Túnel IPsec LAN a LAN entre um Cisco VPN 3000 Concentrator e um roteador com exemplo de configuração AES

Contents

Introduction

Este documento mostra como configurar um túnel de IPsec entre um concentrador Cisco VPN 3000 e um roteador Cisco com padrão de codificação avançado (AES) como o algoritmo de criptografia.

O AES é uma nova publicação do Federal Information Processing Standard (FIPS) criada pelo National Institute of Standards and Technology (NIST) para ser usada como método de criptografia. Este padrão especifica um algoritmo de criptografia simétrica AES que substitui o DES (Data Encryption Standard, Padrão de Criptografia de Dados) como uma transformação de privacidade para IPsec e Internet Key Exchange (IKE). O AES tem três comprimentos de chave diferentes, uma chave de 128 bits (o padrão), uma chave de 192 bits e uma chave de 256 bits. O recurso AES no Cisco IOS® adiciona suporte para o novo padrão de criptografia AES, com CBC (Cipher Block Chaining, encadeamento de bloco de cifra) modo, ao IPsec.

Consulte o site NIST Computer Security Resource Center para obter mais informações sobre AES.

Consulte Túnel IPsec LAN a LAN entre o Cisco VPN 3000 Concentrator e o PIX Firewall Exemplo

para obter mais informações sobre a configuração do túnel LAN a LAN entre um VPN 3000 Concentrator e o PIX Firewall.

Consulte o Exemplo de Configuração de Túnel IPsec Entre PIX 7.x e VPN 3000 Concentrator para obter mais informações quando o PIX tem a versão de software 7.1.

Prerequisites

Requirements

Este documento requer uma compreensão básica do protocolo de IPSec. Consulte Uma Introdução à Criptografia IPSec para saber mais sobre o IPsec.

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- **Requisitos do roteador** - O recurso AES foi introduzido no Cisco IOS Software Release 12.2(13)T. Para habilitar o AES, seu roteador deve suportar IPsec e executar uma imagem do IOS com "k9" longas keys (o subsistema "k9").**Observação:** o suporte de hardware para AES também está disponível nos módulos VPN de aceleração AES Cisco 2600XM, 2691, 3725 e 3745. Este recurso não tem implicações de configuração e o módulo de hardware é selecionado automaticamente se ambos estiverem disponíveis.
- **Requisitos do VPN Concentrator** - O suporte de software para o recurso AES foi introduzido na versão 3.6. O suporte de hardware é fornecido pelo novo processador de criptografia aprimorado e escalável (SEP-E). Este recurso não tem implicações de configuração.**Observação:** no Cisco VPN 3000 Concentrator versão 3.6.3, os túneis não negociam com AES devido à ID de bug da Cisco CSCdy88797 (somente clientes registrados) . Isso foi resolvido na versão 3.6.4.**Observação:** o Cisco VPN 3000 Concentrator usa módulos SEP ou SEP-E, não ambos. Não instale ambos no mesmo dispositivo. Se você instalar um módulo SEP-E em um VPN Concentrator que já contenha um módulo SEP, o VPN Concentrator desabilitará o módulo SEP e usará somente o módulo SEP-E.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware:

- Cisco 3600 Series Router com Cisco IOS Software Release 12.3(5)
- Cisco VPN 3060 Concentrator com Software Release 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

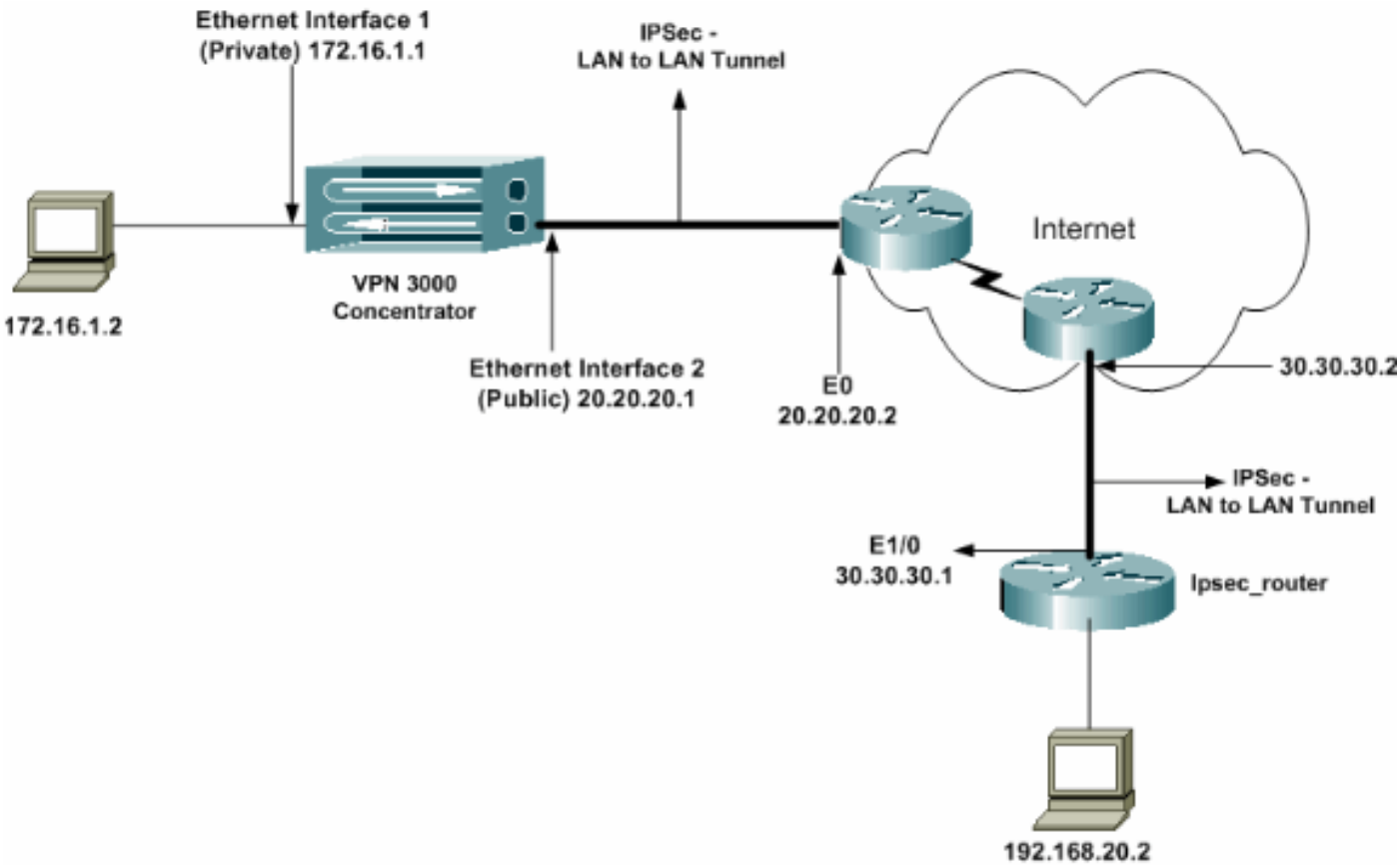
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Roteador IPsec
- Concentrador de VPN

Configuração do ipsec_router

```
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
```

Observação: embora a sintaxe da ACL seja inalterada, os significados são ligeiramente diferentes para ACLs criptografadas. Em ACLs criptografadas, **permit** especifica que os pacotes correspondentes devem ser criptografados, enquanto **deny** especifica que os pacotes correspondentes não precisam ser criptografados.

Configurar o VPN Concentrator

Os VPN Concentrators não são pré-programados com endereços IP em suas configurações de fábrica. Você precisa usar a porta de console para configurar as configurações iniciais que são uma interface de linha de comando (CLI) baseada em menu. Consulte Configurando Concentradores VPN através do Console para obter informações sobre como configurar através do console.

