Configurazione di Cisco VPN 3000 Concentrator su un router Cisco

Sommario

Introduzione

In questa configurazione di esempio viene mostrato come connettere una rete privata con un router con software Cisco IOS® a una rete privata con Cisco VPN 3000 Concentrator. I dispositivi nelle reti si conoscono a vicenda in base ai rispettivi indirizzi privati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Router Cisco 2611 con software Cisco IOS versione 12.3(1a**Nota:** verificare che i router

Cisco serie 2600 siano installati con un'immagine crypto IPsec VPN IOS che supporta la funzionalità VPN.
- Cisco VPN 3000 Concentrator con 4.0.1 B

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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

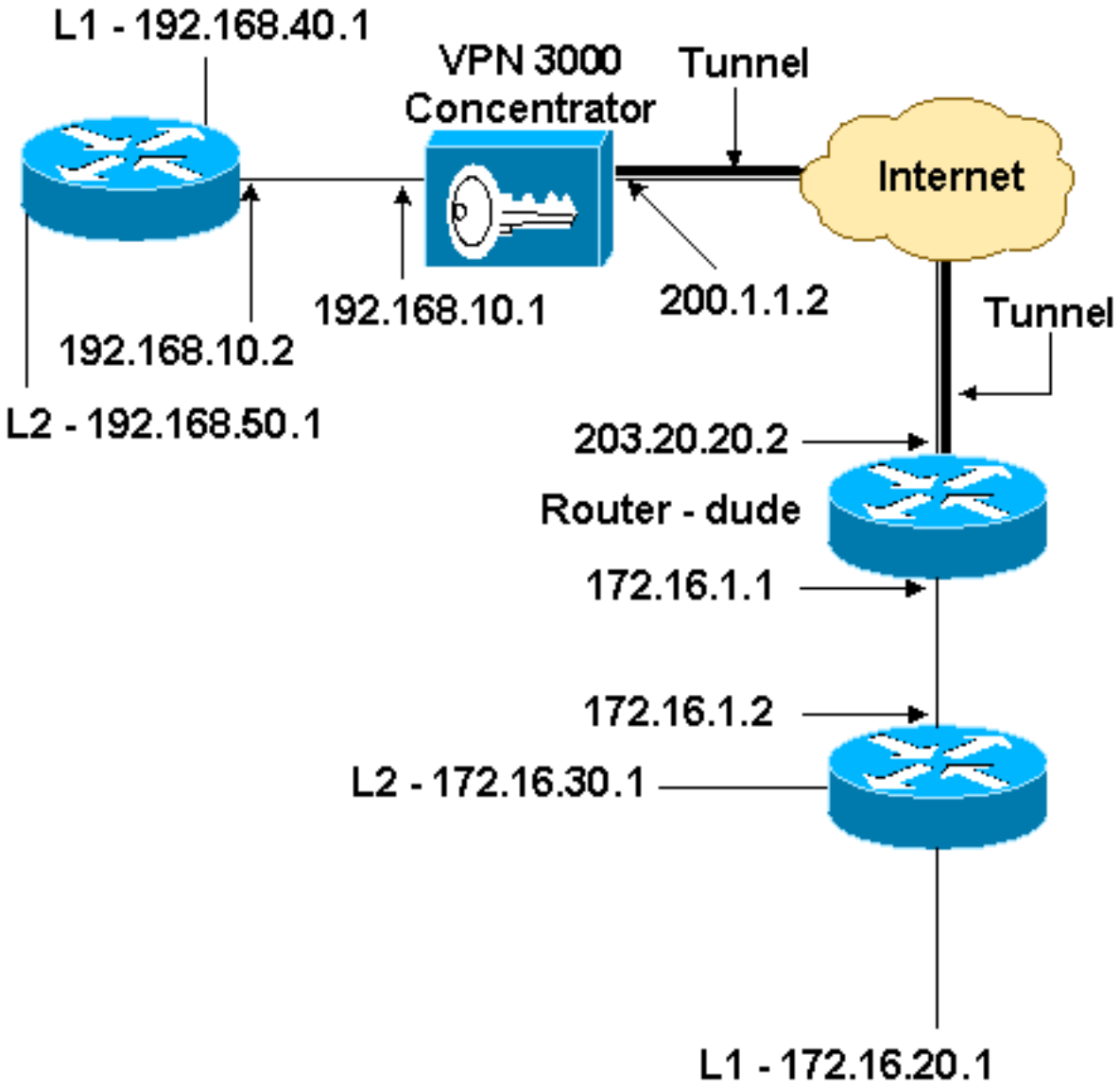
Configurazione

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 questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Configurazioni

Nel documento viene usata questa configurazione.

Configurazione router

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 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 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configurazione VPN Concentrator

In questa impostazione di laboratorio, si accede per la prima volta a VPN Concentrator tramite la porta della console e si aggiunge una configurazione minima per consentire l'ulteriore configurazione tramite l'interfaccia utente grafica (GUI).

Scegliere **Amministrazione > Riavvio del sistema > Pianifica riavvio > Riavvia con la configurazione predefinita/di fabbrica** per assicurarsi che non vi sia alcuna configurazione esistente nel concentratore VPN.

VPN Concentrator viene visualizzato in Configurazione rapida e questi elementi vengono configurati dopo il riavvio:

- Ora/Data
- Interfacce/maschere in **Configurazione > Interfacce** (public=200.1.1.2/24, private=192.168.10.1/24)
- Gateway predefinito in **Configurazione > Sistema > Routing IP > Default_Gateway** (200.1.1.1)

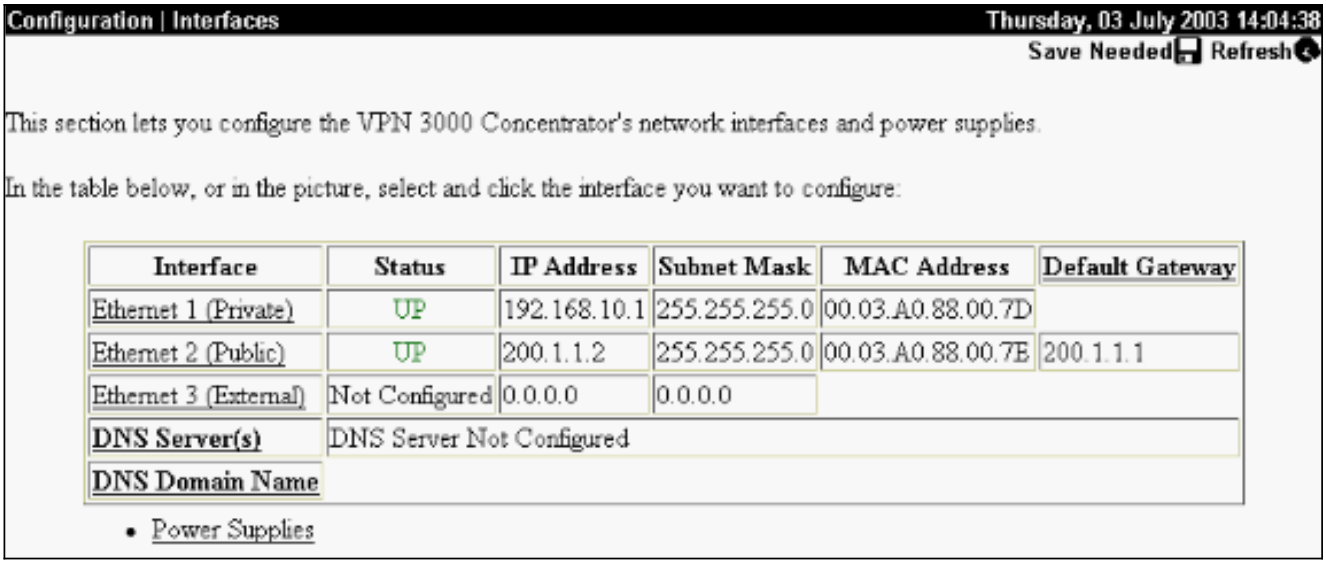
A questo punto, VPN Concentrator è accessibile tramite HTML dalla rete interna.

Nota: poiché VPN Concentrator è gestito dall'esterno, è necessario selezionare anche:

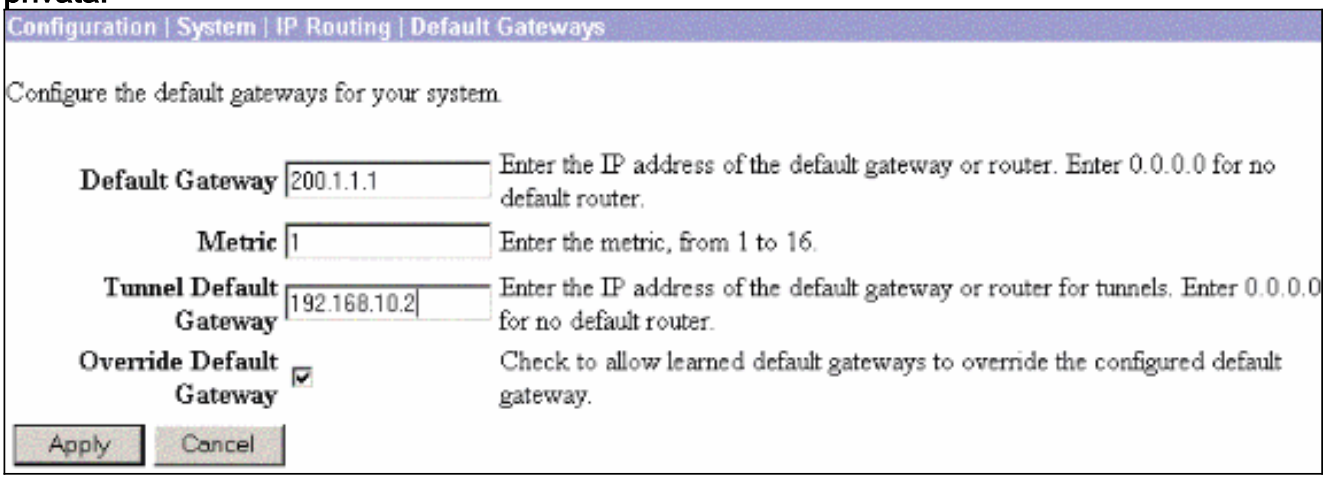
- **Configurazione > Interfacce > 2-public > Select IP Filter > 1. Private (impostazione predefinita)**.
- **Amministrazione > Diritti di accesso > Lista di controllo di accesso > Aggiungi stazione di lavoro Manager** per aggiungere l'indirizzo IP del *gestore esterno*.

Questa operazione non è necessaria a meno che non si gestisca VPN Concentrator dall'*esterno*.

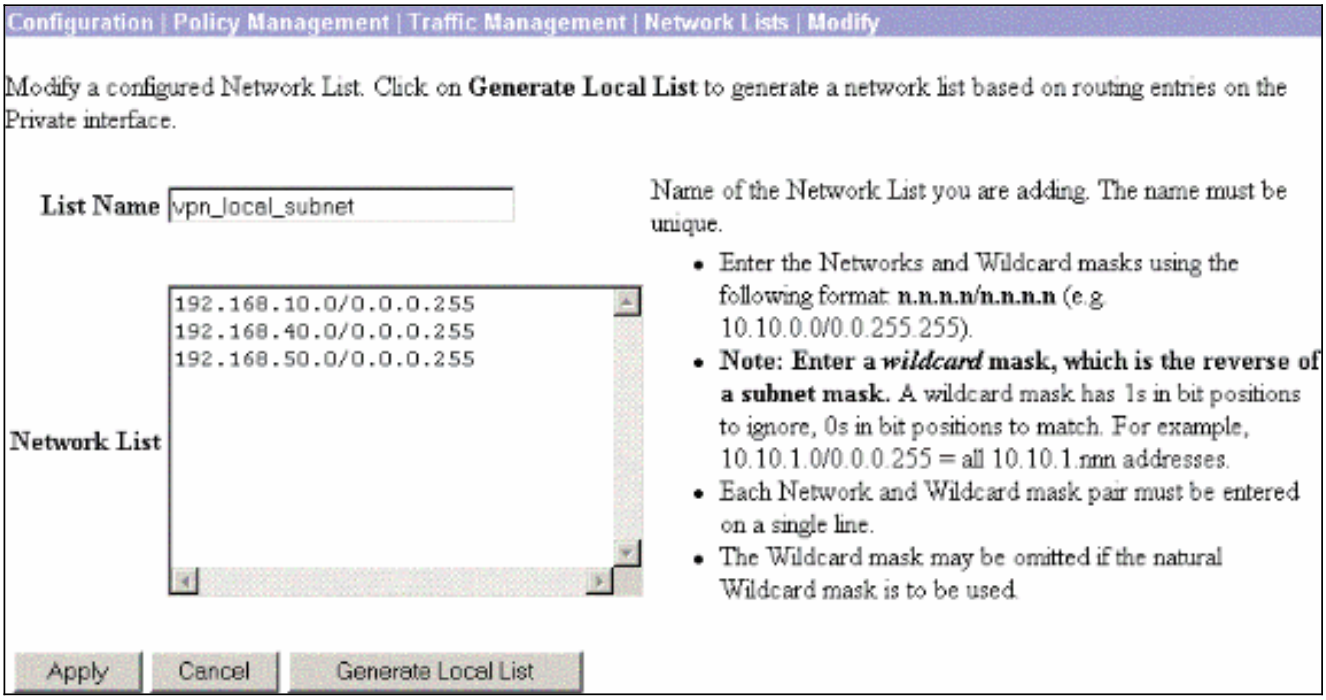
1. Selezionare **Configuration > Interfaces** per ricontrollare le interfacce dopo aver richiamato la GUI.



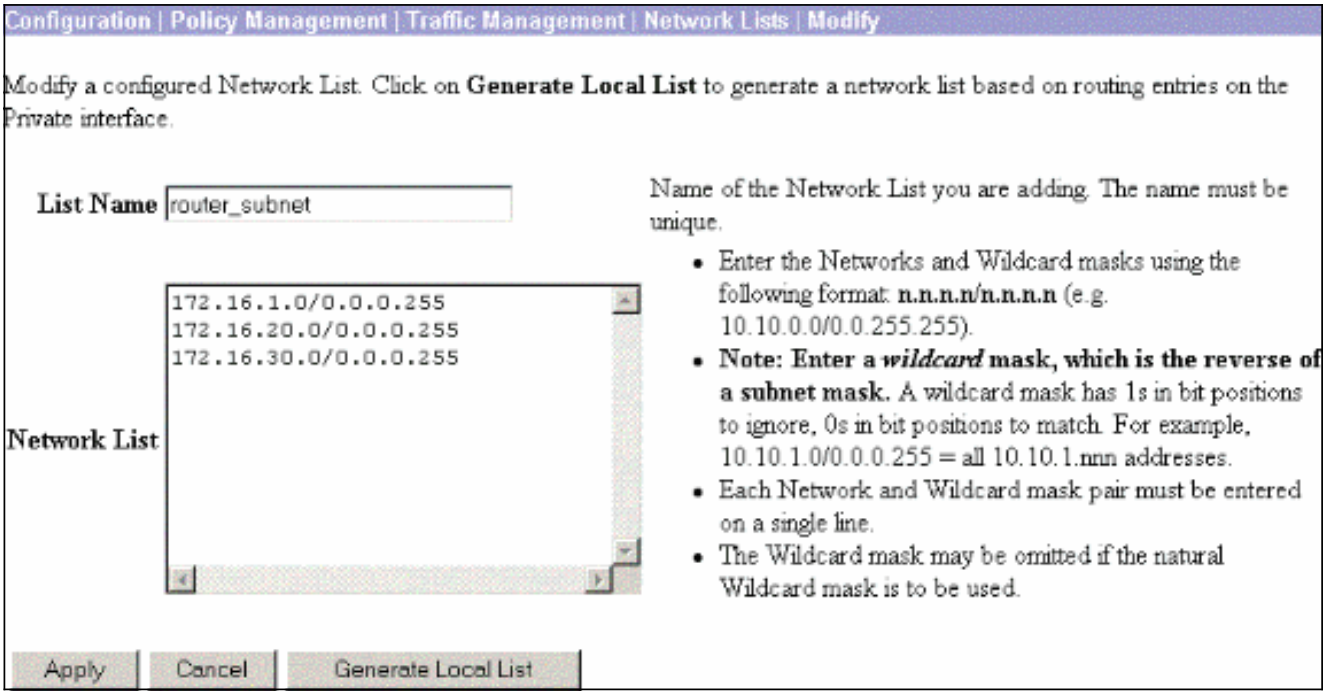
2. Scegliere Configurazione > Sistema > Routing IP > Gateway predefiniti per configurare il gateway predefinito (Internet) e il gateway predefinito del tunnel (interno) **per IPsec in modo da raggiungere le altre subnet nella rete privata.**



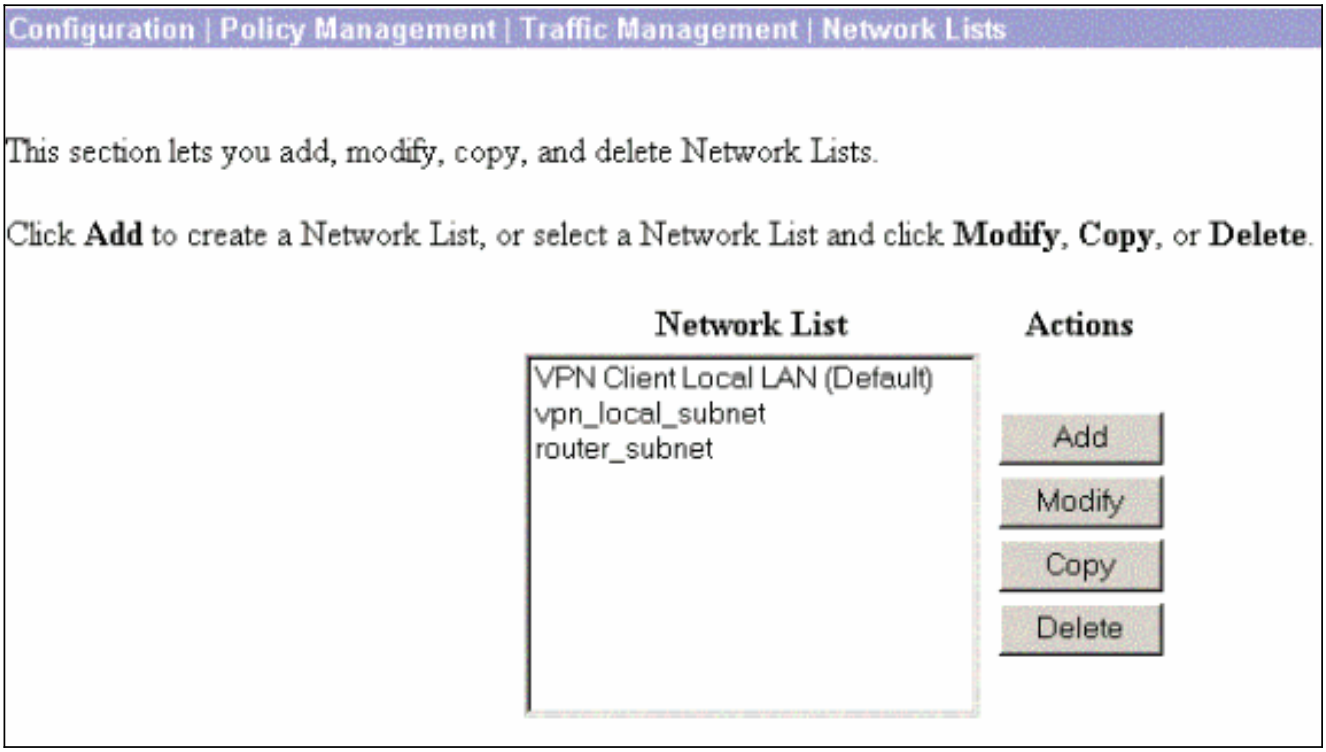
3. Scegliere **Configurazione > Gestione criteri > Elenchi di rete** per creare gli elenchi di rete che definiscono il traffico da crittografare.Queste sono le reti locali:



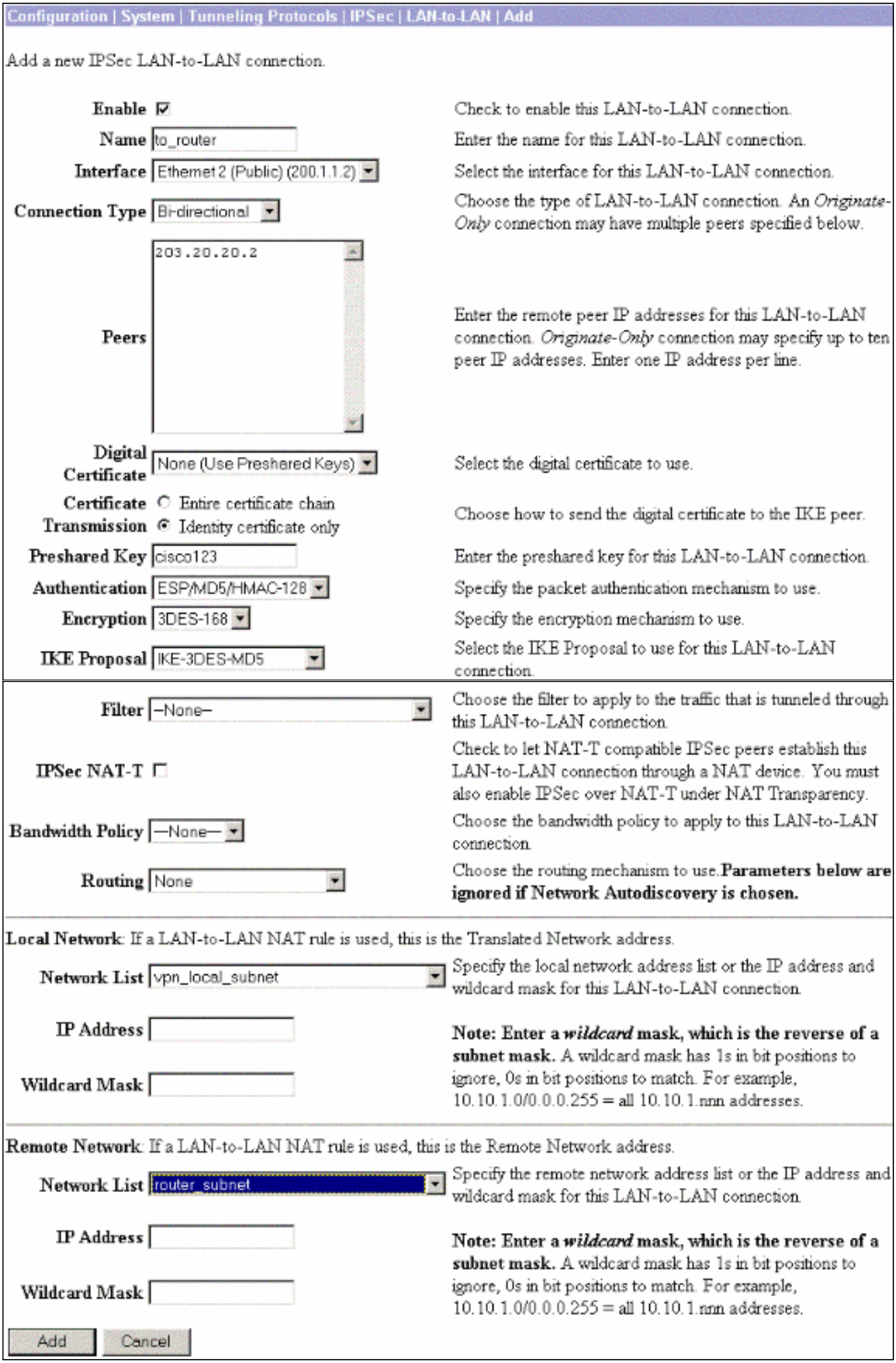
Queste sono le reti
remote:



4. Al termine, questi sono i due elenchi di reti:**Nota:** se il tunnel IPsec non viene visualizzato, verificare se il traffico interessante corrisponde su entrambi i lati. Il traffico interessante è definito dall'elenco degli accessi sul router e sulle scatole PIX. Sono definiti dagli elenchi di reti nei concentratori
VPN.

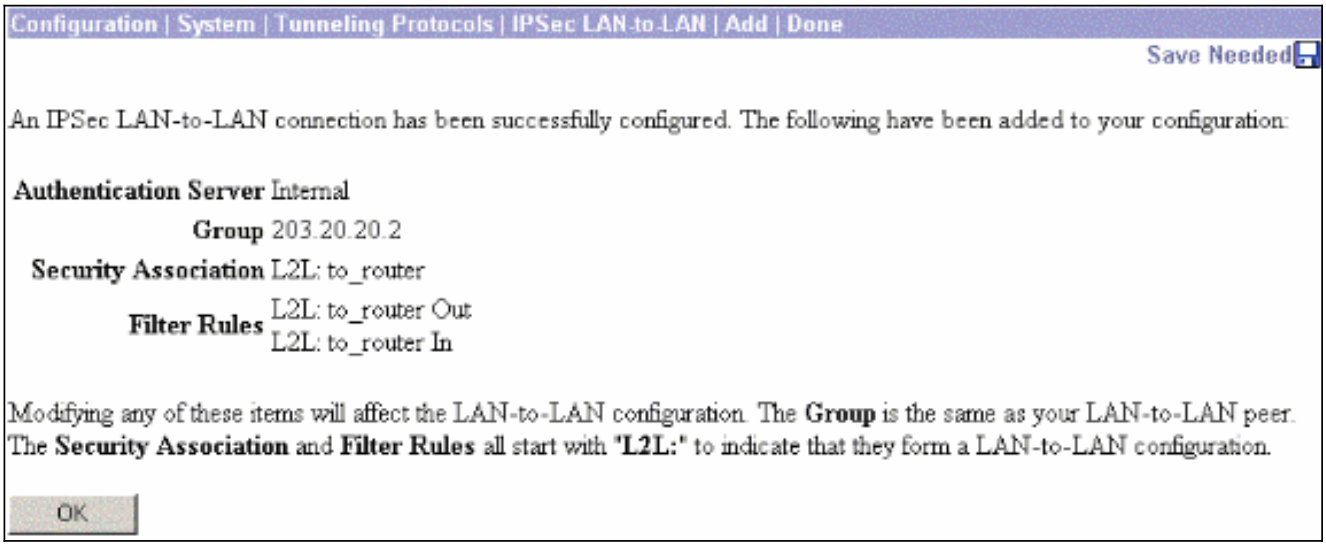


5. Scegliere **Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN** e definire il tunnel da LAN a
LAN.

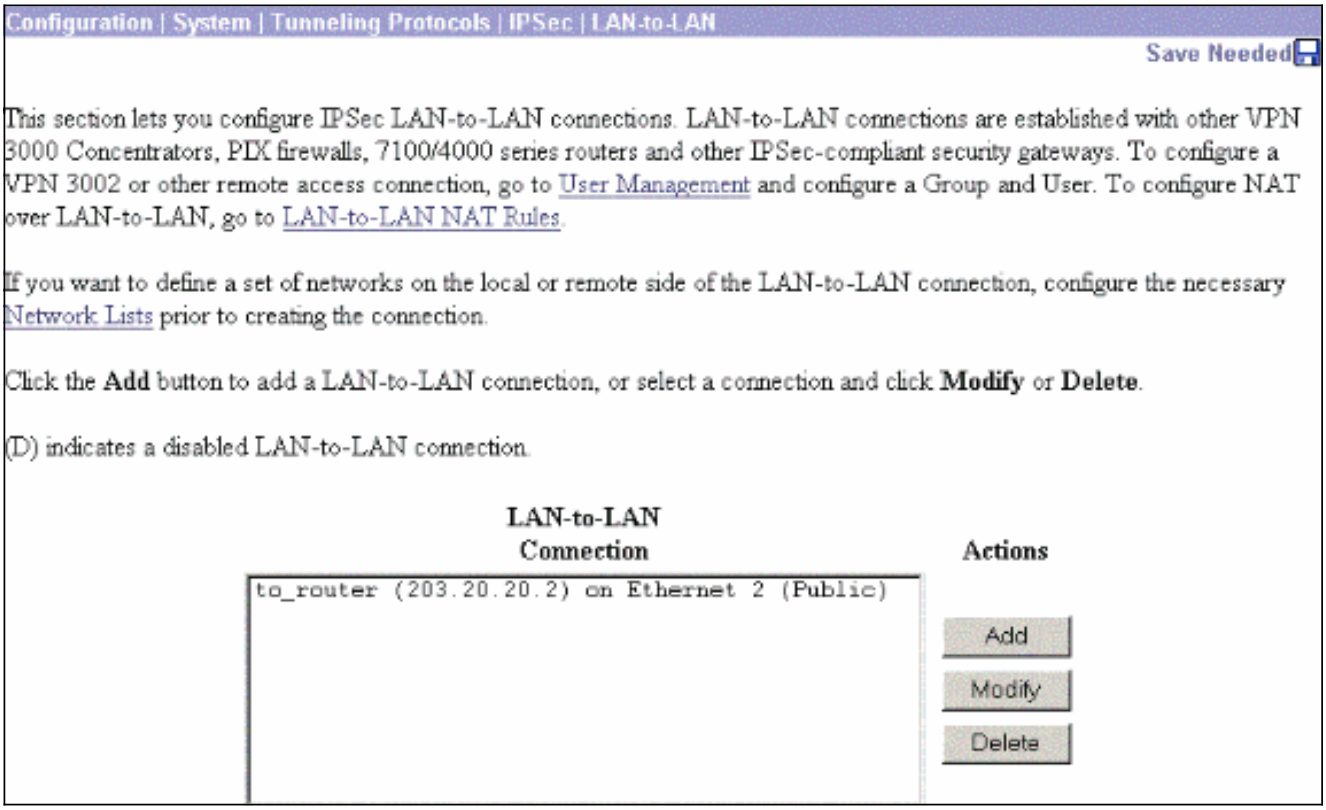


6. Dopo aver fatto clic su **Apply** (Applica), questa finestra viene visualizzata con l'altra

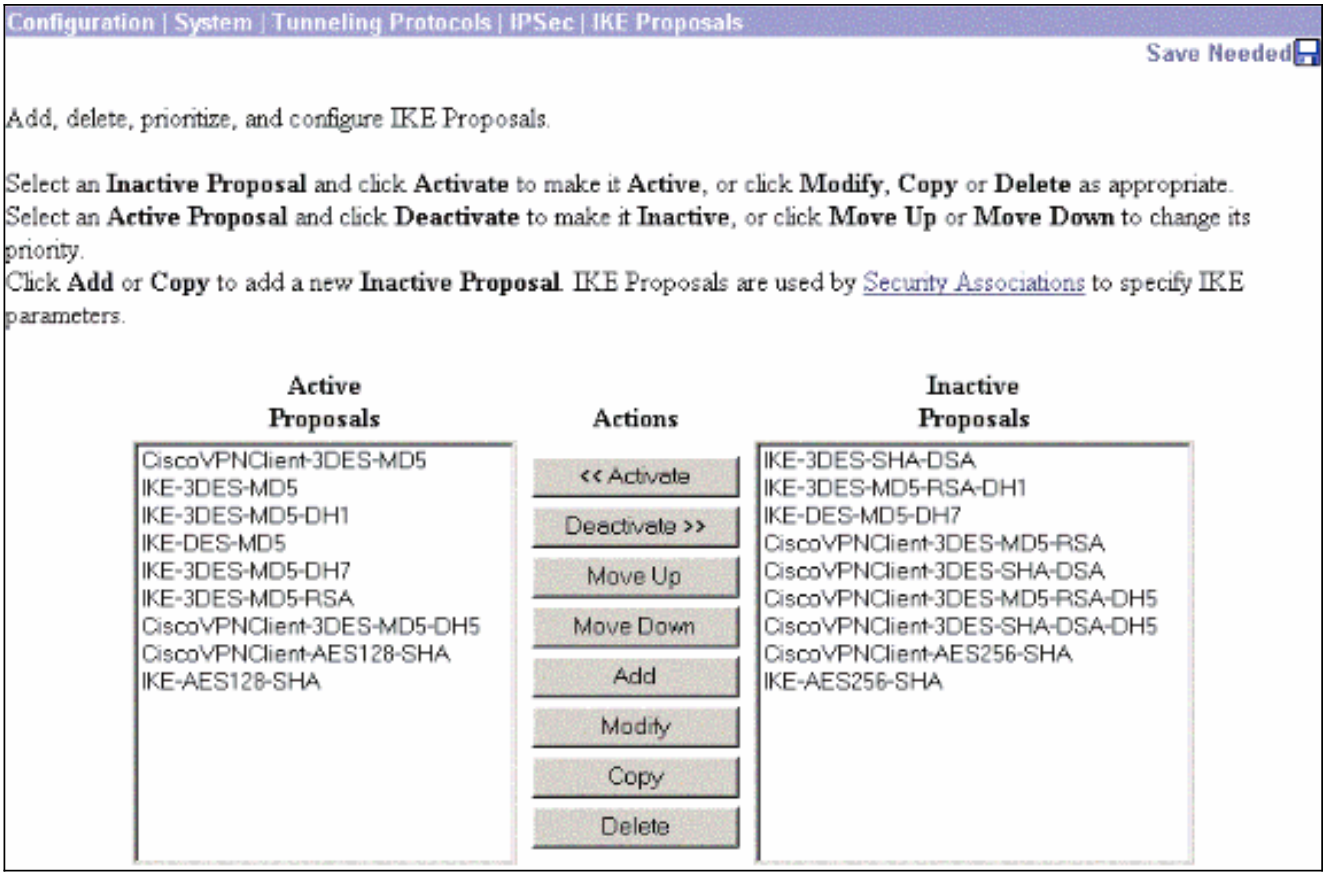
configurazione creata automaticamente come risultato della configurazione del tunnel da LAN a
LAN.



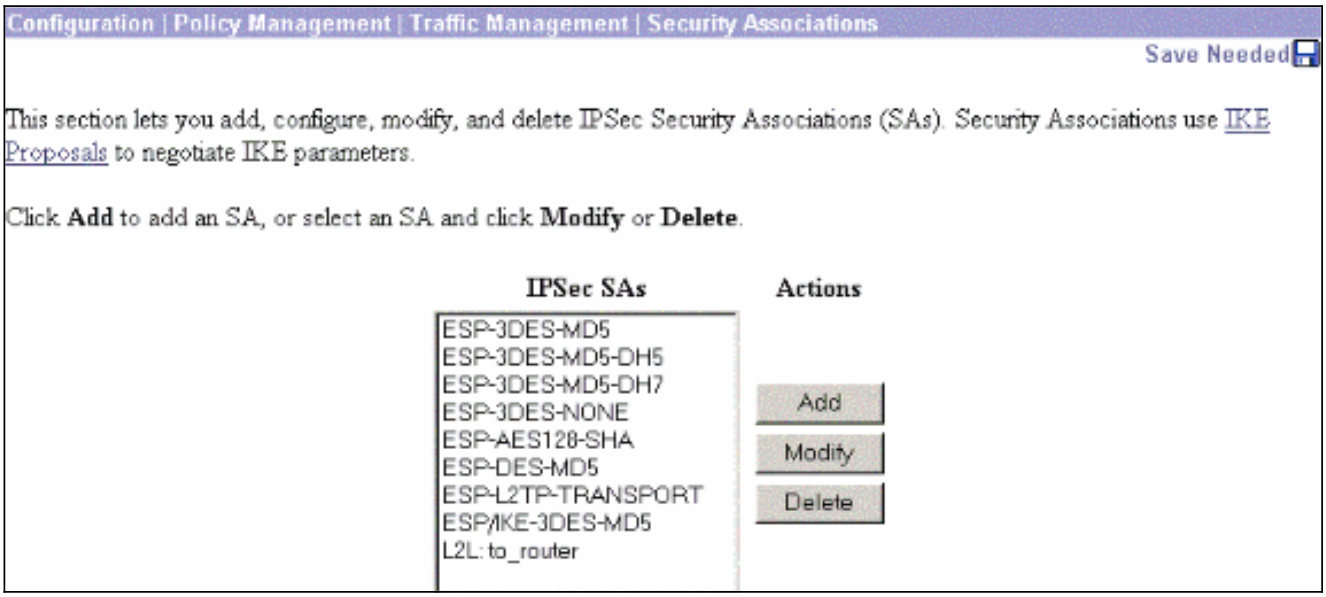
I parametri IPsec da LAN a LAN creati in precedenza possono essere visualizzati o modificati in **Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN**.



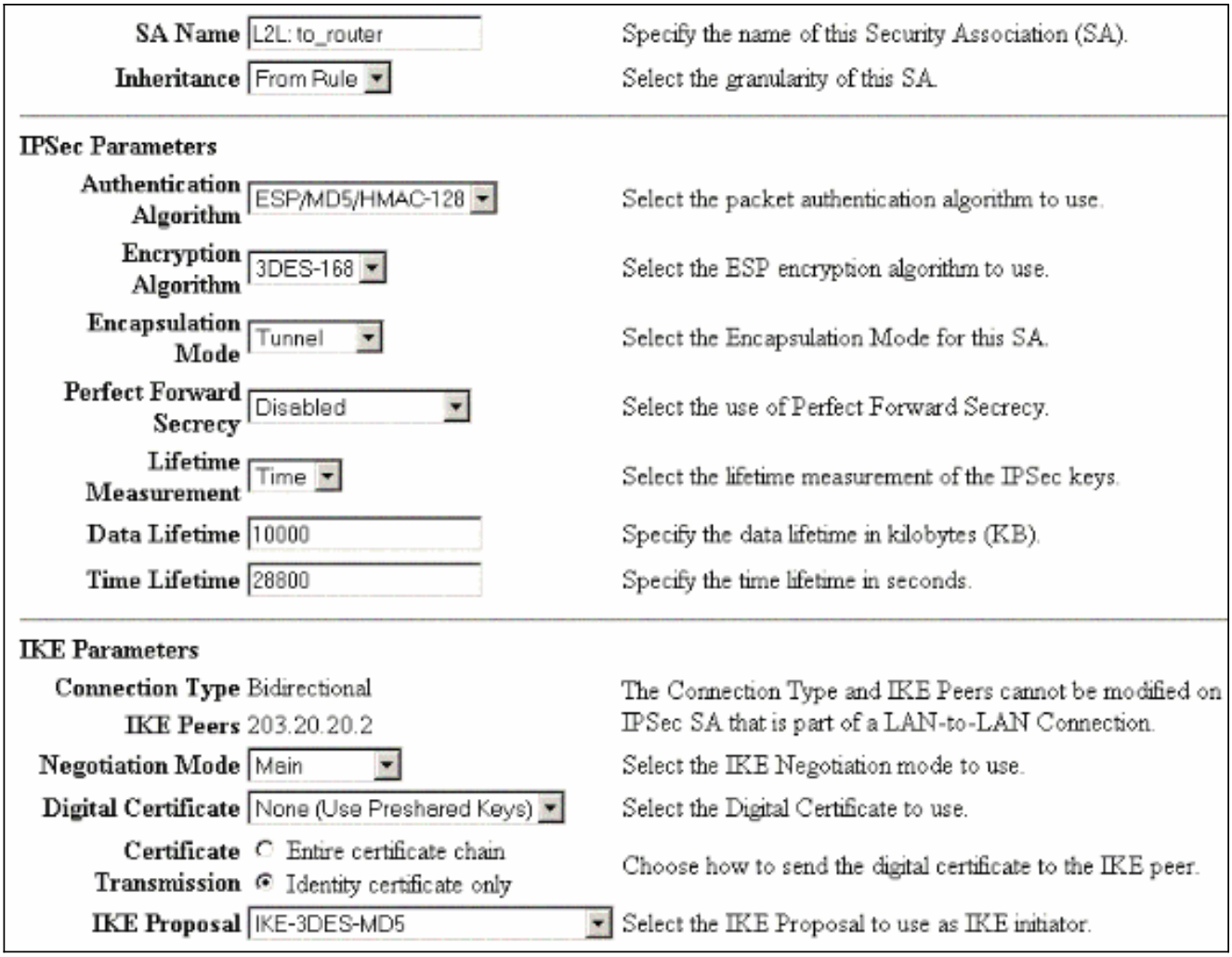
7. Scegliere Configurazione > **Sistema > Protocolli di tunneling > IPSec > Proposte IKE** per confermare la proposta IKE
attiva.



8. Scegliere **Configurazione > Gestione criteri > Gestione traffico > Associazioni di sicurezza** per visualizzare la lista delle associazioni di sicurezza.



9. Fare clic sul nome dell'associazione di protezione e quindi su **Modifica** per verificare le associazioni di protezione.



Verifica

In questa sezione vengono elencati i comandi **show** utilizzati in questa configurazione.

Sul router

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

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

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.
- **show crypto isakmp sa**: visualizza tutte le associazioni di protezione di Internet Key Exchange correnti a un peer.
- **show crypto engine connection active**: visualizza le connessioni di sessione crittografata attive correnti per tutti i motori di crittografia.

Per ulteriori informazioni su comandi specifici, è possibile usare lo strumento di ricerca dei comandi IOS (solo utenti registrati).

Su VPN Concentrator

Scegliere Configurazione > **Sistema** > **Eventi** > **Classi** > **Modifica** per attivare la registrazione. Sono disponibili le seguenti opzioni:

- IKE
- IKEDBG
- CODICE IKEDECODE
- IPSEC
- IPSECDBG
- CODICEIPSEC

Gravità da registrare = 1-13

Gravità alla console = 1-3

Selezionare **Monitoraggio** > **Registro eventi** per recuperare il registro eventi.

Risoluzione dei problemi

Sul router

consultare le informazioni importanti sui comandi di debug prima di provare i comandi di debug.

- **debug crypto engine**: visualizza il traffico crittografato.
- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.

Problema - Impossibile avviare il tunnel

Messaggio di errore

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Soluzione

Completare questa azione per configurare il numero desiderato di accessi simultanei o impostare gli accessi simultanei su 5 per questa associazione di protezione:

Selezionare **Configurazione > Gestione utente > Gruppi > Modifica 10.19.187.229 > Generale > Login a simultanee** e modificare il numero di login in 5.

PFS

Nelle negoziazioni IPsec, PFS (Perfect Forward Secrecy) garantisce che ogni nuova chiave di crittografia non sia correlata a nessuna chiave precedente. Abilitare o disabilitare PFS su entrambi i peer del tunnel. In caso contrario, il tunnel IPsec LAN-to-LAN (L2L) non viene stabilito nei router.

Per specificare che IPsec deve richiedere PFS quando vengono richieste nuove associazioni di sicurezza per questa voce della mappa crittografica o che IPsec richiede PFS quando riceve

richieste per nuove associazioni di sicurezza, utilizzare il comando **set pfs** in modalità di configurazione mappa crittografica. Per specificare che IPsec non deve richiedere PFS, utilizzare la forma **no** di questo comando.

```
set pfs [group1 | group2]
no set pfs
```

Per il comando **set pfs**:

- *group1*: specifica che IPsec deve utilizzare il gruppo di moduli primari Diffie-Hellman a 768 bit quando viene eseguito il nuovo scambio Diffie-Hellman.
- *group2*: specifica che IPsec deve utilizzare il gruppo di moduli primari Diffie-Hellman a 1024 bit quando viene eseguito il nuovo scambio Diffie-Hellman.

Per impostazione predefinita, PFS non è richiesto. Se con questo comando non si specifica alcun gruppo, per impostazione predefinita verrà utilizzato *group1*.

Esempio:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Per ulteriori informazioni sul comando **set pfs**, consultare la guida di riferimento dei comandi di Cisco IOS Security.

Informazioni correlate

- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Cisco VPN serie 3000 concentrator
- Client hardware Cisco VPN 3002
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems