ASA/PIX 8.x: RADIUS Authorization (ACS 4.x) für VPN-Zugriff mit herunterladbarer ACL mit CLI und ASDM - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Sicherheits-Appliance so konfigurieren, dass Benutzer für den Netzwerkzugriff authentifiziert werden. Da RADIUS-Autorisierungen implizit aktiviert werden können, enthält dieser Abschnitt keine Informationen zur Konfiguration der RADIUS-Autorisierung auf der Sicherheits-Appliance. Sie enthält Informationen darüber, wie die Sicherheits-Appliance die von RADIUS-Servern empfangenen Zugriffslisteninformationen behandelt.

Sie können einen RADIUS-Server so konfigurieren, dass er zum Zeitpunkt der Authentifizierung eine Zugriffsliste zur Sicherheitsappliance oder einen Namen für die Zugriffsliste herunterlädt. Der

Benutzer ist berechtigt, nur die in der benutzerspezifischen Zugriffsliste zulässigen Aktionen auszuführen.

Zugriffslisten zum Herunterladen sind die skalierbarste Methode, wenn Sie Cisco Secure ACS verwenden, um für jeden Benutzer die entsprechenden Zugriffslisten bereitzustellen. Weitere Informationen zu herunterladbaren Zugriffslistenfunktionen und dem Cisco Secure ACS finden Sie unter Konfigurieren eines RADIUS-Servers zum Senden herunterladbarer Zugriffskontrolllisten und herunterladbarer IP-Zugriffskontrolllisten.

Weitere Informationen finden Sie unter ASA 8.3 und höher: RADIUS Authorization (ACS 5.x) für VPN-Zugriff mithilfe herunterladbarer ACL mit CLI- und ASDM-Konfigurationsbeispiel für die identische Konfiguration auf der Cisco ASA mit Version 8.3 und höher

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM oder die CLI Konfigurationsänderungen vornehmen können.

Hinweis: Weitere Informationen finden Sie unter Zulassen von HTTPS-Zugriff für ASDM oder PIX/ASA 7.x: SSH im Konfigurationsbeispiel für die Innen- und Außenschnittstelle, um die Remote-Konfiguration des Geräts durch den ASDM oder Secure Shell (SSH) zu ermöglichen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance Software Version 7.x oder höher
- Cisco Adaptive Security Device Manager Version 5.x und höher
- Cisco VPN Client Version 4.x und höher
- Cisco Secure Access Control Server 4.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX Security Appliance Version 7.x oder höher verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Sie können herunterladbare IP-ACLs verwenden, um Gruppen von ACL-Definitionen zu erstellen, die Sie auf viele Benutzer oder Benutzergruppen anwenden können. Diese Gruppen von ACL-Definitionen werden als ACL-Inhalt bezeichnet. Wenn Sie NAFs integrieren, steuern Sie außerdem die ACL-Inhalte, die an den AAA-Client gesendet werden, von dem ein Benutzer Zugriff anfordert. Das heißt, eine herunterladbare IP-ACL umfasst eine oder mehrere ACL-Inhaltsdefinitionen, die jeweils einem NAF oder (standardmäßig) allen AAA-Clients zugeordnet sind. Die NAF steuert die Anwendbarkeit des angegebenen ACL-Inhalts entsprechend der IP-Adresse des AAA-Clients. Weitere Informationen zu NAFs und zur Regulierung herunterladbarer IP-ACLs finden Sie unter Informationen zu Netzwerkzugriffsfiltern.

Herunterladbare IP-Zugriffskontrolllisten funktionieren folgendermaßen:

1. Wenn ACS einem Benutzer Zugriff auf das Netzwerk gewährt, bestimmt ACS, ob diesem Benutzer oder der Benutzergruppe eine herunterladbare IP-ACL zugewiesen wird.
2. Wenn der ACS eine herunterladbare IP-ACL sucht, die dem Benutzer oder der Benutzergruppe zugewiesen ist, bestimmt er, ob ein Eintrag zum ACL-Inhalt dem AAA-Client zugeordnet ist, der die RADIUS-Authentifizierungsanfrage gesendet hat.
3. ACS sendet im Rahmen der Benutzersitzung ein RADIUS-Access-Accept-Paket, ein Attribut, das die benannte ACL und die Version der benannten ACL angibt.
4. Wenn der AAA-Client antwortet, dass die aktuelle Version der ACL nicht im Cache enthalten ist, d. h. die ACL neu ist oder geändert wurde, sendet der ACS die ACL (neu oder aktualisiert) an das Gerät.

Herunterladbare IP-ACLs sind eine Alternative zur Konfiguration von ACLs im RADIUS Cisco cisco-av-pair-Attribut [26/9/1] jedes Benutzers oder jeder Benutzergruppe. Sie können eine herunterladbare IP-Zugriffskontrollliste einmal erstellen, ihr einen Namen geben und dann jedem beliebigen Benutzer oder jeder Benutzergruppe die herunterladbare IP-Zugriffskontrollliste zuweisen, wenn Sie auf den Namen des ACLs verweisen. Diese Methode ist effizienter, als wenn Sie das RADIUS Cisco cisco-av-pair-Attribut für jeden Benutzer oder jede Benutzergruppe konfigurieren.

Wenn Sie NAFs verwenden, können Sie darüber hinaus unterschiedliche ACL-Inhalte auf denselben Benutzer oder dieselbe Benutzergruppe in Bezug auf den von ihnen verwendeten AAA-Client anwenden. Nachdem Sie den AAA-Client für die Verwendung von herunterladbaren IP-ACLs aus dem ACS konfiguriert haben, ist keine zusätzliche Konfiguration des AAA-Clients erforderlich. Herunterladbare ACLs sind durch das Backup- oder Replikationsschema geschützt, das Sie eingerichtet haben.

Wenn Sie die ACL-Definitionen in die ACS-Webschnittstelle eingeben, dürfen Sie keine Schlüsselwort- oder Namenseinträge verwenden. In allen anderen Aspekten sollten die standardmäßige Befehlssyntax und Semantik für die ACL für den AAA-Client verwendet werden, auf den die herunterladbare IP-ACL angewendet werden soll. Die ACL-Definitionen, die Sie in den ACS eingeben, umfassen einen oder mehrere ACL-Befehle. Jeder ACL-Befehl muss in einer separaten Zeile stehen.

Sie können einer herunterladbaren IP-ACL einen oder mehrere benannte ACL-Inhalte hinzufügen. Standardmäßig gilt jeder ACL-Inhalt für alle AAA-Clients. Wenn Sie jedoch NAFs definiert haben, können Sie die Anwendbarkeit jedes ACL-Inhalts auf die AAA-Clients beschränken, die in der NAF aufgeführt sind, der Sie zugeordnet haben. Wenn Sie also NAFs verwenden, können Sie alle ACL-Inhalte innerhalb einer einzigen herunterladbaren IP-Zugriffskontrollliste entsprechend Ihrer Netzwerksicherheitsstrategie auf mehrere verschiedene Netzwerkgeräte oder Netzwerkgerätegruppen anwenden.

Außerdem können Sie die Reihenfolge der ACL-Inhalte in einer herunterladbaren IP-Zugriffskontrollliste ändern. ACS überprüft die ACL-Inhalte, beginnend mit der Tabellenüberschrift, und lädt den ersten von ihr gefundenen ACL-Inhalt mit einem NAF herunter, der den verwendeten AAA-Client enthält. Wenn Sie die Bestellung festlegen, können Sie die Systemeffizienz sicherstellen, wenn Sie den am häufigsten verwendeten ACL-Inhalt höher in der Liste positionieren. Sie müssen sich darüber im Klaren sein, dass, wenn Ihre NAFs eine Population von AAA-Clients enthalten, die sich überschneiden, Sie von der spezifischeren zu der allgemeineren weitergehen müssen. Beispielsweise lädt ACS alle ACL-Inhalte mit der NAF-Einstellung All-AAA-Clients herunter und berücksichtigt keine Inhalte, die in der Liste unten aufgeführt sind.

Um eine herunterladbare IP-ACL auf einem bestimmten AAA-Client zu verwenden, muss der AAA-Client die folgenden Anweisungen befolgen:

- RADIUS für Authentifizierung verwenden
- Unterstützung von herunterladbaren IP-Zugriffskontrolllisten

Beispiele für Cisco Geräte, die herunterladbare IP-Zugriffskontrolllisten unterstützen:

- ASA- und PIX-Geräte
- VPN Concentrators der Serie 3000
- Cisco Geräte, die IOS Version 12.3(8)T oder höher ausführen

Dies ist ein Beispiel für das Format, das Sie verwenden müssen, um im Feld ACL Definitions (ACL-Definitionen) VPN 3000/ASA/PIX 7.x+-ACLs einzugeben:

```
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
```

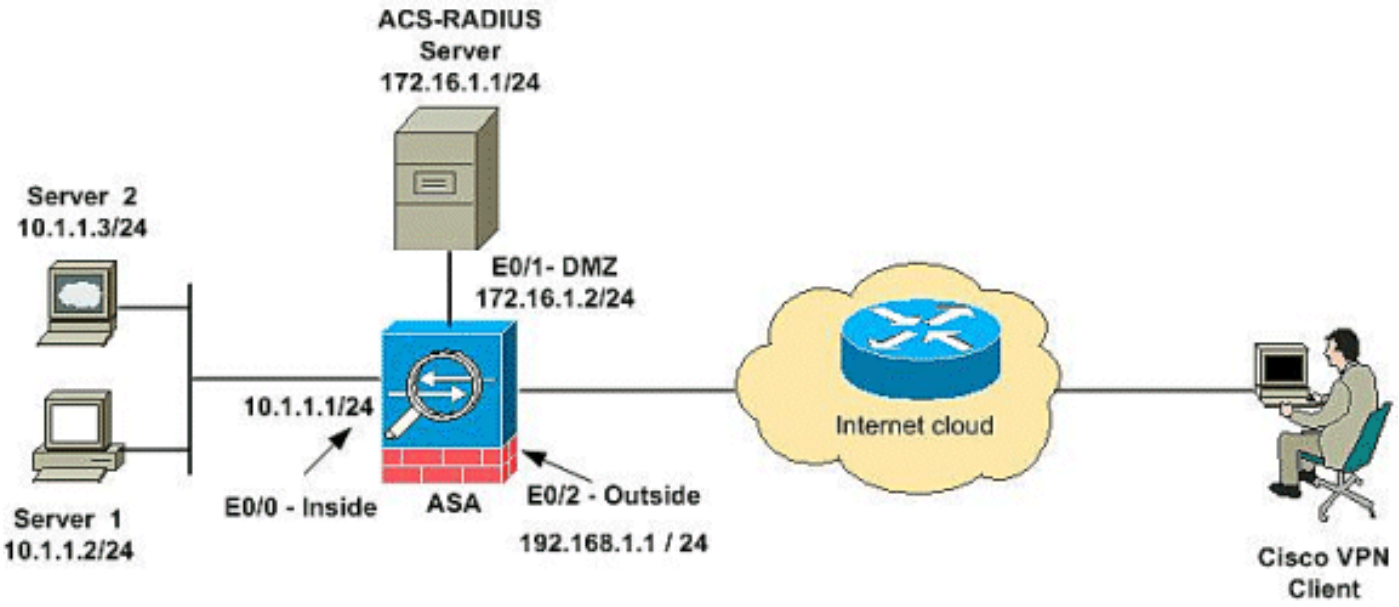
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



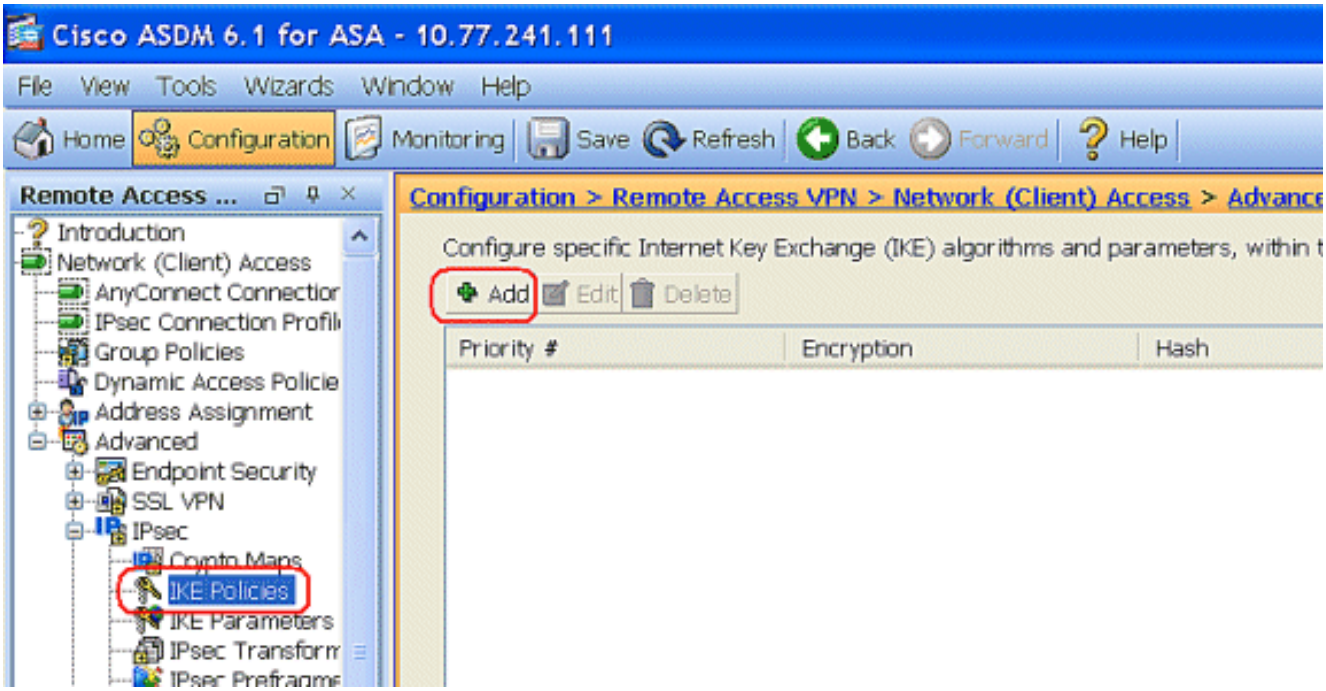
Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurieren von Remote Access VPN (IPSec)

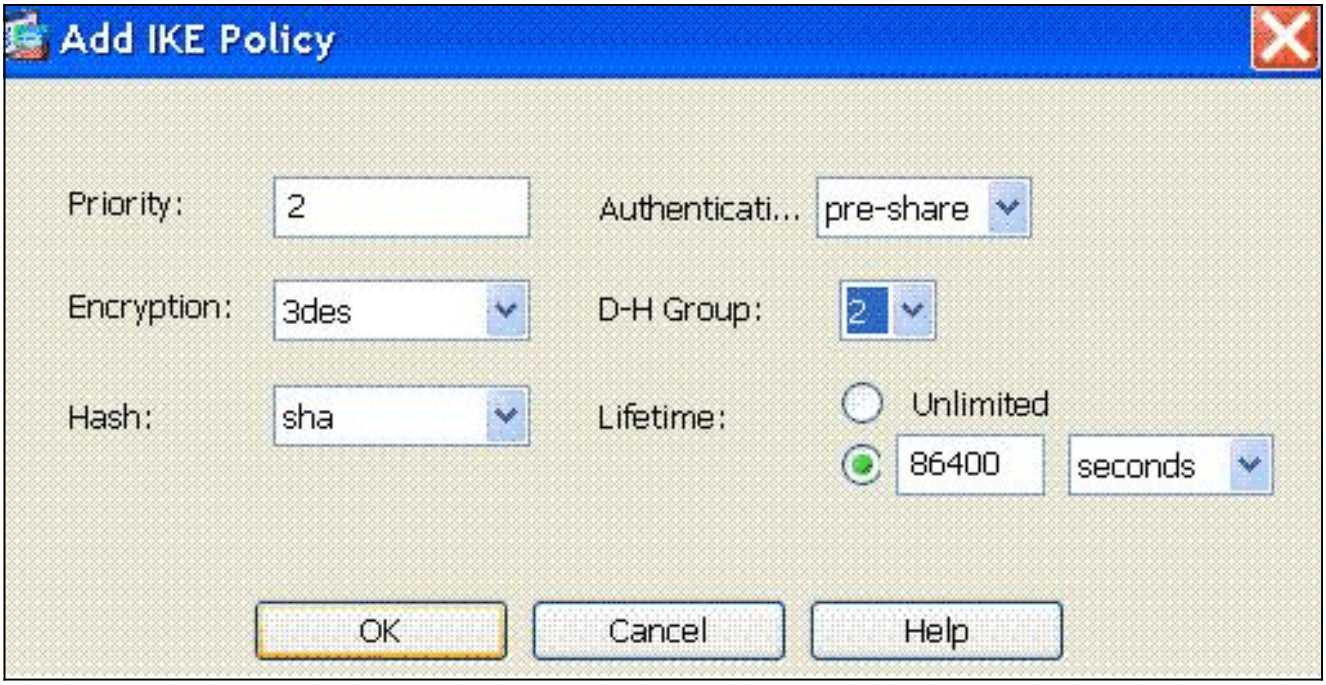
ASDM-Verfahren

Gehen Sie wie folgt vor, um das VPN für den Remote-Zugriff zu konfigurieren:

1. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add**, um eine ISAKMP-Richtlinie zu erstellen.

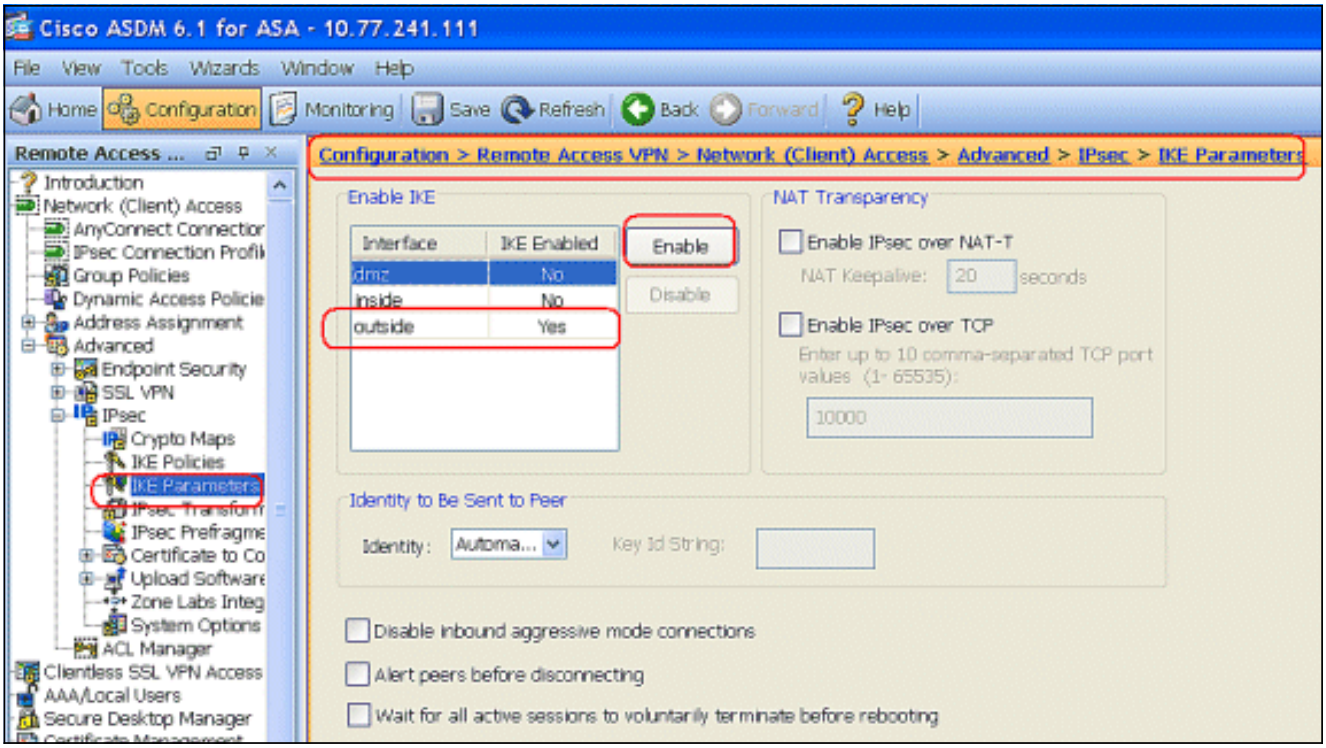


2. Geben Sie die ISAKMP-Richtliniendetails wie gezeigt ein.

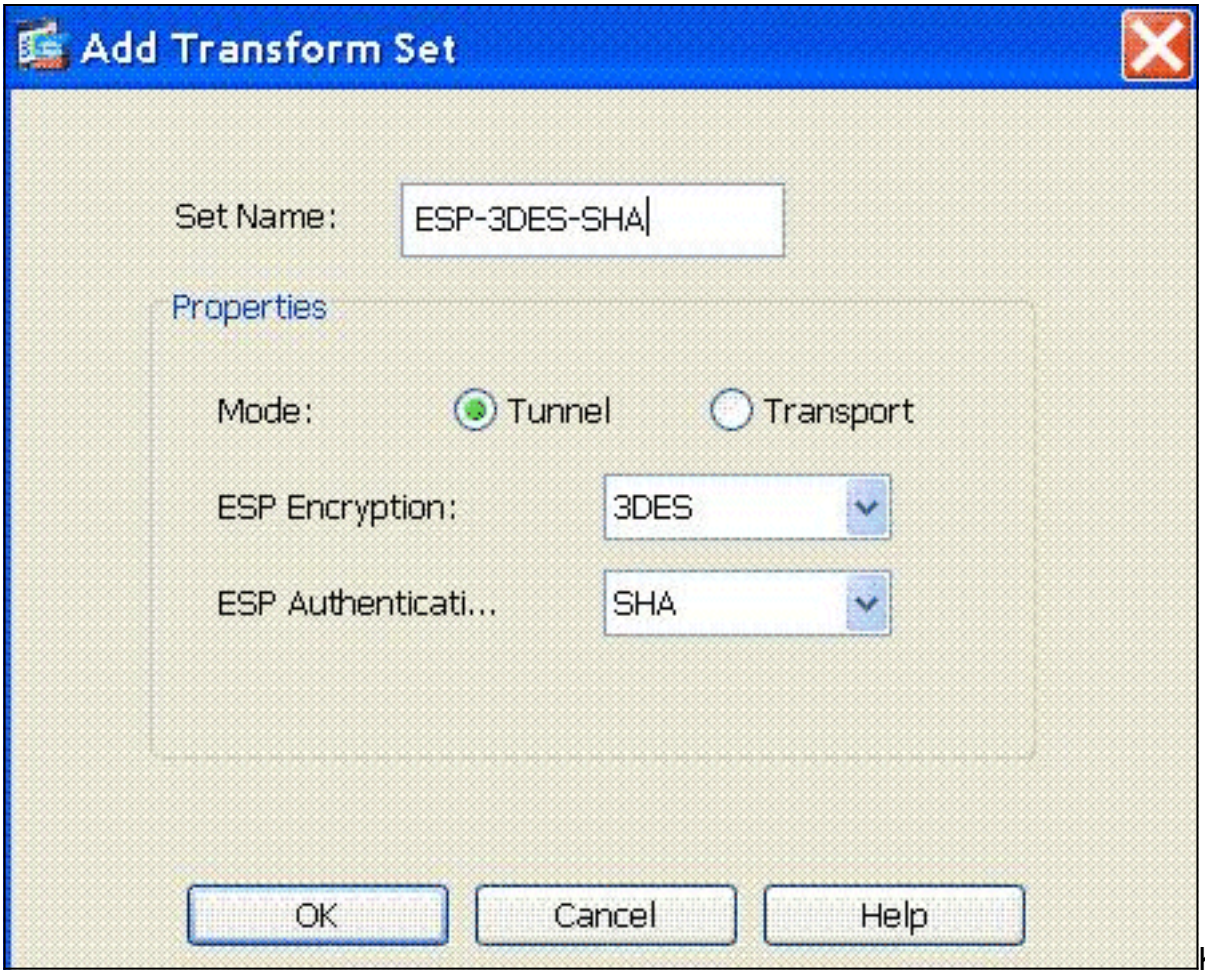


Klicken Sie auf **OK** und **Übernehmen**.

3. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Parameters** aus, um IKE auf der externen Schnittstelle zu aktivieren.

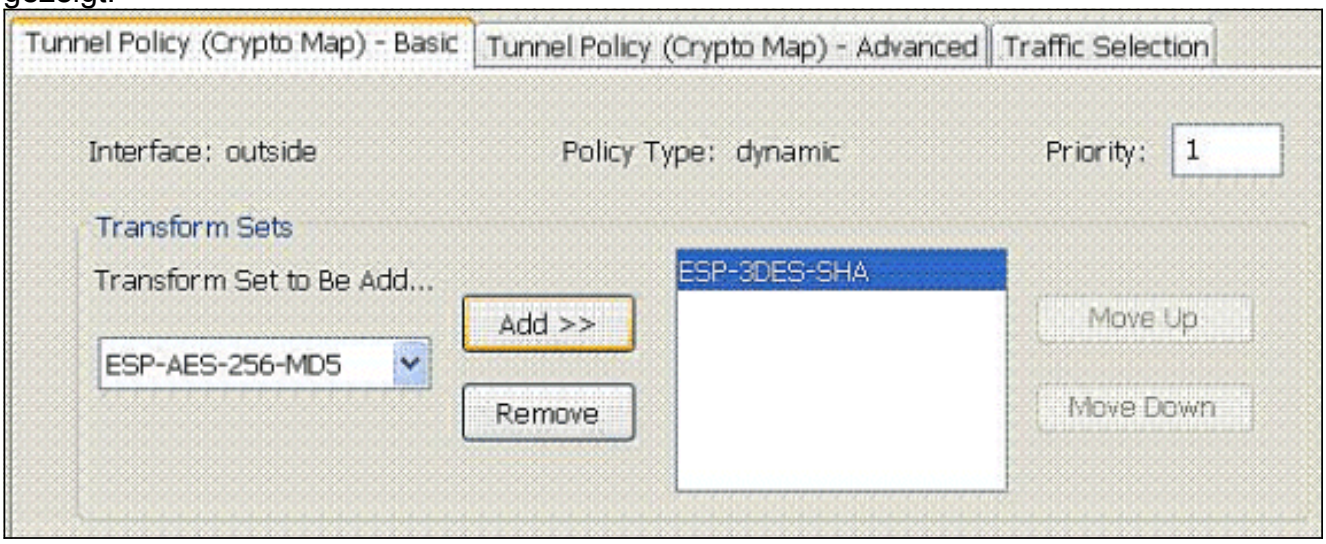


4. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add** aus, um den **ESP-3DES-SHA**-Transformationssatz zu erstellen, wie dargestellt.



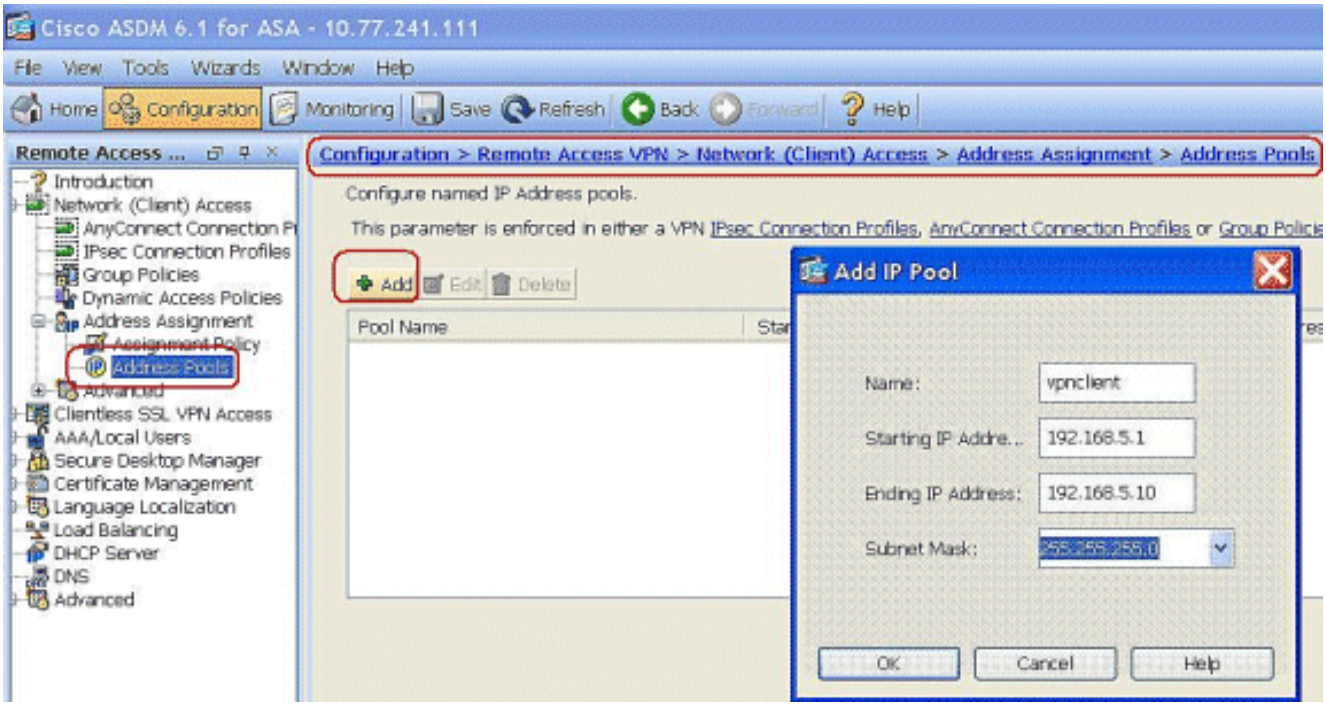
Klicken Sie auf **OK** und **Übernehmen**.

5. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add** aus, um eine Crypto Map mit dynamischer Richtlinie der Priorität 1 zu erstellen, wie gezeigt.

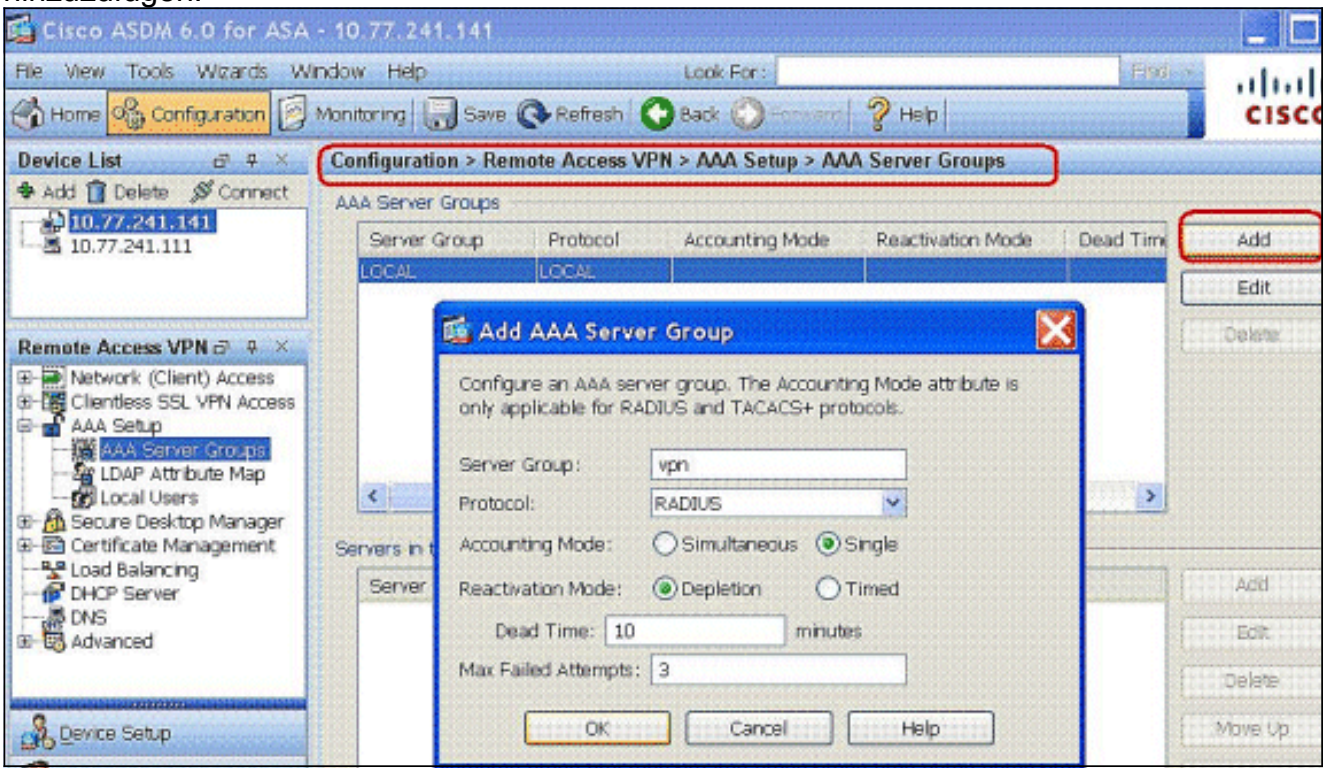


Klicken Sie auf **OK** und **Übernehmen**.

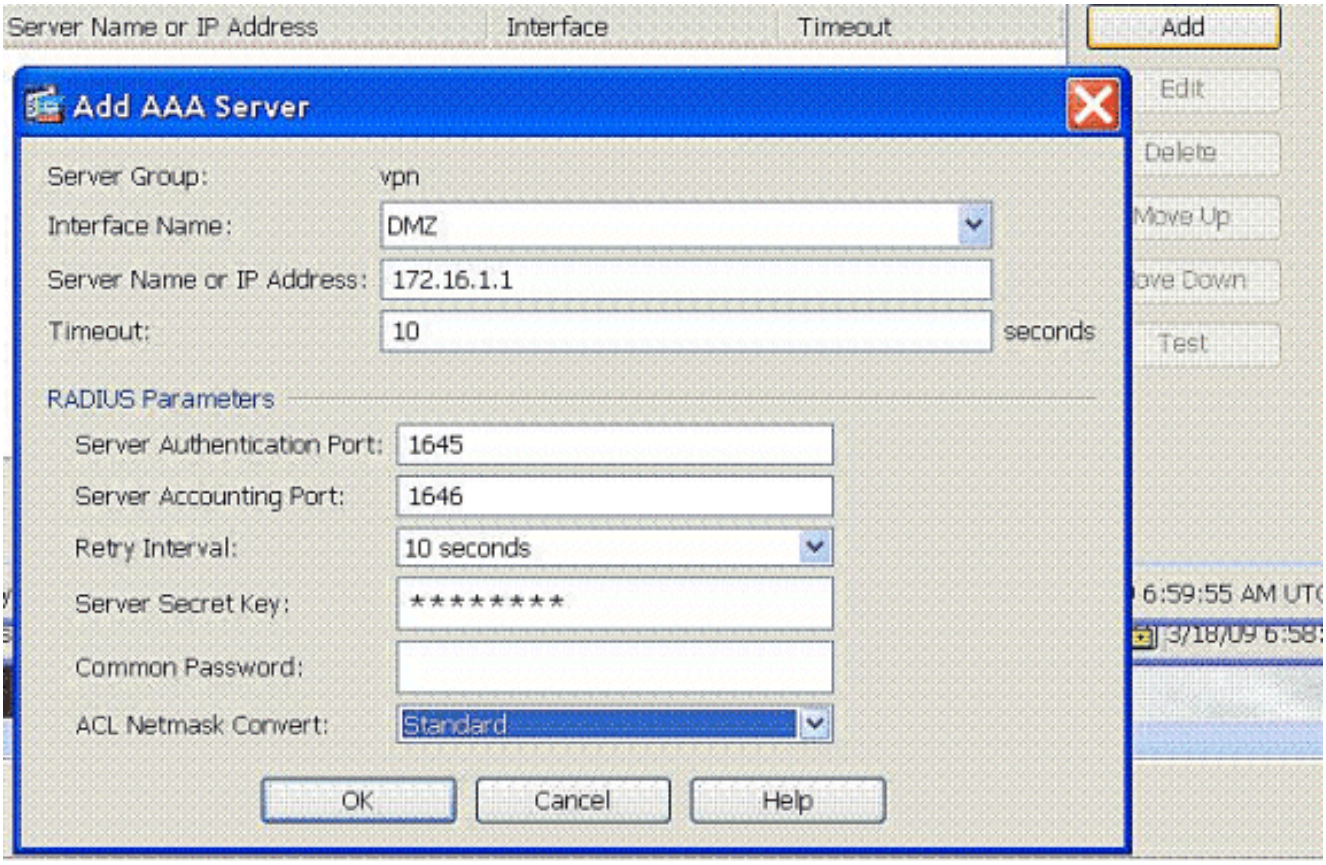
6. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools aus,** und klicken Sie auf **Add**, um den VPN Client für die VPN Client-Benutzer hinzuzufügen.



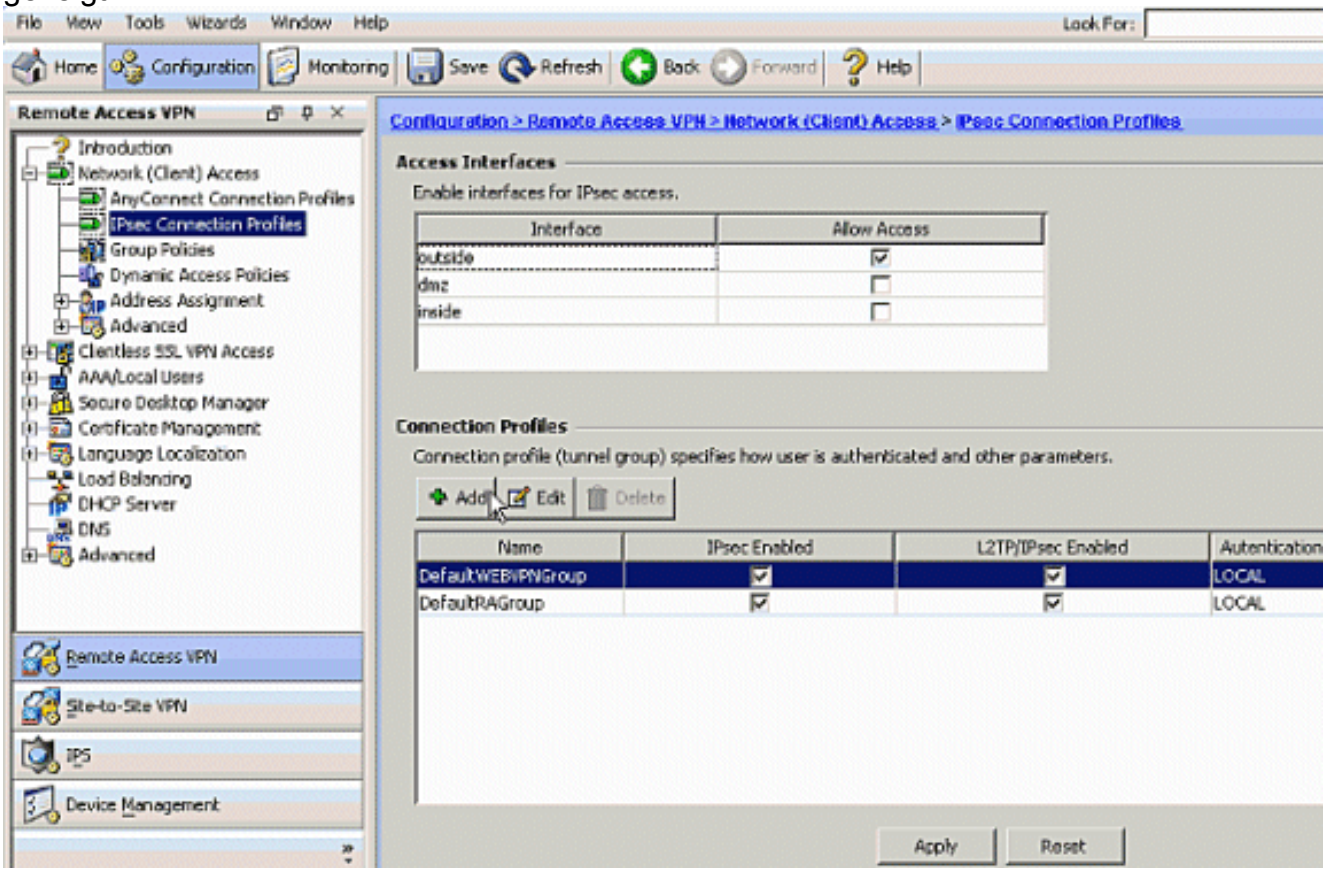
7. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups aus,** und klicken Sie auf **Add**, um den Namen und das Protokoll der AAA-Servergruppe hinzuzufügen.



Fügen Sie die AAA-Server-IP-Adresse (ACS) und die Schnittstelle hinzu, mit der die Verbindung hergestellt wird. Fügen Sie außerdem im Bereich RADIUS Parameters (RADIUS-Parameter) den Schlüssel Server Secret (Servergeheimnis) hinzu. Klicken Sie auf **OK**.

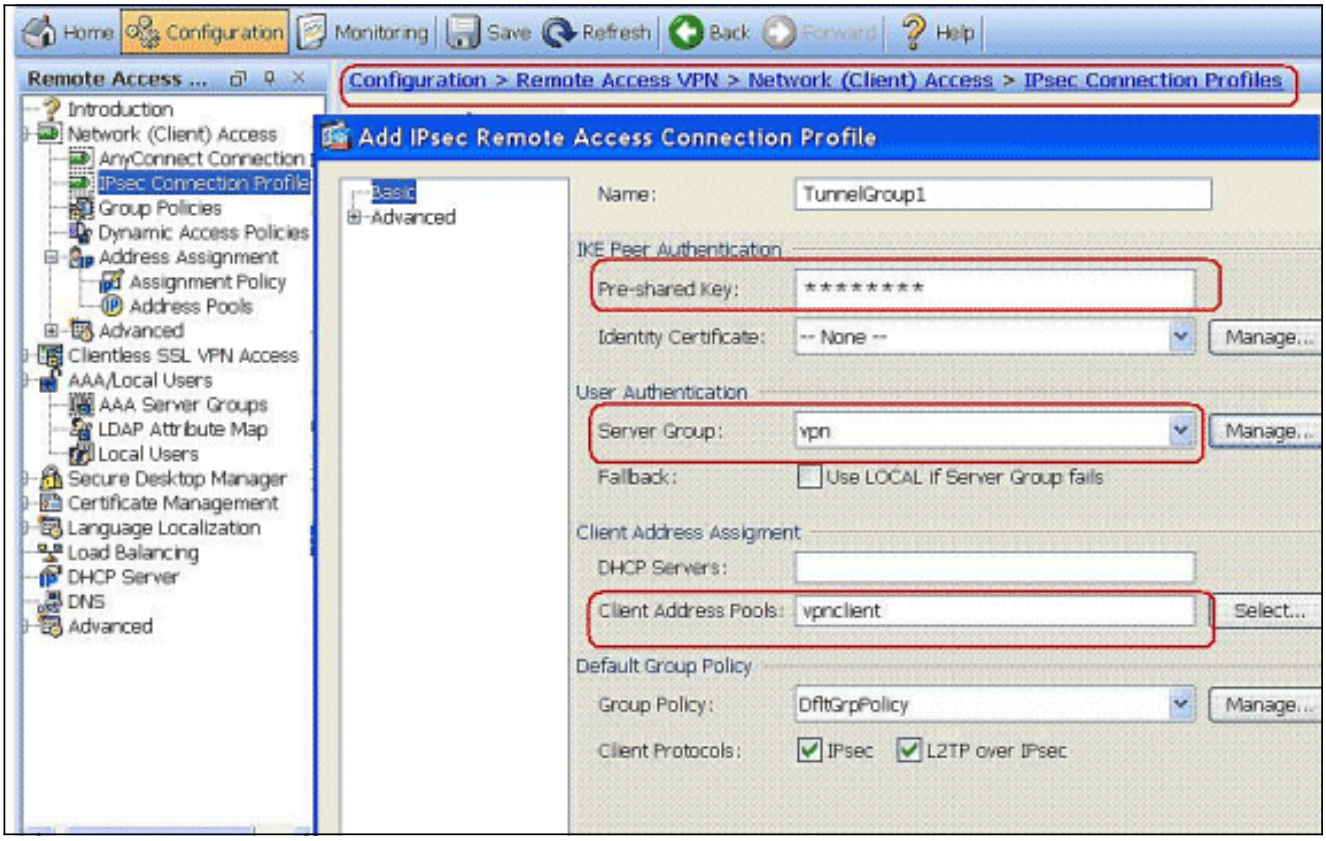


8. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Add** aus, um eine Tunnelgruppe hinzuzufügen, z. B. **TunnelGroup1** und den Preshared Key wie cisco123, wie gezeigt.



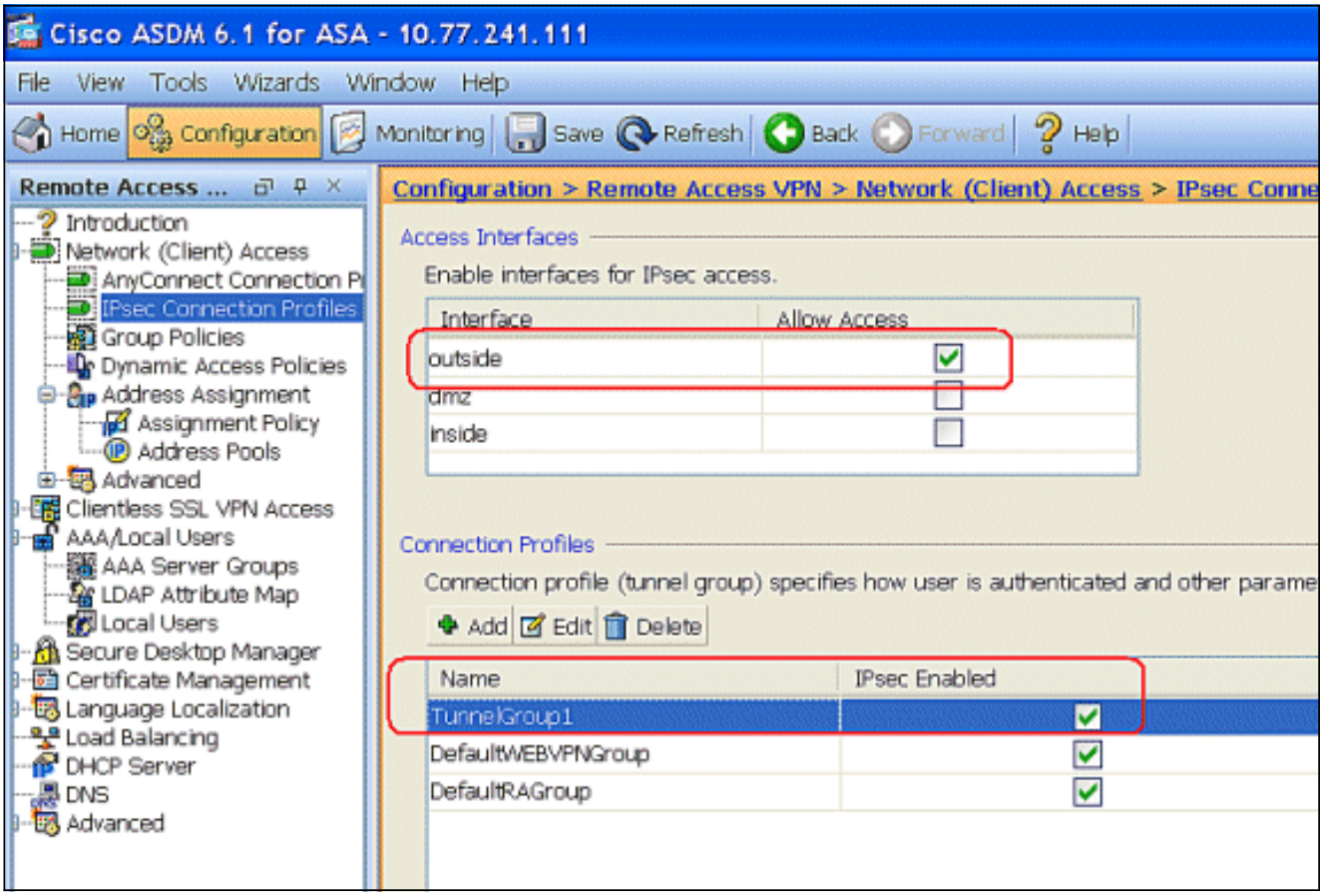
Wählen Sie auf der Registerkarte Basic (Grundlegend) die Servergruppe als **VPN** für das Feld User Authentication (Benutzerauthentifizierung) aus.Wählen Sie **vpnclient** als Client-Adresspools für die VPN-Client-Benutzer

aus.



Klicken Sie auf **OK**.

9. Aktivieren Sie die externe Schnittstelle für IPSec Access. Klicken Sie auf **Apply**, um fortzufahren.



Konfigurieren von ASA/PIX mit CLI

Führen Sie diese Schritte aus, um den DHCP-Server so zu konfigurieren, dass den VPN-Clients über die Befehlszeile IP-Adressen bereitgestellt werden. Weitere Informationen zu den jeweils verwendeten Befehlen finden Sie unter Konfigurieren von Remote Access VPNs oder Cisco Adaptive Security Appliances der Serie ASA 5500 - Befehlsreferenzen für die Cisco Adaptive Security Appliances der Serie 5500.

Ausführen der Konfiguration auf dem ASA-Gerät

```
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
```

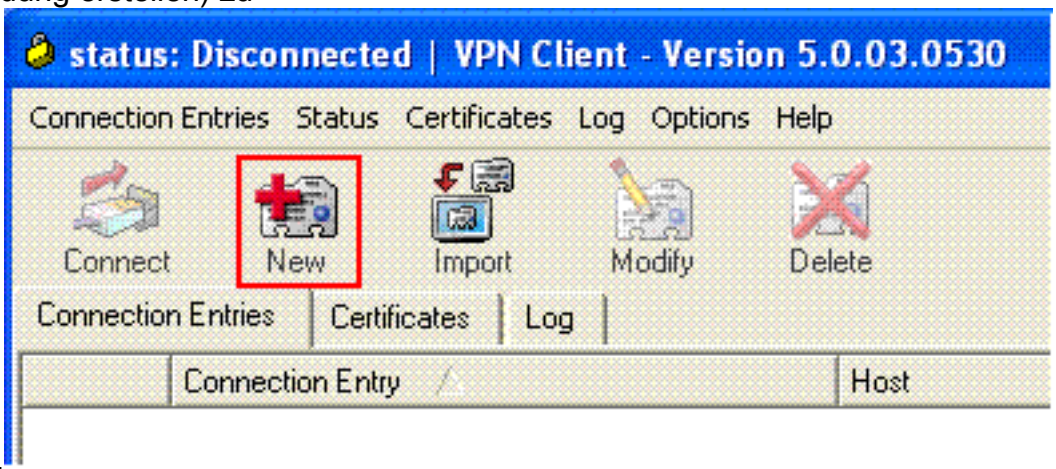
```
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
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#
```

Konfiguration des Cisco VPN-Clients

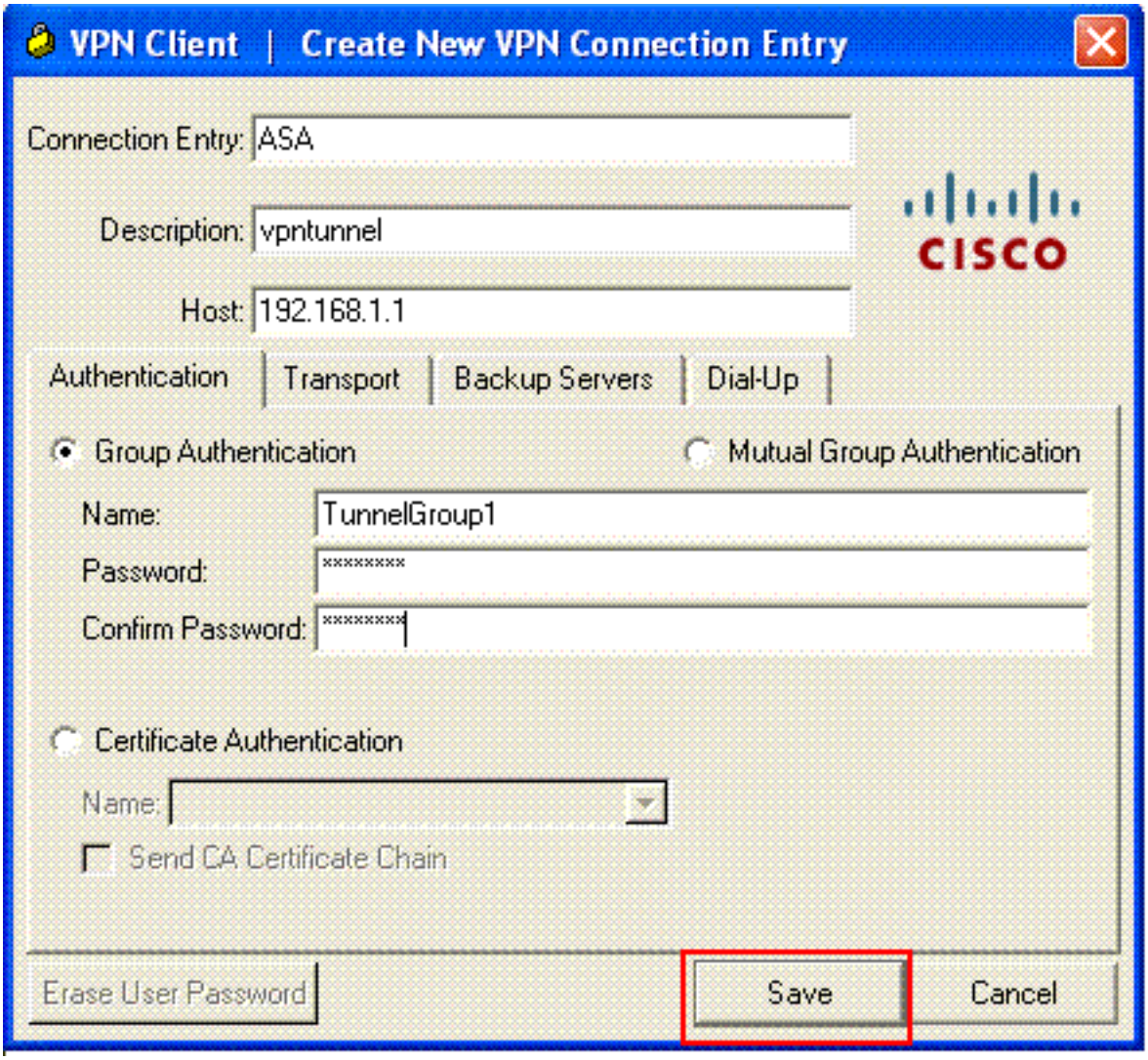
Versuchen Sie, mit dem Cisco VPN-Client eine Verbindung zur Cisco ASA herzustellen, um zu überprüfen, ob die ASA erfolgreich konfiguriert wurde.

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client aus**.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu

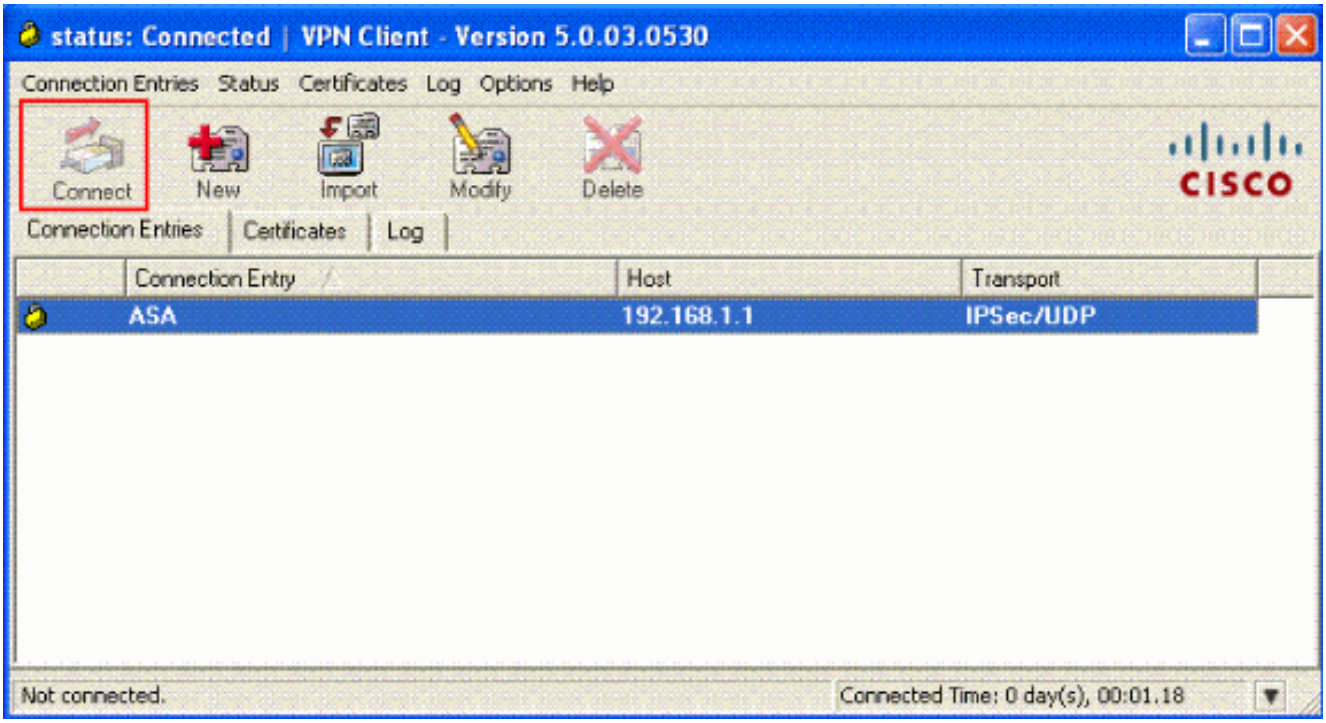


öffnen.

3. Füllen Sie die Details Ihrer neuen Verbindung aus.Geben Sie den Namen des Verbindungseintrags und eine Beschreibung ein. Geben Sie die **externe IP-Adresse der ASA** im Host-Feld ein. Geben Sie dann den VPN-Tunnel-Gruppennamen (TunnelGroup1) und das Kennwort (Pre-shared Key - cisco123) wie in ASA konfiguriert ein. Klicken Sie auf **Speichern**.

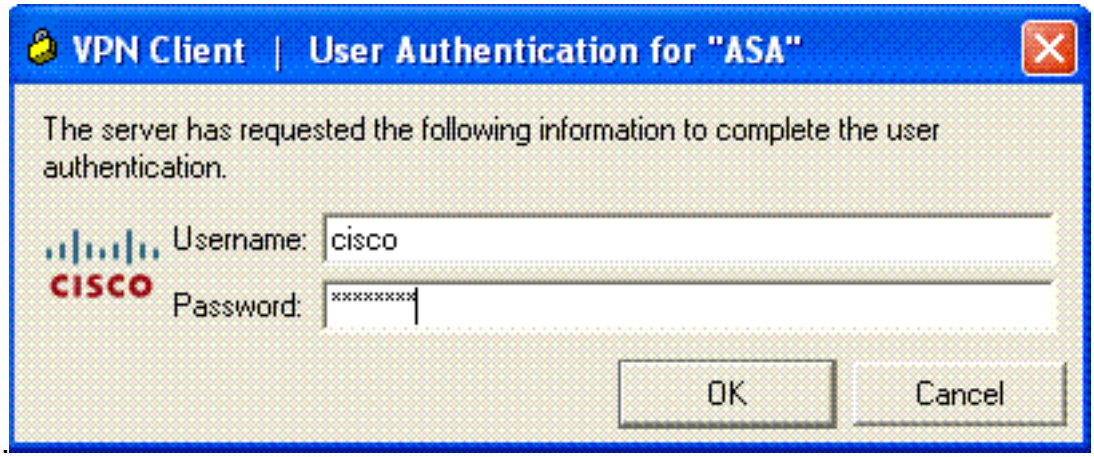


4. Klicken Sie auf die Verbindung, die Sie verwenden möchten, und klicken Sie im Hauptfenster des VPN-Clients auf **Verbinden**.

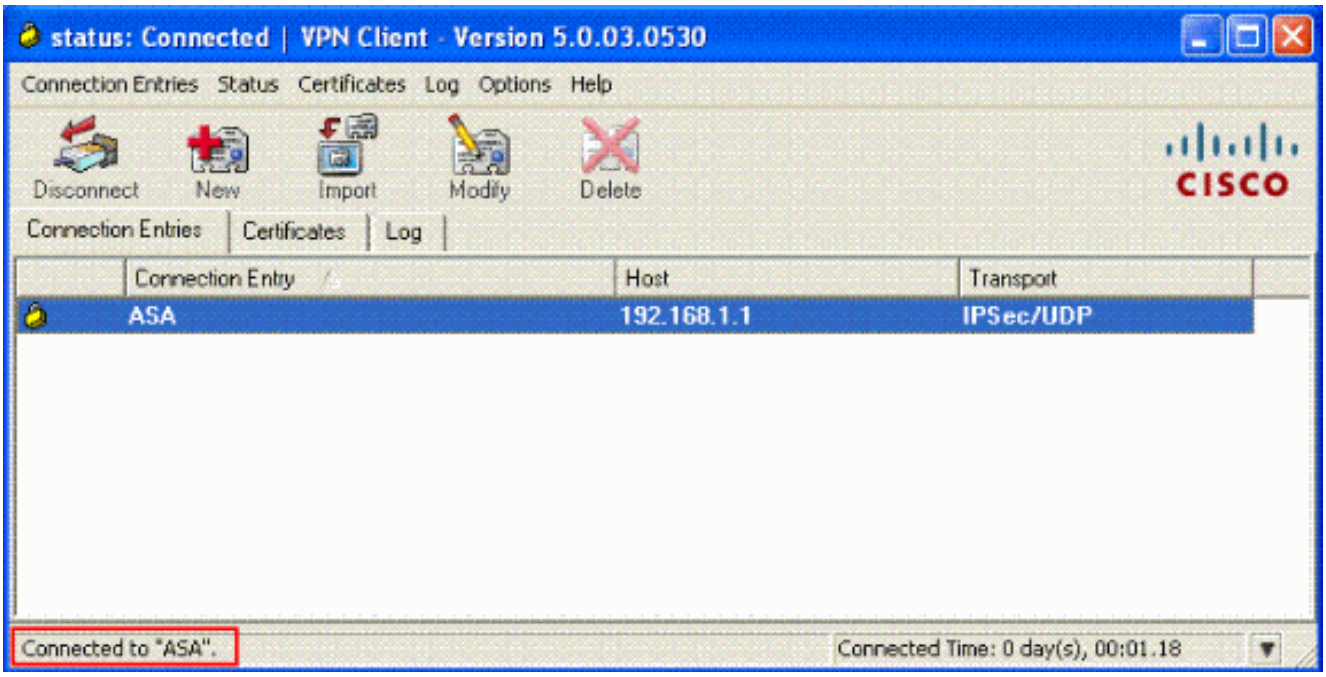


5. Geben Sie bei Aufforderung den **Benutzernamen ein: cisco** und **kennwort: password1** wie in der ASA für xauth konfiguriert, und klicken Sie auf **OK**, um eine Verbindung zum Remote-

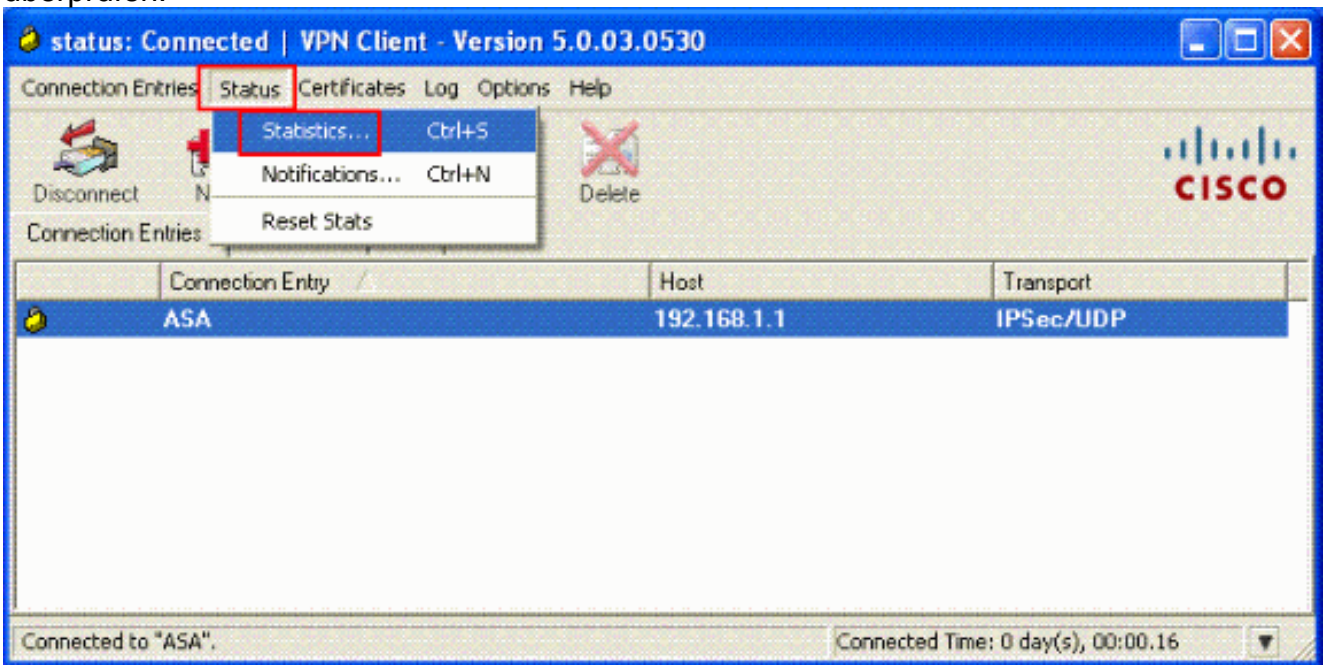
Netzwerk herzustellen.



6. Der VPN-Client ist mit der ASA in der Zentrale verbunden.



7. Wenn die Verbindung erfolgreich hergestellt wurde, wählen Sie im Menü Status die Option **Statistik**, um die Details des Tunnels zu überprüfen.



ACS für herunterladbare ACL für individuelle Benutzer konfigurieren

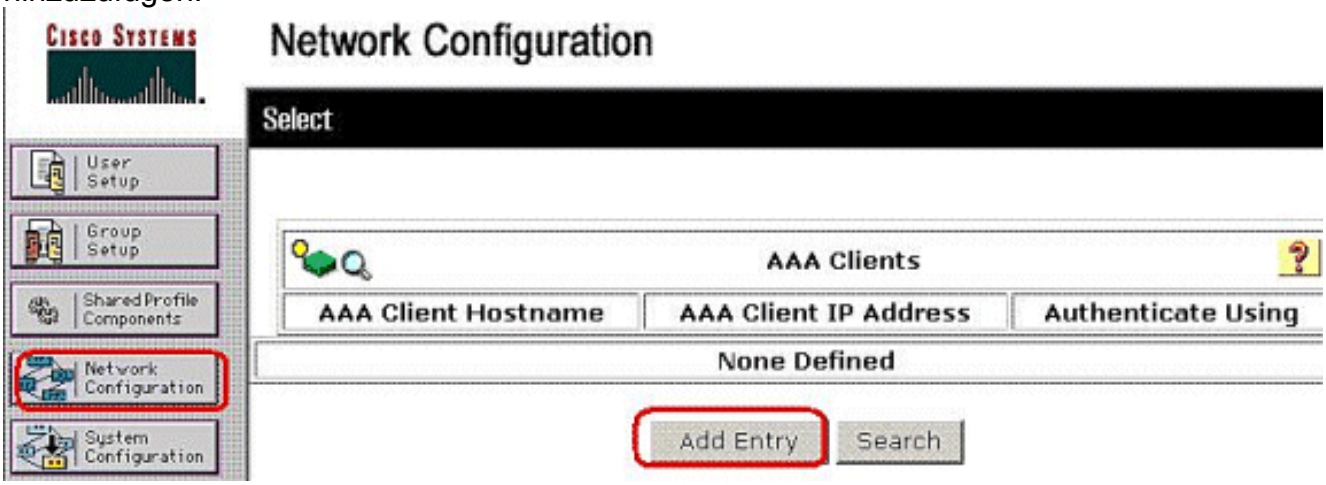
Sie können herunterladbare Zugriffslisten auf Cisco Secure ACS als Komponente für gemeinsam genutzte Profile konfigurieren und diese dann einer Gruppe oder einem einzelnen Benutzer zuweisen.

Um dynamische Zugriffslisten zu implementieren, müssen Sie den RADIUS-Server so konfigurieren, dass dieser unterstützt wird. Bei der Benutzerauthentifizierung sendet der RADIUS-Server eine herunterladbare Zugriffsliste oder einen Namen für die Zugriffsliste an die Sicherheits-Appliance. Der Zugriff auf einen bestimmten Service wird entweder durch die Zugriffsliste zugelassen oder verweigert. Die Sicherheits-Appliance löscht die Zugriffsliste, wenn die Authentifizierungssitzung abläuft.

In diesem Beispiel authentifiziert sich der IPSec VPN-Benutzer **"cisco"** erfolgreich, und der RADIUS-Server sendet eine herunterladbare Zugriffsliste an die Sicherheits-Appliance. Der Benutzer "cisco" kann nur auf den Server 10.1.1.2 zugreifen und verweigert allen anderen Zugriff. Informationen zur Verifizierung der ACL finden Sie im Abschnitt "Herunterladbare ACL für Benutzer/Gruppe".

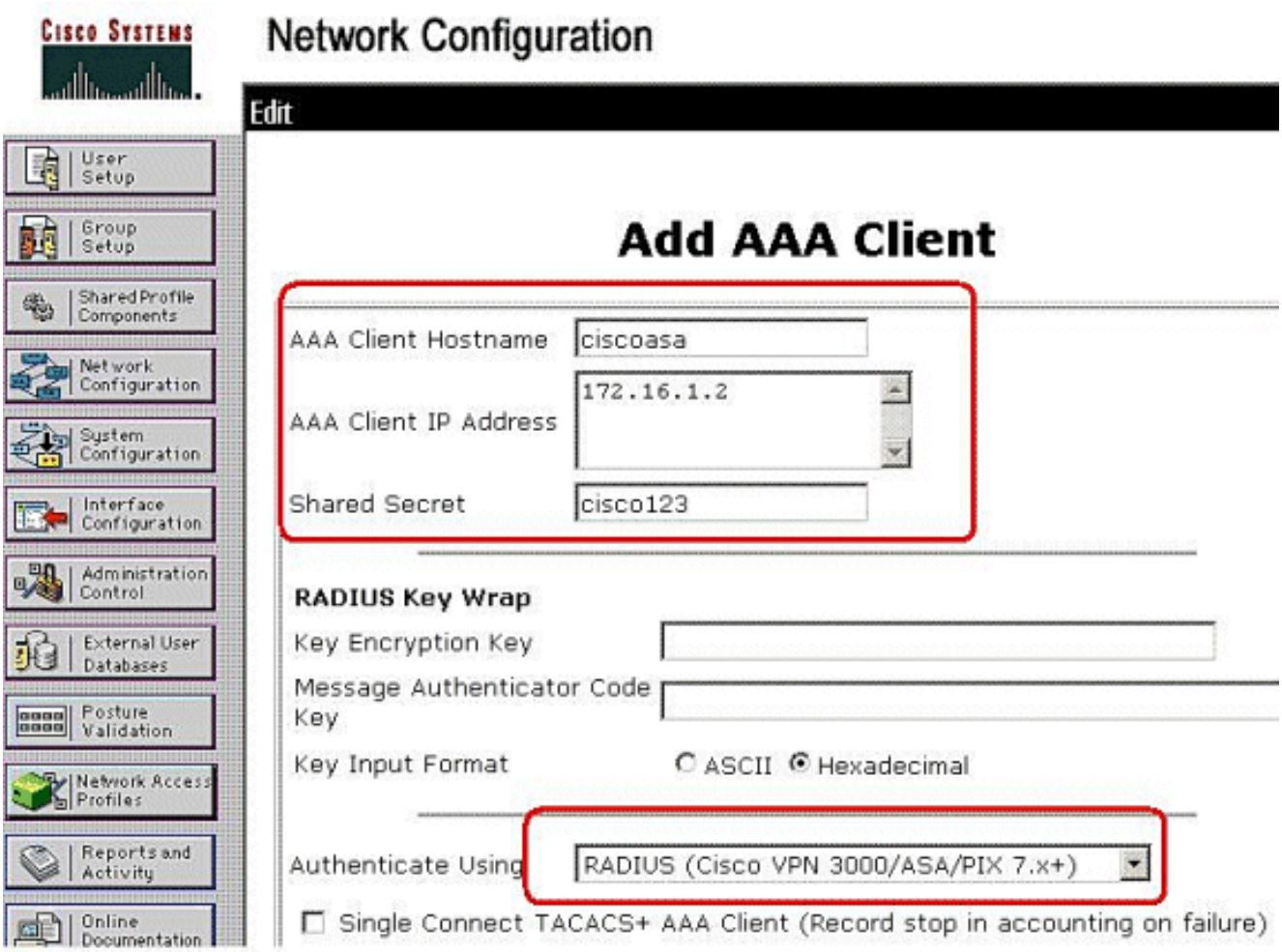
Führen Sie diese Schritte aus, um RADIUS in einem Cisco Secure ACS zu konfigurieren.

1. Wählen Sie links **Network Configuration** (Netzwerkkonfiguration) aus, und klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um einen Eintrag für die ASA in der RADIUS-Serverdatenbank hinzuzufügen.

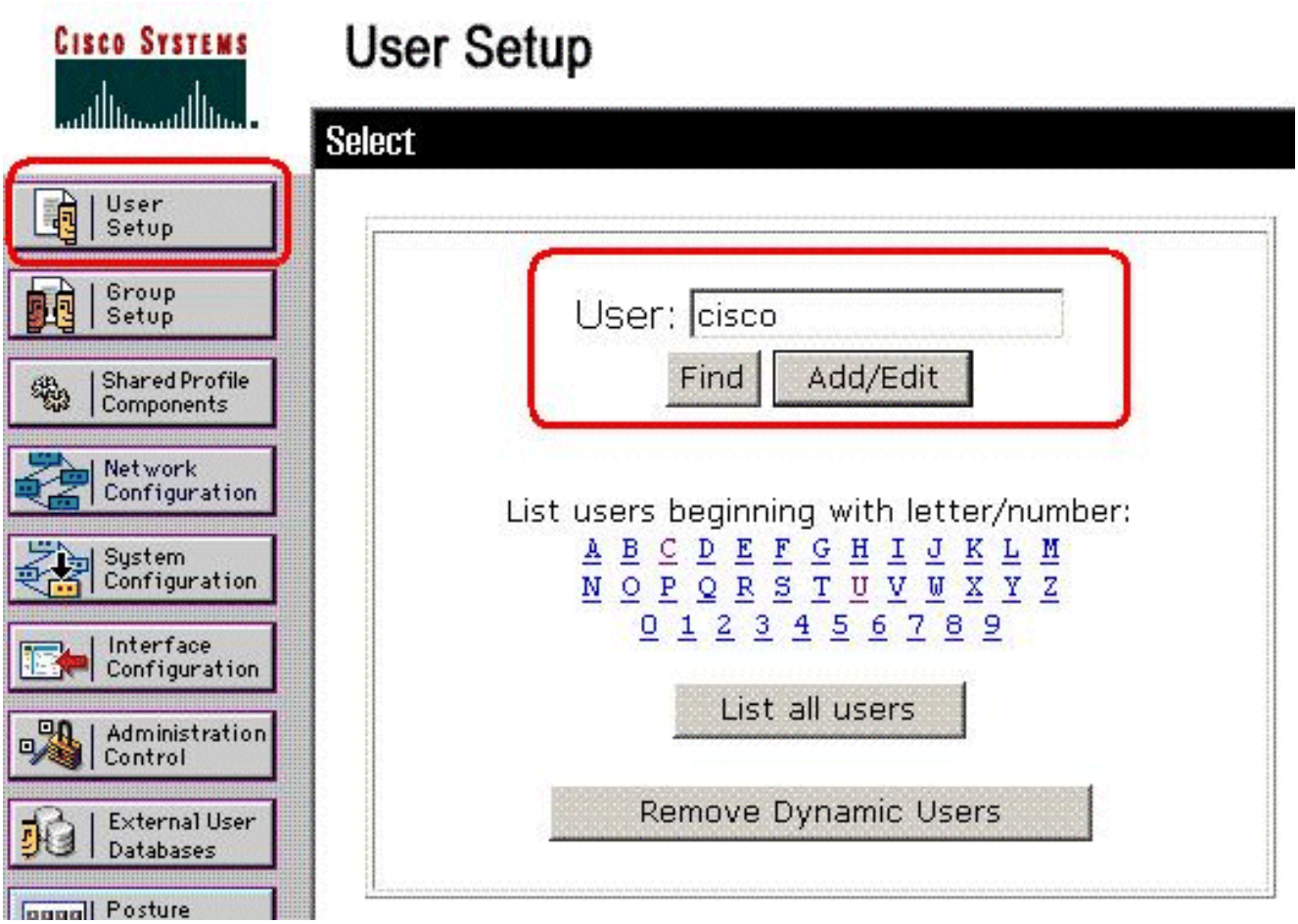


2. Geben Sie **172.16.1.2** in das Feld Client IP address (Client-IP-Adresse) ein, und geben Sie **"cisco123"** in das Feld für den gemeinsamen geheimen Schlüssel ein. Wählen Sie **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** im Dropdown-Feld *Authentifizierung mit*. Klicken Sie auf **Senden**.

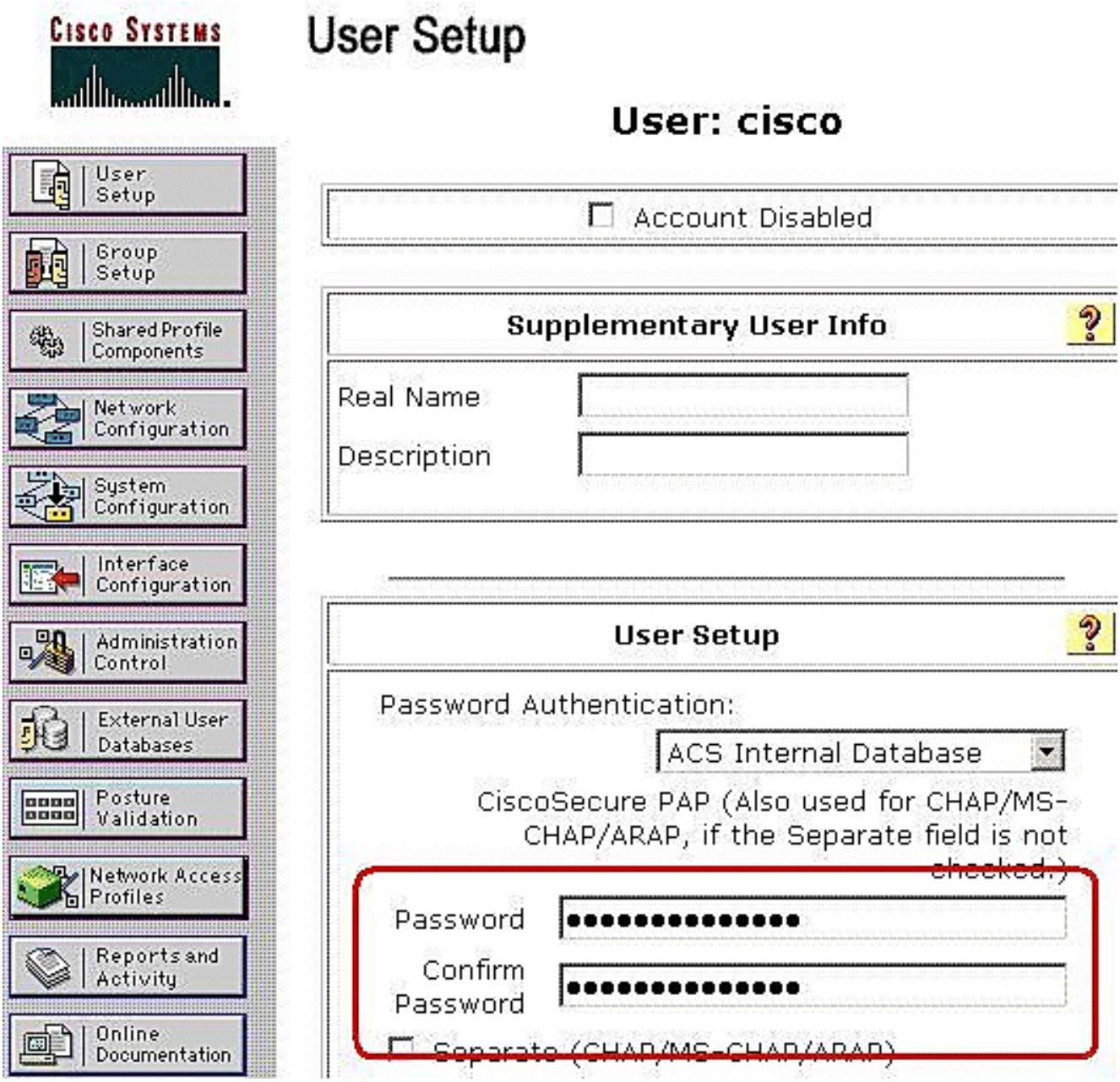
.



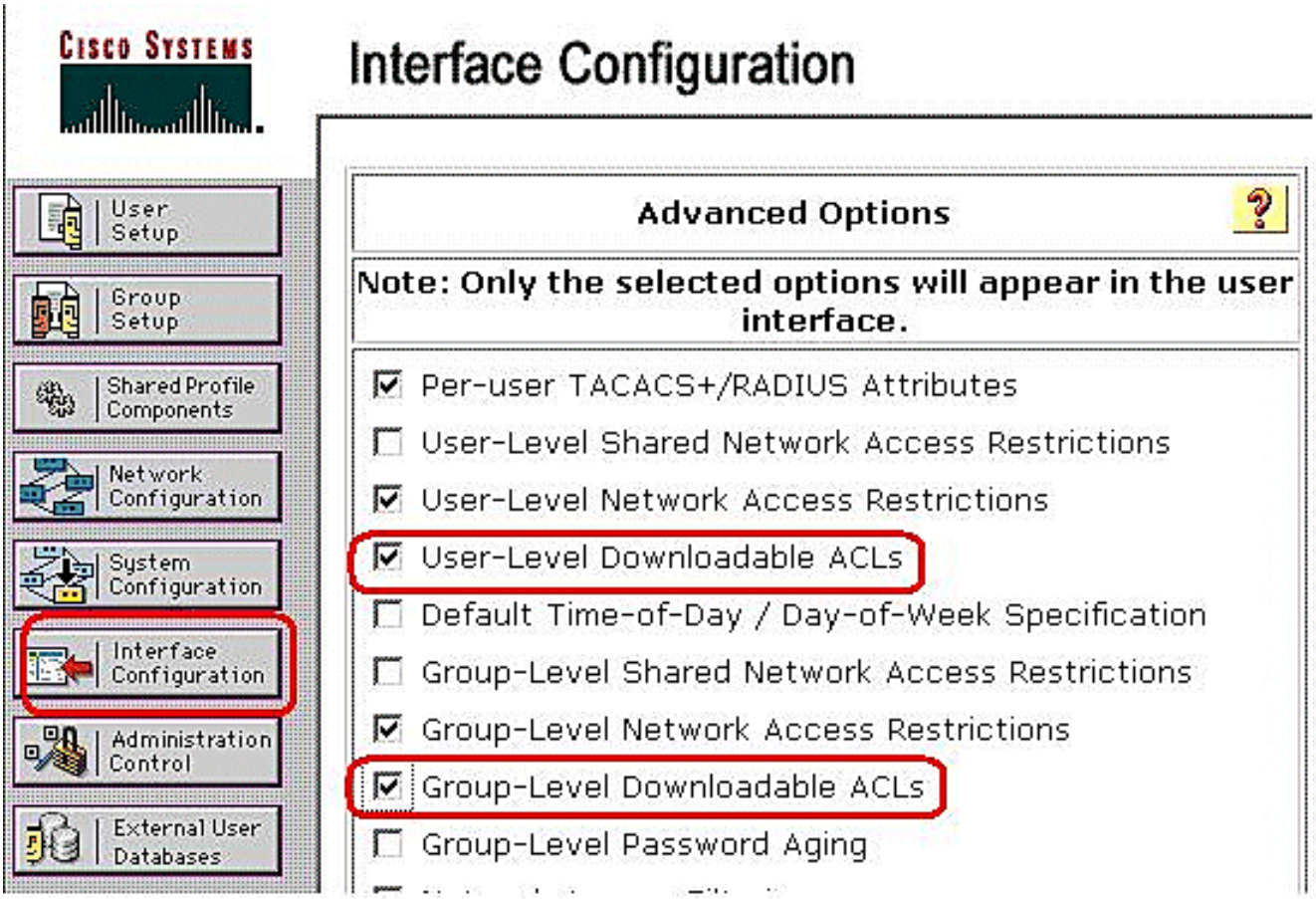
3. Geben Sie in der Cisco Secure-Datenbank im Feld User den Benutzernamen ein, und klicken Sie auf **Add/Edit**.In diesem Beispiel lautet der Benutzername **cisco**.



4. Geben Sie im nächsten Fenster das Kennwort für **"cisco"** ein. In diesem Beispiel lautet das Kennwort auch **password1**. Wenn Sie fertig sind, klicken Sie auf **Senden**.

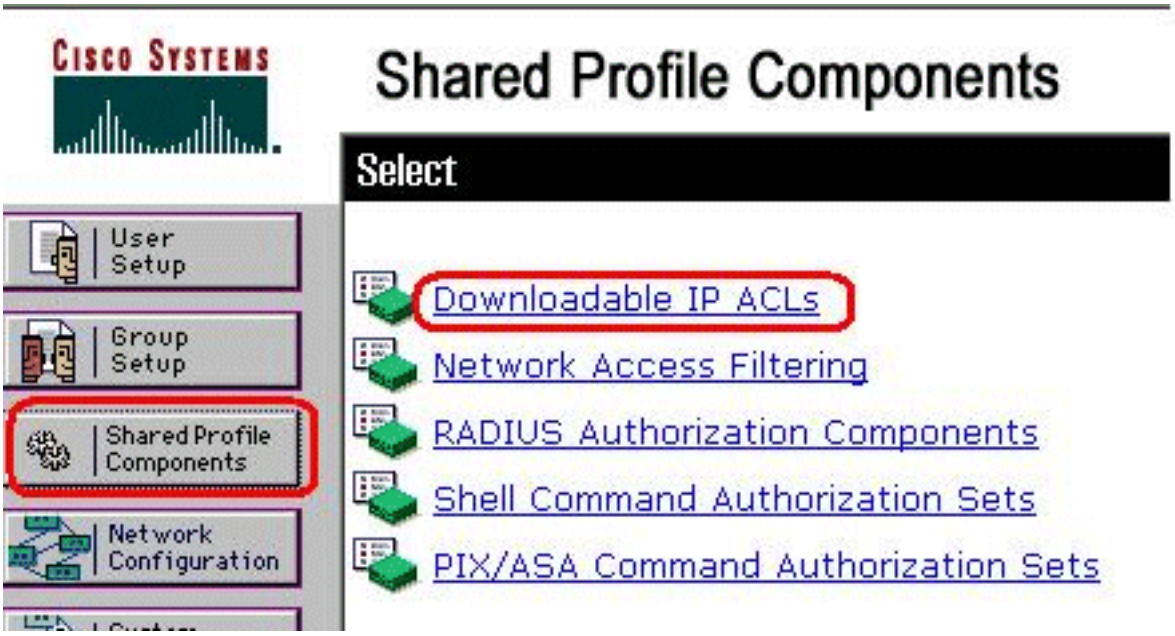


5. Auf der Seite "Erweiterte Optionen" können Sie festlegen, welche erweiterten Optionen der ACS anzeigt. Sie können die Seiten, die in anderen Bereichen der ACS-Webschnittstelle angezeigt werden, vereinfachen, wenn Sie die erweiterten Optionen ausblenden, die Sie nicht verwenden. Klicken Sie auf **Schnittstellenkonfiguration** und dann auf **Erweiterte Optionen**, um die Seite Erweiterte Optionen zu öffnen.

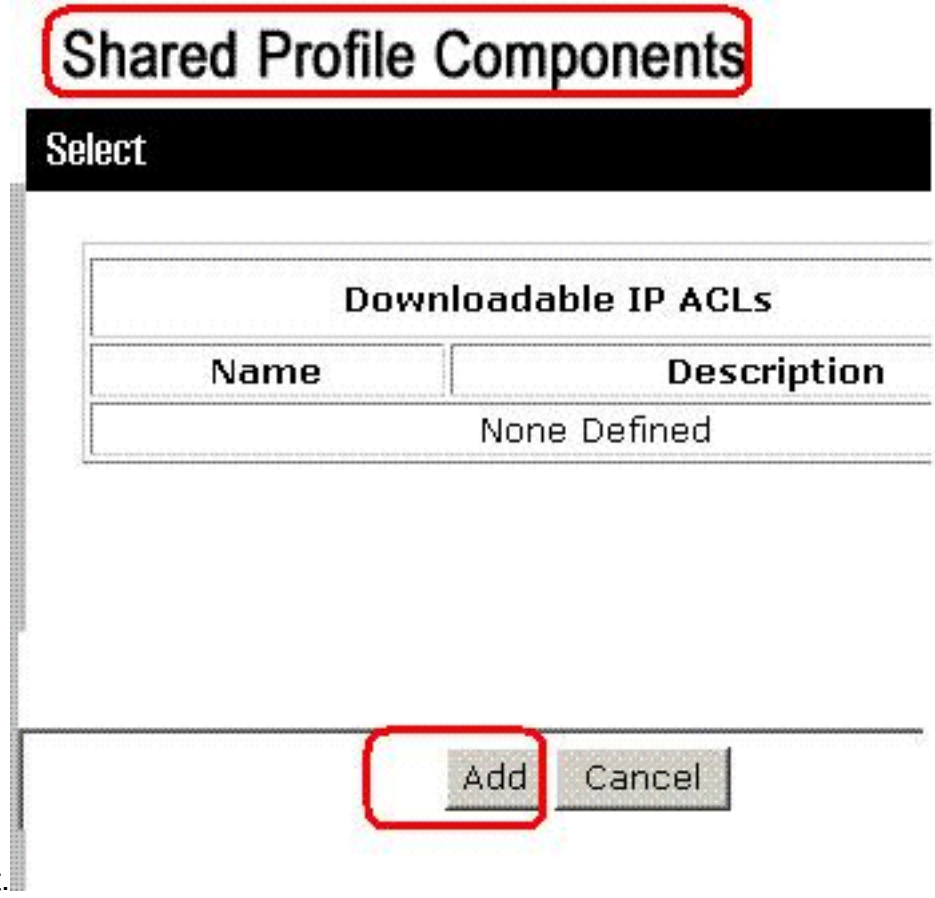


Aktivieren Sie das Kontrollkästchen für **herunterladbare ACLs auf Benutzerebene** und **herunterladbare Zugriffskontrolllisten auf Gruppenebene**.**Herunterladbare ACLs auf Benutzerebene**: Bei Auswahl dieser Option wird der Abschnitt "Herunterladbare ACLs (Zugriffskontrolllisten)" auf der Seite "User Setup" (Benutzereinrichtung) aktiviert.**Herunterladbare Zugriffskontrolllisten auf Gruppenebene**: Bei Auswahl dieser Option wird der Abschnitt "Herunterladbare Zugriffskontrolllisten" auf der Seite "Group Setup" (Gruppeneinrichtung) aktiviert.

6. Klicken Sie in der Navigationsleiste auf **Komponenten für gemeinsam genutzte Profile** und dann auf **herunterladbare IP-Zugriffskontrolllisten**.**Hinweis:** Wenn *herunterladbare IP-ACLs* nicht auf der Seite Komponenten des gemeinsam genutzten Profils angezeigt werden, müssen Sie die herunterladbaren ACLs auf Benutzerebene, die Option herunterladbare ACLs auf Gruppenebene oder beide auf der Seite Erweiterte Optionen im Abschnitt Schnittstellenkonfiguration
aktivieren.

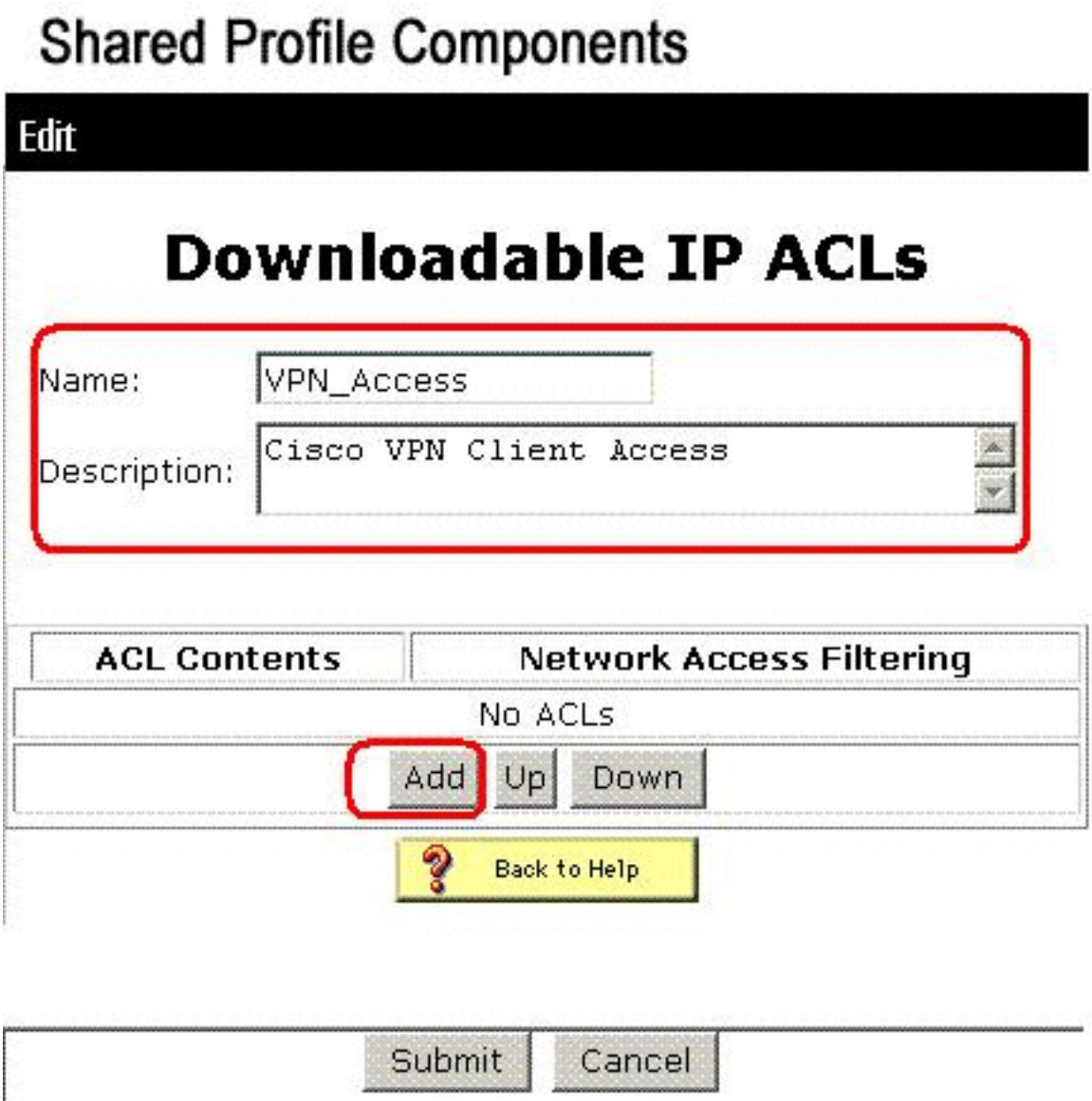


7. Klicken Sie auf **Hinzufügen**. Die Seite herunterladbare IP-Zugriffskontrolllisten wird



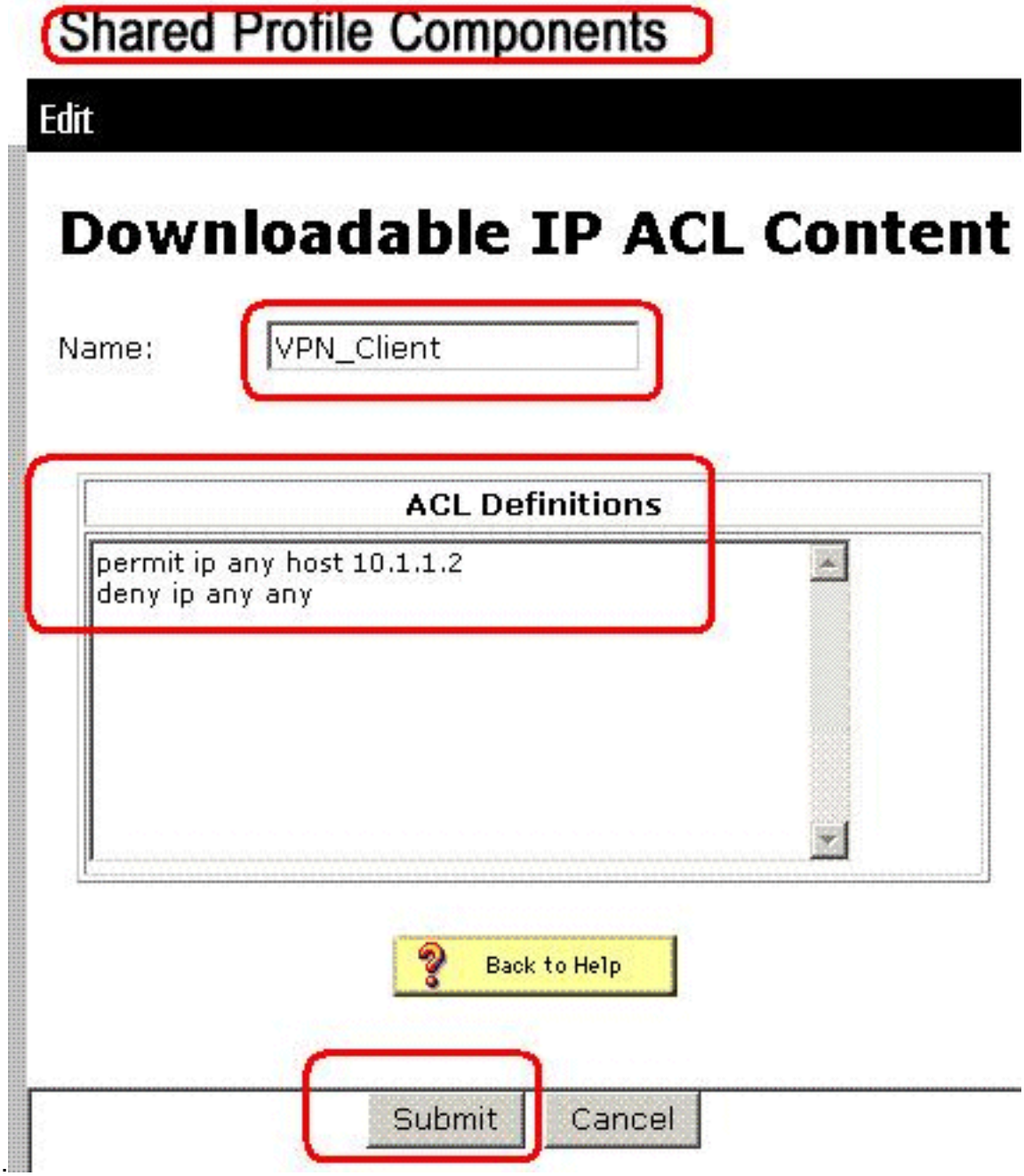
angezeigt.

8. Geben Sie im Feld Name den Namen der neuen IP-Zugriffskontrollliste ein.**Hinweis:** Der Name einer IP-Zugriffskontrollliste kann bis zu 27 Zeichen enthalten. Der Name darf keine Leerzeichen oder eines der folgenden Zeichen enthalten: Bindestrich (-), linke Klammer ([), rechte Klammer (]), Schrägstrich (/), umgekehrter Schrägstrich (\), Anführungszeichen ("), linke spitze Klammer (<), rechte Winkelklammer (>) oder Bindestrich (-).Geben Sie im Feld Description (Beschreibung) eine Beschreibung der neuen IP-Zugriffskontrollliste ein. Die Beschreibung kann bis zu 1.000 Zeichen



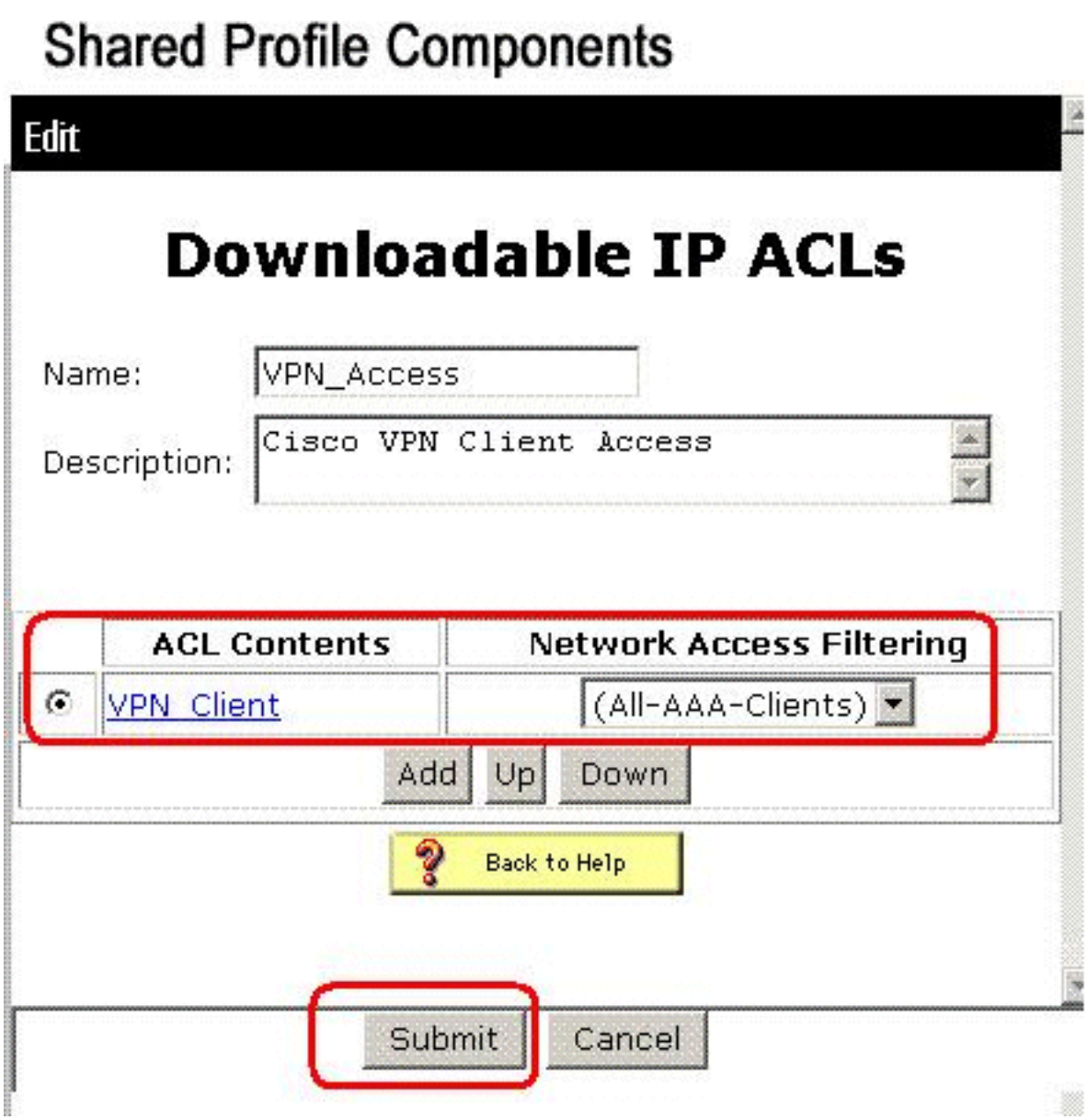
enthalten. U
m der neuen IP-Zugriffskontrollliste einen ACL-Inhalt hinzuzufügen, klicken Sie auf **Hinzufügen**.

9. Geben Sie im Feld Name den Namen des neuen ACL-Inhalts ein.**Hinweis:** Der Name eines ACL-Inhalts kann bis zu 27 Zeichen enthalten. Der Name darf keine Leerzeichen oder eines der folgenden Zeichen enthalten: Bindestrich (-), linke Klammer ([), rechte Klammer (]), Schrägstrich (/), umgekehrter Schrägstrich (\), Anführungszeichen ("), linke spitze Klammer (<), rechte Winkelklammer (>) oder Bindestrich (-).Geben Sie im Feld ACL Definitions (ACL-Definitionen) die neue ACL-Definition ein.**Hinweis:** Wenn Sie die ACL-Definitionen in die ACS-Webschnittstelle eingeben, dürfen Sie keine Stichwort- oder Namenseinträge verwenden. sondern beginnen Sie mit einem permit-Schlüsselwort oder einem deny-Schlüsselwort.Um den ACL-Inhalt zu speichern, klicken Sie auf



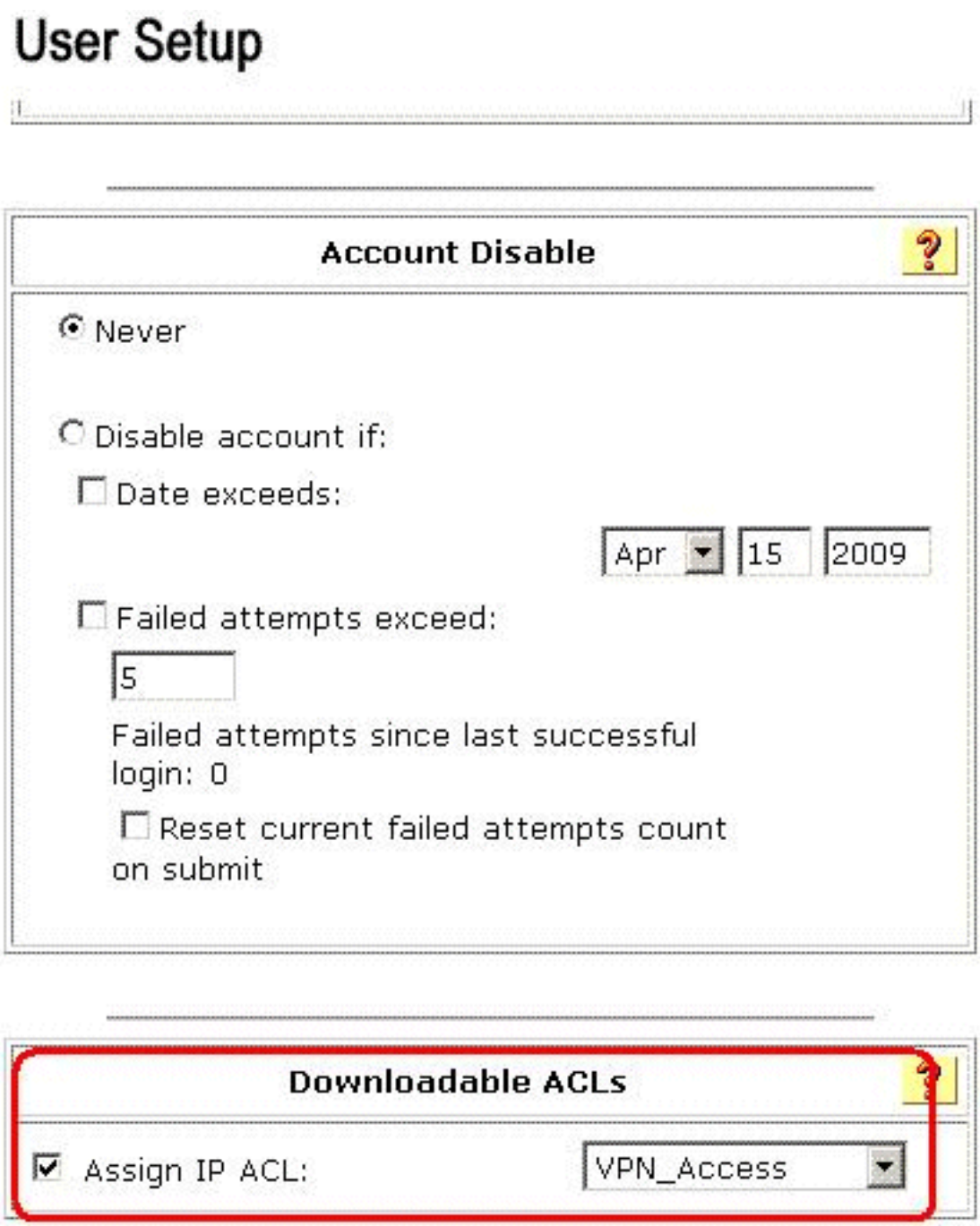
Senden.

10. Die Seite zum Herunterladen von IP-Zugriffskontrolllisten wird mit dem neuen ACL-Inhalt angezeigt, der nach Namen in der Spalte ACL Contents (ACL-Inhalt) aufgeführt ist. Um dem ACL-Inhalt eine NAF zuzuordnen, wählen Sie im Feld Network Access Filtering (Netzwerkzugriffsfilterung) rechts neben dem neuen ACL-Inhalt eine NAF aus. NAF ist standardmäßig (All-AAA-Clients). Wenn Sie keine NAF zuweisen, ordnet ACS den ACL-Inhalt allen Netzwerkgeräten zu (dies ist die Standardeinstellung).



Um die Reihenfolge der ACL-Inhalte festzulegen, klicken Sie auf das Optionsfeld für eine ACL-Definition, und klicken Sie dann auf **Nach oben** oder **Nach unten**, um sie in der Liste neu zu positionieren.Um die IP-Zugriffskontrollliste zu speichern, klicken Sie auf **Senden**.**Hinweis:** Die Reihenfolge der ACL-Inhalte ist von Bedeutung. Von oben nach unten lädt ACS nur die erste ACL-Definition mit einer entsprechenden NAF-Einstellung herunter, die bei Verwendung die Standardeinstellung All-AAA-Clients enthält. In der Regel geht die Liste der ACL-Inhalte von der Liste mit dem spezifischsten (engsten) NAF zur Liste mit dem allgemeinsten (All-AAA-Clients) NAF über.**Hinweis:** ACS gibt die neue IP-Zugriffskontrollliste ein, die sofort wirksam wird. Wenn die IP-ACL beispielsweise für die Verwendung mit PIX-Firewalls vorgesehen ist, kann sie an jede PIX-Firewall gesendet werden, die die Authentifizierung eines Benutzers versucht, dem die herunterladbare IP-ACL seinem Benutzer- oder Gruppenprofil zugewiesen ist.

11. Rufen Sie die Seite User Setup (Benutzereinrichtung) auf, und bearbeiten Sie die Seite User (Benutzer). Klicken Sie im Abschnitt "Herunterladbare ACLs" auf **IP-Zugriffskontrollliste zuweisen:** aktivieren. Wählen Sie eine IP-Zugriffskontrollliste aus der Liste aus. Wenn Sie die Konfiguration der Benutzerkontenoptionen abgeschlossen haben, klicken Sie auf **Senden**, um die Optionen aufzuzeichnen.



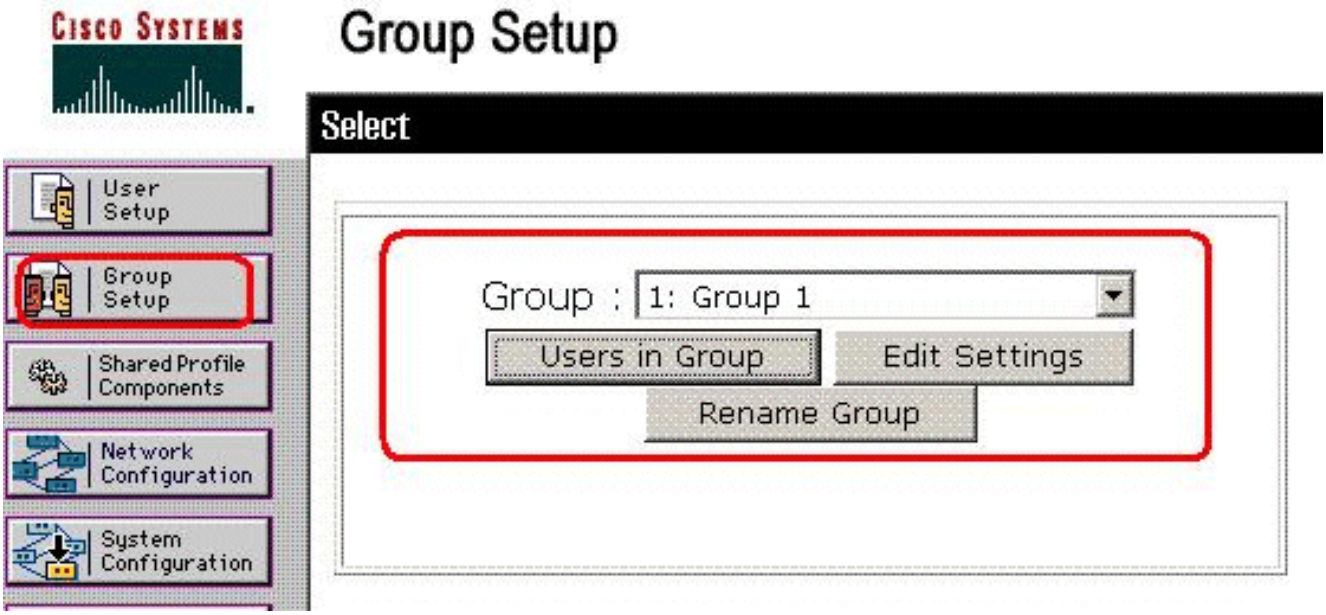
Konfigurieren von ACS für herunterladbare ACL für Gruppen

Führen Sie die Schritte 1 bis 9 der Konfigurationsanweisung für die herunterladbare ACL für individuelle Benutzer aus und befolgen Sie die folgenden Schritte, um die herunterladbare ACL für Gruppen in einem Cisco Secure ACS zu konfigurieren.

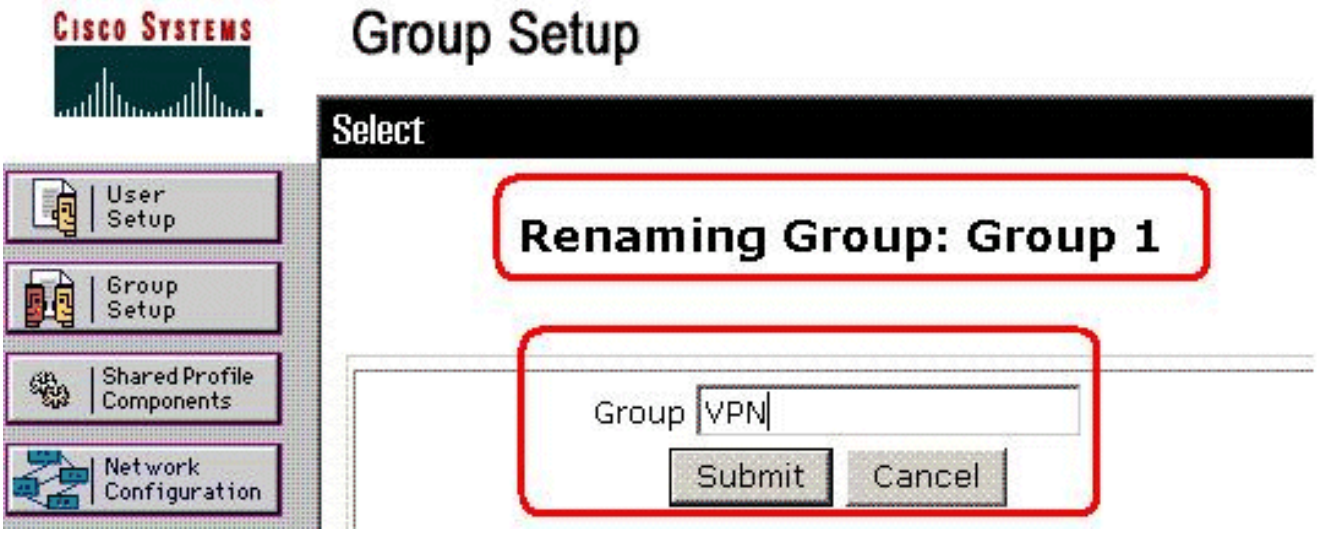
In diesem Beispiel gehört der IPSec-VPN-Benutzer "cisco" zu den VPN-Gruppen. Die VPN-Gruppenrichtlinien werden für alle Benutzer in der Gruppe angewendet.

Der VPN-Gruppenbenutzer **"cisco"** authentifiziert sich erfolgreich, und der RADIUS-Server sendet eine herunterladbare Zugriffsliste an die Sicherheits-Appliance. Der Benutzer "cisco" kann nur auf den Server 10.1.1.2 zugreifen und verweigert allen anderen Zugriff. Informationen zum Überprüfen der Zugriffskontrollliste finden Sie im Abschnitt "Herunterladbare Zugriffskontrollliste für Benutzer/Gruppen".

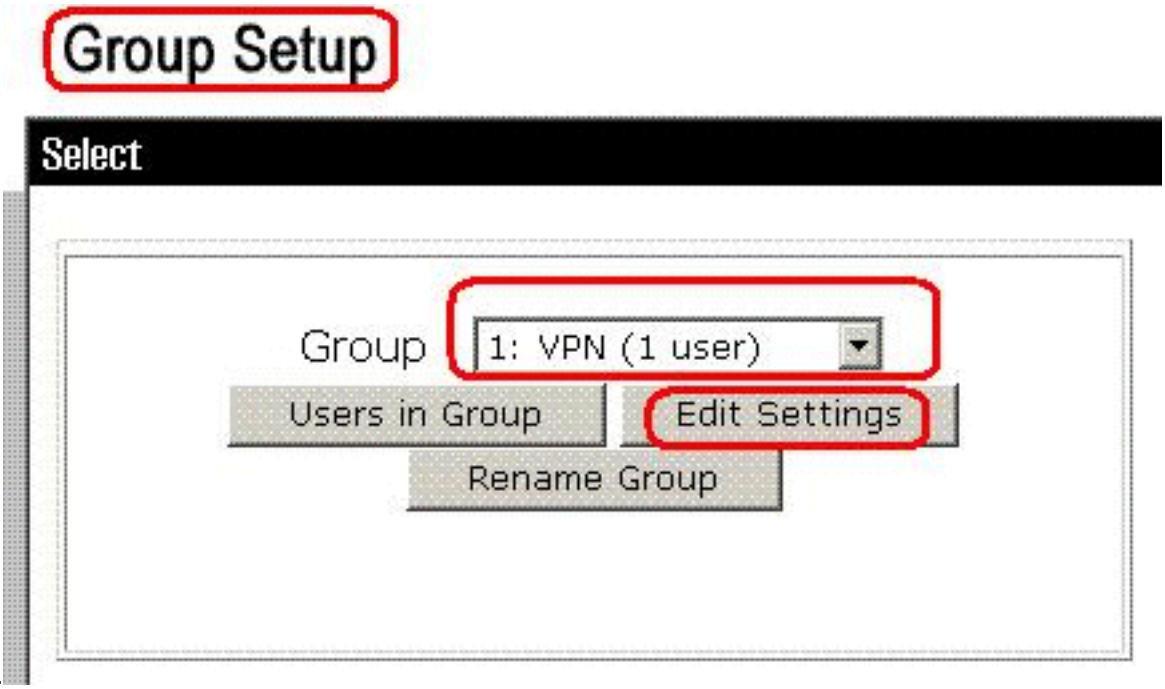
1. Klicken Sie in der Navigationsleiste auf **Gruppeneinrichtung**. Die Seite "Group Setup Select" (Gruppeneinrichtung auswählen) wird geöffnet.



2. Umbenennen Sie Gruppe 1 in **VPN**, und klicken Sie auf **Senden**.

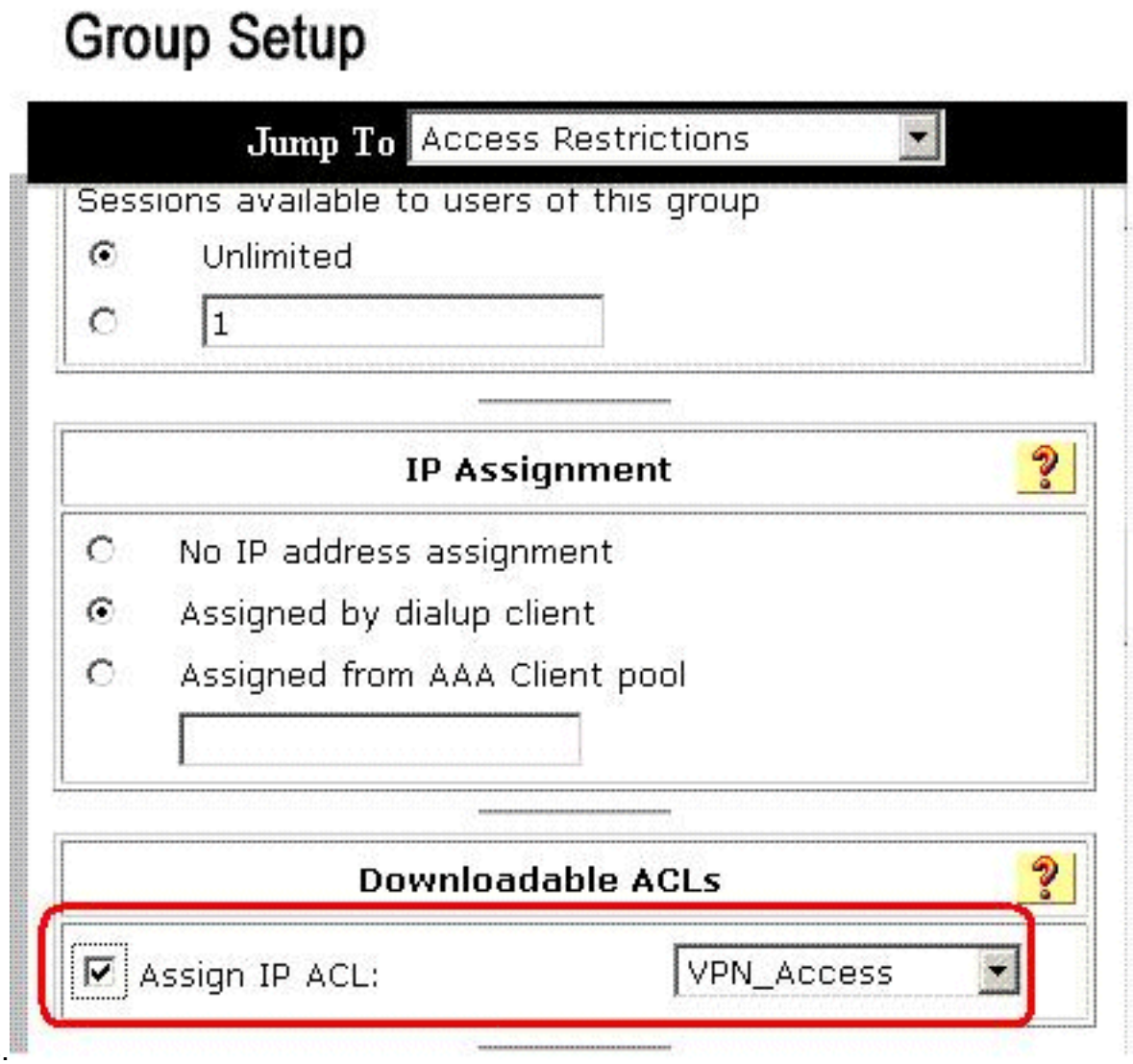


3. Wählen Sie aus der Liste Gruppe eine Gruppe aus, und klicken Sie dann auf **Einstellungen**



bearbeiten.

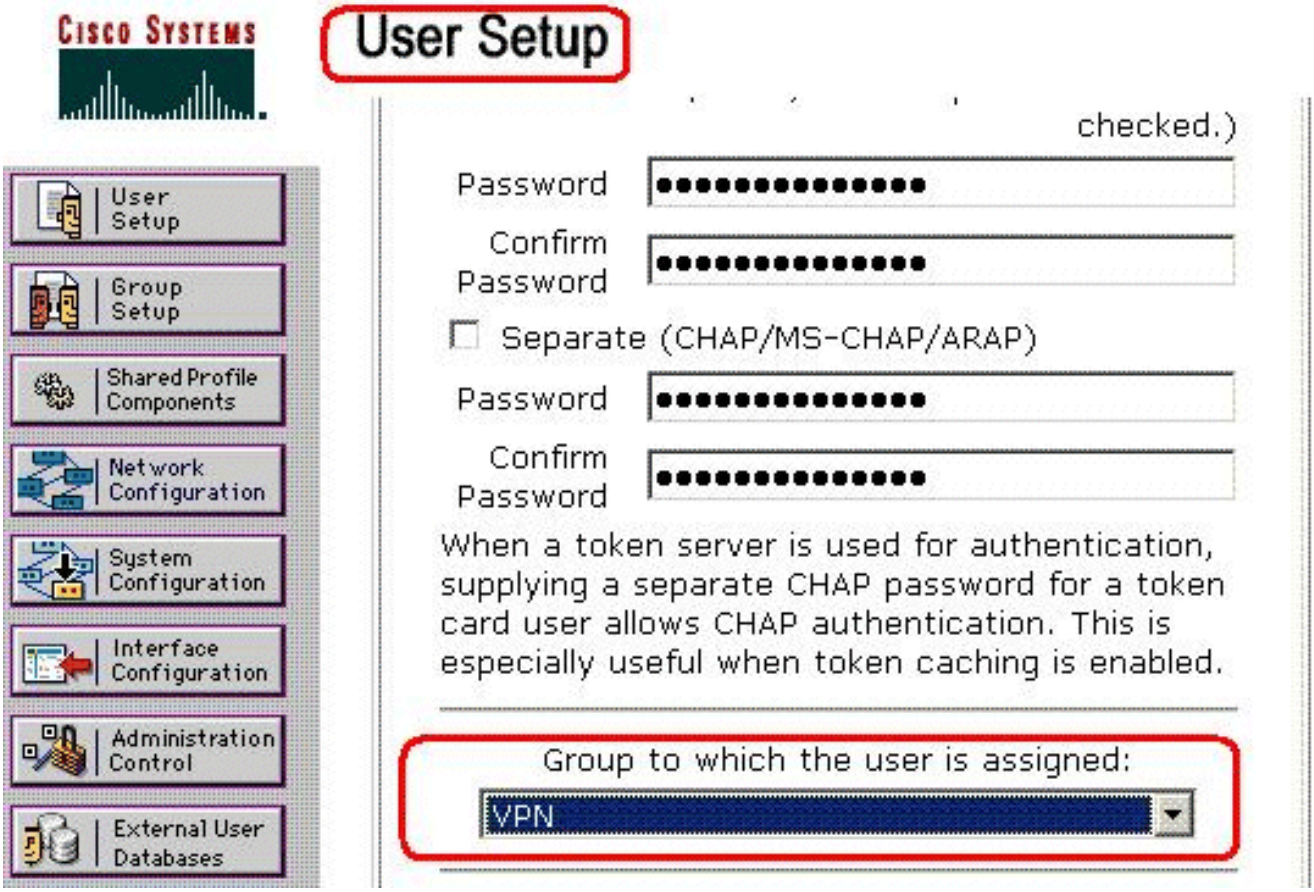
4. Klicken Sie im Abschnitt "Herunterladbare ACLs" auf das Kontrollkästchen **IP-ACL zuweisen**. Wählen Sie eine IP-Zugriffskontrollliste aus der Liste



aus.

5. Um die soeben vorgenommenen Gruppeneinstellungen zu speichern, klicken Sie auf **Senden**.
6. Gehen Sie zum Benutzer-Setup, und bearbeiten Sie den Benutzer, den Sie der Gruppe

hinzufügen möchten: **VPN**. Wenn Sie fertig sind, klicken Sie auf **Senden**.



Nun wird die für die VPN-Gruppe konfigurierte herunterladbare ACL auf diesen Benutzer angewendet.

7. Um weitere Gruppeneinstellungen festzulegen, führen Sie nach Bedarf weitere Verfahren in diesem Kapitel durch.

Konfigurieren der IETF-RADIUS-Einstellungen für eine Benutzergruppe

Um einen Namen für eine Zugriffsliste herunterzuladen, die Sie bereits auf der Sicherheitsappliance vom RADIUS-Server bei der Benutzerauthentifizierung erstellt haben, konfigurieren Sie das IETF RADIUS filter-id-Attribut (Attributnummer 11) wie folgt:

```
filter-id=acl_name
```

Der VPN-Gruppenbenutzer **"cisco"** authentifiziert sich erfolgreich, und der RADIUS-Server lädt einen ACL-Namen (neu) für eine Zugriffsliste herunter, die Sie bereits auf der Sicherheits-Appliance erstellt haben. Der Benutzer "cisco" kann auf alle Geräte im Netzwerk der ASA zugreifen, **mit Ausnahme** des 10.1.1.2-Servers. Informationen zum Überprüfen der ACL finden Sie im Abschnitt Filter-ID-ACL.

Im Beispiel wird die ACL mit dem Namen **new** für das Filtern in ASA konfiguriert.

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

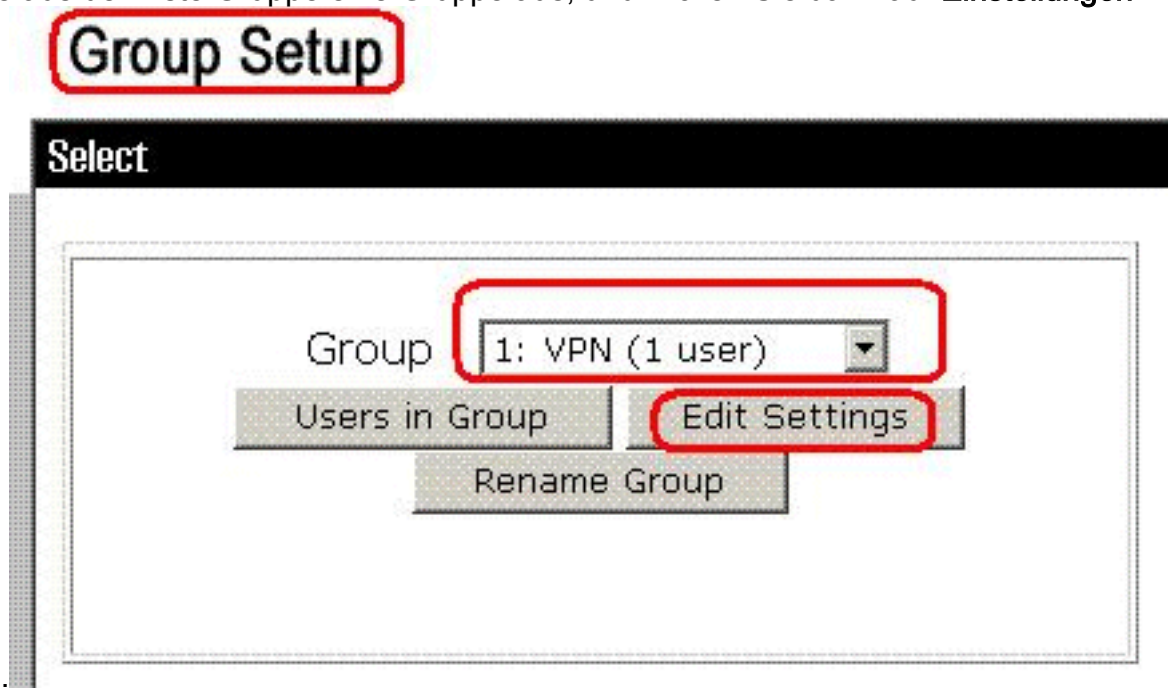
Diese Parameter werden nur angezeigt, wenn sie true sind. Sie haben

- AAA-Client zur Verwendung eines der RADIUS-Protokolle in der Netzwerkkonfiguration
- RADIUS-Gruppenattribute auf der Seite RADIUS (IETF) im Abschnitt "Schnittstellenkonfiguration" der Webschnittstelle

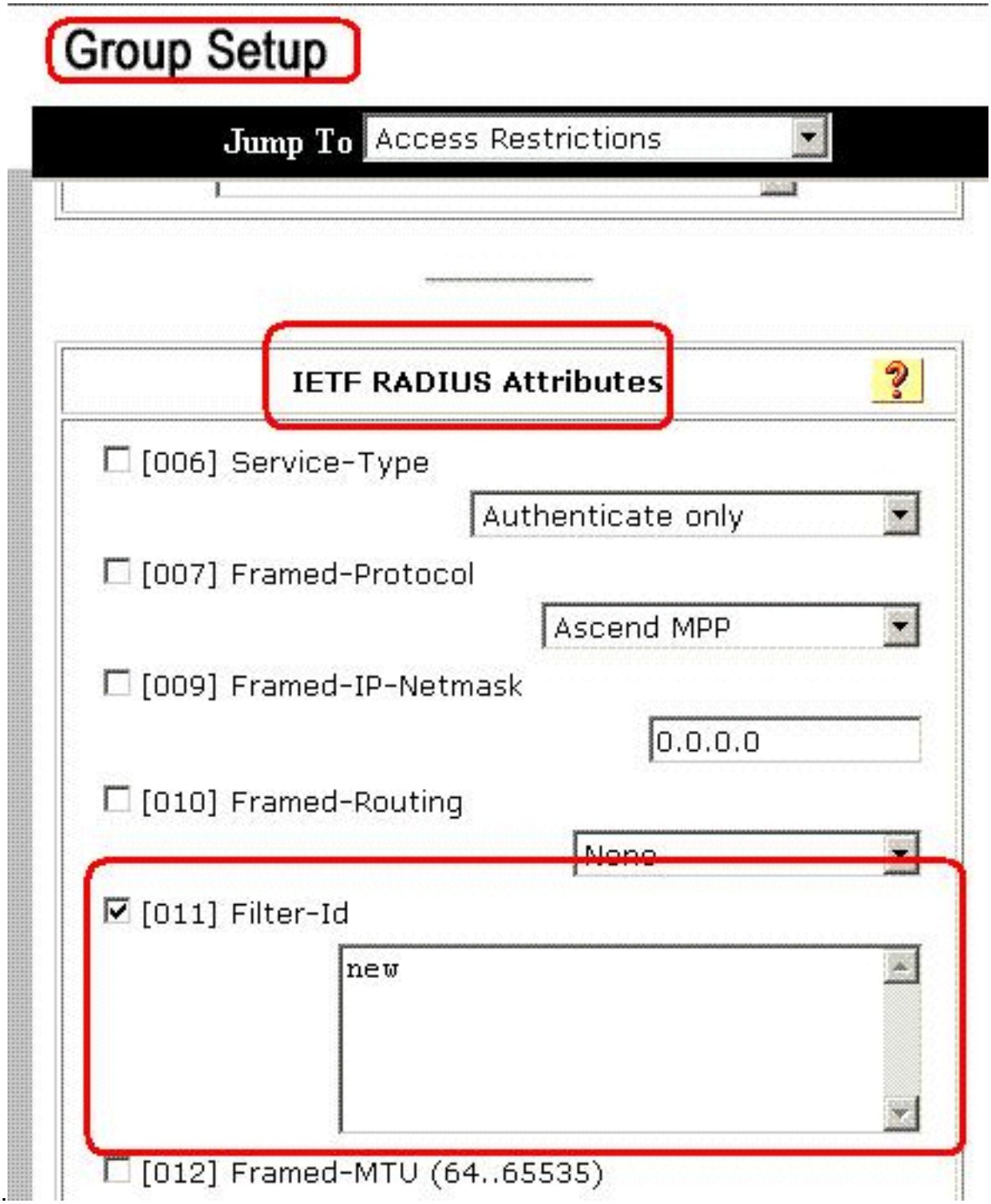
RADIUS-Attribute werden als Profil für jeden Benutzer vom ACS an den anfordernden AAA-Client gesendet.

So konfigurieren Sie die IETF RADIUS-Attributeinstellungen als Autorisierung für jeden Benutzer in der aktuellen Gruppe:

1. Klicken Sie in der Navigationsleiste auf **Gruppeneinrichtung**.Die Seite "Group Setup Select" (Gruppeneinrichtung auswählen) wird geöffnet.
2. Wählen Sie aus der Liste Gruppe eine Gruppe aus, und klicken Sie dann auf **Einstellungen bearbeiten**.



   Der Name der Gruppe wird oben auf der Seite Gruppeneinstellungen angezeigt.
3. Navigieren Sie zu den IEFT-RADIUS-Attributen. Für jedes IETF-RADIUS-Attribut müssen Sie die aktuelle Gruppe autorisieren. Aktivieren Sie das Kontrollkästchen des **[011] Filter-Id-**Attributs, und fügen Sie dann den (**neuen**) ASA Defined ACL-Namen in die Autorisierung für das Attribut im Feld hinzu. Weitere Informationen finden Sie unter ASA *show running configuration*



output.

4. Um die soeben vorgenommenen Gruppeneinstellungen zu speichern und sofort anzuwenden, klicken Sie auf **Senden** und **Übernehmen**.**Hinweis:** Um Ihre Gruppeneinstellungen zu speichern und später anzuwenden, klicken Sie auf **Senden**. Wenn Sie bereit sind, die Änderungen zu implementieren, wählen Sie **Systemkonfiguration > Servicesteuerung aus**. Wählen Sie anschließend **Neu starten aus**.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Krypto-Befehle anzeigen

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE Security Associations (SAs) in einem Peer an.

```
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**: Zeigt die von aktuellen SAs verwendeten Einstellungen.

```
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 zum Download für Benutzer/Gruppe

Überprüfen Sie die herunterladbare ACL für den Benutzer Cisco. ACLs werden vom CSACS heruntergeladen.

```
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
```

Filter-ID ACL

Die [011] Filter-ID wurde für das Group - VPN (Gruppe - VPN) angewendet, und die Benutzer der Gruppe werden entsprechend der in der ASA definierten ACL (neu) gefiltert.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration. Ein Beispiel für eine Debugausgabe wird ebenfalls angezeigt.

Hinweis: Weitere Informationen zur Fehlerbehebung für Remote Access IPSec VPN finden Sie unter Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung.

Sicherheitszuordnungen löschen

Achten Sie bei der Fehlerbehebung darauf, vorhandene Sicherheitszuordnungen zu löschen, nachdem Sie eine Änderung vorgenommen haben. Verwenden Sie im privilegierten Modus des

PIX die folgenden Befehle:

- **clear [crypto] ipsec sa**: Löscht die aktiven IPSec SAs. Das Schlüsselwort crypto ist optional.
- **clear [crypto] isakmp sa**: Löscht die aktiven IKE-SAs. Das Schlüsselwort crypto ist optional.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug crypto ipsec 7**: Zeigt die IPSec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp 7**: Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Befehlsreferenzen
- Support-Seite für Cisco PIX Security Appliances der Serie 500
- Cisco Adaptive Security Device Manager
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Support-Seite für Cisco VPN-Clients
- Cisco Secure Access Control Server für Windows
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems