ASA 7.2(2): SSL VPN Client (SVC) für Public Internet VPN auf einem Stick-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Adaptive Security Appliance (ASA) 7.2.2 einrichten, um SSL-VPN auf einem Stick auszuführen. Diese Konfiguration gilt für einen bestimmten Fall, in dem die ASA Split-Tunneling nicht zulässt und Benutzer eine direkte Verbindung mit der ASA herstellen, bevor sie das Internet nutzen dürfen.

Hinweis: In der ASA-Version 7.2.2 ermöglicht das *Intra-Interface-**Schlüsselwort*** des Konfigurationsmodus **für den Datenverkehr mit identischem Sicherheitsdatenverkehr** den gesamten Datenverkehr, ein- und dieselbe Schnittstelle zu verlassen (nicht nur IPsec-Datenverkehr).

Voraussetzungen

Anforderungen

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

- Die Hub-ASA Security Appliance muss Version 7.2.2 ausführen

- Cisco SSL VPN Client (SVC) 1.x**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 SVC wird auf die Computer der Remote-Benutzer heruntergeladen, um die SSL VPN-Verbindung mit der ASA herzustellen. Weitere Informationen finden Sie im Abschnitt Installation der SVC-Software im *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*.

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
- PC, auf dem Windows 2000 Professional oder Windows XP ausgeführt wird
- 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 der Benutzer die Anmeldung und Authentifizierung erfüllt und die Sicherheits-Appliance den Benutzer als SVC-Benutzer identifiziert, lädt die Sicherheits-Appliance den SVC auf den Remote-Computer herunter. Wenn die Sicherheits-Appliance feststellt, dass der Benutzer die Möglichkeit hat, den SVC zu verwenden, lädt die Sicherheits-Appliance den SVC auf den Remote-Computer herunter und zeigt einen Link auf dem Benutzerbildschirm an, um die SVC-Installation zu überspringen.

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

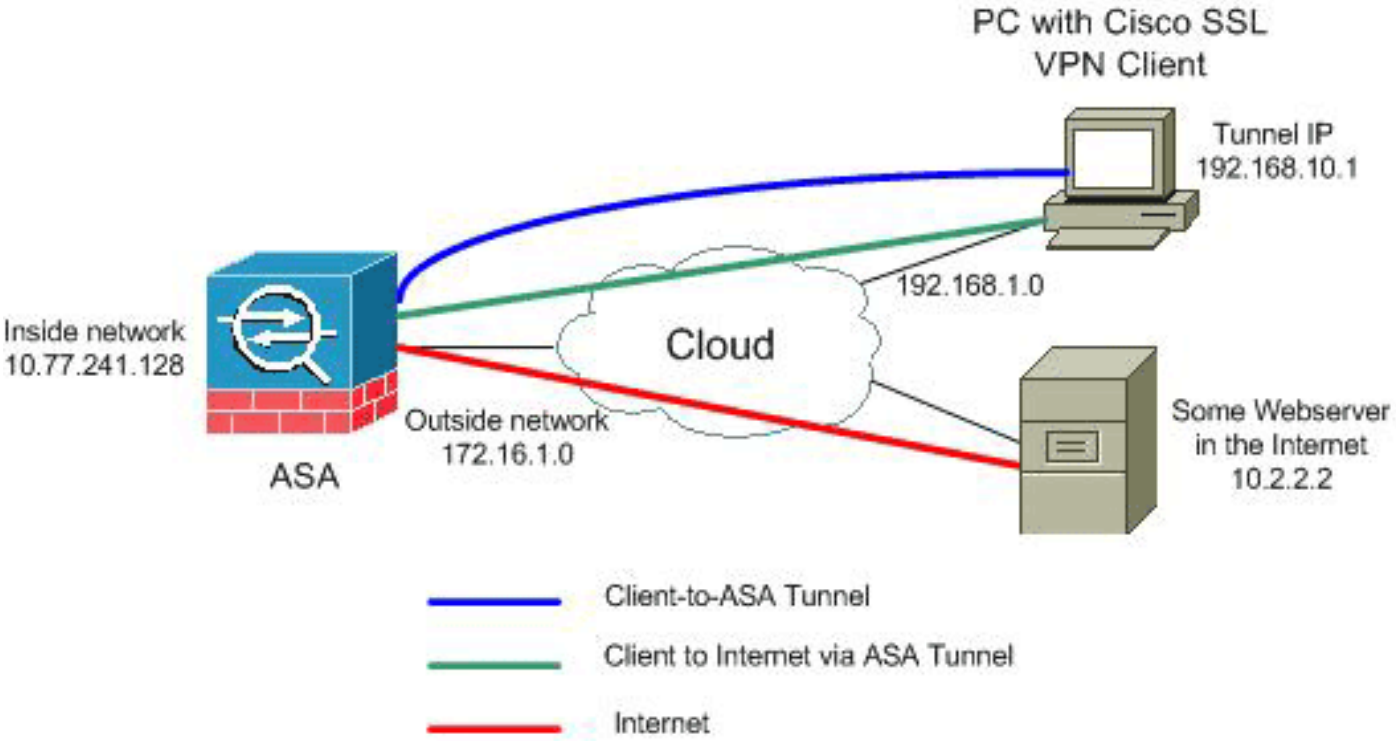
Konfigurieren

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 werden.

ASA 7.2(2)-Konfigurationen mit ASDM 5.2(2)

In diesem Dokument wird davon ausgegangen, dass die Basiskonfigurationen, wie z. B. die Schnittstellenkonfiguration, bereits erstellt wurden und ordnungsgemäß funktionieren.

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

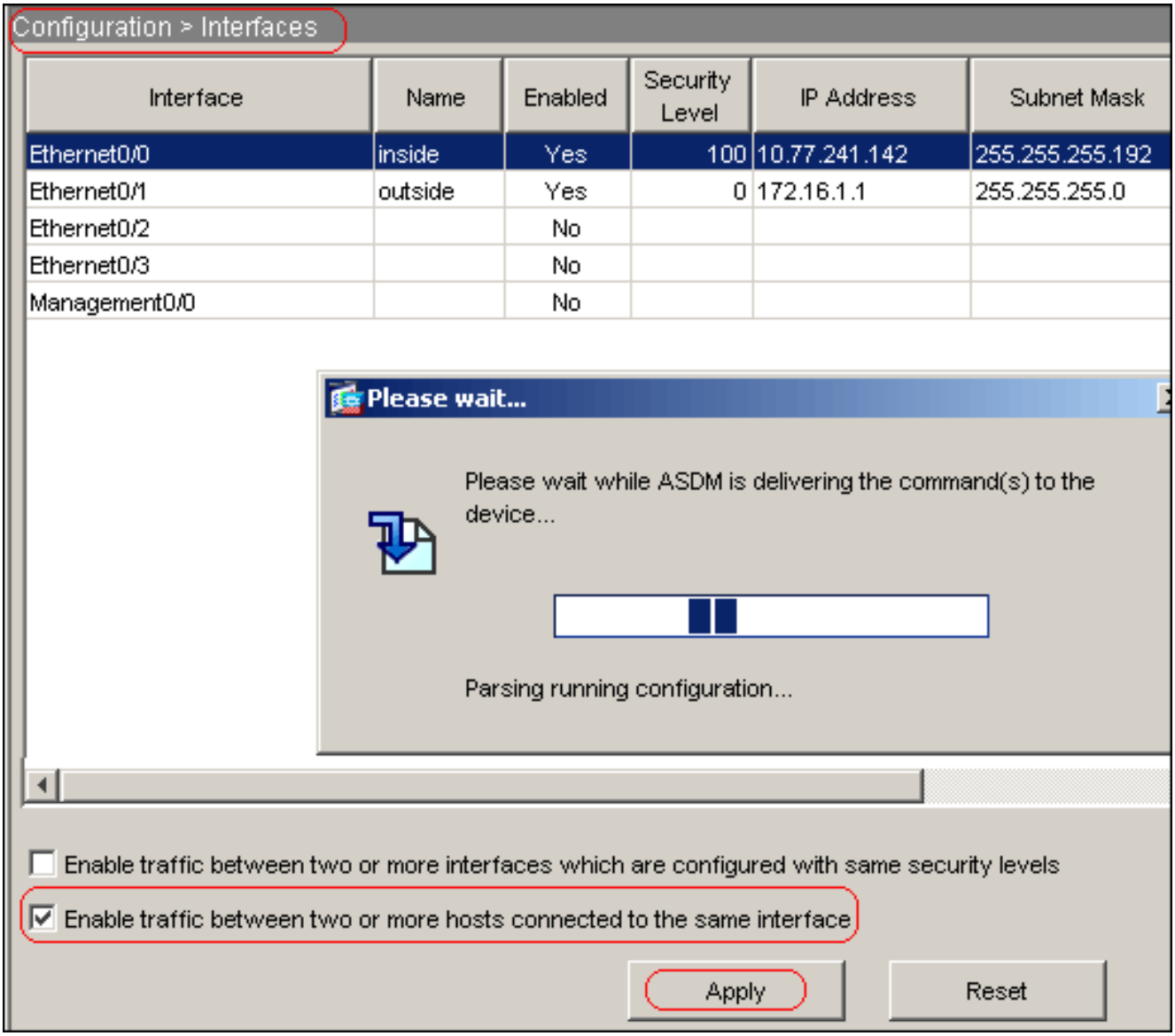
Hinweis: WebVPN und ASDM können nicht auf derselben ASA-Schnittstelle aktiviert werden, es sei denn, Sie ändern die Portnummern. Weitere Informationen finden Sie unter ASDM und WebVPN Enabled auf derselben ASA-Schnittstelle.

Gehen Sie wie folgt vor, um das SSL VPN auf einem Stick in ASA zu konfigurieren:

1. Wählen Sie **Configuration > Interfaces (Konfiguration > Schnittstellen) aus**, und aktivieren Sie das Kontrollkästchen **Enable traffic between two or more hosts connected to the same interface (Datenverkehr zwischen zwei oder mehr Hosts, die mit derselben Schnittstelle verbunden sind,** aktivieren, damit SSL VPN-Datenverkehr dieselbe Schnittstelle betreten und

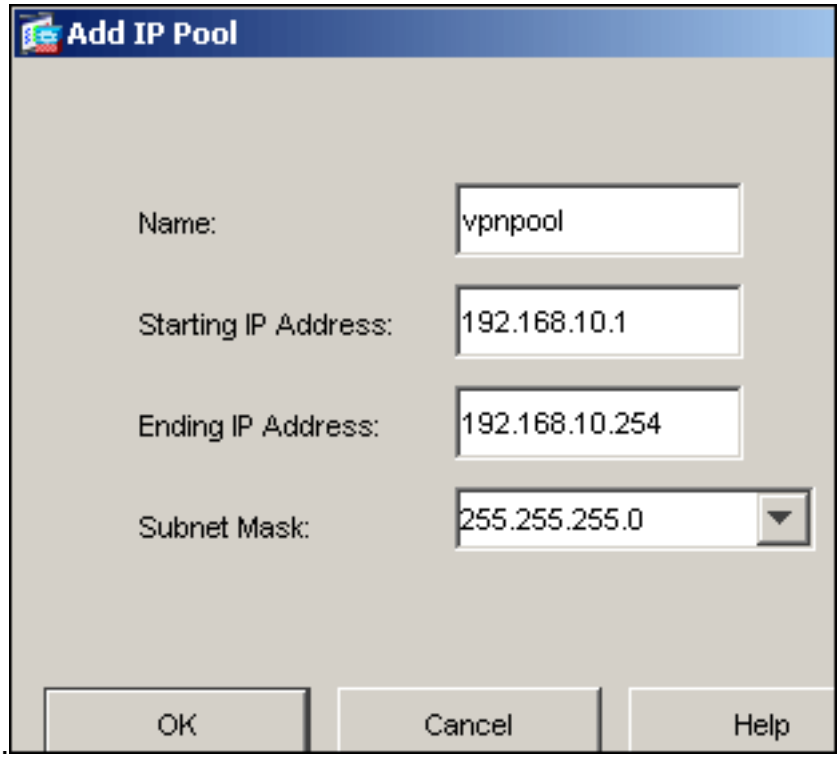
verlassen kann.

2. Klicken Sie auf **Übernehmen**.



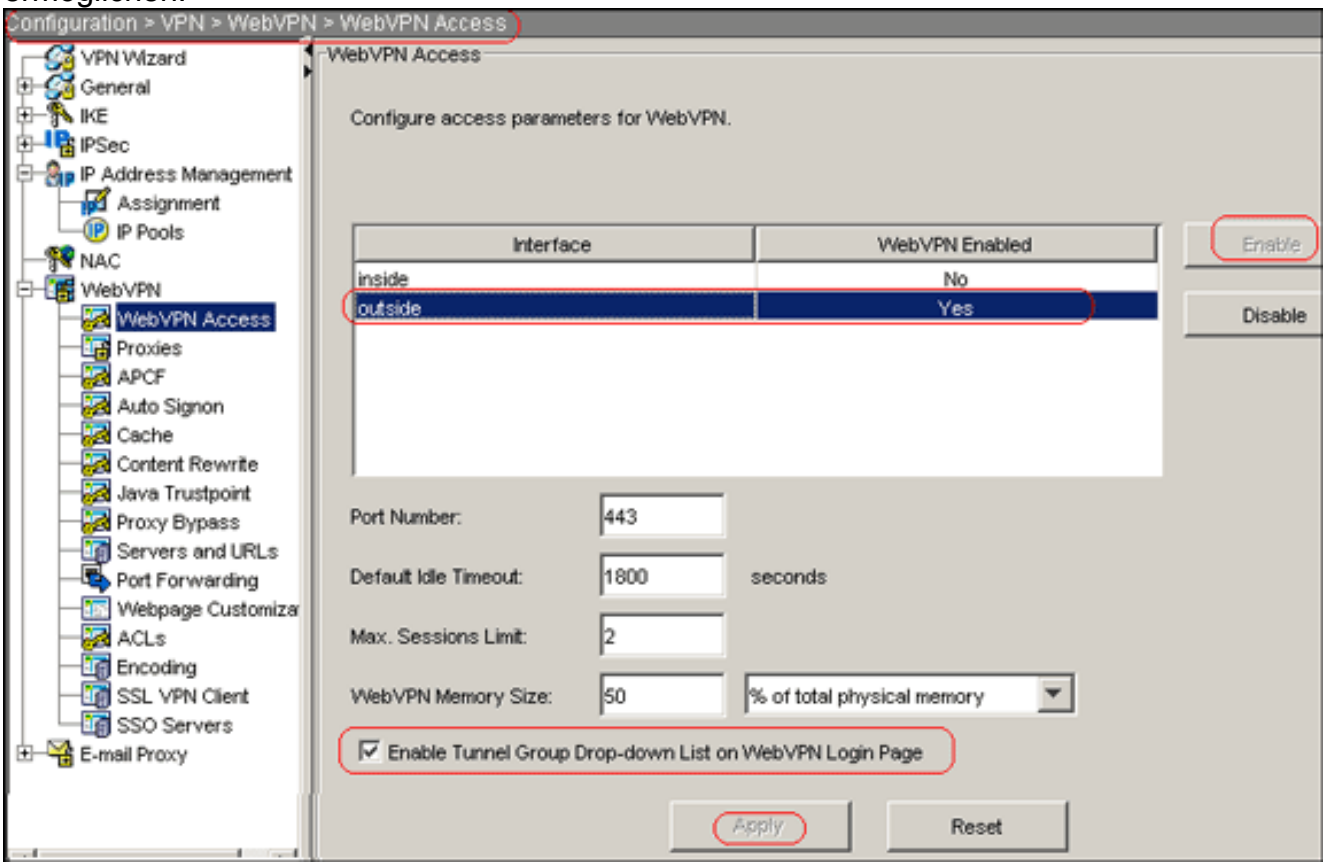
Hinweis: Hier ist der entsprechende CLI-Konfigurationsbefehl:

3. Wählen Sie **Configuration > VPN > IP Address Management > IP Pools > Add** aus, um einen IP-Adresspool mit dem Namen *vpnpool* zu

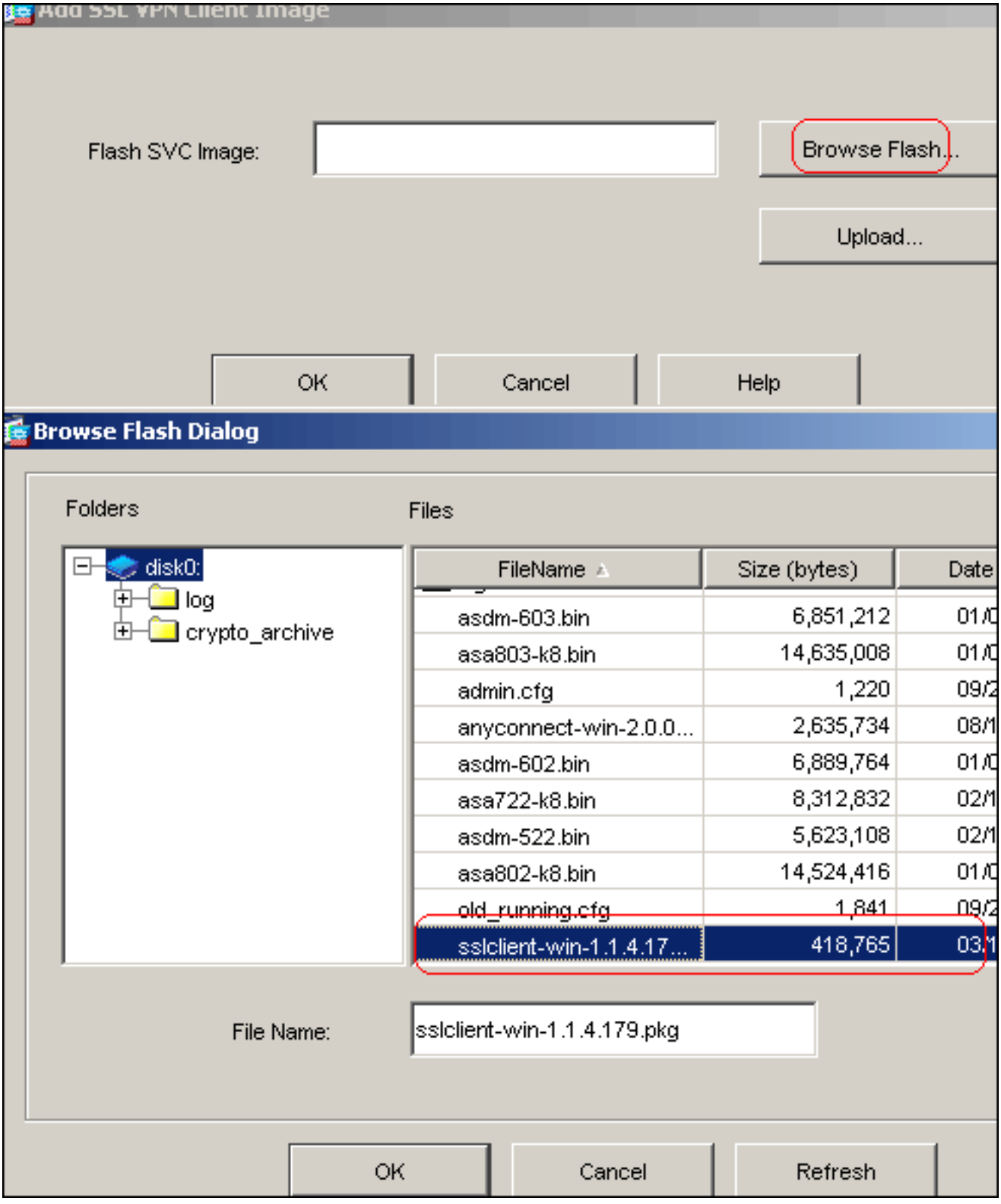


erstellen.

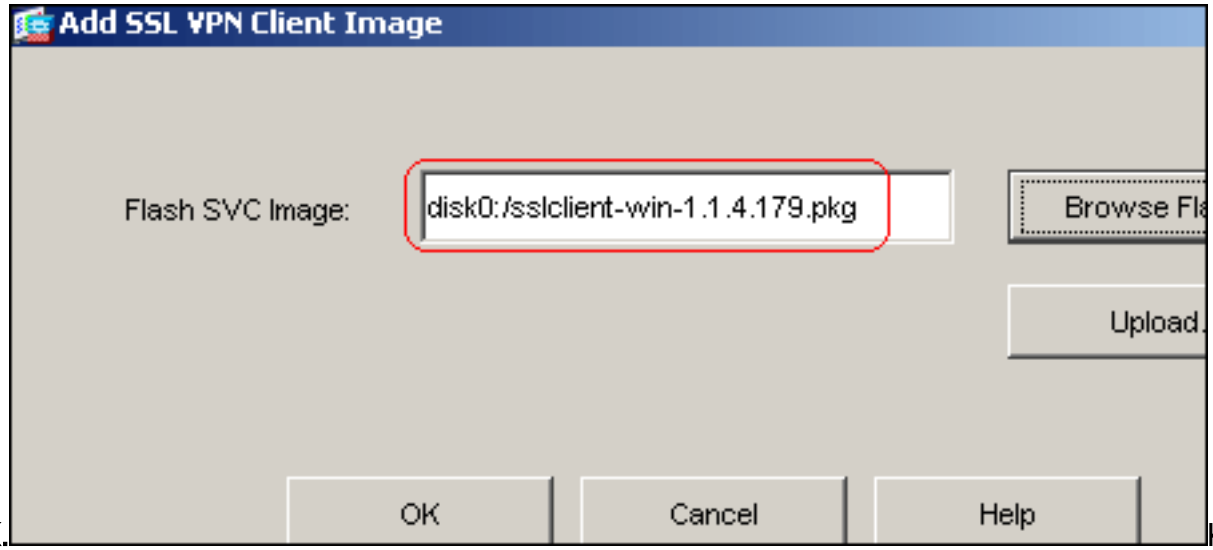
4. Klicken Sie auf **Übernehmen**.**Hinweis:** Hier ist der entsprechende CLI-Konfigurationsbefehl:
5. WebVPN aktivieren:Wählen Sie **Configuration > VPN > WebVPN > WebVPN Access**, und wählen Sie die externe Schnittstelle aus.Klicken Sie auf **Aktivieren**.Aktivieren Sie das Kontrollkästchen **Enable Tunnel Group Drop-Down List on WebVPN Login Page** (**Dropdown-Liste für Tunnelgruppe aktivieren**), um Benutzern die Auswahl der entsprechenden Gruppen auf der Anmeldeseite zu ermöglichen.



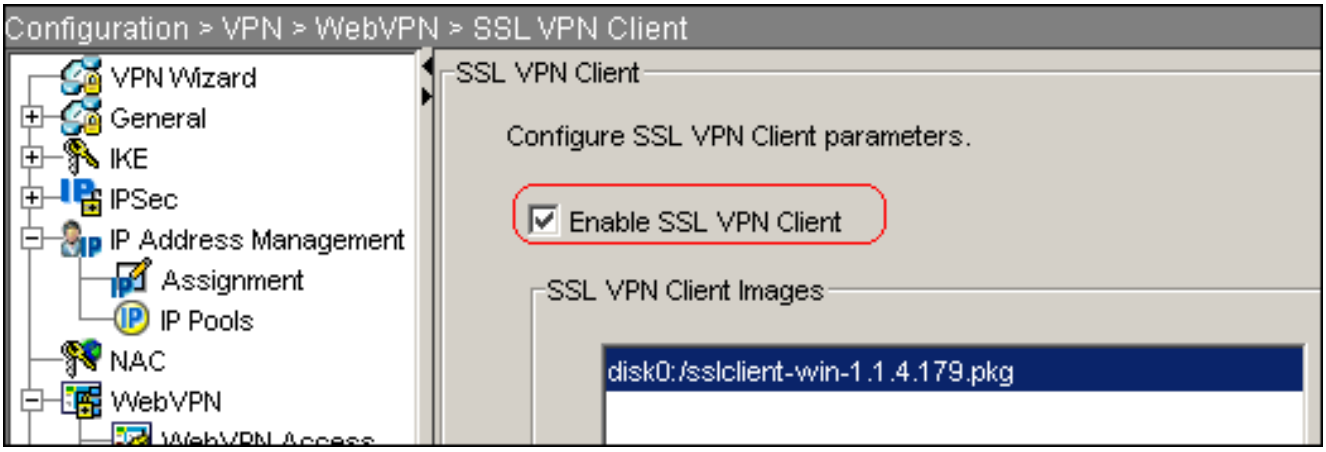
Klicken Sie auf **Übernehmen**.Wählen Sie **Configuration > VPN > WebVPN > SSL VPN Client > Add** aus, um das SSL VPN Client-Image aus dem Flash-Speicher der ASA hinzuzufügen.



Klicken Sie auf

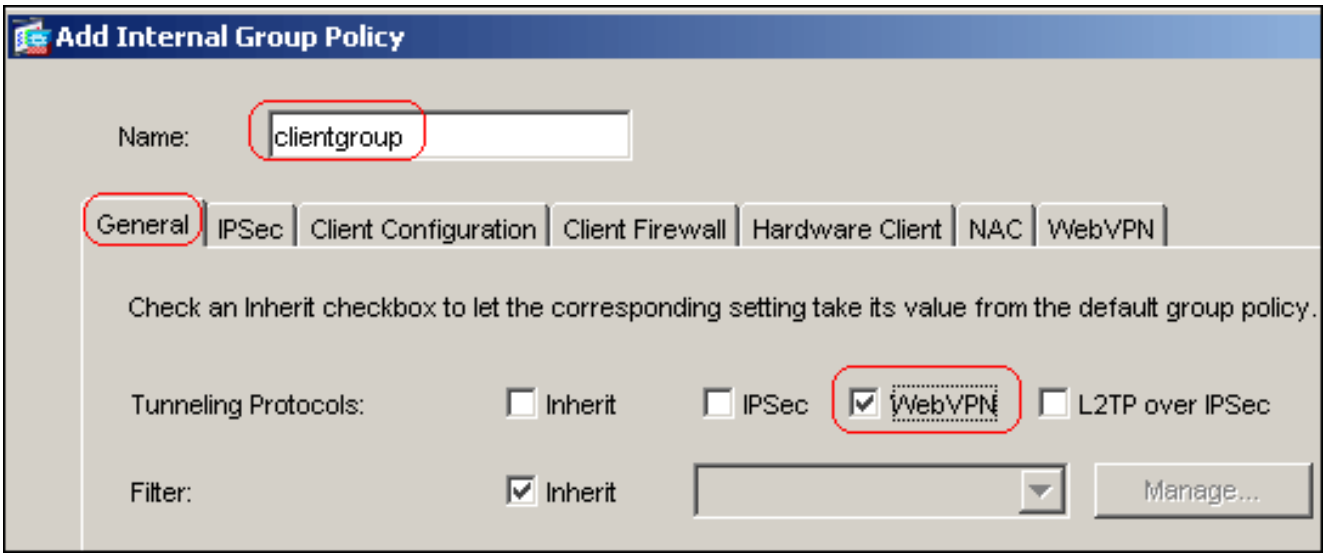


OK. Klicken Sie auf **OK**.Klicken Sie auf das Kontrollkästchen **SSL VPN Client**.



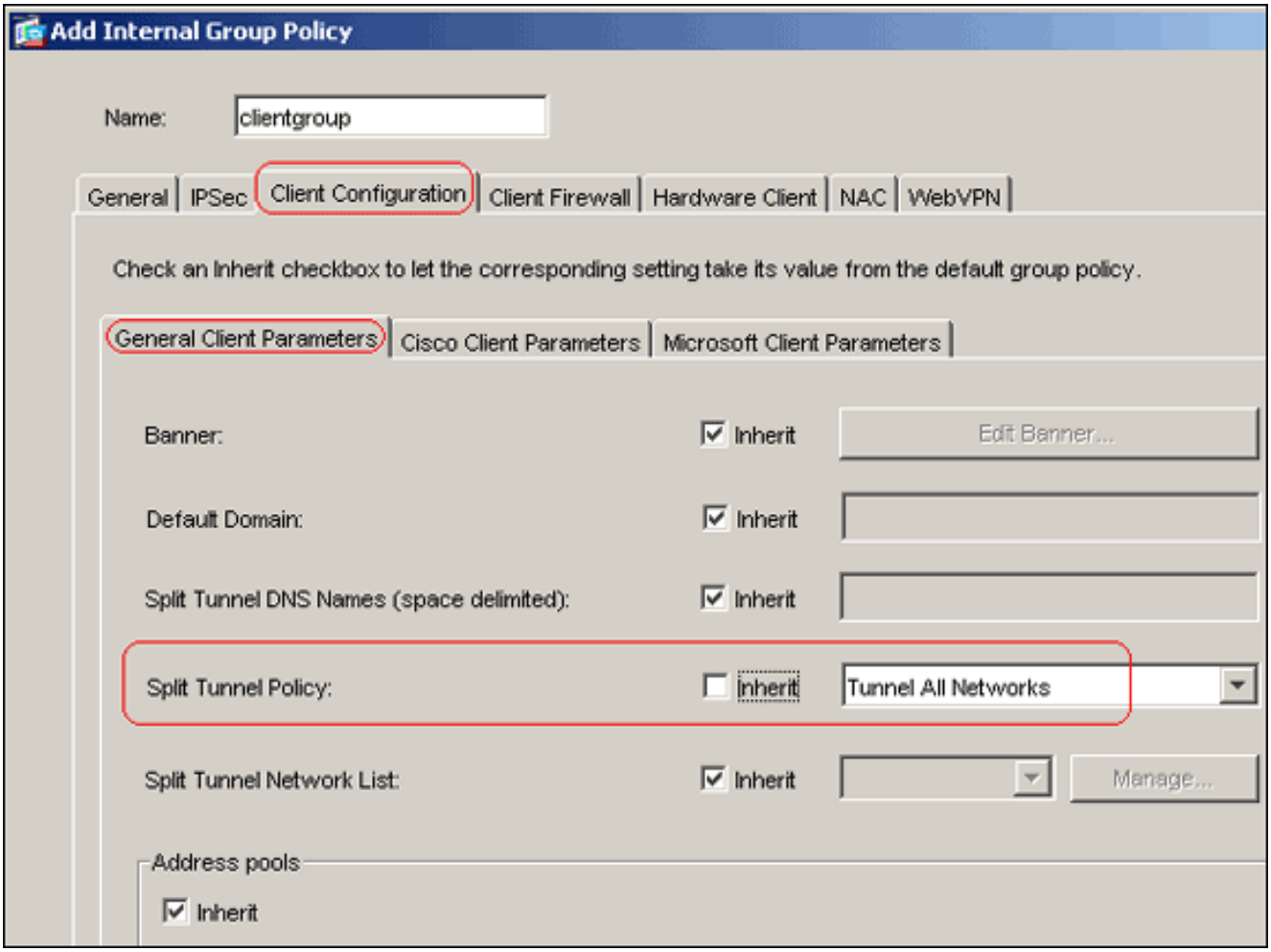
Hinweis: Nachfolgend sind die entsprechenden CLI-Konfigurationsbefehle aufgeführt:

6. Konfigurieren Sie die Gruppenrichtlinie:Wählen Sie **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)**, um eine interne Gruppenrichtlinie mit dem Namen *clientgroup* zu erstellen.Klicken Sie auf die Registerkarte **Allgemein**, und aktivieren Sie das **WebVPN-**Kontrollkästchen, um das WebVPN als Tunneling-Protokoll zu aktivieren.

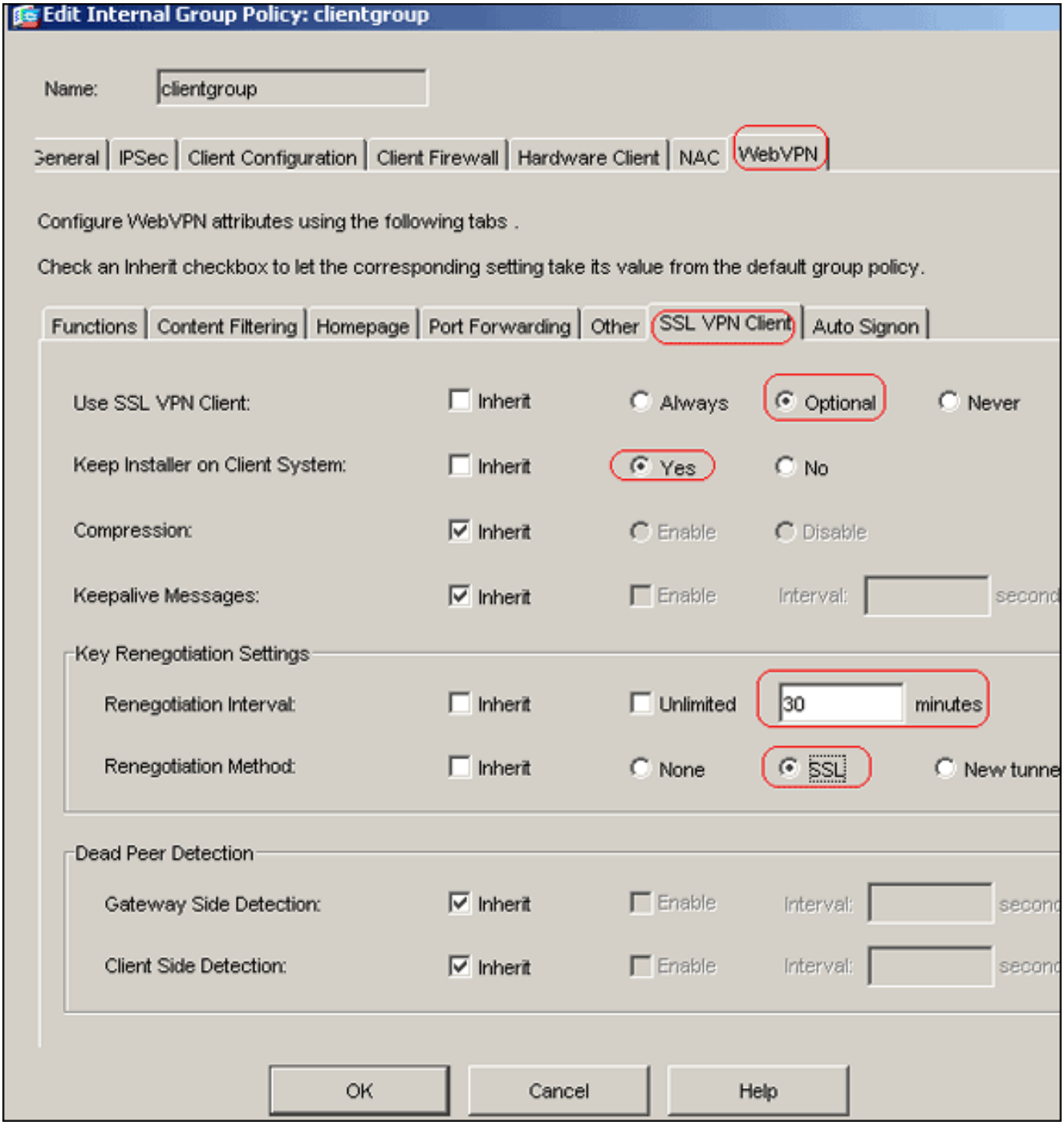


Klicken Sie auf die Registerkarte **Client Configuration** und anschließend auf die Registerkarte **General Client Parameters (Allgemeine Client-Parameter)**.Wählen Sie **Tunnel All Networks** (Alle Netzwerke **Tunnel)** aus der Dropdown-Liste Split Tunnel Policy (Split-Tunnelrichtlinie)

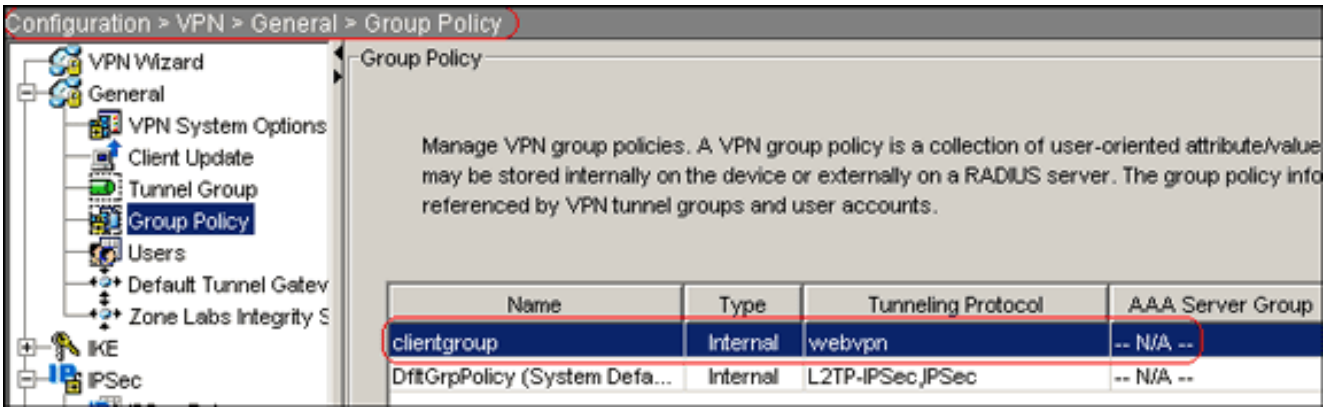
aus, damit alle Pakete vom Remote-PC über einen sicheren Tunnel übertragen werden.



Klicken Sie auf die Registerkarte **WebVPN > SSL VPN Client**, und wählen Sie folgende Optionen aus:Deaktivieren Sie für die Option SSL VPN-Client verwenden das Kontrollkästchen **Erben**, und klicken Sie auf das **Optionsfeld Optional**.Mit dieser Option kann der Remote-Client auswählen, ob er den SVC herunterladen soll oder nicht. 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.**Mit dieser Option 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.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.**Hinweis:** Die Sicherheit wird durch Festlegen von Beschränkungen für die Gültigkeitsdauer eines Schlüssels erhöht.Deaktivieren Sie für die Option Methode der Neuverhandlung das Kontrollkästchen **Erben**, und klicken Sie auf das **SSL-**Optionsfeld.**Hinweis:** 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:



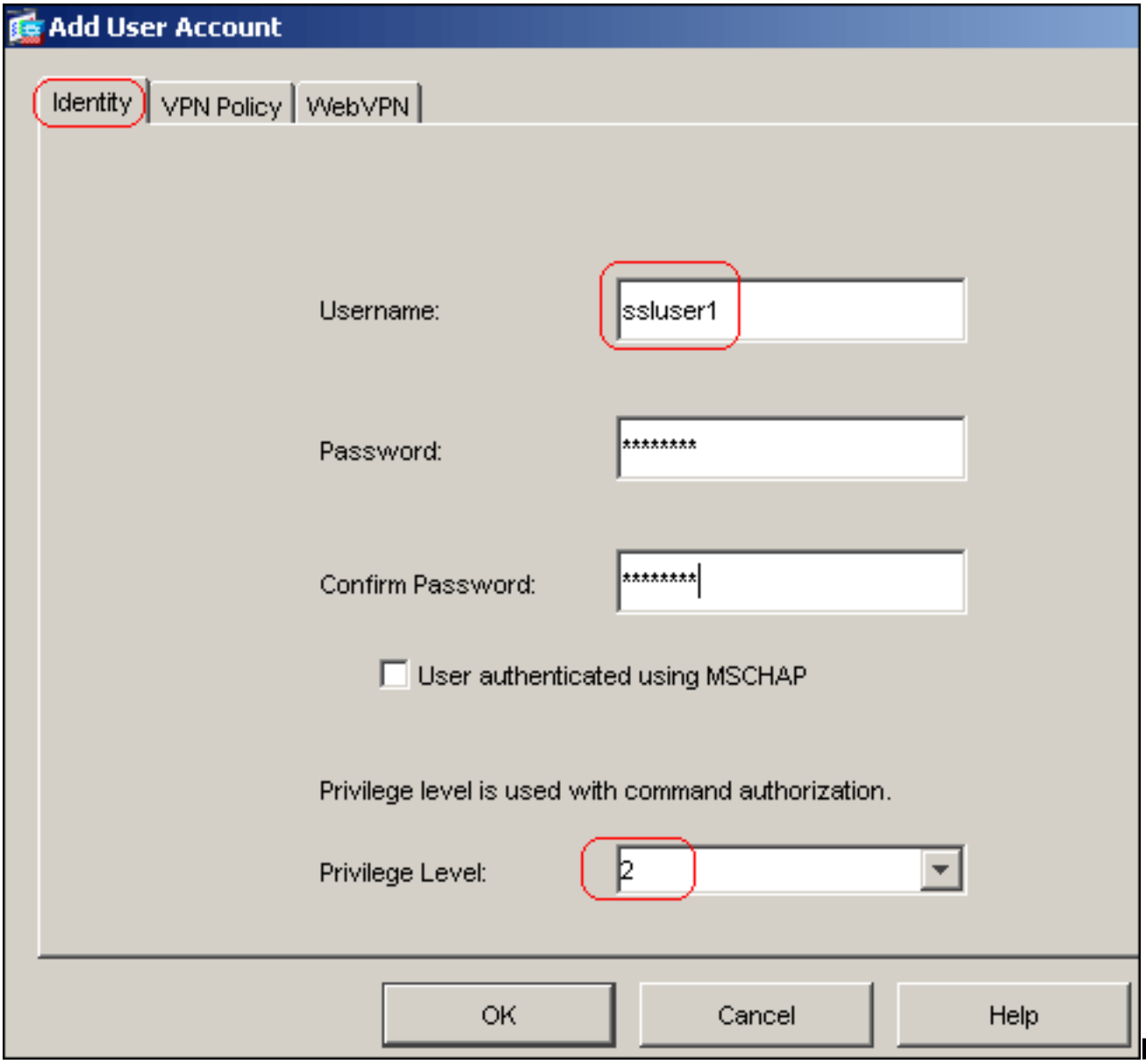
Klicken Sie auf **OK** und dann auf **Übernehmen**.



Hinweis: Nachfolgend sind die entsprechenden CLI-Konfigurationsbefehle aufgeführt:

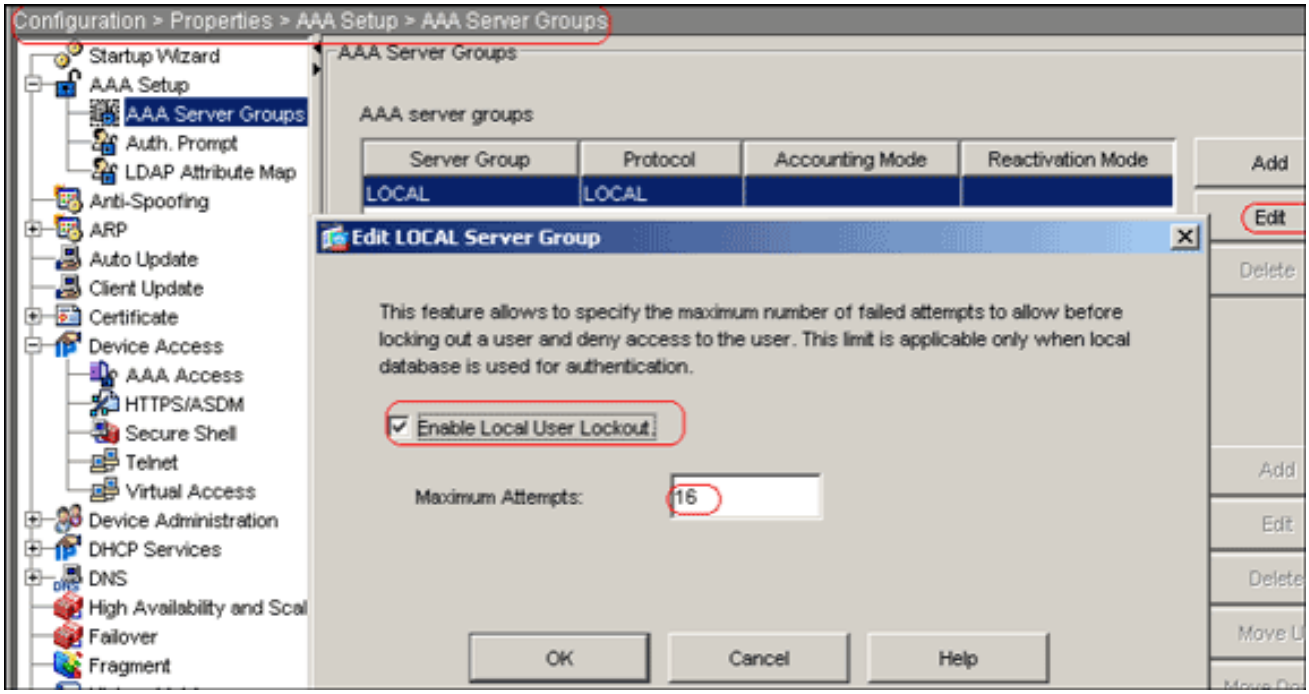
7. Wählen Sie **Configuration > VPN > General > Users > Add**, um ein neues Benutzerkonto *ssluser1* zu erstellen.

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



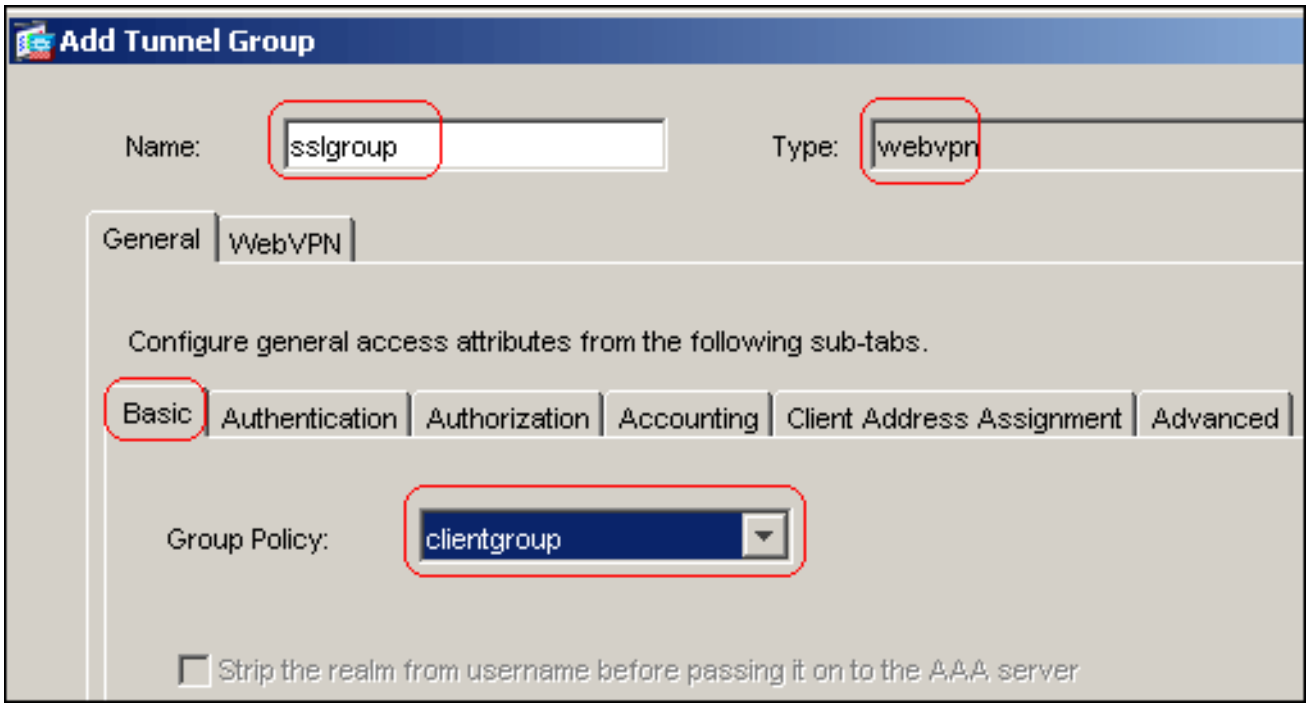
Hinweis: Hier ist der entsprechende CLI-Befehl:

9. Wählen Sie **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit aus**.
10. Wählen Sie die Standardservergruppe *LOCAL aus*, und klicken Sie auf **Edit**.
11. Klicken Sie im Dialogfeld LOKALE Servergruppe bearbeiten auf das Kontrollkästchen **Lokale Benutzersperre aktivieren**, und geben Sie im Textfeld Maximale Versuche 16 ein.
12. Klicken Sie auf **OK**.

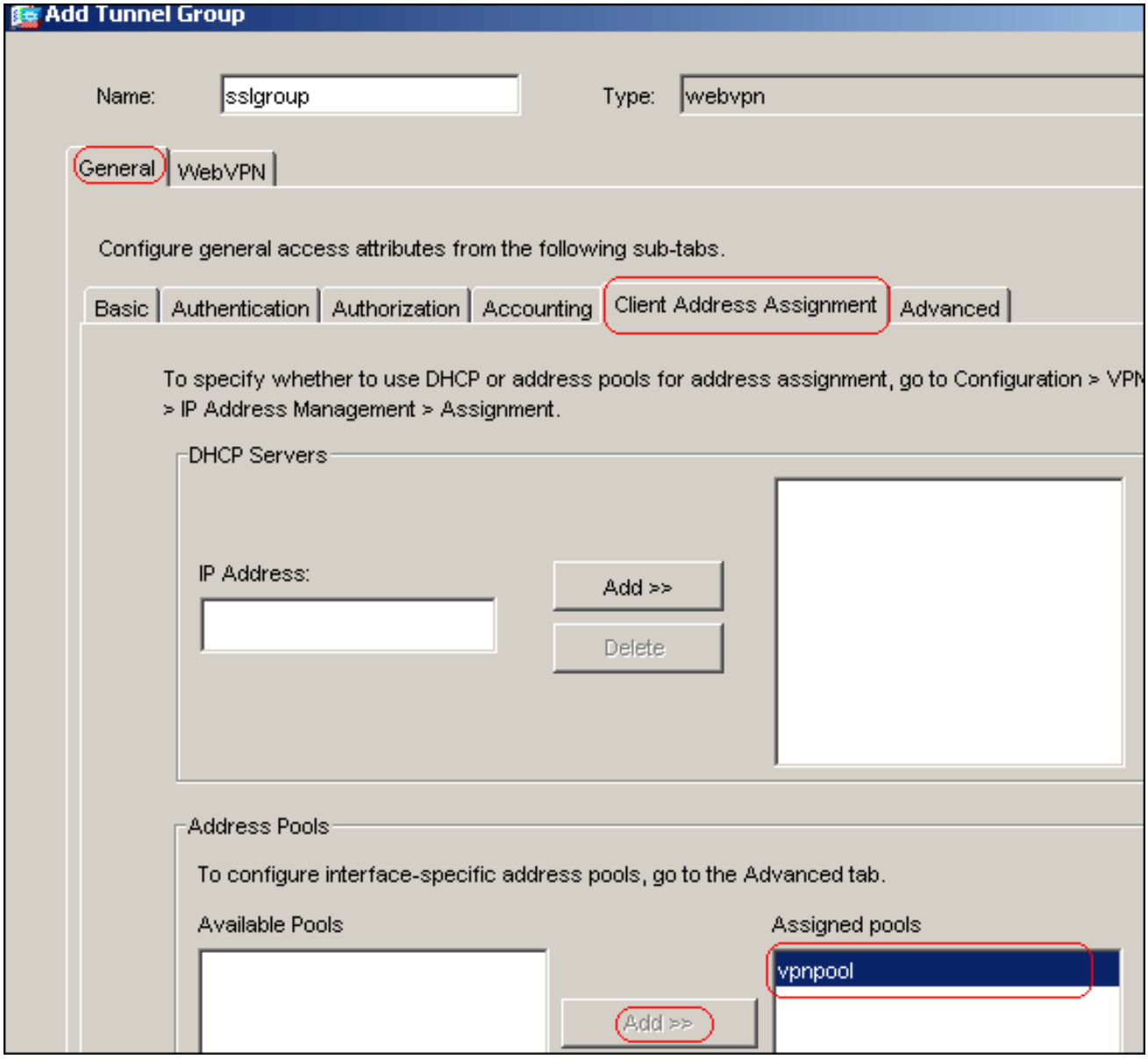


Hinweis: Hier ist der entsprechende CLI-Befehl:

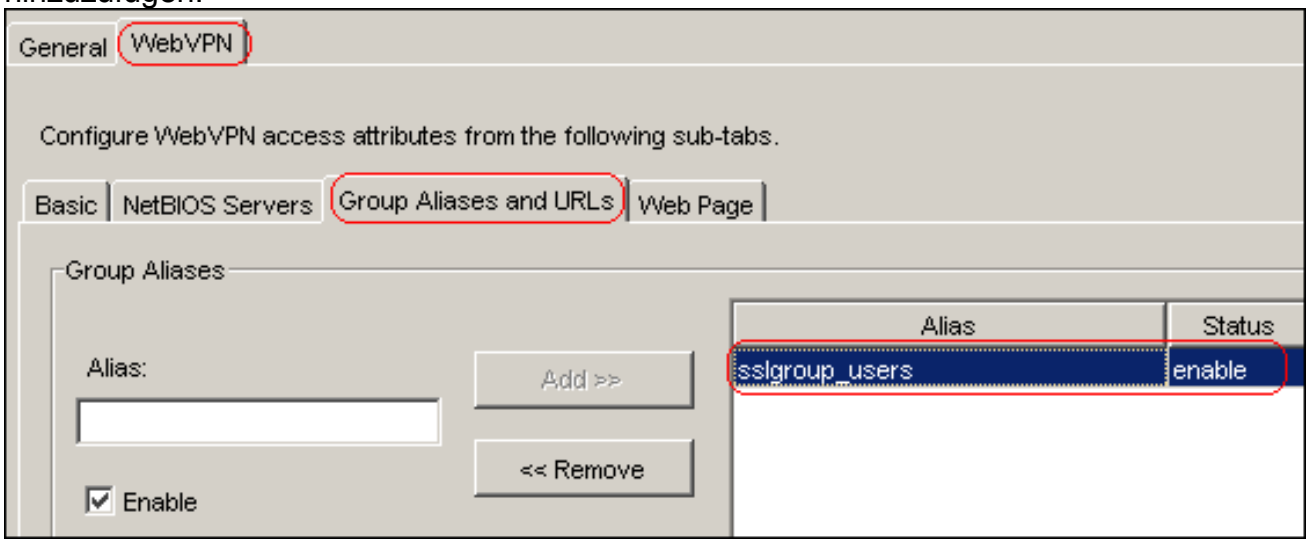
13. Konfigurieren Sie die Tunnelgruppe:Wählen Sie **Configuration > VPN > General > Tunnel Group > Add(WebVPN access)**, um eine neue Tunnelgruppe namens *sslgroup* zu erstellen.Klicken Sie auf die Registerkarte **Allgemein** und anschließend auf die Registerkarte **Grundlegend**.Wählen Sie **clientgroup** aus der Dropdown-Liste Gruppenrichtlinie
aus.



Klicken Sie auf die Registerkarte **Client Address Assignment (Client-Adressenzuweisung)** und dann auf **Add (Hinzufügen)**, um den verfügbaren *vPnpool* für den Adresspool zuzuweisen.



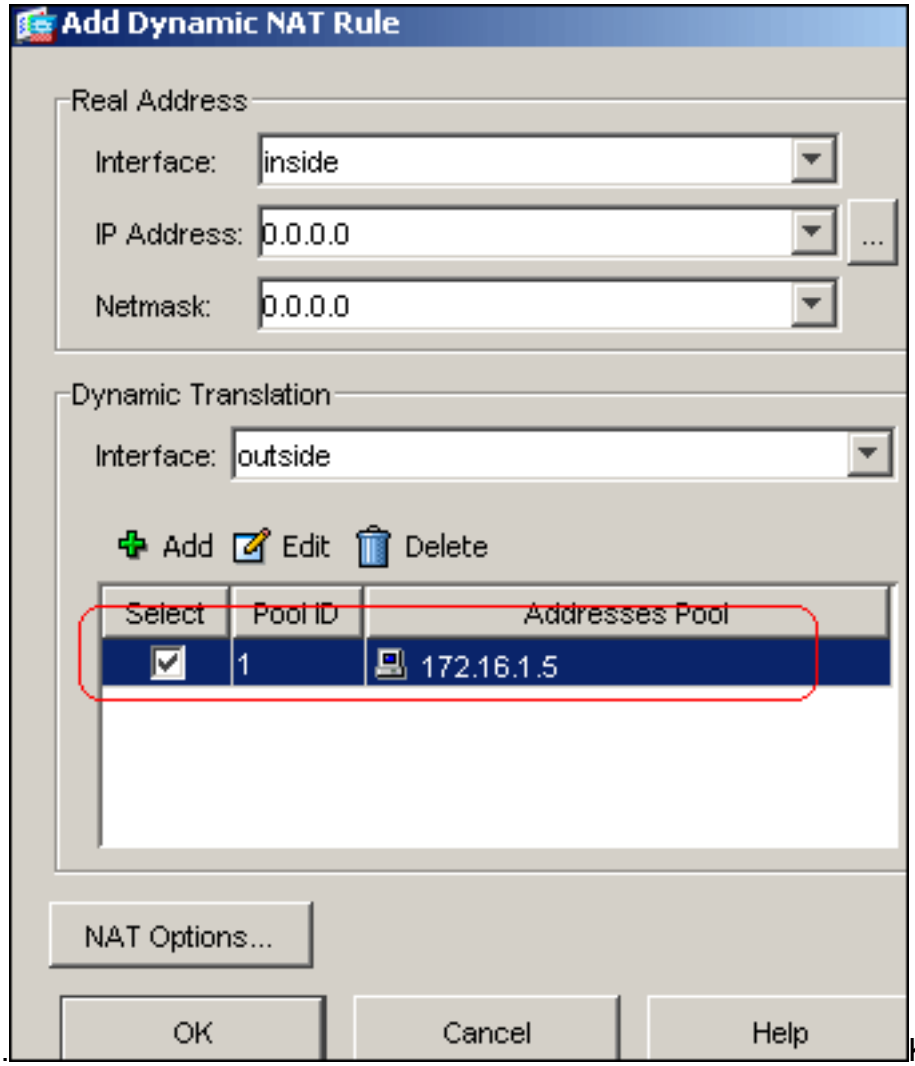
Klicken Sie auf die Registerkarte **WebVPN** und anschließend auf die Registerkarte **GruppenAliase und URLs**.Geben Sie den Aliasnamen in das Parameterfeld ein, und klicken Sie auf **Hinzufügen**, um ihn der Liste der Gruppennamen auf der Anmeldeseite hinzuzufügen.



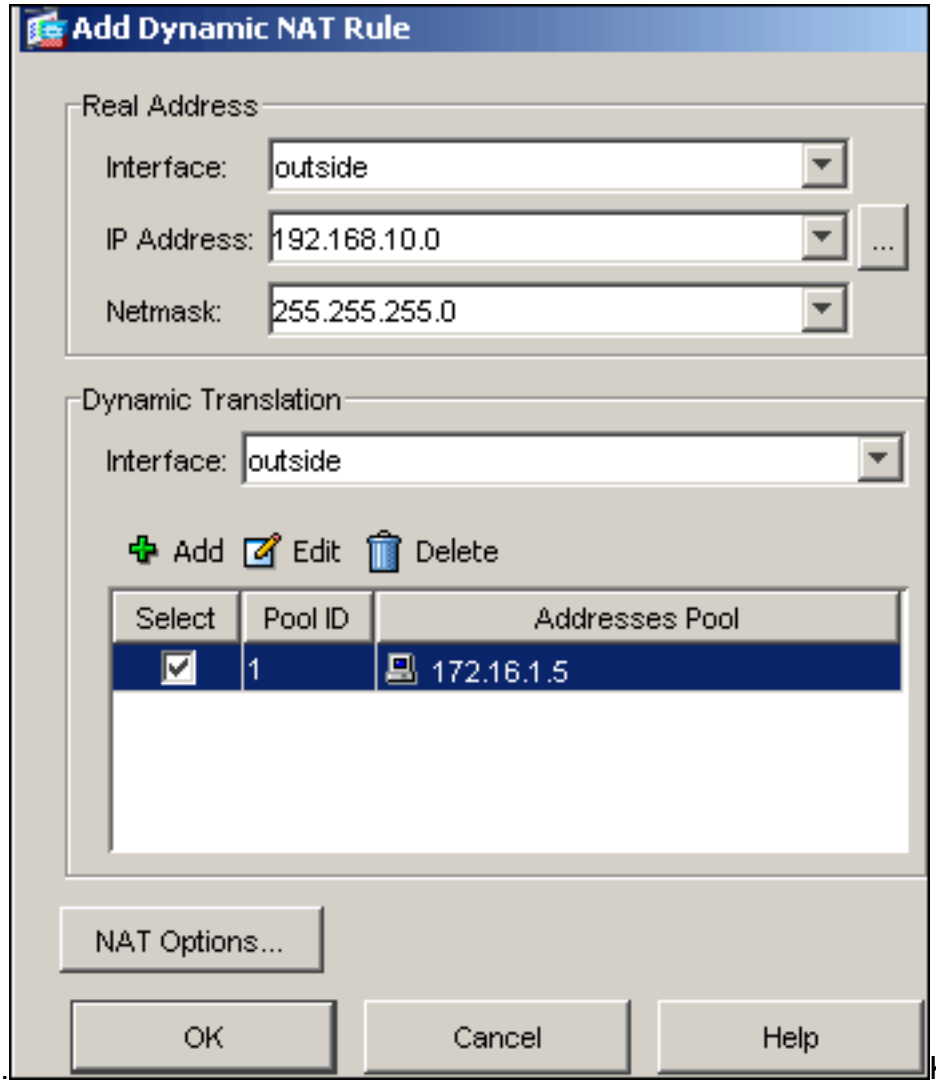
Klicken Sie auf **OK** und dann auf **Übernehmen**.**Hinweis:** Nachfolgend sind die entsprechenden CLI-Konfigurationsbefehle aufgeführt:

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

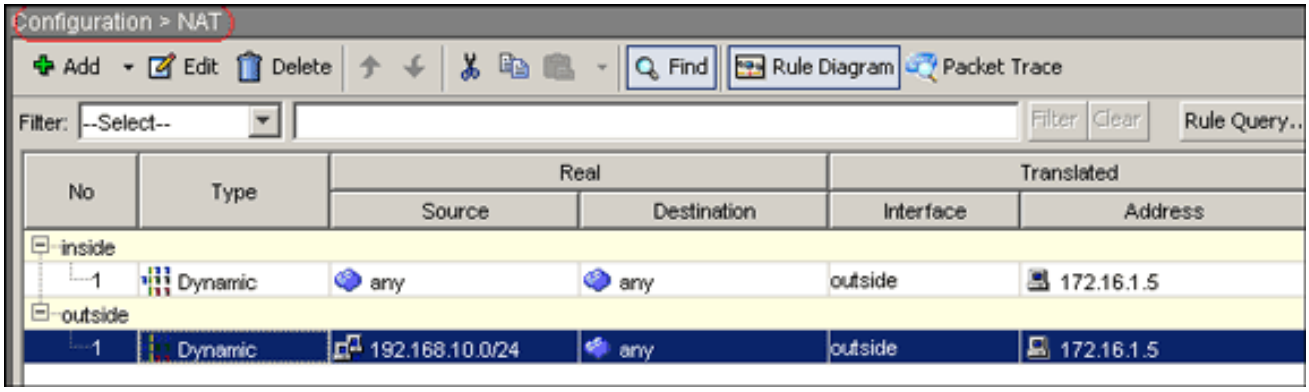
(Konfiguration > NAT > Hinzufügen > Dynamische NAT-Regel hinzufügen, damit der aus dem internen Netzwerk stammende Datenverkehr mithilfe der externen IP-Adresse 172.16.1.5 übersetzt werden



kann. Klicken Sie auf **OK**.Wählen Sie **Configuration > NAT > Add > Add Dynamic NAT Rule (Konfiguration > NAT > Hinzufügen > Dynamische NAT Rule (NAT hinzufügen)**, damit der Datenverkehr aus dem externen Netzwerk 192.168.10.0 mithilfe der externen IP-Adresse 172.16.1.5 übersetzt



werden kann. Klicken Sie auf **OK**.



Klicken Sie auf **Übernehmen**.**Hinweis:** Nachfolgend sind die entsprechenden CLI-Konfigurationsbefehle aufgeführt:

CLI-Konfiguration für ASA 7.2(2)

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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any 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) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

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
```

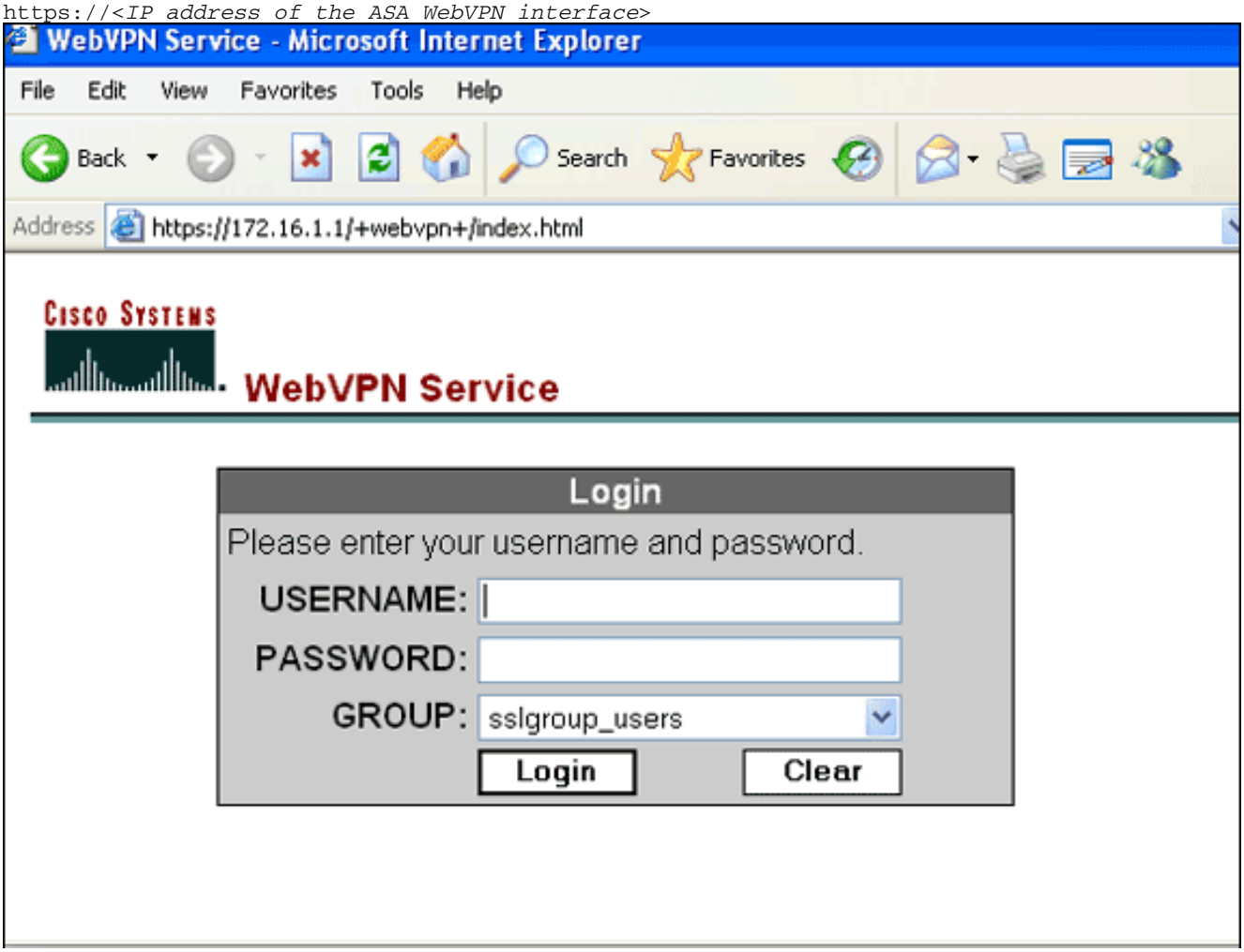
```
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

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

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. 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, 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. 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#
```

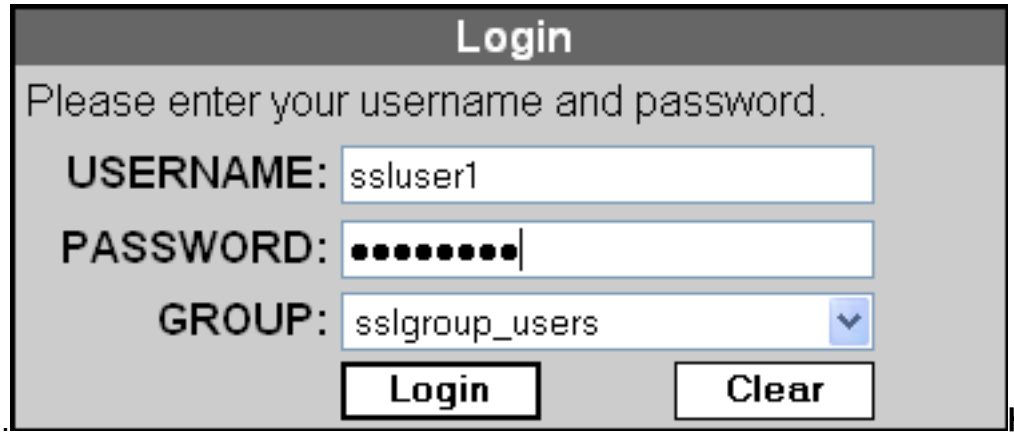
Einrichtung der SSL VPN-Verbindung mit SVC

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

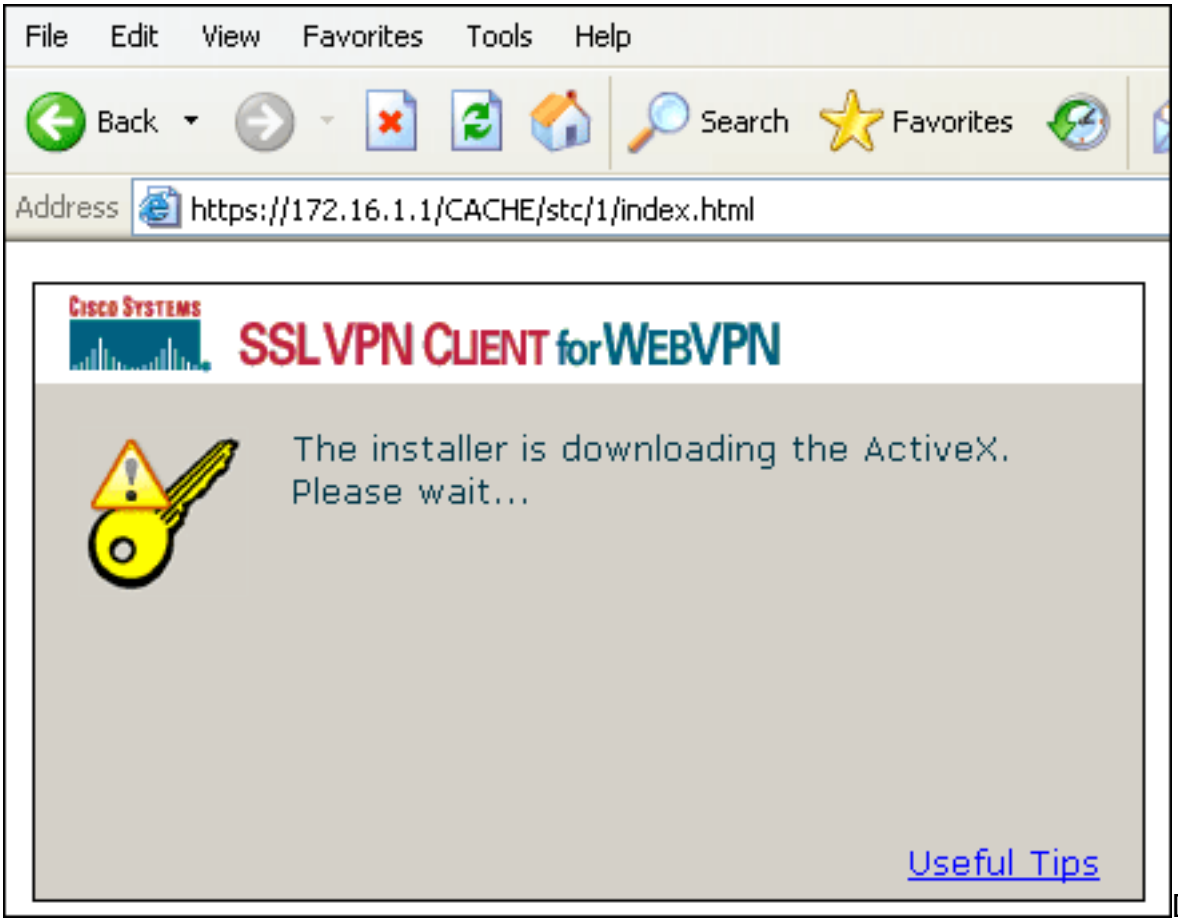
1. Geben Sie im Adressfeld Ihres Webbrowsers die URL oder IP-Adresse für die WebVPN-Schnittstelle der ASA ein.Beispiel:
   `https://<IP address of the ASA WebVPN interface>`



2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und wählen Sie dann in der Dropdown-Liste "Gruppe" die gewünschte Gruppe

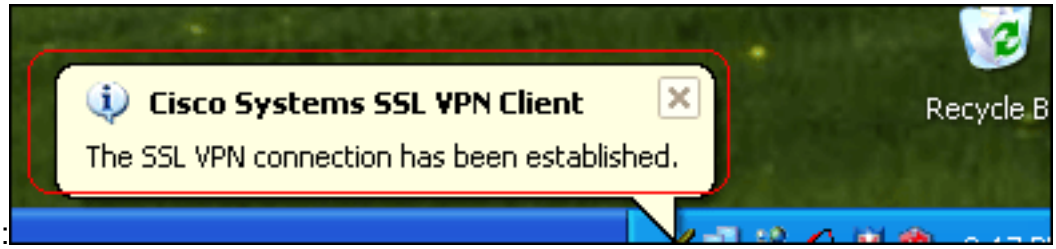


aus.**Hinweis:** Die ActiveX-Software muss auf Ihrem Computer installiert sein, bevor Sie den SSL VPN-Client herunterladen.

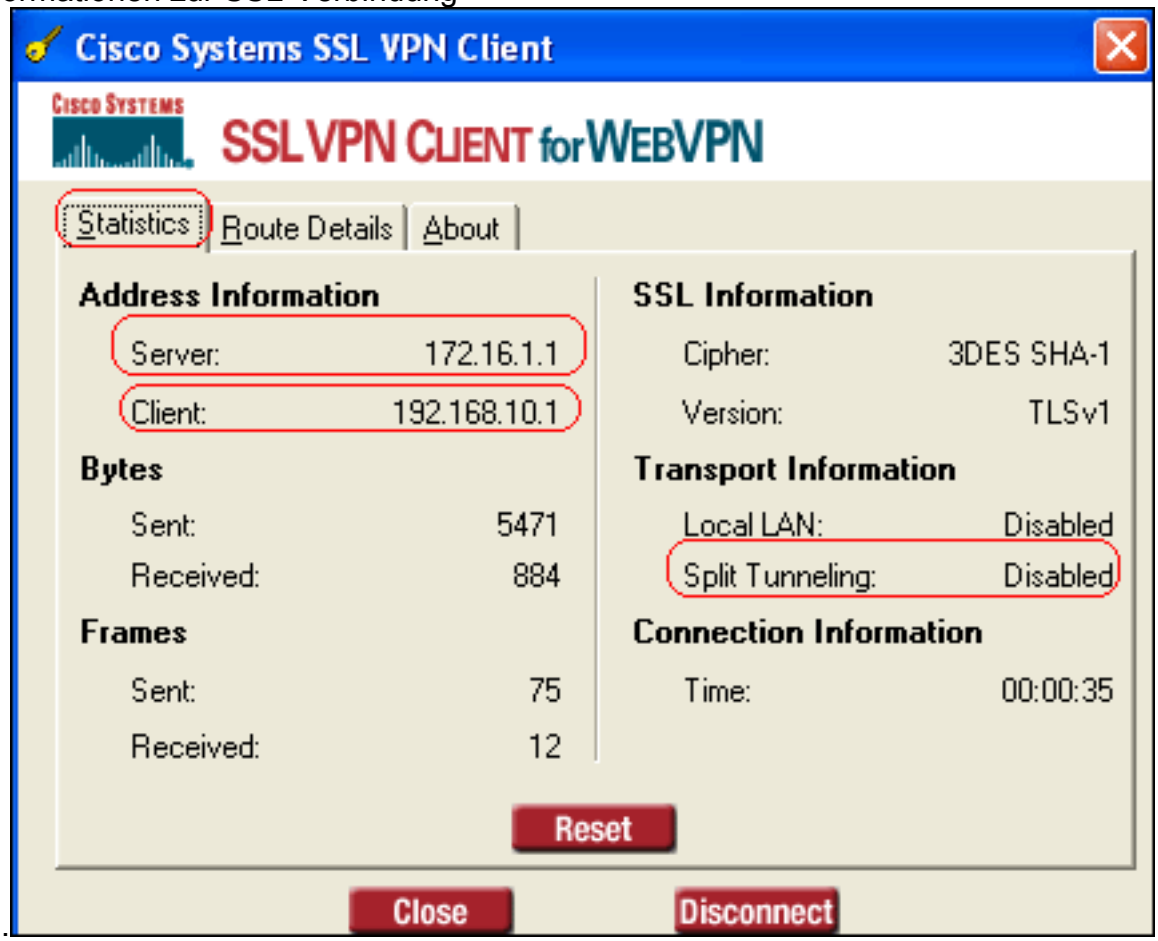


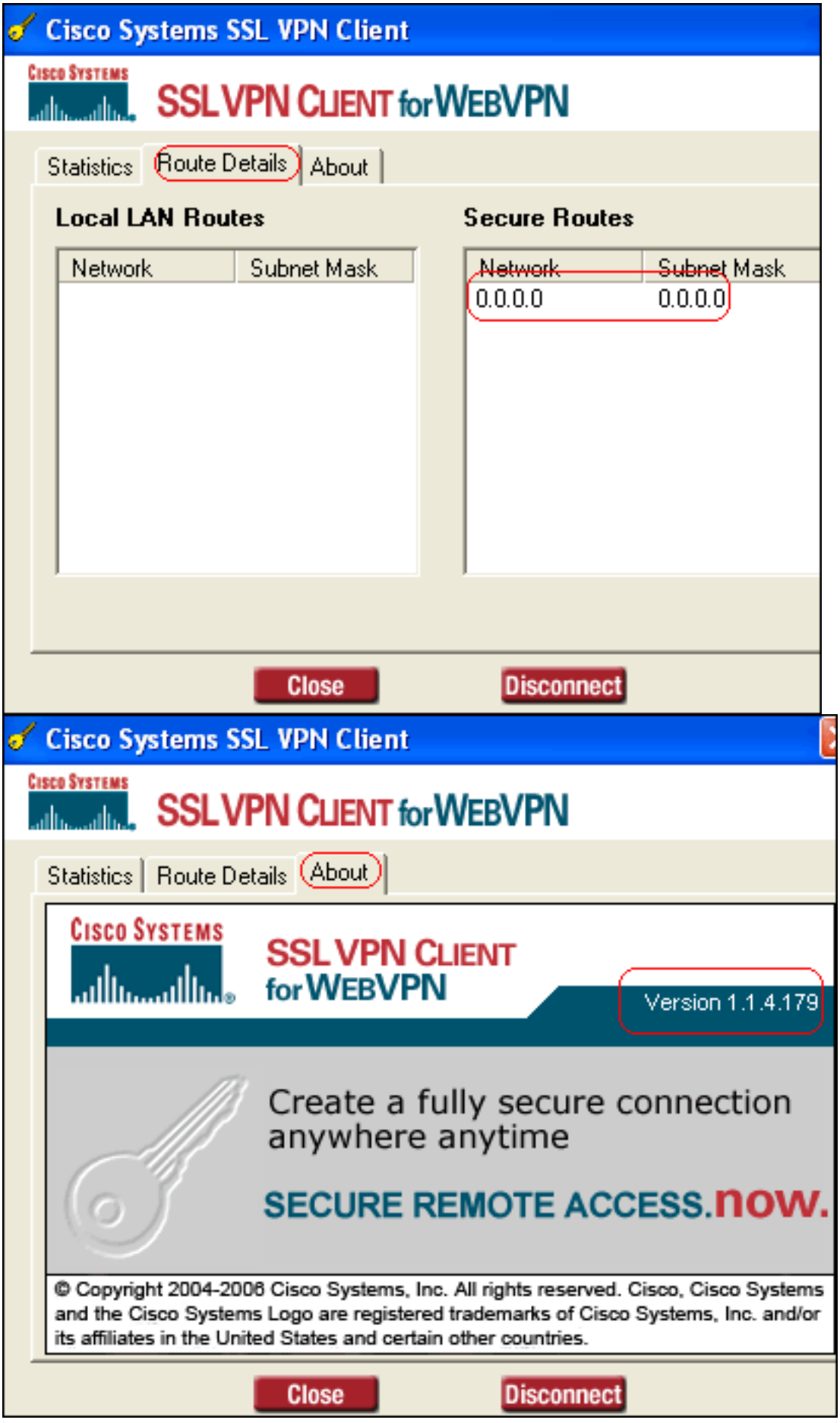
Dieses Dialogfeld wird angezeigt, wenn die Verbindung hergestellt

wurde:Diese Meldung wird angezeigt, sobald die Verbindung hergestellt

wurde: 

3. Doppelklicken Sie nach dem Herstellen der Verbindung auf das gelbe Symbol in der Taskleiste Ihres Computers.Das Dialogfeld Cisco Systems SSL VPN Client zeigt Informationen zur SSL-Verbindung

an. 



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
```

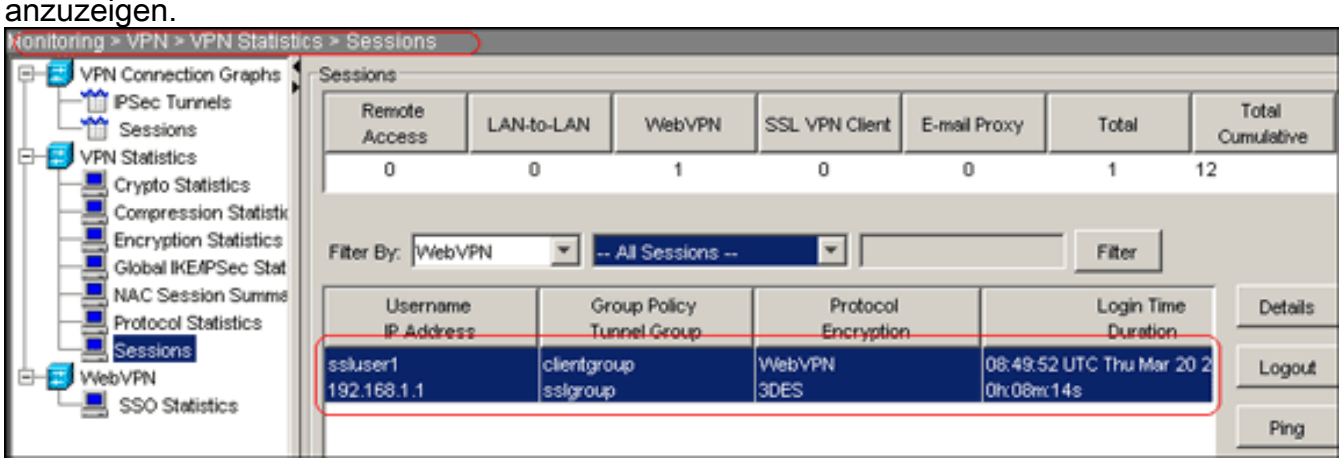
- **show vpn-sessiondb svc**: Zeigt Informationen über die aktuellen SSL-Verbindungen an.

```
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 anzuzeigen.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- **vpn-sessiondb-Protokollname <*Benutzername*>** - Ermöglicht Ihnen, sich bei der SSL VPN-Sitzung für den angegebenen Benutzernamen abzumelden.

```
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.**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
```

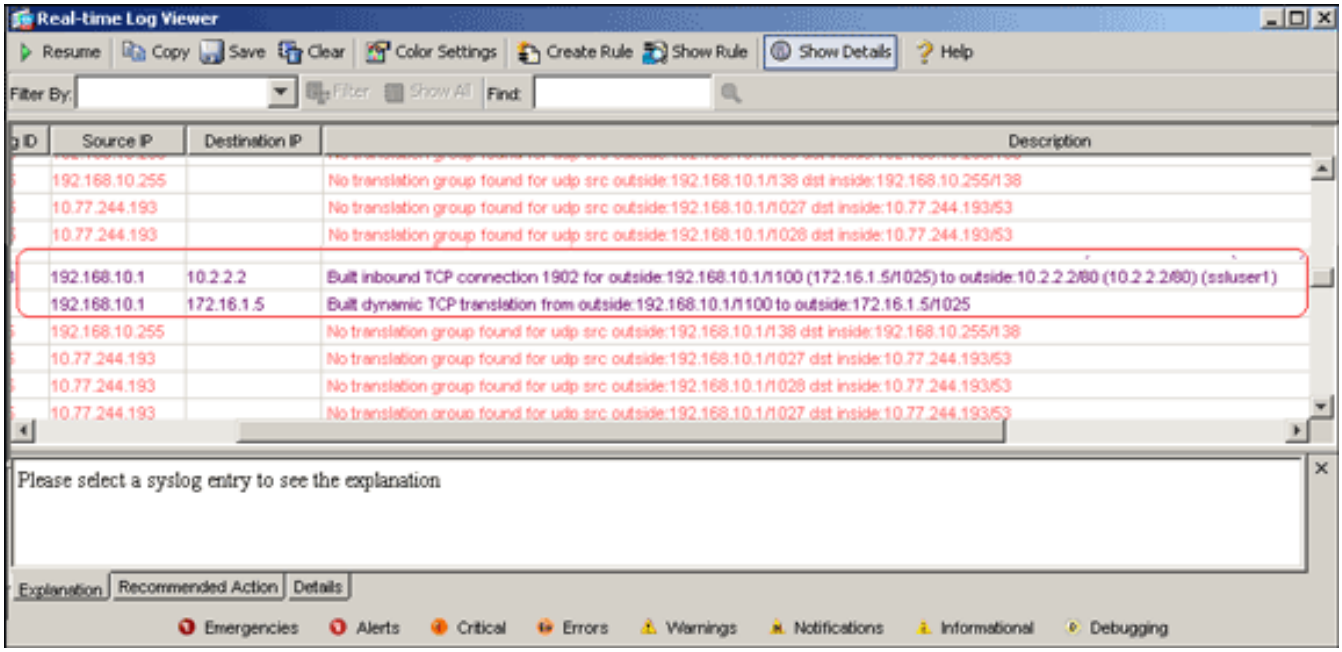
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **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
```

- Wählen Sie im ASDM **Monitoring > Logging > Real-time Log Viewer > View (Überwachung > Anmeldung > Echtzeit-Protokollanzeige > Ansicht**, um die Ereignisse in Echtzeit anzuzeigen. Diese Beispiele zeigen 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

- Support-Seite für Cisco Adaptive Security Appliances der Serie 5500
- 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