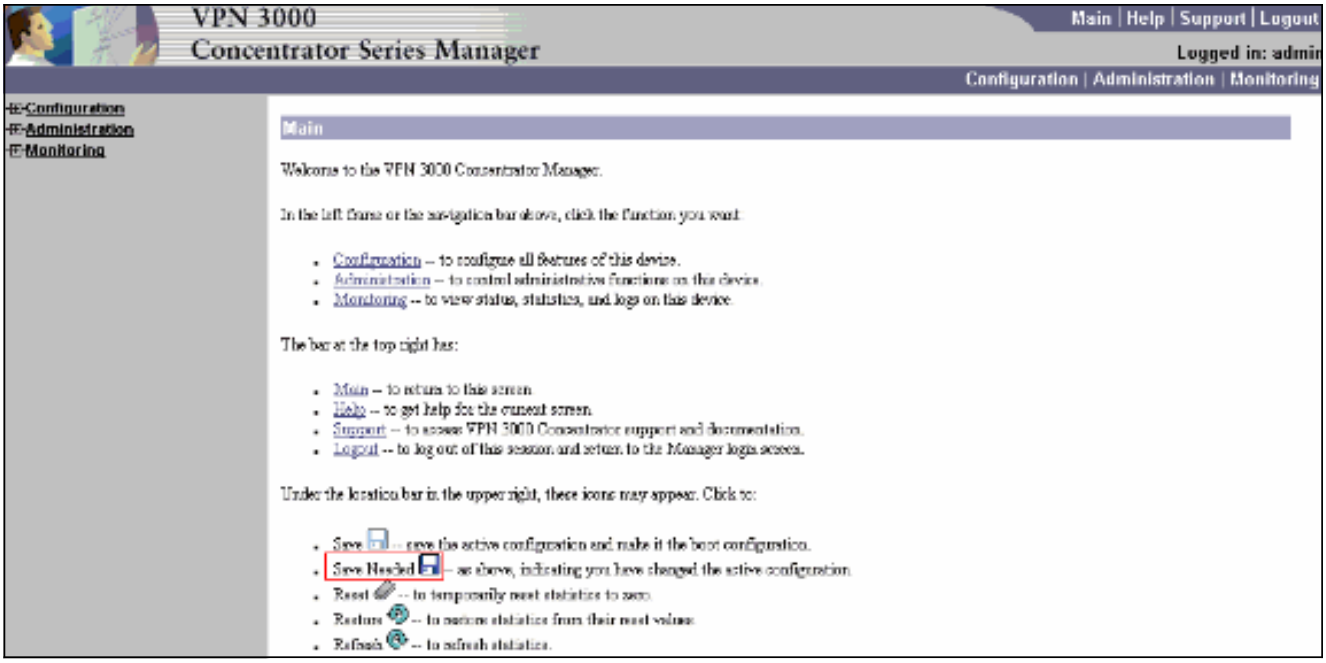
Depois que o endereço IP na interface Ethernet 1 (privada) é configurado, o restante pode ser configurado usando a CLI ou através da interface do navegador. A interface do navegador suporta HTTP e HTTP sobre SSL (Secure Socket Layer).

Esses parâmetros são configurados através do console:

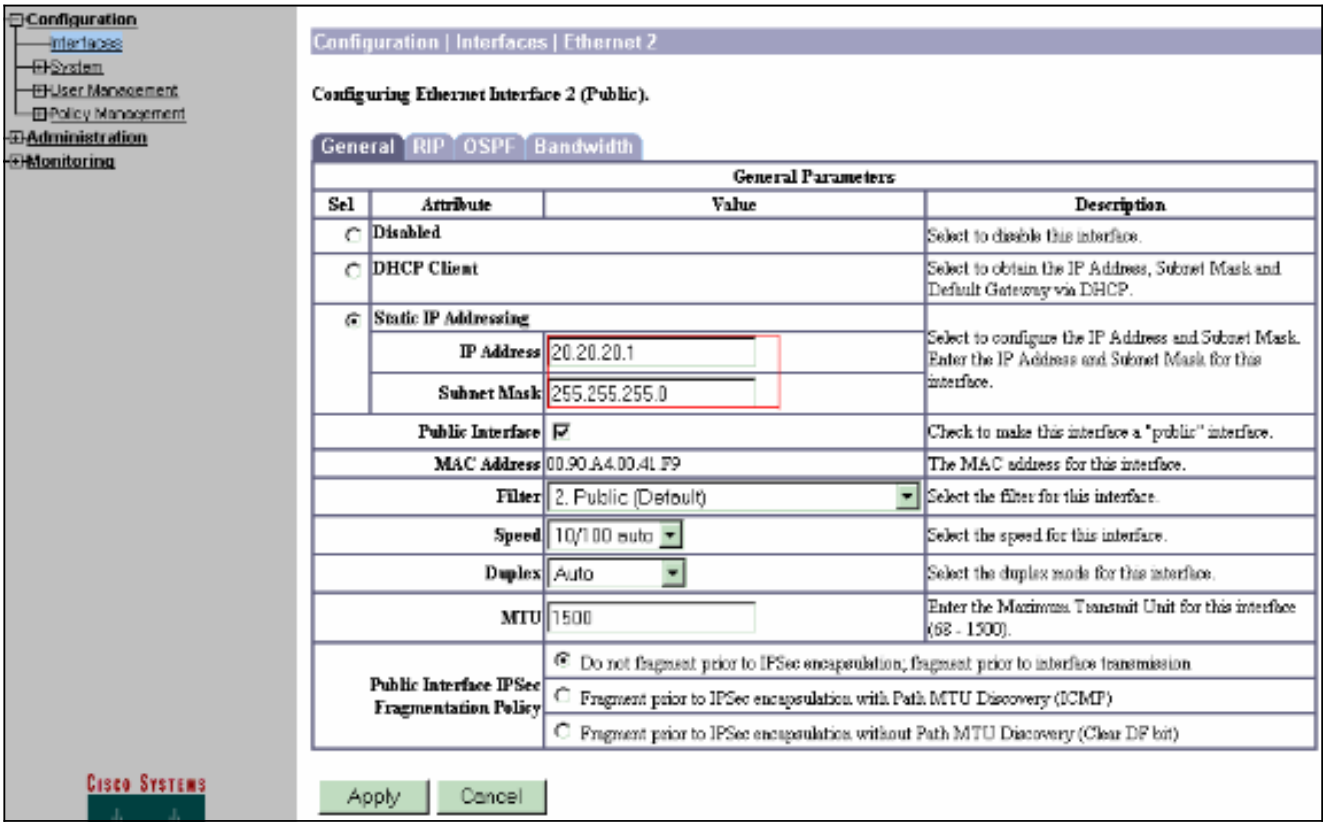
- **Hora/Data** - A hora e a data corretas são muito importantes. Eles ajudam a garantir que os registros e registros contabilísticos sejam precisos e que o sistema possa criar um certificado de segurança válido.
- **Interface Ethernet 1 (privada)** - O endereço IP e a máscara (da nossa topologia de rede 172.16.1.1/24).

Neste ponto, o VPN Concentrator é acessível por meio de um navegador HTML da rede interna. Para obter informações sobre como configurar o VPN Concentrator no modo CLI, consulte Configuração rápida usando CLI.

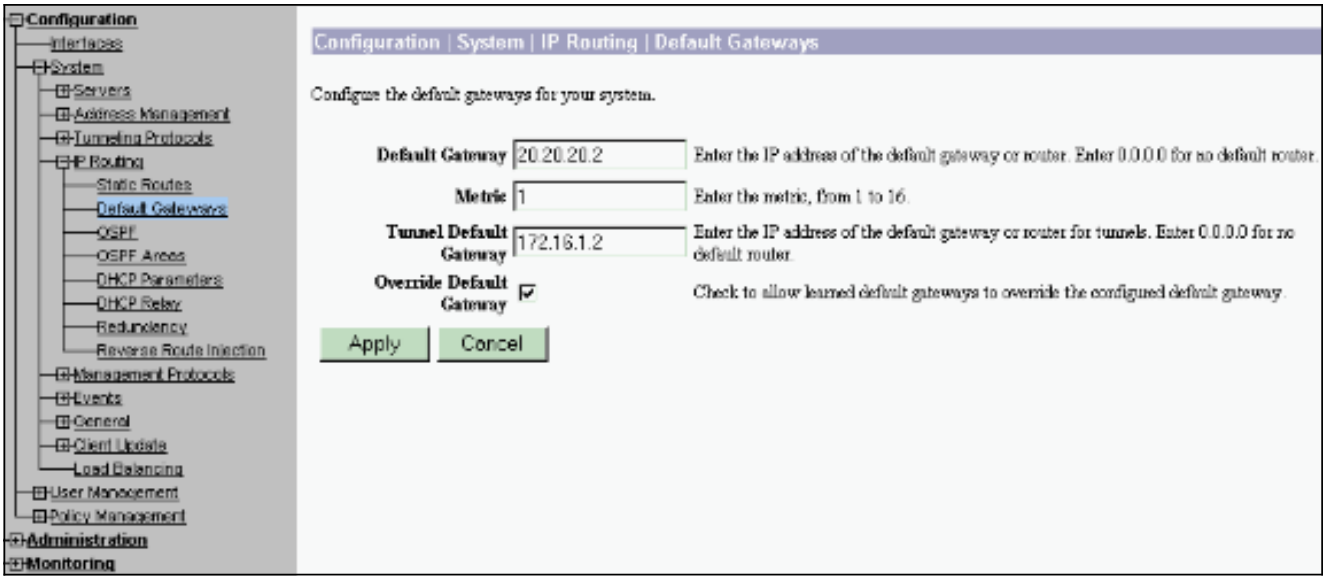
1. Digite o endereço IP da interface privada a partir do navegador da Web para ativar a interface GUI.Clique no ícone **save required** para salvar as alterações na memória. O nome de usuário e a senha padrão de fábrica são "admin", que diferencia maiúsculas de minúsculas.



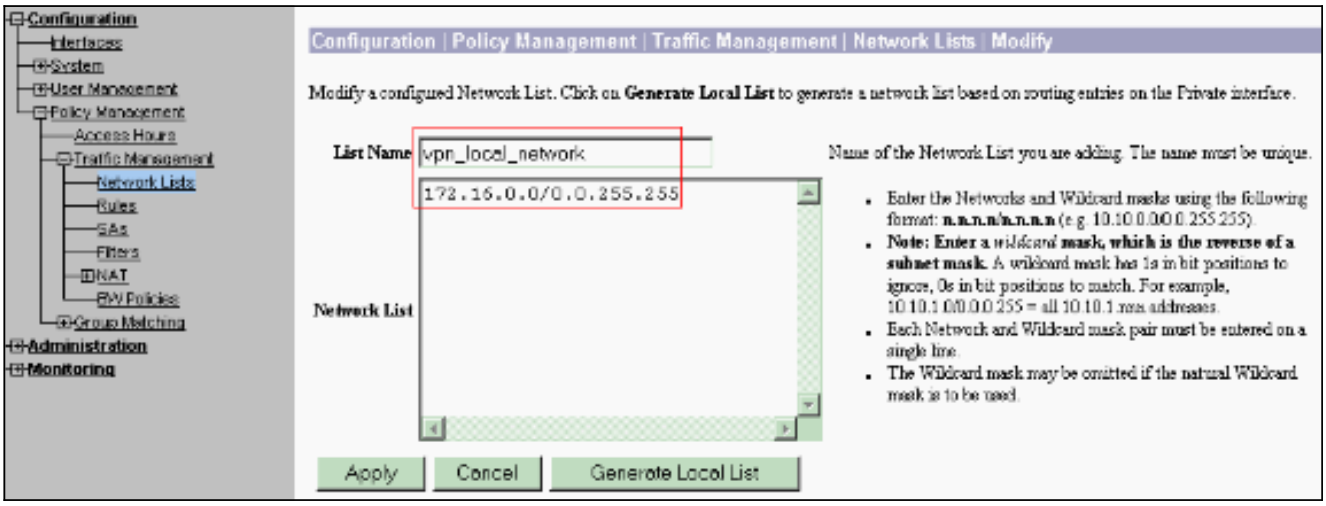
2. Depois de exibir a GUI, selecione **Configuration > Interfaces > Ethernet 2 (Public)** para configurar a interface Ethernet
2.



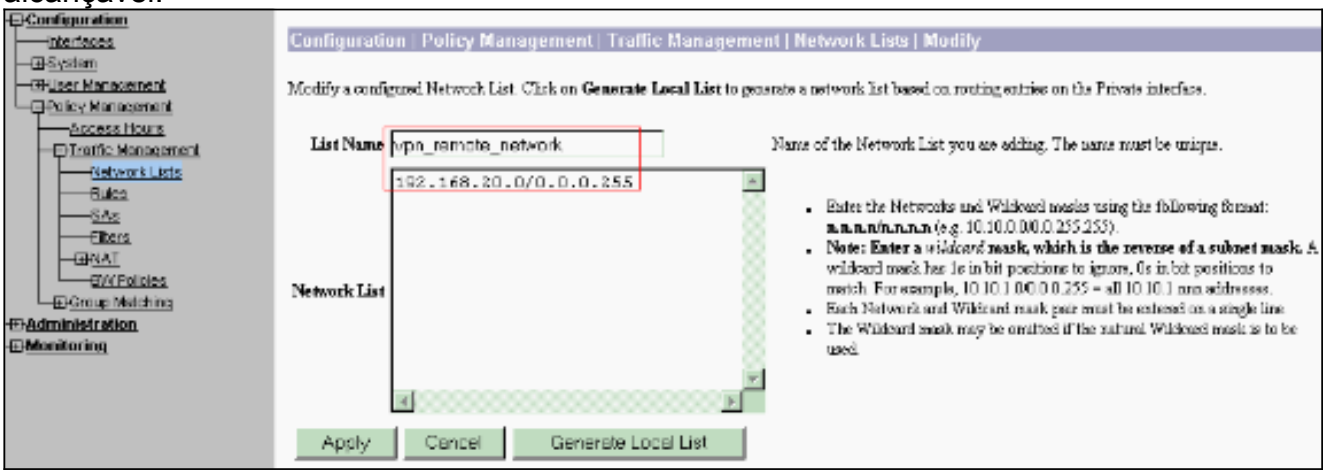
3. Selecione **Configuration > System > IP Routing > Default Gateways** configure o gateway padrão (Internet) e o gateway padrão de túnel (interno) para IPsec para acessar as outras sub-redes na rede privada.Neste cenário, há apenas uma sub-rede disponível na rede interna.



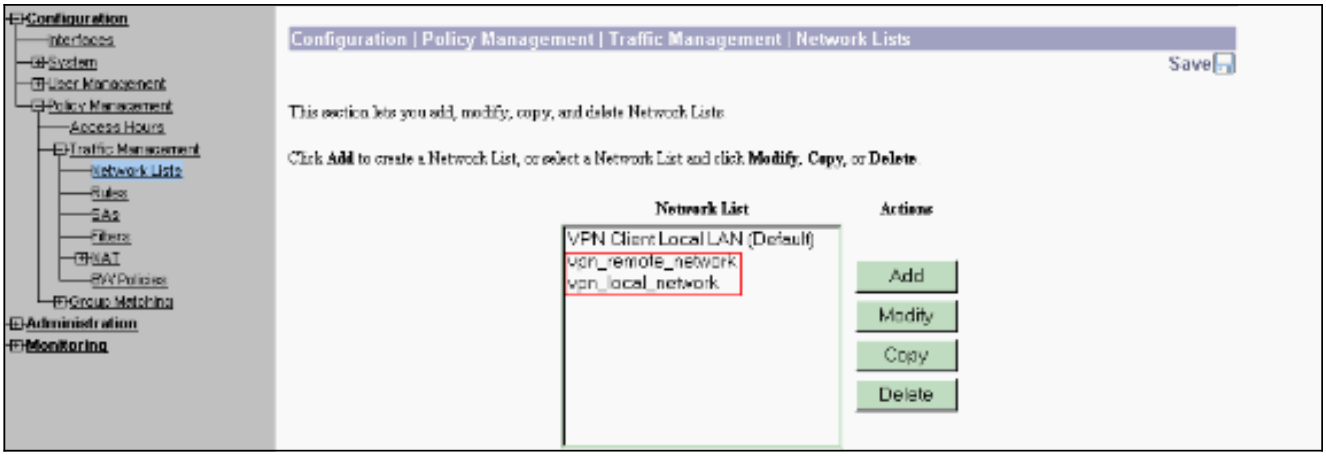
4. Selecione Configuration > **Policy Management > Traffic Management > Network Lists > Add** para criar as listas de rede que definem o tráfego a ser criptografado.As redes mencionadas na lista podem ser acessadas à rede remota. As redes mostradas na lista abaixo são redes locais. Você também pode gerar a lista de redes locais automaticamente via RIP quando clica em **Gerar lista local**.



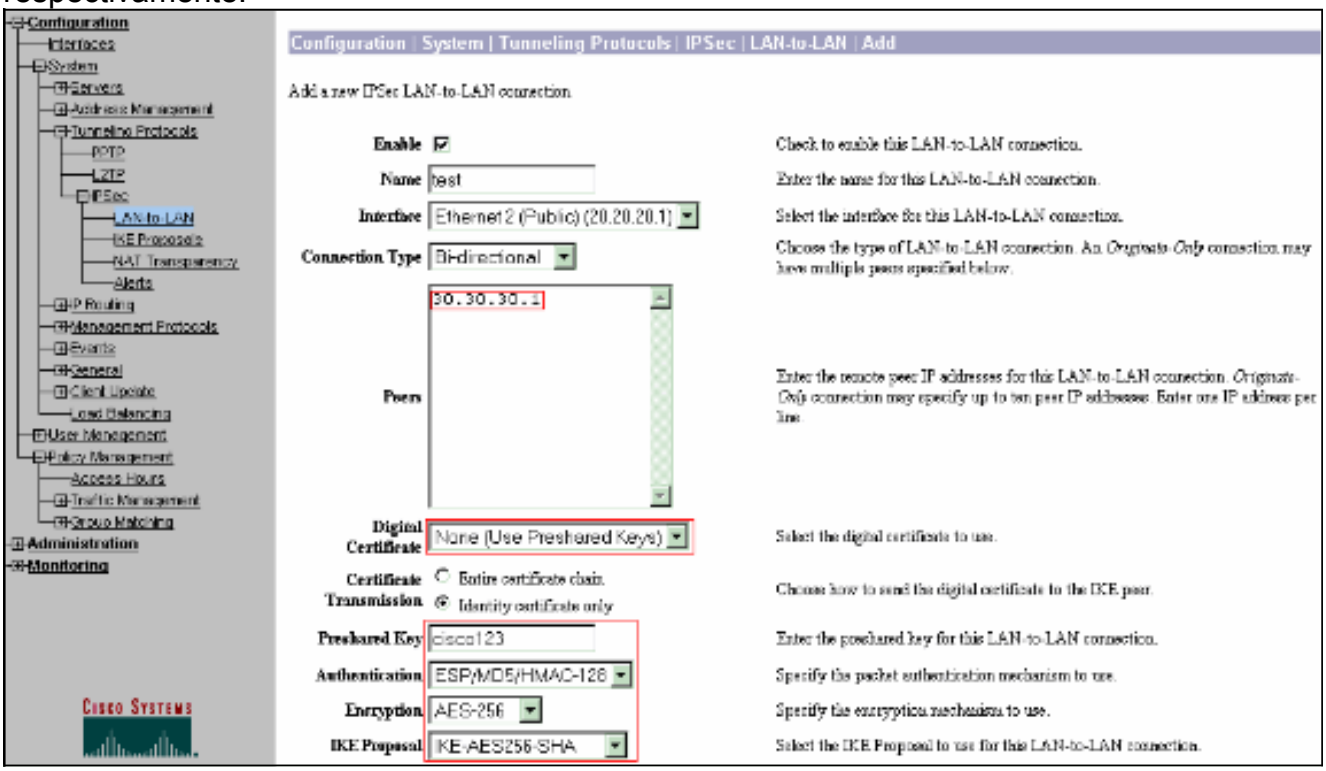
5. As redes nesta lista são redes remotas e precisam ser configuradas manualmente. Para fazer isso, insira a rede/curinga de cada sub-rede alcançável.

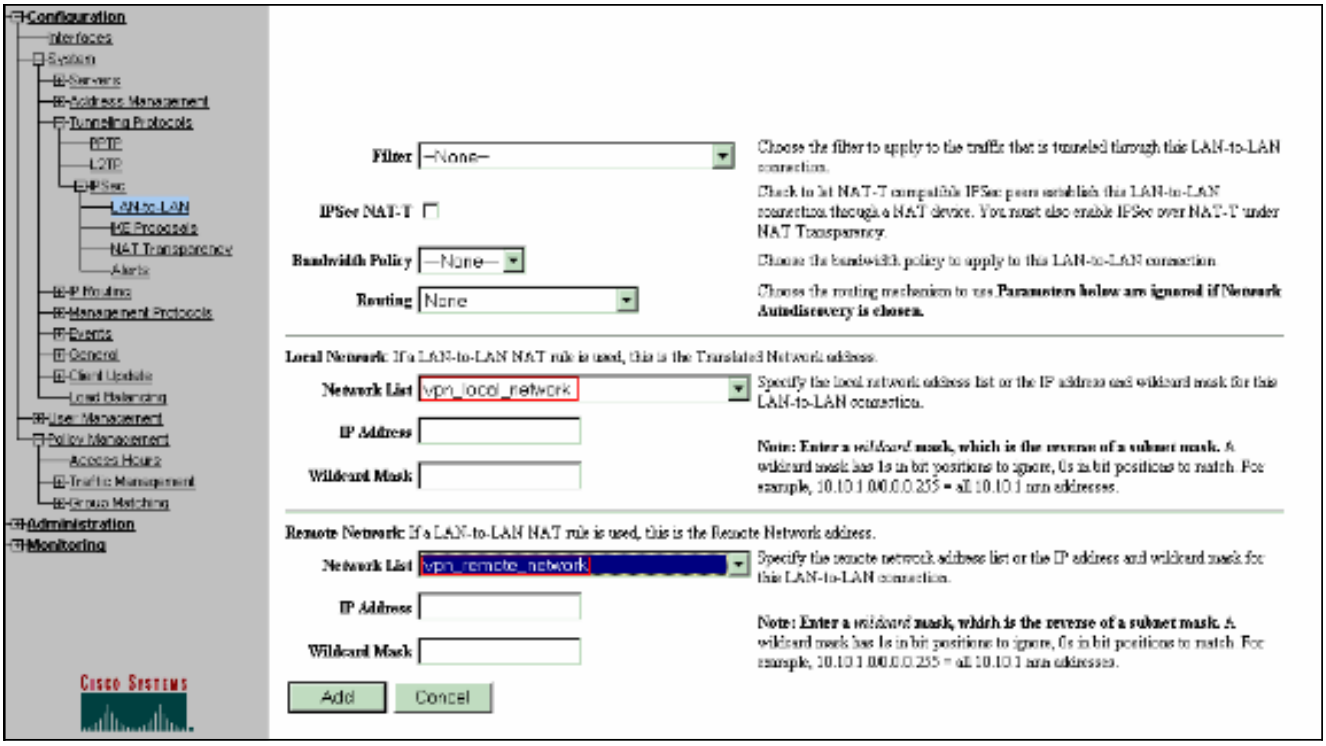


Quando concluídas, estas são as duas listas de rede:

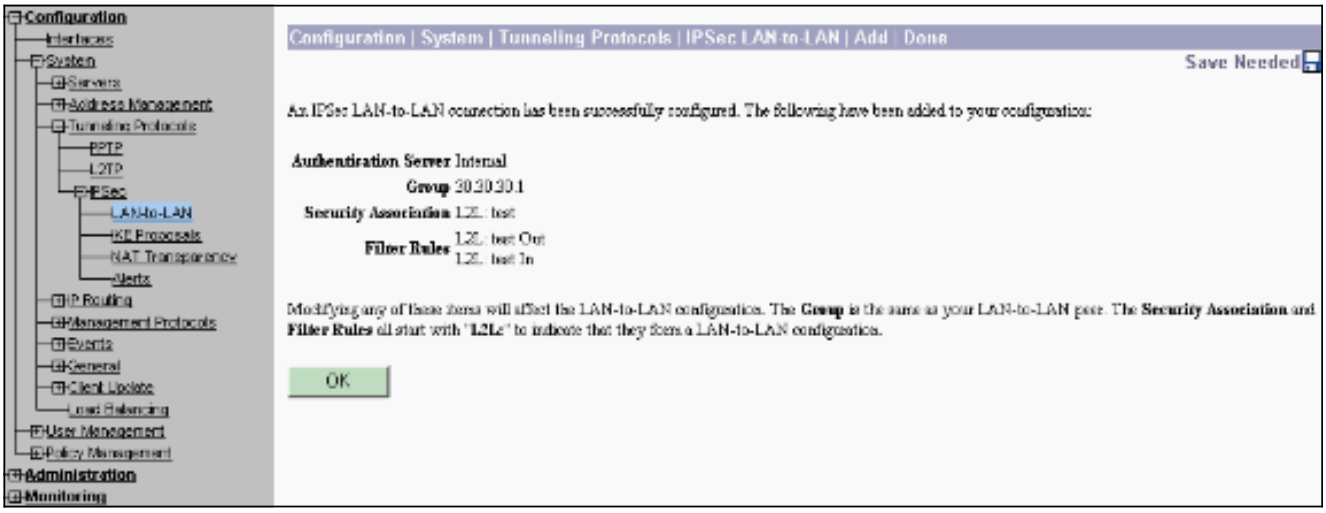


6. Selecione Configuration > **System > Tunneling Protocols > IPSec LAN-to-LAN > Add** e defina o túnel LAN-to-LAN.Esta janela tem três seções. A seção superior é para as informações de rede e as duas seções inferiores são para as listas de rede local e remota. Na seção Network Information (Informações da rede), selecione a criptografia AES, o tipo de autenticação, a proposta IKE e digite a chave pré-compartilhada. Nas seções inferiores, aponte para as listas de rede que você já criou, as listas Local e Remota, respectivamente.



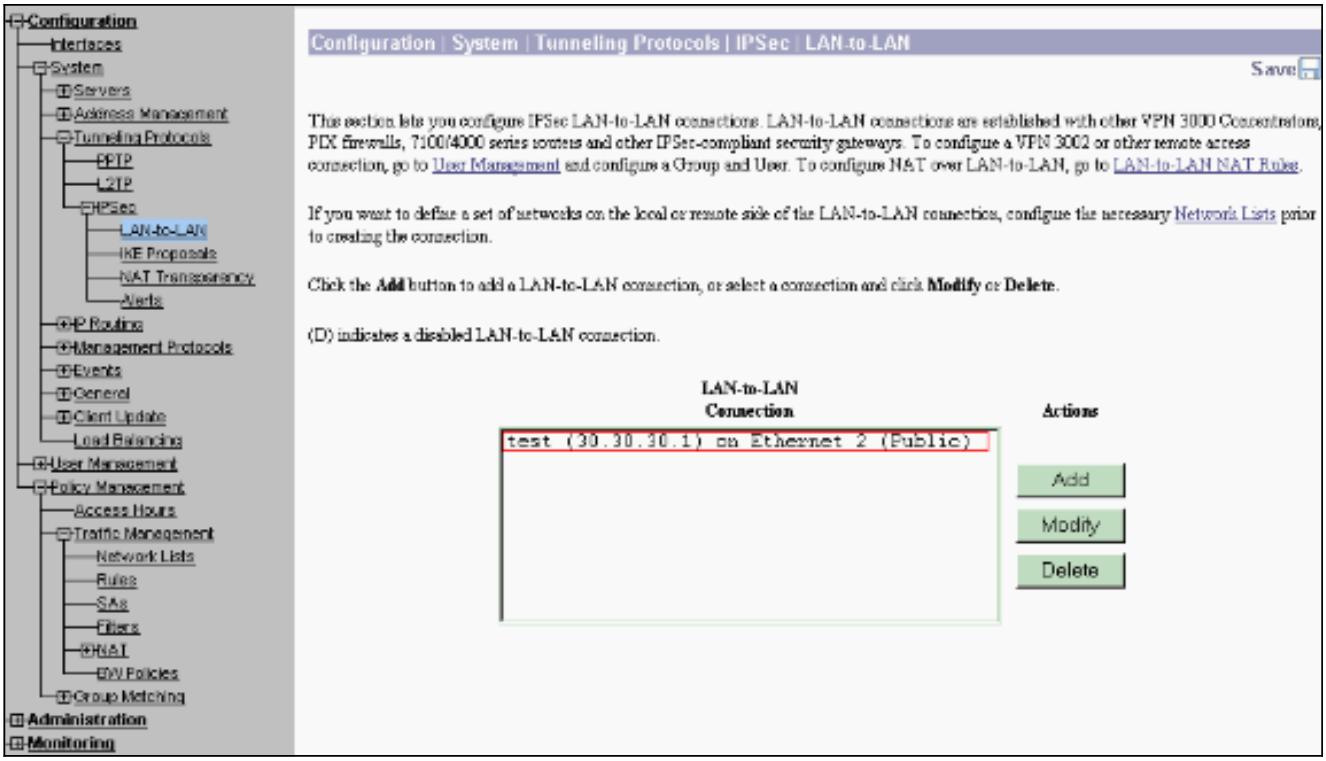


7. Depois de clicar em **Adicionar**, se sua conexão estiver correta, você verá a janela Add-Done de LAN para LAN do IPSec.Essa janela apresenta uma sinopse das informações de configuração do túnel. Ele também configura automaticamente o nome do grupo, o nome SA e o nome do filtro. Você pode editar qualquer parâmetro nesta tabela.



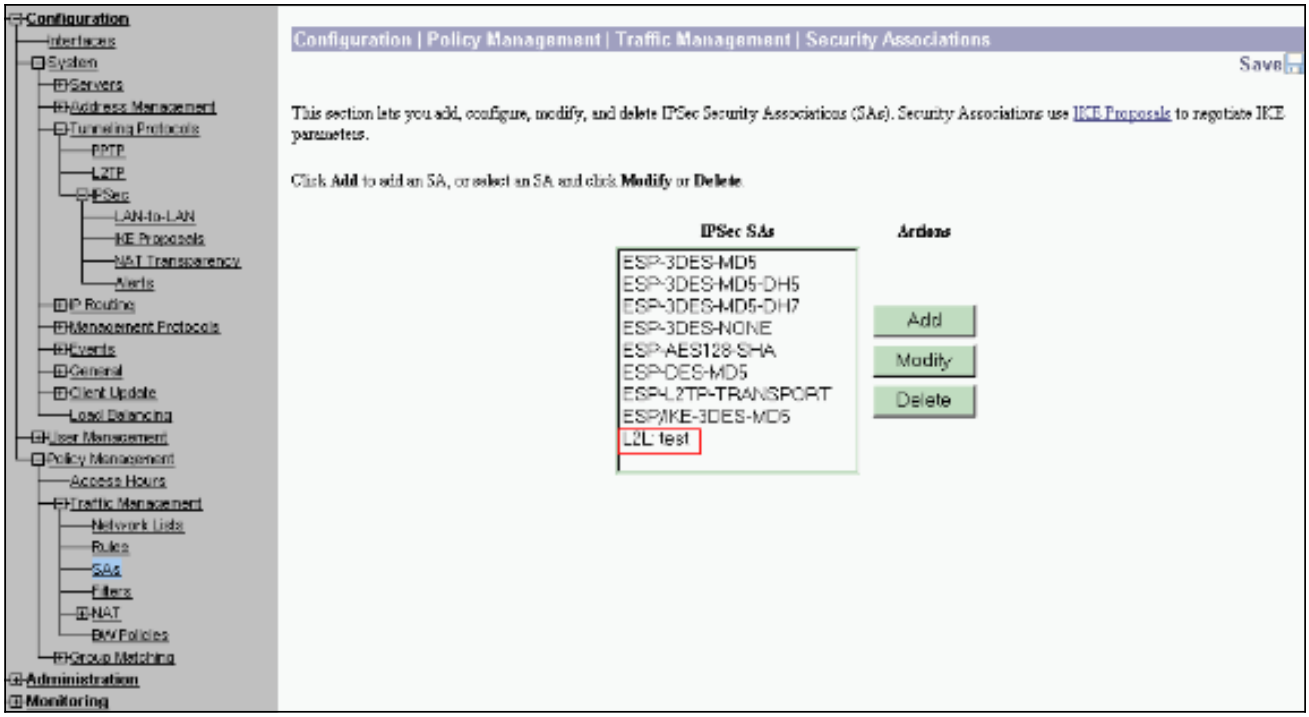
Neste ponto, o túnel de LAN para LAN do IPsec foi configurado e você pode começar a trabalhar. Se, por algum motivo, o túnel não funcionar, você poderá verificar se há configurações incorretas.

8. Você pode visualizar ou modificar os parâmetros de IPsec LAN a LAN criados anteriormente ao selecionar **Configuração > Sistema > Protocolos de tunelamento > IPSec LAN a LAN**.Este gráfico mostra "teste" como o nome do túnel e a interface pública da extremidade remota é 30.30.30.1 conforme o cenário.

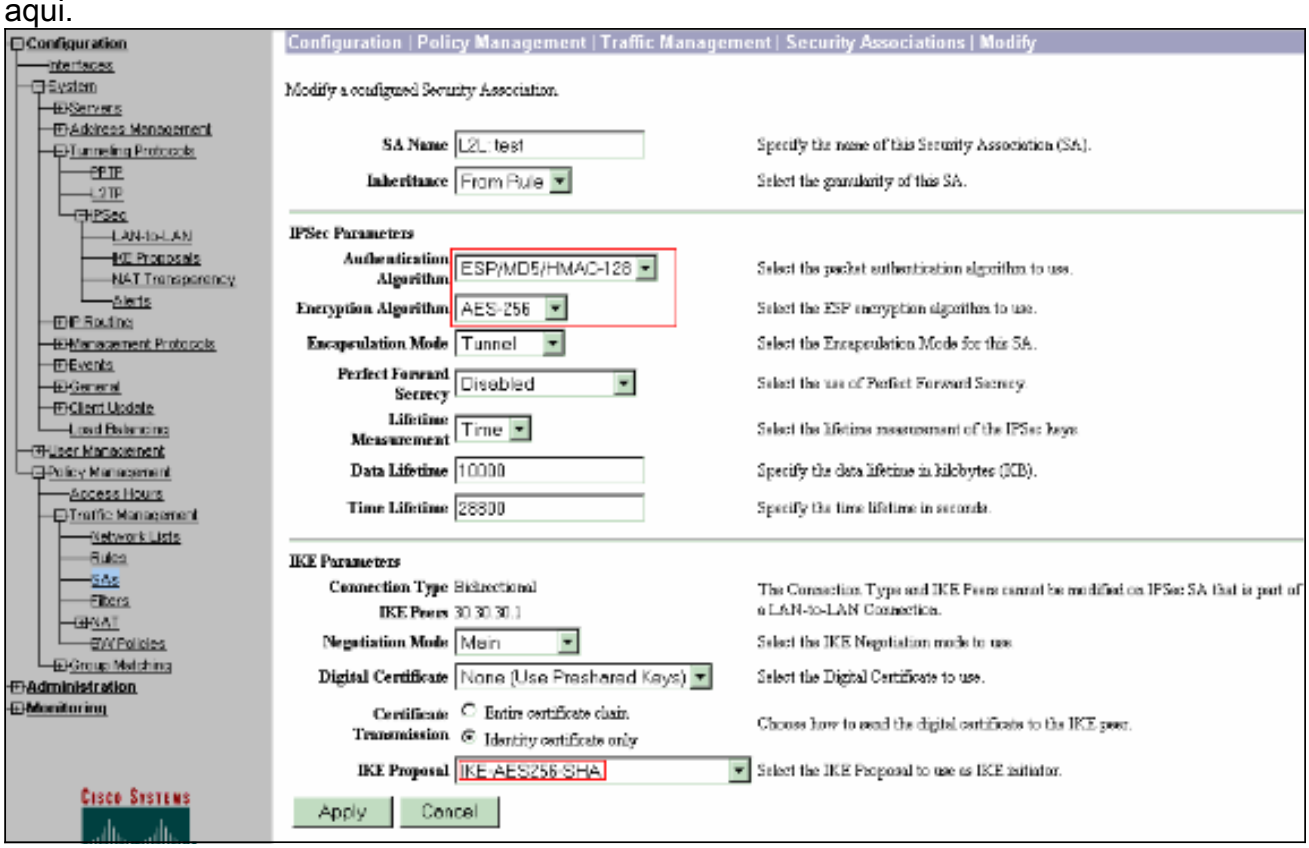


9. Às vezes, seu túnel pode não aparecer se sua proposta de IKE estiver na lista de propostas inativas. Selecione Configuração **> Sistema > Protocolos de tunelamento > IPSec > Propostas IKE** para configurar a proposta IKE ativa.Se sua proposta de IKE estiver na lista "Propostas inativas", você poderá ativá-la quando selecionar a proposta de IKE e clicar no botão **Ativar**. Neste gráfico, a proposta selecionada "IKE-AES256-SHA" está na lista de propostas
ativas.

10. Selecione **Configuration > Policy Management > Traffic Management > Security Associations** para verificar se os parâmetros SA estão
corretos.



11. Clique no nome SA (neste caso, **L2L: teste**) e clique em **Modificar** para verificar as SAs.Se algum dos parâmetros não corresponder à configuração de peer remoto, ele poderá ser alterado
aqui.



Verificar

Verifique a configuração do roteador

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto isakmp sa** — Exibe todas as SAs IKE atuais em um peer. O estado QM_IDLE indica que o SA permanece autenticado com seu par e pode ser usado para trocas de modo rápido subsequentes. Está em um estado silencioso.

```
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** —Exibe as configurações usadas pelas SAs atuais. Verifique os endereços IP dos pares, as redes acessíveis nas extremidades local e remota e o conjunto de transformações usado. Há duas SAs ESP, uma em cada direção. Como os conjuntos de transformação AH são usados, ele está vazio.

```
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:
```

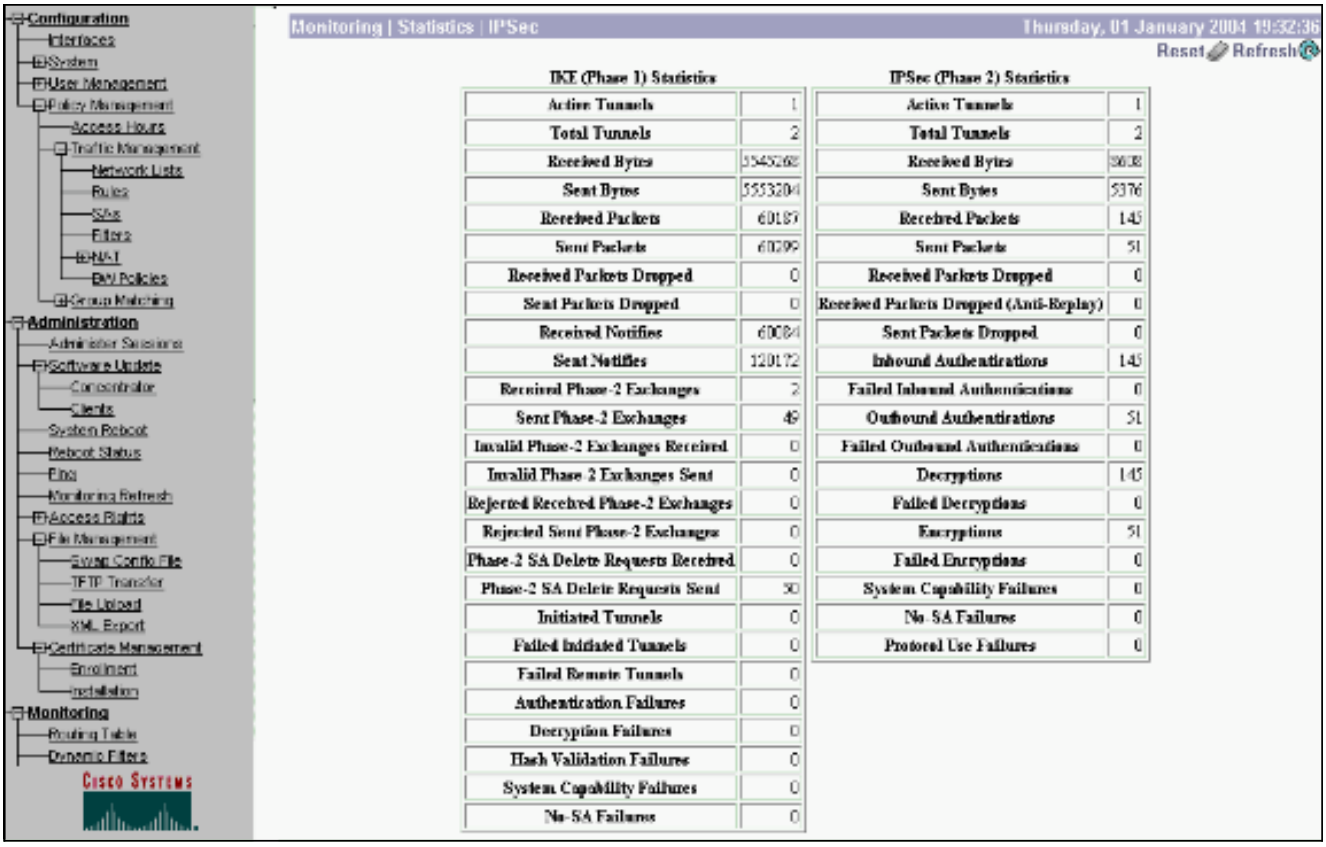
- **show crypto engine connections ative** — Exibe as conexões de sessão criptografada ativas atuais para todos os mecanismos de criptografia. Cada ID de conexão é exclusiva. O número de pacotes criptografados e descriptografados é exibido nas duas últimas colunas.

```
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
```

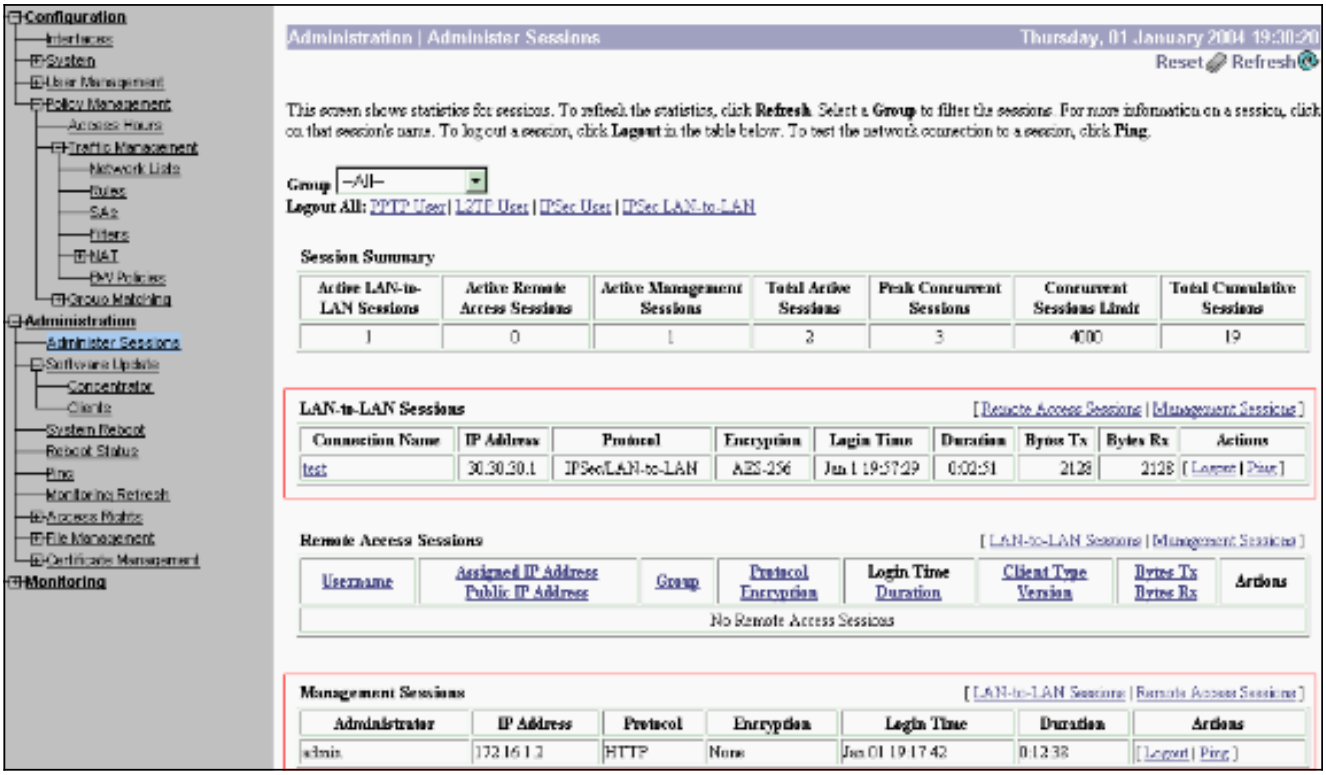
Verifique a configuração do VPN Concentrator

Conclua estes passos para verificar a configuração do VPN Concentrator.

1. Semelhante aos comandos show crypto ipsec sa e **show crypto isakmp sa** nos roteadores, você pode exibir as estatísticas de IPsec e IKE quando seleciona **Monitoring > Statistics > IPSec** nos VPN
   Concentrators.



2. Semelhante ao comando **show crypto engine connections ative** em roteadores, você pode usar a janela Administration-Sessions no VPN Concentrator para exibir os parâmetros e as estatísticas de todas as conexões LAN para LAN IPsec ativas ou túneis.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Solucionar problemas do roteador

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

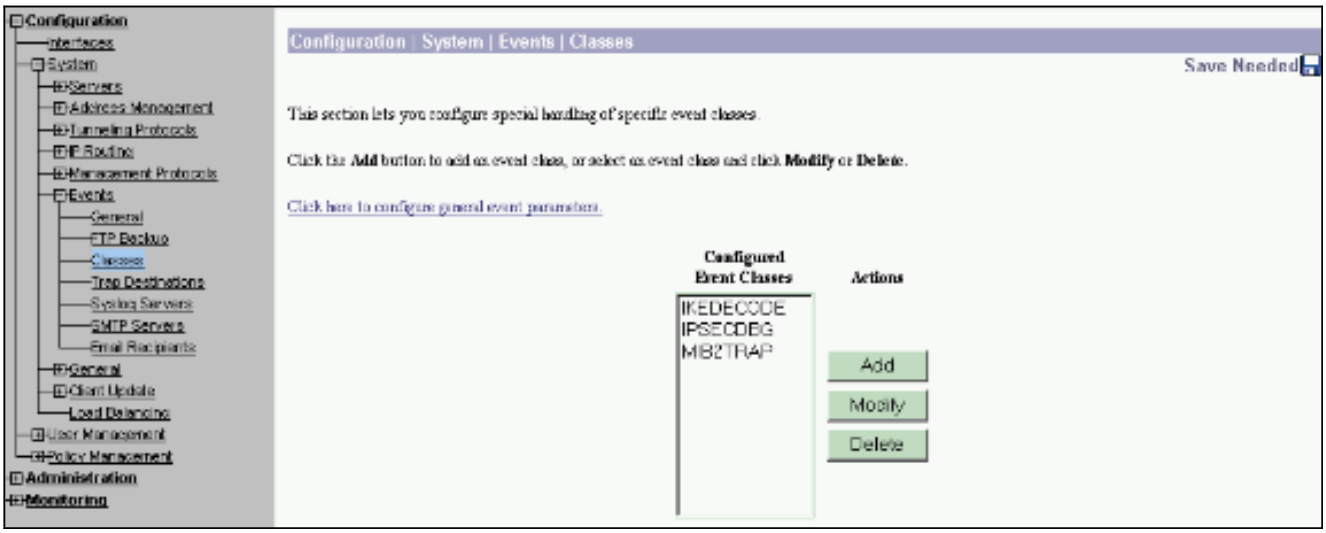
- **debug crypto engine — Exibe o tráfego que está criptografado.** O mecanismo de criptografia é o mecanismo real que executa criptografia e descriptografia. Um mecanismo de criptografia pode ser um software ou um acelerador de hardware.
- **debug crypto isakmp** — Exibe as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1 do IKE.
- **debug crypto ipsec** — Exibe as negociações de IPsec da fase 2 do IKE.

Consulte Solução de problemas de IPSec - Entendendo e usando comandos **debug** para obter informações mais detalhadas e saída de exemplo.

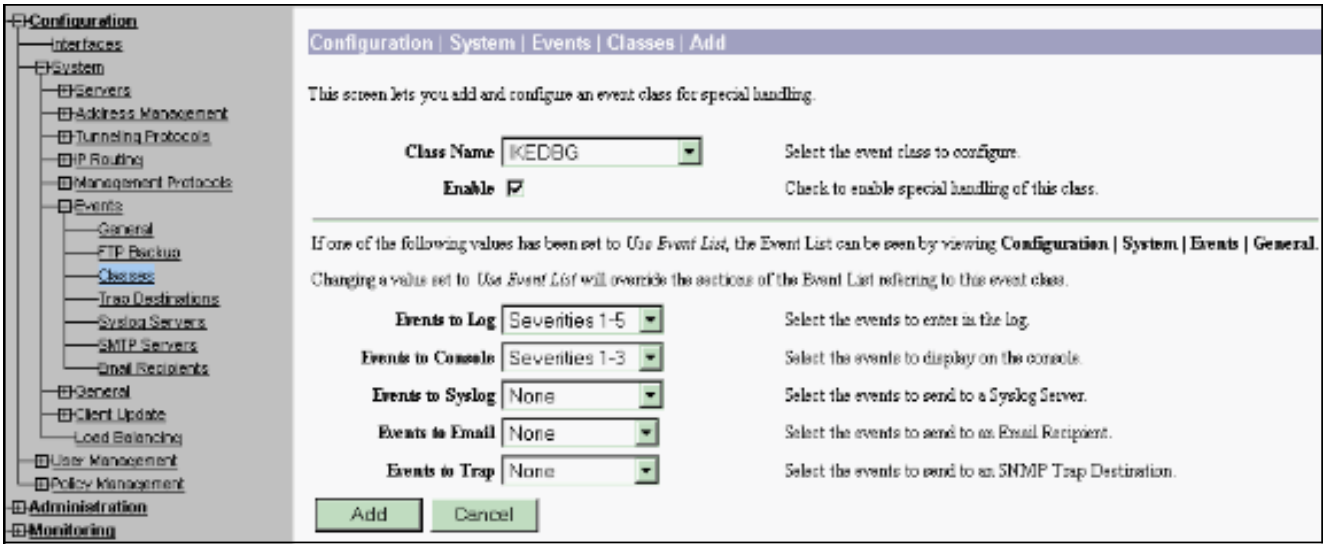
Solucionar problemas do VPN Concentrator

Semelhante aos comandos **debug** nos roteadores Cisco, você pode configurar classes de evento para exibir todos os alarmes.

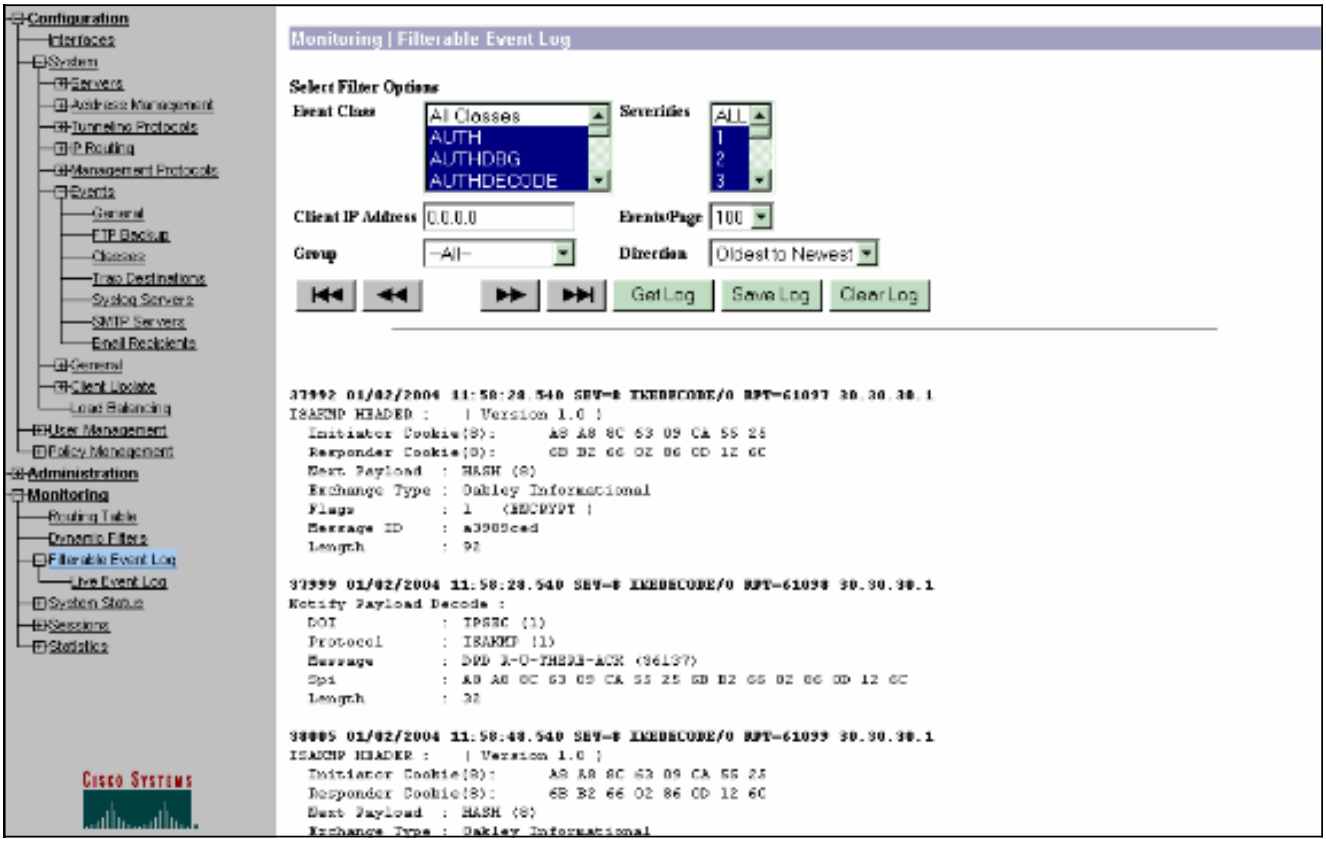
1. Selecione Configuration **> System > Events > Classes > Add** para ativar o registro de classes de evento.Essas classes estão disponíveis para IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. Ao adicionar, você também pode selecionar o nível de Gravidade para cada classe, com base no nível de Gravidade que o alarme é enviado.Os alarmes podem ser tratados por um destes métodos:Por logExibido no consoleEnviado para o servidor Syslog UNIXEnviado como e-mailEnviado como armadilha para um servidor de Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol)



3. Selecione **Monitoring** > **Filterable Event Log** para monitorar os alarmes ativados.



Informações Relacionadas

- Advanced Encryption Standard (AES)
- Módulo de criptografia DES/3DES/AES VPN
- Configurações de exemplo de IPSec
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de Suporte de Negociação IPSec/Protocolos IKE

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.