

# ASA/PIX 8.x:使用CLI和ASDM的可下載ACL進行VPN訪問的RADIUS授權(ACS 4.x)配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[設定遠端存取VPN\(IPSec\)](#)

[使用CLI配置ASA/PIX](#)

[Cisco VPN客戶端配置](#)

[為個人使用者的可下載ACL配置ACS](#)

[為組的可下載ACL配置ACS](#)

[為使用者組配置IETF RADIUS設定](#)

[驗證](#)

[Show Crypto命令](#)

[使用者/組的可下載ACL](#)

[Filter-Id ACL](#)

[疑難排解](#)

[清除安全關聯](#)

[疑難排解指令](#)

[相關資訊](#)

## 簡介

本文檔介紹如何配置安全裝置以對使用者進行網路訪問身份驗證。由於您可以隱式啟用RADIUS授權，因此本節不包含有關在安全裝置上配置RADIUS授權的資訊。它提供關於安全裝置如何處理從RADIUS伺服器接收的訪問清單資訊的資訊。

您可以配置RADIUS伺服器將訪問清單下載到安全裝置或在身份驗證時下載訪問清單名稱。使用者僅有權執行使用者特定訪問清單中允許的行為。

使用Cisco Secure ACS為每個使用者提供適當的訪問清單時，可下載訪問清單是最具可擴充性的方式。如需可下載存取清單功能和Cisco Secure ACS的詳細資訊，請參閱[設定RADIUS伺服器以傳送可下載存取控制清單](#)和[可下載IP ACL](#)。

請參閱[ASA 8.3及更高版本：使用可下載ACL通過CLI進行VPN訪問的RADIUS授權\(ACS 5.x\)和ASDM配置示例](#)在8.3版及更高版本的Cisco ASA上執行相同配置。

## 必要條件

### 需求

本文檔假定ASA已完全正常運行並配置為允許Cisco ASDM或CLI進行配置更改。

註：請參閱[允許ASDM或PIX/ASA 7.x的HTTPS訪問：內部和外部介面上的SSH配置示例](#)，允許通過ASDM或安全外殼(SSH)遠端配置裝置。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科自適應安全裝置軟體版本7.x及更高版本
- 思科自適應安全裝置管理器5.x版及更高版本
- Cisco VPN客戶端4.x版及更高版本
- 思科安全存取控制伺服器4.x

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。

### 相關產品

此配置還可以與Cisco PIX安全裝置7.x版及更高版本配合使用。

### 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 背景資訊

您可以使用可下載的IP ACL建立可應用於許多使用者或使用者組的ACL定義集。這些ACL定義集稱為ACL內容。此外，在合併NAF時，您可以控制傳送到使用者從中尋求訪問的AAA客戶端的ACL內容。即，可下載IP ACL包括一個或多個與所有AAA客戶端相關聯的NAF或（預設情況下）相關聯的ACL內容定義。NAF根據AAA客戶端的IP地址控制指定ACL內容的適用性。有關NAF及其如何監管可下載IP ACL的詳細資訊，請參閱[關於網路訪問過濾器](#)。

可下載IP ACL的運作方式如下：

1. 當ACS向使用者授予網路訪問許可權時，ACS會確定可下載IP ACL是分配給該使用者或使用者組。
2. 如果ACS找到分配給使用者或使用者組的可下載IP ACL，它將確定ACL內容條目是否與傳送RADIUS身份驗證請求的AAA客戶端關聯。
3. 作為使用者會話的一部分，ACS會傳送RADIUS訪問接受資料包、指定命名ACL的屬性和命名ACL的版本。
4. 如果AAA客戶端響應其快取中沒有當前版本的ACL（即ACL是新的或已更改），則ACS會將

ACL (新或更新) 傳送到裝置。

可下載IP ACL是每個使用者或使用者組的RADIUS Cisco-av配對屬性[26/9/1]中設定ACL的替代方案。您可以建立一次可下載IP ACL，為其指定一個名稱，然後在引用其名稱時將可下載IP ACL分配給每個適用的使用者或使用者組。與為每個使用者或使用者組配置RADIUS Cisco-av-pair屬性相比，此方法更有效。

此外，當您使用NAF時，可以將不同的ACL內容應用於與它們使用的AAA客戶端有關的相同使用者或使用者組。將AAA客戶端配置為使用來自ACS的可下載IP ACL後，無需對AAA客戶端進行其他配置。可下載ACL受您建立的備份或複製方法的保護。

在ACS Web介面中輸入ACL定義時，不要使用關鍵字或名稱條目；在所有其他方面，對於要應用可下載IP ACL的AAA客戶端，請使用標準ACL命令語法和語義。您在ACS中輸入的ACL定義包含一條或多條ACL命令。每個ACL命令必須位於單獨的行上。

您可以將一個或多個命名ACL內容新增到可下載IP ACL中。預設情況下，每個ACL內容適用於所有AAA客戶端，但是，如果已定義NAF，則可以將每個ACL內容的適用性限制為與其關聯的NAF中列出的AAA客戶端。也就是說，在使用NAF時，您可以根據您的網路安全策略，使每個ACL內容在一個可下載IP ACL中適用於多個不同的網路裝置或網路裝置組。

此外，您還可以變更ACL內容在可下載IP ACL中的順序。ACS從表的頂部開始檢查ACL內容，並下載它找到的第一個ACL內容與包含所使用的AAA客戶端的NAF一起。設定順序時，如果您將最廣泛適用的ACL內容放在清單的較高位置，就可以確保系統效率。您必須認識到，如果您的NAF包括重疊的AAA客戶端數量，則必須從更具體到更一般地進行。例如，ACS下載任何ACL內容，並使用All-AAA-Clients NAF設定，而不考慮清單下方的內容。

要在特定AAA客戶端上使用可下載IP ACL，AAA客戶端必須遵循以下方向：

- 使用RADIUS進行驗證
- 支援可下載的IP ACL

以下是支援可下載IP ACL的Cisco裝置範例：

- ASA和PIX裝置
- VPN 3000系列集中器
- 執行IOS版本12.3(8)T或更新版本的思科裝置

以下是必須在ACL定義框中輸入VPN 3000/ASA/PIX 7.x+ ACL的格式示例：

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

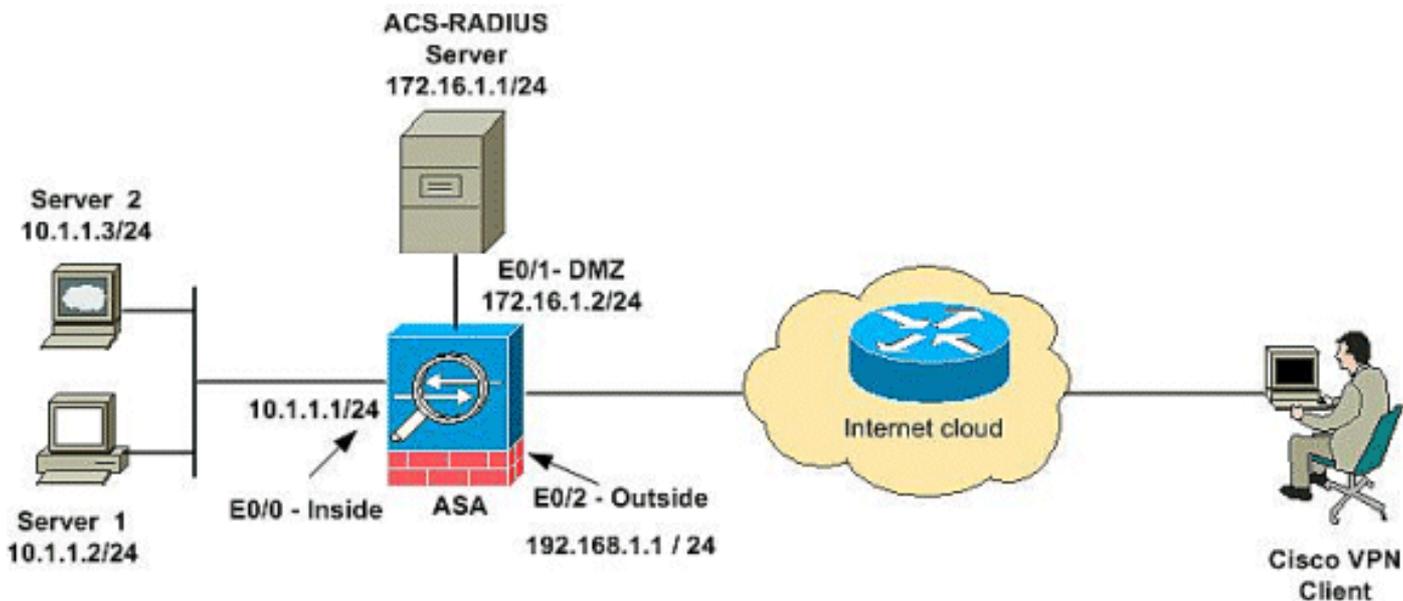
## 設定

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](#)(僅限註冊客戶)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：



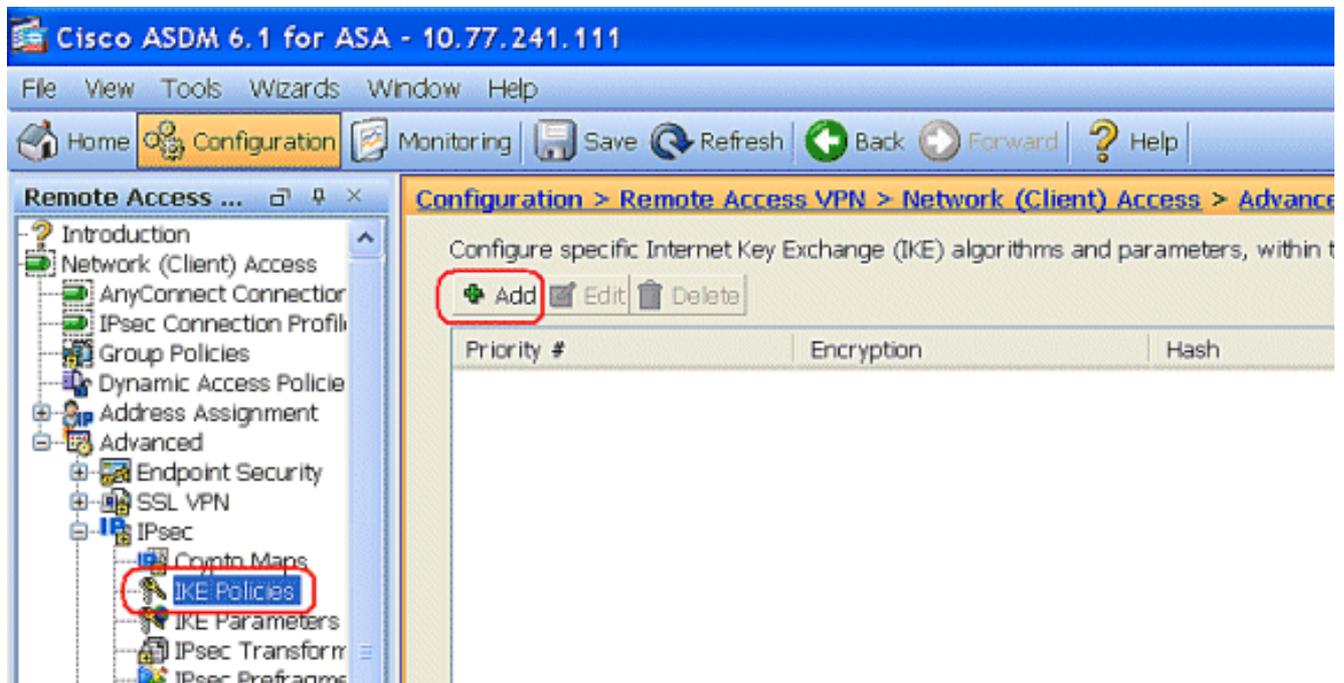
注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

## 設定遠端存取VPN(IPSec)

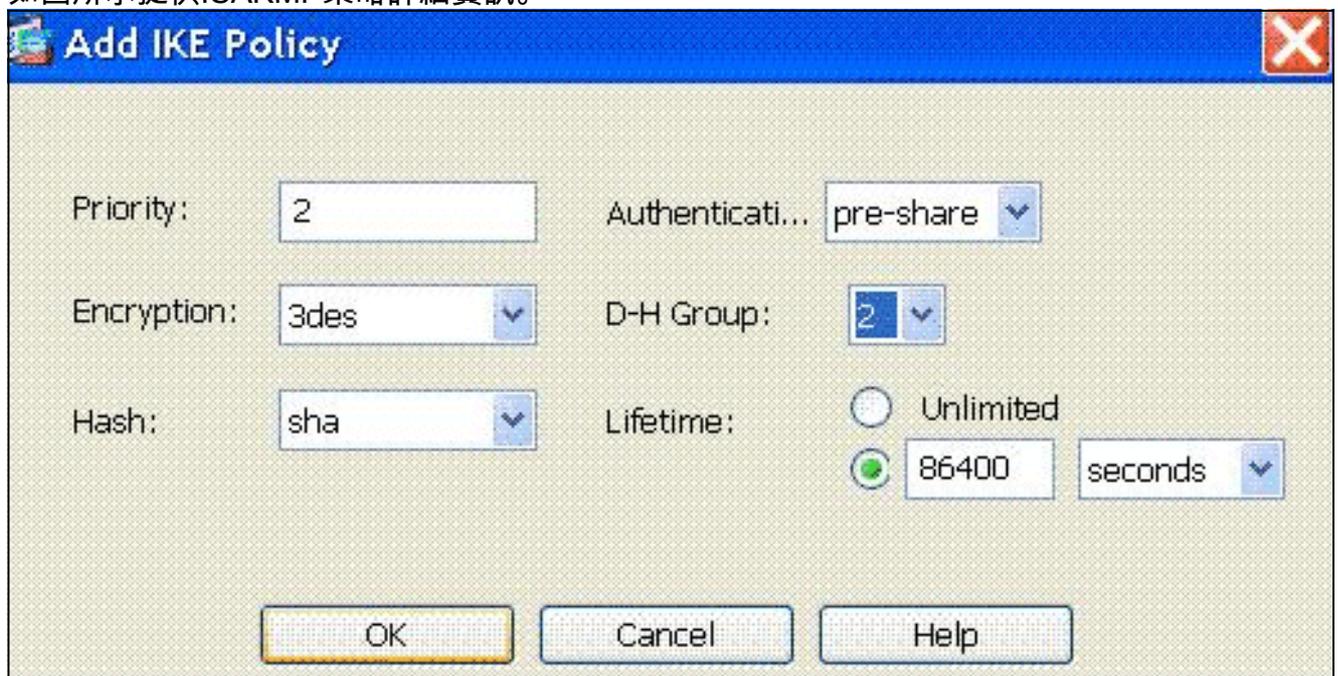
### ASDM過程

完成以下步驟以配置遠端訪問VPN:

1. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies> Add以建立ISAKMP策略。

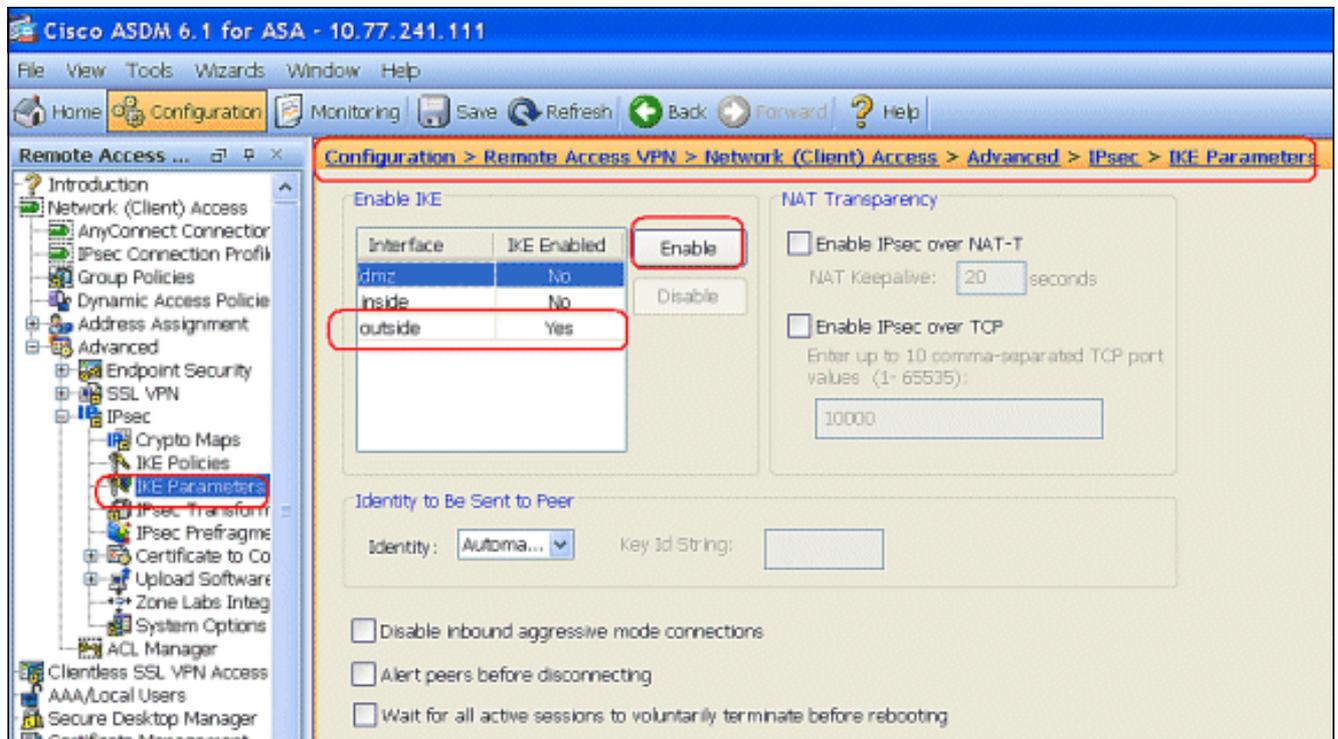


2. 如圖所示提供ISAKMP策略詳細資訊。



按一下「OK」和「Apply」。

3. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > IKE Parameters 以在外部介面上啟用IKE。



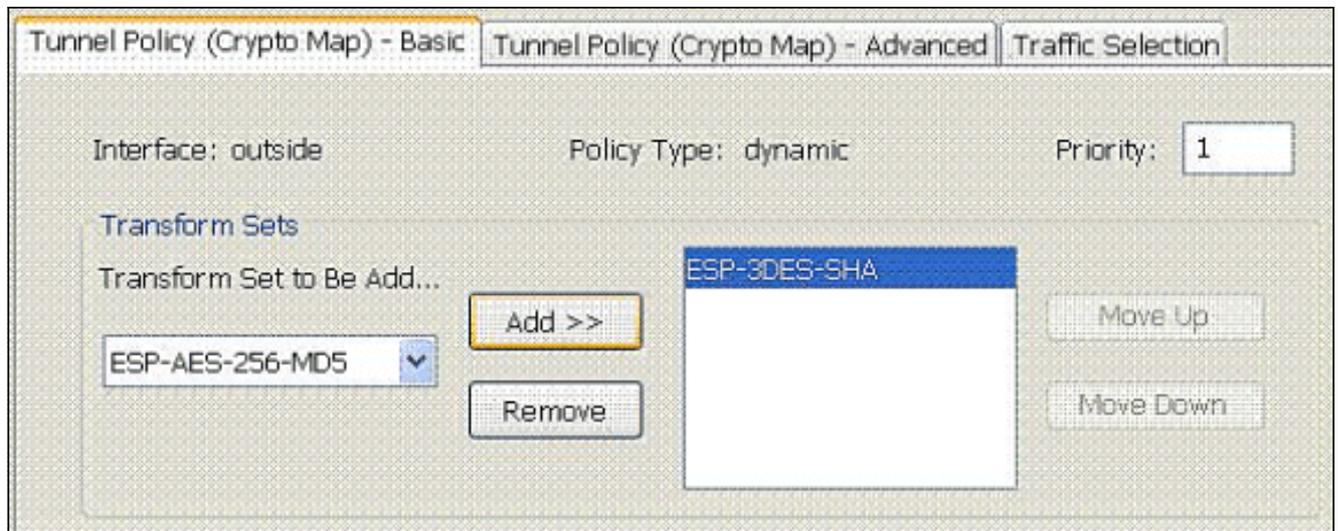
4. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > IPsec Transform Sets > Add 以建立 ESP-3DES-SHA 轉換集，如圖所示。



按一下

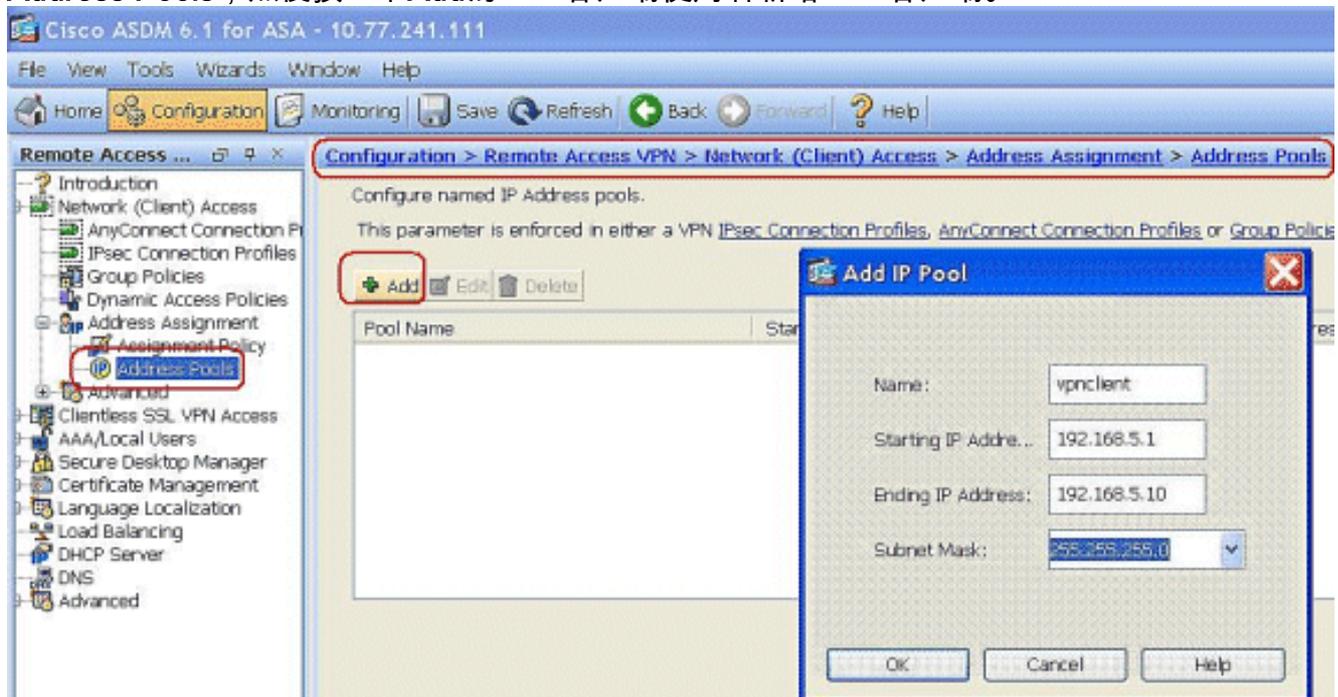
「OK」和「Apply」。

5. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Crypto Maps > Add，以便使用優先順序為1的動態策略建立加密對映，如下所示。

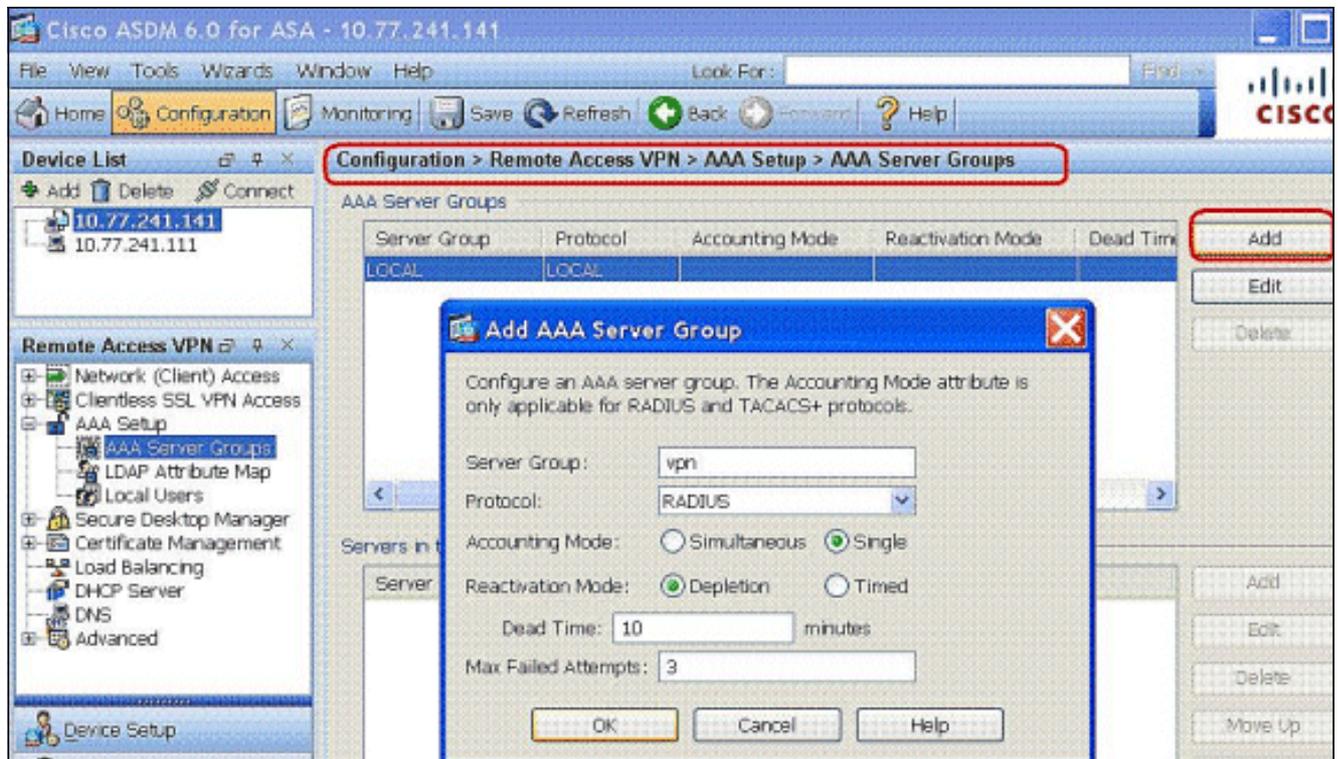


按一下「OK」和「Apply」。

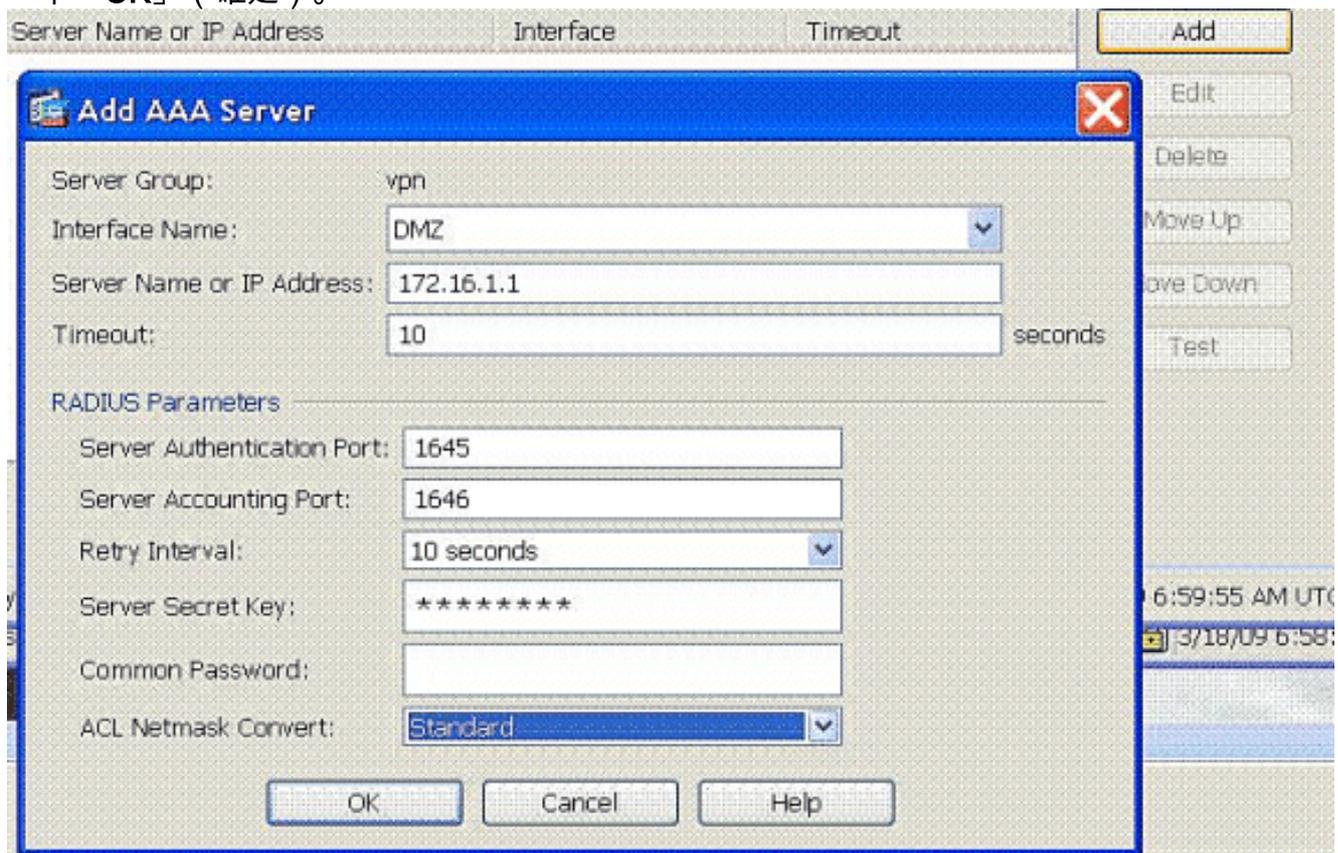
- 選擇 Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools，然後按一下Add為VPN客戶端使用者新增VPN客戶端。



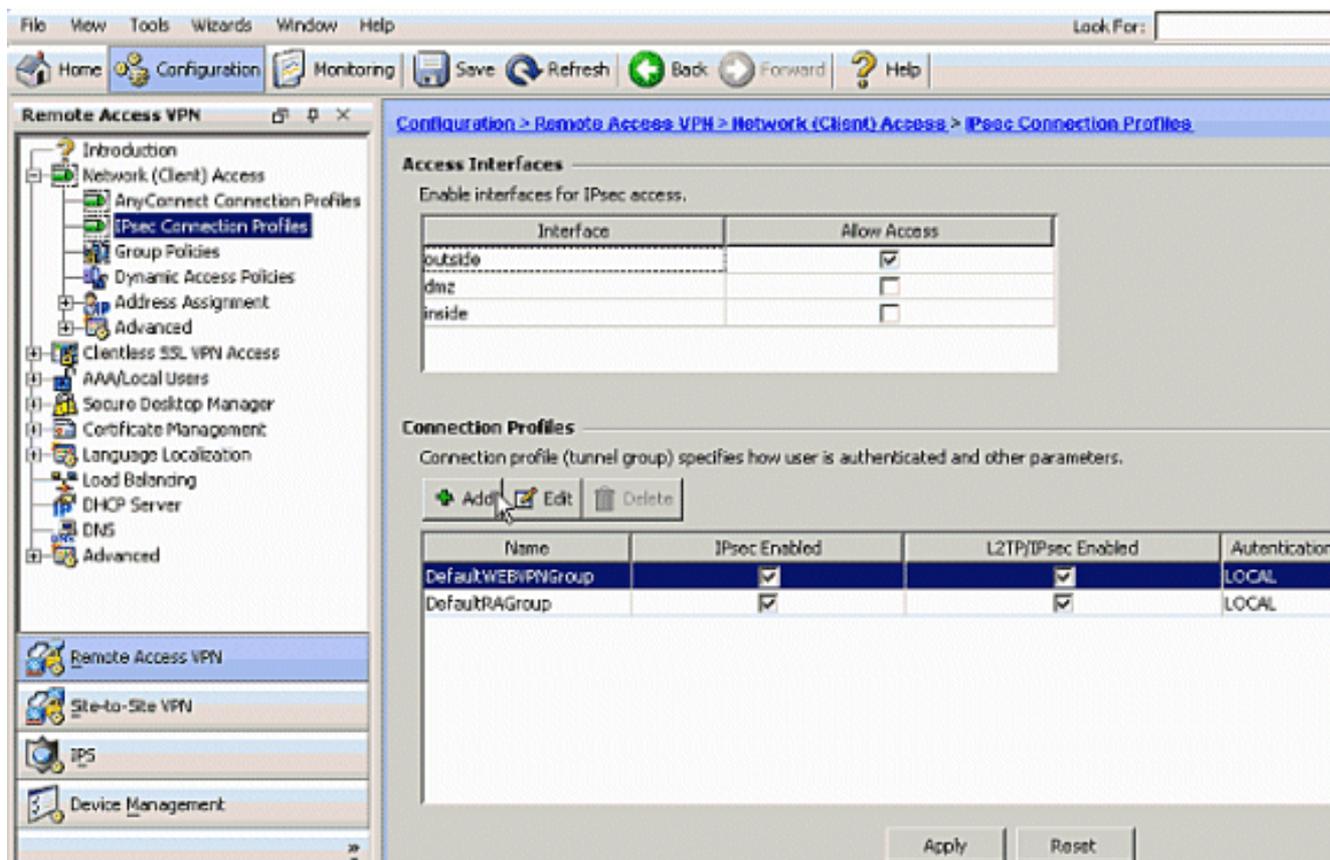
- 選擇 Configuration > Remote Access VPN > AAA Setup > AAA Server Groups，然後按一下Add以新增AAA Server Group名稱和協定。



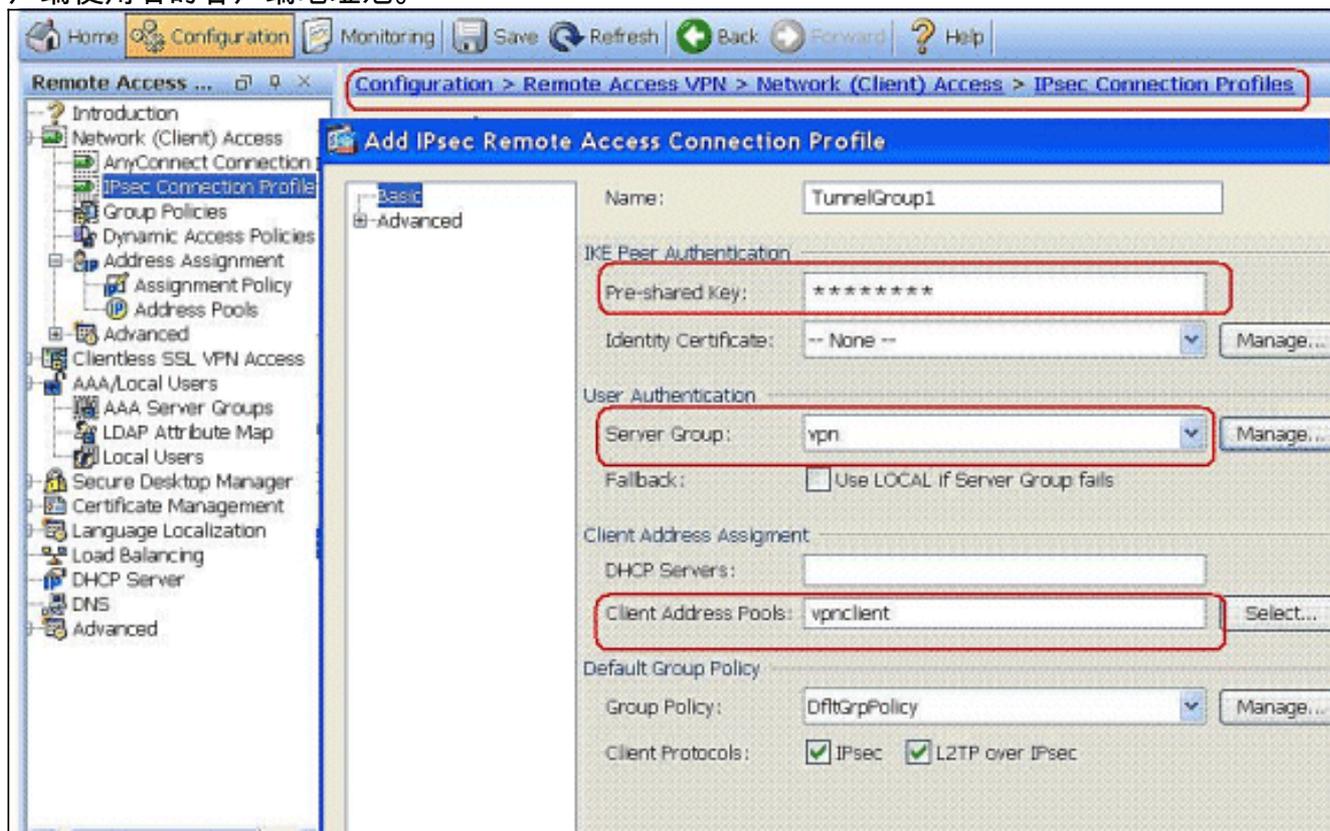
新增AAA伺服器IP地址(ACS)及其連線的介面。同時在RADIUS引數區域新增伺服器金鑰。按一下「OK」(確定)。



8. 選擇 Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Add 以新增隧道組，例如 TunnelGroup1，並將 Preshared key 作為 cisco123，如下所示。

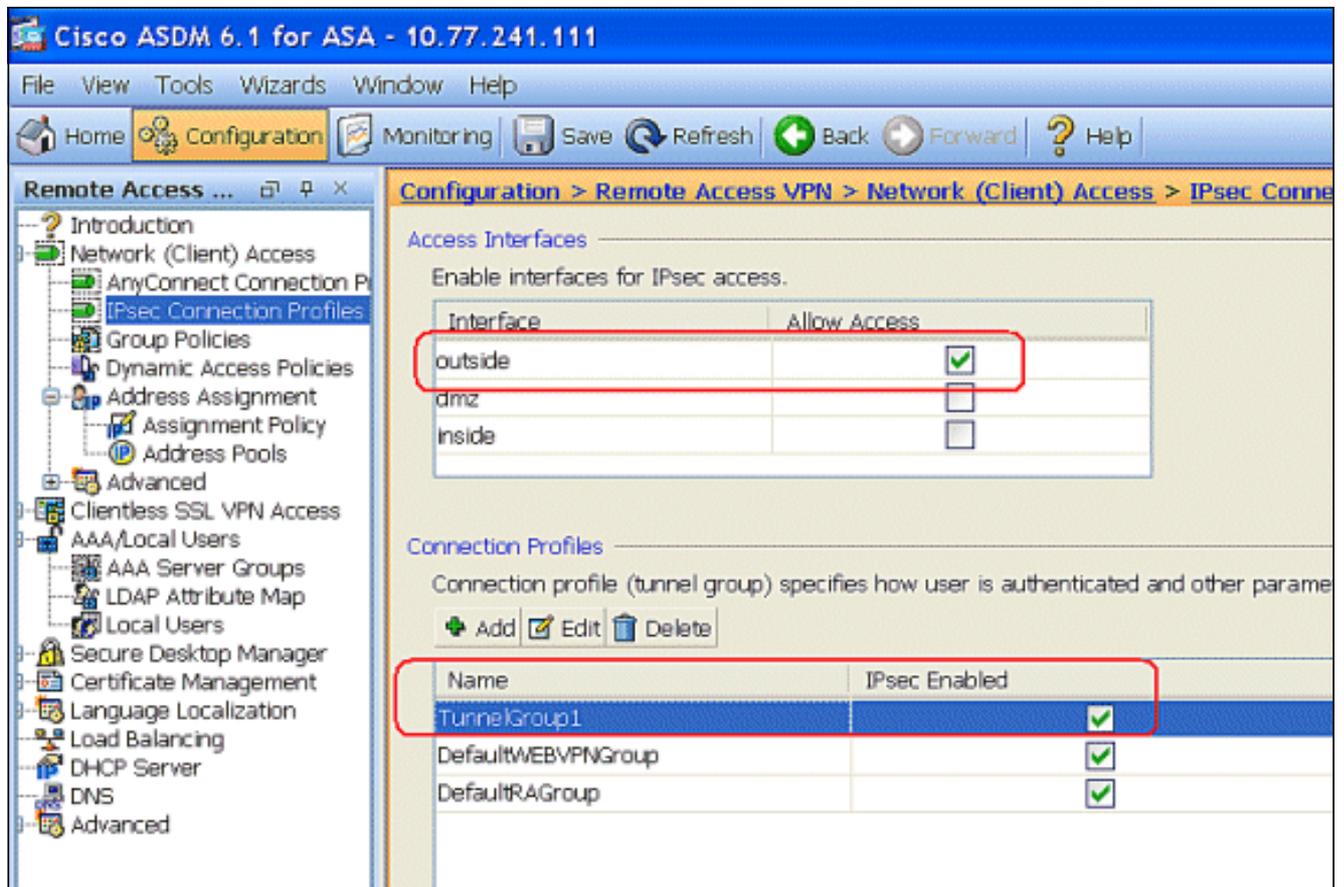


在Basic頁籤下，為User Authentication欄位選擇vpn作為伺服器組。選擇vpnclient作為VPN客戶端使用者的客戶端地址池。



按一下「OK」（確定）。

9. 為IPSec訪問啟用外部介面。按一下Apply繼續。



## 使用CLI配置ASA/PIX

完成這些步驟，以便配置DHCP伺服器從命令列為VPN客戶端提供IP地址。有關所使用的每個命令的詳細資訊，請參閱[配置遠端訪問VPN](#)或[Cisco ASA 5500系列自適應安全裝置 — 命令參考](#)。

### 在ASA裝置上運行配置

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
255.255.255.0 !--- Output is suppressed. passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-
k8.bin ftp mode passive access-list 101 extended permit
ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2
access-list new extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
```

```
ip local pool vpnclient1 192.168.5.1-192.168.5.10 mask
255.255.255.0

no failover
icmp unreachable rate-limit 1 burst-size 1

!--- Specify the location of the ASDM image for ASA to
fetch the image for ASDM access. asdm image disk0:/asdm-
613.bin no asdm history enable arp timeout 14400 global
(outside) 1 192.168.1.5 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 192.168.1.2 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 !--- Create the AAA server group
"vpn" and specify the protocol as RADIUS. !--- Specify
the CSACS server as a member of the "vpn" group and
provide the !--- location and key. aaa-server vpn
protocol radius
max-failed-attempts 5
aaa-server vpn (DMZ) host 172.16.1.1
retry-interval 1
timeout 30
key cisco123
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

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. !--- A Triple DES
encryption with !--- the sha hash algorithm is used.
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac

!--- Defines a dynamic crypto map with !--- the
specified encryption settings. crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-3DES-SHA

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 1 ipsec-isakmp dynamic
outside_dyn_map

!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside

!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside

crypto isakmp policy 2
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

```

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
!
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes
  address-pool vpnclient
  authentication-server-group vpn

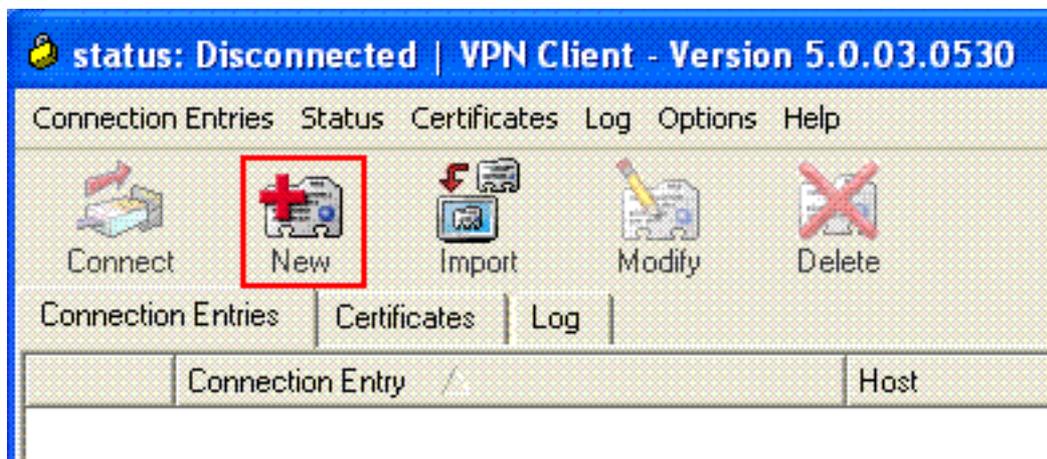
!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group TunnelGroup1 ipsec-
attributes pre-shared-key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#

```

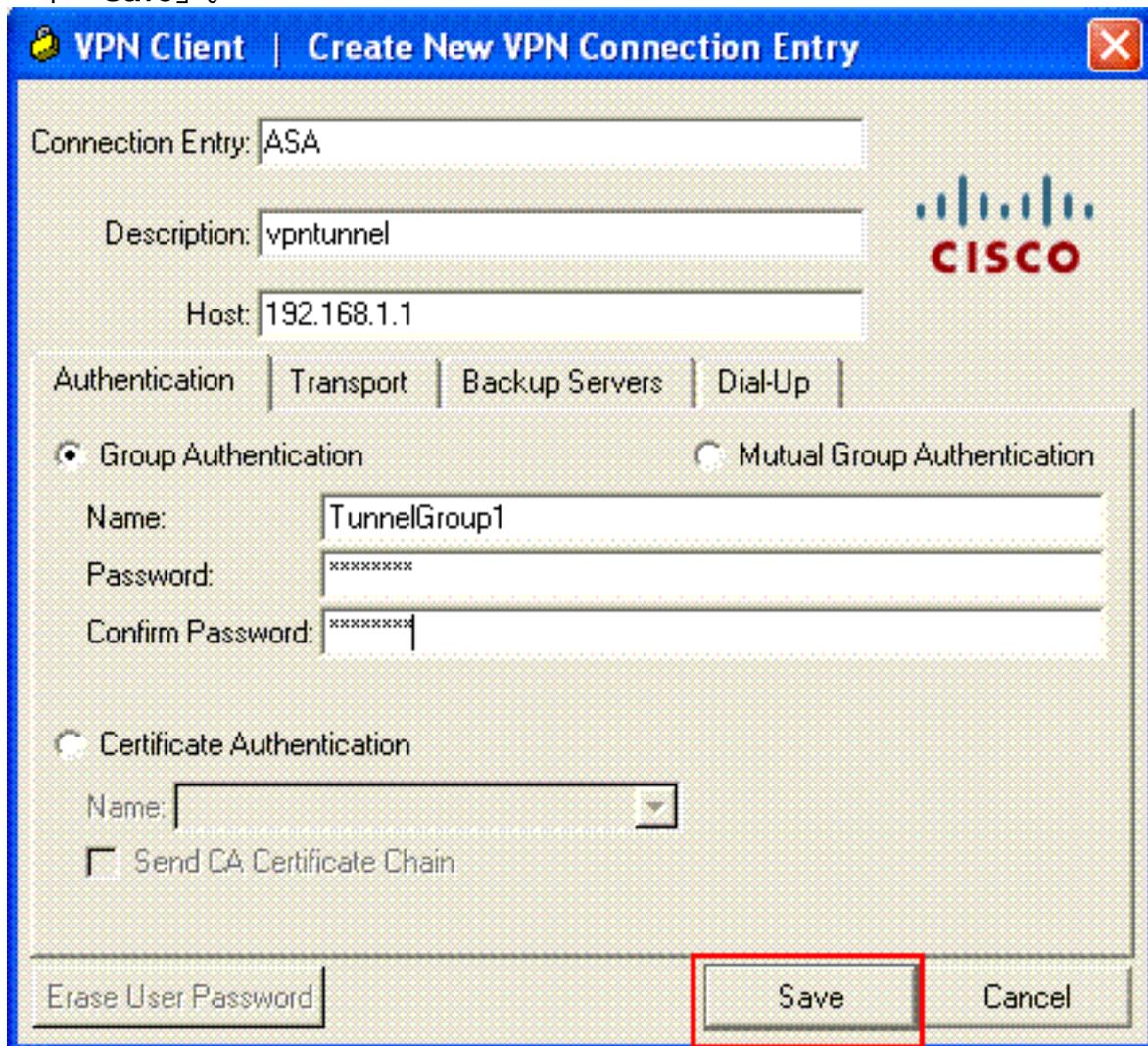
## [Cisco VPN客戶端配置](#)

嘗試使用Cisco VPN客戶端連線到Cisco ASA，以驗證ASA配置是否成功。

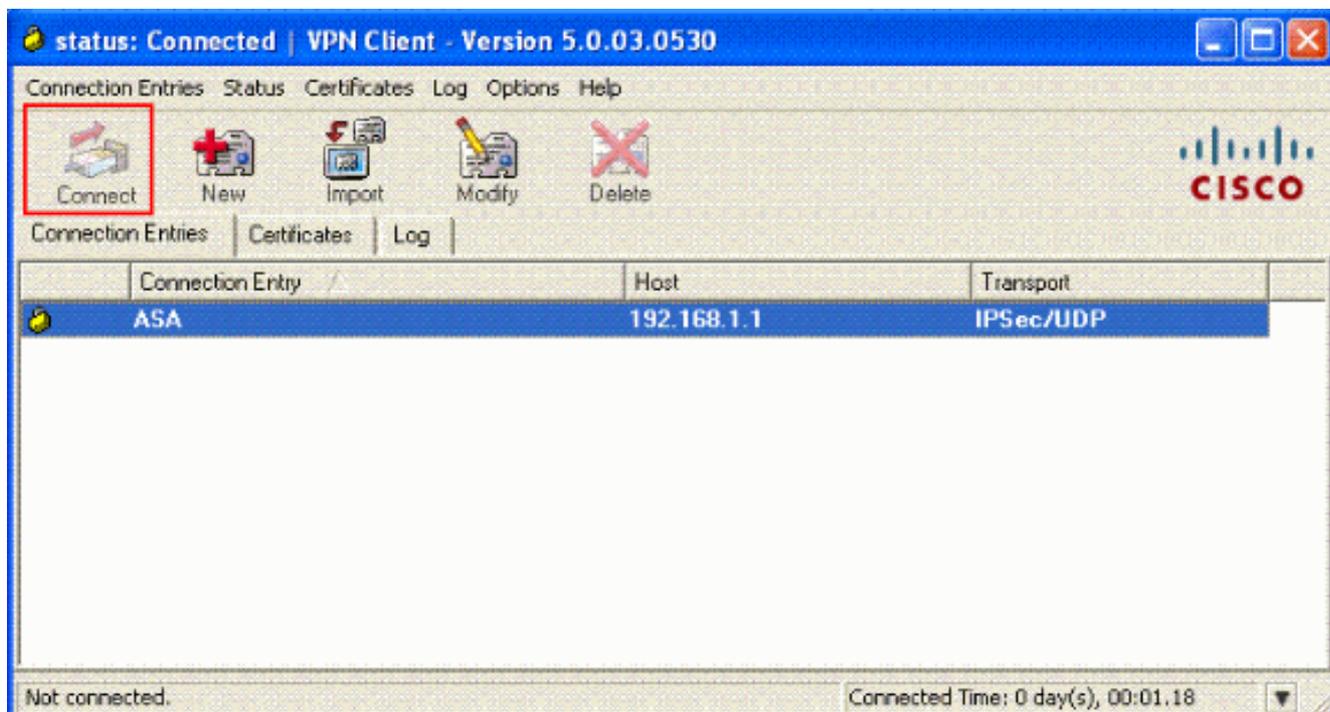
1. 選擇Start > Programs > Cisco Systems VPN Client > VPN Client。
2. 按一下New以啟動Create New VPN Connection Entry視窗。



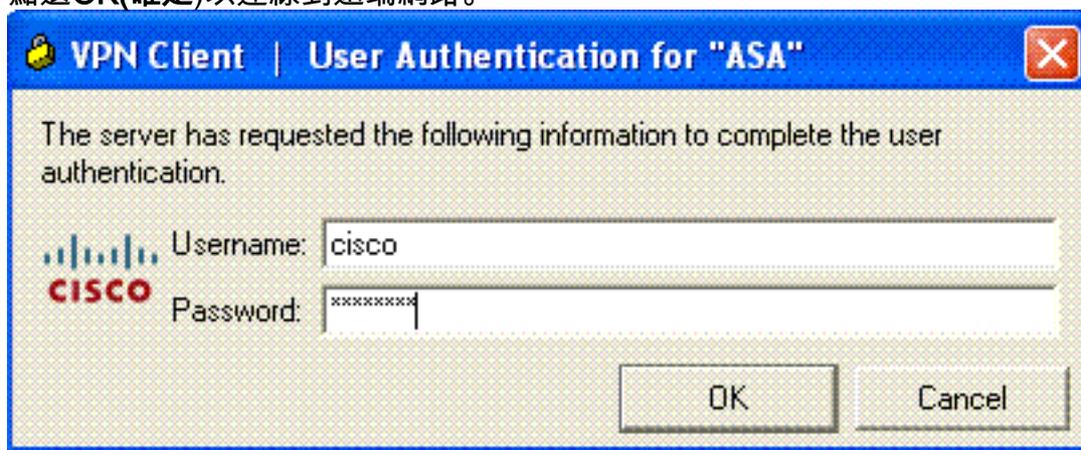
3. 填寫新連線的詳細資訊。輸入連線條目的名稱和說明。在Host框中輸入ASA的外部IP地址。然後輸入ASA中配置的VPN隧道組名稱(TunnelGroup1)和密碼 (預共用金鑰 — cisco123 )。按一下「Save」。



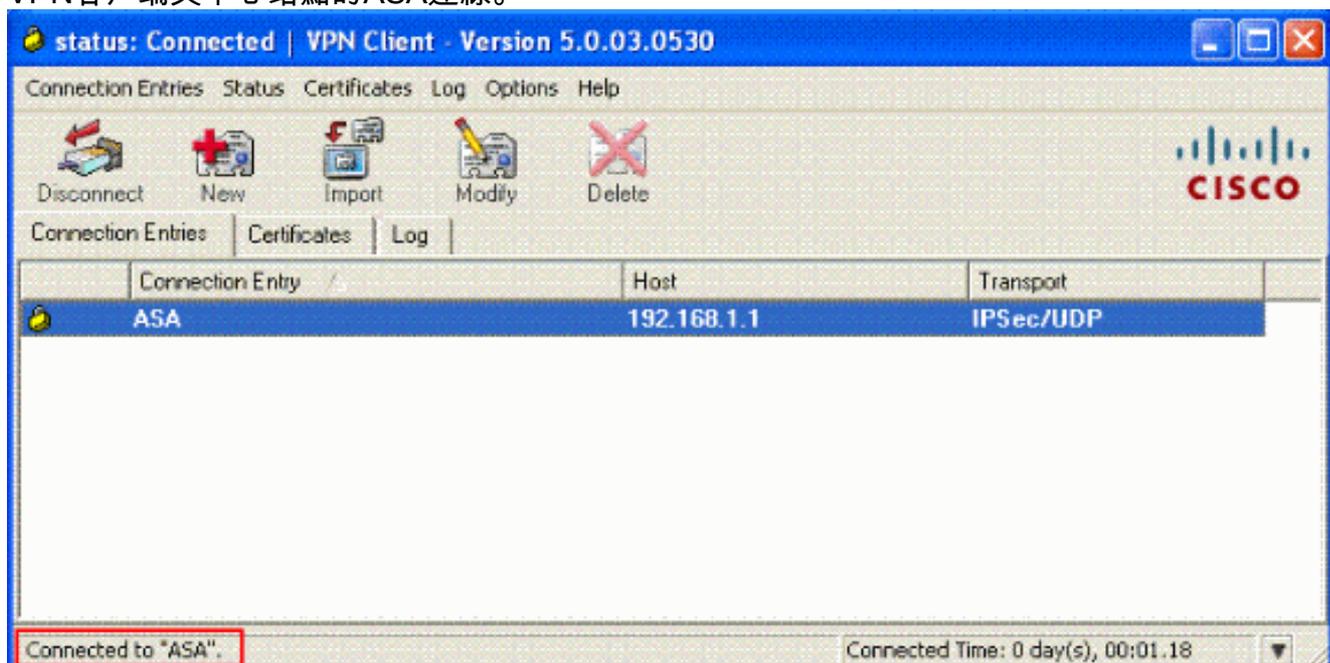
4. 按一下要使用的連線，然後在VPN客戶端主視窗中按一下Connect。



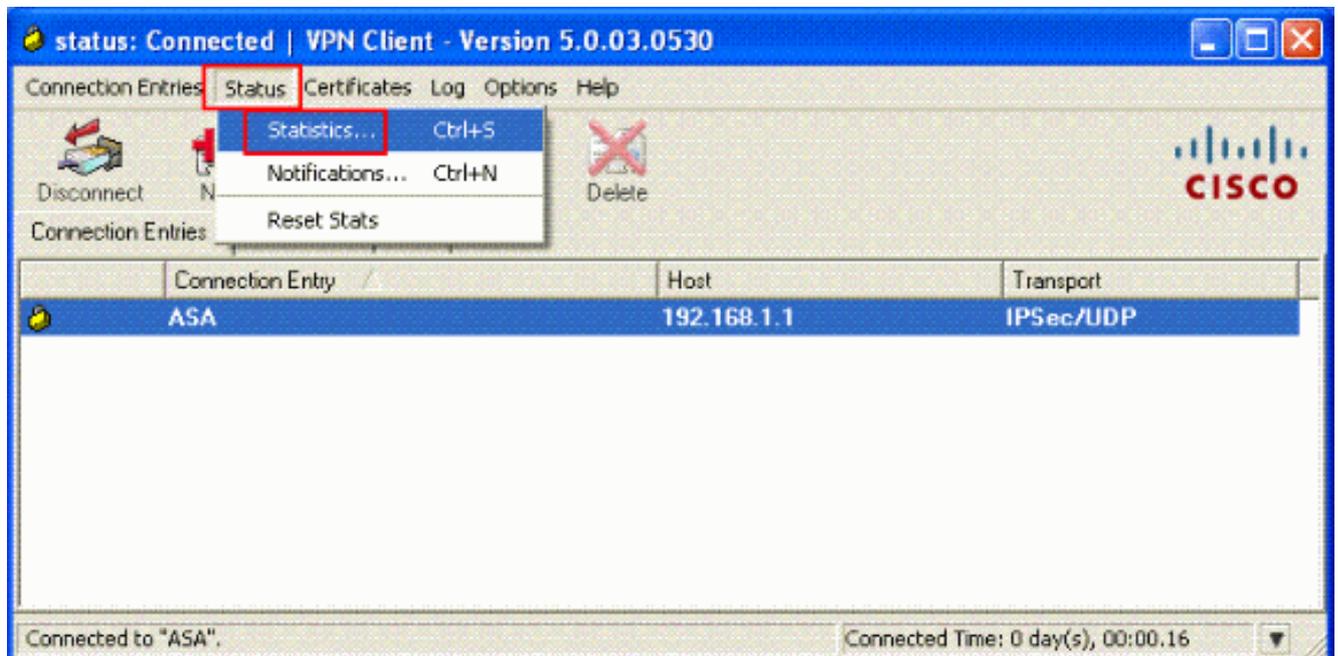
5. 出現提示時，輸入Username:cisco和密碼：password1（如在ASA中為xauth配置的），然後點選OK(確定)以連線到遠端網路。



6. VPN客戶端與中心站點的ASA連線。



7. 成功建立連線後，從Status選單中選擇Statistics以驗證隧道的詳細資訊。



## 為個人使用者的可下載ACL配置ACS

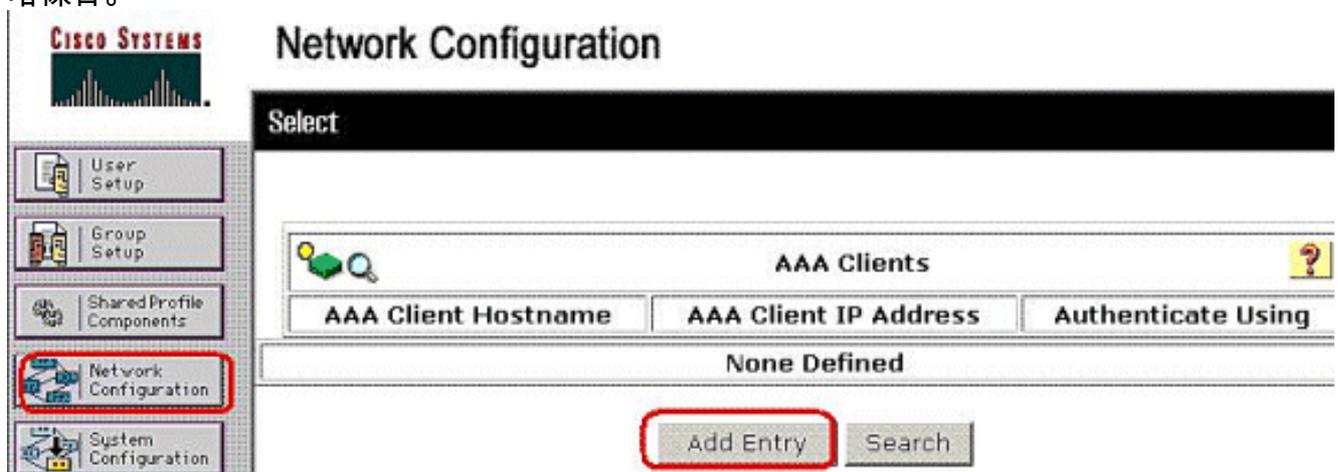
您可以將Cisco Secure ACS上的可下載訪問清單配置為共用配置檔案元件，然後將訪問清單分配給組或單個使用者。

若要實作動態存取清單，您必須設定RADIUS伺服器以支援它。當使用者進行身份驗證時，RADIUS伺服器會向安全裝置傳送可下載的訪問清單或訪問清單名稱。訪問清單允許或拒絕對給定服務的訪問。身份驗證會話到期時，安全裝置將刪除訪問清單。

在此示例中，IPSec VPN使用者「cisco」成功進行身份驗證，RADIUS伺服器向安全裝置傳送可下載訪問清單。使用者「cisco」只能訪問10.1.1.2伺服器並拒絕所有其他訪問。要驗證ACL，請參閱[使用者/組的可下載ACL](#)部分。

完成以下步驟即可在Cisco Secure ACS中設定RADIUS。

1. 在左側選擇**Network Configuration**，然後按一下**Add Entry**在RADIUS伺服器資料庫中為ASA新增條目。



2. 在「客戶端IP地址」欄位中輸入172.16.1.2，並在「共用金鑰」欄位中輸入"cisco123"。在 *Authenticate Using* 下拉框中選擇RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)。按一下「Submit」。



## Network Configuration

Edit



### Add AAA Client

AAA Client Hostname   
AAA Client IP Address   
Shared Secret

#### RADIUS Key Wrap

Key Encryption Key   
Message Authenticator Code Key   
Key Input Format  ASCII  Hexadecimal

Authenticate Using

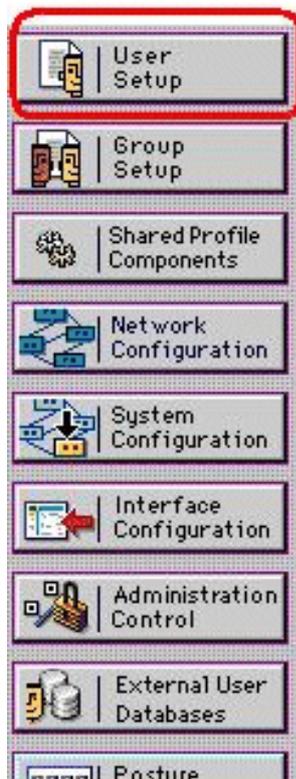
Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

3. 在Cisco Secure資料庫的User欄位中輸入使用者名稱，然後按一下Add/Edit。在本範例中，使用者名稱為cisco。



## User Setup

Select



User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)  
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)  
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

4. 在下一個視窗中，輸入"cisco"的密碼。在本例中，密碼也是password1。完成後，按一下Submit。

**CISCO SYSTEMS**

## User Setup

**User: cisco**

Account Disabled

### Supplementary User Info

Real Name

Description

### User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

5. 使用「高級選項」頁可確定ACS顯示哪些高級選項。如果您隱藏了未使用的高級選項，則可以簡化ACS Web介面其他區域中顯示的頁面。按一下**Interface Configuration**，然後按一下**Advanced Options**以開啟「Advanced Options」頁面。



# Interface Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration**
- Administration Control
- External User Databases

### Advanced Options ?

**Note: Only the selected options will appear in the user interface.**

- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs**
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs**
- Group-Level Password Aging

選中User-Level Downloadable ACL和Group-Level Downloadable ACL覈取方塊。使用者級可下載ACL — 選擇此選項後，將啟用「使用者設定」頁面上的「可下載ACL (訪問控制清單)」部分。組級可下載ACL — 選擇此選項後，將啟用「組設定」頁上的「可下載ACL」部分。

- 在導航欄中，按一下Shared Profile Components，然後按一下Downloadable IP ACL。註：如果「共用配置檔案元件」頁上未顯示可下載IP ACL，則必須在「介面配置」部分的「高級選項」頁上啟用「使用者級可下載ACL」、「組級可下載ACL」選項或同時啟用這兩個選項。



# Shared Profile Components

- User Setup
- Group Setup
- Shared Profile Components**
- Network Configuration

### Select

- Downloadable IP ACLs**
- Network Access Filtering
- RADIUS Authorization Components
- Shell Command Authorization Sets
- PIX/ASA Command Authorization Sets

- 按一下「Add」。系統將顯示Downloadable IP ACL頁面。

## Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
None Defined	

Add

Cancel

8. 在名稱框中，鍵入新IP ACL的名稱。**注意：**IP ACL的名稱最多可包含27個字元。名稱不得包含空格或以下任何字元：連字元(-)、左括弧([)、右括弧(])、斜線(/)、反斜線(\)、引號(")、左尖括弧(<)、右尖括弧(>)或短劃線(-)。在Description框中，鍵入新IP ACL的說明。說明最多可包含1,000個字元。

# Shared Profile Components

Edit

## Downloadable IP ACLs

Name:   
Description:

ACL Contents

Network Access Filtering

No ACLs



Back to Help

若要將

ACL內容新增到新IP ACL中，請按一下Add。

9. 在名稱框中，鍵入新ACL內容的名稱。**注意：**ACL內容的名稱最多可包含27個字元。名稱不得包含空格或以下任何字元：連字元(-)、左括弧([)、右括弧(])、斜線(/)、反斜線(\)、引號(")、左尖括弧(<)、右尖括弧(>)或短劃線(-)。在ACL定義框中，鍵入新的ACL定義。**注意：**在ACS Web介面中輸入ACL定義時，不要使用關鍵字或名稱條目；而是以permit或deny關鍵字開頭。若要儲存ACL內容，請按一下「Submit」。

## Shared Profile Components

Edit

### Downloadable IP ACL Content

Name:

VPN\_Client

#### ACL Definitions

```
permit ip any host 10.1.1.2  
deny ip any any
```



Back to Help

Submit

Cancel

10. 系統將顯示Downloadable IP ACL頁面，在ACL Contents列中按名稱列出新的ACL內容。要將NAF與ACL內容相關聯，請從新ACL內容右側的Network Access Filtering框中選擇NAF。預設情況下，NAF為(All-AAA-Clients)。如果不分配NAF，ACS會將ACL內容關聯到所有網路裝置，這是預設設定。

# Shared Profile Components

**Edit**

## Downloadable IP ACLs

Name:

Description:

ACL Contents	Network Access Filtering
<input checked="" type="radio"/> <a href="#">VPN_Client</a>	(All-AAA-Clients) ▼



若要設定ACL內容的順序，請按一下ACL定義的單選按鈕，然後按一下「Up」或「Down」將其重新定位在清單中。若要儲存IP ACL，請按一下**Submit**。**注意**：ACL內容的順序非常重要。從上到下，ACS僅下載第一個具有適用NAF設定的ACL定義，其中包含全AAA客戶端預設設定（如果使用）。通常，您的ACL內容清單會從具有最特定（最窄）NAF的內容清單繼續到具有最一般（全AAA客戶端）NAF的內容清單。**注意**：ACS會輸入新的IP ACL，它會立即生效。例如，如果IP ACL與PIX防火牆一起使用，則它可以傳送到嘗試對已為其使用者或組配置檔案分配了可下載IP ACL的使用者進行身份驗證的任何PIX防火牆。

11. 轉到「使用者設定」頁並編輯「使用者」頁。在「Downloadable ACLs」部分下，按一下**Assign IP ACL**；覈取方塊。從清單中選擇IP ACL。如果已完成使用者帳戶選項的配置，請按一下**Submit**以記錄選項。

# User Setup

### Account Disable

Never

Disable account if:

Date exceeds: Apr 15 2009

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

### Downloadable ACLs

Assign IP ACL: VPN\_Access

## [為組的可下載ACL配置ACS](#)

完成為個人使用者的可下載ACL配置ACS的步驟1至9，並遵循這些步驟為Cisco Secure ACS中的組配置可下載ACL。

在本示例中，IPSec VPN使用者「cisco」屬於VPN組。VPN組策略應用於組中的所有使用者。

VPN組使用者「cisco」成功進行身份驗證，RADIUS伺服器向安全裝置傳送可下載訪問清單。使用者「cisco」只能訪問10.1.1.2伺服器並拒絕所有其他訪問。若要驗證ACL，請參閱[使用者/群組的可下載ACL](#)一節。

1. 在導航欄中，按一下**Group Setup**。將開啟「組設定選擇」頁。



## Group Setup



Select

Group : 1: Group 1

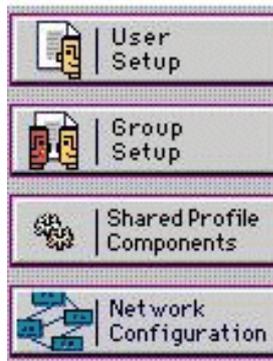
Users in Group Edit Settings

Rename Group

2. 將組1重新命名為VPN，然後按一下Submit。



## Group Setup



Select

Renaming Group: Group 1

Group VPN

Submit Cancel

3. 從「組」清單中選擇一個組，然後按一下編輯設定。

## Group Setup

Select

Group 1: VPN (1 user)

Users in Group Edit Settings

Rename Group

4. 在Downloadable ACLs部分下，按一下Assign IP ACL覈取方塊。從清單中選擇IP ACL。

# Group Setup

**Jump To** Access Restrictions

Sessions available to users of this group

Unlimited

---

**IP Assignment** 

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

---

**Downloadable ACLs** 

Assign IP ACL:

5. 若要儲存您剛剛進行的組設定，請按一下**提交**。
6. 轉到使用者設定並編輯要新增到組中的使用者：**VPN**。完成後，按一下**提交**。

The screenshot shows the Cisco User Setup configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, and External User Databases. The main content area is titled 'User Setup' and includes several password fields and a checkbox for 'Separate (CHAP/MS-CHAP/ARAP)'. Below these is a dropdown menu labeled 'Group to which the user is assigned:' with 'VPN' selected. A red box highlights this dropdown menu.

現在，為此使用者應用了為VPN組配置的可下載ACL。

7. 若要繼續指定其他組設定，請執行本章中的其他步驟（如果適用）

## 為使用者組配置IETF RADIUS設定

要在使用者進行身份驗證時從RADIUS伺服器下載已在安全裝置上建立的訪問清單的名稱，請按照如下方式配置IETF RADIUS filter-id屬性（屬性號11）：

```
filter-id=acl_name
```

VPN組使用者「cisco」成功進行身份驗證，RADIUS伺服器下載已在安全裝置上建立的訪問清單的ACL名稱（新）。使用者「cisco」可以訪問ASA 10.1.1.2伺服器以外的所有網路內的裝置。若要驗證ACL，請參閱[Filter-Id ACL](#)部分。

根據示例，名為new的ACL配置為在ASA中進行過濾。

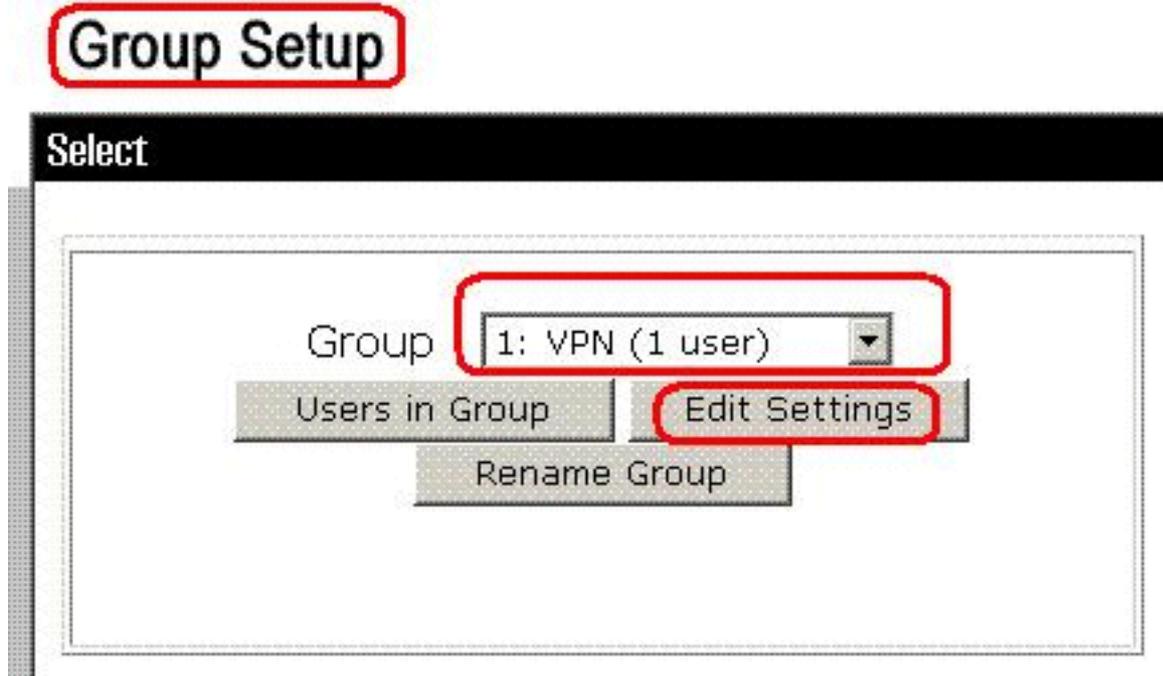
```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

僅當這些引數為真時，才會顯示這些引數。您已配置

- AAA客戶端在網路配置中使用其中一個RADIUS協定
  - Web介面的Interface Configuration部分中RADIUS(IETF)頁面上的組級RADIUS屬性
- RADIUS屬性作為每個使用者的配置檔案從ACS傳送到請求AAA客戶端。

要配置IETF RADIUS屬性設定以應用為當前組中每個使用者的授權，請執行以下步驟：

1. 在導航欄中，按一下**Group Setup**。將開啟「組設定選擇」頁。
2. 從「組」清單中選擇一個組，然後按一下**編輯設定**。



組的名稱顯

示在「組設定」頁面的頂部。

3. 滾動到IETF RADIUS屬性。對於每個IETF RADIUS屬性，您必須授權當前組。選中**[011] Filter-Id**屬性的覈取方塊，然後在欄位中該屬性的授權中新增ASA定義的ACL名稱(**new**)。請參閱ASA *show running configuration*輸出。

## Group Setup

Jump To

### IETF RADIUS Attributes

[006] Service-Type

[007] Framed-Protocol

[009] Framed-IP-Netmask

[010] Framed-Routing

[011] Filter-Id

[012] Framed-MTU (64..65535)

- 若要儲存您剛剛進行的組設定並立即應用它們，請按一下**Submit**和**Apply**。注意：若要儲存組設定並在以後應用，請按一下**提交**。準備好實施更改後，請選擇**System Configuration > Service Control**。然後選擇**Restart**。

## 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 Crypto命令

- `show crypto isakmp sa` — 顯示對等體上的所有當前IKE安全關聯(SA)。

```
ciscoasa# sh crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.10.2
Type      : user          Role       : responder
Rekey     : no           State      : AM_ACTIVE
ciscoasa#
```

• **show crypto ipsec sa** — 顯示當前SA使用的設定。

```
ciscoasa# sh crypto ipsec sa
```

```
interface: outside
Crypto map tag: outside_dyn_map, seq num: 1,
local addr: 192.168.1.1

local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.5.1/255.255.255.255/0/0)
current_peer: 192.168.10.2, username: cisco
dynamic allocated peer ip: 192.168.5.1

#pkts encaps: 65, #pkts encrypt:
65, #pkts digest: 65
#pkts decaps: 65, #pkts decrypt:
65, #pkts verify: 65
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed:
0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures:
0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0,
#decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.10.2

path mtu 1500, ipsec overhead 58,
media mtu 1500
current outbound spi: EEF0EC32

inbound esp sas:
spi: 0xA6F92298 (2801345176)
transform: esp-3des esp-sha-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 86016, crypto-map:
outside_dyn_map
sa timing: remaining key lifetime (sec):
28647
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xEEF0EC32 (4008766514)
transform: esp-3des esp-sha-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 86016, crypto-map:
outside_dyn_map
sa timing: remaining key lifetime (sec): 28647
IV size: 8 bytes
replay detection support: Y
```

## [使用者/組的可下載ACL](#)

驗證使用者Cisco的可下載ACL。ACL會從CSACS下載。

```
ciscoasa(config)# sh access-list
access-list cached ACL log flows: total 0,
  denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
  192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411

access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
  ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
  ip any any (hitcnt=40) 0x7c718bd1
```

## [Filter-Id ACL](#)

[011] Filter-Id已應用於組 — VPN，並且根據ASA中定義的ACL（新）過濾該組的使用者。

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
  denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
  255.255.255.0 192.168.5.0 255.255.255.0
  (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip
  any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
  (hitcnt=39) 0x40e5d57c
```

## [疑難排解](#)

本節提供的資訊可用於對組態進行疑難排解。還顯示了調試輸出示例。

**注意：**有關遠端訪問IPSec VPN故障排除的詳細資訊，請參閱[最常見的L2L和遠端訪問IPSec VPN故障排除解決方案](#)。

## [清除安全關聯](#)

進行故障排除時，請確保在進行更改後清除現有的安全關聯。在PIX的特權模式下，使用以下命令：

- `clear [crypto] ipsec sa` — 刪除活動的IPSec SA。關鍵字crypto是可選的。
- `clear [crypto] isakmp sa` — 刪除活動的IKE SA。關鍵字crypto是可選的。

## [疑難排解指令](#)

[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

。

**附註：**使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- debug crypto ipsec 7 — 顯示第2階段的IPSec協商。
- debug crypto isakmp 7 — 顯示第1階段的ISAKMP協商。

## **相關資訊**

- [Cisco ASA 5500系列自適應安全裝置支援頁](#)
- [Cisco ASA 5500系列自適應安全裝置命令參考](#)
- [Cisco PIX 500系列安全裝置支援頁面](#)
- [思科調適型資安裝置管理員](#)
- [IPsec協商/IKE通訊協定支援頁面](#)
- [Cisco VPN使用者端支援頁面](#)
- [思科安全存取控制伺服器 \( Windows專用 \)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)