ASA/PIX: Esempio di indirizzamento IP statico per client VPN IPSec con CLI e ASDM

Sommario

Introduzione

Questo documento descrive come configurare Cisco serie 5500 Adaptive Security Appliance (ASA) per fornire l'indirizzo IP statico al client VPN con Adaptive Security Device Manager (ASDM) o CLI. ASDM offre funzionalità di monitoraggio e gestione della sicurezza di altissimo livello attraverso un'interfaccia di gestione intuitiva e basata su Web. Una volta completata la configurazione di Cisco ASA, è possibile verificarla con il client VPN Cisco.

Per configurare la connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x, fare riferimento agli esempi di configurazione dell'autenticazione PIX/ASA 7.x e Cisco VPN Client 4.x con Windows 2003 RADIUS (con Active Directory). L'utente client VPN remoto esegue l'autenticazione in Active Directory con un server RADIUS Microsoft Windows 2003 Internet Authentication Service (IAS).

Per configurare una connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x con un Cisco Secure Access Control Server (ACS versione 3.2) per l'autenticazione estesa (Xauth), fare riferimento agli esempi di configurazione di PIX/ASA 7.x e Cisco VPN Client 4.x per l'autenticazione ACS sicura (Cisco).

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM o CLI di apportare modifiche alla configurazione.

Nota: per ulteriori informazioni, fare riferimento al documento sull'autorizzazione dell'accesso HTTPS per ASDM o PIX/ASA 7.x: Esempio di configurazione dell'interfaccia interna ed esterna per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH).

Componenti usati

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

- Software Cisco Adaptive Security Appliance versione 7.x e successive
- Adaptive Security Device Manager versione 5.x e successive
- Cisco VPN Client versione 4.x e successive

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX Security Appliance versione 7.x e successive.

Convenzioni

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

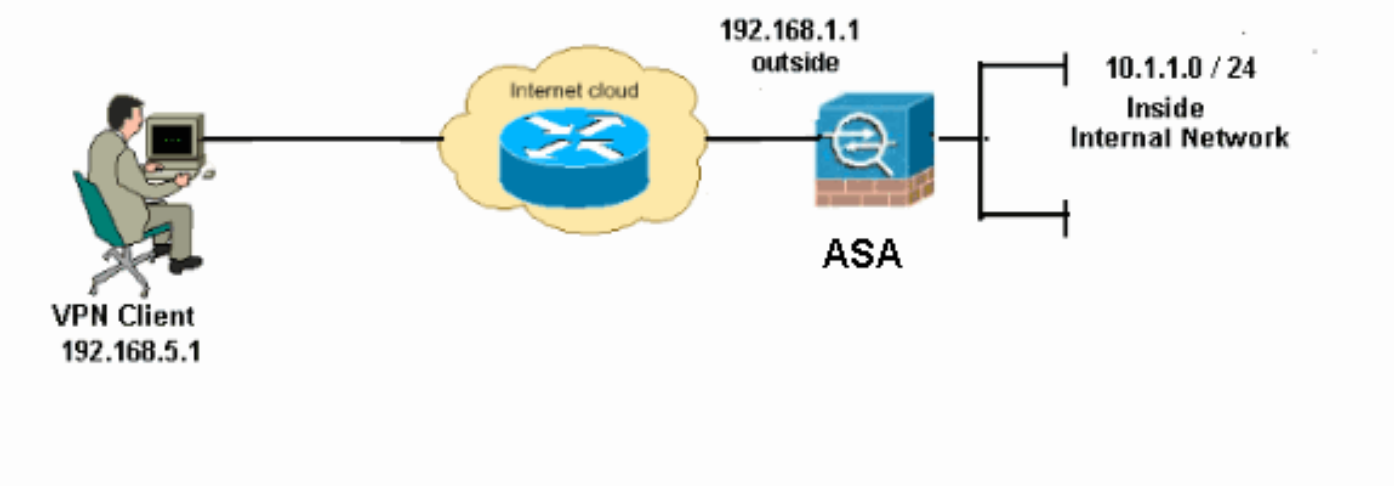
Configurazione

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 questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



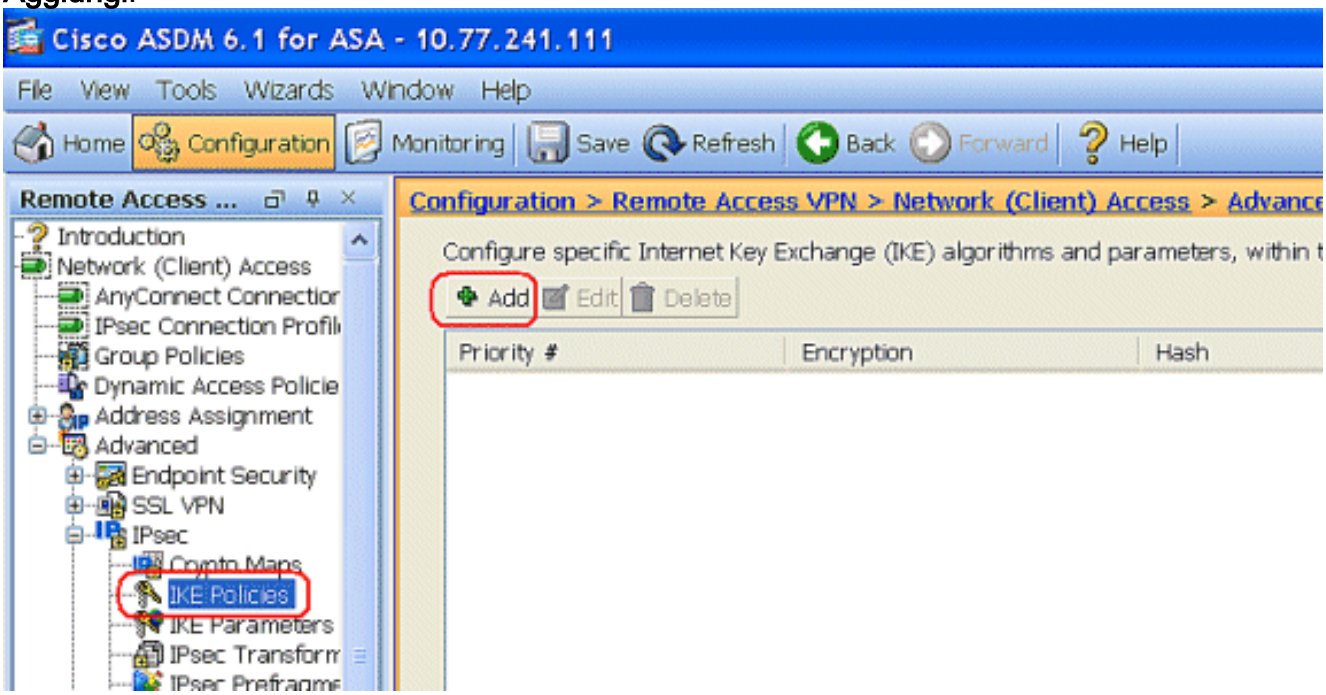
Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurare la VPN di accesso remoto (IPSec)

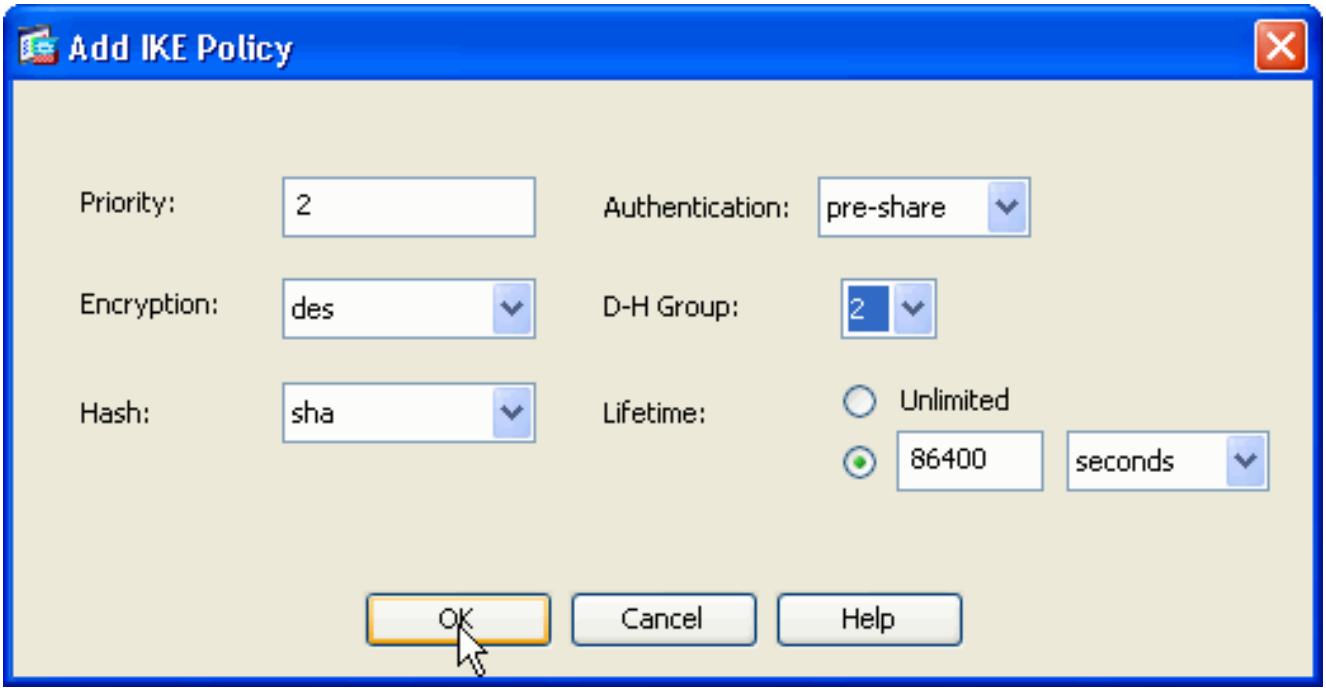
Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

1. Per creare un criterio ISAKMP, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Criteri IKE > Aggiungi**.

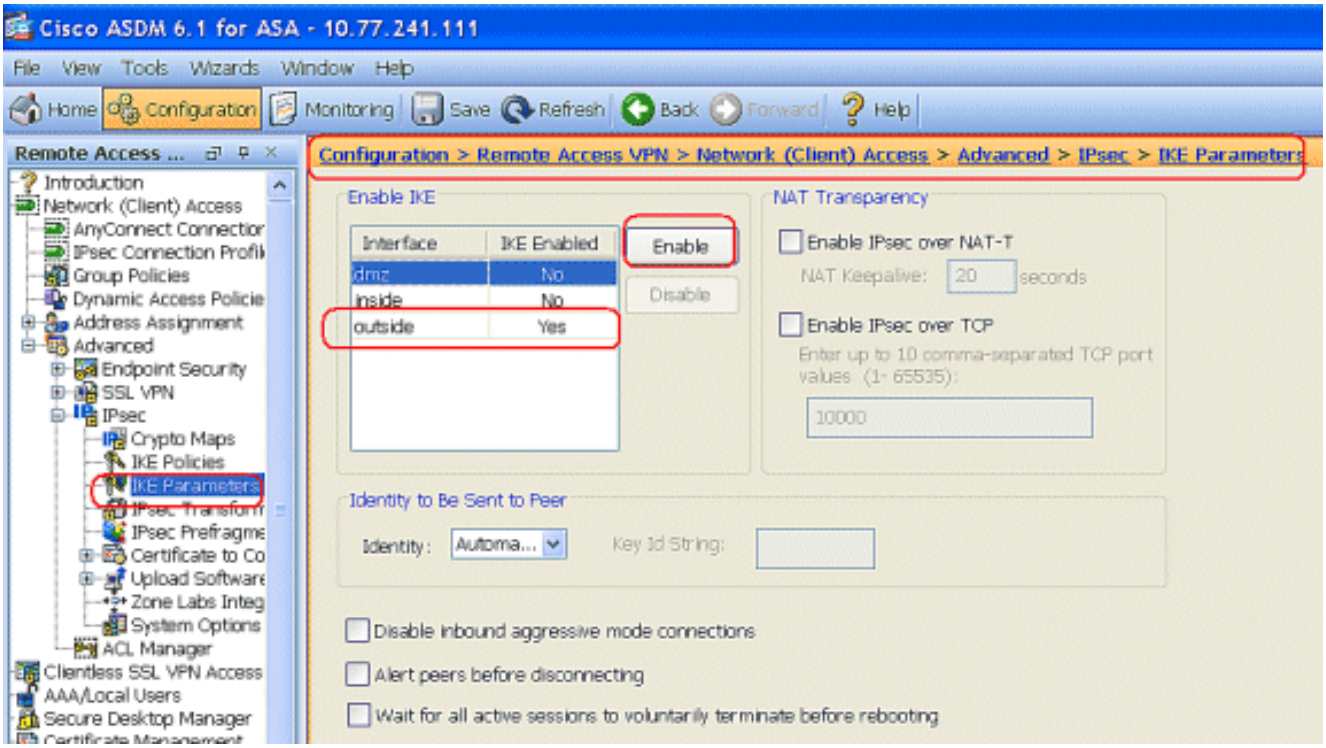


2. Fornire i dettagli del criterio ISAKMP.

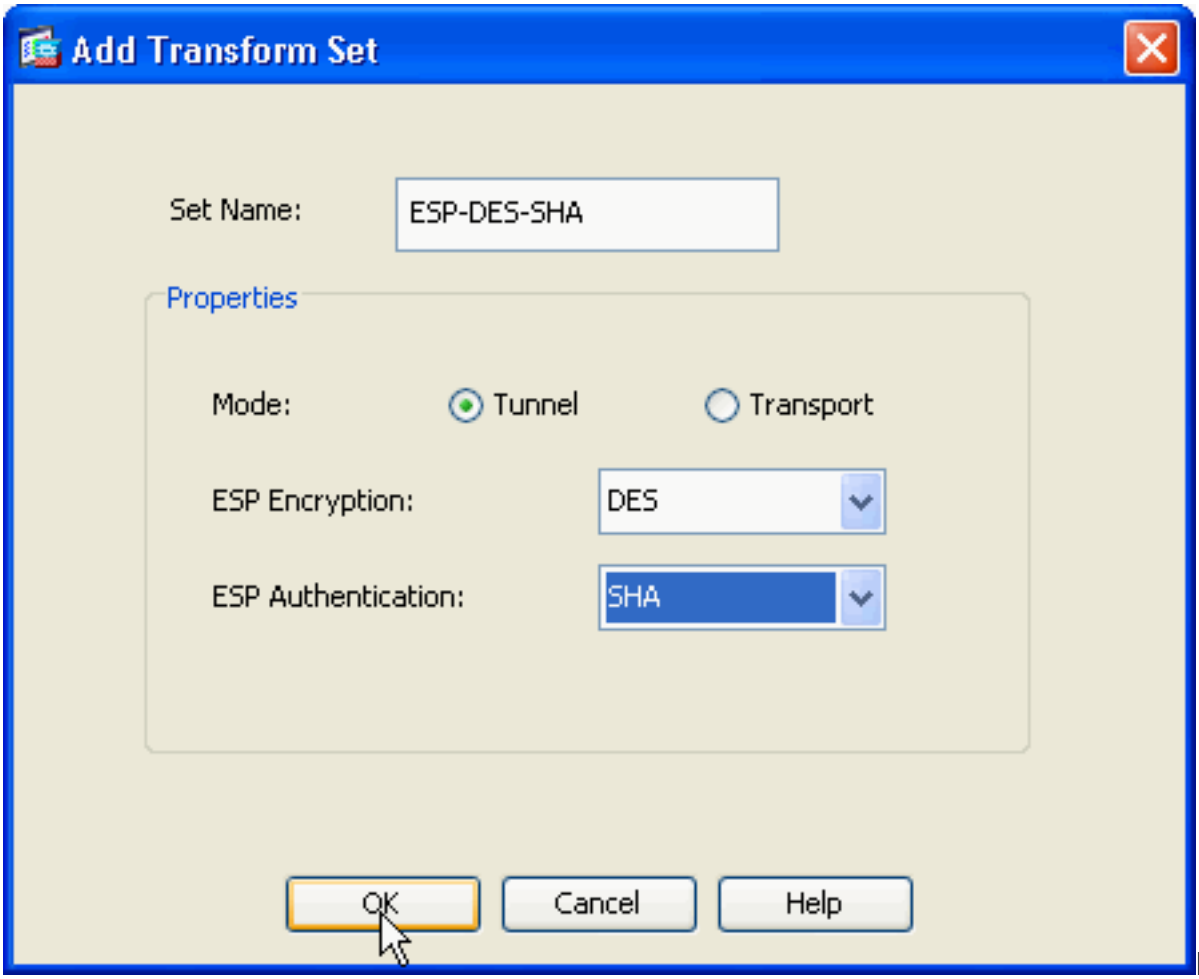


Fare clic su **OK** e su **Applica**.

3. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Parametri IKE** per abilitare IKE sull'interfaccia esterna.

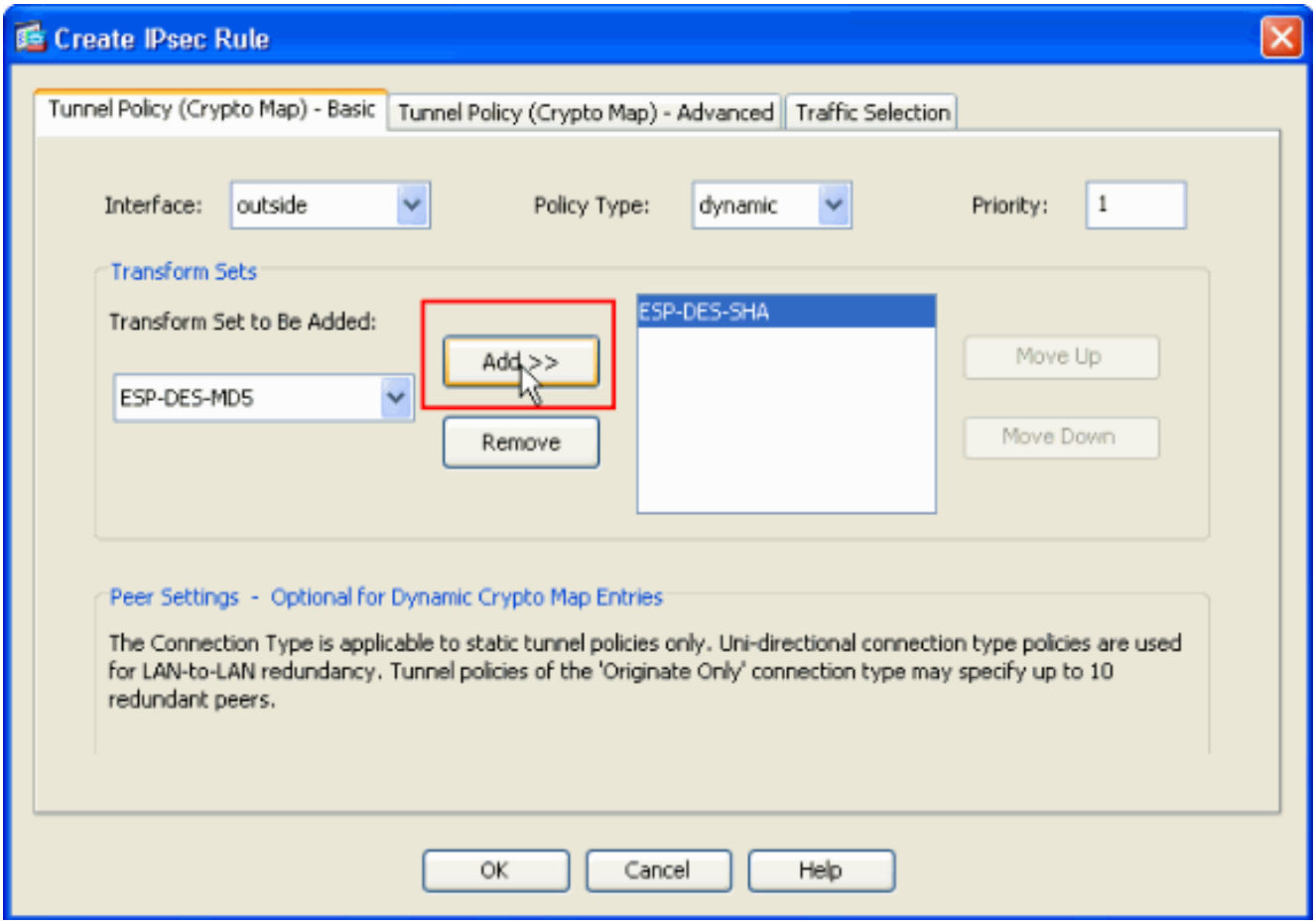


4. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Set trasformazioni IPSec > Aggiungi** per creare il set di trasformazioni **ESP-DES-SHA**, come mostrato.



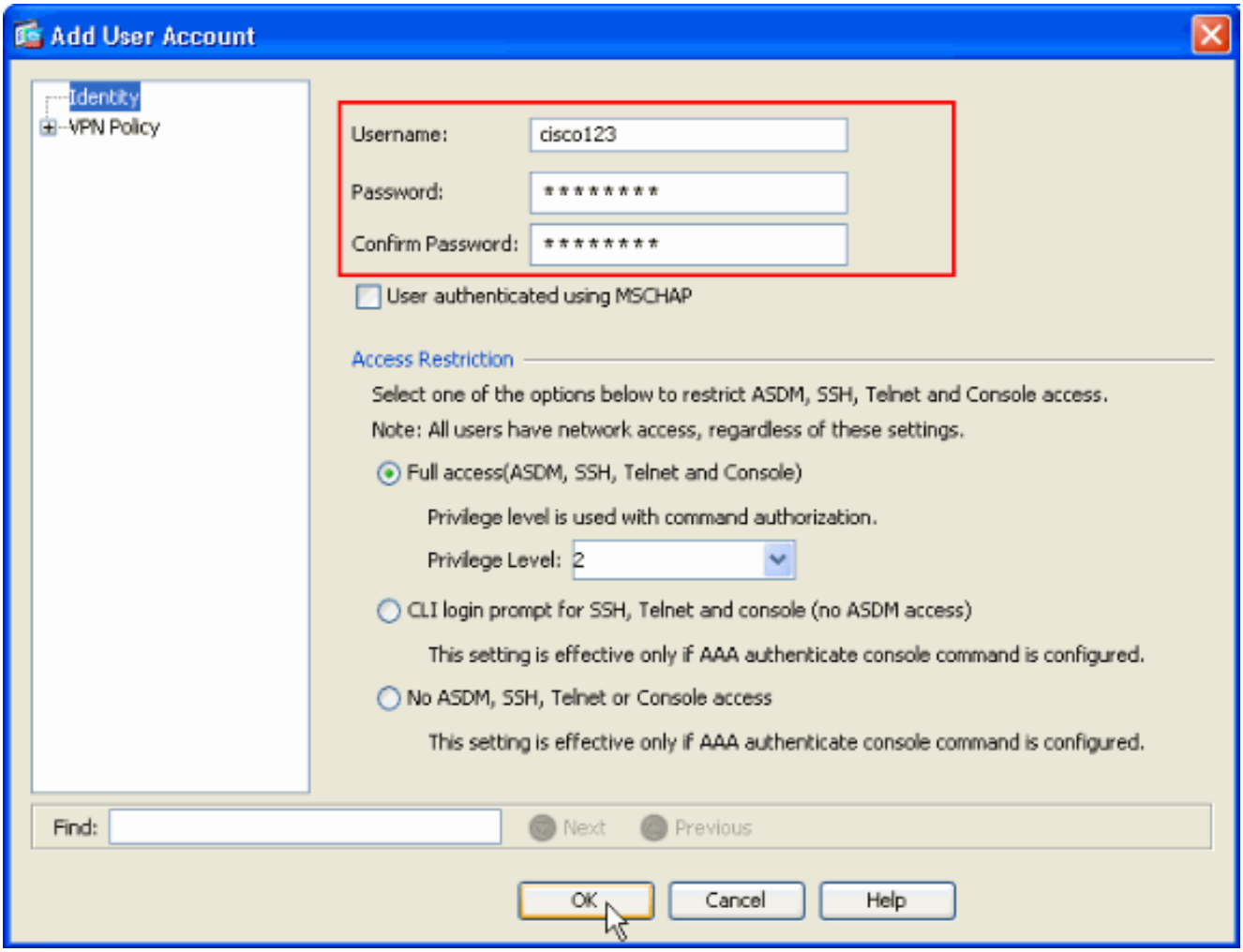
Fare clic su **OK** e su **Applica**.

5. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Mappe crittografiche > Aggiungi** per creare una mappa crittografica con criterio dinamico di priorità 1, come mostrato.

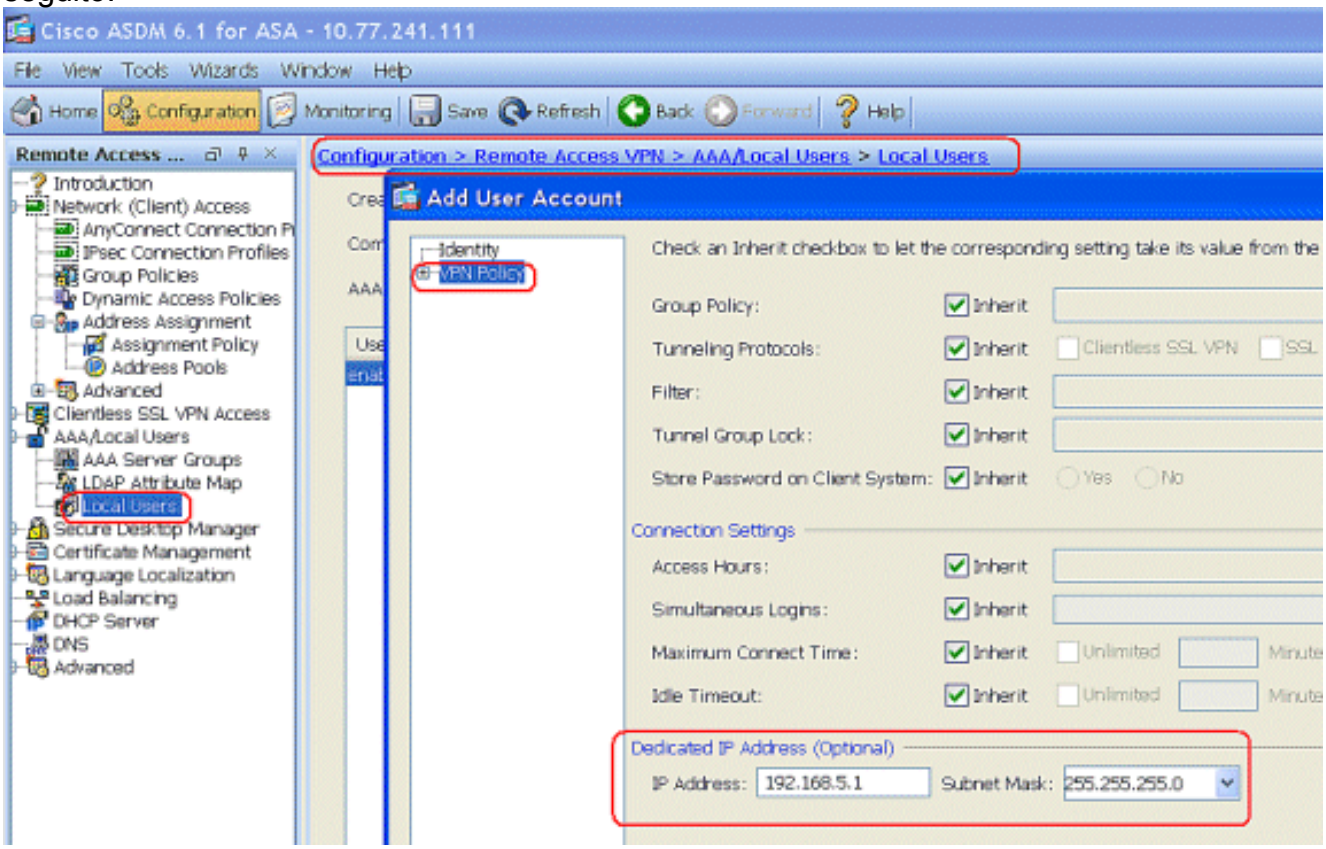


Fare clic su **OK** e su **Applica**.

6. Scegliere **Configurazione > VPN ad accesso remoto > Configurazione AAA > Utenti locali > Aggiungi** per creare l'account utente (ad esempio, nome utente - cisco123 e password - cisco123) per l'accesso ai client
VPN.

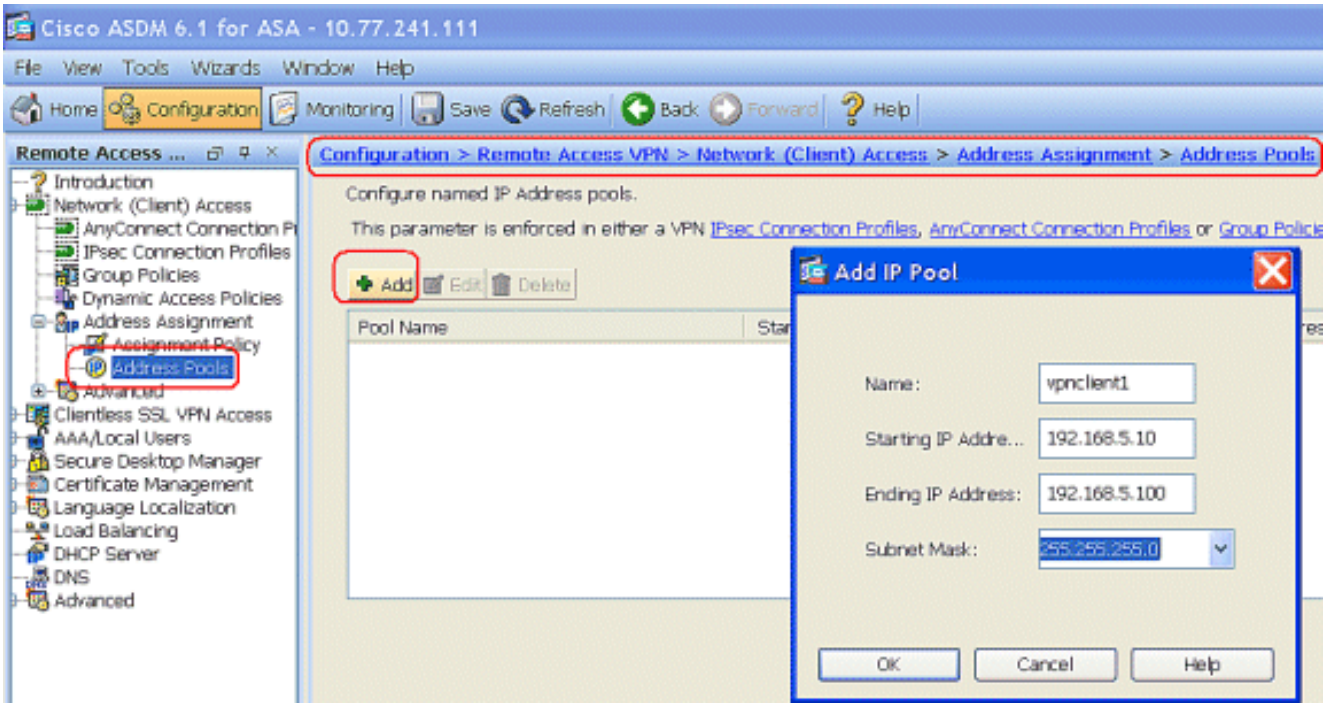


7. Andare a **VPN Policy** (Policy VPN) e aggiungere l'**indirizzo IP statico/dedicato** per l'utente "cisco123", come indicato di seguito.

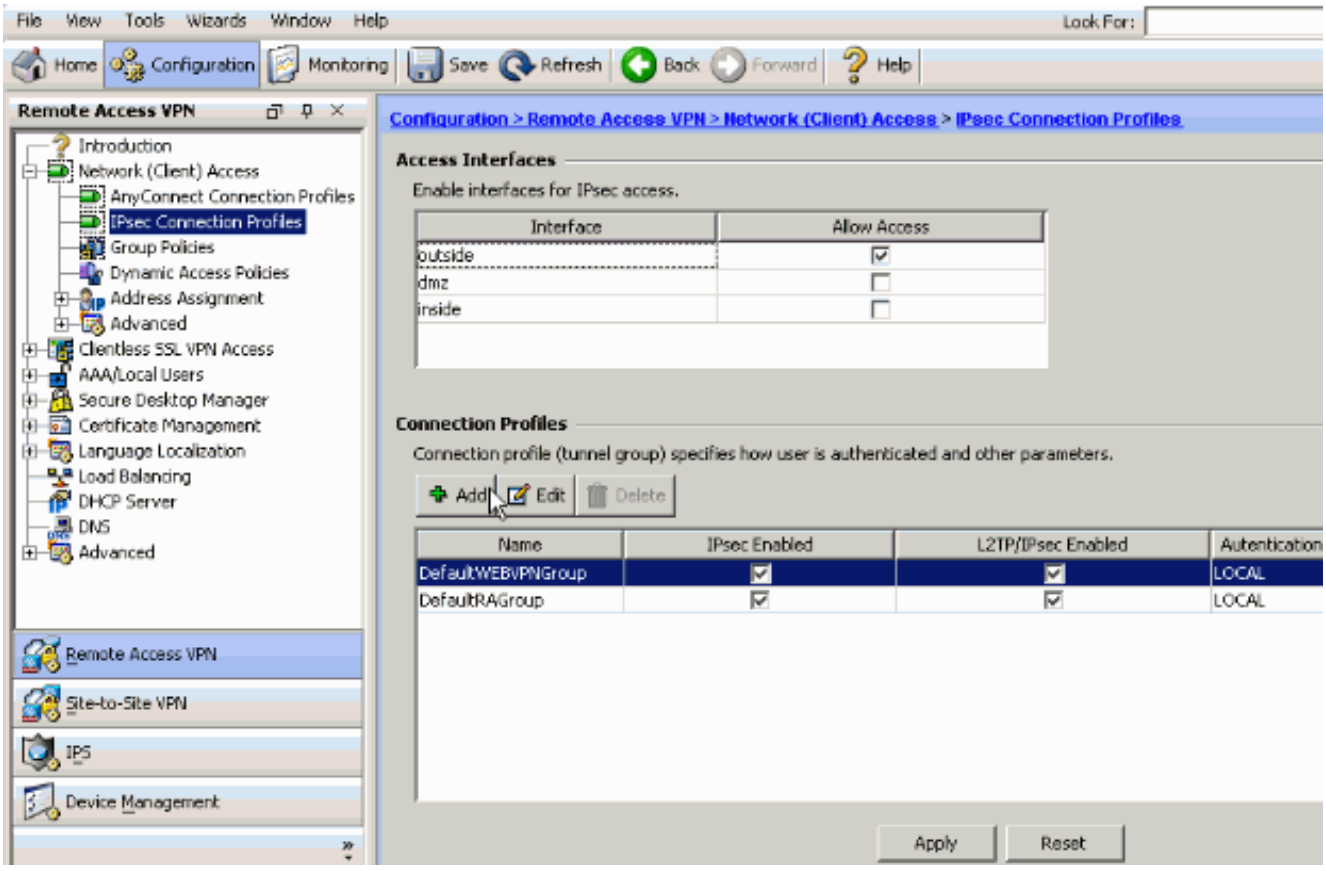


8. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) >**

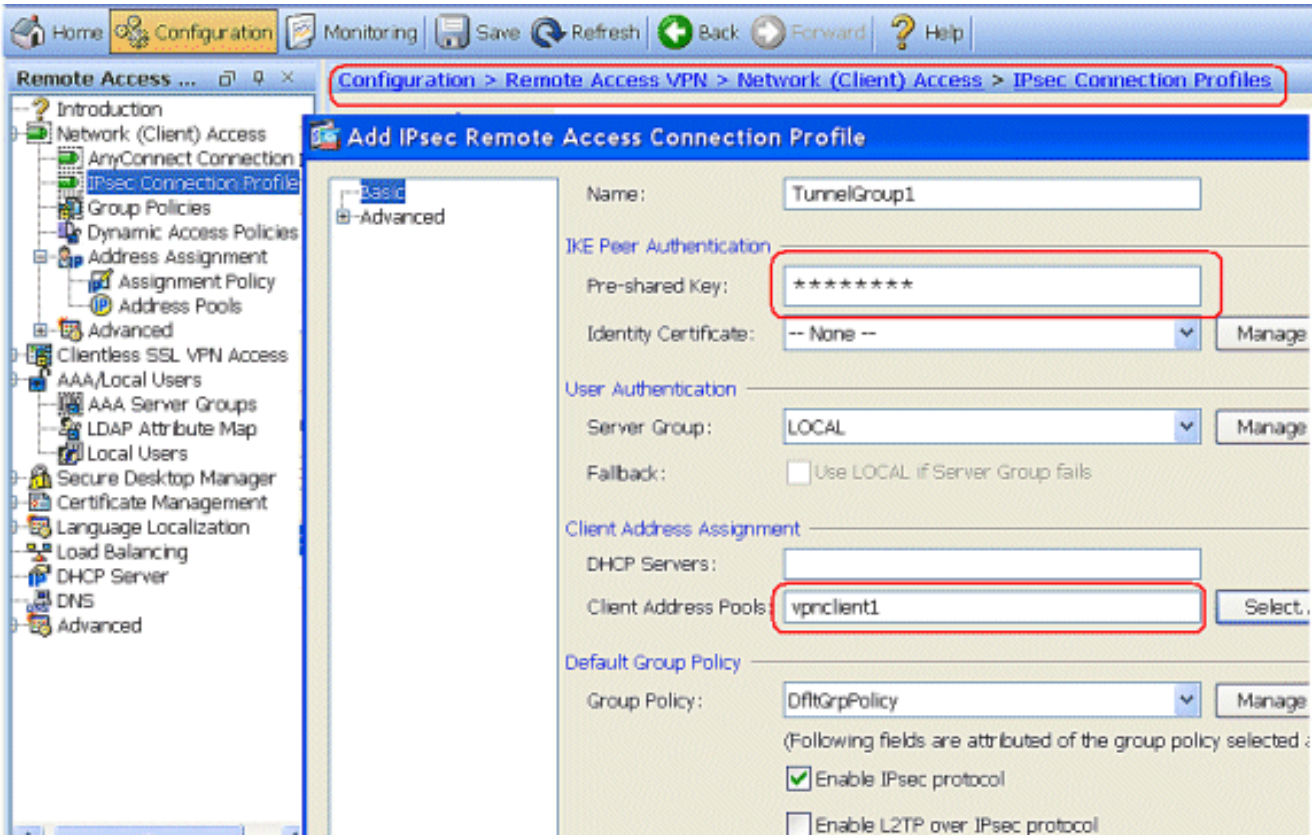
Assegnazione indirizzi > Pool di indirizzi e fare clic su **Aggiungi** per aggiungere il client VPN per gli utenti client
VPN.



9. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione IPSec > Aggiungi** per aggiungere un gruppo di tunnel (ad esempio, TunnelGroup1 e la chiave già condivisa cisco123), come
mostrato.

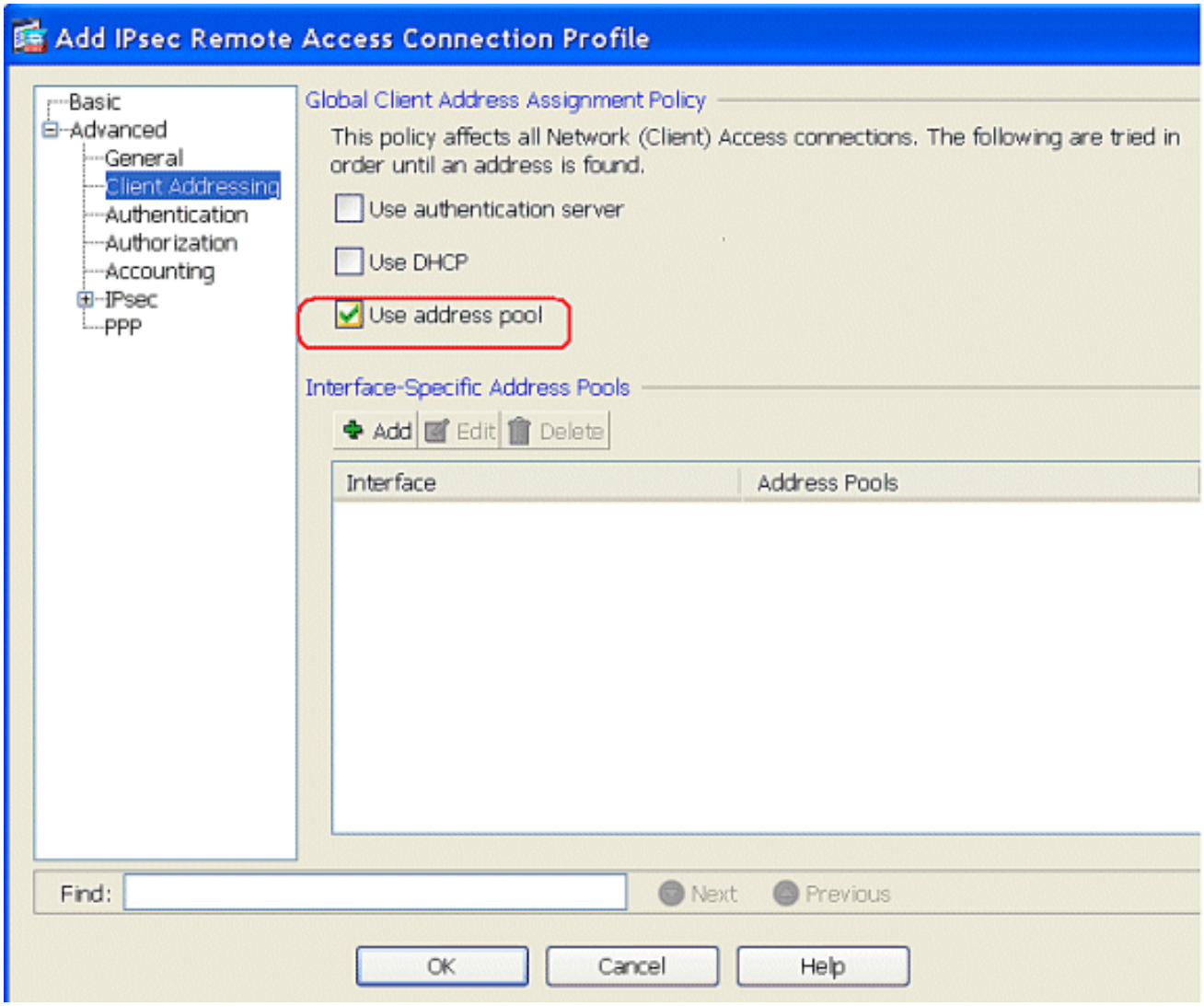


Nella scheda **Base**, scegliere il gruppo di server come **LOCALE** per il campo Autenticazione utente.Selezionare **vpnclient1** come pool di indirizzi client per gli utenti VPN
Client.



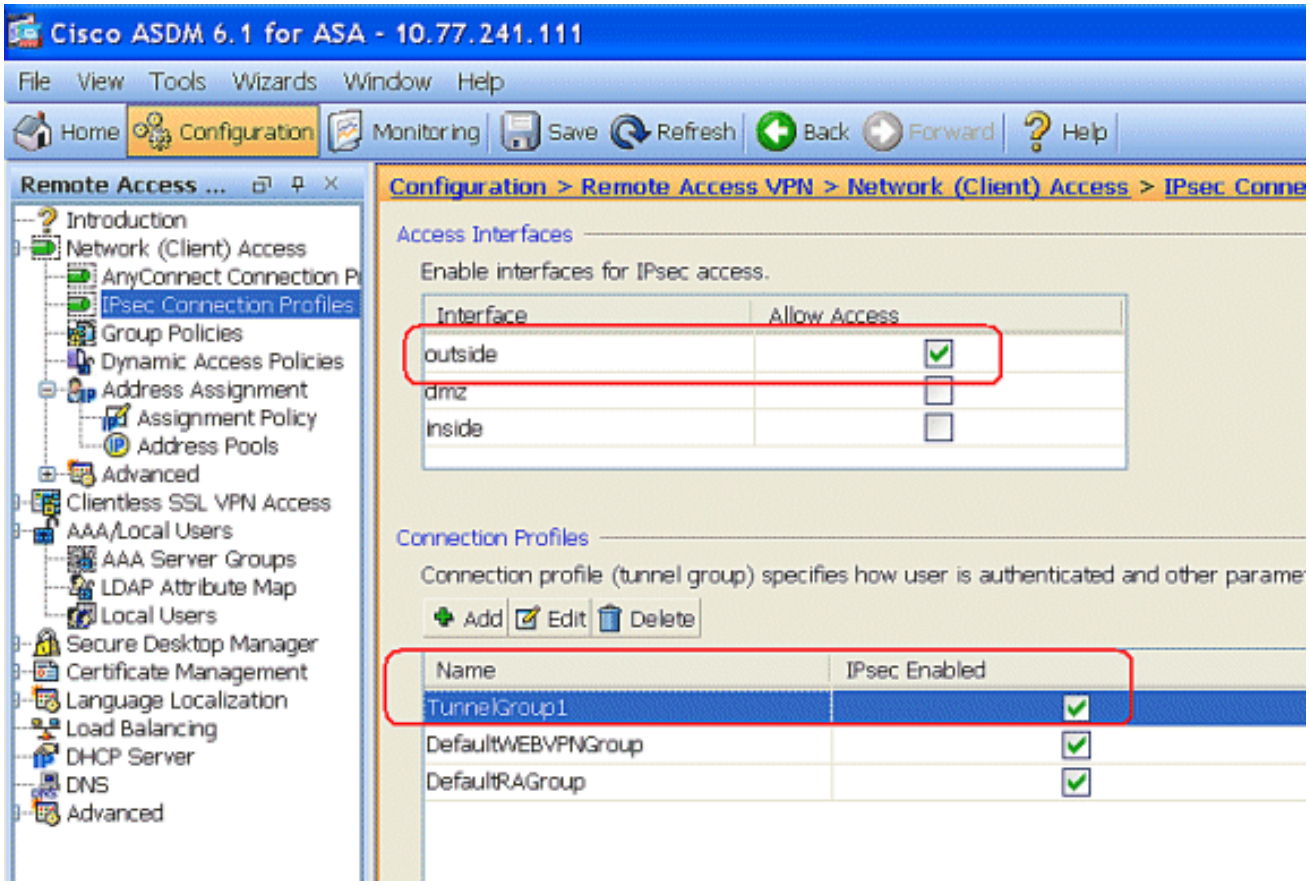
Fare clic su **OK**.

10. Scegliere **Avanzate > Indirizzamento client** e selezionare la casella di controllo **Usa pool di indirizzi** per assegnare l'indirizzo IP ai client VPN.**Nota:** deselezionare le caselle di controllo **Usa server di autenticazione** e **Usa DHCP**.



Fare clic su **OK**.

11. Attivare l'interfaccia **esterna** per l'accesso IPSec. Fare clic su **Apply** (Applica) per continuare.



Configurazione di ASA/PIX con CLI

Completare questa procedura per configurare il server DHCP in modo che fornisca indirizzi IP ai client VPN dalla riga di comando. Per ulteriori informazioni su ciascun comando usato, consultare il documento sulla configurazione delle VPN di accesso remoto o sulla guida di riferimento dei comandi di Cisco ASA serie 5500 Adaptive Security Appliance.

Esecuzione della configurazione sul dispositivo ASA

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0

no failover
icmp unreachable rate-limit 1 burst-size 1
```

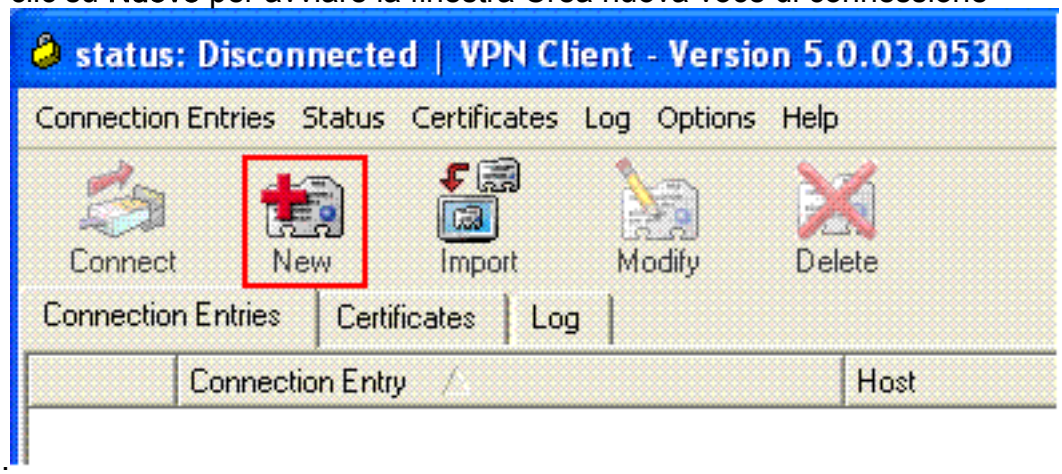
```
!--- Specify the location of the ASDM image for ASA to
fetch the image for ASDM access. asdm image disk0:/asdm-
613.bin no asdm history enable arp timeout 14400 global
(outside) 1 192.168.1.5 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 192.168.1.2 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute dynamic-access-policy-
record DfltAccessPolicy http server enable http 0.0.0.0
0.0.0.0 inside no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-DES-SHA crypto
map outside_map 1 ipsec-isakmp dynamic outside_dyn_map
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses ISAKMP policy 2. !---
The configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption des hash sha group 2 lifetime 86400 no crypto
isakmp nat-traversal !--- Specifies that the IP address
to the vpn clients are assigned by the local and not by
AAA or dhcp. The CLI vpn-addr-assign local for VPN
address assignment through ASA is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign dhcp

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
```

```
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode

username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
  vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

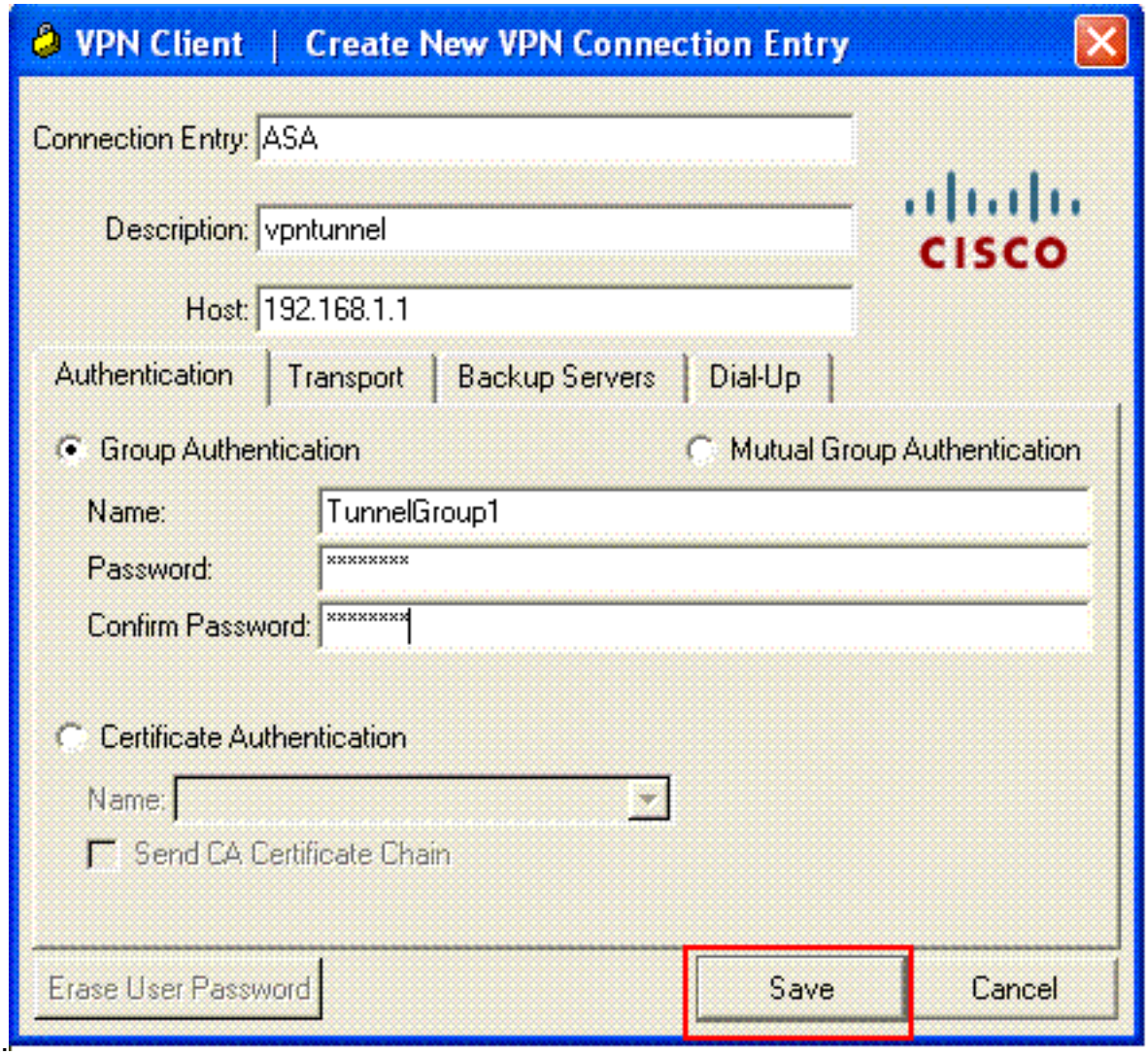
Configurazione client VPN Cisco

Provare a connettersi all'appliance Cisco ASA con il client VPN Cisco per verificare che l'appliance ASA sia configurata correttamente.

1. Scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client**.
2. Fare clic su **Nuovo** per avviare la finestra Crea nuova voce di connessione VPN.

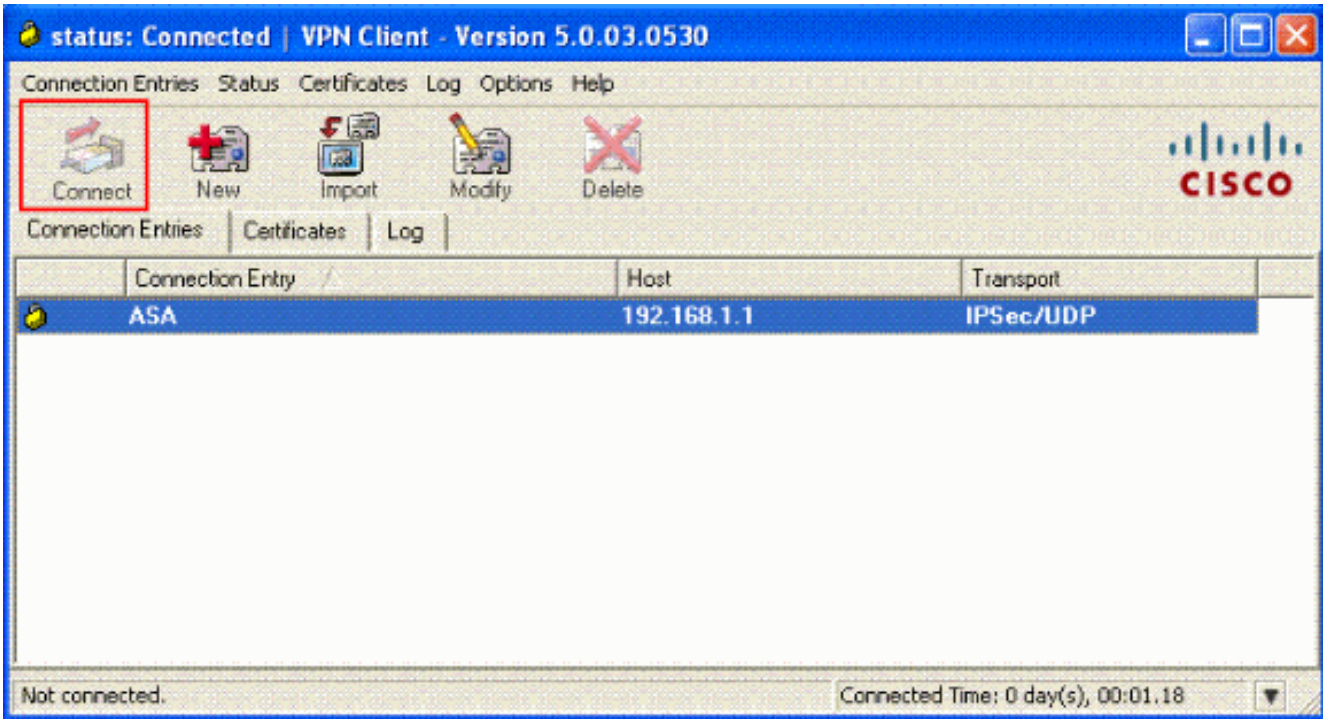


3. Specificare i dettagli della nuova connessione.Immettere il nome della voce di connessione insieme a una descrizione. Immettere l'**indirizzo IP esterno dell'appliance ASA** nella casella Host. Quindi, immettere il nome del gruppo di tunnel VPN (TunnelGroup1) e la password (Chiave già condivisa - cisco123) come configurato nell'ASA. Fare clic su

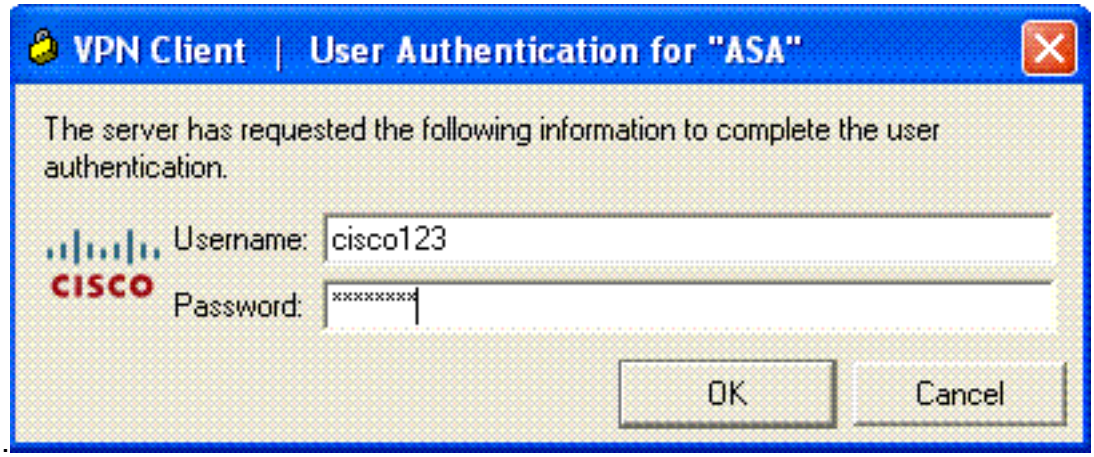


Salva.

4. Fare clic sulla connessione che si desidera utilizzare e fare clic su **Connetti** nella finestra principale del client
VPN.

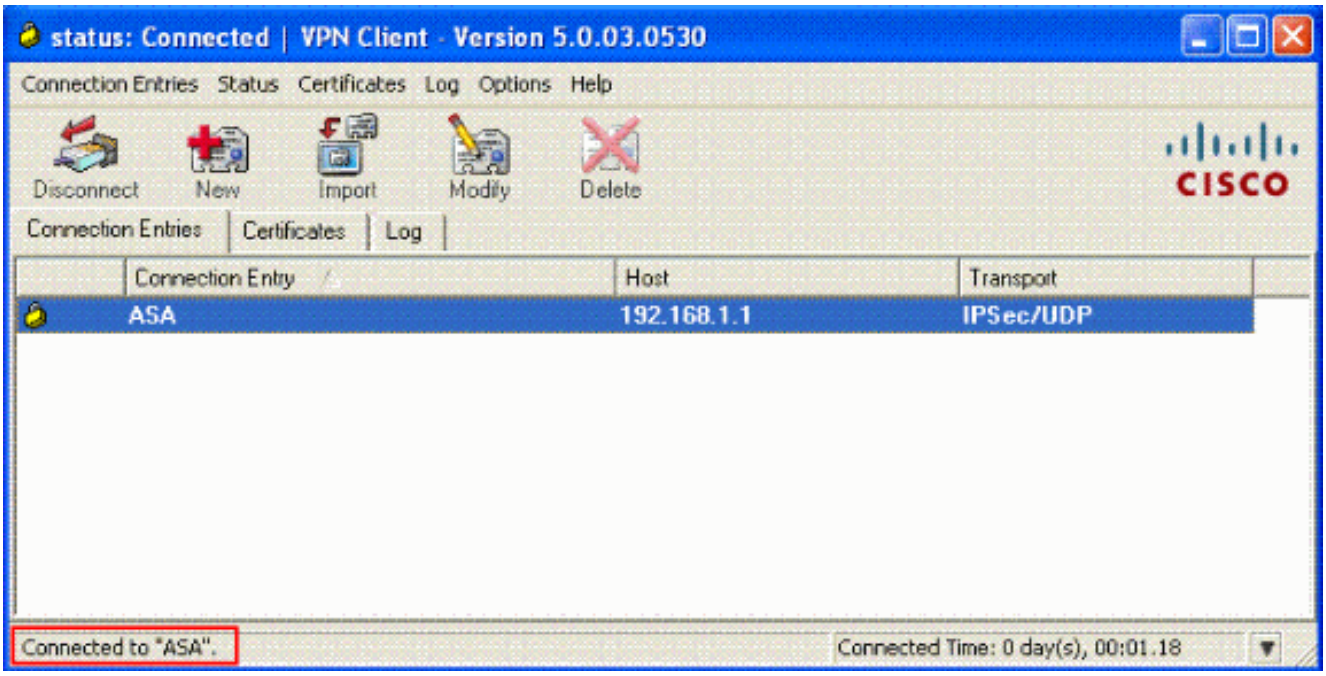


5. Quando richiesto, immettere il **nome utente: cisco123** e **password: cisco123** è stato configurato nell'ASA per Xauth e fare clic su **OK** per connettersi alla rete

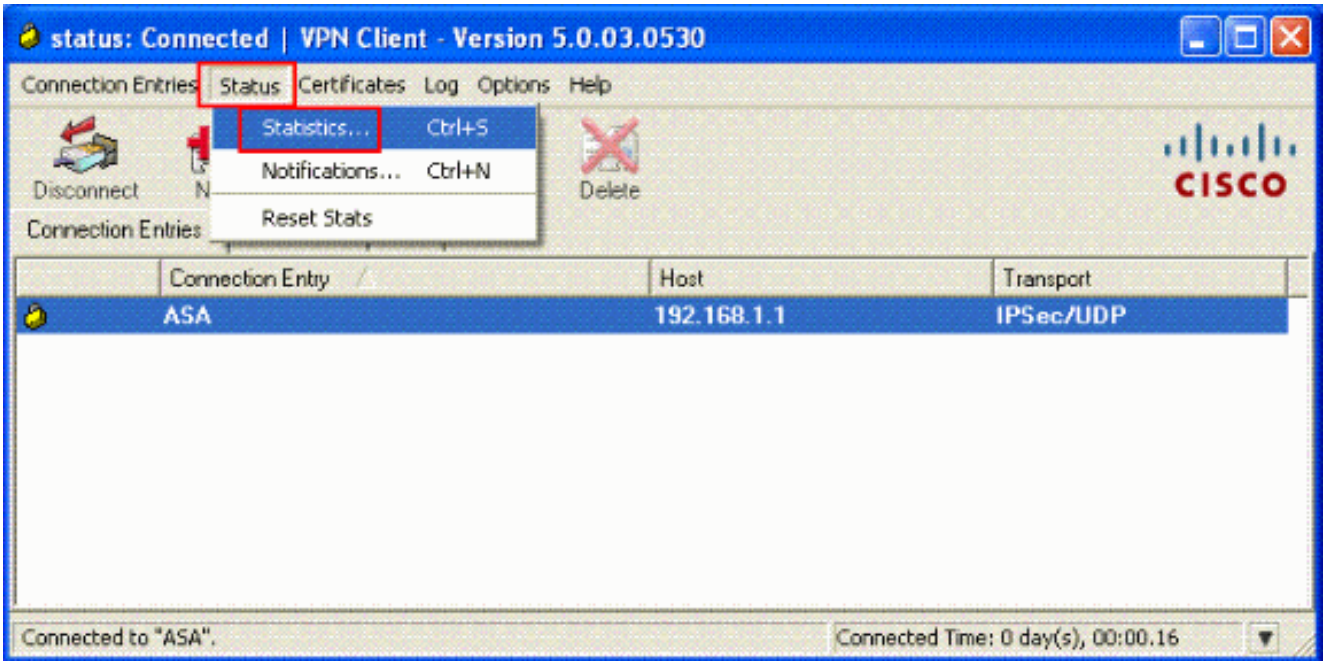


remota.

6. Il client VPN è connesso all'ASA sulla postazione centrale.



7. Una volta stabilita la connessione, scegliere **Statistiche** dal menu Stato per verificare i dettagli del tunnel.



Verifica

Comandi show

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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 isakmp sa**: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Viene visualizzato anche l'output di esempio del comando debug.

Nota: per ulteriori informazioni sulla risoluzione dei problemi relativi alle VPN IPSec di accesso remoto, vedere la sezione relativa alle soluzioni per la risoluzione dei problemi delle VPN IPSec di accesso remoto e L2L più comuni.

Cancella associazioni di protezione

Quando si esegue la risoluzione dei problemi, assicurarsi di cancellare le associazioni di protezione esistenti dopo aver apportato una modifica. In modalità privilegiata di PIX, utilizzare i seguenti comandi:

- **clear [crypto] ipsec sa**: elimina le associazioni di protezione IPSec attive. La parola chiave crypto è facoltativa.
- **clear [crypto] isakmp sa**: elimina le SA IKE attive. La parola chiave crypto è facoltativa.

Comandi per la risoluzione dei problemi

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 ipsec 7**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp 7**: visualizza le negoziazioni ISAKMP della fase 1.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance - Pagina di supporto
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco PIX serie 500 Security Appliance - Pagina di supporto

- Cisco PIX serie 500 Security Appliance - Guida di riferimento ai comandi
- Cisco Adaptive Security Device Manager
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE
- Pagina di supporto per Cisco VPN Client
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems