ASA 7.1/7.2： ASA の SVC に対するスプリット トンネリングの許可の設定例

目次

概要

このドキュメントでは、Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) にトンネリングされているときに、セキュア ソケット レイヤ (SSL) VPN クライアント (SVC) のインターネットへのアクセスを許可する方法の段階的な手順を説明します。 この設定では、SSL 経由で社内のリソースへの SVC のセキュアなアクセスを可能にし、スプリット トンネリングを使用したインターネットへのセキュアではないアクセスを提供します。

同一のインターフェイス上でセキュリティで保護されたトラフィックと保護されていないトラフィックの両方を送信する機能は、スプリット トンネリングという名前で知られています。 スプリット トンネリングでは、どのトラフィックがセキュリティで保護され、そのトラフィックの宛先はどこであるかをユーザが正確に指定する必要があります。それによって、指定されたトラフィックだけがトンネル内に入り、それ以外のトラフィックはパブリック ネットワーク (インターネット) 経由で暗号化されずに送信されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- すべてのリモート ワークステーション上でのローカルな管理者権限

- リモート ワークステーションでの Java コントロールおよび ActiveX コントロール
- 接続パス上のどの場所でも、ポート 443（SSL）がブロックされていないこと

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.2(2) を実行する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- Windows 1.1.4.179 用のバージョンの Cisco SSL VPN Client**注:** Cisco Software Download（登録ユーザ専用）から、SSL VPN Client パッケージ（sslclient-win*.pkg）をダウンロードします。 SVC を ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確立するためにリモート ユーザ コンピュータにダウンロードされます。 詳細は、『ASA コンフィギュレーション ガイド』の「SVC ソフトウェアのインストール」セクションを参照してください。
- Windows 2000 Professional SP4 または Windows XP SP2 が稼働している PC
- Cisco Adaptive Security Device Manager（ASDM）バージョン 5.2(2)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

SSL VPN Client（SVC）は、ネットワーク管理者によるリモート コンピュータへの IPSec VPN クライアントのインストールおよび設定を必要とせずに、リモート ユーザに IPSec VPN クライアントのメリットを提供する VPN トンネリング技術です。 SVC は、リモート コンピュータに既存の SSL 暗号化およびセキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザがブラウザでセキュリティ アプライアンスの IP アドレスを入力し、ブラウザはそのインターフェイスに接続し、WebVPN ログイン画面を表示します。 ログインと認証を完了し、セキュリティ アプライアンスで SVC を必要としていることが確認されると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。 セキュリティ アプライアンスが、SVC を使用するオプションがあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをウィンドウに表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC はインストールと設定を実行します。接続が終了すると、その設定に応じて SVC がリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

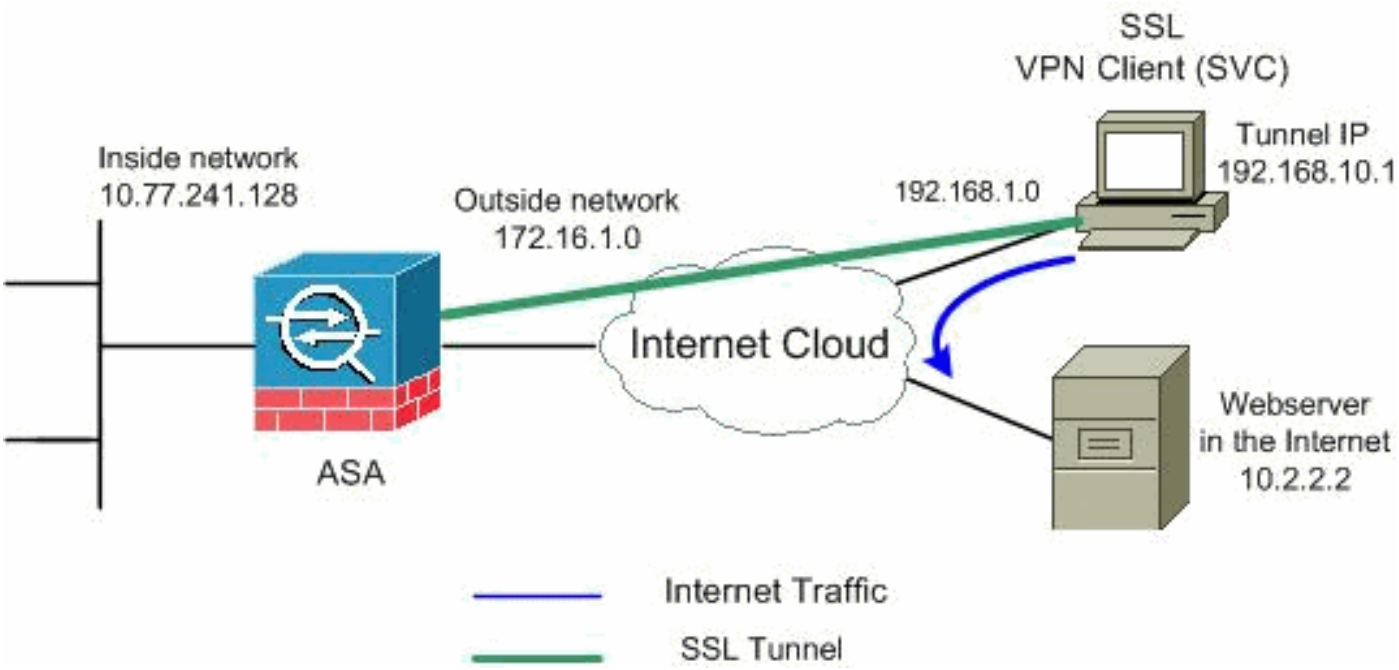
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

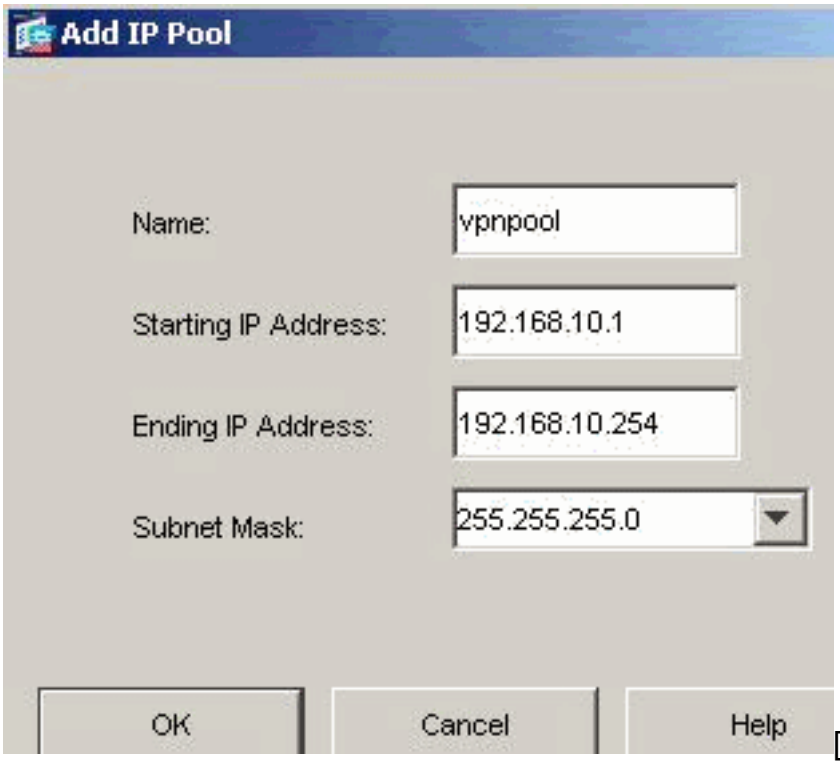


注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 で、 ラボ環境で使用されたアドレスです。

ASDM 5.2(2) を使用した ASA 設定

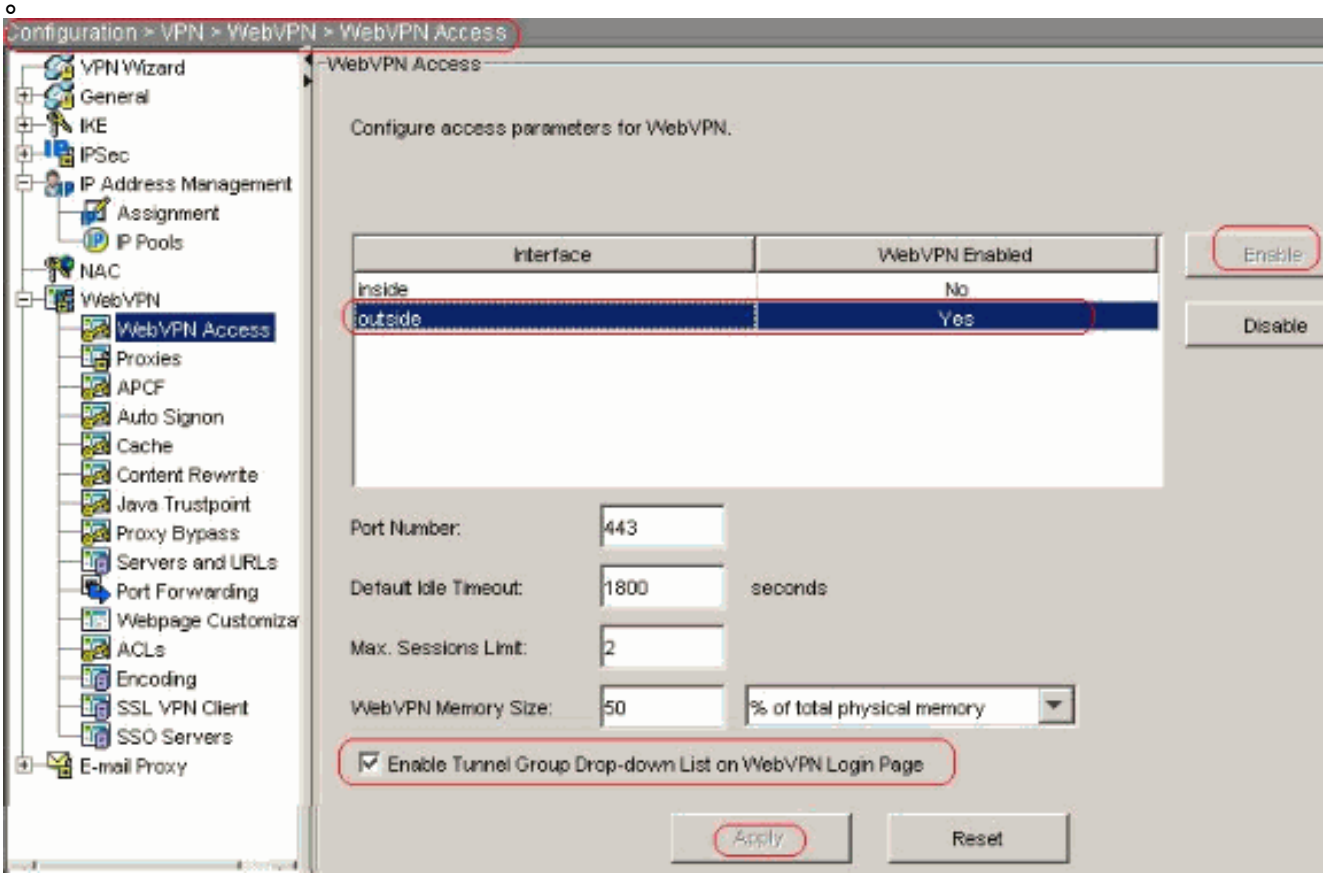
手順を実行すると、次で示されているように ASA 上でスプリット トンネリングを備えた SSL VPN を設定できます。

1. このドキュメントは、インターフェイス設定などの基本設定などがすでに行われていて適切に動作していることを前提としています。**注:** ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。**注:** WebVPN と ASDM は、ポート番号を変更しない限り、同じ ASA インターフェイス上では有効にできません。 詳細については、『ASA の同じインターフェイスで有効になる ASDM および WebVPN』（英語）を参照してください。
2. IP アドレス プールを作成するために、[Configuration] > [VPN] > [IP Address Management]> [IP Pools] を選択します。 **vpnpool** は VPN クライアント向けです。

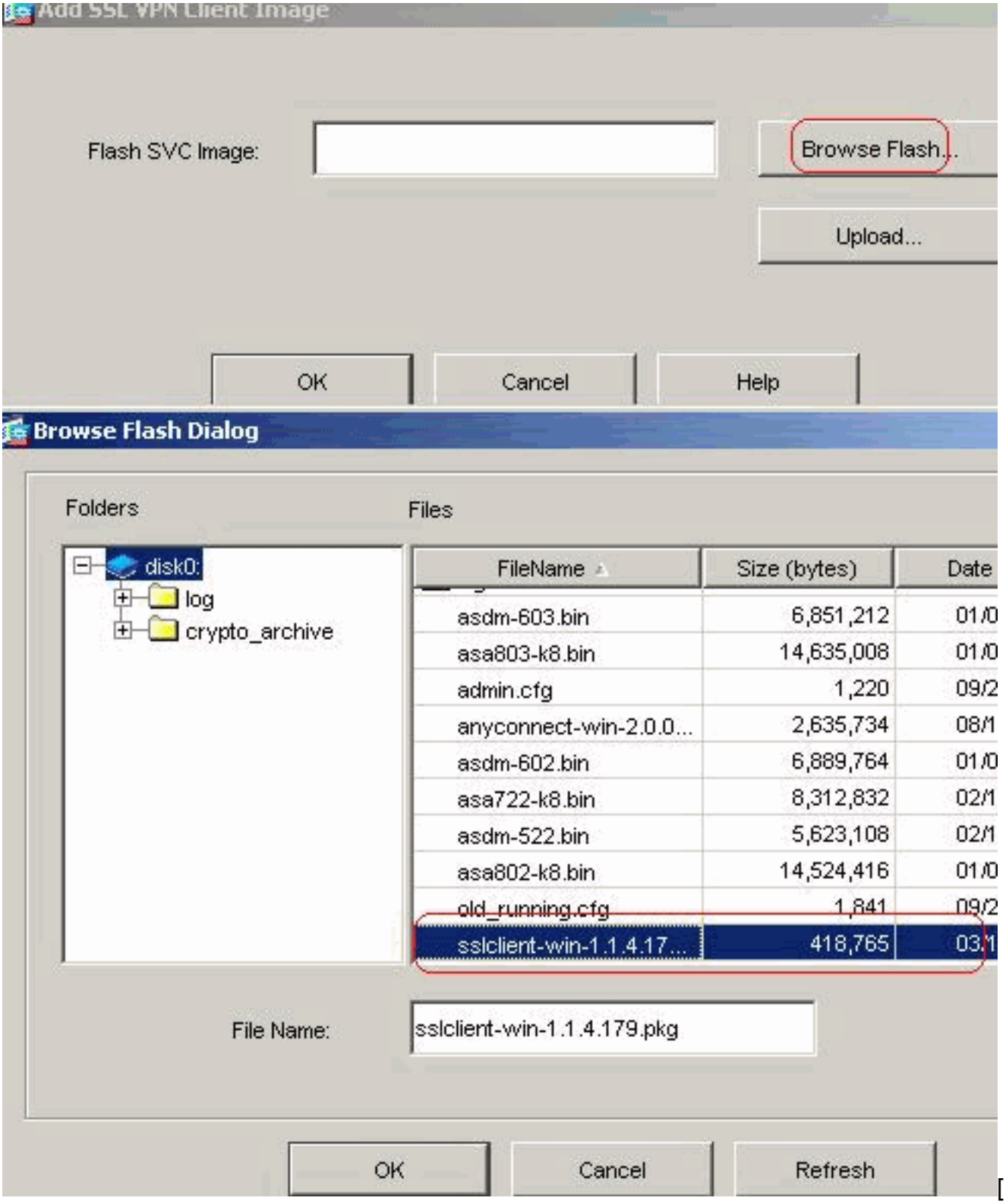


[Apply] をクリックします。

3. **WebVPN の有効化**[Configuration] > [VPN] > [WebVPN] > [WebVPN Access] を選択し、マウスで外部インターフェイスを強調表示して [Enable] をクリックします。 ユーザのログイン ページでドロップ ダウン表示を有効にするために [Enable Tunnel Group Drop-down List on WebVPN Login Page] のチェックボックスをオンにして、それぞれのグループを選択します。



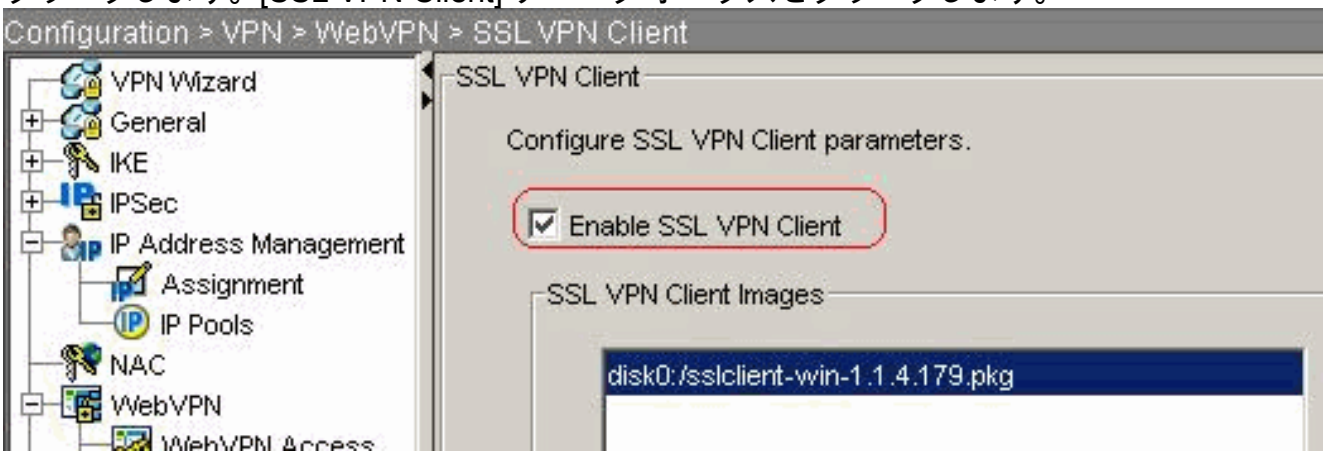
[Apply] をクリックします。[Configuration] > [VPN] > [WebVPN] > [SSL VPN Client] > [Add] を選択し、次に示すように SSL VPN クライアント イメージを ASA のフラッシュ メモリから追加します。


Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin 6,851,212 01/0
asa803-k8.bin 14,635,008 01/0
admin.cfg 1,220 09/2
anyconnect-win-2.0.0... 2,635,734 08/1
asdm-602.bin 6,889,764 01/0
asa722-k8.bin 8,312,832 02/1
asdm-522.bin 5,623,108 02/1
asa802-k8.bin 14,524,416 01/0
old_running.cfg 1,841 09/2
sslclient-win-1.1.4.17... 418,765 03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

[

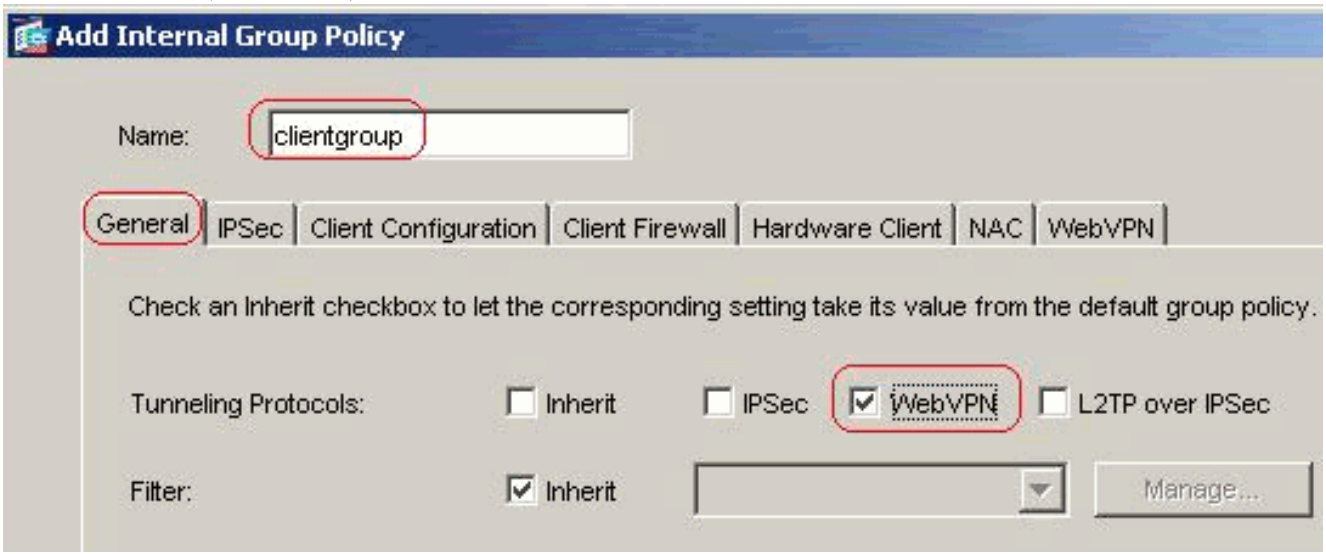
OK] をクリックします。

[OK] をクリックします。[SSL VPN Client] チェック ボックスをクリックします。

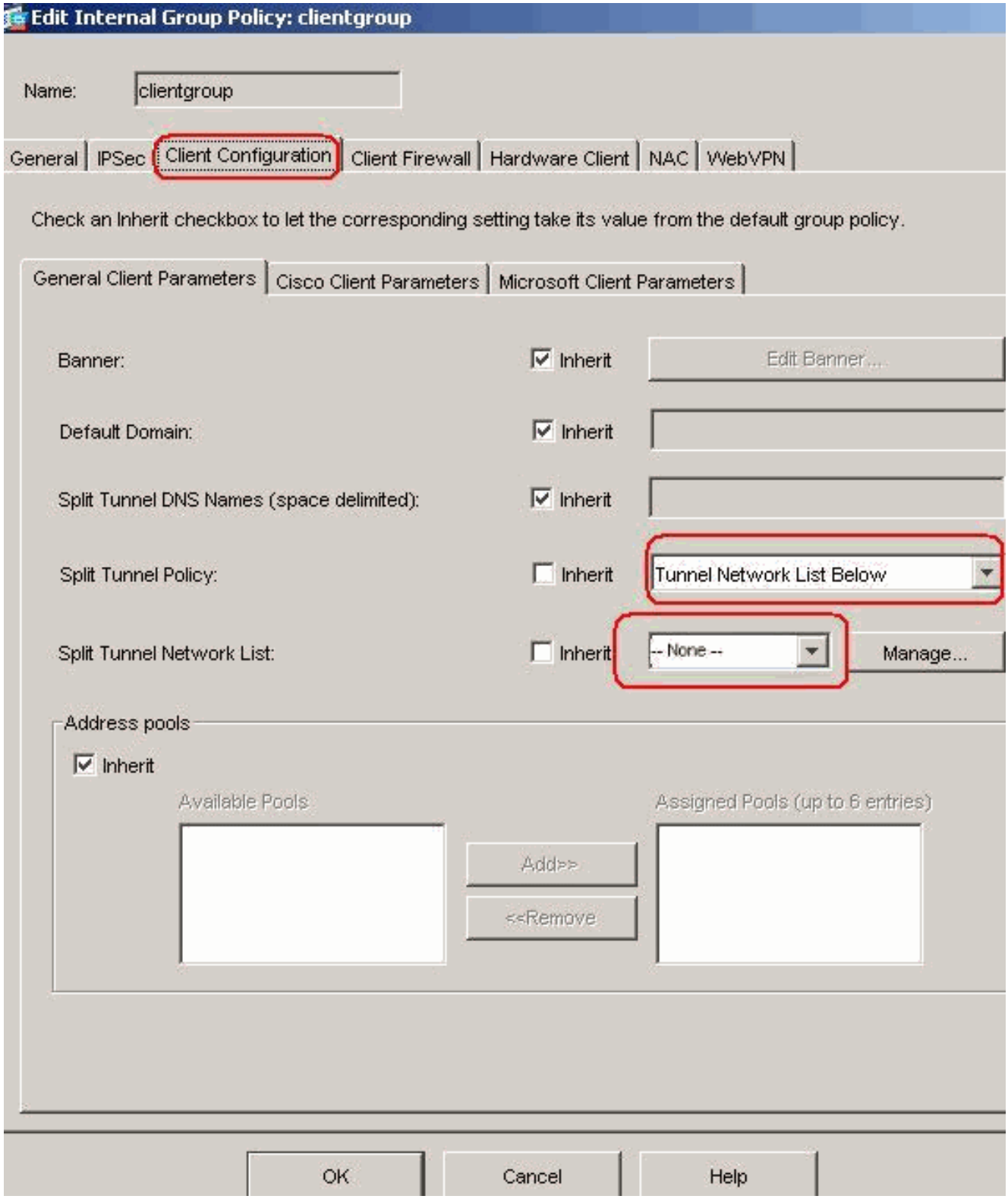


[Apply] をクリックします。**同等の CLI 設定：**

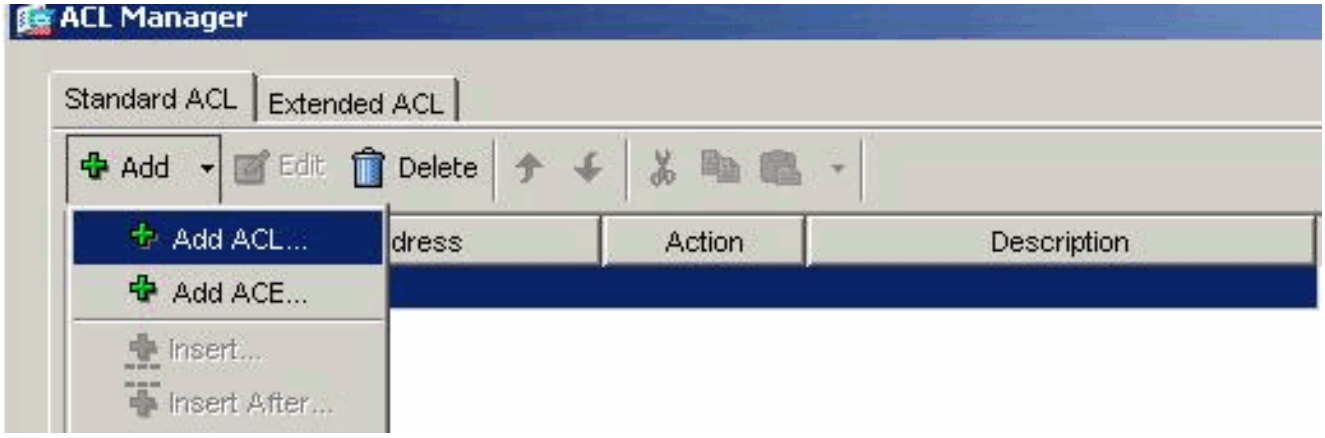
4. **グループ ポリシーの設定**[Configuration] > [VPN] > [General] > [Group Policy] > [Add（ Internal Group Policy ）] を選択し、内部グループ ポリシー **clientgroup** を作成します。 [General] で、[WebVPN] チェックボックスをオンにし、トンネリング プロトコルとして WebVPN を有効にします。



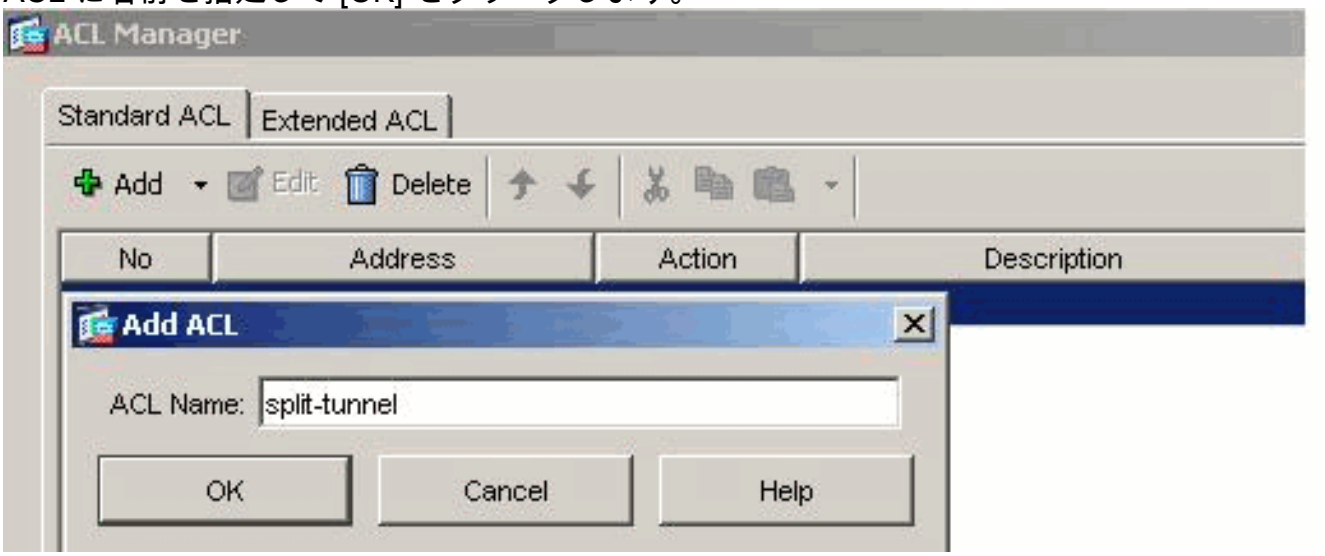
[Client Configuration] > [General Client Parameters] タブでスプリット トンネル ポリシー用の [Inherit] ボックスの選択を解除して、ドロップダウン リストから [Tunnel Network List Below] を選択します。[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。



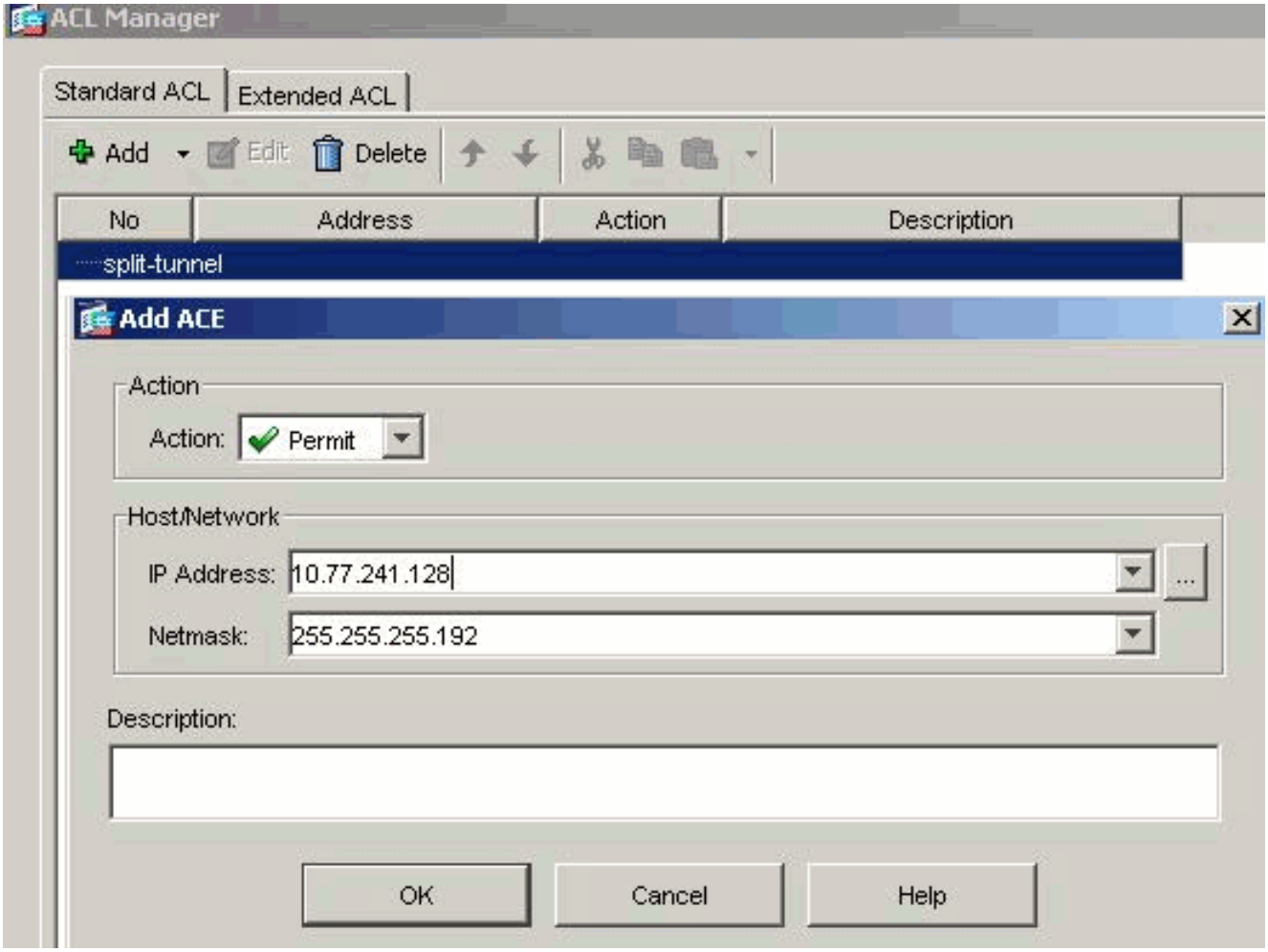
ACL Manager で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。



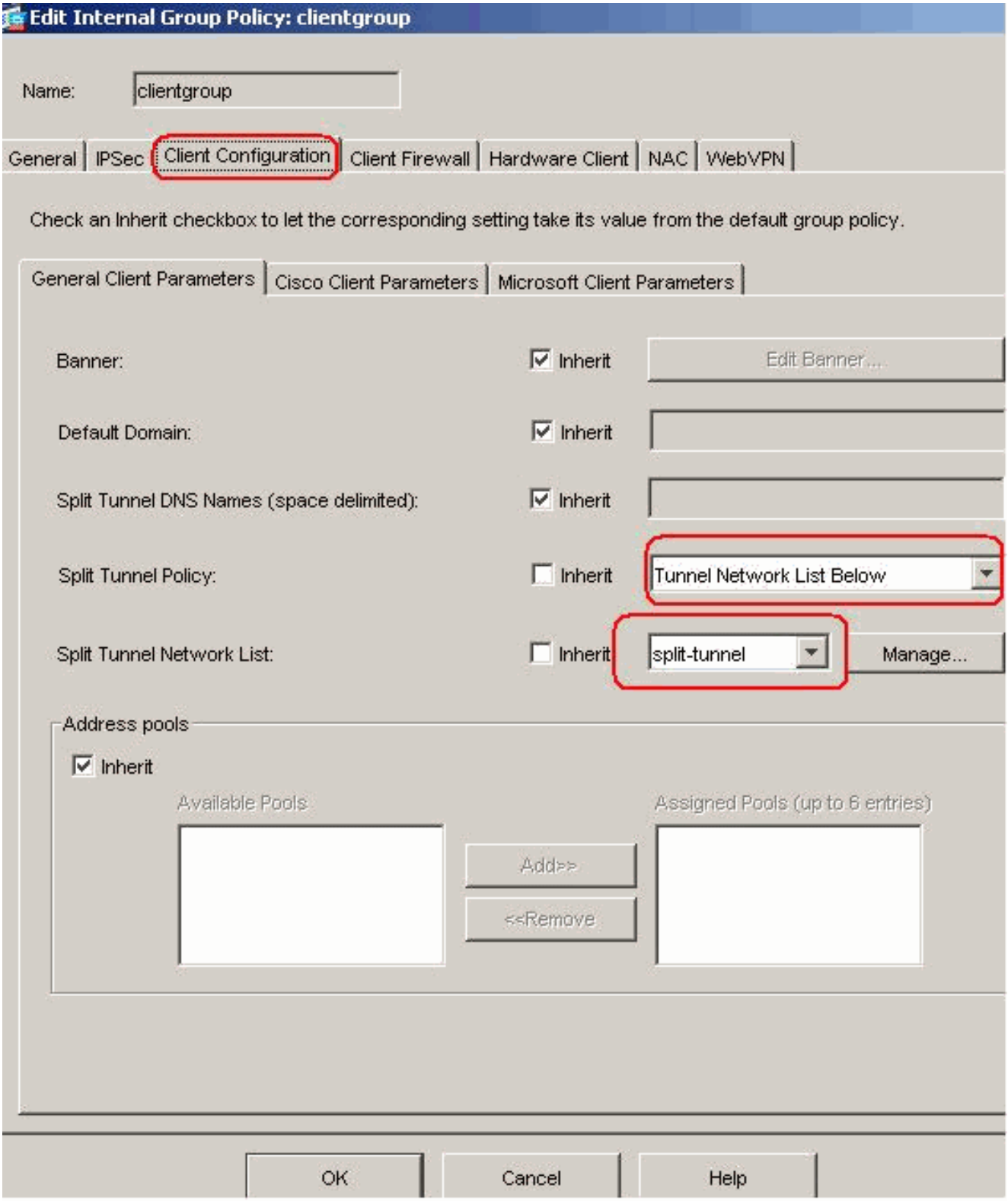
ACL に名前を指定して [OK] をクリックします。



ACL 名が作成されてから、[Add] > [Add ACE] を選択して Access Control Entry (ACE; アクセス コントロール エントリ) を追加します。ASA の背後にある LAN に対応する ACE を定義します。 この場合、ネットワークは 10.77.241.128/26 であり、[Permit] を選択します。[OK] をクリックして ACL Manager を終了します。

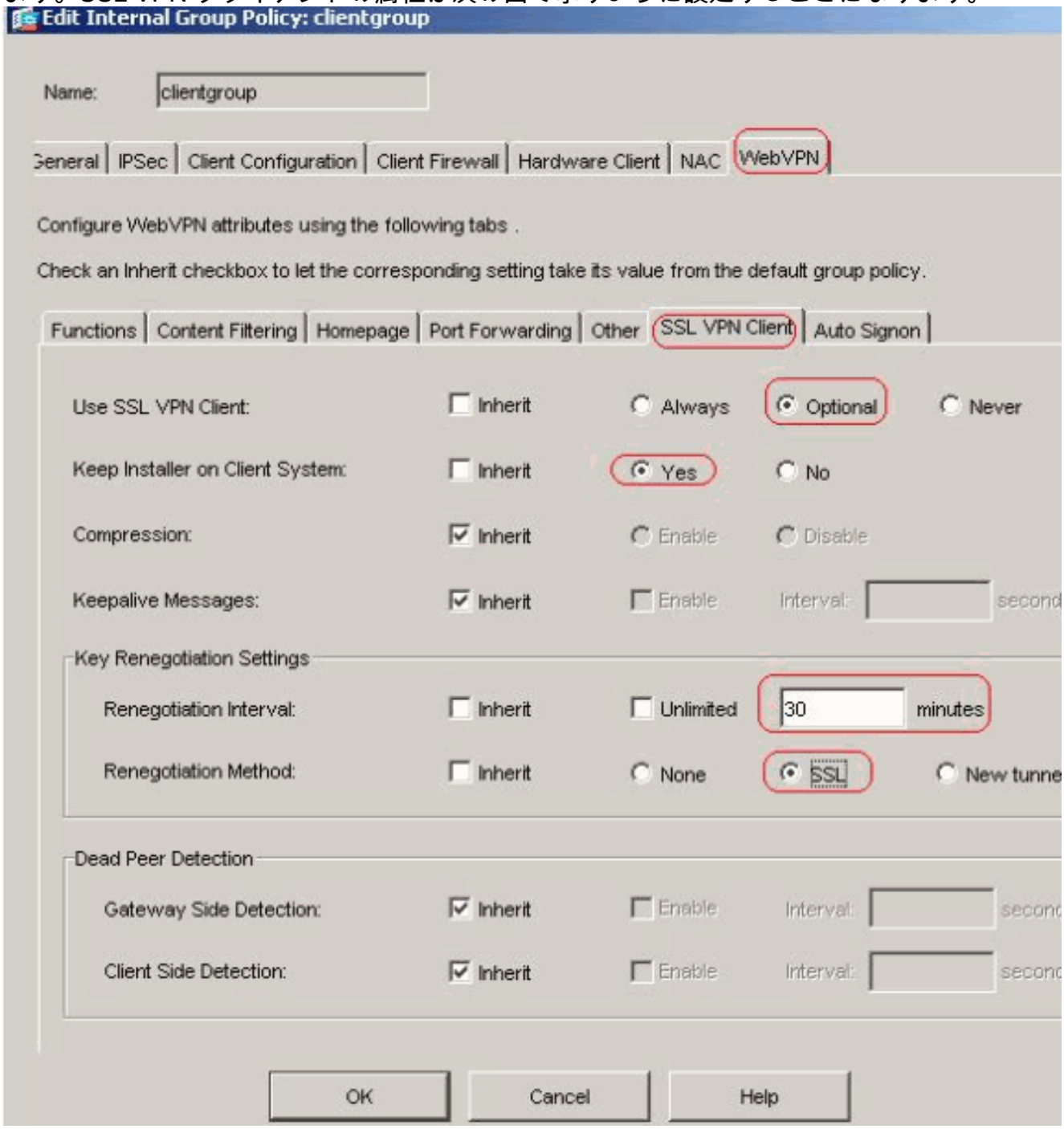


Split Tunnel Network List で、作成した ACL が選択されていることを確認します。[OK] をクリックして、グループ ポリシー設定に戻ります。

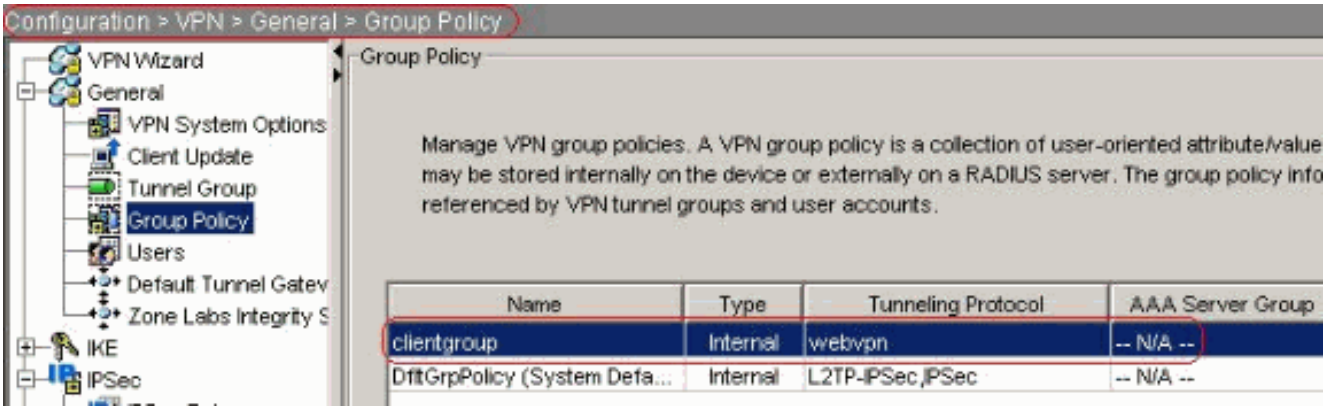


メイン ページで、[Apply] をクリックしてから [Send]（必要な場合）をクリックして、コマンドを ASA に送信します。[Use SSL VPN Client] オプションで、[Inherit] チェック ボックスをオフにし、[Optional] ラジオ ボタンをクリックします。この選択により、リモート クライアントで [WebVPN] > [SSLVPN Client] タブをクリックするかどうかを選択し、これらのオプションを選択できるようになります。SVC はダウンロードしないでください。 Always を選択すると、SSL VPN 接続のたびにリモート ワークステーションに SVC がダウンロードされるようになります。[Keep Installer on Client System] オプションについては、**[Inherit]** チェック ボックスのチェックマークを外して、**[Yes]** オプション ボタンをクリックします。この操作によって、SVC ソフトウェアはクライアント マシン上に留まります。 これにより、ASA は接続が確立するたびに SVC ソフトウェアをクライアントにダウンロードする必要がなくなります。 このオプションは、社内ネットワークに頻繁にアクセスするリモート ユ

ーザが選択するのに適しています。[Renegotiation Interval] オプションで、[Inherit] チェック ボックスをオフにし、[Unlimited] チェック ボックスをオフにし、キーの再生成が行われるまでの時間（分）を入力します。セキュリティは、キーが有効である時間に制限を設けた場合に強化されます。[Renegotiation Method] オプションで、[Inherit] チェック ボックスをオフにして、[SSL] オプション ボタンをクリックします。 再ネゴシエーションは、現在の SSL トンネルまたは再ネゴシエーション用に明示的に作成された新しいトンネルを使用できます。SSL VPN クライアントの属性は次の図で示すように設定することになります。

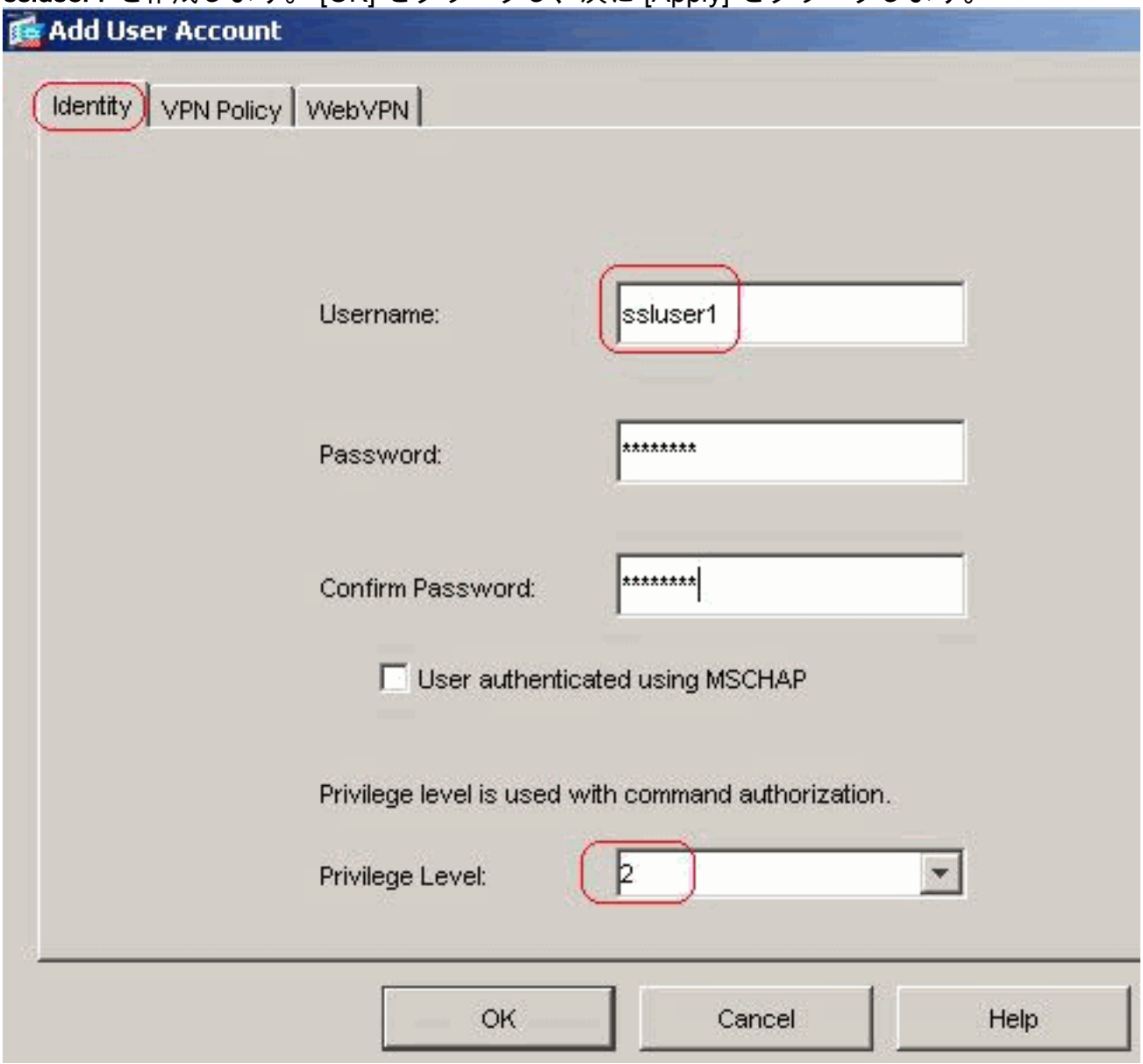


[OK] をクリックし、次に [Apply] をクリックします。



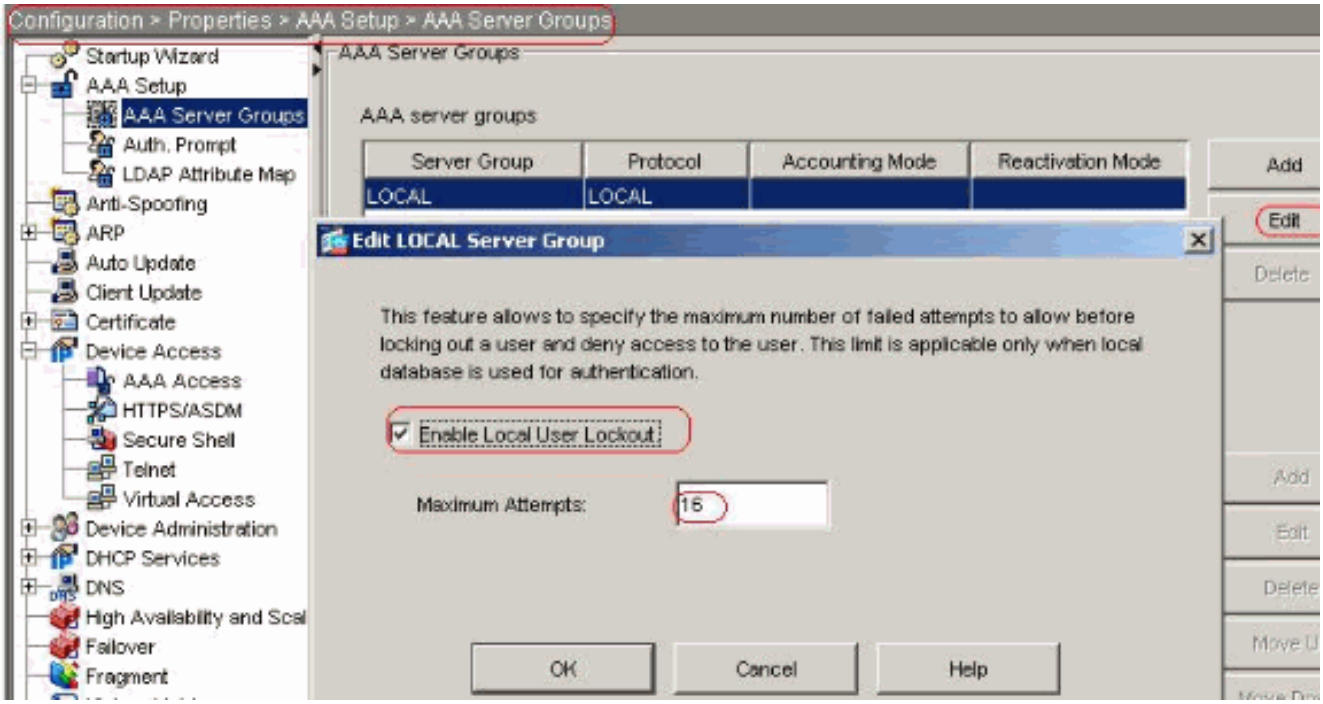
同等の CLI 設定：

5. [Configuration] > [VPN] > [General] > [Users] > [Add] を選択し、新しいユーザ アカウント **ssluser1** を作成します。 [OK] をクリックし、次に [Apply] をクリックします。



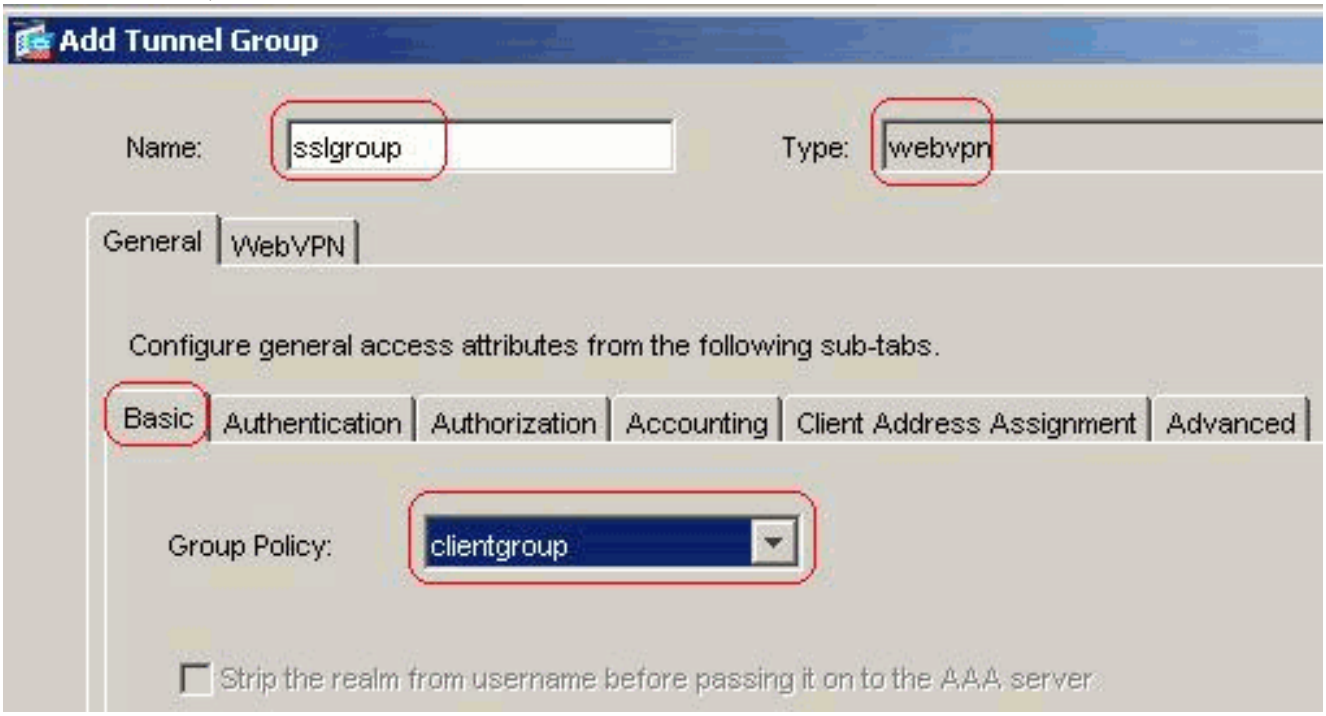
同等の CLI 設定：

6. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers Groups] > [Edit] を選択してデフォルトのサーバ グループ **LOCAL を変更し、** [Enable Local User Lockout] チェック ボックスをオンにして最大試行値の **16** に設定します。

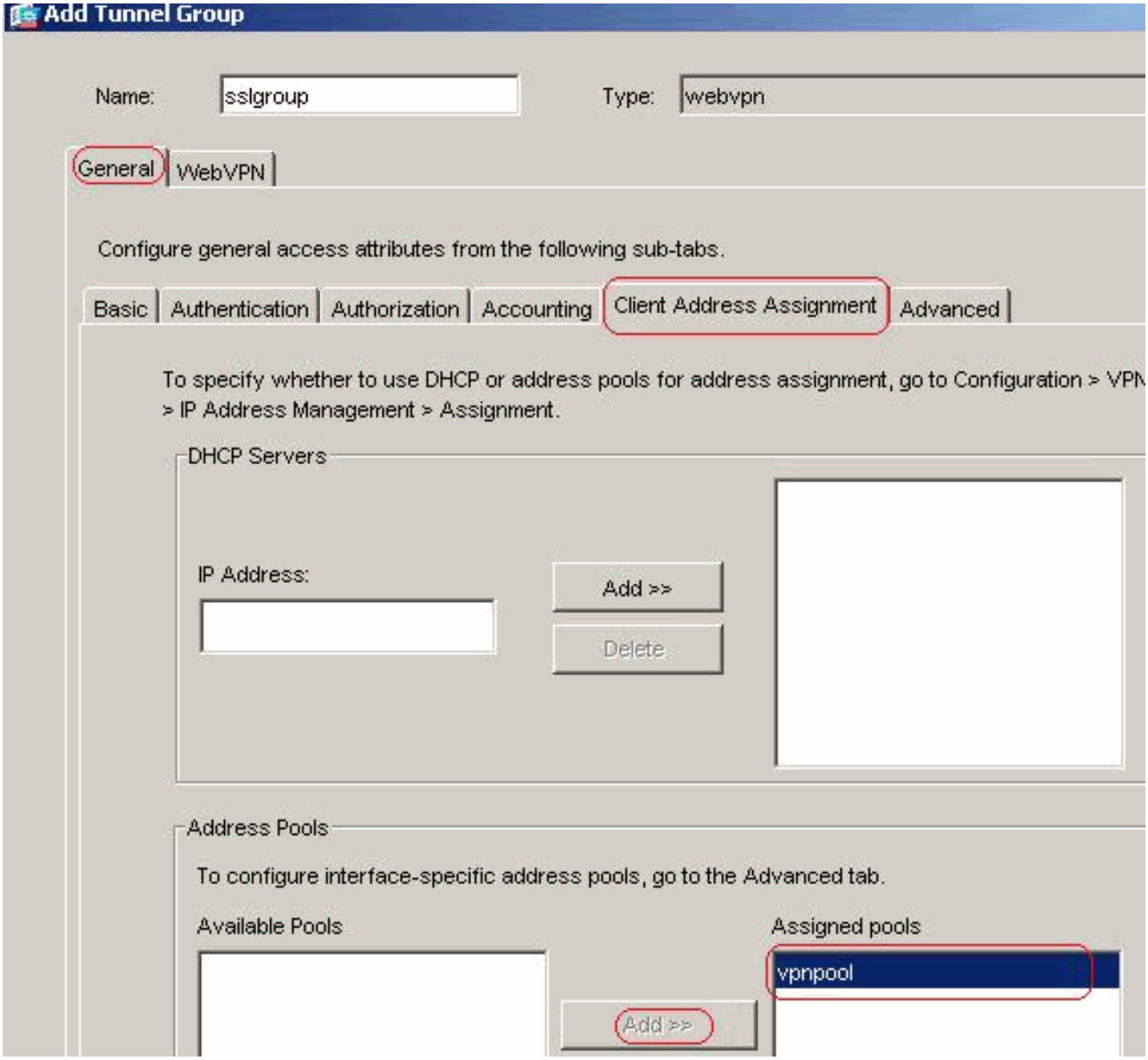


同等の CLI 設定：

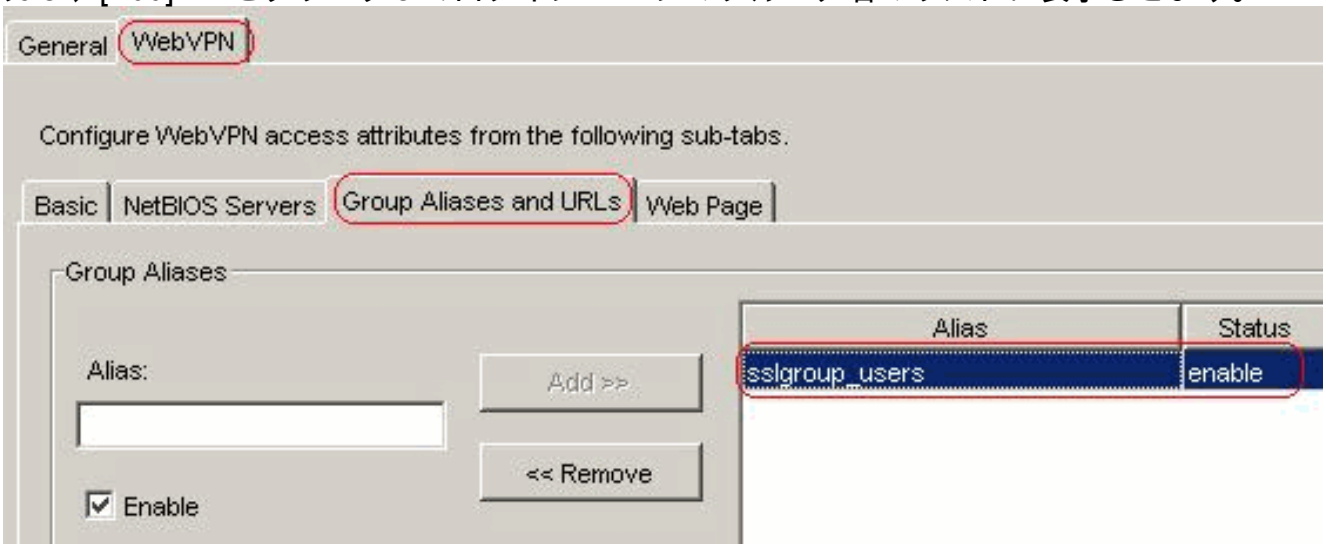
7. **トンネル グループの設定**[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add (WebVPN access)] を選択し、新しいユーザ アカウント **sslgroup** を作成します。[General] > [Basic] タブで、ドロップダウン リストから **clientgroup** としてグループ ポリシーを選択します。



[General] > [Client Address Assignment] タブで、[Address Pools] の下から、[Add] >> をクリックして、利用可能なアドレス プール **vpnpool** を割り当てます。

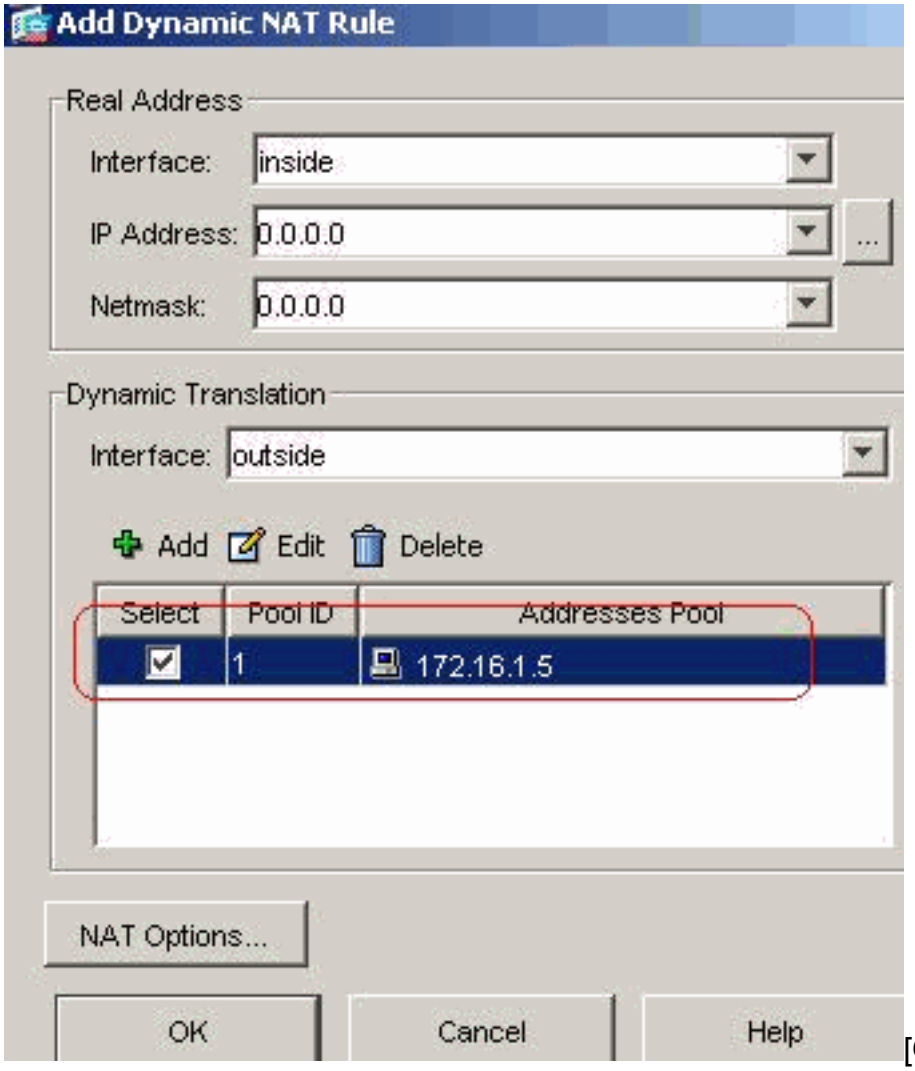


[WebVPN] > [Group Aliases and URLs] タブで、パラメータ ボックス内のエイリアス名を入力し、[Add] >> をクリックしてログイン ページのグループ名のリストに表示させます。



[OK] をクリックし、次に [Apply] をクリックします。**同等の CLI 設定：**

8. **NAT の設定**[Configuration] > [NAT] > [Add] > [Add Dynamic NAT Rule] を選択し、Inside ネットワークからのトラフィックが Outside IP アドレス 172.16.1.5 で変換できるようにしま



す。[OK] をクリックして、メイン ページの [Apply] をクリックします。**同等の CLI 設定：**

9. VPN クライアントにネットワーク内から戻るトラフィックの NAT 免除を設定します。

```
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
```

CLI を使用した ASA 7.2(2) の設定

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
```

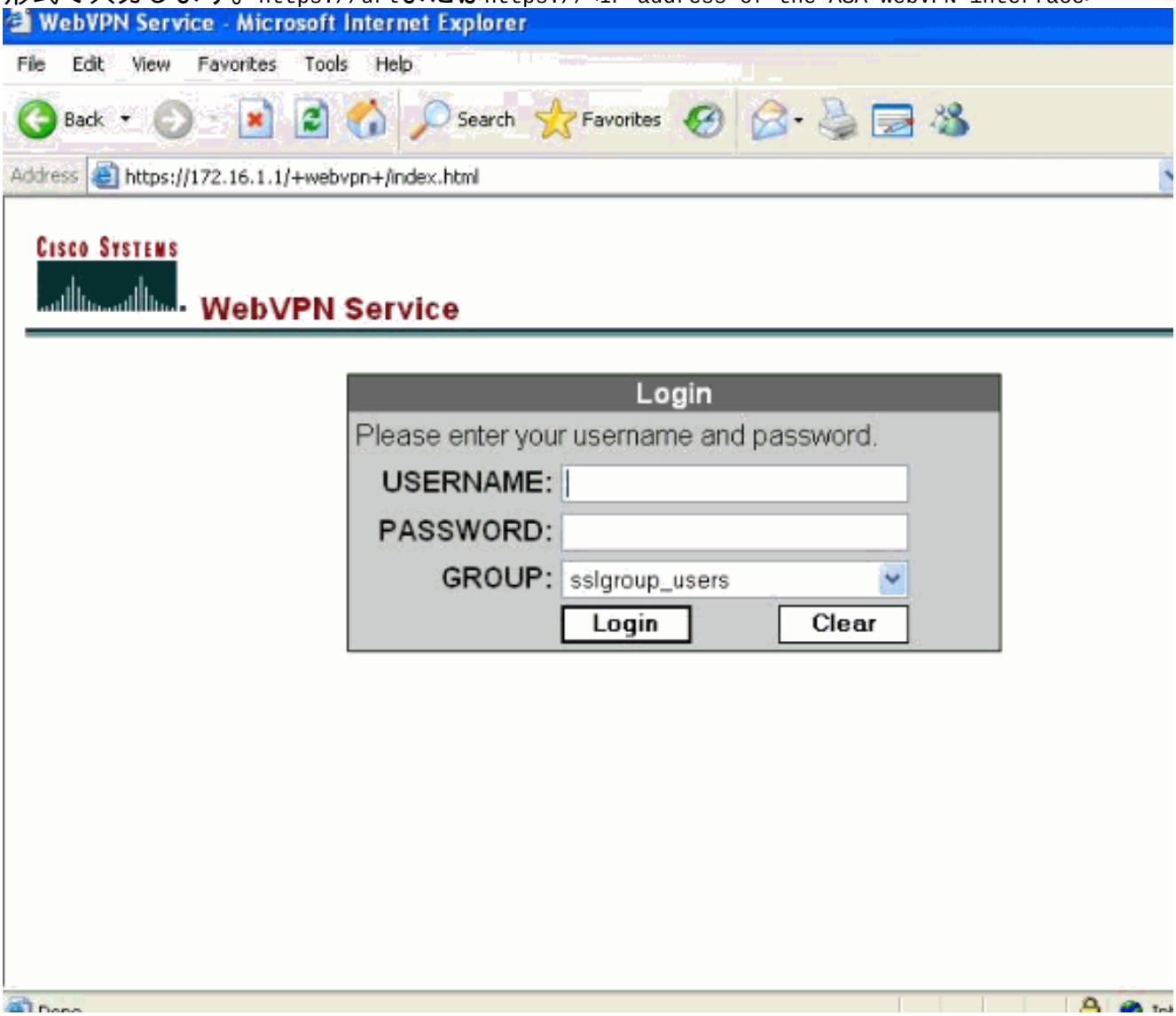
```
the SSL VPN Clients no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no
asdm history enable arp timeout 14400 global (outside) 1
172.16.1.5 !--- The global address for Internet access
used by VPN Clients. !--- Note: Uses an RFC 1918 range
for lab setup. !--- 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#
```

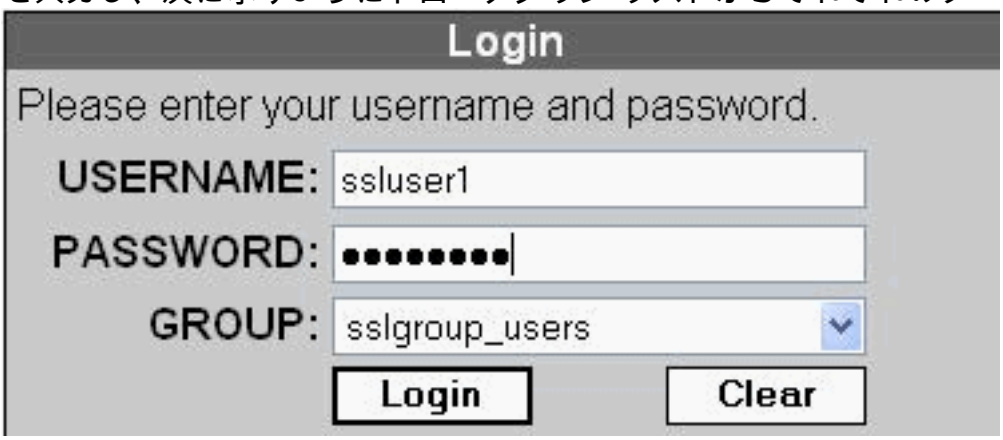
SVC との SSL VPN 接続の確立

次の手順を実行して、ASA との SSL VPN 接続を確立します。

1. Web ブラウザで ASA の WebVPN インターフェイスの URL または IP アドレスを次に示す形式で入力します。`https://url`または`https://<IP address of the ASA WebVPN interface>`



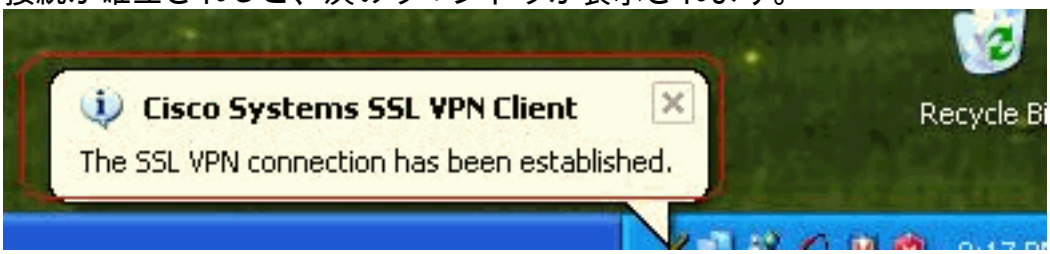
2. ユーザ名とパスワードを入力し、次に示すようにドロップダウン リストからそれぞれのグループを選択します。



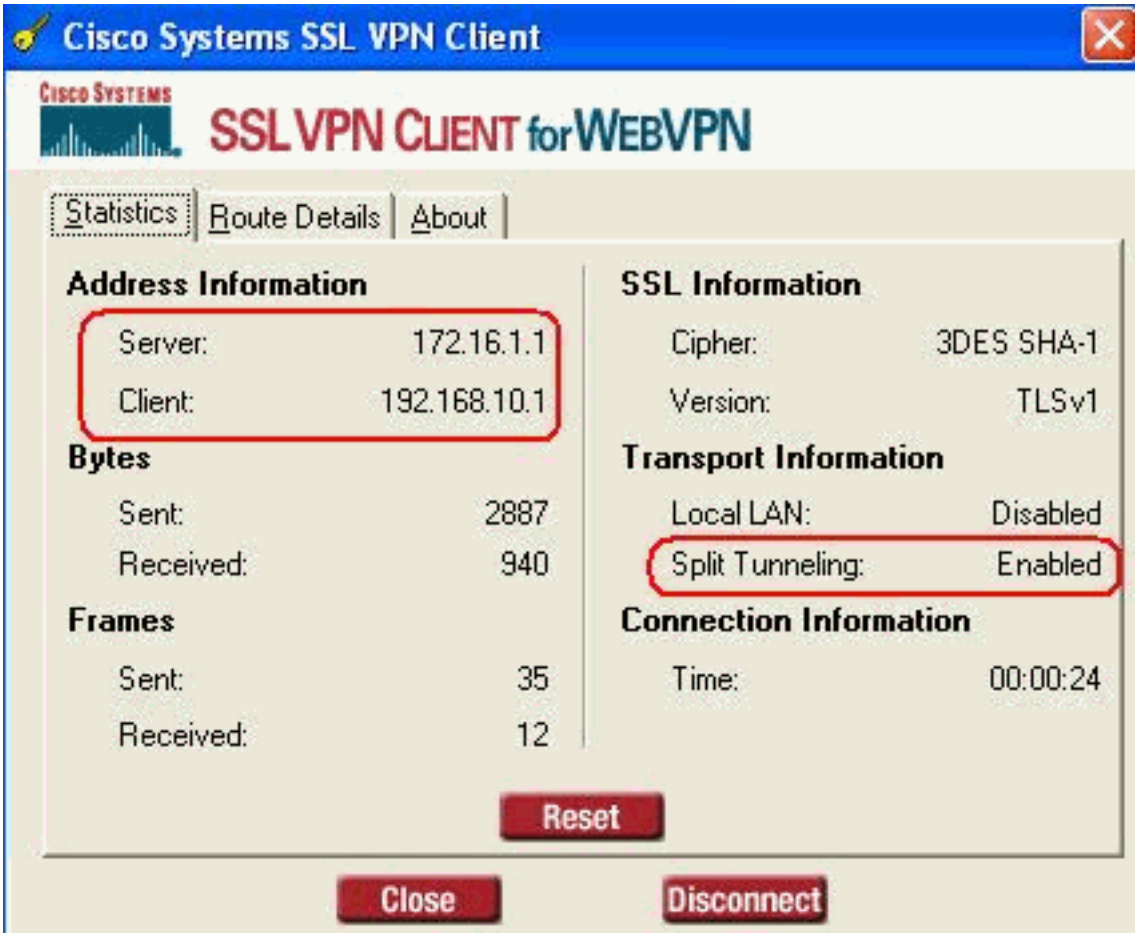
3. SVC をダウンロードする前に ActiveX ソフトウェアをコンピュータにインストールしておく必要があります。

4. SSL VPN 接続が確立される前に次のウィンドウが表示されます。

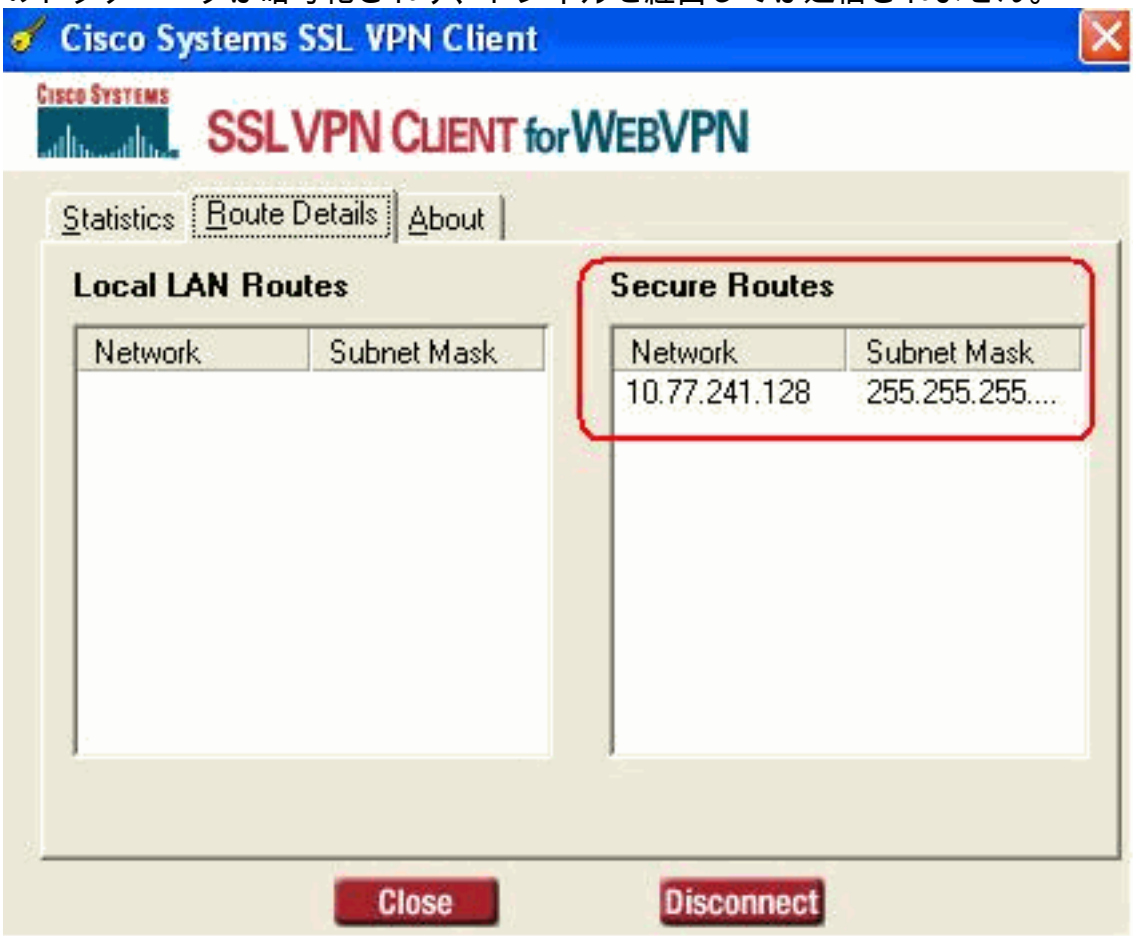
5. 接続が確立されると、次のウィンドウが表示されます。

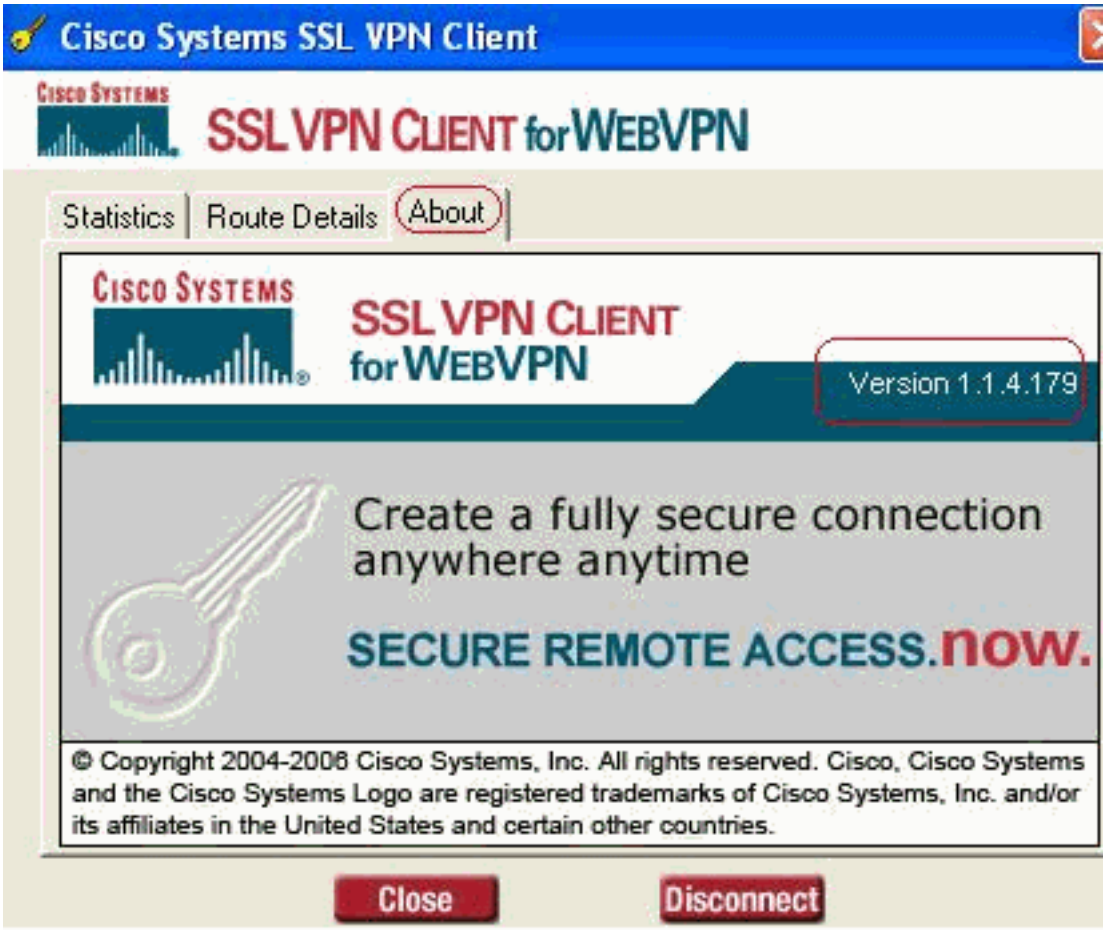


6. コンピュータのタスクバーに表示される黄色いキーをクリックします。 SSL 接続についての情報を提供するウィンドウが表示されます。 たとえば、**192.168.10.1** はクライアントの IP に割り当てられ、サーバ IP アドレスは 172.16.1.1 で、**スプリット トンネリングは有効**、などです。



また、SSL で暗号化されたセキュアなネットワークを確認でき、ネットワークリストは ASA で設定されたスプリットトンネル アクセス リストからダウンロードされます。この例では、SSL VPN クライアントは 10.77.241.128/24 へのアクセスを保護しますが、一方で、他のすべてのトラフィックは暗号化されず、トンネルを経由しては送信されません。



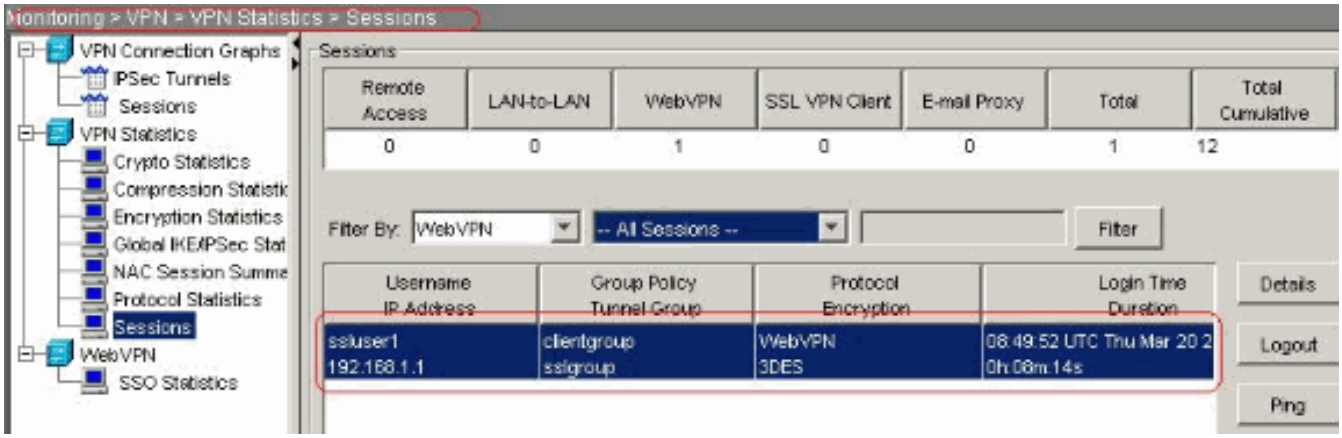


確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

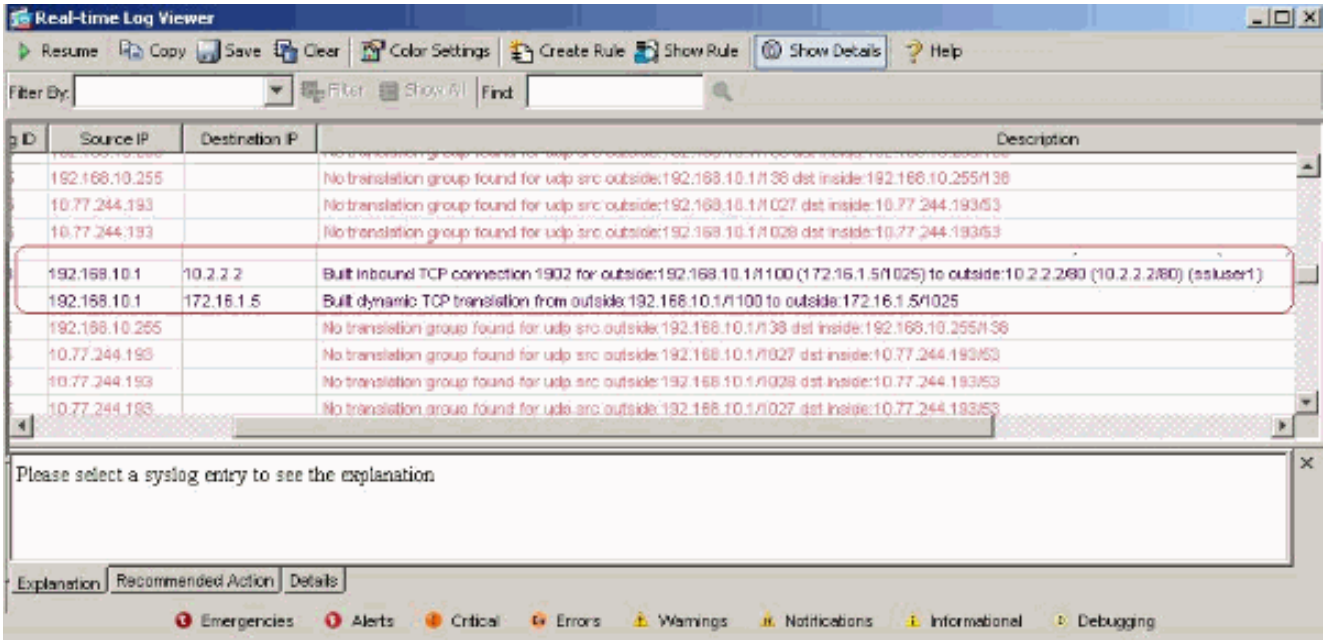
- **show webvpn svc**：ASA フラッシュ メモリに格納された SVC イメージを表示します。
  ```
  ciscoasa#show webvpn svc 1. disk0:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0
  1,1,4,179 Fri 01/18/2008 15:19:49.43 1 SSL VPN Client(s) installed
  ```
- **show vpn-sessiondb svc**：現在の SSL 接続についての情報を表示します。
  ```
  ciscoasa#show 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**：さまざまなグループに対する設定済みの エイリアスを表示します。
  ```
  ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup_users
  enabled
  ```
- ASDM で、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択すると、ASA の現在の WebVPN セッションがわかります。



トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

1. **vpn-sessiondb logoff name <ユーザ名>**：特定のユーザ名の SSL VPN セッションをログオフするコマンドです。`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` 同様に、**vpn-sessiondb logoff svc** コマンドを使用すると、すべての SVC セッションを終了できます。
2. **注:** PC がスタンバイ モードまたは休止状態モードになった場合、SSL VPN 接続を終了することができます。
   `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>**： セッションを確立するために、リアルタイムの webvpn イベントを提供します。
   ```
   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. ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] を選択してリアルタイム イベントを表示します。 次に、ASA 172.16.1.5 経由のインターネットにおける、SVC 192.168.10.1 と Webserver 10.2.2.2 の間のセッション情報の例を示します。



関連情報

- Cisco 5500 シリーズ適応型セキュリティ アプライアンス製品に関するサポート
- ASA/PIX： ASA で VPN クライアントのスプリット トンネリングを許可するための設定例
- スプリット トンネリングを使用する VPN クライアントが IPSec とインターネットに接続するのをルータで許可する設定例
- 公衆インターネット VPN on a Stick のための PIX/ASA 7.x および VPN クライアント間の設定例
- ASDM を使用した ASA での SSL VPN Client（SVC）の設定例
- テクニカルサポートとドキュメント - Cisco Systems