ASA/PIX: Statische IP-Adressierung für IPSec VPN Client mit CLI und ASDM - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Adaptive Security Appliance (ASA) der Serie 5500 so konfiguriert wird, dass sie dem VPN-Client die statische IP-Adresse mit dem Adaptive Security Device Manager (ASDM) oder der CLI bereitstellt. Der ASDM bietet erstklassige Sicherheitsverwaltung und -überwachung über eine intuitive, benutzerfreundliche webbasierte Verwaltungsschnittstelle. Sobald die Cisco ASA-Konfiguration abgeschlossen ist, kann sie mit dem Cisco VPN-Client verifiziert werden.

Weitere Informationen zum Einrichten der VPN-Verbindung zwischen einem Cisco VPN-Client (4.x für Windows) und der PIX/ASA 7.x-Sicherheitslösung der Serie PIX 500 finden Sie unter Konfigurationsbeispiel für die Authentifizierung von RADIUS (gegen Active Directory) und Cisco VPN Client 4.x mit Windows 2003. Der Remote-VPN-Client-Benutzer authentifiziert sich über Active Directory mithilfe eines RADIUS-Servers des Microsoft Windows 2003 Internet Authentication Service (IAS).

Unter PIX/ASA 7.x und Cisco VPN Client 4.x finden Sie ein Konfigurationsbeispiel für die Cisco Secure ACS-Authentifizierung, um eine VPN-Verbindung für den Remote-Zugriff zwischen einem

Cisco VPN-Client (4.x für Windows) und der PIX 500 Security Appliance 7.x mit einem Cisco Secure Access Control Server (ACS Version 3.2) für die erweiterte Authentifizierung (Xauth) einzurichten.

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
- Adaptive Security Device Manager Version 5.x und höher
- Cisco VPN Client Version 4.x und höher

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).

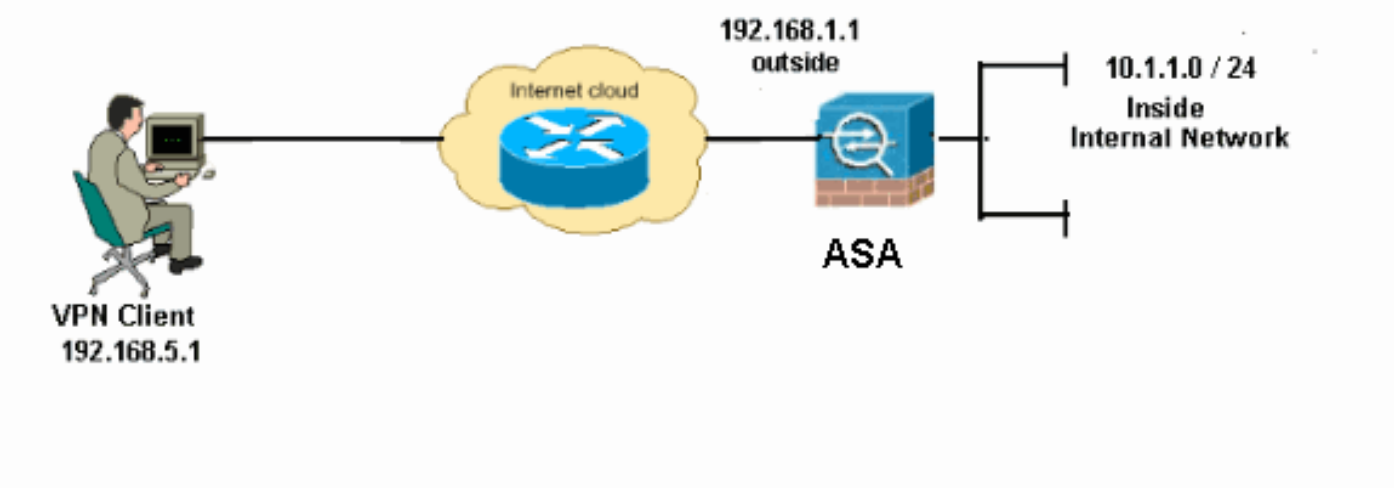
Konfigurieren

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:



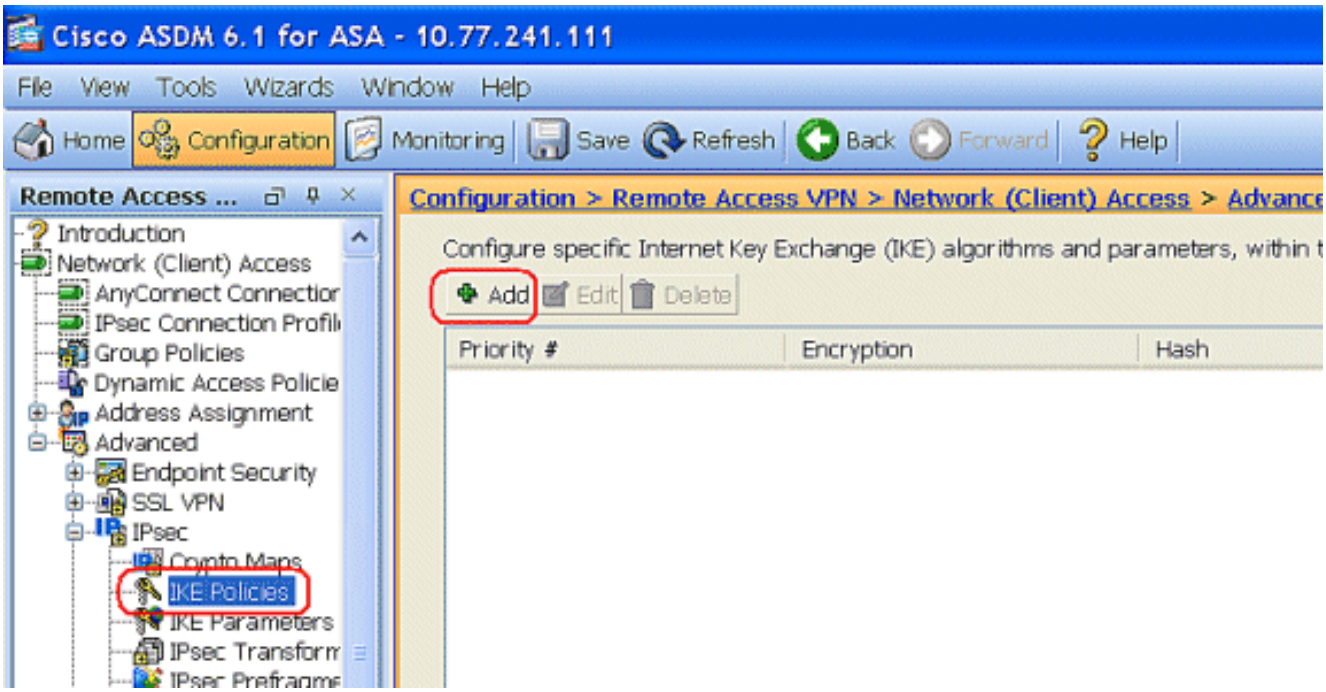
Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurieren von Remote Access VPN (IPSec)

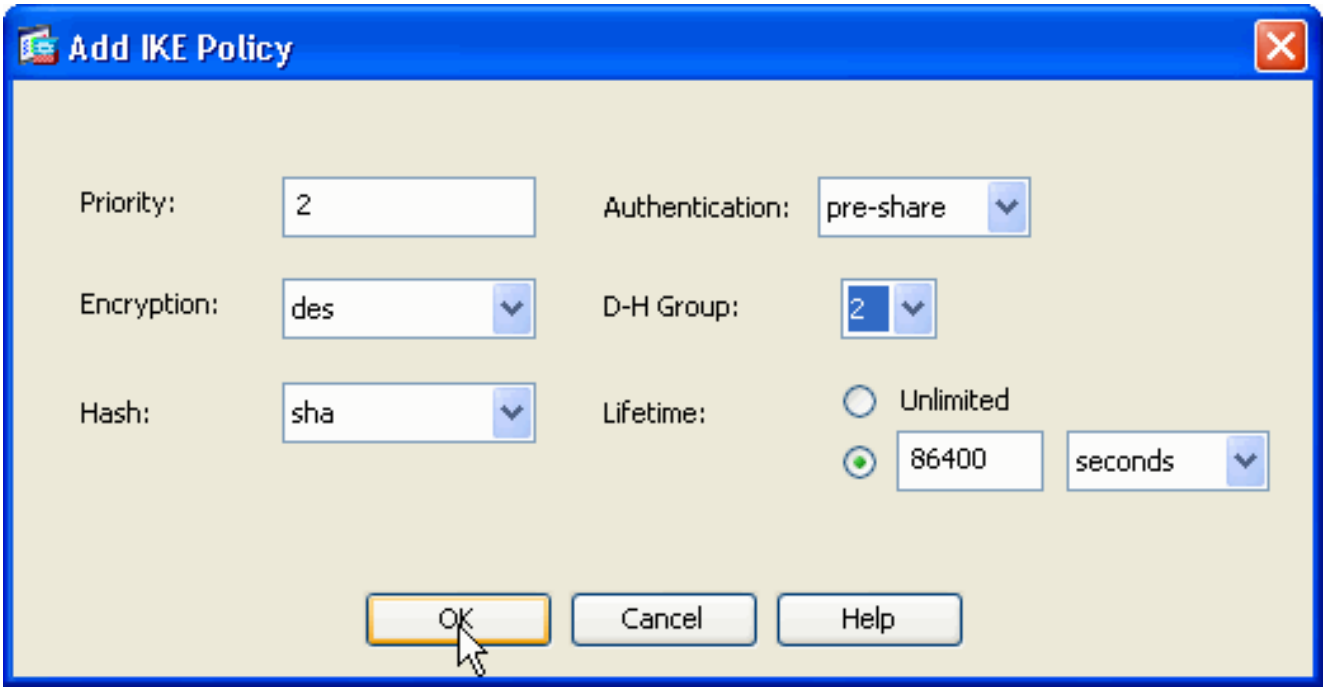
ASDM-Verfahren

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.

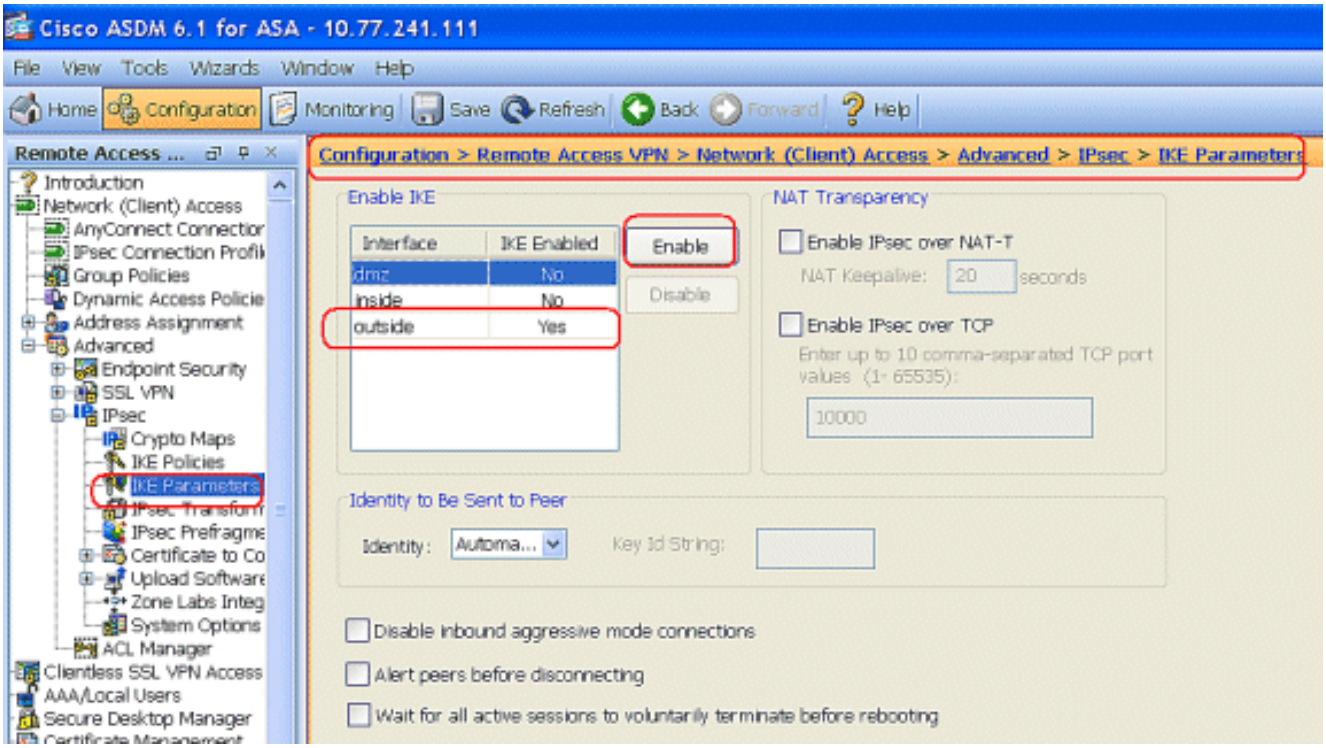


2. Geben Sie die ISAKMP-Richtliniendetails an.

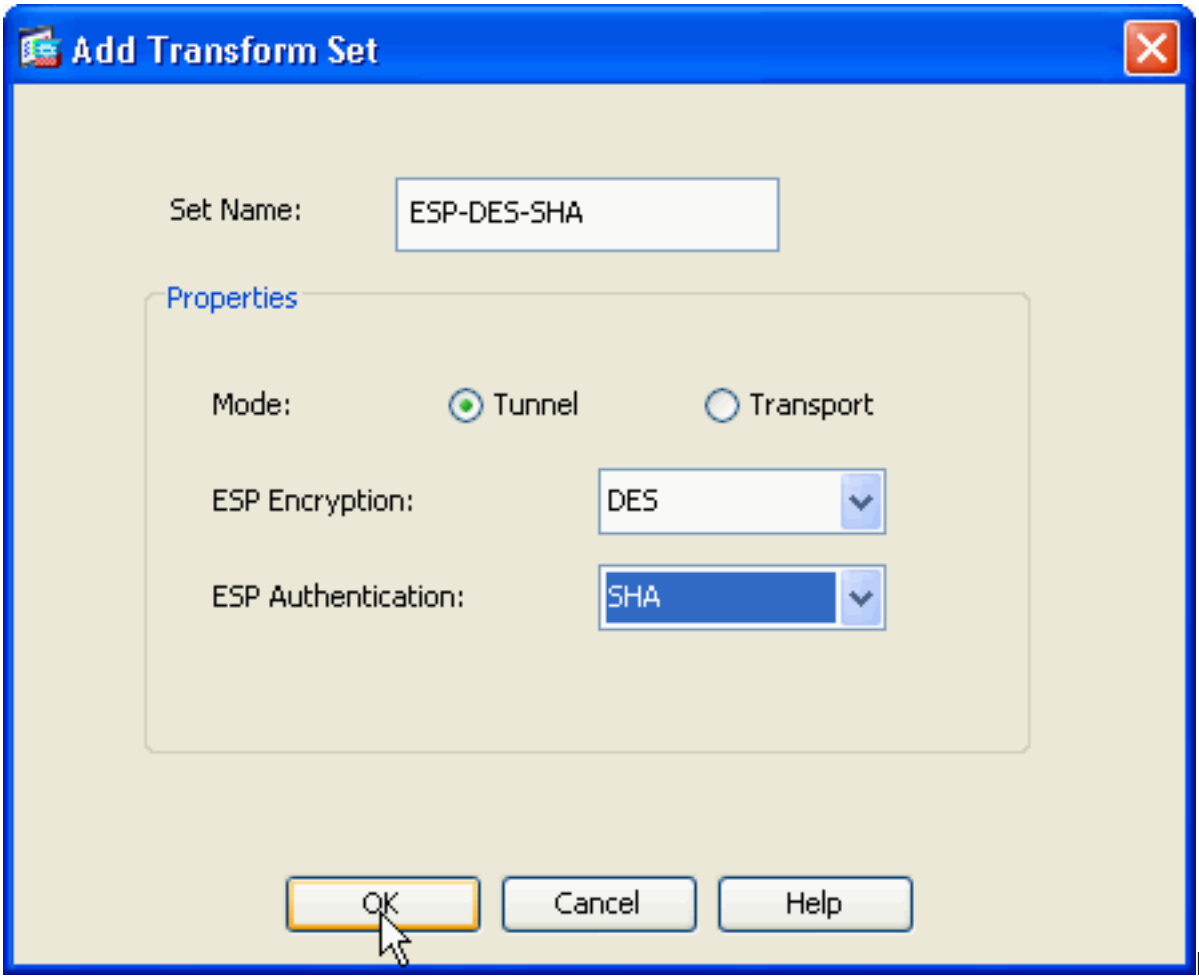


Klicken Sie auf **OK** und **Übernehmen**.

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

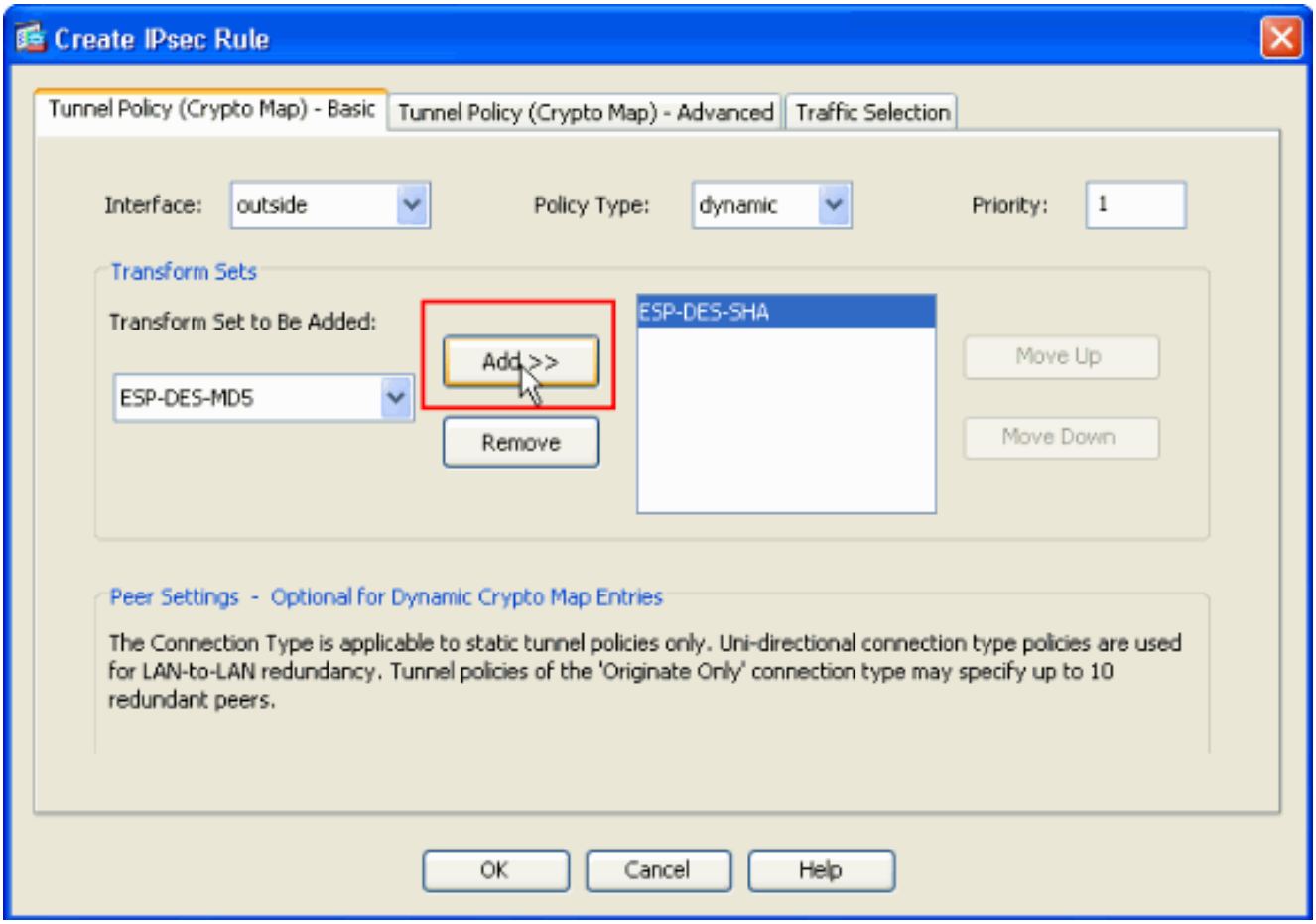


4. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add** aus, um den **ESP-DES-SHA**-Transformationssatz zu erstellen, wie dargestellt.



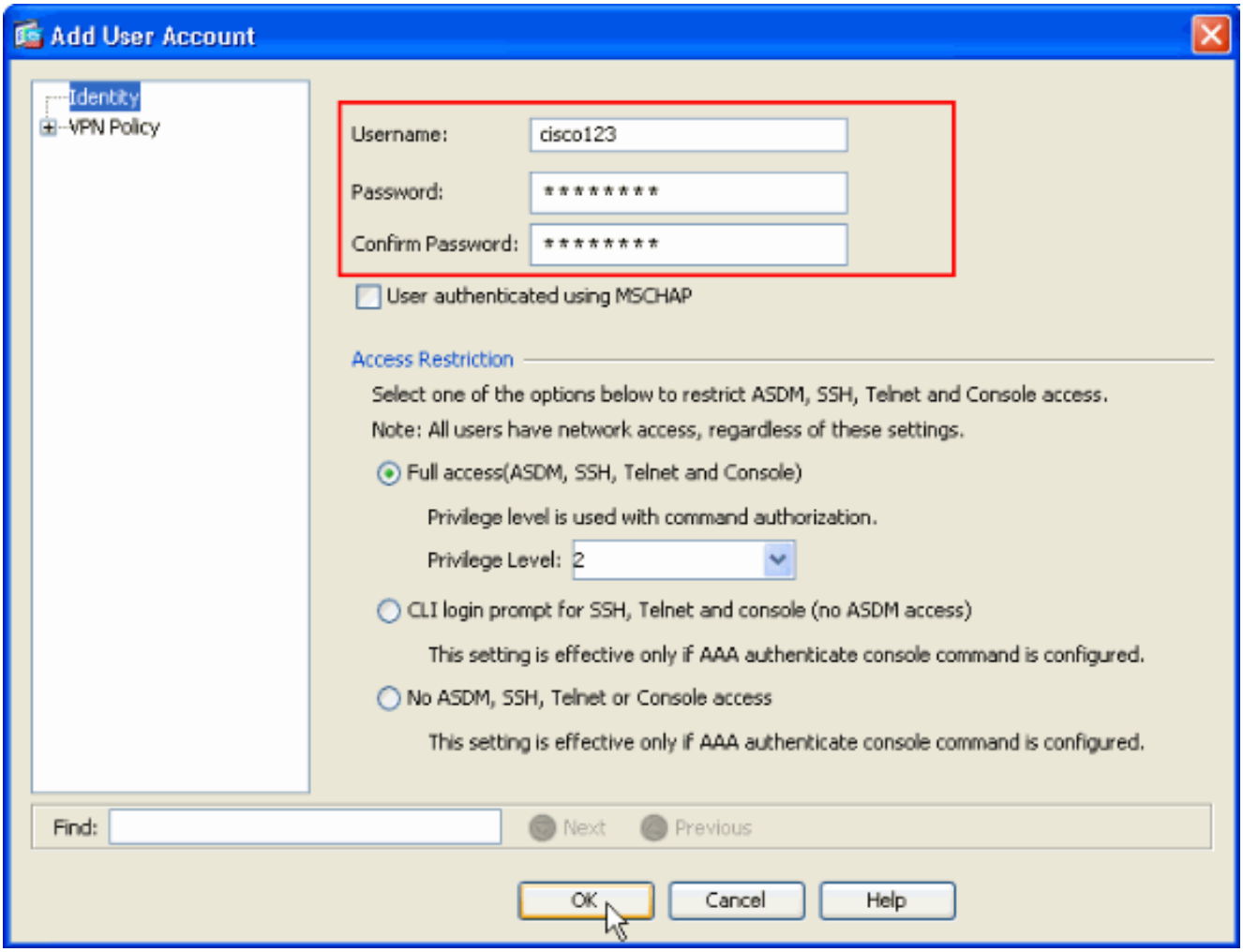
Klicken Sie auf **OK** und **Übernehmen**.

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.

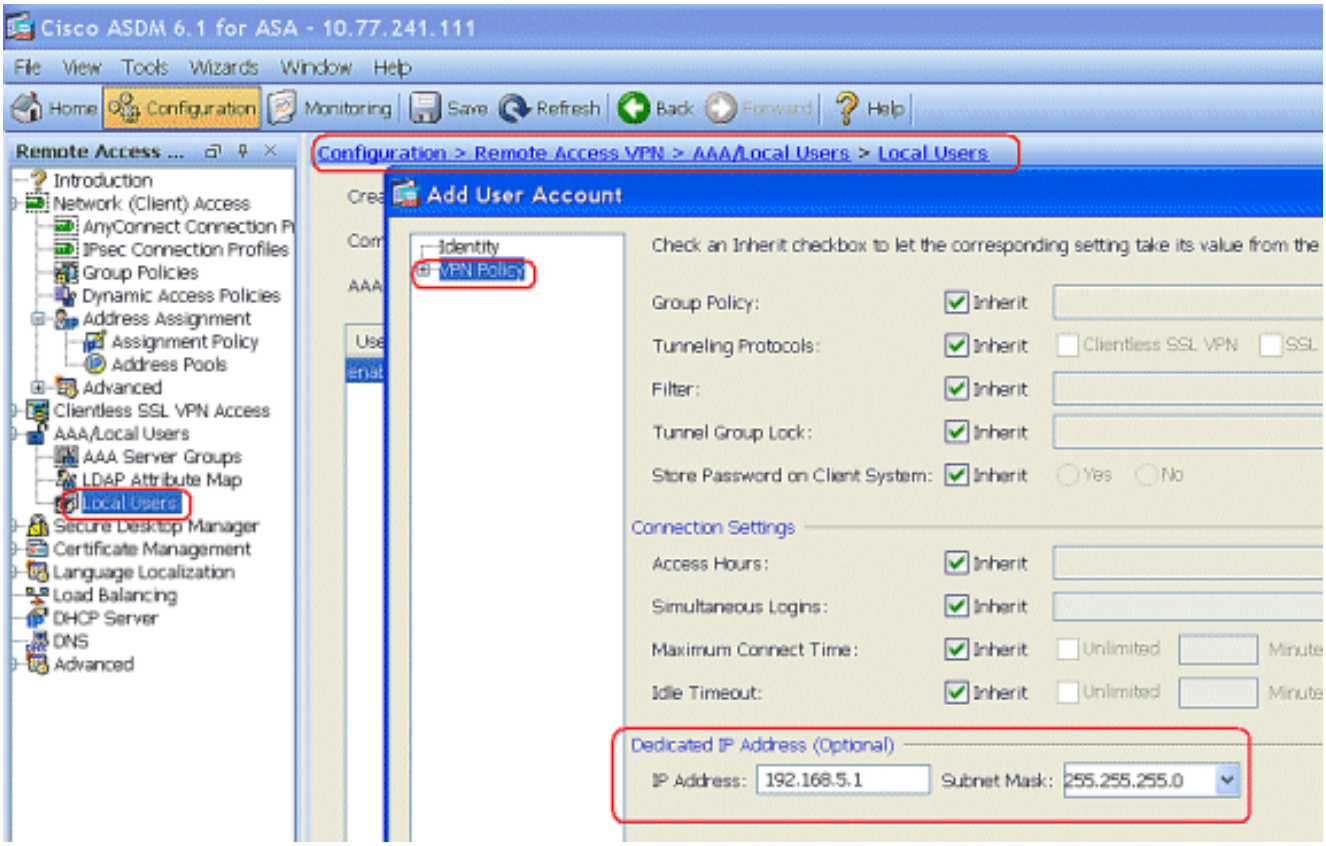


Klicken Sie auf **OK** und **Übernehmen**.

6. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > Local Users > Add**, um das Benutzerkonto (z. B. Benutzername - cisco123 und Kennwort - cisco123) für den VPN-Client-Zugriff zu
erstellen.

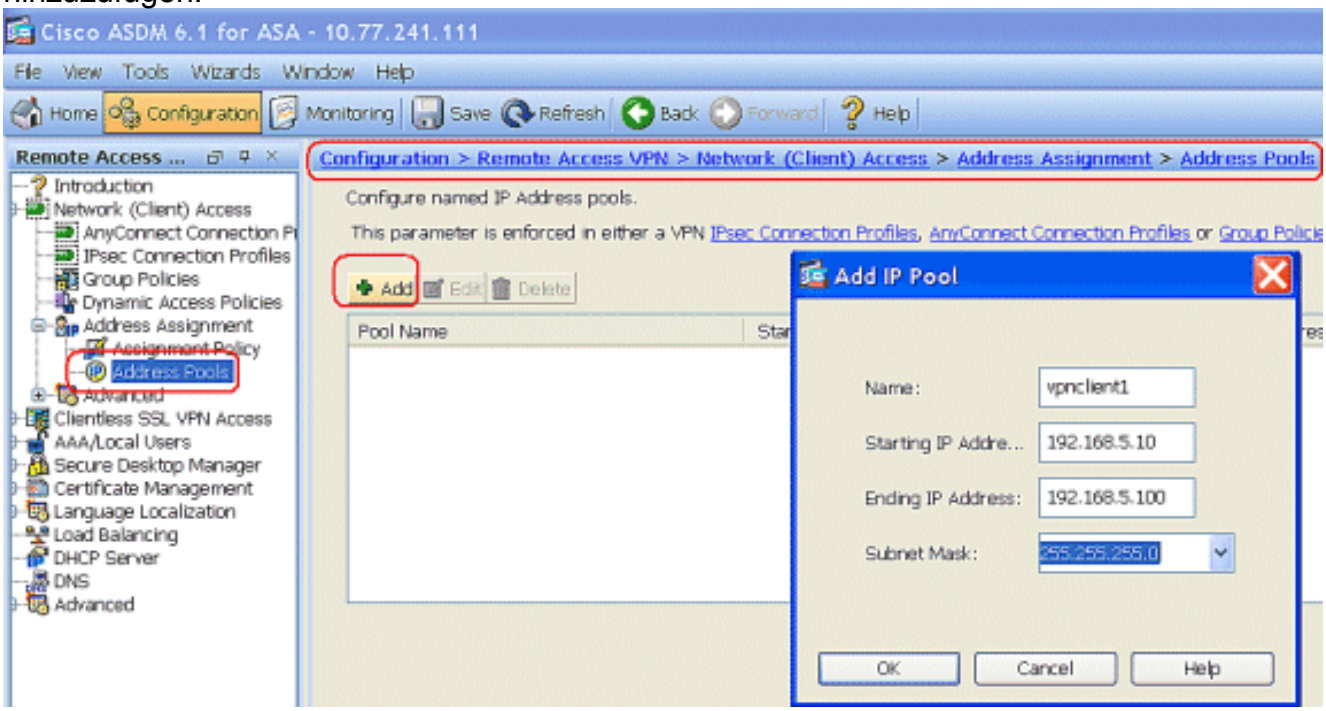


7. Gehen Sie zu **VPN Policy** und fügen Sie die **statische/dedizierte IP-Adresse** für den Benutzer "cisco123" wie folgt
hinzu.

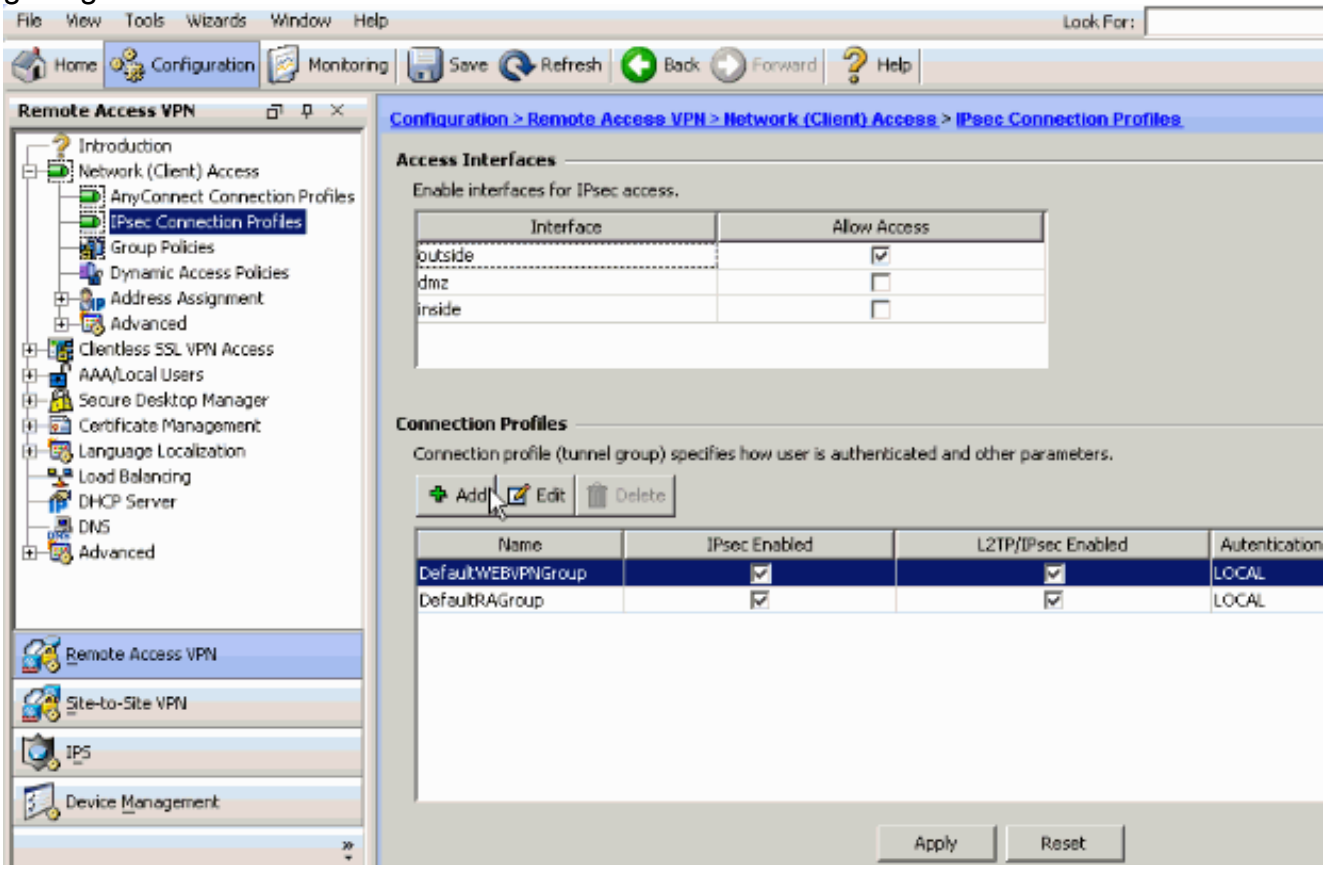


8. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Address**

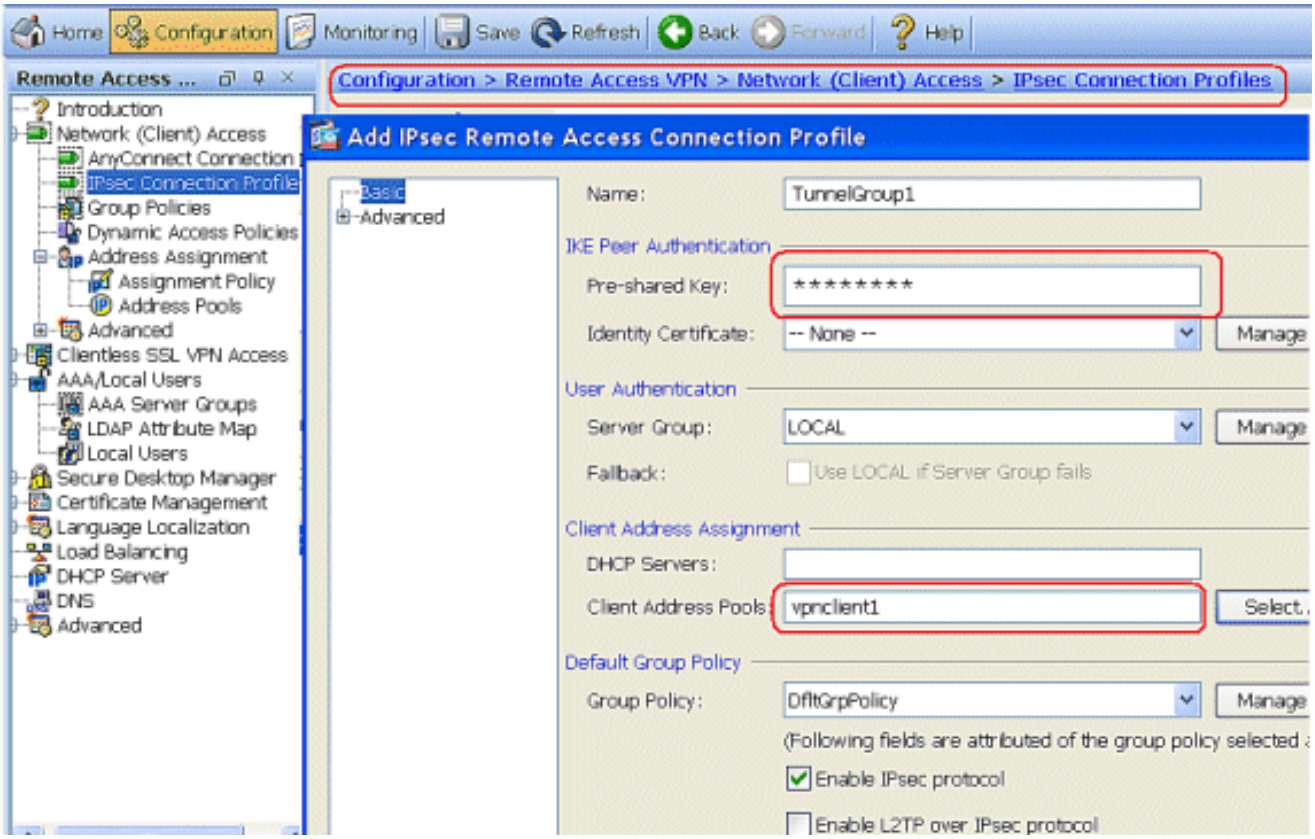
Assignment > Address Pools aus, und klicken Sie auf **Add**, um den VPN-Client für VPN-Client-Benutzer
hinzuzufügen.



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

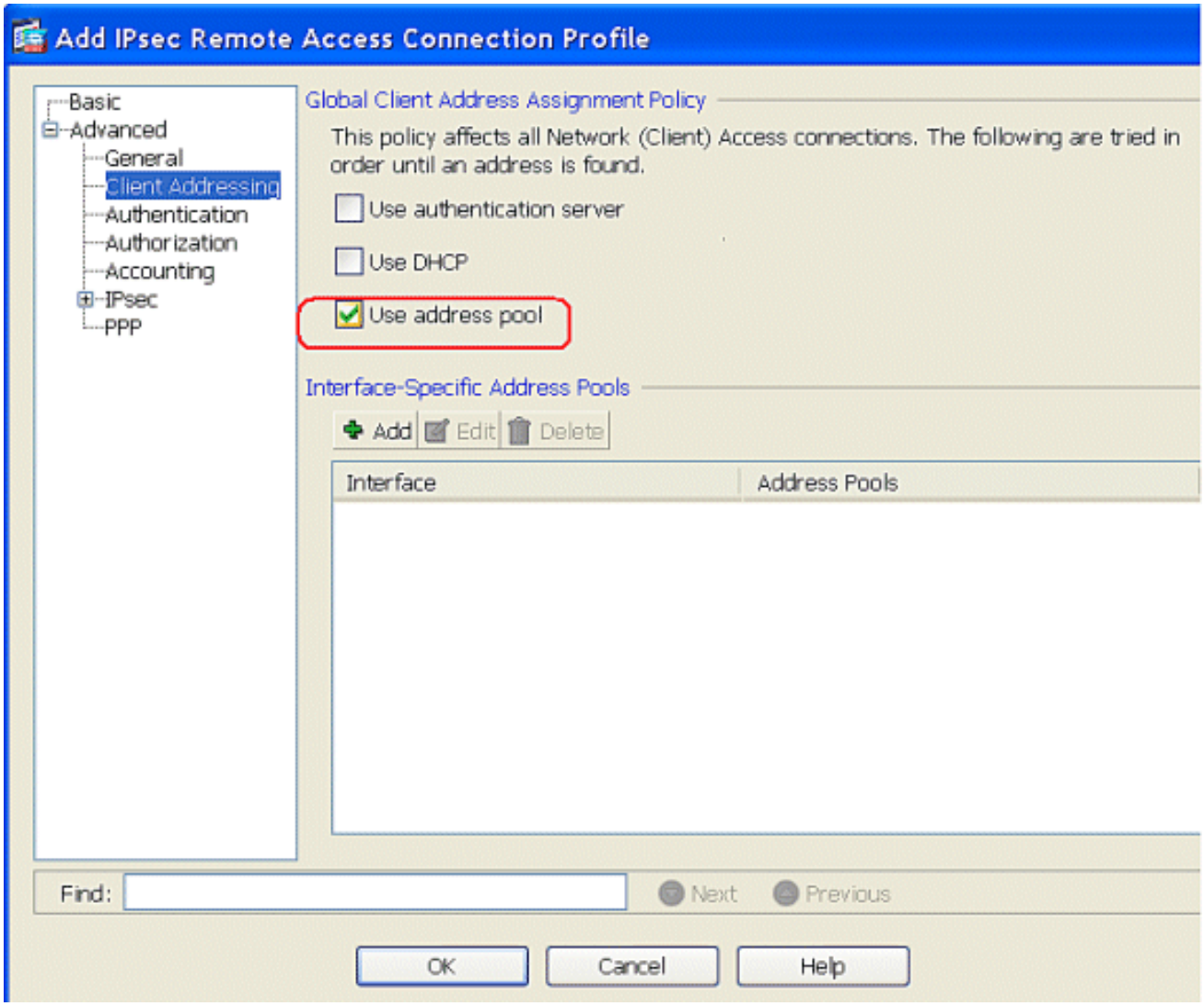


Wählen Sie auf der Registerkarte **Basic (Grundlegend)** die Servergruppe als **LOKAL** für das Feld User Authentication (Benutzerauthentifizierung) aus.Wählen Sie **vpnclient1** als Client-Adresspools für die VPN-Client-Benutzer
aus.



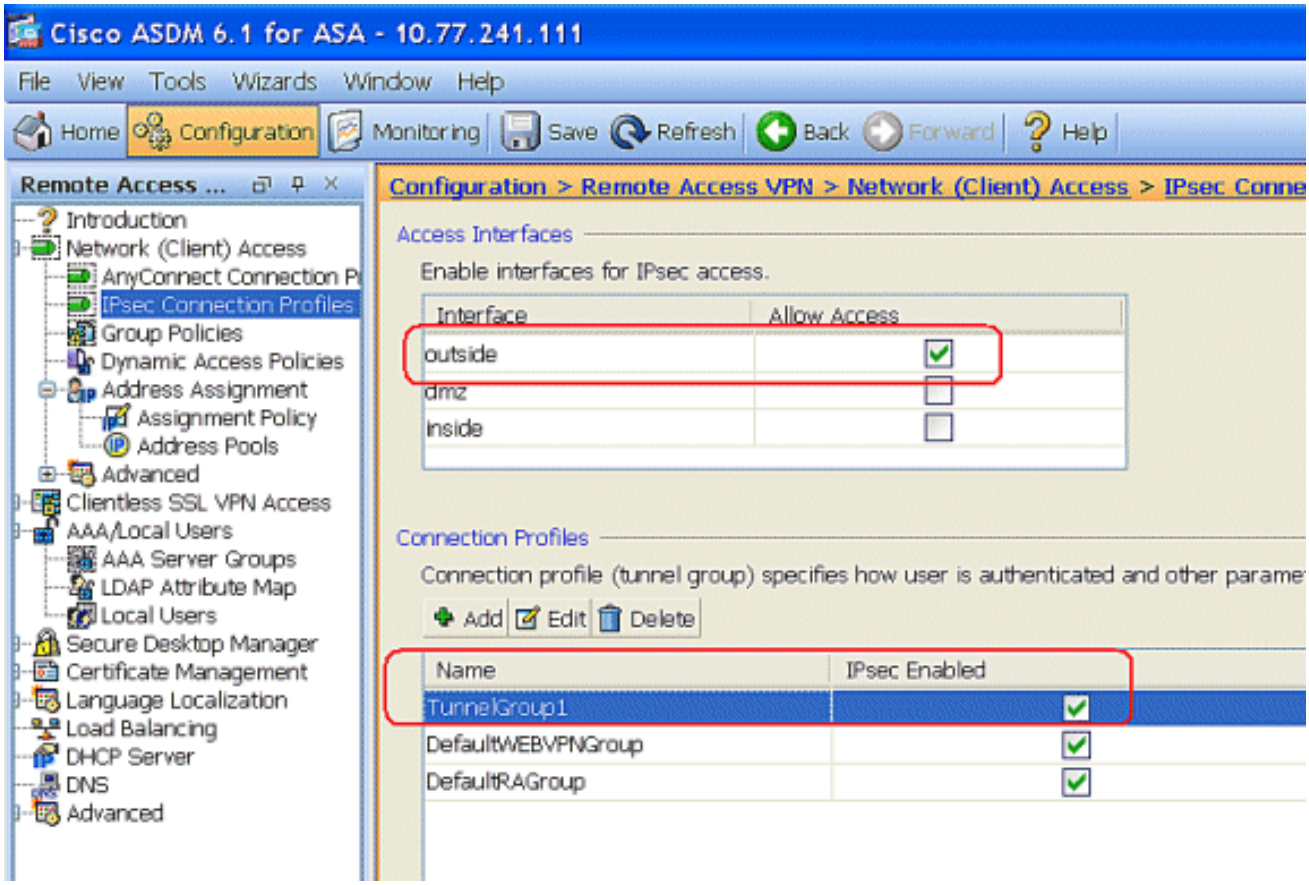
Klicken Sie auf **OK**.

10. Wählen Sie **Advanced > Client Addressing aus**, und aktivieren Sie das Kontrollkästchen Adressen-Pool **verwenden**, um die IP-Adresse den VPN-Clients zuzuweisen.**Hinweis:** Deaktivieren Sie die Kontrollkästchen **Authentifizierungsserver verwenden** und **DHCP verwenden**.



Klicken Sie auf **OK**.

11. 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 outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0

no failover
```

```
icmp unreachable rate-limit 1 burst-size 1

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

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

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

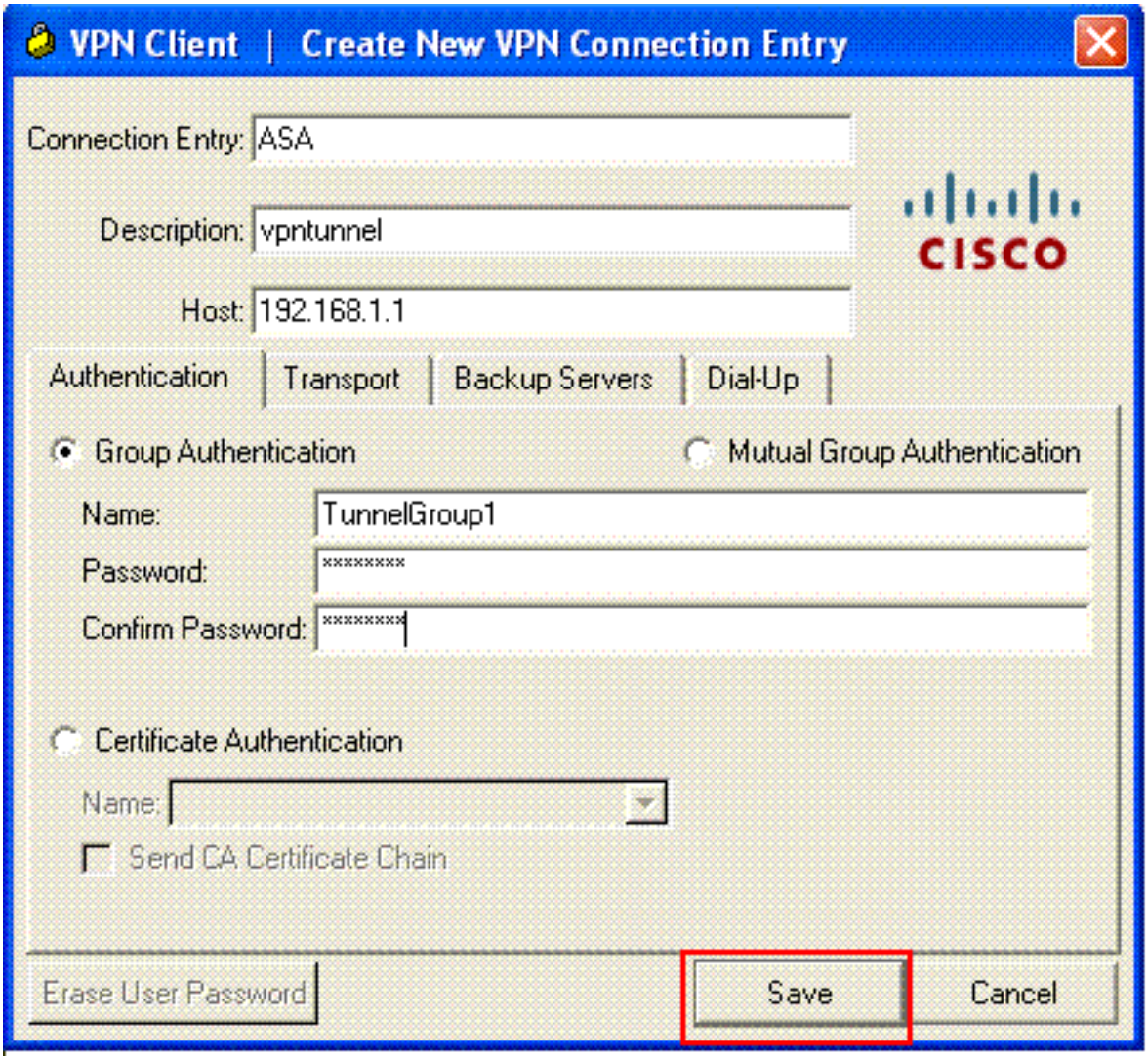
```
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

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

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

Konfiguration des Cisco VPN-Clients

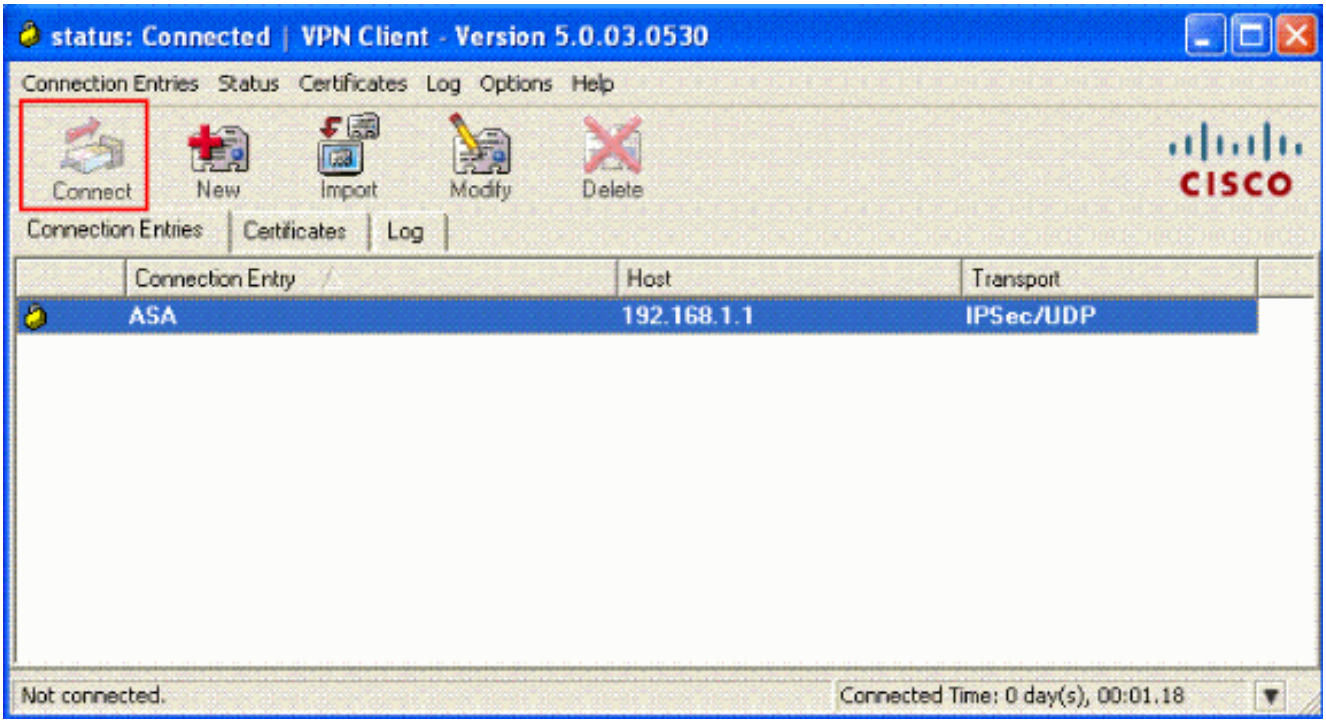
Versuchen Sie, mit dem Cisco VPN-Client eine Verbindung zur Cisco ASA herzustellen, um zu überprüfen, ob die ASA erfolgreich konfiguriert wurde.

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**.

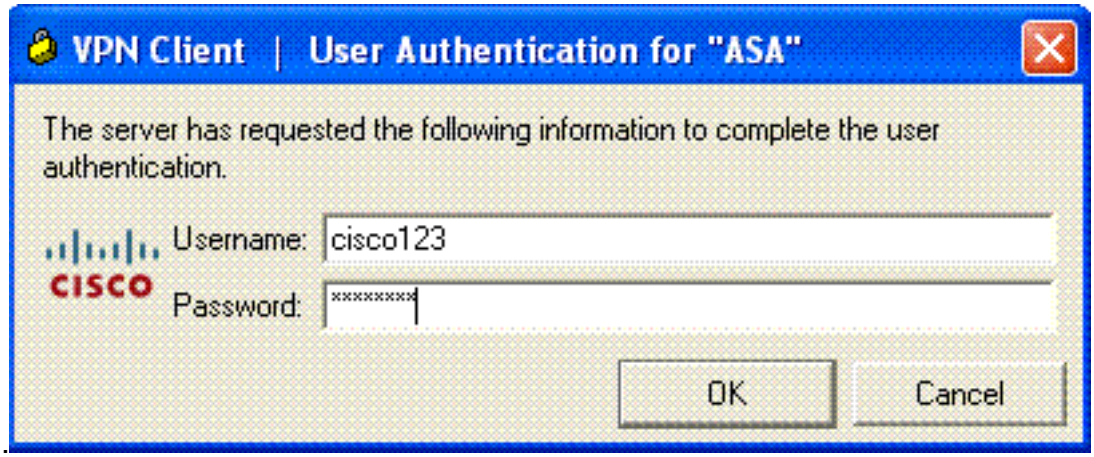


4. Klicken Sie auf die Verbindung, die Sie verwenden möchten, und klicken Sie im Hauptfenster des VPN-Clients auf **Verbinden**.

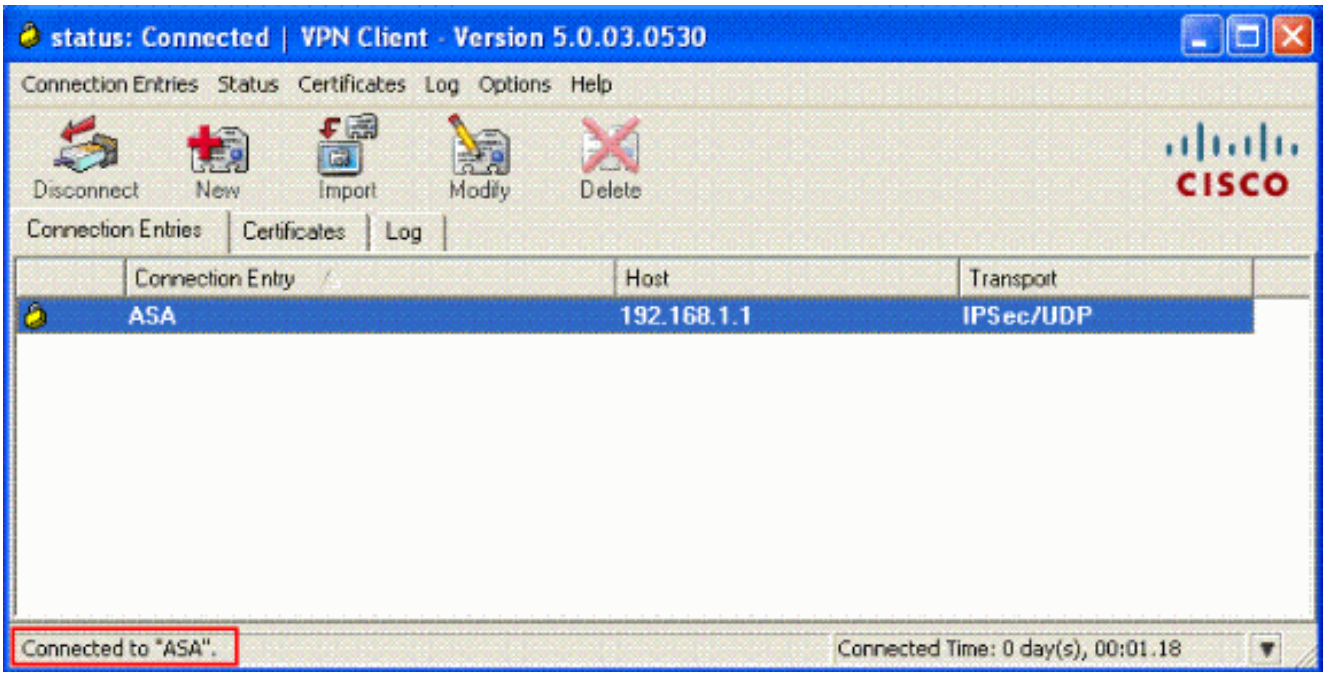


5. Geben Sie bei Aufforderung den **Benutzernamen ein: cisco123** und **Kennwort: cisco123** wie in der ASA für Xauth konfiguriert, und klicken Sie auf **OK**, um eine Verbindung zum Remote-

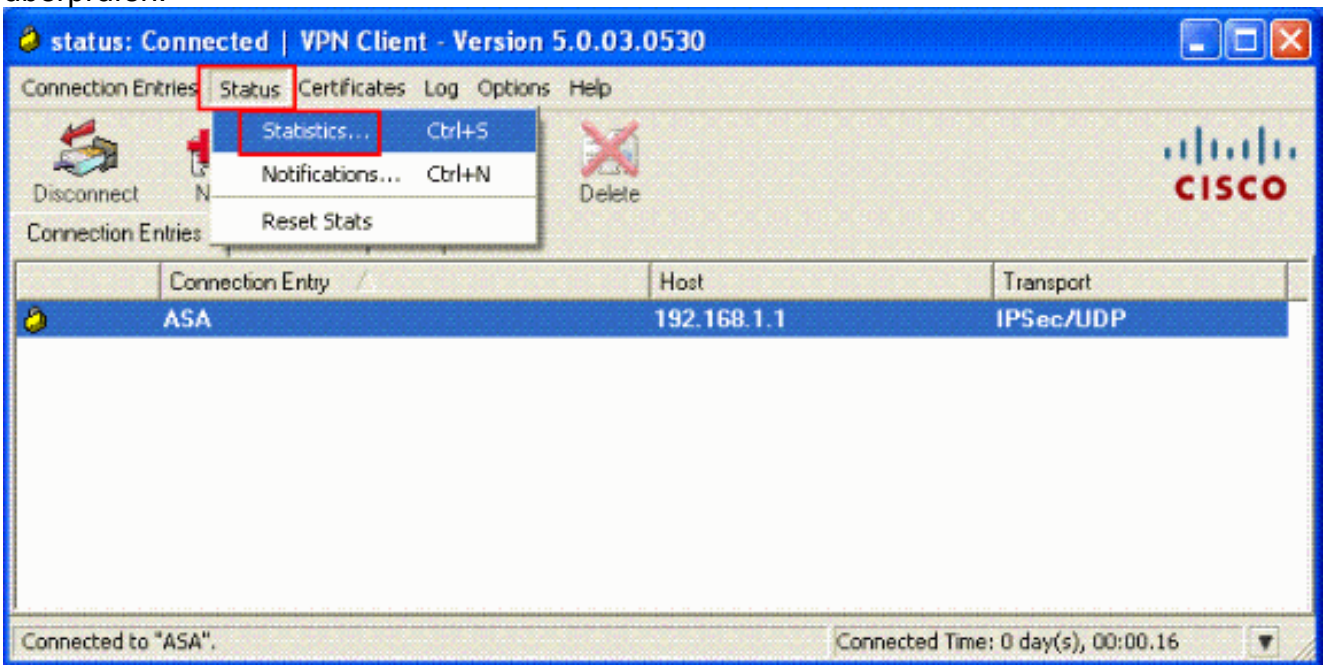
Netzwerk herzustellen.



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.



Überprüfen

Befehle anzeigen

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**.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE Security Associations (SAs) in einem Peer an.
- **show crypto ipsec sa**: Zeigt die von aktuellen SAs verwendeten Einstellungen.

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 in den gängigsten 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
- Befehlsreferenz 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 PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems