Esempio di tunnel IPsec LAN a LAN tra un concentratore Cisco VPN 3000 e un router con configurazione AES

Sommario

Introduzione

In questo documento viene spiegato come configurare un tunnel IPsec tra un concentratore Cisco VPN 3000 e un router Cisco con Advanced Encryption Standard (AES) come algoritmo di crittografia.

AES è una nuova pubblicazione FIPS (Federal Information Processing Standard) creata dal National Institute of Standards and Technology (NIST) per essere utilizzata come metodo di crittografia. Questo standard specifica un algoritmo di crittografia simmetrica AES che sostituisce Data Encryption Standard (DES) come trasformazione della privacy sia per IPsec che per IKE (Internet Key Exchange). AES ha tre diverse lunghezze di chiave, una a 128 bit (predefinita), una a 192 bit e una a 256 bit. La funzionalità AES di Cisco IOS® aggiunge il supporto per il nuovo standard di crittografia AES, con modalità CBC (Cipher Block Chaining), a IPsec.

Per ulteriori informazioni su AES, fare riferimento al sito Centro risorse per la sicurezza dei computer NIST.

Per ulteriori informazioni sulla configurazione del tunnel LAN-LAN tra un concentratore VPN 3000 e un firewall PIX, fare riferimento agli esempi di tunnel IPsec LAN-LAN tra un concentratore VPN

3000 e un firewall PIX.

Per ulteriori informazioni sulla versione del PIX con software 7.1, fare riferimento all'esempio di configurazione del tunnel IPsec tra i PIX 7.x e la VPN 3000 Concentrator.

Prerequisiti

Requisiti

Questo documento richiede una comprensione di base del protocollo IPsec. per ulteriori informazioni su IPSec, fare riferimento a Introduzione alla crittografia IPSec.

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- **Requisiti del router** - La funzione AES è stata introdotta nel software Cisco IOS versione 12.2(13)T. Per abilitare AES, il router deve supportare IPsec ed eseguire un'immagine IOS con chiavi lunghe "k9" (sottosistema "k9").**Nota:** il supporto hardware per AES è disponibile anche sui moduli VPN in accelerazione AES Cisco 2600XM, 2691, 3725 e 3745. Questa funzione non ha implicazioni sulla configurazione e il modulo hardware viene selezionato automaticamente se sono disponibili entrambi.
- **VPN Concentrator Requirements** - Il supporto software per la funzione AES è stato introdotto nella versione 3.6. Il supporto hardware è fornito dal nuovo processore di crittografia scalabile (SEP-E). Questa funzionalità non ha implicazioni a livello di configurazione.**Nota:** in Cisco VPN 3000 Concentrator versione 3.6.3, i tunnel non vengono negoziati su AES a causa dell'ID bug Cisco CSCdy88797 (solo utenti registrati). Questa condizione è stata risolta dalla release 3.6.4.**Nota:** Cisco VPN 3000 Concentrator utilizza moduli SEP o SEP-E, non entrambi. Non installare entrambi sulla stessa periferica. Se si installa un modulo SEP-E in un concentratore VPN che contiene già un modulo SEP, il concentratore VPN disabilita il modulo SEP e utilizza solo il modulo SEP-E.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware:

- Cisco serie 3600 Router con software Cisco IOS versione 12.3(5)
- Cisco VPN 3060 Concentrator con software versione 4.0.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

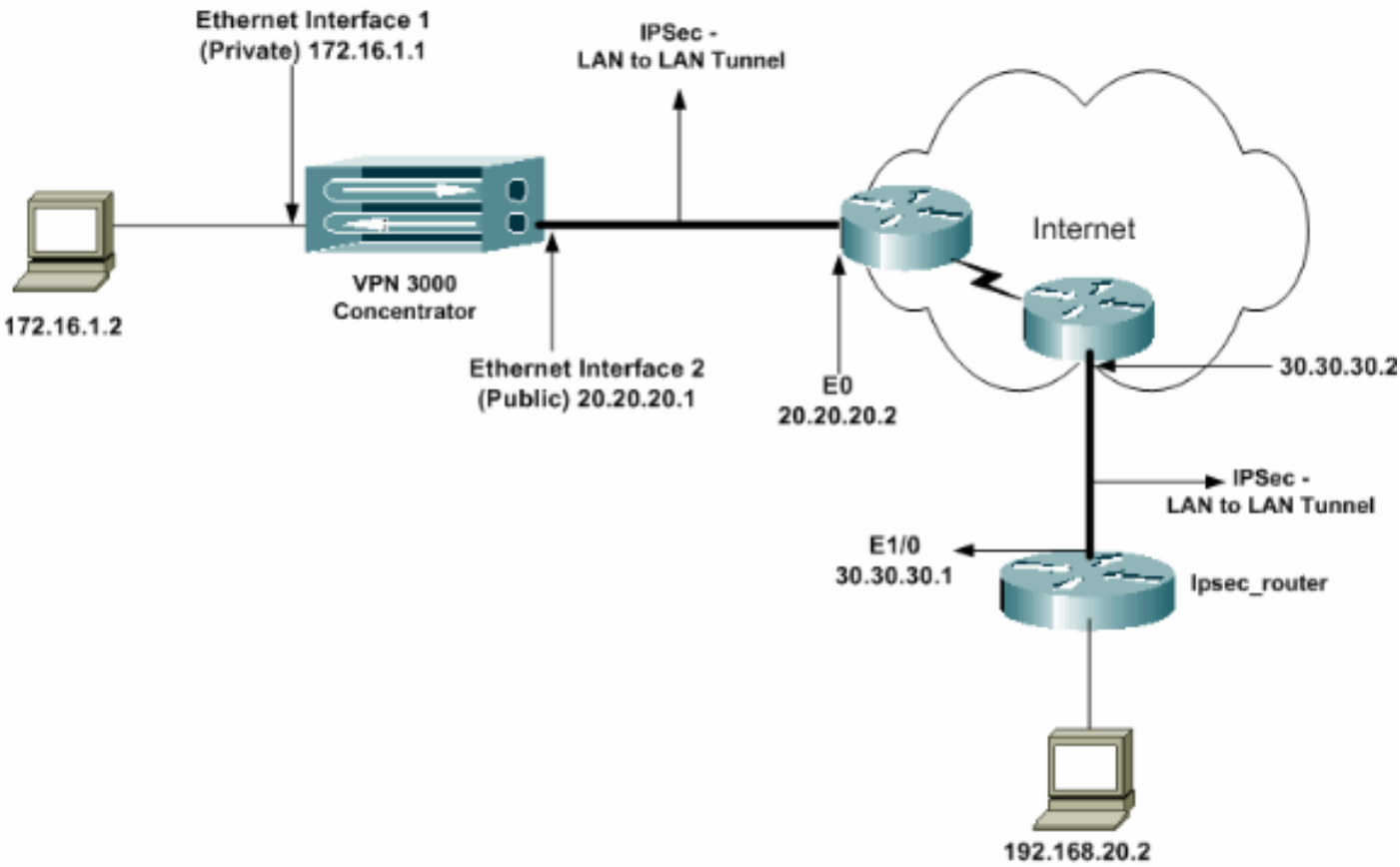
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Router IPsec
- VPN Concentrator

Configurazione 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
```

Nota: anche se la sintassi degli ACL non è stata modificata, i significati sono leggermente diversi per gli ACL crittografici. Negli ACL crittografici, il comando **allow** specifica che i pacchetti corrispondenti devono essere crittografati, mentre il comando **deny** specifica che non è necessario crittografare i pacchetti corrispondenti.

Configurare VPN Concentrator

I concentratori VPN non sono pre-programmati con indirizzi IP nelle impostazioni di fabbrica. È necessario utilizzare la porta della console per configurare le configurazioni iniziali, che sono un'interfaccia della riga di comando (CLI) basata su menu. Per informazioni su come configurare i concentratori VPN tramite la console, consultare il documento sulla configurazione dei concentratori VPN tramite la console.

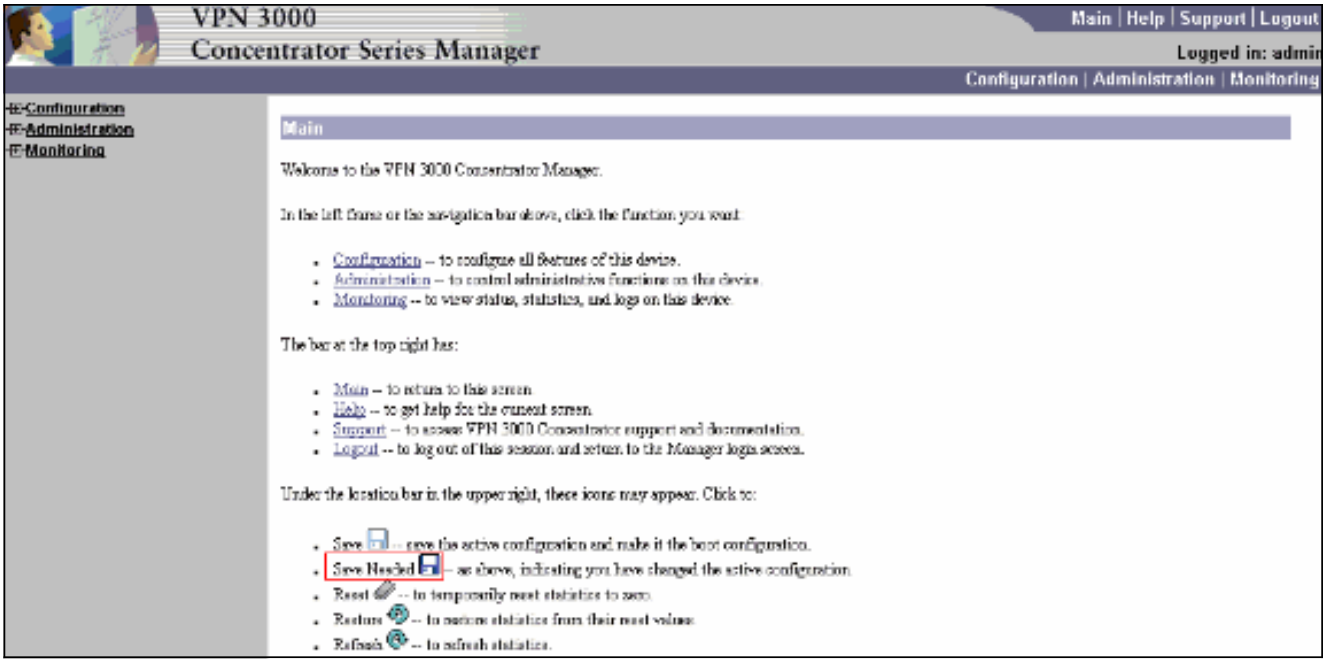
Dopo aver configurato l'indirizzo IP sull'interfaccia Ethernet 1 (privata), il resto può essere configurato sia dalla CLI che dall'interfaccia del browser. L'interfaccia del browser supporta sia HTTP che HTTP su SSL (Secure Sockets Layer).

Questi parametri vengono configurati tramite la console:

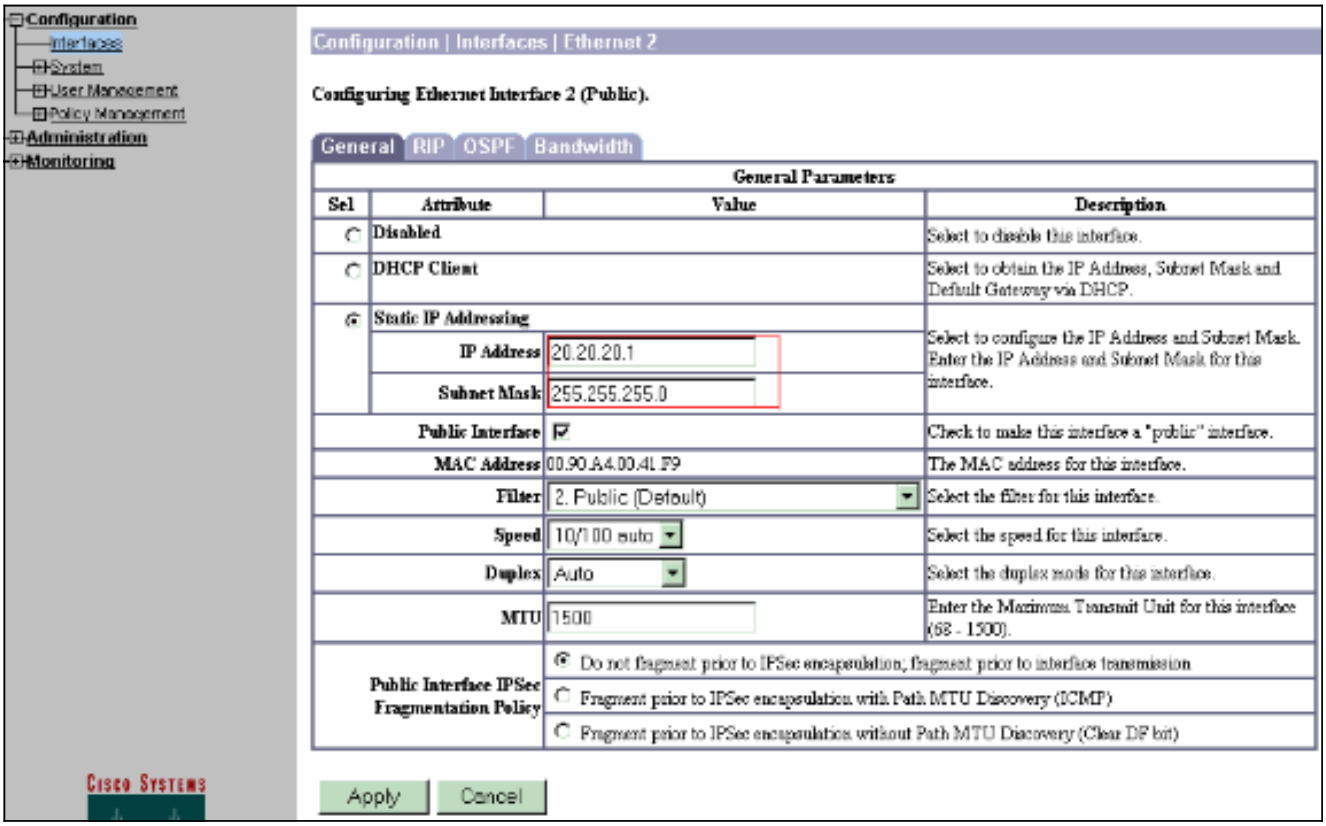
- **Ora/Data** - L'ora e la data corrette sono molto importanti. Garantiscono l'accuratezza delle voci di registrazione e di accounting e la possibilità di creare un certificato di protezione valido.
- **Ethernet 1 (private) interface** - Indirizzo IP e maschera (dalla topologia di rete 172.16.1.1/24).

A questo punto, VPN Concentrator è accessibile dalla rete interna tramite un browser HTML. Per informazioni sulla configurazione di VPN Concentrator in modalità CLI, consultare il documento sulla configurazione rapida tramite CLI.

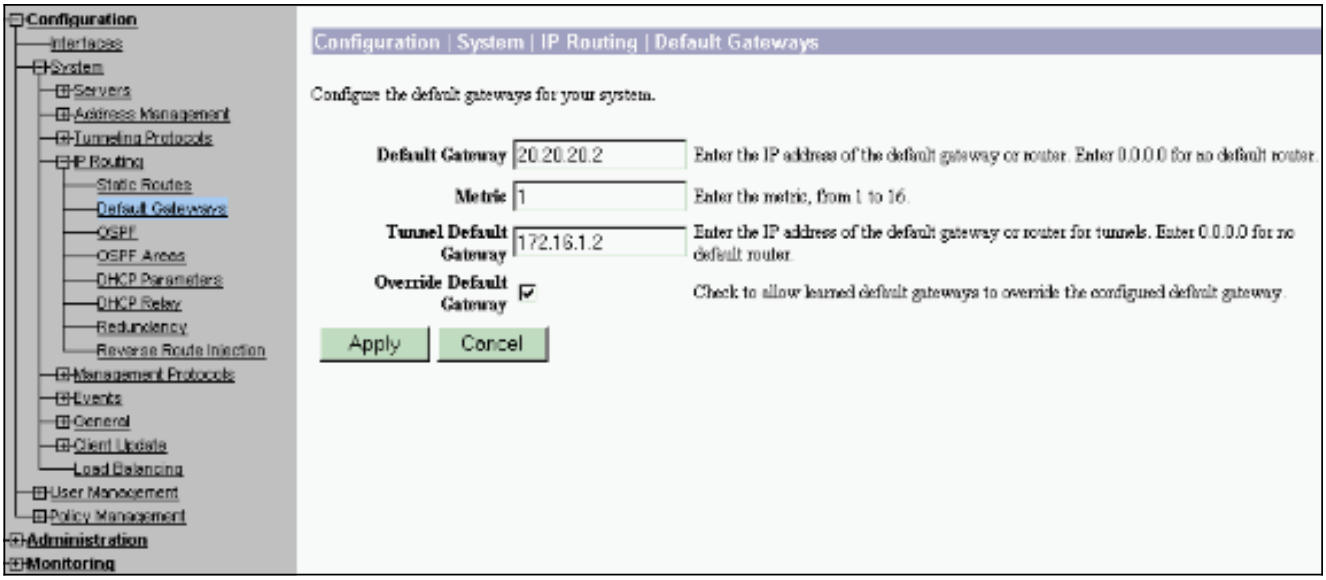
1. Digitare l'indirizzo IP dell'interfaccia privata dal browser Web per abilitare l'interfaccia GUI.Fare clic sull'icona **Save needed** (Salva le modifiche necessarie) per salvare le modifiche in memoria. Il nome utente e la password predefiniti di fabbrica sono "admin", che fa distinzione tra maiuscole e
minuscole.



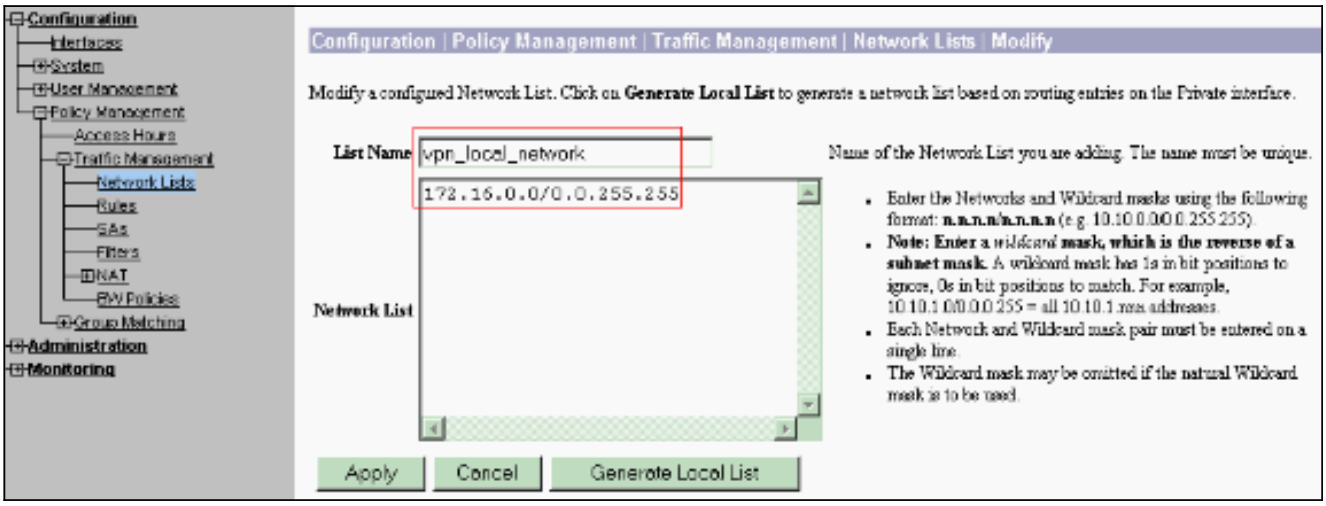
2. Dopo aver avviato la GUI, selezionare **Configuration > Interfaces > Ethernet 2 (Public)** per configurare l'interfaccia Ethernet
2.



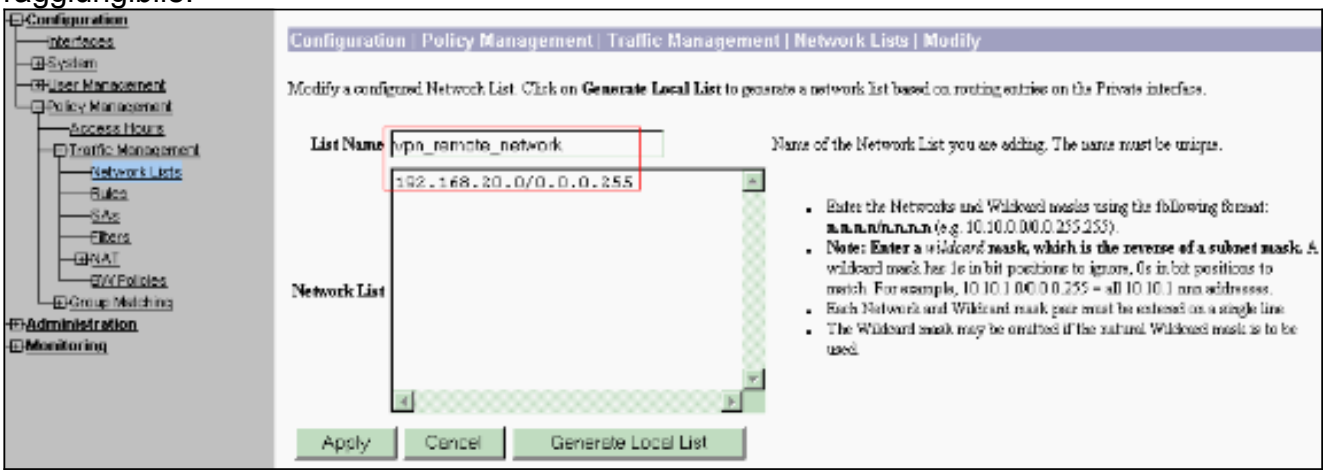
3. Selezionare **Configurazione > Sistema > Routing IP > Gateway predefiniti** configurare il gateway predefinito (Internet) e il gateway predefinito del tunnel (interno) in modo che IPsec raggiunga le altre subnet nella rete privata.In questo scenario, nella rete interna è disponibile una sola
subnet.



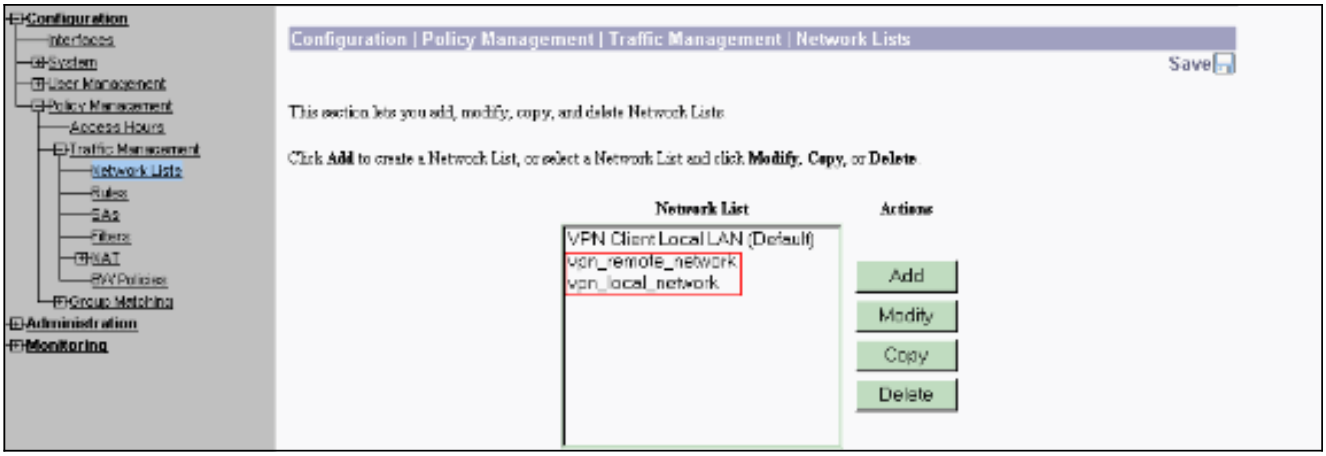
4. Selezionare Configurazione > **Gestione policy > Gestione traffico > Elenchi di rete > Aggiungi** per creare gli elenchi di rete che definiscono il traffico da crittografare.Le reti menzionate nell'elenco sono raggiungibili dalla rete remota. Le reti mostrate nell'elenco seguente sono reti locali. È inoltre possibile generare automaticamente l'elenco delle reti locali tramite RIP quando si fa clic su **Genera elenco locale**.



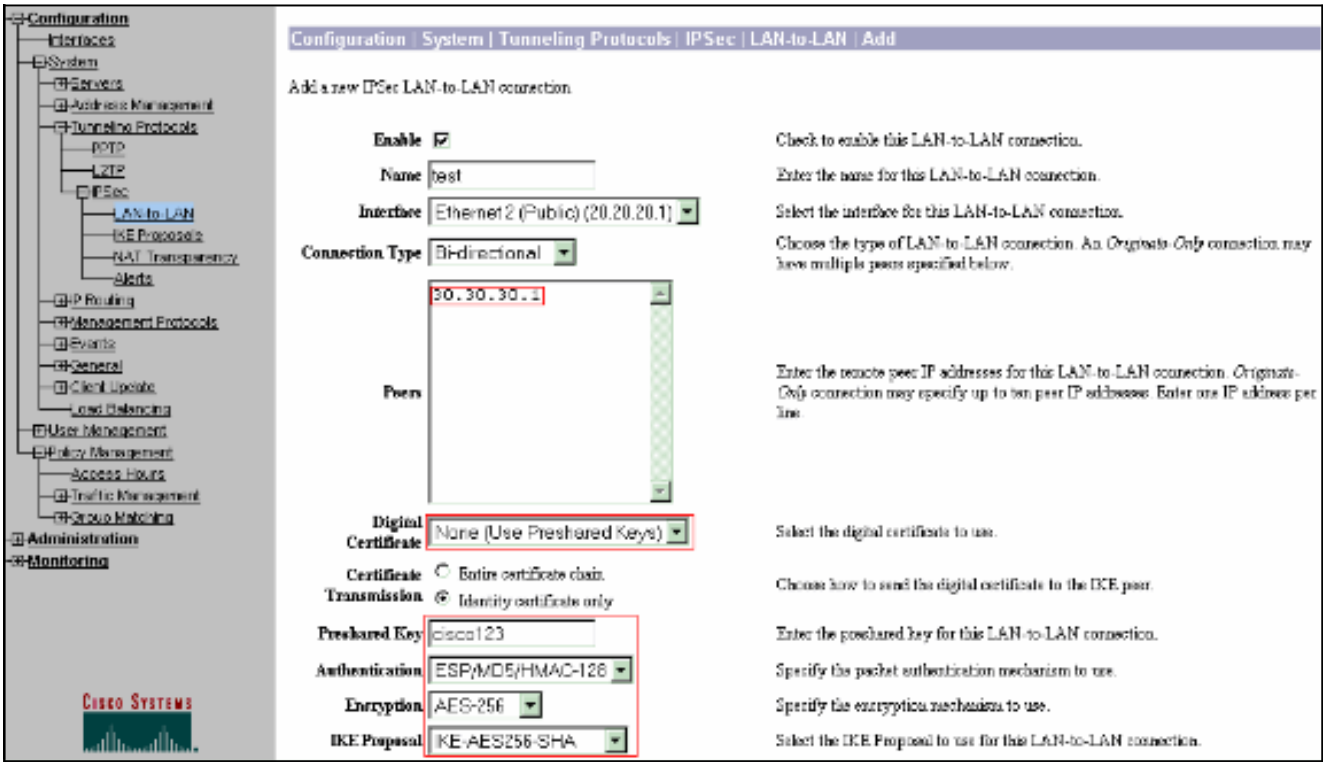
5. Le reti in questo elenco sono reti remote e devono essere configurate manualmente. A tale scopo, immettere il valore network/wildcard per ciascuna subnet raggiungibile.

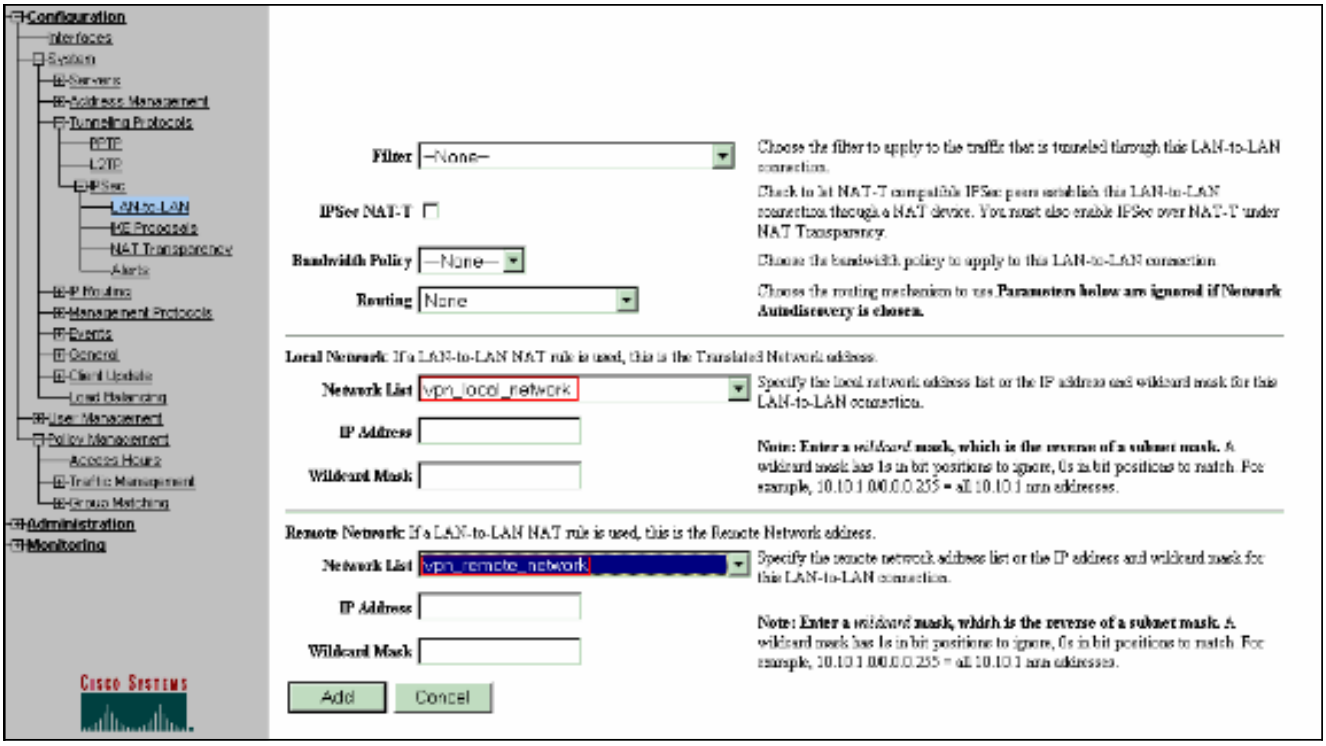


Al termine, questi sono i due elenchi di reti:

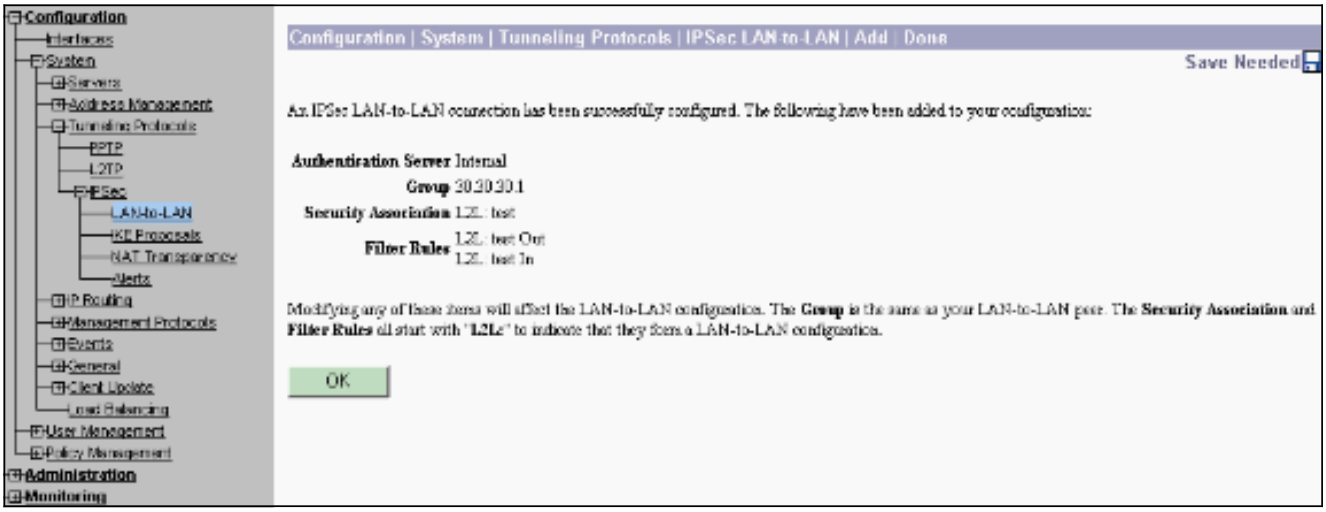


6. Selezionare Configurazione > **Sistema > Protocolli di tunneling > IPSec da LAN a LAN > Aggiungi** e definire il tunnel da LAN a LAN.Questa finestra è suddivisa in tre sezioni. La sezione superiore si riferisce alle informazioni di rete, mentre le due sezioni inferiori si riferiscono agli elenchi delle reti locali e remote. Nella sezione Informazioni di rete selezionare la crittografia AES, il tipo di autenticazione, la proposta IKE e digitare la chiave già condivisa. Nelle sezioni inferiori selezionare gli elenchi Rete già creati, ovvero gli elenchi Locale e
Remoto.



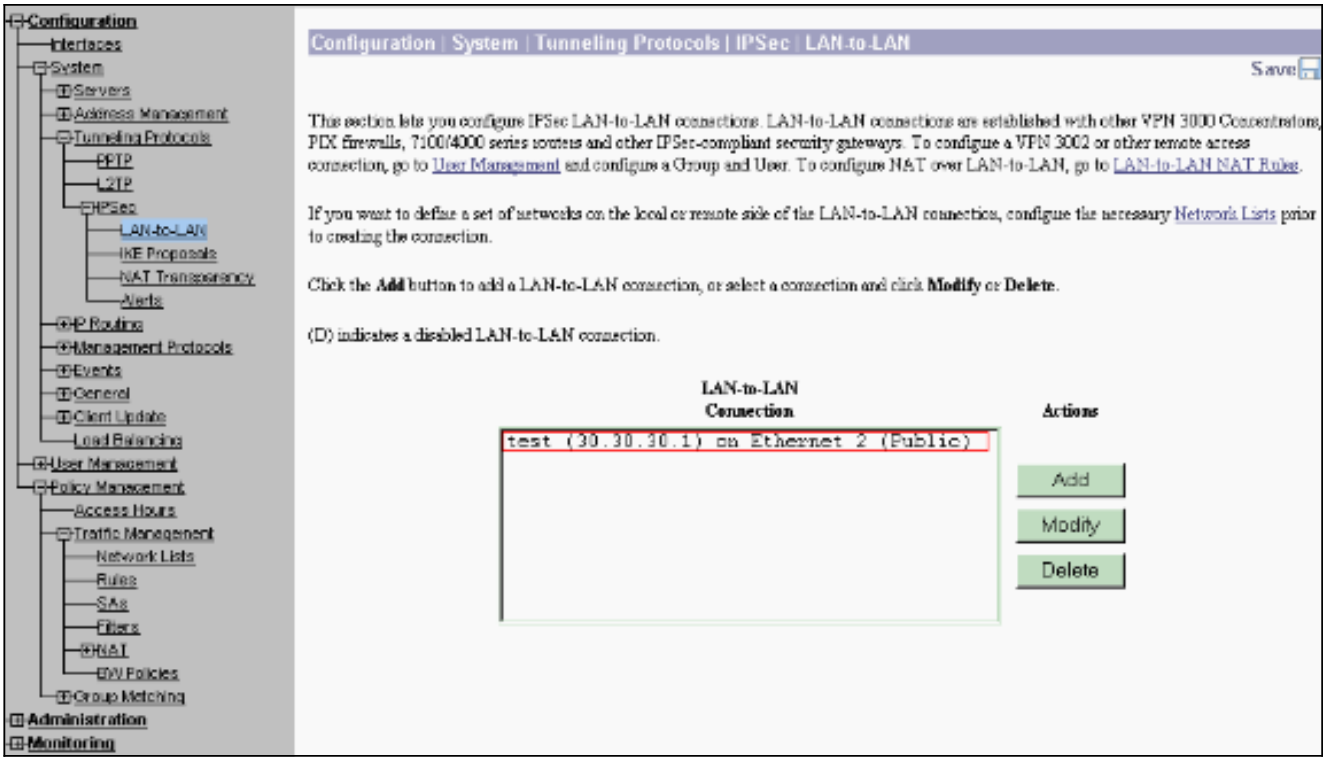


7. Dopo aver fatto clic su **Add**, se la connessione è corretta, viene visualizzata la finestra IPSec LAN-to-LAN-Add-Done.In questa finestra viene presentata una sintesi delle informazioni di configurazione del tunnel. Vengono inoltre configurati automaticamente il Nome gruppo, il Nome associazione di protezione e il Nome filtro. È possibile modificare qualsiasi parametro di questa
tabella.

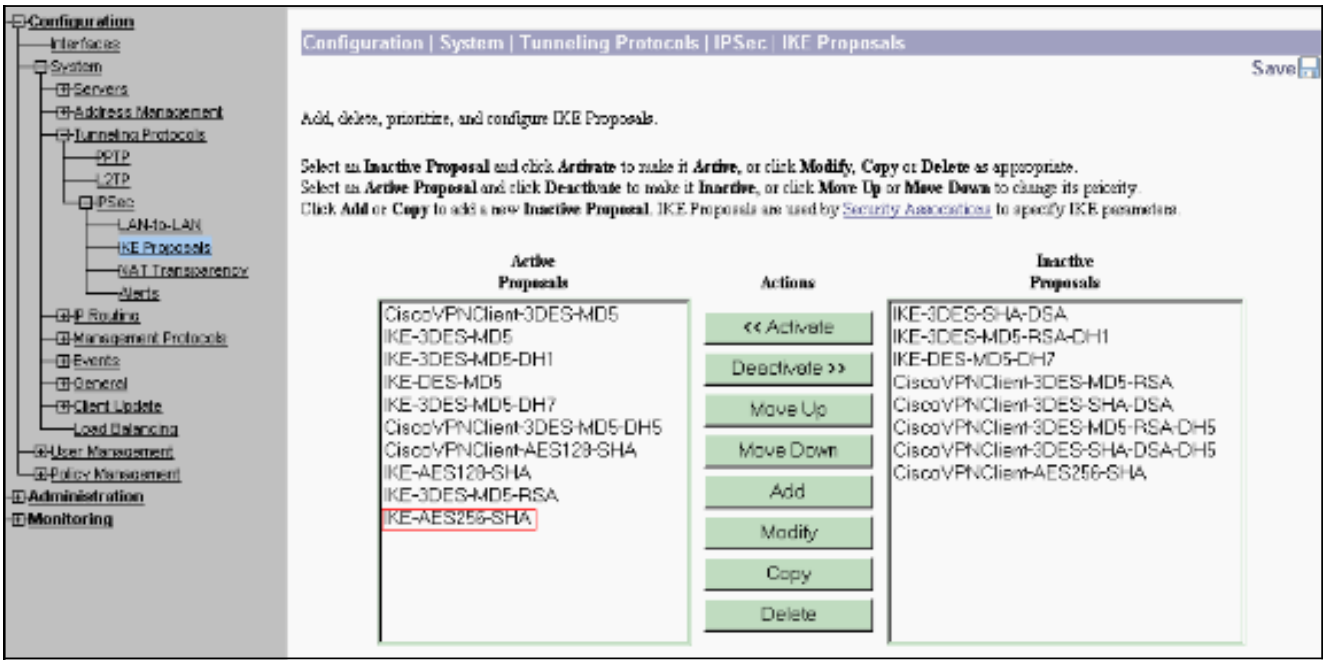


A questo punto, è stato configurato il tunnel IPsec LAN-LAN e si può iniziare a lavorare. Se per qualche motivo il tunnel non funziona, è possibile verificare la presenza di configurazioni errate.

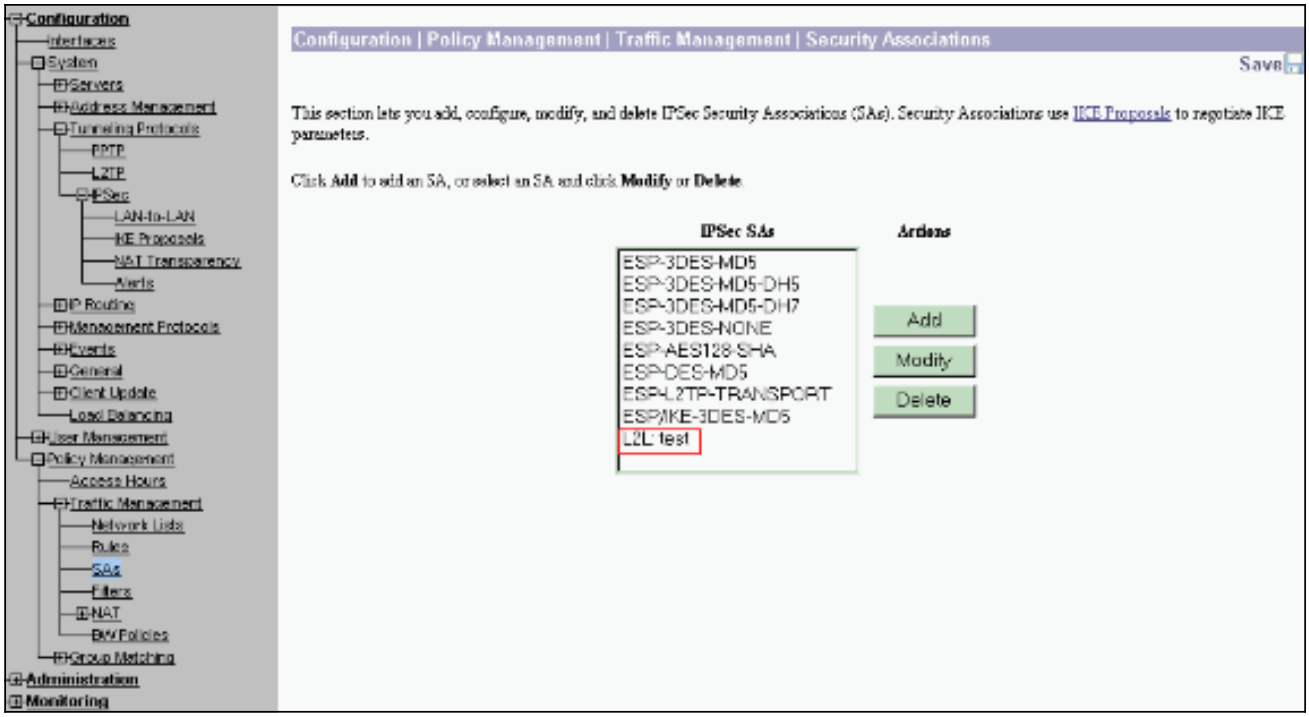
8. Per visualizzare o modificare i parametri IPsec da LAN a LAN creati in precedenza, selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN**.L'immagine mostra "test" come nome del tunnel e l'interfaccia pubblica dell'estremità remota è 30.30.30.1 come
nell'esempio.



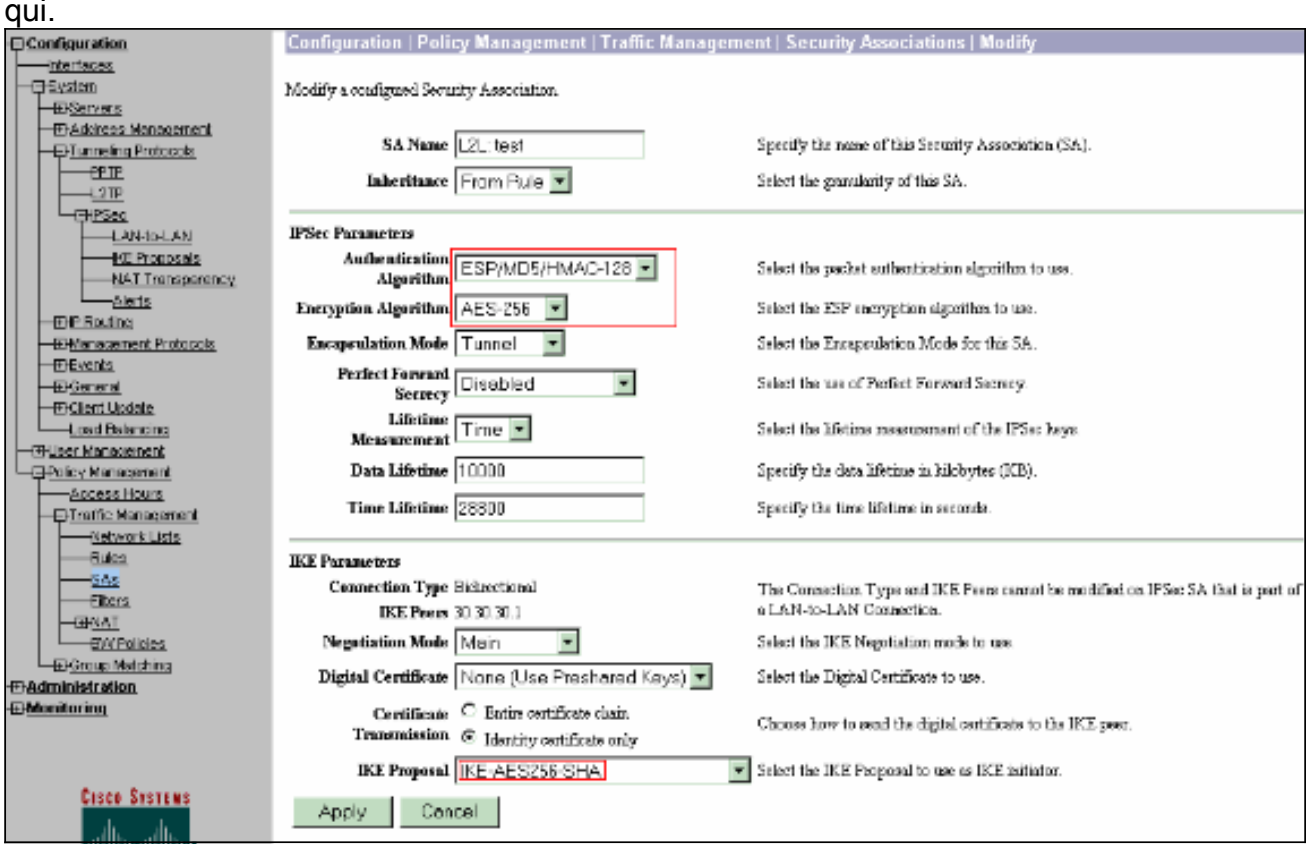
9. In alcuni casi, il tunnel potrebbe non essere disponibile se la proposta IKE è inclusa nell'elenco Proposte inattive. Selezionare Configurazione **> Sistema > Protocolli di tunneling > IPSec > Proposte IKE** per configurare la proposta IKE attiva.Se la proposta IKE è inclusa nell'elenco "Proposte inattive", è possibile abilitarla selezionando la proposta IKE e facendo clic sul pulsante **Attiva**. In questo grafico la proposta selezionata "IKE-AES256-SHA" è inclusa nell'elenco Proposte
attive.



10. Selezionare **Configurazione > Gestione criteri > Gestione traffico > Associazioni di sicurezza** per verificare se i parametri SA sono
corretti.



11. Fare clic sul nome dell'associazione di protezione (in questo caso, **L2L: test**) e quindi fare clic su **Modifica** per verificare le associazioni di protezione.Se uno dei parametri non corrisponde alla configurazione peer remota, è possibile modificarlo qui.



Verifica

Verifica della configurazione del router

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto isakmp sa**: visualizza tutte le SA IKE correnti in un peer. Lo stato QM_IDLE indica che l'associazione di sicurezza rimane autenticata con il peer e può essere utilizzata per successivi scambi in modalità rapida. È in uno stato silenzioso.

```
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**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti. Verificare gli indirizzi IP dei peer, le reti accessibili sia a livello locale che remoto e il set di trasformazioni utilizzato. Esistono due associazioni di protezione ESP, una per ogni direzione. Poiché vengono utilizzati set di trasformazioni AH, è vuoto.

```
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:
```

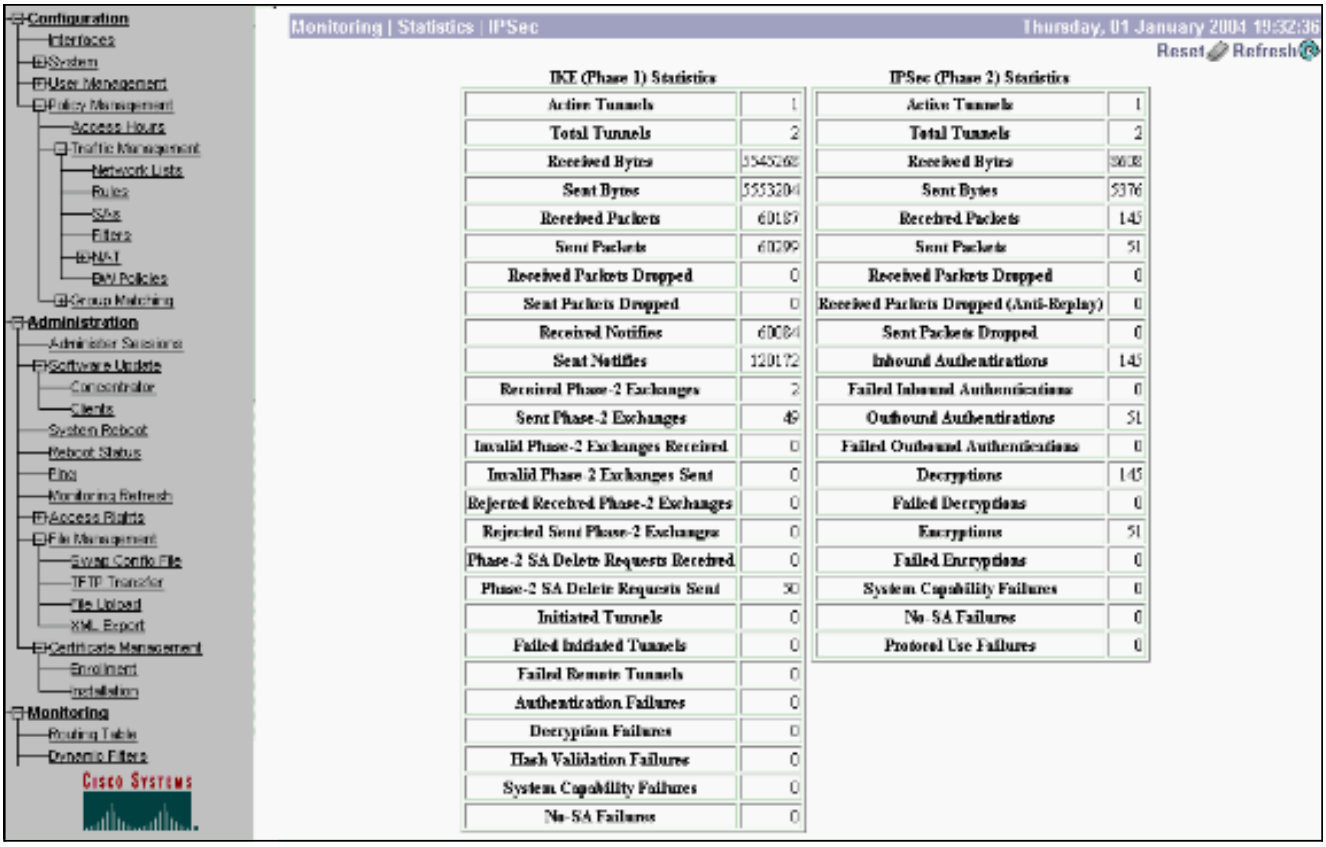
- **show crypto engine connections active**: visualizza le connessioni correnti attive alle sessioni crittografate per tutti i motori di crittografia. Ogni ID connessione è univoco. Il numero di pacchetti crittografati e decrittografati viene visualizzato nelle ultime due colonne.

```
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
```

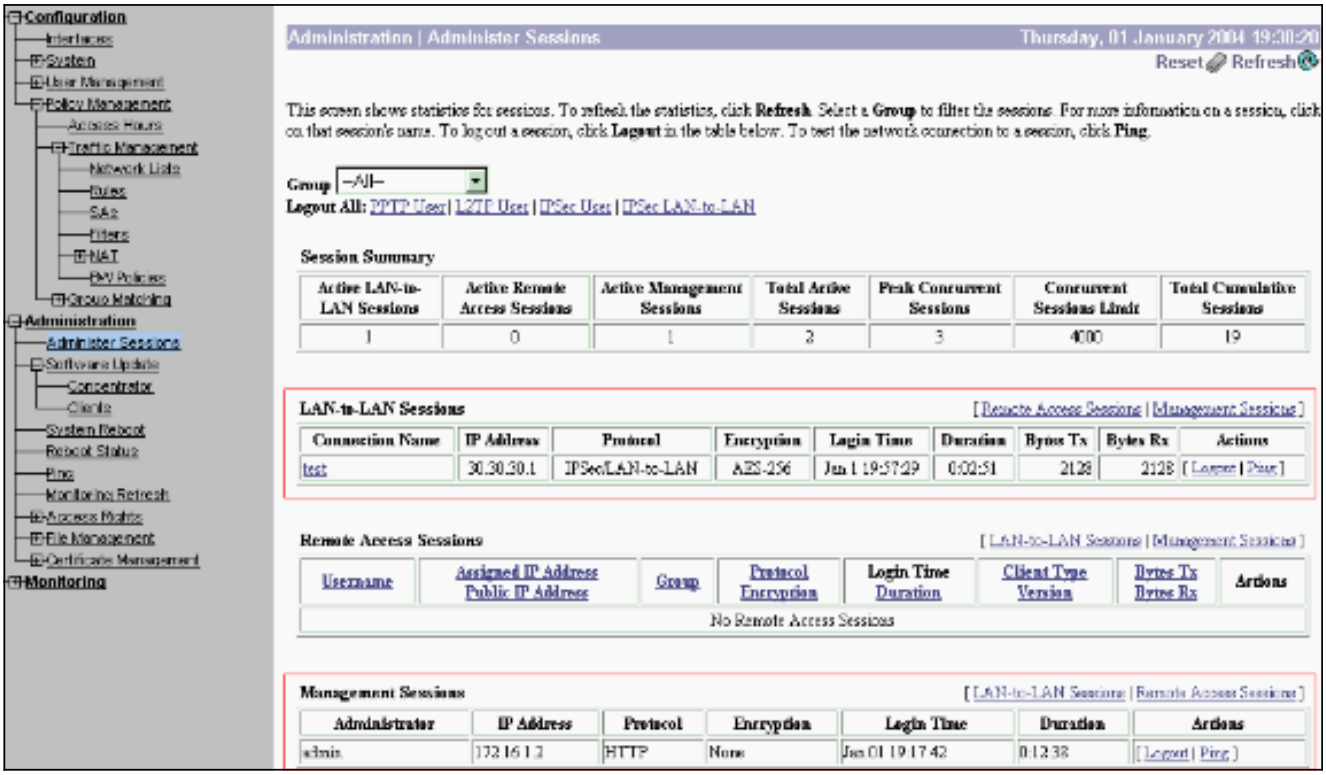
Verifica della configurazione di VPN Concentrator

Completare questa procedura per verificare la configurazione di VPN Concentrator.

1. Analogamente ai comandi show crypto ipsec sa e **show crypto isakmp sa** sui router, è possibile visualizzare le statistiche IPsec e IKE quando si seleziona **Monitoraggio > Statistiche > IPSec** sui concentratori
   VPN.



2. Analogamente al comando **show crypto engine connections active** sui router, è possibile utilizzare la finestra Administration-Sessions su VPN Concentrator per visualizzare i parametri e le statistiche di tutte le connessioni o i tunnel IPsec LAN a LAN attivi.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Risoluzione dei problemi del router

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

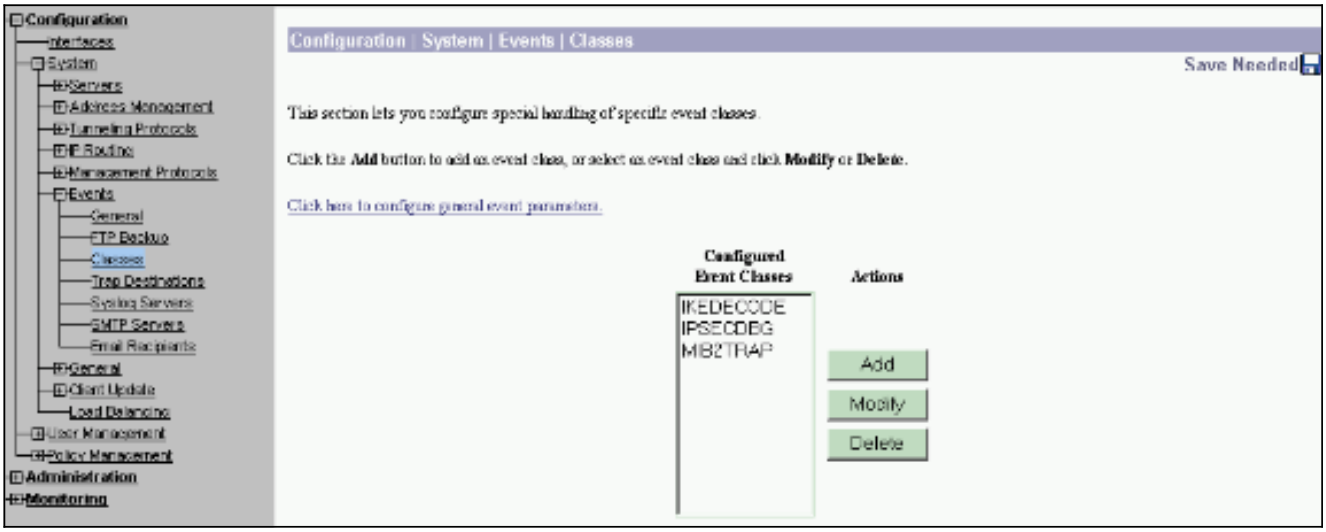
- **debug crypto engine**: visualizza il traffico crittografato. Il motore di crittografia è il meccanismo che esegue la crittografia e la decrittografia. Un motore di crittografia può essere un acceleratore software o hardware.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1 di IKE.
- **debug crypto ipsec**: visualizza le negoziazioni IPsec di IKE fase 2.

Per informazioni più dettagliate e un output di esempio, fare riferimento a Risoluzione dei problemi di IPSec - Comprensione e uso dei comandi di **debug**.

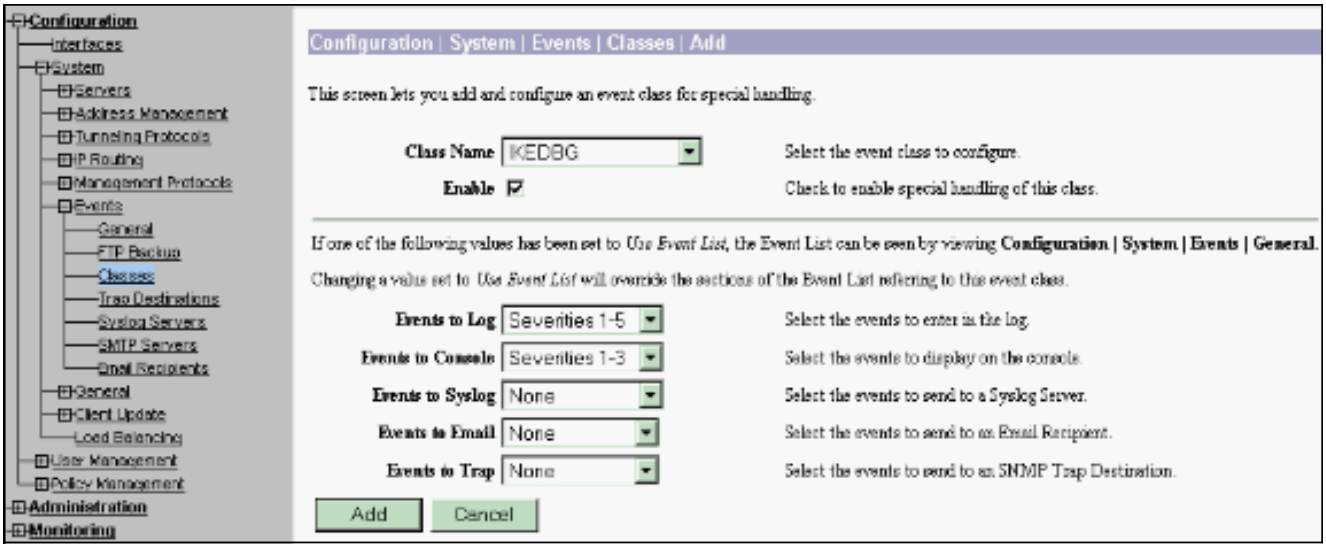
Risoluzione dei problemi di VPN Concentrator

Analogamente ai comandi **debug** sui router Cisco, è possibile configurare le classi Event per visualizzare tutti gli allarmi.

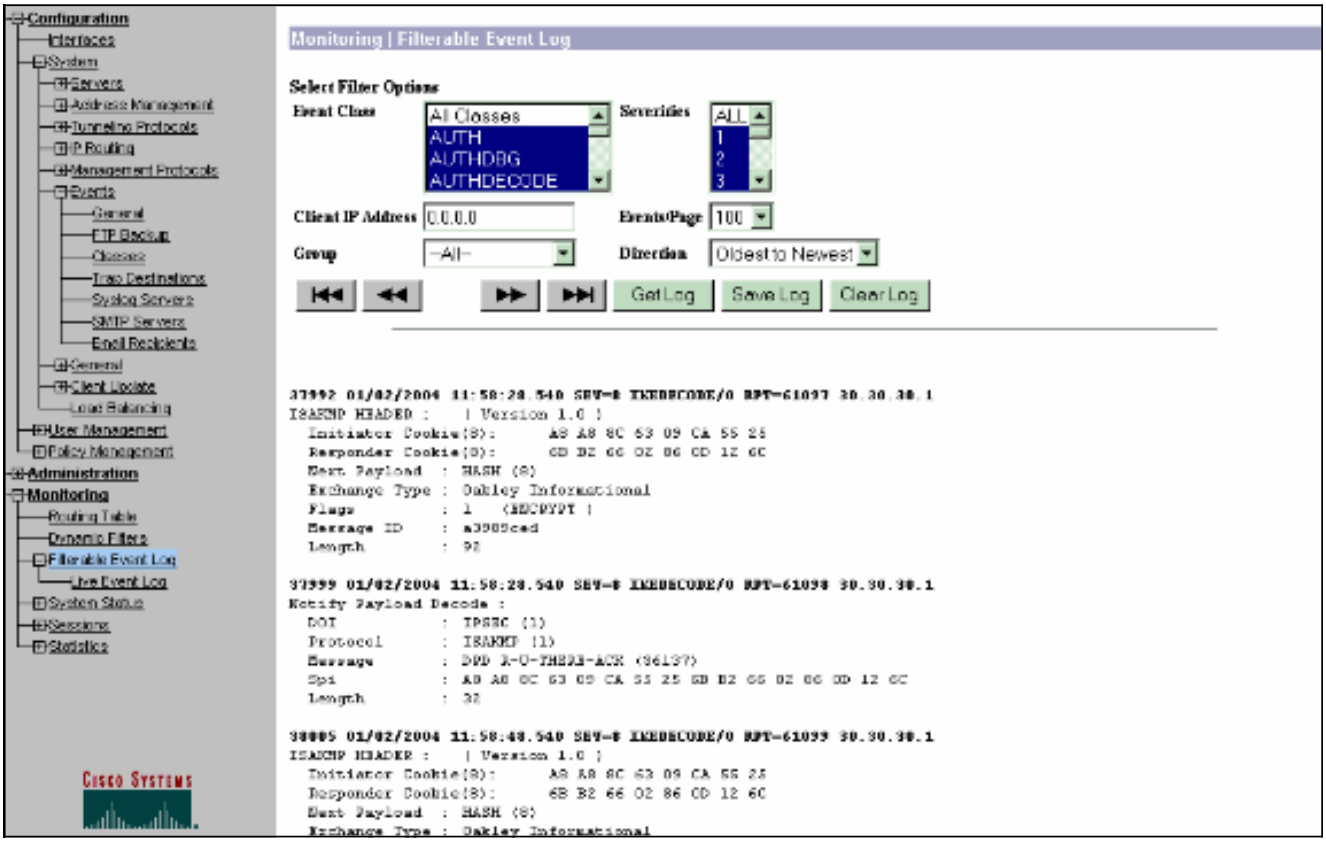
1. Selezionare Configurazione > **Sistema** > **Eventi** > **Classi** > **Aggiungi** per attivare la registrazione delle classi di evento.Le classi seguenti sono disponibili per IPSec:IKEIKEDBGCODICE IKEDECODEIPSECIPSECDBGCODICEIPSEC



2. Durante l'aggiunta, è inoltre possibile selezionare il livello di gravità per ogni classe, in base al livello di gravità inviato dall'allarme.Gli allarmi possono essere gestiti usando uno dei seguenti metodi:Per registroVisualizzato sulla consoleInviato al server Syslog UNIXInviato come messaggio di posta elettronicaInviato come trap a un server SNMP (Simple Network Management
Protocol)



3. Selezionare **Monitoraggio > Registro eventi filtrabile** per monitorare gli allarmi attivati.



Informazioni correlate

- Advanced Encryption Standard (AES)
- DES/3DES/AES VPN Encryption Module
- Configurazioni di esempio IPSec
- Cisco VPN serie 3000 Client Support Page
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).