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

Contents

Introduction

本文显示如何用Advance Encryption Standard (AES)配置在Cisco VPN 3000 Concentrator和Cisco路由器之间的一个IPSec隧道作为加密算法。

AES是美国标准技术研究所(NIST)创建的一新的联邦信息处理的标准的(FIP)出版物将使用作为加密方法。此标准指定替换数据加密标准(DES)作为IPsec和Internet Key Exchange (IKE)的一次保密性转换的AES对称加密算法。AES有三个不同的密钥长度、一个128-bit键(默认值)，一个192-bit键和一个256-bit键。在Cisco IOS的AES功能添加新的加密标准AES的技术支持，同密码块连锁(CBC)模式，到IPsec。

请参见NIST计算机安全资源中心站点 关于AES的更多信息。

请参见在Cisco VPN 3000 Concentrator和PIX防火墙配置示例之间的LAN到LAN IPSec隧道关于在VPN 3000 Concentrator和PIX防火墙之间的LAN对LAN隧道配置的更多信息。

当PIX有软件版本7.1时，请参考在PIX 7.x和VPN 3000 Concentrator配置示例之间的IPSec隧道欲知更多信息。

Prerequisites

Requirements

本文要求IPSec协议基本的了解。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：

- **路由器需求**- AES功能在Cisco IOS Software Release 12.2(13)T被介绍了。为了enable (event) AES，您的路由器必须支持IPsec和运行IOS镜像以"k9"长的键("k9"子系统)。**Note:** AES的硬件技术支持也是可用的在Cisco 2600XM， 2691个， 3725个和3745个AES加速度VPN模块。此功能没有配置暗示，并且硬件模块自动地选择，如果两个是可用的。
- **VPN集中器需求**- AES功能的软件支持在版本3.6被引入。新的改进的，可升级的加密处理器提供硬件技术支持(SEP-E)。此功能没有配置暗示。**Note:** 在Cisco VPN 3000 Concentrator版本3.6.3中，隧道不协商对AES由于Cisco Bug ID CSCdy88797 (仅限注册用户)。这从版本3.6.4被解决了。**Note:** Cisco VPN 3000 Concentrator使用SEP或SEP-E模块，不是两个。在同一个设备上请勿安装两个。如果在已经包含一个SEP模块的VPN集中器上安装一个SEP-E模块，VPN集中器禁用SEP模块并且使用仅SEP-E模块。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 与Cisco IOS软件版本12.3(5)的Cisco 3600 Series Router
- Cisco VPN 3060 Concentrator用软件版本4.0.3

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

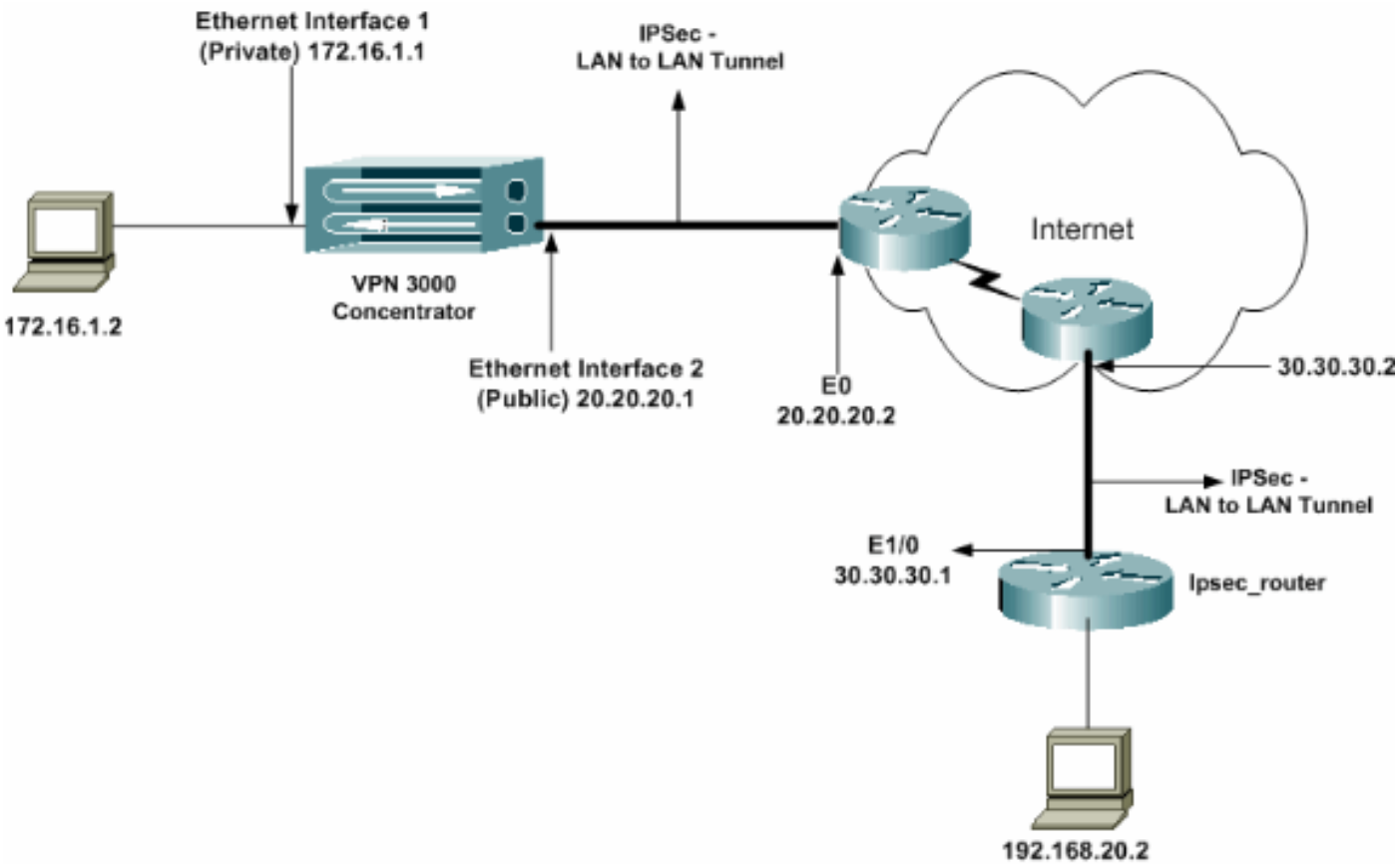
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Network Diagram

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
```

Note: 虽然ACL语法是没有变化的，含义为加密ACL是有些不同的。在加密ACL，**许可证**指定那配比的信息包应该加密，而请**拒绝**指定那配比的信息包不需要被加密。

配置VPN集中器

VPN集中器没有预编程序用在他们的出厂设置的IP地址。您必须使用控制台端口配置是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。

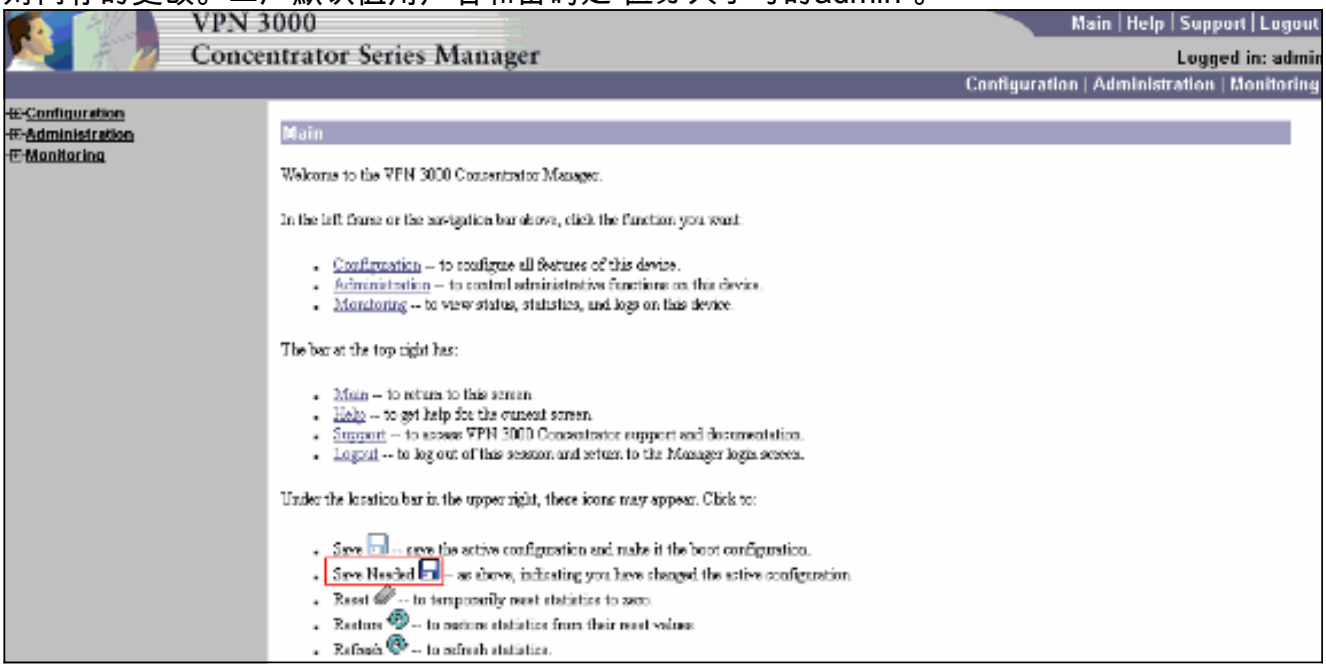
在Ethernet 1的IP地址以后(配置专用的)接口，可以配置其余或者使用CLI或通过浏览器接口。浏览器界面支持 HTTP 和使用安全套接字层 (SSL) 的 HTTP。

以下参数通过控制台进行配置：

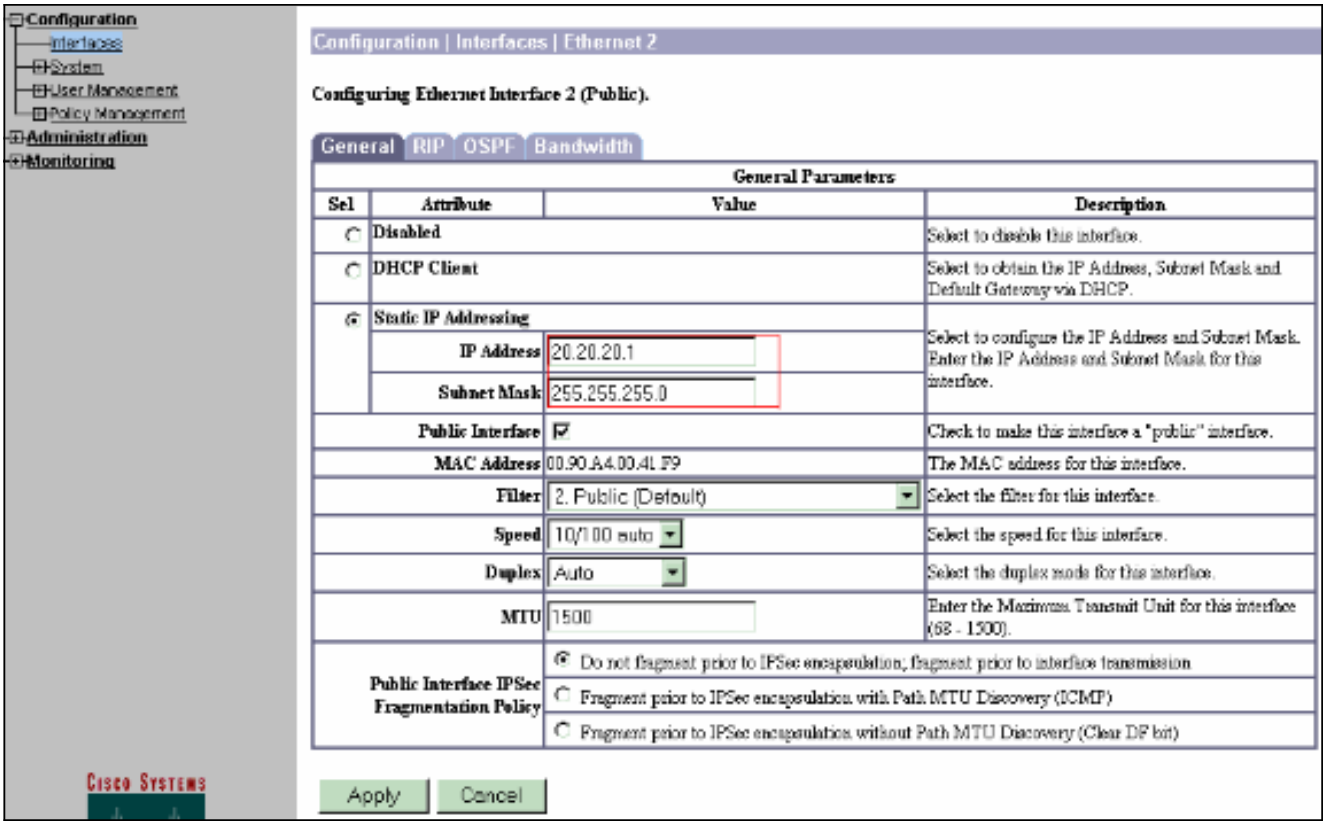
- **时刻/日期**-正确时间和日期是非常重要的。他们帮助保证记录和记帐条目是准确的，并且系统能创建一有效安全证书。
- **Ethernet 1 (专用的)接口**- IP地址和掩码(从我们的网络拓扑172.16.1.1/24)。

这时， VPN集中器通过从内部网络的一个HTML浏览器是可取得。使用CLI，关于配置VPN集中器的信息在CLI模式下，请参见快速配置。

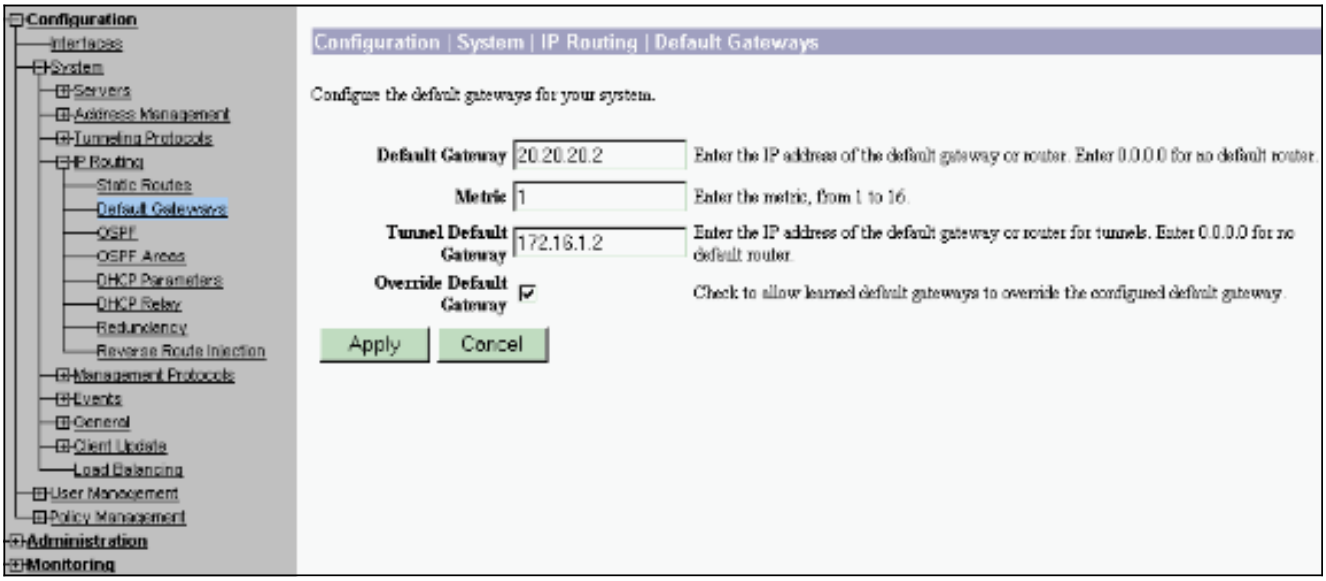
1. 键入专用接口的IP地址从Web浏览器的到enable (event) GUI界面。点击**保存必要的**图标保存对内存的更改。工厂默认值用户名和密码是“区分大小写的admin”。



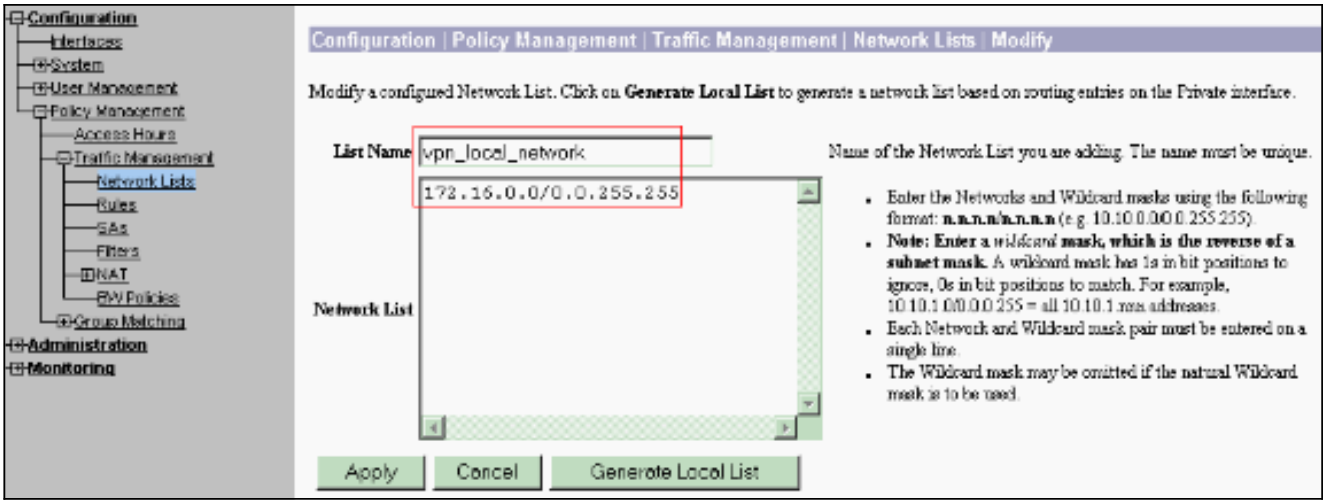
2. 在您提出GUI后，请选择**Configuration > Interfaces > Ethernet 2 (公共)**配置Ethernet2接口。



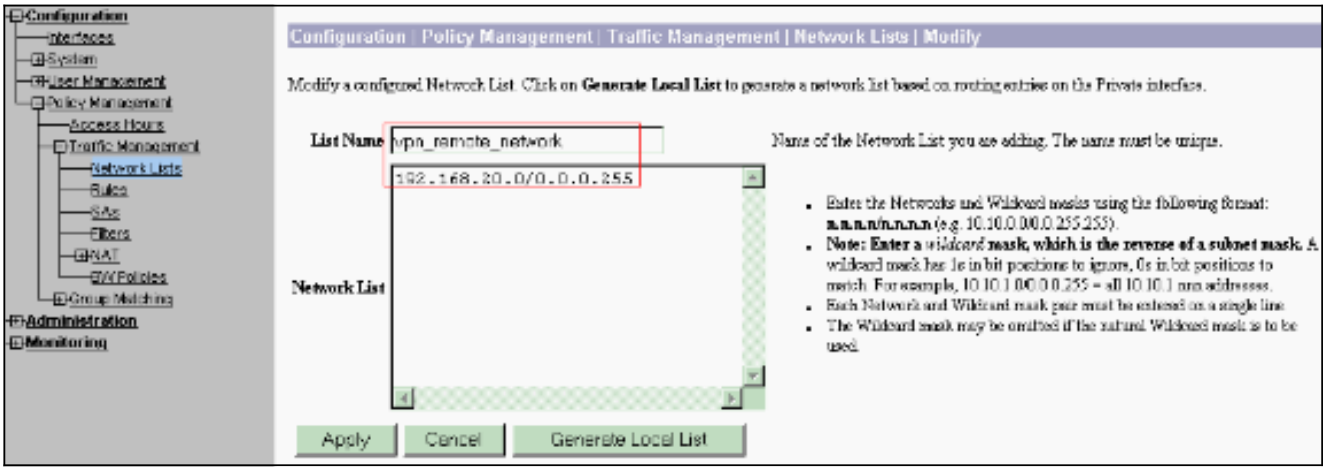
3. 选择**Configuration > System** > IP Routing > Default Gateways配置默认(互联网)网关和隧道默认(里面)网关IPsec的能到达其他子网在专用网络。在此方案中，只有一个子网可用在内部网络。



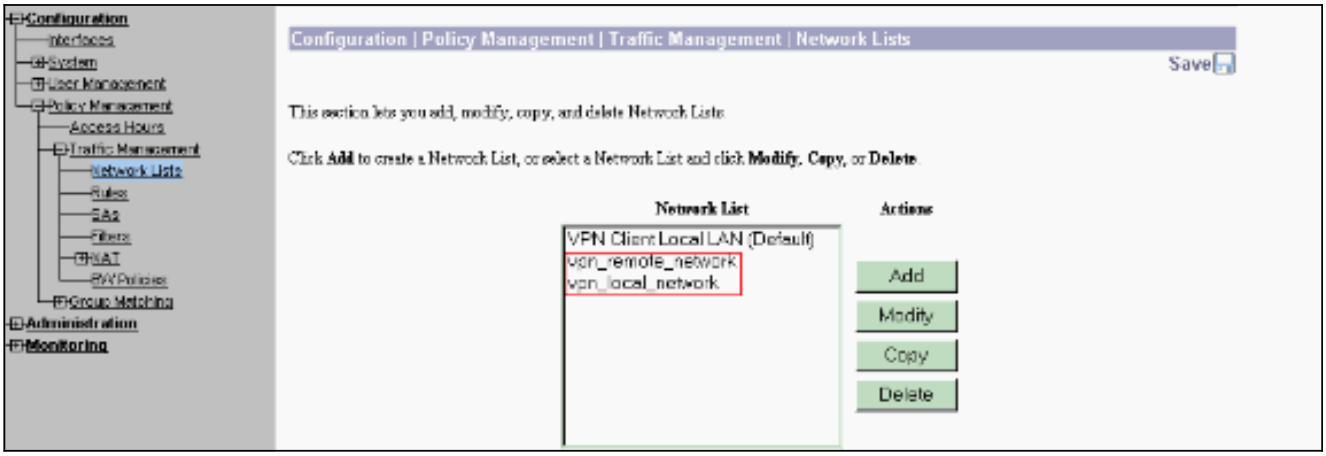
4. 选择**Configuration > Policy Management > Traffic Management > Network Lists** >Add建立定义数据流的网络列表将被加密。在列表提及的网络是可及的对远程网络。在列表显示的网络下面是本地网络。当您点击**Generate Local List时**，您能通过RIP自动地也生成本地网络列表。



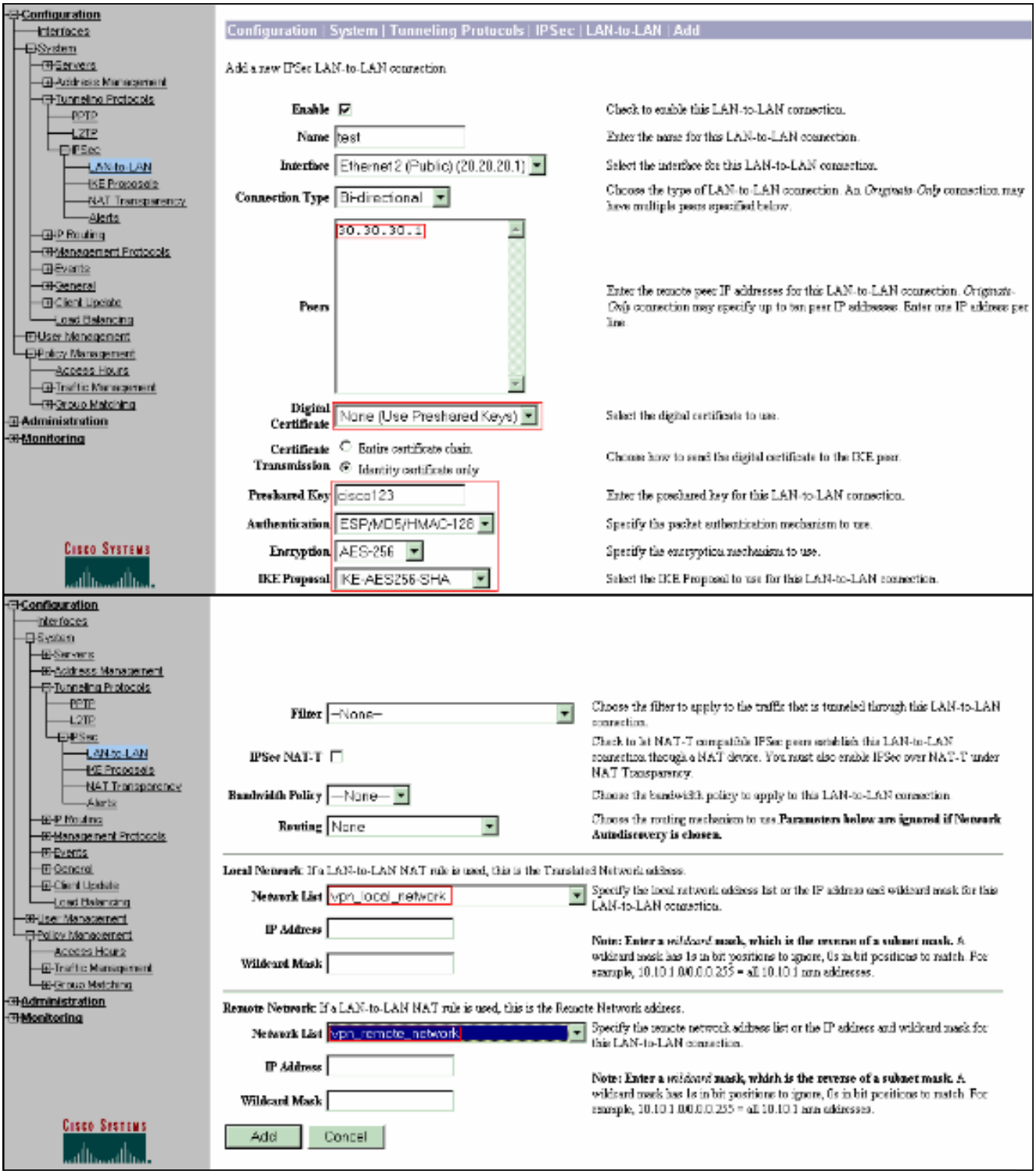
5. 在此列表的网络是远程网络并且需要手工被配置。为了执行此，请进入网络/通配符每个可及的子网的。



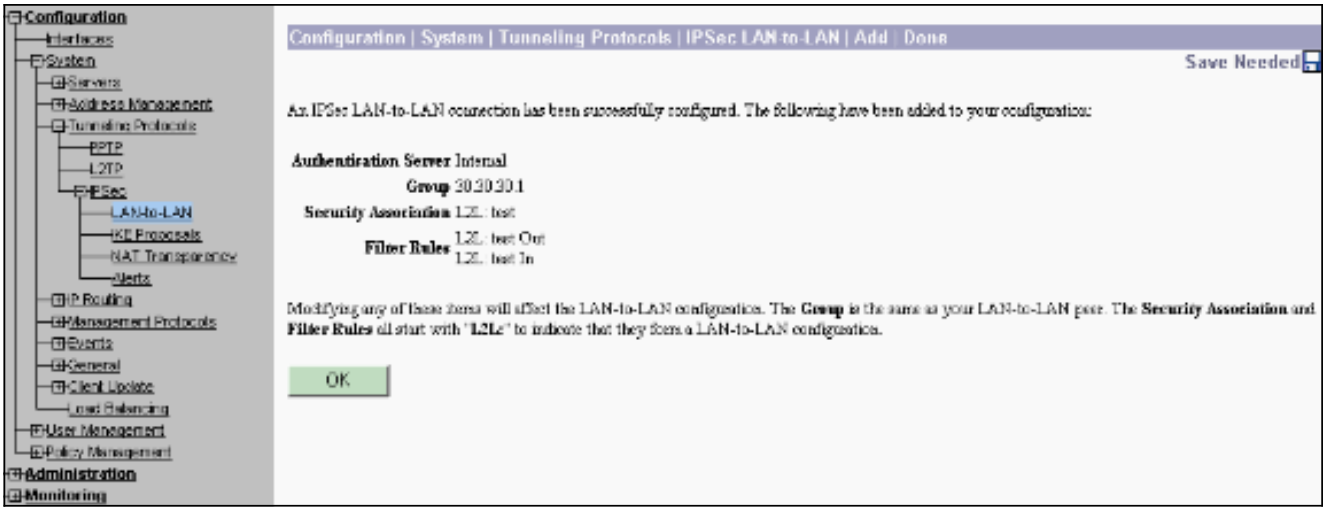
当完成，这些是两张网络列表：



6. 选择Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add并且定义LAN-to-LAN隧道。此窗口有三个部分。顶部是为网络信息，并且底下两个部分是为本地和远程网络列表。在网络信息部分，请选择AES加密，认证类型， IKE建议，并且键入预共享密钥。在底下部分，请指向您已经建立，各自本地和远程列表的网络列表。

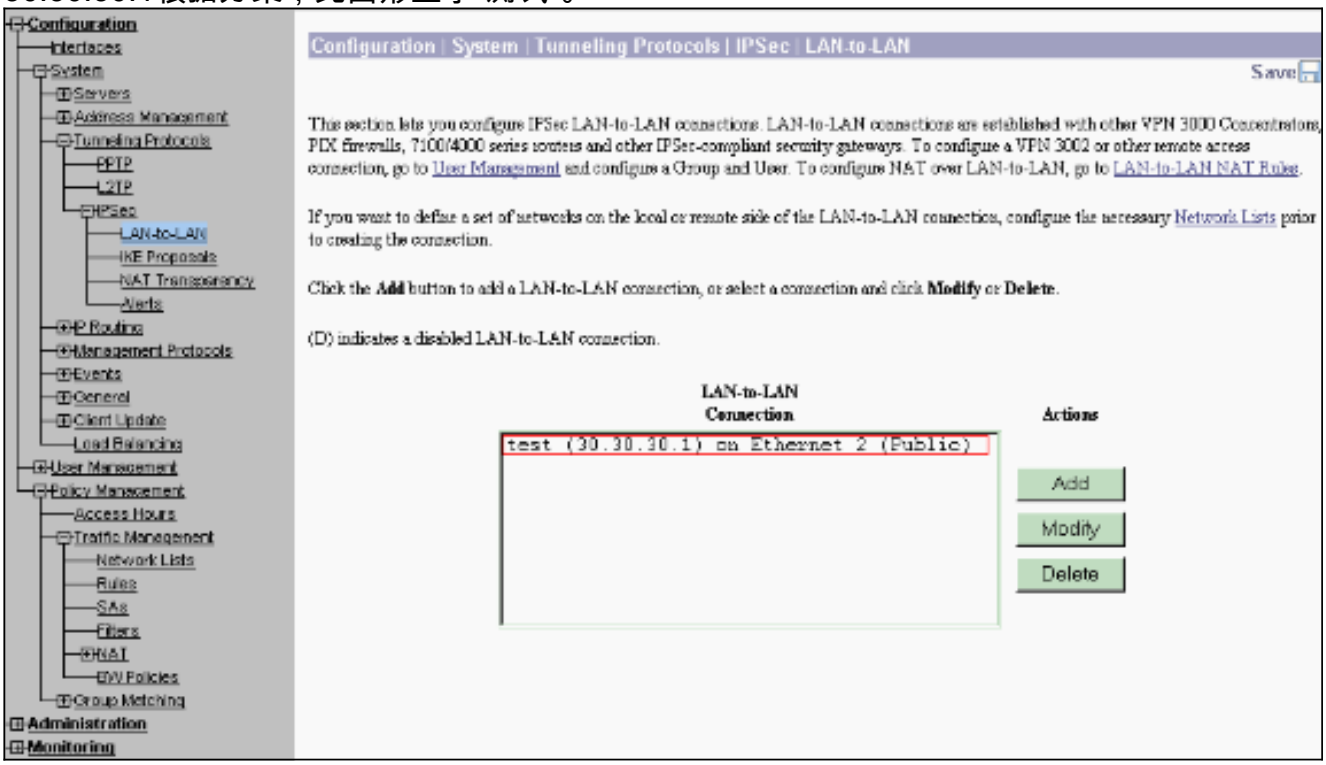


7. 在您点击后请**添加**，如果您的连接是正确的，您看到IPSec LAN-to-LAN-Add-Done窗口。此窗口提交隧道配置信息的总结。它自动地也配置组名、SA名字和过滤器名称。您在此表里能编辑所有参数。

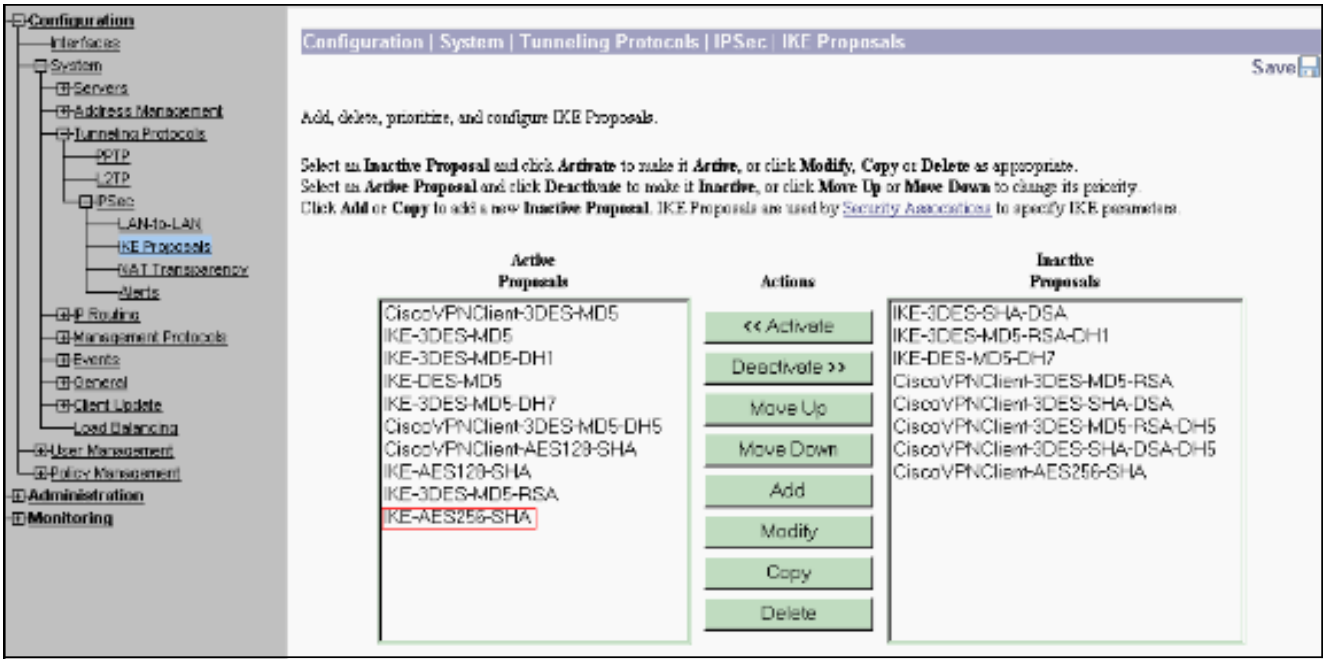


这时IPSec LAN到LAN隧道设置，并且您能开始工作。如果，由于某种原因，隧道不工作，您能检查误配置。

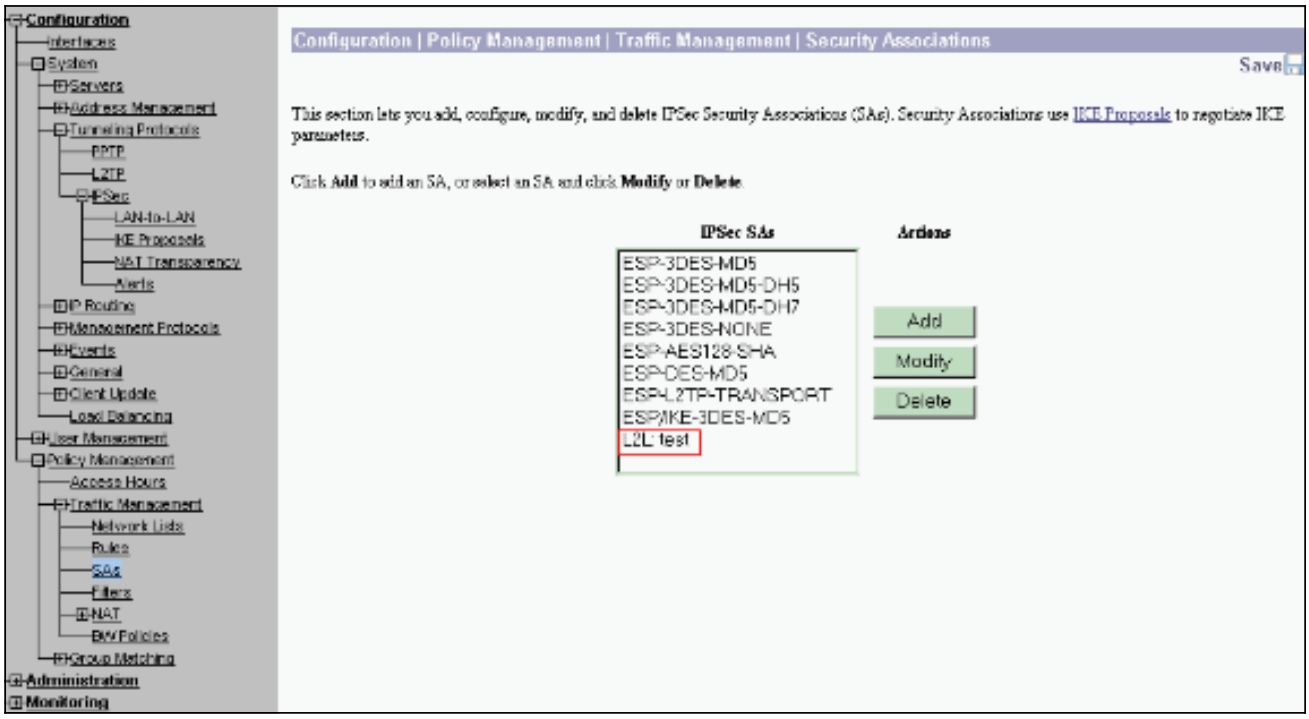
8. 当您选择**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN时，**您能查看或修改以前创建的LAN对LAN IPSec参数。因为隧道和远程终端的公共接口的名字是30.30.30.1根据方案，此图形显示“测试”。



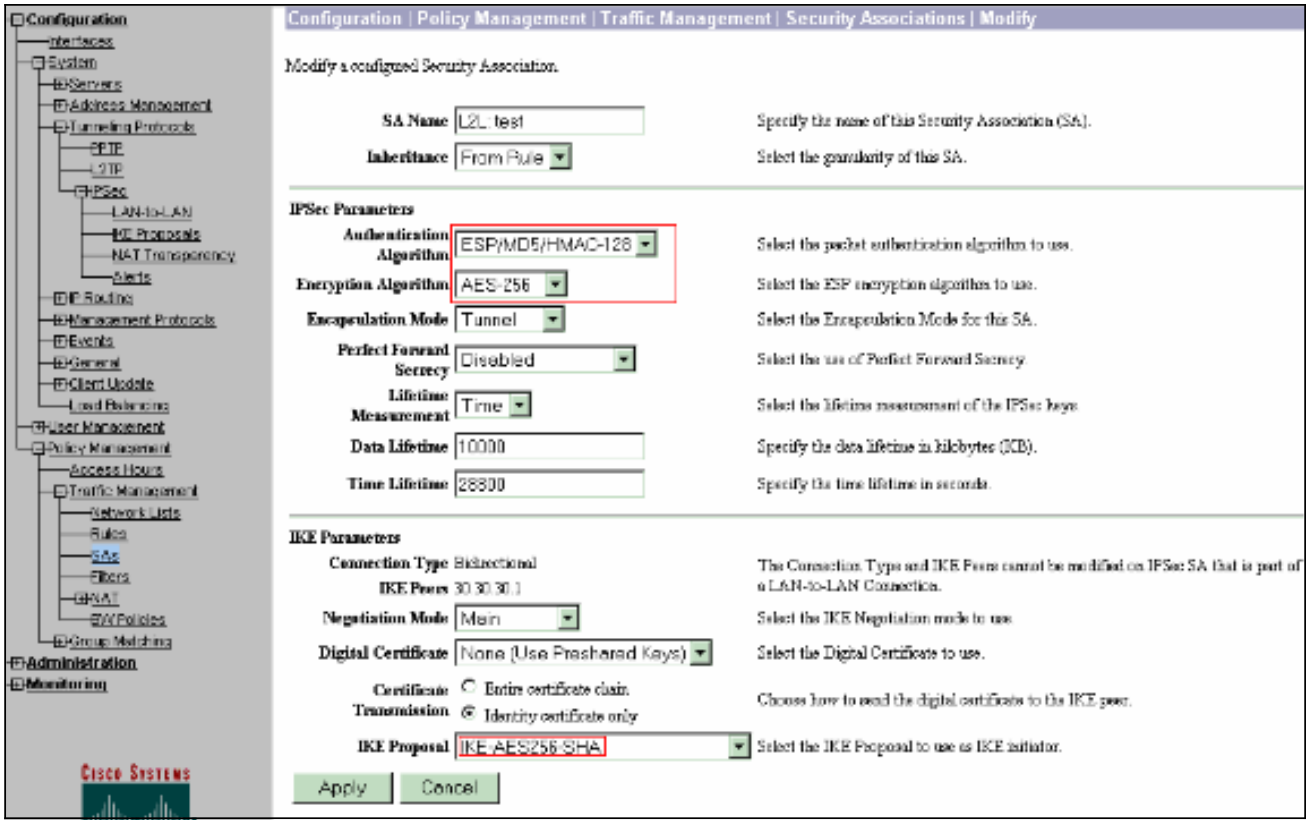
9. 通常，如果您的IKE建议在Inactive Proposals列表，您的隧道也许不过来。选择**Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**配置活动IKE建议。如果您的IKE建议在“非激活建议”列出您能enable (event)它，当您选择IKE建议并且点击**激活**按钮时。在此图形所选的建议"IKE-AES256-SHA"在有效建议列表。



10. 选择**Configuration > Policy Management > Traffic Management >** Security**关联**验证SA参数是否是正确的。



11. 点击SA名字(在这种情况下， **L2L ：测试**)，然后点击**修改**验证SAS。如果其中任一个参数与远端对等体配置不配比，可以更改这里。



Verify

验证路由器配置

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保持验证与其对等体，并且可以用于随后的快速模式交换。它在一个淡静状态。

```
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。因为AH使用转换集，它是空的。

```
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的会话连接。每连接ID是唯一。被加密并且解码信息包的数量在前两列显示。

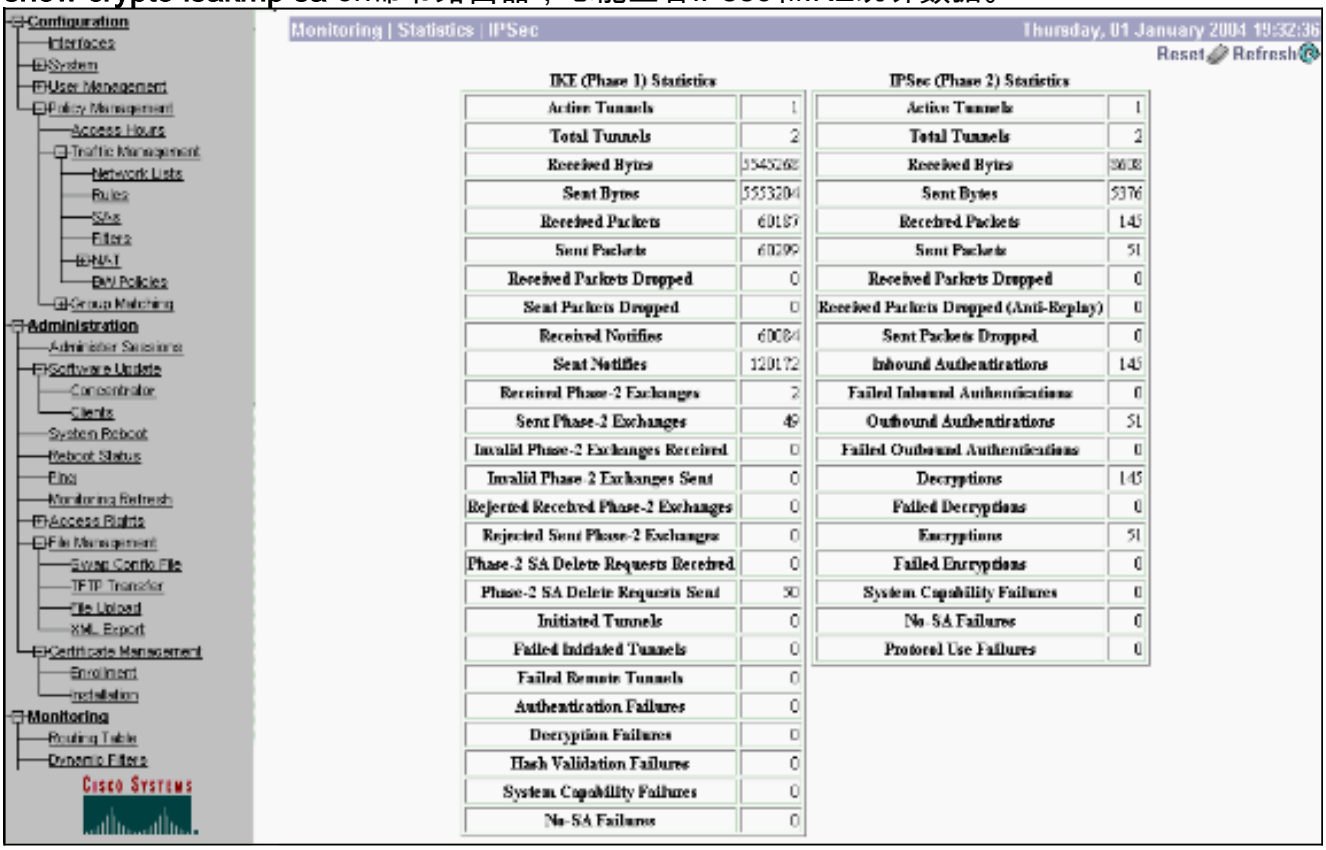
```
ipsec_router#show crypto engine connections active
```

```
  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
```

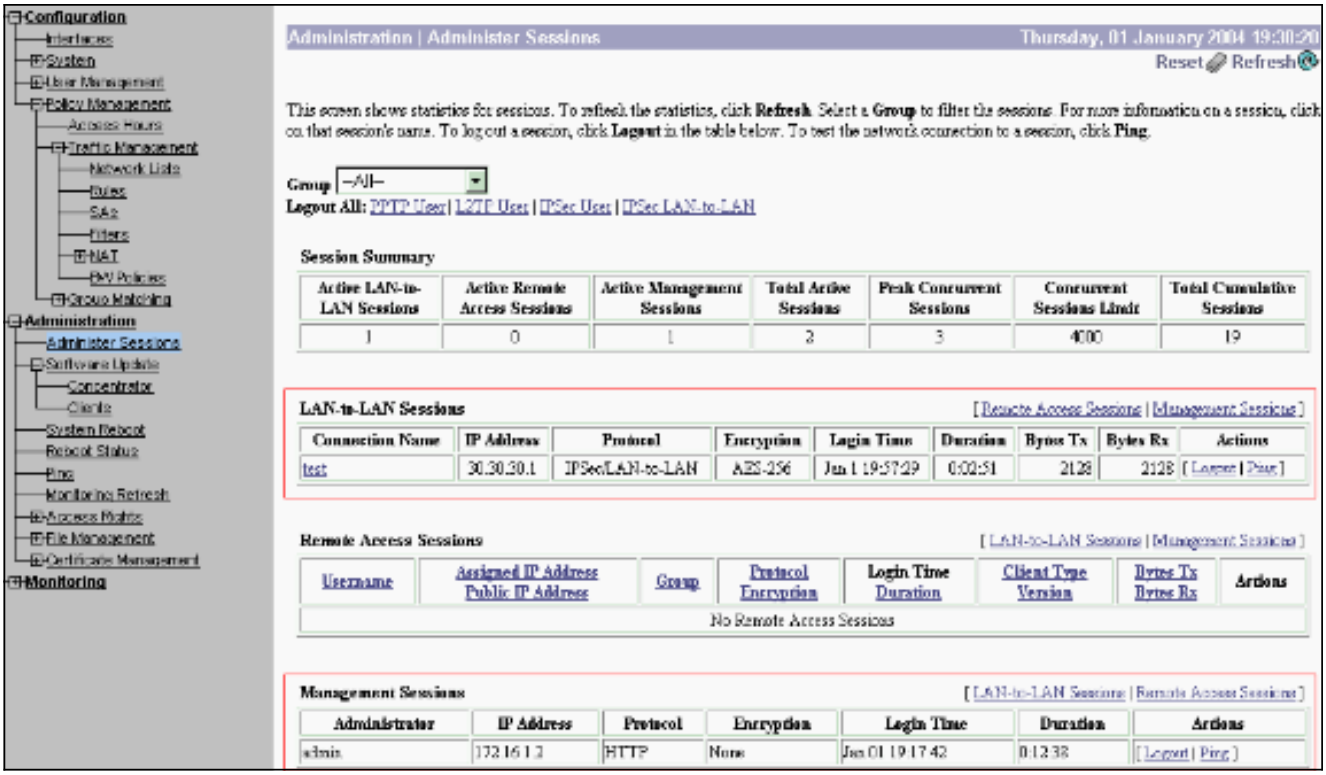
验证VPN集中器配置

完成这些步骤验证VPN集中器配置。

1. 当您选择在VPN集中器时的**Monitoring > Statistics > IPSec**类似于**show crypto ipsec sa**和**show crypto isakmp sa** on命令路由器，您能查看IPsec和IKE统计数据。



2. 类似于**show crypto engine connections active命令**在路由器，您能使用在VPN集中器的Administration-Sessions窗口查看参数和统计数据所有活动IPSec LAN-到-LAN连接或隧道的。



Troubleshoot

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。

Note: 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

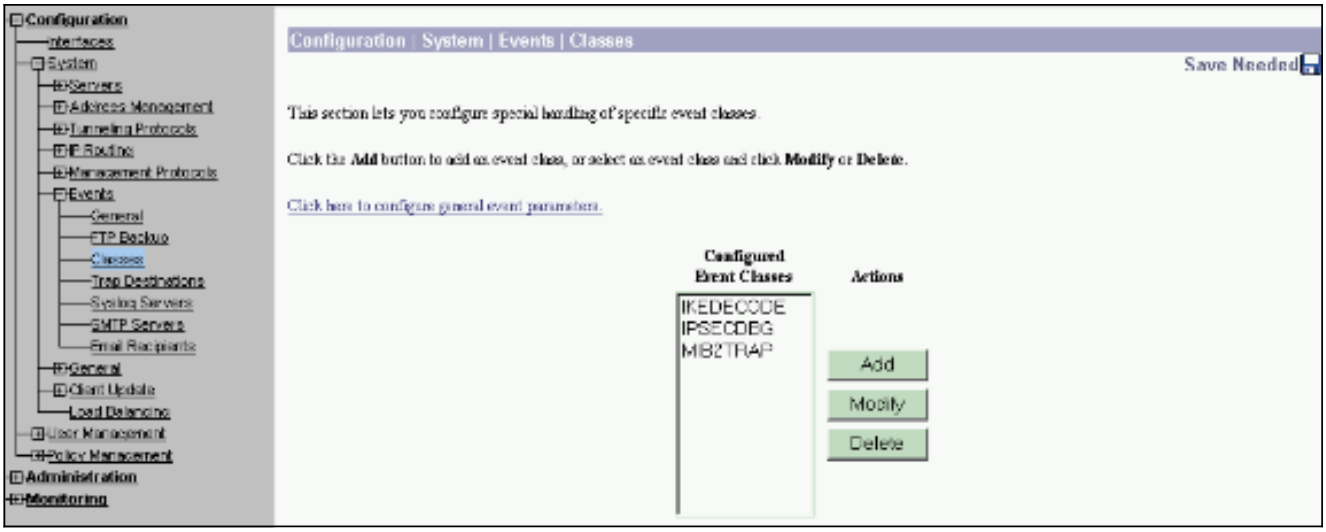
- **debug crypto engine** - 显示已加密的流量。加密引擎是进行加密和解密的实际机制。加密引擎可以是软件或硬件加速器。
- **debug crypto isakmp** —显示IKE第1.的互联网安全协会和密钥管理协议(ISAKMP)协商阶段。
- **debug crypto ipsec** - 显示 IKE 第 2 阶段的 IPsec 协商。

参考IPSec排除故障-了解和使用调试指令详细信息和输出示例:。

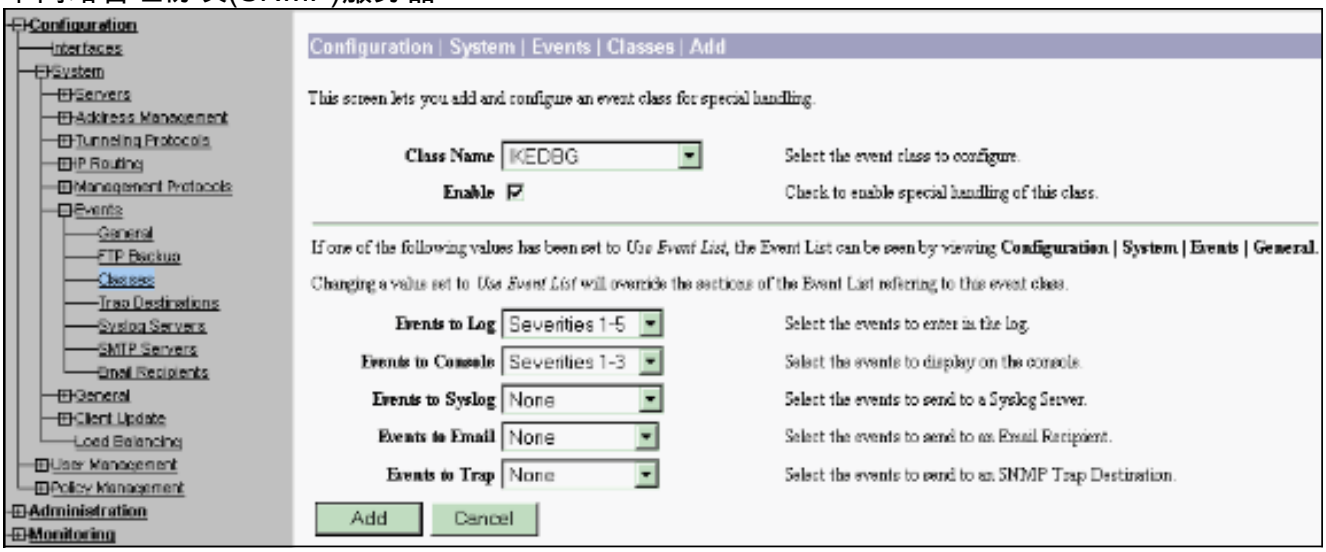
排除VPN集中器故障

类似**调试**on命令Cisco路由器，您能配置事件类查看所有警报。

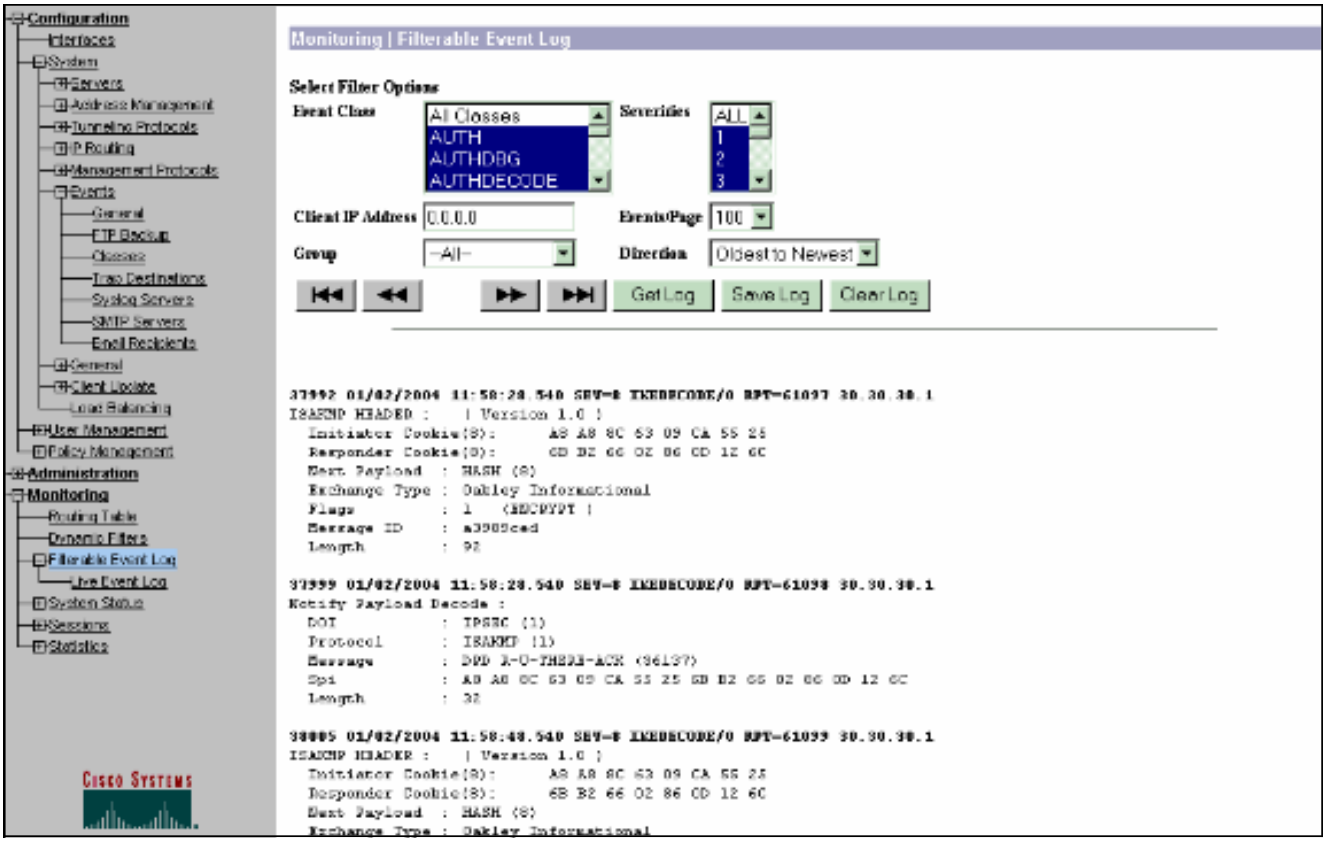
1. 选择**Configuration > System > Events > Classes > Add**启用登录事件类。这些组为IPsec是可用的
   ：IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. 当添加时，您能为每个组也选择告警级别，根据告警级别发送警报。警报可以由这些方法之一处理：由日志显示在控制台发送到UNIX系统日志服务器发送作为电子邮件发送作为陷井到简单网络管理协议(SNMP)服务器



3. 选择**Monitoring > Filterable Event Log**监控启用警报。



Related Information

- 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