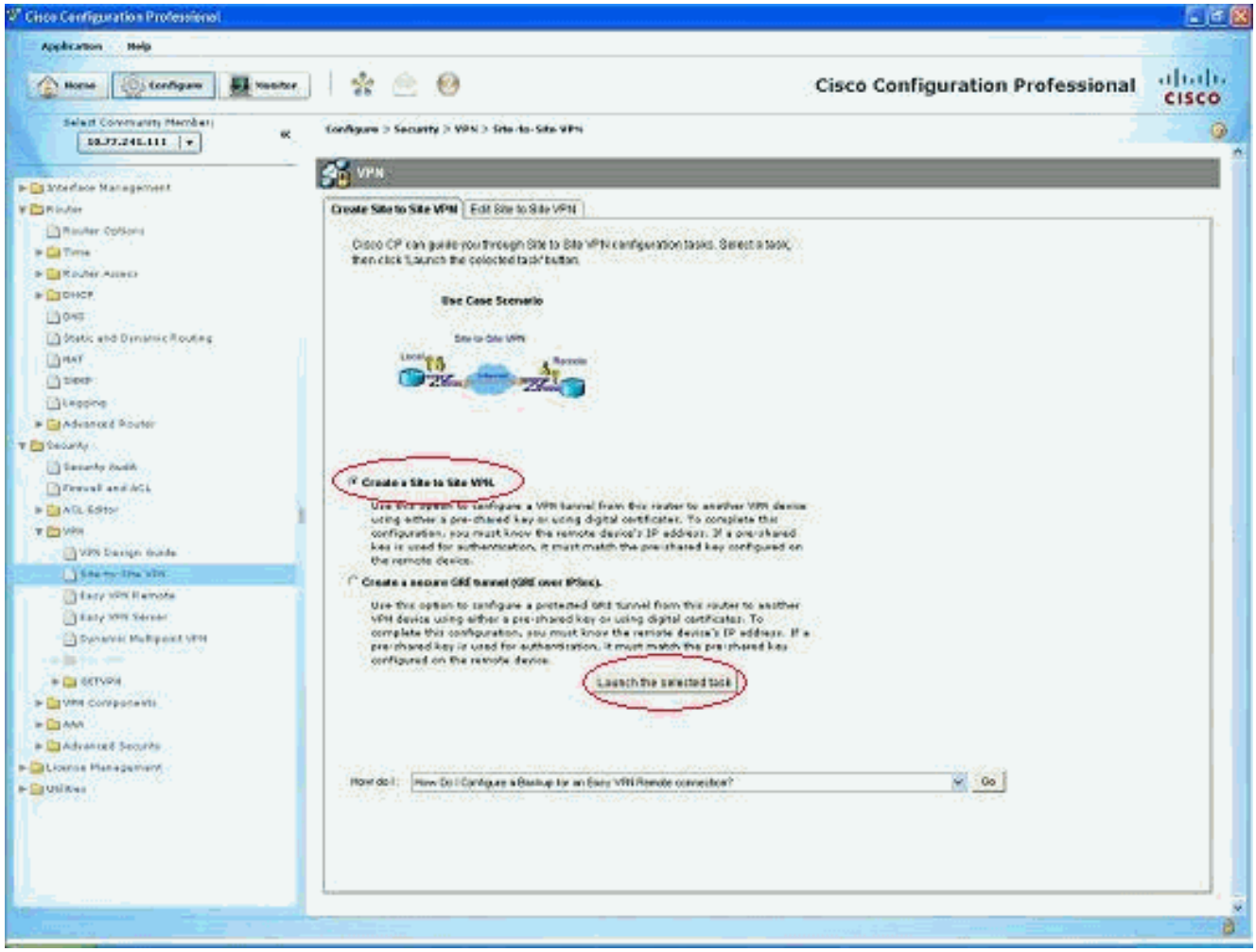
In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



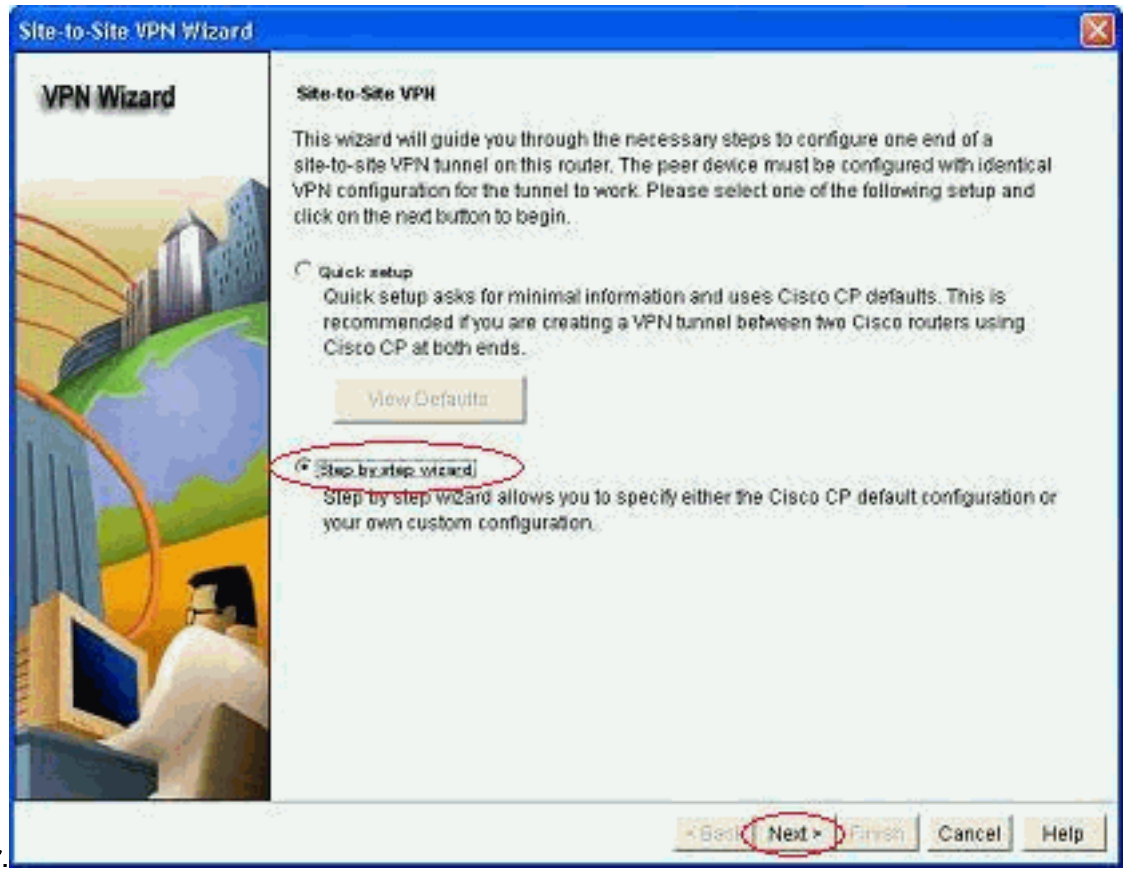
Konfigurationen

Dies ist die IPsec-VPN-Konfiguration auf dem VPN-Router mit CCP. Gehen Sie wie folgt vor:

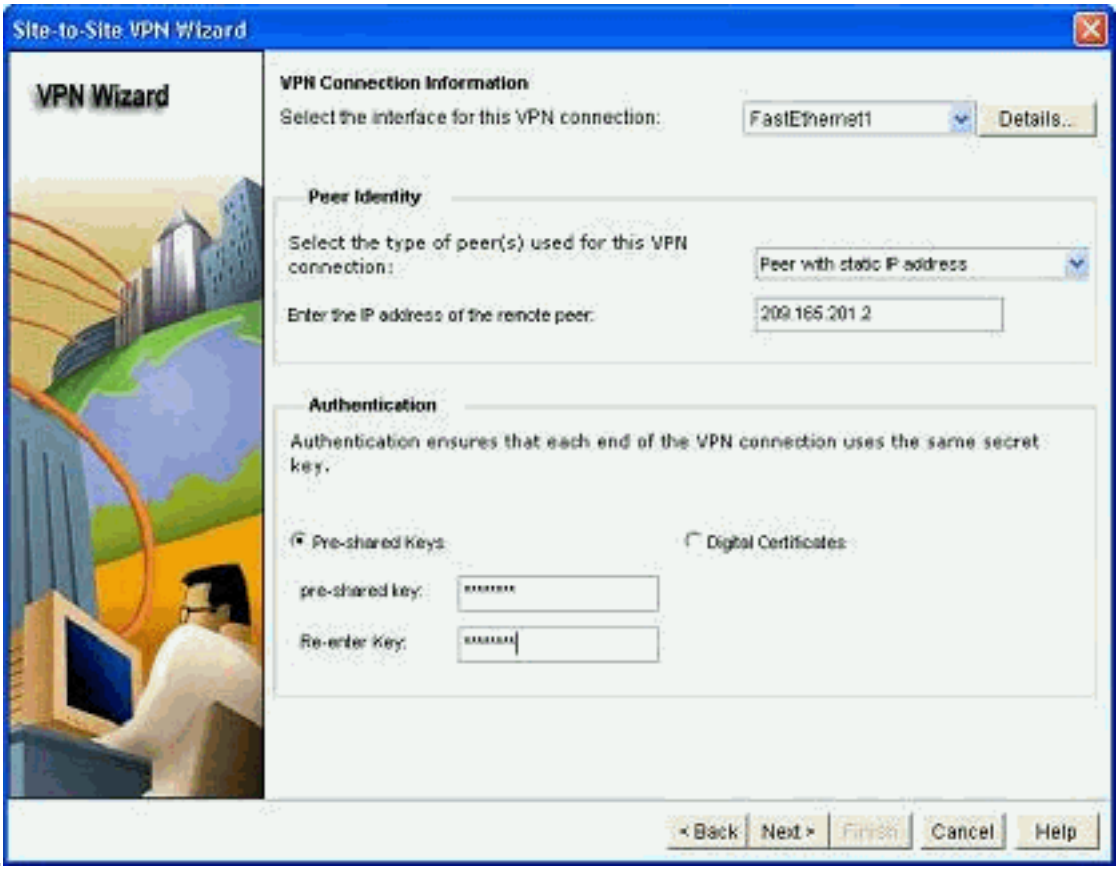
1. Öffnen Sie die CCP-Anwendung, und wählen Sie **Configure > Security > VPN > Site-to-Site-VPN aus**. Klicken Sie auf die **Registerkarte Ausgewählte starten**.



2. Wählen Sie **Schritt für Schritt den Assistenten aus** und klicken Sie dann auf **Weiter**.

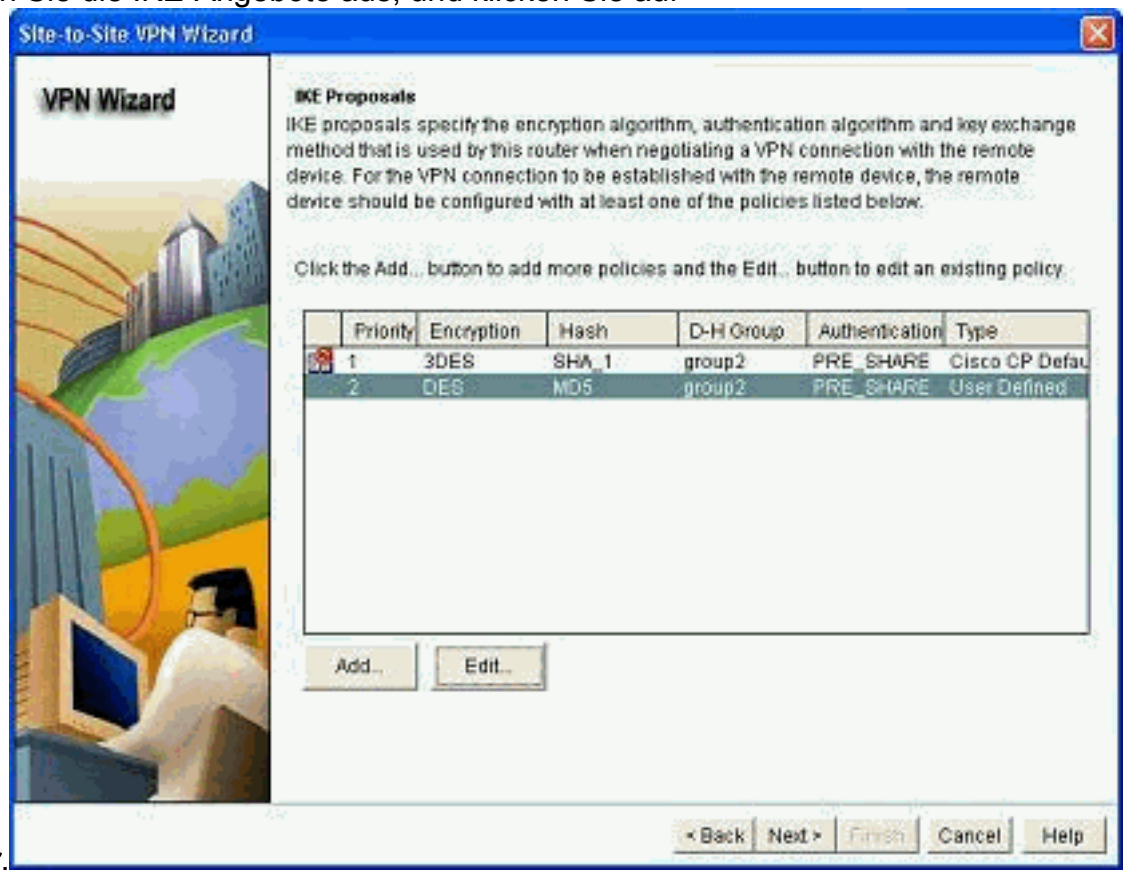


3. Geben Sie die IP-Adresse des Remote-Peers zusammen mit den Authentifizierungsdetails



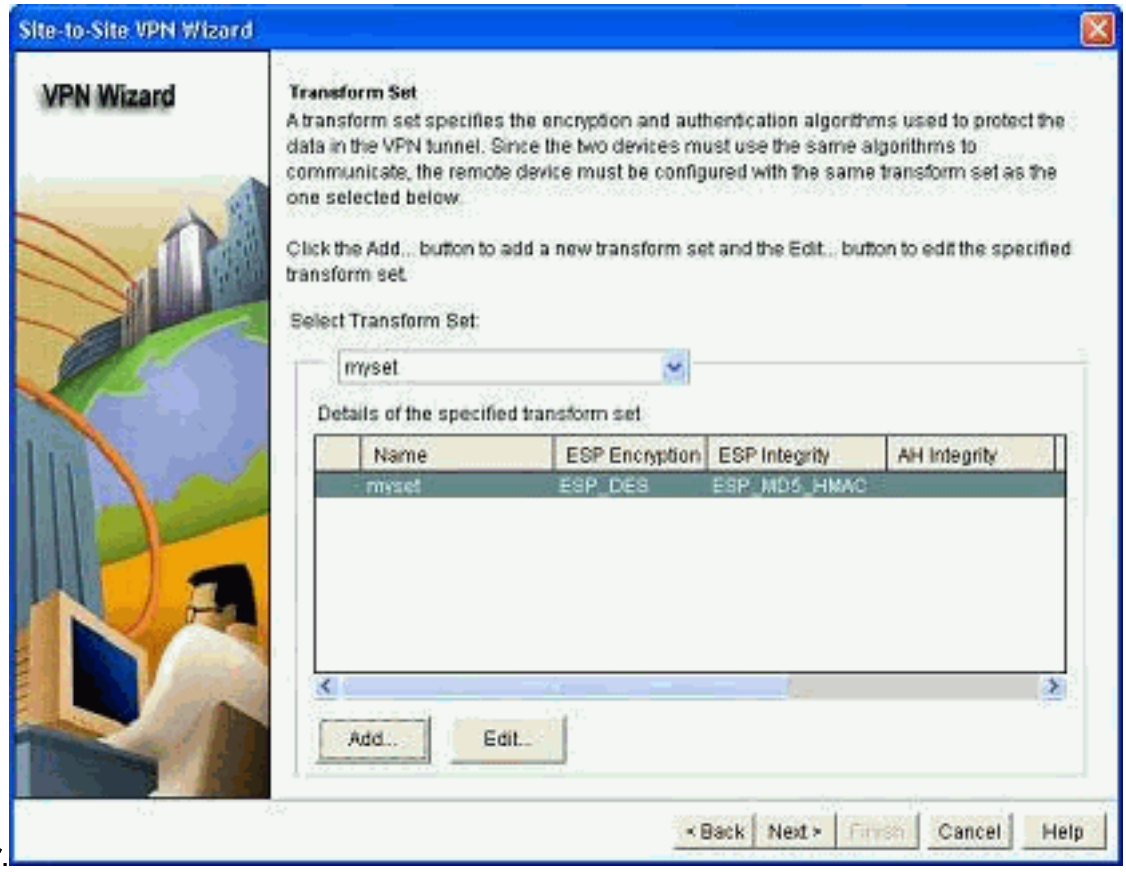
ein.

4. Wählen Sie die IKE-Angebote aus, und klicken Sie auf



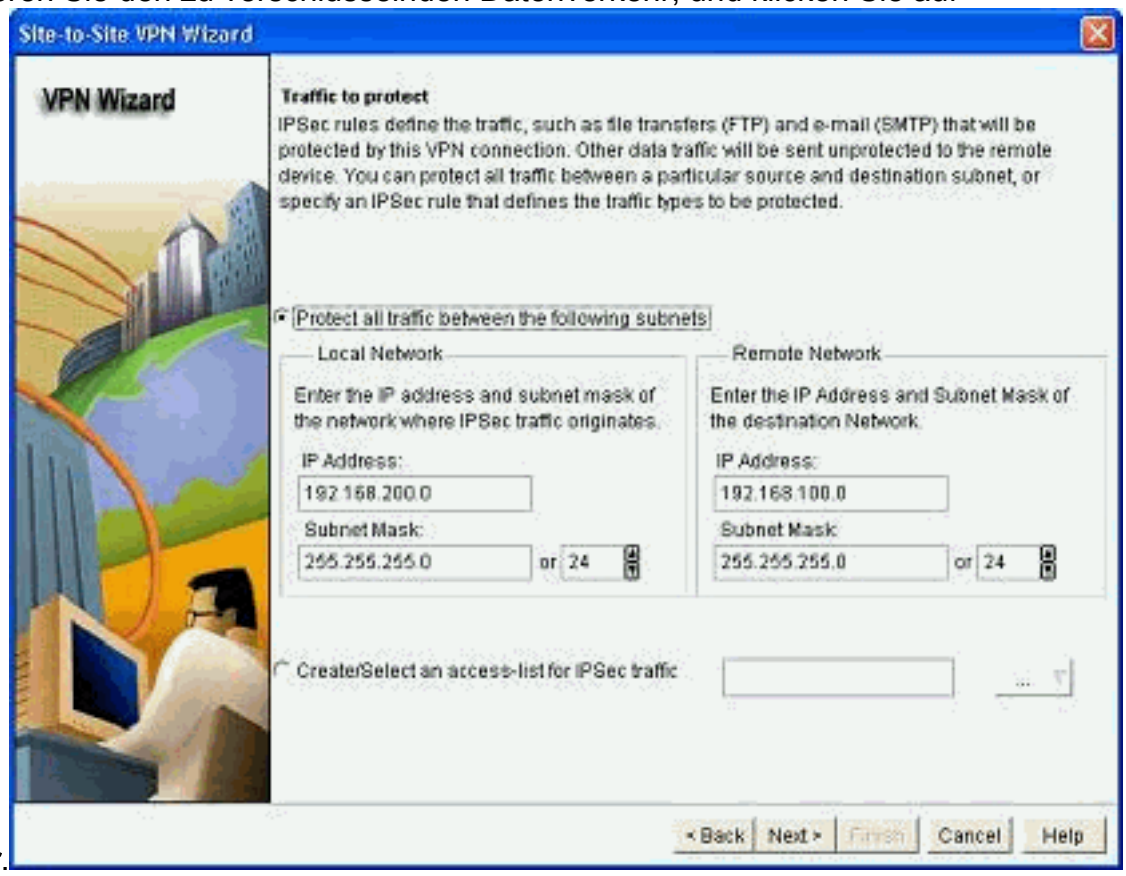
Weiter.

5. Definieren Sie die Details zum Transformationssatz, und klicken Sie auf



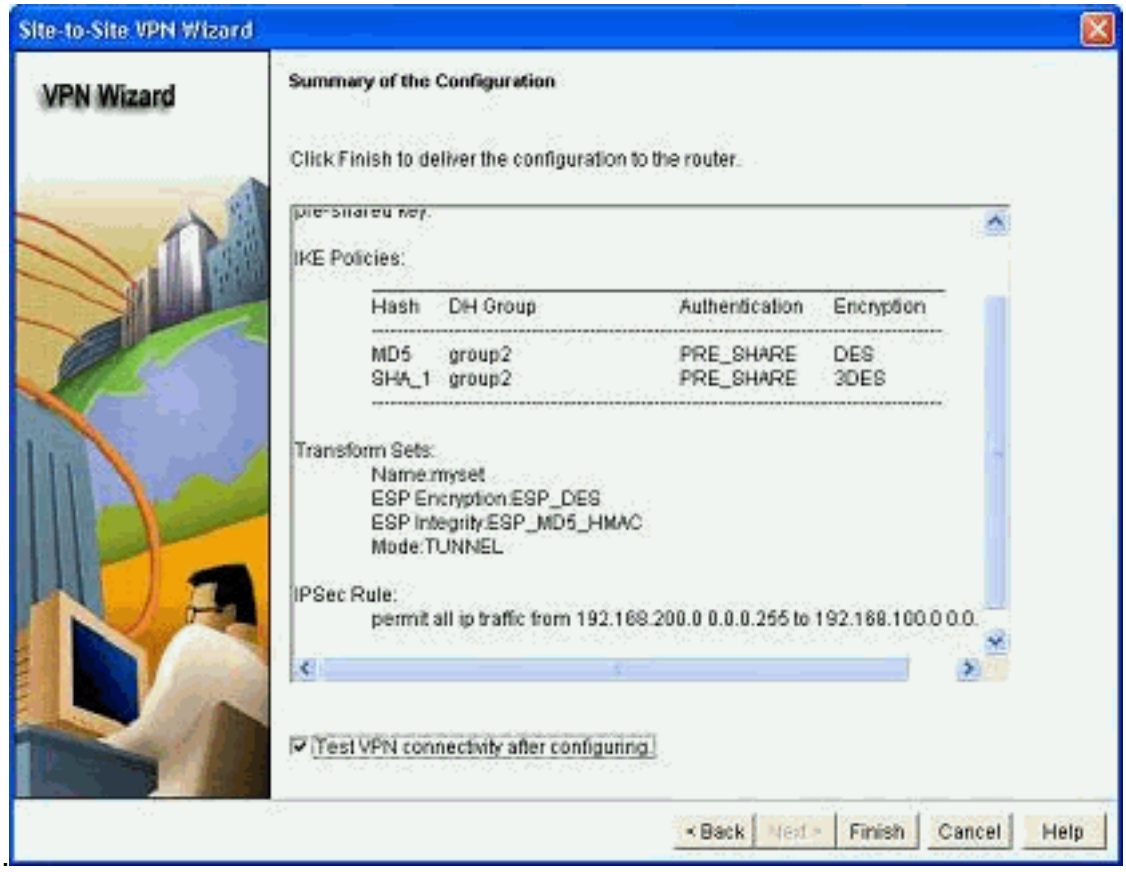
Weiter.

6. Definieren Sie den zu verschlüsselnden Datenverkehr, und klicken Sie auf



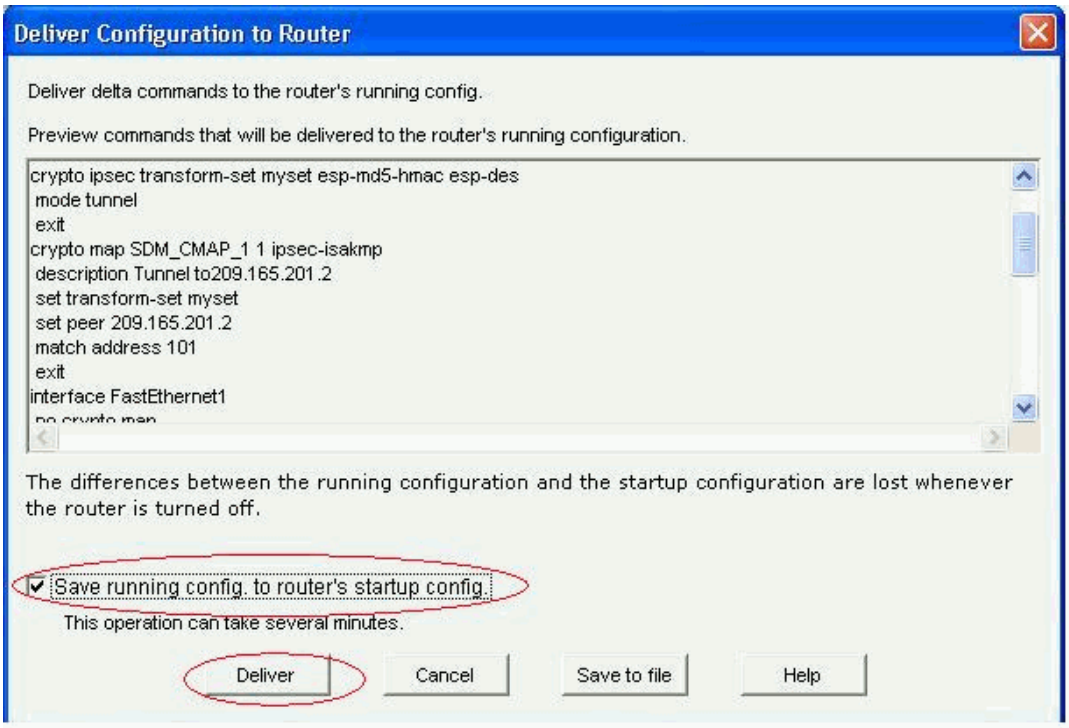
Weiter.

7. Überprüfen Sie die Zusammenfassung der IPsec-Konfiguration für die Verschlüsselung, und klicken Sie auf **Fertig**

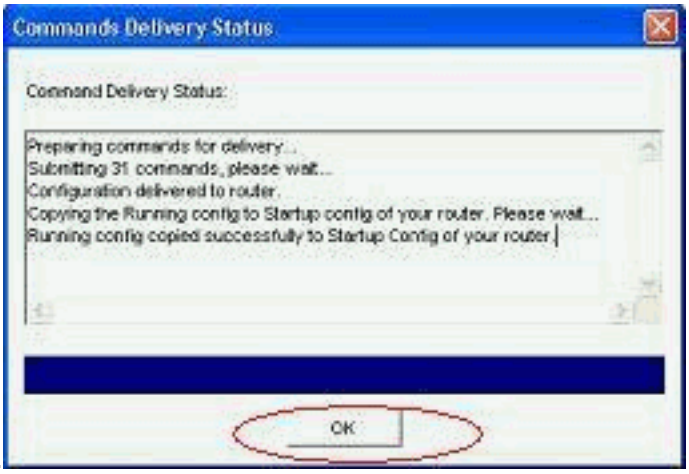


stellen.

8. Klicken Sie auf **Deliver**, um die Konfiguration an den VPN-Router zu senden.



9. Klicken Sie auf **OK**.



CLI-Konfiguration

- Ciscoasa
- VPN-Router

Ciscoasa

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0

no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
!
route outside 0.0.0.0 0.0.0.0 209.165.201.1 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
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
!
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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:d41d8cd98f00b204e9800998ecf8427e
: end
ciscoasa(config)#
```

CCP erstellt diese Konfiguration auf dem VPN-Router.

VPN-Router

```
VPN-Router#show run
Building configuration...
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
!
!
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQO1
!
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
 encrypt 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 hash md5
 authentication pre-share
 group 2
!
!
crypto isakmp key cisco123 address 209.165.201.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
!
crypto map SDM_CMAP_1 1 IPSec-isakmp
 description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
 match address 101
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio1
 no ip address
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
 station-role root
!
interface FastEthernet0
 ip address 192.168.200.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address dhcp
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
interface FastEthernet4
 no ip address
 shutdown
!
interface FastEthernet5
 no ip address
 shutdown
!
interface FastEthernet6
 no ip address
 shutdown
!
interface FastEthernet7
 no ip address
 shutdown
!
interface FastEthernet8
 no ip address
 shutdown
!
interface FastEthernet9
 no ip address
 shutdown
```

```
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet ssh
!
no scheduler allocate
end
```

Überprüfen

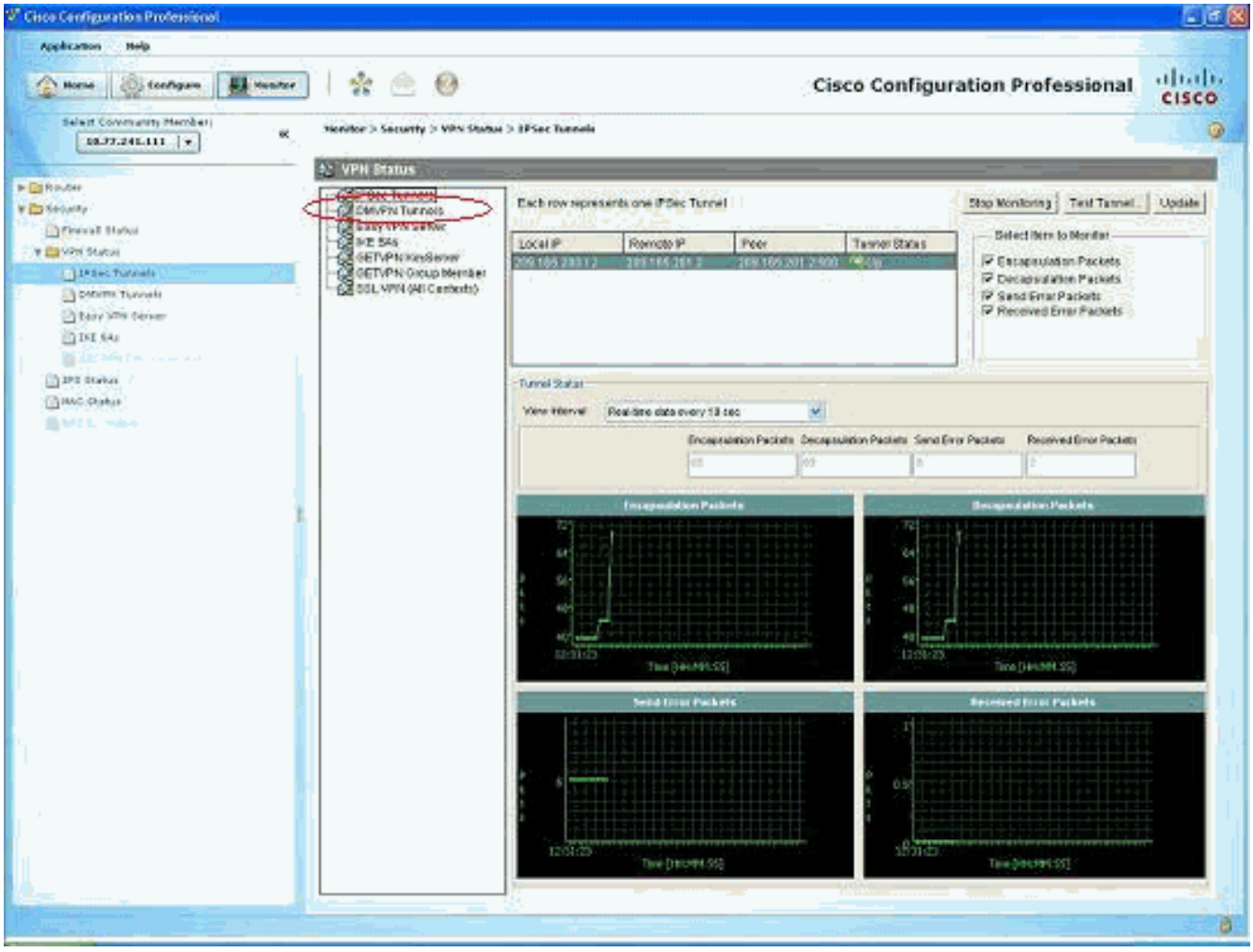
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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**.

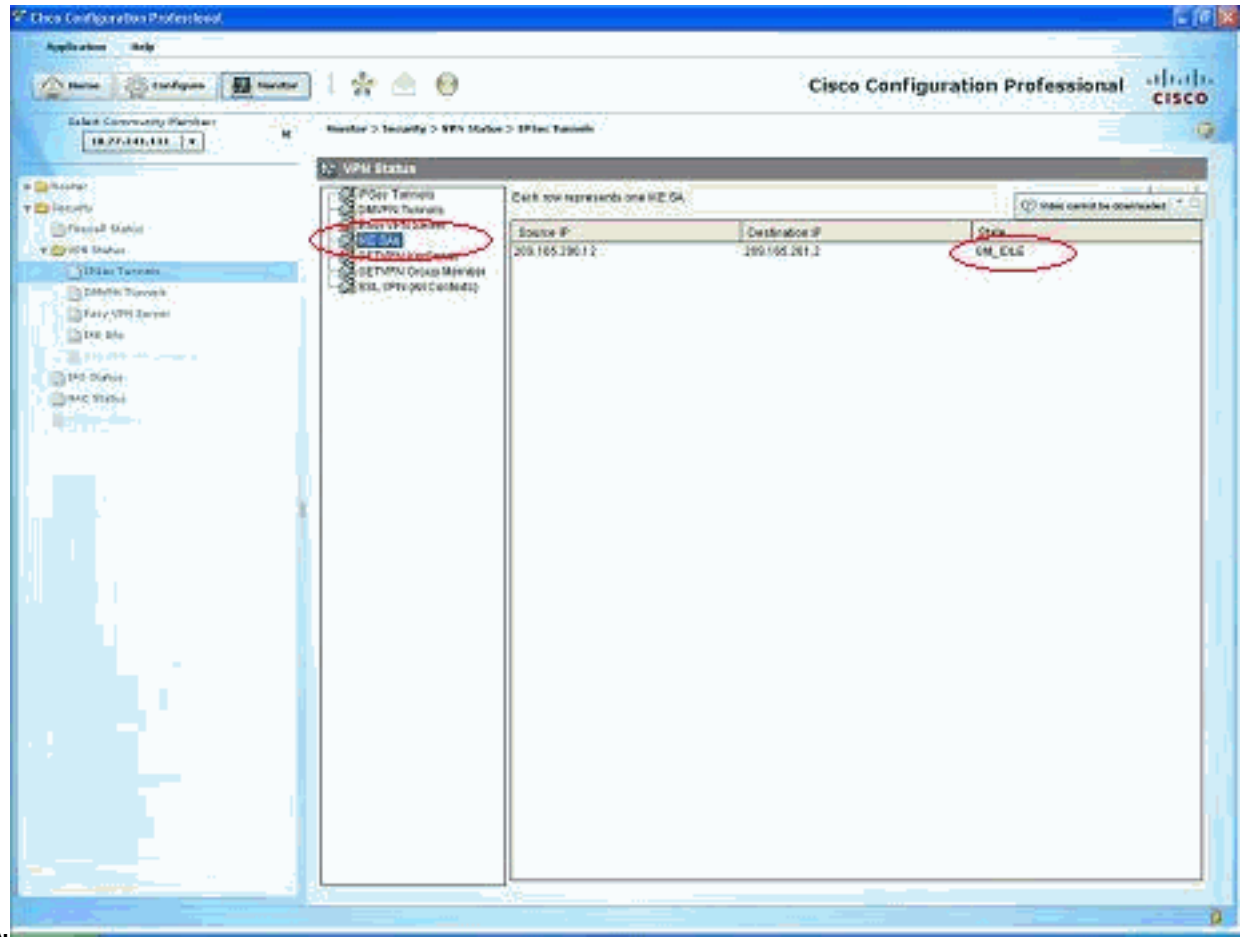
- Überprüfen der Tunnelparameter über CCP
- Überprüfen des Tunnelstatus über die ASA CLI
- Überprüfen der Tunnelparameter über die Router-CLI

Überprüfung von Tunnelparametern durch CCP

- Überwachen des Datenverkehrs durch den IPsec-Tunnel



- Überwachen Sie den Status der Phase I ISAKMP SA.



Überprüfen des Tunnelstatus über die ASA CLI

- Überprüfen Sie den Status von Phase I ISAKMP SA.

```
ciscoasa#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: 209.165.200.12
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ciscoasa#
```

Hinweis: Beachten Sie die Rolle als Responder, die angibt, dass der Initiator dieses Tunnels am anderen Ende ist, z. B. der VPN-Router.

- Überprüfen Sie die Parameter der Phase II IPSEC SA.

```
ciscoasa#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2

      local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
      current_peer: 209.165.200.12

      #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
      #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 29, #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.: 209.165.201.2, remote crypto endpt.: 209.165.200.12

      path mtu 1500, IPSec overhead 58, media mtu 1500
      current outbound spi: E7B37960

    inbound esp sas:
      spi: 0xABB49C64 (2880740452)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 4096, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (4274997/3498)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xE7B37960 (3887298912)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 4096, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (4274997/3498)
         IV size: 8 bytes
         replay detection support: Y
```

Überprüfen Sie die Tunnelparameter über die Router-CLI.

- Überprüfen Sie den Status von Phase I ISAKMP SA.

```
VPN-Router#show crypto isakmp sa
dst             src             state          conn-id slot status
209.165.201.2   209.165.200.12  QM_IDLE              1    0 ACTIVE
```

- Überprüfen Sie die Parameter der Phase II IPSEC SA.

```
VPN-Router#show crypto ipsec sa

interface: FastEthernet1
    Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
   current_peer 209.165.201.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
    #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

     local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xABB49C64(2880740452)

     inbound esp sas:
      spi: 0xE7B37960(3887298912)
        transform: esp-des esp-md5-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): (4481818/3375)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xABB49C64(2880740452)
        transform: esp-des esp-md5-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): (4481818/3371)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Abbau der vorhandenen Kryptoverbindungen.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa

VPN-Router#clear crypto isakmp
```

- Verwenden Sie **Debug-**Befehle, um Probleme mit dem VPN-Tunnel zu beheben.**Hinweis:** Wenn Sie Debugging aktivieren, kann dies den Betrieb des Routers unterbrechen, wenn bei Internetworks hohe Ladebedingungen auftreten.**Verwenden Sie debug-Befehle mit Vorsicht. Im Allgemeinen wird empfohlen, dass diese Befehle nur unter der Anleitung des technischen Supports für den Router verwendet werden, wenn spezifische Probleme behoben werden.**

```
ciscoasa#debug crypto engine
ciscoasa#debug crypto isakmp
ciscoasa#debug crypto IPSec
ciscoasa#

VPN-Router#debug crypto engine
Crypto Engine debugging is on
VPN-Router#debug crypto isakmp
Crypto ISAKMP debugging is on
VPN-Router#debug crypto ipsec
Crypto IPSEC debugging is on
VPN-Router#
```

Weitere Informationen zu Debugbefehlen finden Sie unter debug crypto isakmp in Understanding and Using debug Commands.

Zugehörige Informationen

- Support-Seite für IPSEC-Verhandlung/IKE-Protokolle
- Dokumentation für die Betriebssystem-Software der Cisco ASA Security Appliance
- Häufigste IPSEC VPN-Fehlerbehebungslösungen
- Anforderungen für Kommentare (RFCs)