

Configurazione di Cisco VPN 3000 Concentrator su un router Cisco

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione VPN Concentrator](#)

[Verifica](#)

[Sul router](#)

[Su VPN Concentrator](#)

[Risoluzione dei problemi](#)

[Sul router](#)

[Problema - Impossibile avviare il tunnel](#)

[PFS](#)

[Informazioni correlate](#)

[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(1)**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](#).

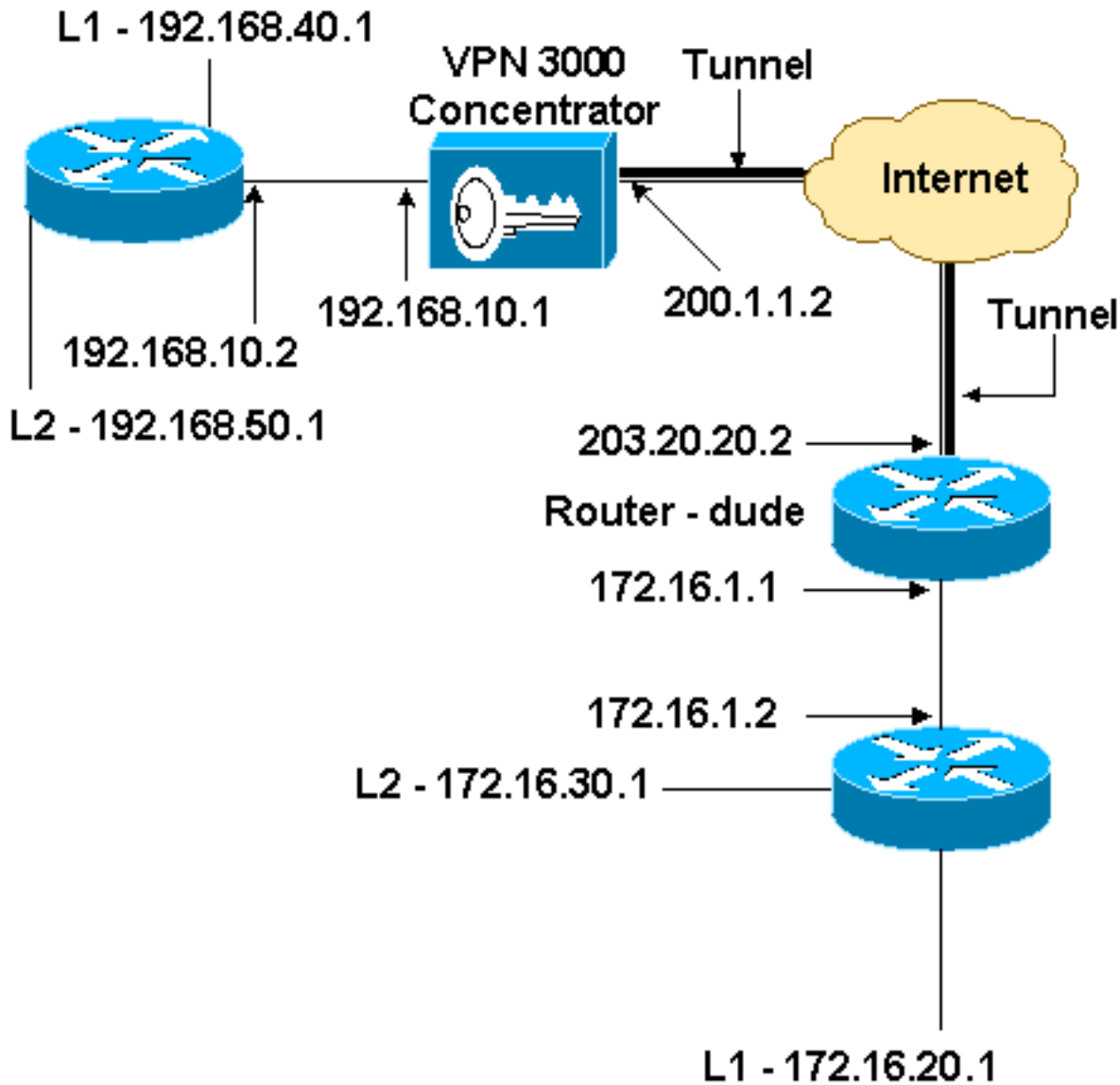
Configurazione

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.

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)

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.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

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:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

192.168.10.0/0.0.0.255
 192.168.40.0/0.0.0.255
 192.168.50.0/0.0.0.255

- Enter the Networks and Wildcard masks using the following format: n.n.n.n/n.n.n.n (e.g. 10.10.0.0/0.0.255.255).
- **Note:** Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Queste sono le reti remote:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

Apply Cancel Generate Local List

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.

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	Add Modify Copy Delete

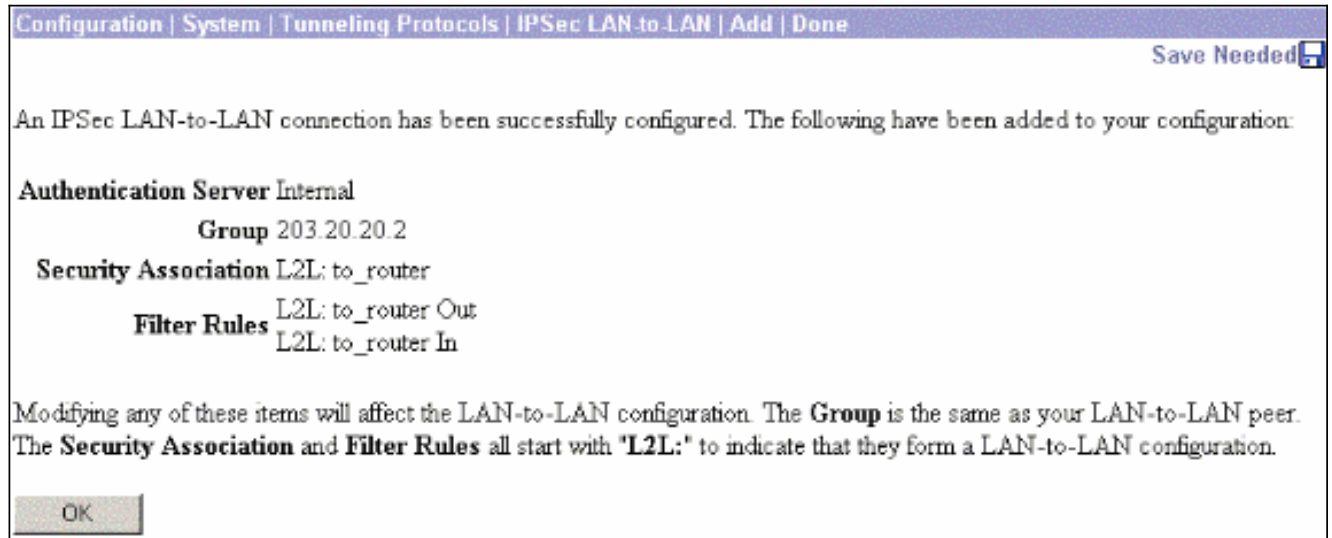
5. Scegliere **Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN** e definire il tunnel da LAN a LAN.

Add a new IPSec LAN-to-LAN connection.

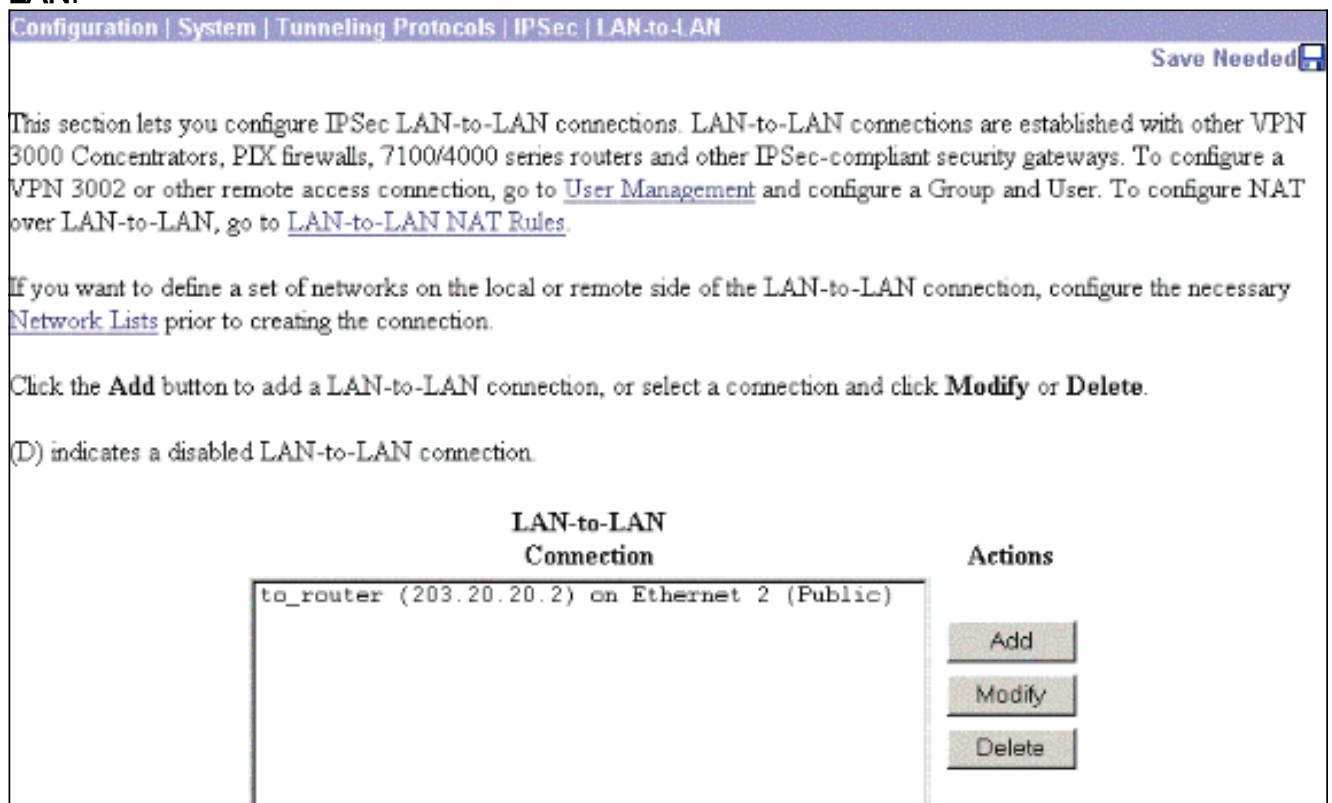
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
<p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

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.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="« Activate"/> <input type="button" value="Deactivate »"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

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

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5 ESP-3DES-MD5-DH5 ESP-3DES-MD5-DH7 ESP-3DES-NONE ESP-AES128-SHA ESP-DES-MD5 ESP-L2TP-TRANSPORT ESP/IKE-3DES-MD5 L2L: to_router	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

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

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	203.20.20.2	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

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](#)