

Konfigurieren des Cisco VPN 300 Concentrator für einen Cisco Router

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfiguration des VPN-Concentrators](#)

[Überprüfen](#)

[Auf dem Router](#)

[Im VPN Concentrator](#)

[Fehlerbehebung](#)

[Auf dem Router](#)

[Problem - Der Tunnel kann nicht initiiert werden.](#)

[PFS](#)

[Zugehörige Informationen](#)

[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)**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).

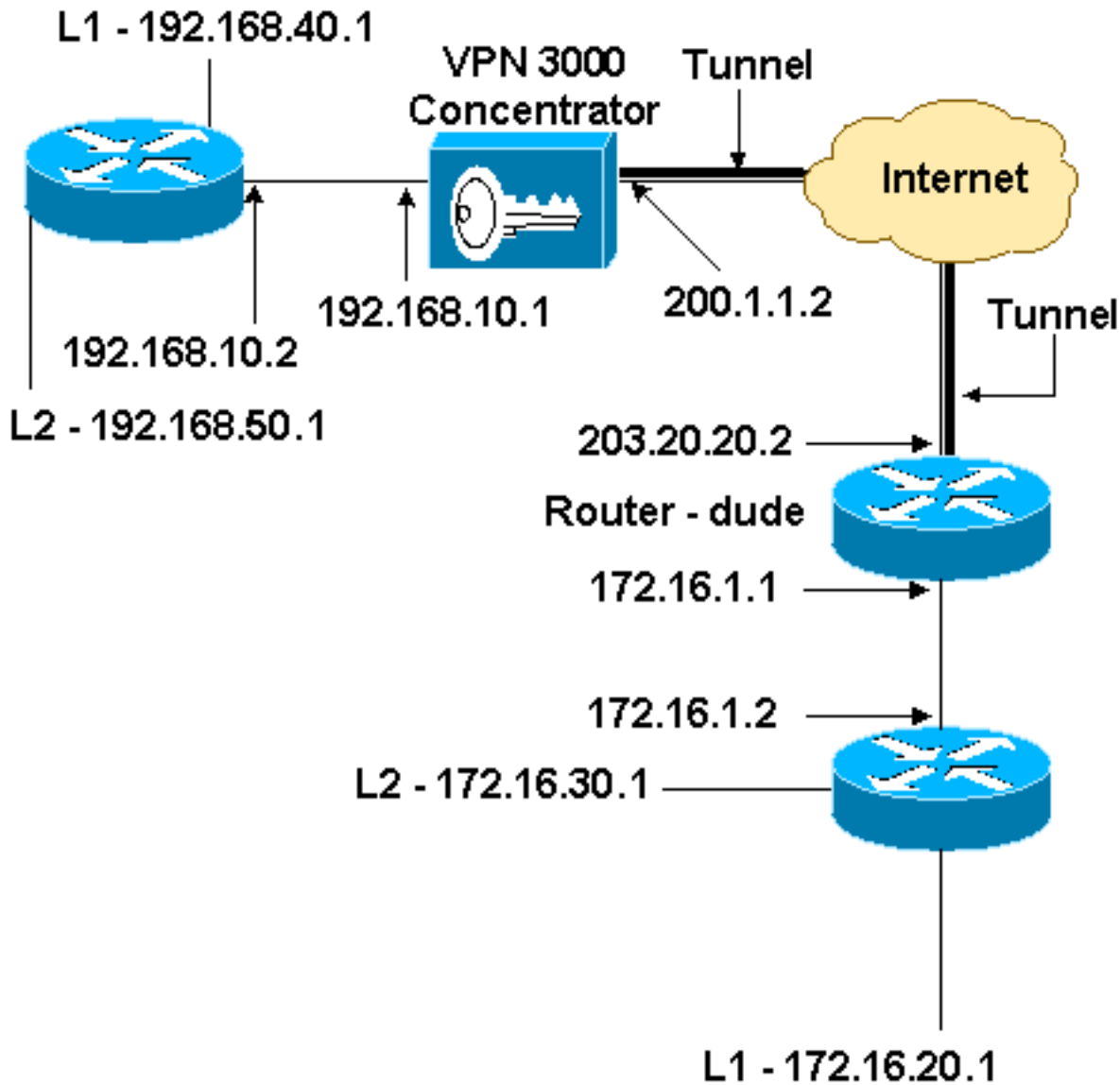
[Konfigurieren](#)

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.

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supplies](#)

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**.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

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:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
192.168.10.0/0.0.0.255
192.168.40.0/0.0.0.255
192.168.50.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Apply Cancel Generate Local List

Dies sind die Remote-Netzwerke:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Apply Cancel Generate Local List

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.

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

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

Add a new IPSec LAN-to-LAN connection.

<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid black; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
--	--

Filter	<input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T	<input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy	<input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	<input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.		
Network List	<input type="text" value="vpn_local_subnet"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.		
Network List	<input type="text" value="router_subnet"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

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.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

```

Authentication Server Internal
  Group 203.20.20.2
  Security Association L2L: to_router
    Filter Rules L2L: to_router Out
                 L2L: to_router In

```

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

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

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN Save Needed

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary [Network Lists](#) prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN Connection	Actions
to_router (203.20.20.2) on Ethernet 2 (Public)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

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

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="<< Activate"/> <input type="button" value="Deactivate >>"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

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

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPsec SAs	Actions
ESP-3DES-MD5	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	
L2L: to_router	

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

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPsec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPsec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	<input type="text" value="Bidirectional"/>	The Connection Type and IKE Peers cannot be modified on IPsec SA that is part of a LAN-to-LAN Connection.
IKE Peers	<input type="text" value="203.20.20.2"/>	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

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

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 > Simultaneous 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](#)