LAN-to-LAN IPsec-Tunnel zwischen einem Cisco VPN 3000-Concentrator und Router mit AES-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird die Konfiguration eines IPsec-Tunnels zwischen einem Cisco VPN 3000-Concentrator und einem Cisco Router mit Advanced Encryption Standard (AES) als Verschlüsselungsalgorithmus erläutert.

AES ist eine neue Publikation des Federal Information Processing Standard (FIPS), die vom National Institute of Standards and Technology (NIST) erstellt wurde und als Verschlüsselungsmethode verwendet wird. Dieser Standard legt einen symmetrischen AES-Verschlüsselungsalgorithmus fest, der den DES (Data Encryption Standard) als Datenschutztransformation sowohl für IPsec als auch für Internet Key Exchange (IKE) ersetzt. AES verfügt über drei verschiedene Schlüssellängen, eine 128-Bit-Taste (Standard), eine 192-Bit-Taste und eine 256-Bit-Taste. Die AES-Funktion in Cisco IOS® bietet IPsec Unterstützung für den neuen Verschlüsselungsstandard AES, mit dem Cipher Block Chaining (CBC) Mode.

Weitere Informationen zu AES finden Sie auf der NIST Computer Security Resource Center-Website .

Weitere Informationen zur Konfiguration des LAN-to-LAN-Tunnels zwischen dem Cisco VPN

3000-Konzentrator und der PIX-Firewall finden Sie im Konfigurationsbeispiel für den LAN-to-LAN-Tunnel zwischen einem VPN 3000-Concentrator und der PIX-Firewall.

Weitere Informationen zu PIX-Softwareversion 7.1 finden Sie unter Konfigurationsbeispiel des IPsec-Tunnels zwischen PIX 7.x und VPN 3000 Concentrator.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert ein grundlegendes Verständnis des IPsec-Protokolls. Weitere Informationen zu IPsec finden Sie unter Einführung in die IPSec-Verschlüsselung.

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

- **Routeranforderungen** - Die AES-Funktion wurde in Version 12.2(13)T der Cisco IOS-Software eingeführt. Um AES zu aktivieren, muss der Router IPsec unterstützen und ein IOS-Image mit langen Tasten "k9" (Subsystem "k9") ausführen.**Hinweis:** Hardware-Unterstützung für AES ist auch auf Cisco 2600XM-, 2691-, 3725- und 3745 AES-Acceleration-VPN-Modulen verfügbar. Diese Funktion hat keine Auswirkungen auf die Konfiguration, und das Hardwaremodul wird automatisch ausgewählt, wenn beide verfügbar sind.
- **VPN Concentrator-Anforderungen** - Die Softwareunterstützung für die AES-Funktion wurde in Version 3.6 eingeführt. Der neue erweiterte, skalierbare Verschlüsselungsprozessor (SEP-E) bietet Hardwareunterstützung. Diese Funktion hat keine Auswirkungen auf die Konfiguration.**Hinweis:** In Cisco VPN 300 Concentrator Version 3.6.3 verhandeln Tunnel aufgrund der Cisco Bug-ID CSCdy88797 nicht mit AES (nur registrierte Kunden). Dies wurde in Version 3.6.4 behoben.**Hinweis:** Der Cisco VPN 3000 Concentrator verwendet entweder SEP- oder SEP-E-Module, nicht beide. Installieren Sie nicht beide auf demselben Gerät. Wenn Sie ein SEP-E-Modul auf einem VPN Concentrator installieren, der bereits ein SEP-Modul enthält, deaktiviert der VPN Concentrator das SEP-Modul und verwendet nur das SEP-E-Modul.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Versionen Software und Hardware:

- Cisco Router der Serie 3600 mit Cisco IOS Software, Version 12.3(5)
- Cisco VPN 3060 Concentrator mit Softwareversion 4.0.3

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).

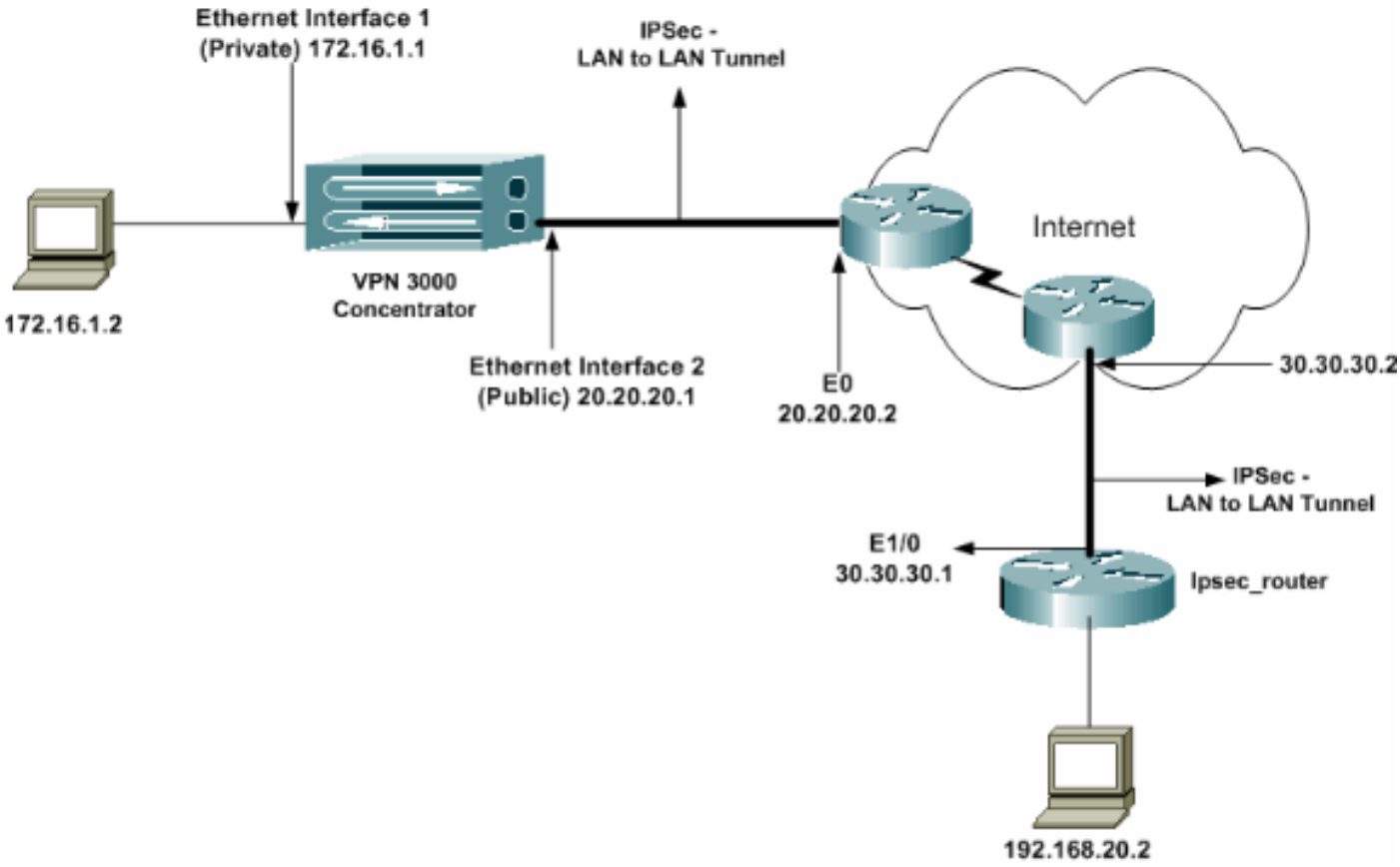
Konfigurieren

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

In diesem Dokument werden folgende Konfigurationen verwendet:

- IPsec-Router
- VPN-Konzentrator

Konfiguration des ipsec_Routers

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
```

```
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
```

```
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Hinweis: Obwohl die ACL-Syntax unverändert ist, unterscheiden sich die Bedeutungen für Krypto-ACLs geringfügig. Bei Krypto-ACLs gibt **permit** an, dass übereinstimmende Pakete verschlüsselt werden sollen, während **deny** angibt, dass übereinstimmende Pakete nicht verschlüsselt werden müssen.

Konfigurieren des VPN-Concentrators

VPN Concentrators sind in den Werkseinstellungen nicht vorprogrammiert und verfügen nicht über IP-Adressen. Sie müssen den Konsolenport verwenden, um die Erstkonfigurationen zu konfigurieren, bei denen es sich um eine menübasierte Befehlszeilenschnittstelle (CLI) handelt. Informationen zur Konfiguration über die Konsole finden Sie unter Konfigurieren von VPN-Concentrators über die Konsole.

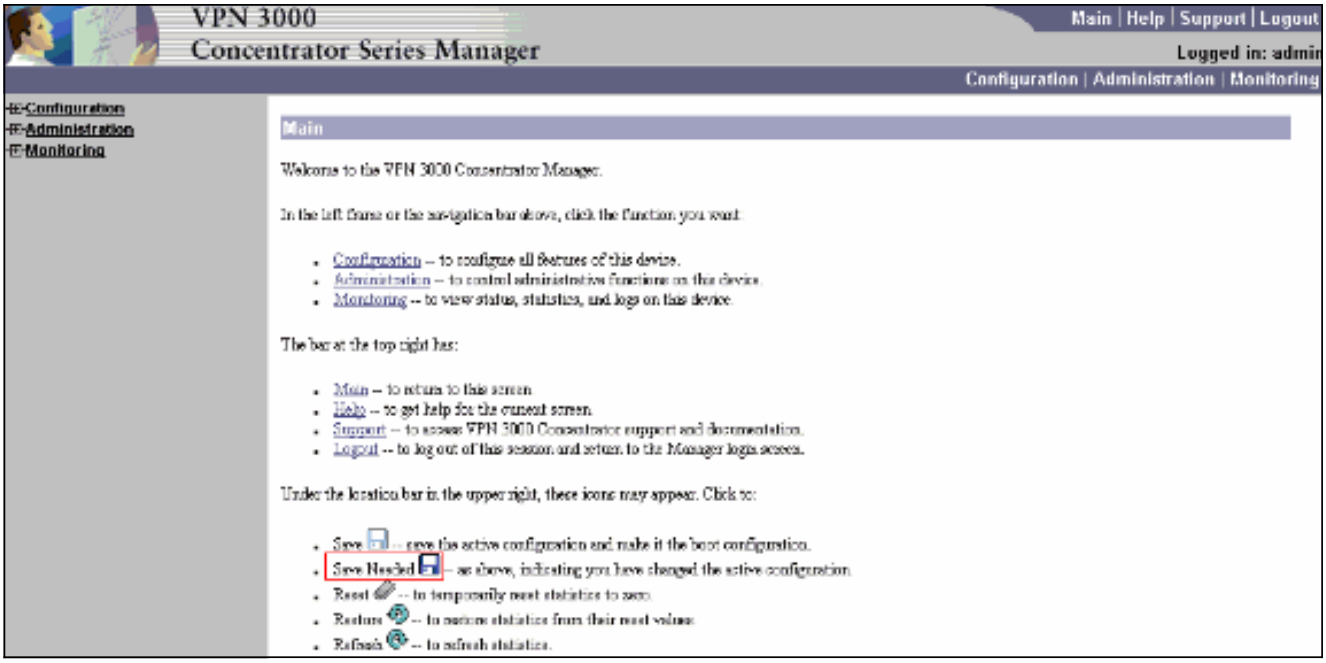
Nachdem die IP-Adresse der Ethernet 1-Schnittstelle (privat) konfiguriert wurde, kann der Rest entweder über die CLI oder die Browserschnittstelle konfiguriert werden. Die Browserschnittstelle unterstützt sowohl HTTP als auch HTTP über Secure Socket Layer (SSL).

Diese Parameter werden über die Konsole konfiguriert:

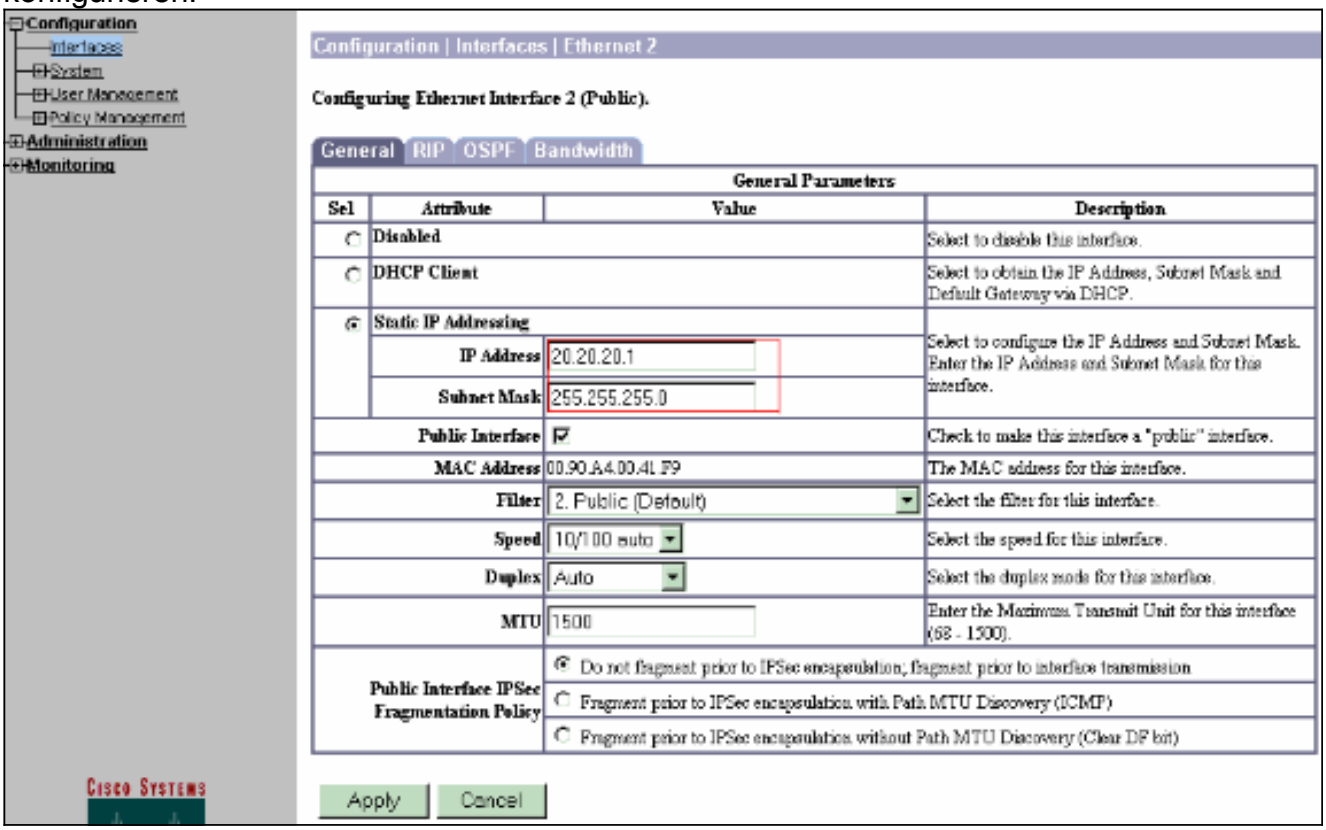
- **Uhrzeit/Datum** - Die korrekte Uhrzeit und das richtige Datum sind sehr wichtig. Sie stellen sicher, dass Protokollierungs- und Abrechnungseinträge korrekt sind und dass das System ein gültiges Sicherheitszertifikat erstellen kann.
- **Ethernet 1 (private) Schnittstelle** - Die IP-Adresse und -Maske (aus unserer Netzwerktopologie 172.16.1.1/24).

Der Zugriff auf den VPN Concentrator erfolgt über einen HTML-Browser aus dem internen Netzwerk. Informationen zur Konfiguration des VPN Concentrator im CLI-Modus finden Sie unter Schnellkonfiguration mit CLI.

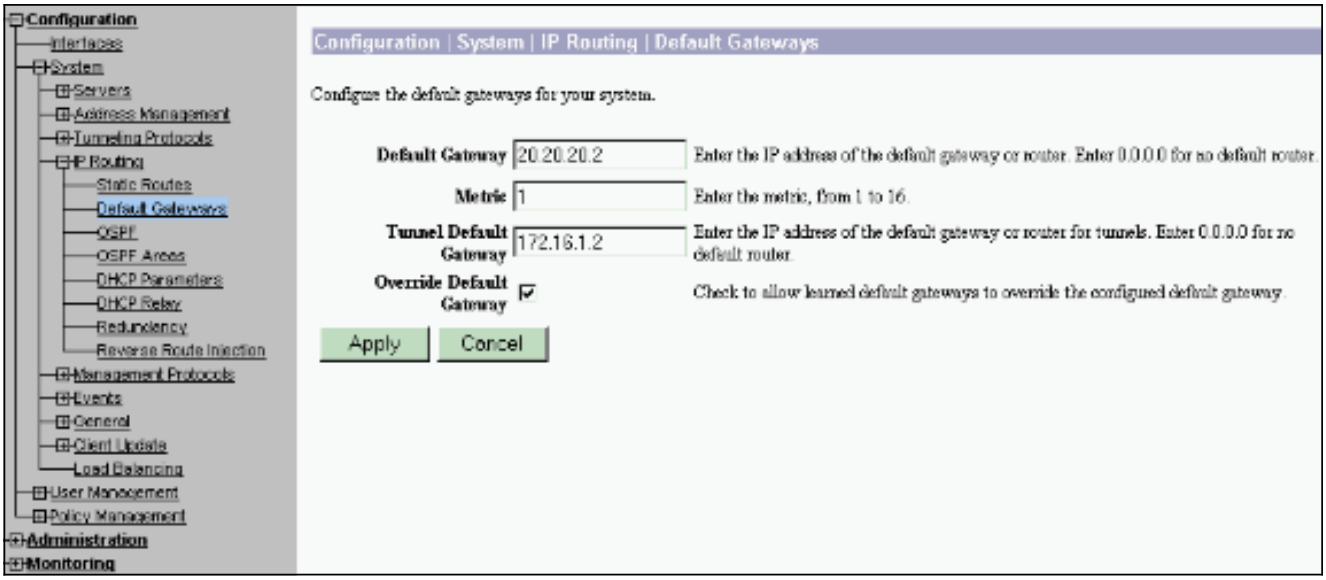
1. Geben Sie die IP-Adresse der privaten Schnittstelle im Webbrowser ein, um die GUI-Schnittstelle zu aktivieren.Klicken Sie auf das Symbol **zum Speichern der** Änderungen im Speicher. Der werksseitig voreingestellte Benutzername und das werkseitige Kennwort sind "admin". Groß- und Kleinschreibung ist zu beachten.



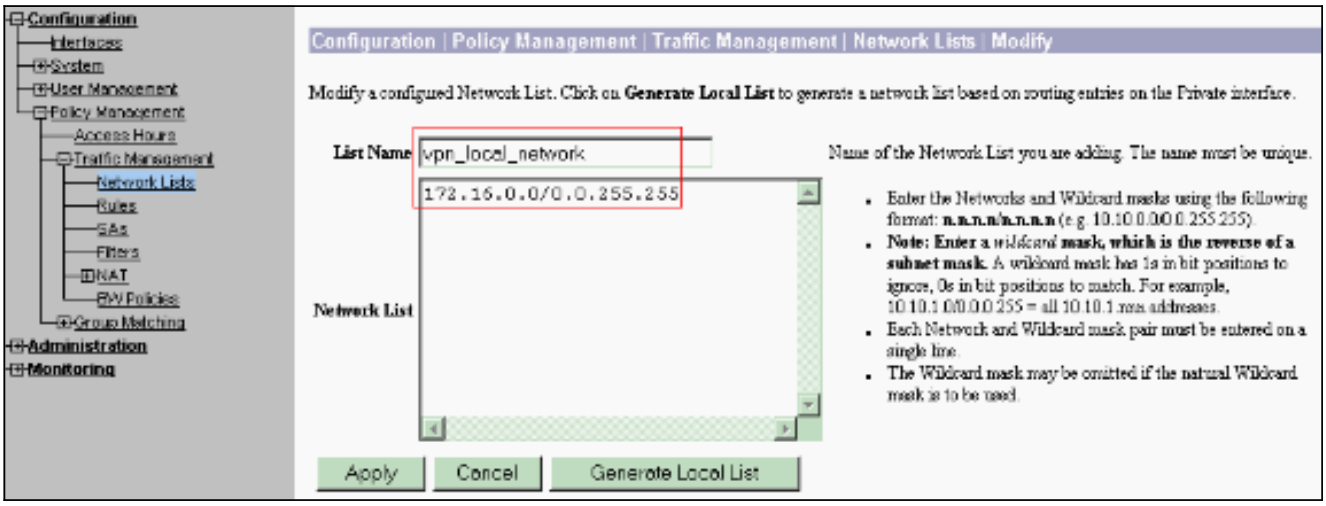
2. Wenn Sie die Benutzeroberfläche aufgerufen haben, wählen Sie **Configuration > Interfaces > Ethernet 2 (Public)** aus, um die Ethernet 2-Schnittstelle zu konfigurieren.



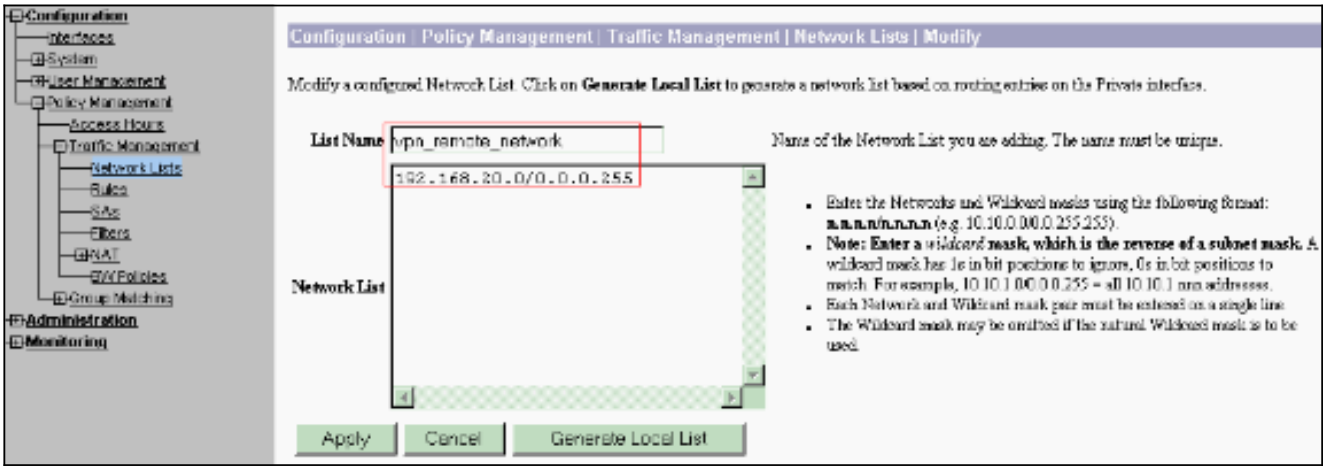
3. Wählen Sie **Configuration > System > IP Routing > Default Gateways** aus, konfigurieren Sie das Standard-Internet-Gateway und das Tunnel-Standardgateway (innen), damit IPsec die anderen Subnetze im privaten Netzwerk erreicht.In diesem Szenario ist im internen Netzwerk nur ein Subnetz
verfügbar.



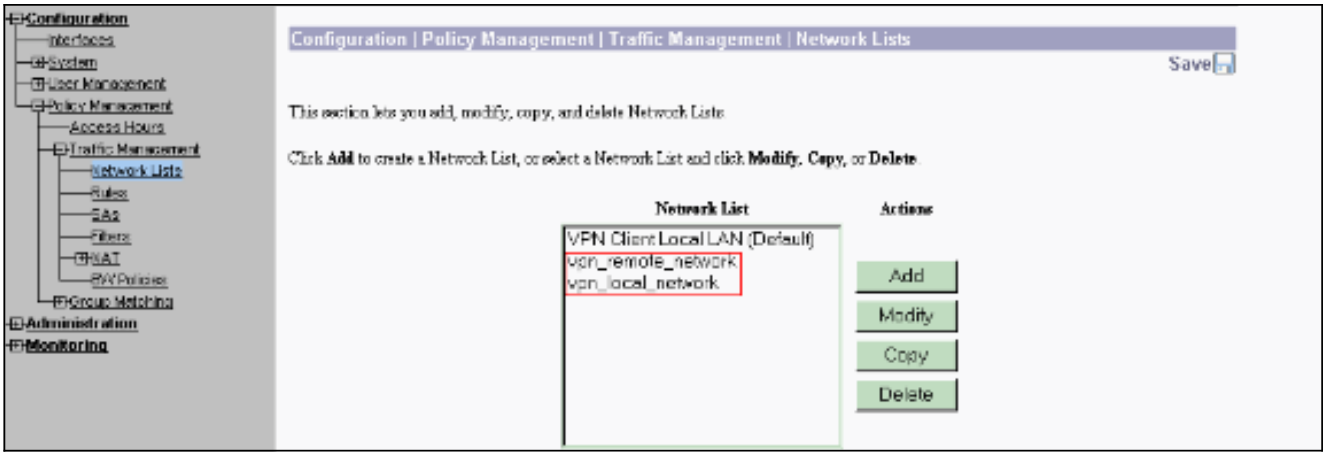
4. Wählen Sie **Configuration > Policy Management > Traffic Management > Network Lists > Add aus, um die Netzwerklisten zur Definition des zu verschlüsselnden Datenverkehrs zu erstellen.**Die in der Liste aufgeführten Netzwerke sind für das Remote-Netzwerk erreichbar. Die Netzwerke in der folgenden Liste sind lokale Netzwerke. Sie können die Liste Lokaler Netzwerke auch automatisch über RIP erstellen, wenn Sie auf **Lokale Liste generieren** klicken.



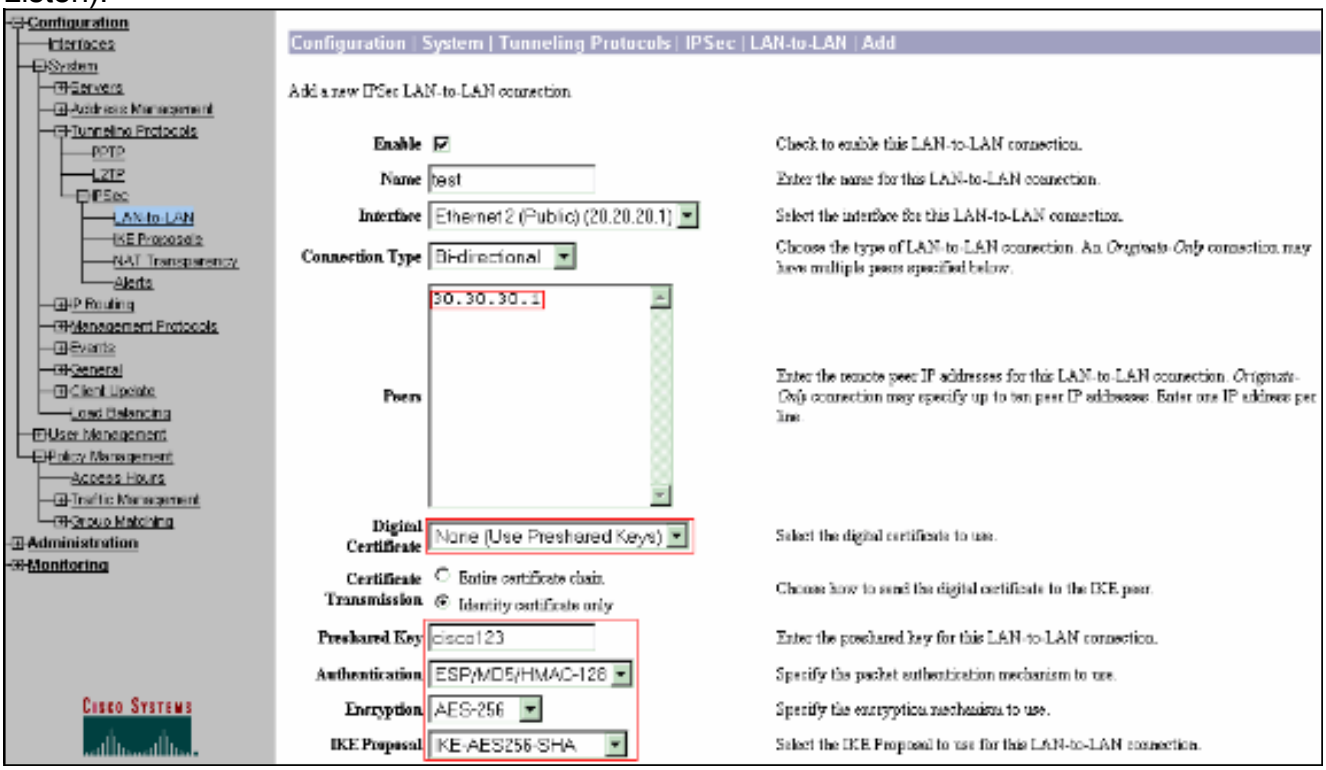
5. Die Netzwerke in dieser Liste sind Remote-Netzwerke und müssen manuell konfiguriert werden. Geben Sie dazu das Netzwerk/den Platzhalter für jedes erreichbare Subnetz ein.

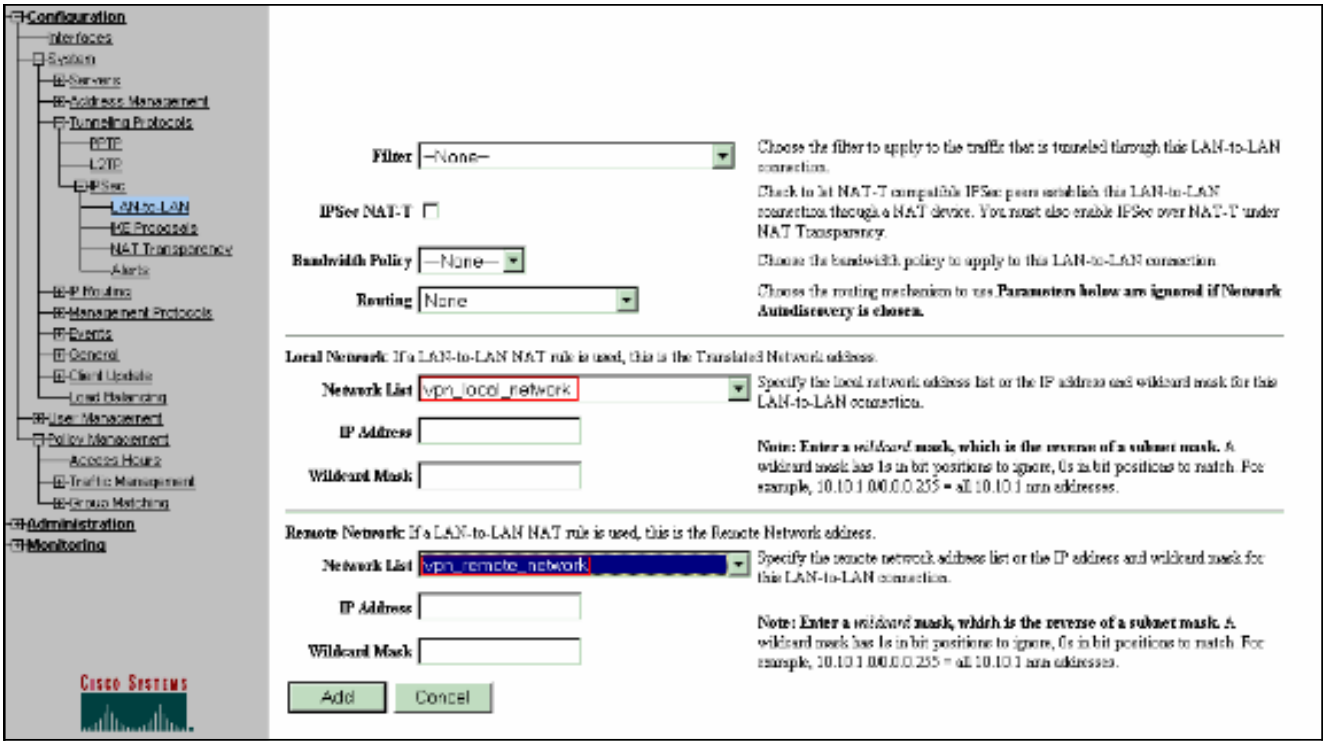


Nach Fertigstellung werden die folgenden beiden Netzwerklisten angezeigt:

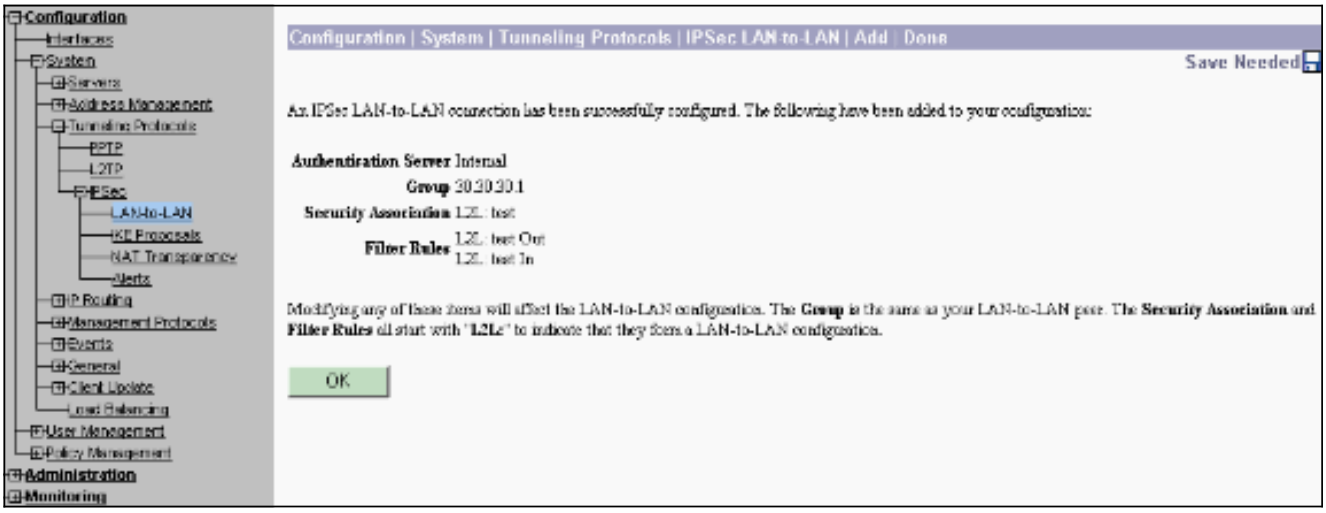


6. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add and define the LAN-to-LAN tunnel.**Dieses Fenster hat drei Bereiche. Der obere Bereich dient zur Anzeige der Netzwerkinformationen, die beiden unteren Abschnitte sind für die Listen "Lokales Netzwerk" und "Remote". Wählen Sie im Abschnitt "Netzwerkinformationen" die AES-Verschlüsselung, den Authentifizierungstyp und das IKE-Angebot aus, und geben Sie den vorinstallierten Schlüssel ein. Zeigen Sie in den unteren Abschnitten auf die bereits erstellten Netzwerklisten (sowohl lokale als auch Remote-Listen).



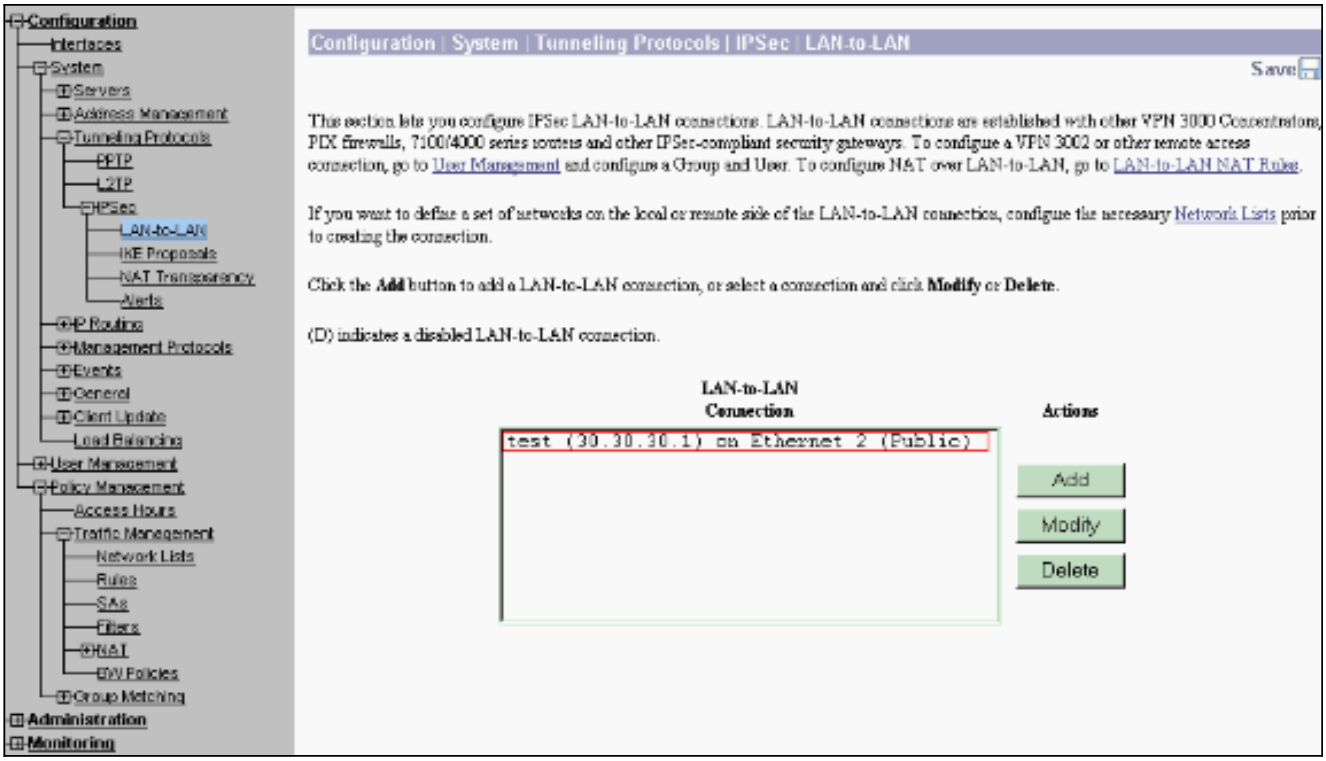


7. Wenn Sie auf **Hinzufügen** klicken, wird Ihnen das Fenster IPSec LAN-to-LAN-Add-Done angezeigt, wenn Ihre Verbindung korrekt ist.Dieses Fenster zeigt eine Zusammenfassung der Tunnelkonfigurationsinformationen. Außerdem werden der Gruppenname, der SA-Name und der Filtername automatisch konfiguriert. Sie können alle Parameter in dieser Tabelle bearbeiten.

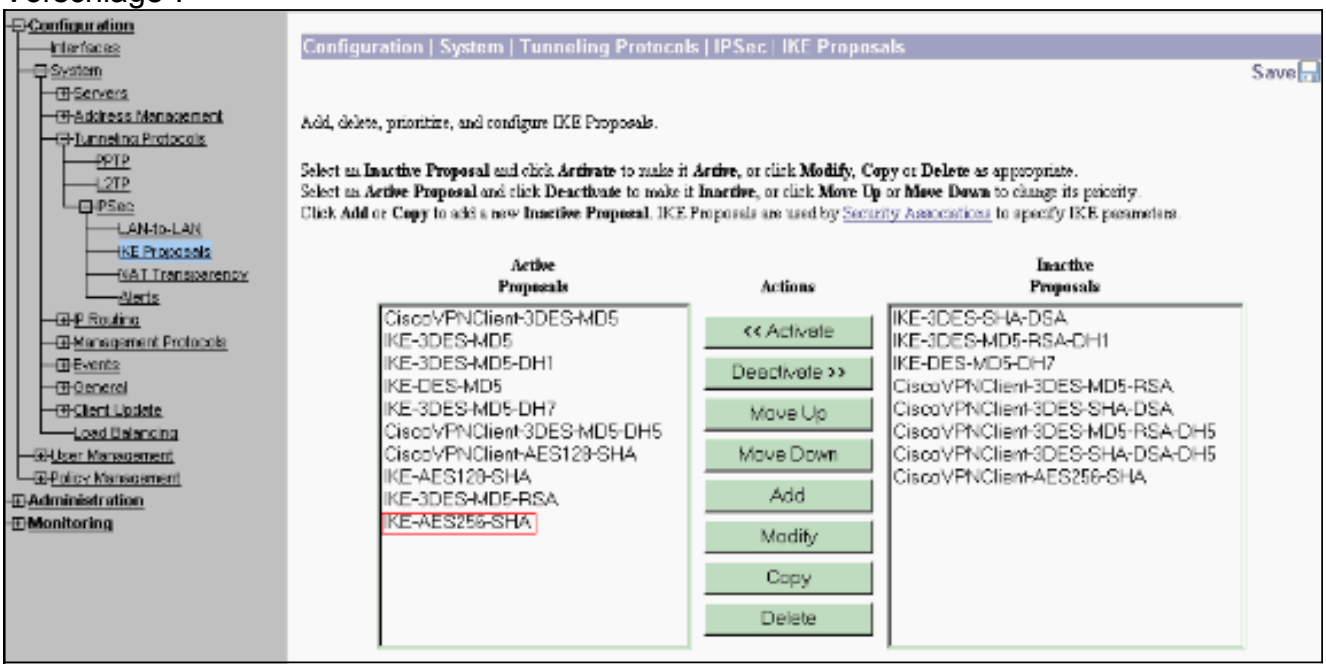


An diesem Punkt wurde der IPsec LAN-to-LAN-Tunnel eingerichtet, und Sie können mit der Arbeit beginnen. Wenn der Tunnel aus irgendeinem Grund nicht funktioniert, können Sie nach Fehlkonfigurationen suchen.

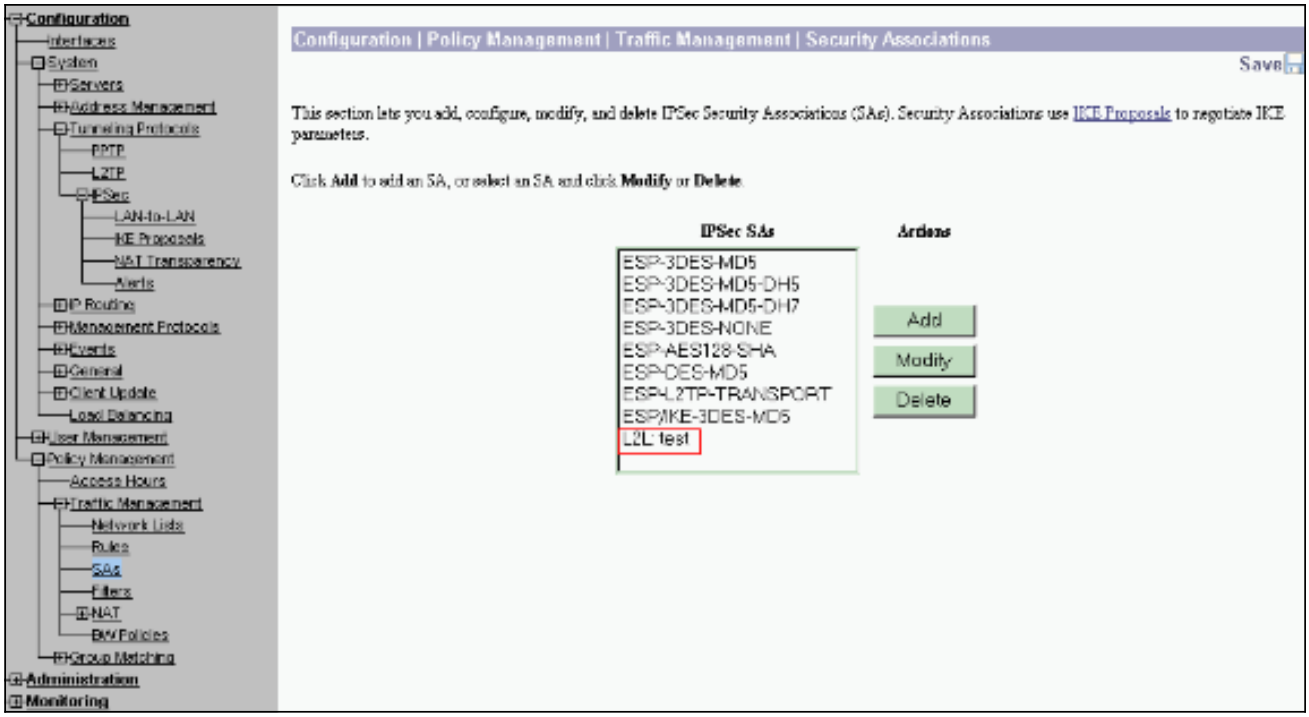
8. Sie können die zuvor erstellten LAN-to-LAN-IPsec-Parameter anzeigen oder ändern, wenn Sie **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** auswählen.In dieser Grafik wird "test" angezeigt, da der Name des Tunnels und die öffentliche Schnittstelle des Remote-Endgeräts gemäß dem Szenario 30.30.30.1
lautet.



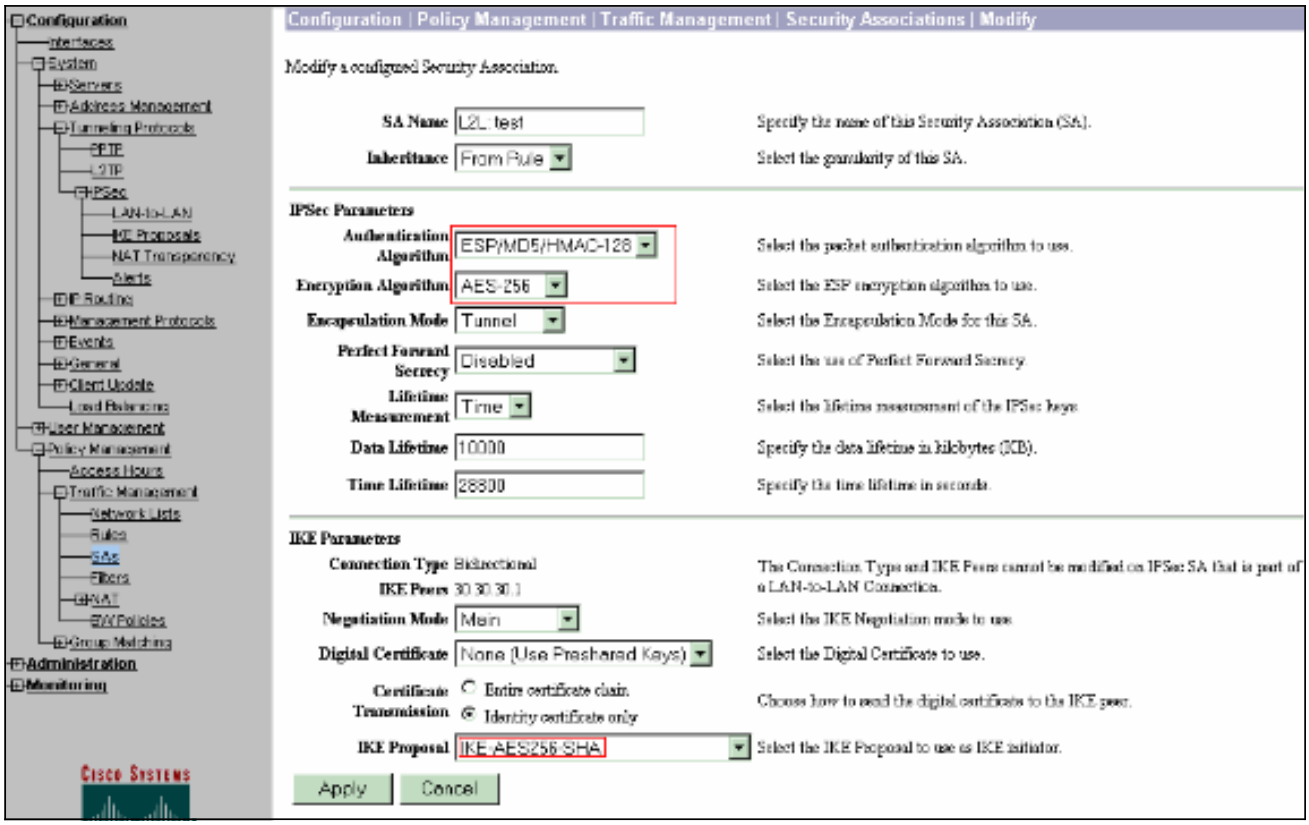
9. Manchmal wird Ihr Tunnel möglicherweise nicht angezeigt, wenn Ihr IKE-Vorschlag in der Liste der inaktiven Vorschläge enthalten ist. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals aus, um das aktive IKE-Angebot zu konfigurieren.**Wenn Ihr IKE-Angebot in der Liste "Inaktive Vorschläge" enthalten ist, können Sie ihn aktivieren, wenn Sie das IKE-Angebot auswählen und auf die Schaltfläche **Aktivieren** klicken. In dieser Grafik befindet sich der ausgewählte Vorschlag "IKE-AES256-SHA" in der Liste "Aktive Vorschläge".



10. Wählen Sie **Configuration > Policy Management > Traffic Management > Security Associations (Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Sicherheitszuordnungen** aus, um zu überprüfen, ob die SA-Parameter korrekt sind.



11. Klicken Sie auf den SA-Namen (in diesem Fall **L2L: Test**), und klicken Sie dann auf **Ändern**, um die SAs zu überprüfen.Wenn einer der Parameter nicht mit der Remote-Peer-Konfiguration übereinstimmt, kann er hier geändert werden.



Überprüfen

Überprüfen der Router-Konfiguration

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto isakmp sa**: Zeigt alle aktuellen IKE-SAs in einem Peer an. Der Status QM_IDLE gibt an, dass die SA mit dem zugehörigen Peer authentifiziert bleibt und für spätere Schnellwechselvorgänge verwendet werden kann. Es ist ruhig.

```
ipsec_router#show crypto isakmp sa

 dst            src           state    conn-id   slot

 20.20.20.1     30.30.30.1    QM_IDLE        1      0
```

- **show crypto ipsec sa** - Zeigt die von aktuellen SAs verwendeten Einstellungen an. Prüfen Sie, ob die Peer-IP-Adressen, die Netzwerke, auf die sowohl die lokalen als auch die Remote-Endgeräte zugreifen können, und das verwendete Transformationssatz verwendet werden. Es gibt zwei ESP-SAs, eine in jede Richtung. Da AH-Transformationssätze verwendet werden, sind sie leer.

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

       Crypto map tag: vpn, local addr. 30.30.30.1

       protected vrf:

        local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

       remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

       current_peer: 20.20.20.1:500

         PERMIT, flags={origin_is_acl,}

        #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

        #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

        #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.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

        path mtu 1500, media mtu 1500

        current outbound spi: 54FA9805

       inbound esp sas:

       spi: 0x4091292(67703442)

        transform: esp-256-aes esp-md5-hmac ,

        in use settings ={Tunnel, }

        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
```

```
 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

inbound ah sas:

inbound pcp sas:

 outbound esp sas:

spi: 0x54FA9805(1425709061)

 transform: esp-256-aes esp-md5-hmac ,

 in use settings ={Tunnel, }

 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

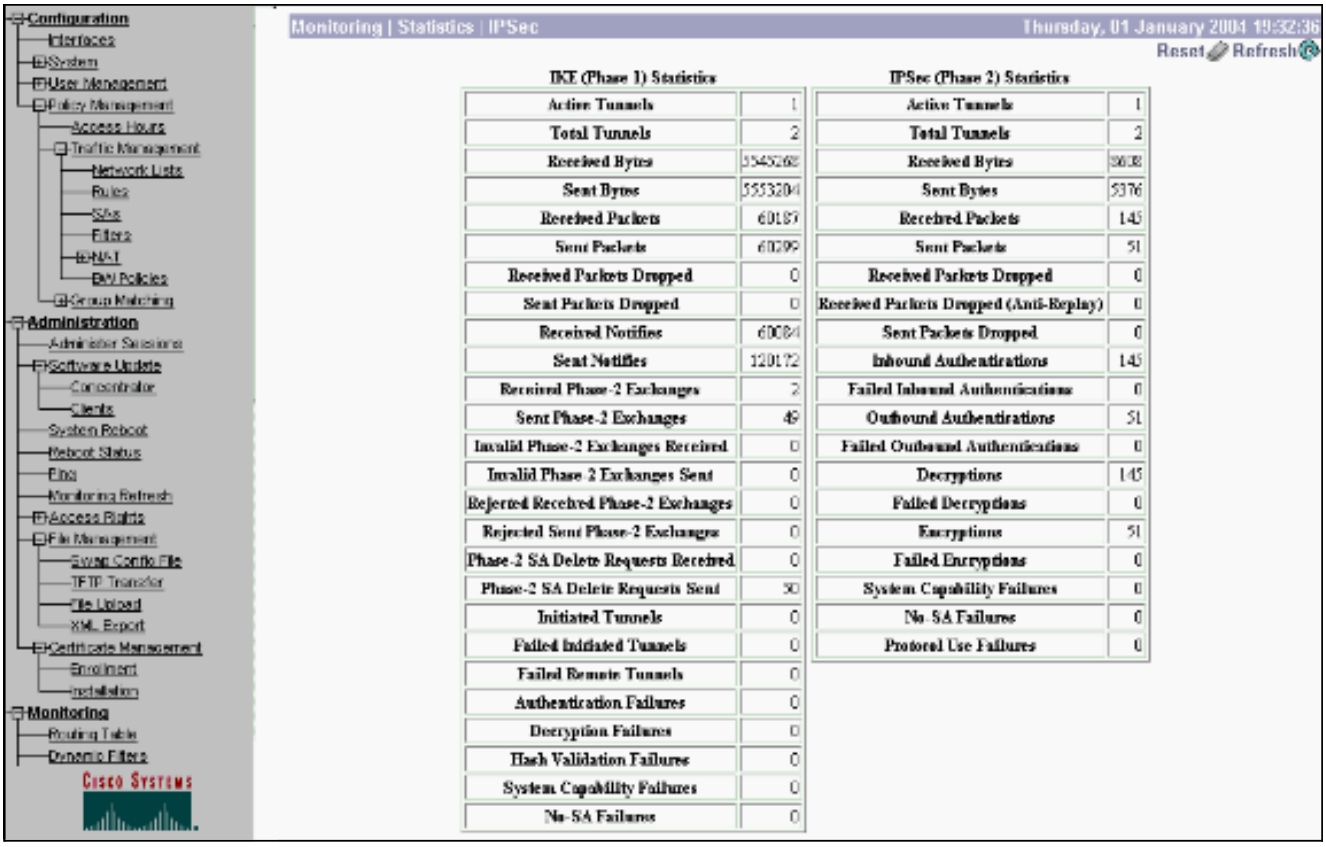
- **show crypto engine connections active** - Zeigt die aktuell aktiven verschlüsselten session connections für all crypto engines an. Jede Verbindungs-ID ist eindeutig. Die Anzahl der verschlüsselten und entschlüsselten Pakete wird in den letzten beiden Spalten angezeigt.

```
ipsec_router#show crypto engine connections active
   ID     Interface     IP-Address   State   Algorithm          Encrypt Decrypt

    1     Ethernet1/0   30.30.30.1   set     HMAC_SHA+AES_256_C       0       0

 2000     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C       0      19

 2001     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C      19       0
```

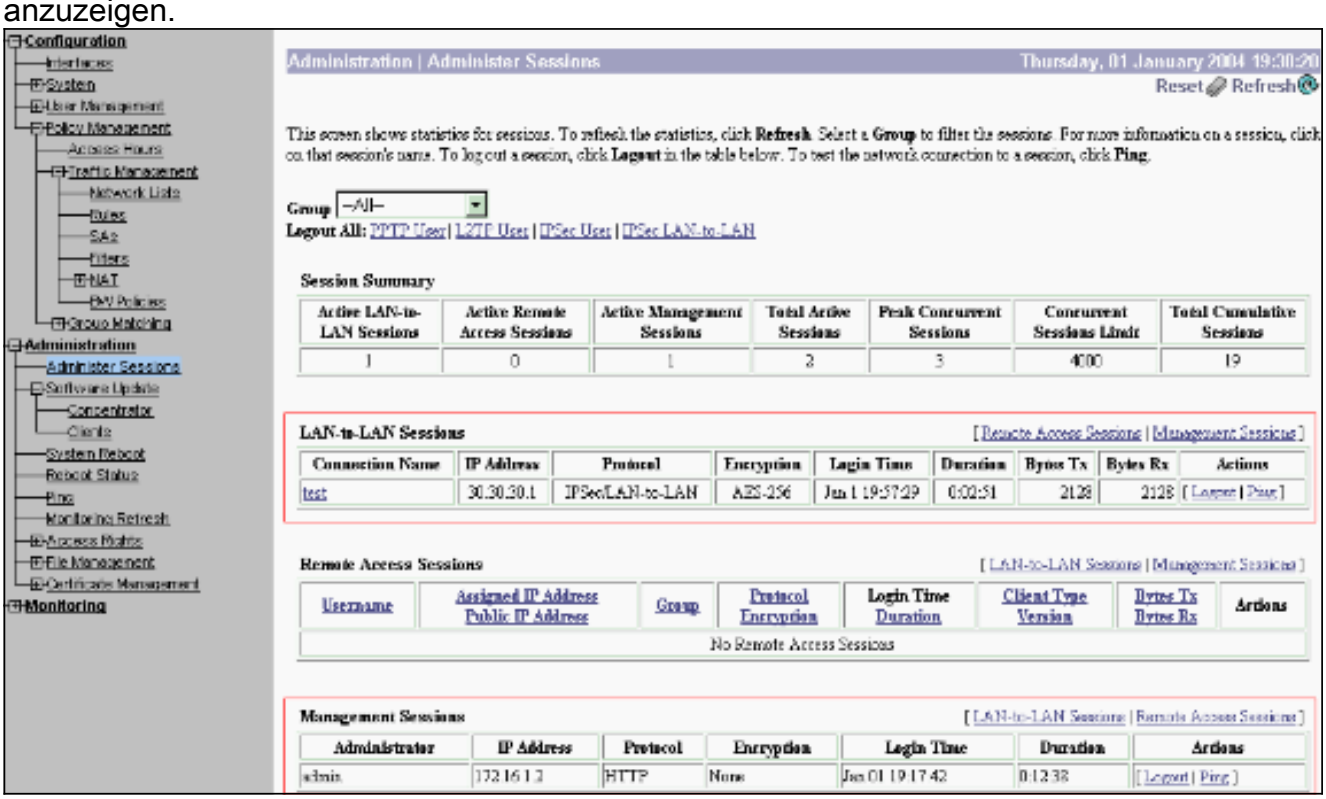
Überprüfen der Konfiguration des VPN Concentrators

Gehen Sie wie folgt vor, um die Konfiguration des VPN-Konzentrators zu überprüfen.

1. Ähnlich wie bei der **Anzeige von crypto ipsec sa** und der **Anzeige von crypto isakmp sa** Befehlen auf Routern können Sie die IPsec- und IKE-Statistiken anzeigen, wenn Sie **Überwachung > Statistics > IPSec auf den VPN-Konzentratoren** auswählen.



2. Ähnlich wie der Befehl **show crypto engine connections active** auf Routern können Sie das Fenster Administration-Sessions im VPN Concentrator verwenden, um die Parameter und Statistiken für alle aktiven IPsec-LAN-to-LAN-Verbindungen oder -Tunnel anzuzeigen.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Fehlerbehebung beim Router

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: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

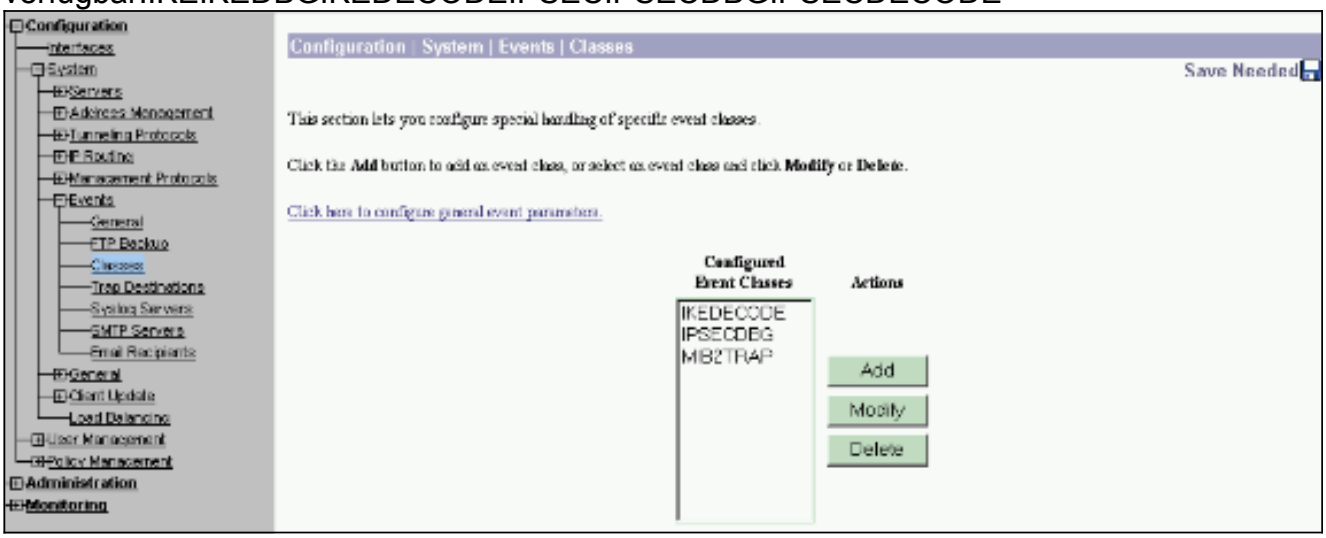
- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an. Die Krypto-Engine ist der eigentliche Mechanismus, der Verschlüsselung und Entschlüsselung durchführt. Eine Krypto-Engine kann Software oder Hardware-Beschleuniger sein.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen (Internet Security Association and Key Management Protocol) der IKE-Phase 1 an.
- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für IKE Phase 2 an.

Weitere Informationen und Beispielausgabe finden Sie unter IPSec-Fehlerbehebung - Understanding and Using **debug** Commands (IPSec-Fehlerbehebung - Understanding and Using **debug** Commands).

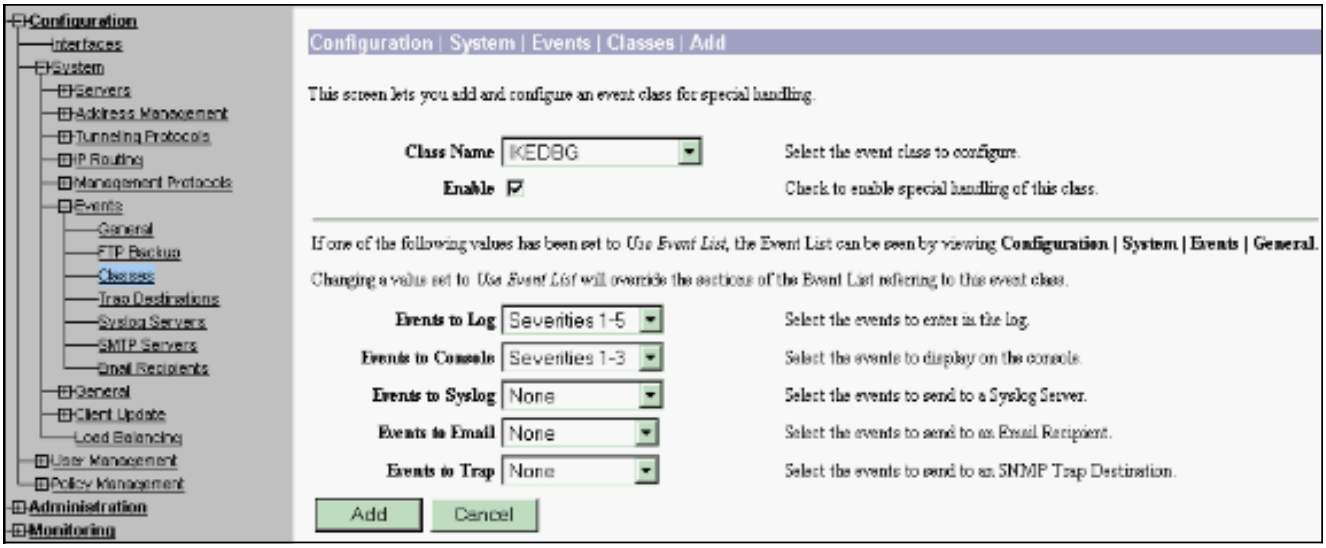
Fehlerbehebung beim VPN Concentrator

Ähnlich wie die **Debugbefehle** auf den Cisco Routern können Sie Ereignisklassen so konfigurieren, dass alle Alarme angezeigt werden.

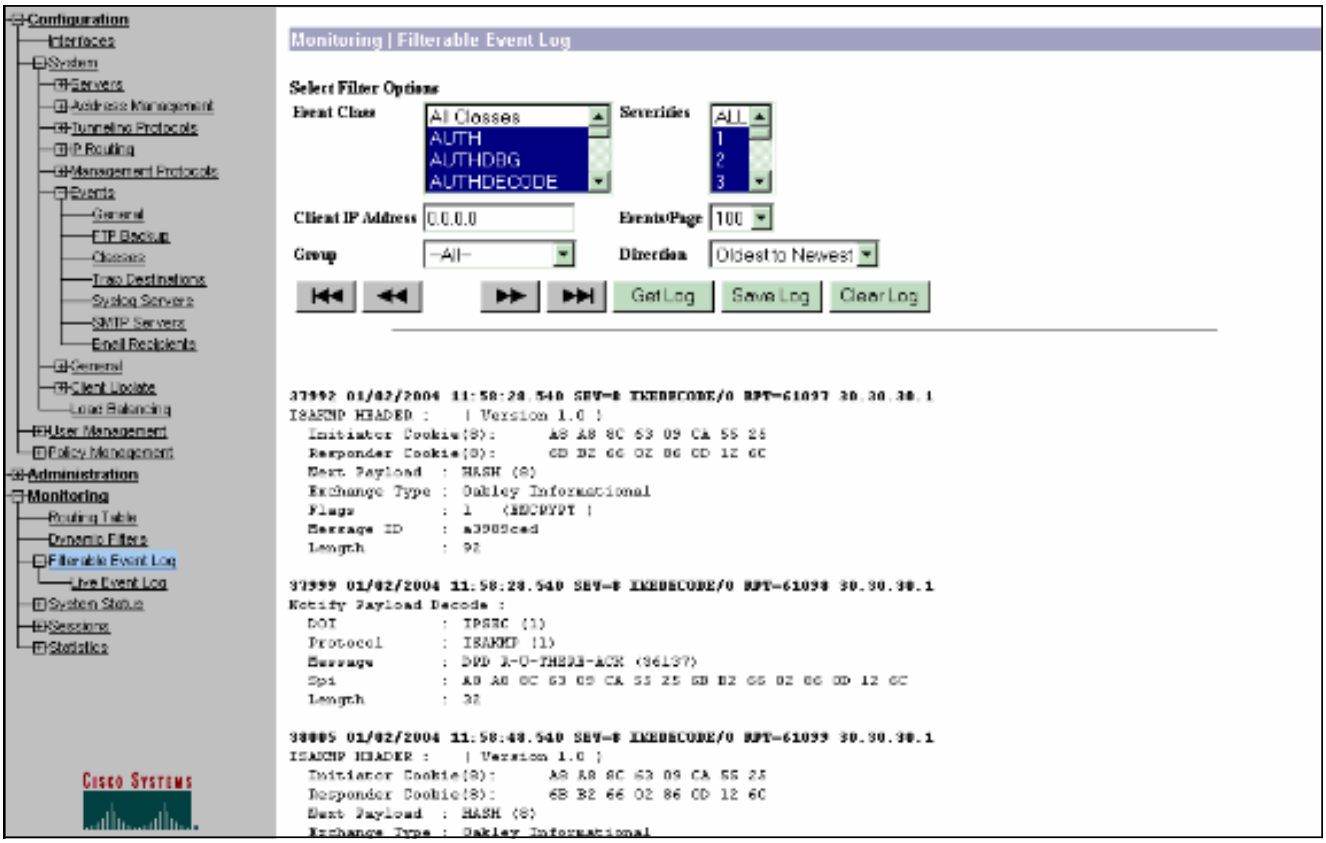
1. Wählen Sie **Configuration > System > Events > Classes > Add aus, um die Protokollierung der Ereignisklassen zu aktivieren.**Diese Klassen sind für IPsec verfügbar:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. Beim Hinzufügen können Sie auch den Schweregrad für jede Klasse auswählen, basierend auf dem Schweregrad, der gesendet wird.Die Alarme können mit einer der folgenden Methoden behandelt werden:Nach ProtokollAuf der Konsole angezeigtGesendet an UNIX Syslog-ServerAls E-Mail gesendetGesendet als Trap an einen SNMP-Server (Simple Network Management
Protocol)



3. Wählen Sie **Monitoring > Filterable Event Log** (**Überwachung > Filterbares Ereignisprotokoll**) aus, um die aktivierten Alarme zu überwachen.



Zugehörige Informationen

- Advanced Encryption Standard (AES)
- DES/3DES/AES-VPN-Verschlüsselungsmodul
- IPSec-Beispielkonfigurationen
- Cisco VPN Client Support-Seite der Serie 3000
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle