

ASA 8.x:在ASA上允許對AnyConnect VPN客戶端進行拆分隧道配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[使用ASDM 6.0\(2\)的ASA配置](#)

[ASA CLI配置](#)

[使用SVC建立SSL VPN連線](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文提供分步說明，說明如何允許Cisco AnyConnect VPN客戶端在通過隧道連線到Cisco Adaptive Security Appliance(ASA)8.0.2時訪問網際網路。此配置允許客戶端通過SSL安全訪問公司資源，同時允許使用拆分隧道進行不安全的網際網路訪問。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- ASA安全裝置需要運行版本8.x
- Cisco AnyConnect VPN使用者端2.x**注意**：從Cisco [Software Download](#) (僅限註冊客戶) 下載AnyConnect VPN客戶端包(anyconnect-win*_pkg)。將AnyConnect VPN客戶端複製到ASA的快閃記憶體，該快閃記憶體將下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。有關詳細資訊，請參閱ASA配置指南的[安裝AnyConnect客戶端](#)部分。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.0(2)的Cisco 5500系列ASA
- 適用於Windows 2.0.0343的Cisco AnyConnect SSL VPN客戶端版本
- 運行Microsoft Vista、Windows XP SP2或Windows 2000 Professional SP4 (帶有Microsoft Installer 3.1版) 的PC
- 思科調適型安全裝置管理員(ASDM)版本6.0(2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

背景資訊

Cisco AnyConnect VPN客戶端為遠端使用者提供到安全裝置的安全SSL連線。如果沒有先前安裝的客戶端，遠端使用者在其瀏覽器中輸入配置為接受SSL VPN連線的介面的IP地址。除非安全裝置配置為將http://請求重定向到https://，否則使用者必須以https://<address>的形式輸入URL。

輸入URL後，瀏覽器會連線到該介面並顯示登入螢幕。如果使用者滿足登入和身份驗證要求，且安全裝置將使用者識別為需要客戶端，則它會下載與遠端電腦的作業系統匹配的客戶端。下載後，客戶端將自行安裝和配置，建立安全SSL連線，並在連線終止時自行保留或解除安裝 (取決於安全裝置配置)。

如果是以前安裝的客戶端，當使用者進行身份驗證時，安全裝置會檢查客戶端的修訂版本，並根據需要升級客戶端。

當客戶端與安全裝置協商SSL VPN連線時，它會使用傳輸層安全(TLS)連線，也可以使用資料包傳輸層安全(DTLS)連線。DTLS可避免與某些SSL連線相關的延遲和頻寬問題，並提高對資料包延遲敏感的即時應用的效能。

AnyConnect客戶端可以從安全裝置下載，也可以由系統管理員手動安裝在遠端PC上。有關如何手動安裝客戶端的詳細資訊，請參閱[Cisco AnyConnect VPN客戶端管理員指南](#)。

安全裝置根據建立連線的使用者的組策略或使用者名稱屬性下載客戶端。您可以將安全裝置配置為自動下載客戶端，也可以將其配置為提示遠端使用者是否下載客戶端。在後一種情況下，如果使用者沒有響應，您可以將安全裝置配置為在超時時間後下載客戶端或顯示登入頁面。

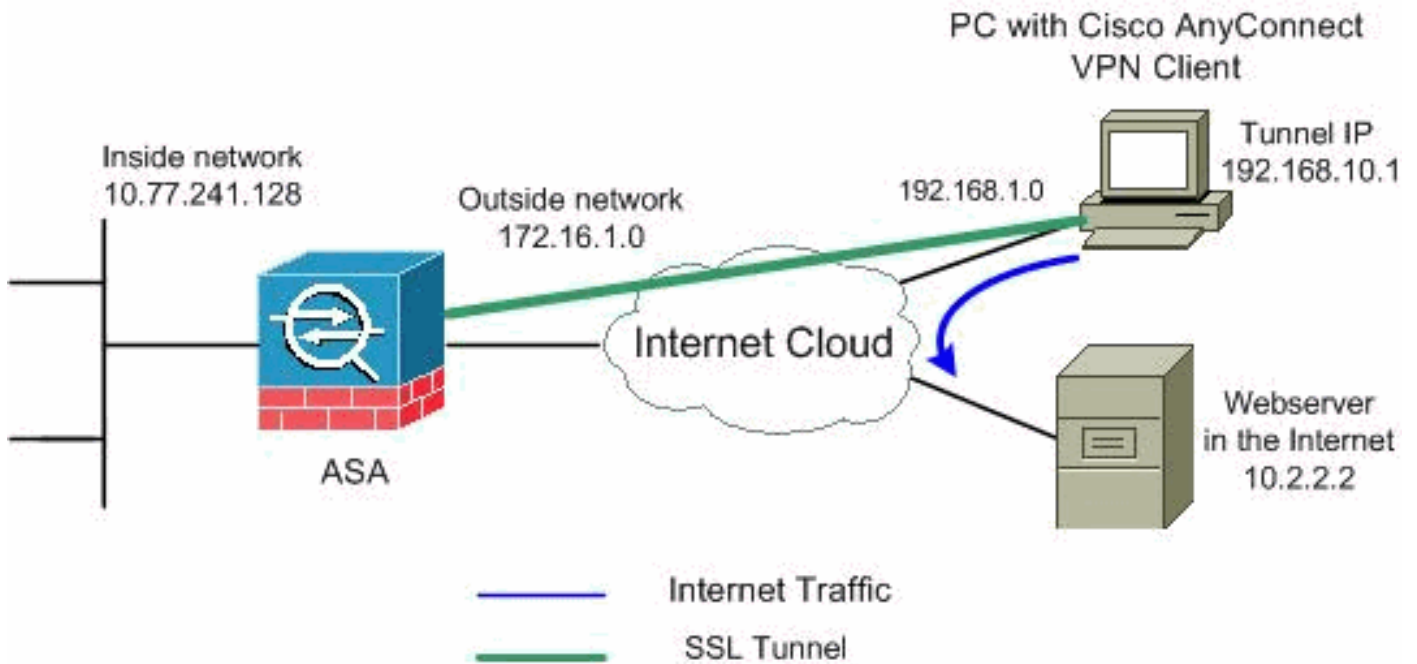
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是[RFC 1918](#)，已在實驗室環境中使用。

使用ASDM 6.0(2)的ASA配置

本檔案假設已建立基本組態（例如介面組態）且運作正常。

註：請參閱[允許ASDM進行HTTPS訪問](#)，以便允許ASDM配置ASA。

注意：除非更改埠號，否則不能在同一個ASA介面上啟用WebVPN和ASDM。有關詳細資訊，請參閱[在同一介面ASA上啟用ASDM和WebVPN](#)。

完成以下步驟，以便使用分割隧道在ASA上配置SSL VPN:

1. 選擇**Configuration > Remote Access VPN > Network(Client)Access > Address Management > Address Pools > Add**以建立IP地址池vpnpool。

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

OK Cancel Help

2. 按一下「Apply」。等效的CLI配置：

3. 啟用WebVPN。選擇**Configuration > Remote Access VPN > Network(Client)Access > SSL VPN Connection Profiles**，並在**Access Interfaces**下按一下外部介面的**Allow Access**和**Enable DTLS**釐取方塊。此外，選中**Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below**釐取方塊，以在外部介面上啟用SSL VPN。

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

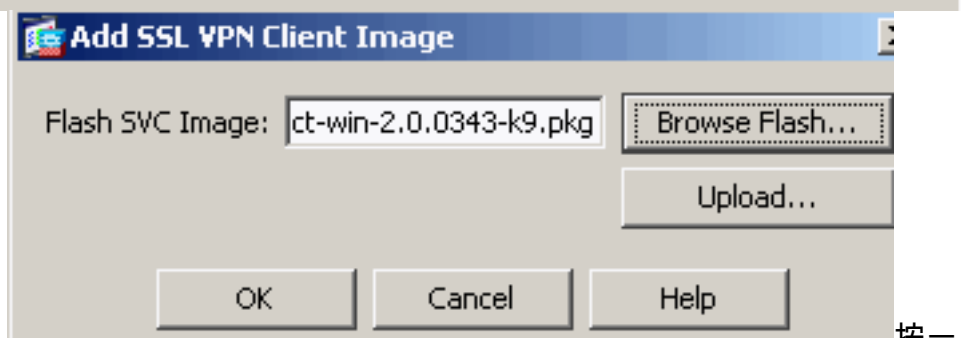
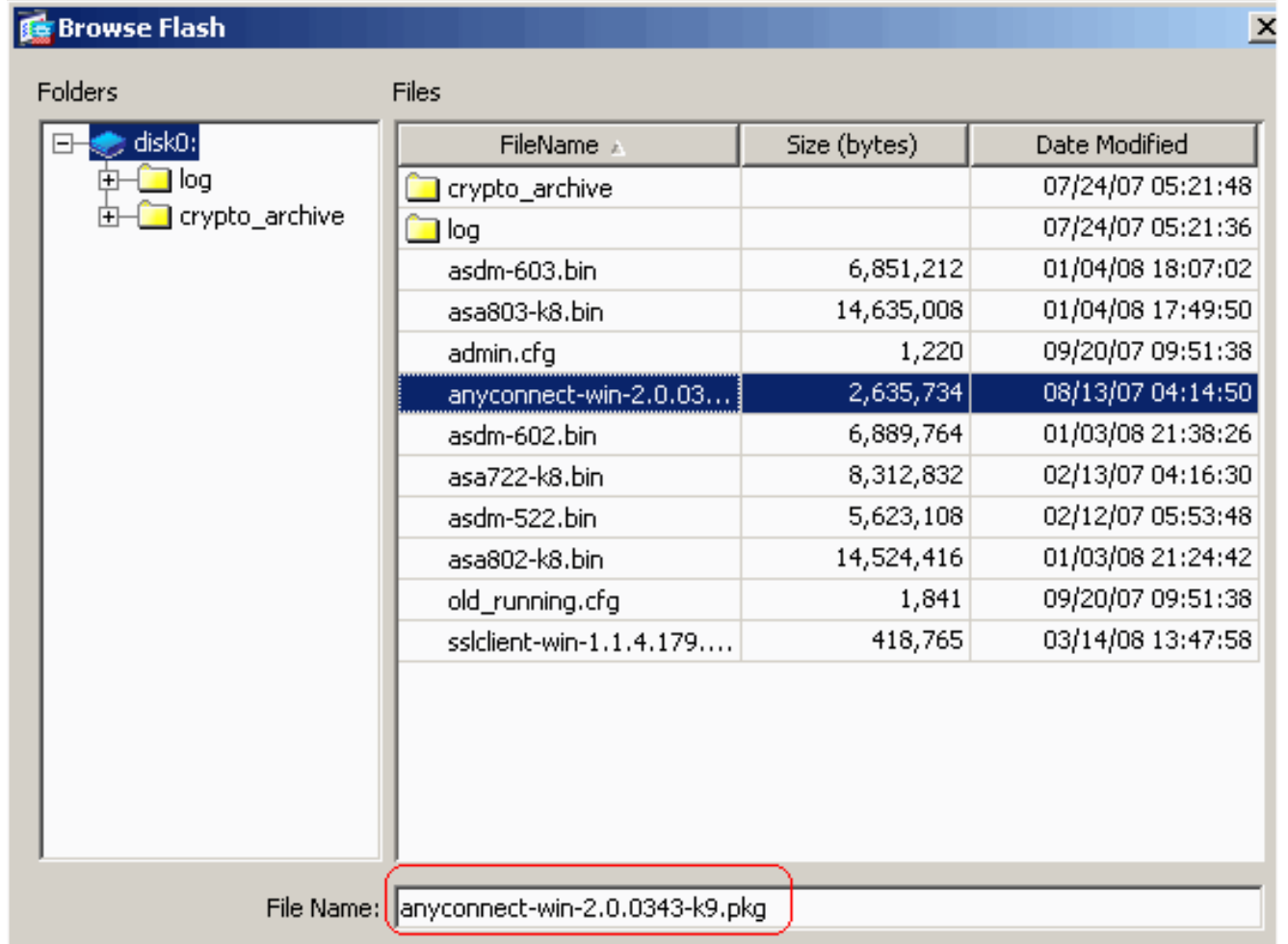
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

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:

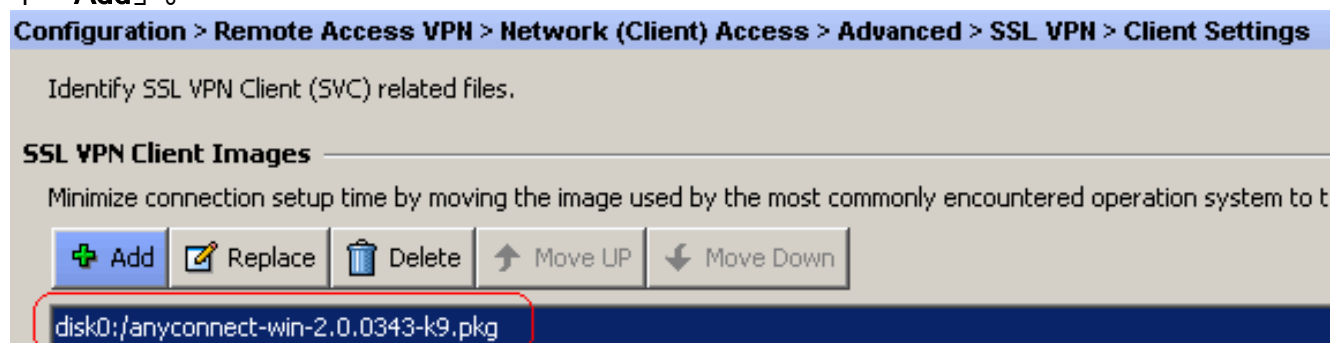
Click here to [Assign Certificate to Interface](#).

按一下「Apply」。選擇**Configuration > Remote Access VPN > Network(Client)Access > Advanced > SSL VPN > Client Settings > Add**，以便從ASA的快閃記憶體中新增Cisco AnyConnect VPN客戶端映像，如下所示。



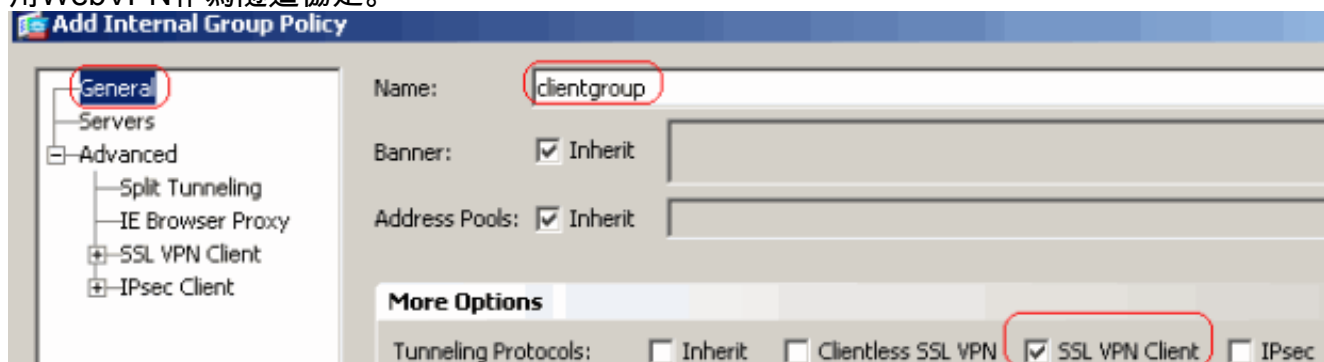
按一下「OK」(確定)。
下「Add」。

按一

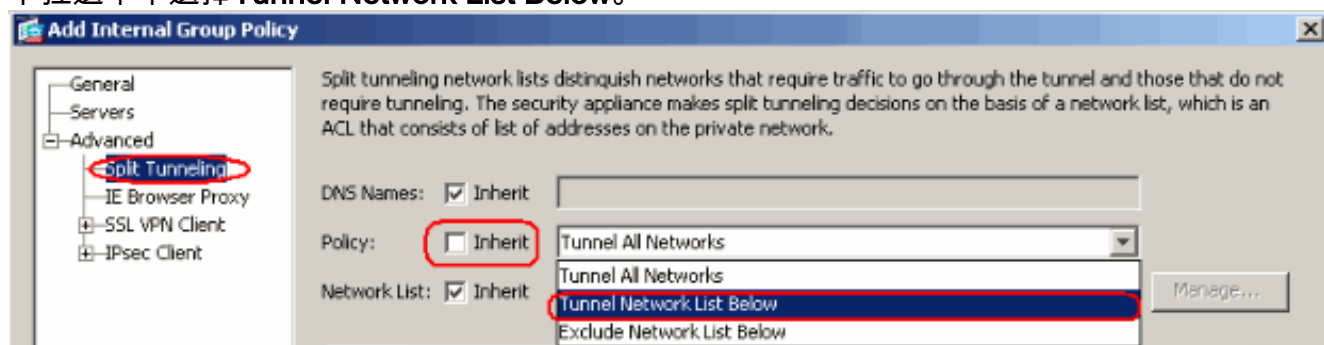


等效的CLI配置：

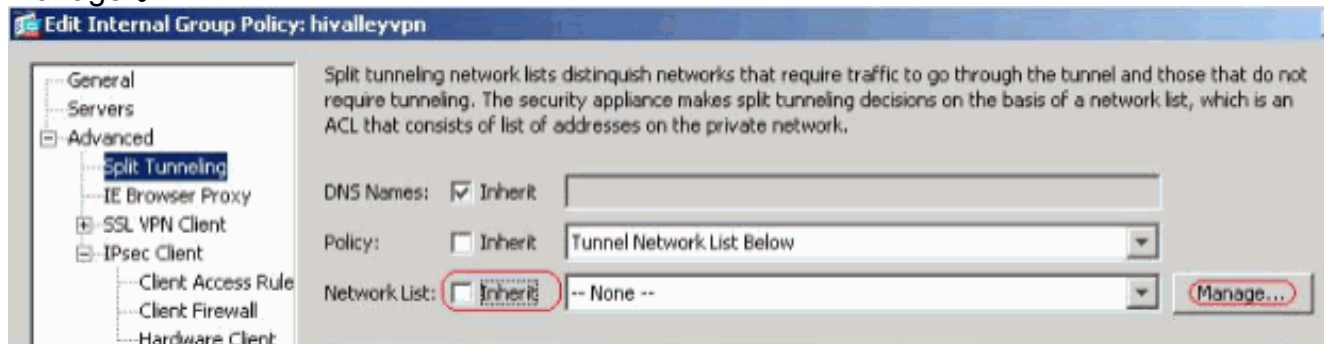
4. 配置組策略。選擇 Configuration > Remote Access VPN > Network(Client)Access > Group Policies，以建立內部組策略客戶端組。在 General 頁籤下，選中 SSL VPN Client 覆取方塊以啟用 WebVPN 作為隧道協定。



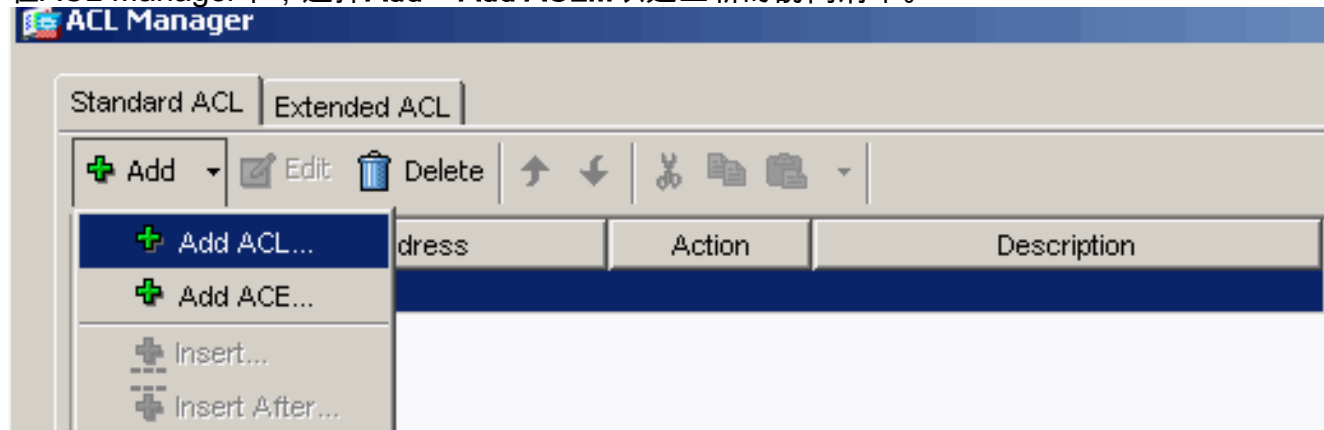
在 Advanced > Split Tunneling 頁籤中，取消選中 Split Tunnel Policy 的 Inherit 覆取方塊，然後從下拉選單中選擇 Tunnel Network List Below。



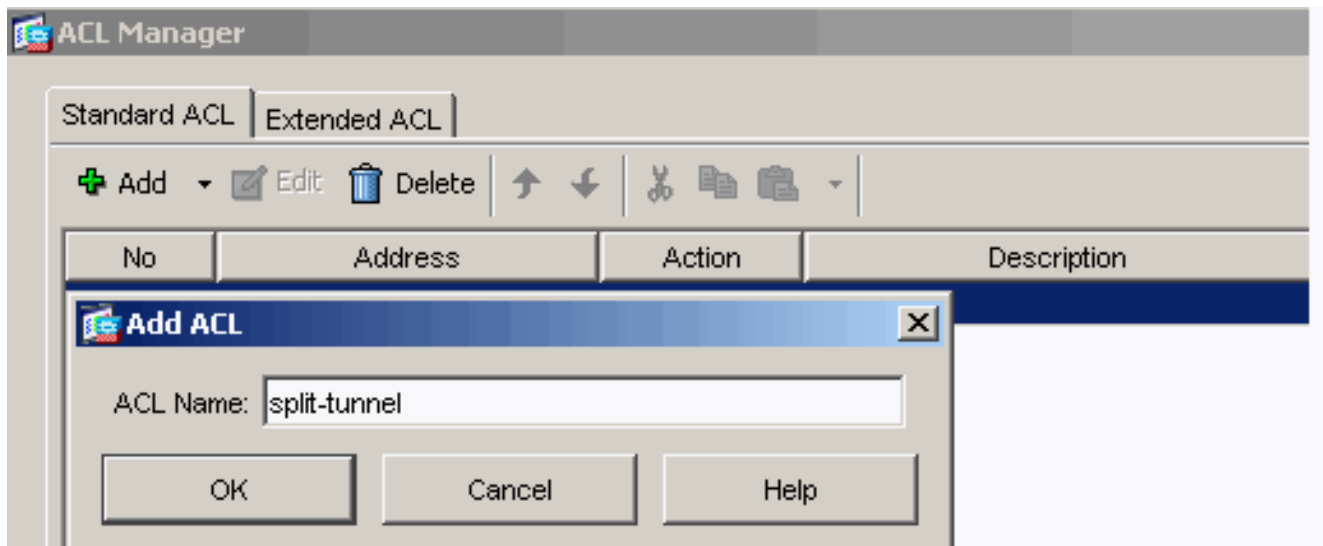
取消選中 Split Tunnel Network List 的 Inherit 覆取方塊，然後按一下 Manage 以啟動 ACL Manager。



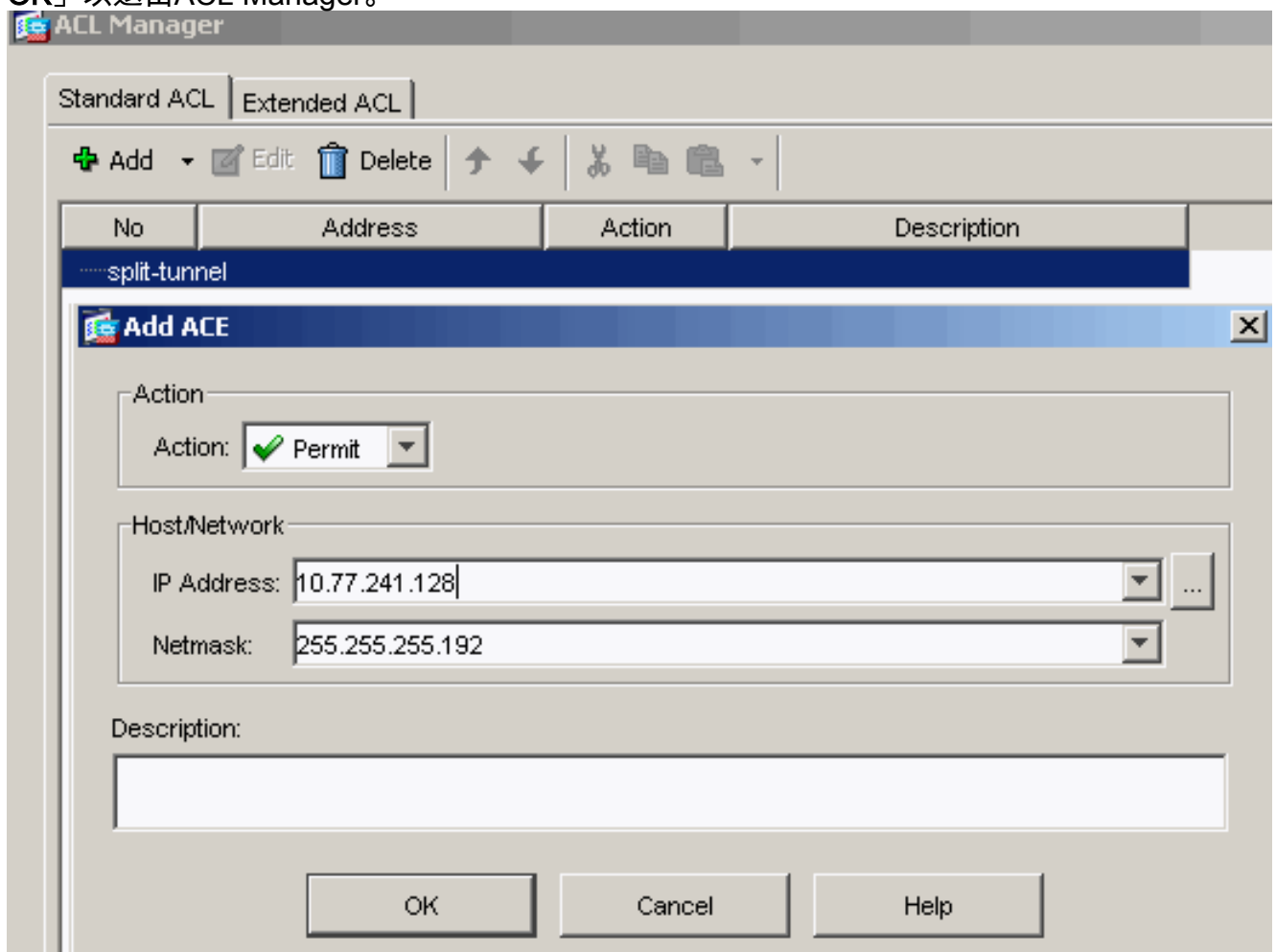
在 ACL Manager 中，選擇 Add > Add ACL... 以建立新的訪問清單。



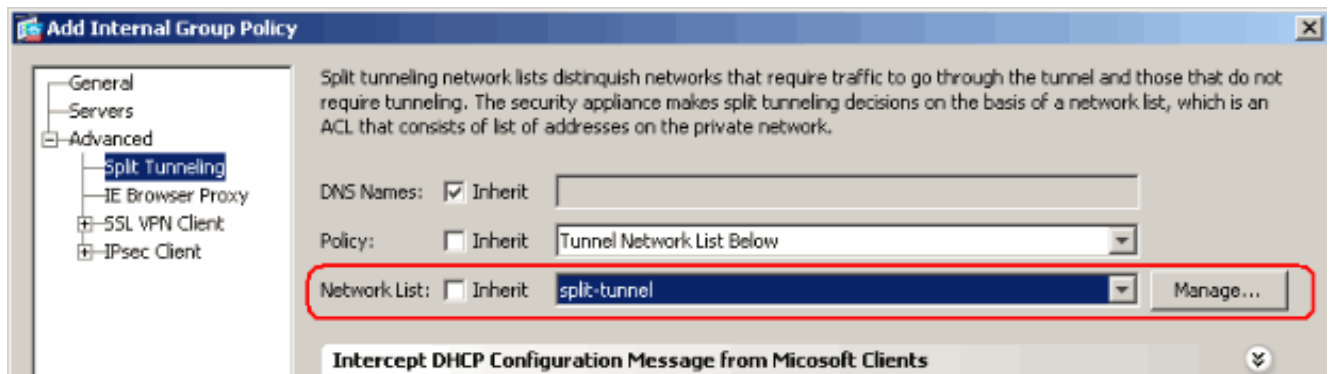
提供 ACL 的名稱，然後按一下 OK。



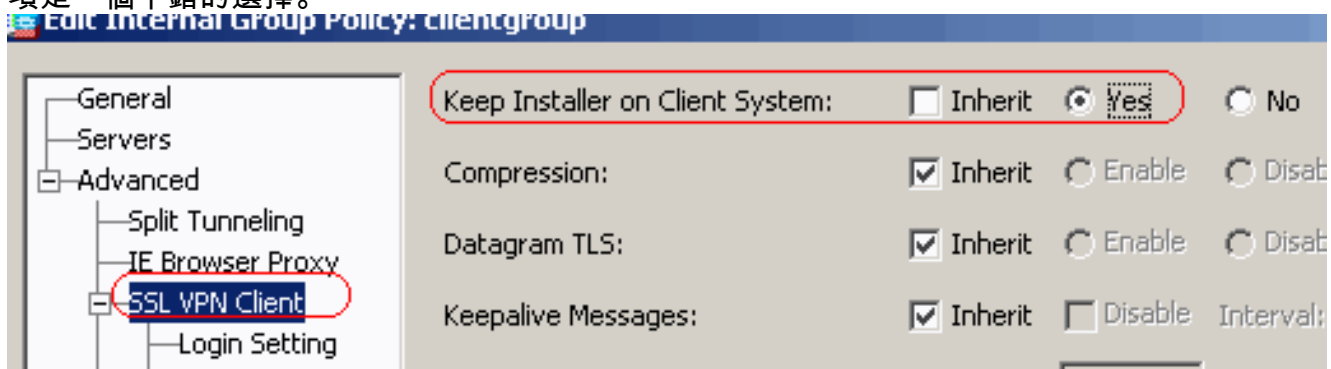
建立ACL名稱后，選擇Add > Add ACE以新增訪問控制條目(ACE)。定義與ASA後面的LAN對應的ACE。在這種情況下，網路為10.77.241.128/26，然後選擇Permit作為Action。按一下「OK」以退出ACL Manager。



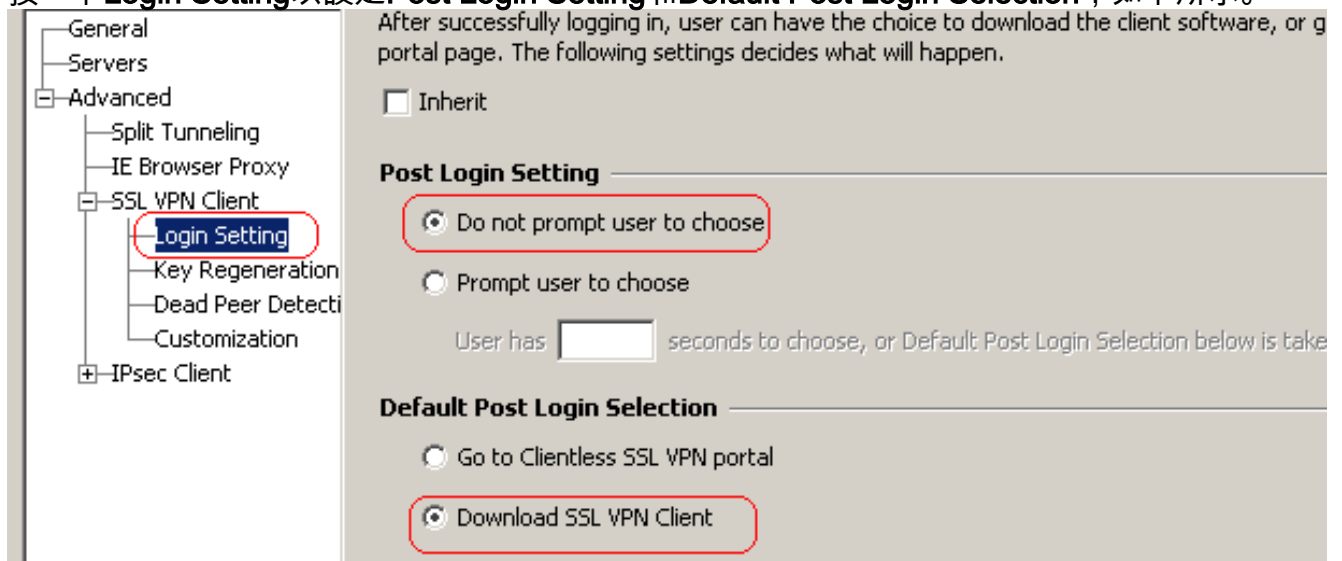
確保為分割隧道網路清單選擇了您剛剛建立的ACL。按一下OK以返回組策略配置。



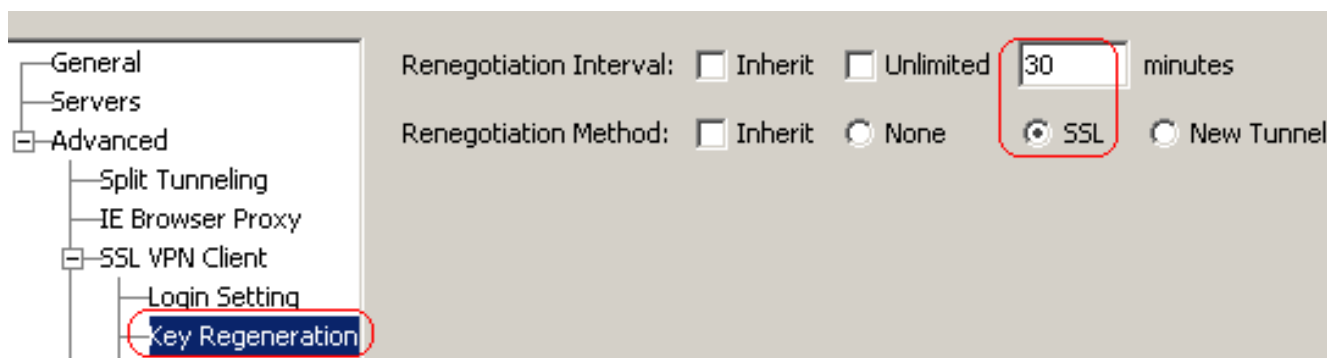
在首頁上，按一下**Apply**，然後按一下**Send**（如果需要），以將命令傳送到ASA。在組策略模式下配置SSL VPN設定。對於Keep Installer on Client System選項，取消選中**Inherit**覈取方塊，然後按一下**Yes**單選按鈕。此操作允許SVC軟體保留在客戶端電腦上。因此，每次建立連線時，都不需要ASA將SVC軟體下載到客戶端。對於經常訪問公司網路的遠端使用者來說，此選項是一個不錯的選擇。



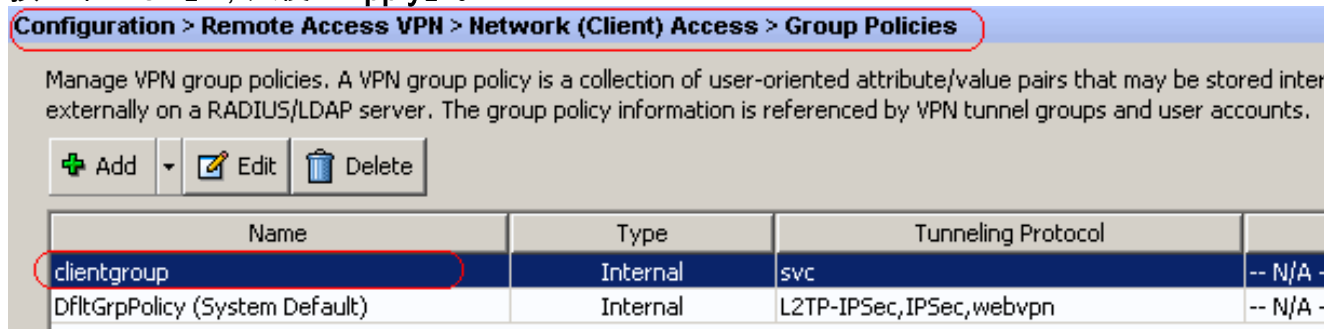
按一下**Login Setting**以設定**Post Login Setting**和**Default Post Login Selection**，如下所示。



對於Renegotiation Interval選項，取消選中**Inherit**框，取消選中**Unlimited**覈取方塊，並輸入重新生成金鑰之前的分鐘數。通過對金鑰的有效時間長度設定限制來提高安全性。對於Renegotiation Method選項，取消選中**Inherit**覈取方塊，然後按一下**SSL**單選按鈕。重新交涉可以使用目前的SSL通道或專門為重新交涉建立的新通道。

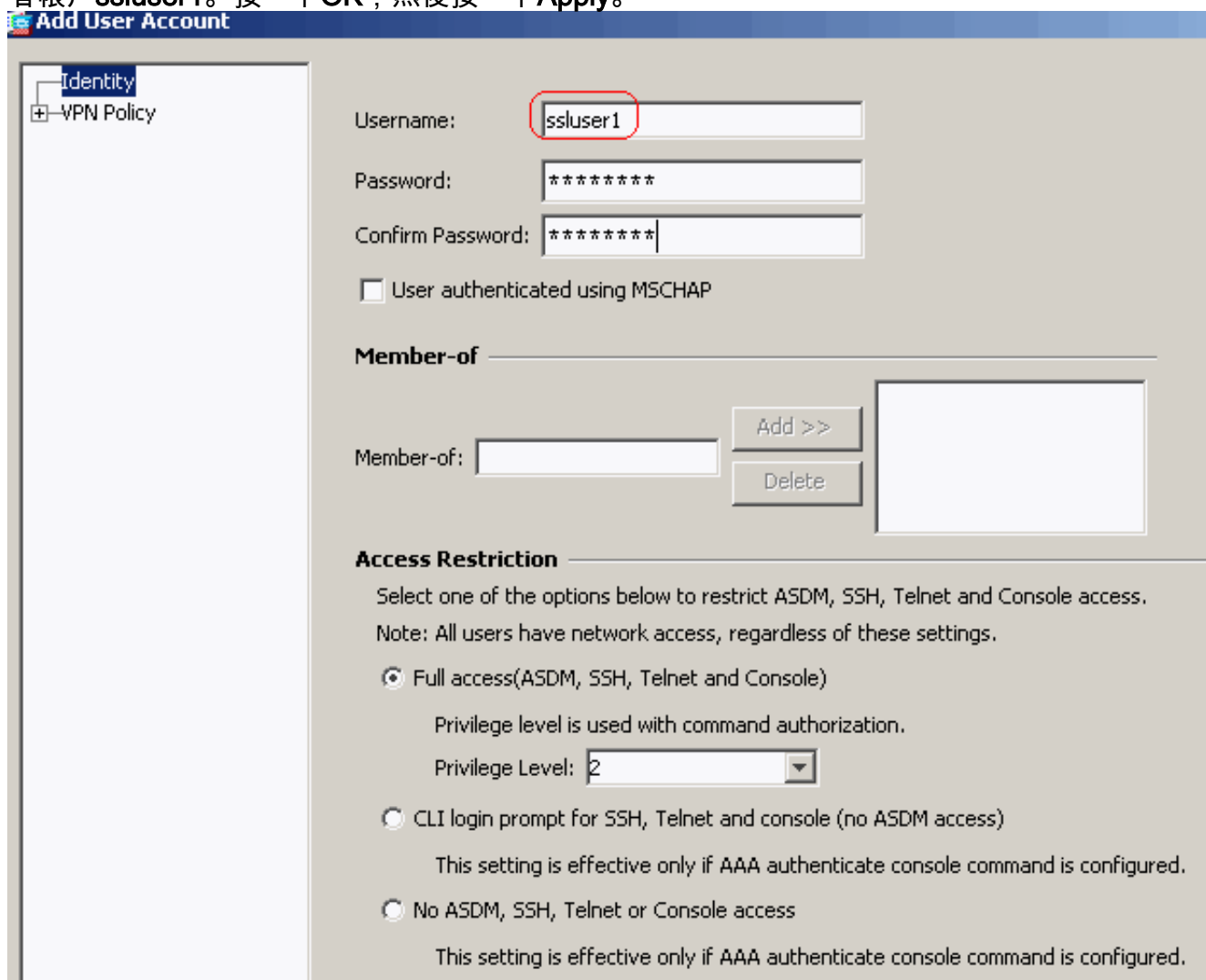


按一下「OK」，然後「Apply」。



等效的CLI配置：

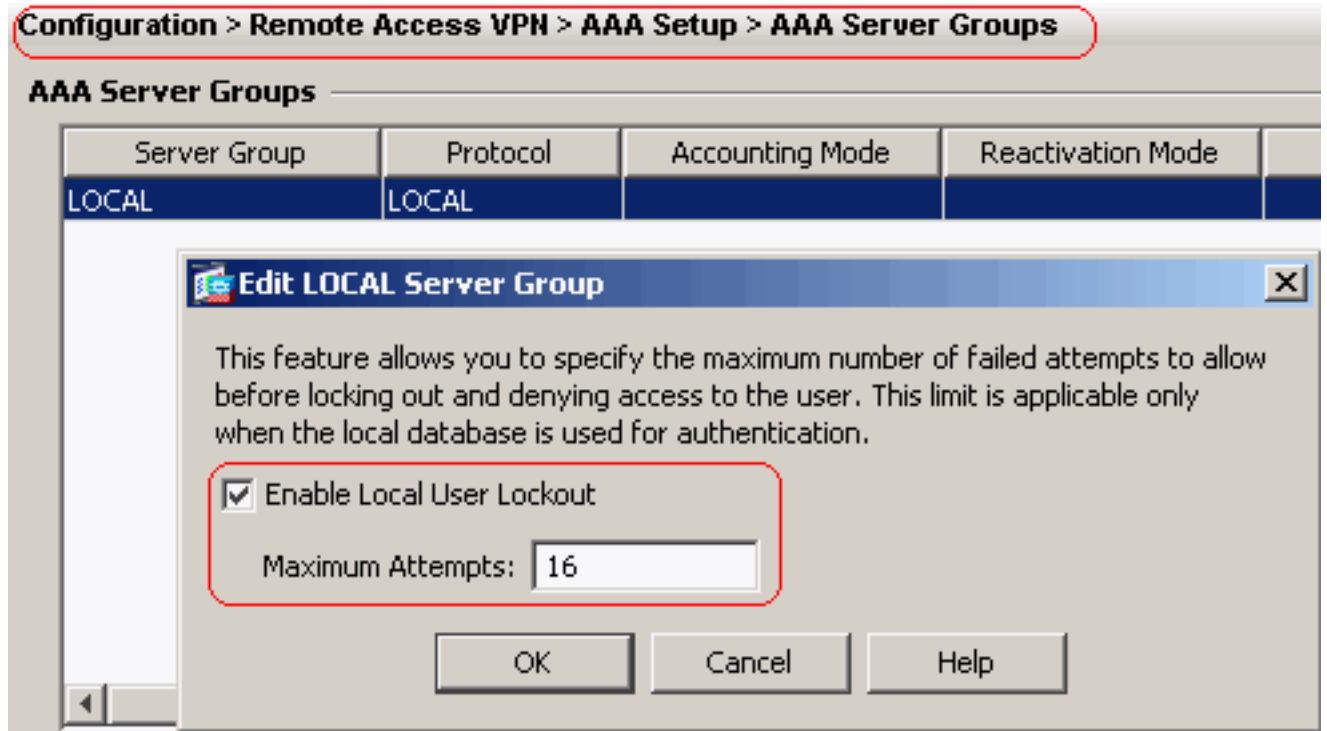
- 選擇 Configuration > Remote Access VPN > AAA Setup > Local Users > Add 以建立新的使用者帳戶 `ssluser1`。按一下 OK，然後按一下 Apply。



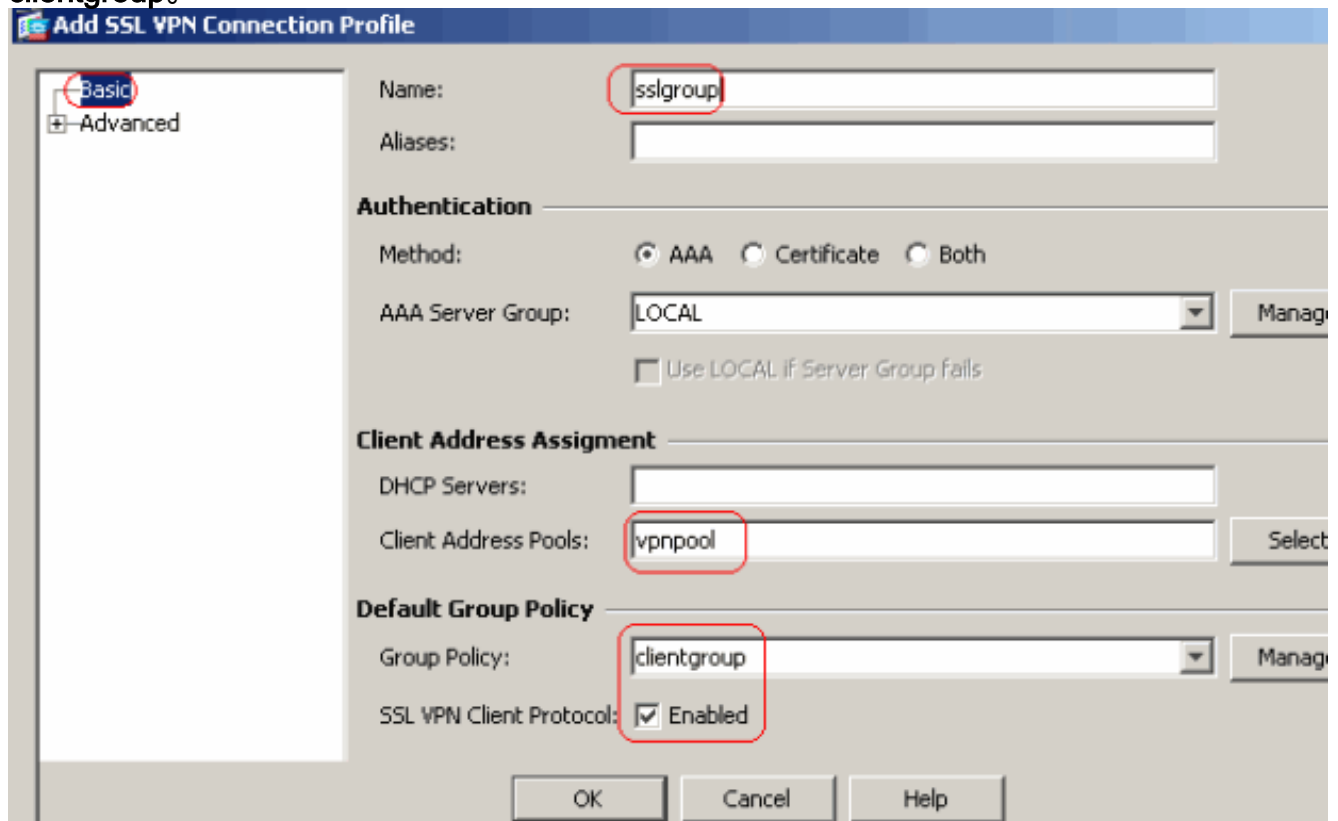
等效的CLI配置：

- 選擇 Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit，以通

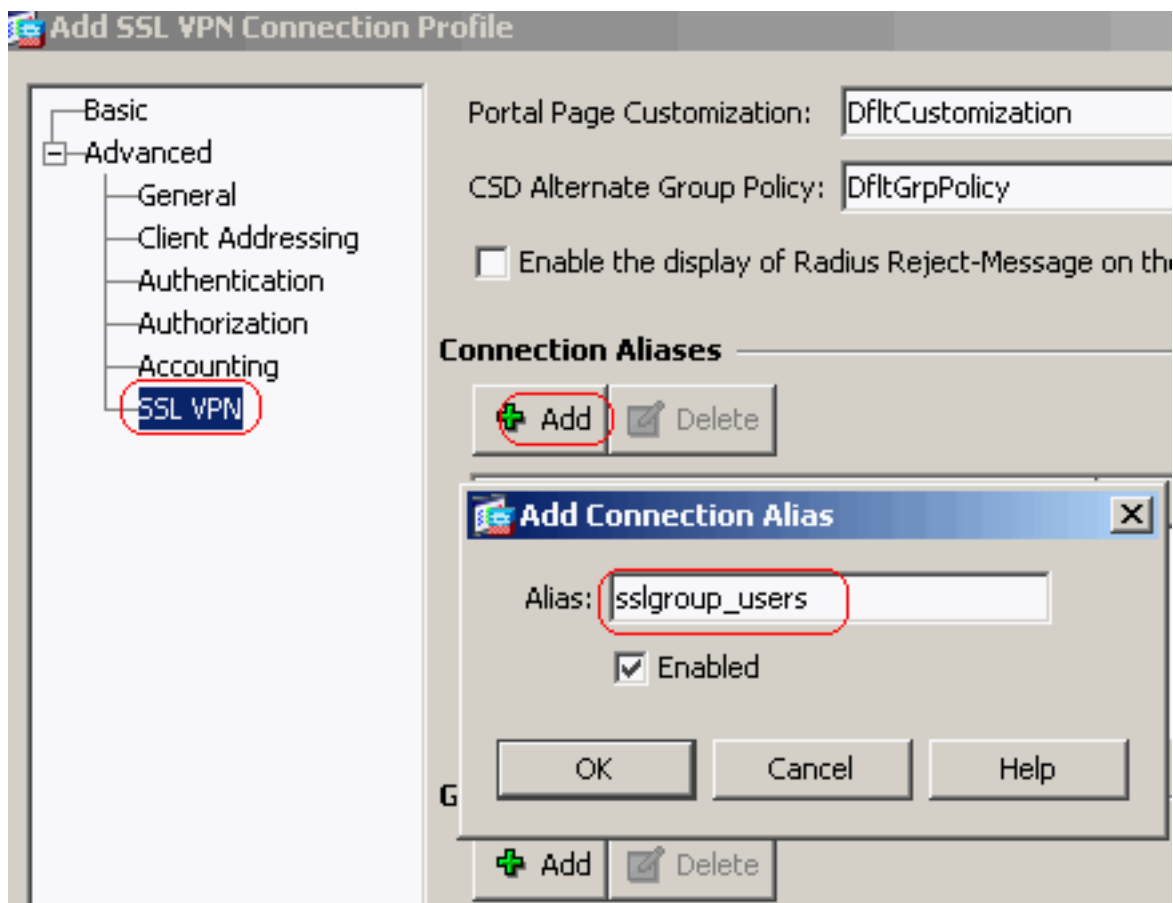
過選中Enable Local User Lockout覈取方塊(最大嘗試次數值為16)來修改預設伺服器組LOCAL。



7. 按一下「OK」，然後「Apply」。等效的CLI配置：
8. 配置隧道組。選擇Configuration > Remote Access VPN > Network(Client)Access > SSL VPN Connection Profiles Connection Profiles > Add以建立新的隧道組sslgroup。在Basic索引標籤中，您可以執行以下配置清單：將隧道組命名為sslgroup。在Client Address Assignment下，從下拉選單中選擇地址池vpnpool。在Default Group Policy下，從下拉選單中選擇組策略clientgroup。



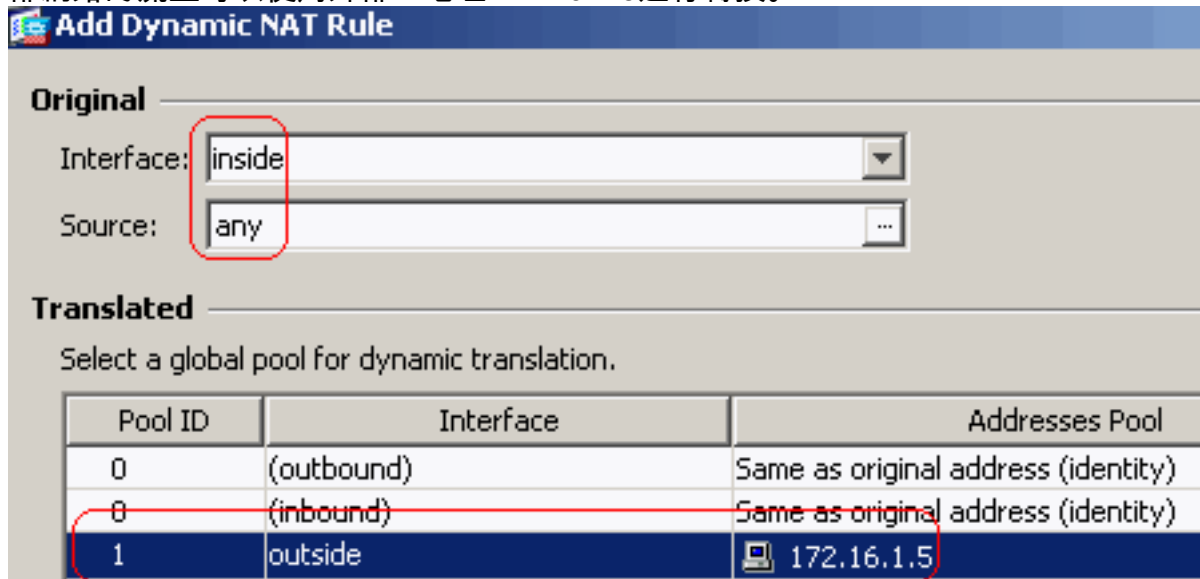
在SSL VPN > Connection Aliases頁籤下，將組別名指定為sslgroup_users，然後按一下OK。



按一下「

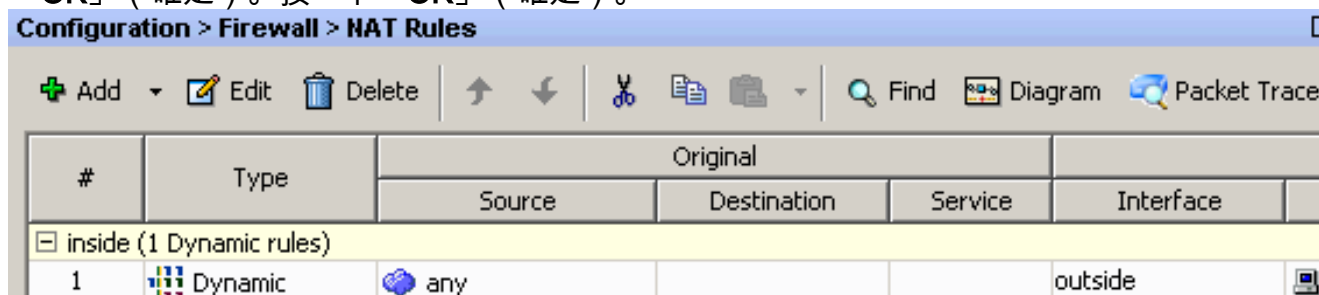
OK」，然後「Apply」。等效的CLI配置：

9. 配置NAT。選擇 Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule，以便來自內部網路的流量可以使用外部IP地址172.16.1.5進行轉換。



按一下

「OK」(確定)。按一下「OK」(確定)。



按一下「Apply」。等效的CLI配置：

10. 為從內部網路到VPN客戶端的返回流量配置nat免除。

```
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配置

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)#

```

使用SVC建立SSL VPN連線

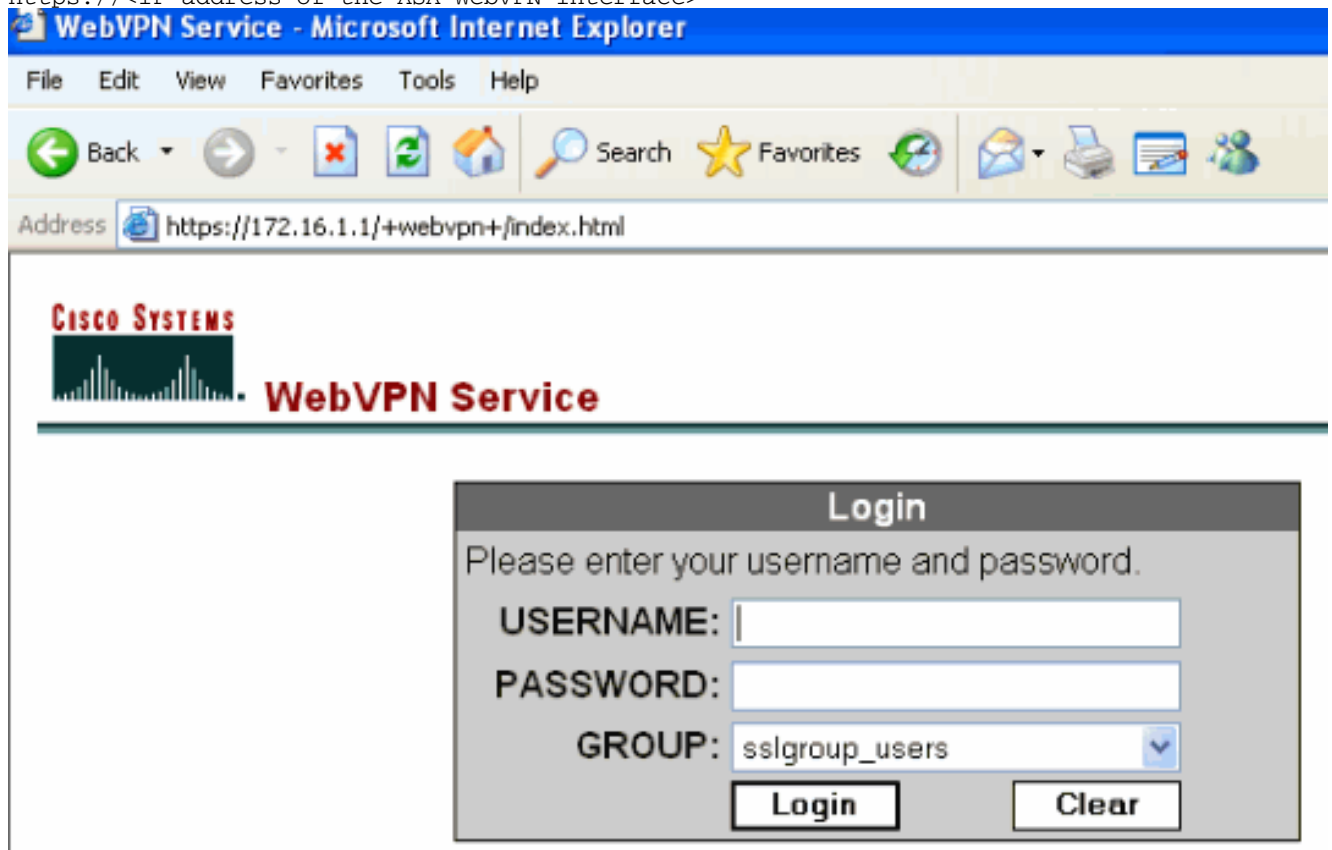
完成以下步驟，以便與ASA建立SSL VPN連線：

1. 在Web瀏覽器中，按如下所示格式輸入ASA WebVPN介面的URL或IP地址。

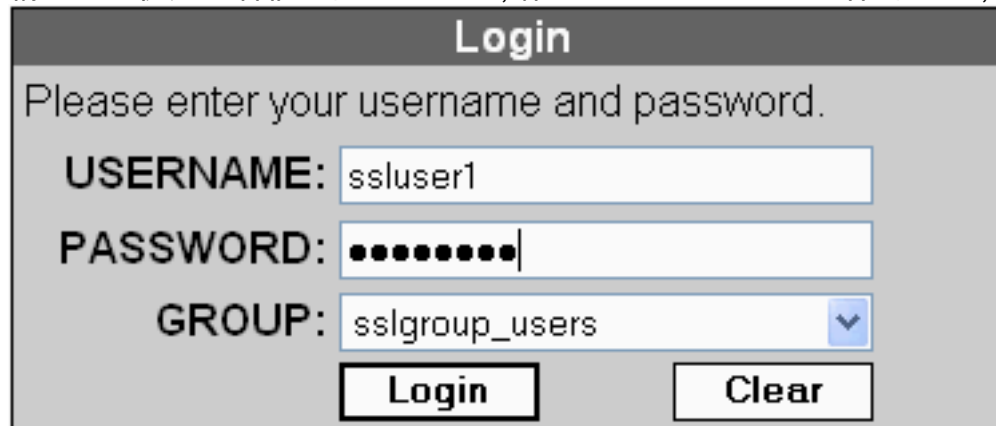
https://url

或

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



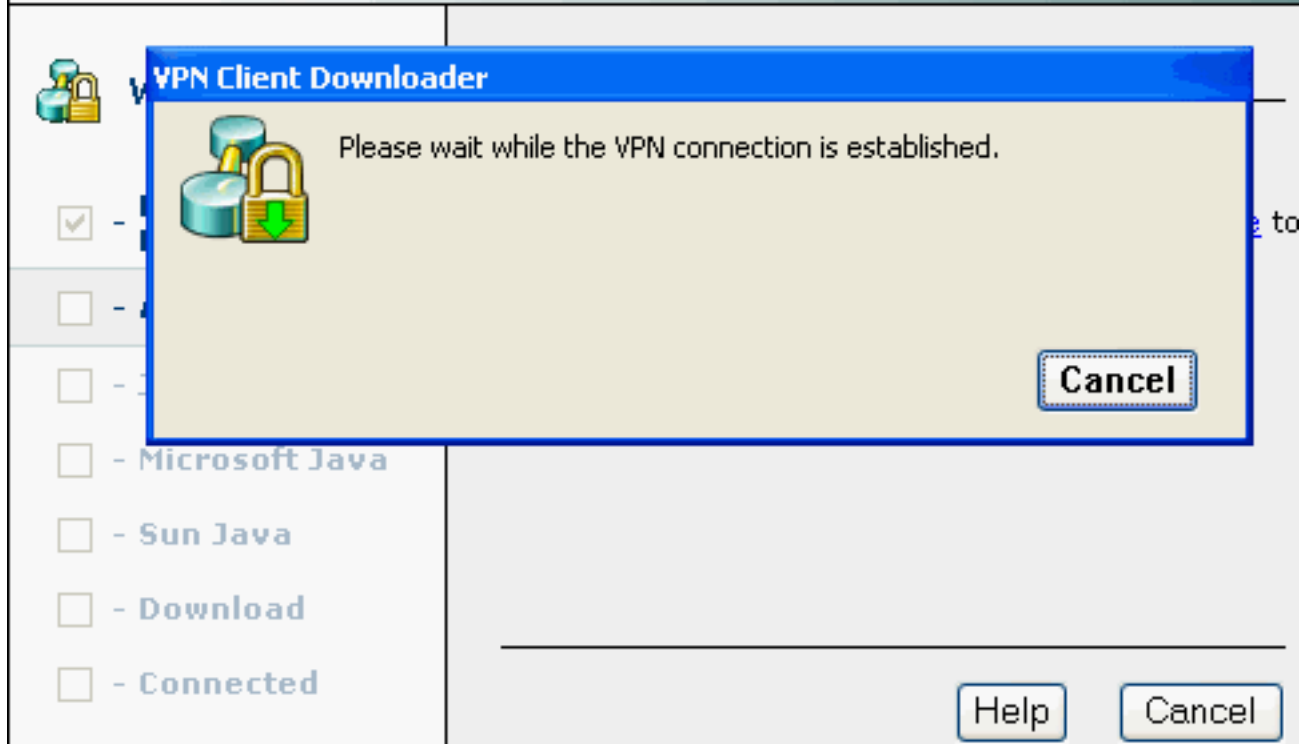
2. 輸入您的使用者名稱和密碼。此外，請從下拉選單中選擇您各自的組，如下所示。



此視窗在建立SSL
VPN連線之前出現。



Cisco AnyConnect VPN Client



注意：下載SVC之前，必須在電腦中安裝ActiveX軟體。一旦建立連線，您就會收到此視窗。



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:



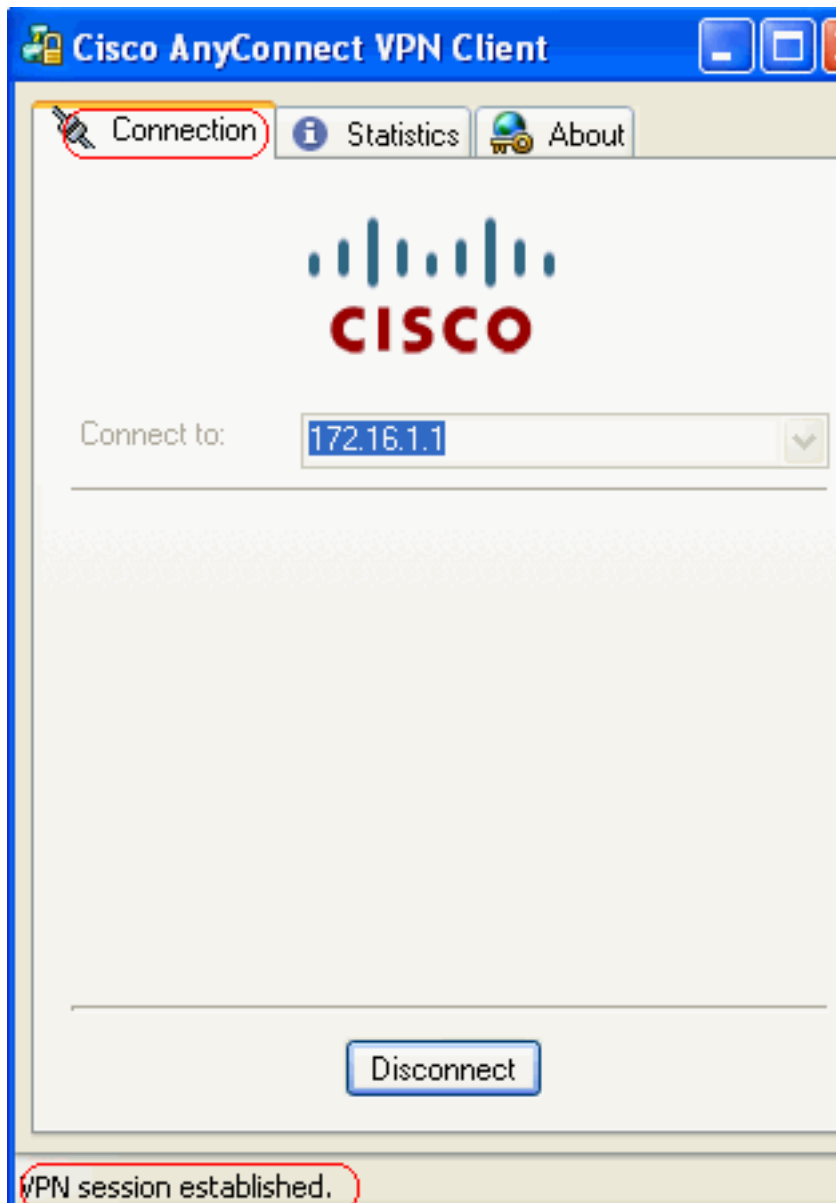
Help

Cancel

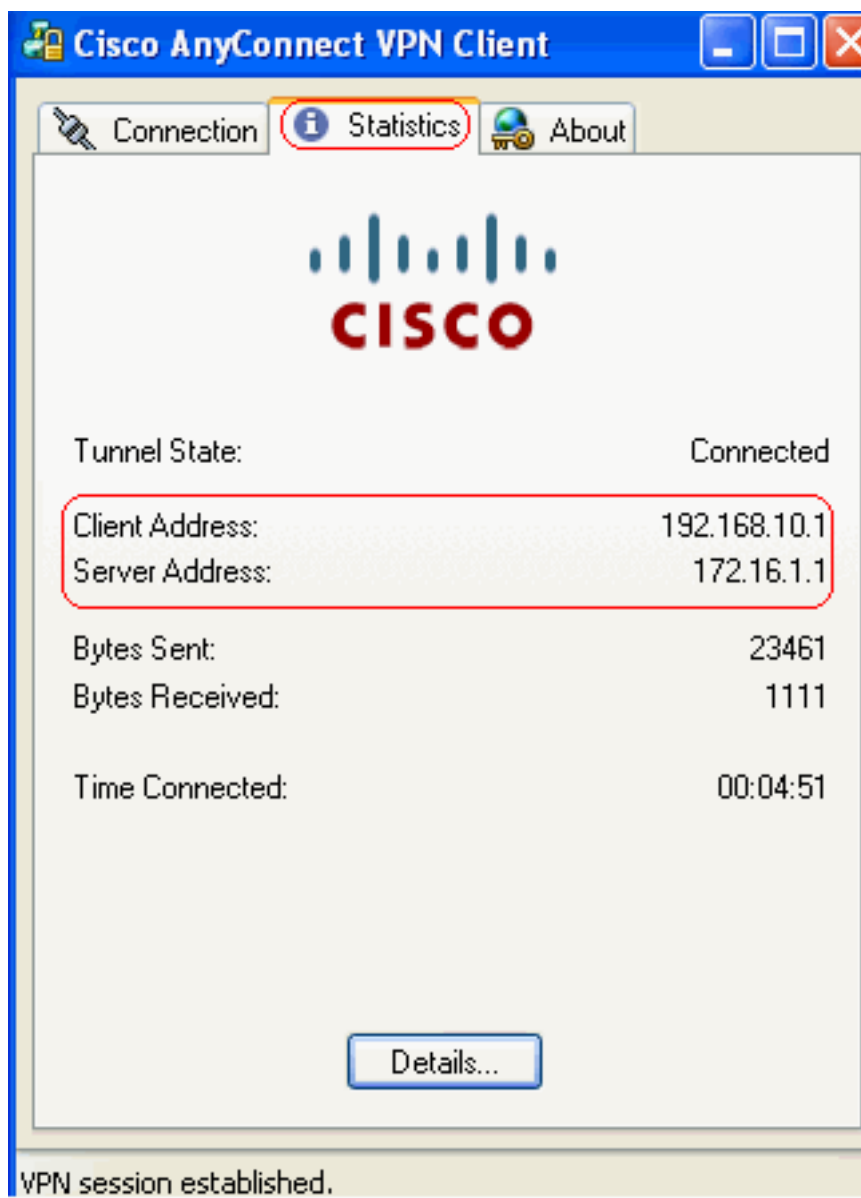
system... anyconnect - Paint

Cisco AnyConnect Connected

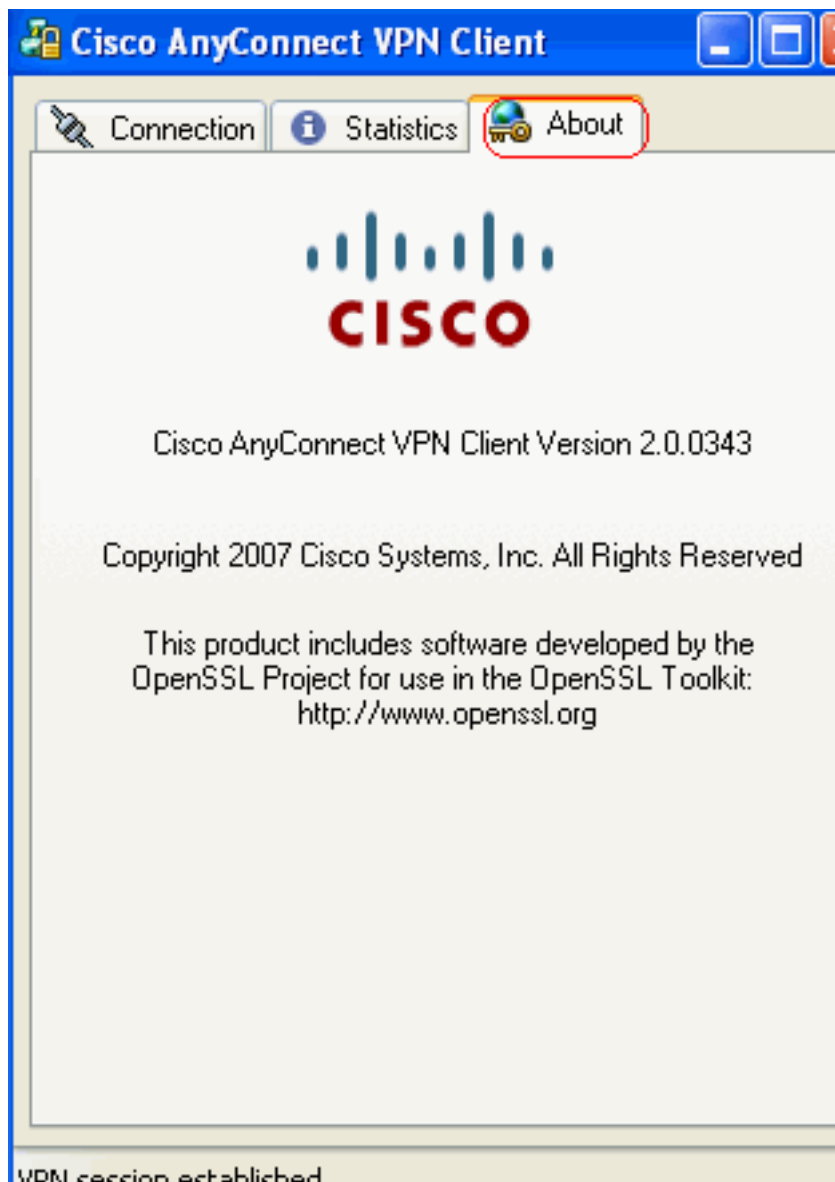
3. 按一下出現在電腦工作列中的鎖定。



出現此視窗並提供有關SSL連線的資訊。例如，192.168.10.1是ASA分配的IP，等等。



此視窗顯示Cisco AnyConnect



VPN客戶端版本資訊。 VPN session established

驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

- **show webvpn svc** — 顯示儲存在ASA快閃記憶體中的SVC映像。

```
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** — 顯示有關當前SSL連線的資訊。

```
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** — 顯示各種組的已配置別名。

```

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

```

- 在ASDM中，選擇Monitoring > VPN > VPN Statistics > Sessions以瞭解ASA中的當前WebVPN會話。

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

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. **vpn-sessiondb logoff name <username>** — 用於註銷特定使用者名稱的SSL VPN會話的命令

```

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)

```

同樣，您可以使用**vpn-sessiondb logoff svc**命令終止所有SVC會話。

2. **注意**：如果PC進入待機或休眠模式，SSL VPN連線可以終止。

```

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> — 提供即時webvpn事件以建立會話。

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

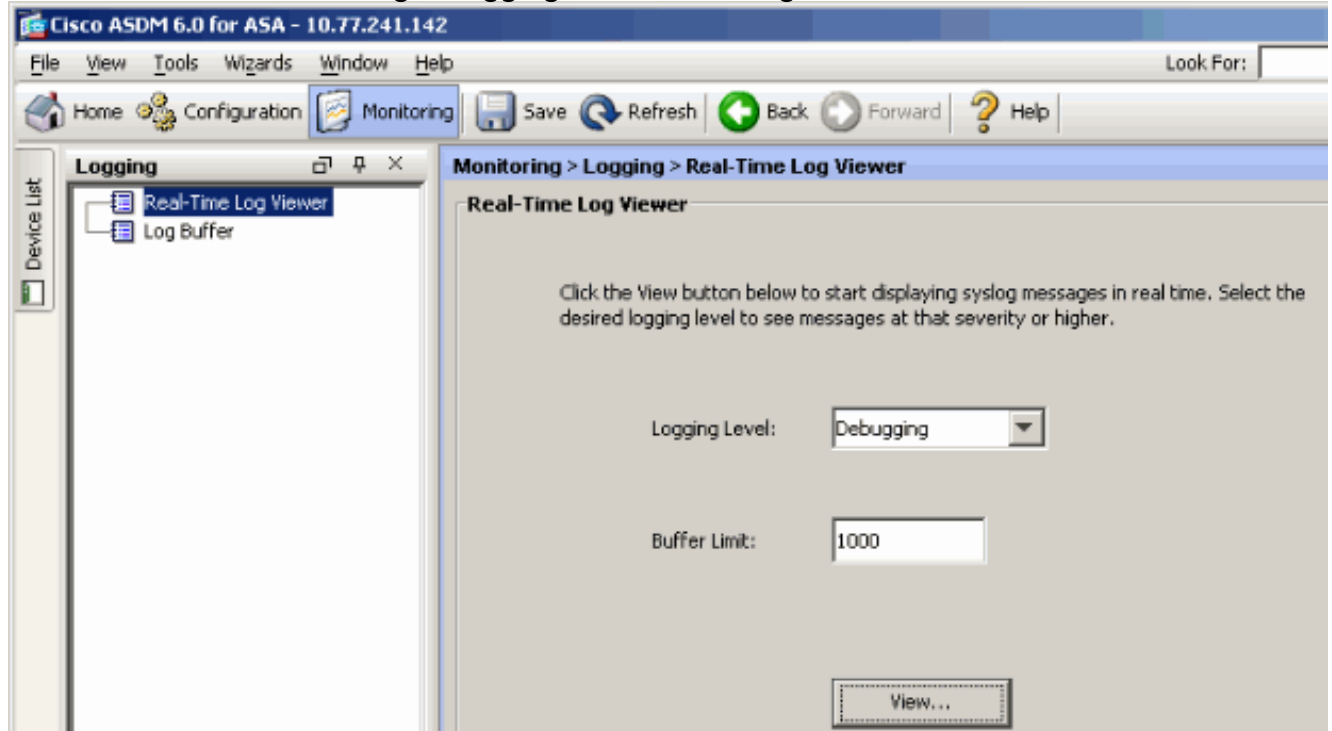
```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: 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: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AF9B9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AF9B9501758FF3B7B5545973C06F6393C92E59693'
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
```

```

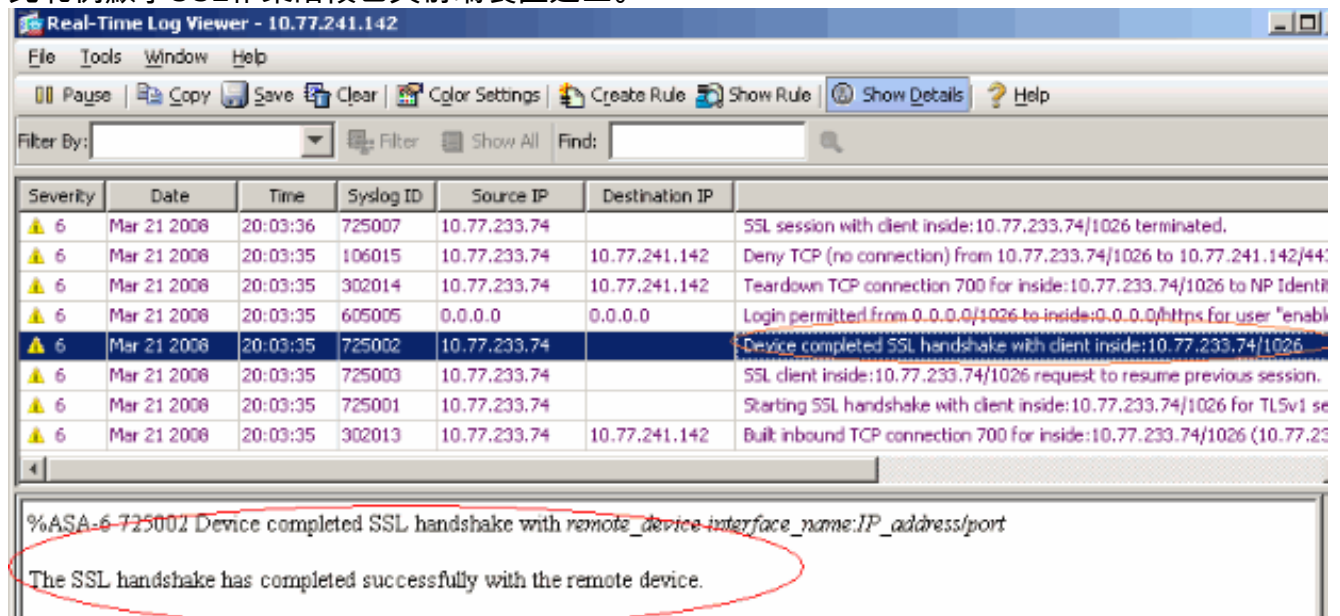
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy

```

4. 在ASDM中，選擇Monitoring > Logging > Real-time Log Viewer > View以檢視即時事件。



此範例顯示SSL作業階段已與前端裝置建立。



相關資訊

- [Cisco 5500系列調適型安全裝置支援頁面](#)
- [AnyConnect VPN客戶端2.0版發行說明](#)

- [ASA/PIX:允許在ASA上為VPN客戶端分割隧道的配置示例](#)
- [路由器允許VPN客戶端使用分割隧道連線IPsec和Internet的配置示例](#)
- [單臂公共網際網路VPN的PIX/ASA 7.x和VPN客戶端配置示例](#)
- [帶ASDM的ASA上的SSL VPN客戶端\(SVC\)配置示例](#)
- [技術支援與文件 - Cisco Systems](#)