

# ASA 8.x: Split Tunneling für AnyConnect VPN-Client im ASA-Konfigurationsbeispiel zulassen

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[ASA-Konfiguration mit ASDM 6.0\(2\)](#)

[ASA CLI-Konfiguration](#)

[Einrichtung der SSL VPN-Verbindung mit SVC](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Dieses Dokument enthält schrittweise Anweisungen, wie Cisco AnyConnect VPN-Client-Zugriff auf das Internet ermöglicht wird, während sie in eine Cisco Adaptive Security Appliance (ASA) 8.0.2 getunnelt werden. Diese Konfiguration ermöglicht dem Client den sicheren Zugriff auf Unternehmensressourcen über SSL und bietet gleichzeitig ungesicherten Zugriff auf das Internet durch Split-Tunneling.

## [Voraussetzungen](#)

### [Anforderungen](#)

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- ASA Security Appliance muss Version 8.x ausführen
- Cisco AnyConnect VPN Client 2.x **Hinweis:** Laden Sie das AnyConnect VPN Client-Paket (anyconnect-win\*.pkg) vom Cisco [Software Download herunter](#) ([nur registrierte Kunden](#)). Kopieren Sie den AnyConnect VPN-Client in den Flash-Speicher der ASA, der auf die Computer der Remote-Benutzer heruntergeladen werden soll, um die SSL VPN-Verbindung mit der ASA herzustellen. Weitere Informationen finden Sie im Abschnitt [Installation des AnyConnect Client](#) im ASA-Konfigurationsleitfaden.

## Verwendete Komponenten

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

- Cisco ASA der Serie 5500 mit Softwareversion 8.0(2)
- Cisco AnyConnect SSL VPN Client-Version für Windows 2.0.0343
- PC mit Microsoft Vista, Windows XP SP2 oder Windows 2000 Professional SP4 und Microsoft Installer Version 3.1
- Cisco Adaptive Security Device Manager (ASDM) Version 6.0(2)

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 in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Hintergrundinformationen

Der Cisco AnyConnect VPN Client stellt sichere SSL-Verbindungen zur Sicherheits-Appliance für Remote-Benutzer bereit. Ohne einen zuvor installierten Client geben Remote-Benutzer die IP-Adresse einer Schnittstelle in ihrem Browser ein, die für die Annahme von SSL VPN-Verbindungen konfiguriert ist. Wenn die Sicherheits-Appliance nicht so konfiguriert ist, dass http:// Anfragen an https:// umgeleitet werden, müssen Benutzer die URL im Formular https://<address> eingeben.

Nach der Eingabe der URL stellt der Browser eine Verbindung zu dieser Schnittstelle her und zeigt den Anmeldebildschirm an. Wenn der Benutzer die Anmeldung und Authentifizierung erfüllt und die Sicherheits-Appliance den Benutzer als den Client erfordert, lädt sie den Client herunter, der dem Betriebssystem des Remote-Computers entspricht. Nach dem Herunterladen installiert und konfiguriert sich der Client selbst, stellt eine sichere SSL-Verbindung her und bleibt bzw. deinstalliert sich beim Beenden der Verbindung (abhängig von der Konfiguration der Sicherheits-Appliance) selbst.

Bei einem bereits installierten Client überprüft die Sicherheits-Appliance bei der Benutzerauthentifizierung die Client-Version und aktualisiert den Client bei Bedarf.

Wenn der Client eine SSL VPN-Verbindung mit der Security Appliance aushandelt, wird die Verbindung über Transport Layer Security (TLS) und optional über Datagram Transport Layer Security (DTLS) hergestellt. DTLS vermeidet Latenz- und Bandbreitenprobleme im Zusammenhang mit einigen SSL-Verbindungen und verbessert die Leistung von Echtzeitanwendungen, die empfindlich auf Paketverzögerungen reagieren.

Der AnyConnect-Client kann von der Sicherheits-Appliance heruntergeladen oder vom Systemadministrator manuell auf dem Remote-PC installiert werden. Weitere Informationen zur manuellen Installation des Clients finden Sie im [Administratorhandbuch](#) für den Cisco AnyConnect VPN Client.

Die Sicherheits-Appliance lädt den Client basierend auf den Gruppenrichtlinien- oder Benutzernamen-Attributen des Benutzers, der die Verbindung herstellt, herunter. Sie können die Sicherheitsappliance so konfigurieren, dass der Client automatisch heruntergeladen wird, oder Sie können sie so konfigurieren, dass der Remote-Benutzer aufgefordert wird, den Client herunterzuladen. Im letzteren Fall, wenn der Benutzer nicht antwortet, können Sie die Sicherheits-Appliance so konfigurieren, dass der Client entweder nach einer Timeout-Periode heruntergeladen wird oder die Anmeldeseite angezeigt wird.

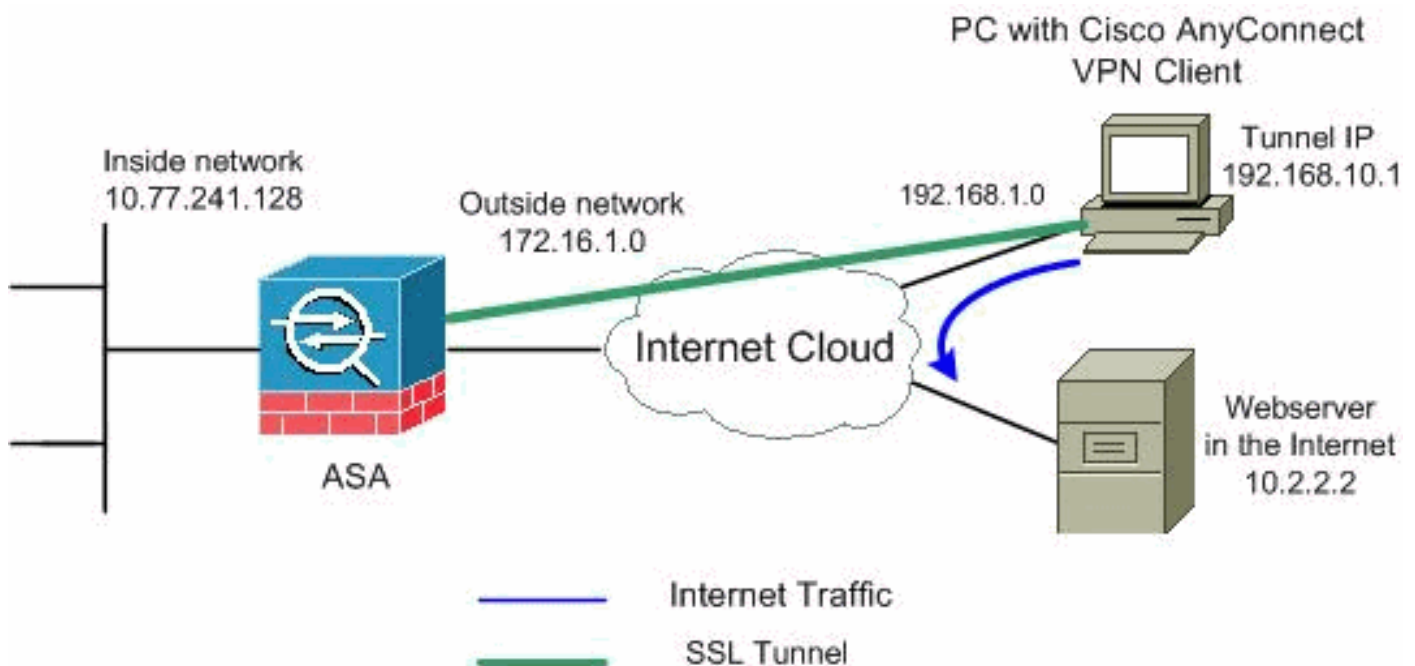
## Konfigurieren

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.

## Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



**Hinweis:** Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind [RFC 1918](#) -Adressen, die in einer Laborumgebung verwendet werden.

## ASA-Konfiguration mit ASDM 6.0(2)

In diesem Dokument wird davon ausgegangen, dass die Basiskonfiguration, z. B. die Schnittstellenkonfiguration, bereits erstellt wurde und ordnungsgemäß funktioniert.

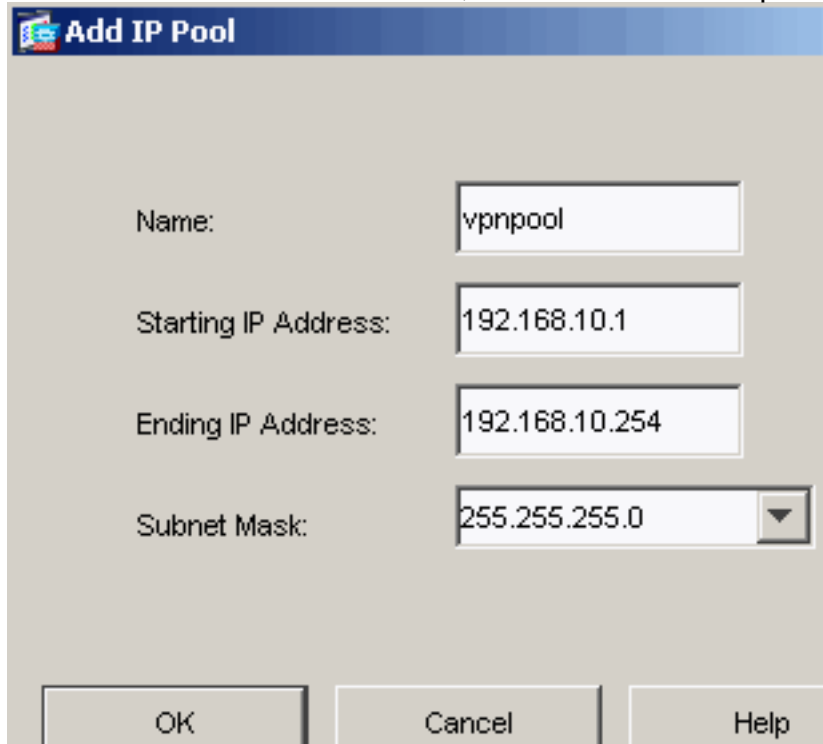
**Hinweis:** Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter [Zulassen von HTTPS-Zugriff für ASDM](#).

**Hinweis:** WebVPN und ASDM können nicht auf derselben ASA-Schnittstelle aktiviert werden, es sei denn, Sie ändern die Portnummern. Weitere Informationen finden Sie unter [ASDM und](#)

[WebVPN Enabled auf derselben ASA-Schnittstelle.](#)

Gehen Sie wie folgt vor, um das SSL VPN auf ASA mit Split-Tunneling zu konfigurieren:

1. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add** aus, um einen IP-Adresspool **vpnpool** zu



The screenshot shows a dialog box titled "Add IP Pool" with the following fields:

- Name: vpnpool
- Starting IP Address: 192.168.10.1
- Ending IP Address: 192.168.10.254
- Subnet Mask: 255.255.255.0

Buttons: OK, Cancel, Help

erstellen.

2. Klicken Sie auf **Übernehmen**. Entsprechende CLI-Konfiguration:
3. Aktivieren Sie WebVPN. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** aus, und klicken Sie unter **Access Interfaces** auf die Kontrollkästchen **Allow Access** and **Enable DTLS for the external interface**. Aktivieren Sie außerdem das Kontrollkästchen **Enable Cisco AnyConnect VPN Client or Legacy SSL VPN Client access (Cisco AnyConnect VPN-Client oder Legacy-SSL VPN-Client-Zugriff aktivieren)** in der in der Tabelle unten ausgewählten Schnittstelle, um SSL VPN auf der externen Schnittstelle zu aktivieren.

**Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles**

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

**Access Interfaces**

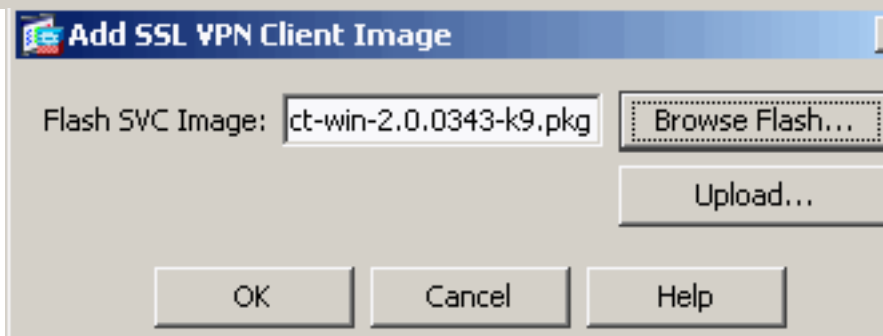
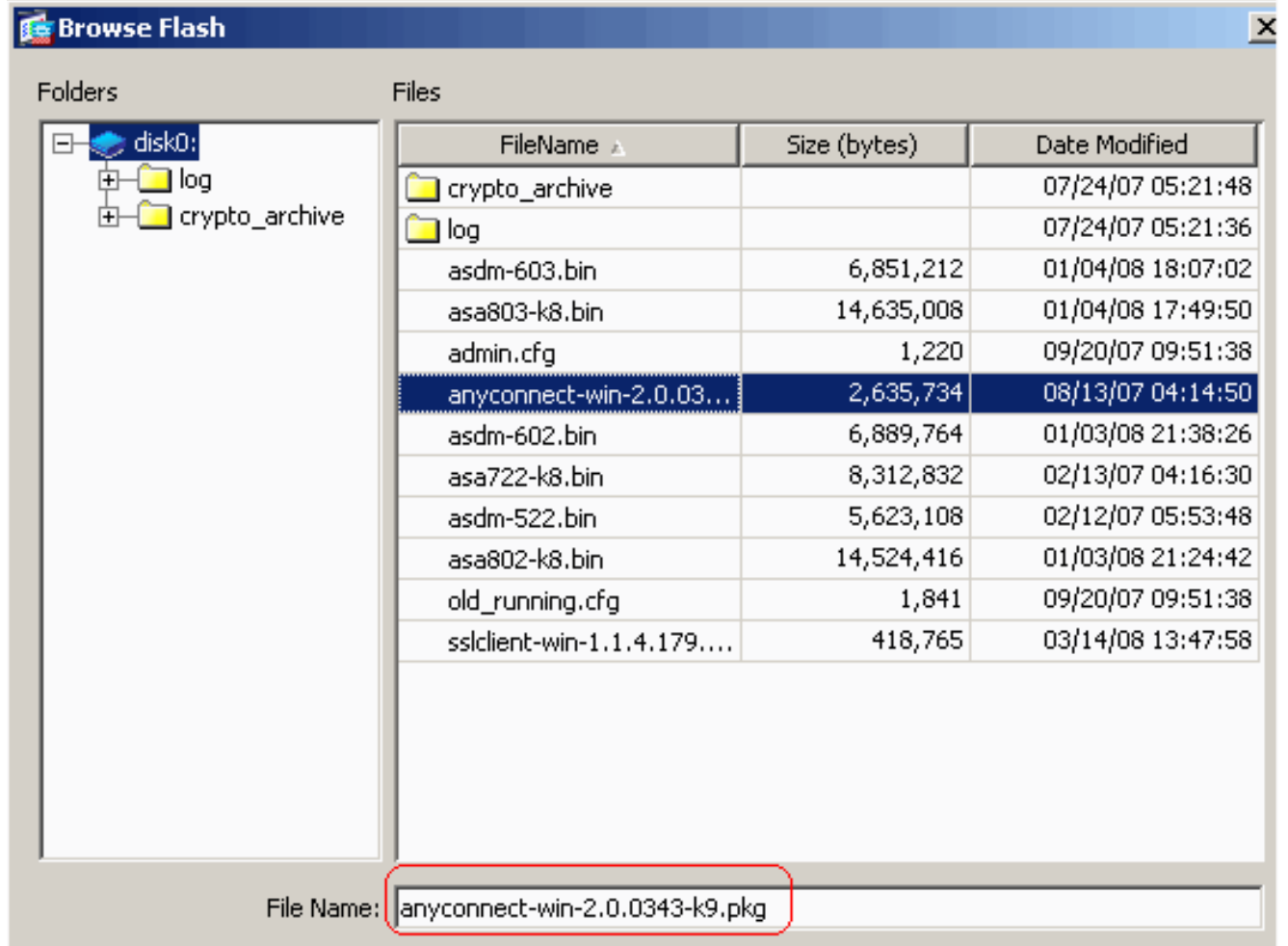
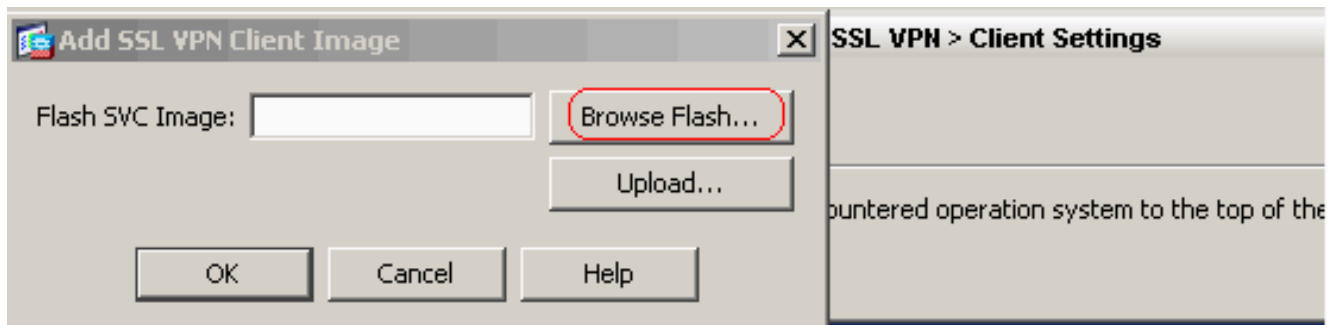
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:  DTLS Port:

Click here to [Assign Certificate to Interface](#).

Klicken Sie auf **Übernehmen**. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add**, um das Cisco AnyConnect VPN-Client-Image aus dem Flash-Speicher der ASA hinzuzufügen, wie gezeigt.



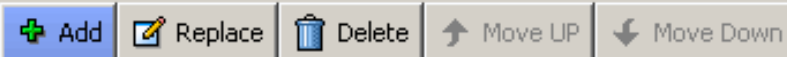
Klicken Sie auf **OK**.  
auf  
Hinzufügen.

Klicken Sie

Identify SSL VPN Client (SVC) related files.

### SSL VPN Client Images

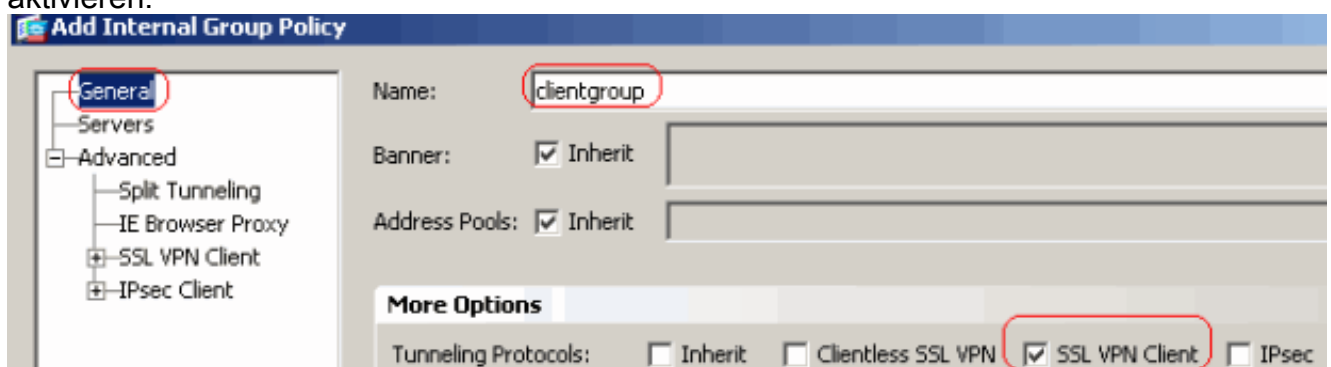
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t



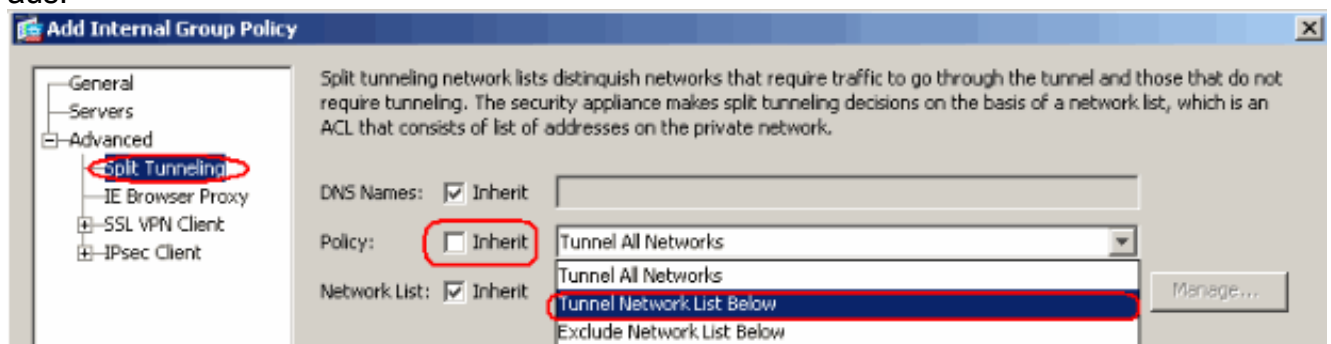
disk0:/anyconnect-win-2.0.0343-k9.pkg

### Entsprechende CLI-Konfiguration:

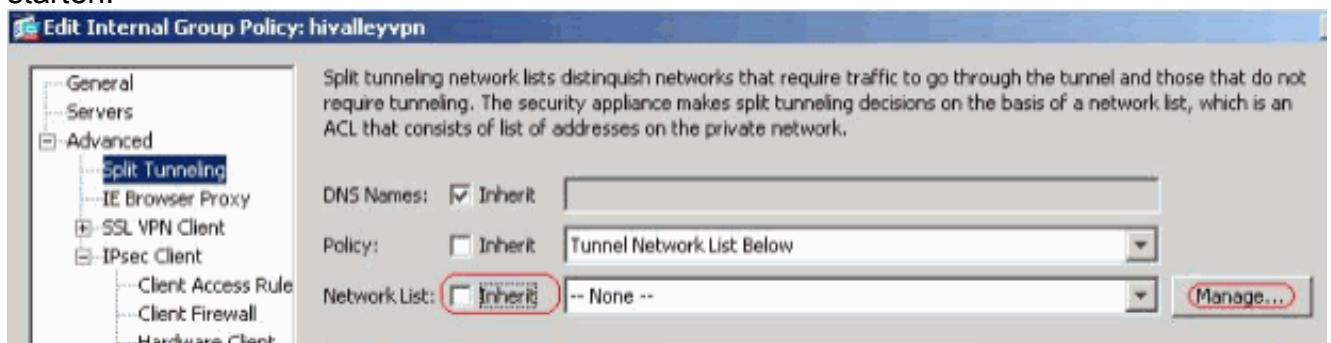
4. Konfigurieren Sie die Gruppenrichtlinie. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policies (Konfigurationsrichtlinien)**, um eine interne Gruppenrichtlinien-Clientgruppe zu erstellen. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **SSL VPN Client**, um das WebVPN als Tunneling-Protokoll zu aktivieren.



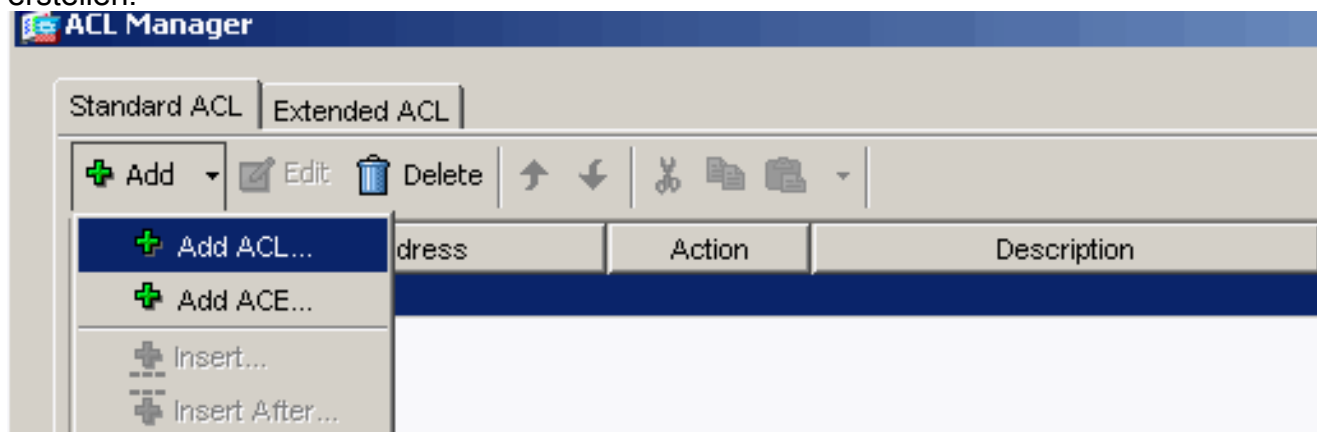
- Deaktivieren Sie auf der Registerkarte **Erweitert > Getrenntes Tunneling** das Kontrollkästchen **Erben** für Split Tunnel Policy (Tunnel-Richtlinie teilen), und wählen Sie **unten** in der Dropdown-Liste die Option **Tunnel Network List (Tunnel-Netzwerkliste)** aus.



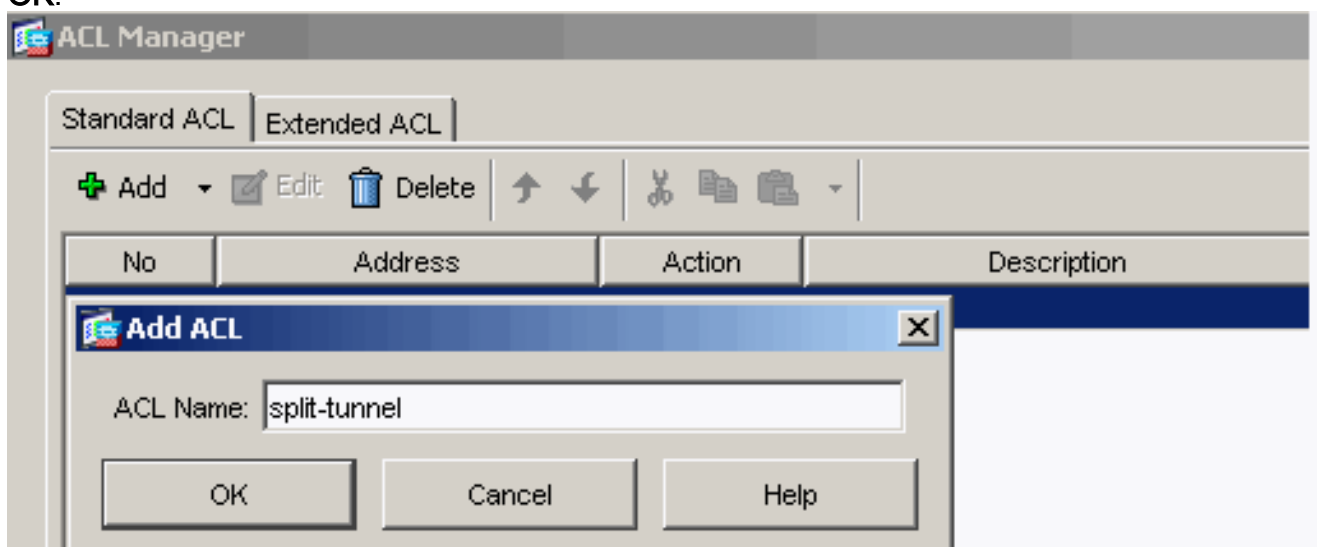
- Deaktivieren Sie das Kontrollkästchen **Erben** für die **Split Tunnel Network List (Kanalliste für Tunnel-Netzwerk teilen)**, und klicken Sie dann auf **Manage (Verwalten)**, um den ACL Manager zu starten.



Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu erstellen.

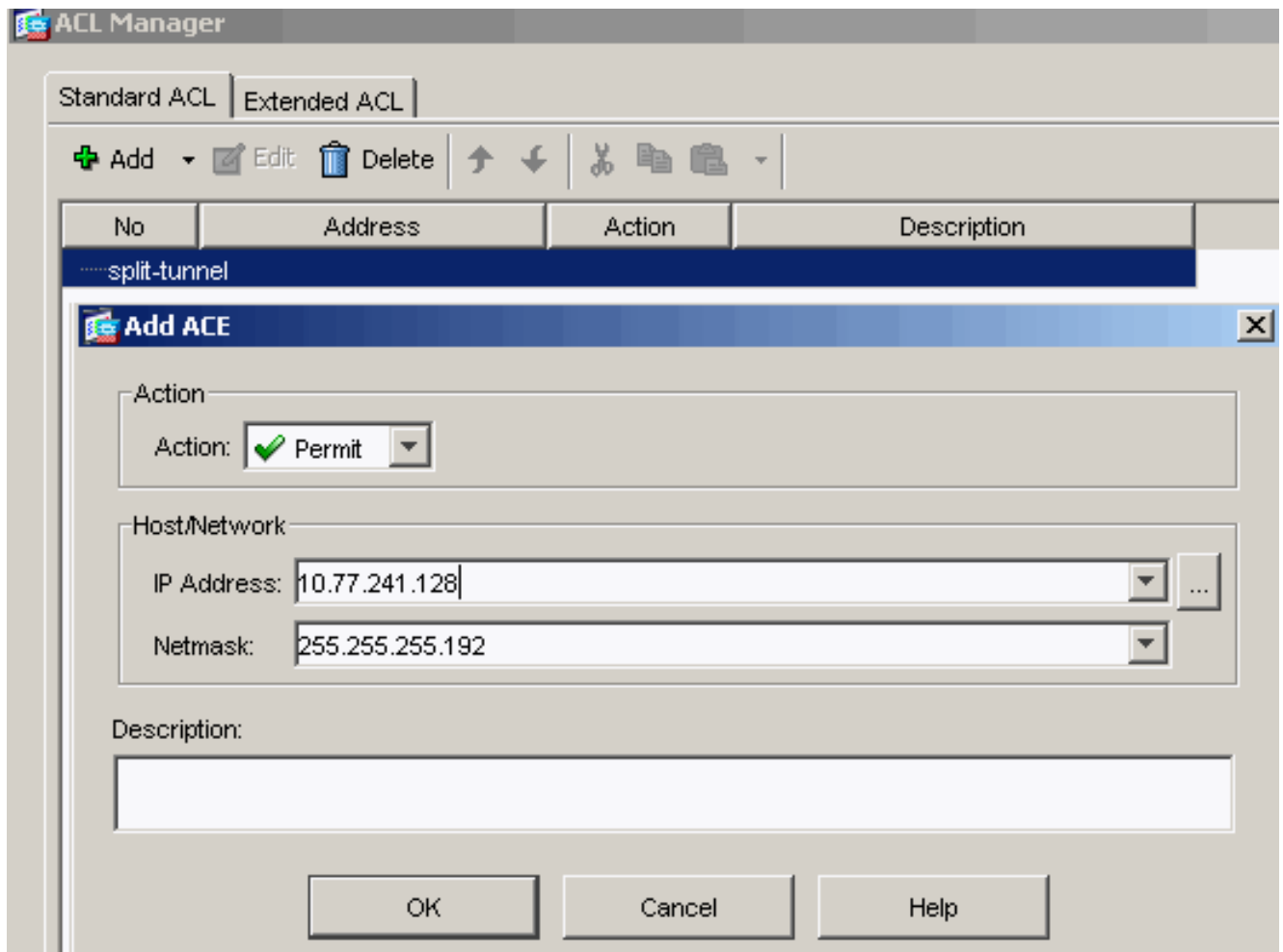


Geben Sie einen Namen für die ACL an, und klicken Sie auf **OK**.

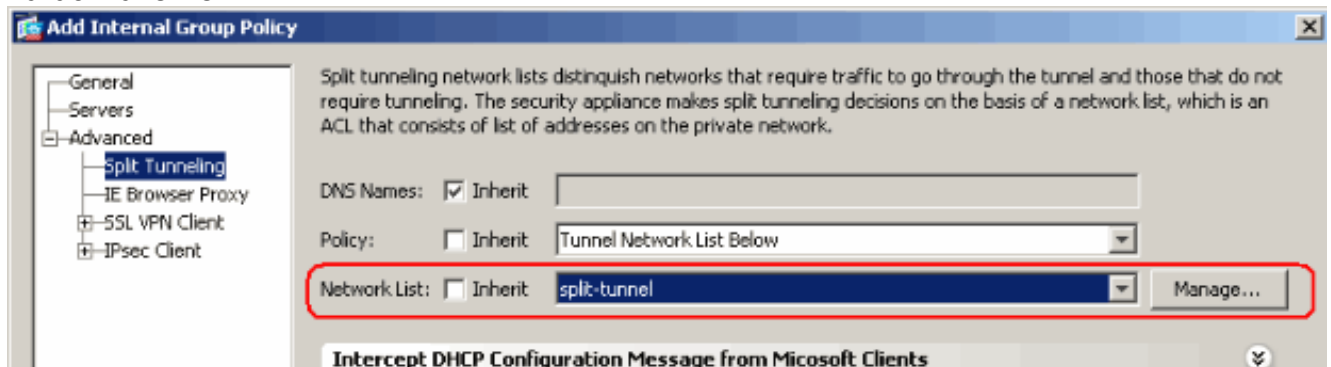


Sobald der ACL-Name erstellt wurde, wählen Sie **Add > Add ACE (Hinzufügen > ACE hinzufügen)**, um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen. Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.77.241.128/26 und wählen **Zulassen** als Aktion aus. Klicken Sie auf **OK**, um den ACL Manager zu verlassen.

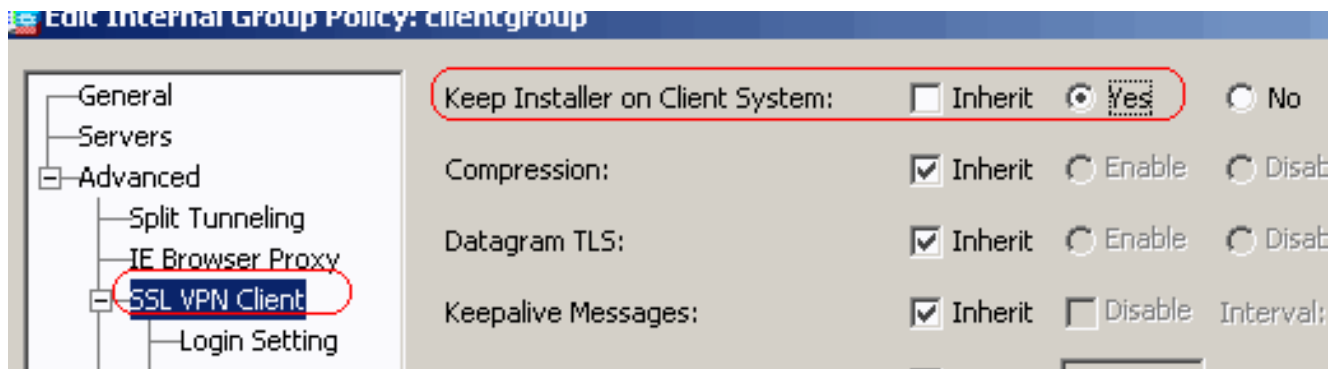




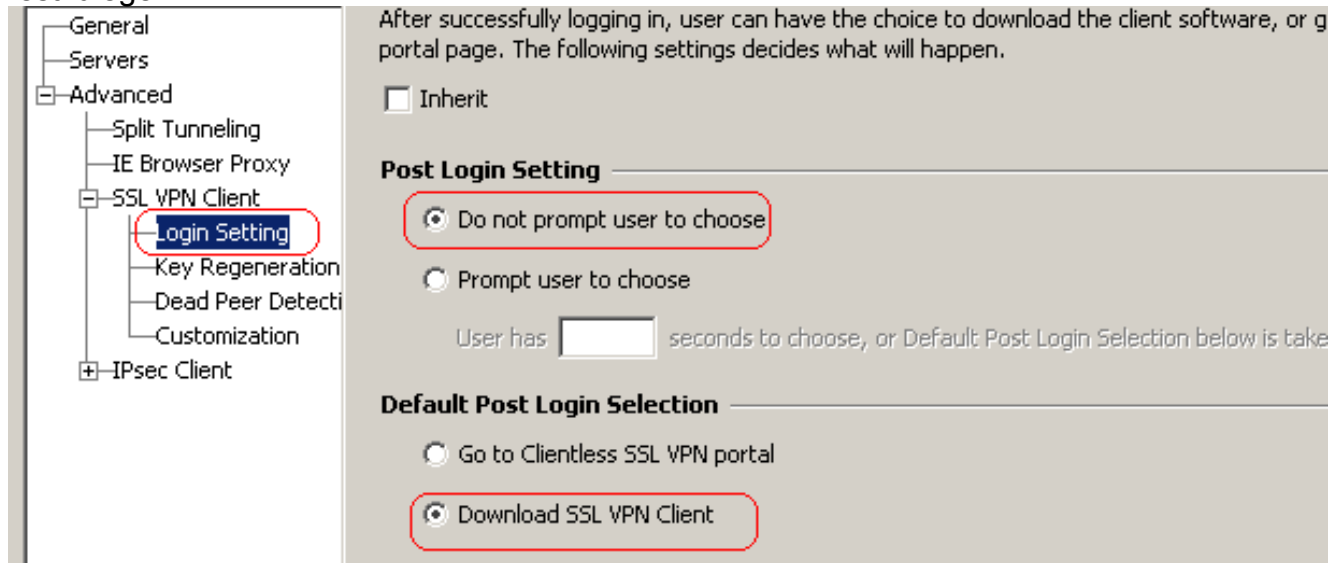
Stellen Sie sicher, dass die gerade erstellte ACL für die Split-Tunnel-Netzwerkliste ausgewählt ist. Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration zurückzukehren.



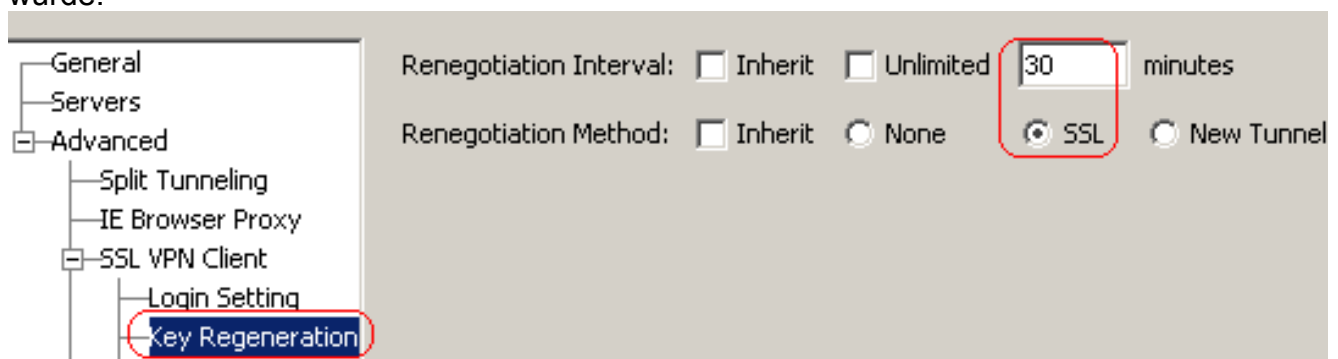
Klicken Sie auf der Hauptseite auf **Übernehmen** und dann auf Senden (falls erforderlich), um die Befehle an die ASA zu senden. Konfigurieren Sie die **SSL VPN**-Einstellungen im Gruppenrichtlinienmodus. Deaktivieren Sie für die Option Installer auf Client-System beibehalten das Kontrollkästchen **Erben**, und klicken Sie auf das Optionsfeld **Ja**. Dadurch kann die SVC-Software auf dem Client-Rechner verbleiben. Daher muss die ASA die SVC-Software nicht jedes Mal auf den Client herunterladen, wenn eine Verbindung hergestellt wird. Diese Option ist eine gute Wahl für Remote-Benutzer, die häufig auf das Unternehmensnetzwerk zugreifen.



Klicken Sie auf **Login Setting**, um die **Post Login-Einstellung** und die **Post Login-Standardauswahl** wie dargestellt festzulegen.






Deaktivieren Sie bei der Option zum Intervall der Neuverhandlung das Kontrollkästchen **Erben**, deaktivieren Sie das Kontrollkästchen **Unlimited (Unbegrenzt)**, und geben Sie die Anzahl der Minuten bis zum erneuten Auftreten ein. Die Sicherheit wird verbessert, indem die Gültigkeitsdauer eines Schlüssels beschränkt wird. Deaktivieren Sie für die Option Methode der Neuverhandlung das Kontrollkästchen **Erben**, und klicken Sie auf das **SSL-Optionsfeld**. Bei der Neuverhandlung kann der aktuelle SSL-Tunnel oder ein neuer Tunnel verwendet werden, der speziell für die Neuverhandlung erstellt wurde.



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

## Configuration > Remote Access VPN > Network (Client) Access > Group Policies

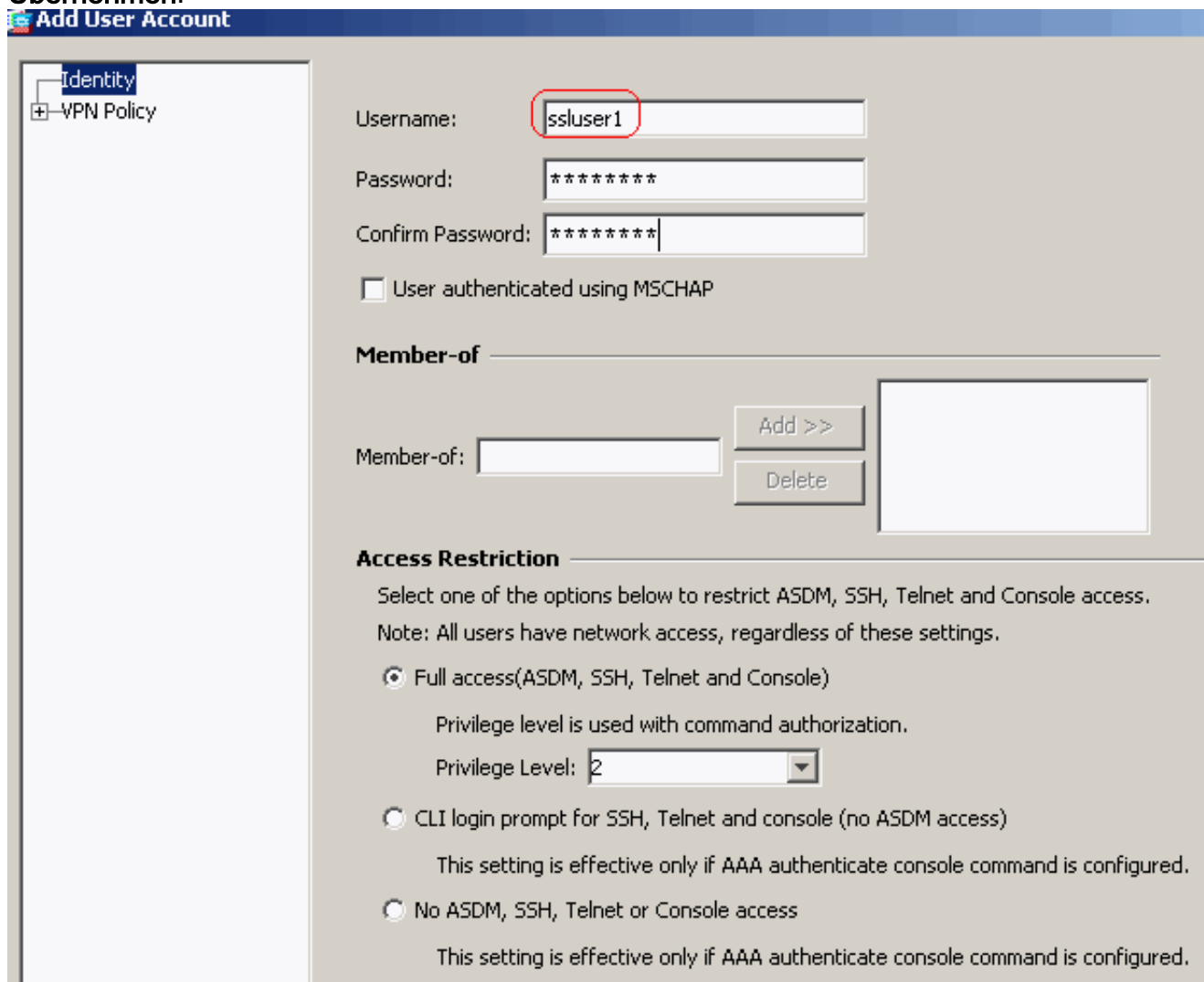
Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

 Add  Edit  Delete

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A -
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A -

### Entsprechende CLI-Konfiguration:

5. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** aus, um ein neues Benutzerkonto **ssluser1** zu erstellen. Klicken Sie auf **OK** und dann auf **Übernehmen**.



**Add User Account**

Identity  
+ VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

**Member-of**

Member-of:

**Access Restriction**

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.  
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)  
Privilege level is used with command authorization.  
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)  
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access  
This setting is effective only if AAA authenticate console command is configured.

### Entsprechende CLI-Konfiguration:

6. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit** aus, um die Standardservergruppe LOCAL zu ändern, indem Sie das Kontrollkästchen **Enable Local User Lockout (Lokale Benutzersperre aktivieren)** mit dem Wert für maximale Zugriffsversuche auf 16 aktivieren.

Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

### AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

#### Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts:

OK

Cancel

Help

7. Klicken Sie auf **OK** und dann auf **Übernehmen**. Entsprechende CLI-Konfiguration:

8. Konfigurieren Sie die Tunnelgruppe. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles Profile > Add**, um eine neue Tunnelgruppen-**SSL-Gruppe** zu erstellen. Auf der Registerkarte **Basic** (Grundlegende) können Sie die folgende Konfigurationsliste ausführen: Geben Sie der Tunnelgruppe den Namen **sslgroup**. Wählen Sie unter Client Address Assignment (Client-Adressenzuweisung) den Adresspool **vpnpool** aus der Dropdown-Liste aus. Wählen Sie unter Default Group Policy (Standardgruppenrichtlinie) die Gruppenrichtlinien-**Clientgruppe** aus der Dropdown-Liste aus.

#### Add SSL VPN Connection Profile

Basic  
Advanced

Name:

sslgroup

Aliases:

#### Authentication

Method:

AAA  Certificate  Both

AAA Server Group:

LOCAL

Use LOCAL if Server Group fails

#### Client Address Assignment

DHCP Servers:

Client Address Pools:

vpnpool

#### Default Group Policy

Group Policy:

clientgroup

SSL VPN Client Protocol:

Enabled

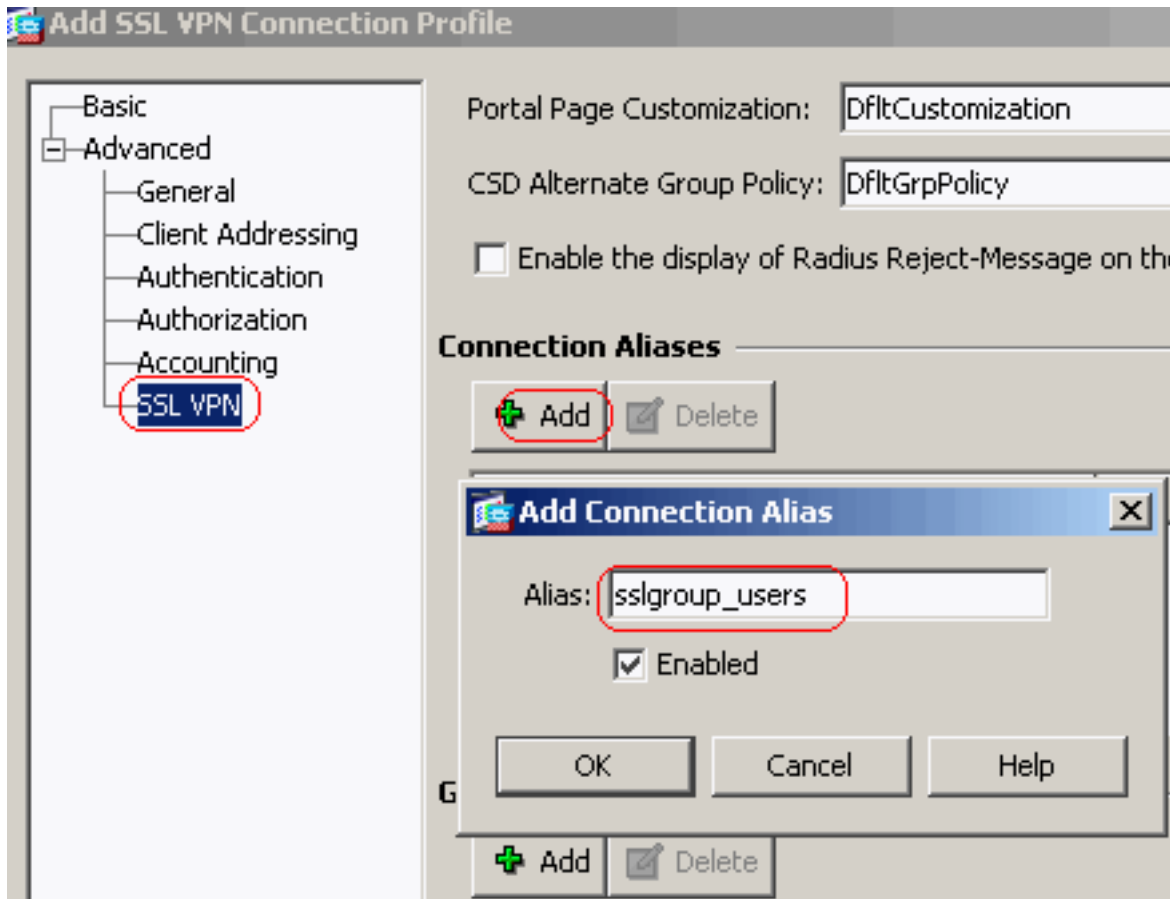
OK

Cancel

Help

Geben Sie auf der Registerkarte **SSL VPN > Connection Aliases** (SSL VPN >

VerbindungsAliase) den Namen des Gruppen-Alias als **sslgroup\_users** an, und klicken Sie auf

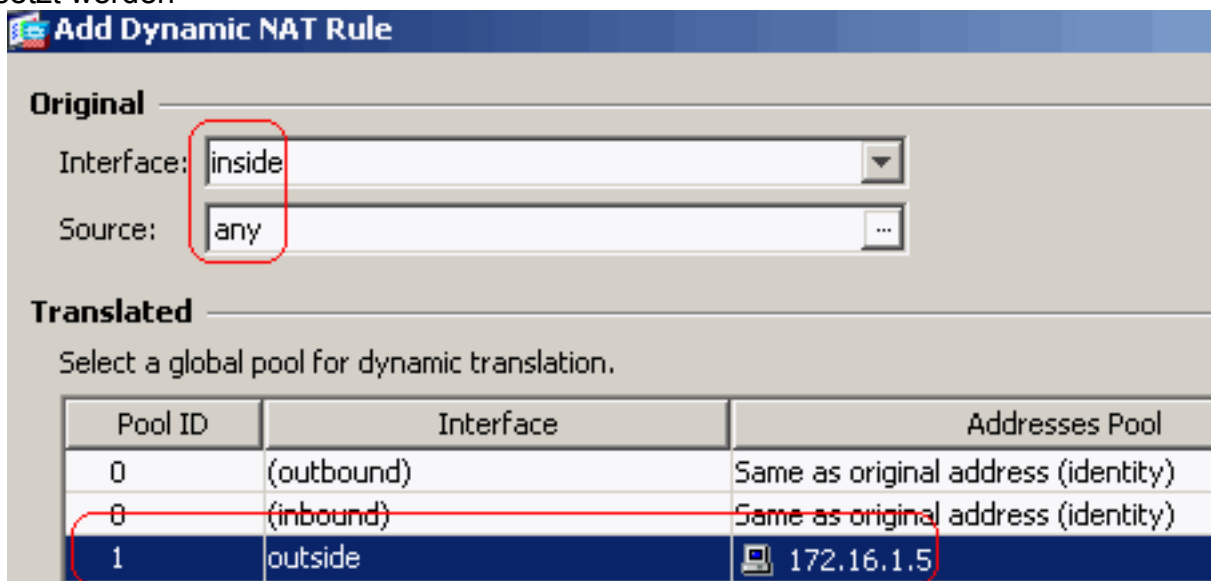


OK.

Klicke

n Sie auf **OK** und dann auf **Übernehmen**. Entsprechende CLI-Konfiguration:

- Konfigurieren Sie NAT. Wählen Sie **Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule** (Konfiguration > Firewall > NAT-Regeln > Dynamische NAT-Regel hinzufügen, damit der Datenverkehr aus dem internen Netzwerk mit der externen IP-Adresse 172.16.1.5 übersetzt werden



kann.

Kli

cken Sie auf **OK**. Klicken Sie auf **OK**.

Configuration > Firewall > NAT Rules						
#	Type	Original			Interface	
		Source	Destination	Service		
[-] inside (1 Dynamic rules)						
1	Dynamic	any			outside	

Klicken Sie auf **Übernehmen**. Entsprechende CLI-Konfiguration:

10. Konfigurieren Sie die NAT-Ausnahme für den Rückverkehr vom internen Netzwerk zum VPN-Client.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

## [ASA CLI-Konfiguration](#)

### Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
```

```

boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
  domain-name default.domain.invalid
access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !---
- ACL to define the traffic to be exempted from NAT.
pager lines 24 logging enable logging asdm informational
mtu inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN
Clients no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.bin no asdm history
enable arp timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
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
webvpn
  enable outside

  !--- Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1

  !--- Assign an order to the AnyConnect SSL VPN Client
image svc enable

  !--- Enable the security appliance to download SVC
images to remote computers tunnel-group-list enable

  !--- Enable the display of the tunnel-group list on the
WebVPN Login page group-policy clientgroup internal

  !--- Create an internal group policy "clientgroup"
group-policy clientgroup attributes
  vpn-tunnel-protocol svc

  !--- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified
  split-tunnel-network-list value split-tunnel

  !--- Encrypt the traffic specified in the split tunnel
ACL only webvpn
  svc keep-installer installed

  !--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of the
connection. svc rekey time 30

  !--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week). svc rekey method ssl

  !--- Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

  !--- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access

  !--- Create a tunnel group "sslgroup" with type as
remote access tunnel-group sslgroup general-attributes
  address-pool vpnpool

  !--- Associate the address pool vpnpool created default-
group-policy clientgroup

  !--- Associate the group policy "clientgroup" created
```



```

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#

```

## Einrichtung der SSL VPN-Verbindung mit SVC

Gehen Sie wie folgt vor, um eine SSL VPN-Verbindung mit ASA herzustellen:

1. Geben Sie die URL oder die IP-Adresse der WebVPN-Schnittstelle der ASA in Ihrem Webbrowser im gezeigten Format ein.

https://url

ODER

https://<IP address of the ASA WebVPN interface>



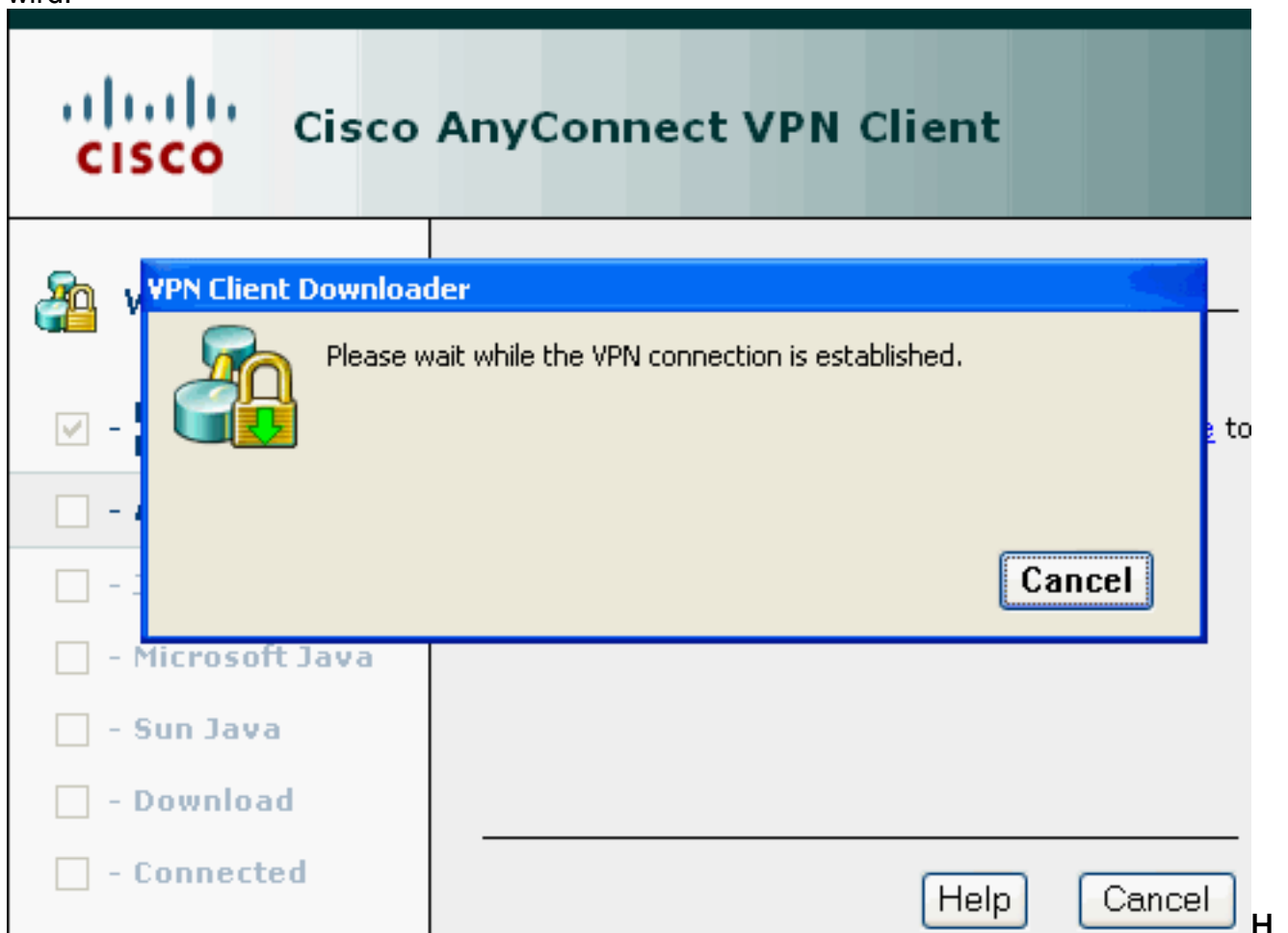
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wählen Sie auch Ihre jeweilige Gruppe aus der Dropdown-Liste aus, wie

dargestellt.

Dieses

Fenster wird angezeigt, bevor die SSL VPN-Verbindung hergestellt

wird.



**inweis:** Die ActiveX-Software muss auf Ihrem Computer installiert sein, bevor Sie den SVC herunterladen können. Sie erhalten dieses Fenster, sobald die Verbindung hergestellt ist.



## Cisco AnyConnect VPN Client



### WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Microsoft Java
- Sun Java
- Download
- Connected

### Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:



Help

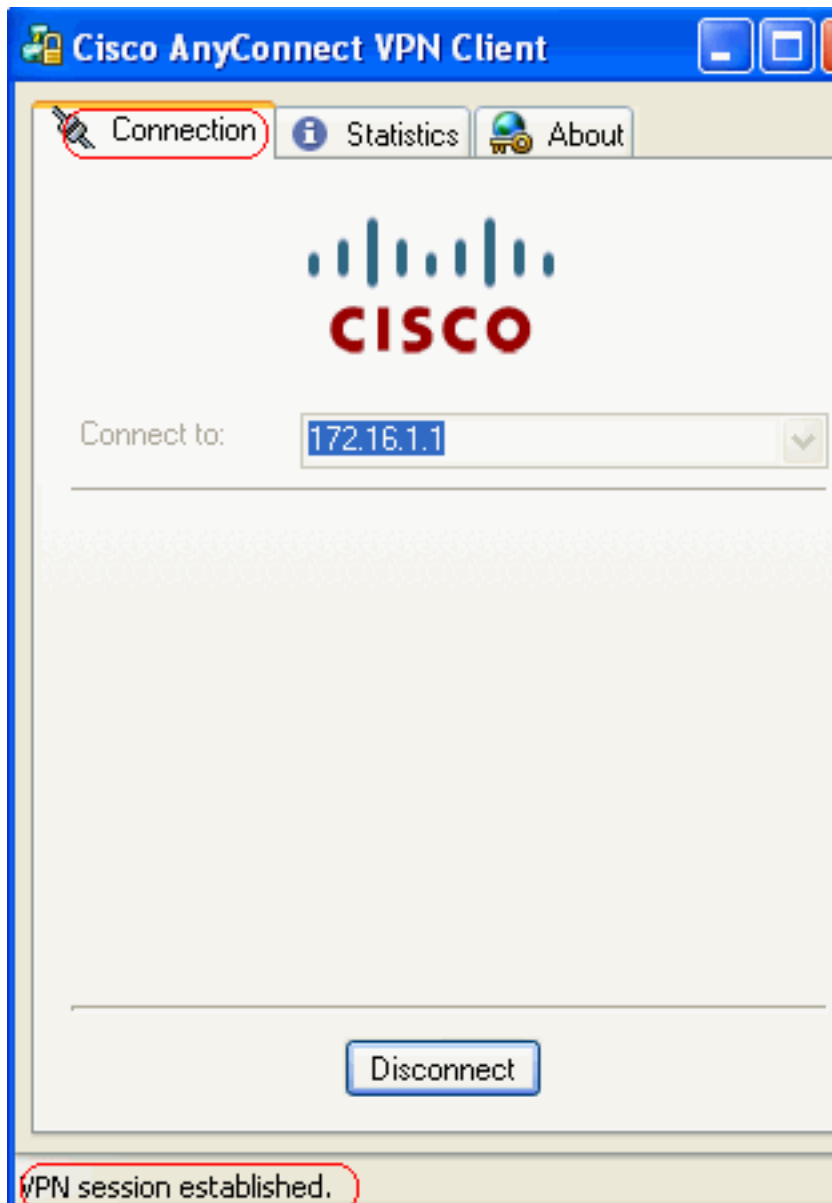
Cancel

system...

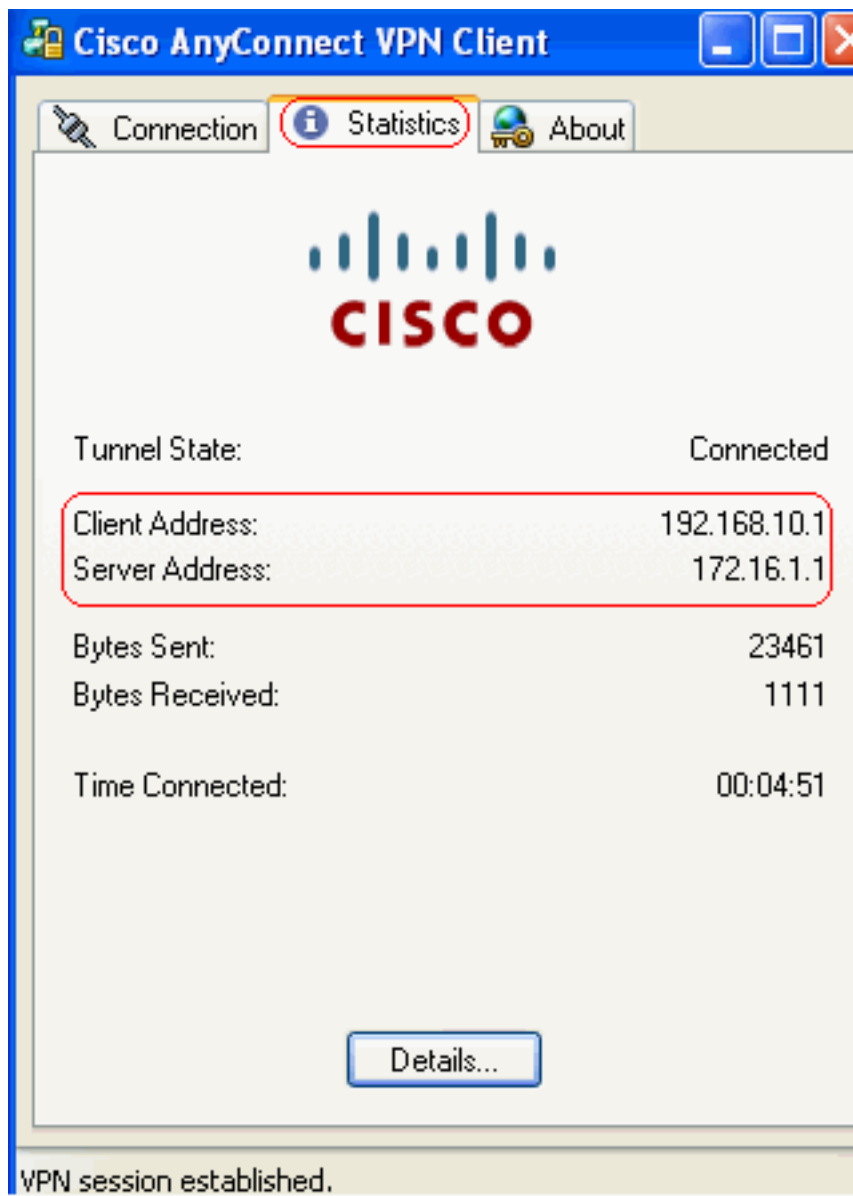
anyconnect - Paint

Cisco AnyConnect  
Connected

3. Klicken Sie auf die Sperre, die in der Taskleiste Ihres Computers angezeigt



wird. **VPN session established.** Dieses Fenster wird angezeigt und enthält Informationen zur SSL-Verbindung. Beispielsweise ist **192.168.10.1** die zugewiesene IP von der ASA



usw. VPN session established.

In diesem Fenster werden

die Versionsinformationen des Cisco AnyConnect VPN-Clients



angezeigt. VPN session established

## 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**.

- **show webvpn svc**: Zeigt die im ASA-Flash-Speicher gespeicherten SVC-Images an.

```
ciscoasa#show webvpn svc
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Mon 04/23/2007 4:16:34.63

1 SSL VPN Client(s) installed
```

- **show vpn-sessiondb svc**: Zeigt Informationen über die aktuellen SSL-Verbindungen an.

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC
```

```
Username      : ssluser1                Index      : 12
```

```

Assigned IP   : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 194118                  Bytes Rx    : 197448
Group Policy : clientgroup             Tunnel Group : sslgroup
Login Time   : 17:12:23 IST Mon Mar 24 2008
Duration     : 0h:12m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none

```

- **show webvpn group-alias:** Zeigt den konfigurierten Alias für verschiedene Gruppen an.

```

ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled

```

- Wählen Sie im ASDM **Monitoring > VPN > VPN Statistics > Sessions** aus, um die aktuellen WebVPN-Sitzungen in der ASA zu erfassen.

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
		Clientless	With Client	Total		
0	0	0	0	0	0	0

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

1. **vpn-sessiondb logoff name <username>:** Befehl zum Abmelden der SSL VPN-Sitzung für den jeweiligen Benutzernamen.

```

ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)

```

Ebenso können Sie den Befehl **vpn-sessiondb logoff svc** verwenden, um alle SVC-Sitzungen zu beenden.

2. **Hinweis:** Wenn der PC in den Standby- oder Ruhemodus wechselt, kann die SSL VPN-Verbindung beendet werden.

```

webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL

```

```
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)
```

```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

### 3. debug webvpn svc <1-255>: Stellt die Webvpn-Ereignisse in Echtzeit bereit, um die Sitzung einzurichten.

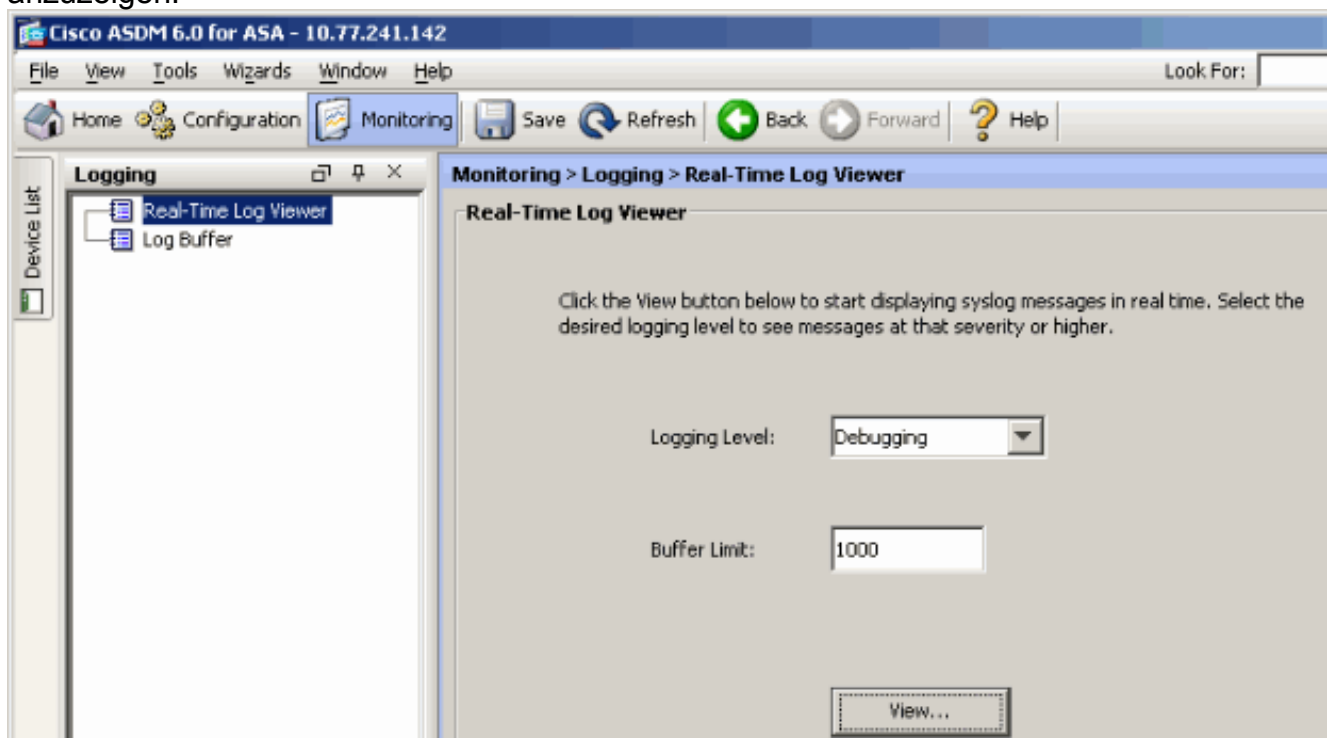
```
Ciscoasa#debug webvpn svc 7
```

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AF9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AF9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
```



```
SVC: NP setup
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

4. Wählen Sie im ASDM Monitoring > Logging > Real-time Log Viewer > View (Überwachung > Anmeldung > Echtzeit-Protokollanzeige > Anzeigen), um die Ereignisse in Echtzeit anzuzeigen.



Dieses Beispiel zeigt, dass die SSL-Sitzung mit dem Headend-Gerät eingerichtet wurde.

Real-Time Log Viewer - 10.77.241.142

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Show All Find:

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Message
6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.
6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44:
6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identit
6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl
6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026
6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.
6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TL5v1 se
6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23

%ASA-6-725002 Device completed SSL handshake with remote\_device interface\_name:IP\_address/port

The SSL handshake has completed successfully with the remote device.

## Zugehörige Informationen

- [Support-Seite für Cisco Adaptive Security Appliances der Serie 5500](#)
- [Versionshinweise für AnyConnect VPN Client, Version 2.0](#)
- [ASA/PIX: Split Tunneling für VPN-Clients im ASA-Konfigurationsbeispiel zulassen](#)
- [Router ermöglicht VPN-Clients die Verbindung von IPsec und Internet mithilfe des Split Tunneling-Konfigurationsbeispiels](#)
- [Beispiel für eine Stick-Konfiguration: PIX/ASA 7.x und VPN-Client für Public Internet VPN](#)
- [SSL VPN Client \(SVC\) auf ASA mit ASDM - Konfigurationsbeispiel](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)