在Cisco VPN 3000集中器和路由器之间的LAN到LAN IPSec隧道有AES的配置示例的

目录

简介

本文说明如何将Cisco VPN 3000集中器和带有新一代加密标准(AES)的Cisco路由器之间的IPSec隧道配置为加密算法。

AES是美国标准技术研究所(NIST)新发布的联邦信息处理标准(FIPS)，将用作加密方法。此标准规定AES对称加密算法（替换数据加密标准)需进行保密转换，供IPSec和互联网密钥交换(IKE)使用。AES有三个不同的密钥长度、一个128位密钥(默认值)，一个192位密钥和一个256位密钥。Cisco IOS®中的AES在IPSec中支持新的加密标准AES，同时提供密码链块(CBC)模式。

有关AES的详细信息，请参阅NIST计 算机安全资源中心站点。

有关VPN 3000集中器和PIX防火墙之间的LAN到LAN隧道配置的详细信息，请参阅Cisco VPN 3000集中器和PIX防火墙之间的LAN到LAN IPsec隧道配置示例。

当PIX具有软件版本7.1时，有关详细信息，请参阅PIX 7.x和VPN 3000集中器之间的IPsec隧道配置示例。

先决条件

要求

本文档需要对 IPSec 协议拥有基本的了解。要了解有关 IPsec 的详细信息，请参阅 IPsec 加密简介。

尝试进行此配置之前，请确保满足以下要求：

- **路由器要求** — AES功能在Cisco IOS软件版本12.2(13)T中引入。要启用AES，您的路由器必须支持IPsec并运行带有“k9”长密钥（“k9”子系统）的IOS映像。**注意：**Cisco 2600XM、2691、3725和3745 AES加速VPN模块也提供AES硬件支持。此功能没有配置暗示，并且如果两个都可用，硬件模块自动地选择。
- **VPN集中器要求** — 版本3.6中引入了对AES功能的软件支持。新的增强的可扩展加密处理器(SEP-E)提供了硬件支持。 此功能不涉及配置。**注意：**在Cisco VPN 3000集中器版本3.6.3中，由于Cisco Bug ID CSCdy88797(仅限注册客户)，隧道不会协商到AES。 这已从版本3.6.4中解决。**注意：**Cisco VPN 3000集中器使用SEP或SEP-E模块，而不同时使用这两个模块。请勿在同一设备上同时安装两者。如果您将SEP-E模块安装在包含一个SEP模块的VPN集中器上，那么VPN集中器就禁用SEP模块，只使用SEP-E模块。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Cisco IOS软件版本12.3(5)的Cisco 3600系列路由器
- 带软件版本4.0.3的思科VPN 3060集中器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

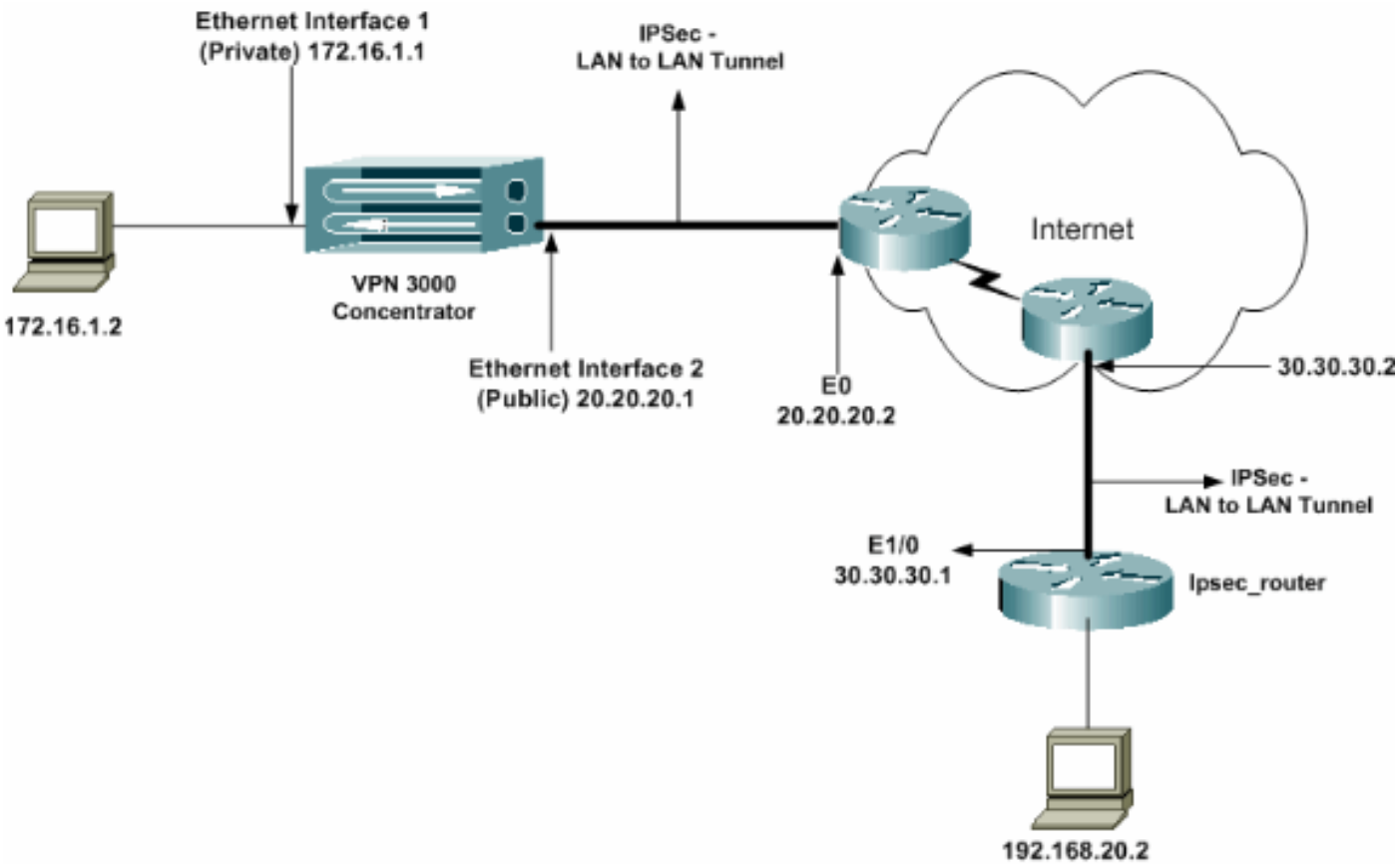
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- IPsec路由器
- VPN 集中器

ipsec_router配置

```
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
```

注意：虽然ACL语法保持不变，但加密ACL的含义稍有不同。在加密ACL中，**permit**指定应加密匹配的数据包，而**deny** 指定不需要加密匹配的数据包。

配置 VPN 集中器

VPN集中器在他们的出厂设置中没有预编程序设置IP地址。您必须使用控制台端口配置基于菜单的命令行界面(CLI)的初始配置。 有关如何通过控制台进行配置的信息，请参阅通过控制台配置 VPN 集中器。

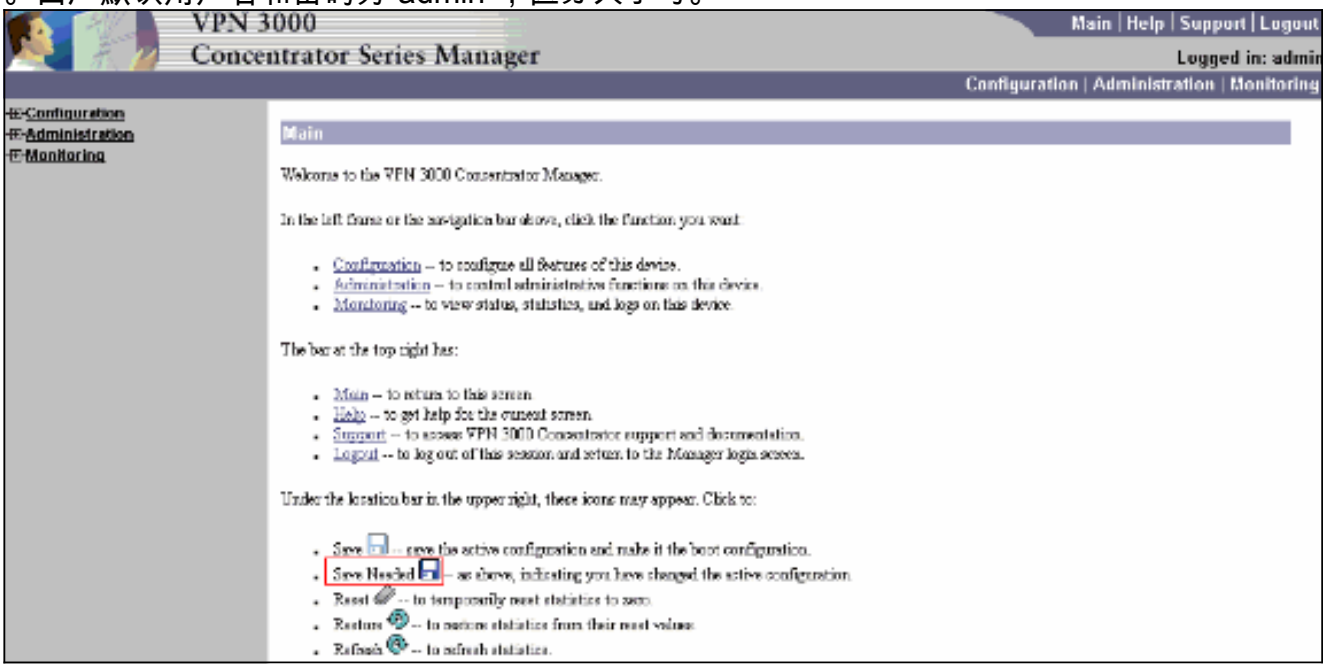
在Ethernet 1（专用）接口上配置IP地址后，可以使用CLI或浏览器界面配置其余地址。浏览器界面支持 HTTP 和使用安全套接字层 (SSL) 的 HTTP。

以下参数通过控制台进行配置：

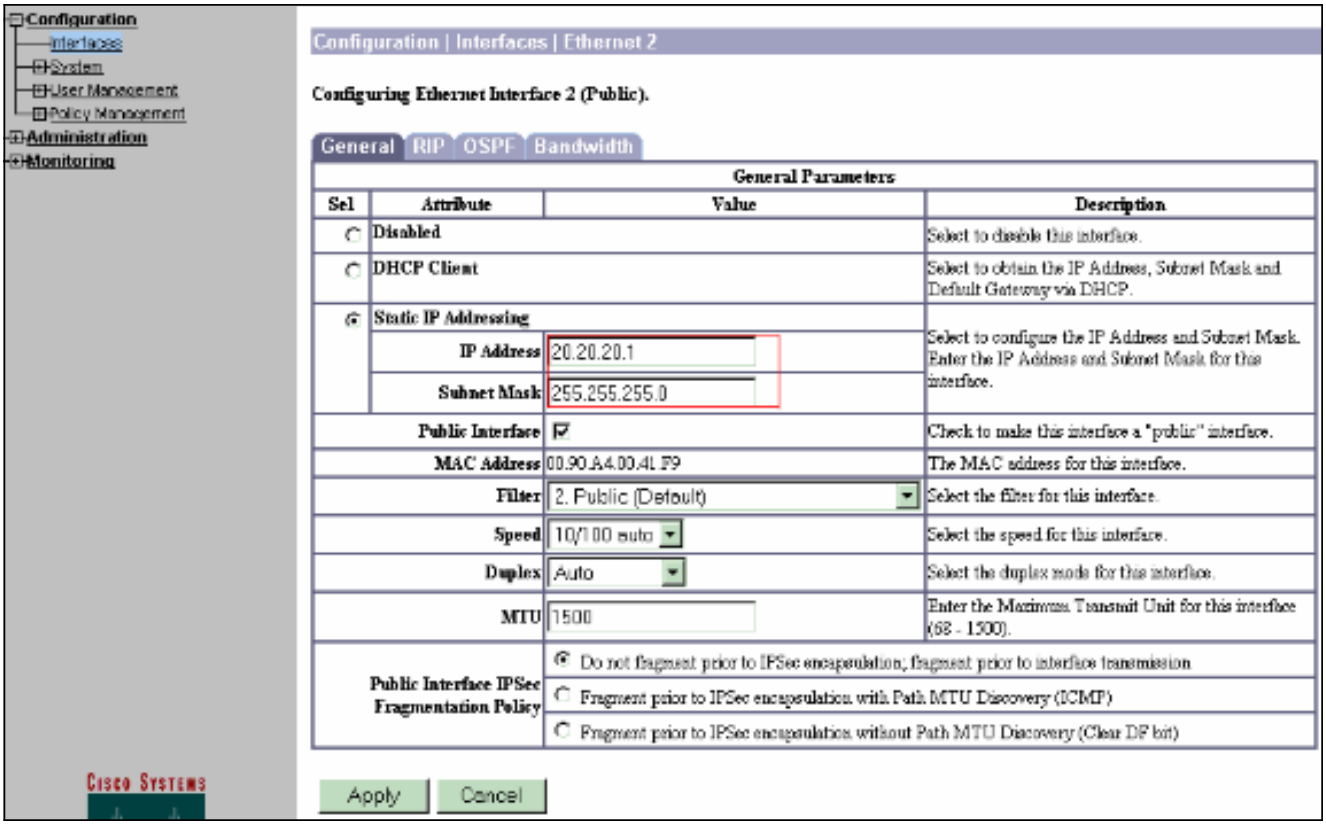
- **时间/日期** — 正确的时间和日期非常重要。他们帮助保证记录和记帐条目是准确的，并且系统能创建一个有效安全证书。
- **以太网1（专用）接口** — IP地址和掩码(来自我们的网络拓扑172.16.1.1/24)。

此时，VPN集中器可通过HTML浏览器从内部网络访问。欲了解在CLI模式下配置VPN集中器的信息，使用CLI参见快速配置。

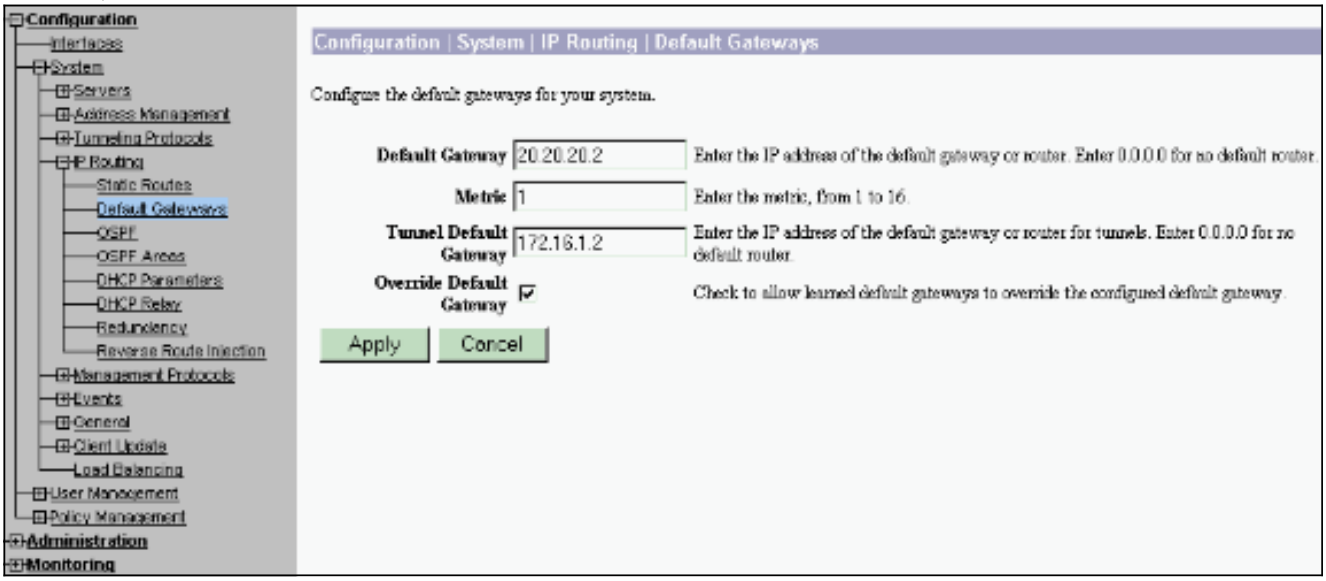
1. 从Web浏览器键入专用接口的IP地址以启用GUI界面。单击“保存**所需**”图标将更改保存到内存。出厂默认用户名和密码为“admin”，区分大小写。



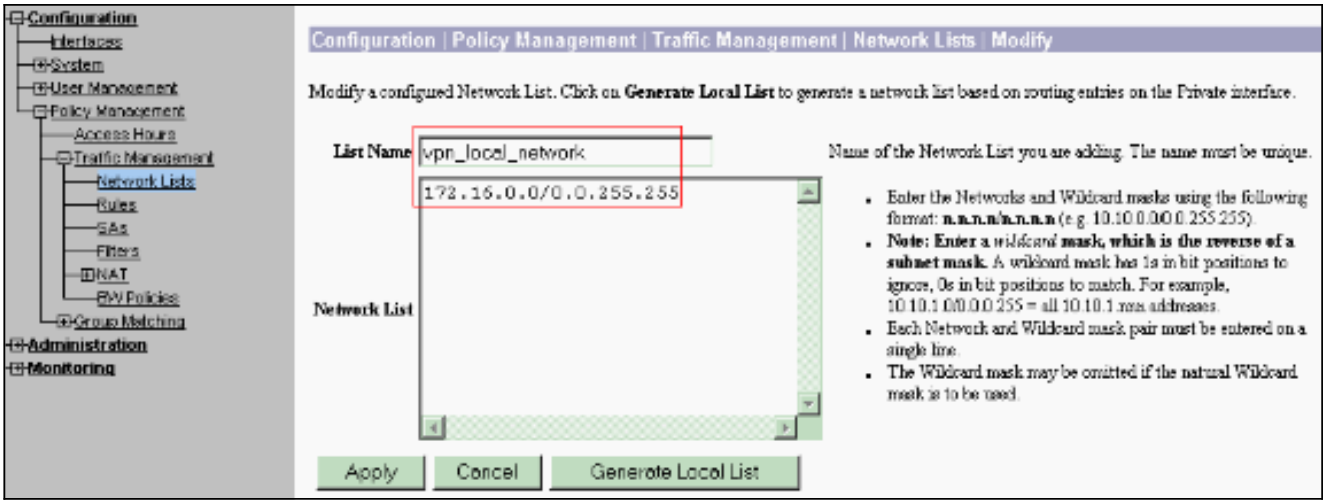
2. 在启动GUI后，选择**Configuration > Interfaces > Ethernet 2(Public)**以配置Ethernet 2接口。



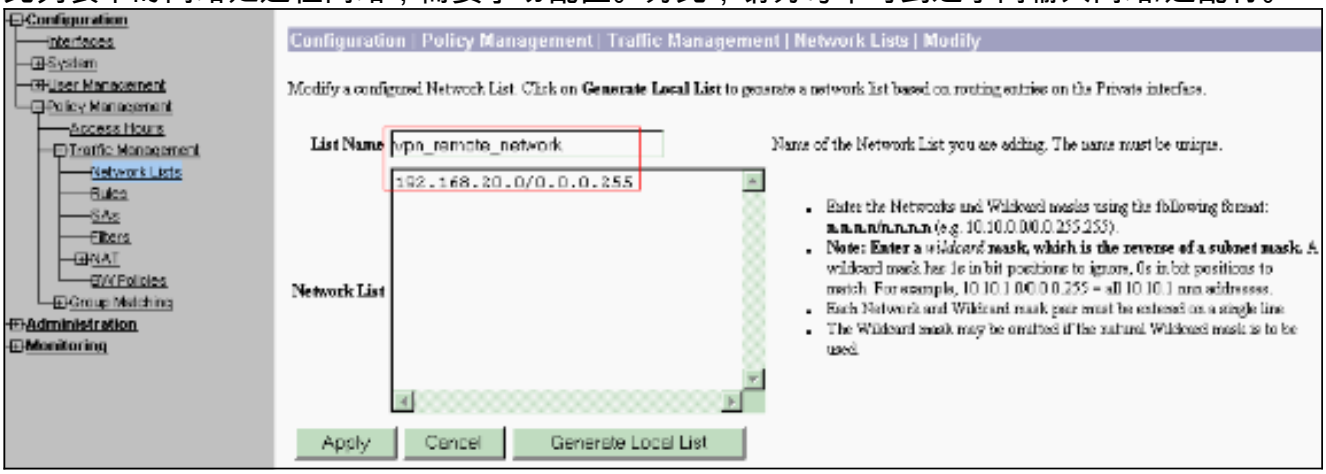
3. 选择**Configuration > System > IP Routing > Default Gateways** 配置IPsec的默认(Internet)网关和隧道默认（内部）网关，以到达专用网络中的其他子网。在此场景中，内部网络中只有一个子网可用。



4. 选择Configuration > **Policy Management > Traffic Management** > Network Lists > Add以创建定义要加密的流量的网络列表。列表中提到的网络可到达远程网络。以下列表中显示的网络是本地网络。单击“生成本地列表”时，也可以通过RIP自动生**成本地网络列表**。

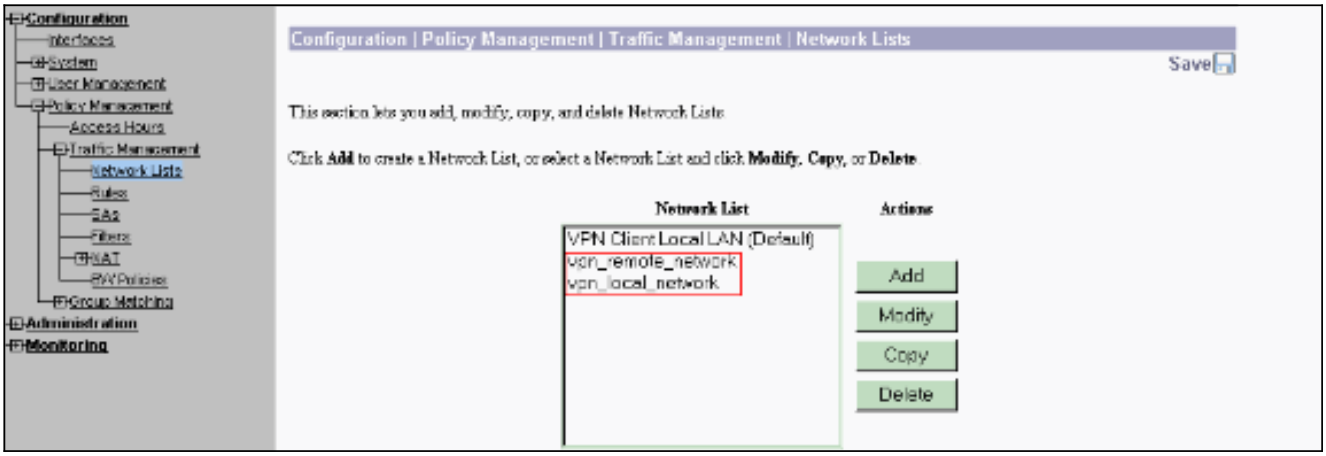


5. 此列表中的网络是远程网络，需要手动配置。为此，请为每个可到达子网输入网络/通配符。

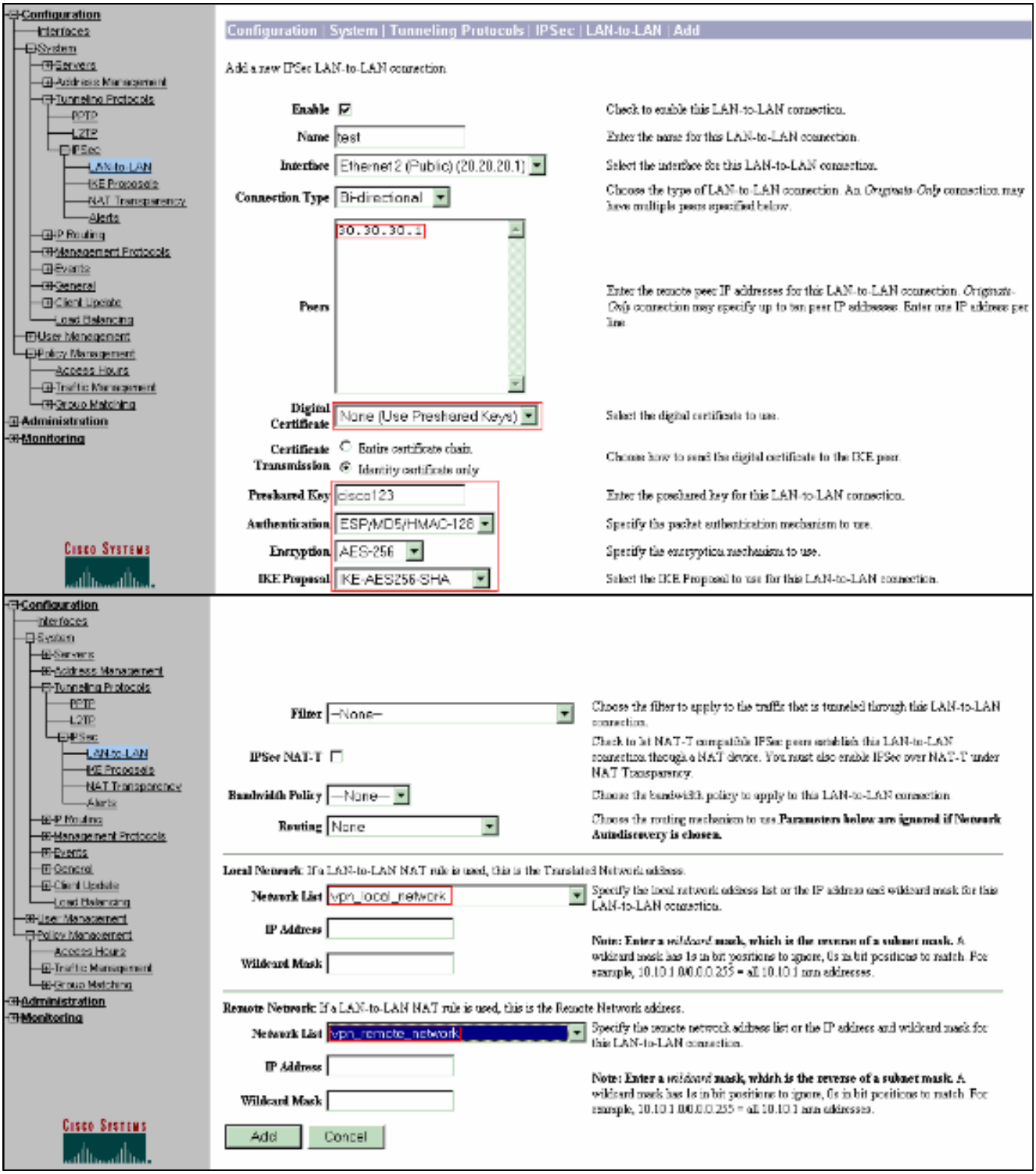


完成后，以下是两个网络列表

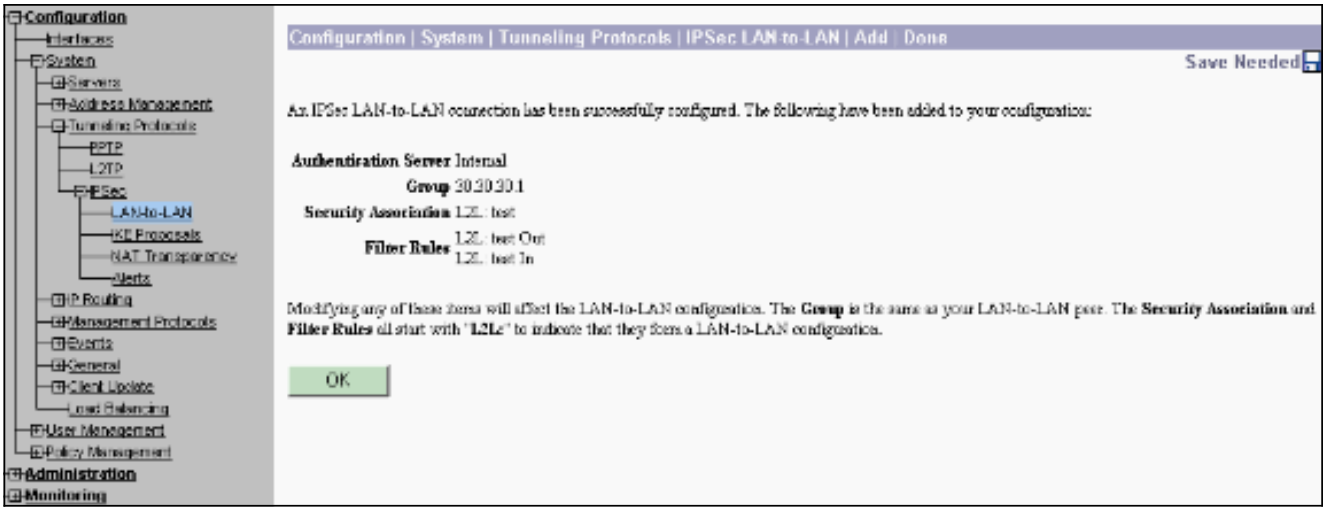
：



6. 选择Configuration > **System** > Tunneling Protocols > **IPSec LAN-to-LAN** > Add并定义LAN到LAN隧道。此窗口包含三个部分。上面的部分是网络信息，而下面的两部分是本地和远程网络列表。在Network Information（网络信息）部分，选择AES加密、身份验证类型、IKE提议，并键入预共享密钥。在底部部分中，分别指向已创建的网络列表（本地和远程）。

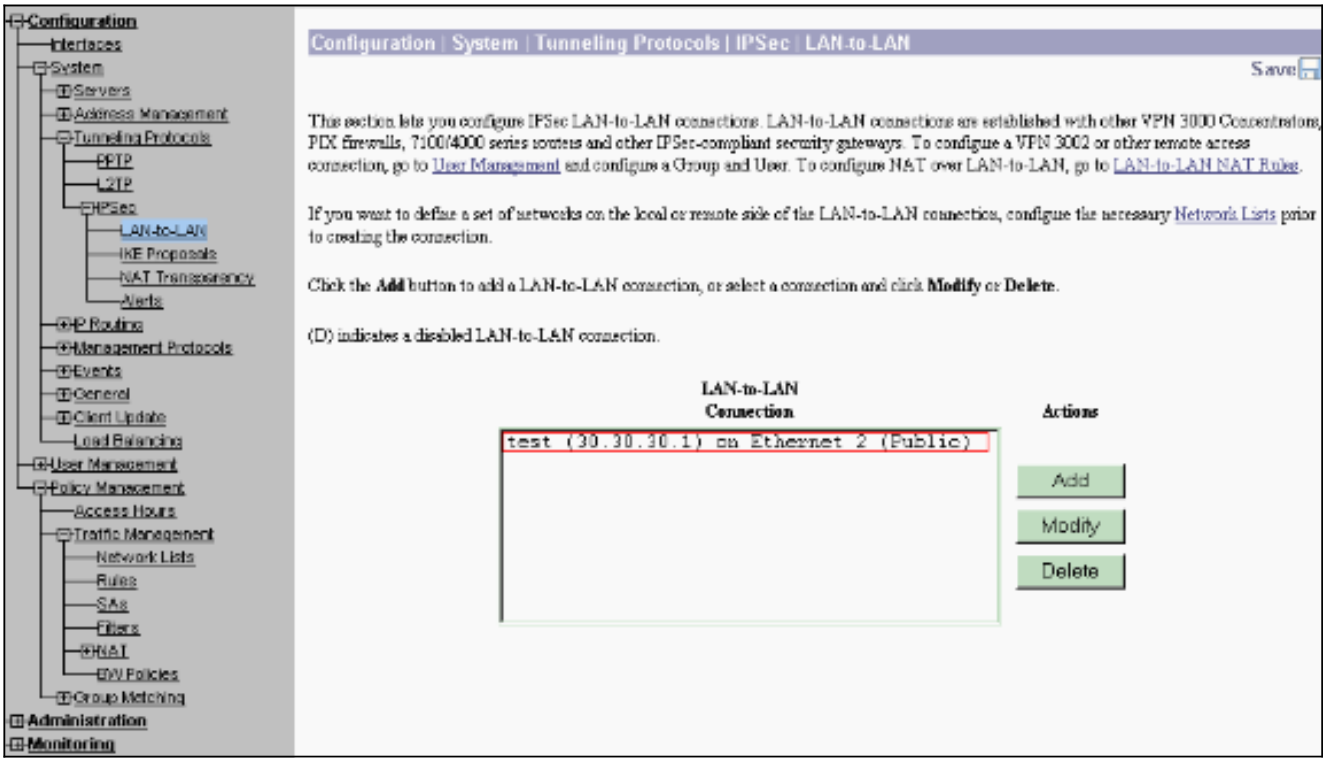


7. 单击Add后，如果连接正确，系统将显示“IPSec LAN-to-LAN-Add-Done”窗口。此窗口提供隧道配置信息的概要。它还自动配置组名、SA名和过滤器名。可以编辑此表中的任何参数。

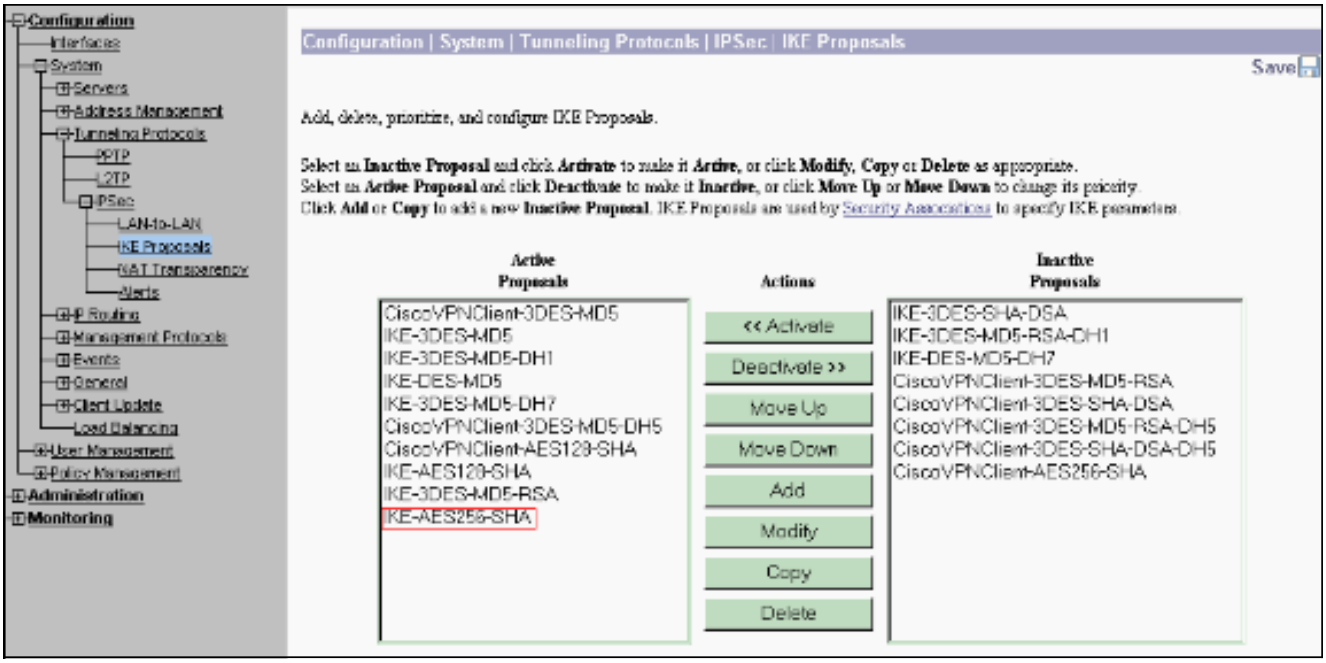


此时，IPsec LAN到LAN隧道已设置，您可以开始工作。如果由于某种原因隧道不工作，您可以检查配置错误。

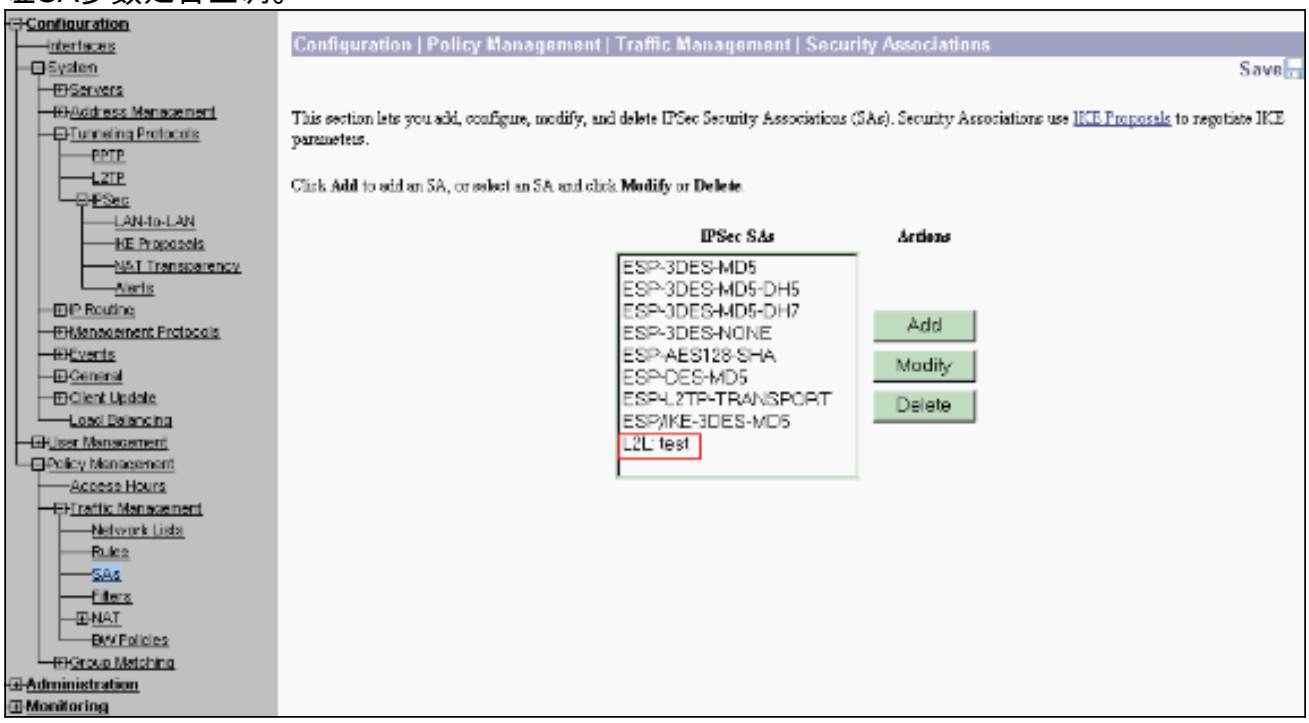
8. 选择**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**时，可以查看或修改之前创建的LAN到LAN IPsec参数。此图显示隧道名称为“test”，根据场景，远程端的公共接口为30.30.30.1。



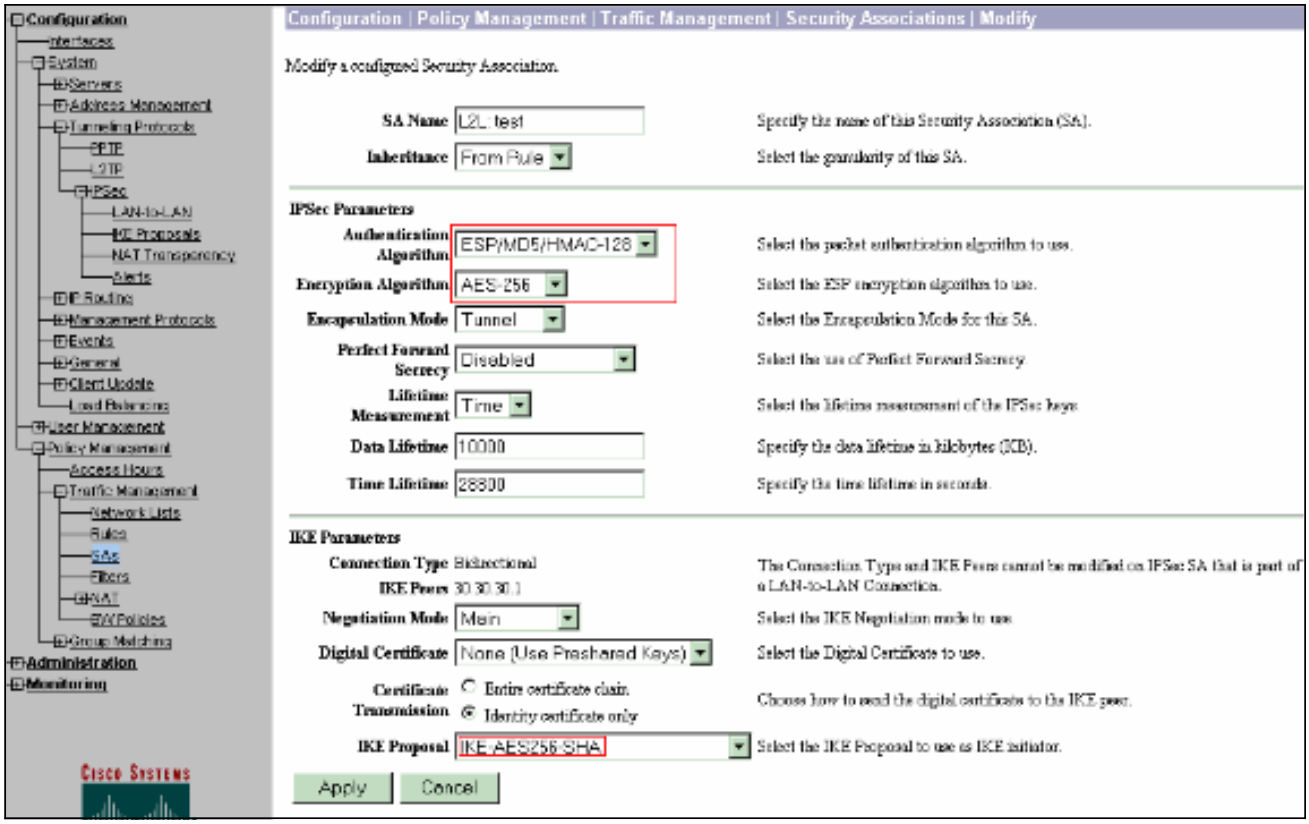
9. 有时，如果IKE提议在Inactive Proposals列表中，则隧道可能无法打开。选择Configuration > **System >** Tunneling Protocols > **IPSec** > IKE Proposals以配置活动IKE建议。如果您的IKE建议在“非活动建议”列表中，则在选择IKE建议并单击“激活”按钮时可以启**用该**建议。在此图中，所选建议“IKE-AES256-SHA”在“活动建议”列表中。



10. 选择Configuration > Policy Management > Traffic Management > Security Associations以验证SA参数是否正确。



11. 单击SA名称(在本例中为L2L:test)，然后单击Modify以验证SA。如果任何参数与远程对等体配置不匹配，可在此处更改。



验证

检验路由器配置

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。**状态QM_IDLE表示SA保持与其对等体的身份验证，并可用于后续快速模式交换。它处于静止状态。

```
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** - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的网络，以及所使用的转换集。有两个 ESP SA，每个方向一个。由于使用AH转换集，因此它为空。

```
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** — 显示所有加密引擎的当前活动加密会话连接。每个连接ID都是唯一的。加密和解密信息包的数量在前二列中显示。

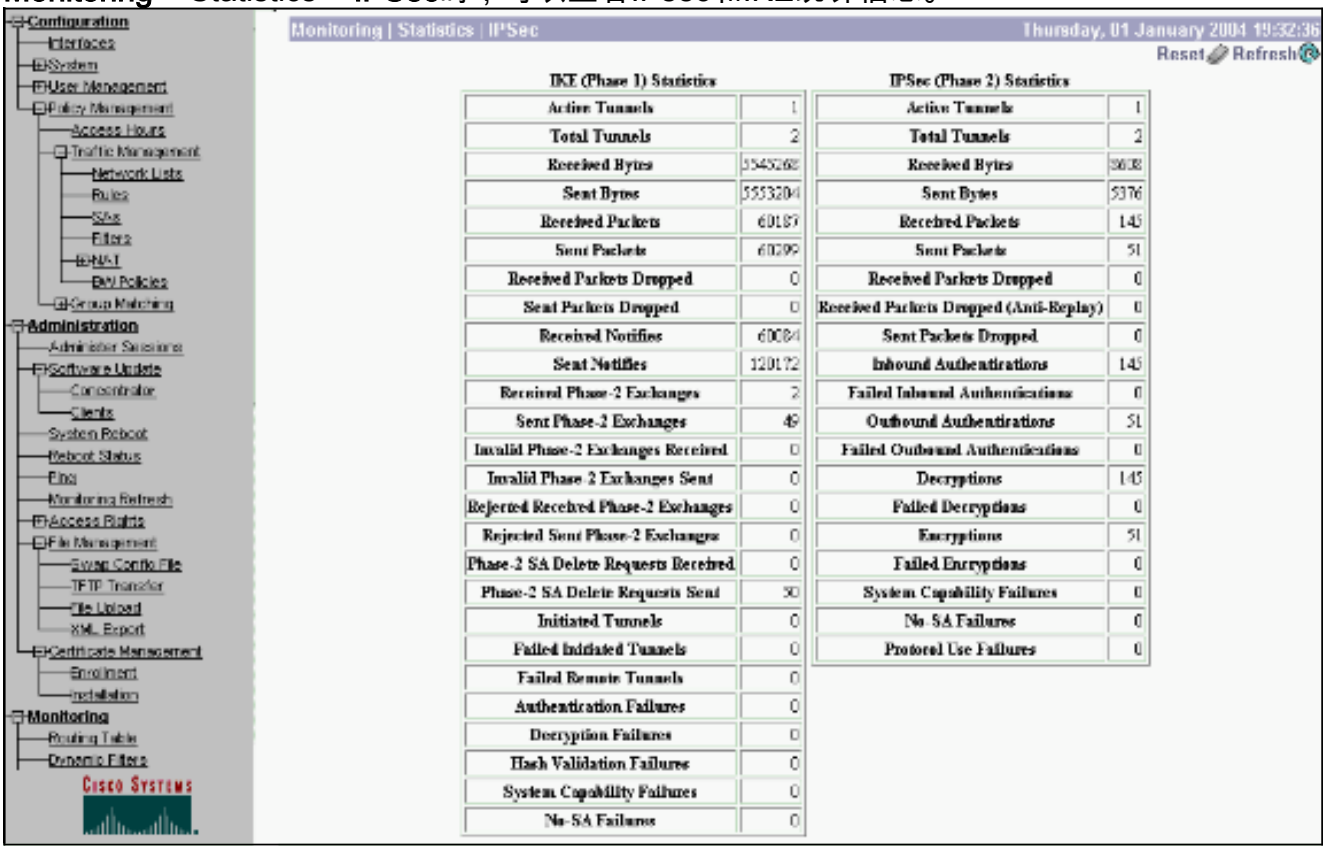
```
ipsec_router#show crypto engine connections active
```

```
  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
```

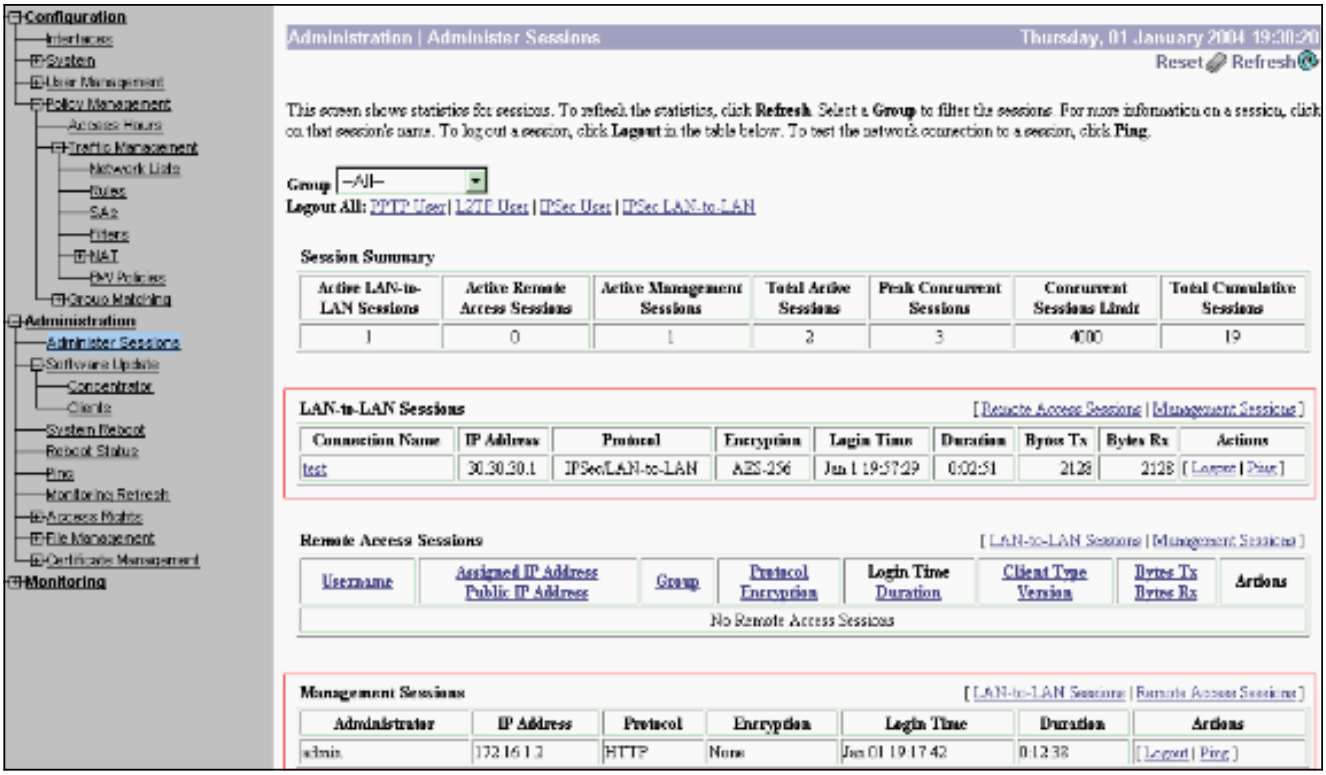
验证VPN集中器配置

完成以下步骤以验证VPN集中器配置。

1. 与在路由器上显示crypto ipsec sa和**show crypto isakmp sa命令类似，在VPN集中器上选择Monitoring** > Statistics > **IPSec**时，可以查看IPsec和IKE统计信息。



2. 与路由器上的show crypto engine connections active命令相似，您可以使用VPN集中器上的管理会话窗口查看所有IPSec LAN-到-LAN有效连接或隧道参数和统计数据。



故障排除

本部分提供的信息可用于对配置进行故障排除。

排除路由器故障

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

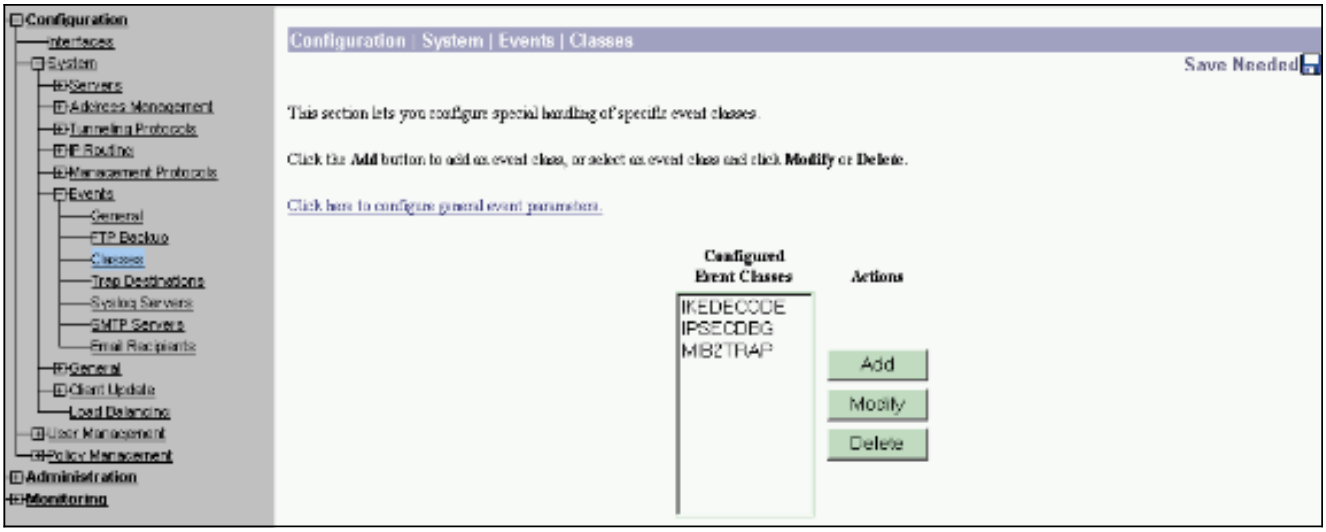
- **debug crypto engine - 显示已加密的流量。**加密引擎是执行加密和解密的实际机制。加密引擎可以是软件或硬件加速器。
- **debug crypto isakmp** — 显示IKE第1阶段的互联网安全关联和密钥管理协议(ISAKMP)协商。
- **debug crypto ipsec - 显示 IKE 第 2 阶段的 IPsec 协商。**

有关详细信息和输出示例，请参阅IPSec故障排除 — 了解和**使用**debug命令。

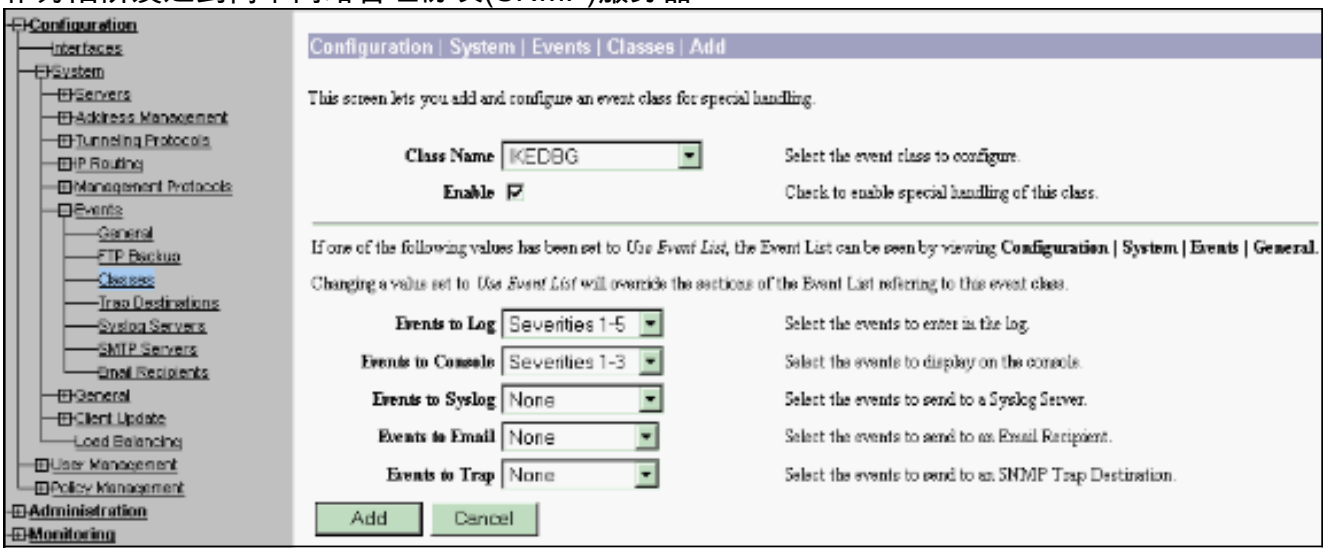
排除VPN集中器故障

类似于Cisco路由器的debug命令，您能配置事件类型，以查看所有告警。

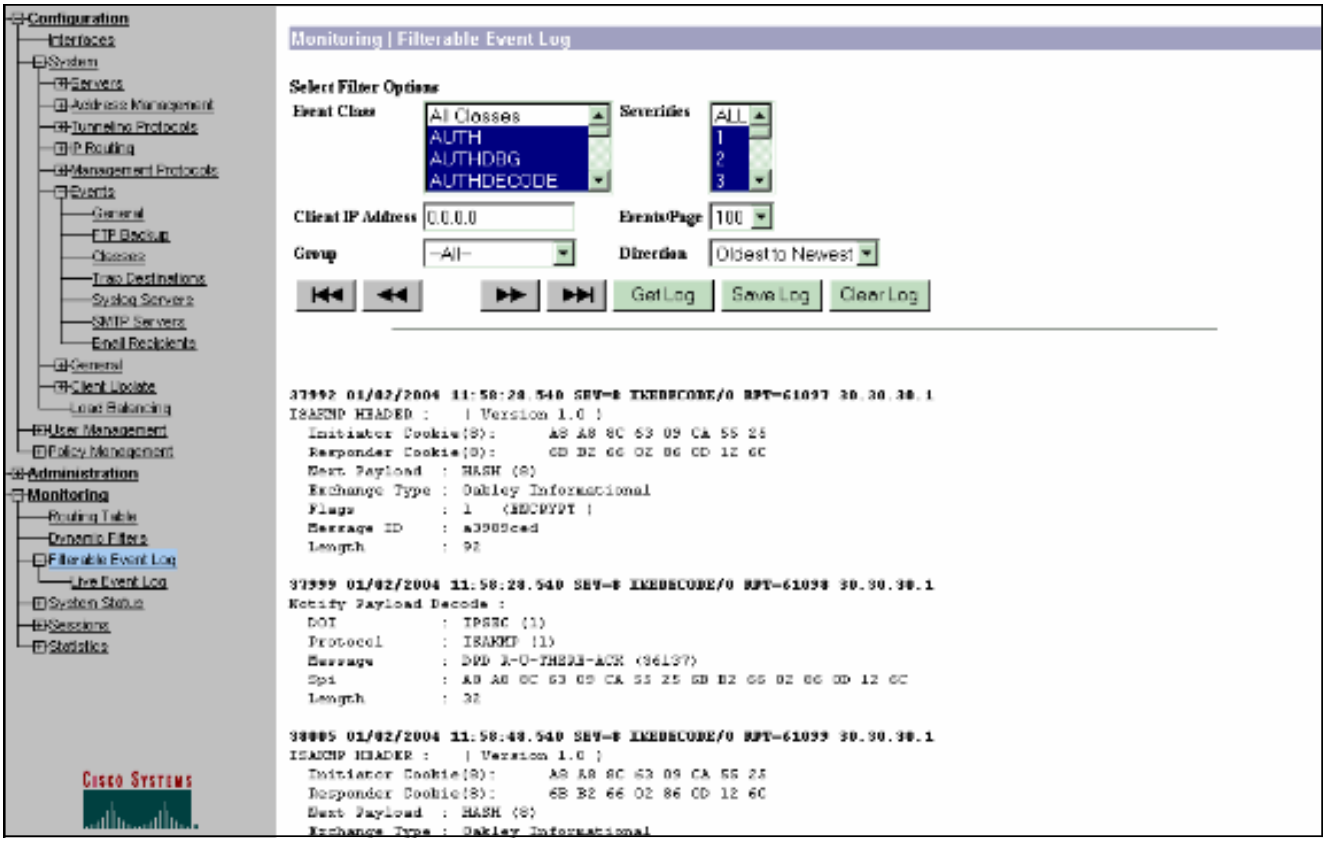
1. 选择Configuration > **System** > Events > **Classes** > Add以启用事件类的日志记录。IPsec可使用以下类
   ：IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. 当添加时，您还能为每个组选择严重级别，警告是根据根据这些安全级别发送的。警报可以通过以下方法之一处理：按日志显示在控制台上发送到UNIX系统日志服务器作为电子邮件发送作为陷阱发送到简单网络管理协议(SNMP)服务器



3. 选择**Monitoring > Filterable Event Log** 以监控已启用的警报。



相关信息

- 高级加密标准 (AES)
- DES/3DES/AES VPN加密模块
- IPSec配置示例
- Cisco VPN 3000 系列客户端支持页
- IPsec 协商/IKE 协议支持页