ASA 7.1/7.2: Split Tunneling für SVC im ASA-Konfigurationsbeispiel zulassen

Inhalt

Einführung

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

Die Möglichkeit, sicheren und ungesicherten Datenverkehr über dieselbe Schnittstelle zu übertragen, wird als Split-Tunneling bezeichnet. Beim Split-Tunneling müssen Sie genau angeben, welcher Datenverkehr gesichert ist und welches Ziel dieser Datenverkehr ist, sodass nur der angegebene Datenverkehr in den Tunnel gelangt, während der Rest unverschlüsselt über das öffentliche Netzwerk (Internet) übertragen wird.

Voraussetzungen

Anforderungen

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

- Lokale Administratorberechtigungen für alle Remote-Workstations

- Java- und ActiveX-Steuerelemente auf der Remote-Workstation
- Port 443(SSL) wird am Verbindungspfad nicht blockiert

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 7.2(2)
- Cisco SSL VPN Client-Version für Windows 1.1.4.179**Hinweis:** Laden Sie das SSL VPN Client-Paket (sslclient-win*.pkg) vom Cisco Software Download herunter (nur registrierte Kunden). Kopieren Sie den SVC in den Flash-Speicher der ASA, der auf die Computer der Remote-Benutzer heruntergeladen werden soll, um die SSL VPN-Verbindung mit ASA herzustellen. Weitere Informationen finden Sie im Abschnitt Installation der SVC-Software im ASA-Konfigurationsleitfaden.
- PC mit Windows 2000 Professional SP4 oder Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) Version 5.2(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 SSL VPN Client (SVC) ist eine VPN-Tunneling-Technologie, die Remote-Benutzern die Vorteile eines IPsec-VPN-Clients bietet, ohne dass Netzwerkadministratoren IPsec-VPN-Clients auf Remote-Computern installieren und konfigurieren müssen. Der SVC verwendet die SSL-Verschlüsselung, die bereits auf dem Remote-Computer vorhanden ist, sowie die WebVPN-Anmeldung und -Authentifizierung der Sicherheits-Appliance.

Um eine SVC-Sitzung einzurichten, gibt der Remote-Benutzer die IP-Adresse einer WebVPN-Schnittstelle der Sicherheits-Appliance im Browser ein. Der Browser stellt eine Verbindung zu dieser Schnittstelle her und zeigt den WebVPN-Anmeldebildschirm an. Wenn Sie die Anmeldeinformationen und die Authentifizierung einhalten und die Sicherheits-Appliance Sie als den SVC erforderlich identifiziert, lädt die Sicherheits-Appliance den SVC auf den Remote-Computer. Wenn die Sicherheits-Appliance Sie mit der Option zur Verwendung des SVC identifiziert, lädt die Sicherheits-Appliance den SVC auf den Remote-Computer herunter, während ein Link im Fenster angezeigt wird, über den die SVC-Installation übersprungen werden kann.

Nach dem Herunterladen installiert und konfiguriert sich der SVC selbst, und der SVC bleibt bzw. deinstalliert sich je nach Konfiguration vom Remote-Computer, wenn die Verbindung beendet wird.

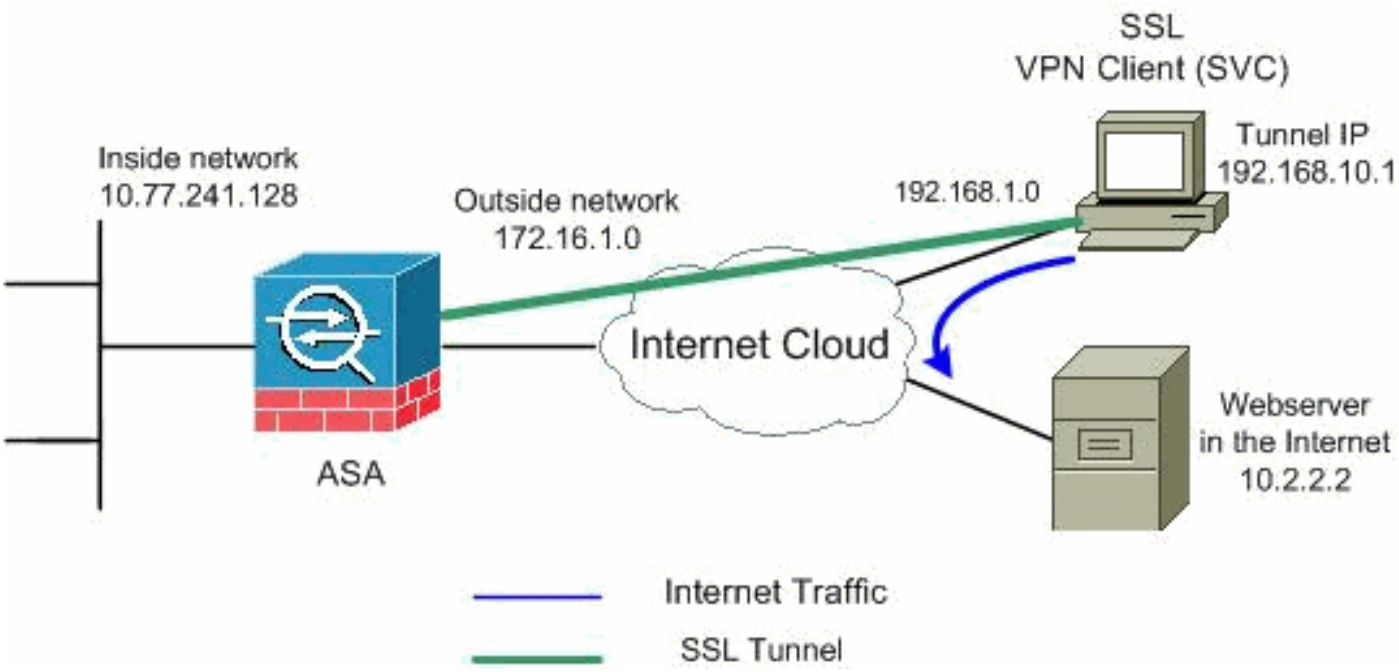
Konfigurieren

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.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

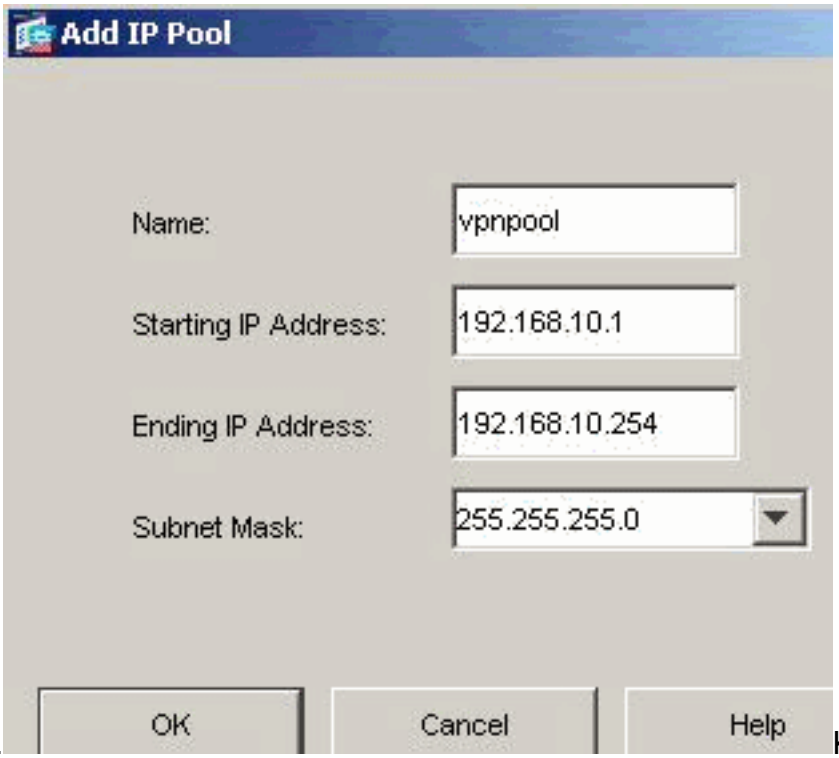


Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

ASA-Konfigurationen mit ASDM 5.2(2)

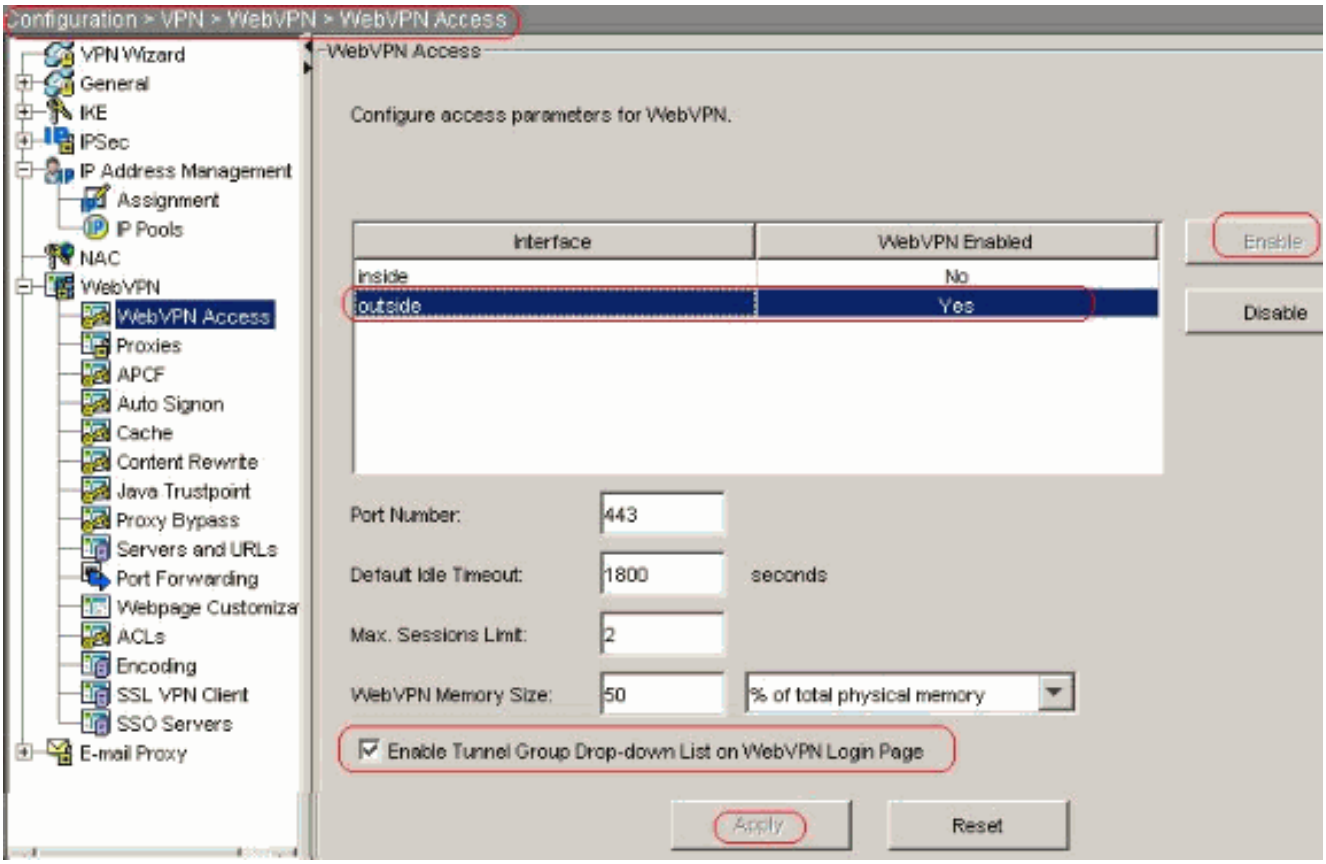
Gehen Sie wie folgt vor, um das SSL VPN auf ASA mit Split Tunneling zu konfigurieren:

1. Im Dokument wird davon ausgegangen, dass die Basiskonfiguration, z. B. die Schnittstellenkonfiguration usw., bereits vorgenommen 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.
2. Wählen Sie **Configuration > VPN > IP Address Management > IP Pools**, um einen IP-Adresspool zu erstellen: **vpnpool** für VPN-



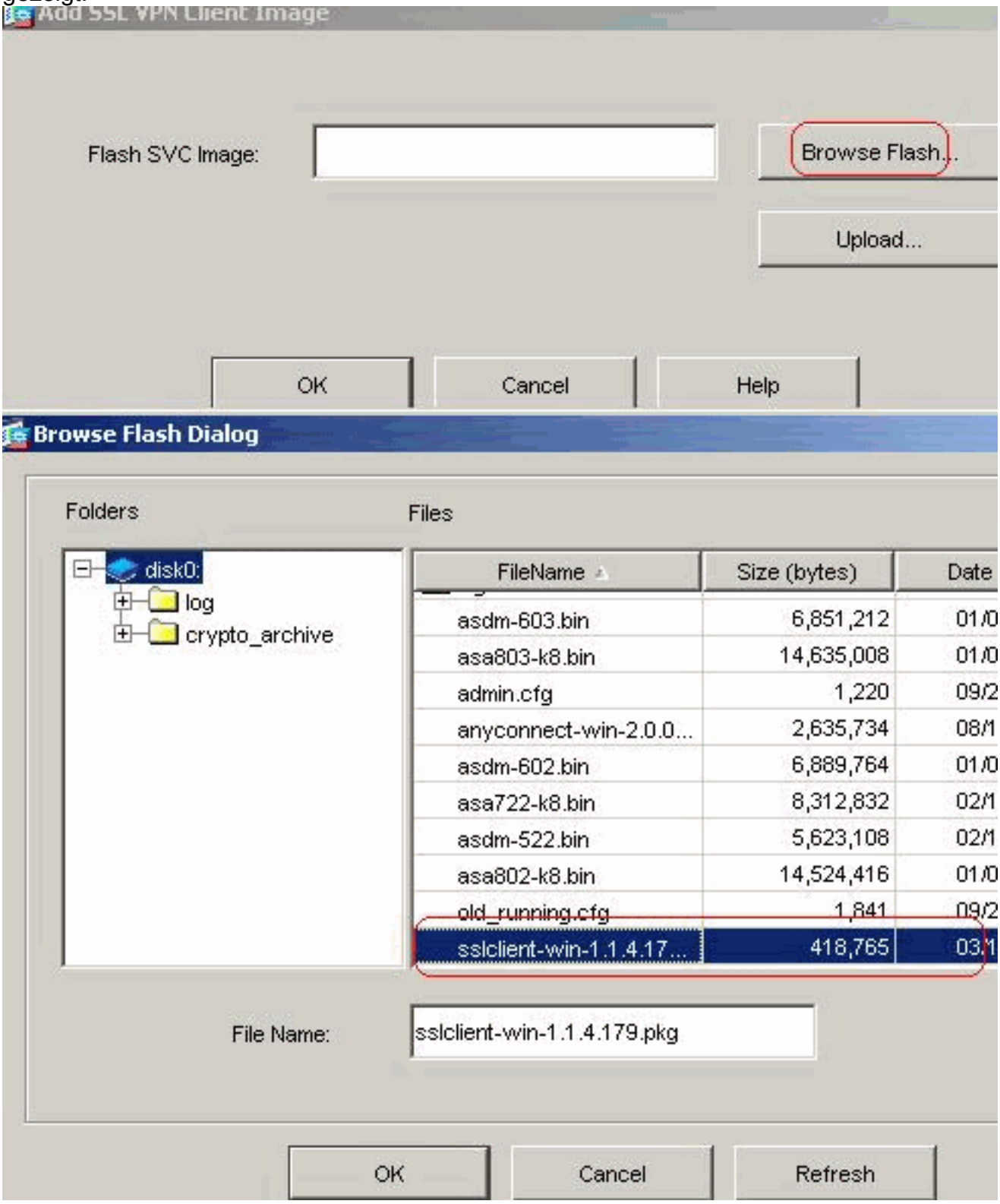
Clients. Klicken Sie auf **Übernehmen**.

3. **WebVPN aktivieren**Wählen Sie **Configuration > VPN > WebVPN > WebVPN Access (Konfiguration > VPN > WebVPN > WebVPN-Zugriff)**, markieren Sie die externe Schnittstelle mit der Maus, und klicken Sie auf **Enable (Aktivieren)**. Aktivieren Sie das Kontrollkästchen **Enable Tunnel Group Drop-Down List on WebVPN Login Page** (Tunnelgruppenliste aktivieren), um das Dropdown-Menü auf der Anmeldeseite für Benutzer zu aktivieren und die entsprechenden Gruppen
auszuwählen.

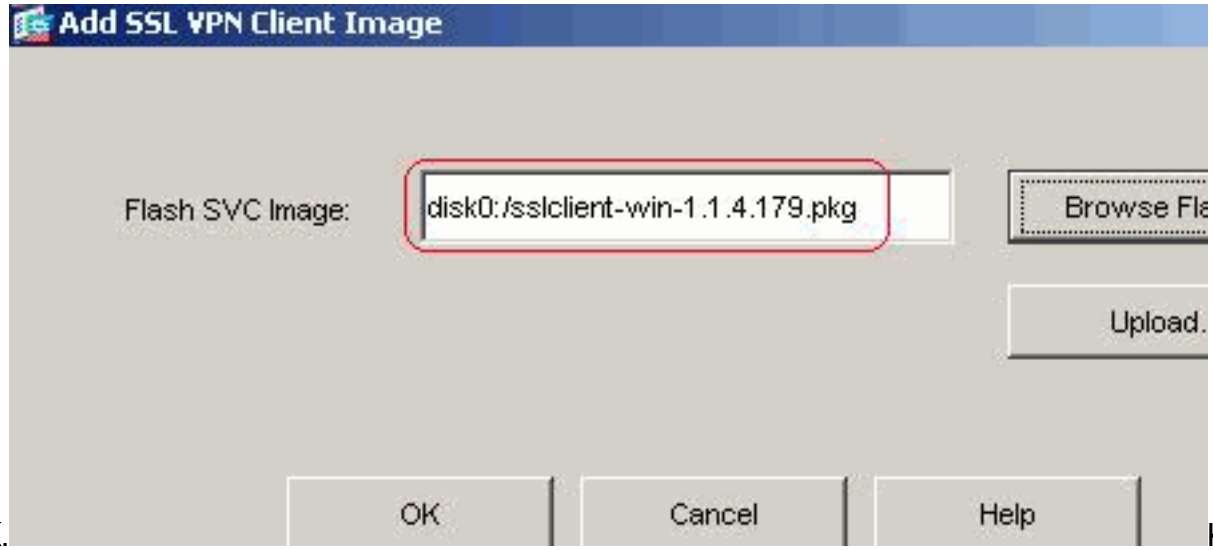


Klicken Sie auf **Übernehmen**.Wählen Sie **Configuration > VPN > WebVPN > SSL VPN Client > Add** aus, um das SSL VPN Client-Image aus dem Flash-Speicher der ASA hinzuzufügen,

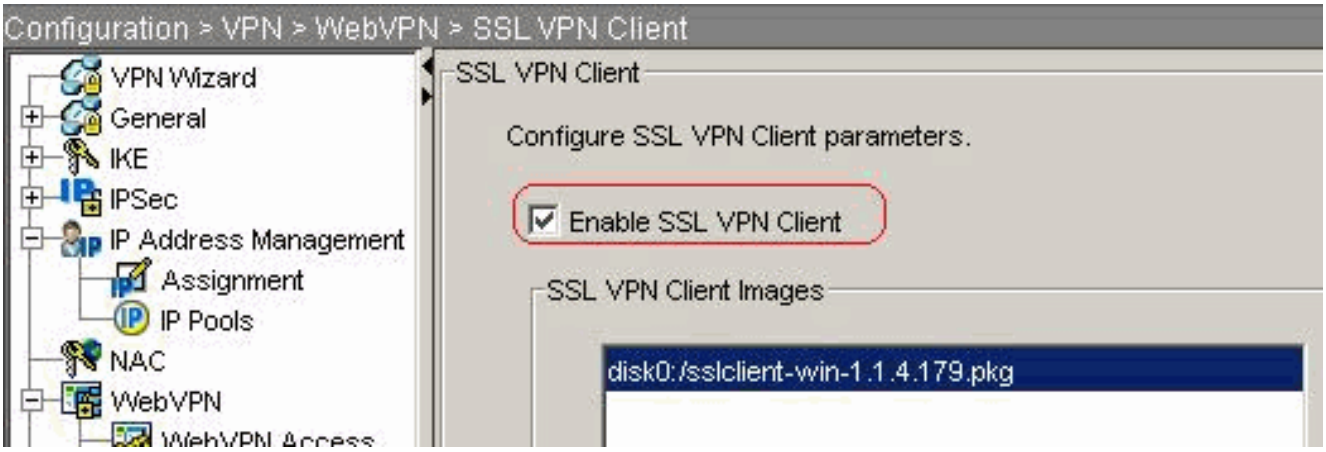
wie
gezeigt.



Klicken Sie auf

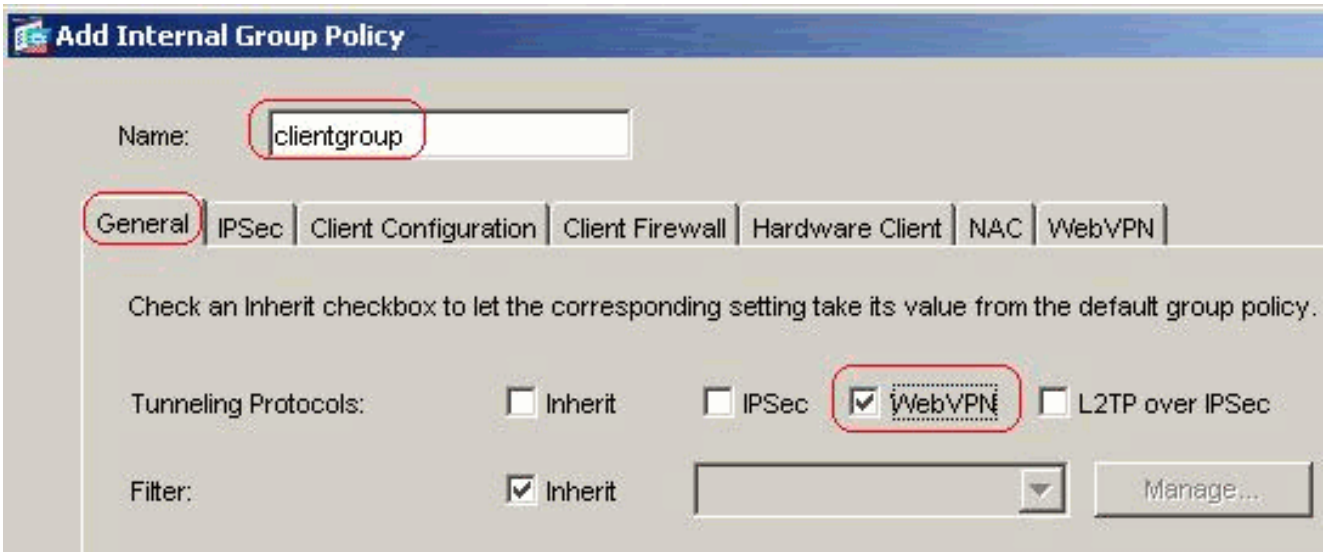


OK.Klicken Sie auf **OK**.Klicken Sie auf das Kontrollkästchen **SSL VPN Client**.



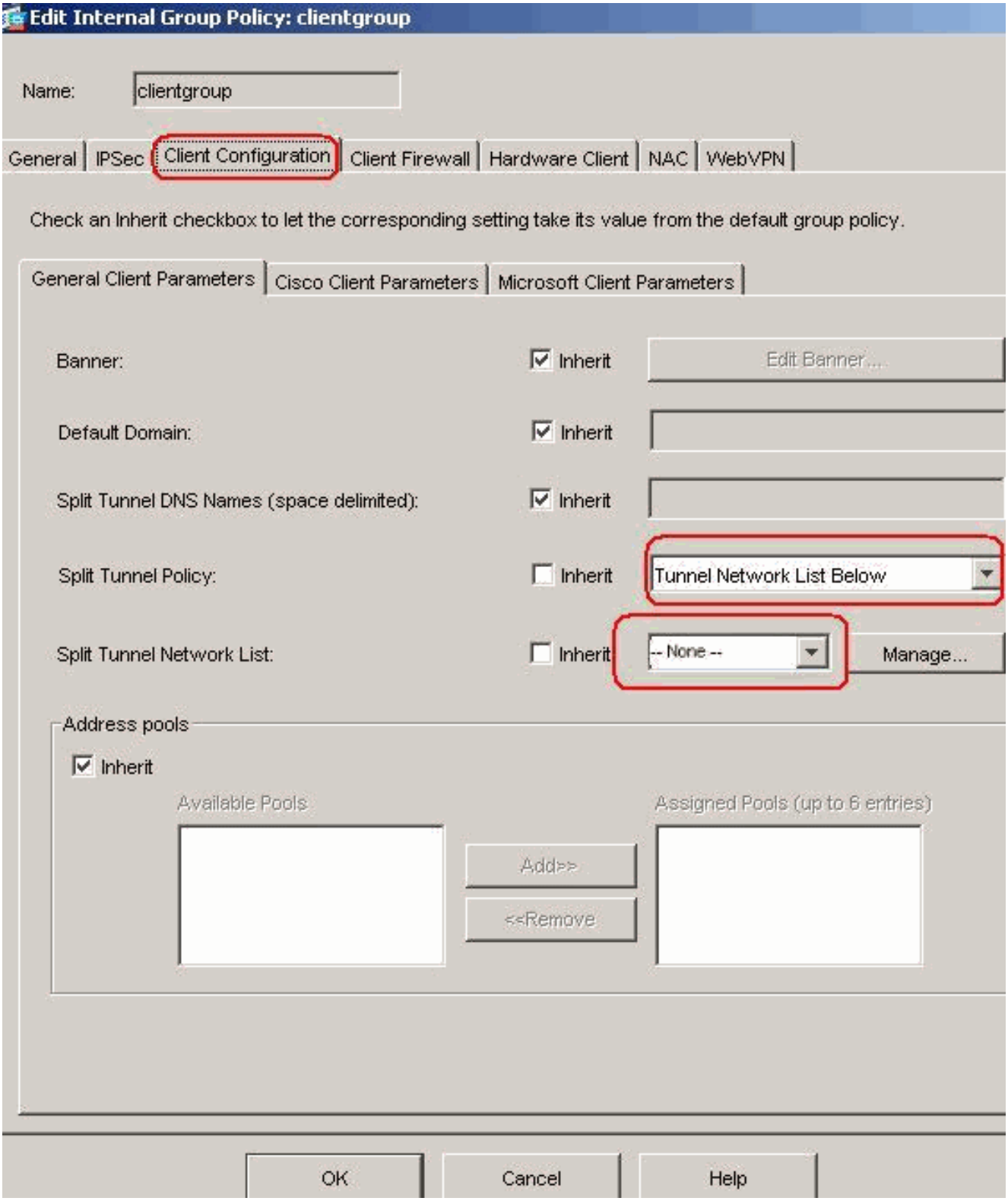
Klicken Sie auf **Übernehmen**.**Entsprechende CLI-Konfiguration:**

4. **Gruppenrichtlinie konfigurieren**Wählen Sie **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)**, um eine interne Gruppenrichtlinien-**Clientgruppe** zu erstellen. Wählen Sie unter **Allgemein** das **WebVPN-**Kontrollkästchen aus, um das WebVPN als Tunneling-Protokoll zu aktivieren.

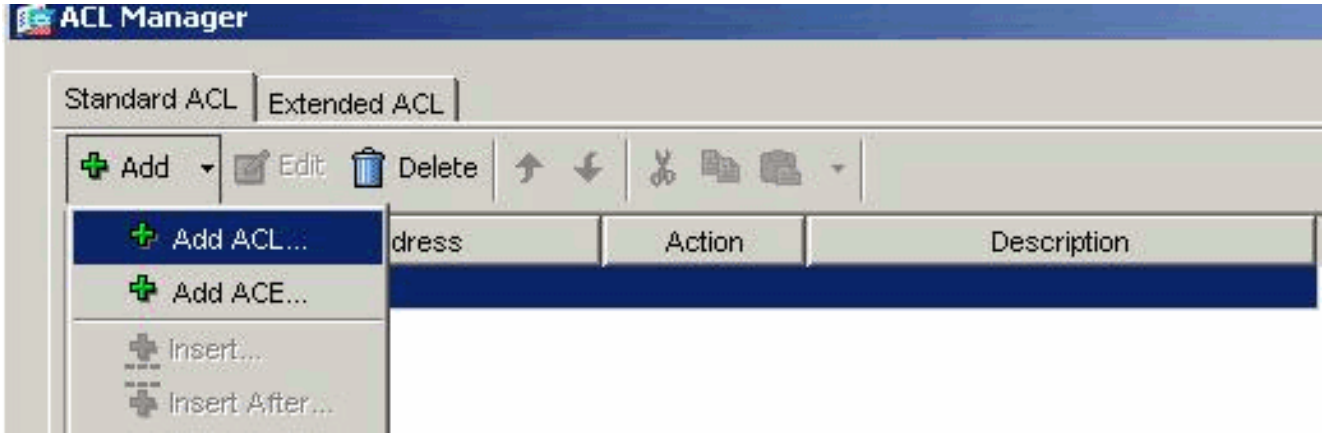


Deaktivieren Sie auf der Registerkarte **Client Configuration > General Client Parameters das** Kontrollkästchen **Inherit** for Split Tunnel Policy (Client-Konfiguration > Allgemeine Client-Parameter), und wählen Sie **Tunnel Network List (Tunnel-Netzwerkliste) unten** aus der

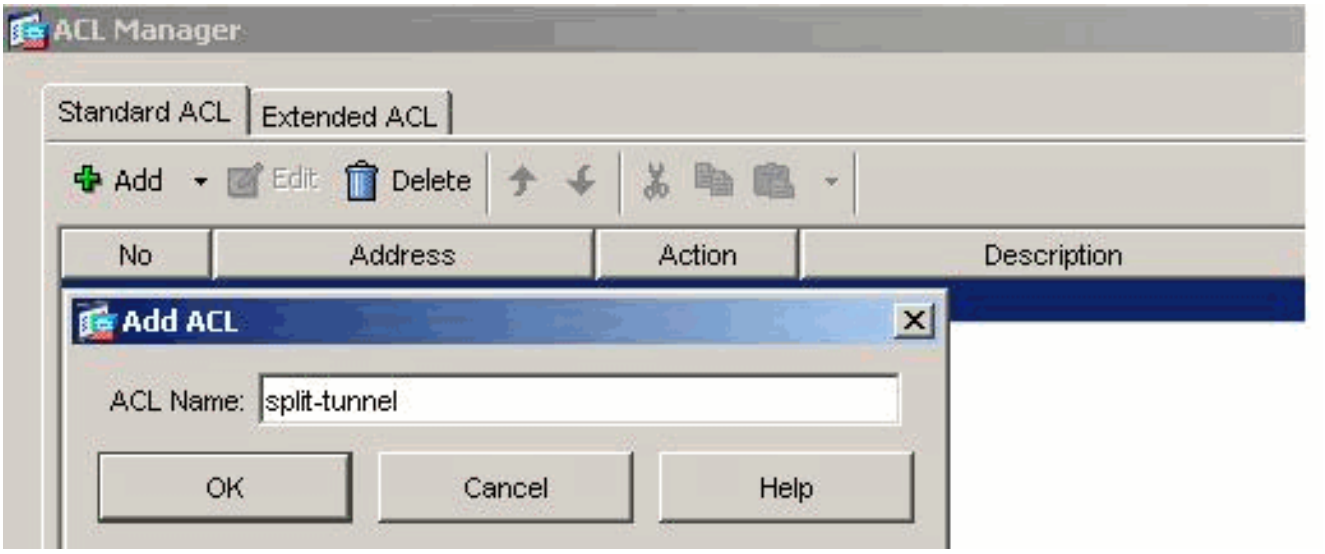
Dropdown-Liste aus.Deaktivieren Sie das Kontrollkästchen **Erben** für die **Split Tunnel Network List (Kanalliste für Tunnel-Netzwerk teilen)**, und klicken Sie dann auf **Manage (Verwalten)**, um den ACL Manager zu
starten.



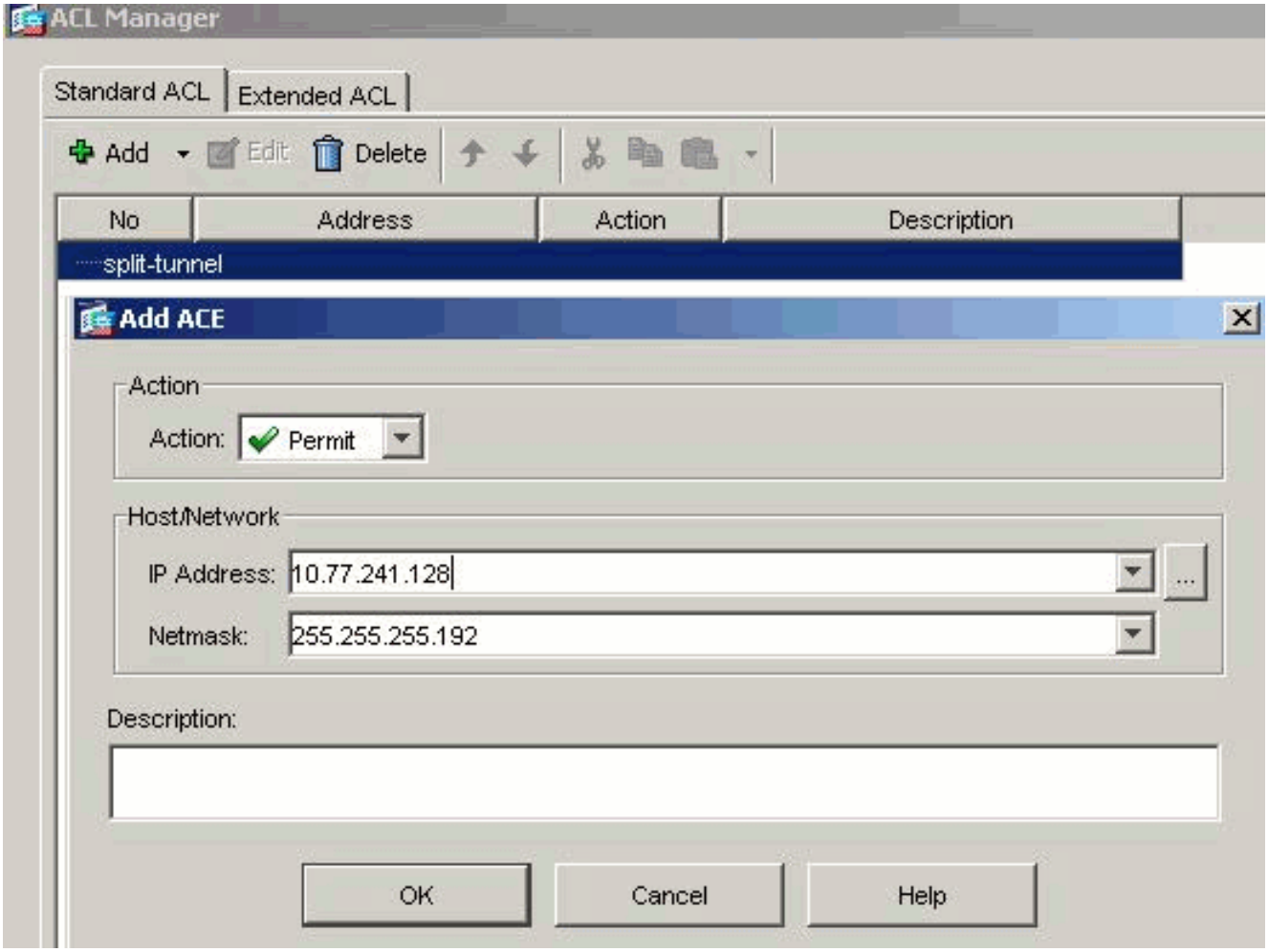
Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu
erstellen.



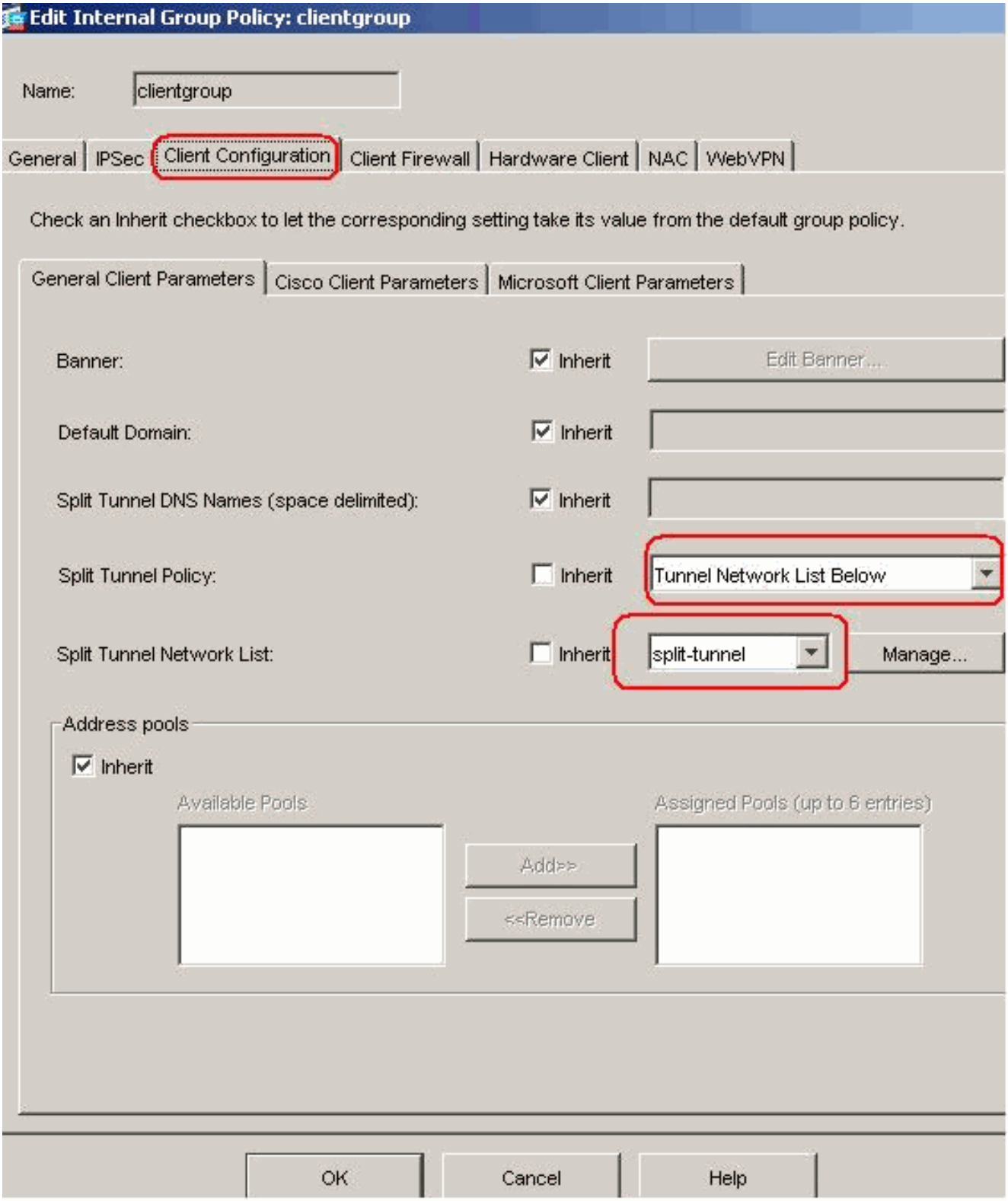
Geben Sie einen Namen für die ACL an, und klicken Sie auf **OK**.



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 lautet das Netzwerk 10.77.241.128/26, und wählen Sie **Zulassen aus**.Klicken Sie auf **OK**, um den ACL Manager zu
verlassen.

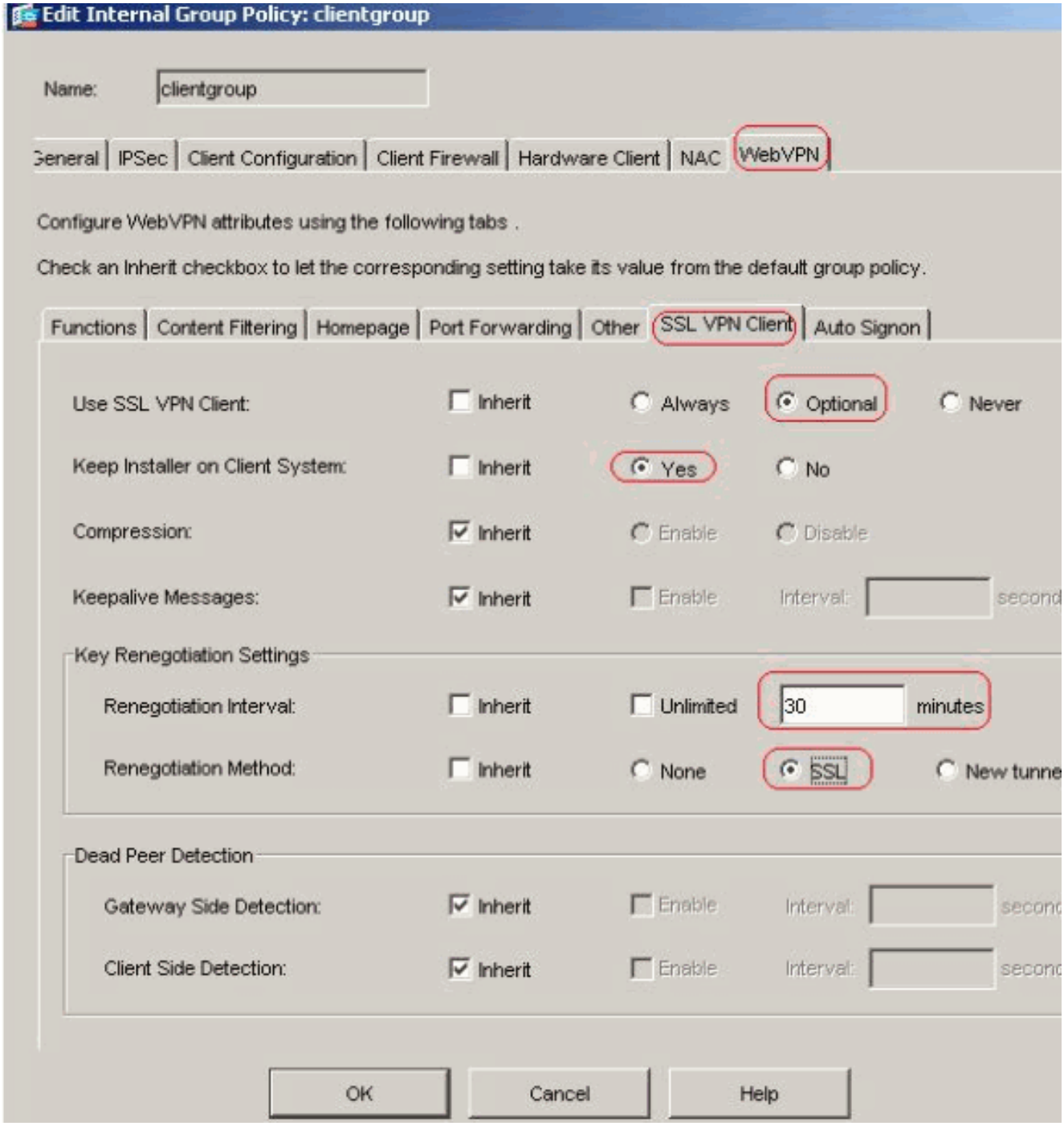


Stellen Sie sicher, dass die gerade erstellte ACL für die Split Tunnel Network List (Netzwerkliste des Split-Tunnels) ausgewählt ist.Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration zurückzukehren.

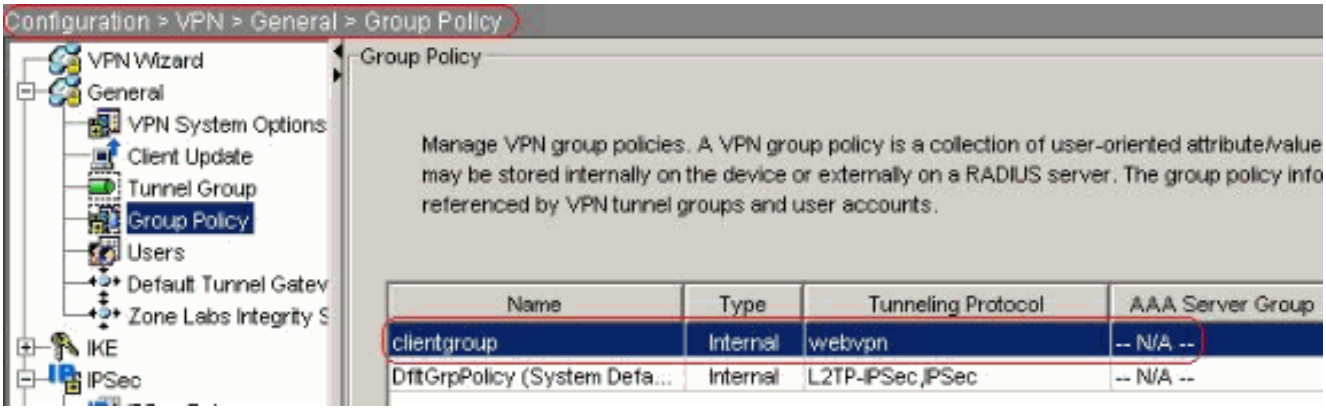


Klicken Sie auf der Hauptseite auf **Apply** und dann auf **Send** (falls erforderlich), um die Befehle an die ASA zu senden.Deaktivieren Sie für die Option SSL VPN-Client verwenden das Kontrollkästchen **Erben**, und klicken Sie auf das **Optionsfeld Optional**.Bei dieser Auswahl kann der Remote-Client wählen, ob er auf die Registerkarte **WebVPN > SSL VPN Client** klicken und folgende Optionen auswählen soll:Laden Sie den SVC nicht herunter. Die Always-Option stellt sicher, dass der SVC während jeder SSL-VPN-Verbindung auf die Remote-Workstation heruntergeladen wird.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-Computer 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.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, wenn Sie die Gültigkeitsdauer eines Schlüssels begrenzen.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.Die Attribute des SSL VPN-Clients sollten wie in diesem Bild gezeigt konfiguriert
werden:

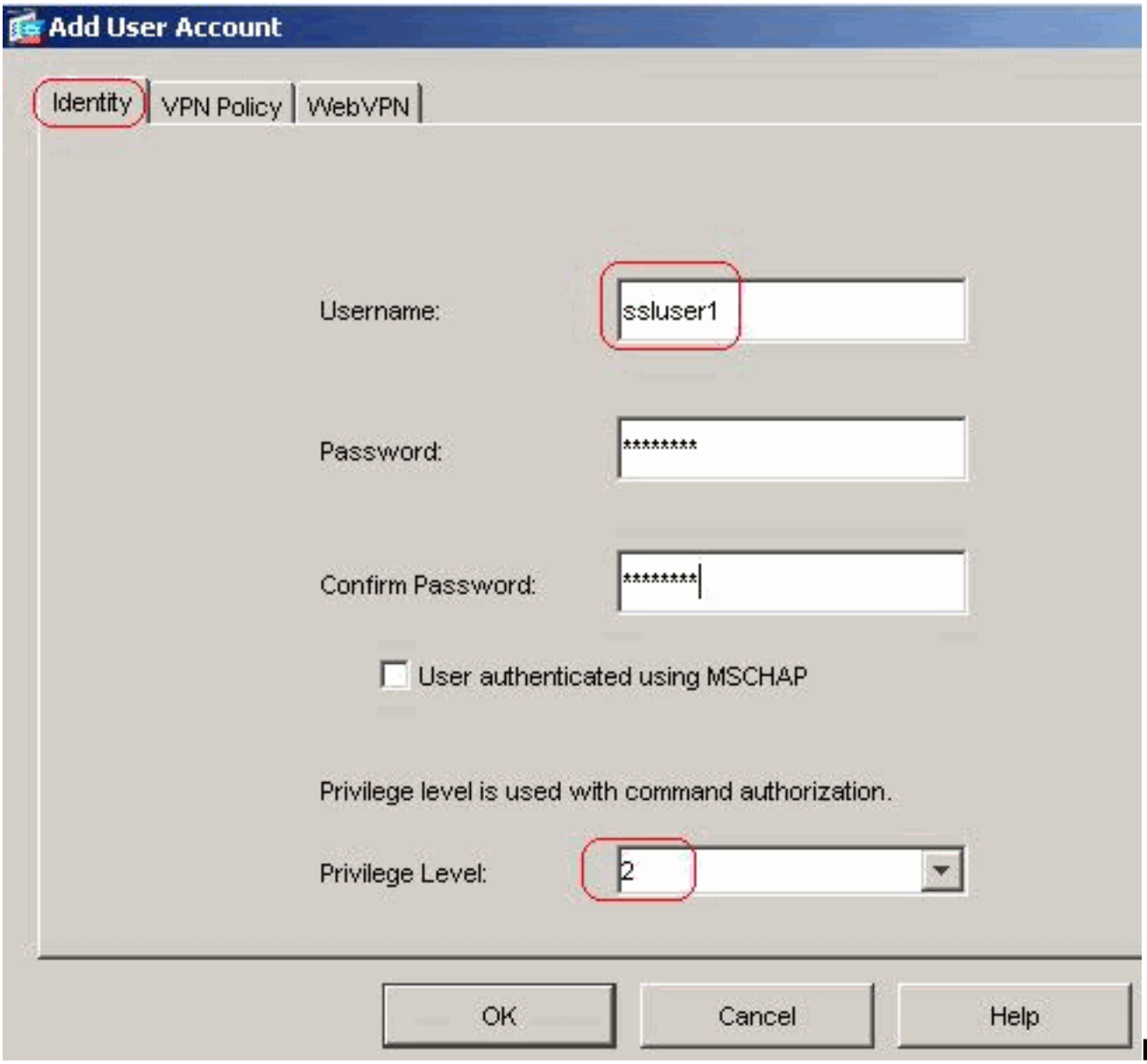


Klicken Sie auf **OK** und dann auf **Übernehmen**.



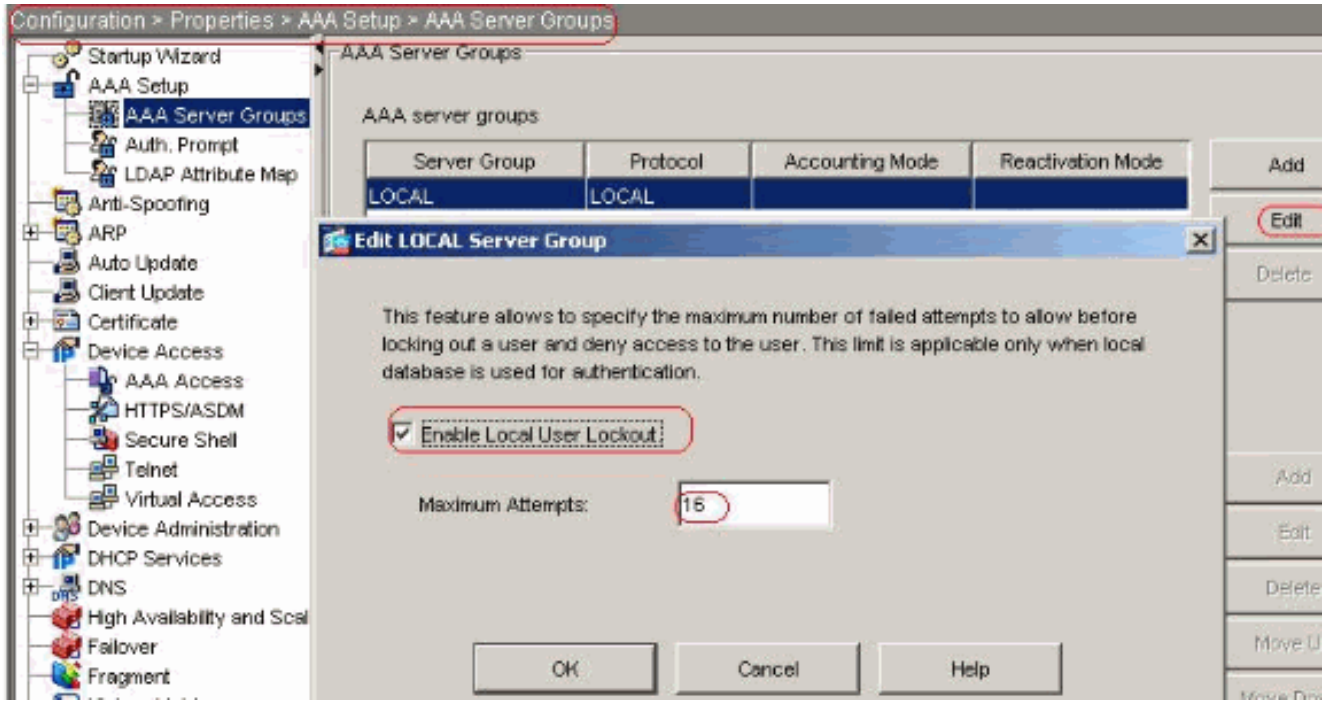
Entsprechende CLI-Konfiguration:

5. Wählen Sie **Configuration > VPN > General > Users > Add**, um ein neues Benutzerkonto **ssluser1** zu erstellen. Klicken Sie auf **OK** und dann auf **Übernehmen**.



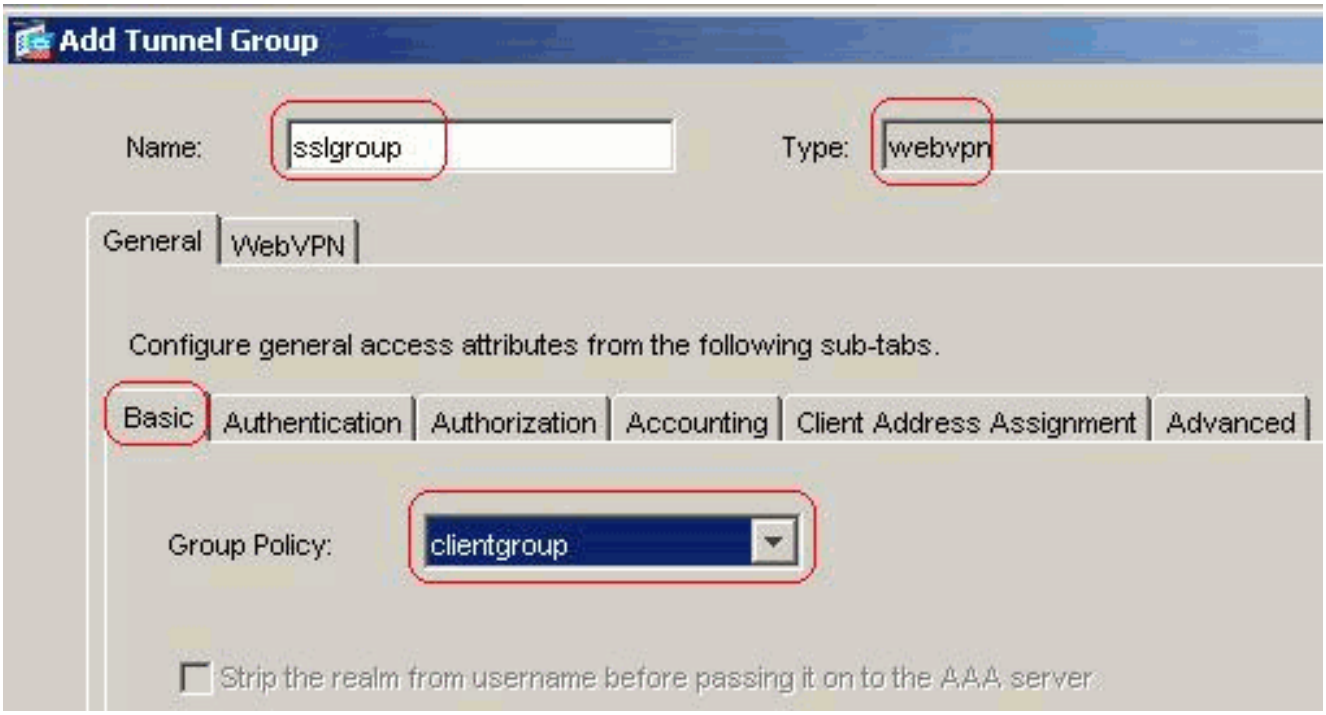
Entsprechende CLI-Konfiguration:

6. Wählen Sie **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit** aus, um die Standard-Servergruppe **LOCAL** zu ändern, und aktivieren Sie das Kontrollkästchen Enable Local User Lockout (Lokale **Benutzersperre aktivieren) mit dem Wert 16** für maximale Zugriffsversuche.

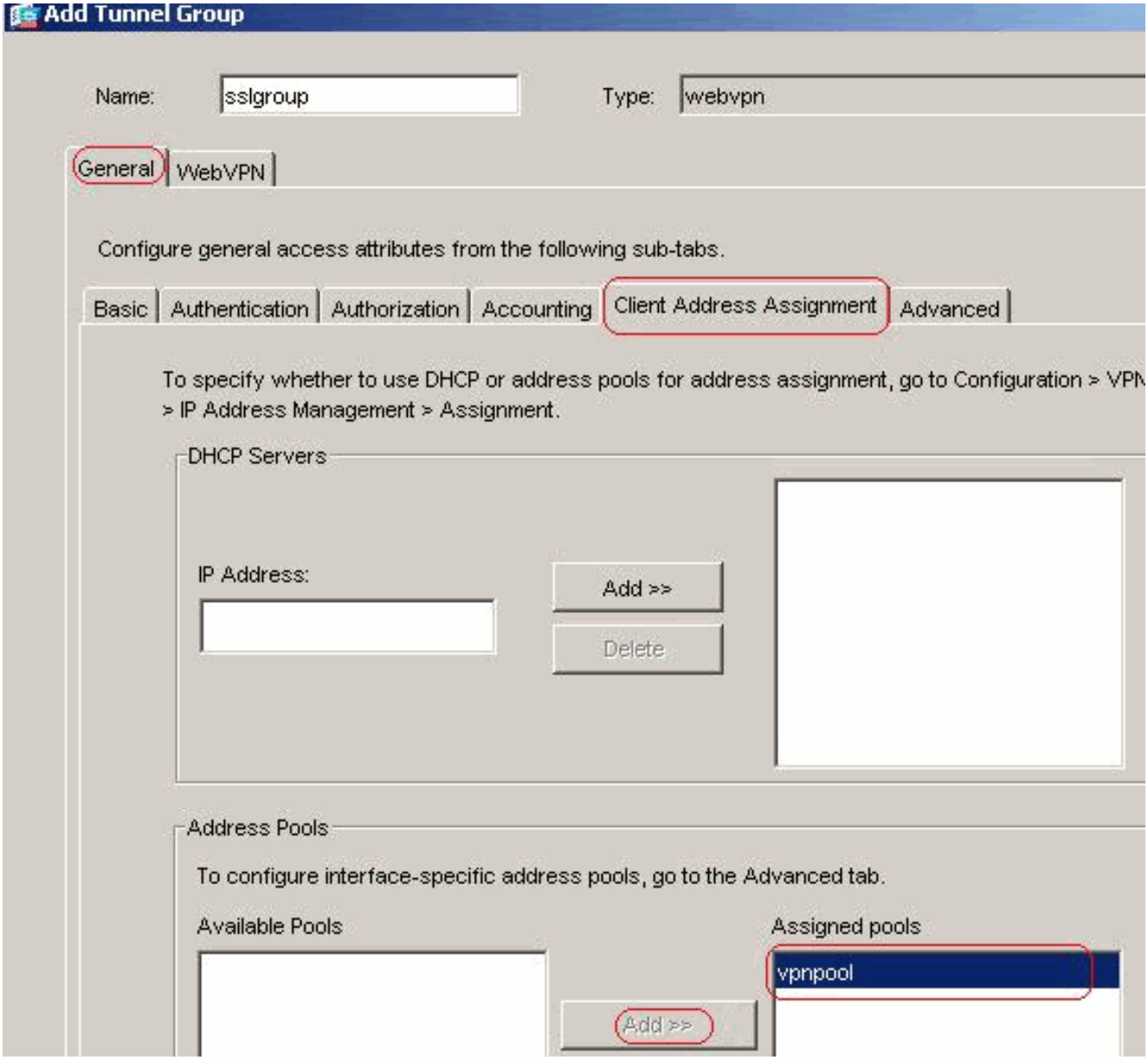


Entsprechende CLI-Konfiguration:

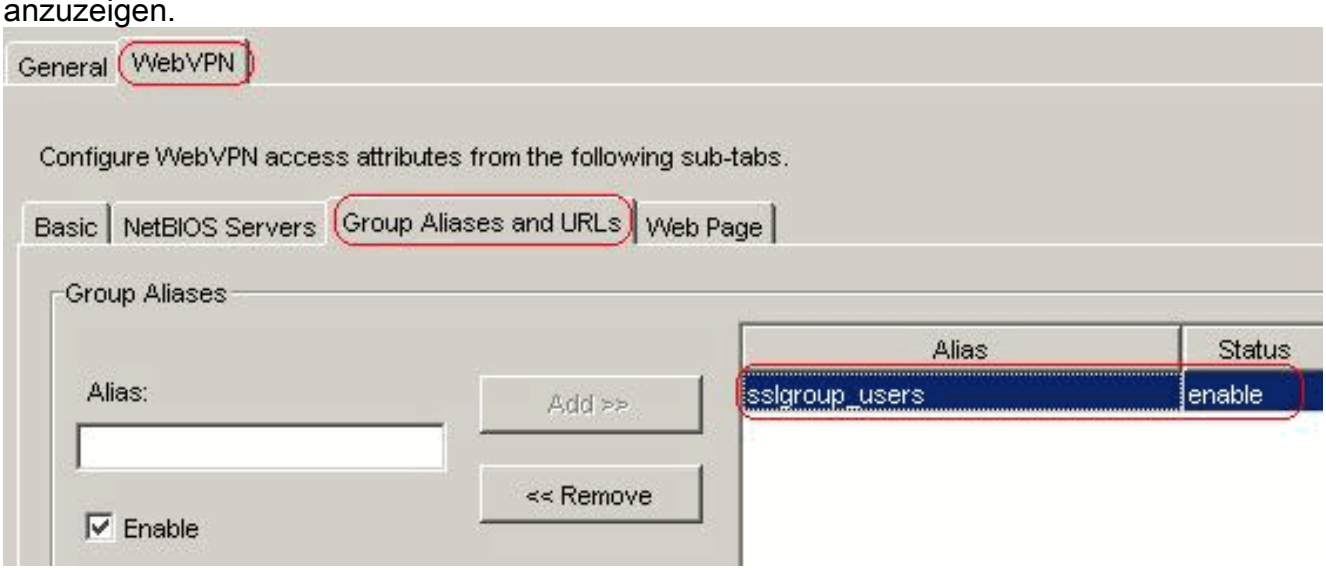
7. **Tunnelgruppe konfigurieren**Wählen Sie **Configuration > VPN > General > Tunnel Group > Add (WebVPN access)**, um eine neue Tunnelgruppen-**Gruppe** zu erstellen.Wählen Sie auf der Registerkarte **Allgemein > Grundlegend** die Option Gruppenrichtlinie als **Clientgruppe** aus der Dropdown-Liste
aus.



Klicken Sie auf der Registerkarte **General > Client Address Assignment (Allgemein > Client-Adressenzuweisung**) unter Address Pools auf **Add >>**, um den verfügbaren Adresspool **vpnpool**
zuzuweisen.



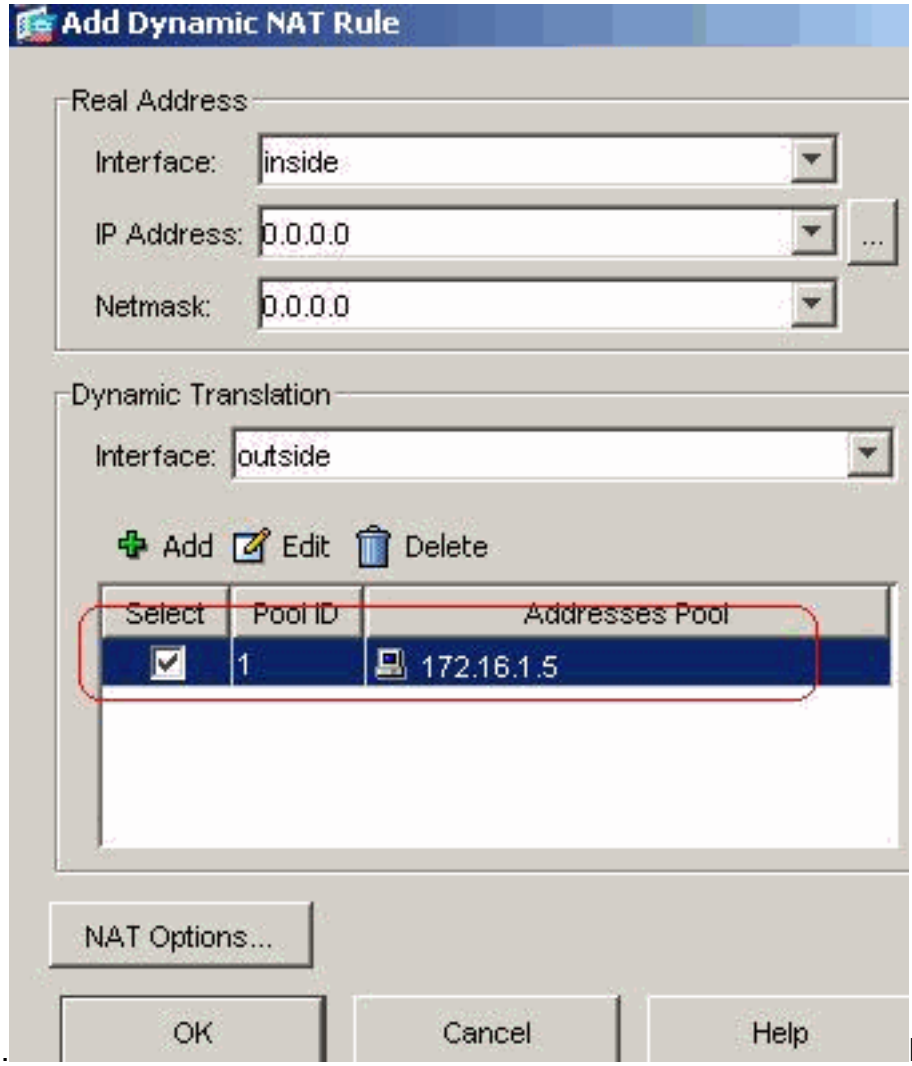
Geben Sie auf der Registerkarte **WebVPN > Group Aliases and URLs (WebVPN > GruppenAliase und URLs**) den Aliasnamen im Parameterfeld ein, und klicken Sie auf **Hinzufügen >>**, um ihn in der Liste der Gruppennamen auf der Anmeldeseite anzuzeigen.



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

8. **Konfigurieren von NAT**Wählen Sie **Configuration > NAT > Add > Add Dynamic NAT Rule**

(Konfiguration > NAT > Hinzufügen > Dynamische NAT-Regel hinzufügen für den Datenverkehr aus dem internen Netzwerk, der mit der externen IP-Adresse 172.16.1.5 übersetzt werden



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

9. 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 7.2(2)-Konfiguration mit CLI

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
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
ftp mode passive

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 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.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


access-group 100 in interface outside
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup".
```

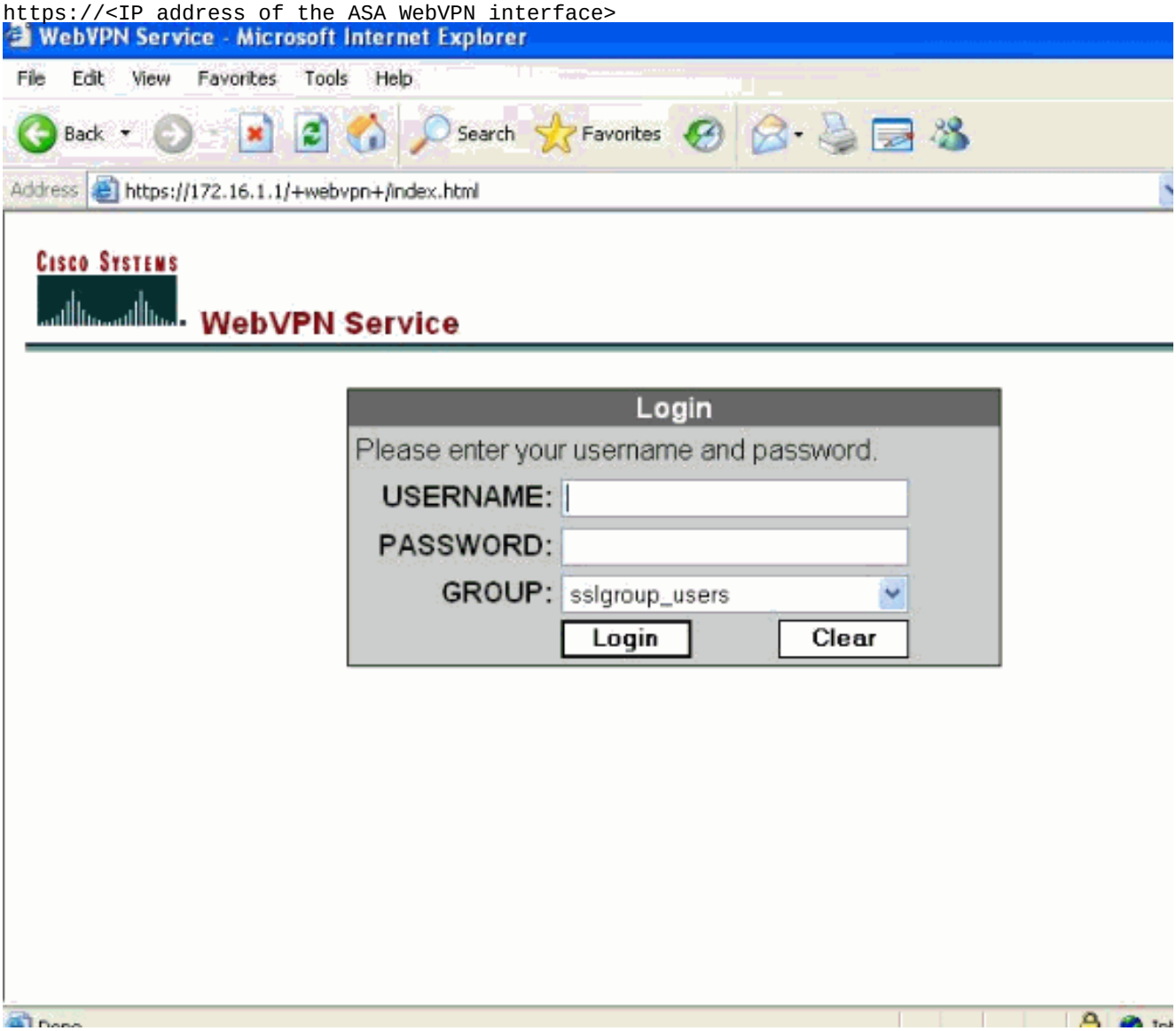
```
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as 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 required

!--- Activate the SVC under webvpn mode. svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, !--- they renegotiate the crypto keys and
initialization vectors, !--- and increase 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. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1". aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. 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 tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. 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. telnet
timeout 5 ssh timeout 5 console timeout 0 ! 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:/sslclient-win-1.1.4.179.pkg 1
```

```
!--- Assign an order to the SVC 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. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

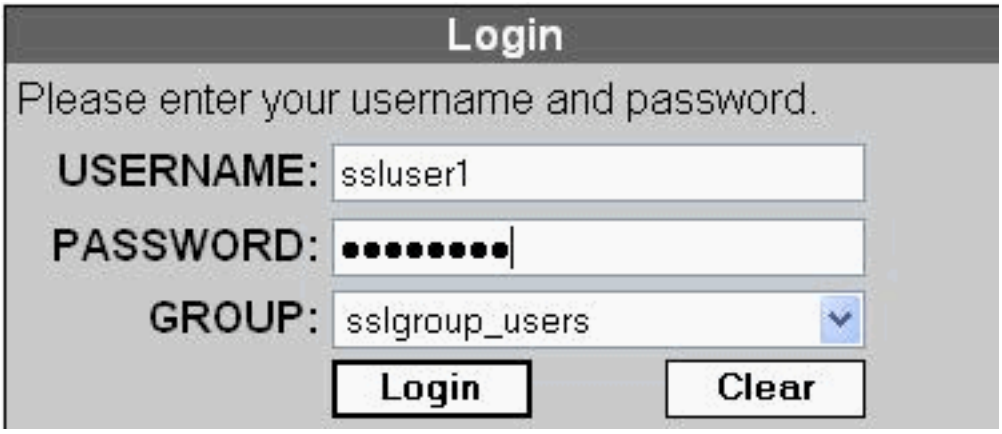
Einrichtung der SSL VPN-Verbindung mit SVC

Führen Sie diese Schritte aus, um eine SSL VPN-Verbindung mit ASA herzustellen.

1. Geben Sie die URL oder IP-Adresse der WebVPN-Schnittstelle der ASA in Ihren Webbrowser im gezeigten Format ein.
   `https://url`
   ODER
   `https://<IP address of the ASA WebVPN interface>`



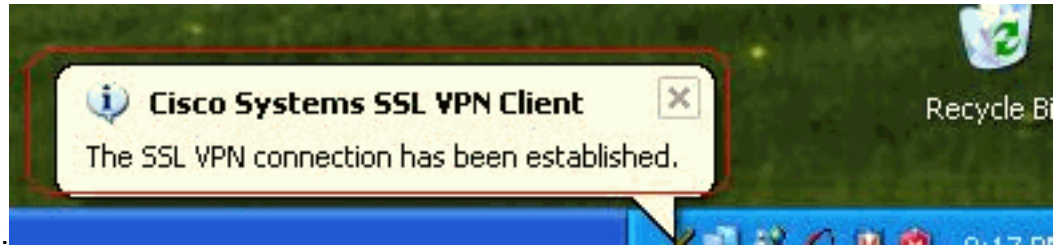
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und wählen Sie dann Ihre entsprechende Gruppe aus der Dropdown-Liste

aus. 

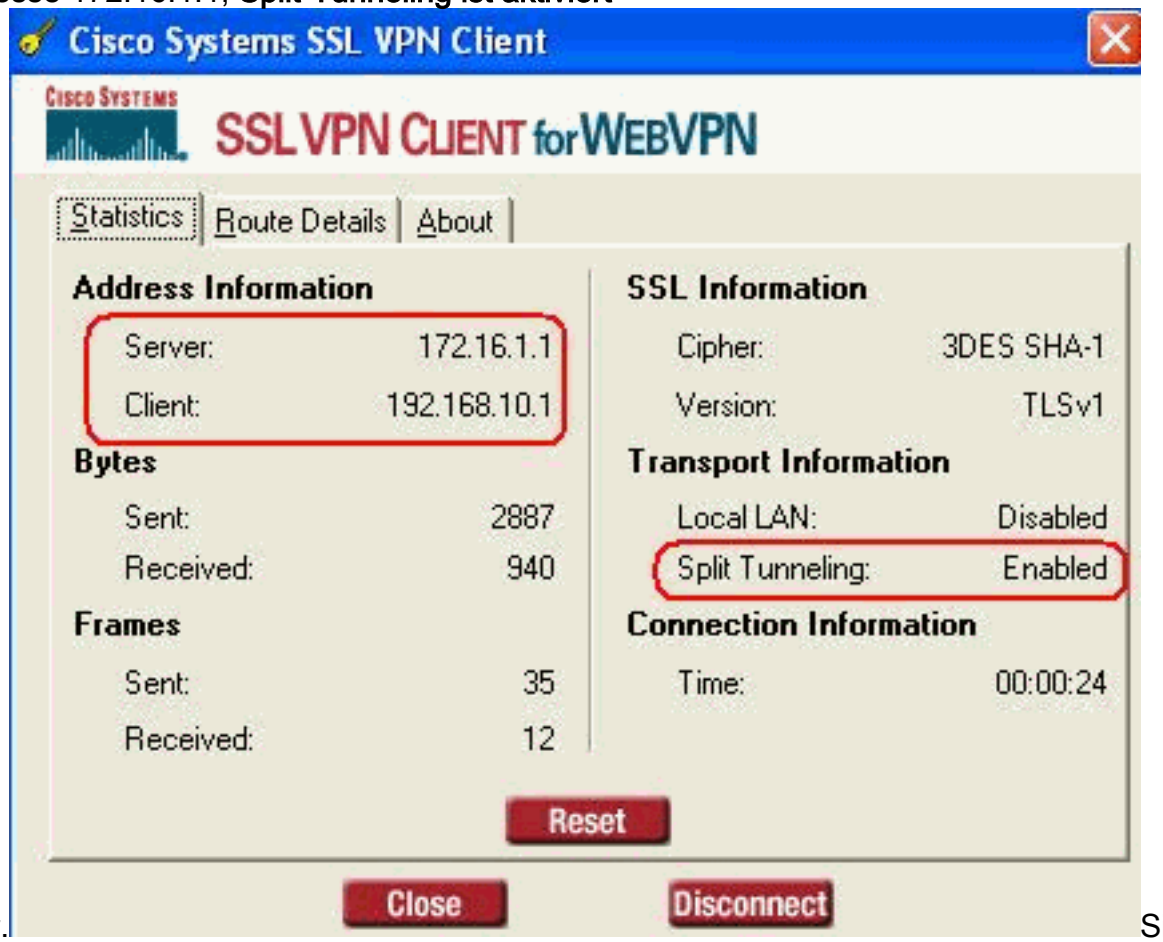
3. Die ActiveX-Software muss auf Ihrem Computer installiert sein, bevor Sie den SVC herunterladen können. 

4. Diese Fenster werden angezeigt, bevor die SSL VPN-Verbindung hergestellt wird. 

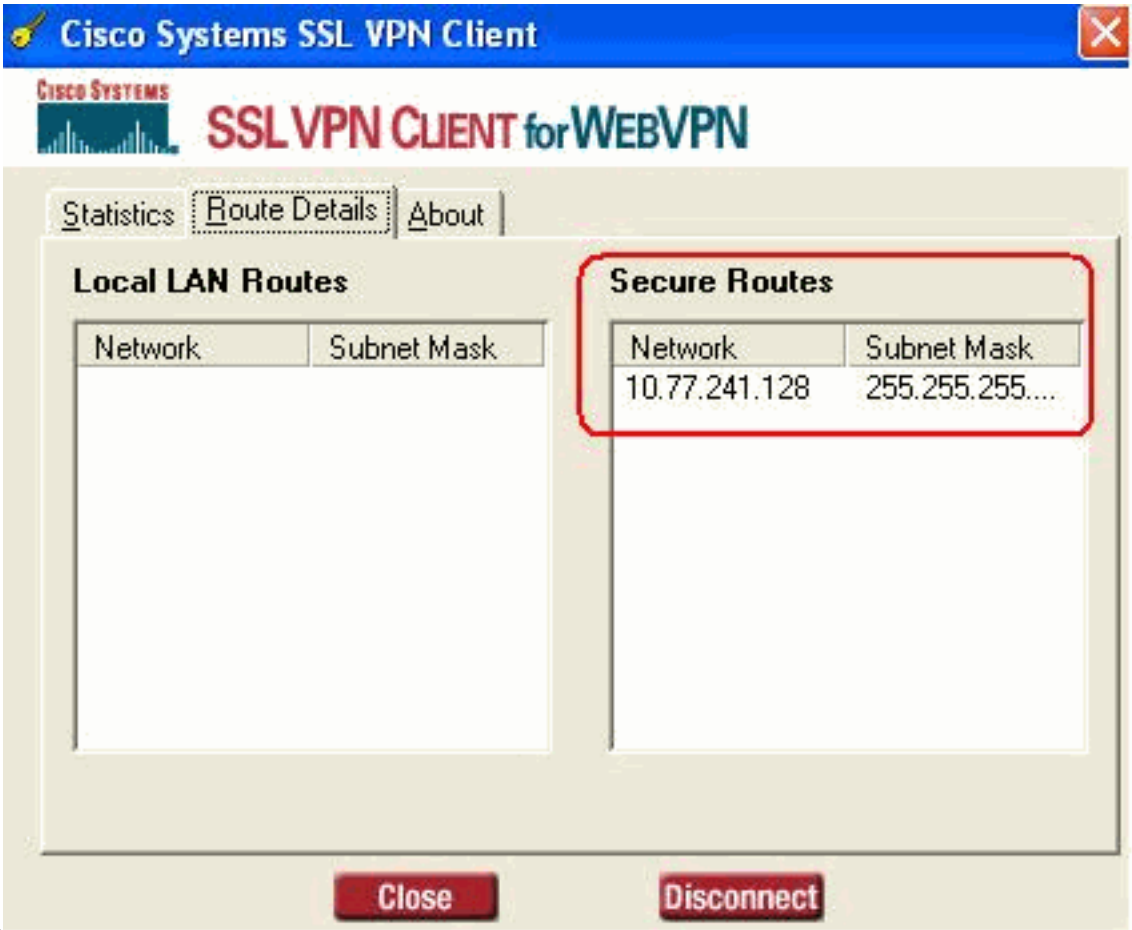
5. Sie können diese Fenster abrufen, sobald die Verbindung hergestellt

ist. 

6. Klicken Sie auf die gelbe Taste, die in der Taskleiste Ihres Computers angezeigt wird. Diese Fenster werden angezeigt, die Informationen über die SSL-Verbindung bereitstellen. Beispielsweise ist **192.168.10.1** die zugewiesene IP-Adresse für die Client- und Server-IP-Adresse 172.16.1.1, **Split-Tunneling ist aktiviert**



usw. Sie können auch das gesicherte Netzwerk überprüfen, das durch SSL verschlüsselt werden soll. Die Netzwerkliste wird aus der in ASA konfigurierten Split-Tunnel-Zugriffsliste heruntergeladen.In diesem Beispiel sichert der SSL VPN Client den Zugriff auf 10.77.241.128/24, während der gesamte andere Datenverkehr nicht verschlüsselt und nicht über den Tunnel gesendet



wird.

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:/sslclient-win-1.1.4.179.pkg 1
  CISCO STC win2k+ 1.0.0
  1,1,4,179
  Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```

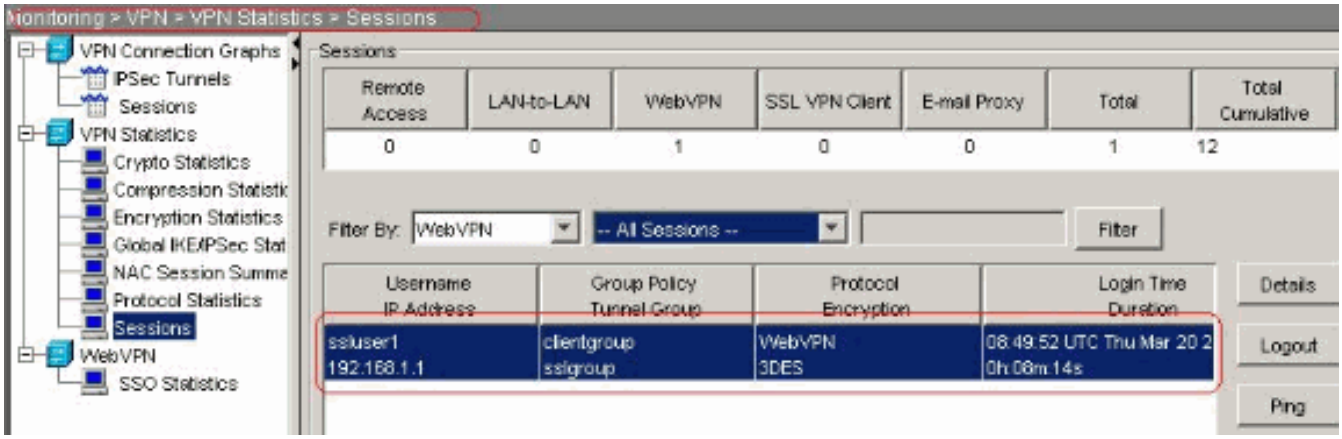
- **show vpn-sessiondb svc**: Zeigt Informationen über die aktuellen SSL-Verbindungen an.

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : SVC                    Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                 Bytes Rx     : 5082
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
Filter Name  :
```

- **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 Informationen über die aktuellen WebVPN-Sitzungen in der ASA zu erhalten.



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
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

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.

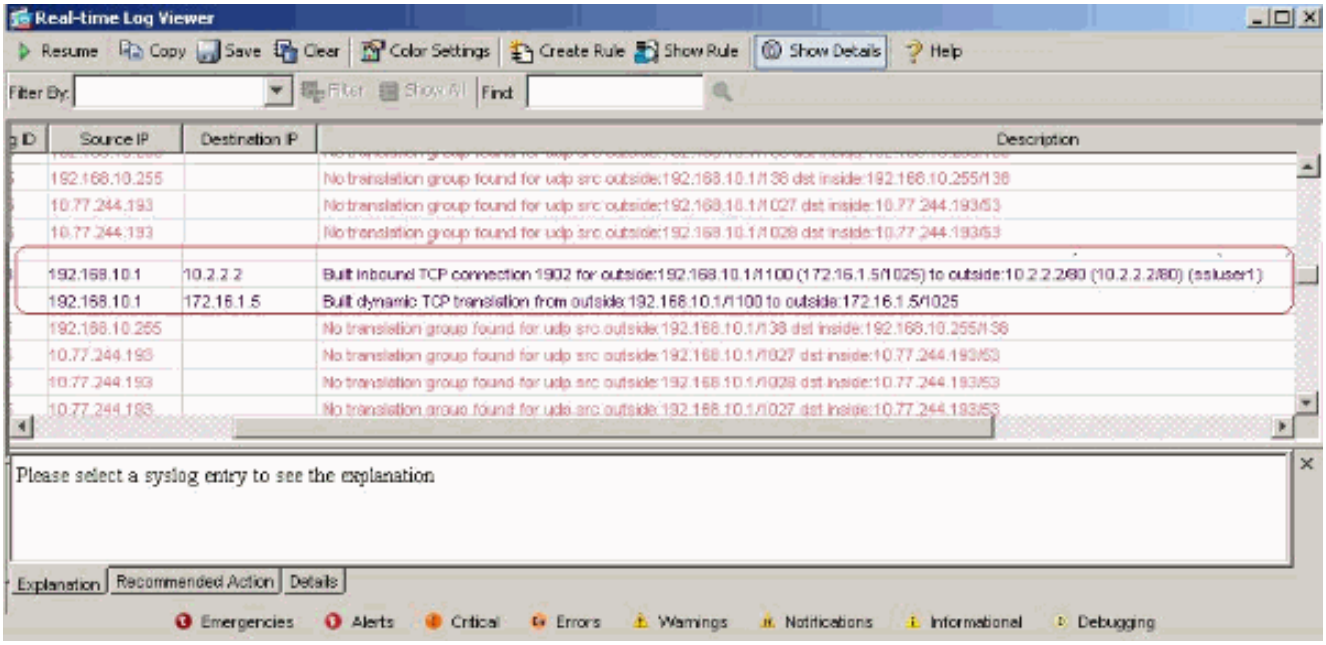
```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL



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

3. **Debug webvpn svc <1-255>**: Stellt die Webvpn-Ereignisse in Echtzeit zum Einrichten der Sitzung bereit.

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -1
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 Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
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: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
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
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

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 die Sitzungsinformationen zwischen dem SVC 192.168.10.1 und dem Webserver 10.2.2.2 im Internet über ASA 172.16.1.5.



Zugehörige Informationen

- Produkt-Support für Cisco Adaptive Security Appliance der Serie 5500
- 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