Konfigurieren des Cisco VPN 300 Concentrator für einen Cisco Router

Inhalt

Einführung

Diese Beispielkonfiguration zeigt, wie ein privates Netzwerk hinter einem Router, auf dem die Cisco IOS® Software ausgeführt wird, mit einem privaten Netzwerk hinter dem Cisco VPN 3000 Concentrator verbunden wird. Die Geräte in den Netzwerken kennen sich untereinander durch ihre privaten Adressen aus.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco 2611-Router mit Cisco IOS-Software, Version 12.3.(1)a**Hinweis:** Stellen Sie sicher, dass die Router der Cisco Serie 2600 mit einem IPsec-VPN-IOS-Image installiert sind, das die VPN-Funktion unterstützt.
- Cisco VPN 3000 Concentrator mit 4,0,1 B

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 unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

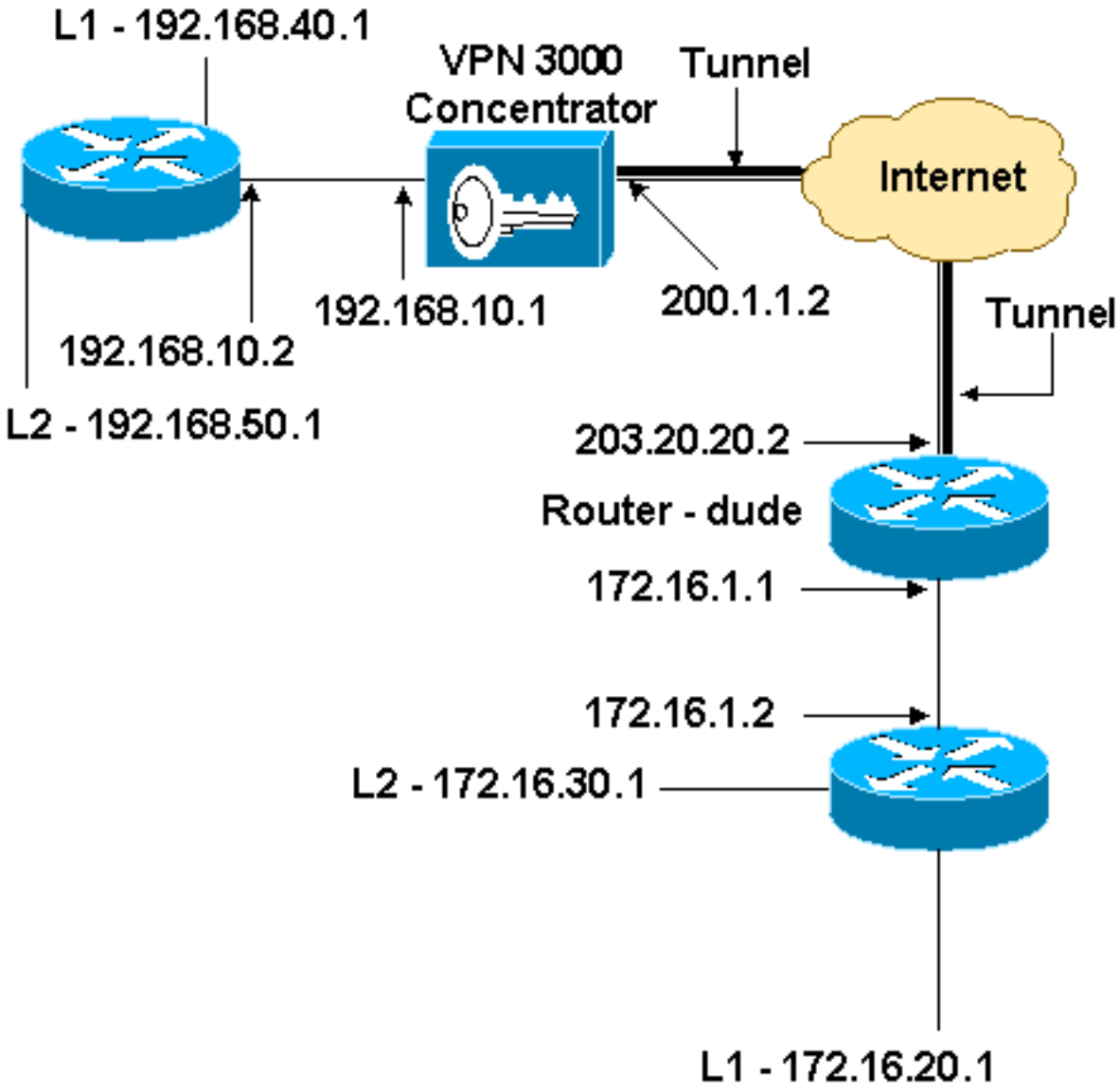
Konfigurieren

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

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

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument wird diese Konfiguration verwendet.

Routerkonfiguration

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Konfiguration des VPN-Concentrators

In dieser Übung wird zuerst auf den VPN Concentrator über den Konsolenport zugegriffen und eine minimale Konfiguration hinzugefügt, sodass die weitere Konfiguration über die grafische Benutzeroberfläche (GUI) vorgenommen werden kann.

Wählen Sie **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration**, um sicherzustellen, dass der VPN Concentrator keine vorhandene Konfiguration enthält.

Der VPN Concentrator wird in der Schnellkonfiguration angezeigt, und diese Artikel werden nach dem Neustart konfiguriert:

- Uhrzeit/Datum
- Schnittstellen/Masken in **Konfiguration > Schnittstellen** (public=200.1.1.2/24, private=192.168.10.1/24)
- Standard-Gateway in **Konfiguration > System > IP-Routing > Default_Gateway** (200.1.1.1)

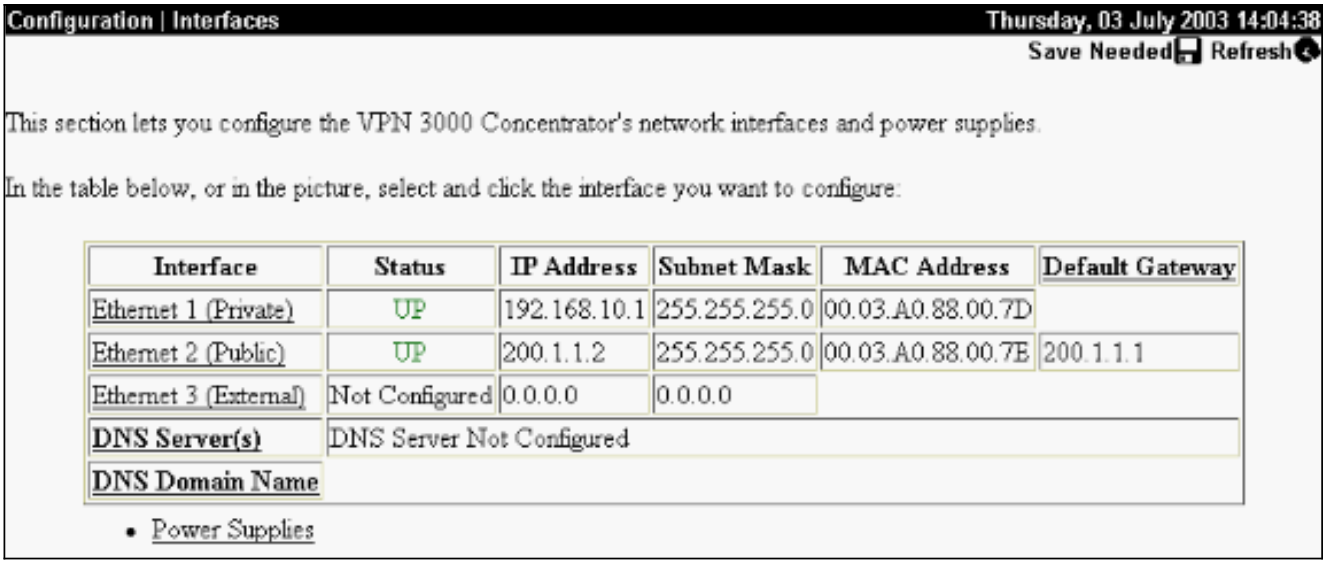
Der Zugriff auf den VPN Concentrator erfolgt über HTML aus dem internen Netzwerk.

Hinweis: Da der VPN Concentrator von außen verwaltet wird, müssen Sie auch Folgendes auswählen:

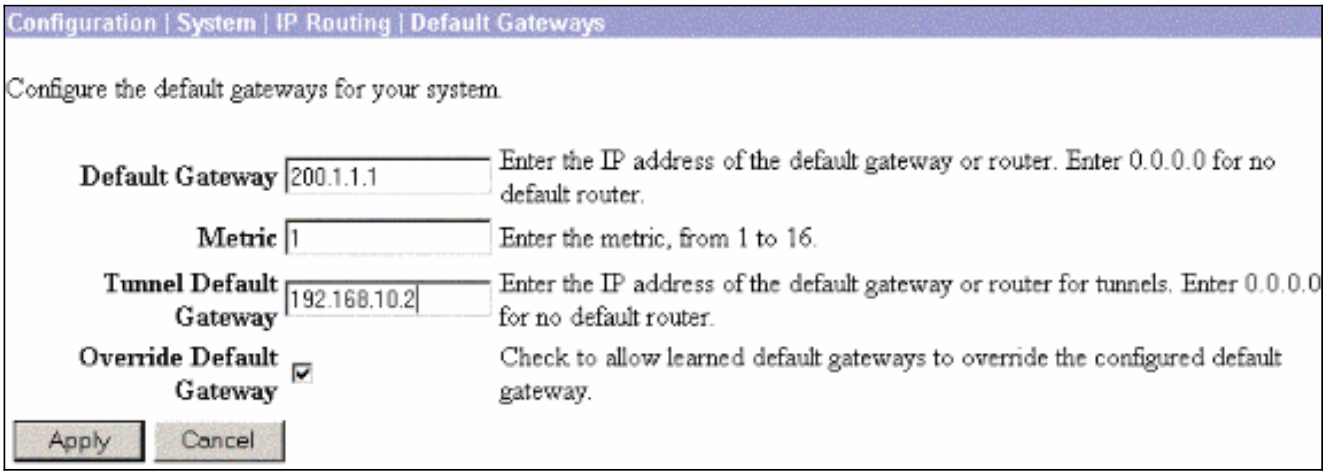
- **Konfiguration > Schnittstellen > 2-public > IP Filter > 1 auswählen. Private (Standard)**.
- **Administration > Access Rights > Access Control List > Add Manager Workstation** zum Hinzufügen der IP-Adresse des *externen* Managers

Dies ist nur erforderlich, wenn Sie den VPN Concentrator von *außen* verwalten.

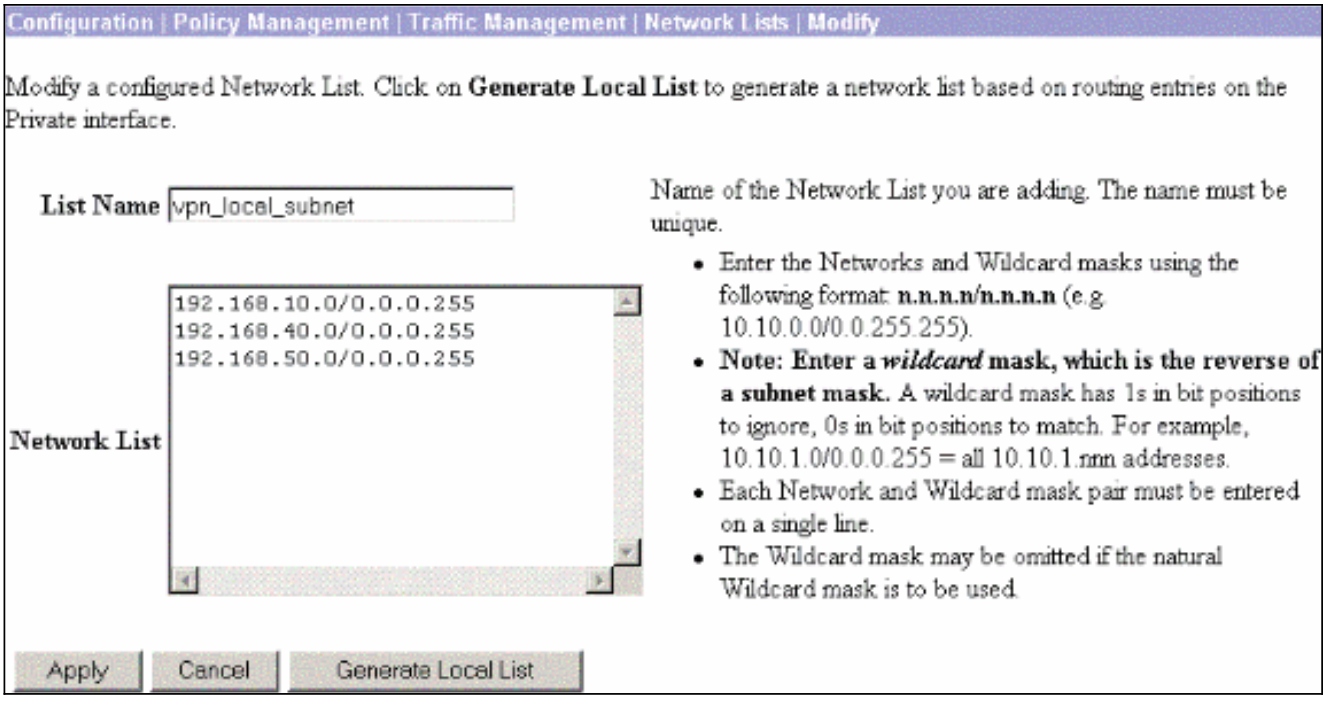
1. Wählen Sie **Configuration > Interfaces (Konfiguration >** Schnittstellen) aus, um die Schnittstellen nach dem Aufrufen der Benutzeroberfläche erneut zu überprüfen.



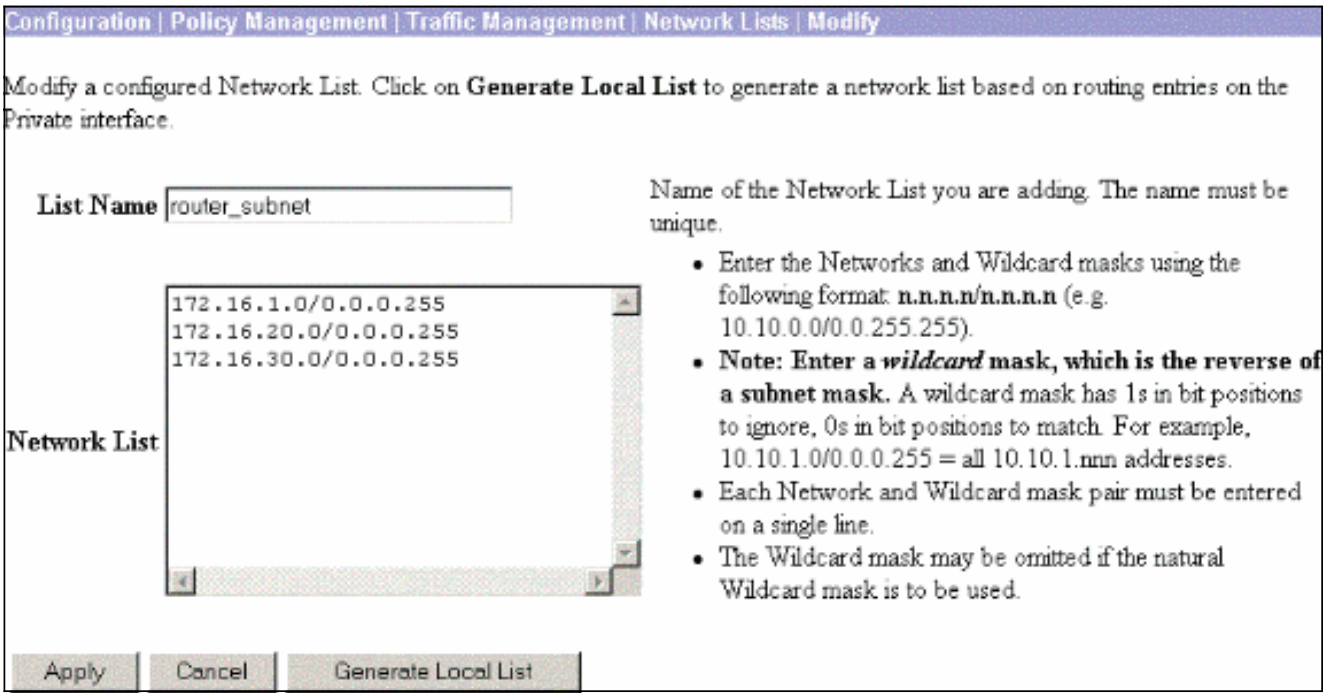
2. Wählen Sie Configuration > System > IP Routing > Default Gateways (Konfiguration > System > IP Routing > Default Gateways (Standard-(Internet)-Gateway) und **Tunnel Default** (inside) **Gateway für IPsec, um die anderen Subnetze im privaten Netzwerk zu erreichen.**



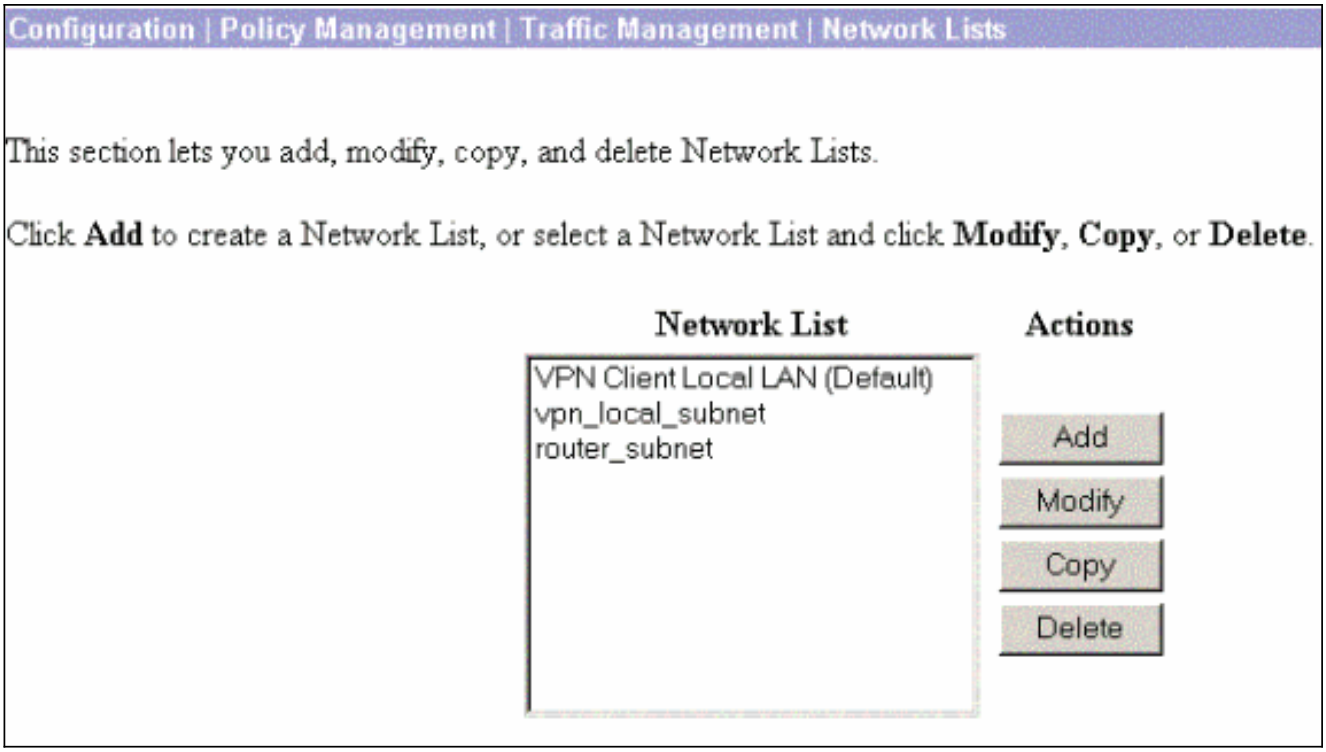
3. Wählen Sie **Configuration > Policy Management > Network Lists (Konfiguration > Richtlinienmanagement >** Netzwerklisten), um die Netzwerklisten zu erstellen, die den zu verschlüsselnden Datenverkehr definieren.Dies sind die lokalen Netzwerke:



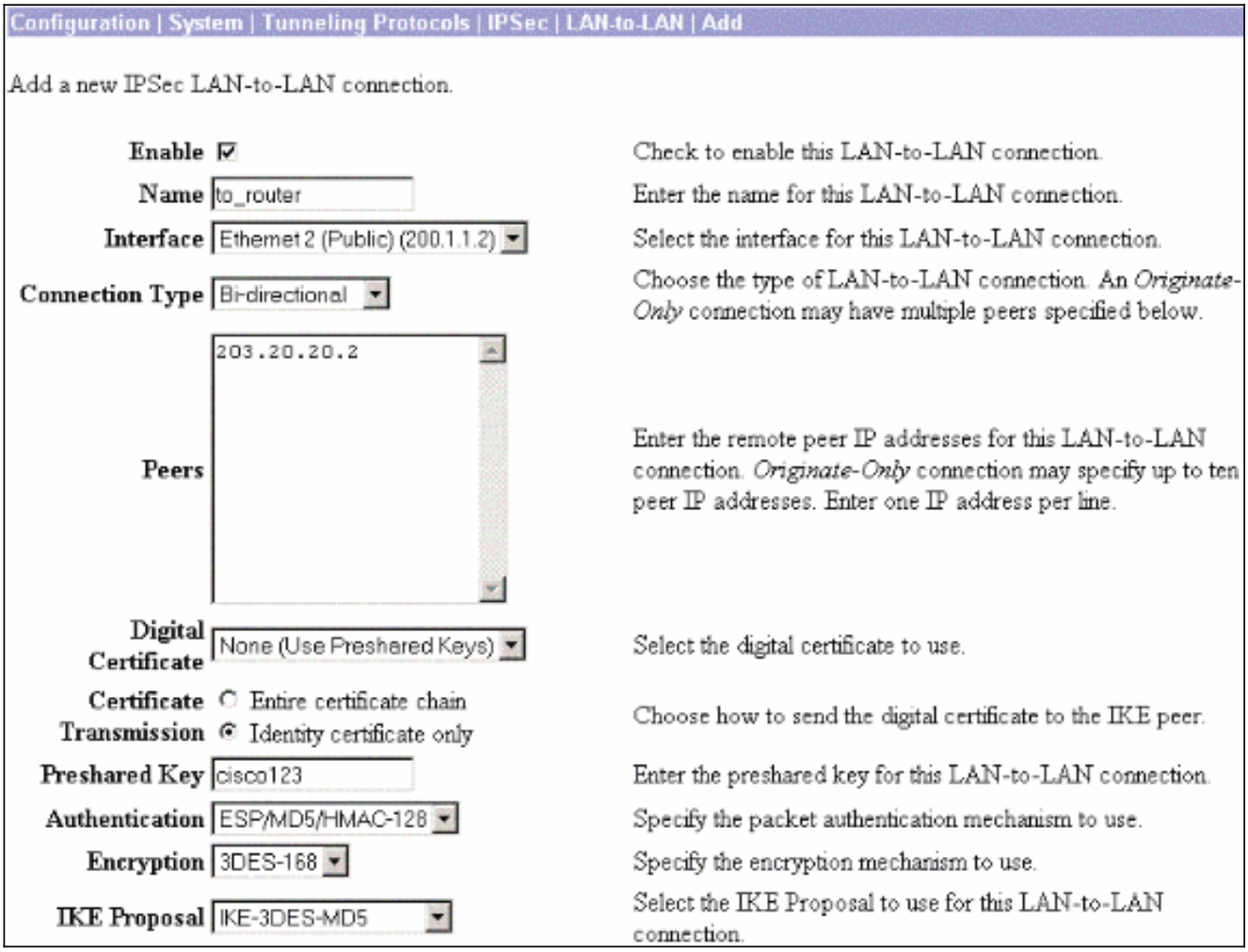
Dies sind die Remote-
Netzwerke:

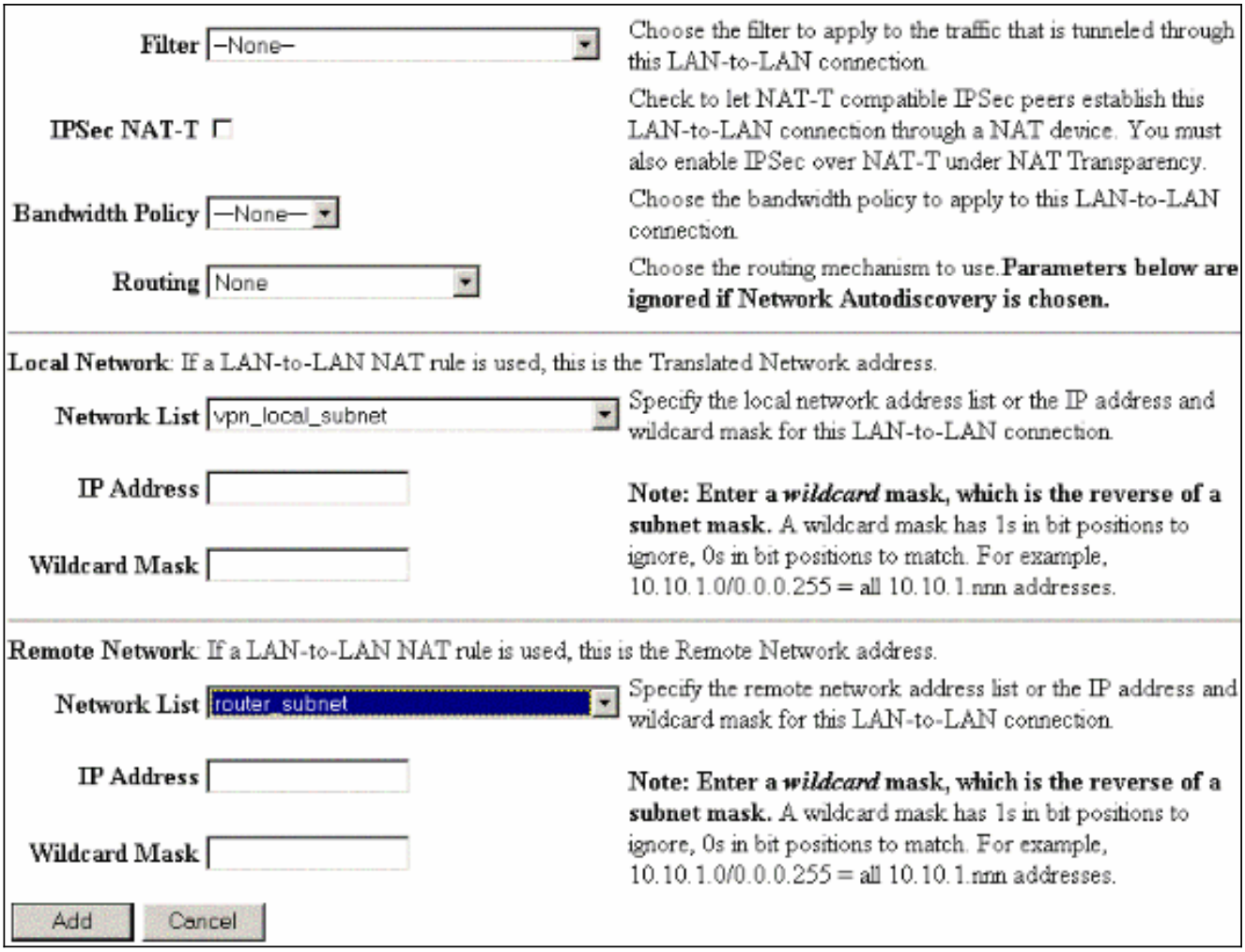


4. Nach Fertigstellung werden die folgenden beiden Netzwerklisten angezeigt:**Hinweis:** Wenn der IPsec-Tunnel nicht angezeigt wird, prüfen Sie, ob der interessante Datenverkehr auf beiden Seiten übereinstimmt. Der interessante Datenverkehr wird durch die Zugriffsliste auf dem Router und den PIX-Feldern definiert. Sie werden durch Netzwerklisten in den VPN Concentrators
definiert.

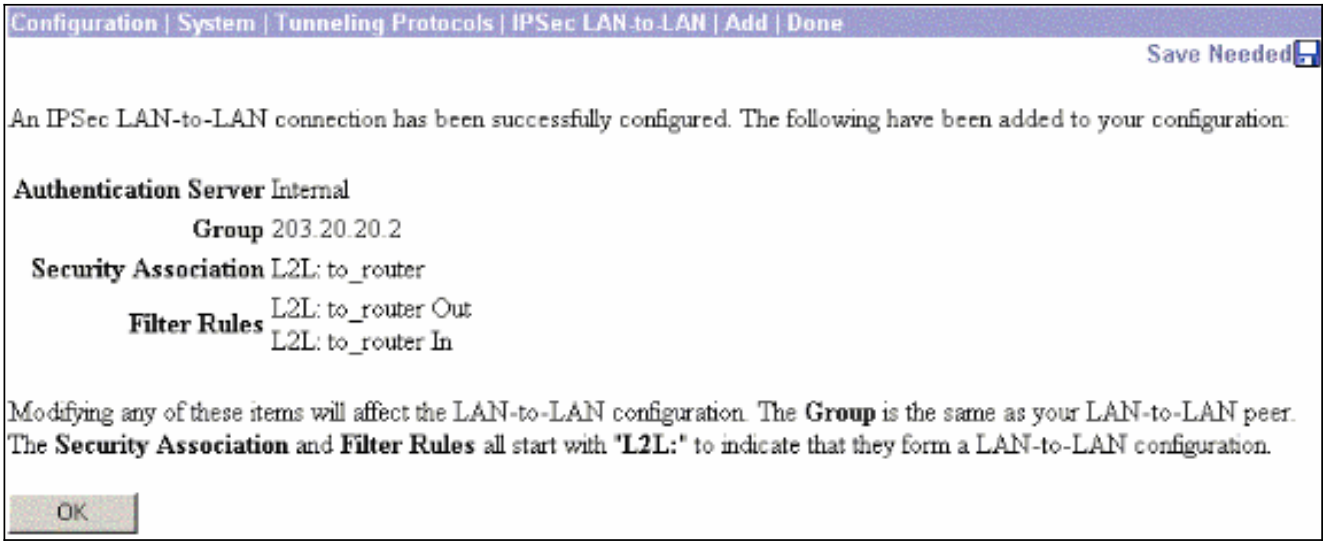


5. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** aus, und definieren Sie den LAN-to-LAN-Tunnel.

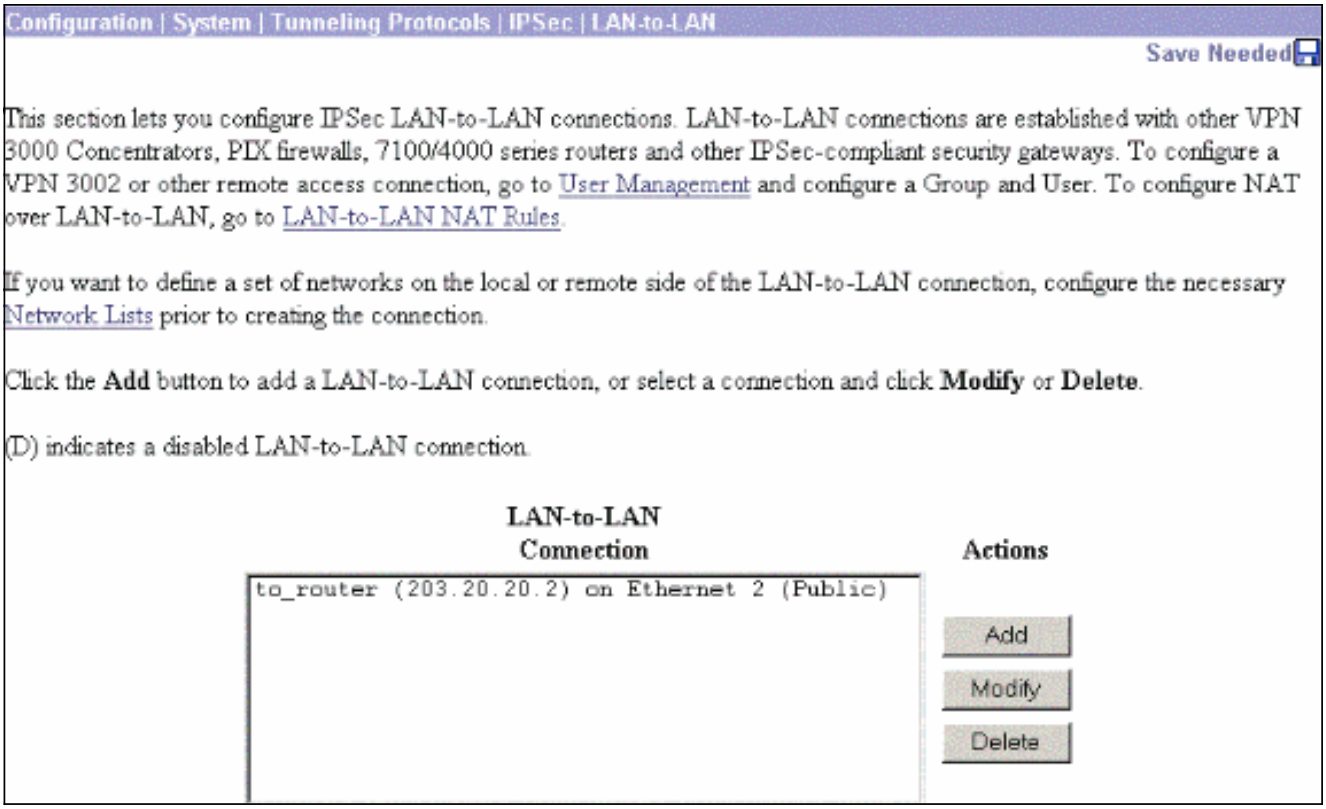




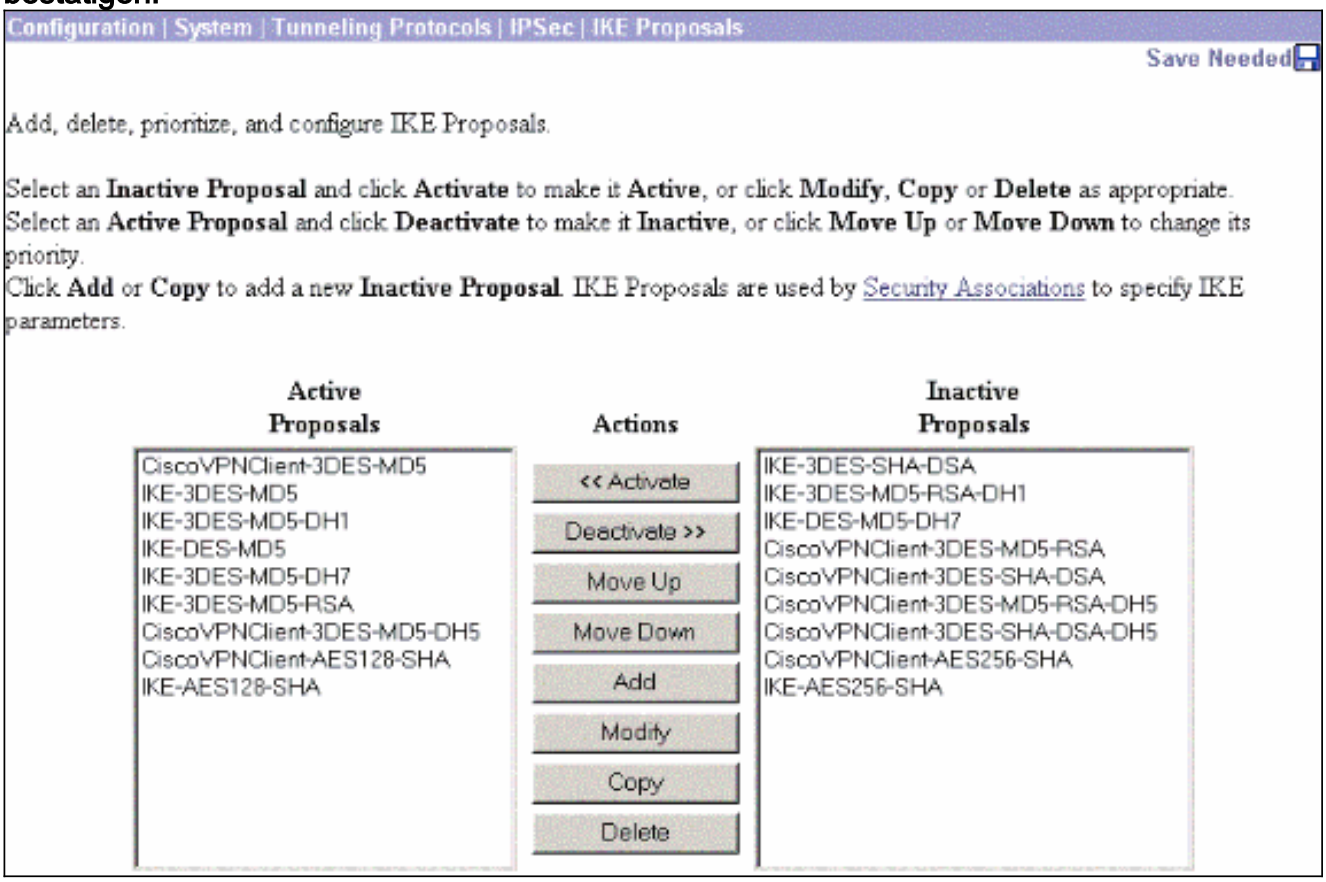
6. Wenn Sie auf **Apply** klicken, wird dieses Fenster mit der anderen Konfiguration angezeigt, die automatisch als Ergebnis der LAN-zu-LAN-Tunnelkonfiguration erstellt wird.



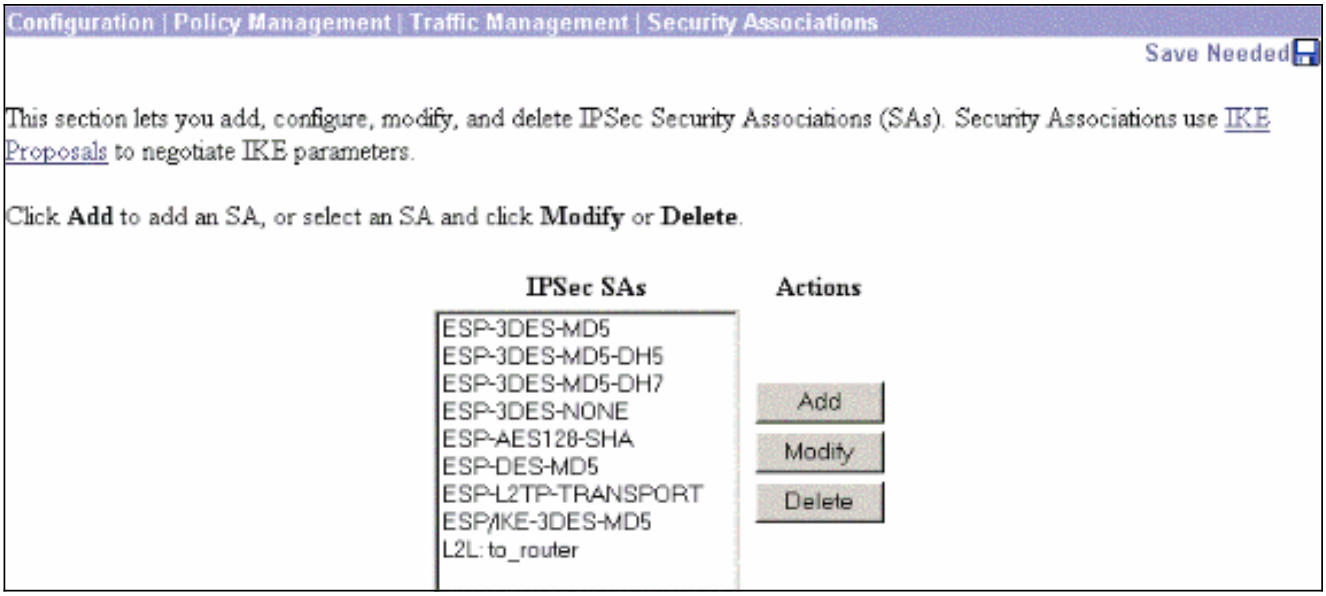
Die zuvor erstellten LAN-to-LAN IPsec-Parameter können unter **Configuration** > **System** > **Tunneling** Protocols > **IPSec LAN-to-LAN** angezeigt oder geändert werden.



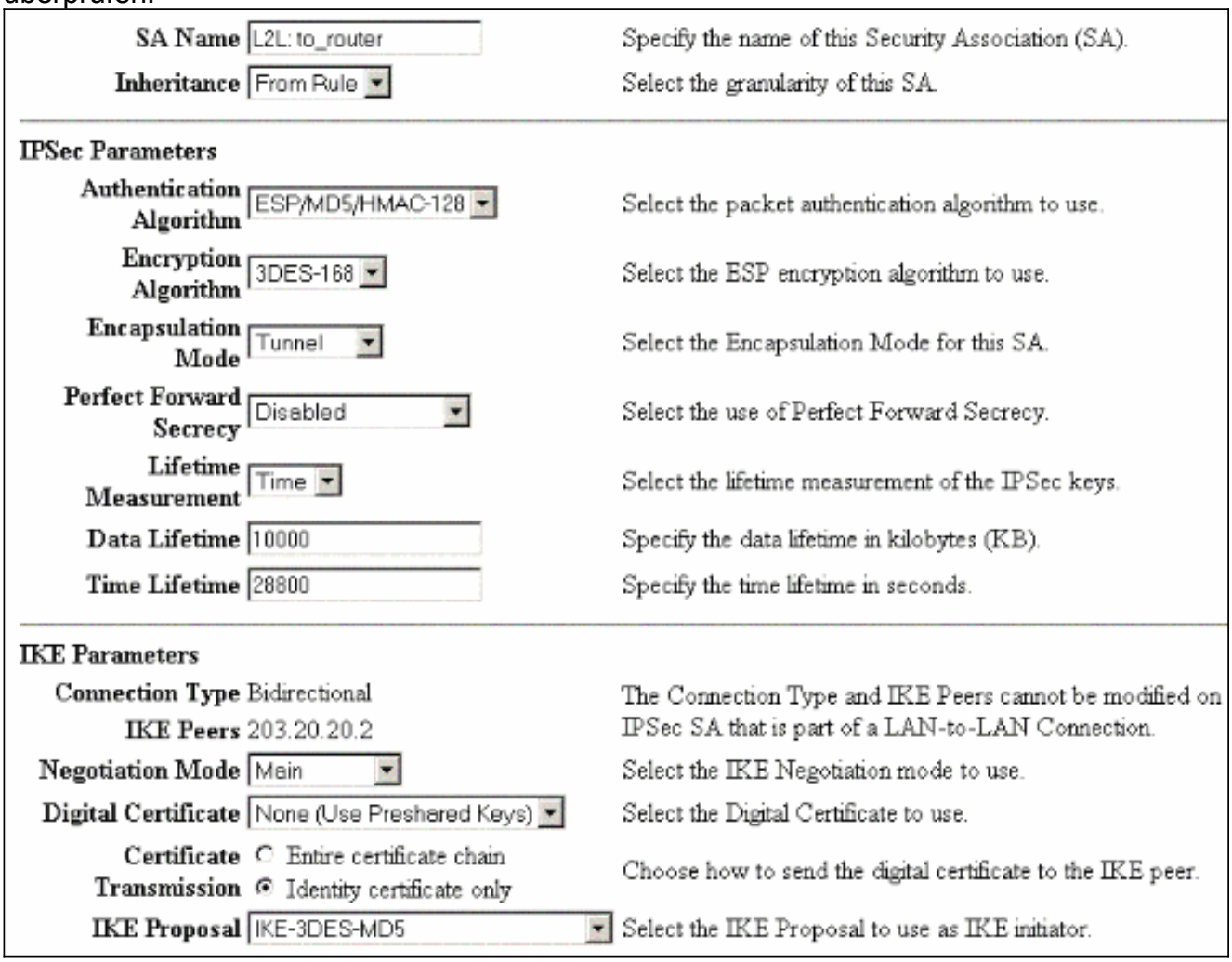
7. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec > IKE-Vorschläge aus, um das aktive IKE-Angebot zu bestätigen.**



8. Wählen Sie **Configuration > Policy Management > Traffic Management > Security Associations (Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Sicherheitszuordnungen**, um die Liste der Sicherheitszuordnungen anzuzeigen.



9. Klicken Sie auf den Namen der Sicherheitszuordnung, und klicken Sie dann auf **Ändern**, um die Sicherheitszuordnungen zu überprüfen.



Überprüfen

In diesem Abschnitt werden die in dieser Konfiguration verwendeten **show**-Befehle aufgelistet.

Auf dem Router

Dieser Abschnitt enthält Informationen zur Bestätigung, dass 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 ipsec sa**: Zeigt die von aktuellen Sicherheitszuordnungen verwendeten Einstellungen.
- **show crypto isakmp sa** - Zeigt alle aktuellen Internet Key Exchange Security Associations in einem Peer an.
- **show crypto engine connection active** - Zeigt die aktuell aktiven verschlüsselten Sitzungsverbindungen für alle Krypto Engines an.

Sie können das IOS Command Lookup Tool (nur registrierte Kunden) verwenden, um weitere Informationen zu bestimmten Befehlen anzuzeigen.

Im VPN Concentrator

Wählen Sie **Configuration > System > Events > Classes > Modify, um die Protokollierung zu aktivieren.** Diese Optionen sind verfügbar:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Schweregrad des Protokolls = 1-13

Schweregrad der Konsole = 1-3

Wählen Sie **Monitoring > Event Log (Ereignisprotokoll)** aus, um das Ereignisprotokoll abzurufen.

Fehlerbehebung

Auf dem Router

Weitere Informationen zu Debug-Befehlen finden Sie unter Wichtige Informationen, bevor Sie Debugbefehle ausführen.

- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an.
- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.

Problem - Der Tunnel kann nicht initiiert werden.

Fehlermeldung

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
```

```
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Lösung

Gehen Sie wie folgt vor, um die gewünschte Anzahl gleichzeitiger Anmeldungen zu konfigurieren oder die gleichzeitigen Anmeldungen für diese SA auf 5 festzulegen:

Gehen Sie zu **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins**, und ändern Sie die Anzahl der Anmeldungen in 5.

PFS

Bei IPsec-Verhandlungen stellt Perfect Forward Secrecy (PFS) sicher, dass jeder neue kryptografische Schlüssel nicht mit einem vorherigen Schlüssel in Beziehung steht. Aktivieren oder deaktivieren Sie PFS auf beiden Tunnel-Peers. Andernfalls wird der LAN-to-LAN (L2L)-IPsec-Tunnel nicht in Routern eingerichtet.

Um anzugeben, dass IPsec PFS anfordern soll, wenn neue Sicherheitszuordnungen für diesen Crypto Map-Eintrag angefordert werden oder dass IPsec PFS erfordert, wenn sie Anforderungen für neue Sicherheitszuordnungen empfängt, verwenden Sie den **set pfs-**Befehl im Konfigurationsmodus "crypto map". Um anzugeben, dass IPsec kein PFS anfordern soll, verwenden Sie die **no**-Form dieses Befehls.

```
set pfs [group1 | group2]
no set pfs
```

Für den Befehl **set pfs**:

- *group1* - Gibt an, dass IPsec die 768-Bit-Diffie-Hellman-Primmodulusgruppe verwenden soll, wenn der neue Diffie-Hellman-Austausch durchgeführt wird.
- *group2* - Gibt an, dass IPsec die 1024-Bit-Diffie-Hellman-Primmodulusgruppe verwenden soll, wenn der neue Diffie-Hellman-Austausch durchgeführt wird.

PFS wird standardmäßig nicht angefordert. Wenn mit diesem Befehl keine Gruppe angegeben wird, **wird *group1* als** Standardwert verwendet.

Beispiel:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Weitere Informationen zum Befehl **set pfs** finden Sie in der Cisco IOS Security Command Reference.

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Cisco VPN Concentrators der Serie 3000
- Cisco VPN 3002 Hardware-Clients

- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems