ASA/PIX 8.x: Esempio di autorizzazione Radius (ACS 4.x) per l'accesso VPN con ACL scaricabile con CLI e ASDM

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Prodotti correlati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurare la VPN di accesso remoto (IPSec)](#)
[Configurazione di ASA/PIX con CLI](#)
[Configurazione client VPN Cisco](#)
[Configurazione di ACS per ACL scaricabili per un singolo utente](#)
[Configurazione di ACS per ACL scaricabili per gruppo](#)
[Configurare le impostazioni RADIUS IETF per un gruppo di utenti](#)
[Verifica](#)
[Mostra comandi di crittografia](#)
[ACL scaricabile per utente/gruppo](#)
[ACL Filter-Id](#)
[Risoluzione dei problemi](#)
[Cancella associazioni di protezione](#)
[Comandi per la risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'appliance di sicurezza per autenticare gli utenti per l'accesso alla rete. Poiché è possibile attivare in modo implicito le autorizzazioni RADIUS, in questa sezione non vengono fornite informazioni sulla configurazione dell'autorizzazione RADIUS sull'accessorio di sicurezza. Vengono fornite informazioni sul modo in cui l'accessorio di protezione gestisce le informazioni dell'elenco degli accessi ricevute dai server RADIUS.

Èpossibile configurare un server RADIUS in modo che al momento dell'autenticazione venga scaricato un elenco degli accessi all'accessorio di protezione o un nome di elenco degli accessi.

L'utente è autorizzato a eseguire solo le operazioni consentite nell'elenco degli accessi specifico.

Gli elenchi degli accessi scaricabili sono il metodo più scalabile quando si usa Cisco Secure ACS per fornire gli elenchi degli accessi appropriati per ciascun utente. Per ulteriori informazioni sulle funzionalità delle liste di accesso scaricabili e su Cisco Secure ACS, consultare il documento sulla configurazione di un server RADIUS per inviare liste di controllo degli accessi scaricabili e ACL IP scaricabili.

Fare riferimento alla versione ASA 8.3 e successive: Esempio di autorizzazione Radius (ACS 5.x) per accesso VPN con ACL scaricabile con CLI e ASDM per la stessa configurazione sull'appliance Cisco ASA con versioni 8.3 e successive.

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
- Cisco Adaptive Security Device Manager versione 5.x e successive
- Cisco VPN Client versione 4.x e successive
- Cisco Secure Access Control Server 4.x

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.

Premesse

Èpossibile usare gli ACL IP scaricabili per creare set di definizioni di ACL che possono essere applicate a molti utenti o gruppi di utenti. Questi set di definizioni ACL sono chiamati contenuti ACL. Inoltre, quando si incorporano i NAF, è possibile controllare il contenuto degli ACL inviato al client AAA da cui l'utente richiede l'accesso. Ovvero, un ACL IP scaricabile comprende una o più definizioni di contenuto ACL, ognuna delle quali è associata a un NAF o (per impostazione predefinita) associata a tutti i client AAA. Il NAF controlla l'applicabilità dei contenuti degli ACL specificati in base all'indirizzo IP del client AAA. Per ulteriori informazioni sui NAF e sulla loro modalità di gestione degli ACL IP scaricabili, vedere About Network Access Filters.

Gli ACL IP scaricabili funzionano nel modo seguente:

1. Quando ACS concede a un utente l'accesso alla rete, determina se a tale utente o al gruppo di utenti è assegnato un ACL IP scaricabile.
2. Se ACS individua un ACL IP scaricabile assegnato all'utente o al gruppo di utenti, determina se una voce di contenuto ACL è associata al client AAA che ha inviato la richiesta di autenticazione RADIUS.
3. ACS invia, come parte della sessione utente, un pacchetto RADIUS access-accept, un attributo che specifica l'ACL con nome e la versione dell'ACL con nome.
4. Se il client AAA risponde che la versione corrente dell'ACL non è presente nella cache, ossia l'ACL è nuovo o è stato modificato, ACS invia l'ACL (nuovo o aggiornato) al dispositivo.

Gli ACL IP scaricabili sono un'alternativa alla configurazione degli ACL nell'attributo RADIUS Cisco cisco-av-pair [26/9/1] di ciascun utente o gruppo di utenti. È possibile creare un ACL IP scaricabile una volta sola, assegnargli un nome e quindi assegnare l'ACL IP scaricabile a ciascun utente o gruppo di utenti applicabile se si fa riferimento al nome. Questo metodo è più efficiente di quello che si ottiene configurando l'attributo RADIUS Cisco cisco-av-pair per ciascun utente o gruppo di utenti.

Inoltre, quando si usano i NAF, è possibile applicare contenuti ACL diversi allo stesso utente o gruppo di utenti in relazione al client AAA che usano. Dopo aver configurato il client AAA in modo che usi gli ACL IP scaricabili da ACS, non è necessaria alcuna configurazione aggiuntiva del client AAA. Gli ACL scaricabili sono protetti dal regime di backup o di replica stabilito.

Quando si immettono le definizioni degli ACL nell'interfaccia Web di ACS, non usare parole chiave o nomi; per tutti gli altri aspetti, usare la sintassi dei comandi ACL standard e la semantica del client AAA a cui si intende applicare l'ACL IP scaricabile. Le definizioni ACL immesse in ACS comprendono uno o più comandi ACL. Ogni comando ACL deve essere su una riga separata.

Èpossibile aggiungere uno o più contenuti ACL con nome a un ACL IP scaricabile. Per impostazione predefinita, ogni contenuto ACL si applica a tutti i client AAA, ma, se sono stati definiti NAF, è possibile limitare l'applicabilità di ogni contenuto ACL ai client AAA elencati nel NAF a esso associato. In altre parole, quando si utilizzano i NAF, è possibile rendere ciascun contenuto ACL, all'interno di un singolo ACL IP scaricabile, applicabile a più dispositivi di rete o gruppi di dispositivi di rete diversi in base alla strategia di sicurezza di rete adottata.

Inoltre, è possibile modificare l'ordine dei contenuti dell'ACL in un ACL IP scaricabile. ACS esamina il contenuto degli ACL, a partire dalla parte superiore della tabella, e scarica il primo contenuto ACL trovato con un NAF che include il client AAA utilizzato. Quando si imposta l'ordine, è possibile garantire l'efficienza del sistema posizionando più in alto nell'elenco i contenuti degli ACL applicabili. Se i NAF includono gruppi di client AAA che si sovrappongono, è necessario passare dal più specifico al più generale. Ad esempio, ACS scarica qualsiasi contenuto ACL con l'impostazione NAF All-AAA-Clients e non prende in considerazione gli elementi che si trovano in una posizione inferiore nell'elenco.

Per utilizzare un ACL IP scaricabile su un particolare client AAA, il client AAA deve seguire queste istruzioni:

- Utilizza RADIUS per l'autenticazione
- Supporto di ACL IP scaricabili

Di seguito sono riportati alcuni esempi di dispositivi Cisco che supportano ACL IP scaricabili:

- Dispositivi ASA e PIX
- VPN serie 3000 concentrator
- Dispositivi Cisco con IOS versione 12.3(8)T o successive

Questo è un esempio del formato da usare per immettere gli ACL VPN 3000/ASA/PIX 7.x+ nella casella Definizioni ACL:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

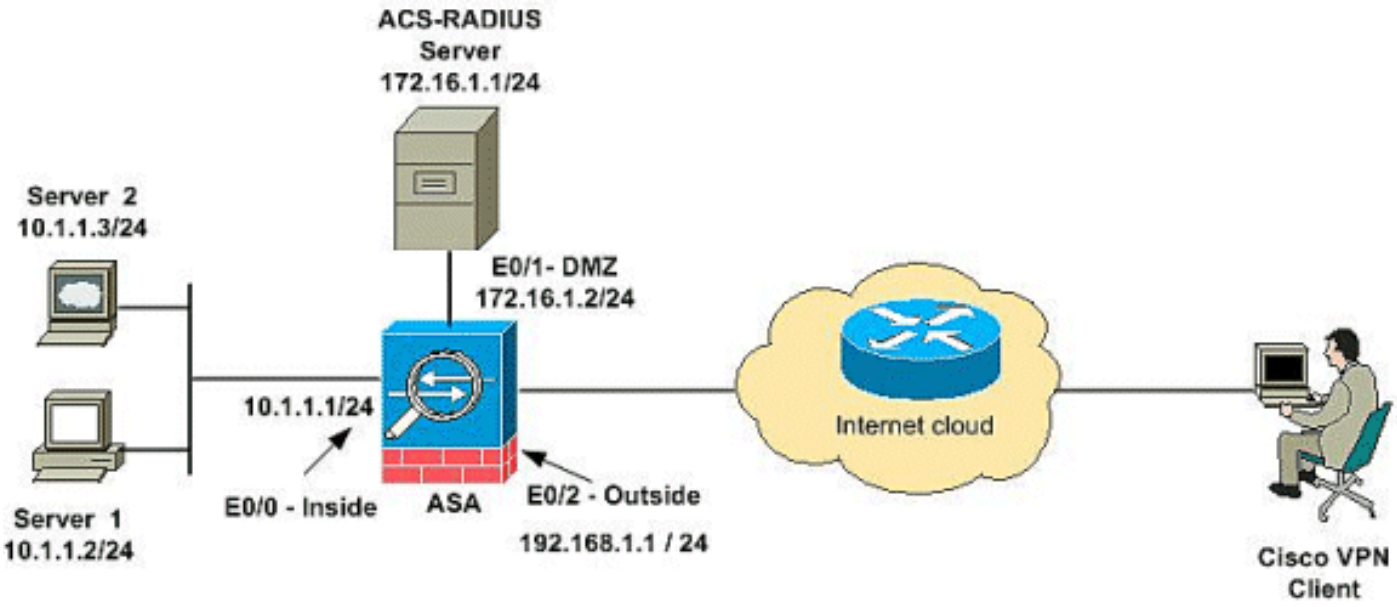
Configurazione

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:



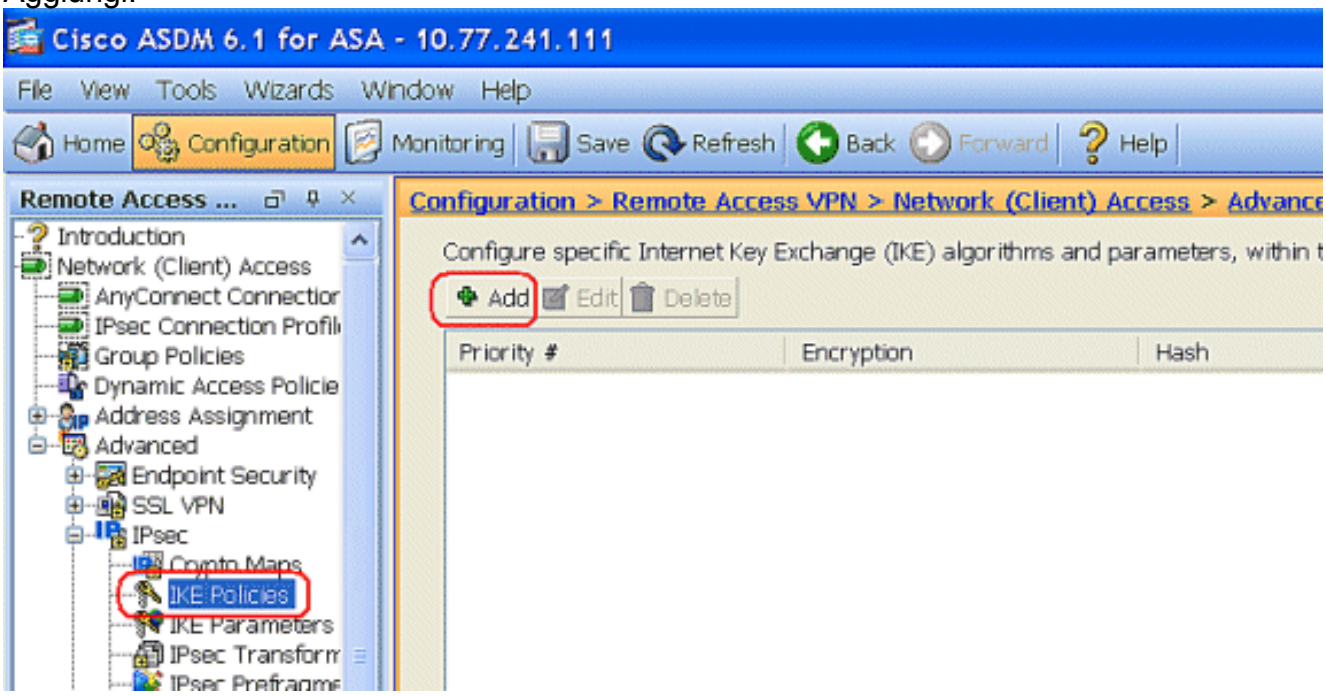
Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurare la VPN di accesso remoto (IPSec)

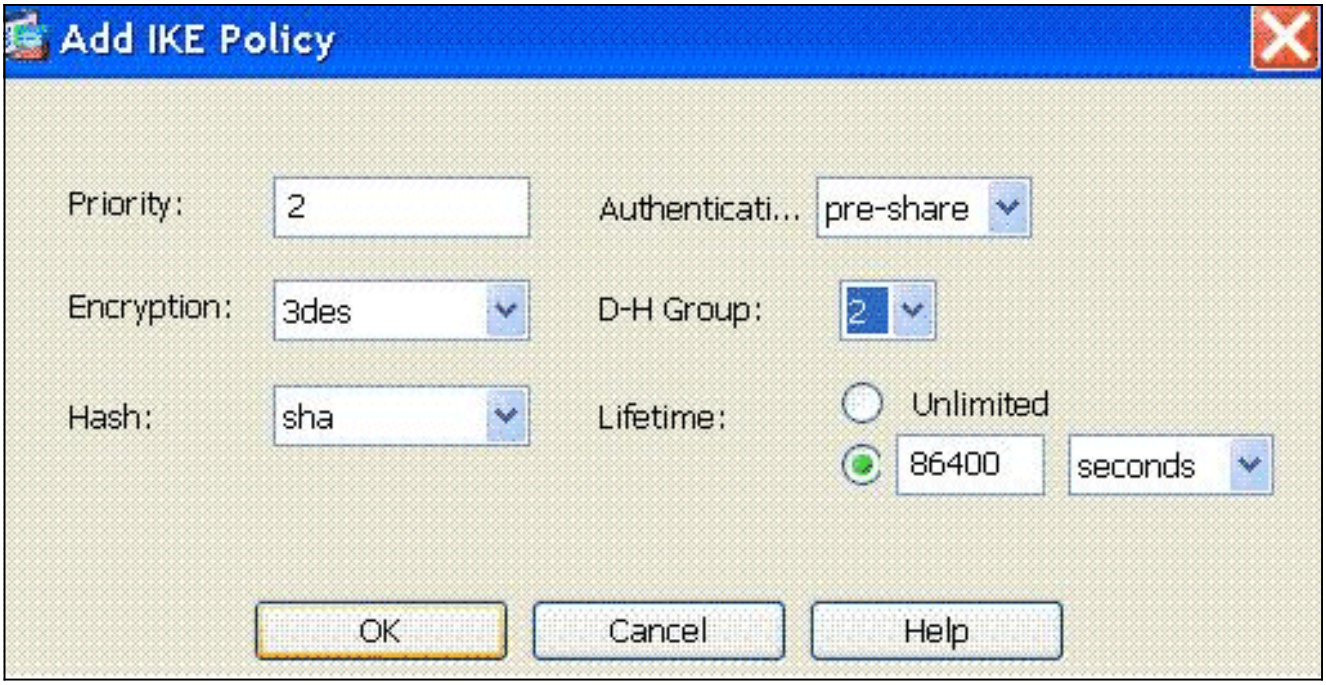
Procedura ASDM

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.

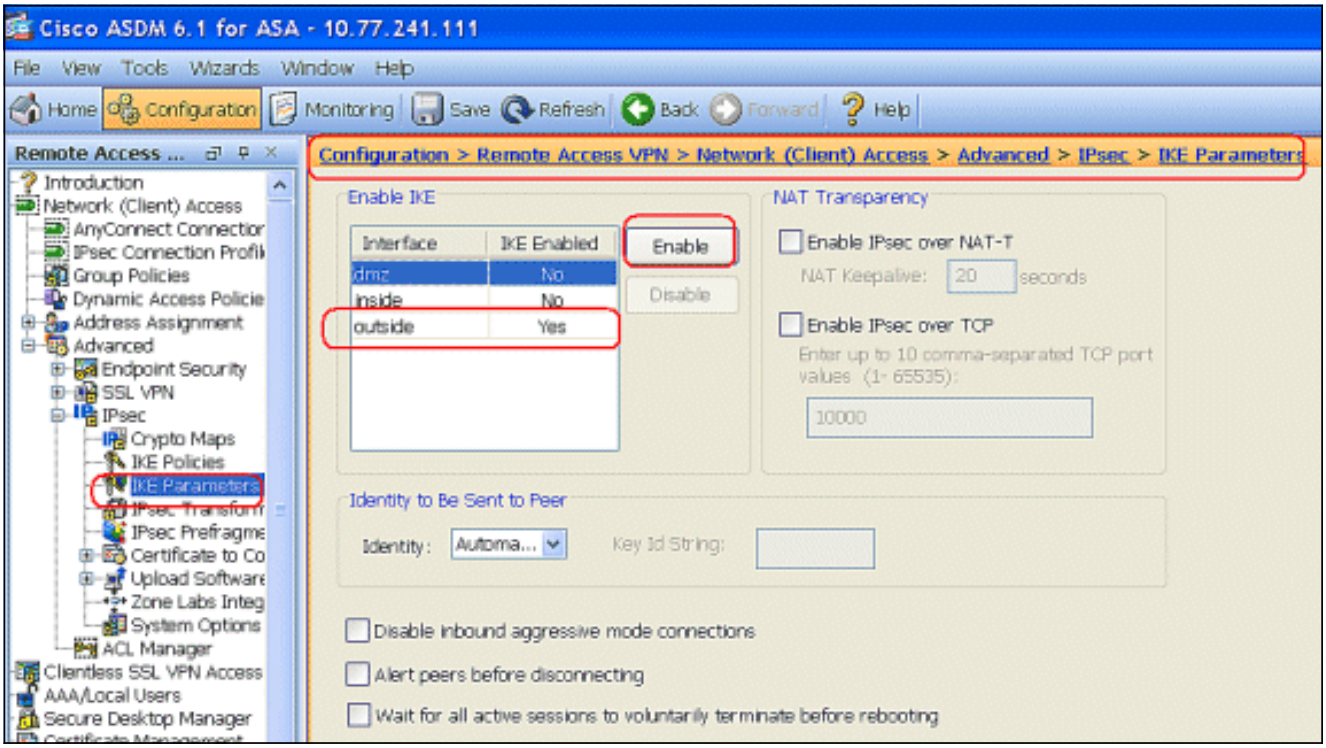


2. Fornire i dettagli del criterio ISAKMP come mostrato.

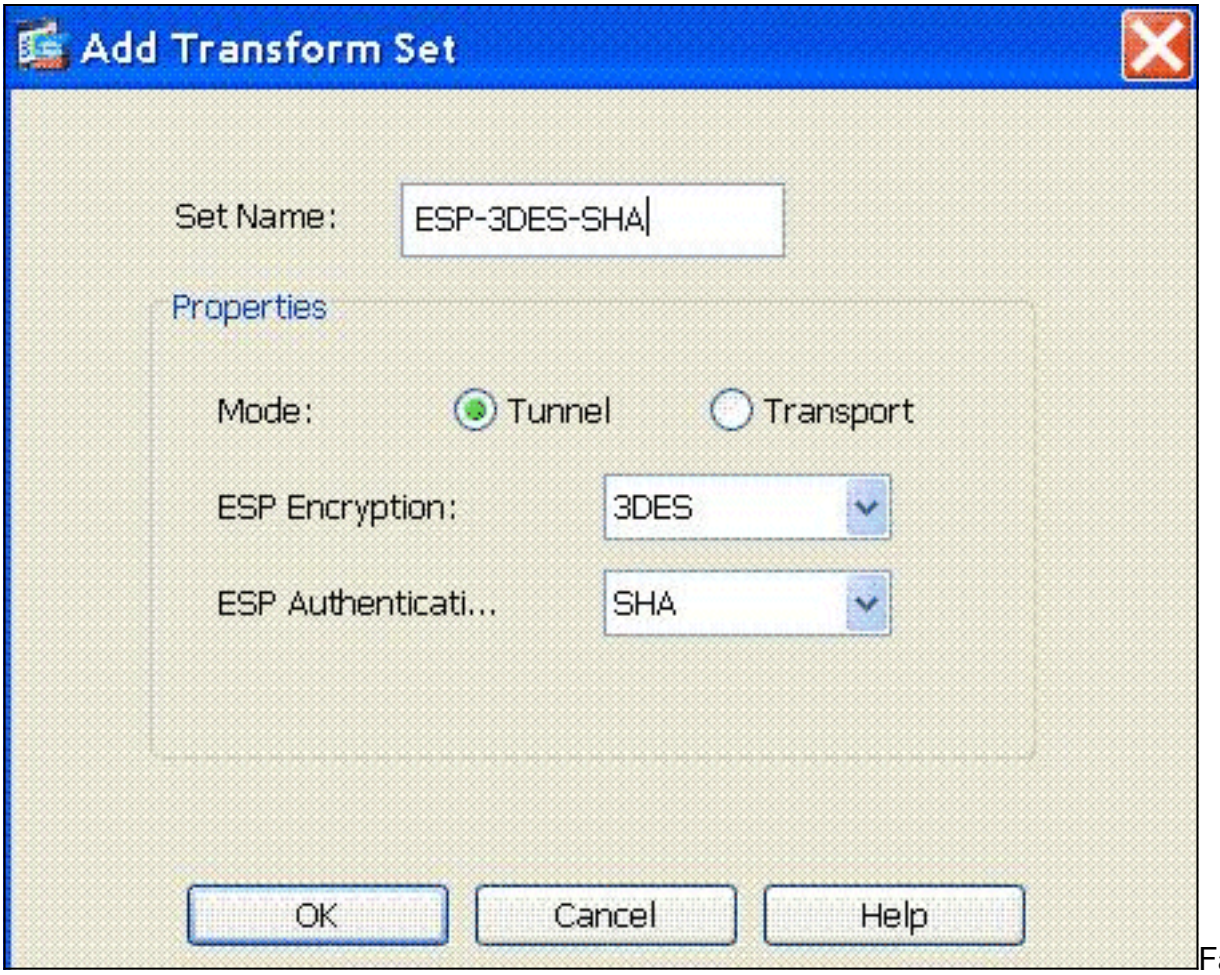


Fare clic su **OK** e su **Applica**.

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

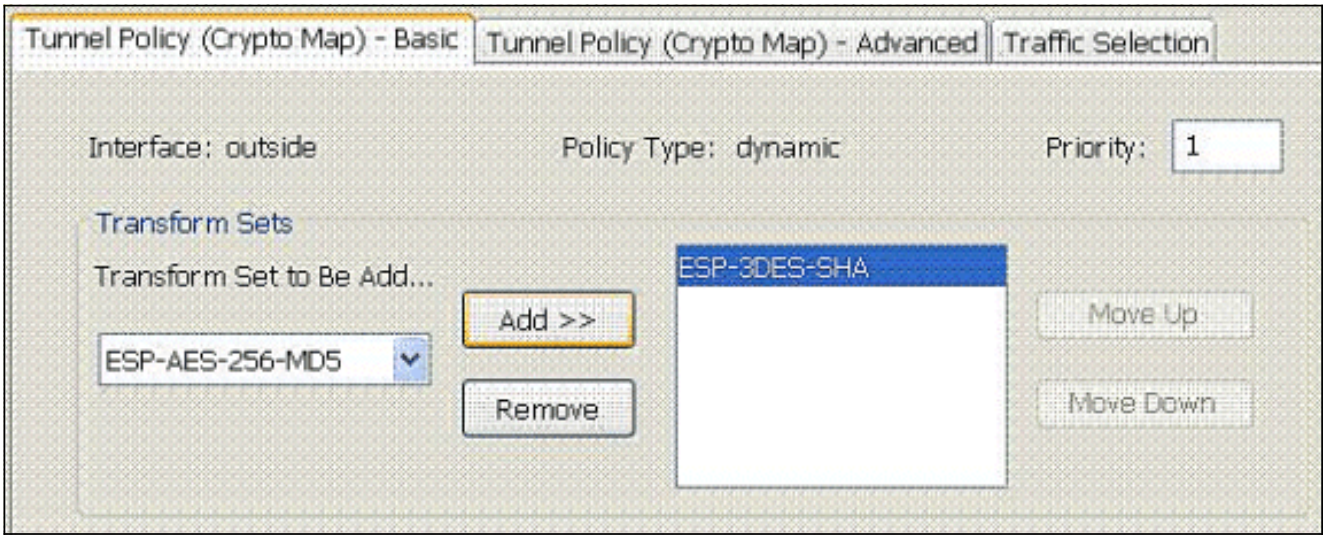


4. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Set trasformazioni IPSec > Aggiungi** per creare il set di trasformazioni **ESP-3DES-SHA**, come mostrato.



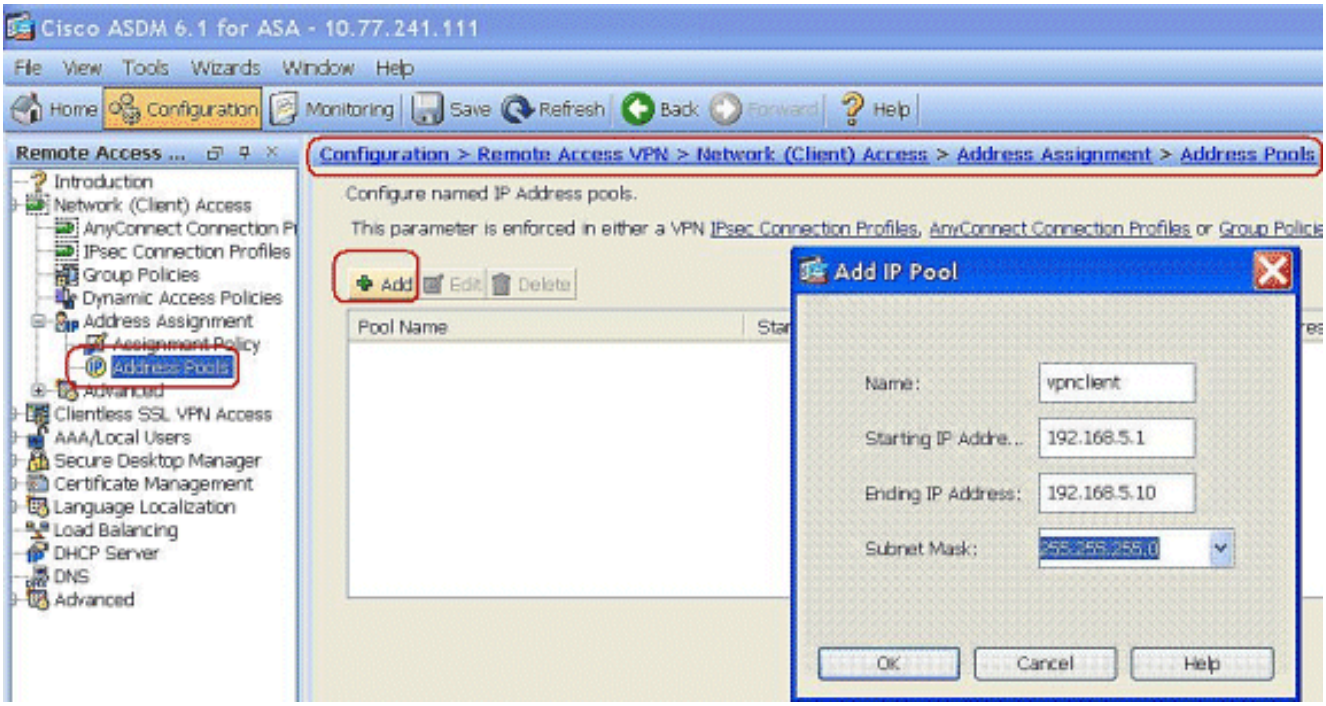
Fare clic su **OK** e su **Applica**.

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.

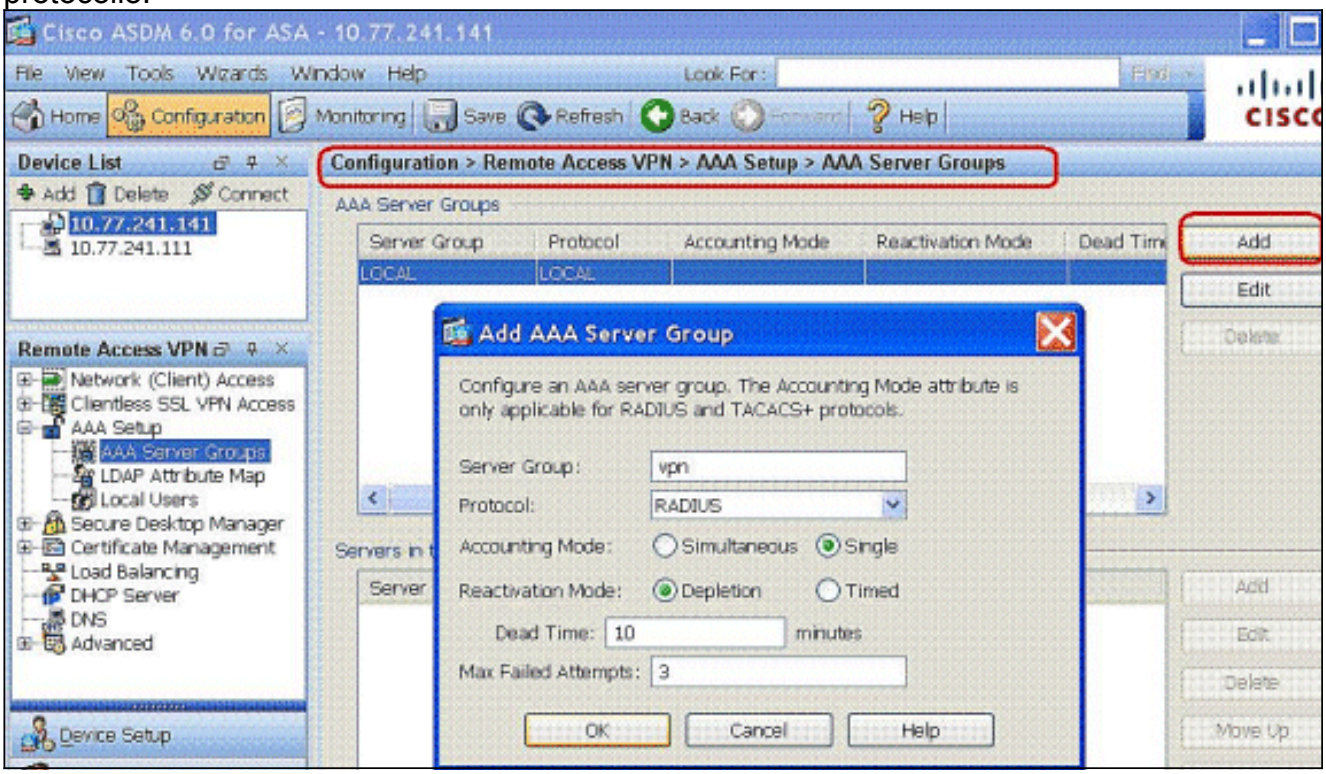


Fare clic su **OK** e su **Applica**.

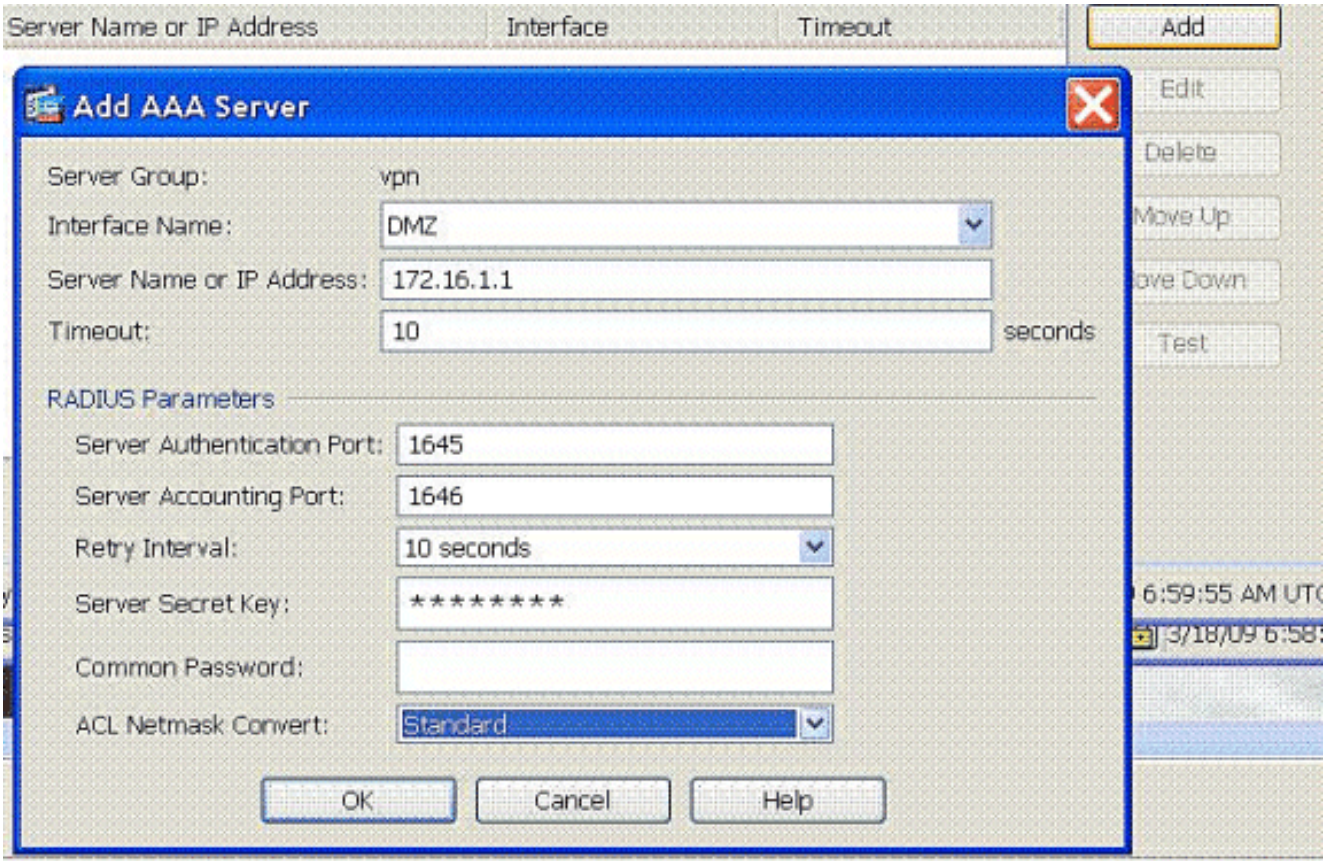
6. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Assegnazione indirizzi > Pool di indirizzi** e fare clic su **Aggiungi** per aggiungere il client VPN per gli utenti del client VPN.



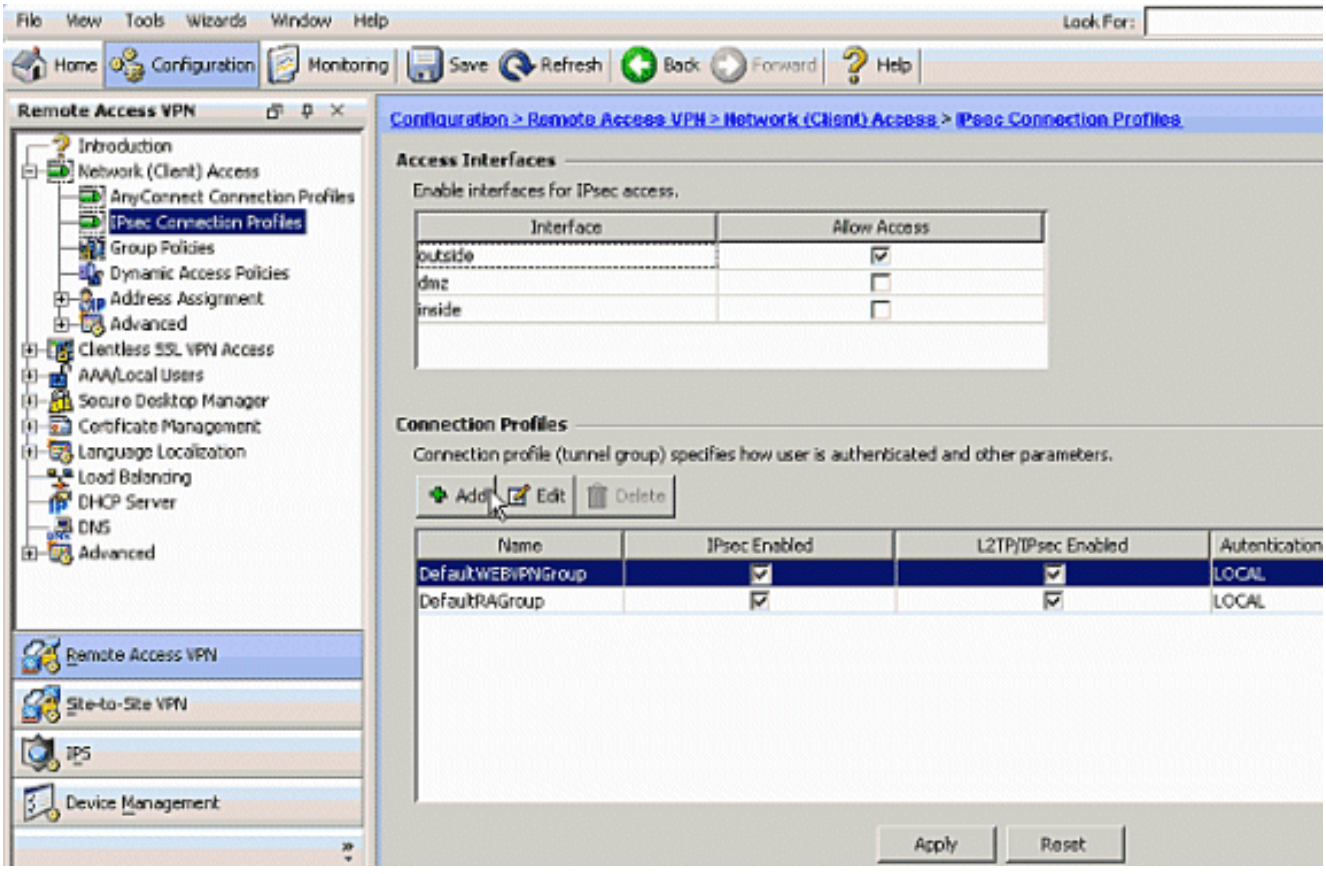
7. Scegliere **Configurazione > VPN ad accesso remoto > Configurazione AAA > Gruppi di server AAA** e fare clic su **Aggiungi** per aggiungere il nome del gruppo di server AAA e il protocollo.



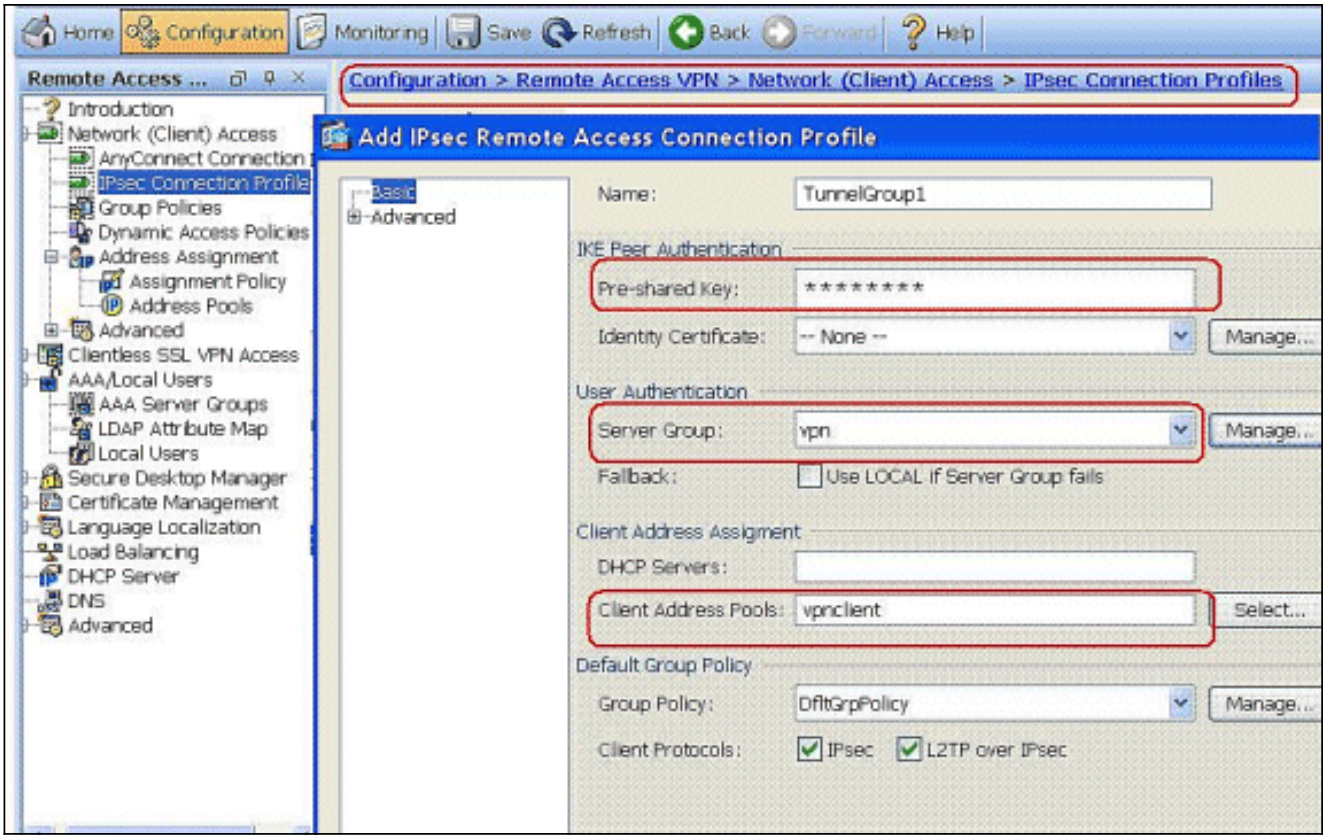
Aggiungere l'indirizzo IP del server AAA (ACS) e l'interfaccia connessa. Aggiungere inoltre la chiave Server Secret nell'area Parametri RADIUS. Fare clic su
OK.



8. 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 come cisco123, come mostrato.

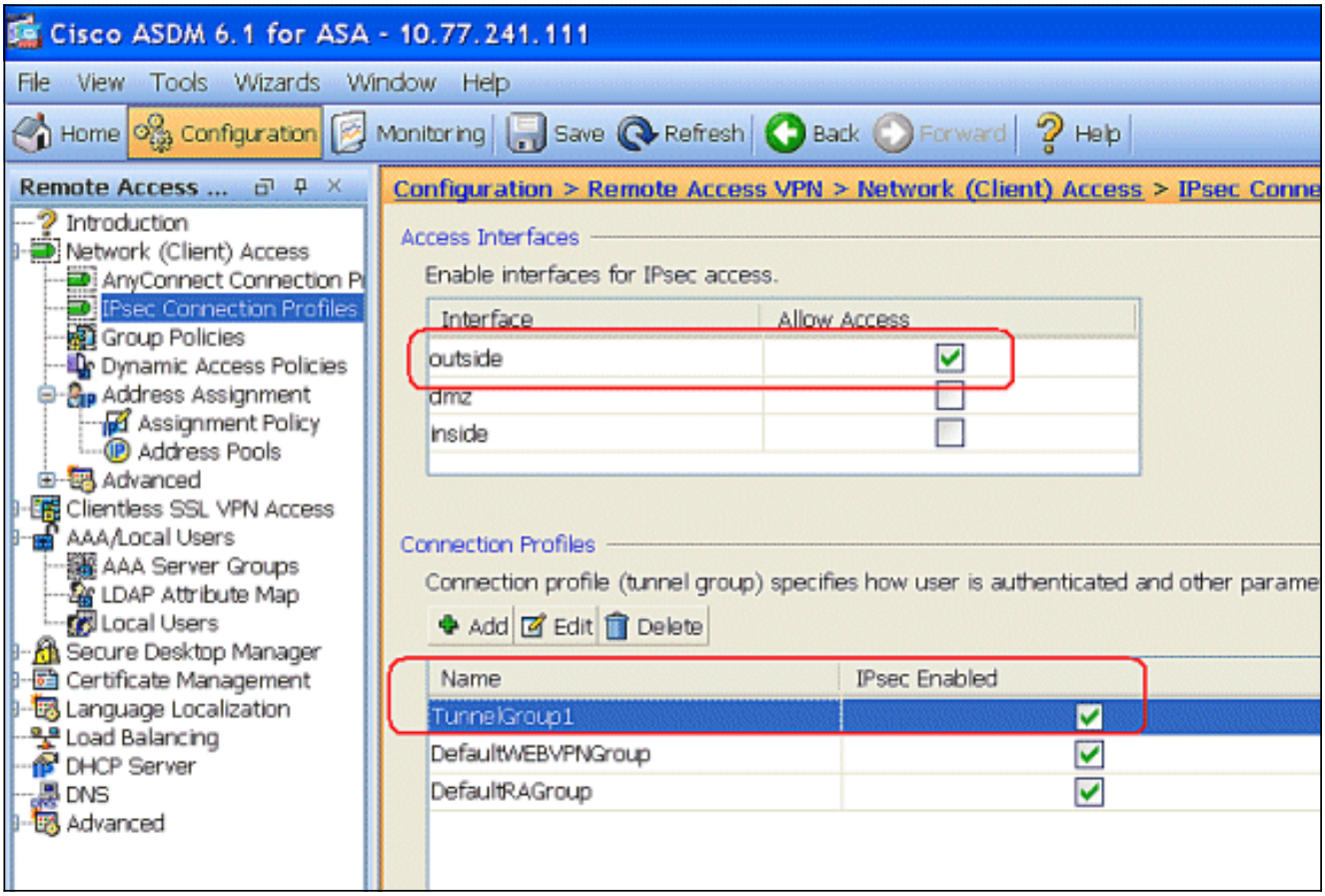


Nella scheda Base, scegliere il gruppo di server come **vpn** per il campo Autenticazione utente.Selezionare **vpnclient** come pool di indirizzi client per gli utenti del client VPN.



Fare clic su **OK**.

9. 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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2
access-list new extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool vpnclient1 192.168.5.1-192.168.5.10 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 !--- Create the AAA server group
"vpn" and specify the protocol as RADIUS. !--- Specify
the CSACS server as a member of the "vpn" group and
provide the !--- location and key. aaa-server vpn
protocol radius
 max-failed-attempts 5
aaa-server vpn (DMZ) host 172.16.1.1
 retry-interval 1
 timeout 30
 key cisco123
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

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. !--- A Triple DES
encryption with !--- the sha hash algorithm is used.
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac

!--- Defines a dynamic crypto map with !--- the
specified encryption settings. crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-3DES-SHA

!--- Binds the dynamic map to the IPsec/ISAKMP process.
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 3des
 hash sha
 group 2
 lifetime 86400

no crypto isakmp nat-traversal

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
```

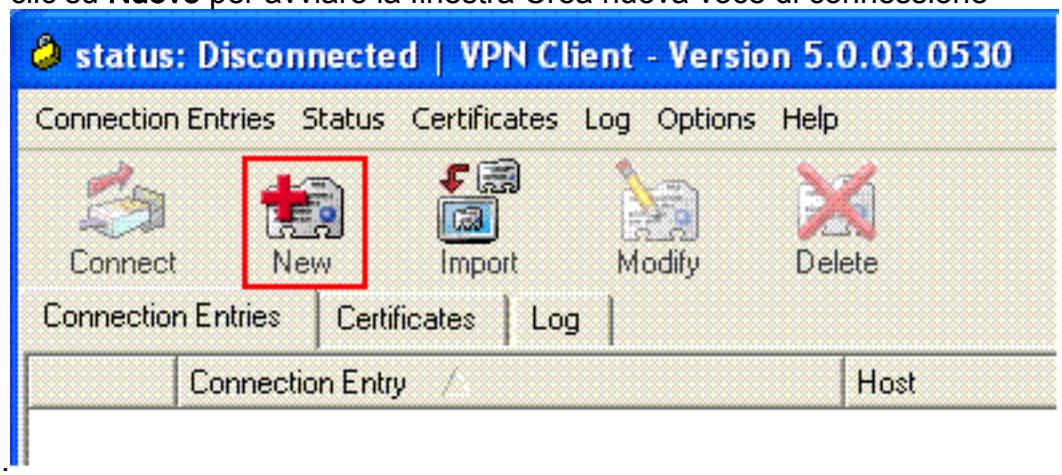
```
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes
 address-pool vpnclient
 authentication-server-group vpn

!--- 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

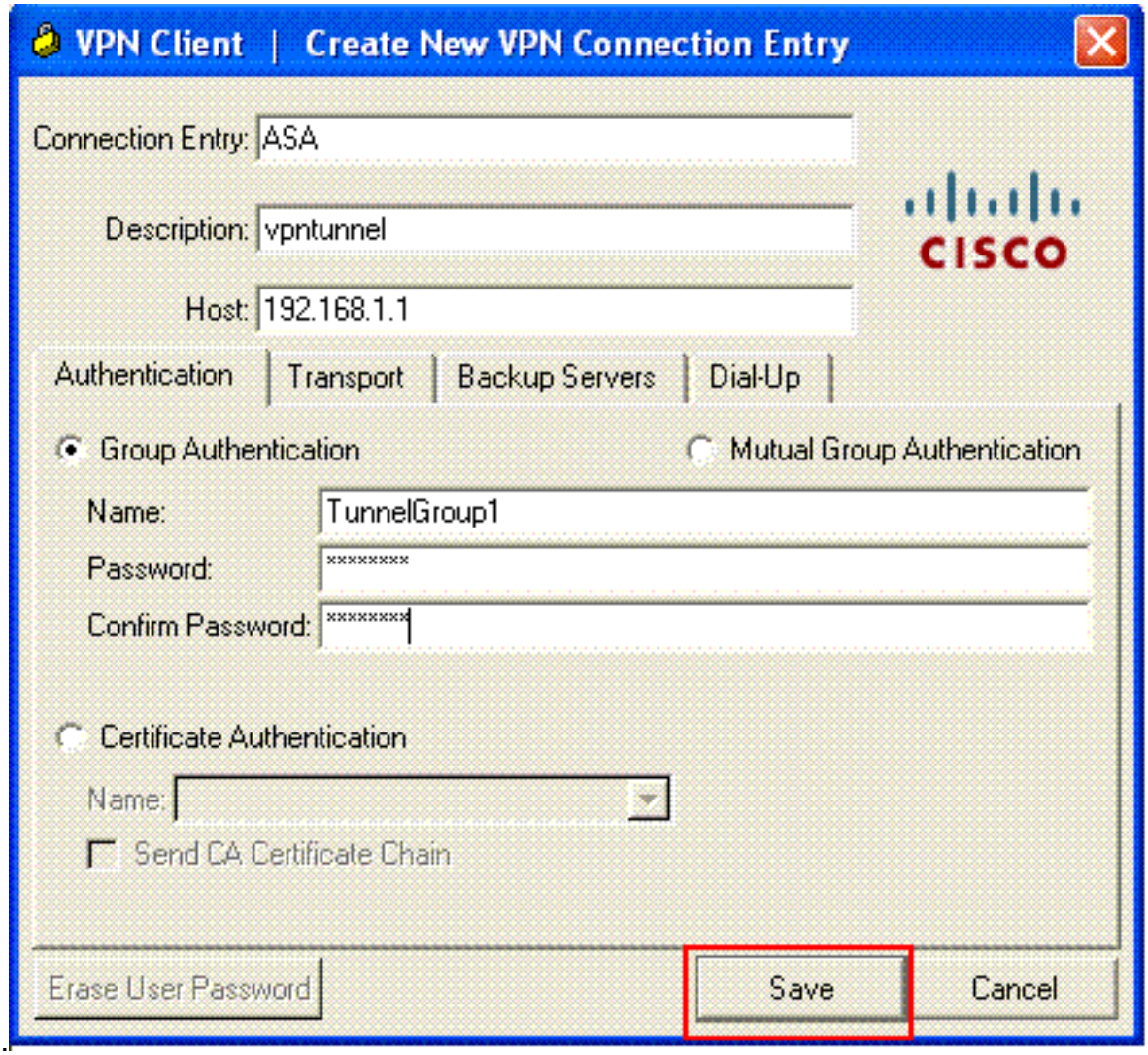
Provare a connettersi all'appliance Cisco ASA con il client VPN Cisco per verificare che l'appliance ASA sia configurata correttamente.

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



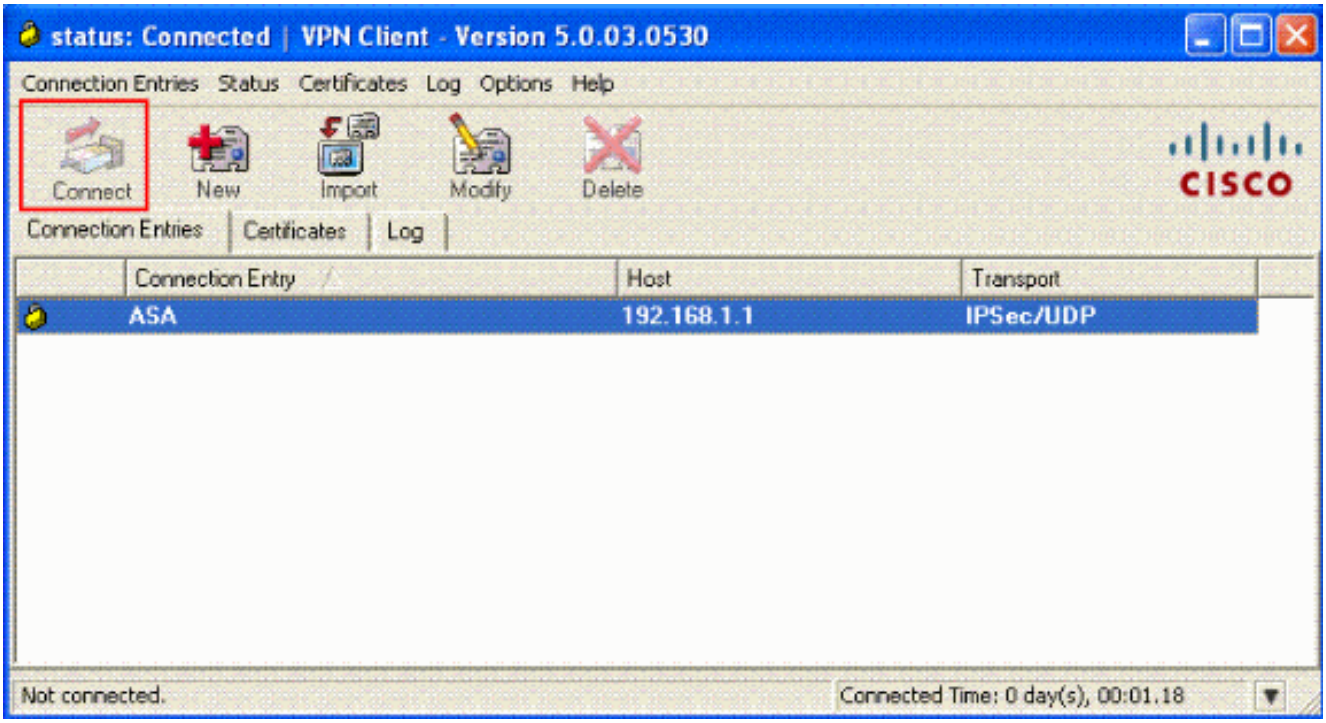
VPN.

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

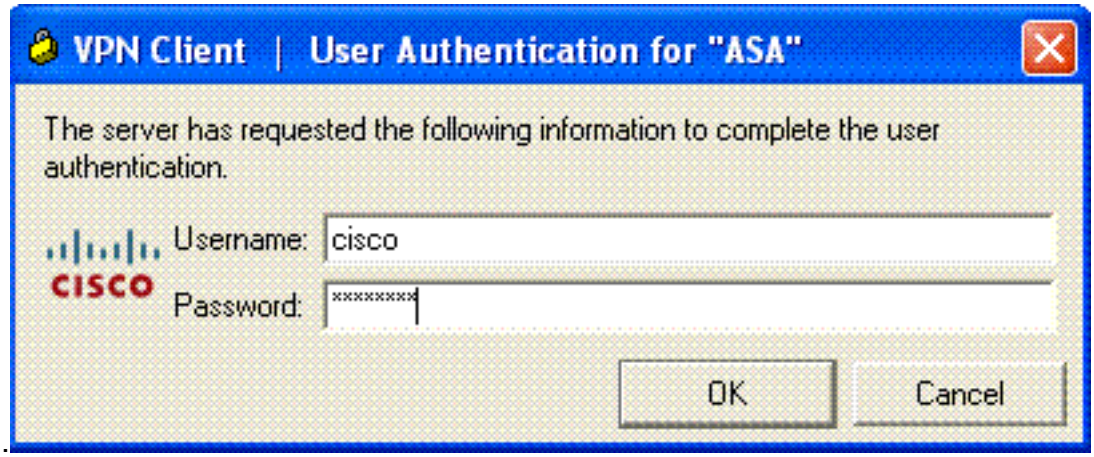


Salva.

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

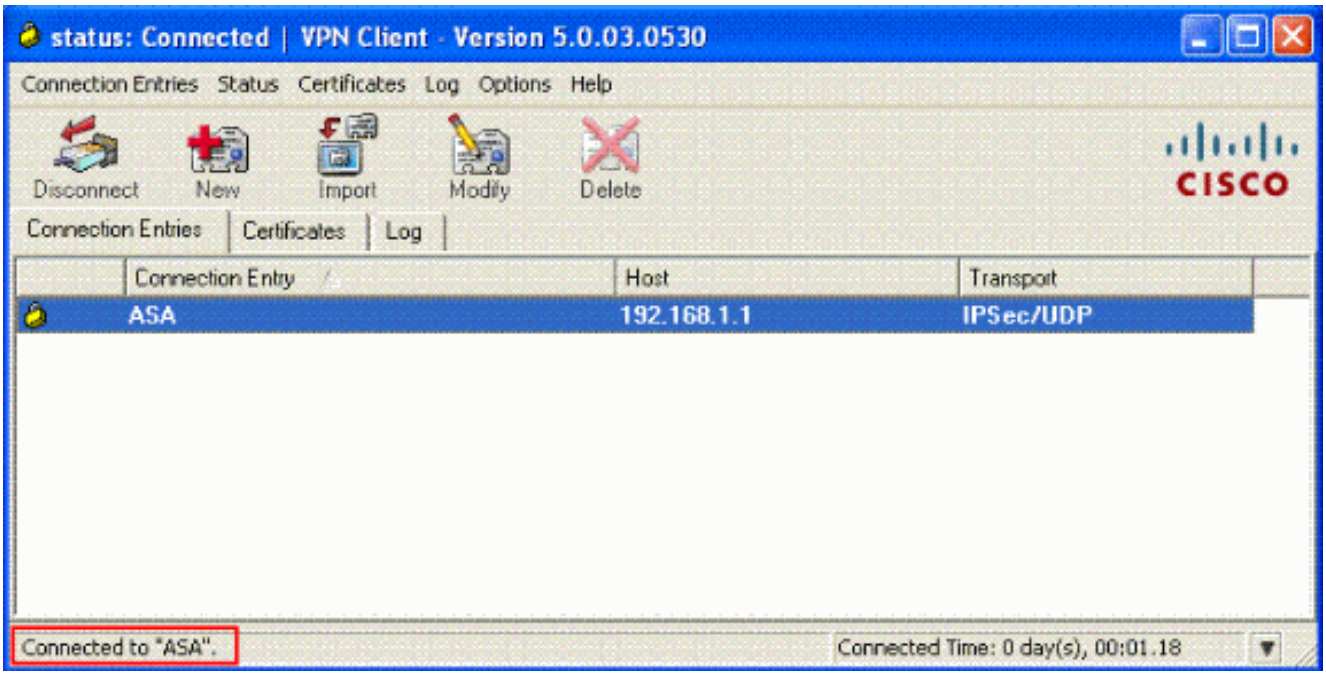


5. Quando richiesto, immettere il **nome utente: cisco** e **password: password1** è stata configurata nell'appliance ASA per xauth e fare clic su **OK** per connettersi alla rete

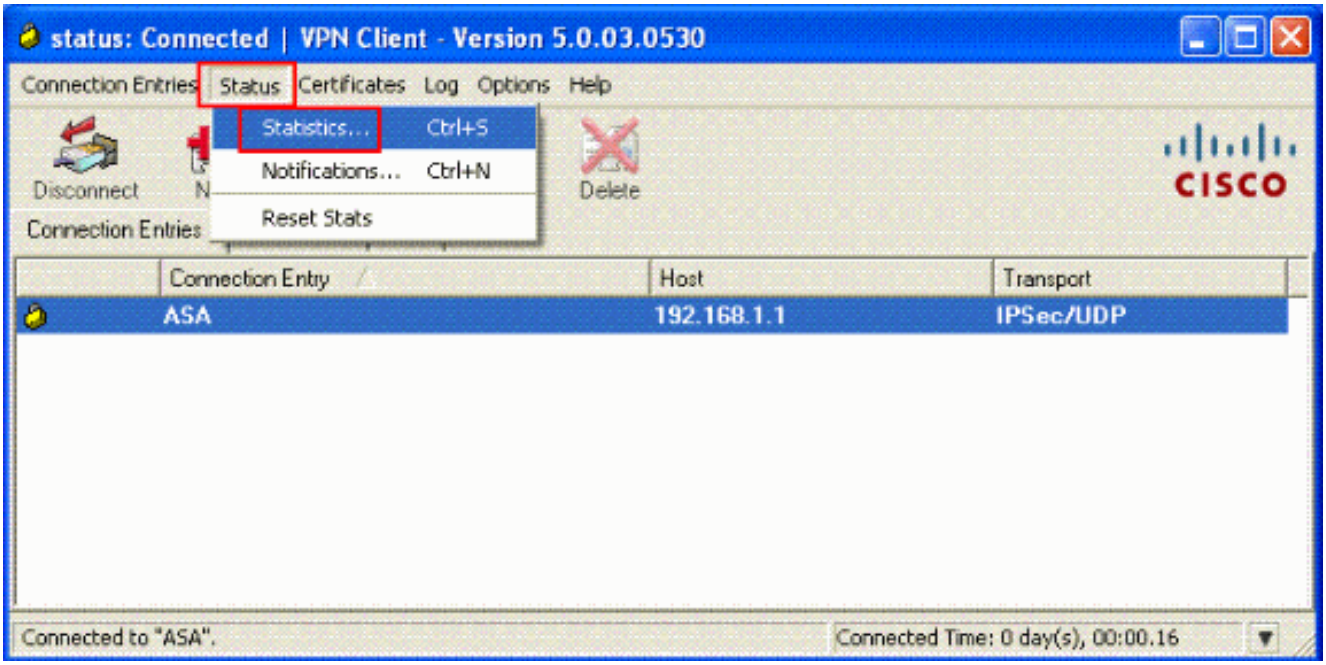


remota.

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.



Configurazione di ACS per ACL scaricabili per un singolo utente

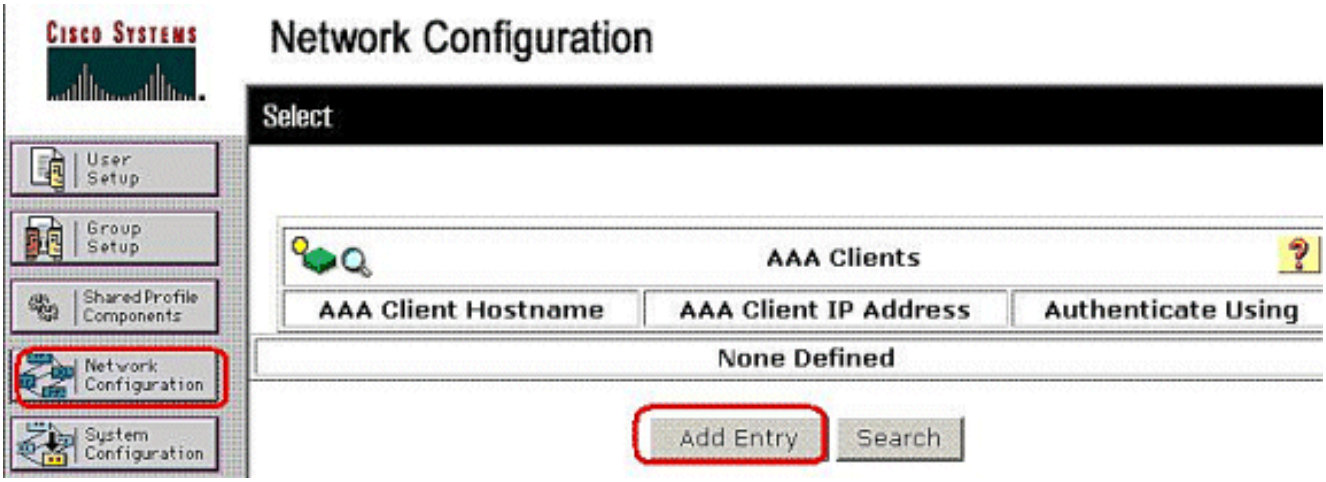
Èpossibile configurare gli elenchi degli accessi scaricabili su Cisco Secure ACS come componenti di un profilo condiviso e quindi assegnare l'elenco degli accessi a un gruppo o a un singolo utente.

Per implementare gli elenchi degli accessi dinamici, è necessario configurare il server RADIUS in modo che lo supporti. Quando l'utente esegue l'autenticazione, il server RADIUS invia un elenco degli accessi scaricabile o un nome di elenco degli accessi all'accessorio di protezione. L'accesso a un determinato servizio è consentito o negato dall'elenco degli accessi. L'elenco degli accessi verrà eliminato alla scadenza della sessione di autenticazione.

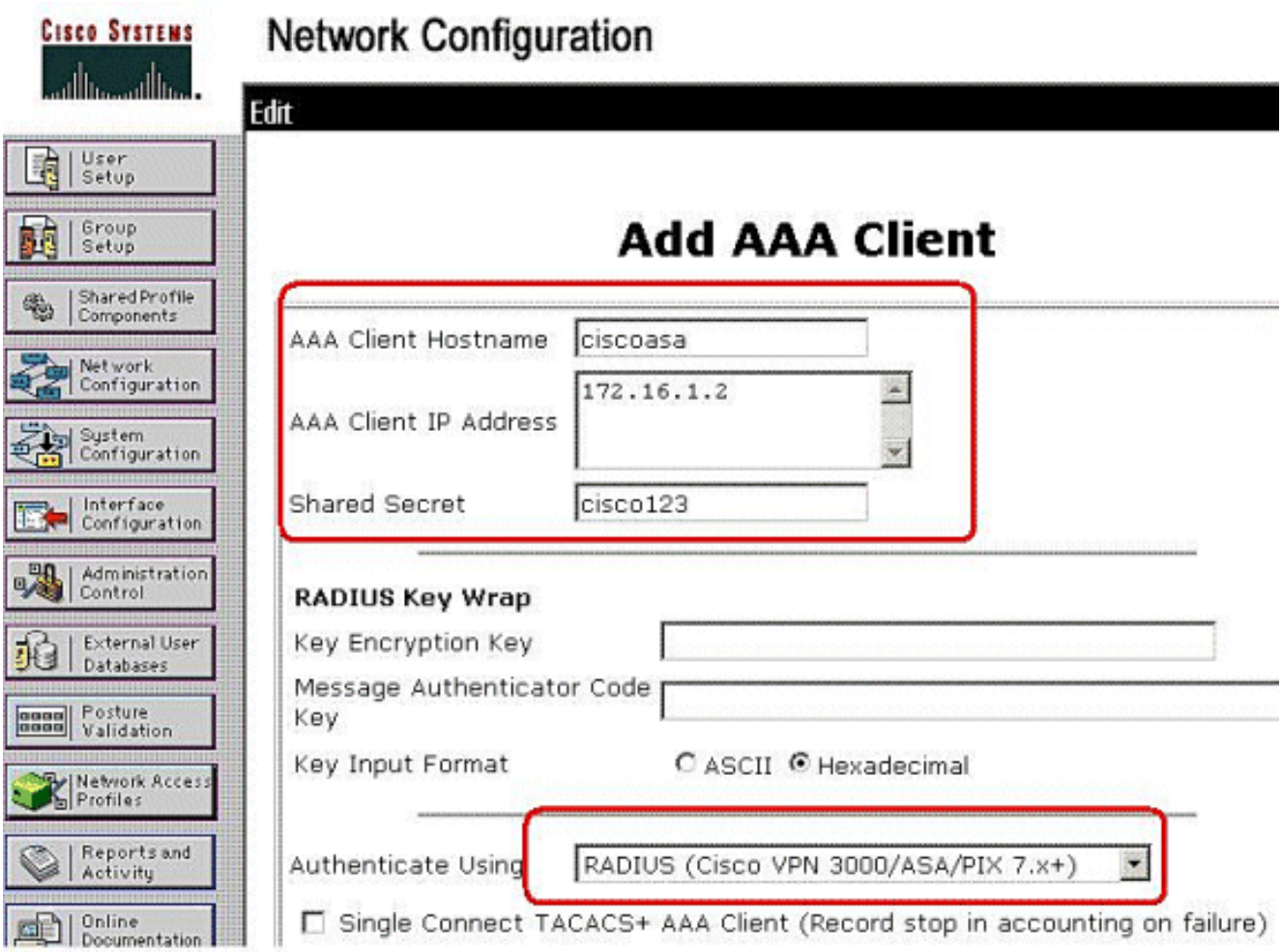
Nell'esempio, l'utente VPN IPSec **"cisco"** viene autenticato correttamente e il server RADIUS invia un elenco degli accessi scaricabile all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione ACL scaricabili per utente/gruppo.

Completare questa procedura per configurare RADIUS in un Cisco Secure ACS.

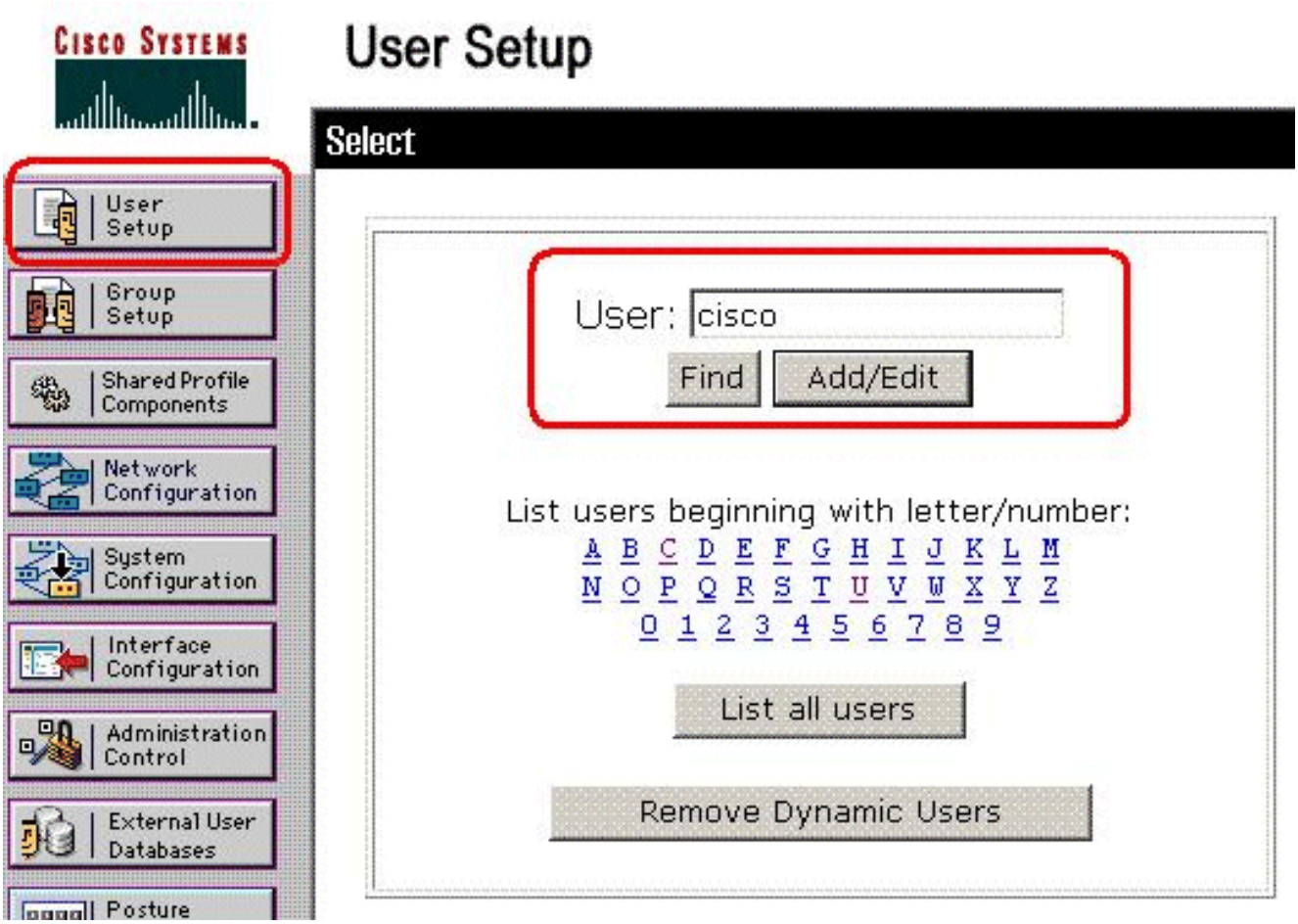
1. Scegliere **Configurazione di rete** a sinistra e fare clic su **Aggiungi voce** per aggiungere una voce per l'appliance ASA nel database del server RADIUS.



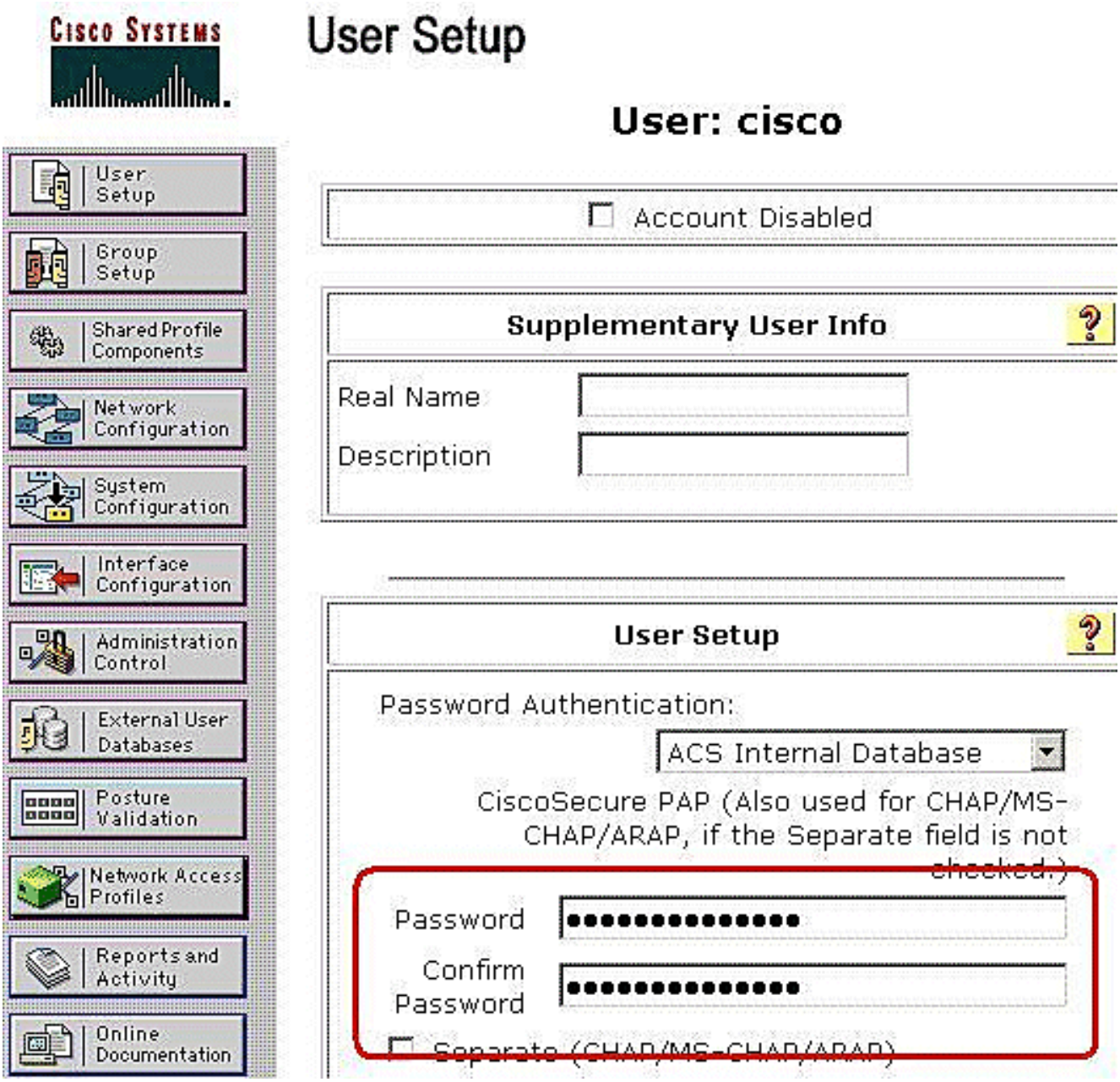
2. Immettere **172.16.1.2** nel campo Indirizzo IP client e immettere **"cisco123"** per il campo Chiave segreta condivisa. Selezionare **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** nella casella a discesa *Autentica con*. Fare clic su **Invia**.
.



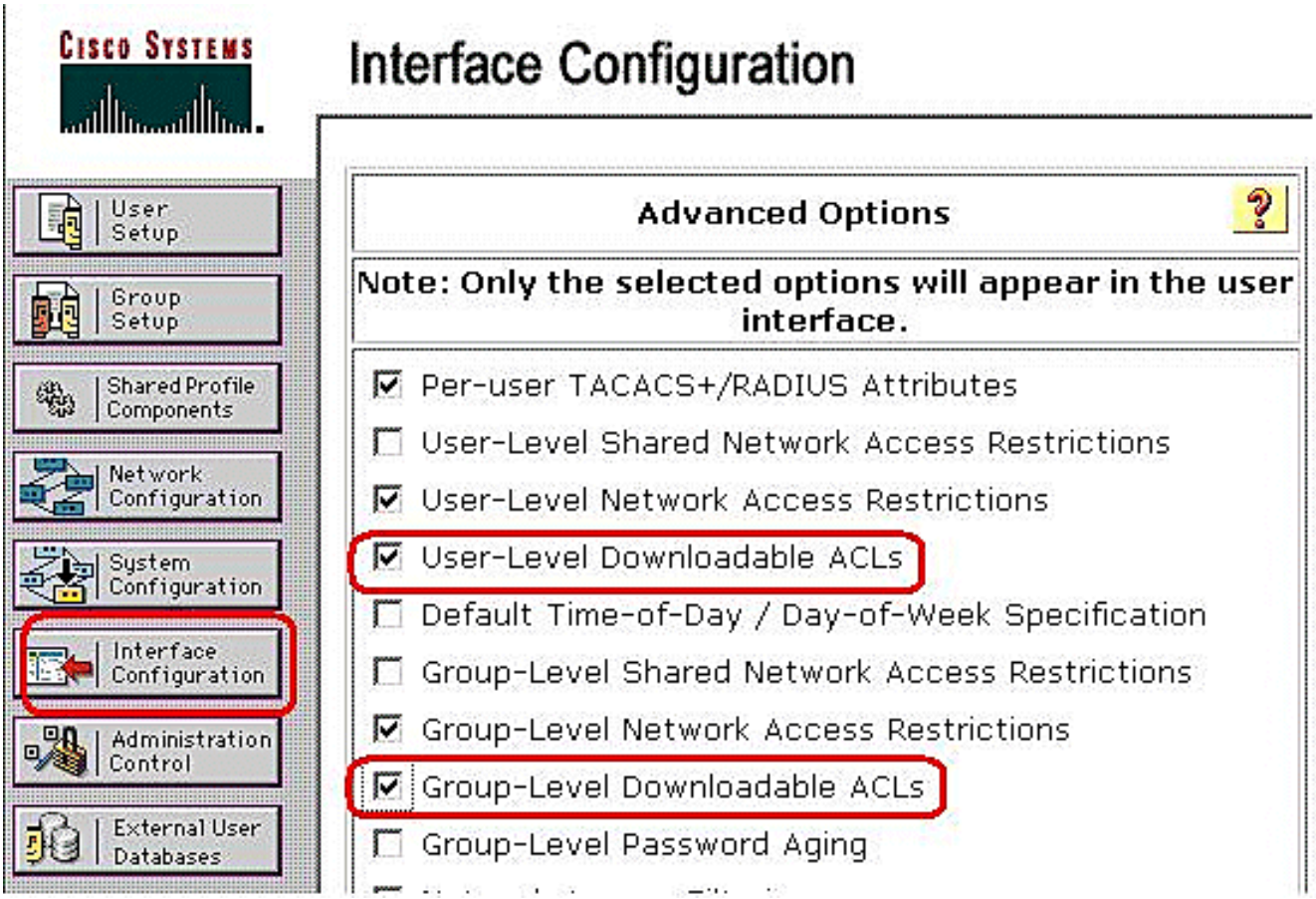
3. Immettere il nome utente nel campo Utente nel database Cisco Secure e fare clic su **Aggiungi/Modifica**.Nell'esempio, il nome utente è **cisco**.



4. Nella finestra successiva, immettere la password per **"cisco"**. In questo esempio, la password è anche **password1**. Al termine, fare clic su **Invia**.

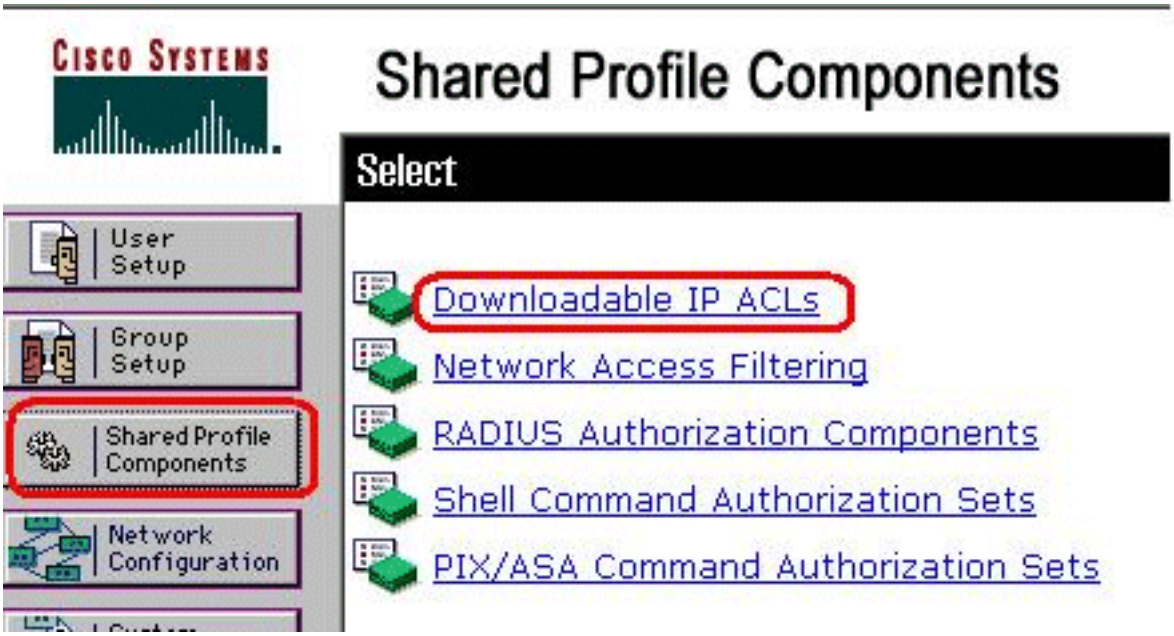


5. La pagina Opzioni avanzate consente di determinare le opzioni avanzate visualizzate da ACS. Se si nascondono le opzioni avanzate che non si utilizzano, è possibile semplificare le pagine visualizzate in altre aree dell'interfaccia Web di ACS. Fare clic su **Configurazione interfaccia** e quindi su **Opzioni avanzate** per aprire la pagina Opzioni avanzate.

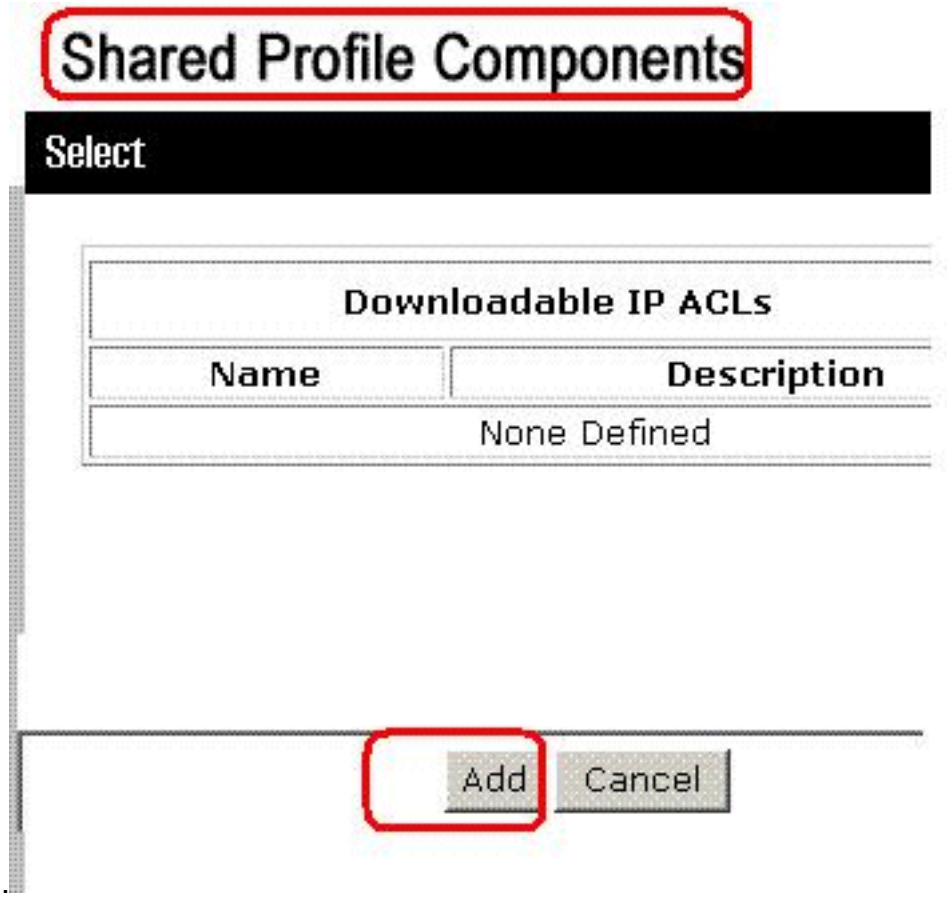


Selezionare la casella per gli **ACL scaricabili a livello di utente** e per **gli ACL scaricabili a livello di gruppo**.**ACL scaricabili a livello utente**: se selezionata, questa opzione abilita la sezione ACL scaricabili (elenchi di controllo dell'accesso) nella pagina di configurazione utente.**ACL scaricabili a livello di gruppo**: se selezionata, questa opzione abilita la sezione ACL scaricabili nella pagina Configurazione gruppo.

6. Nella barra di navigazione, fare clic su **Shared Profile Components**, quindi su **Downloadable IP ACLs** (ACL IP scaricabili).**Nota:** se *gli ACL IP scaricabili* non vengono visualizzati nella pagina Componenti del profilo condiviso, è necessario abilitare l'opzione ACL scaricabili a livello di utente, ACL scaricabili a livello di gruppo o entrambe nella pagina Opzioni avanzate della sezione Configurazione
interfaccia.

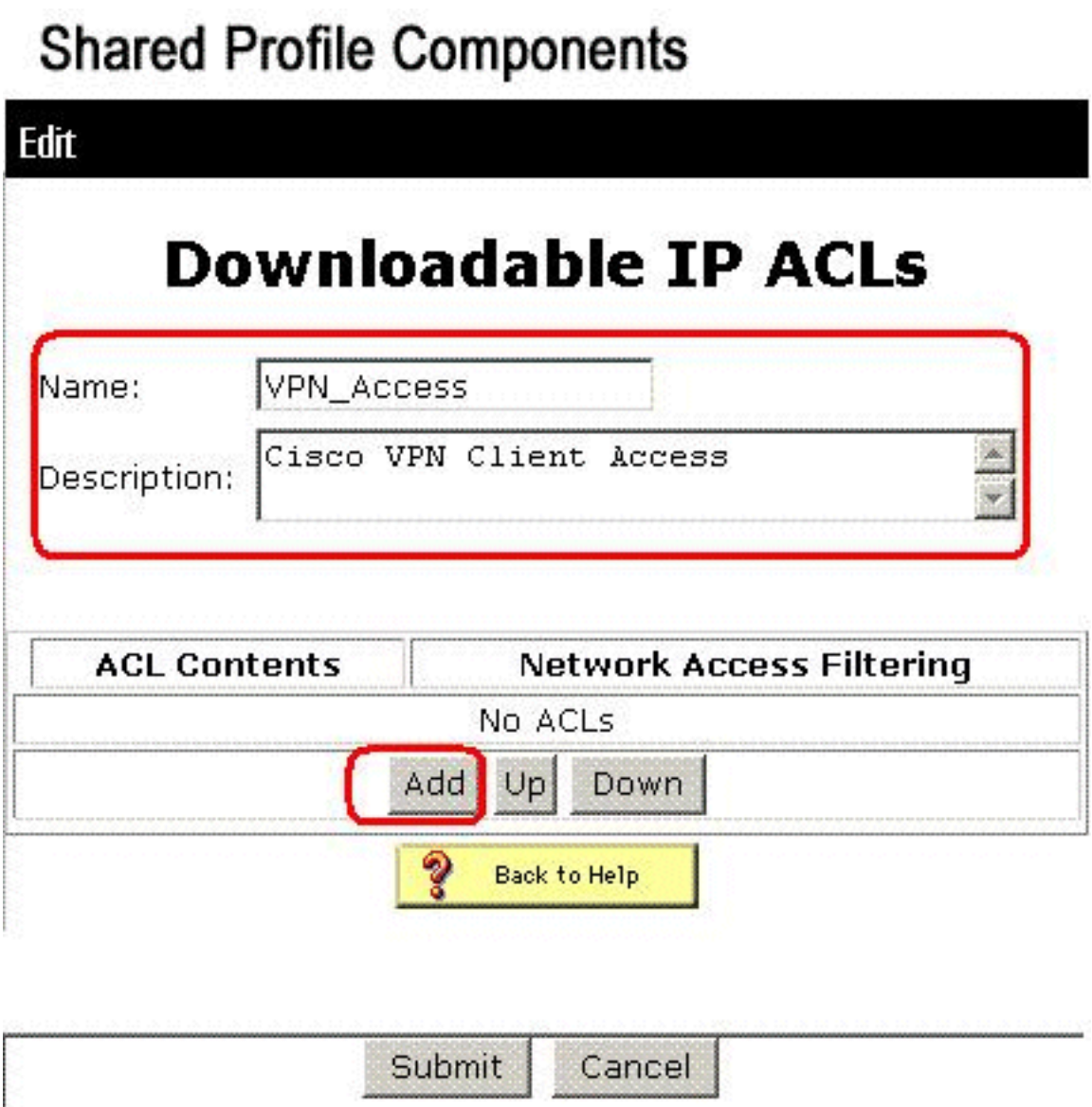


7. Fare clic su **Add**. Viene visualizzata la pagina ACL IP



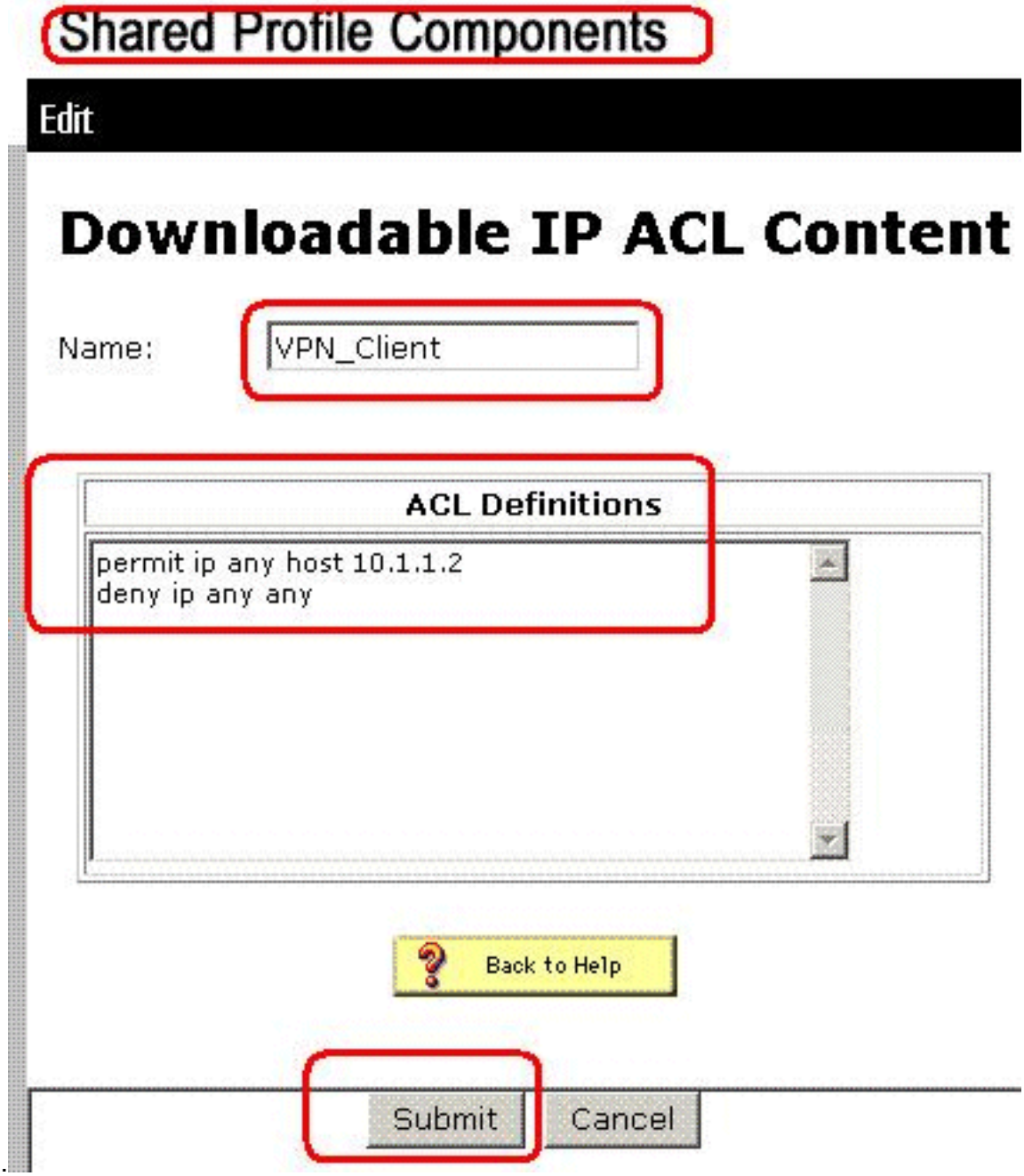
scaricabili.

8. Nella casella Nome digitare il nome del nuovo ACL IP.**Nota:** il nome di un ACL IP può contenere fino a 27 caratteri. Il nome non può contenere spazi né i seguenti caratteri: trattino (-), parentesi quadra aperta ([), parentesi quadra chiusa (]), barra (/), barra rovesciata (\), virgolette ("), parentesi angolare sinistra (<), parentesi angolare destra (>) o trattino (-).Nella casella Descrizione digitare una descrizione del nuovo ACL IP. La descrizione può contenere un massimo di 1.000



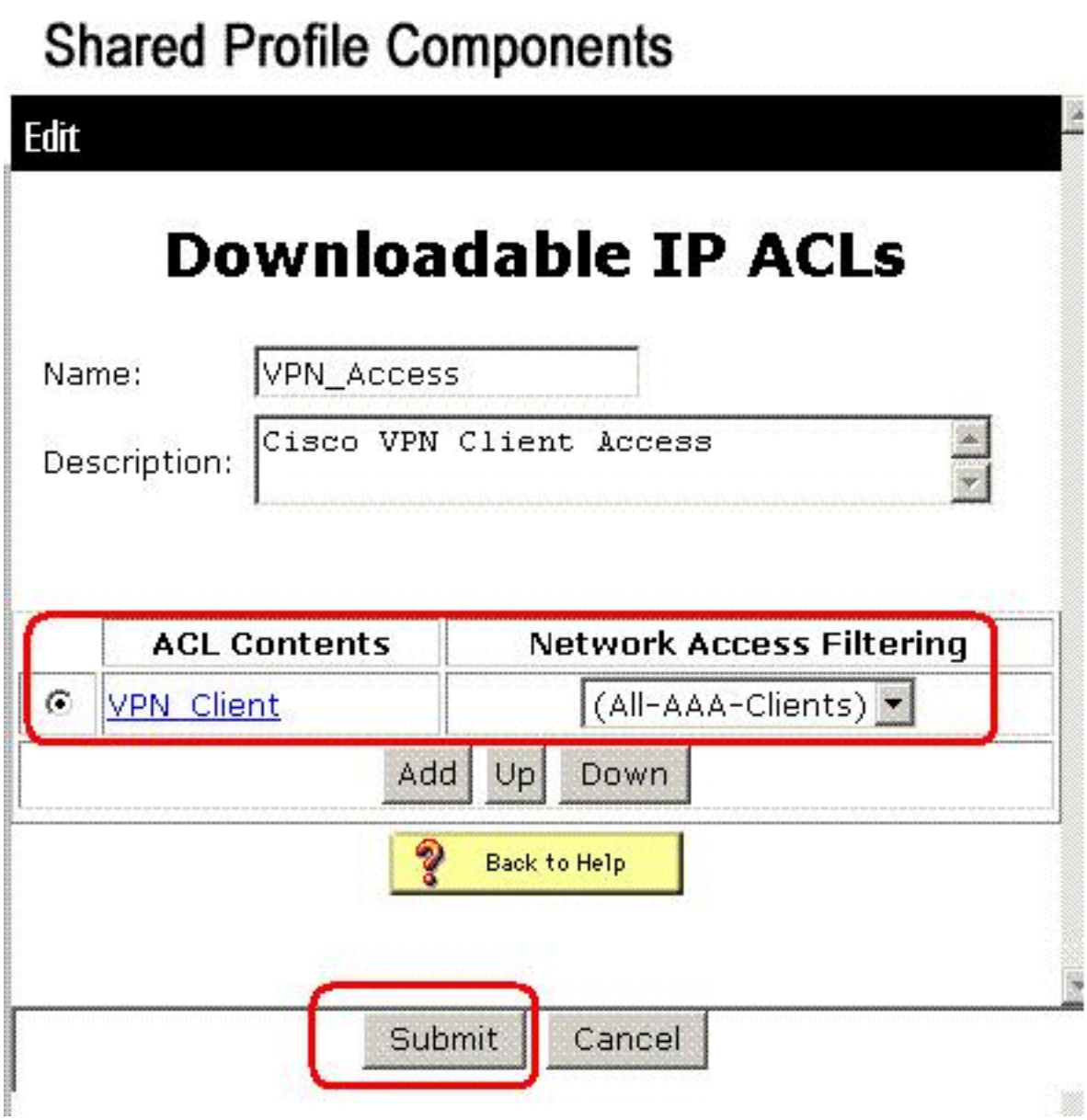
caratteri. Per aggiungere un contenuto ACL al nuovo ACL IP, fare clic su **Add** (Aggiungi).

9. Nella casella Nome digitare il nome del nuovo contenuto ACL.**Nota:** il nome di un contenuto ACL può contenere fino a 27 caratteri. Il nome non può contenere spazi né i seguenti caratteri: trattino (-), parentesi quadra aperta ([), parentesi quadra chiusa (]), barra (/), barra rovesciata (\), virgolette ("), parentesi angolare sinistra (<), parentesi angolare destra (>) o trattino (-).Nella casella Definizioni ACL digitare la nuova definizione dell'ACL.**Nota:** quando si immettono le definizioni degli ACL nell'interfaccia Web di ACS, non usare parole chiave o nomi; iniziare piuttosto con una parola chiave allow o deny.Per salvare il contenuto dell'ACL, fare clic su **Submit**



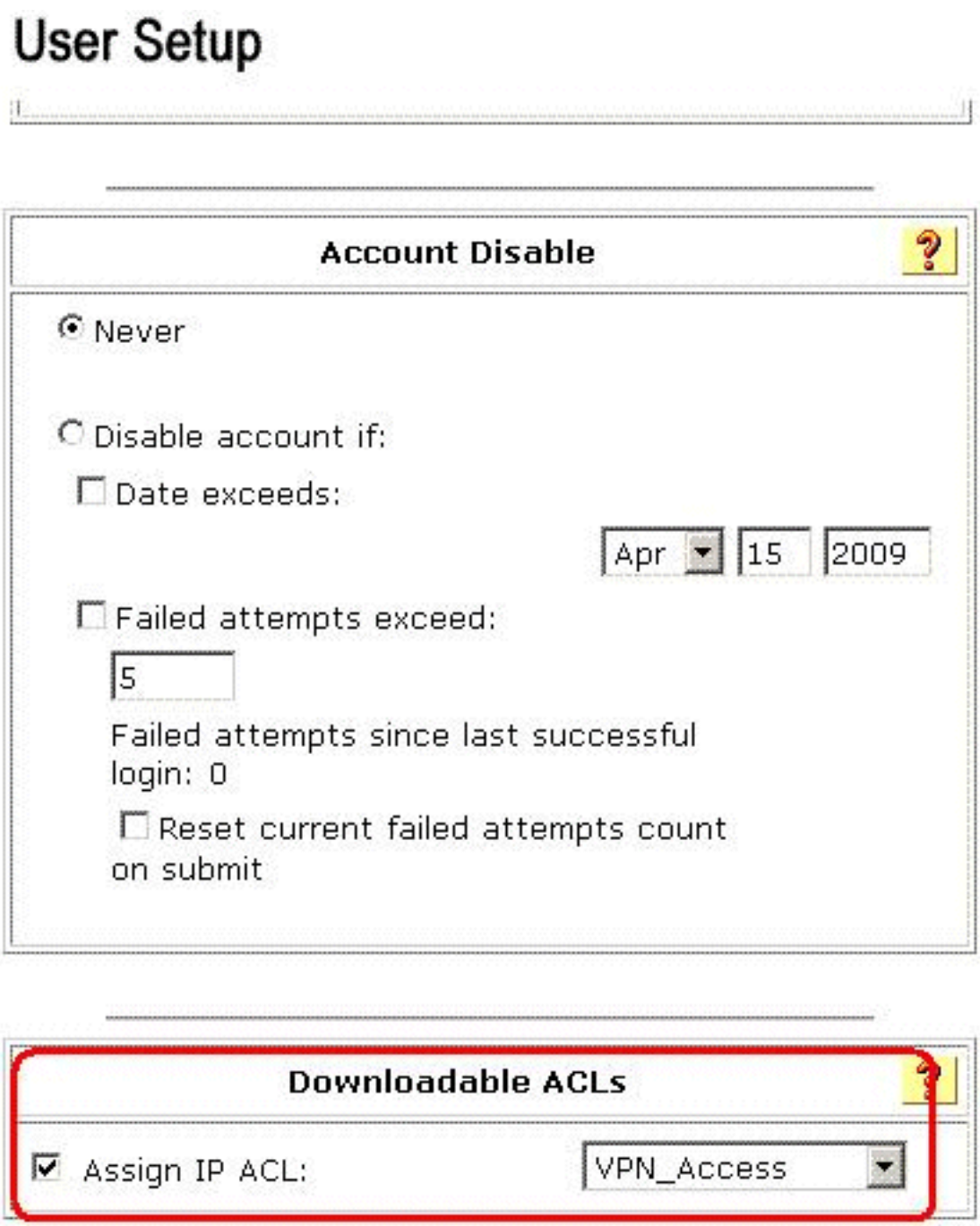
(Invia).

10. Viene visualizzata la pagina ACL IP scaricabili con il nuovo contenuto ACL elencato per nome nella colonna Contenuto ACL. Per associare un NAF al contenuto ACL, scegliere un NAF dalla casella Network Access Filtering (Filtro accesso alla rete) a destra del nuovo contenuto ACL. Per impostazione predefinita, NAF è (All-AAA-Clients). Se non si assegna un NAF, ACS associa il contenuto ACL a tutti i dispositivi di rete (impostazione predefinita).



Per impostare l'ordine dei contenuti degli ACL, fare clic sul pulsante di scelta relativo a una definizione di ACL, quindi fare clic su **Su** o **Giù** per riposizionarlo nell'elenco.Per salvare l'ACL IP, fare clic su **Submit** (Invia).**Nota:** l'ordine dei contenuti degli ACL è significativo. Dall'alto in basso, ACS scarica solo la prima definizione di ACL con un'impostazione NAF applicabile, che include l'impostazione predefinita Tutti-AAA-Client, se utilizzata. In genere, l'elenco di contenuti ACL va da quello con il NAF più specifico (più stretto) a quello con il NAF più generale (client All-AAA).**Nota:** ACS immette il nuovo ACL IP, che ha effetto immediato. Ad esempio, se l'ACL IP deve essere usato con i firewall PIX, è disponibile per l'invio a qualsiasi firewall PIX che tenti l'autenticazione di un utente a cui è stato assegnato l'ACL IP scaricabile al proprio profilo utente o di gruppo.

11. Andare alla pagina Impostazione utente e modificare la pagina Utente. Nella sezione Download di ACL, fare clic su **Assegna ACL IP:** casella di controllo. Selezionare un ACL IP dall'elenco. Dopo aver completato la configurazione delle opzioni dell'account utente, fare clic su **Invia** per registrare le



opzioni.

Configurazione di ACS per ACL scaricabili per gruppo

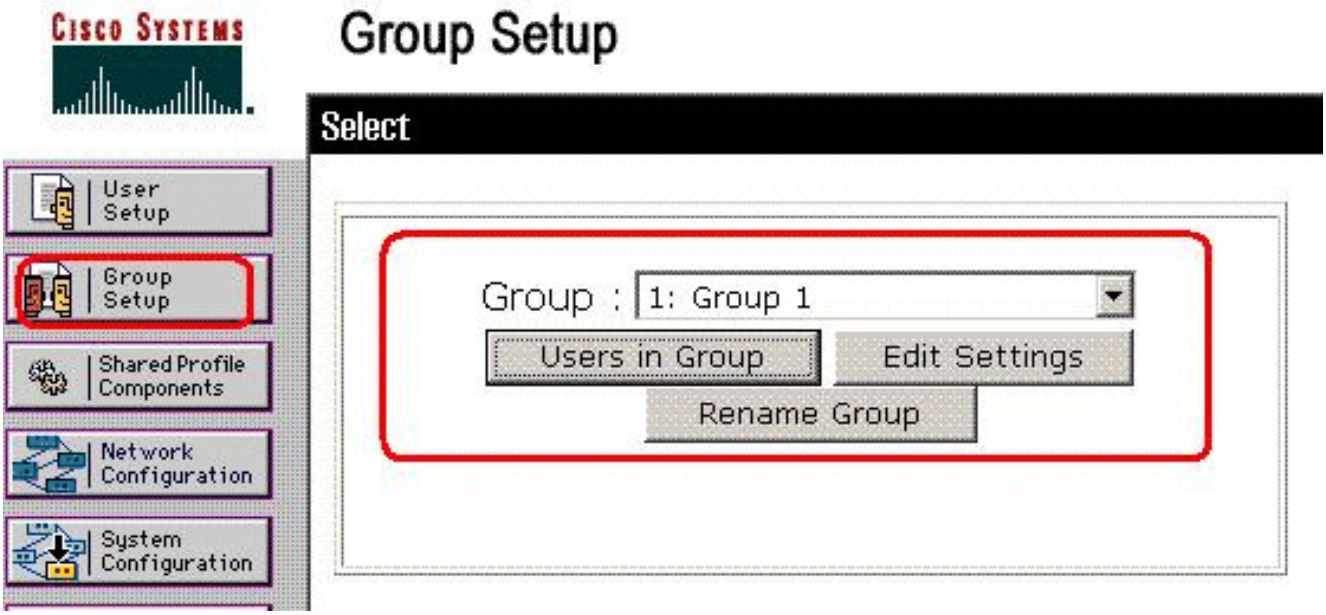
Completare i passaggi da 1 a 9 di Configure ACS for Downloadable ACL for Individual User (Configura ACL scaricabili per un singolo utente) e attenersi alla seguente procedura per configurare ACL scaricabili per un gruppo in un ACS Cisco Secure.

Nell'esempio, l'utente VPN IPSec "cisco" appartiene ai gruppi VPN. I criteri di gruppo VPN vengono applicati a tutti gli utenti del gruppo.

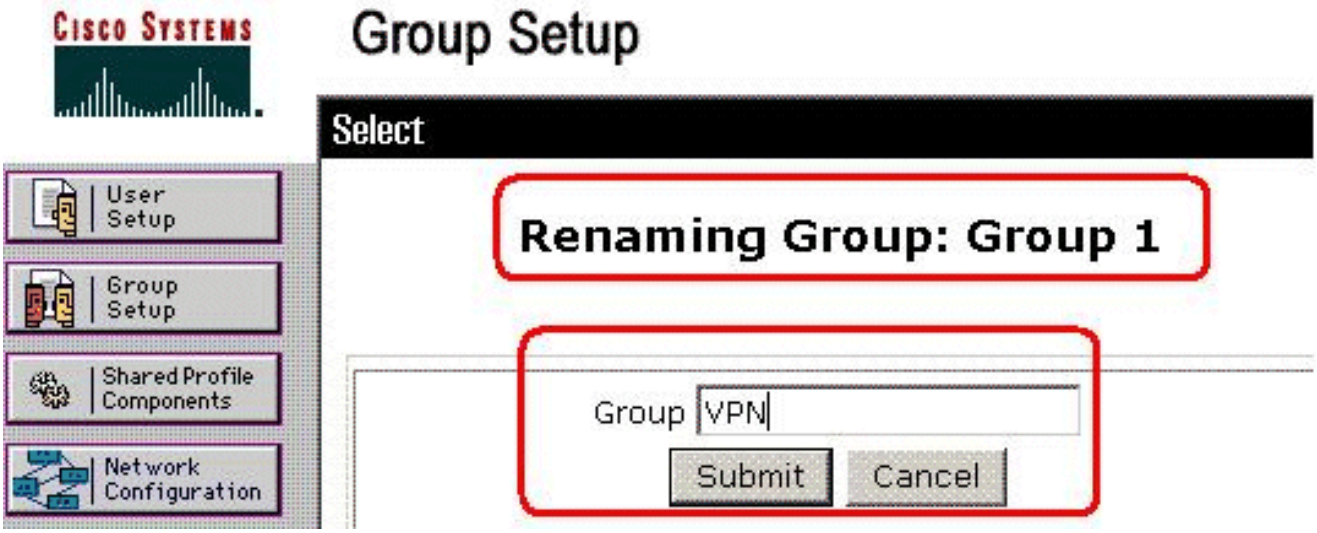
L'utente del gruppo VPN **"cisco"** esegue l'autenticazione e il server RADIUS invia un elenco degli accessi scaricabile all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione ACL scaricabili per utente/gruppo.

1. Nella barra di spostamento fare clic su **Imposta gruppo**. Viene visualizzata la pagina

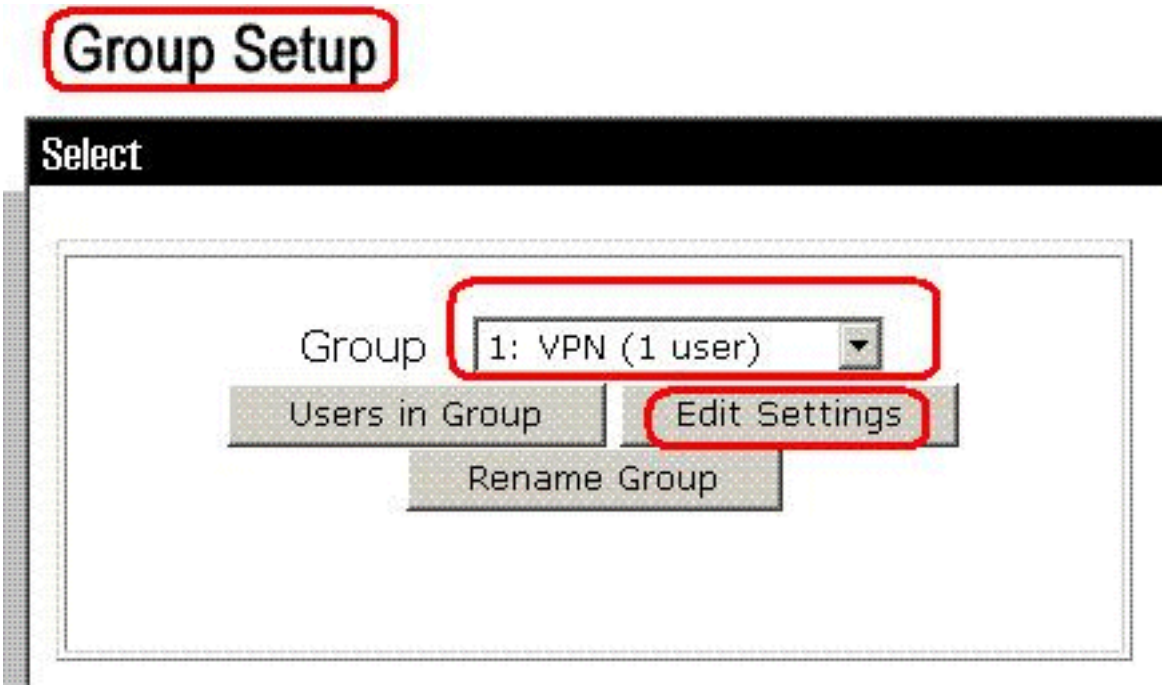
Selezione impostazione gruppo.



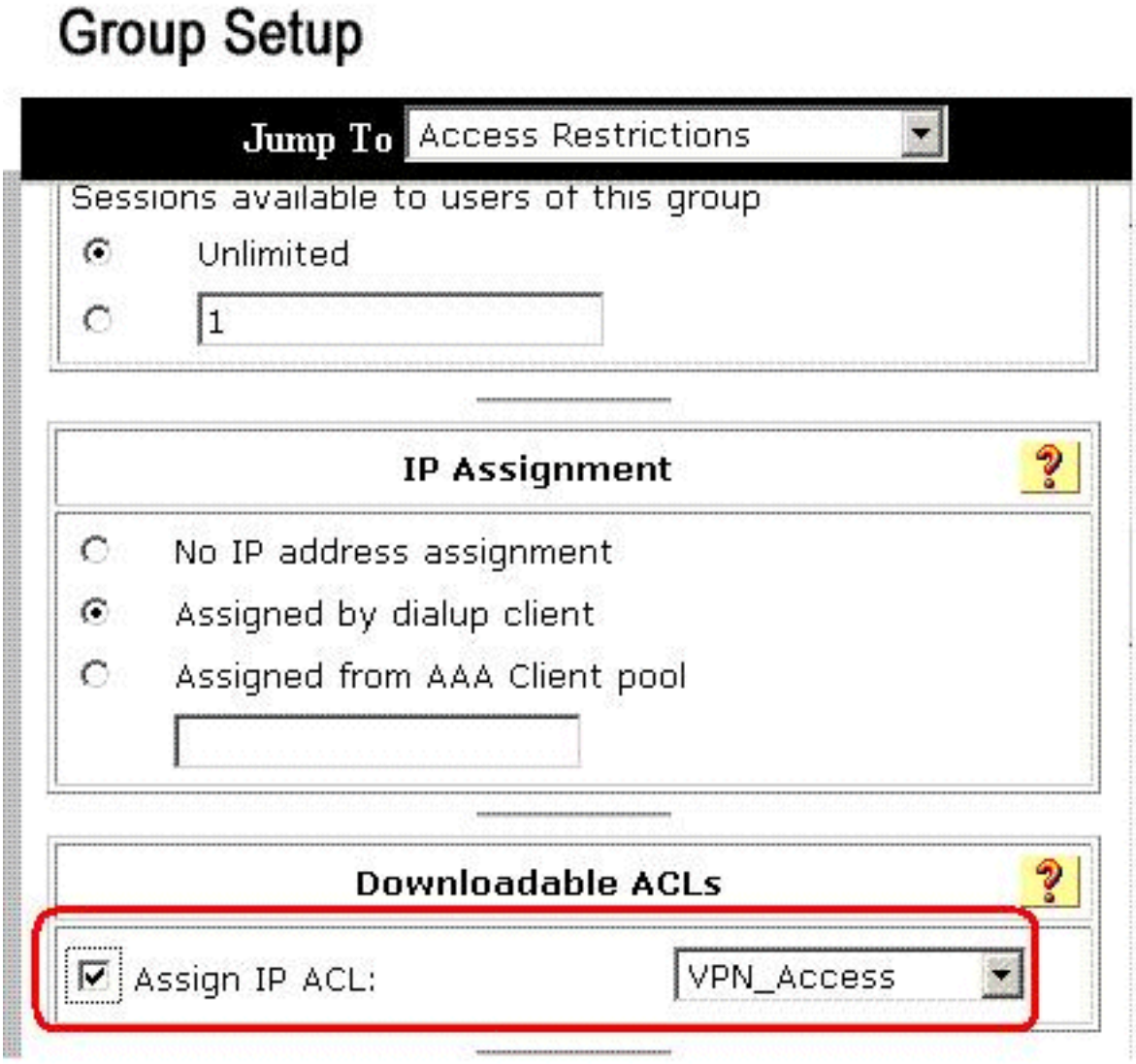
2. Rinominare il Gruppo 1 come **VPN** e fare clic su **Invia**.



3. Nell'elenco Gruppo scegliere un gruppo e quindi fare clic su **Modifica impostazioni**.

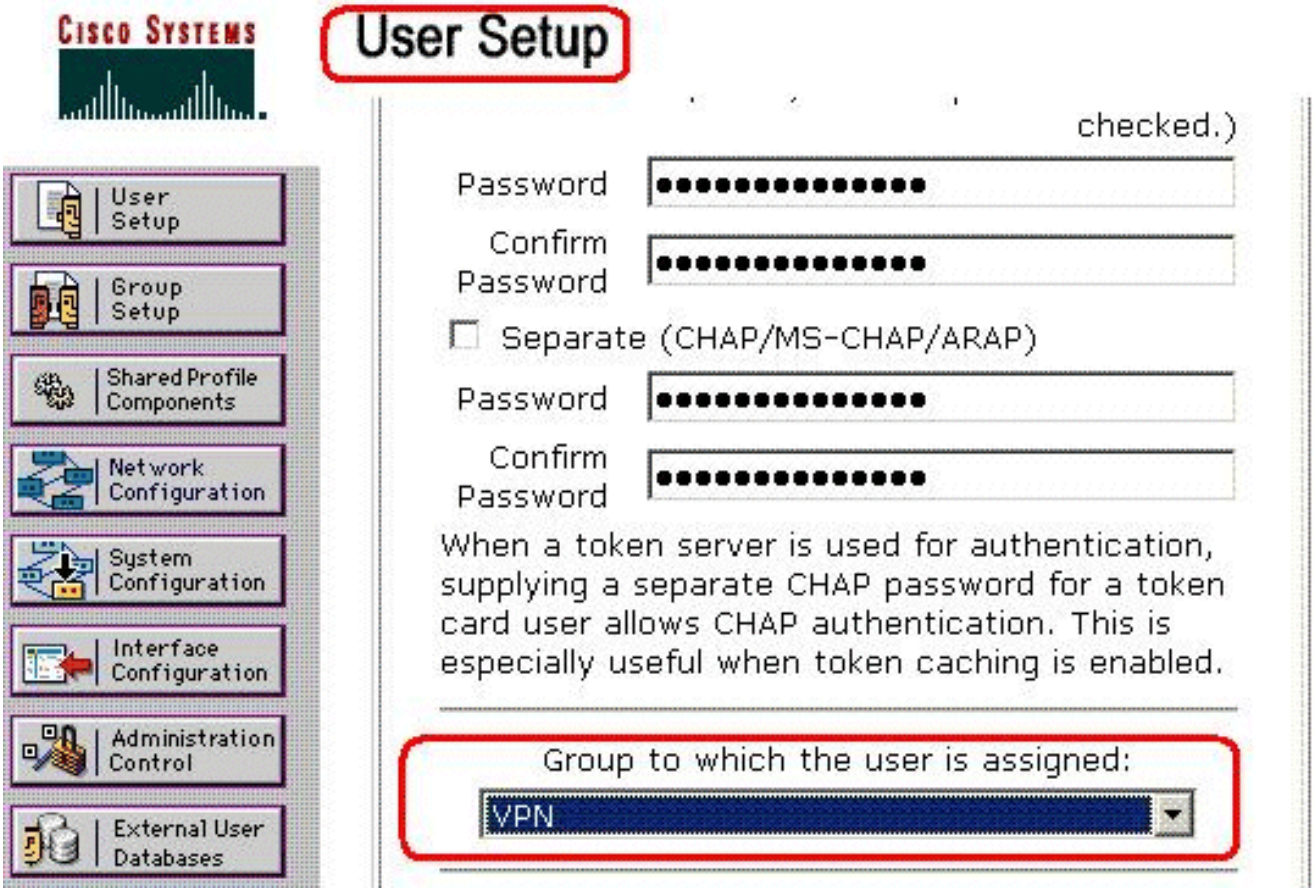


4. Nella sezione ACL scaricabili, selezionare la casella di controllo **Assegna ACL IP**. Selezionare un ACL IP dall'elenco.



5. Per salvare le impostazioni di gruppo appena definite, fare clic su **Invia**.
6. Andare alla finestra di dialogo Impostazione utente e modificare l'utente che si desidera

aggiungere al gruppo: **VPN**. Al termine, fare clic su **Invia**.



A questo punto, l'ACL scaricabile configurato per il gruppo VPN viene applicato per questo utente.

7. Per continuare a specificare altre impostazioni di gruppo, eseguire le procedure descritte in questo capitolo, se applicabili

Configurare le impostazioni RADIUS IETF per un gruppo di utenti

Per scaricare dal server RADIUS il nome di un elenco degli accessi già creato sull'accessorio di sicurezza durante l'autenticazione, configurare l'attributo IETF RADIUS filter-id (numero attributo 11) come segue:

```
filter-id=acl_name
```

L'utente del gruppo VPN **"cisco"** esegue l'autenticazione e il server RADIUS scarica un nome ACL (nuovo) per un elenco degli accessi già creato sull'appliance di sicurezza. L'utente "cisco" può accedere a tutti i dispositivi che si trovano all'interno della rete dell'ASA, **ad eccezione** del server 10.1.1.2. Per verificare l'ACL, consultare la sezione ACL Filter-Id.

Come mostrato nell'esempio, l'ACL con nome **new** è configurato per il filtro nell'appliance ASA.

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

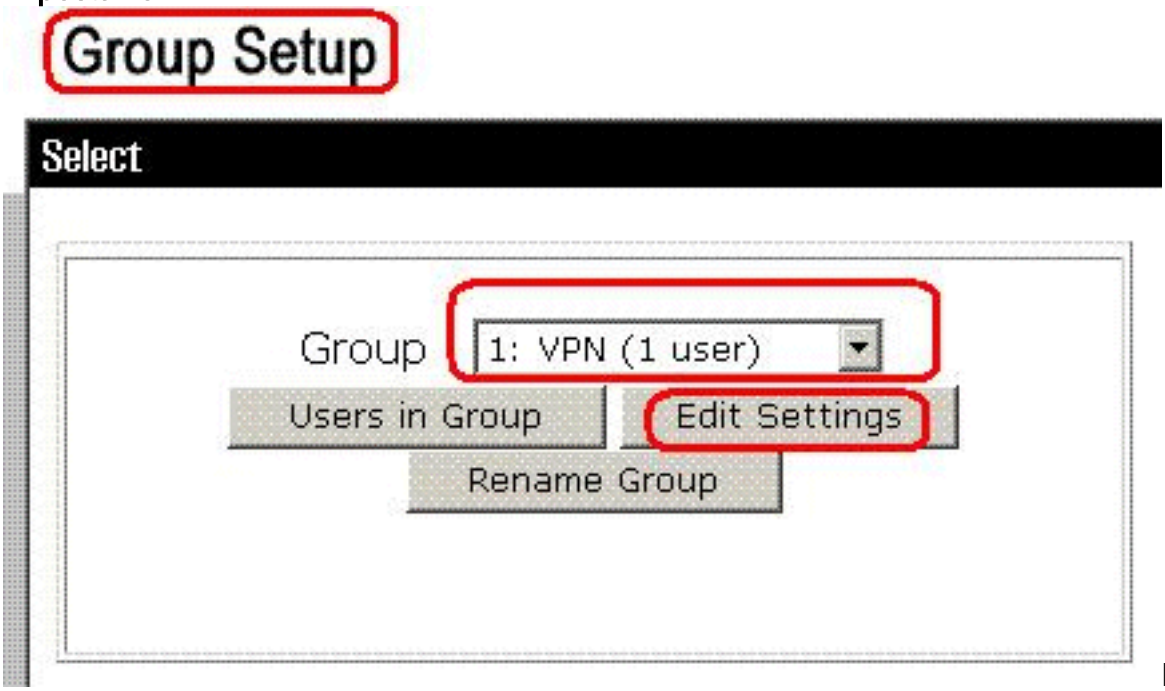
Questi parametri vengono visualizzati solo quando sono veri. È stato configurato

- Client AAA per utilizzare uno dei protocolli RADIUS in Configurazione rete
- Attributi RADIUS a livello di gruppo nella pagina RADIUS (IETF) della sezione Configurazione interfaccia dell'interfaccia Web

Gli attributi RADIUS vengono inviati come profilo per ogni utente da ACS al client AAA richiedente.

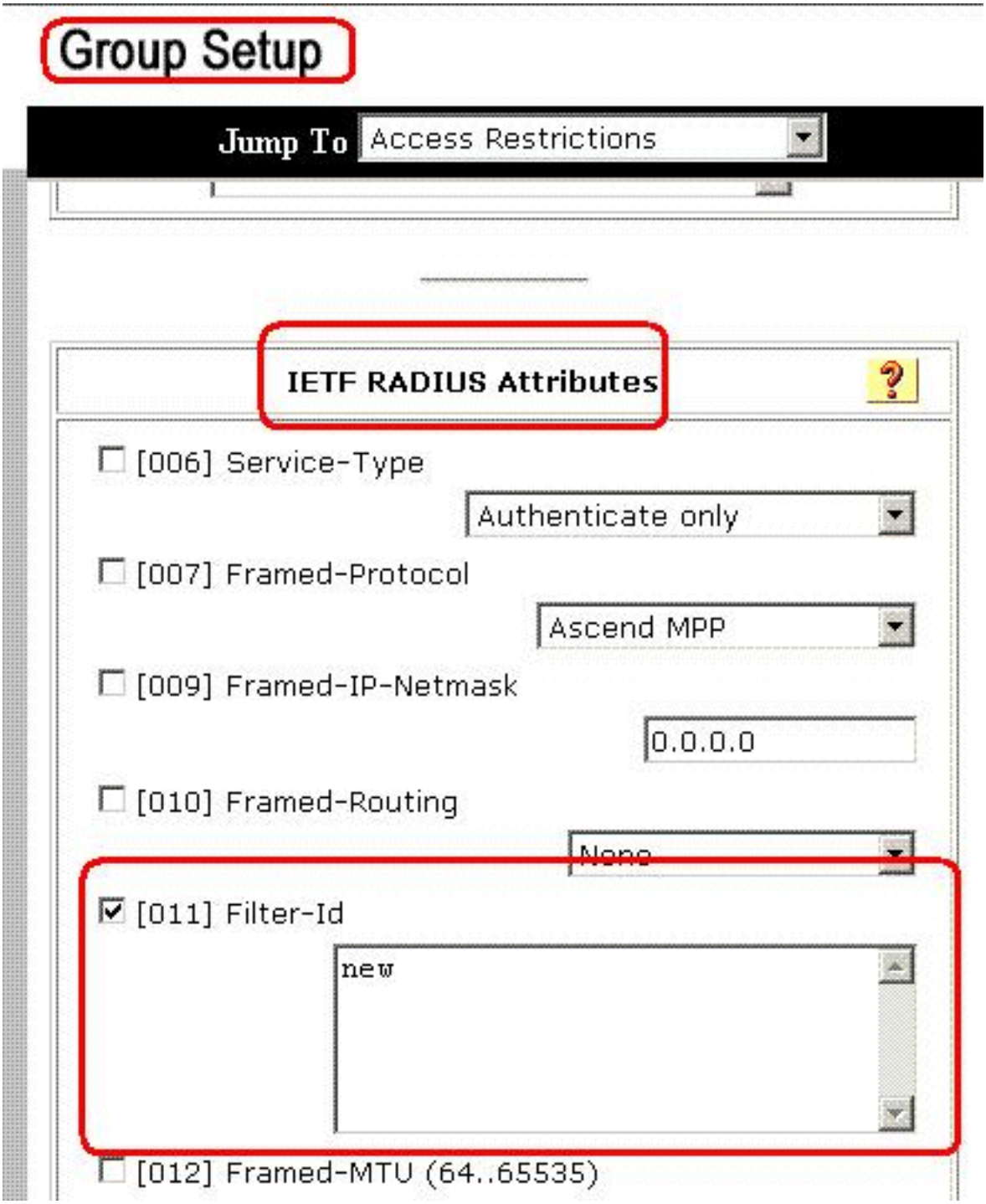
Per configurare le impostazioni degli attributi RADIUS IETF da applicare come autorizzazione per ogni utente del gruppo corrente, eseguire le azioni seguenti:

1. Nella barra di spostamento fare clic su **Imposta gruppo**.Viene visualizzata la pagina Selezione impostazione gruppo.
2. Nell'elenco Gruppo scegliere un gruppo e quindi fare clic su **Modifica impostazioni**.



Il nome del gruppo viene visualizzato nella parte superiore della pagina Impostazioni gruppo.

3. Scorrete fino agli attributi IEFT RADIUS. Per ogni attributo RADIUS IETF, è necessario autorizzare il gruppo corrente. Selezionare la casella di controllo dell'attributo **[011] Filter-Id**, quindi aggiungere il nome ACL definito dall'ASA (**new**) nell'autorizzazione dell'attributo nel campo. Fare riferimento all'output *del comando* ASA *show running configuration*.



4. Per salvare le impostazioni di gruppo appena definite e applicarle immediatamente, fare clic su **Invia** e **Applica**.**Nota:** per salvare le impostazioni del gruppo e applicarle in seguito, fare clic su **Invia**. Quando si è pronti per implementare le modifiche, scegliere **Configurazione di sistema > Controllo servizio**. Quindi scegliere **Riavvia**.

Verifica

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**.

Mostra comandi di crittografia

- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.

```
ciscoasa# sh crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active
   and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.10.2
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1,
   local addr: 192.168.1.1

      local ident (addr/mask/prot/port):
   (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
   (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.10.2, username: cisco
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 65, #pkts encrypt:
   65, #pkts digest: 65
      #pkts decaps: 65, #pkts decrypt:
   65, #pkts verify: 65
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed:
   0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures:
   0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0,
   #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.1,
   remote crypto endpt.: 192.168.10.2

      path mtu 1500, ipsec overhead 58,
   media mtu 1500
      current outbound spi: EEF0EC32

    inbound esp sas:
      spi: 0xA6F92298 (2801345176)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec):
   28647
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xEEF0EC32 (4008766514)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec): 28647
```

```
            IV size: 8 bytes
            replay detection support: Y
```

ACL scaricabile per utente/gruppo

Verificare l'ACL scaricabile per l'utente Cisco. Gli ACL vengono scaricati dai CSACS.

```
ciscoasa(config)# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
   192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411

access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
   ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
   ip any any (hitcnt=40) 0x7c718bd1
```

ACL Filter-Id

Il Filter-Id [011] è stato applicato al gruppo - VPN e gli utenti del gruppo sono filtrati in base all'ACL (nuovo) definito nell'ASA.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
   255.255.255.0 192.168.5.0 255.255.255.0
   (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip
   any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
   (hitcnt=39) 0x40e5d57c
```

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 alla VPN IPSec di accesso remoto, fare riferimento alle soluzioni per la risoluzione dei problemi relativi alla VPN IPSec di accesso remoto e all'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 Adaptive Security Device Manager
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Pagina di supporto per Cisco VPN Client
- Cisco Secure Access Control Server per Windows
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems