Esempio di configurazione del tunneling ripartito per i client VPN su VPN 3000 Concentrator

Sommario

Introduzione

Questo documento offre istruzioni dettagliate su come consentire ai client VPN di accedere a Internet mentre sono tunneling in un concentratore VPN serie 3000. Questa configurazione consente ai client VPN di accedere in modo sicuro alle risorse aziendali tramite IPsec e di accedere a Internet in modo non protetto.

Nota: la configurazione del tunneling ripartito può rappresentare un potenziale rischio per la sicurezza. Poiché i client VPN hanno accesso non protetto a Internet, possono essere compromessi da un utente non autorizzato. L'utente non autorizzato potrebbe quindi accedere alla LAN aziendale tramite il tunnel IPsec. Un compromesso tra il tunneling completo e il tunneling suddiviso può essere quello di consentire solo l'accesso LAN locale ai client VPN. per ulteriori informazioni, fare riferimento a Consenti accesso LAN locale per i client VPN sull'esempio di configurazione di VPN 3000 Concentrator.

Prerequisiti

Requisiti

In questo documento si presume che nel concentratore VPN esista già una configurazione VPN ad accesso remoto funzionante. Fare riferimento all'esempio di configurazione di IPsec con client VPN su VPN 3000 Concentrator se non ne è già stato configurato uno.

Componenti usati

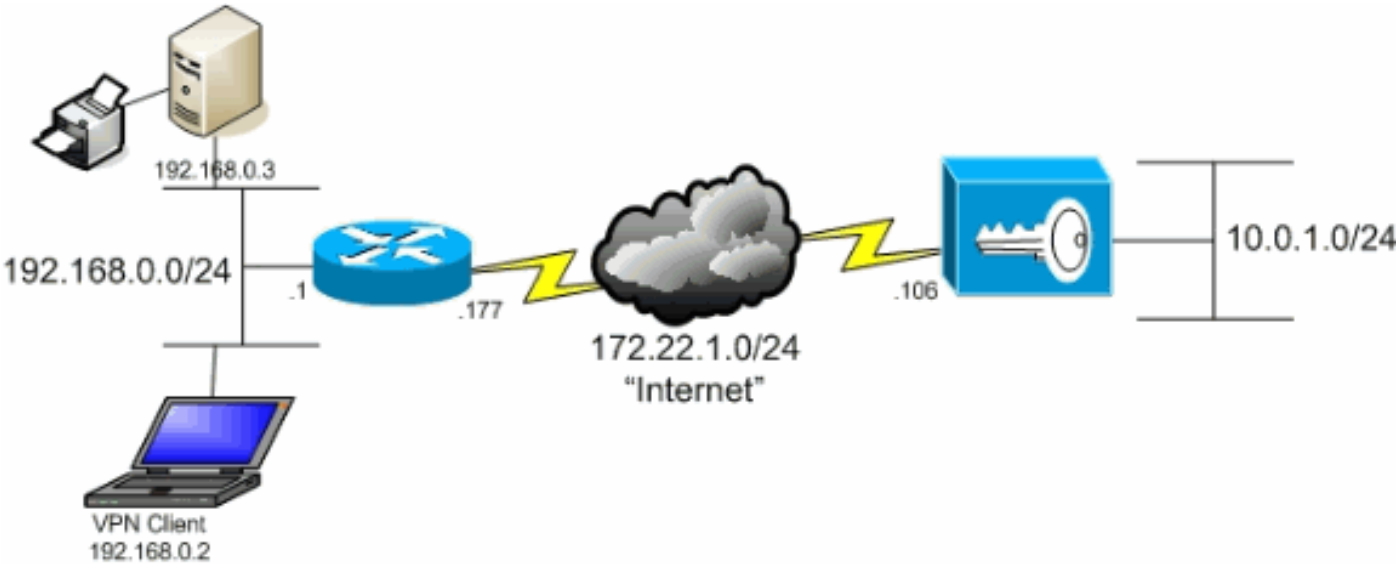
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco VPN serie 3000 Concentrator versione 4.7.2.H
- Cisco VPN Client versione 4.0.5

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.

Esempio di rete

Il client VPN si trova su una tipica rete SOHO e si connette tramite Internet all'ufficio principale.



Convenzioni

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

Premesse

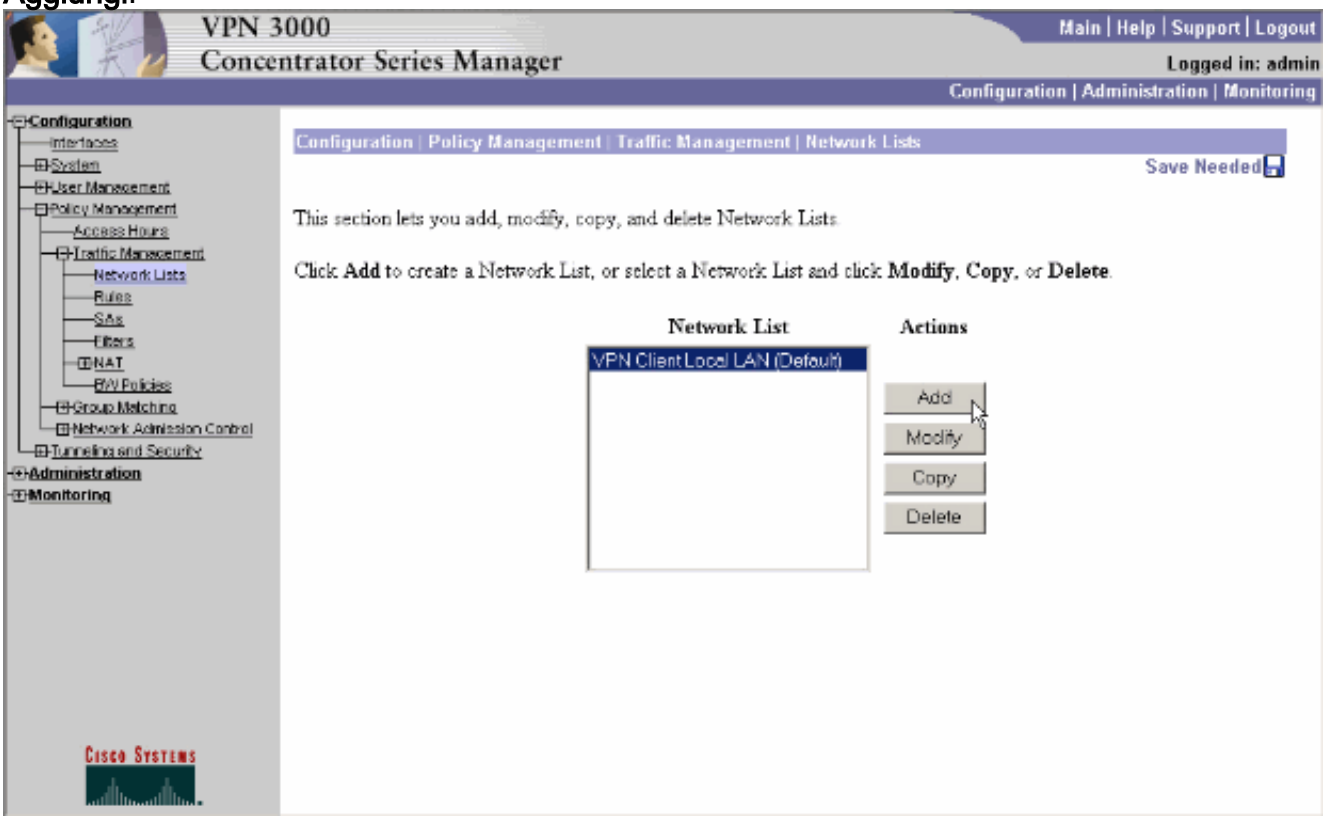
In uno scenario di base da client VPN a concentratore VPN, tutto il traffico proveniente dal client VPN viene crittografato e inviato al concentratore VPN, a prescindere dalla destinazione. In base alla configurazione e al numero di utenti supportati, tale configurazione può richiedere un utilizzo intensivo della larghezza di banda. Il tunneling ripartito può risolvere questo problema consentendo agli utenti di inviare solo il traffico destinato alla rete aziendale attraverso il tunnel. Tutto il resto del traffico, ad esempio messaggistica istantanea, e-mail o navigazione casuale, viene inviato a Internet tramite la LAN locale del client VPN.

Configurazione del tunneling ripartito sul concentratore VPN

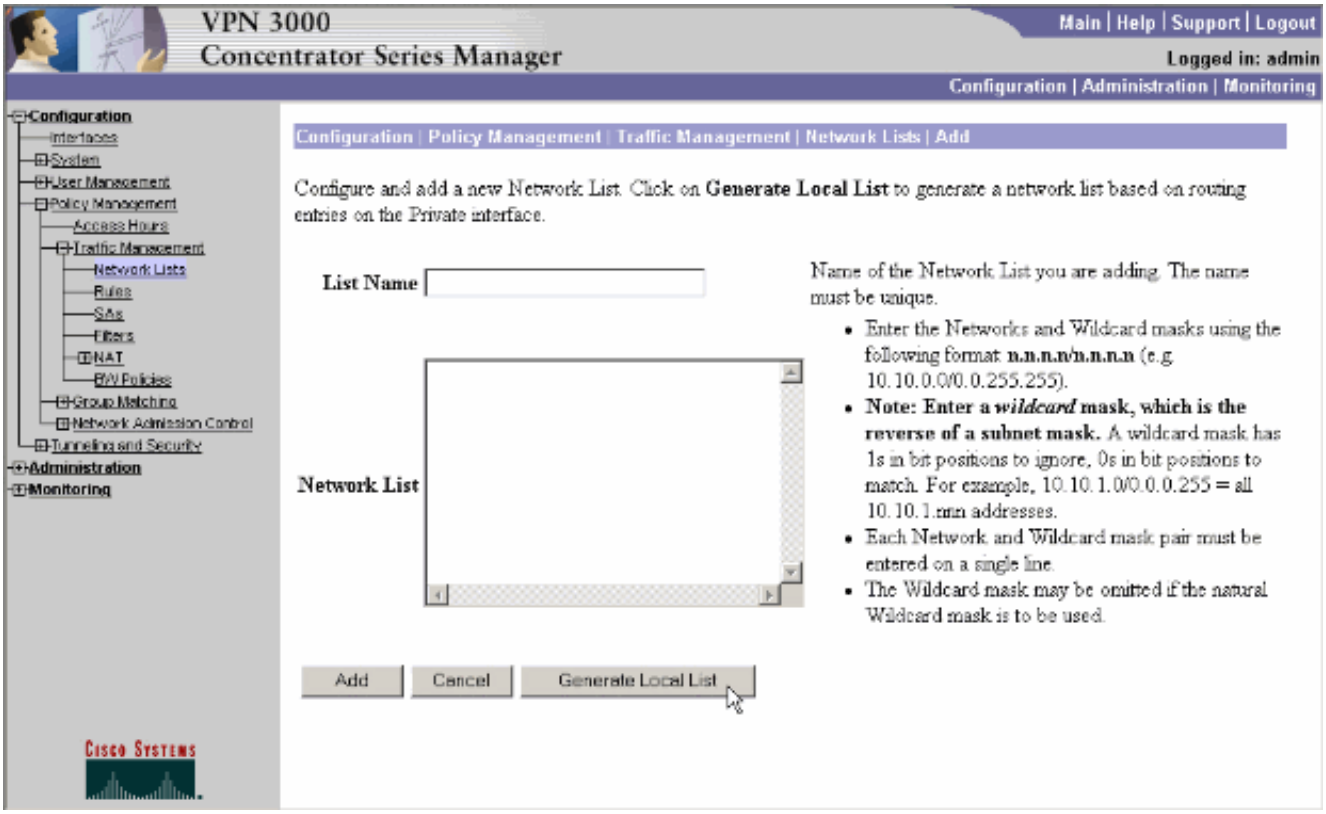
Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling

suddiviso per gli utenti del gruppo. Creare innanzitutto un elenco delle reti. Questo elenco definisce le reti di destinazione a cui il client VPN invia il traffico crittografato. Una volta creato l'elenco, aggiungerlo ai criteri di tunneling suddiviso del gruppo di tunnel client.

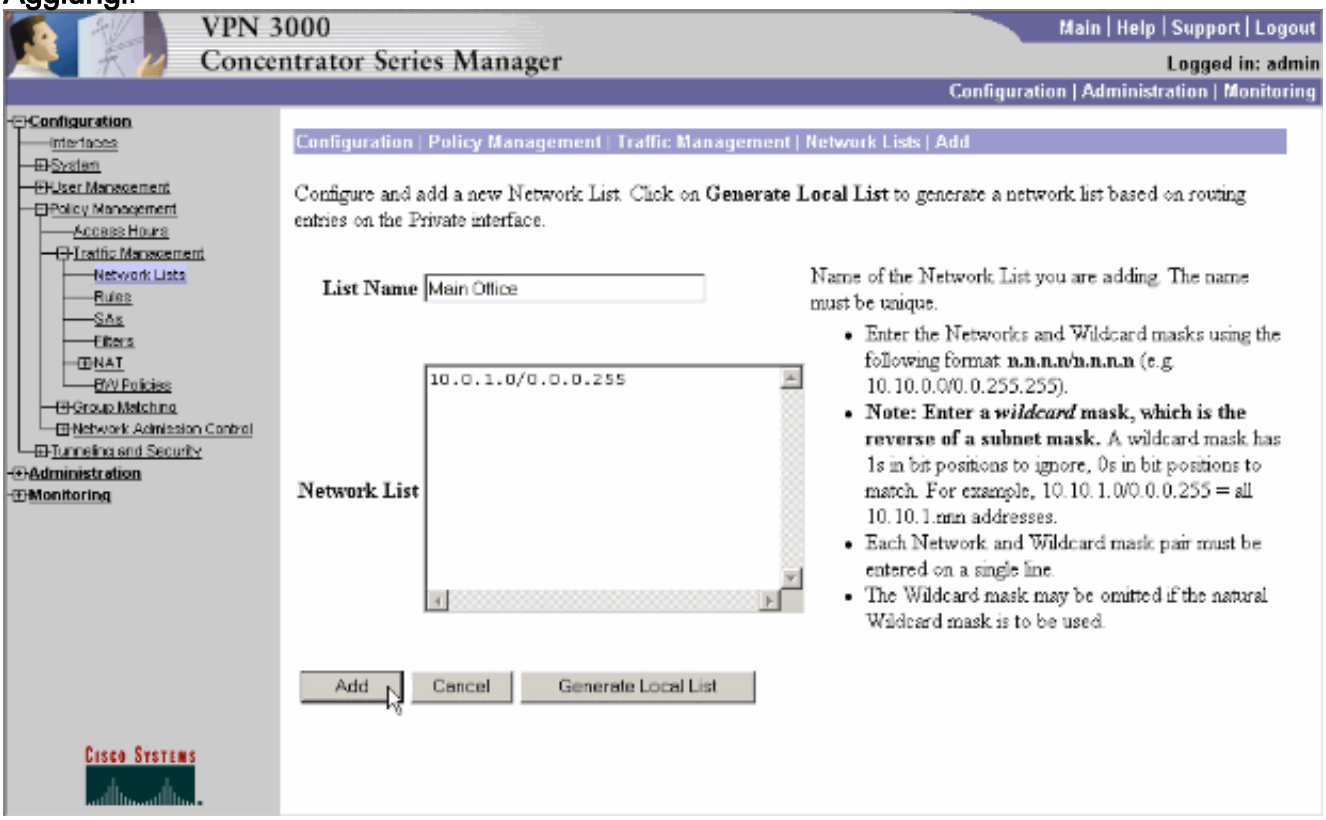
1. Scegliere **Configurazione > Gestione delle policy > Gestione del traffico > Elenchi di rete** e fare clic su **Aggiungi**.



2. Questo elenco definisce le reti di destinazione a cui il client VPN invia il traffico crittografato. Immettere manualmente queste reti o fare clic su **Genera elenco locale** per creare un elenco basato sulle voci di routing sull'interfaccia privata di VPN Concentrator.Nell'esempio riportato sotto, l'elenco è stato creato automaticamente.

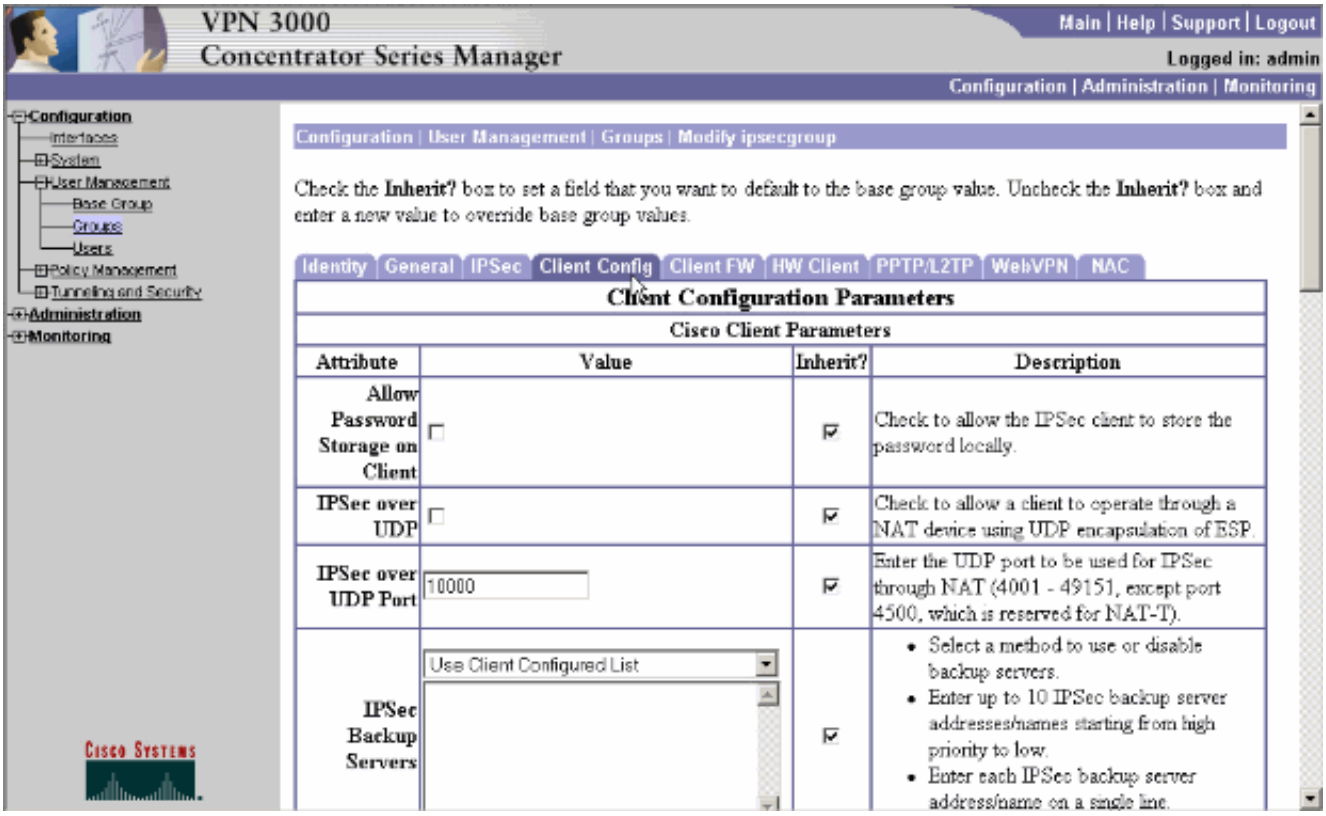


3. Una volta creato o compilato, fornire un nome per l'elenco e fare clic su **Aggiungi**.

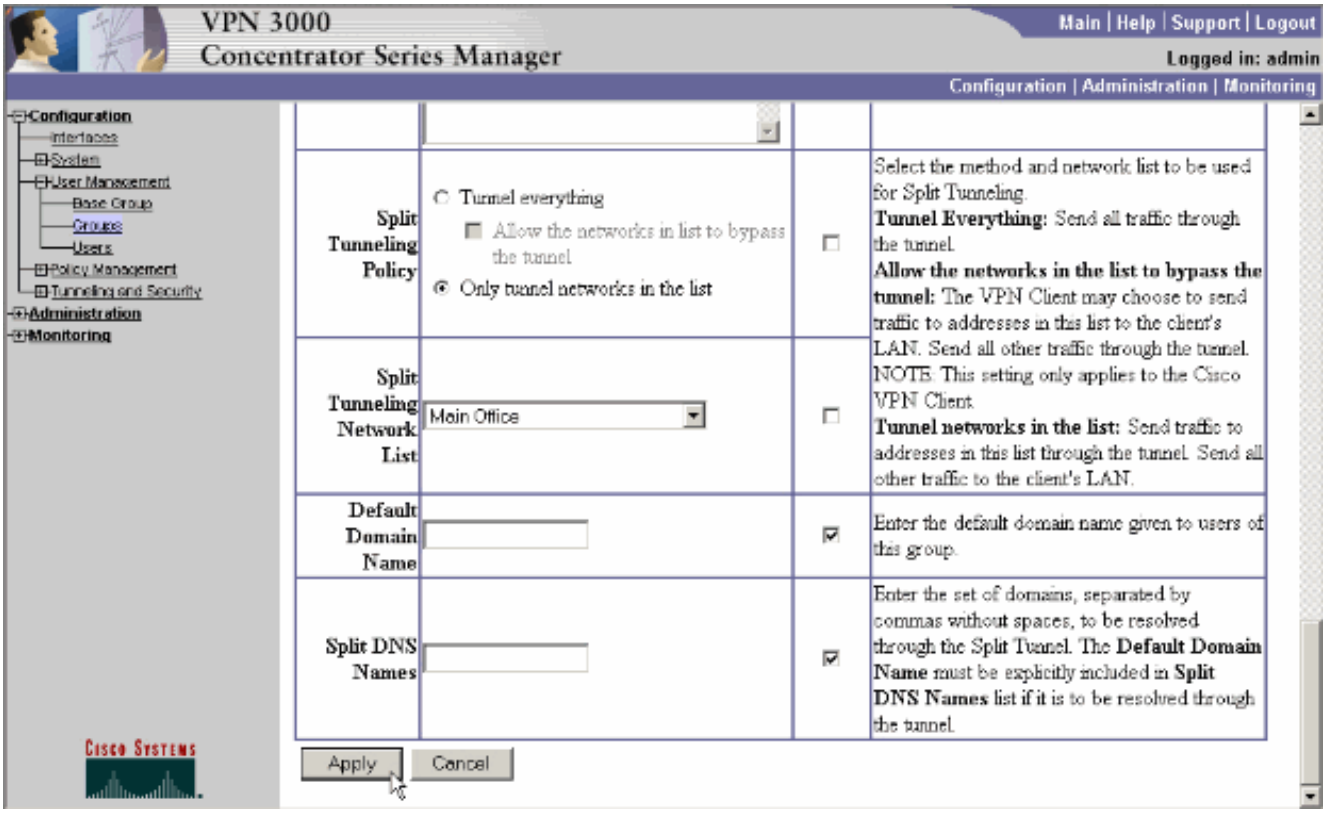


4. Dopo aver creato l'elenco delle reti, assegnarlo a un gruppo di tunnel. Scegliere **Configurazione > Gestione utente > Gruppi**, selezionare il gruppo che si desidera modificare e fare clic su **Modifica gruppo**.

5. Andare alla scheda Configurazione client del gruppo che si è scelto di modificare.



6. Scorrere l'elenco fino alle sezioni Criteri di tunneling suddivisi e Elenco reti tunneling suddivise e fare clic su **Solo reti tunnel nell'elenco**.
7. Selezionare l'elenco creato in precedenza dall'elenco a discesa. In questo caso si tratta dell'**ufficio principale**. L'eredità? le caselle di controllo vengono svuotate automaticamente in entrambi i
casi.



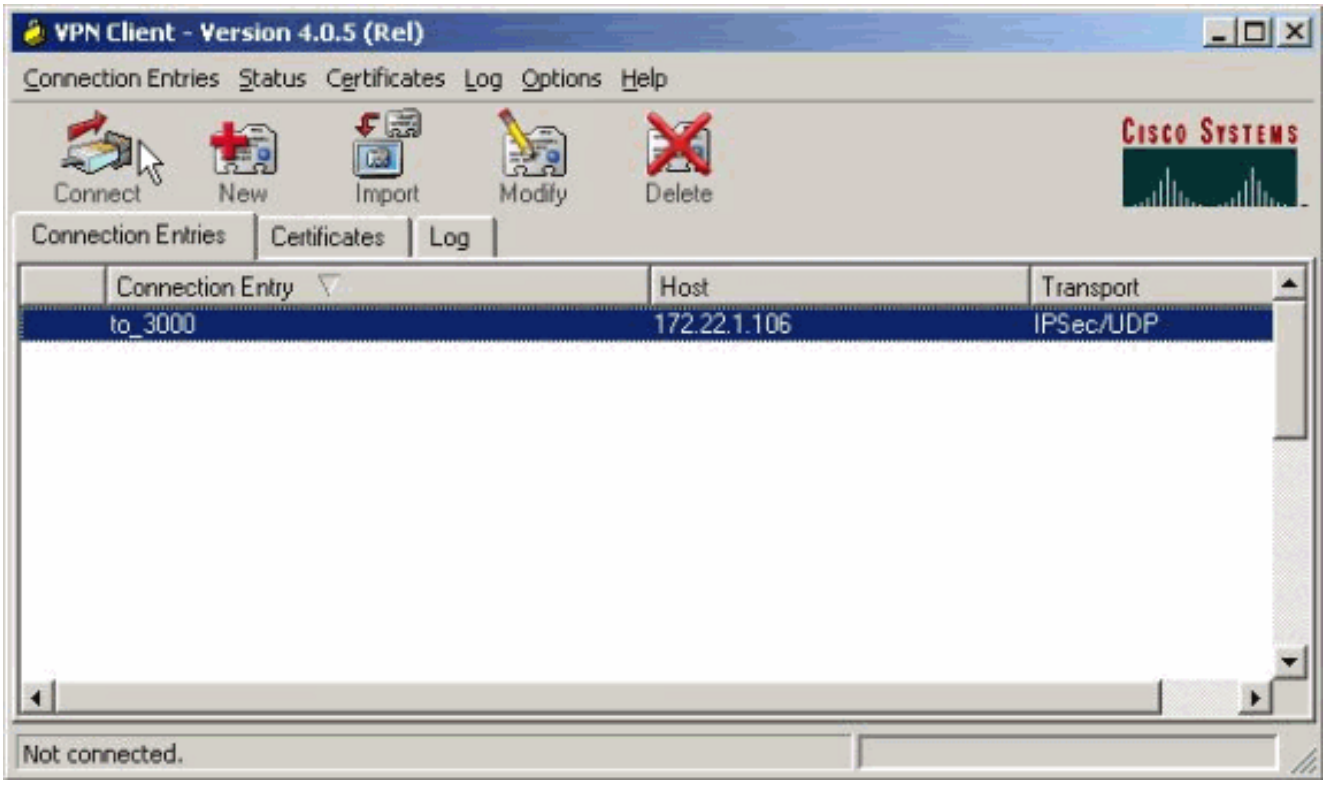
8. Al termine, fare clic su **Apply** (Applica).

Verifica

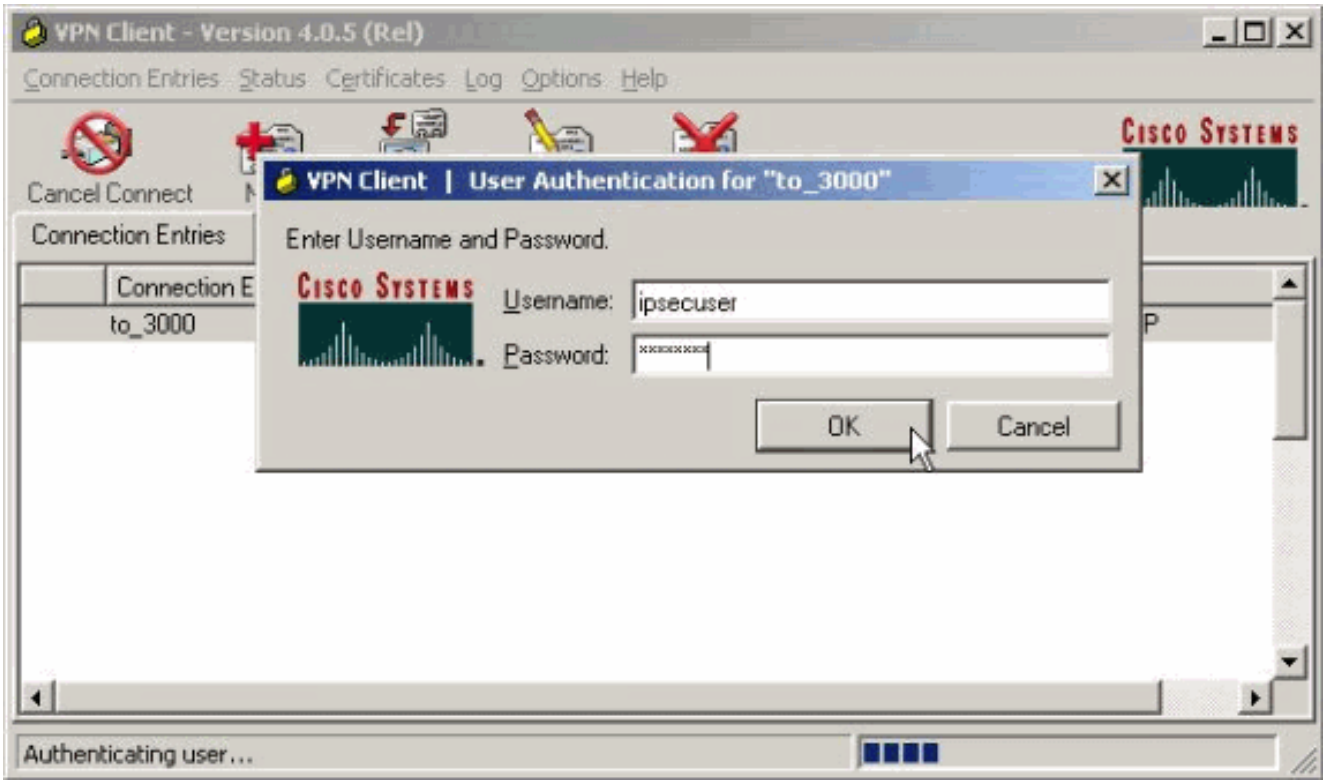
Connessione con il client VPN

Connettere il client VPN a VPN Concentrator per verificare la configurazione.

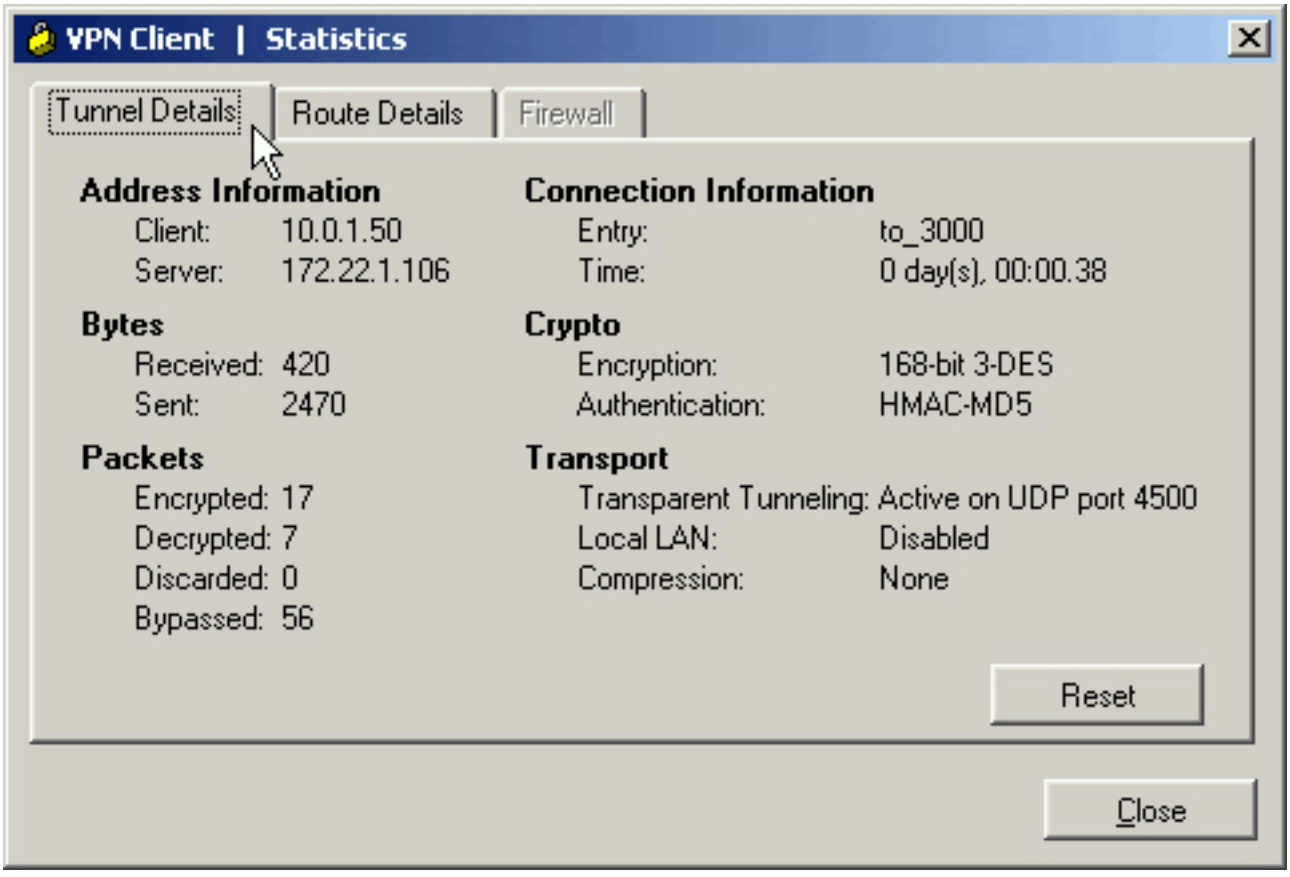
1. Scegliere la voce di connessione dall'elenco e fare clic su **Connetti**.



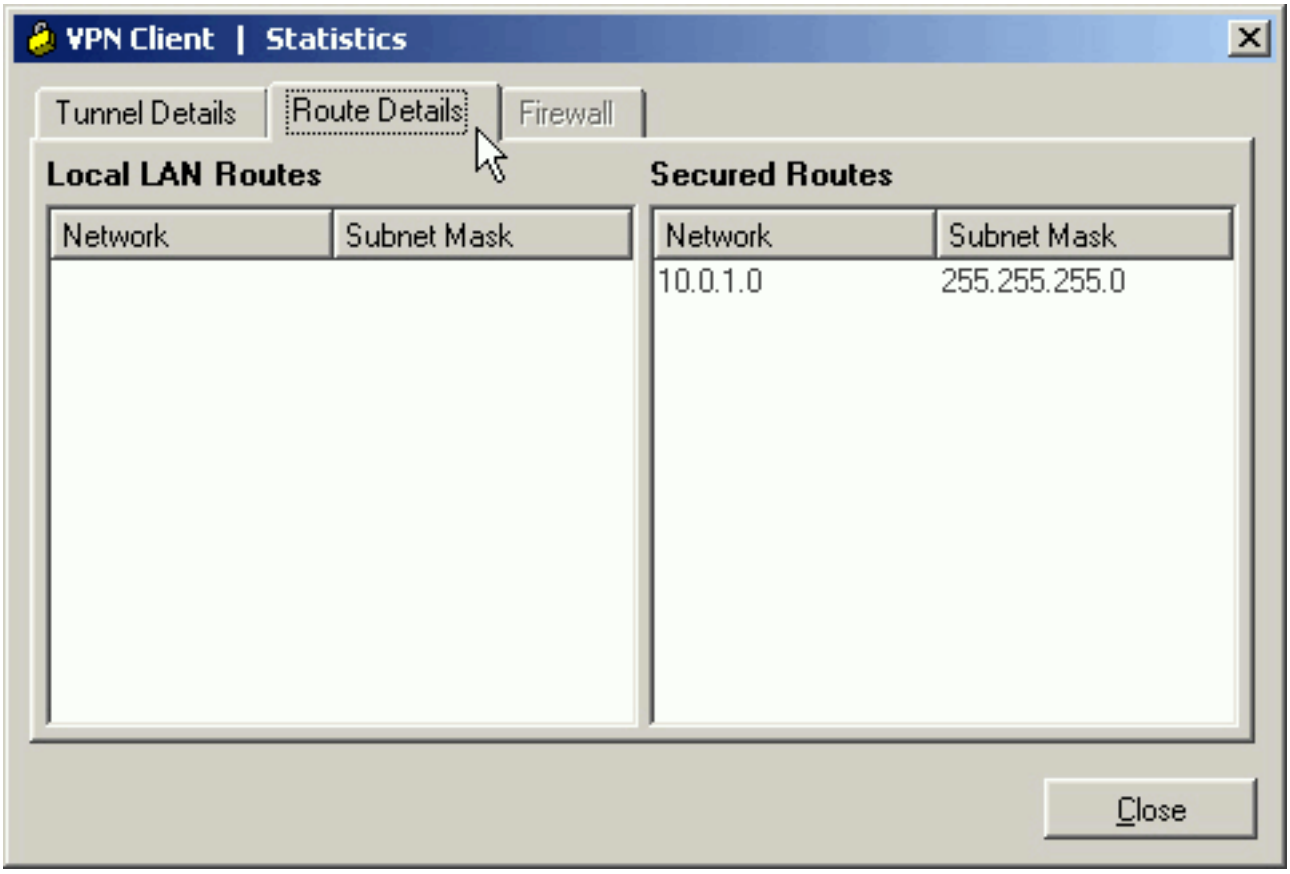
2. Immettere le credenziali.



3. Scegliere **Stato > Statistiche...** per visualizzare la finestra Dettagli tunnel, in cui è possibile esaminare i dettagli del tunnel e verificare il flusso del traffico.

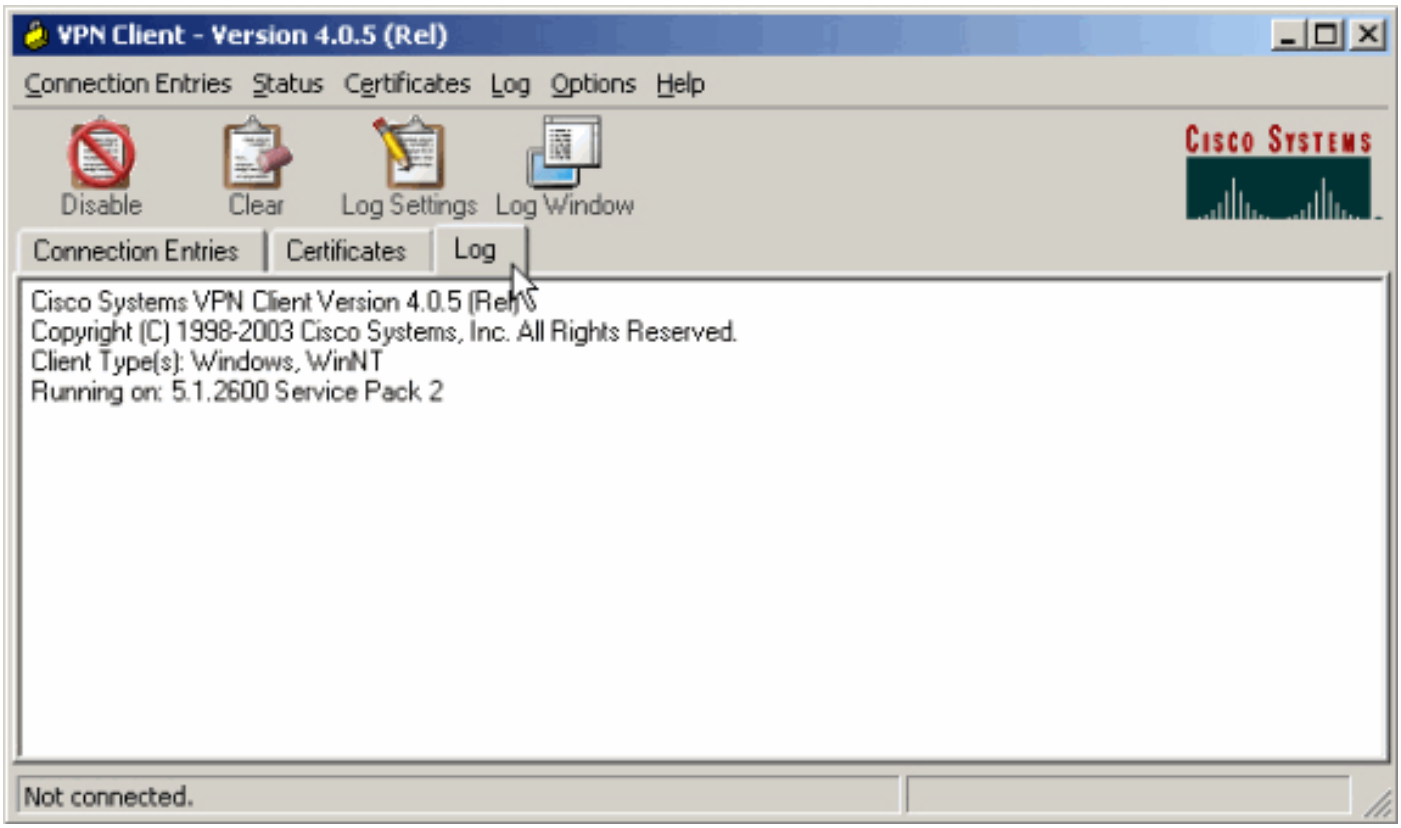


4. Andare alla scheda Dettagli route per vedere a quali reti il client VPN invia il traffico crittografato. Nell'esempio, il client VPN comunica in modo sicuro con 10.0.1.0/24, mentre tutto il resto del traffico viene inviato a Internet in modalità non crittografata.



Visualizza registro client VPN

Quando si esamina il registro del client VPN, è possibile determinare se è impostato o meno il parametro che consente il tunneling suddiviso. Andare alla scheda Log nel client VPN per visualizzare il log. Fare clic su **Log Settings** (Impostazioni registro) per regolare gli elementi registrati. Nell'esempio, IKE e IPsec sono impostati su **3- High** mentre tutti gli altri elementi del log sono impostati su **1 - Low**.



```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:21:43.106  07/21/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.
```

Risoluzione dei problemi

Per informazioni generali sulla risoluzione dei problemi relativi a questa configurazione, fare riferimento a Esempio di configurazione di IPsec con VPN Client su VPN 3000 Concentrator.

Informazioni correlate

- Esempio di configurazione di IPsec con VPN Client su VPN 3000 Concentrator
- Cisco VPN serie 3000 concentrator
- Cisco VPN Client
- Documentazione e supporto tecnico – Cisco Systems