

Configurazione dell'accesso del client AnyConnect alla LAN locale

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Premesse](#)

[Configurazione dell'accesso LAN locale per il client AnyConnect Secure Mobility](#)

[Configurazione dell'ASA con ASDM](#)

[Configurazione dell'ASA dalla CLI](#)

[Configurazione del client Cisco AnyConnect Secure Mobility](#)

[Preferenze utente](#)

[Esempio di profilo XML](#)

[Verifica](#)

[Cisco AnyConnect Secure Mobility Client](#)

[Test dell'accesso LAN locale con ping](#)

[Risoluzione dei problemi](#)

[Impossibile stampare o cercare per nome](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come consentire al client Cisco AnyConnect Secure Mobility di accedere alla LAN locale mentre è connesso a una appliance Cisco ASA.

Prerequisiti

Requisiti

In questo documento si presume che esista già una configurazione VPN ad accesso remoto funzionale su Cisco Adaptive Security Appliance (ASA).

Fare riferimento alla [CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17](#) per l'assistenza alla configurazione, se necessario.

Componenti usati

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

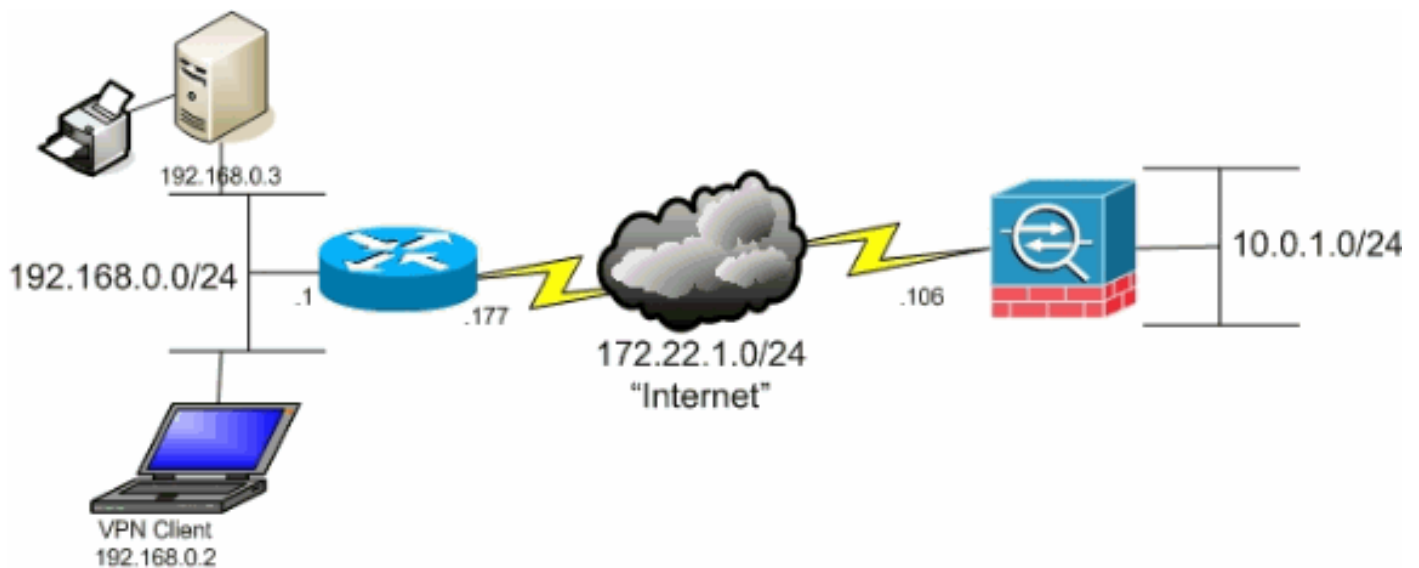
hardware:

- Cisco ASA serie 5500 versione 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) versione 7.1(6)
- Cisco AnyConnect Secure Mobility Client versione 3.1.05152

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 si trova su una rete SOHO (Small Office / Home Office) tipica e si connette tramite Internet all'ufficio principale.



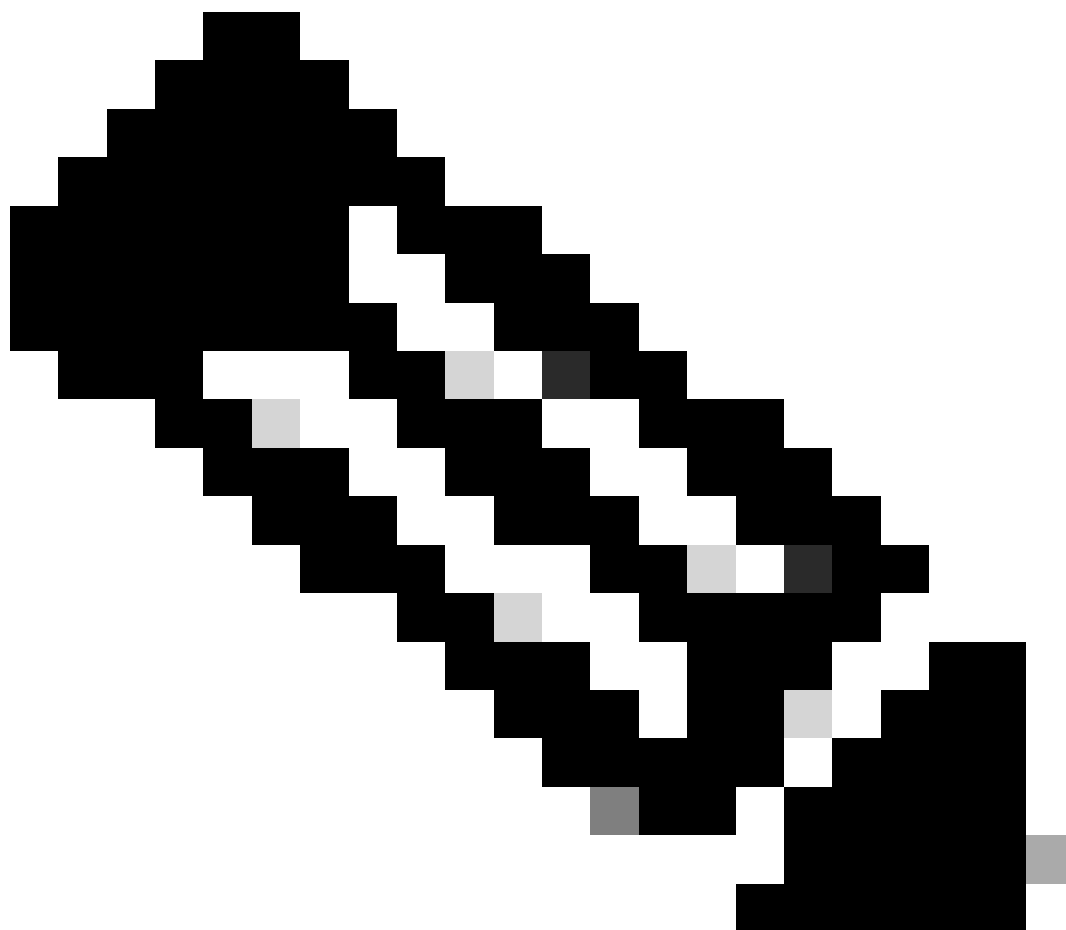
Premesse

Questa configurazione consente a Cisco AnyConnect Secure Mobility Client di accedere in modo sicuro alle risorse aziendali tramite IPsec, Secure Sockets Layer (SSL) o Internet Key Exchange versione 2 (IKEv2) e allo stesso tempo permette al client di eseguire attività quali la stampa del percorso in cui si trova. Se autorizzato, il traffico destinato a Internet viene comunque tunnelato sull'appliance ASA.


A differenza di uno scenario classico di tunneling con split, in cui tutto il traffico Internet viene inviato in modalità non crittografata, quando si abilita l'accesso LAN locale per i client VPN, questi client possono comunicare in modalità non crittografata solo con i dispositivi della rete in cui si trovano. Ad esempio, un client a cui è consentito l'accesso LAN locale mentre è connesso all'appliance ASA da casa può stampare con la propria stampante ma non può accedere a Internet a meno che non invii prima il traffico sul tunnel.

L'elenco degli accessi viene usato per consentire l'accesso alla LAN locale nello stesso modo in cui il tunneling suddiviso è configurato sull'appliance ASA. Tuttavia, a differenza dello scenario di

tunneling suddiviso, questo elenco degli accessi non definisce le reti che devono essere crittografate. Definisce invece quali reti non devono essere crittografate. Inoltre, a differenza dello scenario di tunneling suddiviso, le reti effettive nell'elenco non devono essere note. L'ASA fornisce invece una rete predefinita di 0.0.0.0/255.255.255.255, ossia la LAN locale del client.



Nota: non si tratta di una configurazione per il tunneling suddiviso in cui il client ha accesso non crittografato a Internet mentre è connesso all'appliance ASA. Per informazioni su come configurare il tunneling suddiviso sull'appliance ASA, consultare il documento [Set the Split-Tunneling Policy](#) in CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17.

 Nota: quando il client è connesso e configurato per l'accesso LAN locale, non è possibile stampare o sfogliare per nome sulla LAN locale. Tuttavia, è possibile sfogliare o stampare in base all'indirizzo IP. Per ulteriori informazioni e soluzioni per questa situazione, vedere la sezione [Risoluzione dei problemi](#) di questo documento.

Configurazione dell'accesso LAN locale per il client AnyConnect Secure Mobility

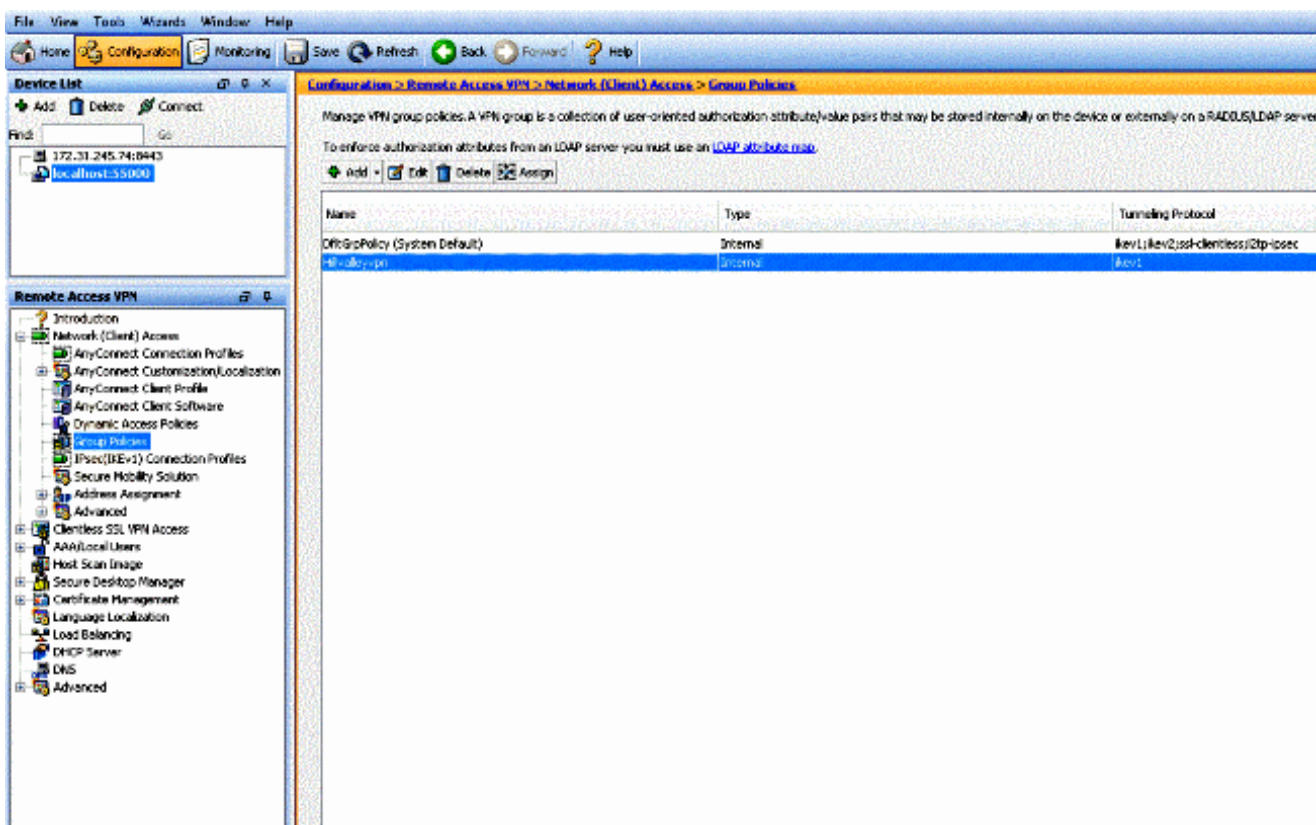
Per consentire ai client Cisco AnyConnect Secure Mobility di accedere alla LAN locale mentre sono connessi all'appliance ASA, completare le seguenti attività:

- [Configurare l'ASA tramite ASDM](#) o [configurare l'ASA tramite la CLI](#)
- [Configurazione del client Cisco AnyConnect Secure Mobility](#)

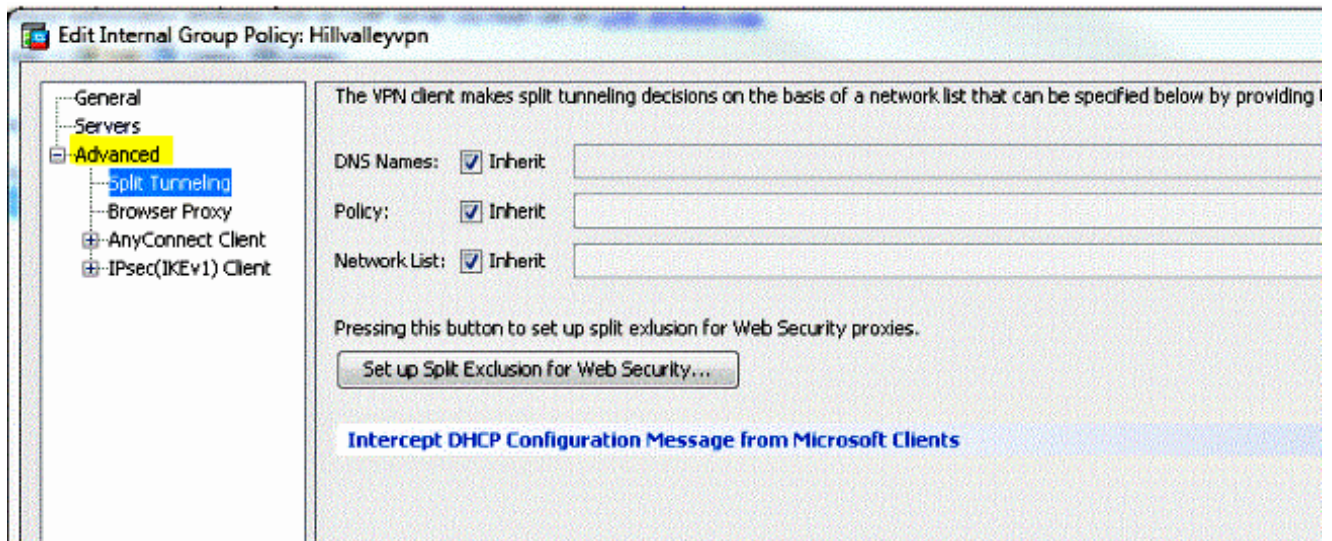
Configurazione dell'ASA con ASDM

Completare questi passaggi nell'ASDM per consentire ai client VPN di avere accesso LAN locale mentre sono connessi all'ASA:

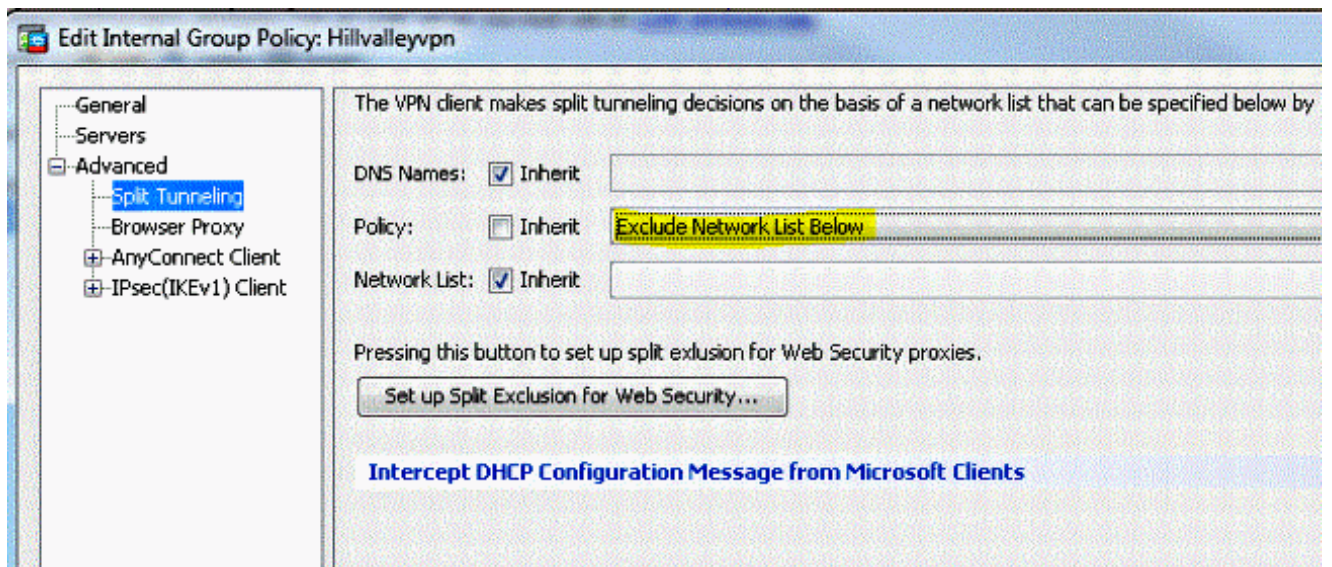
1. Scegliere **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** e selezionare i Criteri di gruppo per i quali si desidera abilitare l'accesso LAN locale. Quindi fate clic su **Edit**.



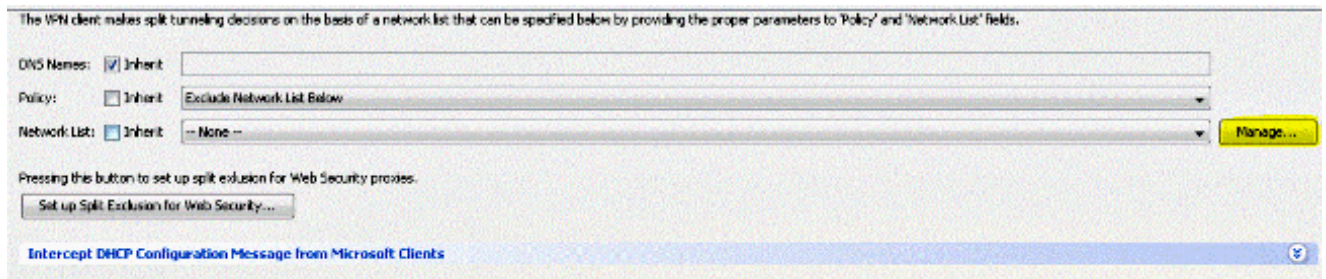
- Vai a **Advanced > Split Tunneling**.



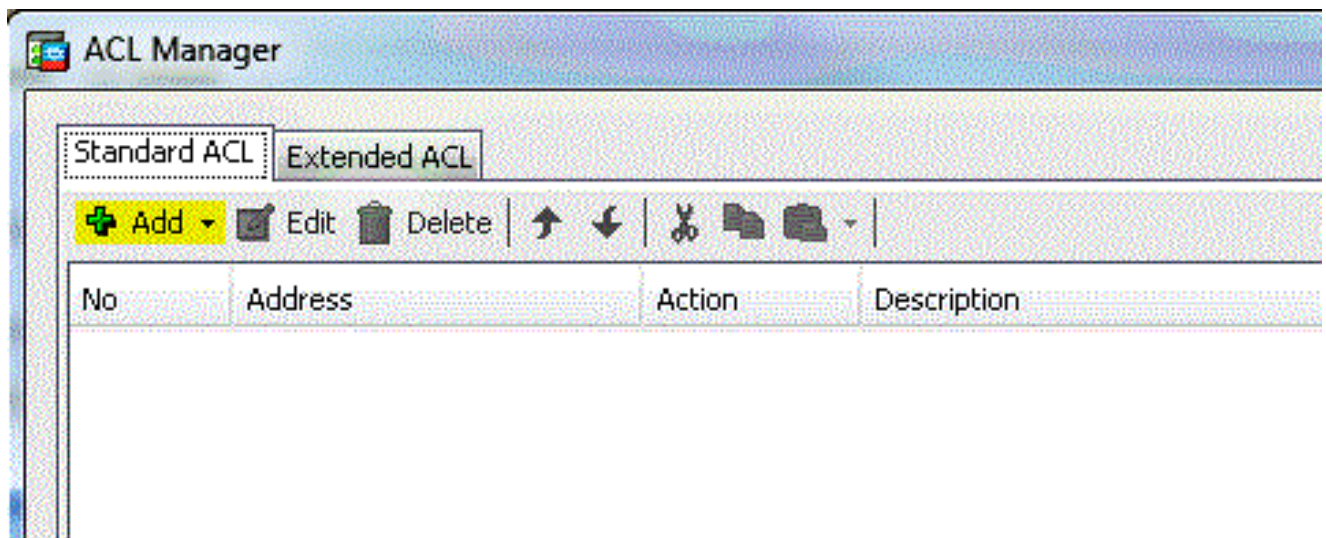
- Deselezionare la **Inherit** casella per Criterio e scegliere **Exclude Network List Below**.



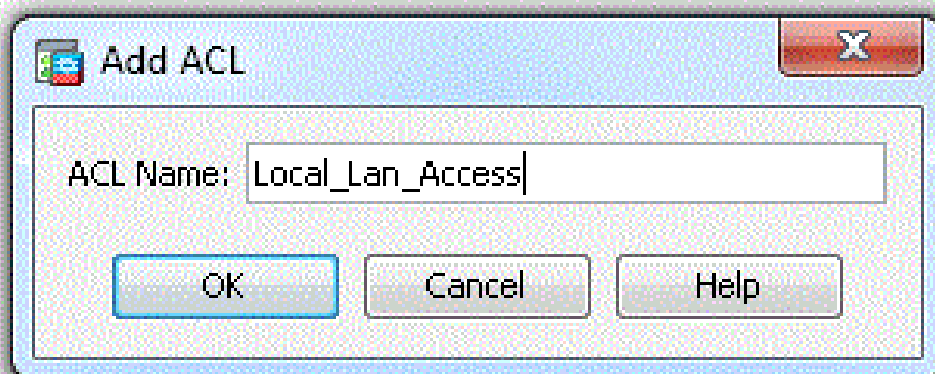
- Deselezionare la **Inherit** casella per Elenco reti e fare clic su **Manage** per avviare Gestione elenchi di controllo di accesso (ACL).



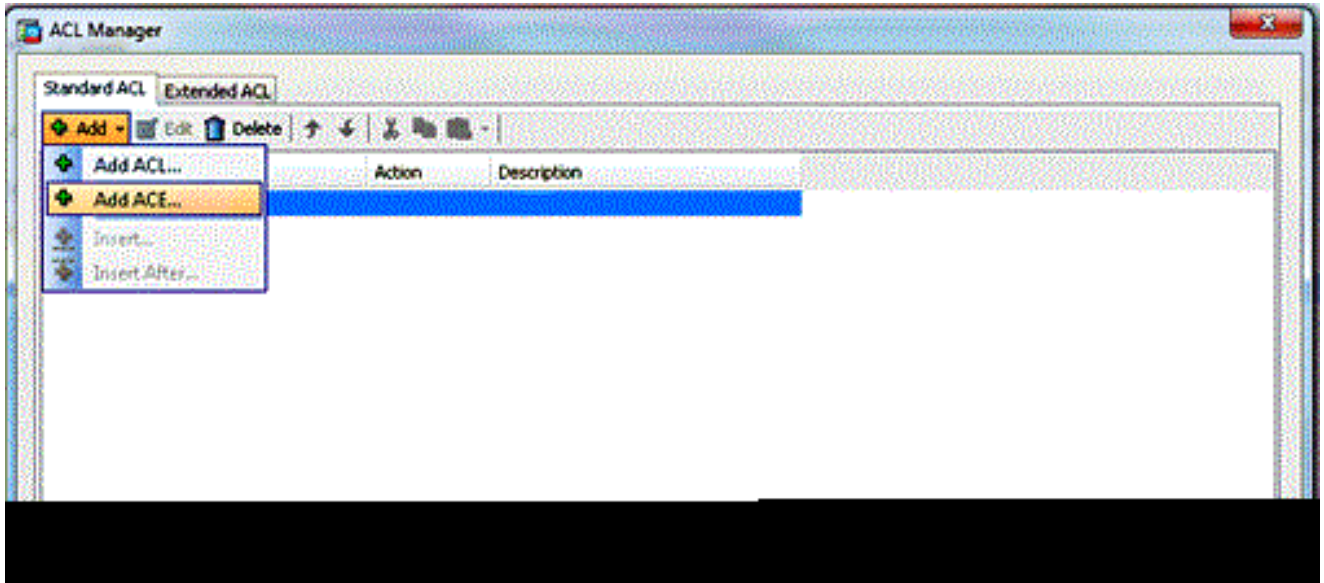
- In Gestione ACL, selezionare **Add > Add ACL...** il comando per creare un nuovo elenco degli accessi.



- Specificare un nome per l'ACL e fare clic su **OK**.



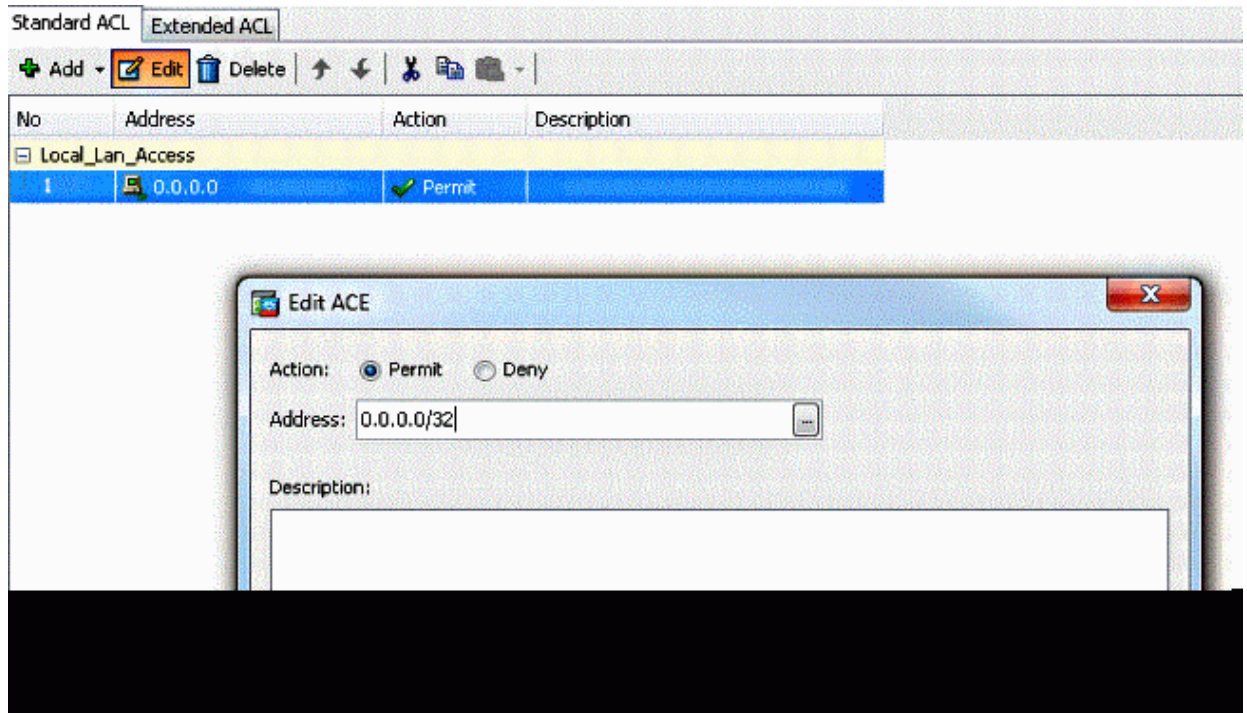
- Una volta creato l'ACL, scegliere **Add > Add ACE...** di aggiungere una voce di controllo di accesso (ACE, Access Control Entry).



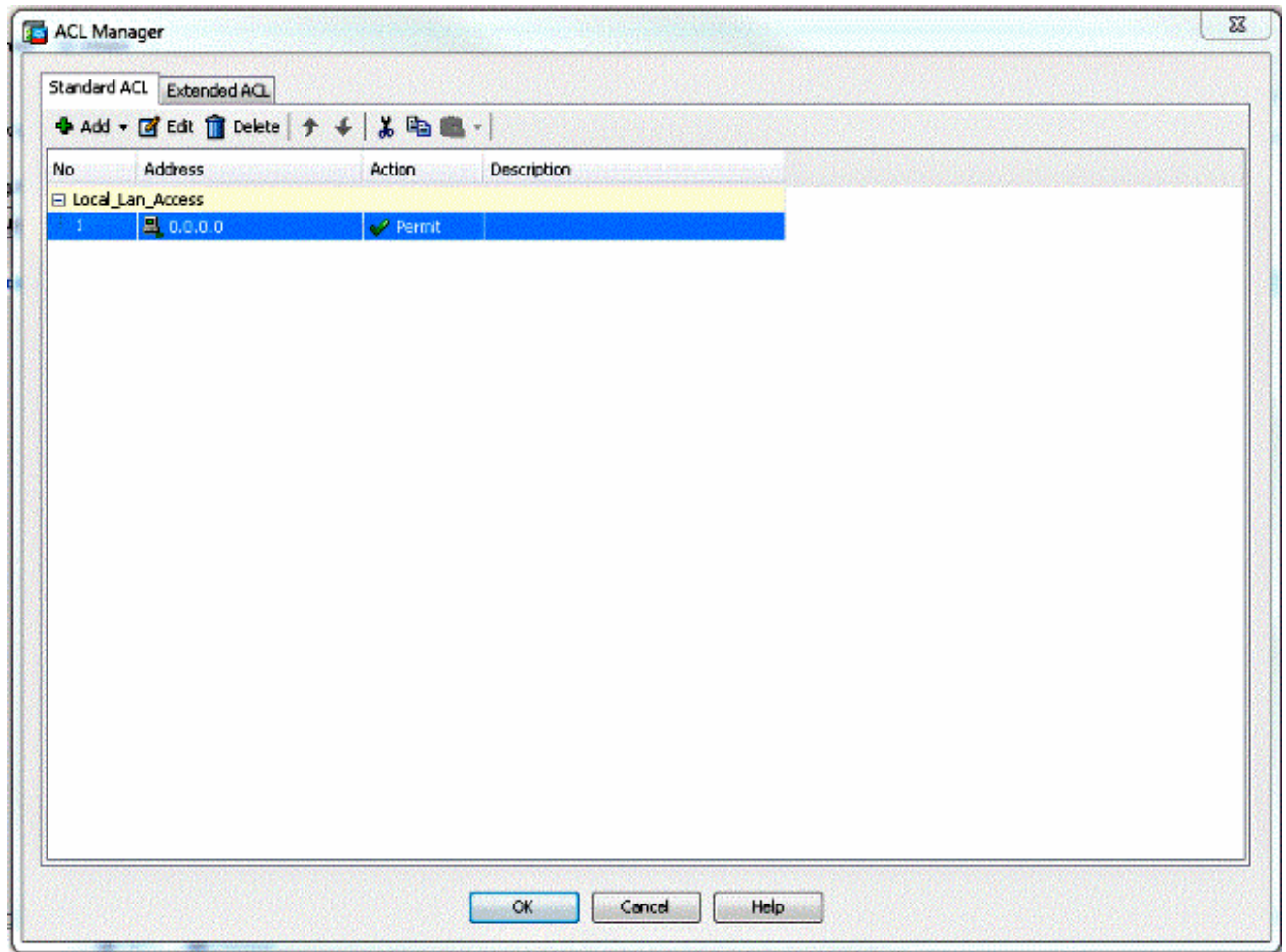
- Definire la voce ACE corrispondente alla LAN locale del client.

a. Scegliere **Permit**.

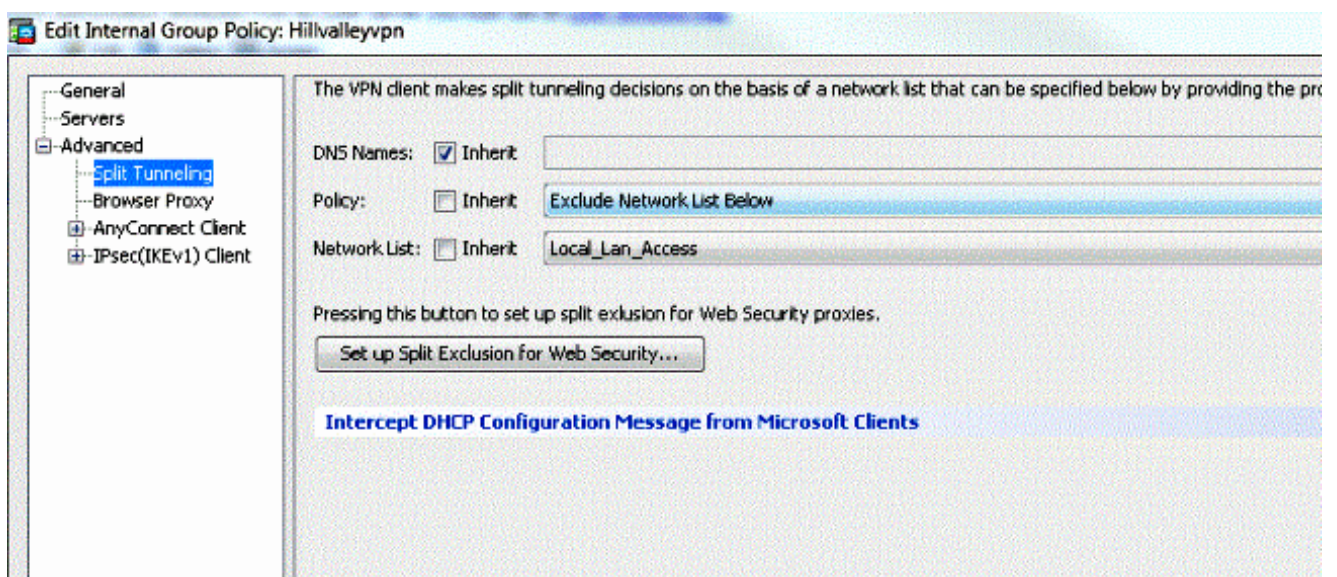
- Scegliere un indirizzo IP di **0.0.0.0**
- Scegliere una maschera di rete di **/32**.
- *(Facoltativo)* Fornire una descrizione.
- Fare clic su **. OK**



- Fare clic su **OK** per uscire da Gestione ACL.



- Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.



- Fare clic **OK** per tornare alla configurazione di Criteri di gruppo.

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameter

DNS Names: Inherit

Policy: Inherit

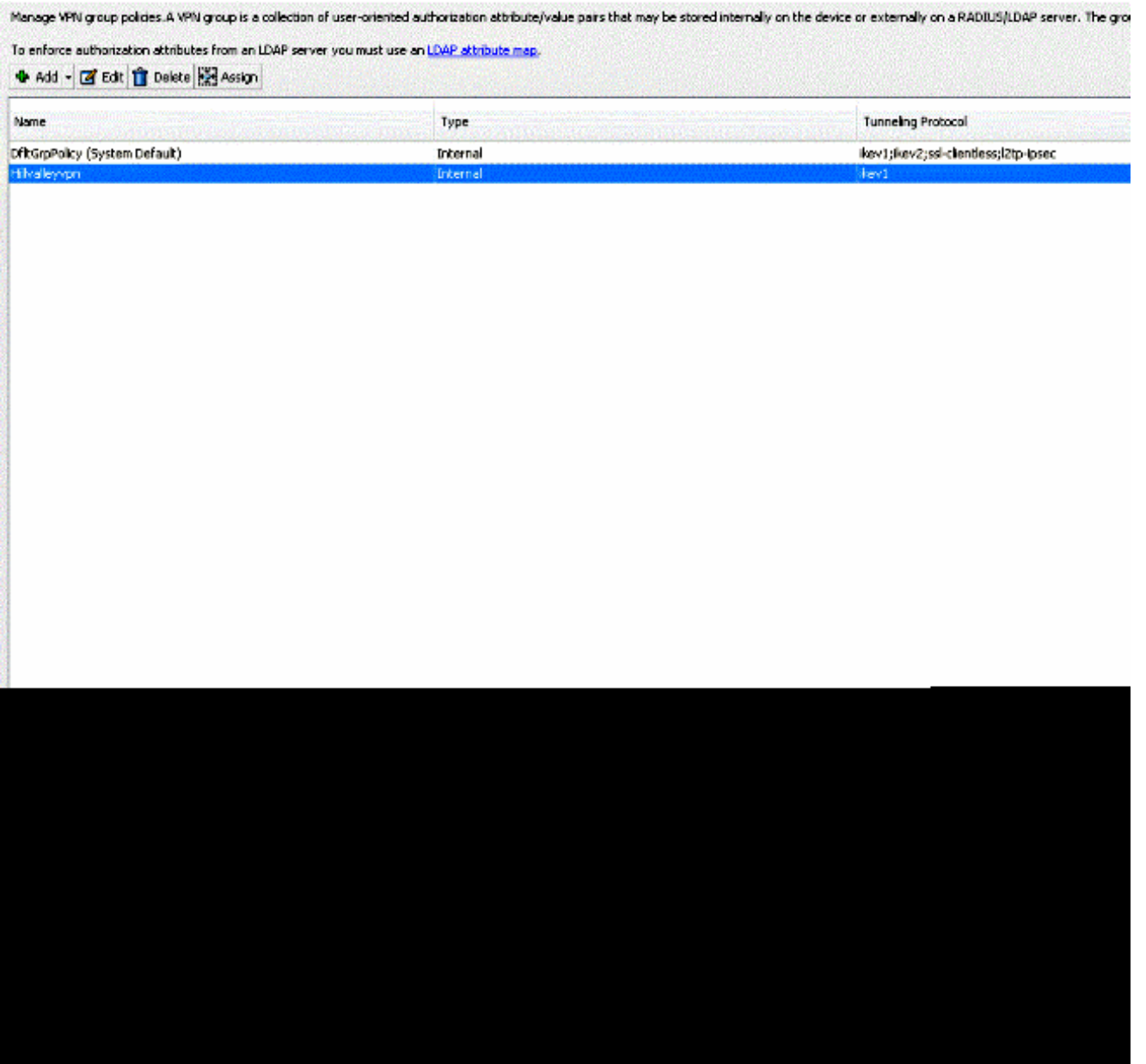
Network List: Inherit

Pressing this button to set up split exclusion for Web Security proxies.

Intercept DHCP Configuration Message from Microsoft Clients

Next Previous

- Fare clic su **Apply** e quindi **Send** (se necessario) per inviare i comandi all'appliance ASA.



Configurazione dell'ASA dalla CLI

Anziché utilizzare ASDM, è possibile completare questi passaggi nella CLI dell'ASA per consentire ai client VPN di avere accesso alla LAN locale mentre sono connessi all'ASA:

- Accedere alla modalità di configurazione.

```
<#root>
```

```
ciscoasa>
```

enable

Password:
ciscoasa#

configure terminal

ciscoasa(config)#

- Creare l'elenco degli accessi per consentire l'accesso alla LAN locale.

<#root>

ciscoasa(config)#

access-list Local_LAN_Access remark Client Local LAN Access

ciscoasa(config)#

access-list Local_LAN_Access standard permit host 0.0.0.0

- Immettere la modalità di configurazione di Criteri di gruppo per il criterio che si desidera modificare.

<#root>

ciscoasa(config)#

```
group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

- Specificare i criteri per il tunnel suddiviso. In questo caso, la politica è `excludespecified`.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-policy excludespecified
```

- Specificare l'elenco degli accessi al tunnel suddiviso. In questo caso, l'elenco è `Local_LAN_Access`.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-network-list value Local_LAN_Access
```

- Immettere questo comando

```
<#root>
```

```
ciscoasa(config)#
```

```
tunnel-group hillvalleyvpn general-attributes
```

- Associare i Criteri di gruppo al gruppo di tunnel.

```
<#root>
```

```
ciscoasa(config-tunnel-ipsec)#
```

```
default-group-policy hillvalleyvpn
```

- Uscire dalle due modalità di configurazione.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
exit
```

```
ciscoasa(config)#
```

```
exit
```

```
ciscoasa#
```

- **Salvare** la configurazione nella memoria RAM non volatile (NVRAM) e premere **Enter** quando richiesto per specificare il nome del file di origine.

```
<#root>
```

```
ciscoasa#
```

```
copy running-config startup-config
```

```
Source filename [running-config]?  
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a  
  
3847 bytes copied in 3.470 secs (1282 bytes/sec)  
ciscoasa#
```

Configurazione del client Cisco AnyConnect Secure Mobility

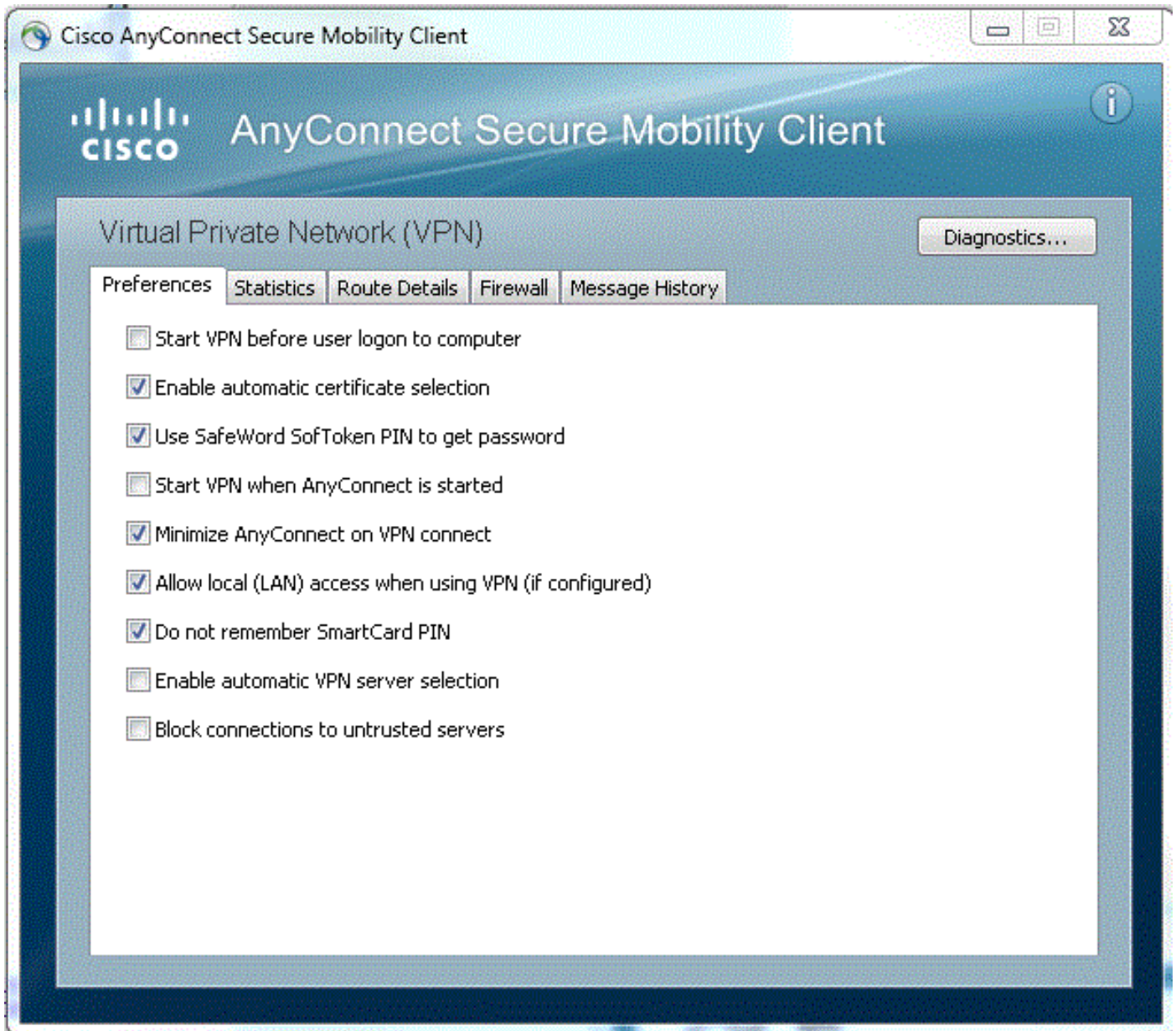
Per configurare Cisco AnyConnect Secure Mobility Client, fare riferimento alla sezione [Configure AnyConnect Connections](#) del *manuale CLI 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17*.

Il tunneling split-exclude richiede l'abilitazione **AllowLocalLanAccess** di AnyConnect nel client. Tutto il tunneling split-exclude è considerato come accesso LAN locale. Per usare la funzione di esclusione dello split-tunneling, è necessario abilitare la **AllowLocalLanAccess** preferenza nelle preferenze del client VPN AnyConnect. Per impostazione predefinita, l'accesso LAN locale è disabilitato.

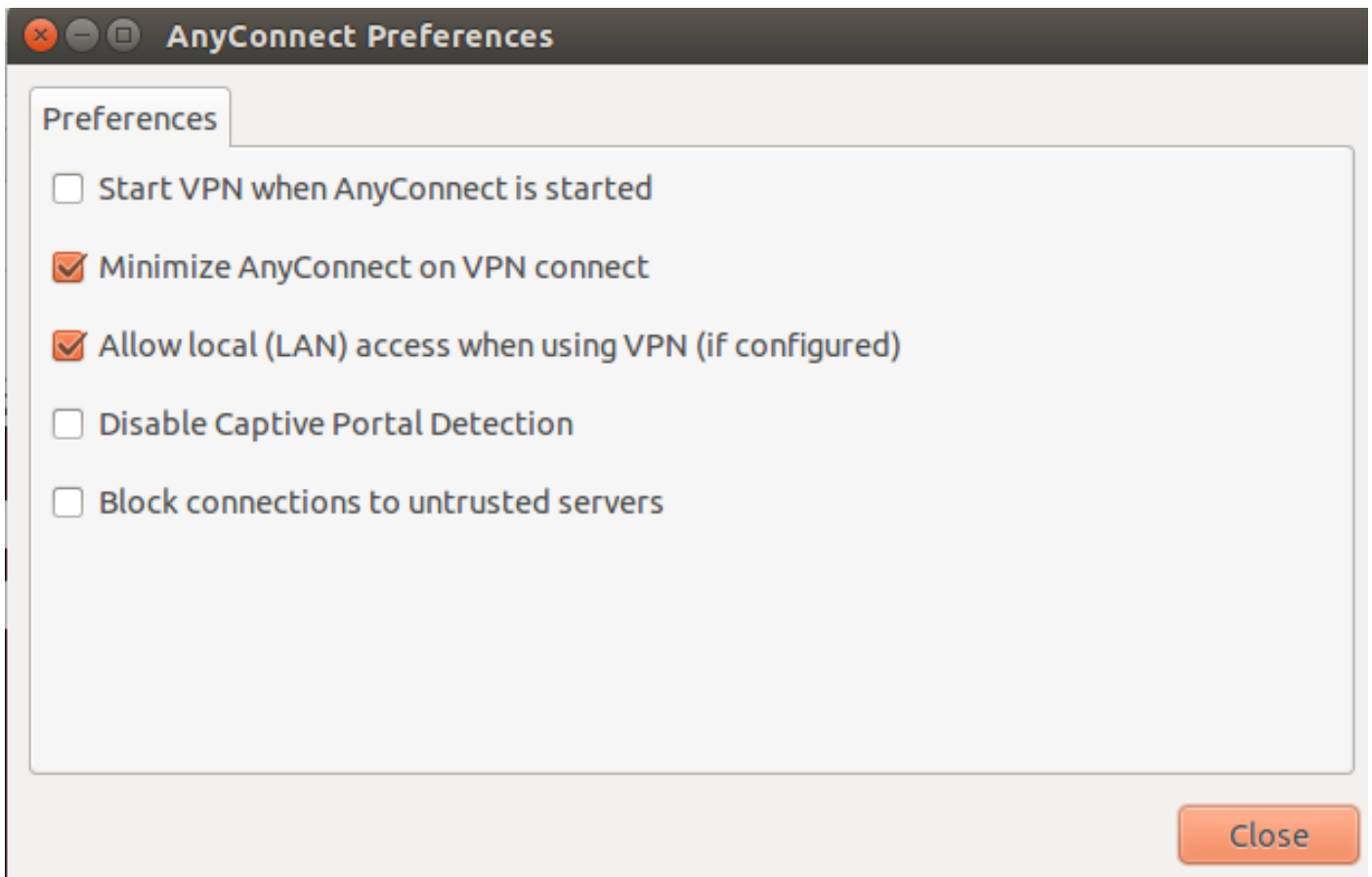
Per consentire l'accesso LAN locale e quindi il tunneling split-exclude, un amministratore di rete può abilitarlo nel profilo oppure gli utenti possono abilitarlo nelle impostazioni delle preferenze (vedere l'immagine nella sezione successiva). Per consentire l'accesso alla LAN locale, un utente seleziona la **Allow Local LAN access** casella di controllo se sul gateway sicuro è abilitato lo split-tunneling e se questo è configurato con il split-tunnel-policy exclude specified criterio. Inoltre, è possibile configurare il profilo client VPN se l'accesso LAN locale è consentito con **<LocalLanAccess UserControllable="true">true</LocalLanAccess>**.

Preferenze utente

Di seguito sono elencate le selezioni da effettuare nella scheda Preferenze di Cisco AnyConnect Secure Mobility Client per consentire l'accesso alla LAN locale.



Su Linux



Esempio di profilo XML

Di seguito è riportato un esempio di come configurare VPN Client Profile con XML.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">Automatic
```

```
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

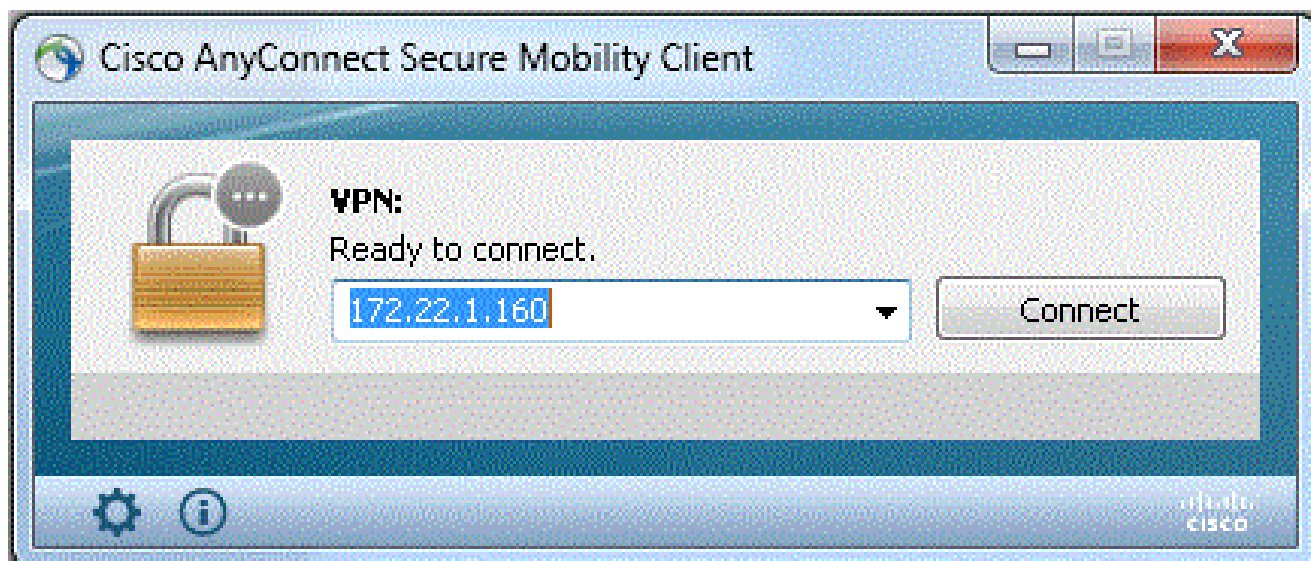
Verifica

Per verificare la configurazione, completare la procedura descritta nelle sezioni seguenti:

- [Visualizzare il DART](#)
- [Test dell'accesso LAN locale con ping](#)

Per verificare la configurazione, connettere Cisco AnyConnect Secure Mobility Client all'appliance ASA.

- Scegliere la voce di connessione dall'elenco dei server e fare clic su **Connect**.



- Scegliere questa opzione **Advanced Window for All Components > Statistics...** per visualizzare la modalità tunnel.

Statistics

VPN

Virtual Private Network (VPN)


Statistics | Route Details | Firewall | Message History

Connection Information		Address Information	
State:	Connected	Client (IPv4):	192.168.11.1
Tunnel Mode (IPv4):	Split Exclude	Client (IPv6):	Not Available
Tunnel Mode (IPv6):	Drop All Traffic	Server:	64.102.156.87
Duration:	00:01:11	Transport Information	
Bytes		Protocol:	DTLS
Sent:	49749	Cipher:	RSA_3DES_168_SHA1
Received:	9298	Compression:	LZS
Frames		Proxy Address:	No Proxy
Sent:	710	Feature Configuration	
Received:	3	FIPS Mode:	Disabled
Control Frames		Trusted Network Detection:	Disabled
Sent:	7	Always On:	Disabled
Received:	5	Secure Mobility Solution	
Client Management		Status:	Unconfirmed
Profile Name:	pro_locallan.xml	Appliance:	Not Available
Administrative Domain:	Undefined		

Reset Export Stats...

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | Route Details



Connection Information		Address Information	
State:	Connected	Client (IPv4):	20.20.20.1
Connection Mode (IPv4):	Split Exclude	Server:	10.48.67.223
Connection Mode (IPv6):	Drop All Traffic	Client (IPv6):	Not Available
Duration:	00:16:22		
Session Disconnect:	None		
Bytes		Transport Information	
Sent:	0	Protocol:	DTLS
Received:	20550	Cipher:	RSA_AES_256_SHA1
		Compression:	None
		Proxy Address:	No Proxy
Frames		Feature Configuration	
Sent:	0	FIPS Mode:	Disabled
Received:	5	Trusted Network Detection:	Disabled
Control Frames			
Sent:	132		
Received:	65		

- Fare clic sulla **Route Details** scheda per visualizzare le route verso cui Cisco AnyConnect Secure Mobility Client ha ancora accesso locale.

Nell'esempio, al client è consentito l'accesso LAN locale ai siti 10.150.52.0/22 e 169.254.0.0/16, mentre tutto il resto del traffico viene crittografato e inviato attraverso il tunnel.

Statistics

VPN

Virtual Private Network (VPN)


Statistics | **Route Details** | Firewall | Message History

Route Details

- ▼ Non-Secured Routes (IPv4)
 - 10.150.52.0/22
 - 169.254.0.0/16
- ▼ Secured Routes (IPv4)
 - 0.0.0.0/0
- Non-Secured Routes (IPv6)
- Secured Routes (IPv6)

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | **Route Details**



Non-Secured Routes

Destination	Subnet Mask
192.168.171.0	24

Secured Routes

Destination	Subnet Mask
0.0.0.0	0

Cisco AnyConnect Secure Mobility Client

Quando si esaminano i log di AnyConnect dal bundle DART (Diagnostics and Reporting Tool), è possibile stabilire se è impostato o meno il parametro che consente l'accesso alla LAN locale.

Date : 11/25/2011
 Time : 13:01:48
 Type : Information
 Source : acvpndownloader

Description : Current Preference Settings:
 ServiceDisable: false
 CertificateStoreOverride: false
 CertificateStore: All
 ShowPreConnectMessage: false
 AutoConnectOnStart: false
 MinimizeOnConnect: true
 LocalLanAccess: true
 AutoReconnect: true
 AutoReconnectBehavior: DisconnectOnSuspend
 UseStartBeforeLogon: false
 AutoUpdate: true
 RSA SecurID Integration: Automatic
 Windows Logon Enforcement: SingleLocalLogon
 Windows VPN Establishment: LocalUsersOnly
 Proxy Settings: Native
 AllowLocalProxyConnections: true

PPPEExclusion: Disable
PPPEExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true

Test dell'accesso LAN locale con ping

Un modo aggiuntivo per verificare che il client VPN disponga ancora dell'accesso LAN locale durante il tunneling all'headend VPN consiste nell'utilizzare il **ping** comando dalla riga di comando di Microsoft Windows. Di seguito è riportato un esempio in cui la LAN locale del client è 192.168.0.0/24 e un altro host è presente sulla rete con un indirizzo IP di 192.168.0.3.

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

```
malhyari@ubuntu:~$ ping 192.168.171.131
PING 192.168.171.131 (192.168.171.131) 56(84) bytes of data.
64 bytes from 192.168.171.131: icmp_seq=1 ttl=128 time=0.474 ms
64 bytes from 192.168.171.131: icmp_seq=2 ttl=128 time=0.315 ms
64 bytes from 192.168.171.131: icmp_seq=3 ttl=128 time=0.336 ms
64 bytes from 192.168.171.131: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.171.131: icmp_seq=5 ttl=128 time=0.337 ms
64 bytes from 192.168.171.131: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.171.131: icmp_seq=7 ttl=128 time=0.252 ms
```

Risoluzione dei problemi

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

Impossibile stampare o cercare per nome

Quando il client VPN è connesso e configurato per l'accesso LAN locale, non è possibile stampare o sfogliare per nome sulla LAN locale. Per risolvere questa situazione, sono disponibili due opzioni:

- Sfoglia o stampa per indirizzo IP.
 - Per sfogliare, invece della sintassi `\\sharename`, utilizzare la sintassi `\\x.x.x.x`, dove `x.x.x.x` è l'indirizzo IP del computer host.
 - Per stampare, modificare le proprietà della stampante di rete in modo da utilizzare un indirizzo IP anziché un nome. Ad esempio, al posto della sintassi `\\sharename\printername`, utilizzare `\\x.x.x.x\printername`, dove `x.x.x.x` è un indirizzo IP.
- Creare o modificare il file VPN Client LMHOSTS. Un file LMHOSTS in un PC con Microsoft Windows consente di creare mapping statici tra nomi host e indirizzi IP. Ad esempio, un file LMHOSTS può avere il seguente aspetto:

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```

In Microsoft Windows XP Professional Edition, il file LMHOSTS si trova in `%SystemRoot%\System32\Drivers\Etc`. Per ulteriori informazioni, consultare la documentazione di Microsoft.

Informazioni correlate

- [CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17](#)
- [Cisco ASA serie 5500-X Firewall](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).