ASA 8.3 und höher: RADIUS Authorization (ACS 5.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 Sie RADIUS-Autorisierungen implizit aktivieren können, enthält dieses Dokument 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 den Cisco Secure Access Control Server (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/PIX 8.x: Radius Authorization (ACS) für den Netzwerkzugriff mit herunterladbarer ACL mit CLI und ASDM - Konfigurationsbeispiel für die identische Konfiguration auf der Cisco ASA mit Version 8.2 und früher.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Adaptive Security Appliance (ASA) voll funktionsfähig und so konfiguriert ist, dass der Cisco Adaptive Security Device Manager (ASDM) oder die CLI Konfigurationsänderungen vornehmen kann.

Hinweis: Unter Zulassen von HTTPS-Zugriff für ASDM wird verwiesen, um die Remote-Konfiguration des Geräts durch ASDM oder Secure Shell (SSH) zu ermöglichen.

Verwendete Komponenten

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

- Cisco ASA Software Version 8.3 oder höher
- Cisco ASDM ab Version 6.3
- Cisco VPN Client Version 5.x oder höher
- Cisco Secure ACS 5.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.

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.

Herunterladbare IP-Zugriffskontrolllisten funktionieren folgendermaßen:

1. Wenn der ACS einem Benutzer Zugriff auf das Netzwerk gewährt, bestimmt der ACS, ob dem Authorization Profile (Autorisierungsprofil) im Ergebnisabschnitt eine herunterladbare IP-ACL zugewiesen wird.
2. Wenn der ACS eine IP-ACL zum Herunterladen sucht, die dem Authorization Profile zugewiesen wird, sendet der ACS ein Attribut (als Teil der Benutzersitzung im RADIUS Access-Accept-Paket), das die benannte ACL und die Version der benannten ACL angibt.
3. Wenn der AAA-Client antwortet, dass er nicht über die aktuelle Version der ACL im Cache verfügt (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 die herunterladbare IP-Zugriffskontrollliste einem beliebigen Autorisierungsprofil zuweisen, wenn Sie auf den Namen des ACLs verweisen. Diese Methode ist effizienter, als wenn Sie das RADIUS Cisco cisco-av-pair-Attribut für das Authorization Profile konfigurieren.

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.

In ACS können Sie mehrere herunterladbare IP-ACLs definieren und in verschiedenen Autorisierungsprofilen verwenden. Basierend auf den Bedingungen in den Zugriffsdienstautorisierungsregeln können Sie verschiedene Autorisierungsprofile mit herunterladbaren IP-Zugriffskontrolllisten an verschiedene AAA-Clients senden.

Außerdem können Sie die Reihenfolge der ACL-Inhalte in einer herunterladbaren IP-ACL ändern. ACS überprüft die ACL-Inhalte, beginnend mit der Tabellenüberschrift, und lädt den ersten gefundenen ACL-Inhalt herunter. Wenn Sie die Bestellung festlegen, können Sie die Systemeffizienz sicherstellen, wenn Sie den am häufigsten verwendeten ACL-Inhalt höher in der Liste positionieren.

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

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

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

- ASA
- Cisco Geräte, die IOS Version 12.3(8)T und höher ausführen

Dies ist ein Beispiel für das Format, das Sie verwenden müssen, um ASA ACLs im Feld ACL Definitions (ACL-Definitionen) 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
```

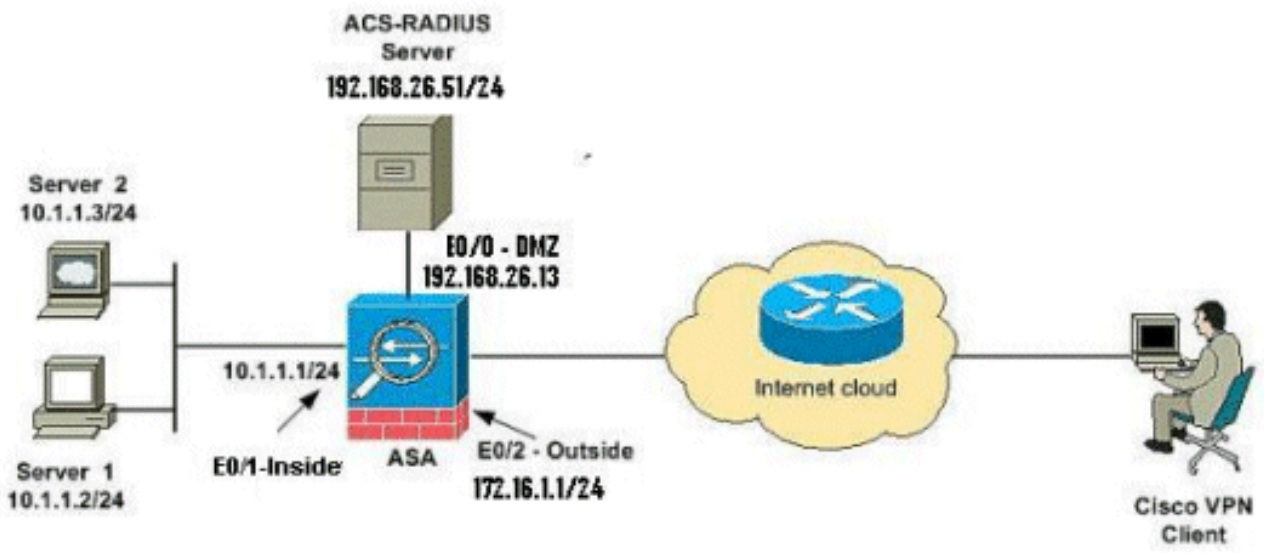
```
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 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.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



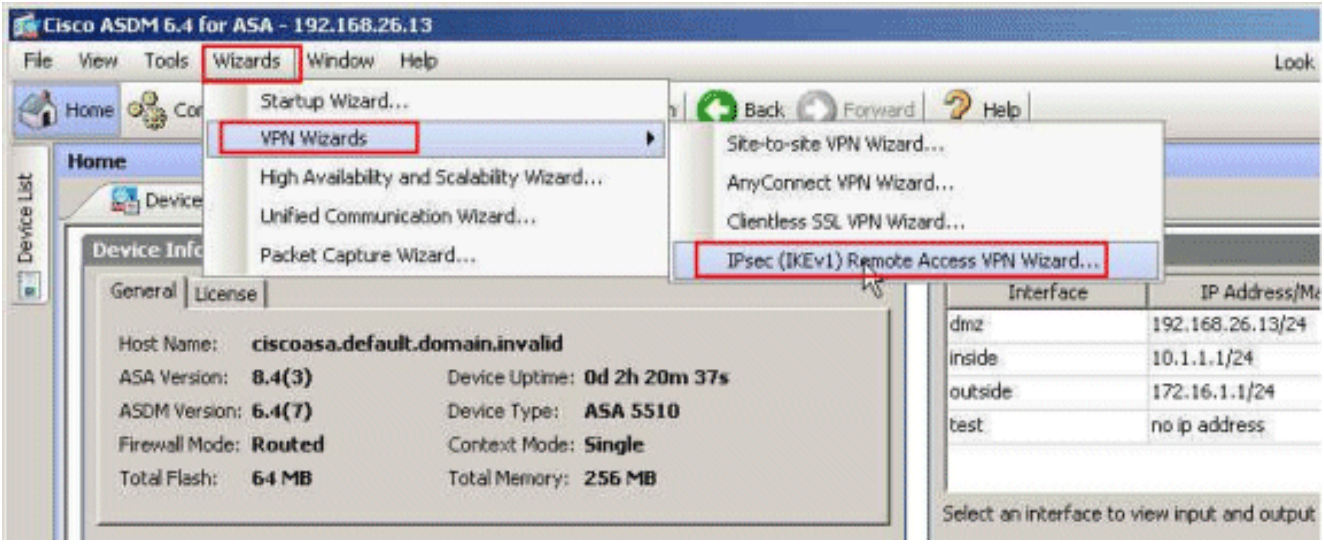
Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurieren von Remote Access VPN (IPsec)

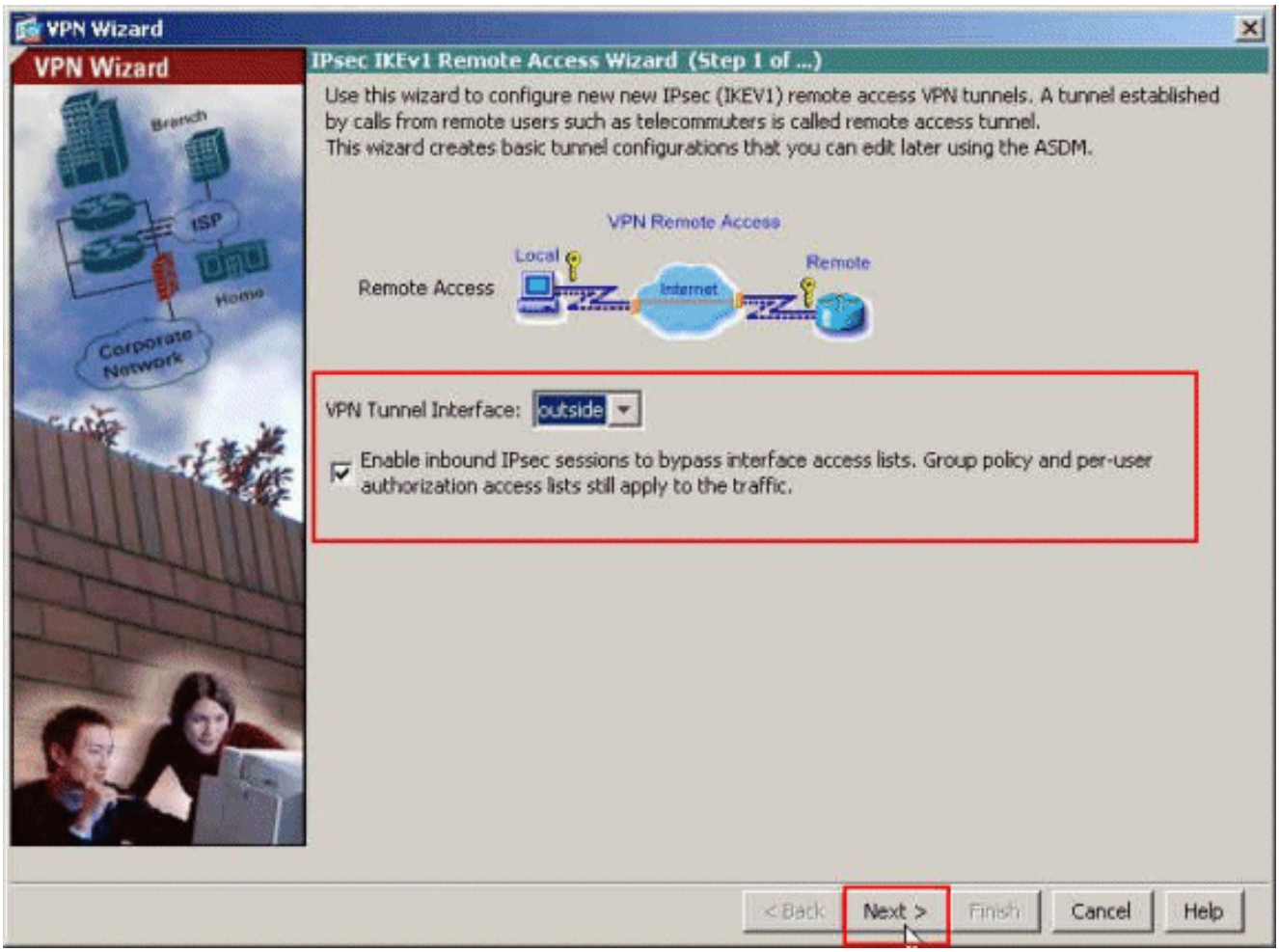
ASDM-Verfahren

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

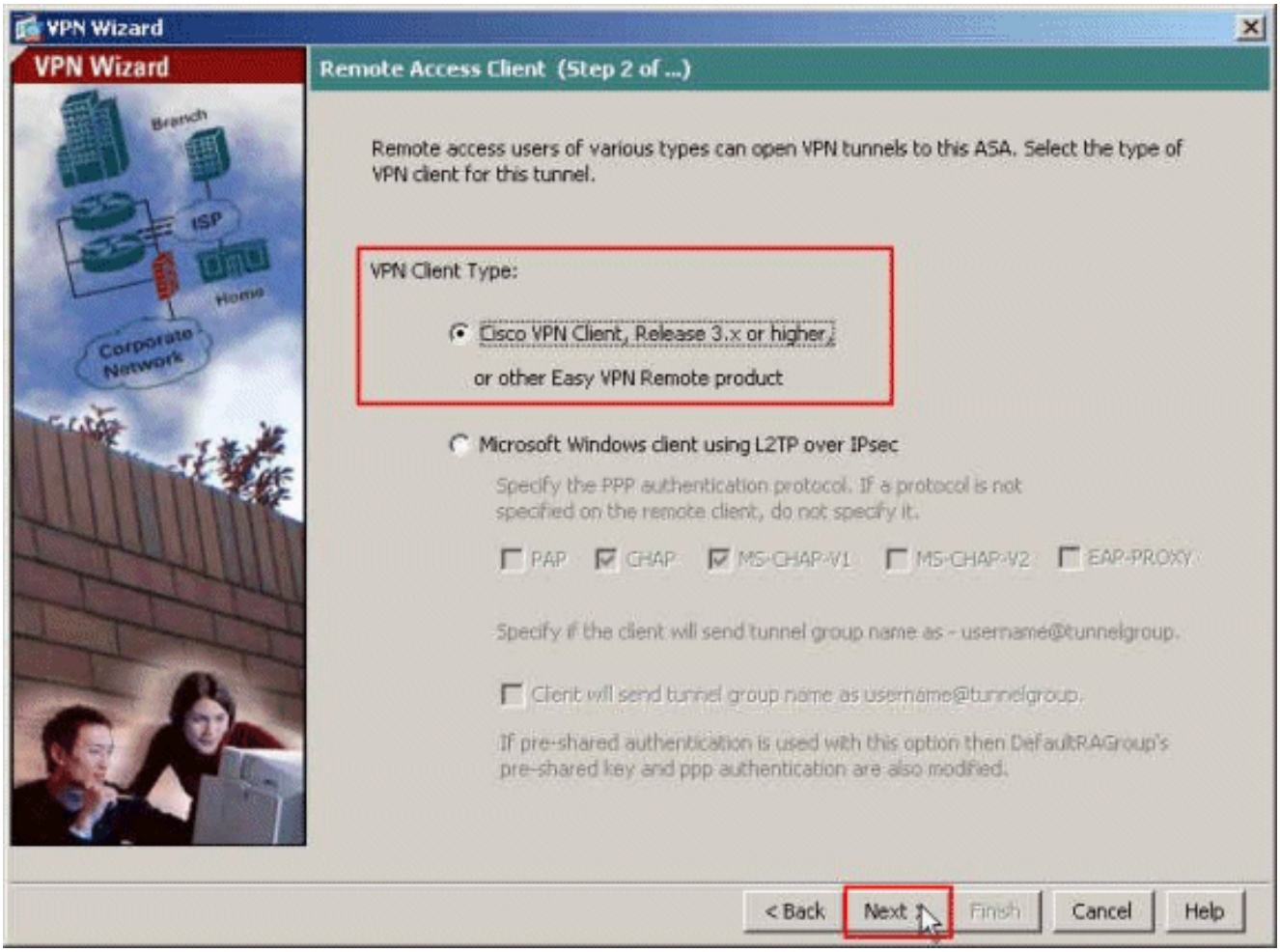
1. Wählen Sie **Assistenten > VPN Wizards > IPsec(IKEv1) Remote Access VPN Wizard** aus dem Home-Fenster
   aus.



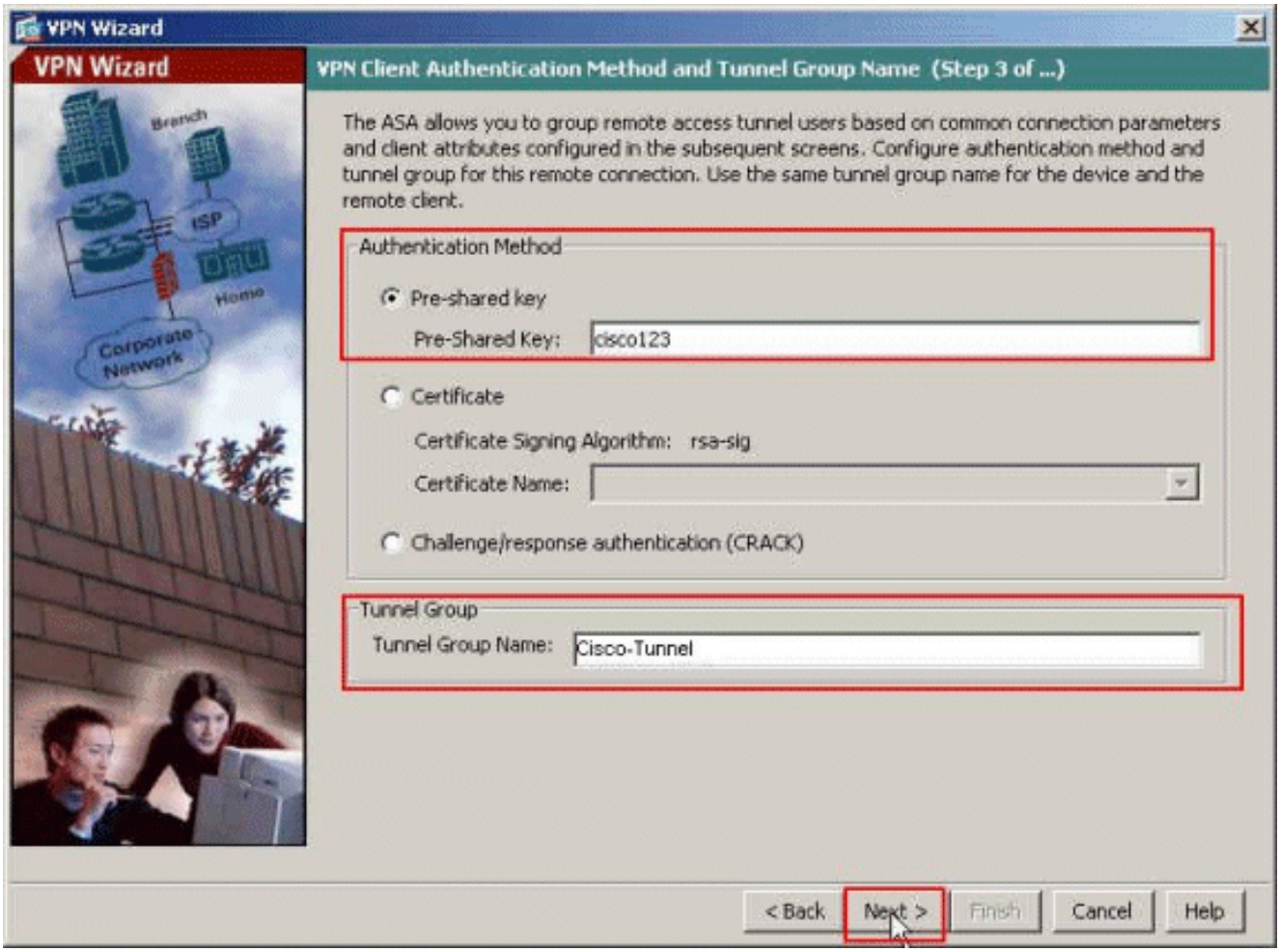
2. Wählen Sie die **VPN-Tunnel-Schnittstelle** nach Bedarf (**außerhalb**, in diesem Beispiel) aus, und stellen Sie außerdem sicher, dass das Kontrollkästchen neben **Eingehende IPsec-Sitzungen aktivieren, um Schnittstellenzugriffslisten zu umgehen** aktiviert
   ist.



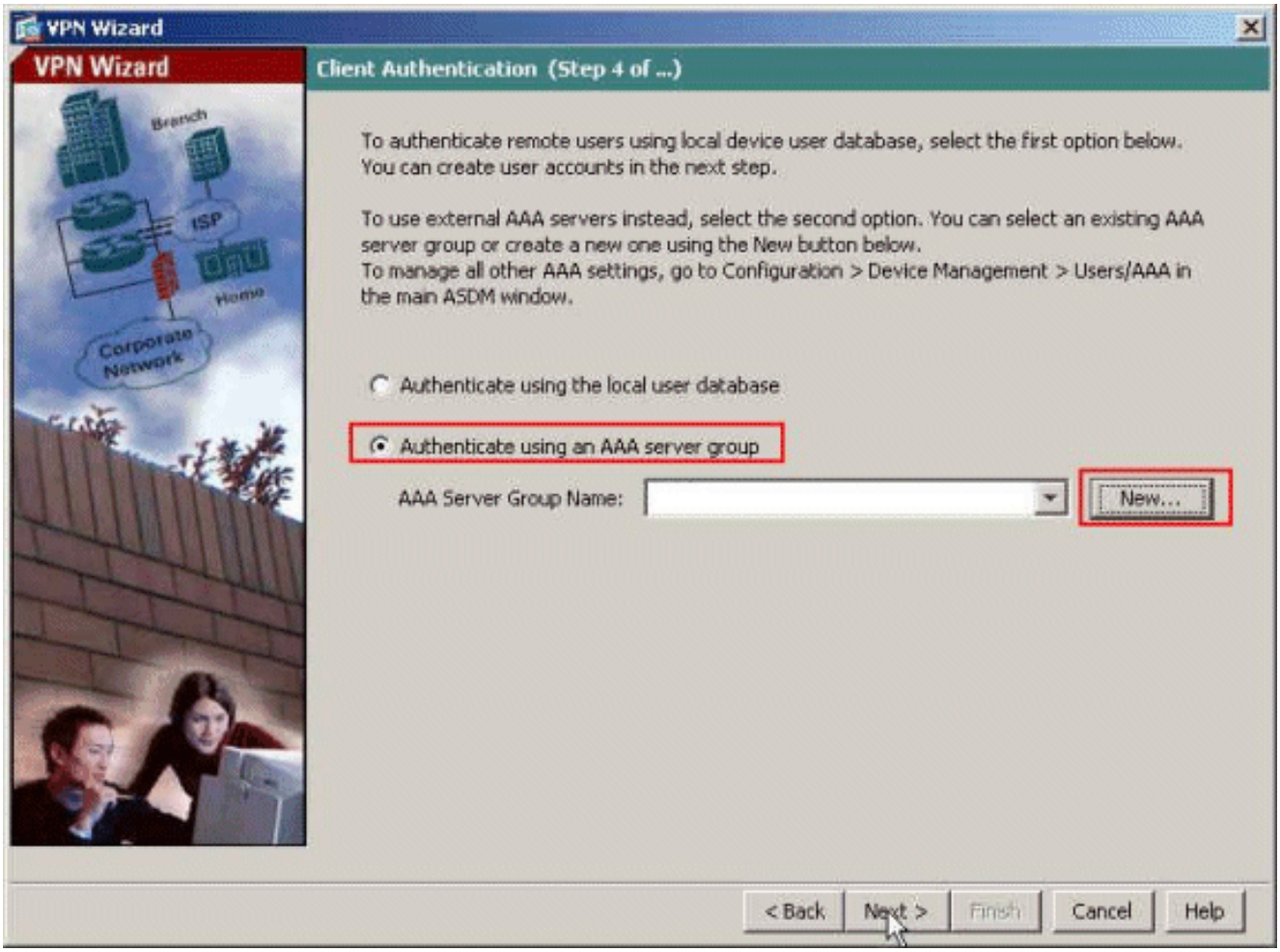
3. Wählen Sie den VPN-Client-Typ als **Cisco VPN Client, Version 3.x oder höher aus**. Klicken Sie auf
   Weiter.



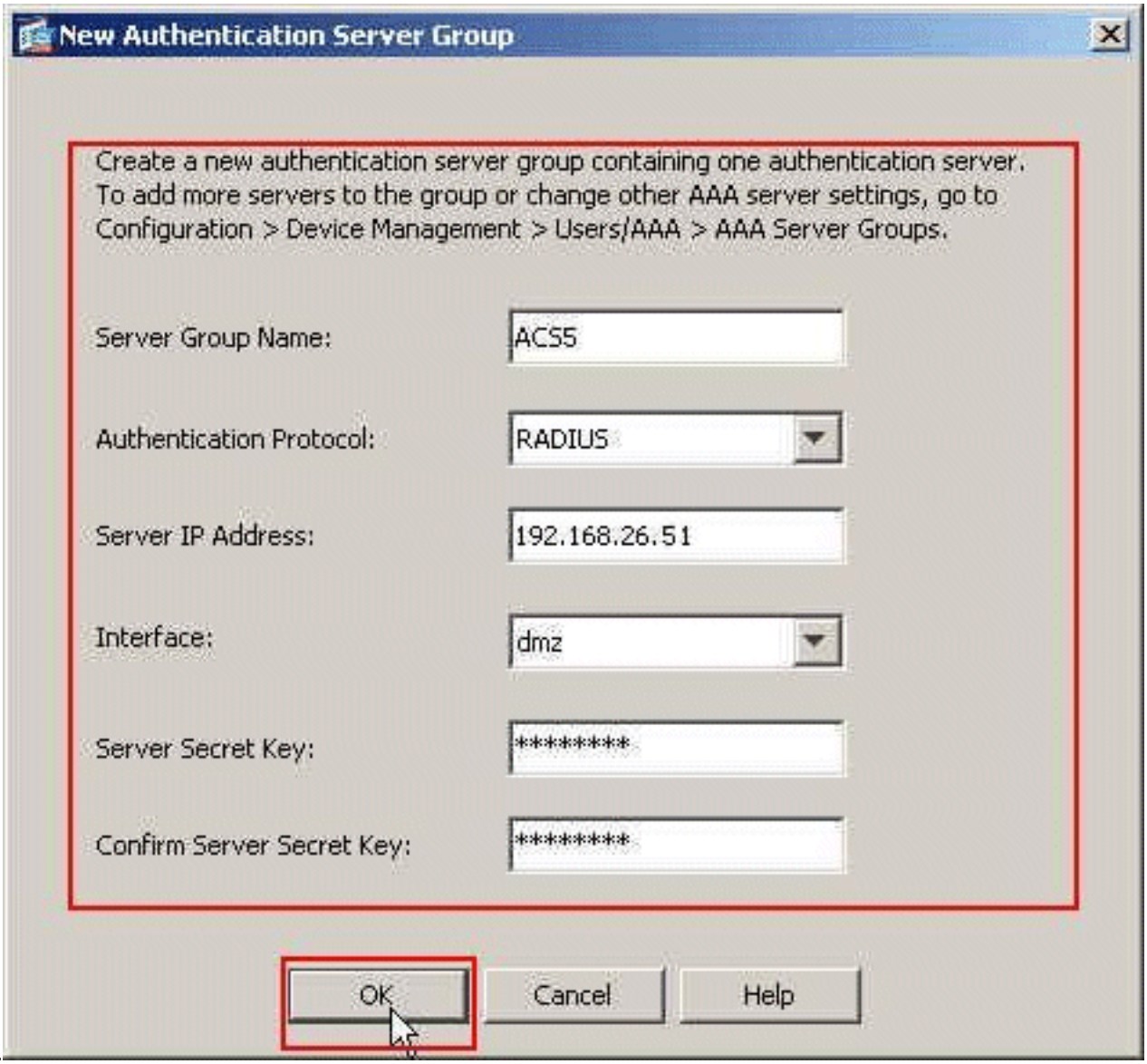
4. Wählen Sie die **Authentifizierungsmethode** aus, und geben Sie die Authentifizierungsinformationen an. Die hier verwendete Authentifizierungsmethode ist **Pre-Shared Key**. Geben Sie außerdem einen **Tunnelgruppennamen** im dafür vorgesehenen Bereich an. Der **hier** verwendete **Pre-shared Key** ist **cisco123**, und der **hier** verwendete Tunnelgruppenname **Cisco-Tunnel**. Klicken Sie auf **Weiter**.



5. Wählen Sie aus, ob Remote-Benutzer in der lokalen Benutzerdatenbank oder in einer externen AAA-Servergruppe authentifiziert werden sollen. Wählen Sie **Authentifizieren mithilfe einer AAA-Servergruppe aus**. Klicken Sie neben dem Feld "AAA-Servergruppenname" auf **Neu**, um einen neuen AAA-Servergruppennamen zu erstellen.

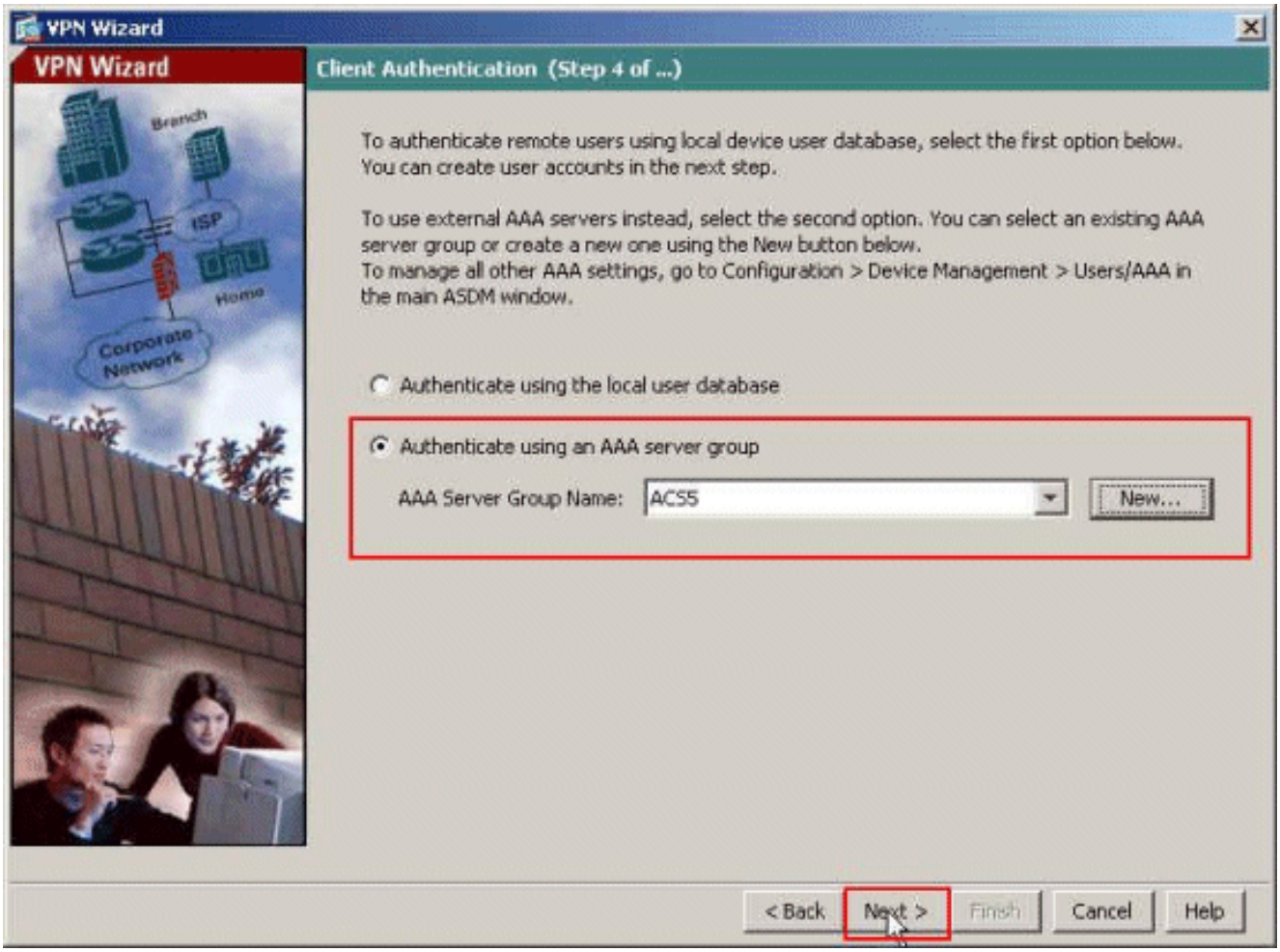


6. Geben Sie in den angegebenen Leerzeichen den Namen der Servergruppe, das Authentifizierungsprotokoll, die IP-Adresse des Servers, den Namen der Schnittstelle und den Schlüssel des Servergeheimnisses an, und klicken Sie auf

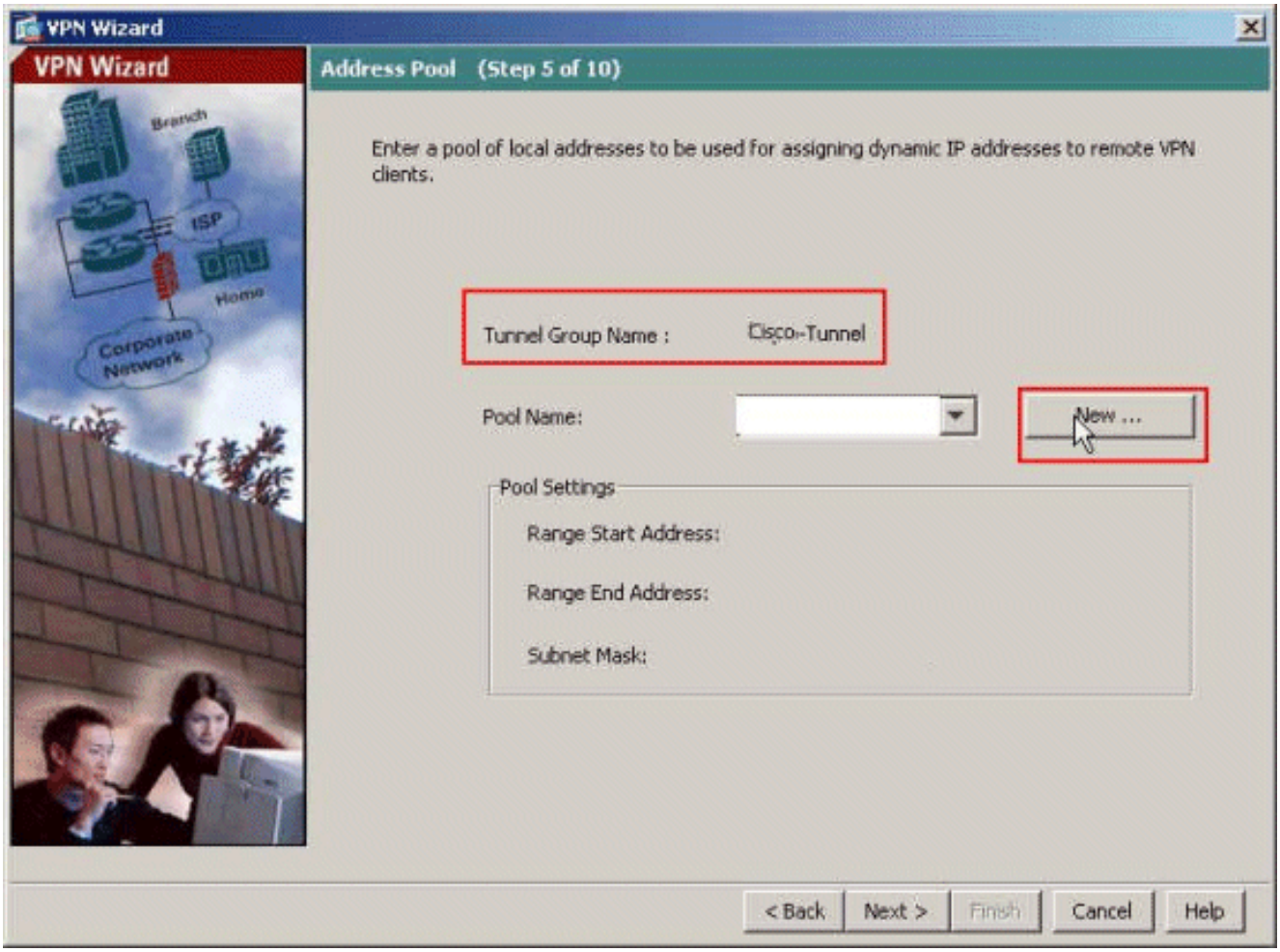


OK.

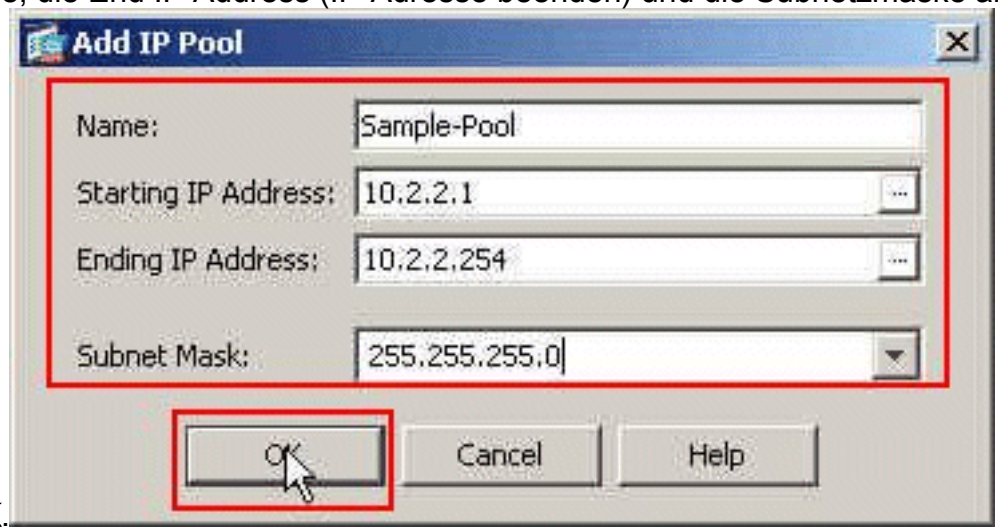
7. Klicken Sie auf **Weiter**.



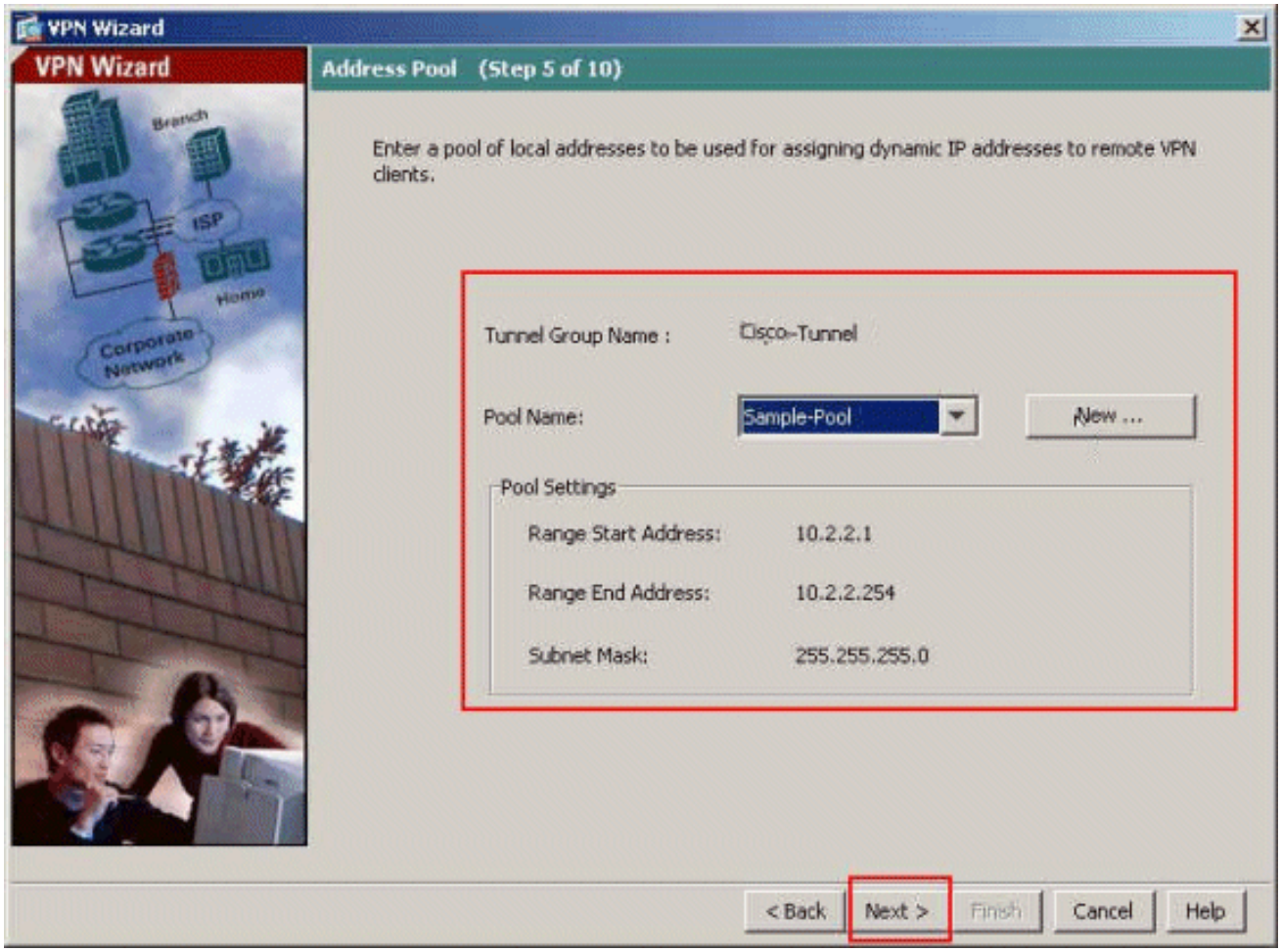
8. Definieren Sie einen Pool lokaler Adressen, der Remote-VPN-Clients bei der Verbindung dynamisch zugewiesen wird. Klicken Sie auf **Neu**, um einen neuen Pool lokaler Adressen zu erstellen.



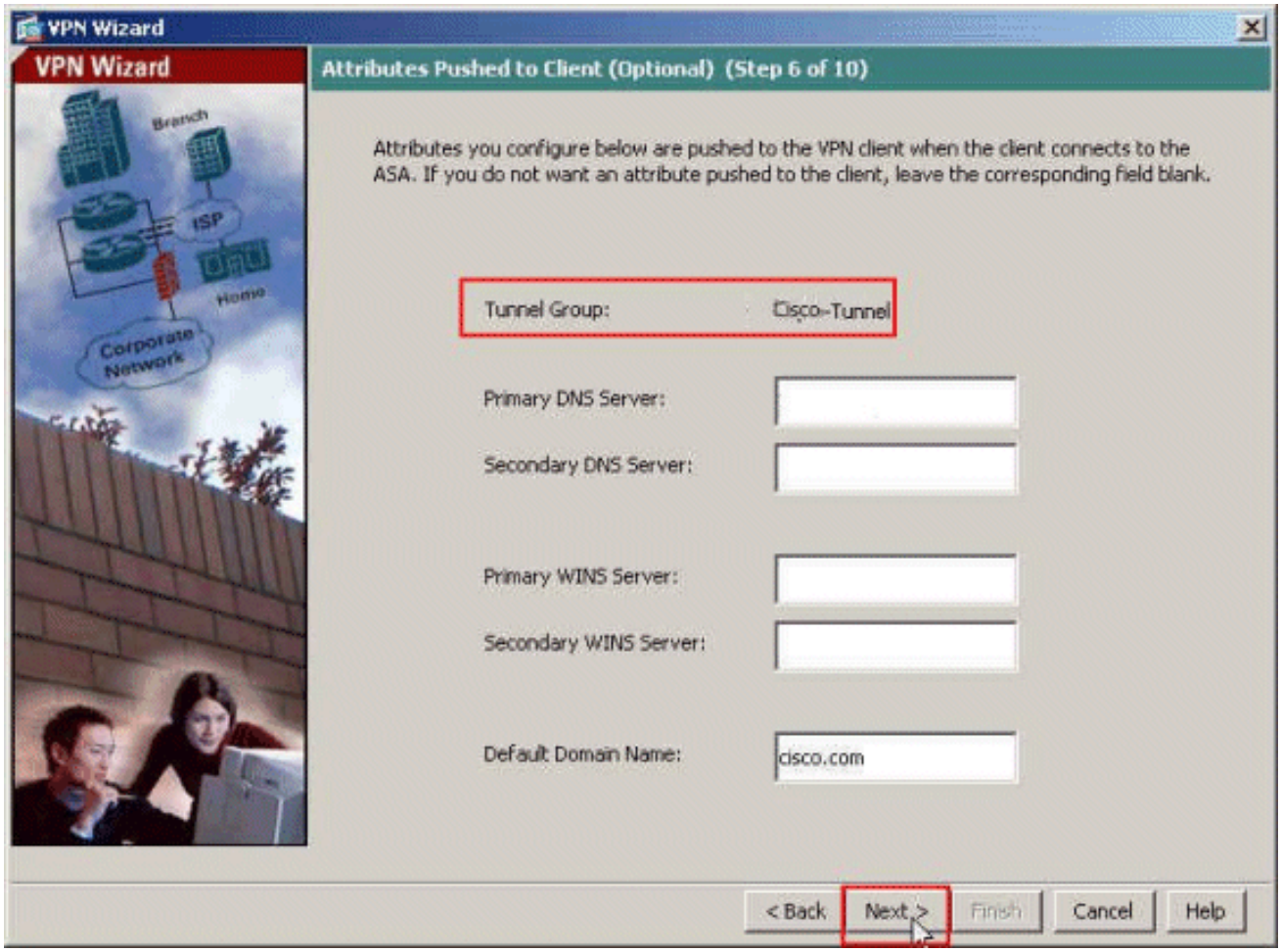
9. Geben Sie im Fenster Add IP Pool (IP-Pool hinzufügen) den Poolnamen, die Start-IP-Adresse, die End IP Address (IP-Adresse beenden) und die Subnetzmaske an. Klicken Sie auf **OK**.



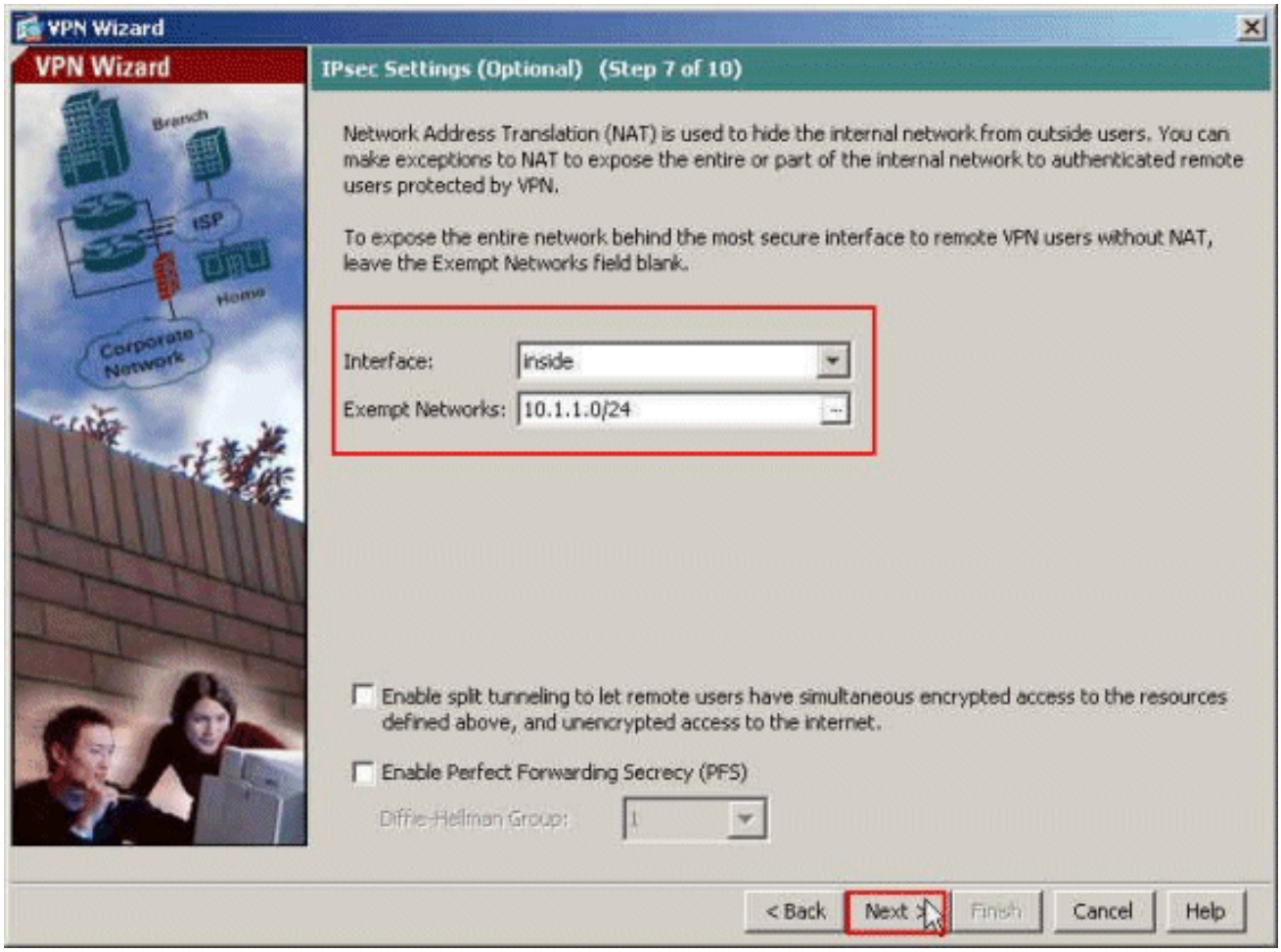
10. Wählen Sie den Poolnamen aus der Dropdown-Liste aus, und klicken Sie auf **Weiter**. Der Poolname für dieses Beispiel ist **Sample-Pool**, der in Schritt 9 erstellt wurde.



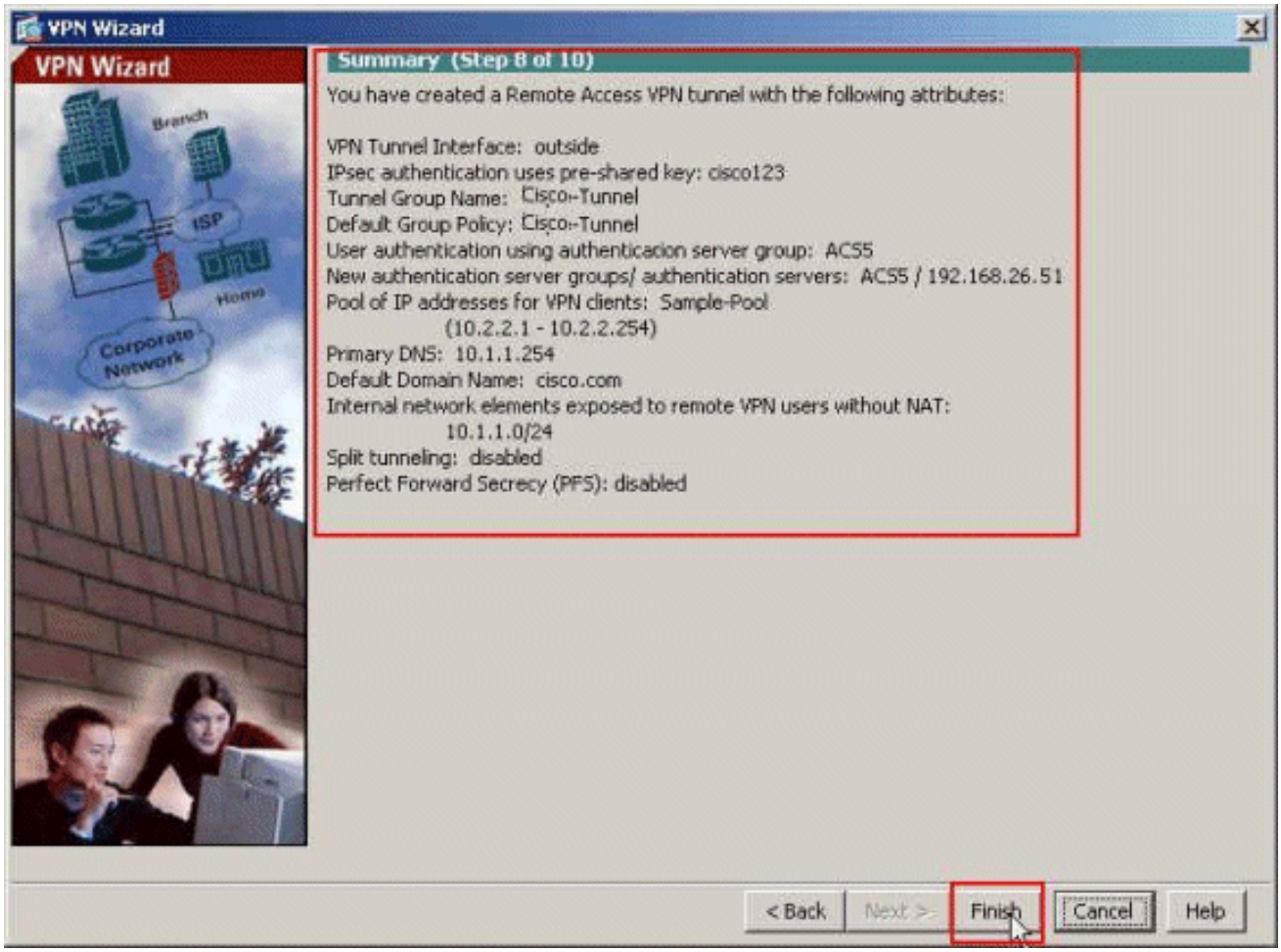
11. *Optional:* Geben Sie die DNS- und WINS-Serverinformationen und einen Standard-Domänennamen an, der an Remote-VPN-Clients übertragen werden soll.



12. Geben Sie an, welche internen Hosts oder Netzwerke ggf. Remote-VPN-Benutzern ausgesetzt werden sollen. Klicken Sie auf **Weiter**, nachdem Sie den Schnittstellennamen und die Netzwerke angegeben haben, für die im Feld "Netzwerke ausnehmen" eine Ausnahme gilt.Wenn Sie diese Liste leer lassen, können Remote-VPN-Benutzer auf das gesamte interne Netzwerk der ASA zugreifen.In diesem Fenster können Sie auch Split-Tunneling aktivieren. Split-Tunneling verschlüsselt den Datenverkehr mit den zuvor in diesem Verfahren definierten Ressourcen und bietet im Allgemeinen unverschlüsselten Zugriff auf das Internet, indem dieser Datenverkehr nicht getunnelt wird. Wenn Split-Tunneling *nicht* aktiviert ist, wird der gesamte Datenverkehr von Remote-VPN-Benutzern an die ASA getunnelt. Je nach Konfiguration kann dies zu einer sehr hohen Bandbreite und einem hohen Prozessor
führen.



13. In diesem Fenster wird eine Zusammenfassung der von Ihnen ergriffenen Maßnahmen angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie mit Ihrer Konfiguration zufrieden sind.



Konfigurieren der ASA mit CLI

Dies ist die CLI-Konfiguration:

Ausführen der Konfiguration auf dem ASA-Gerät

```
ASA# sh run
ASA Version 8.4(3)
!
!--- Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !---
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
!--- Output is suppressed. boot system disk0:/asa843-
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any !--- This is the Access-List whose name will be sent
by !--- RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
access-list new extended deny ip any any
pager lines 24
logging enable
```

```
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool Sample-Pool 10.2.2.1-10.2.2.254 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-647.bin no asdm history enable arp timeout
14400 !--- Specify the NAT from internal network to the
Sample-Pool. nat (inside,outside) source static
NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
destination static NETWORK_OBJ_10.2.2.0_24
NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup
access-group OUTIN in interface outside !--- Create the
AAA server group "ACS5" and specify the protocol as
RADIUS. !--- Specify the ACS 5.x server as a member of
the "ACS5" group and provide the !--- location and key.
aaa-server ACS5 protocol radius
aaa-server ACS5 (dmz) host 192.168.26.51
timeout 5
key *****

aaa authentication http console LOCAL
http server enable 2003
http 0.0.0.0 0.0.0.0 inside


!--- PHASE 2 CONFIGURATION ---! !--- The encryption &
hashing types for Phase 2 are defined here. We are using
!--- all the permutations of the PHASE 2 parameters.
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-
aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-
aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-
aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-
aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes
esp-md5-hmac


!--- Defines a dynamic crypto map with !--- the
specified transform-sets created earlier. We are
specifying all the !--- transform-sets. crypto dynamic-
map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-
set
   ESP-AES-128-SHA ESP-AES-128-MD5
```

```
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_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 policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside

crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
```

```
group 2
lifetime 86400

crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 130
authentication crack
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400


webvpn
group-policy Cisco-Tunnel internal
group-policy Cisco-Tunnel attributes
vpn-tunnel-protocol ikev1
```

```
default-domain value cisco.com
username admin password CdOTKv3uhDhHIw3A encrypted
privilege 15
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (ACS5) with the tunnel group. tunnel-group Cisco-
Tunnel type remote-access tunnel-group Cisco-Tunnel
general-attributes
address-pool Sample-Pool
authentication-server-group ACS5
default-group-policy Cisco-Tunnel

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group Cisco-Tunnel ipsec-
attributes
ikev1 pre-shared-key *****

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```

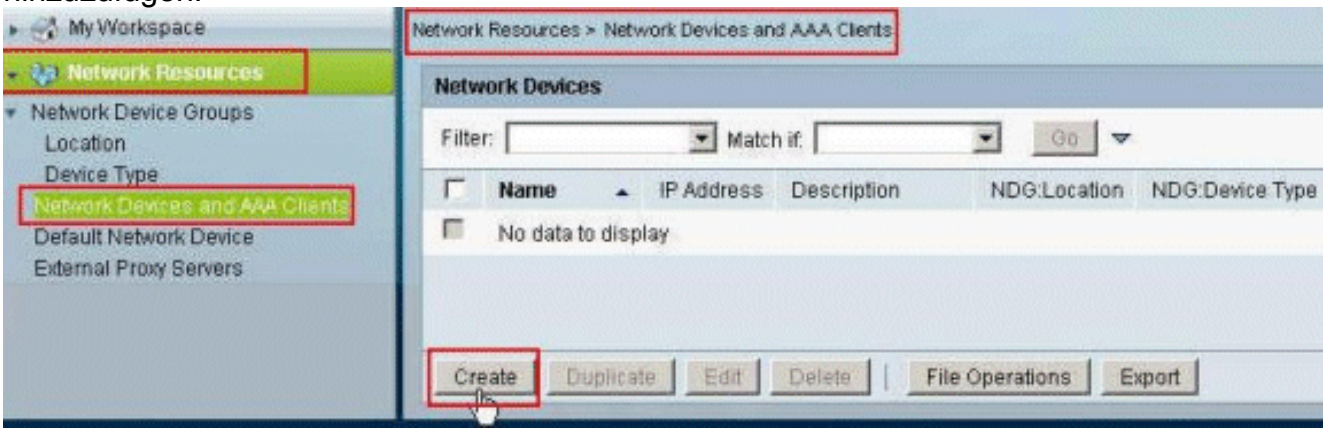
ACS für herunterladbare ACL für individuelle Benutzer konfigurieren

Sie können herunterladbare Zugriffslisten auf Cisco Secure ACS 5.x als benanntes Berechtigungsobjekt konfigurieren und sie dann einem Autorisierungsprofil zuweisen, das im Ergebnisabschnitt der Regel im Access-Service ausgewählt wird.

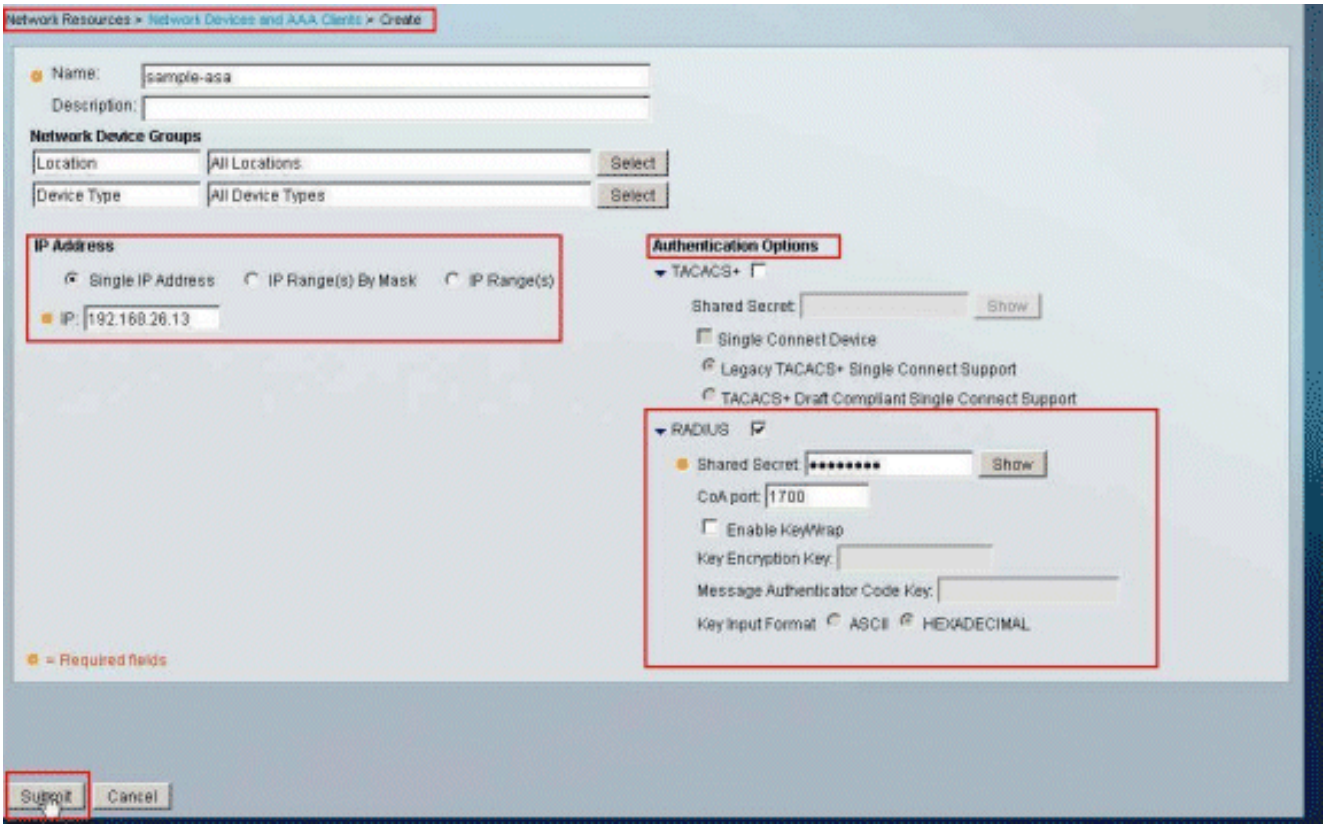
In diesem Beispiel authentifiziert sich der IPsec VPN-Benutzer **cisco** erfolgreich, und der RADIUS-Server sendet eine herunterladbare Zugriffsliste an die Sicherheits-Appliance. Der Benutzer "cisco" kann nur auf den Server 10.1.1.2 zugreifen und verweigert allen anderen Zugriff. Informationen zur Verifizierung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

Gehen Sie wie folgt vor, um den RADIUS-Client in einem Cisco Secure ACS 5.x zu konfigurieren:

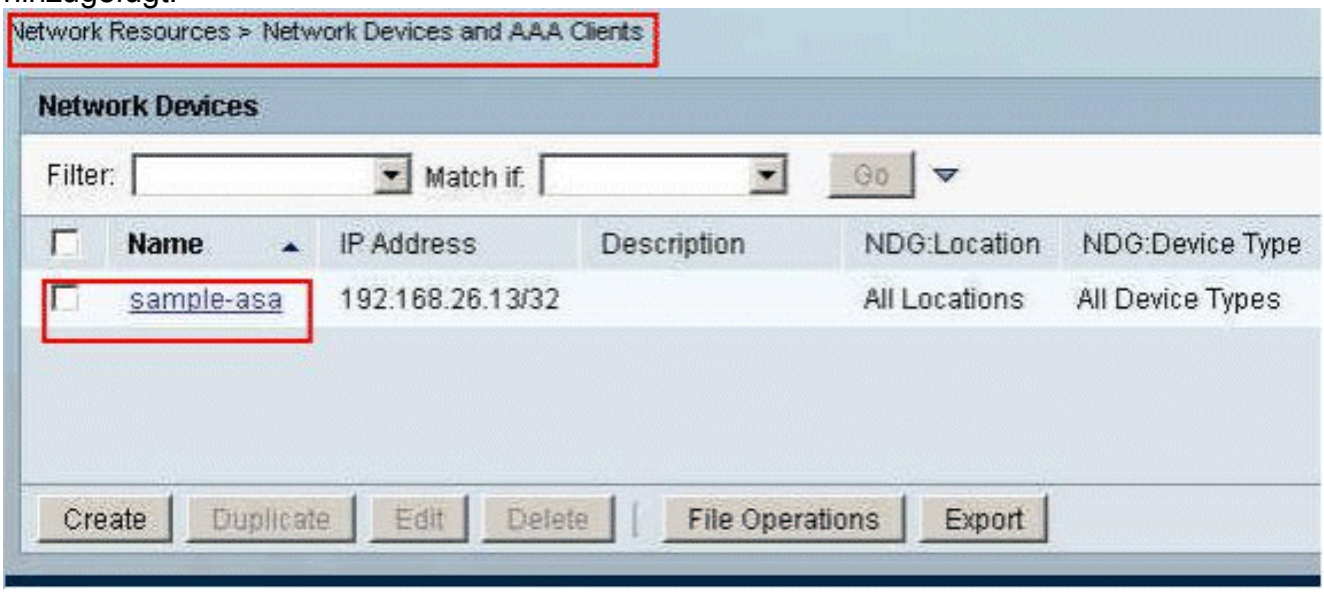
1. Wählen Sie **Netzwerkressourcen > Netzwerkgeräte und AAA-Clients**, und klicken Sie auf **Erstellen**, um einen Eintrag für die ASA in der RADIUS-Serverdatenbank hinzuzufügen.



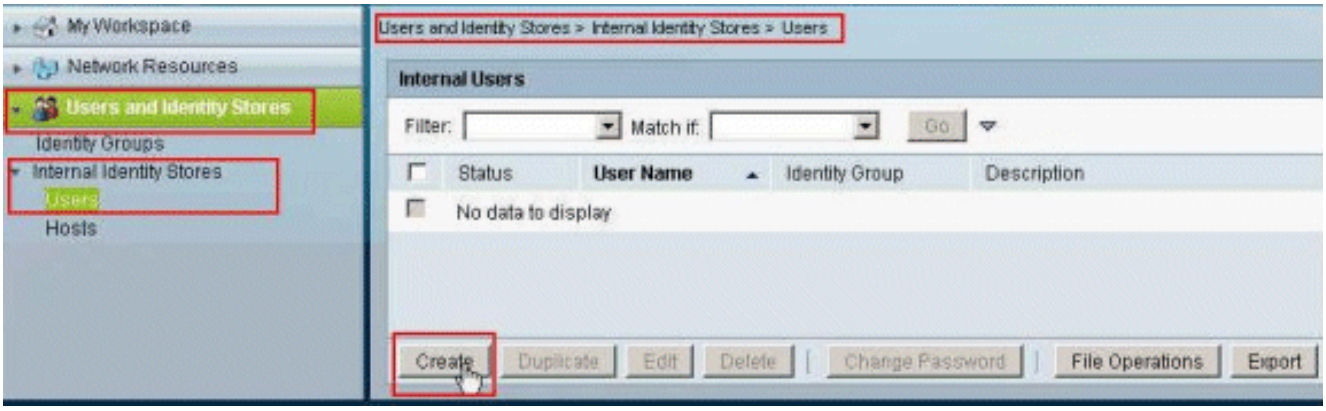
2. Geben Sie einen lokal signifikanten Namen für die ASA ein (**Beispiel-asa** in diesem Beispiel), und geben Sie dann **192.168.26.13** in das IP-Adressfeld ein. Wählen Sie **RADIUS** im Abschnitt "Authentifizierungsoptionen" aus, indem Sie das **RADIUS-**Kontrollkästchen aktivieren und **cisco123** für das Feld "Freier geheimer Schlüssel" eingeben. Klicken Sie auf **Senden**.



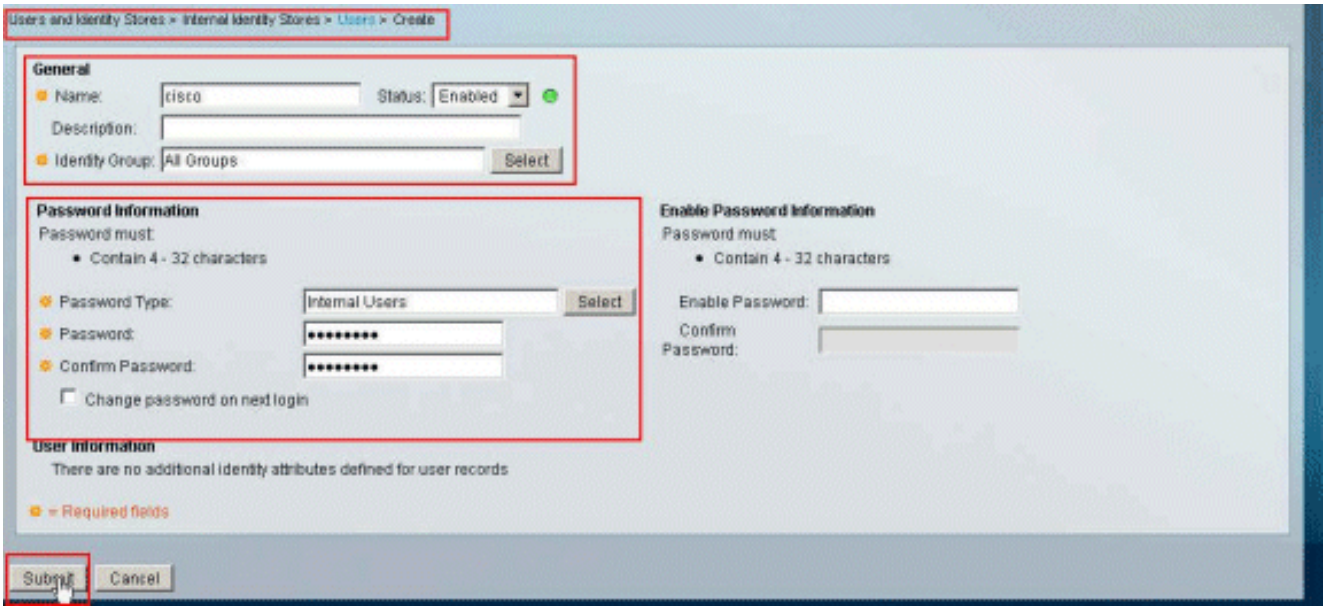
3. Die ASA wird der RADIUS-Server-Datenbank (ACS) erfolgreich hinzugefügt.



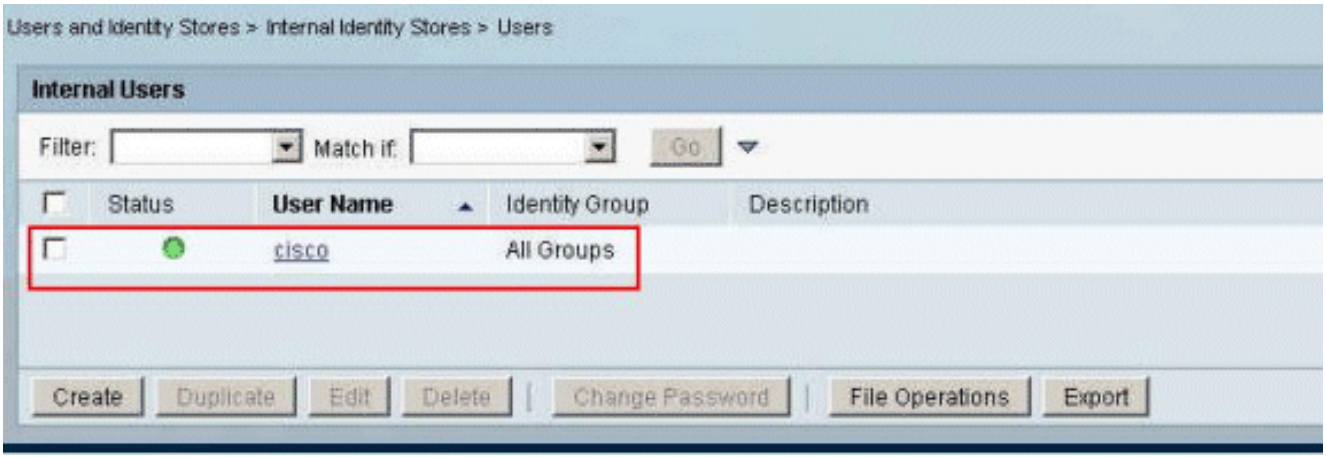
4. Wählen Sie **Benutzer und Identity Stores > Internal Identity Stores > Users aus**, und klicken Sie auf **Create** (Erstellen), um einen Benutzer in der lokalen Datenbank des ACS für die VPN-Authentifizierung zu erstellen.



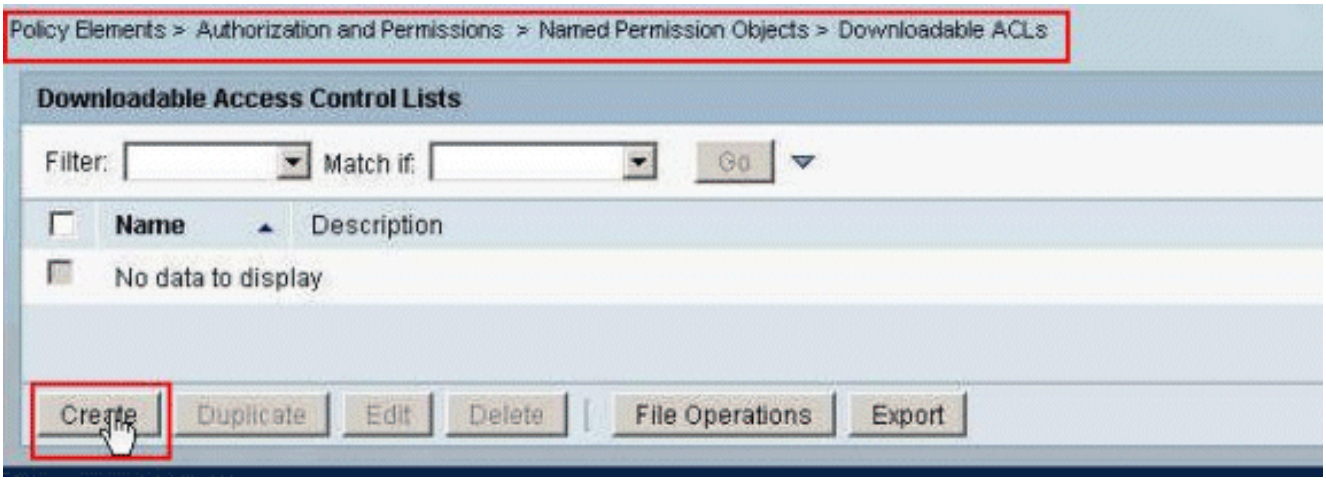
5. Geben Sie den Benutzernamen **cisco ein**. Wählen Sie den Kennworttyp als **Interne Benutzer aus**, und geben Sie das Kennwort ein (in diesem Beispiel **cisco123**). Bestätigen Sie das Kennwort, und klicken Sie auf **Senden**.



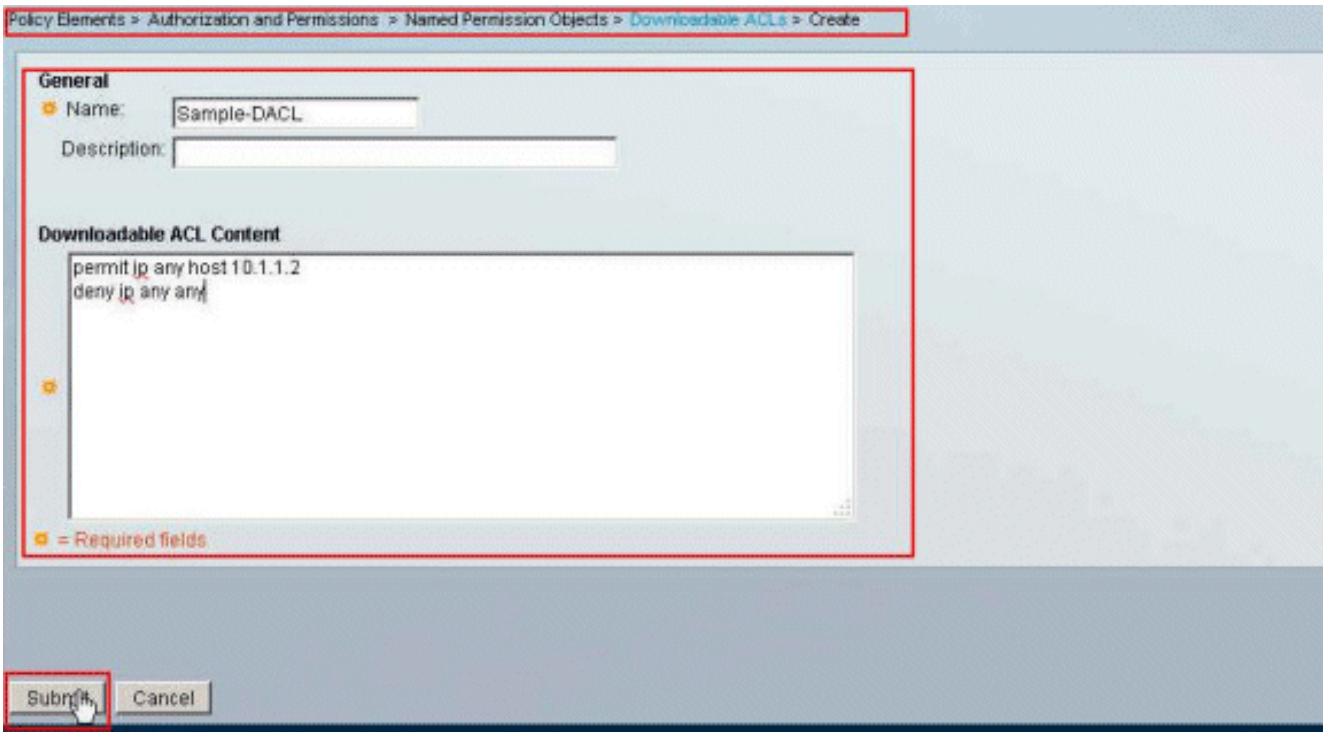
6. Der Benutzer **cisco** wurde erfolgreich erstellt.



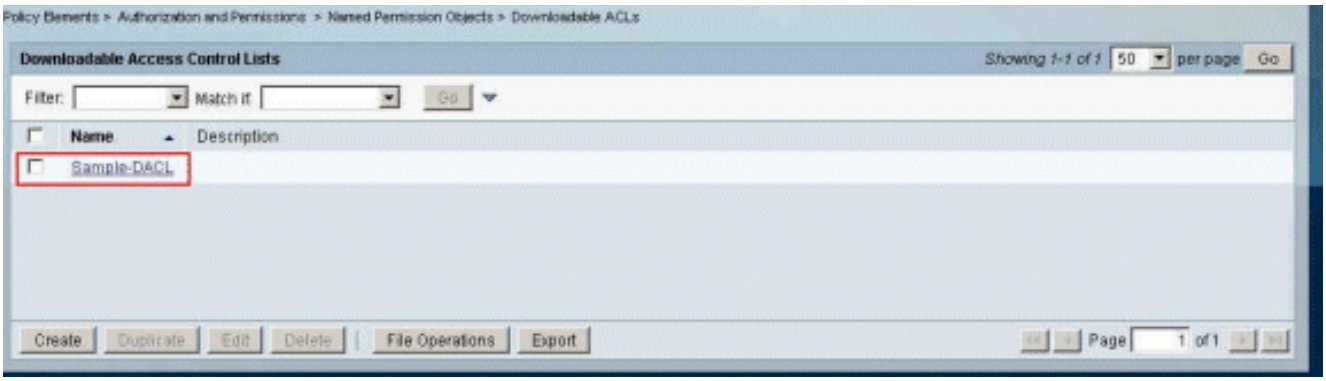
7. Um eine herunterladbare ACL zu erstellen, wählen Sie **Richtlinienelemente > Autorisierung und Berechtigungen > Named Permission Objects > Download ACLs aus**, und klicken Sie dann auf **Erstellen.**



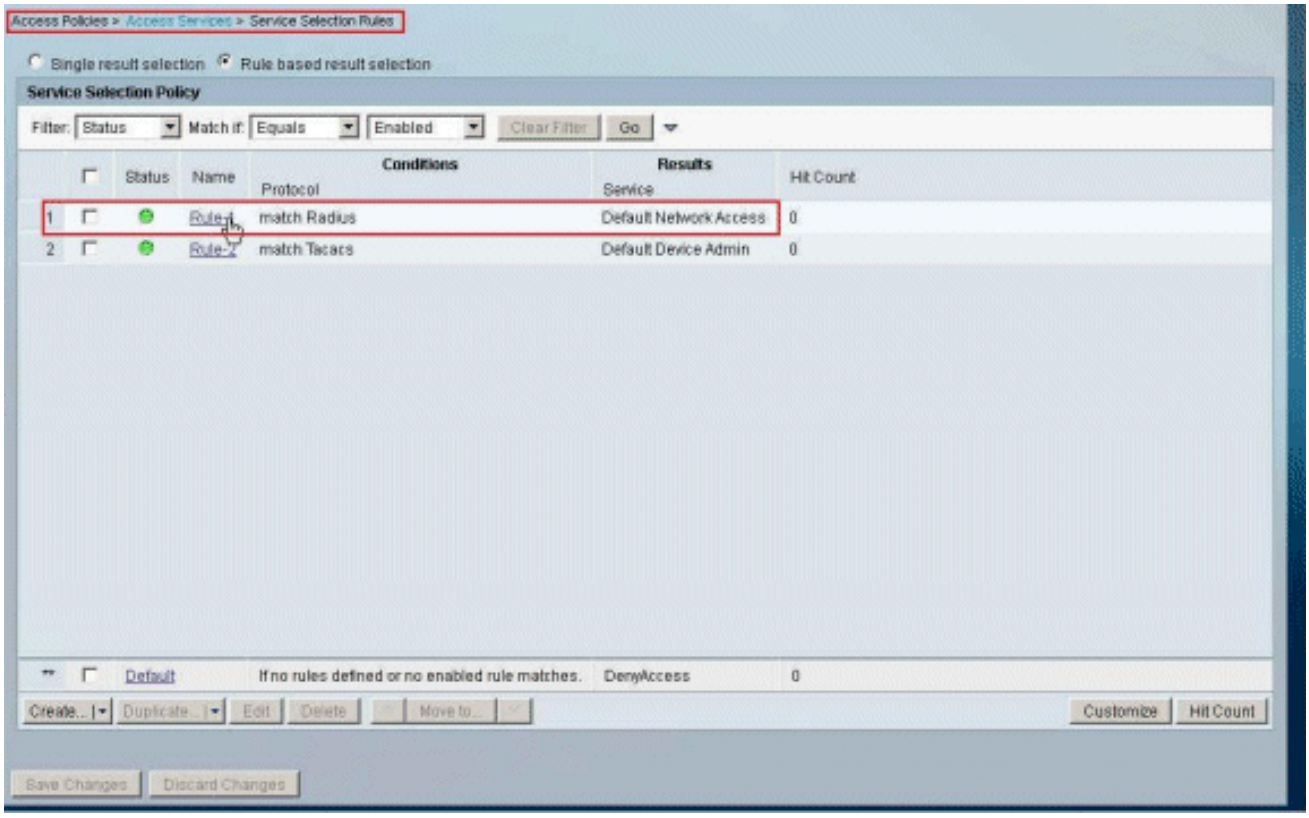
8. Geben Sie den **Namen** für die herunterladbare ACL sowie den **ACL-Inhalt an**. Klicken Sie auf **Senden**.



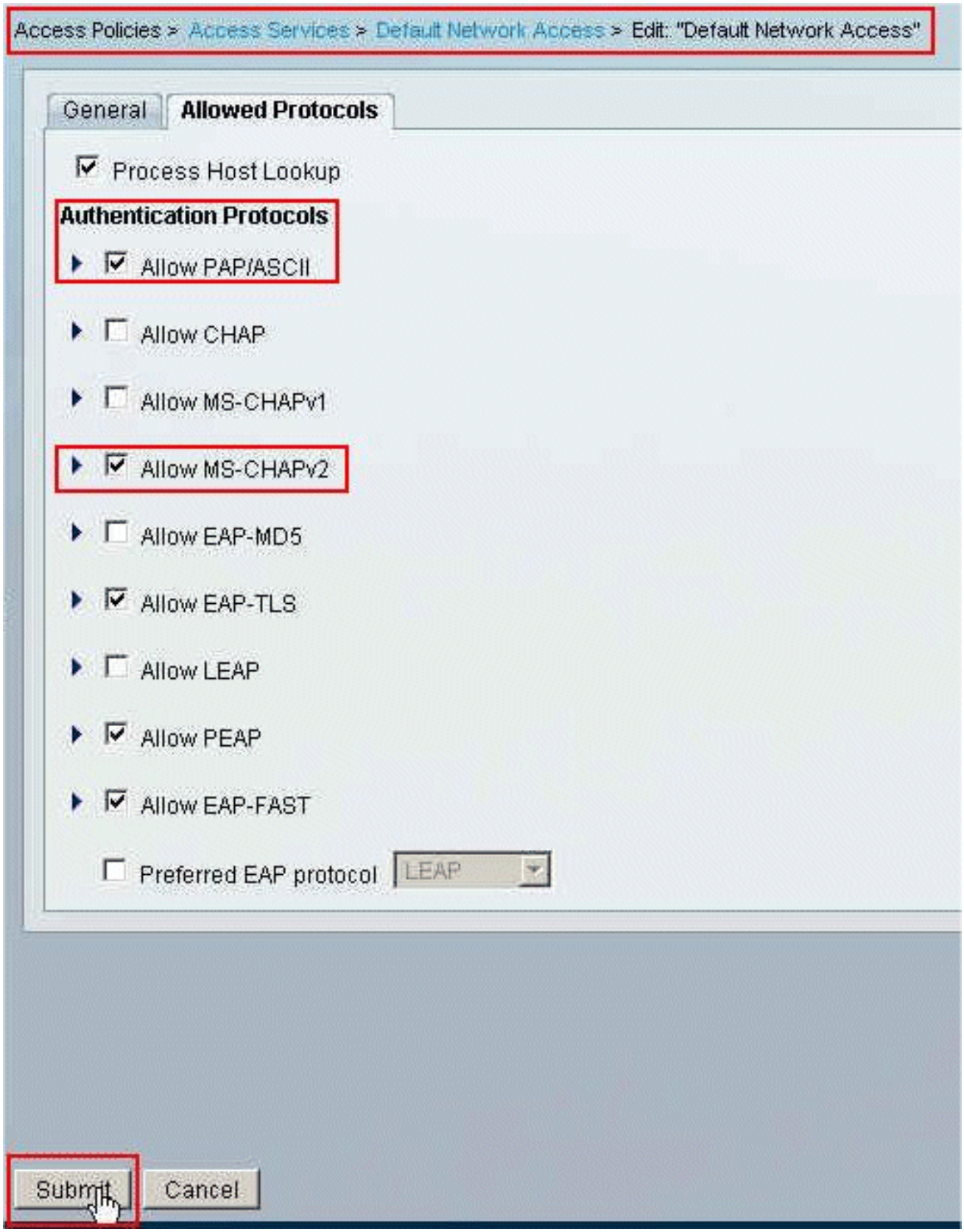
9. Die **Beispiel-DACL** zum Herunterladen wurde erfolgreich erstellt.



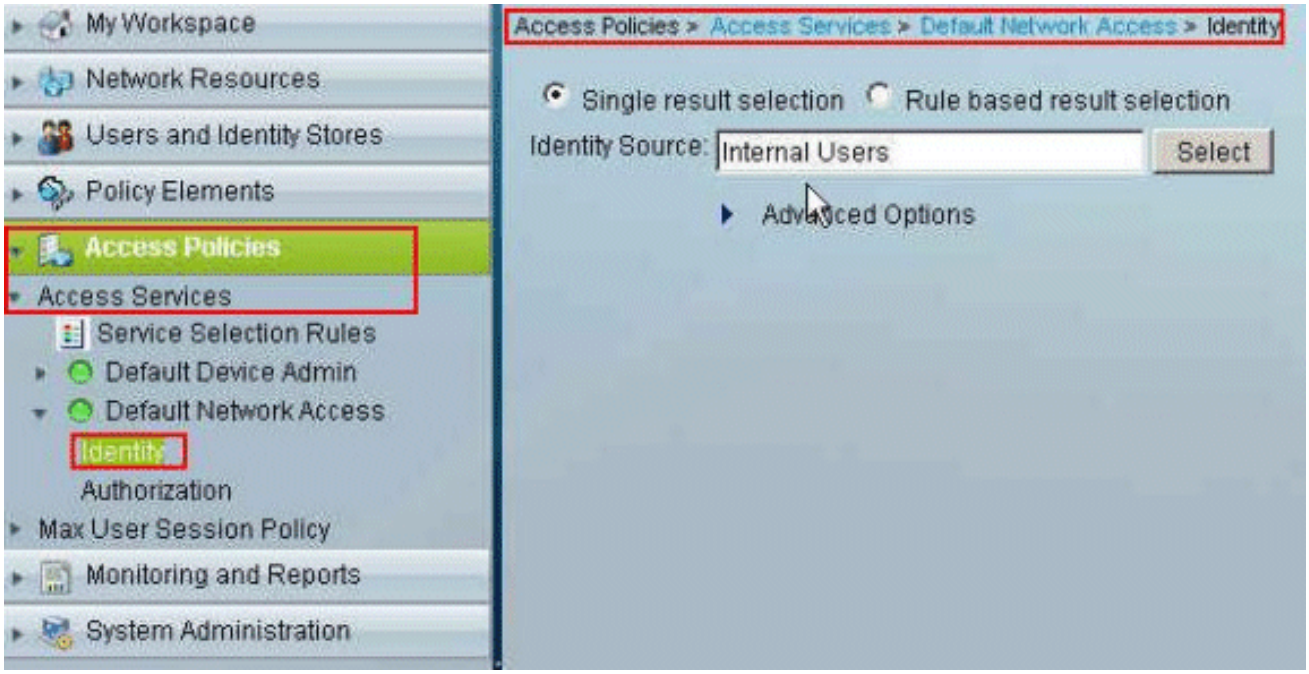
10. Um die Zugriffsrichtlinien für die VPN-Authentifizierung zu konfigurieren, wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Service Selection Rules (Dienstauswahlregeln) aus**, und legen Sie fest, welcher Service für das RADIUS-Protokoll verwendet wird. In diesem Beispiel stimmt **Regel 1 mit RADIUS** überein, und der Standard-Netzwerkzugriff erfüllt die RADIUS-
Anforderung.



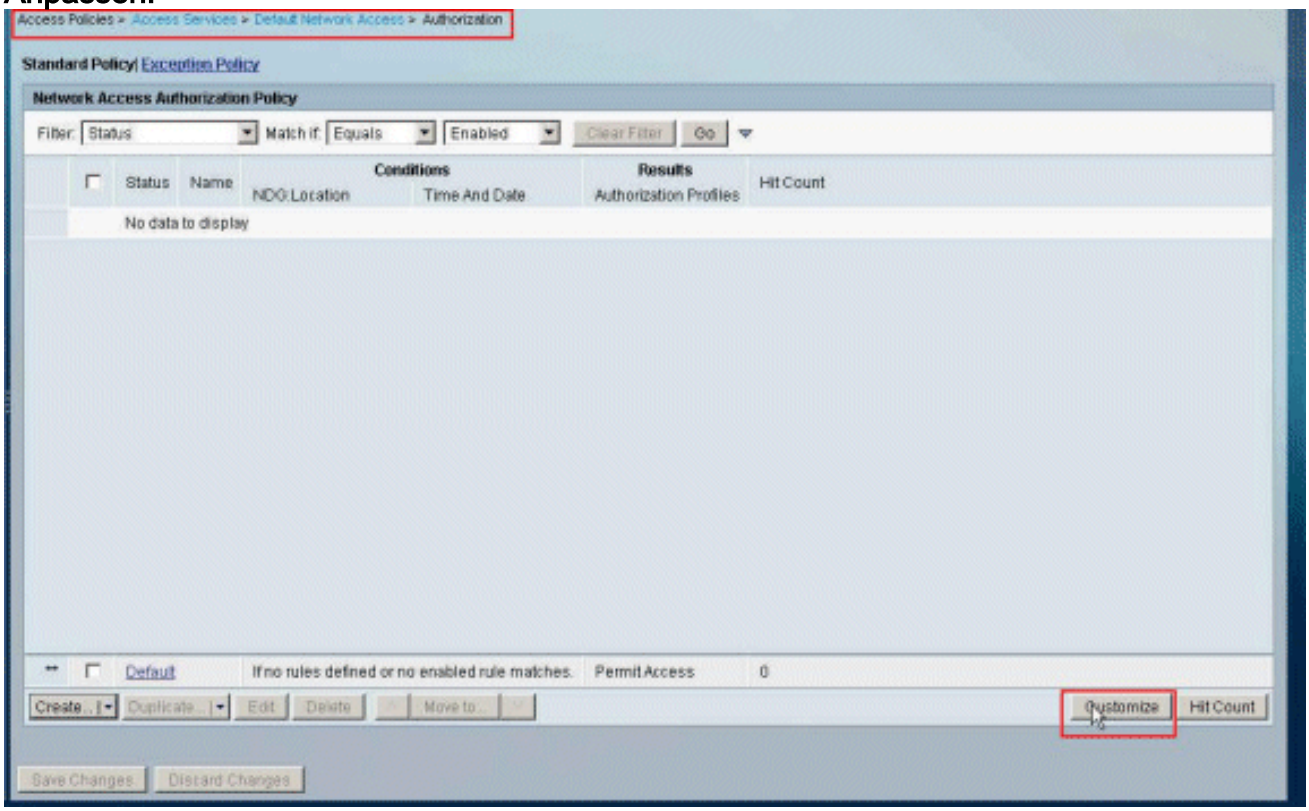
11. Wählen Sie den aus Schritt 10 bestimmten **Zugriffsdienst** aus. In diesem Beispiel wird **Standard-Netzwerkzugriff** verwendet. Wählen Sie die Registerkarte **Zulässige Protokolle aus**, und stellen Sie sicher, dass **PAP/ASCII** und **MS-CHAPv2 zulassen** ausgewählt sind.Klicken Sie auf
Senden.



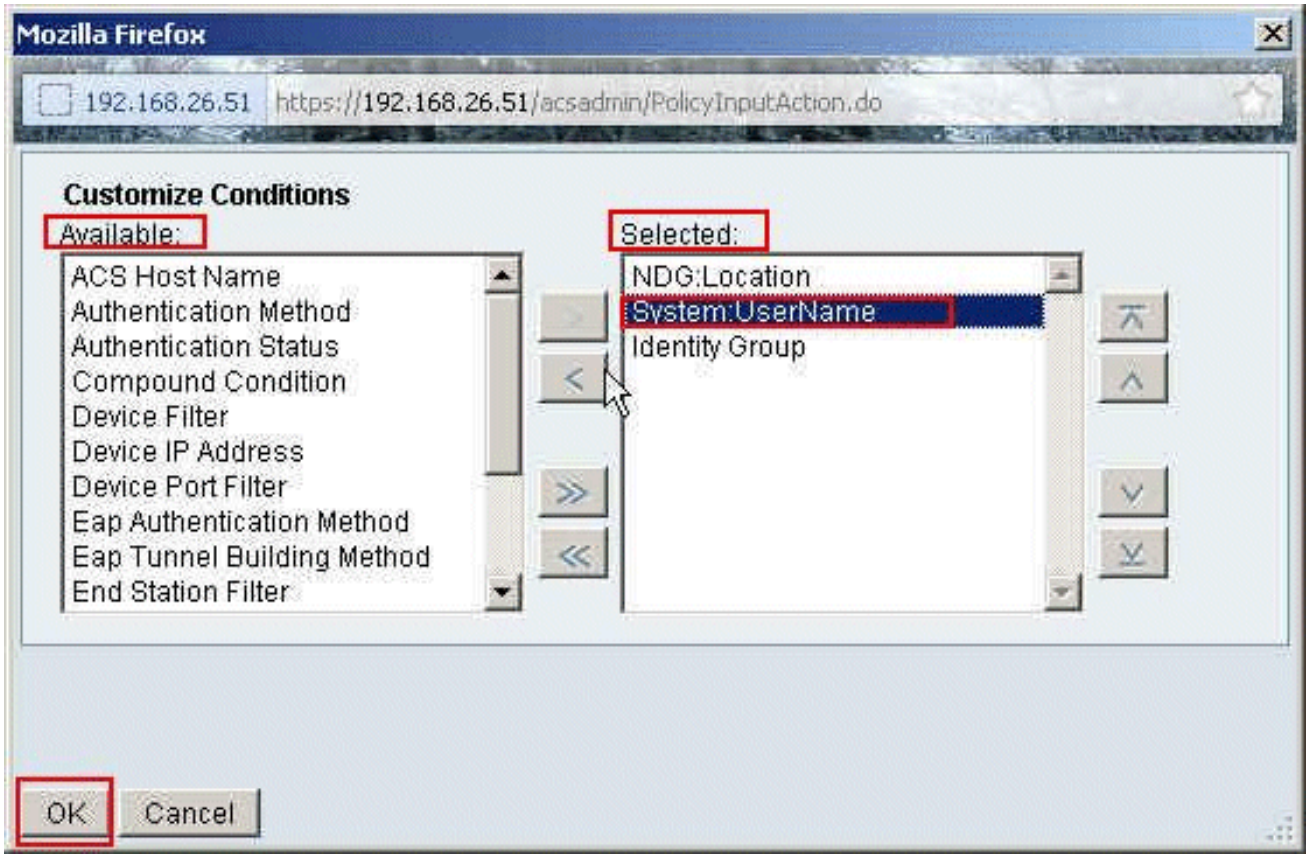
12. Klicken Sie auf den **Identitätsbereich** der **Zugriffsdienste**, und stellen Sie sicher, dass **Interne Benutzer** als Identitätsquelle ausgewählt ist. In diesem Beispiel haben wir den Standard-Netzwerkzugriff
genommen.



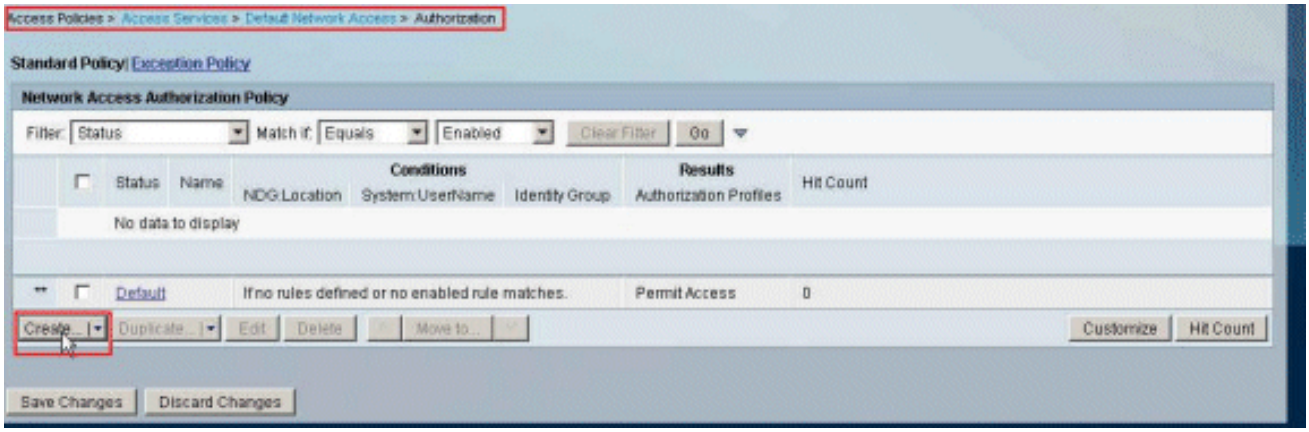
13. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Autorisierung aus**, und klicken Sie auf **Anpassen.**



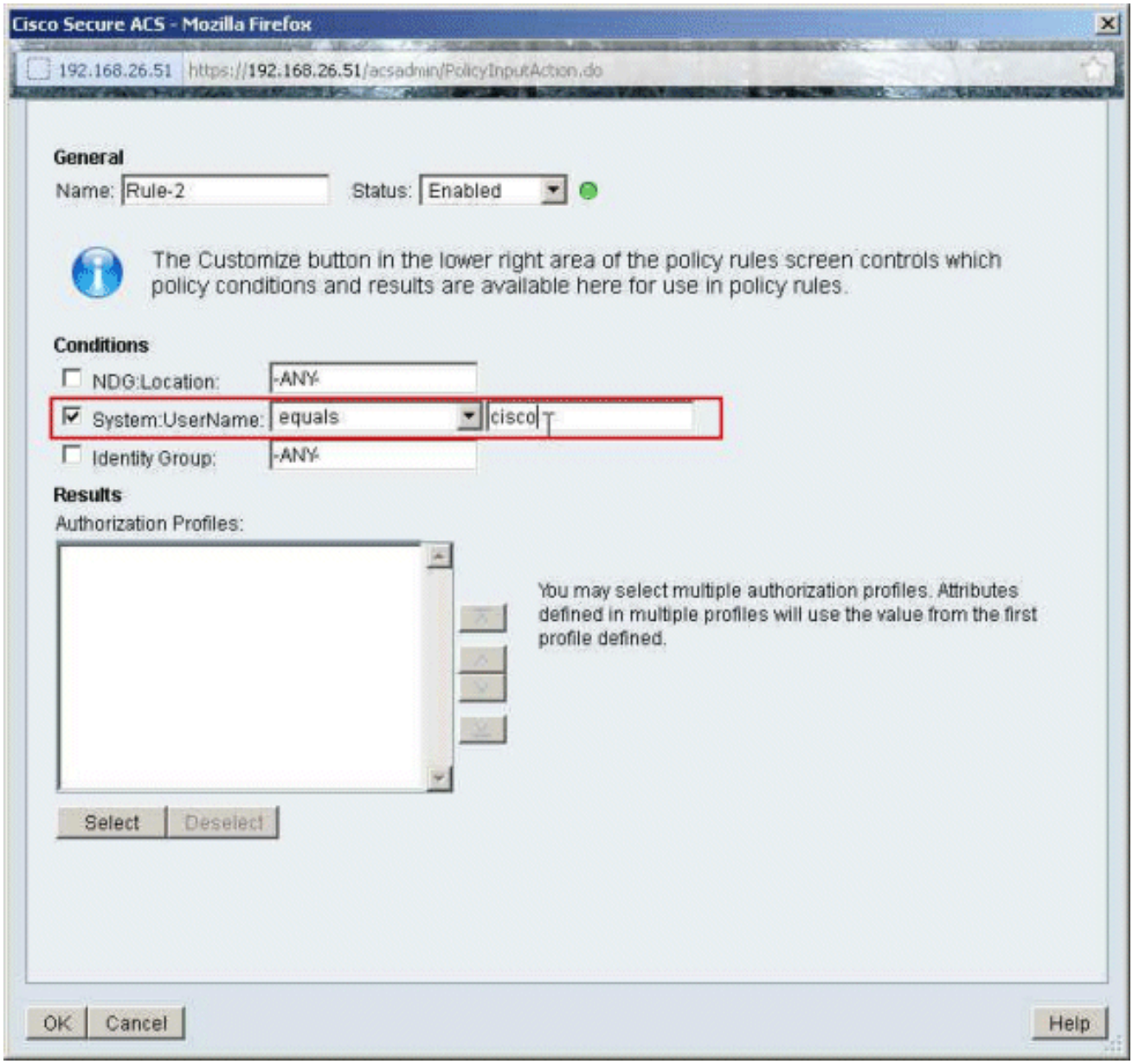
14. Verschieben Sie **System:UserName** aus der Spalte **Verfügbar** in die **Spalte Ausgewählt**, und klicken Sie auf **OK**.



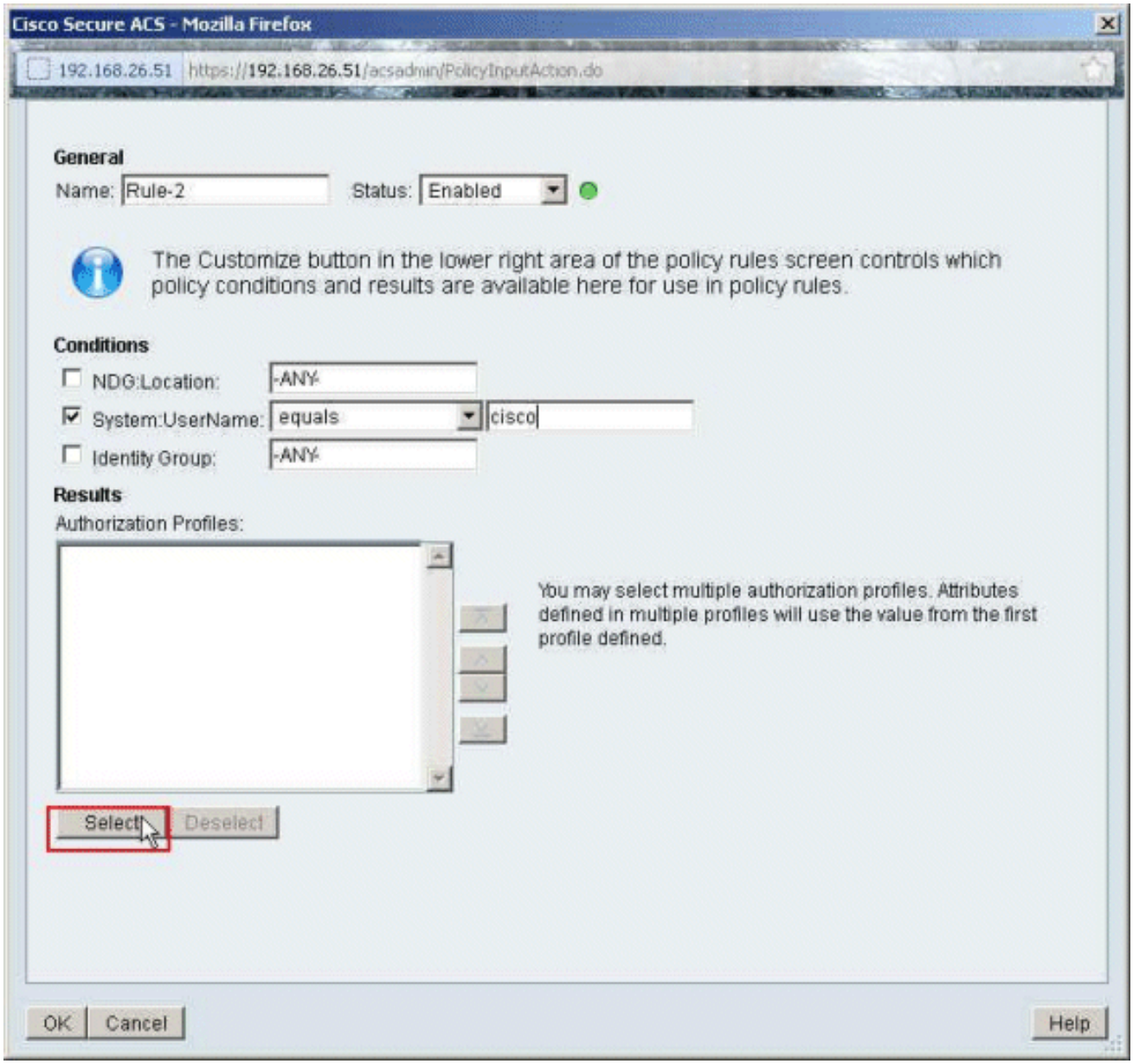
15. Klicken Sie auf **Erstellen**, um eine neue Regel zu erstellen.



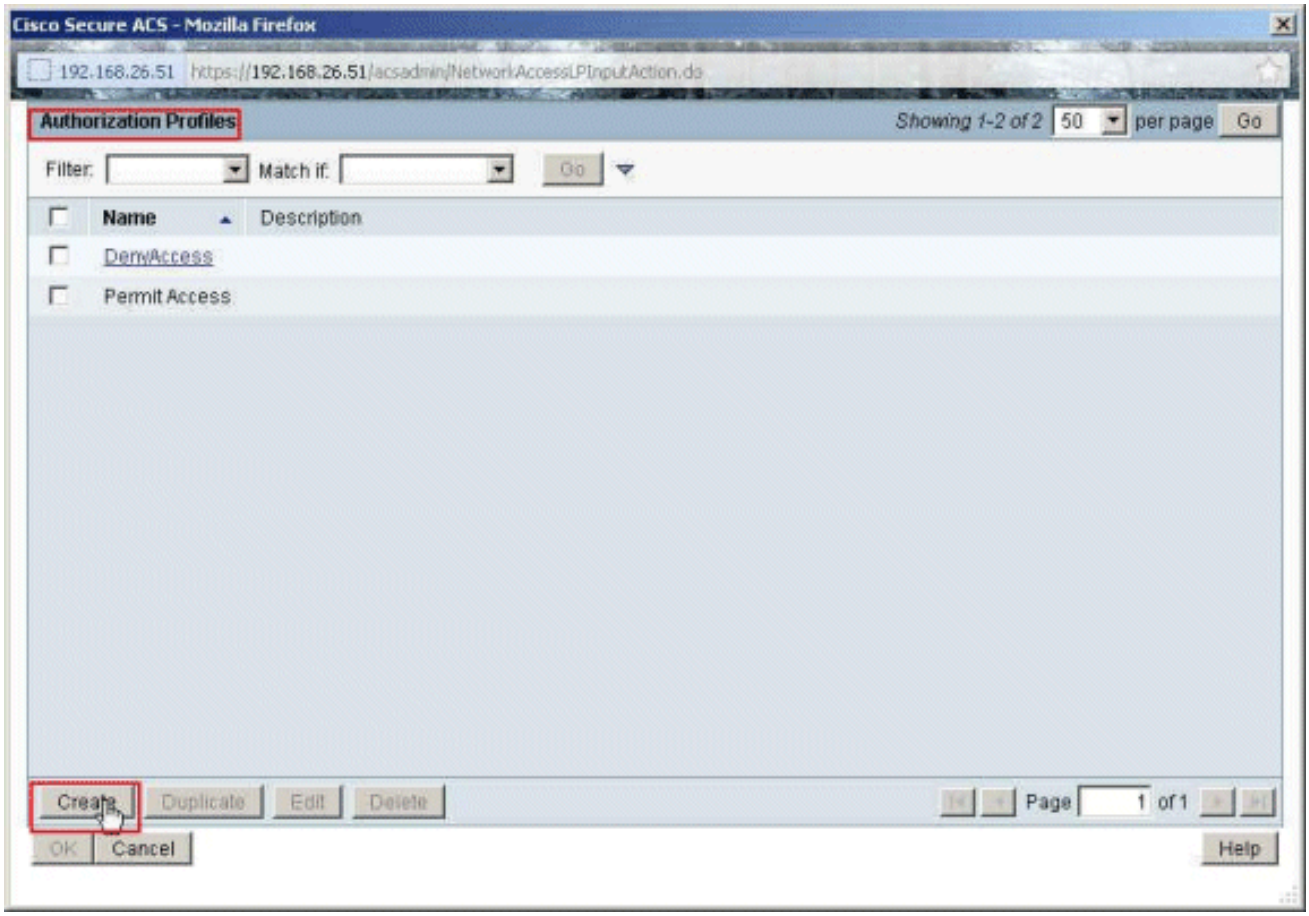
16. Vergewissern Sie sich, dass das Kontrollkästchen neben **System:UserName** aktiviert ist, wählen Sie **aus** der Dropdown-Liste aus, und geben Sie den Benutzernamen **cisco ein**.



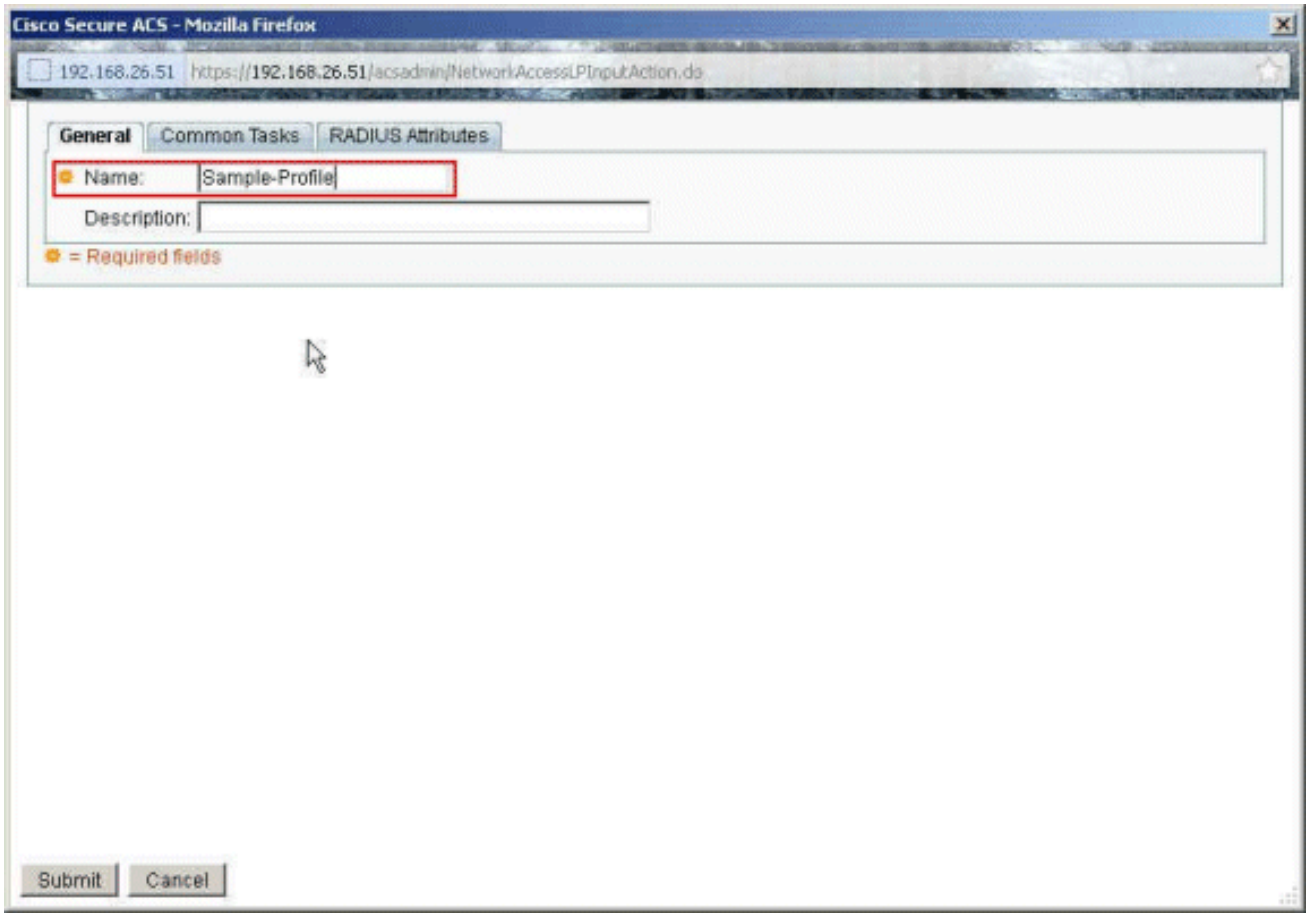
17. Klicken Sie auf **Auswählen**.



18. Klicken Sie auf **Erstellen**, um ein neues Autorisierungsprofil zu erstellen.

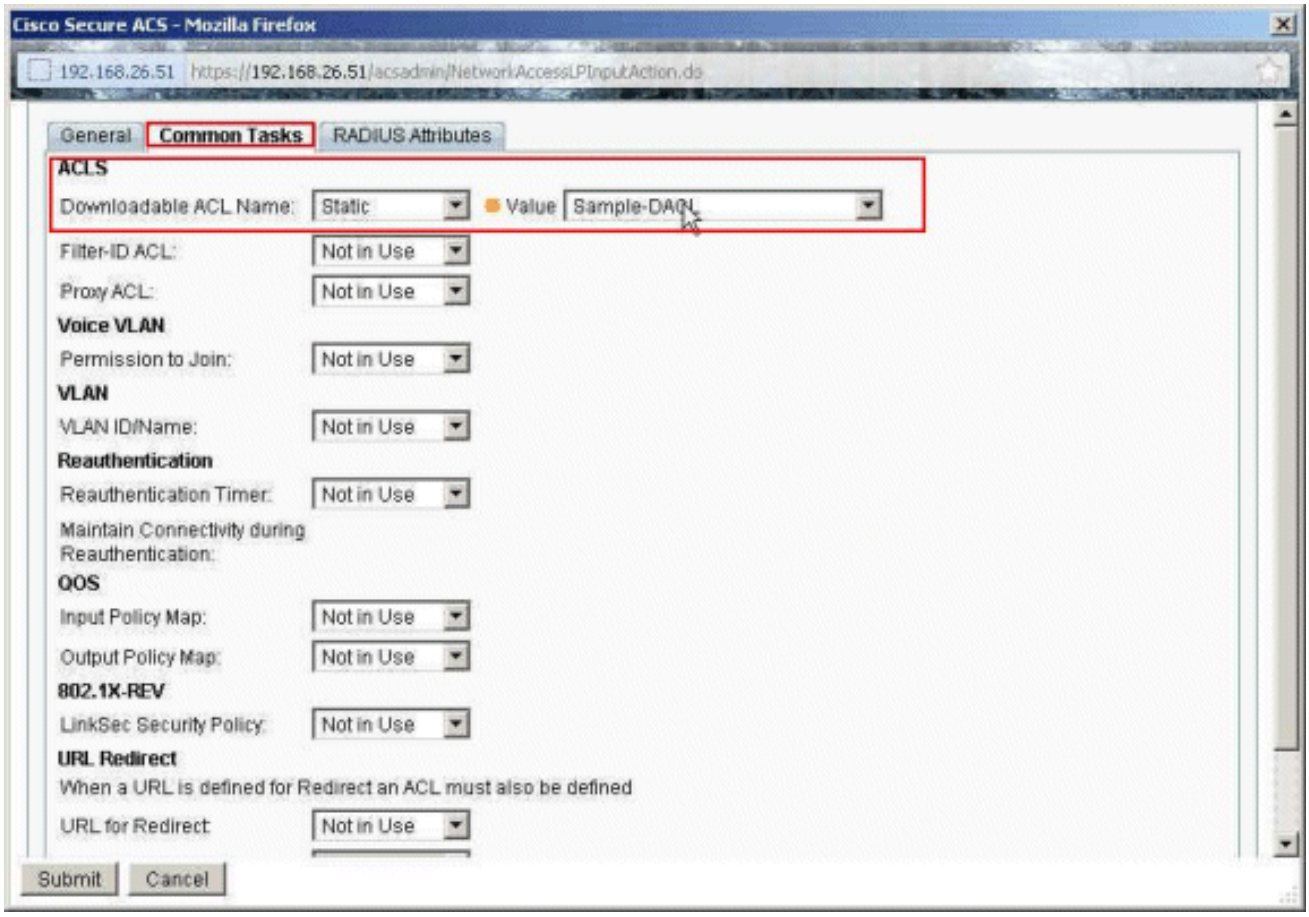


19. Geben Sie einen Namen für das **Autorisierungsprofil an**. **In** diesem Beispiel wird **Beispielprofil** verwendet.

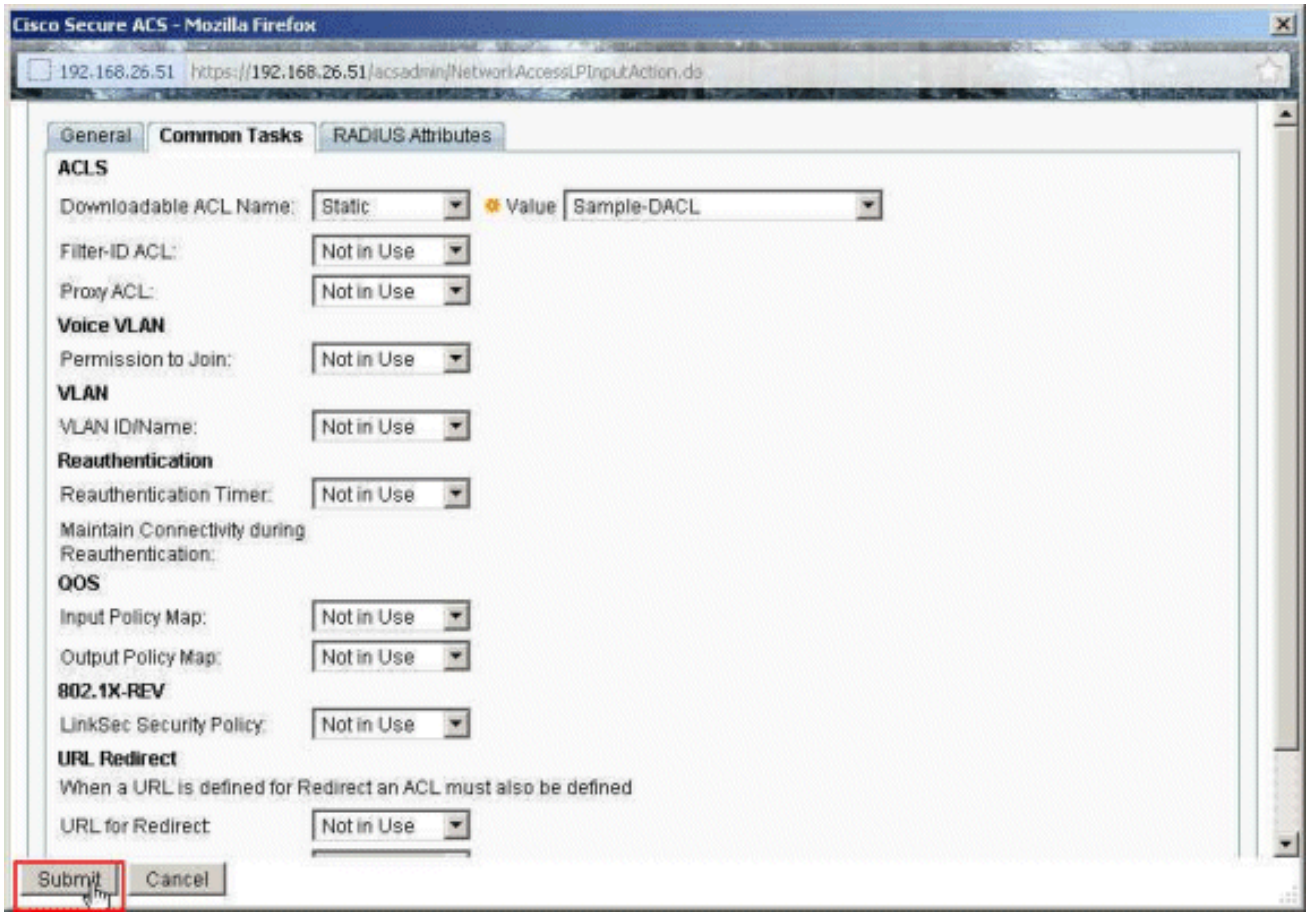


20. Wählen Sie die Registerkarte **Allgemeine Aufgaben**, und wählen Sie **Statisch** aus der Dropdown-Liste für den **Namen herunterladbarer ACL aus**. Wählen Sie die neu erstellte

DACL (Sample-DACL) aus der Dropdown-Liste Wert aus.

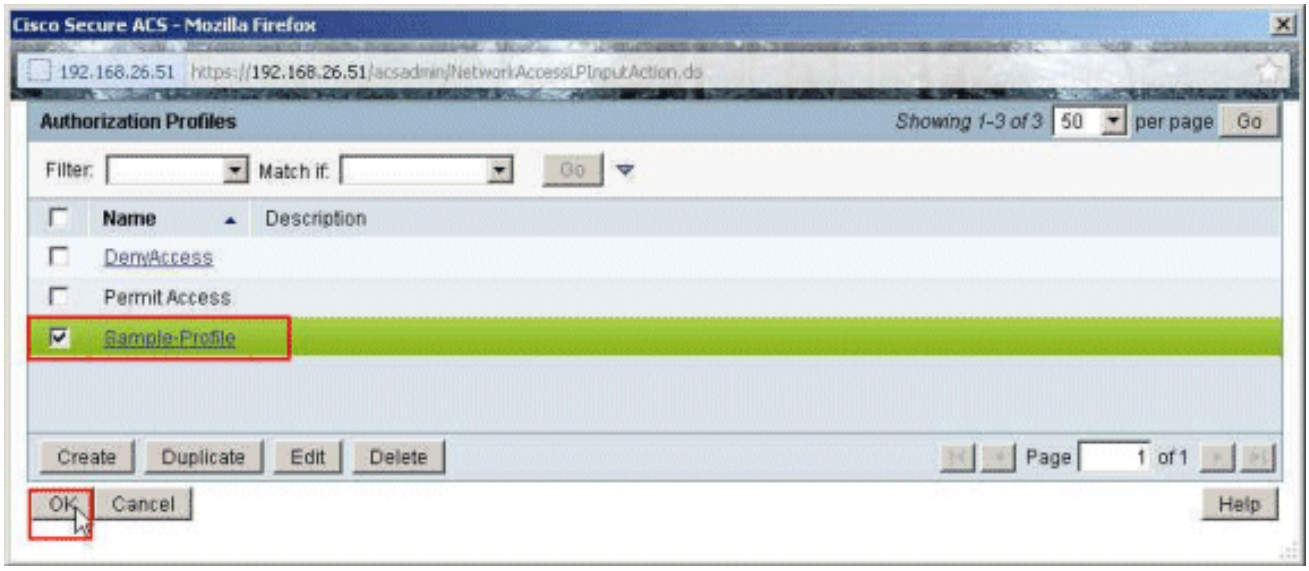


21. Klicken Sie auf **Senden**.

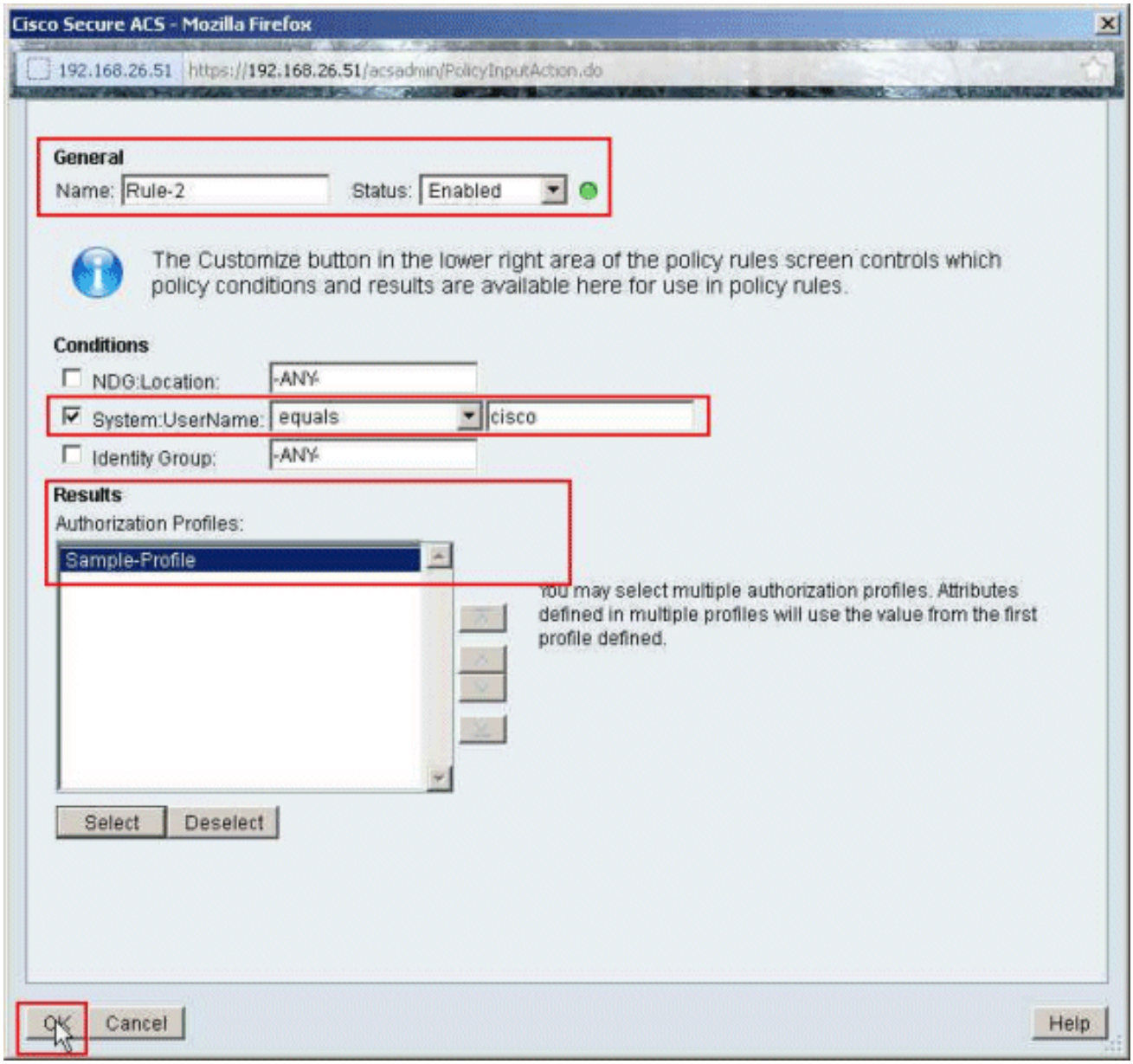


22. Stellen Sie sicher, dass das Kontrollkästchen neben **Sample-Profile** (das neu erstellte

Authorization Profile) aktiviert ist, und klicken Sie auf **OK**.

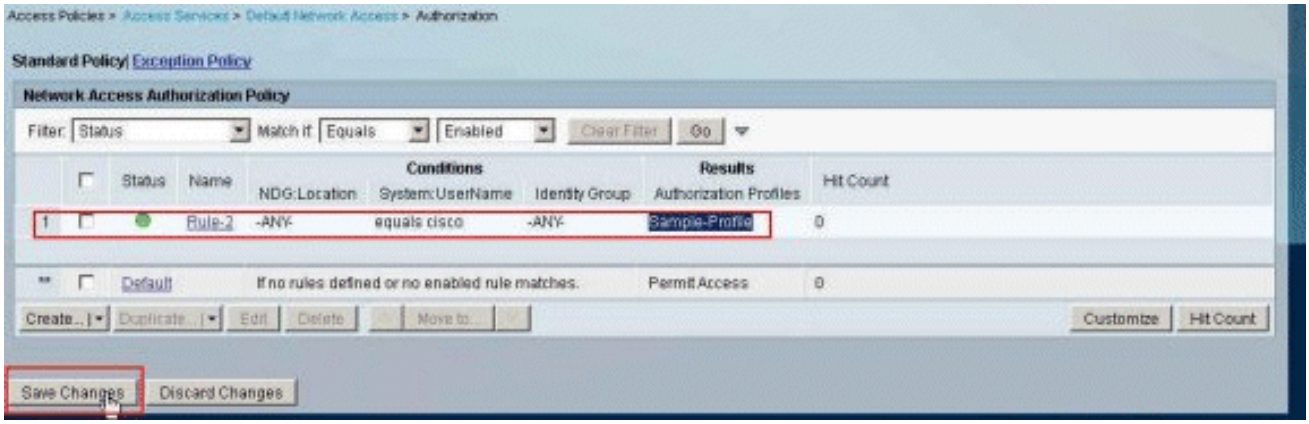


23. Wenn Sie überprüft haben, dass das neu erstellte **Beispielprofil** im Feld **Autorisierungsprofile** ausgewählt ist, klicken Sie auf **OK**.



24. Überprüfen Sie, ob die neue Regel (**Regel-2**) mit System:UserName **cisco-**Bedingungen

und **Beispielprofil** als Ergebnis erstellt wird. Klicken Sie auf **Änderungen speichern**. Regel 2 wurde erfolgreich
erstellt.



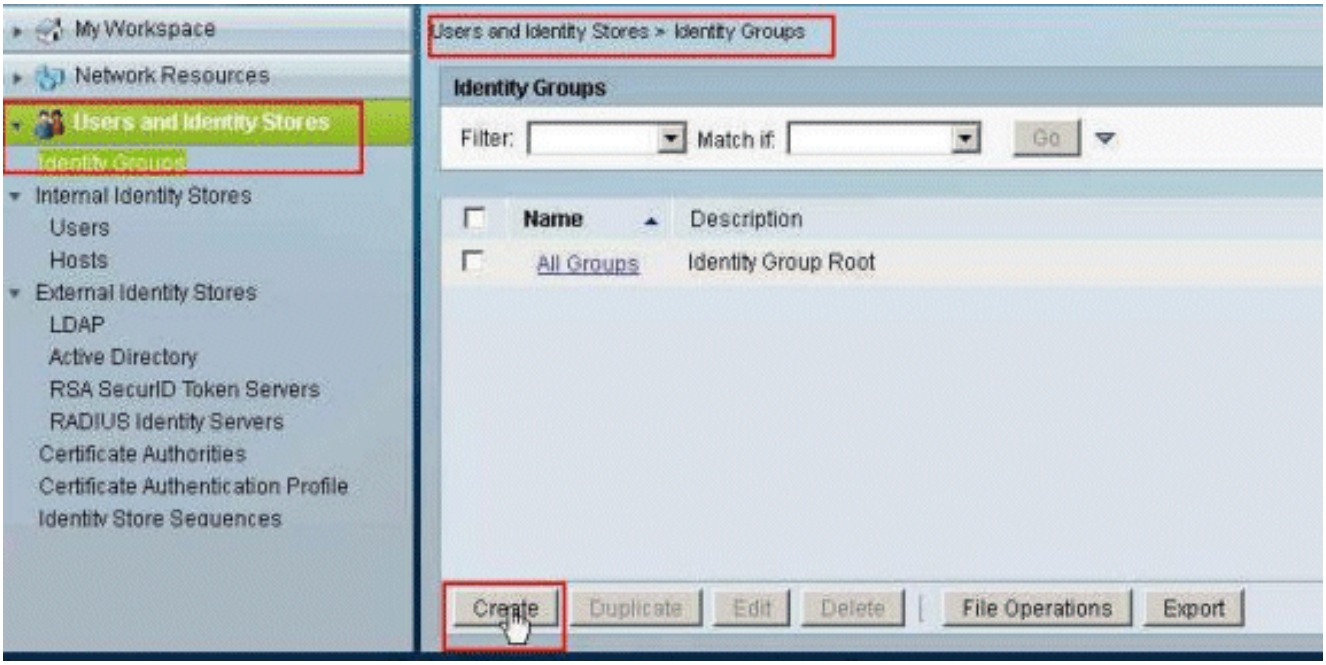
Konfigurieren von ACS für herunterladbare ACL für Gruppen

Führen Sie die Schritte 1 bis 12 der Konfigurationsanweisung für ACS für herunterladbare ACL für individuelle Benutzer aus und führen Sie diese Schritte aus, um die herunterladbare ACL für Gruppen in einem Cisco Secure ACS zu konfigurieren.

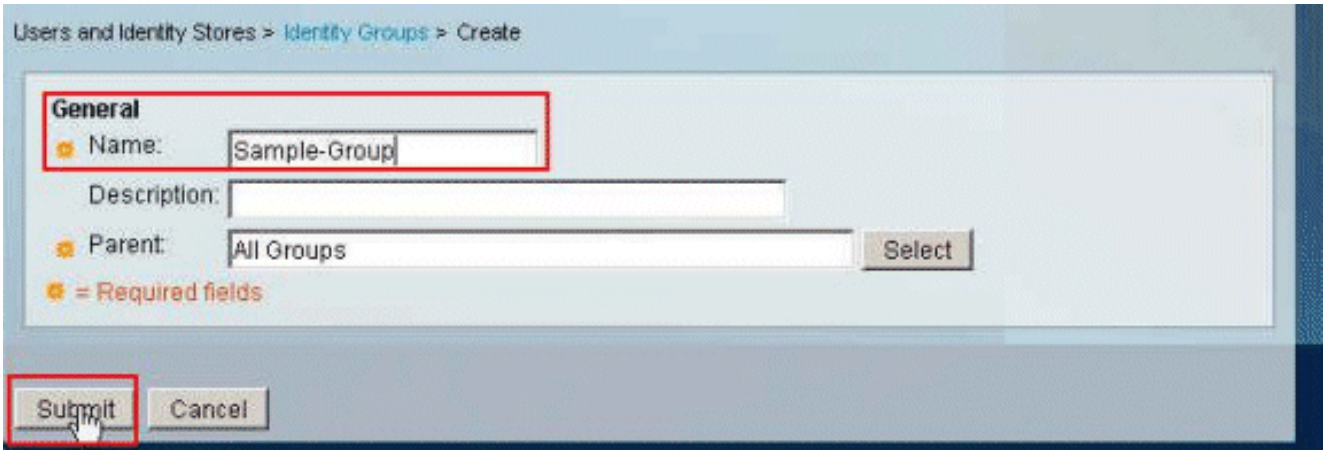
In diesem Beispiel gehört der IPsec-VPN-Benutzer "cisco" zur **Sample-Group**.

Der **Beispielgruppen-**Benutzer **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".

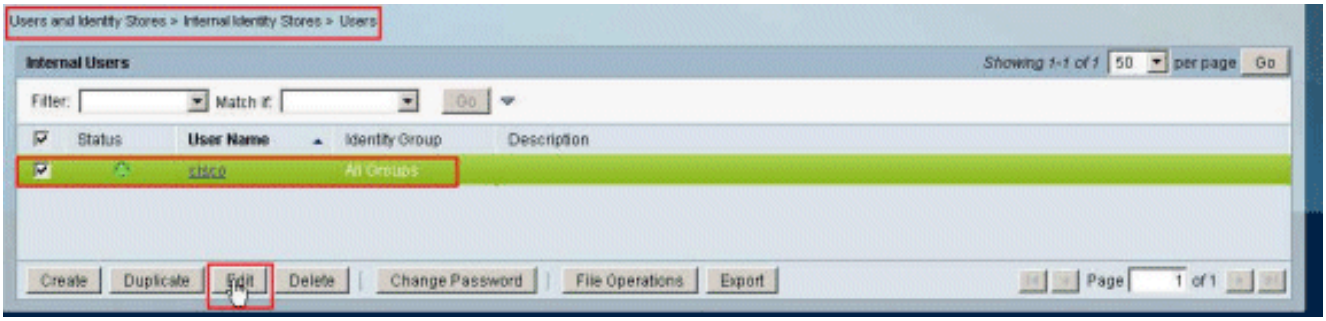
1. Klicken Sie in der Navigationsleiste auf **Benutzer und Identitätsdaten > Identitätsgruppen**, und klicken Sie auf **Erstellen**, um eine neue Gruppe zu
erstellen.



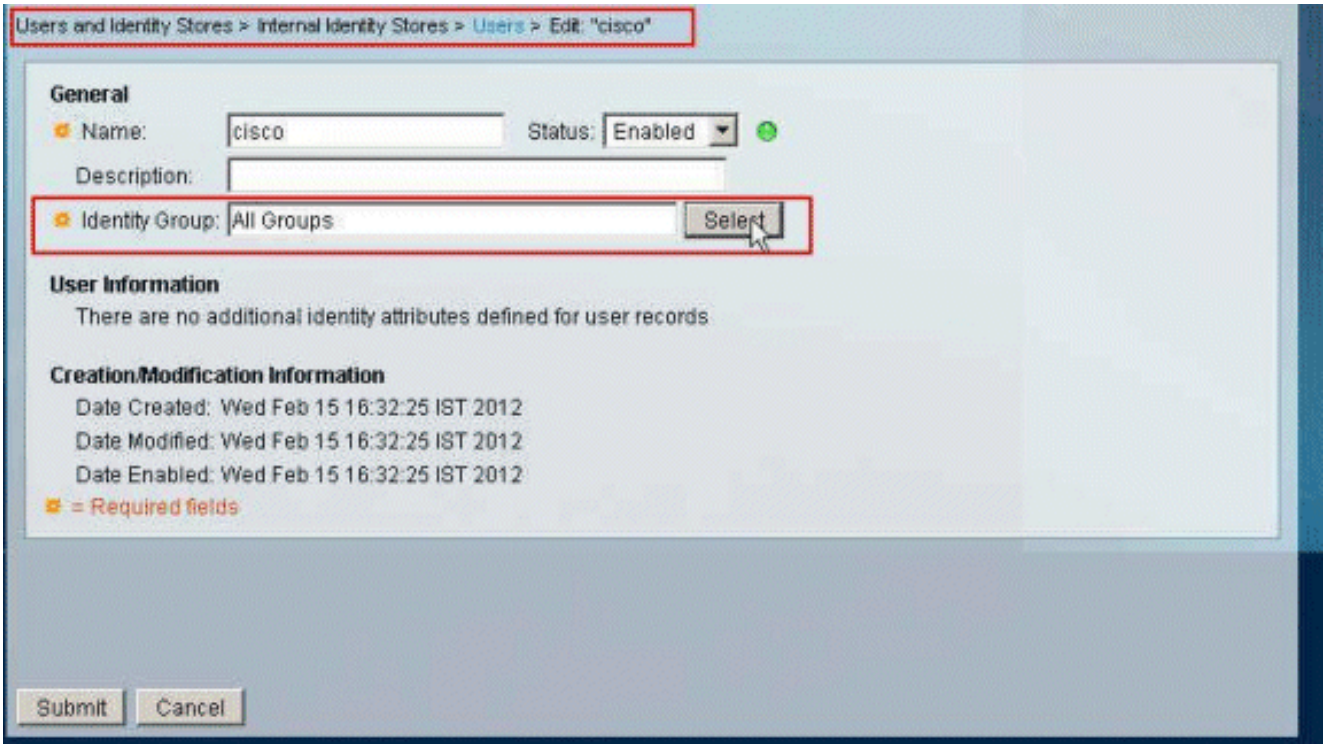
2. Geben Sie einen Gruppennamen (**Beispielgruppe**) ein, und klicken Sie auf **Senden**.



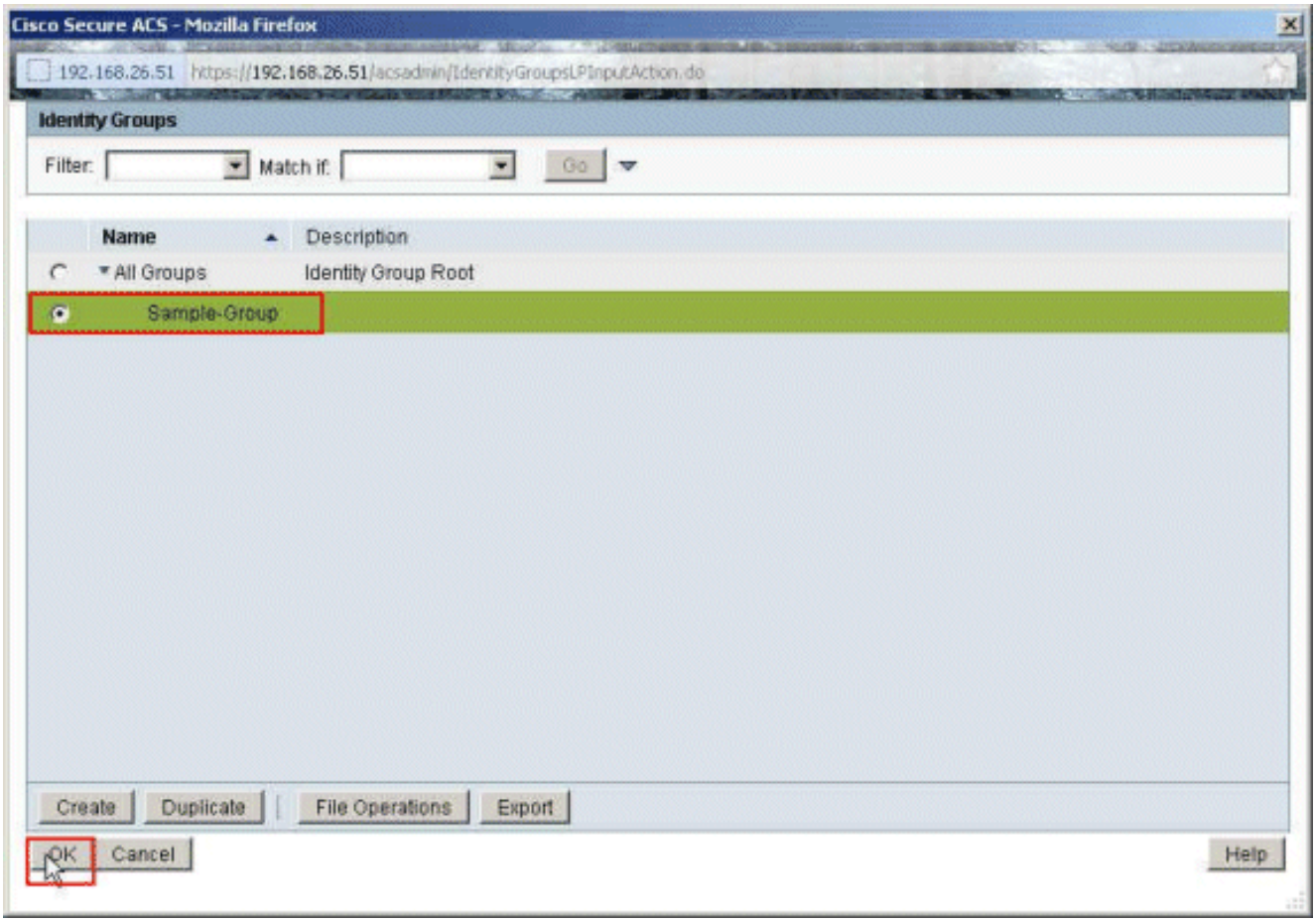
3. Wählen Sie **User Identity Stores > Internal Identity Stores > Users aus**, und wählen Sie den Benutzer **cisco aus**. Klicken Sie auf **Bearbeiten**, um die Gruppenmitgliedschaft dieses Benutzers zu
ändern.



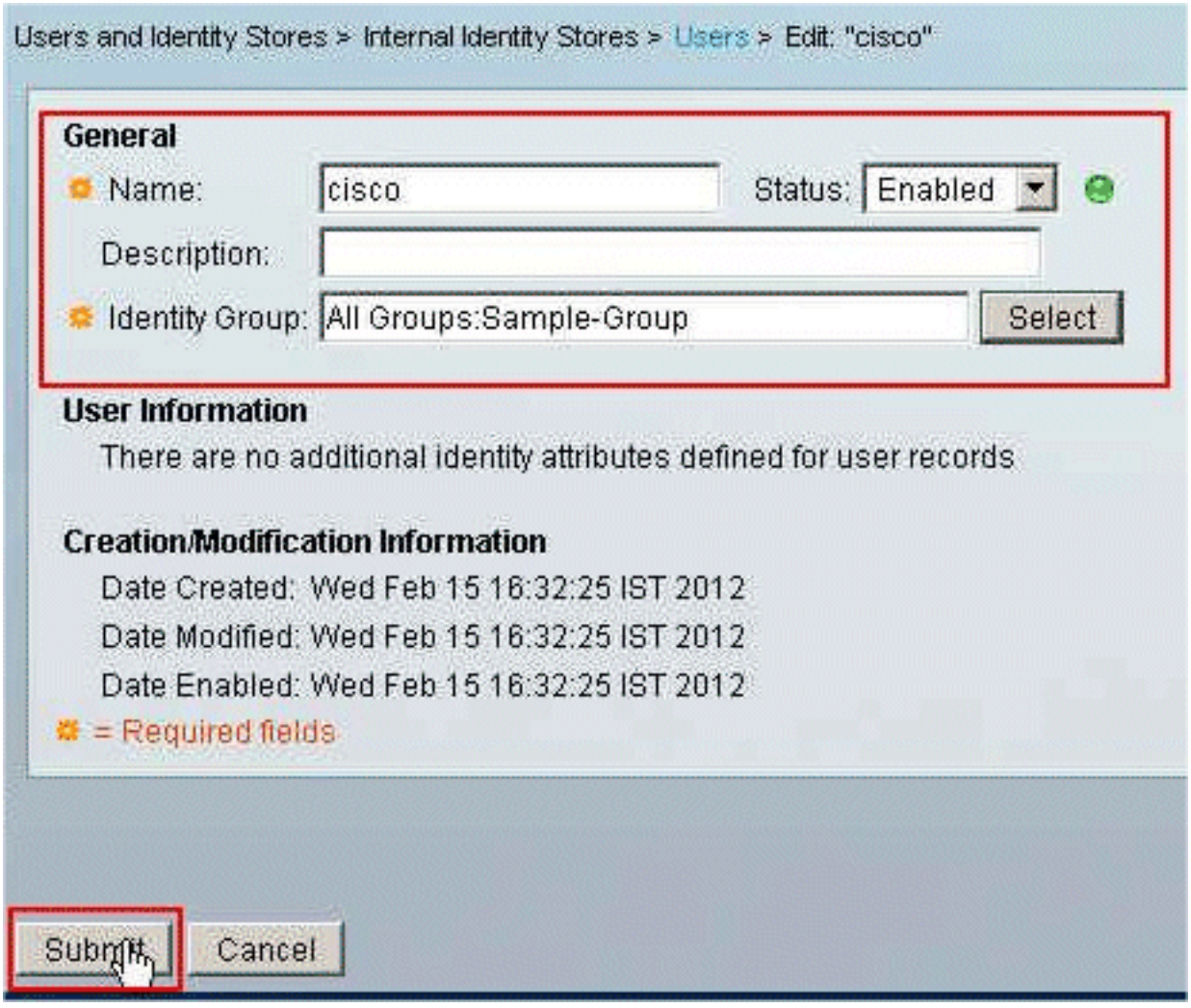
4. Klicken Sie neben der Identitätsgruppe auf **Auswählen**.



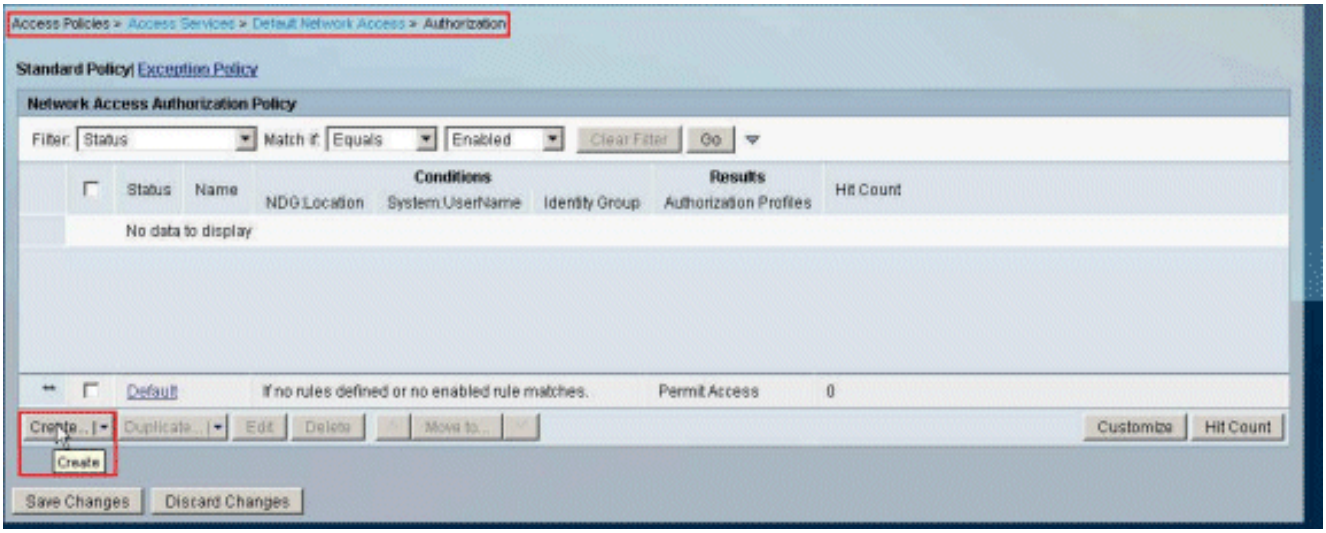
5. Wählen Sie die neu erstellte Gruppe aus (d. h. **Beispielgruppe**), und klicken Sie auf **OK**.



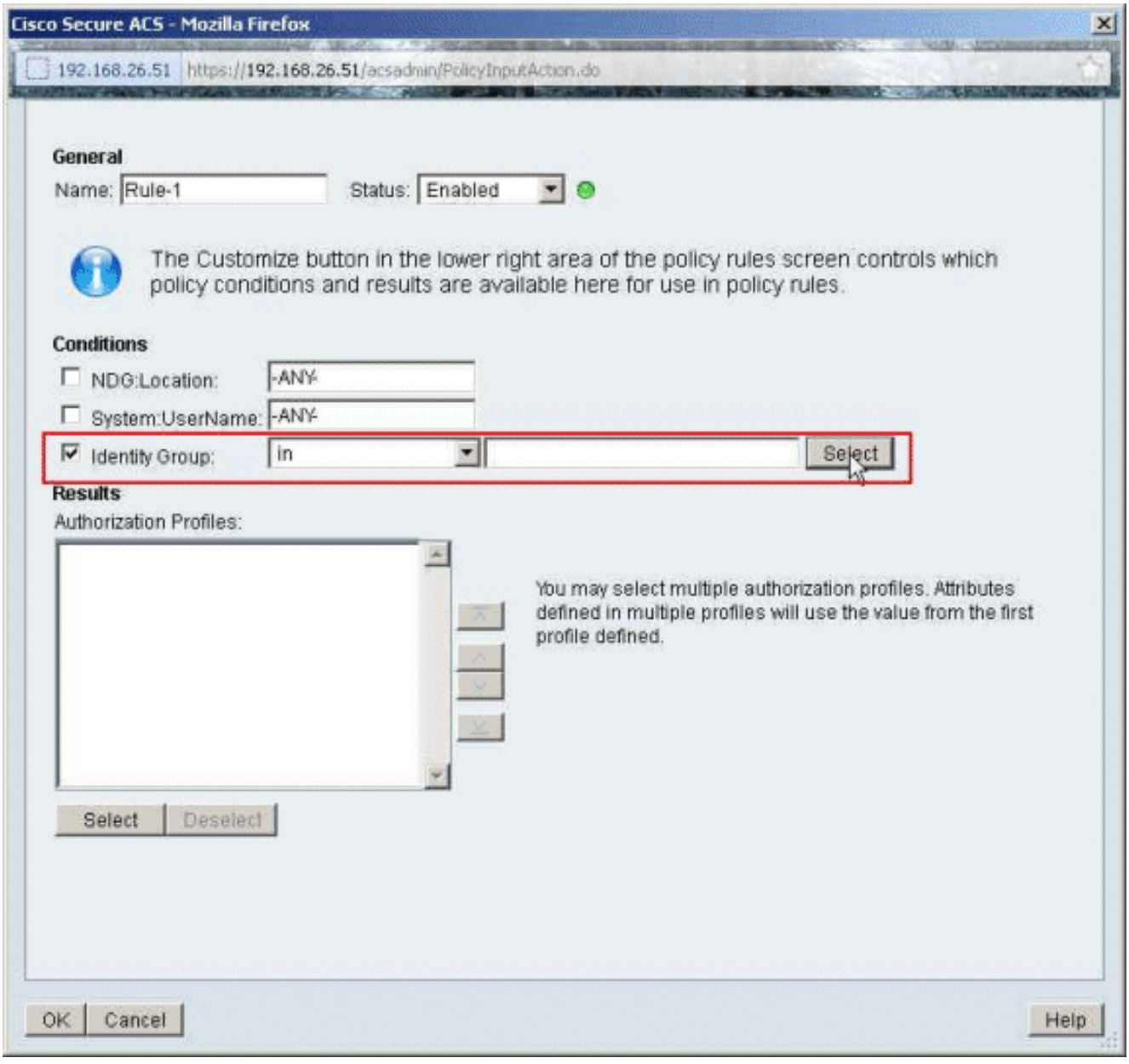
6. Klicken Sie auf **Senden**.



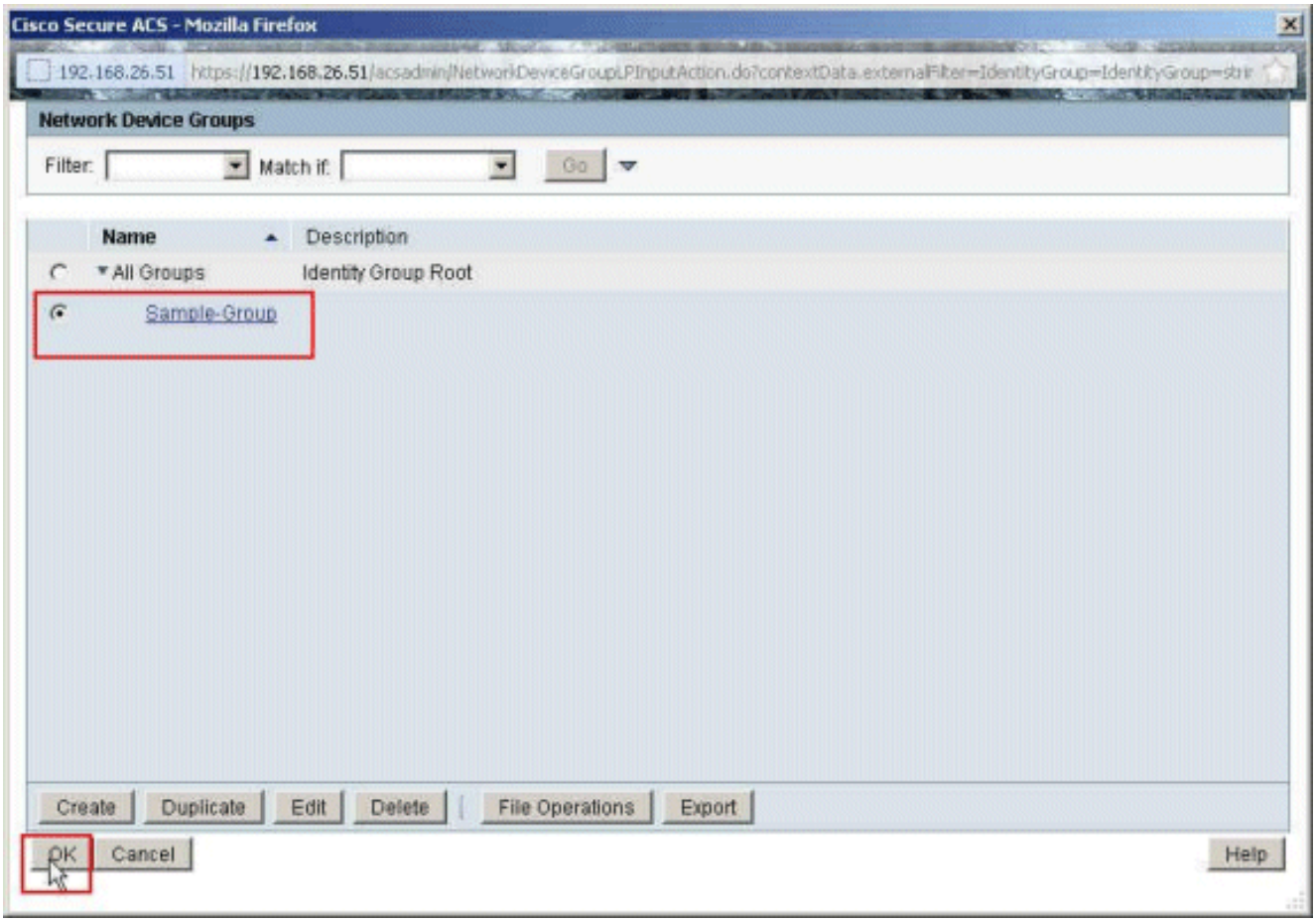
7. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Autorisierung** aus, und klicken Sie **auf Erstellen, um eine neue Regel zu erstellen.**



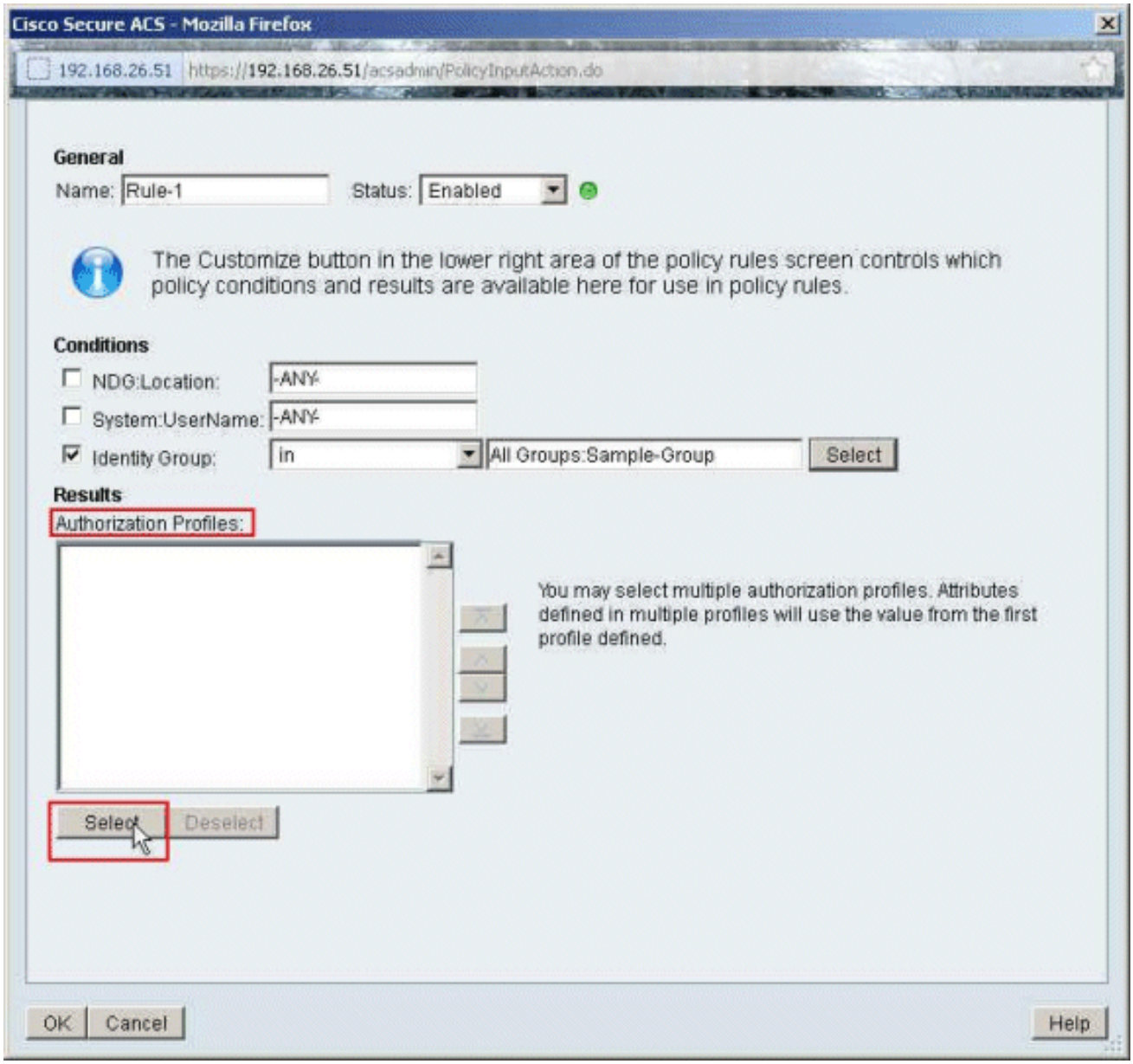
8. Stellen Sie sicher, dass das Kontrollkästchen neben **Identitätsgruppe** aktiviert ist, und klicken Sie auf **Auswählen**.



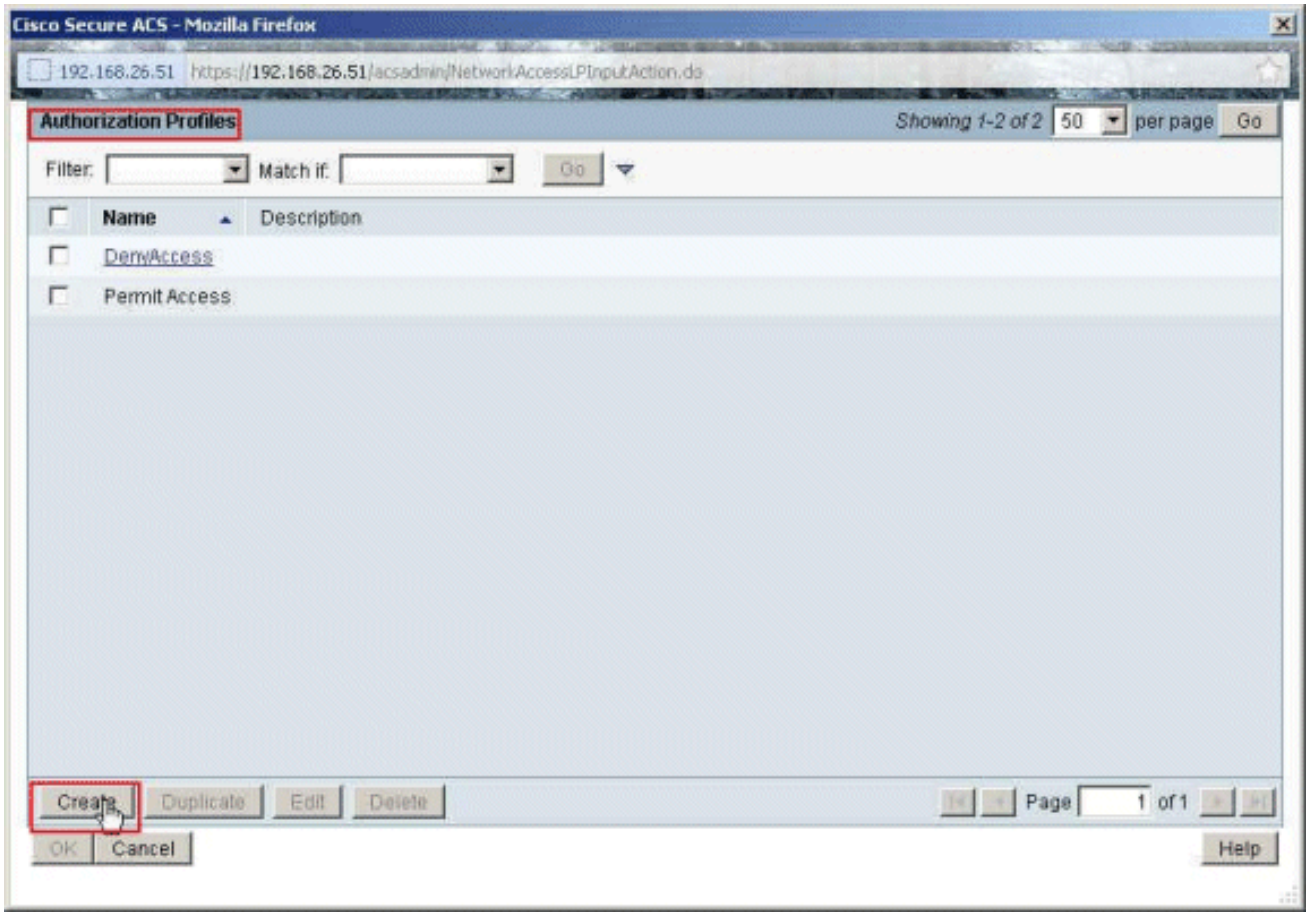
9. Wählen Sie **Sample-Group** aus, und klicken Sie auf **OK**.



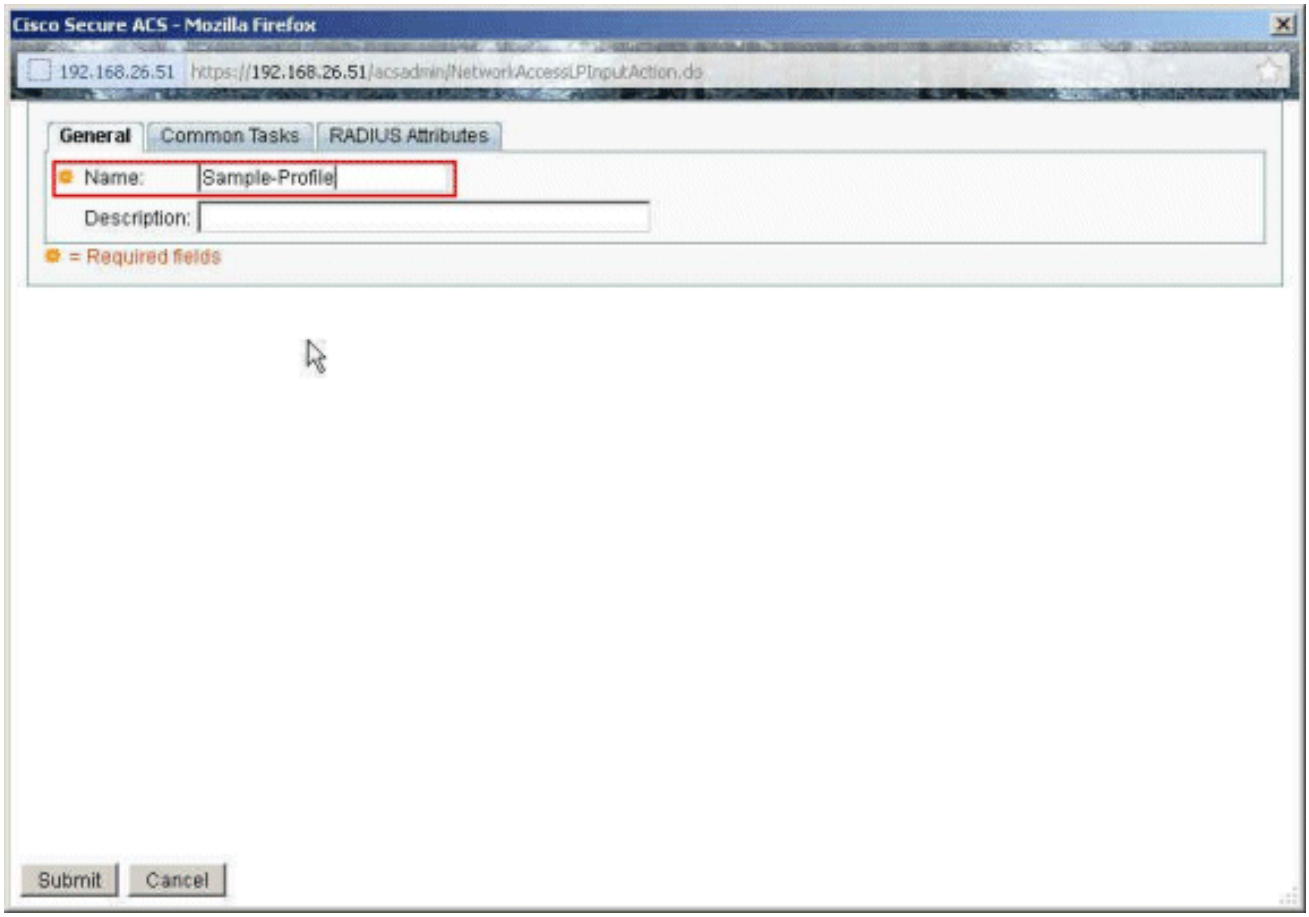
10. Klicken Sie im Abschnitt Autorisierungsprofile auf **Auswählen**.



11. Klicken Sie auf **Erstellen**, um ein neues Autorisierungsprofil zu erstellen.

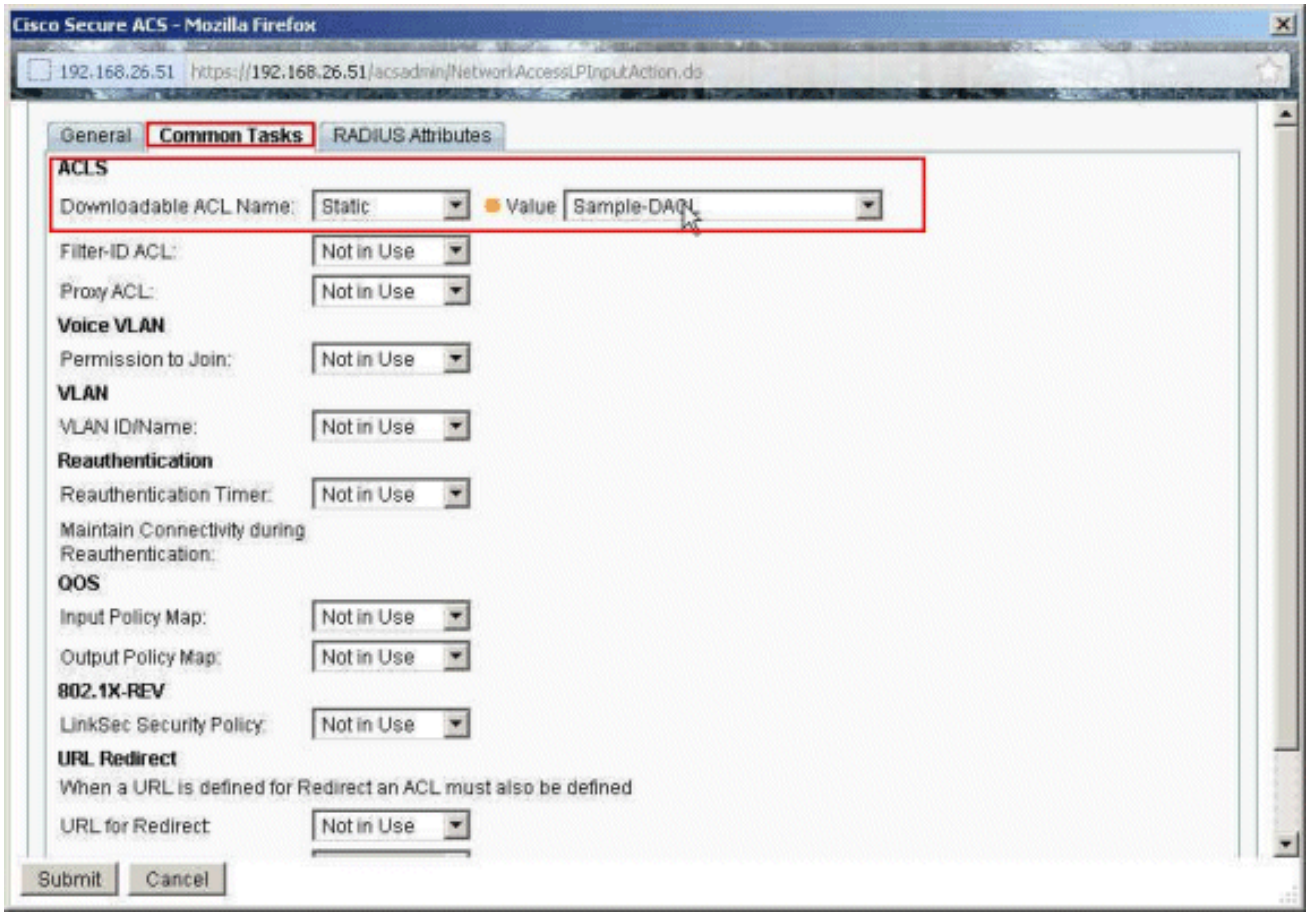


12. Geben Sie einen Namen für das **Autorisierungsprofil an**. **Ein Beispielprofil** ist der in diesem Beispiel verwendete
Name.

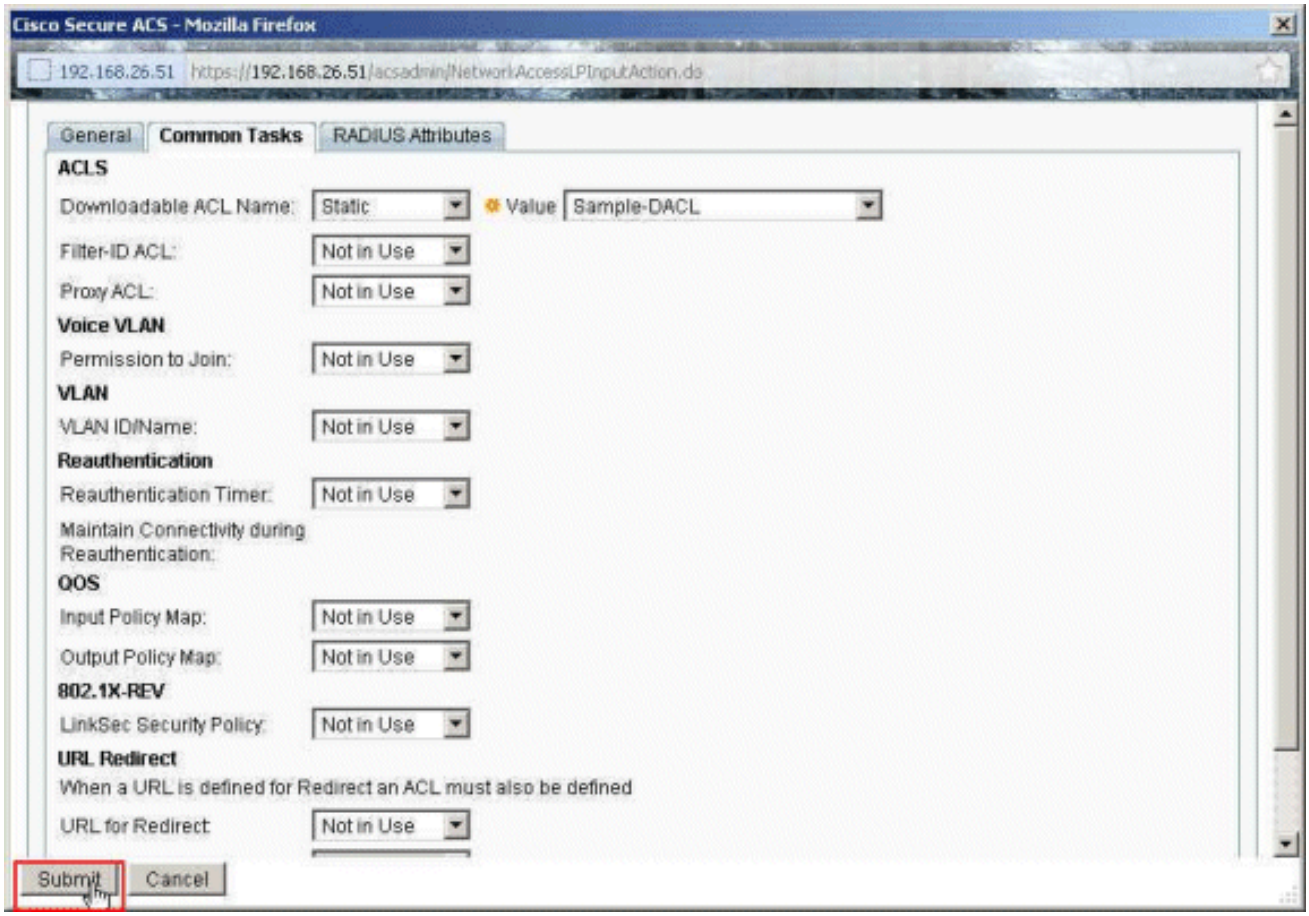


13. Wählen Sie die Registerkarte **Allgemeine Aufgaben**, und wählen Sie **Statisch** aus der Dropdown-Liste für den **Namen herunterladbarer ACL aus**. Wählen Sie die neu erstellte

DACL (Sample-DACL) aus der Dropdown-Liste Value (Wert) aus.

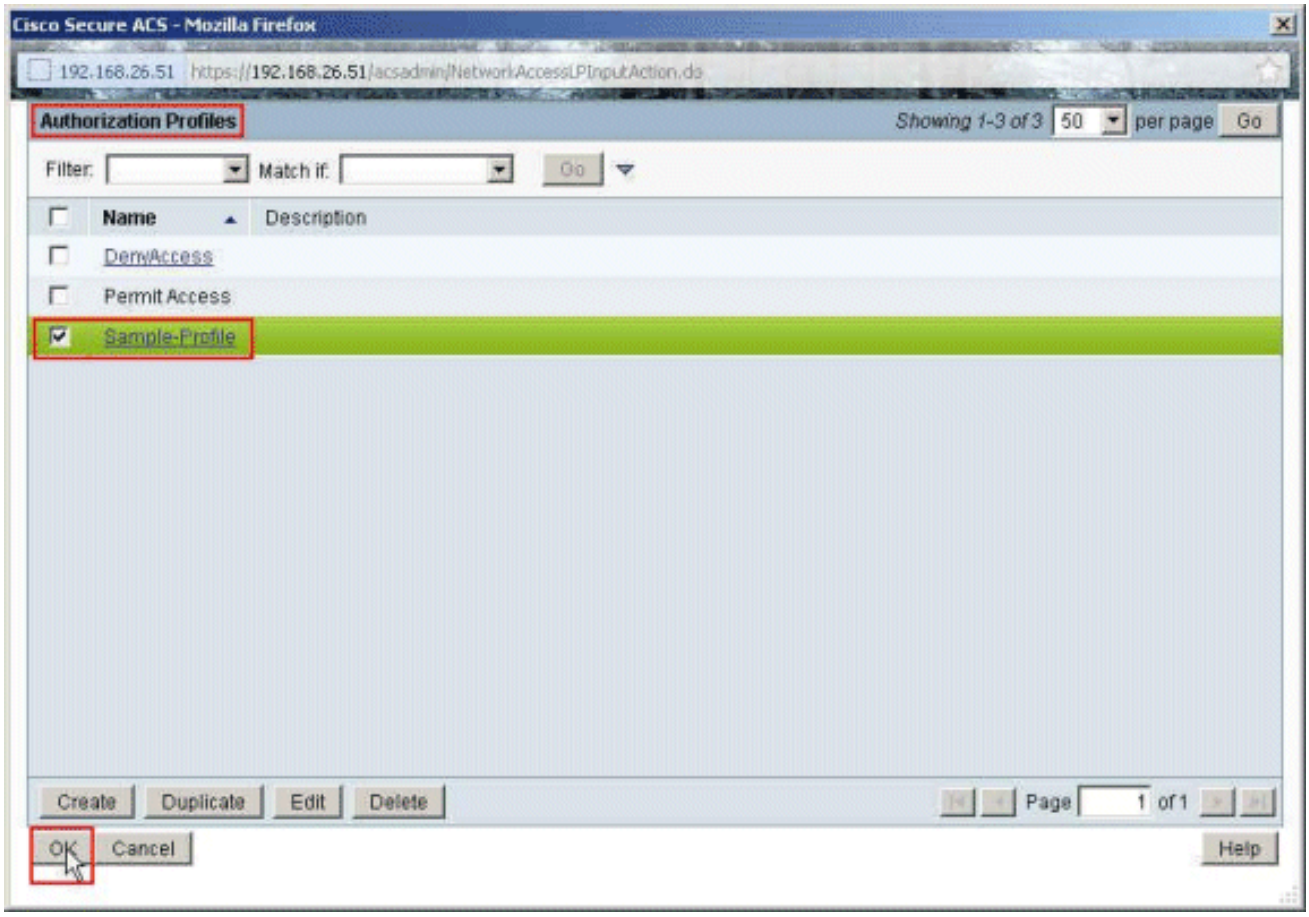


14. Klicken Sie auf **Senden**.

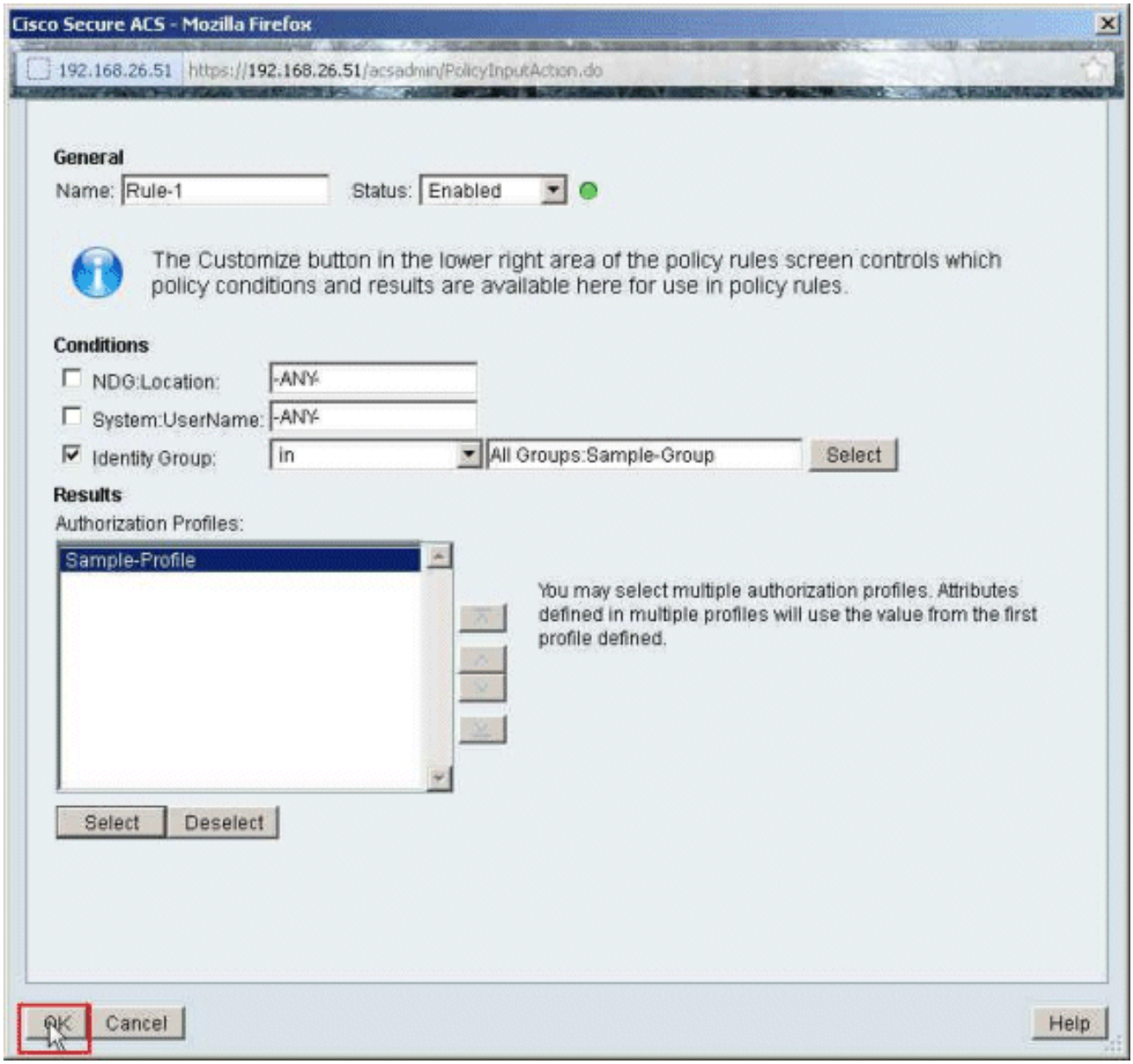


15. Wählen Sie das zuvor erstellte **Beispiel-Profil für** Autorisierungsprofile aus, und klicken Sie

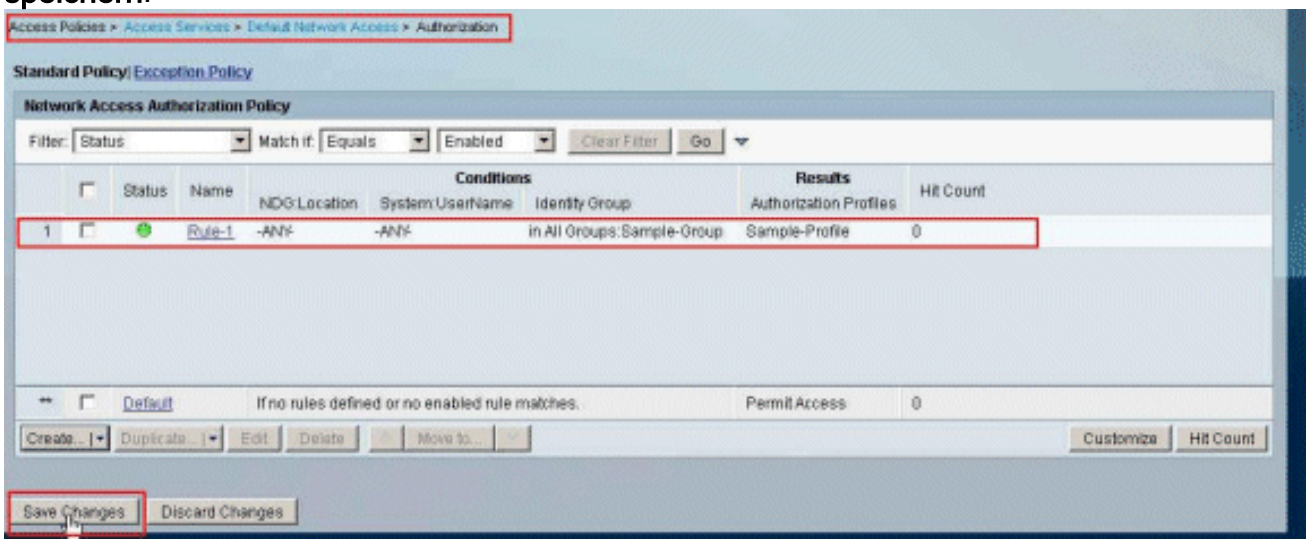
auf
OK.



16. Klicken Sie auf
OK.



17. Überprüfen Sie, ob **Regel 1** mit der **Beispielgruppe** für **Identitätsgruppen** als Bedingung und **Beispielprofil** als Ergebnis erstellt wird. Klicken Sie auf **Änderungen speichern**.



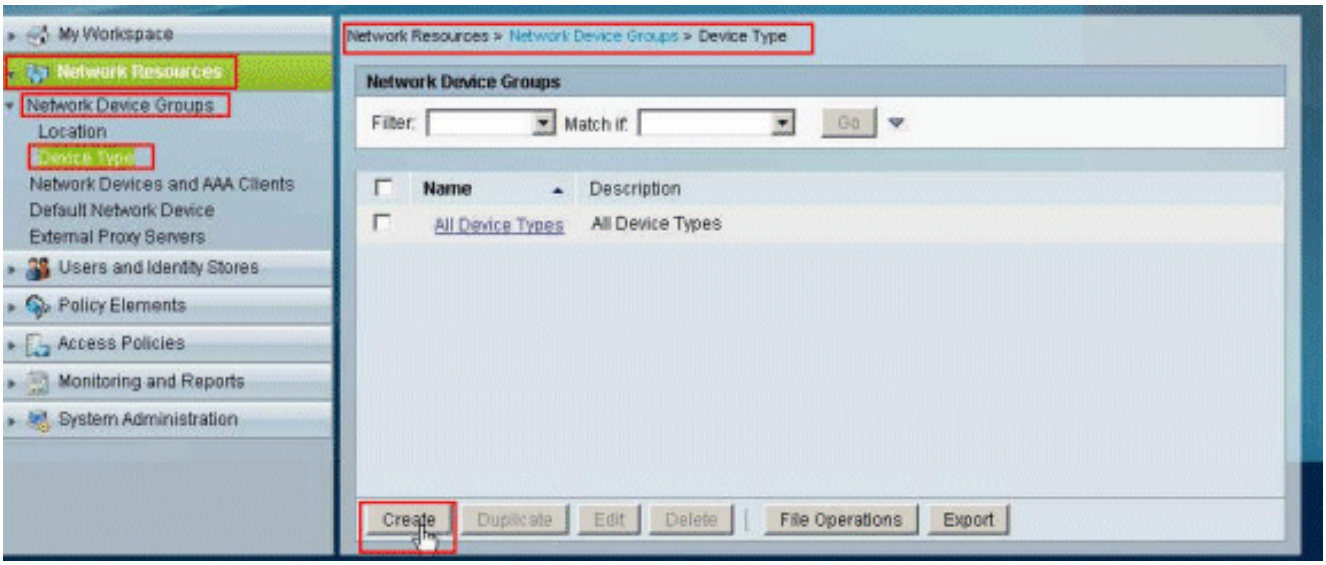
Konfigurieren des ACS für herunterladbare ACL für eine Netzwerkgerätegruppe

Führen Sie die Schritte 1 bis 12 der Konfigurationsanweisung für ACS für herunterladbare ACL für

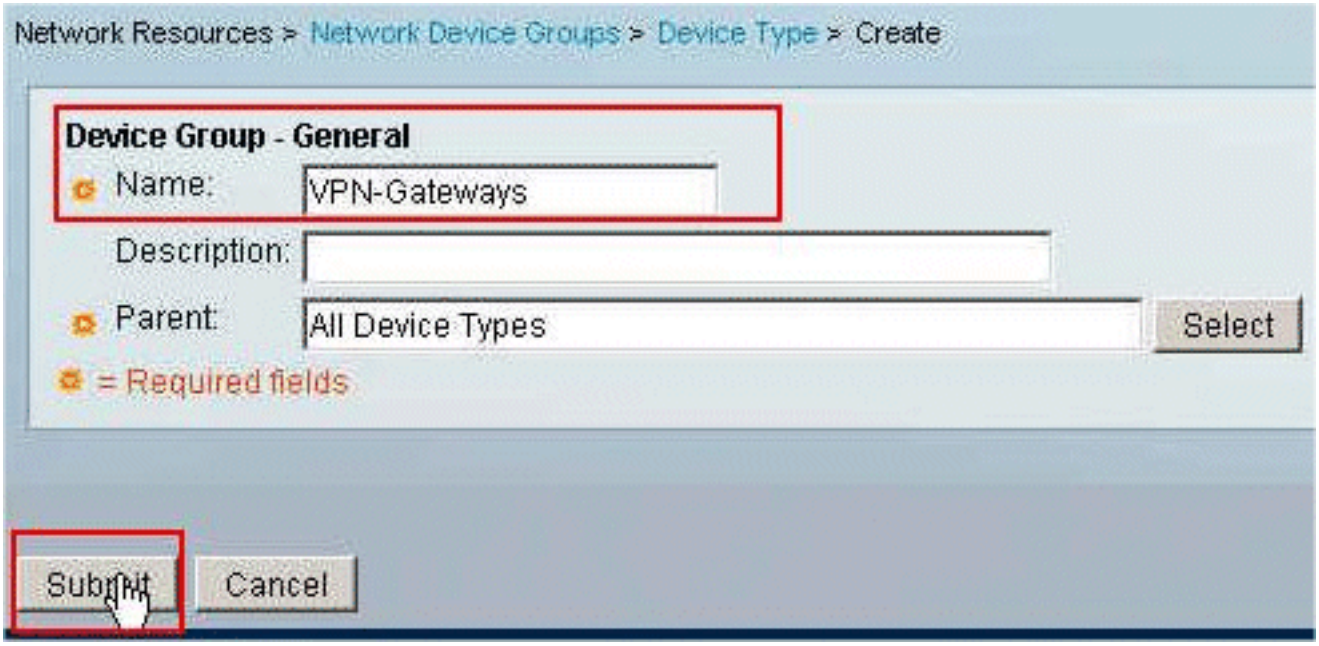
individuelle Benutzer aus und führen Sie diese Schritte aus, um die herunterladbare ACL für eine Netzwerkgerätegruppe in einem Cisco Secure ACS zu konfigurieren.

In diesem Beispiel gehört der RADIUS-Client (ASA) zu den **VPN-Gateways** der Netzwerkgerätegruppe.Die VPN-Authentifizierungsanfrage von ASA für den Benutzer "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".

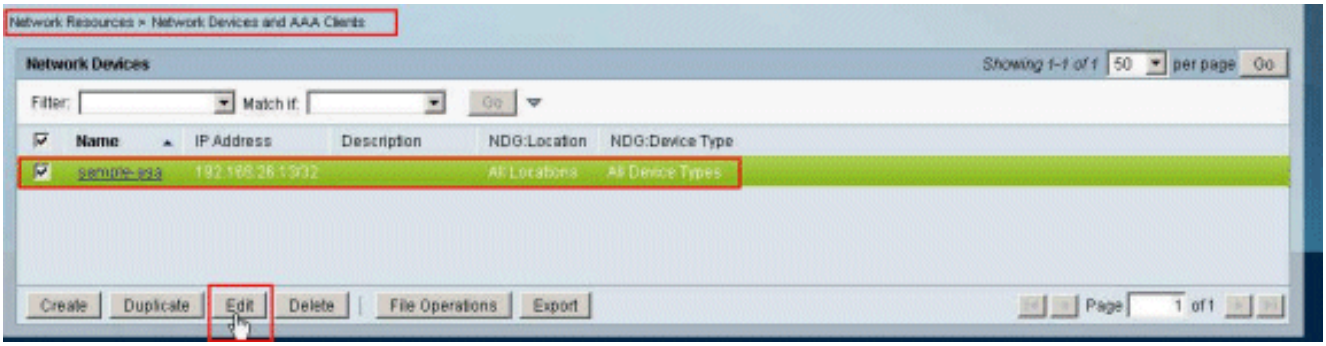
1. Wählen Sie **Netzwerkressourcen > Netzwerkgerätegruppen > Gerätetyp aus**, und klicken Sie auf **Erstellen**, um eine neue Netzwerkgerätegruppe zu erstellen.



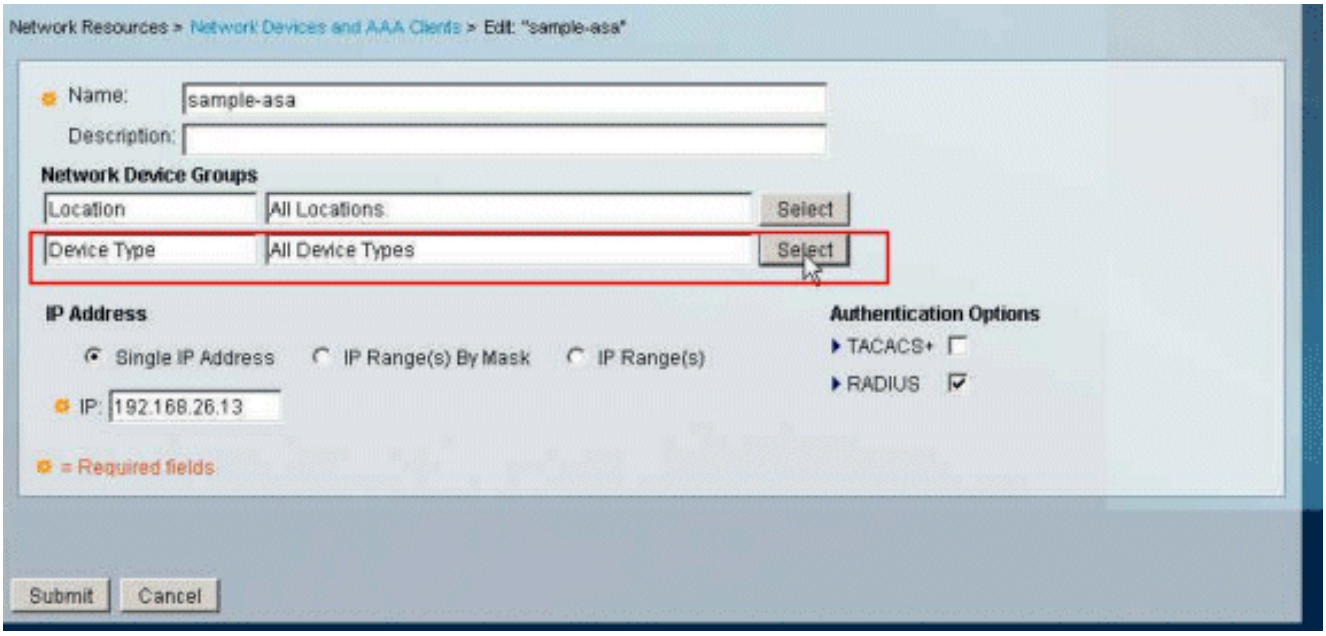
2. Geben Sie einen **Netzwerkgerätegruppennamen** an (in diesem Beispiel **VPN-Gateways**), und klicken Sie auf **Senden**.



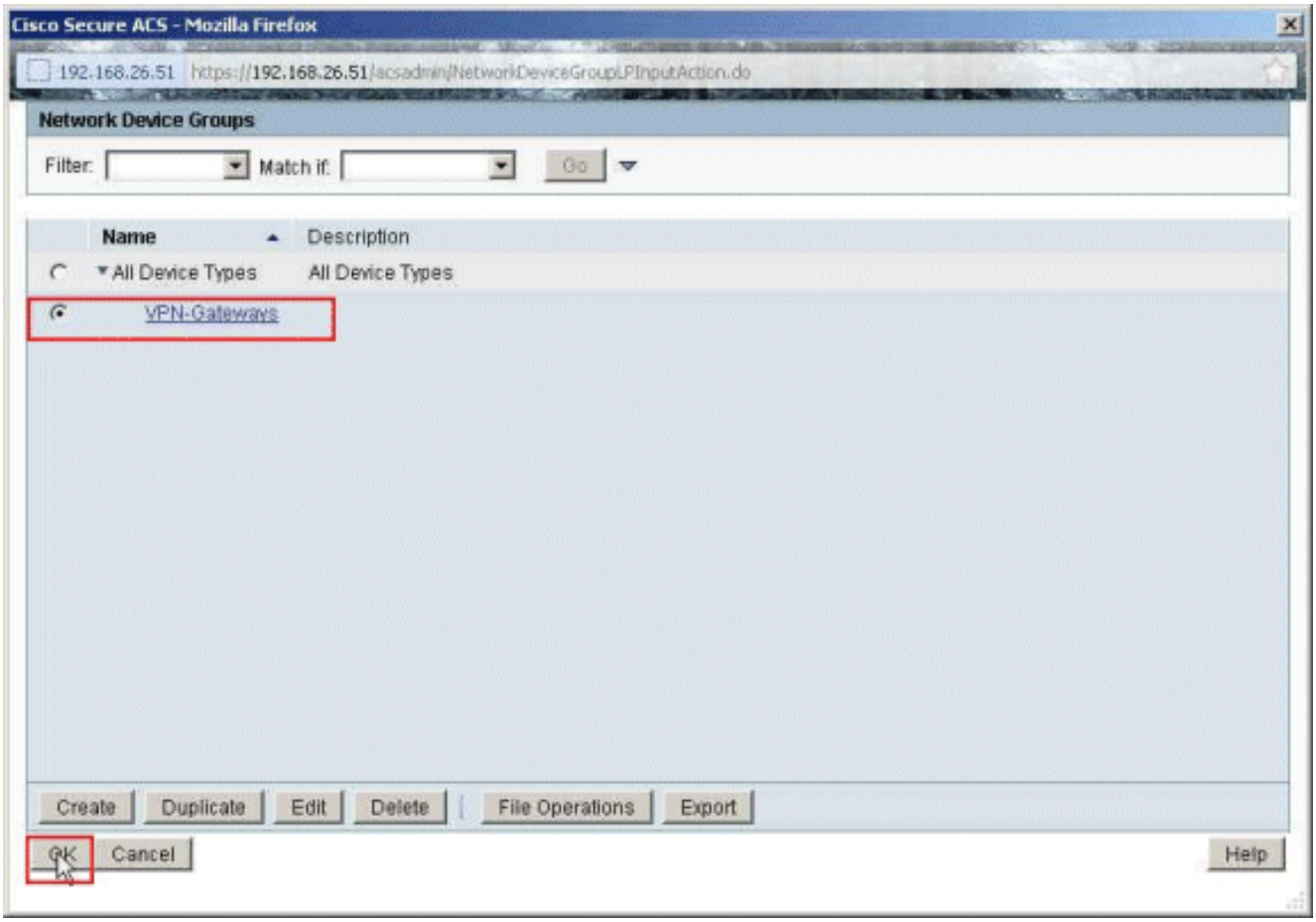
3. Wählen Sie **Netzwerkressourcen > Netzwerkgeräte und AAA-Clients**, und wählen Sie die zuvor erstellte **RADIUS-Client-Beispielasa aus**. Klicken Sie auf **Bearbeiten**, um die **Netzwerkgerätegruppenmitgliedschaft** dieses RADIUS-Clients (ASA) zu ändern.



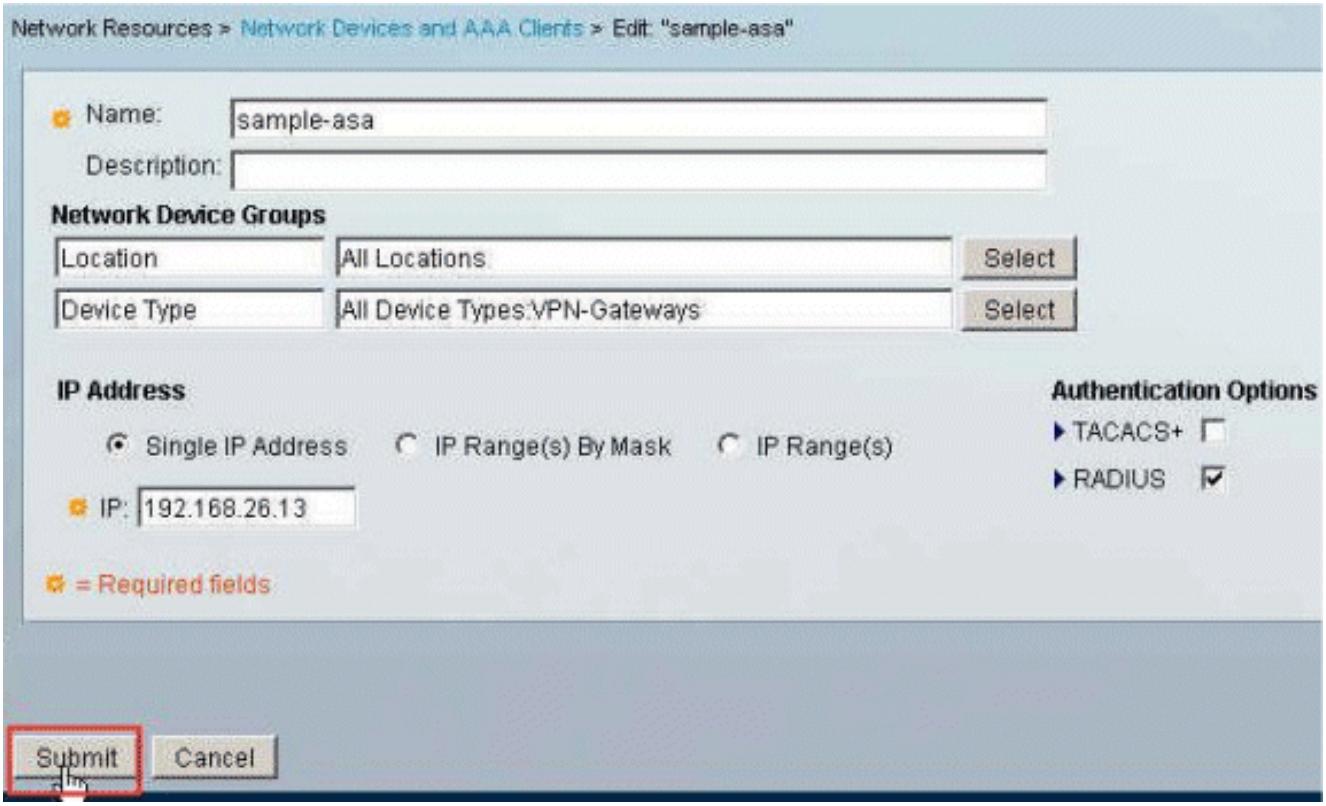
4. Klicken Sie neben dem Gerätetyp auf **Auswählen**.



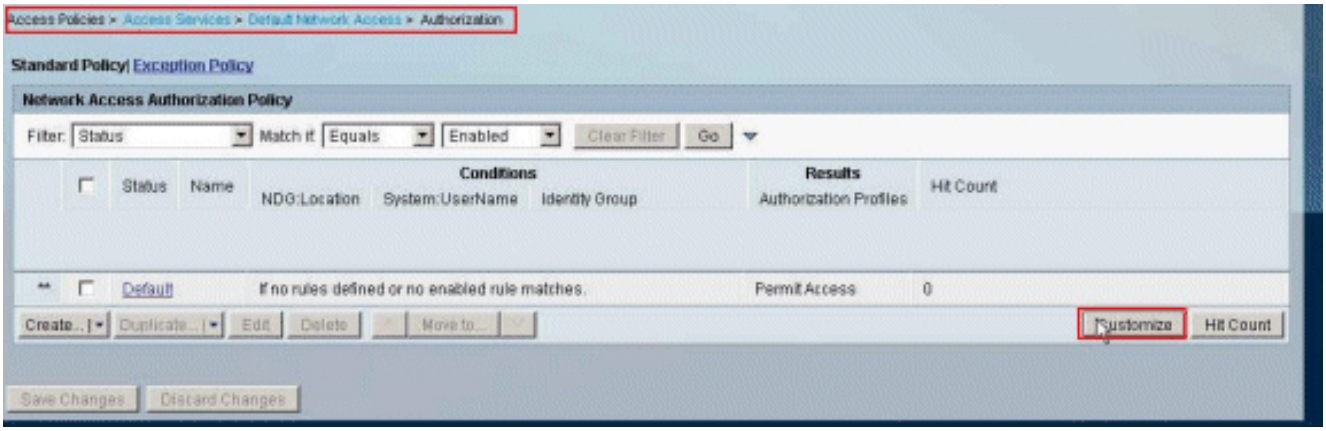
5. Wählen Sie die neu erstellte Netzwerkgerätegruppe (**VPN-Gateways**) aus, und klicken Sie auf **OK**.



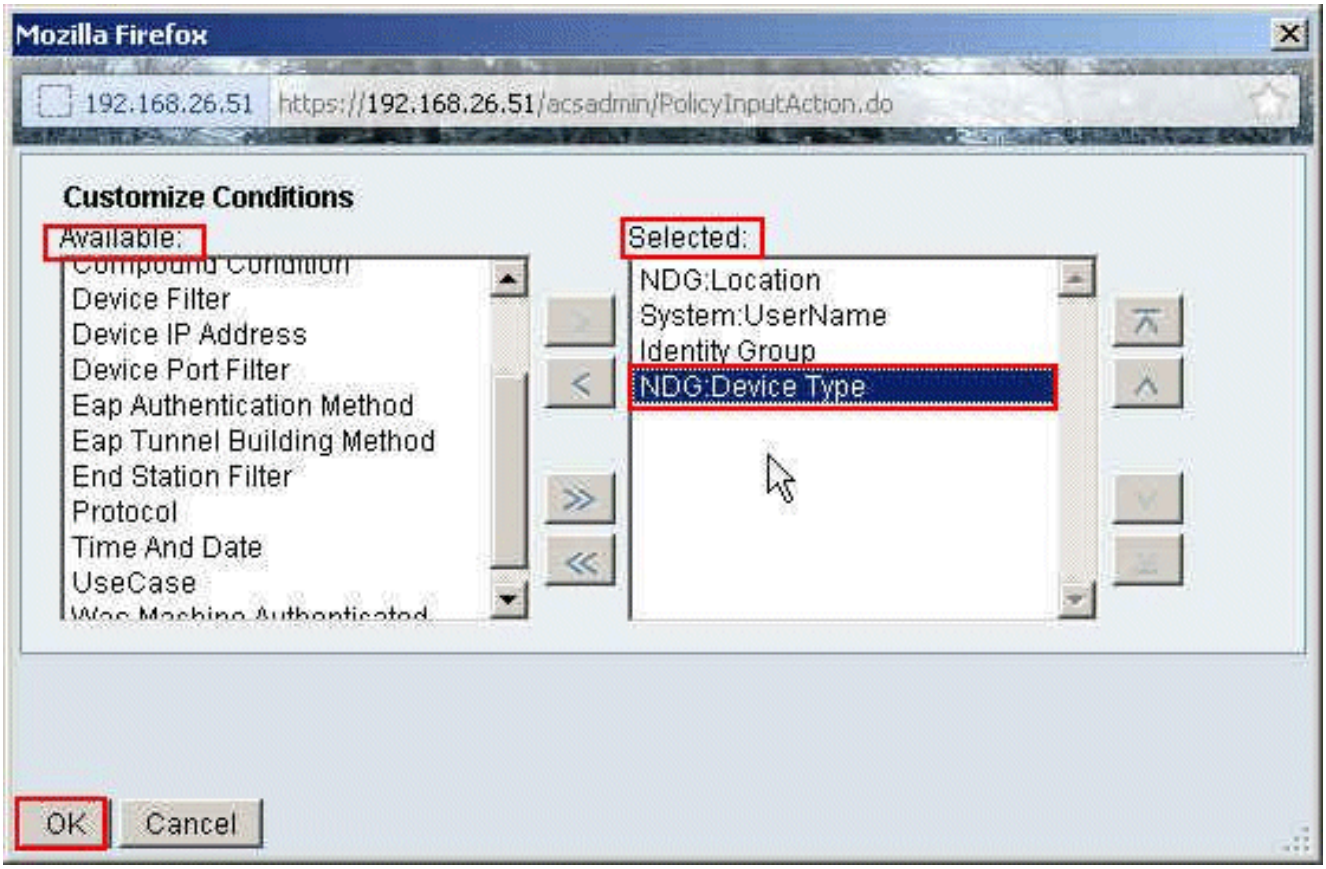
6. Klicken Sie auf **Senden**.



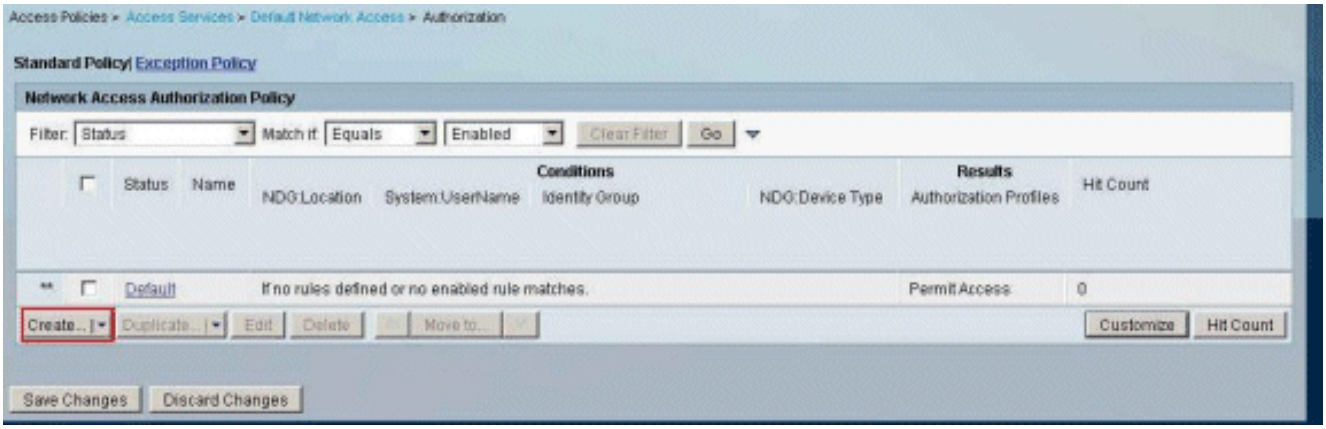
7. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Autorisierung aus**, und klicken Sie auf **Anpassen.**



8. Verschieben Sie **NDG:Gerätetyp** aus dem **Abschnitt Verfügbar** in den **Abschnitt Ausgewählt**, und klicken Sie auf **OK**.

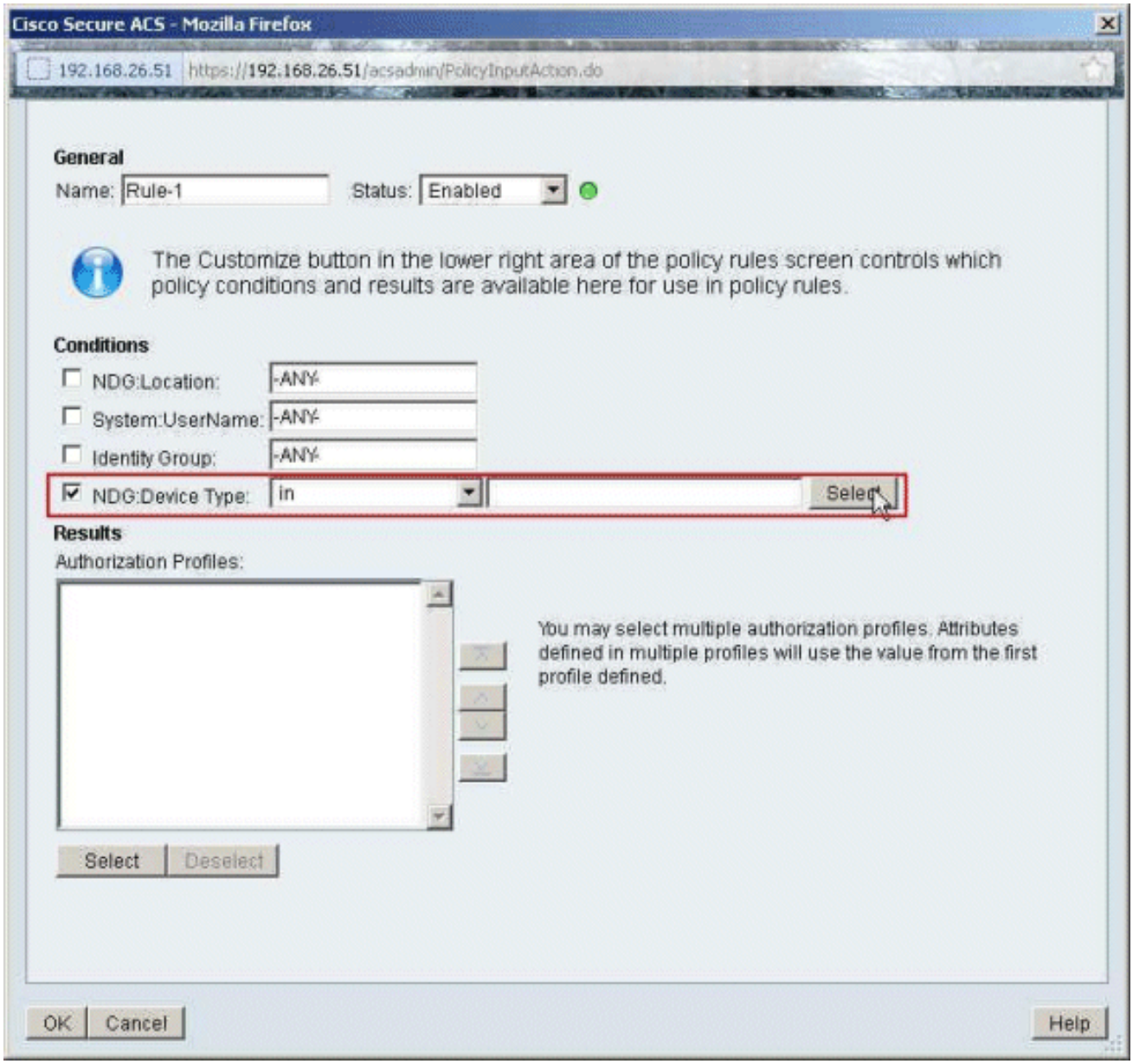


9. Klicken Sie auf **Erstellen**, um eine neue Regel zu erstellen.

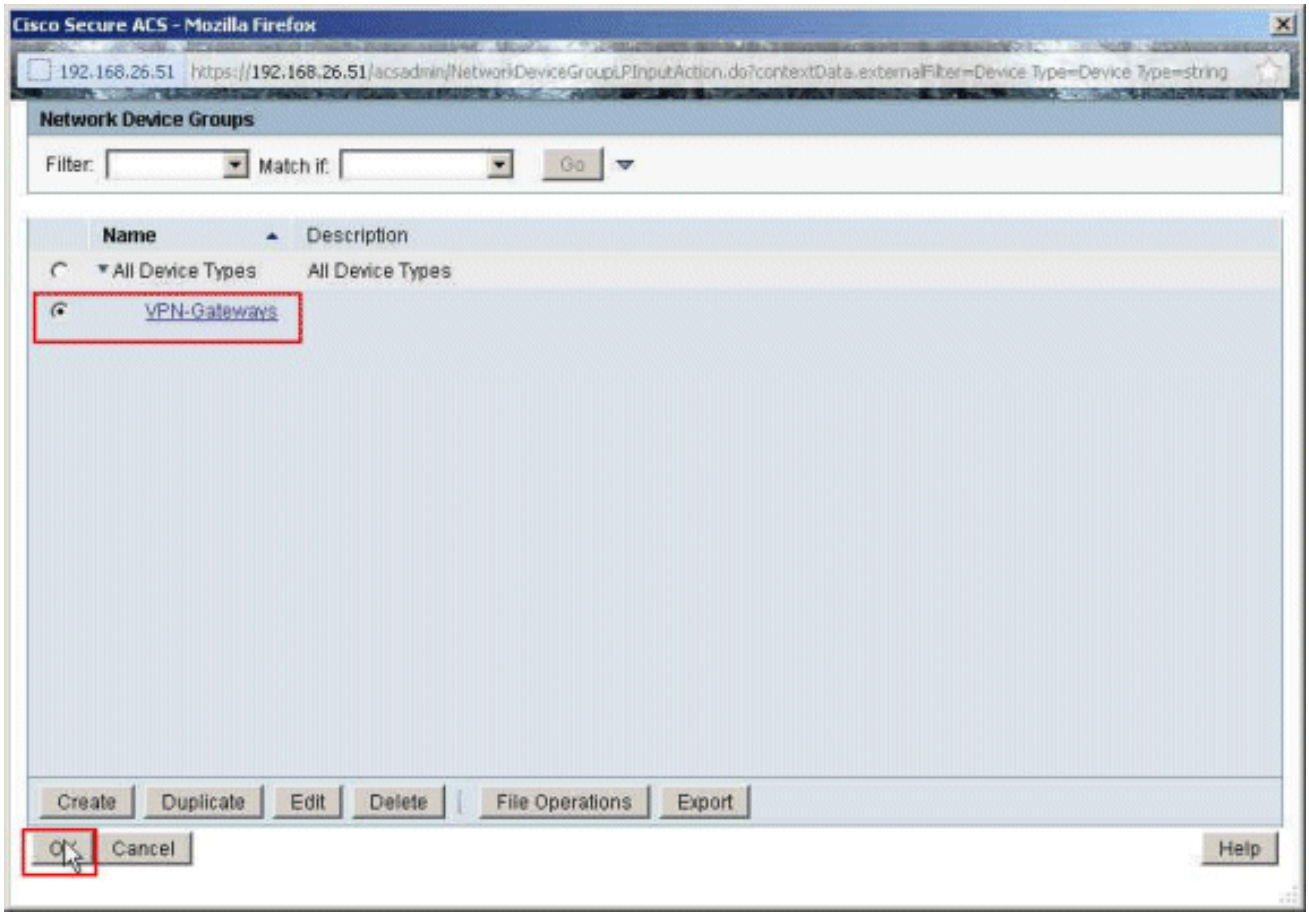


10. Stellen Sie sicher, dass das Kontrollkästchen neben **NDG:Device Type** aktiviert ist, und wählen Sie **in** der Dropdown-Liste aus. Klicken Sie auf

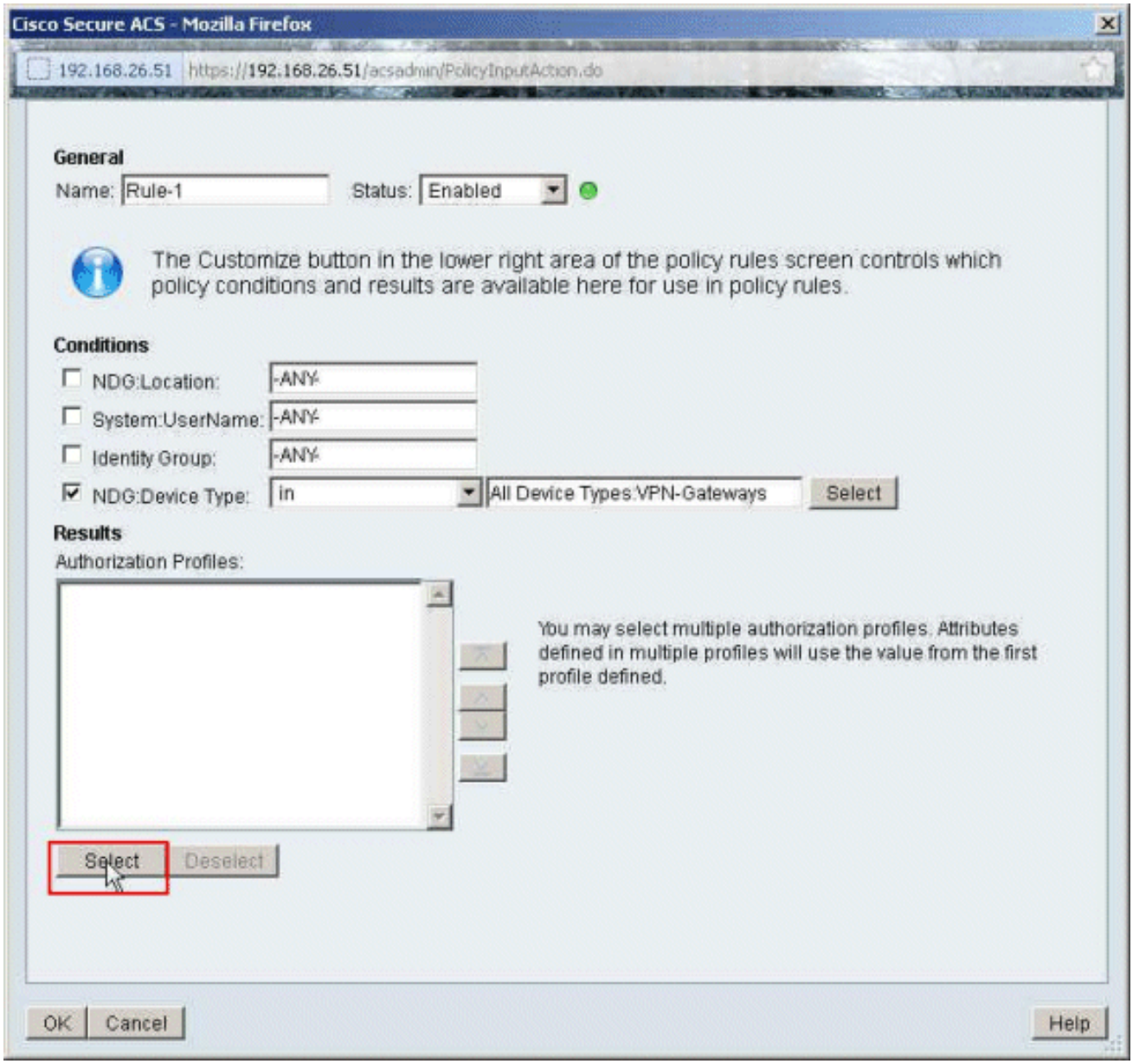
Auswählen.



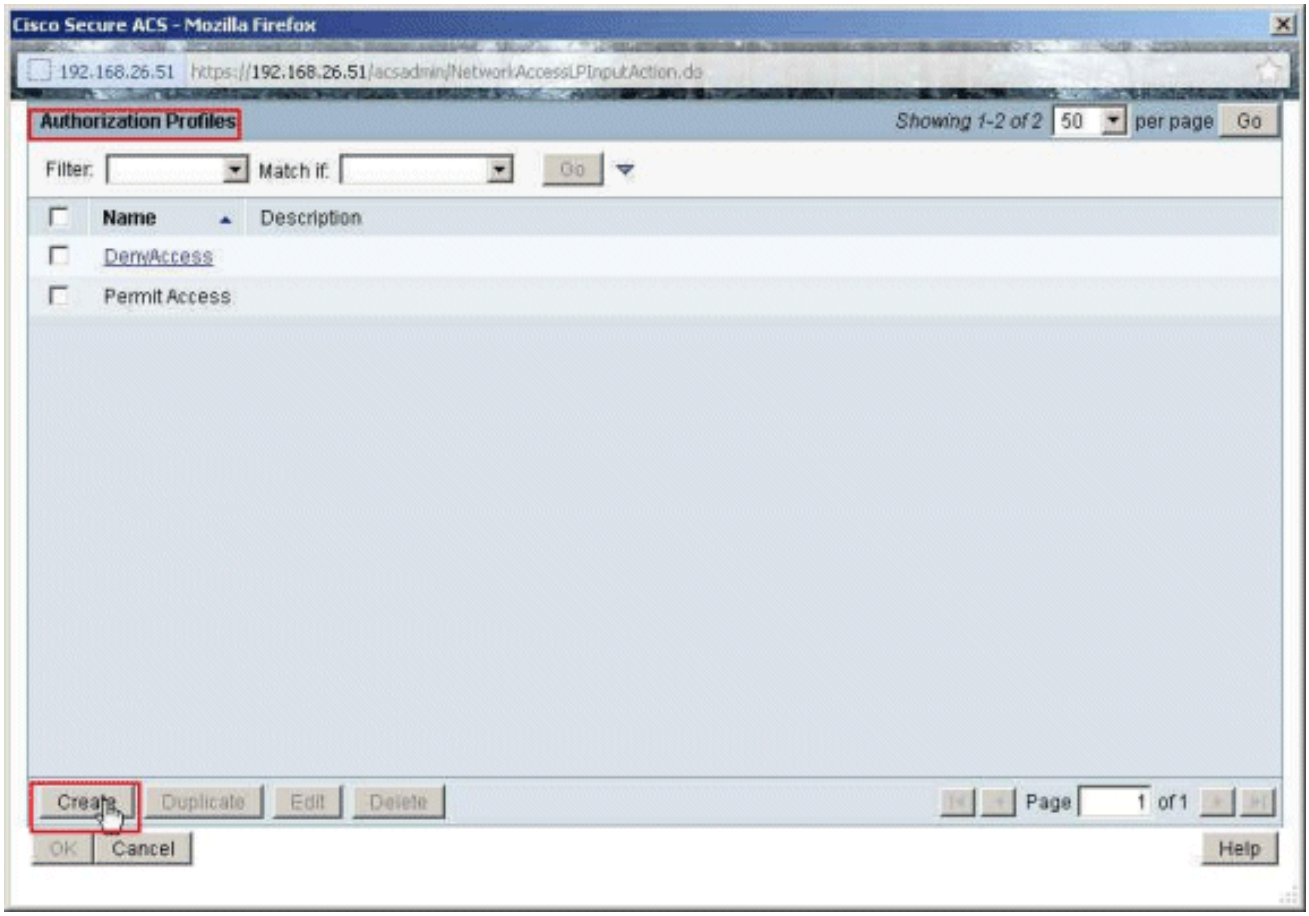
11. Wählen Sie die zuvor erstellten **VPN-Gateways** der Netzwerkgerätegruppe aus, und klicken Sie auf
OK.



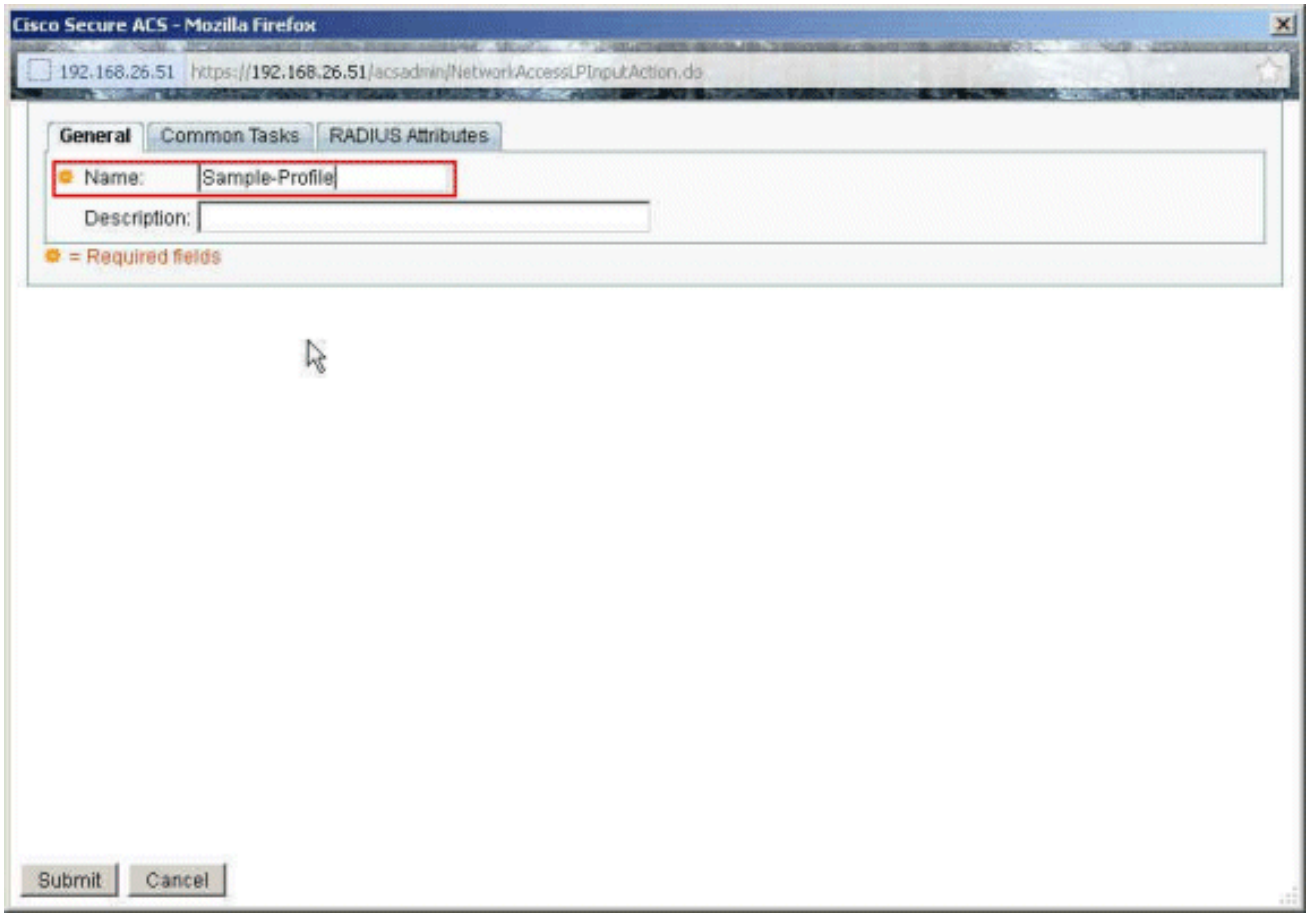
12. Klicken Sie auf **Auswählen**.



13. Klicken Sie auf **Erstellen**, um ein neues Autorisierungsprofil zu erstellen.

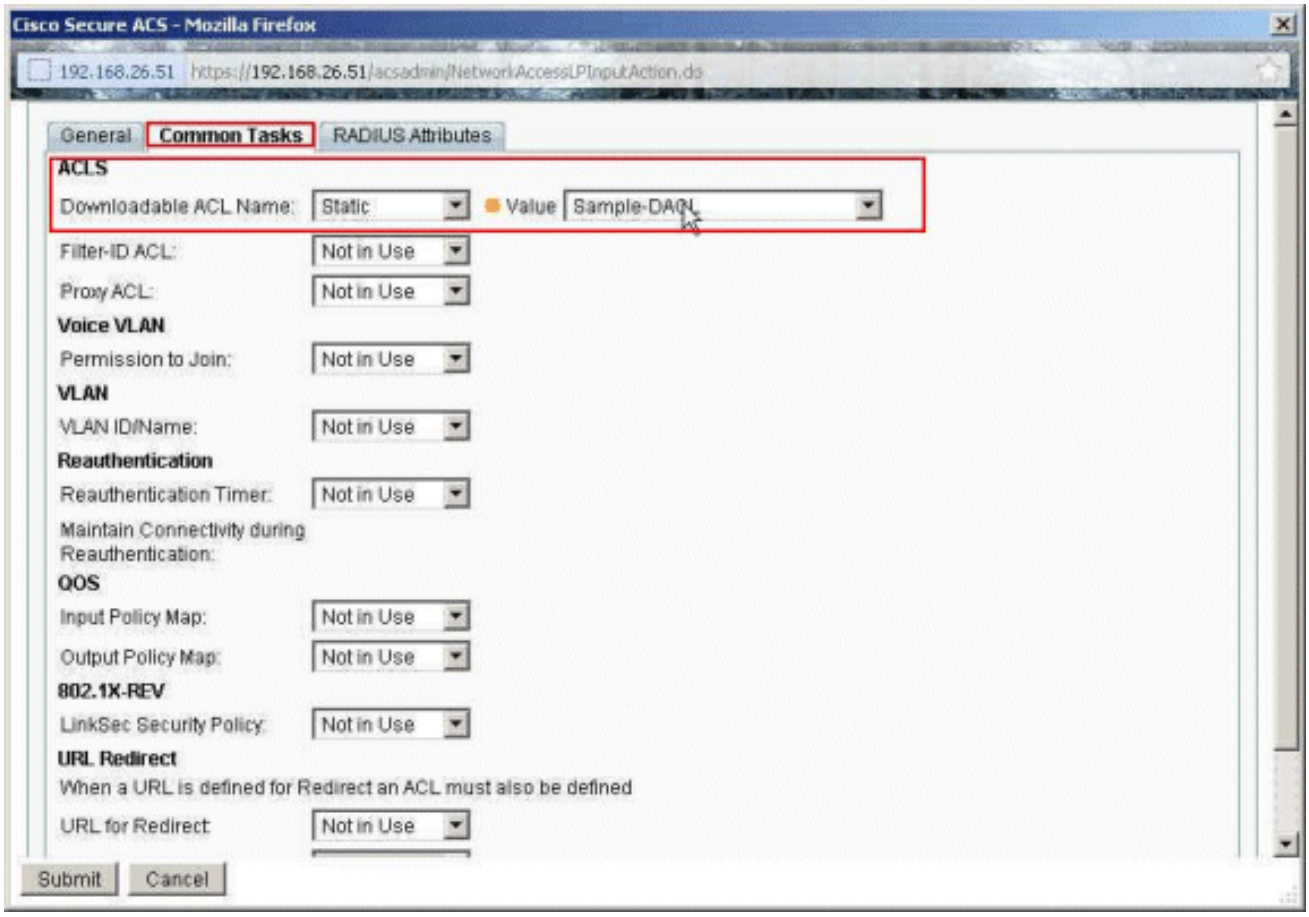


14. Geben Sie einen Namen für das **Autorisierungsprofil an**. **Ein Beispielprofil** ist der in diesem Beispiel verwendete
Name.

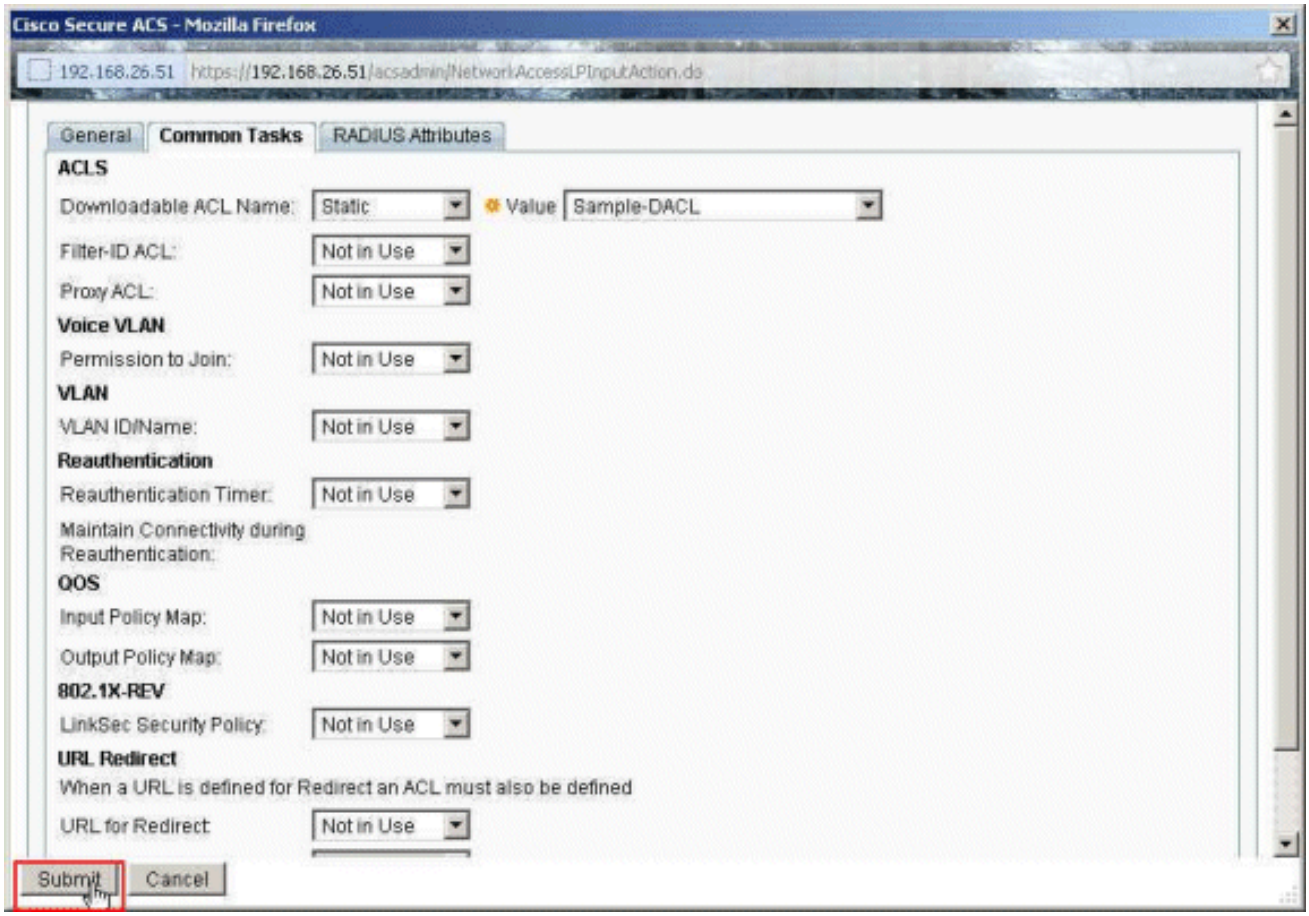


15. Wählen Sie die Registerkarte **Allgemeine Aufgaben**, und wählen Sie **Statisch** aus der Dropdown-Liste für den Namen der herunterladbaren ACL aus. Wählen Sie die neu erstellte

DACL (Sample-DACL) aus der Dropdown-Liste Wert aus.

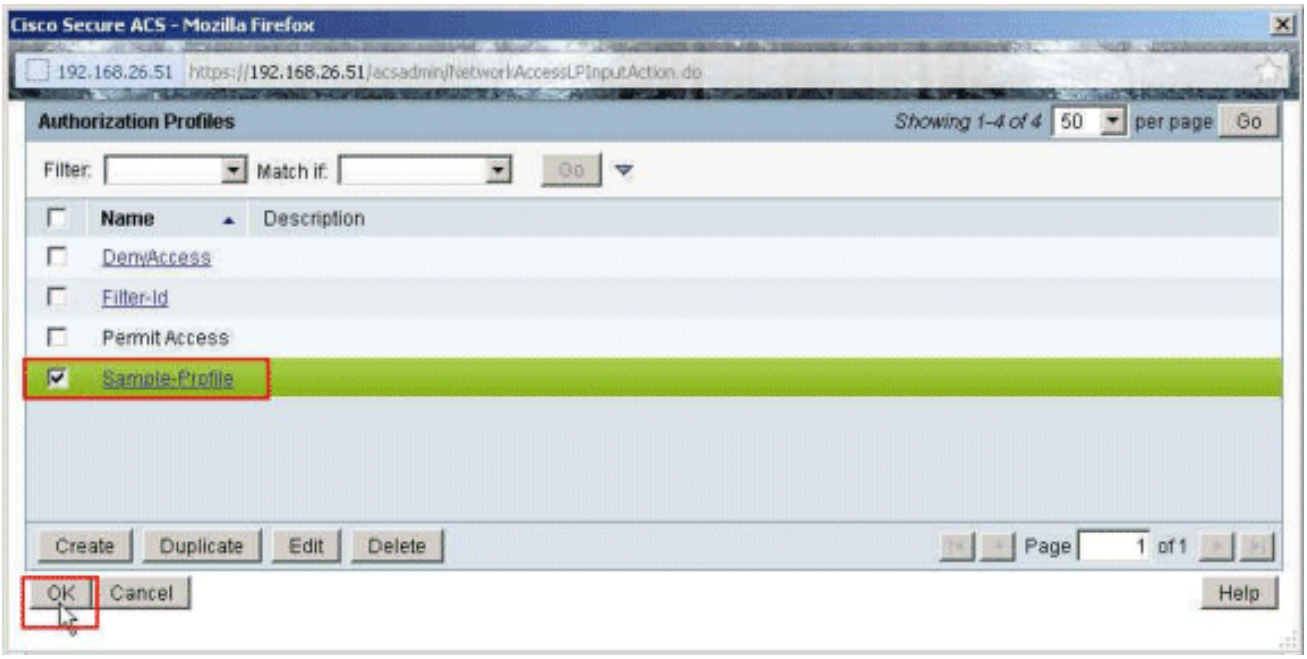


16. Klicken Sie auf **Senden**.

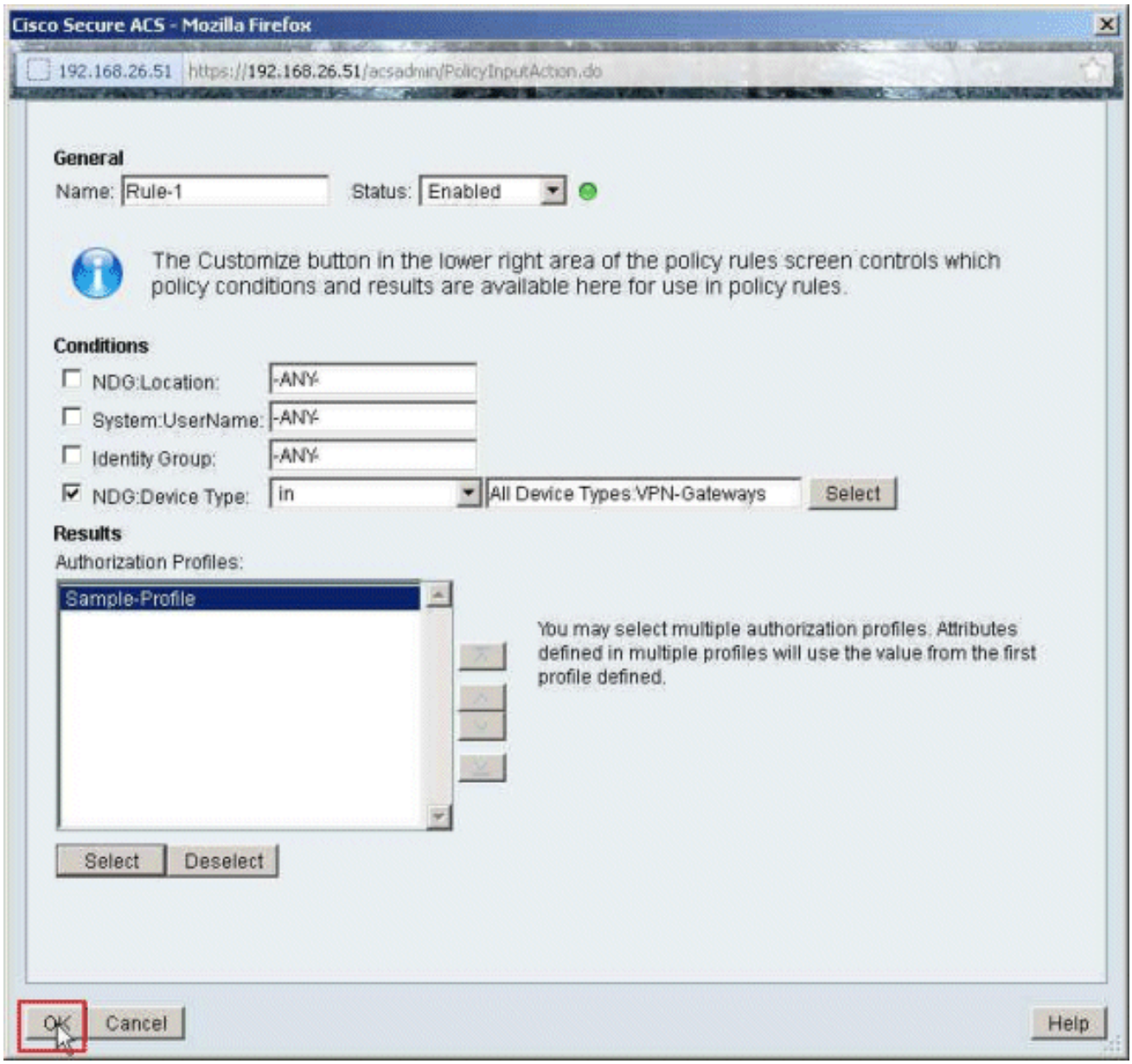


17. Wählen Sie **Beispielprofil aus**, das zuvor erstellt wurde, und klicken Sie auf

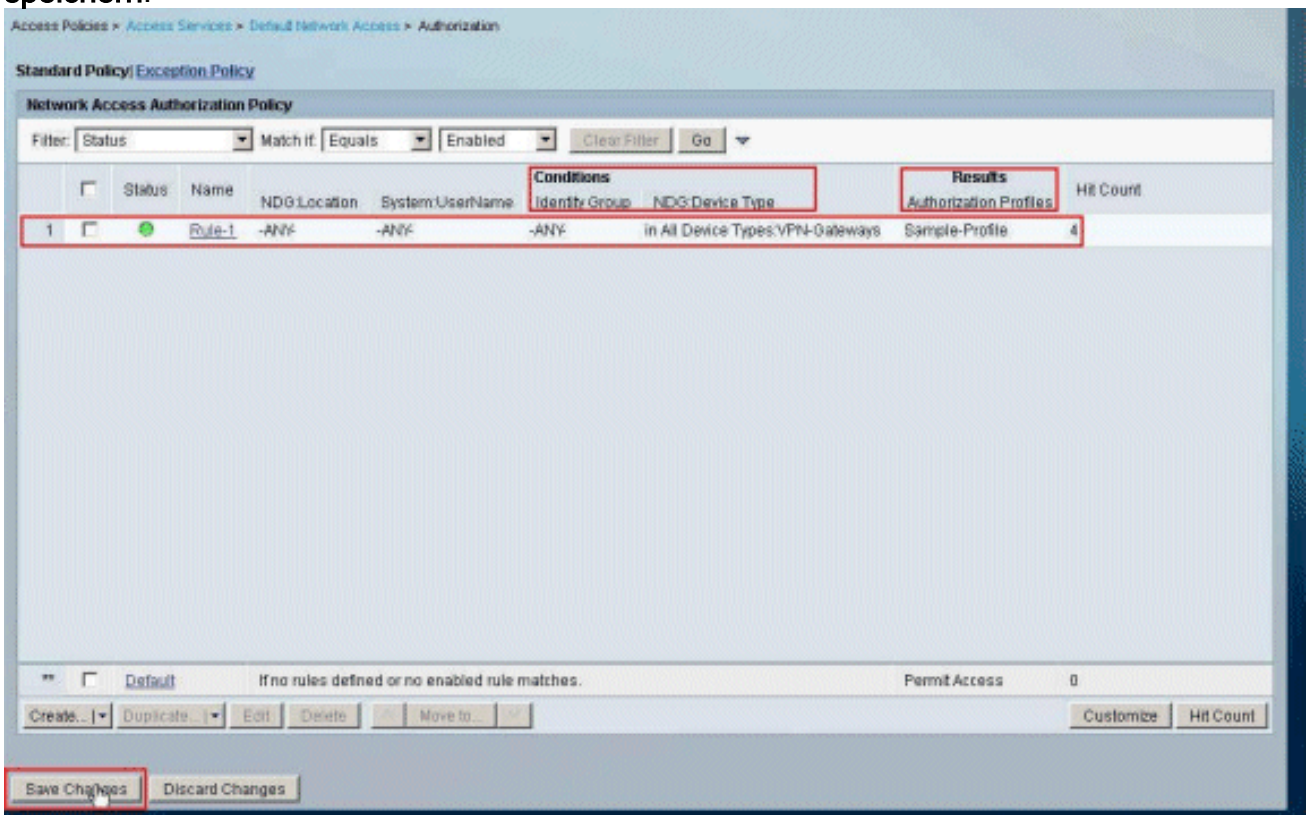
OK.



18. Klicken Sie auf
OK.



19. Überprüfen Sie, ob **Regel 1** mit **VPN-Gateways** als NDG:Gerätetyp als Bedingung und **Beispielprofil** als Ergebnis erstellt wird. Klicken Sie auf **Änderungen speichern**.



Konfigurieren der IETF-RADIUS-Einstellungen für eine Benutzergruppe

Um einen Namen für eine Zugriffsliste herunterzuladen, die Sie bereits auf der Sicherheits-Appliance vom RADIUS-Server erstellt haben, wenn sich ein Benutzer authentifiziert, konfigurieren Sie das IETF RADIUS-Filter-ID-Attribut (Attributnummer 11):

```
filter-id=acl_name
```

Der Sample-Group **usercisco** 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 konfiguriert:

- AAA-Client zur Verwendung eines der RADIUS-Protokolle in der Netzwerkkonfiguration
- Im Ergebnisbereich der Regel im Access-Service wird ein Autorisierungsprofil mit RADIUS

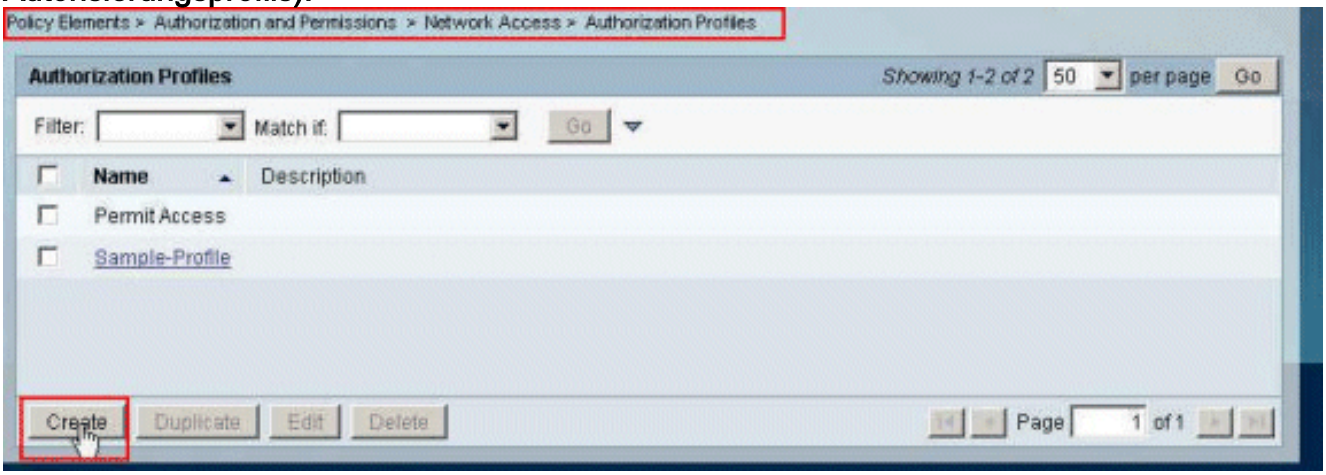
(IETF) Filter-ID ausgewählt.

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

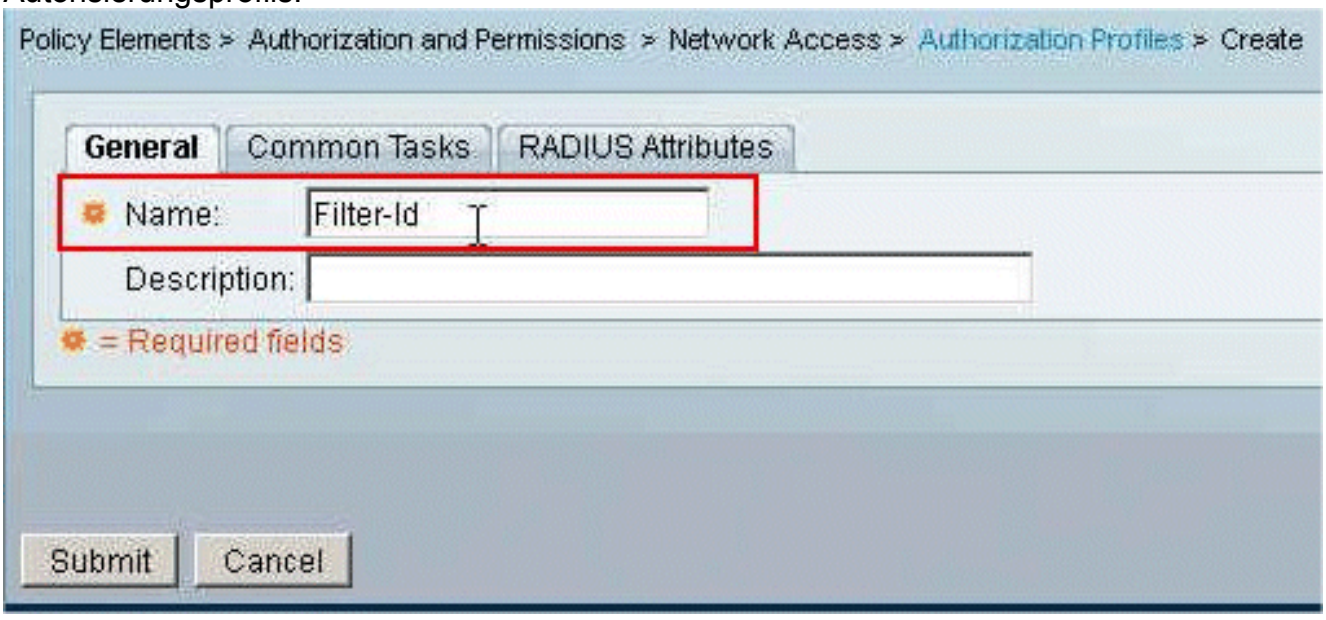
Führen Sie die Schritte 1 bis 6 und 10 bis 12 des Configure ACS for Download able ACL for Individual User aus, gefolgt von den Schritten 1 bis 6 des Dokuments Configure ACS for Download able ACL for Group, und führen Sie die Schritte in diesem Abschnitt aus, um die Filter-ID im Cisco Secure ACS zu konfigurieren.

So konfigurieren Sie die **IETF RADIUS-**Attributeinstellungen so, dass sie wie im Autorisierungsprofil angewendet werden:

1. Wählen Sie **Richtlinienelemente > Authorization and Permissions > Network Access > Authorization Profiles** (Richtlinienelemente **> Autorisierungsprofile > Network Access > Authorization Profiles (Autorisierungsprofile)** aus, und klicken Sie **auf Create (Erstellen eines neuen Autorisierungsprofils).**

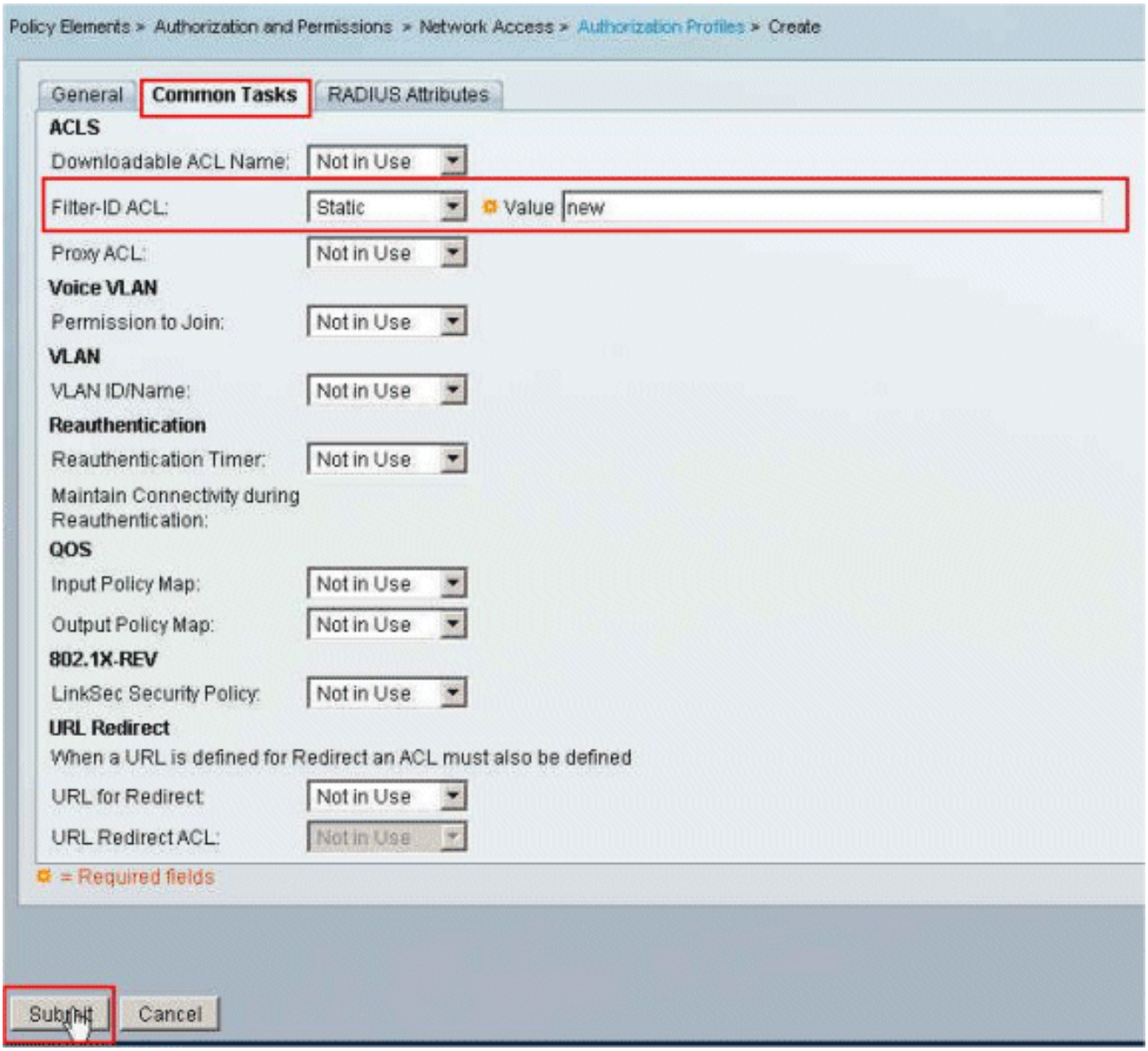


2. Geben Sie einen Namen für das **Autorisierungsprofil an**. **Filter-ID** ist der in diesem Beispiel aus Gründen der Einfachheit ausgewählte Name des Autorisierungsprofils.

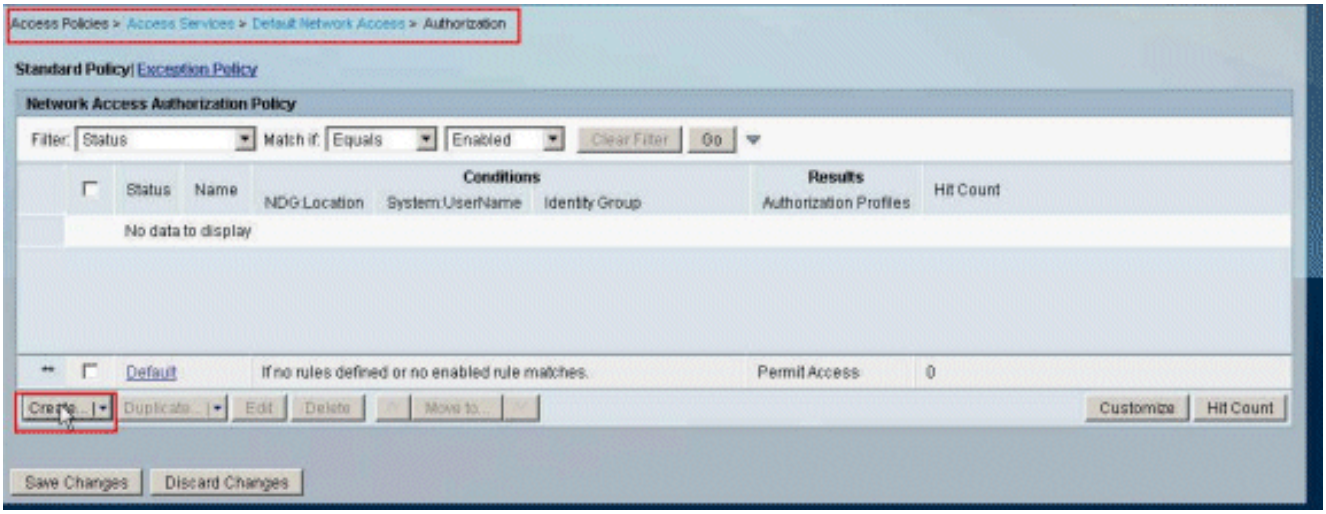


3. Klicken Sie auf die Registerkarte **Allgemeine Aufgaben**, und wählen Sie in der Dropdown-Liste für **Filter-ID-ACL** die Option **Statisch**. Geben Sie den Namen der Zugriffsliste als **neu** in das Feld Wert ein, und klicken Sie auf

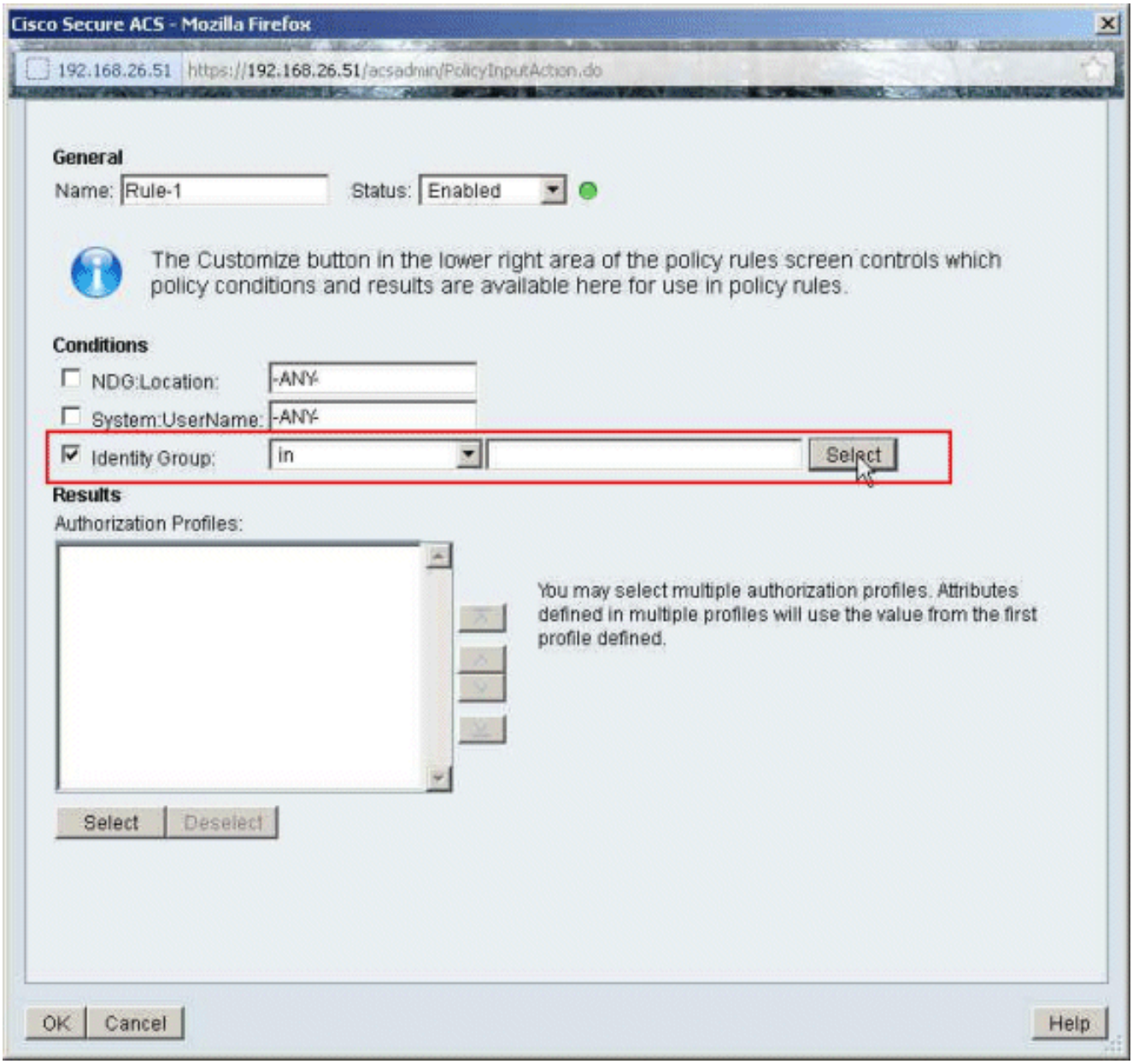
Senden.



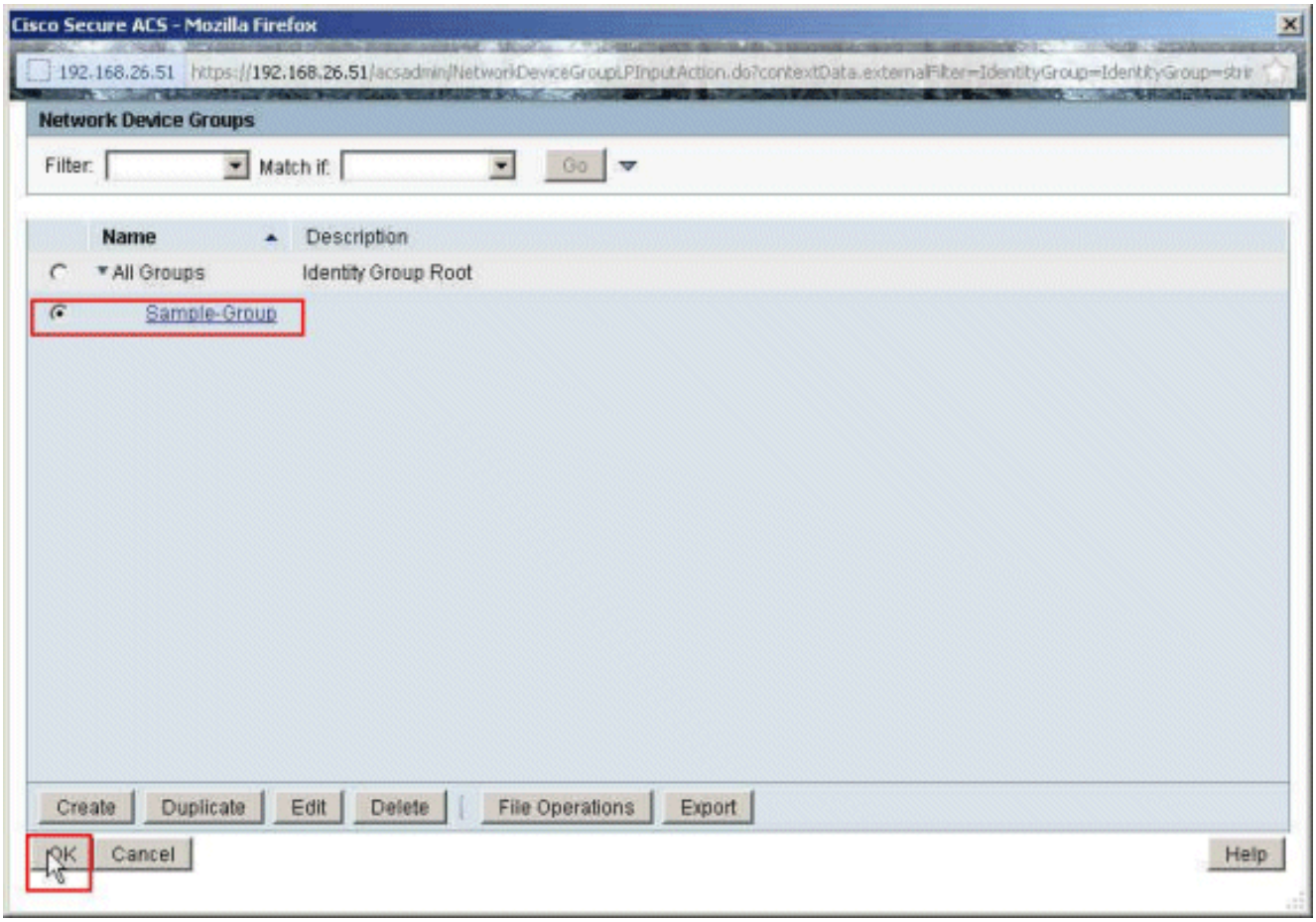
4. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Autorisierung** aus, und klicken Sie **auf Erstellen, um eine neue Regel zu erstellen.**



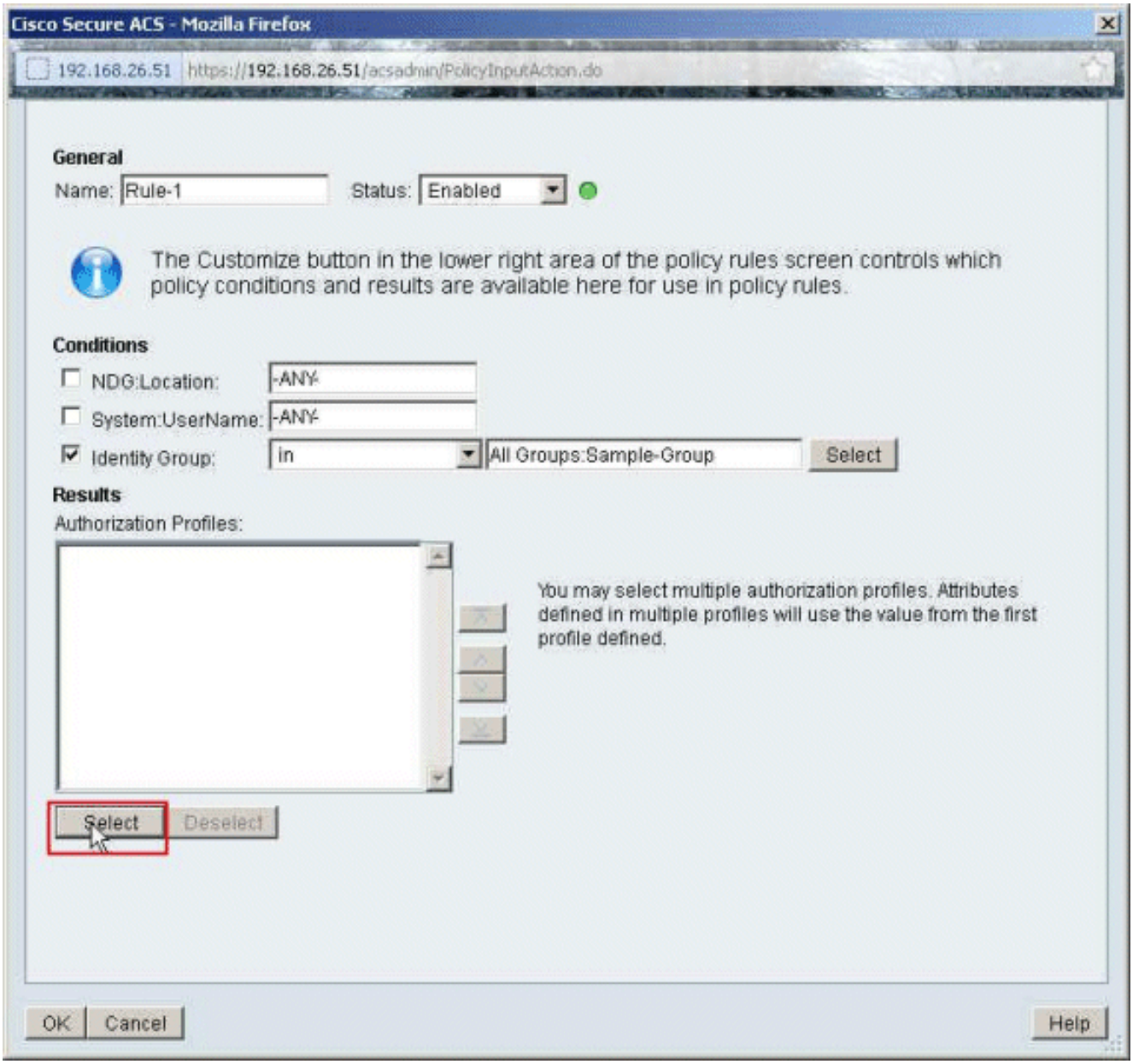
5. Stellen Sie sicher, dass das Kontrollkästchen neben **Identitätsgruppe** aktiviert ist, und klicken Sie auf **Auswählen**.



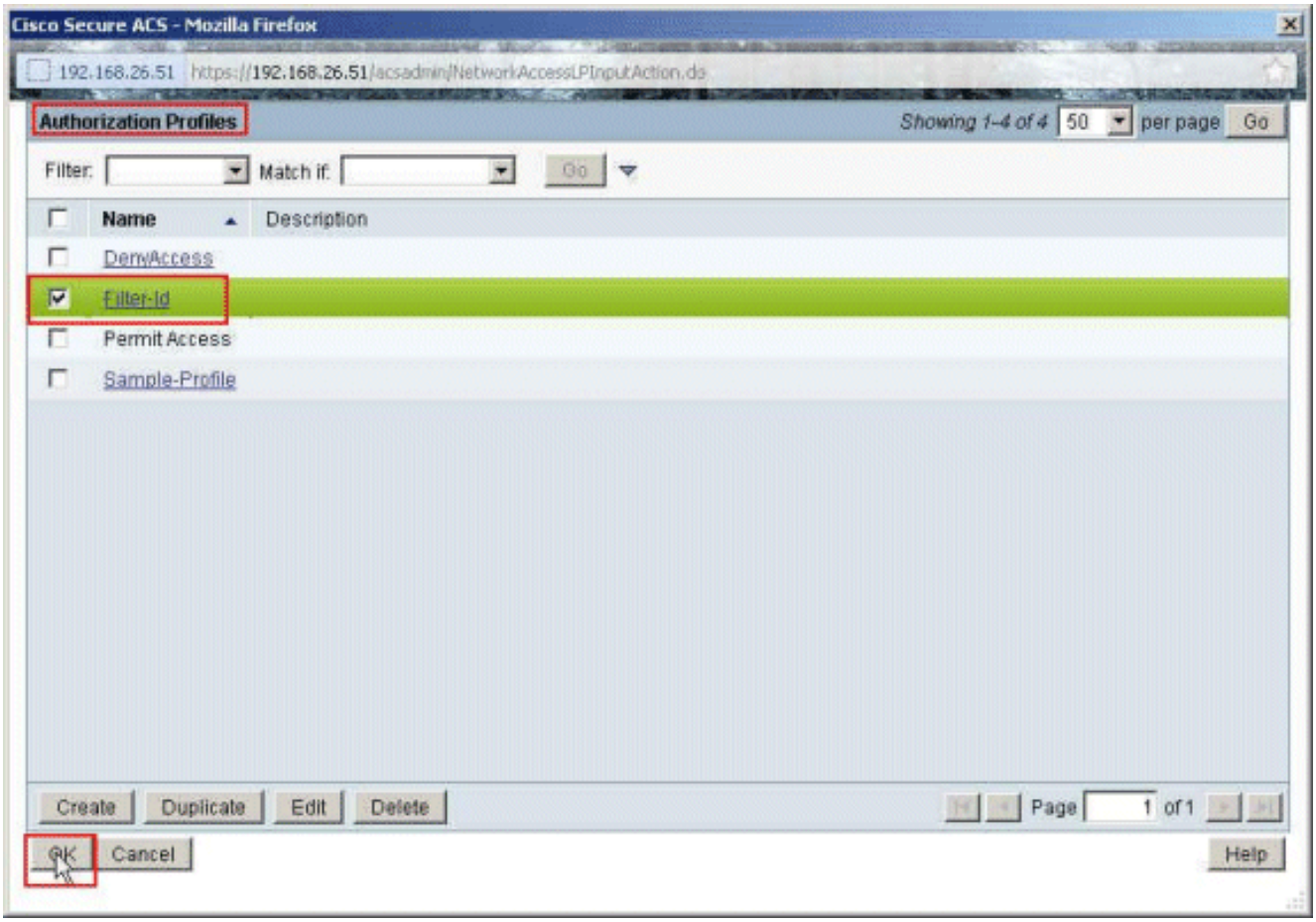
6. Wählen Sie **Sample-Group** aus, und klicken Sie auf **OK**.



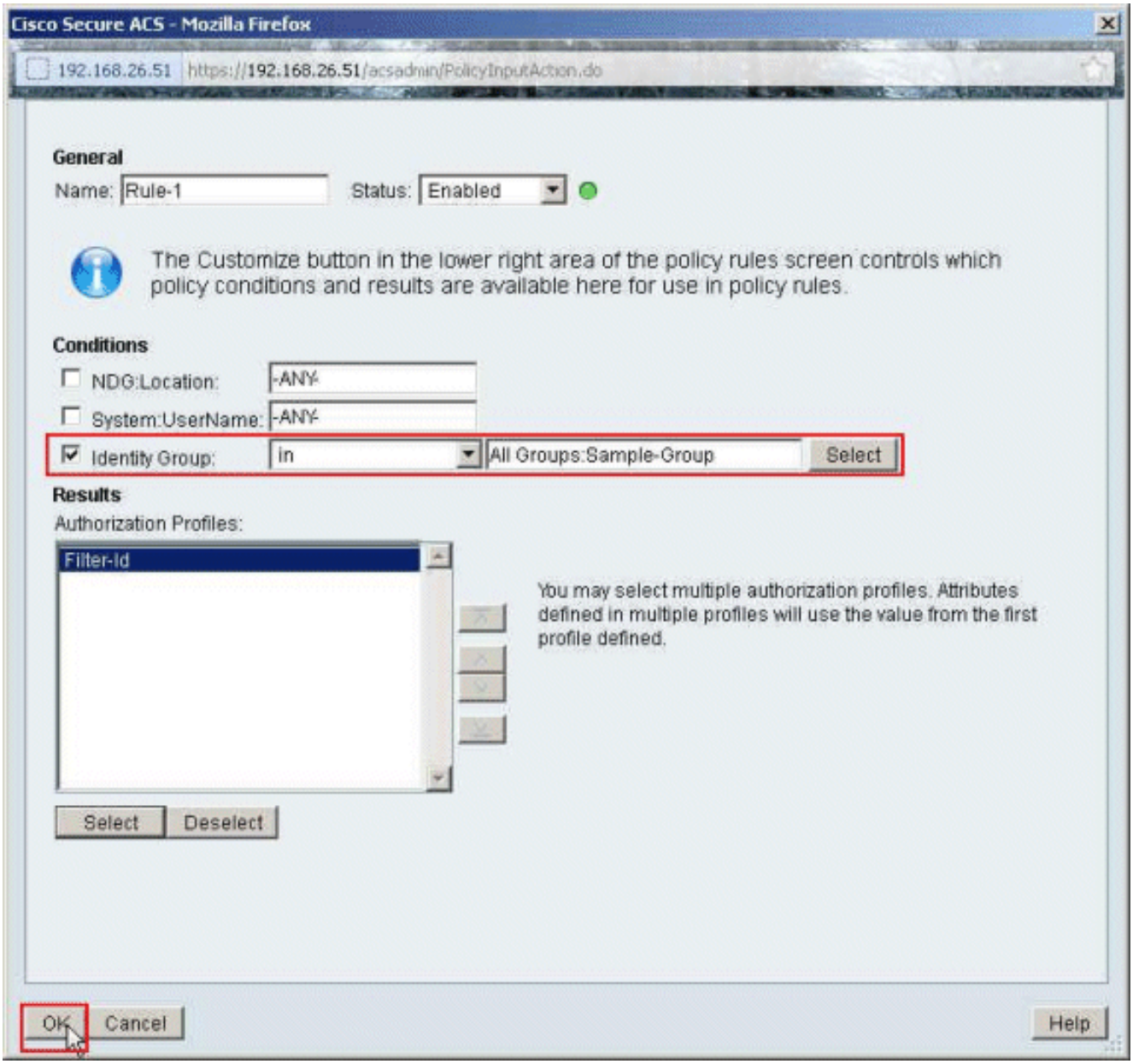
7. Klicken Sie im Abschnitt Autorisierungsprofile auf **Auswählen**.



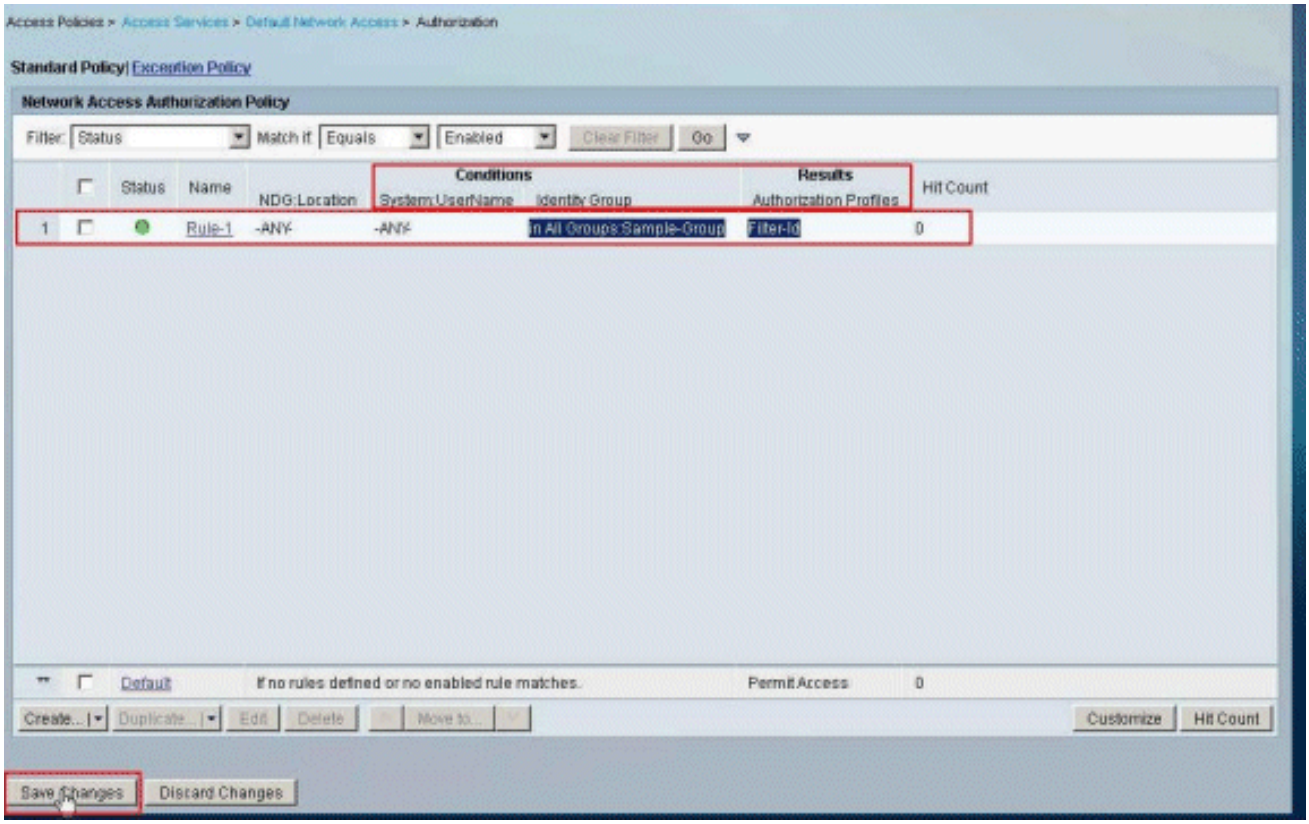
8. Wählen Sie die zuvor erstellte **Filter-ID für das** Autorisierungsprofil **aus**, und klicken Sie auf **OK**.



9. Klicken Sie auf **OK**.



10. Überprüfen Sie, ob **Regel 1** mit **der** Identitätsgruppen**-Beispielgruppe** als Bedingung und **Filter-ID** als Ergebnis erstellt wird. Klicken Sie auf **Änderungen speichern**.

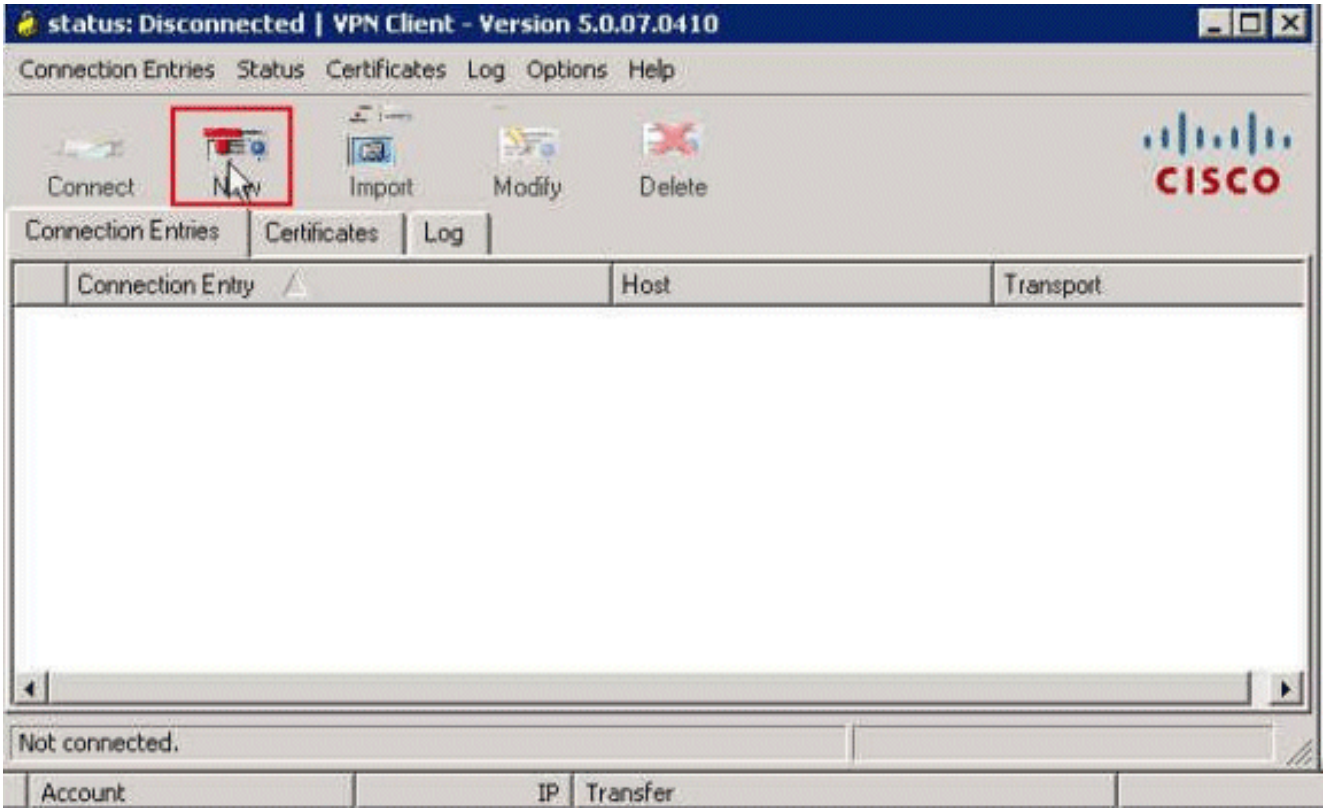


Konfiguration des Cisco VPN-Clients

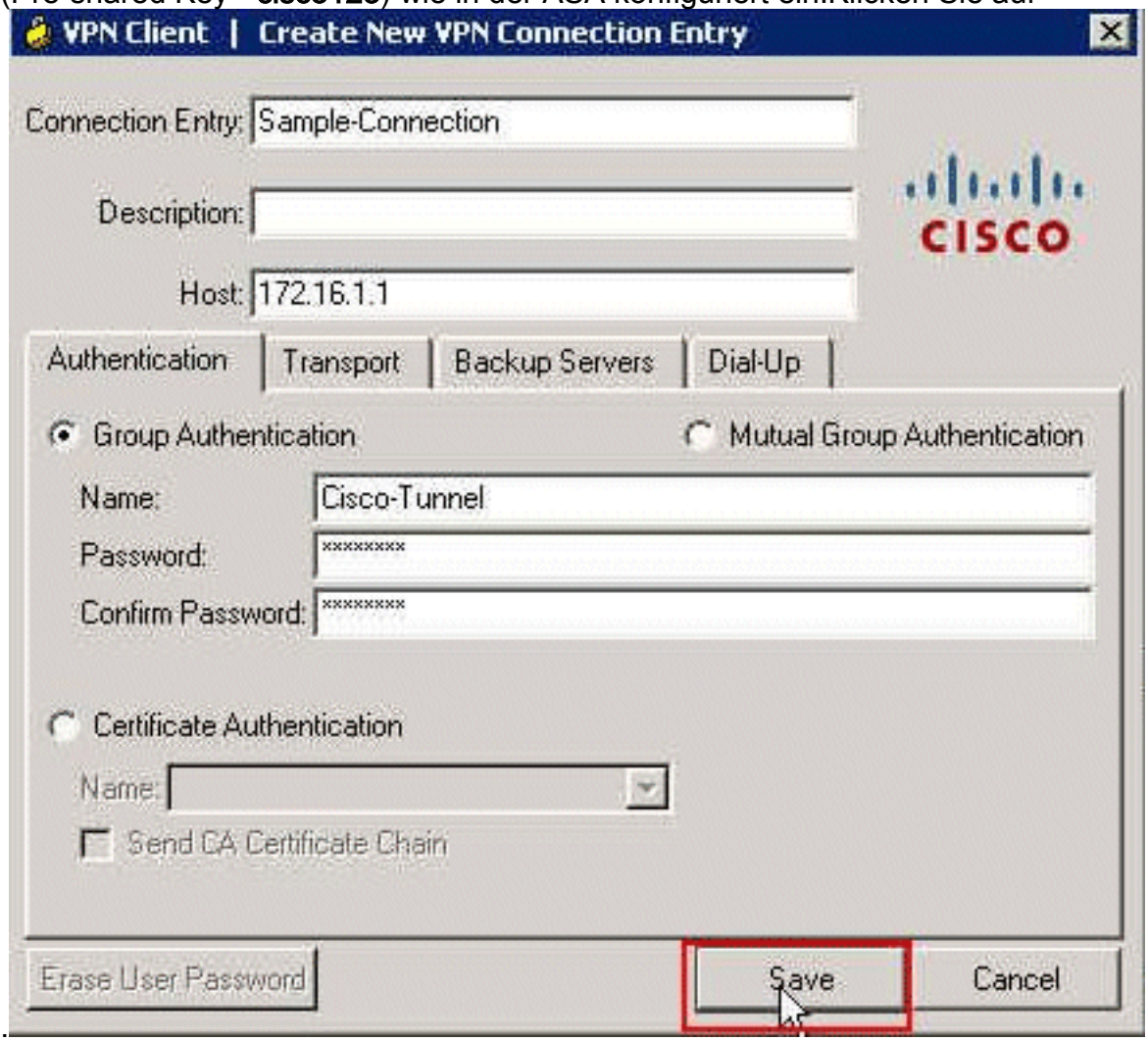
Stellen Sie mit dem Cisco VPN Client eine Verbindung zur Cisco ASA her, um zu überprüfen, ob die ASA erfolgreich konfiguriert wurde.

Gehen Sie wie folgt vor:

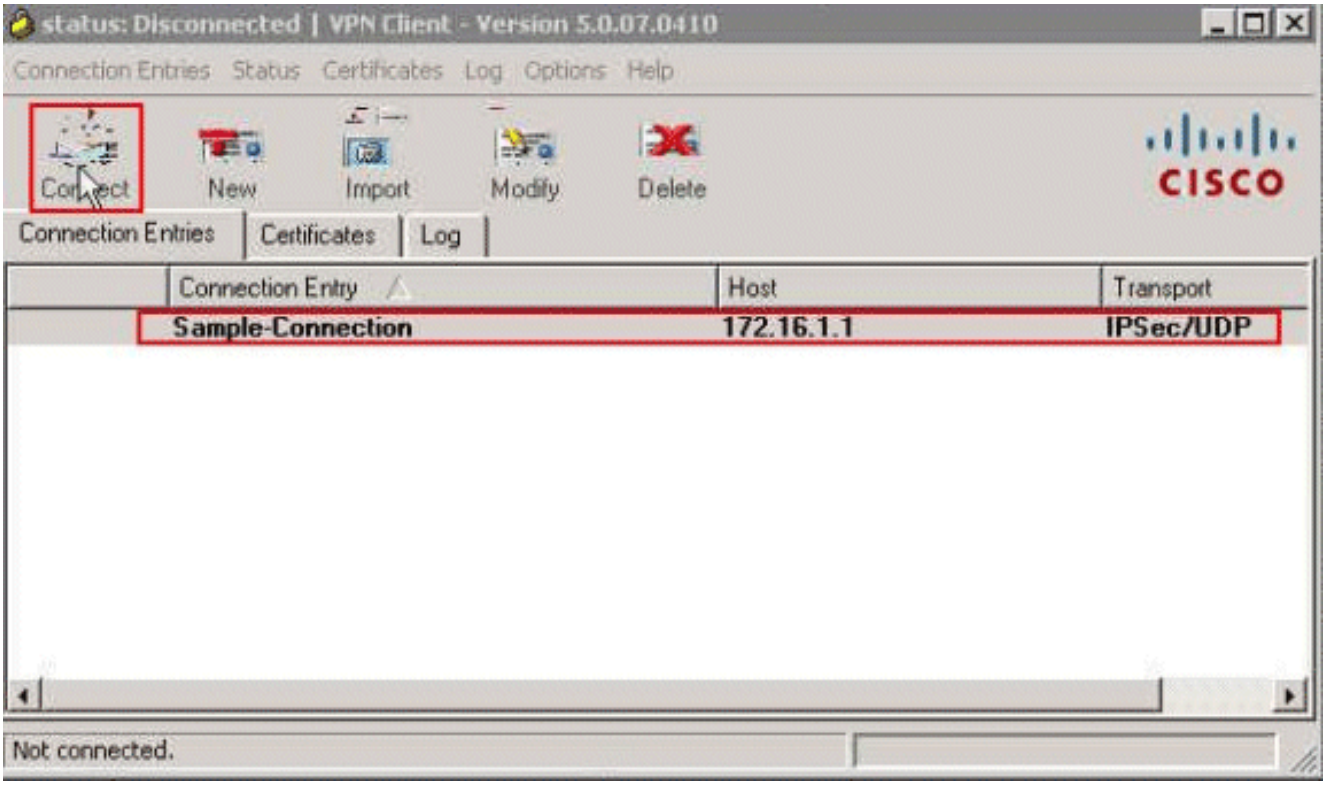
1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client aus**.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu
   öffnen.



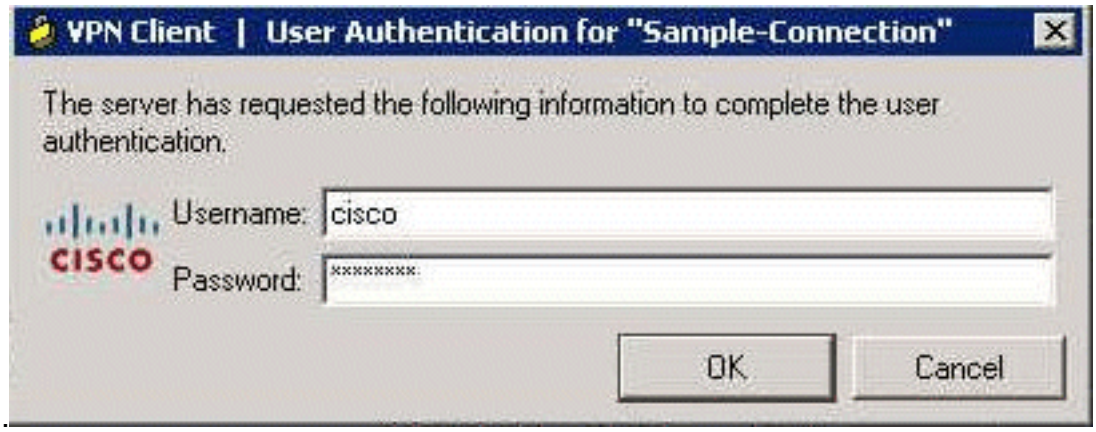
3. Geben Sie die Details Ihrer neuen Verbindung an:Geben Sie den Namen des Verbindungseintrags und eine Beschreibung ein.Geben Sie die **externe IP-Adresse der ASA** im Host-Feld ein.Geben Sie den VPN-Tunnel-Gruppennamen (**Cisco-Tunnel**) und das Kennwort (Pre-shared Key - **cisco123**) wie in der ASA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



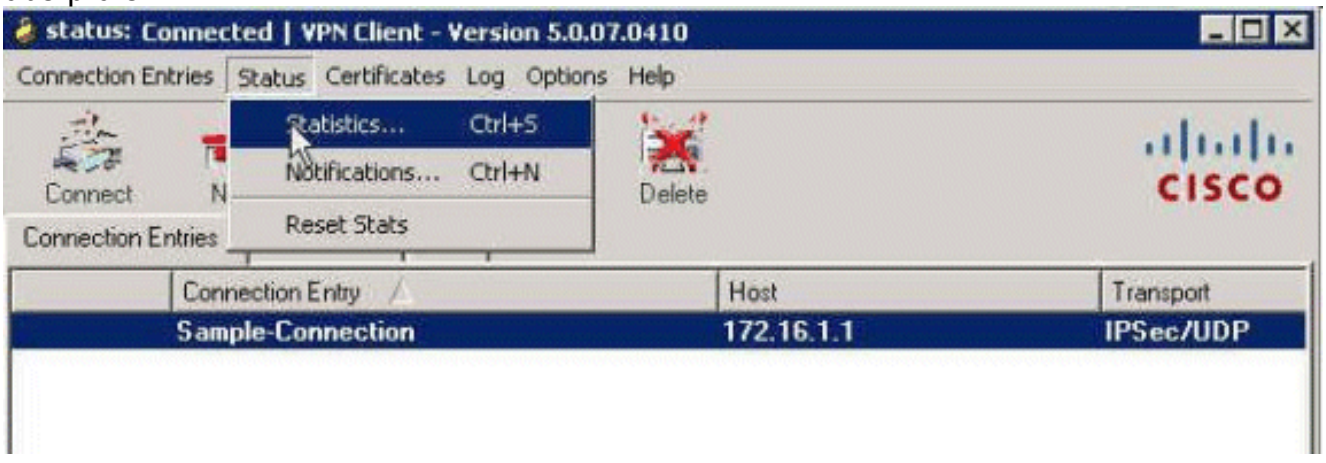
4. Klicken Sie auf die Verbindung, die Sie verwenden möchten, und klicken Sie im Hauptfenster des VPN-Clients auf **Verbinden**.



5. Geben Sie bei Aufforderung den Benutzernamen **cisco** und das Kennwort **cisco123** wie in der ASA für die Authentifizierung konfiguriert ein, und klicken Sie auf **OK**, um eine Verbindung zum Remote-Netzwerk herzustellen.



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



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

IKEv1 SAs:

   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: 172.16.1.50
    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: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
       172.16.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 172.16.1.50, username: cisco
      dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
      #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 9A06E834
      current inbound spi : FA372121

    inbound esp sas:
      spi: 0xFA372121 (4197916961)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
```

```
spi: 0x9A06E834 (2584143924)
   transform: esp-aes esp-sha-hmac no compression
   in use settings ={RA, Tunnel, }
   slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
   sa timing: remaining key lifetime (sec): 28678
   IV size: 16 bytes
   replay detection support: Y
   Anti replay bitmap:
    0x00000000 0x00000001
```

ACL zum Download für Benutzer/Gruppe

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

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
           alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

Filter-ID ACL

Die [011] Filter-ID wurde für die Gruppe "Sample-Group" (Beispielgruppe) 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 OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list new; 2 elements; name hash: 0xa39433d3
access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
   0x58a3ea12
access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration. Außerdem wird eine Beispielausgabe für das **Debuggen** angezeigt.

Hinweis: Weitere Informationen zur Fehlerbehebung bei IPsec-VPN für Remote-Zugriff finden Sie unter Häufigste L2L- und IPsec-VPN-Lösungen zur Fehlerbehebung für Remote-Zugriff.

Sicherheitszuordnungen löschen

Achten Sie bei der Fehlerbehebung darauf, vorhandene SAs nach der Änderung zu löschen.

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
- Cisco Adaptive Security Device Manager
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Support-Seite für Cisco VPN-Clients
- Cisco Secure Access Control System
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems