在ASA上配置無客戶端SSL VPN(WebVPN)

目錄

簡介

本文檔為思科自適應安全裝置(ASA)5500系列提供簡單配置，以允許無客戶端安全套接字層(SSL)VPN訪問內部網路資源。無客戶端SSL虛擬專用網路(WebVPN)允許從任何位置對公司網路進行有限但寶貴的安全訪問。使用者可以隨時實現基於瀏覽器的企業資源安全訪問。無需額外的客戶端即可訪問內部資源。使用通過SSL連線的超文本傳輸協定提供訪問。

無客戶端SSL VPN幾乎可以從任何可以訪問超文本傳輸協定網際網路(HTTP)站點的電腦保安輕鬆地訪問大量Web資源以及支援Web的應用程式和舊版應用程式。其中包括：

- 內部網站
- Microsoft SharePoint 2003、2007和2010
- Microsoft Outlook Web Access 2003、2007和2013
- Microsoft Outlook Web App 2010
- Domino Web Access(DWA)8.5和8.5.1
- Citrix Metaframe演示伺服器4.x
- Citrix XenApp版本5至6.5
- Citrix XenDesktop版本5至5.6和7.5

- VMware View 4

在受支援的Cisco ASA 5500系列的VPN平台中可找到支援的軟體清單。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 啟用SSL的瀏覽器
- 7.1或更高版本的ASA
- 頒發給ASA域名的X.509證書
- TCP埠443，在從客戶端到ASA的路徑上不得阻塞

有關要求的完整清單，請參閱支援的VPN平台Cisco ASA 5500系列。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA版本9.4(1)
- 調適型安全裝置管理員(ASDM)版本7.4(2)
- ASA 5515-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）的組態開始。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。

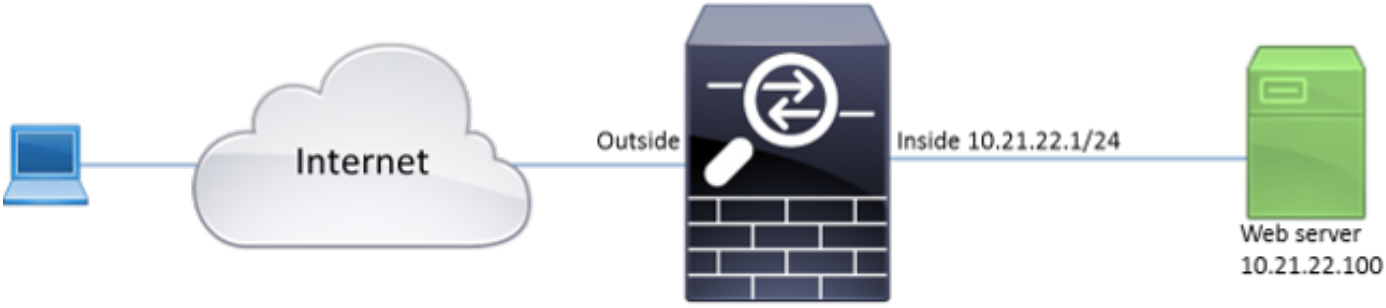
設定

本文描述ASDM和CLI的配置過程。您可以選擇使用任一工具來配置WebVPN，但某些配置步驟只能通過ASDM完成。

> **註：使**用命令查詢工具(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：



背景資訊

WebVPN使用SSL協定來保護客戶端和伺服器之間傳輸的資料。當瀏覽器啟動與ASA的連線時，ASA向瀏覽器顯示其證書以驗證其自身。為了確保客戶端與ASA之間的連線是安全的，您需要向ASA提供由客戶端已信任的證書頒發機構簽名的證書。否則，客戶端將無法驗證ASA的真實性，這會導致中間人攻擊和使用者體驗差，因為瀏覽器會發出連線不可信的警告。

> **附註**：預設情況下，ASA在啟動時生成自簽名X.509證書。預設情況下，此證書用於為客戶端連線提供服務。建議不要使用此證書，因為瀏覽器無法驗證其真實性。此外，此證書會在每次重新啟動時重新生成，因此每次重新啟動後都會更改。

證書安裝不在本文檔的討論範圍之內。

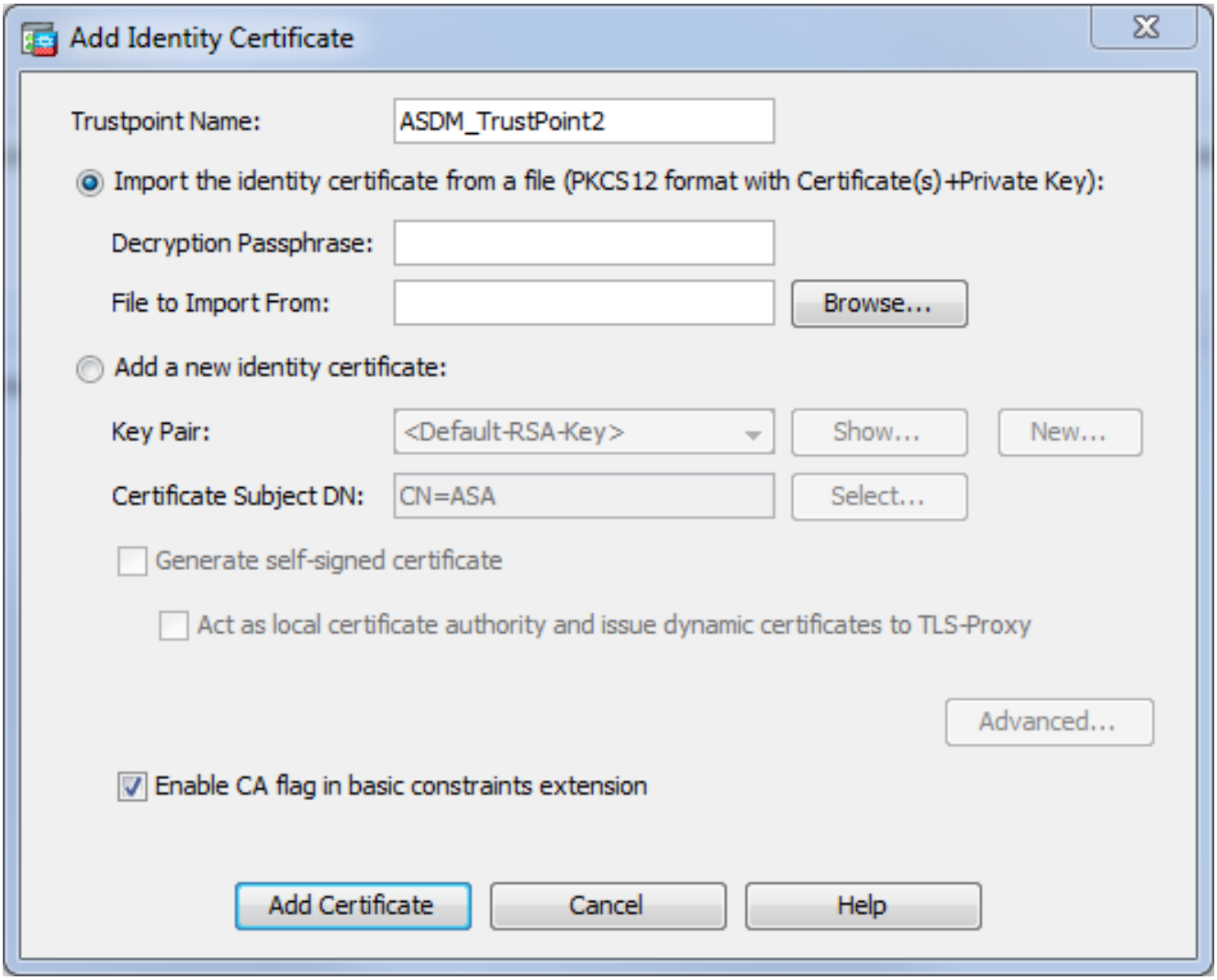
組態

在ASA上配置WebVPN的五個主要步驟：

- 配置ASA將使用的證書。
- 在ASA介面上啟用WebVPN。
- 為WebVPN訪問建立伺服器和/或統一資源定位器(URL)的清單。
- 為WebVPN使用者建立組策略。
- 將新組策略應用到隧道組。

> **附註**：在版本9.4以後的ASA版本中，用於選擇SSL密碼的演算法已更改(請參閱Cisco ASA系列的版本說明，9.4(x))。如果僅使用支援橢圓曲線的客戶端，則對證書使用橢圓曲線私鑰是安全的。否則，應使用自定義密碼套件，以避免ASA提供自簽名的臨時證書。您可以將ASA配置為僅使用基於RSA的密碼，並使用**ssl cipher tlsv1.2自定義「AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:RC4-SHA:RC4-RC4-MD5」命**命令。

1. **選項1** — 使用pkcs12檔案匯入證書。選擇**Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**。您可以使用pkcs12檔案安裝該檔案，或以隱私增強型郵件(PEM)格式貼上內容。

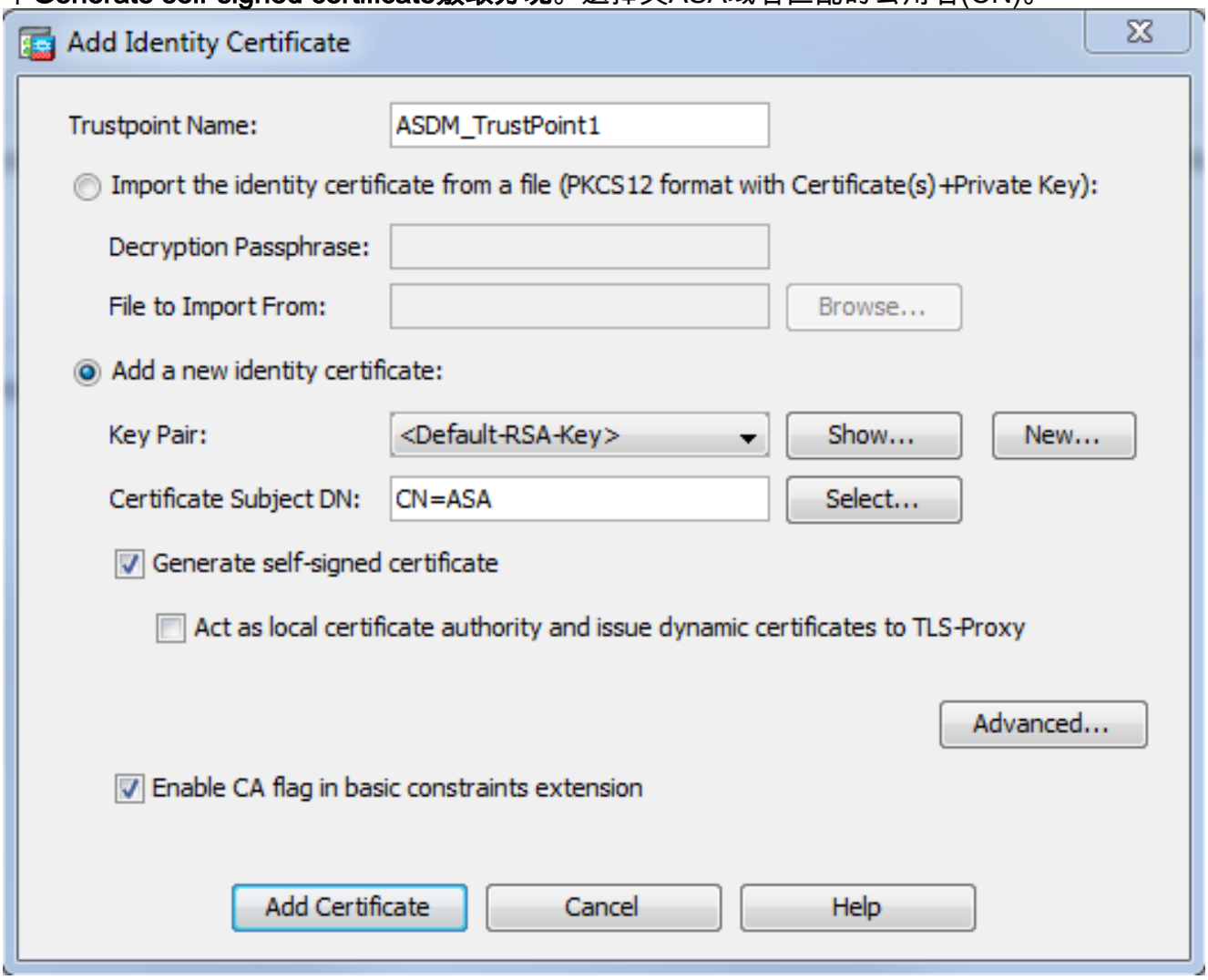


CLI:

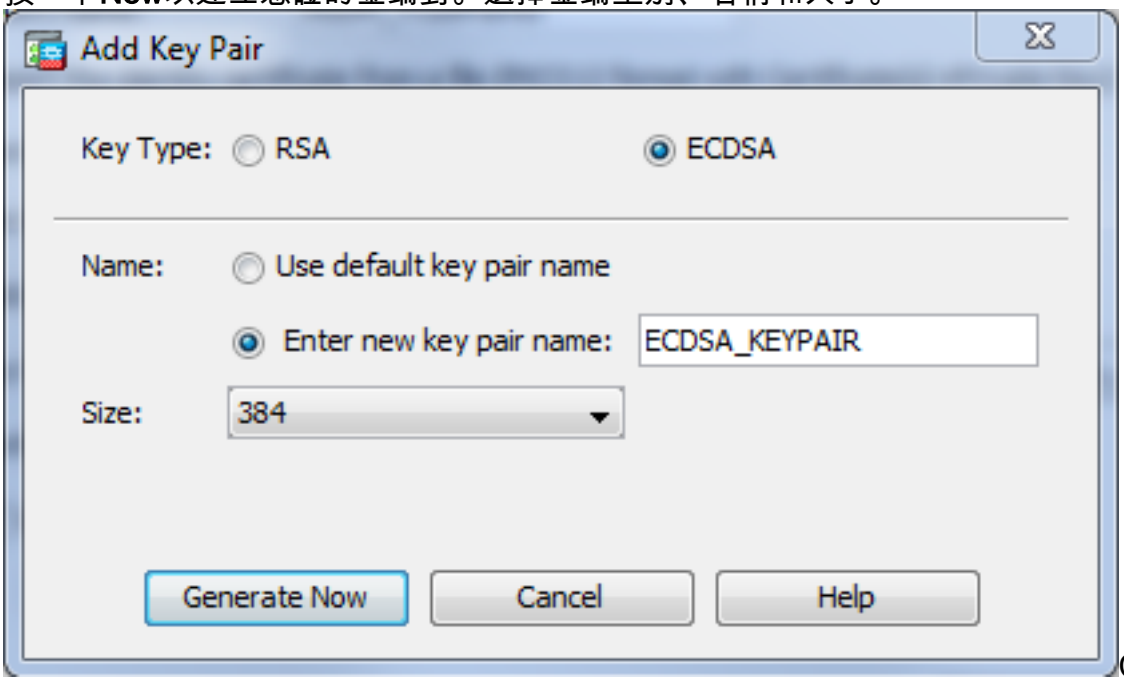
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b


--- output ommited ---


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b

quit
```

```
INFO: Import PKCS12 operation completed successfully
```

選項2 — 建立自簽名的憑證。選擇Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add。按一下Add a new identity certificate單選按鈕。選中Generate self-signed certificate覈取方塊。選擇與ASA域名匹配的公用名(CN)。



按一下New以建立憑證的金鑰對。選擇金鑰型別、名稱和大小。

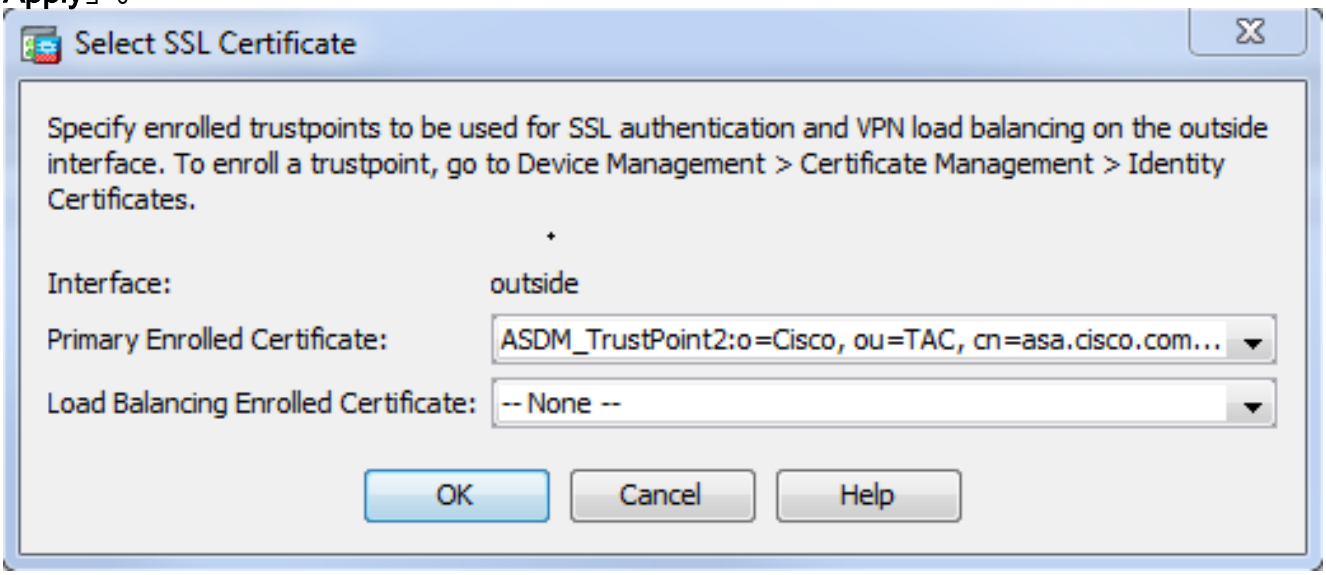


CLI:

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

```
ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

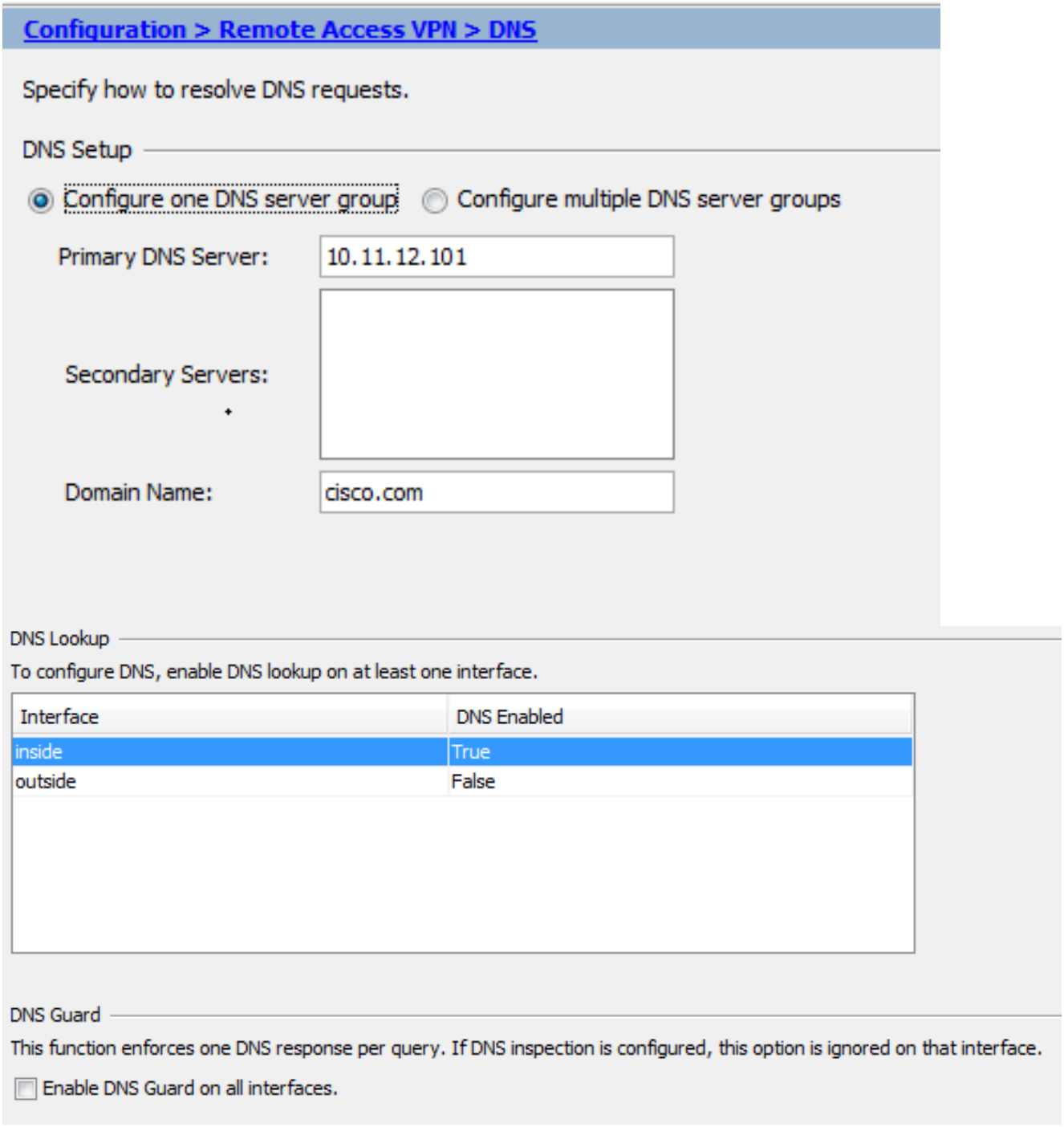
2. 選擇將用於WebVPN連線的證書。選擇**Configuration > Remote Access VPN > Advanced > SSL Settings**。從Certificates選單中，為外部介面選擇與所需證書相關聯的信任點。按一下「**Apply**」。



等效的CLI配置：

```
ASA(config)# ssl trust-point
```

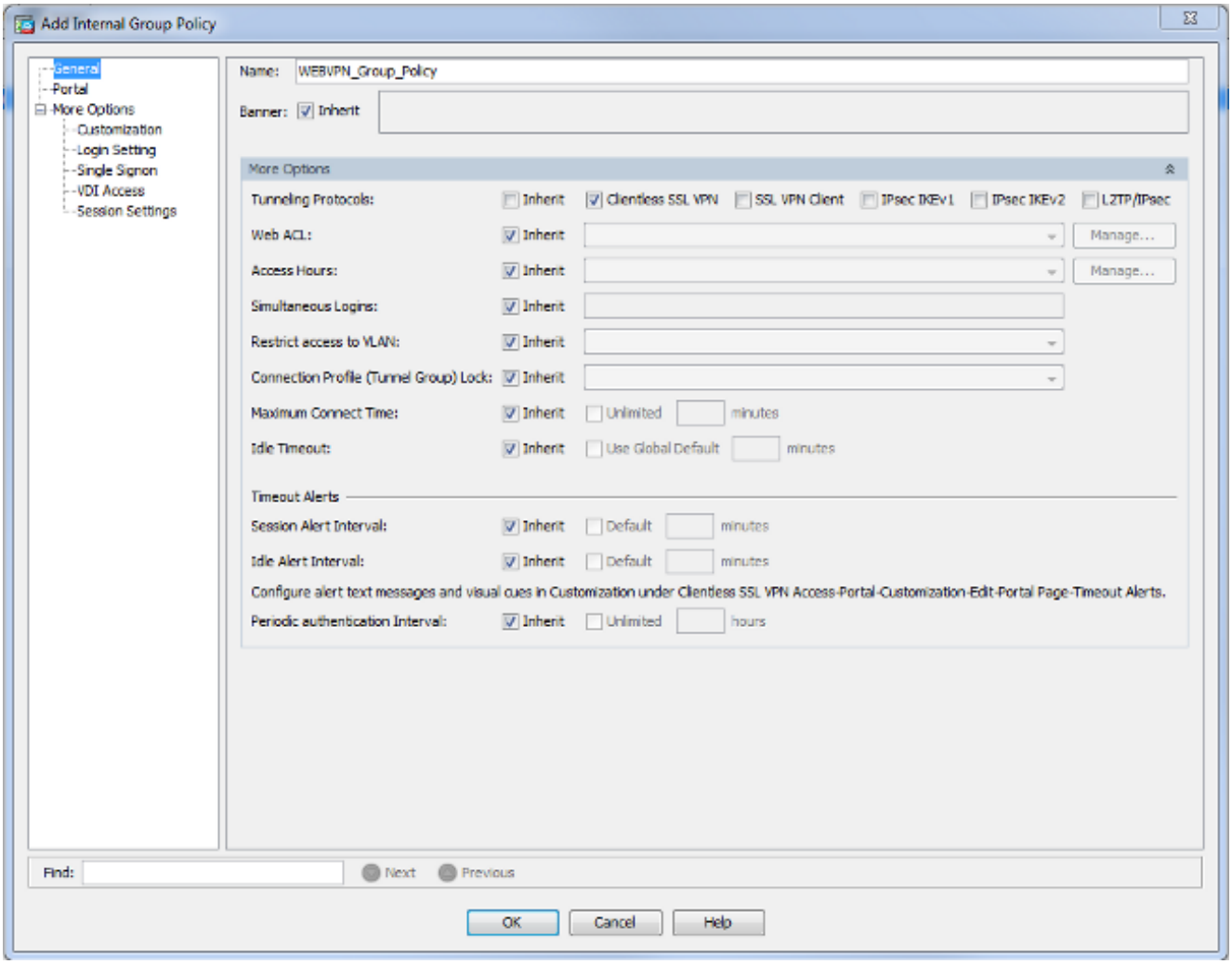
3. （可選）啟用域名伺服器(DNS)查詢。WebVPN伺服器充當客戶端連線的代理。這意味著ASA代表客戶端建立與資源的連線。如果客戶端需要連線到使用域名的資源，則ASA需要執行DNS查詢。選擇**Configuration > Remote Access VPN > DNS**。配置至少一個DNS伺服器，並在面向DNS伺服器的介面上啟用DNS查詢。



CLI:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. （可選）為WEBVPN連線建立組策略。選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy**。在General Options下，將Tuneling Protocols值更改為Clientless SSL VPN。



CLI:

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

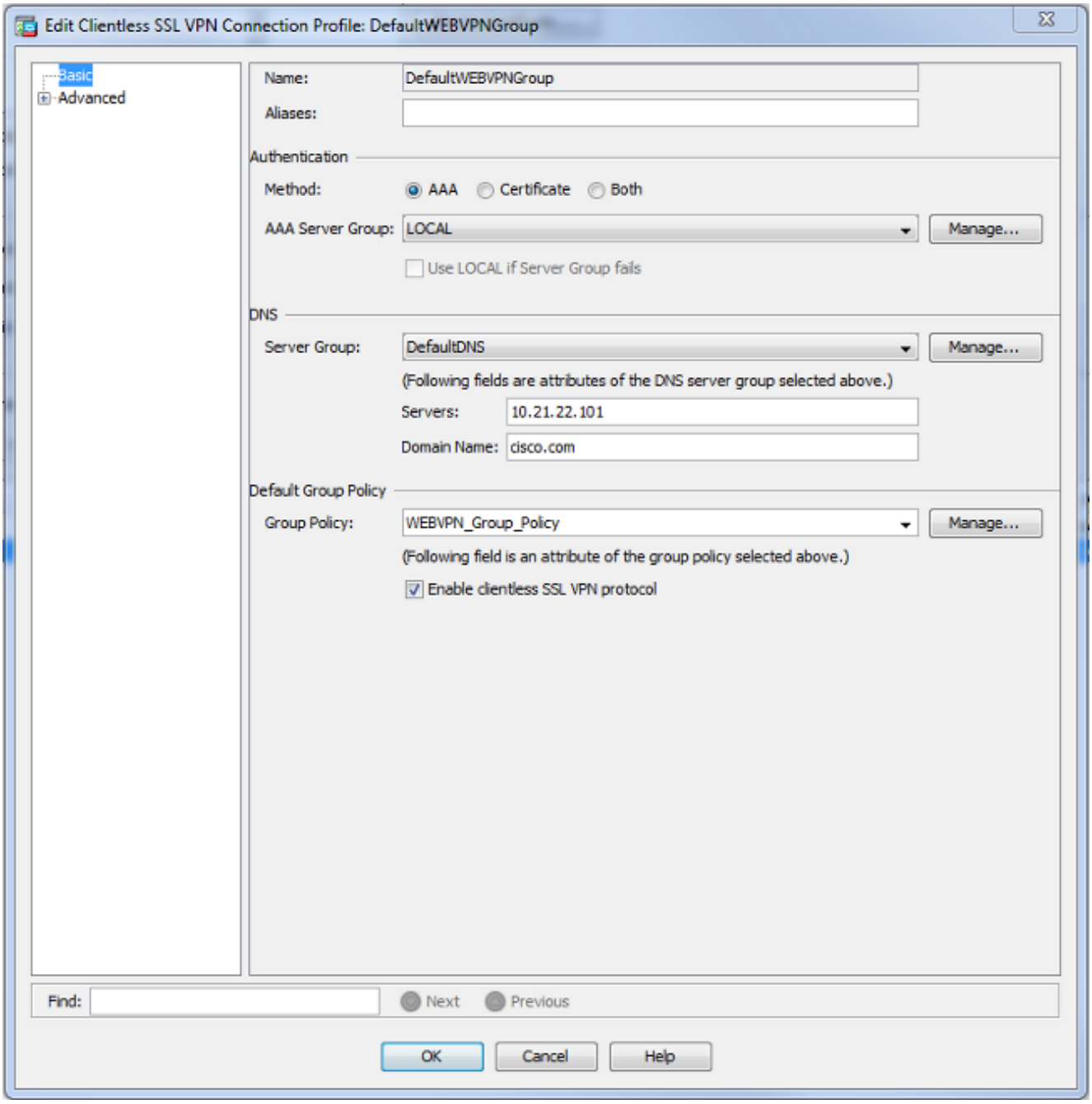
5. 配置連線配置檔案。在ASDM中，選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**。
有關連線配置檔案和組策略的概述，請參閱Cisco ASA系列VPN CLI配置指南9.4 — 連線配置檔案、組策略和使用者。預設情況下，WebVPN連線使用DefaultWEBVPNGroup配置檔案。您可以建立其他配置檔案。**附註：**有多種方法可以將使用者分配到其他配置檔案。

— 使用者可以從下拉選單中選擇連線配置檔案或使用特定URL。請參閱ASA 8.x:允許使用者通過Group-Alias和Group-URL方法在WebVPN登入時選擇組。

— 使用LDAP伺服器時，可以根據從LDAP伺服器接收的屬性分配使用者配置檔案，請參閱ASA使用LDAP屬性對映配置示例。

— 使用基於證書的客戶端身份驗證時，可以根據證書中包含的欄位將使用者對映到配置檔案，請參閱Cisco ASA系列VPN CLI配置指南9.4 — 配置IKEv1的證書組匹配。

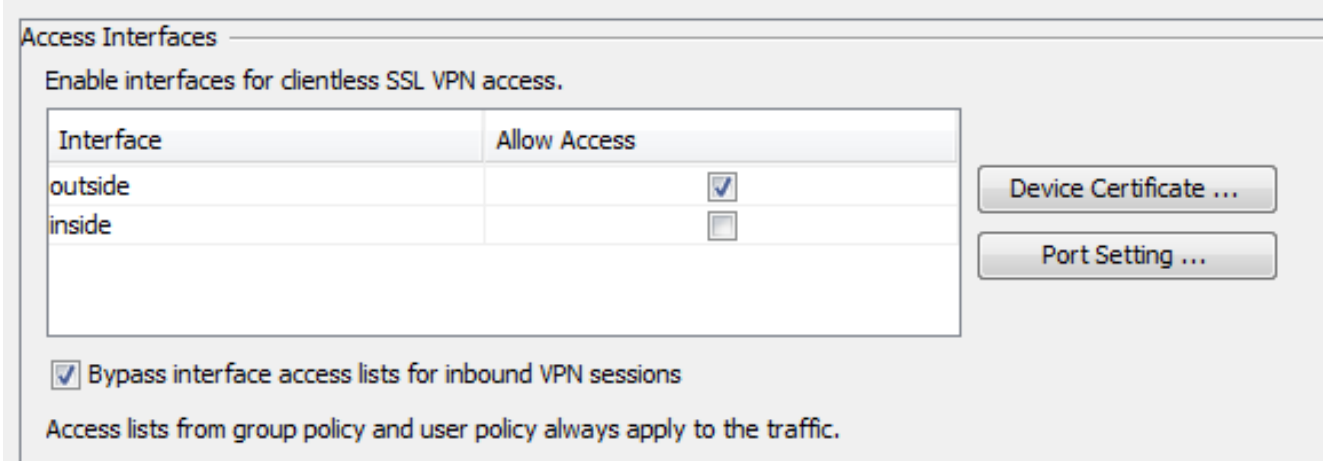
— 要手動將使用者分配給組策略，請參閱Cisco ASA系列VPN CLI配置指南9.4 — 配置單個使用者的屬性編輯DefaultWEBVPNGroup配置檔案，並在Default Group Policy下選擇WEBVPN_Group_Policy。



CLI:

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

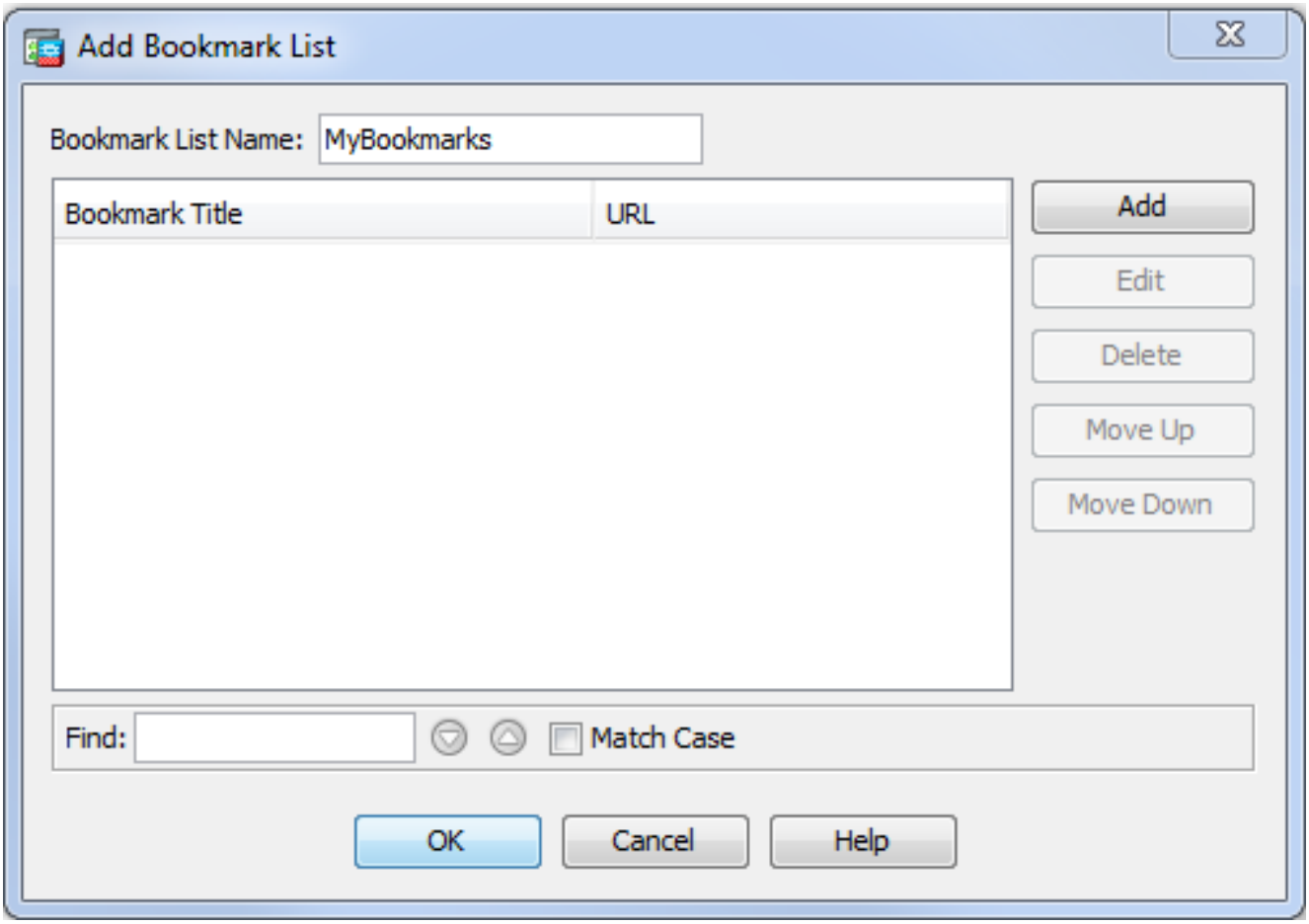
6. 要在外部介面上啟用WebVPN，請選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**。勾選外部介面旁邊的**Allow Access**覈取方塊。



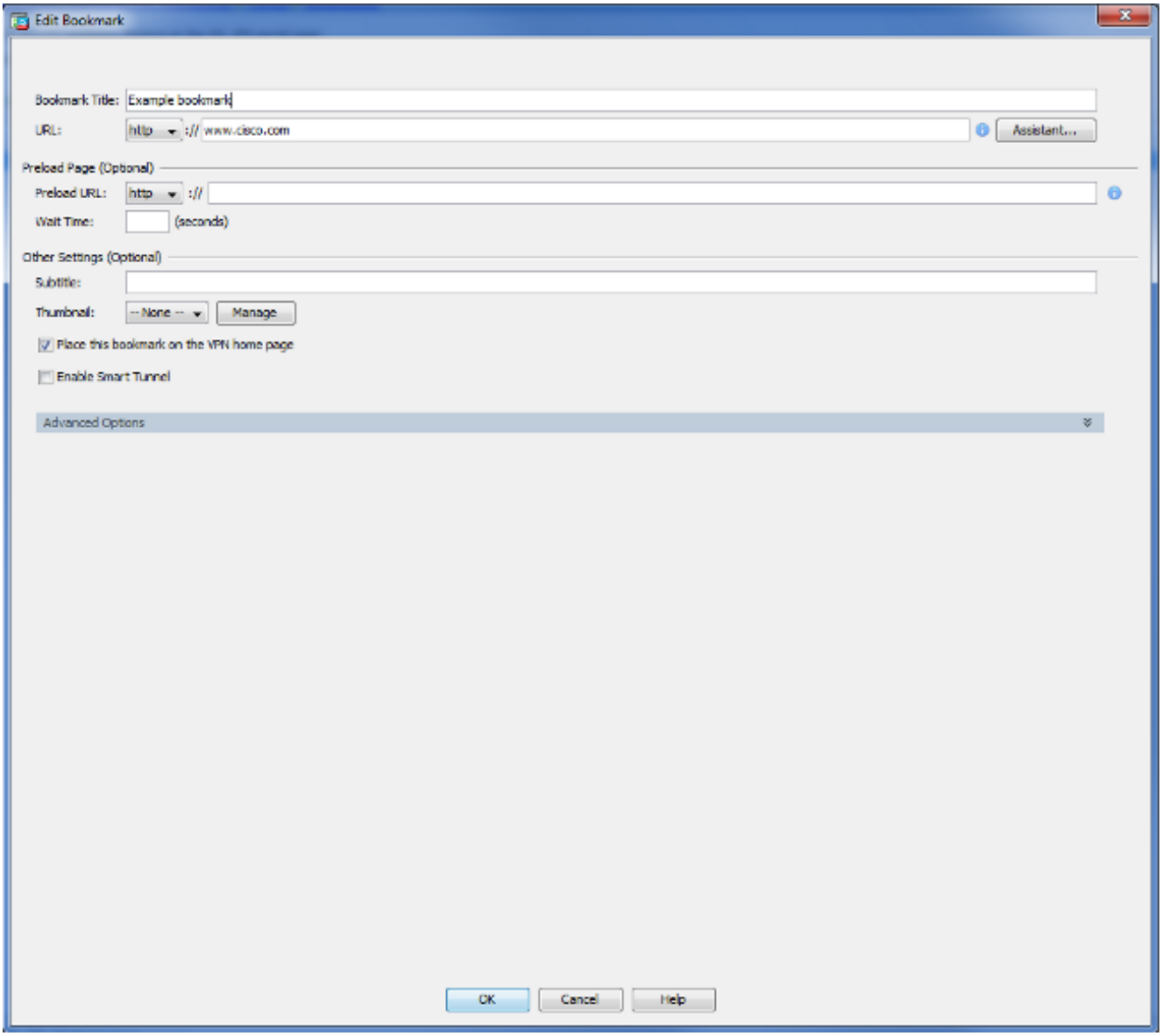
CLI:

```
ASA(config)# webvpn
ASA(config-webvpn)# enable outside
```

7. （可選）為內容建立書籤。書籤允許使用者輕鬆瀏覽內部資源，而不必記住URL。要建立書籤，請選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add**。

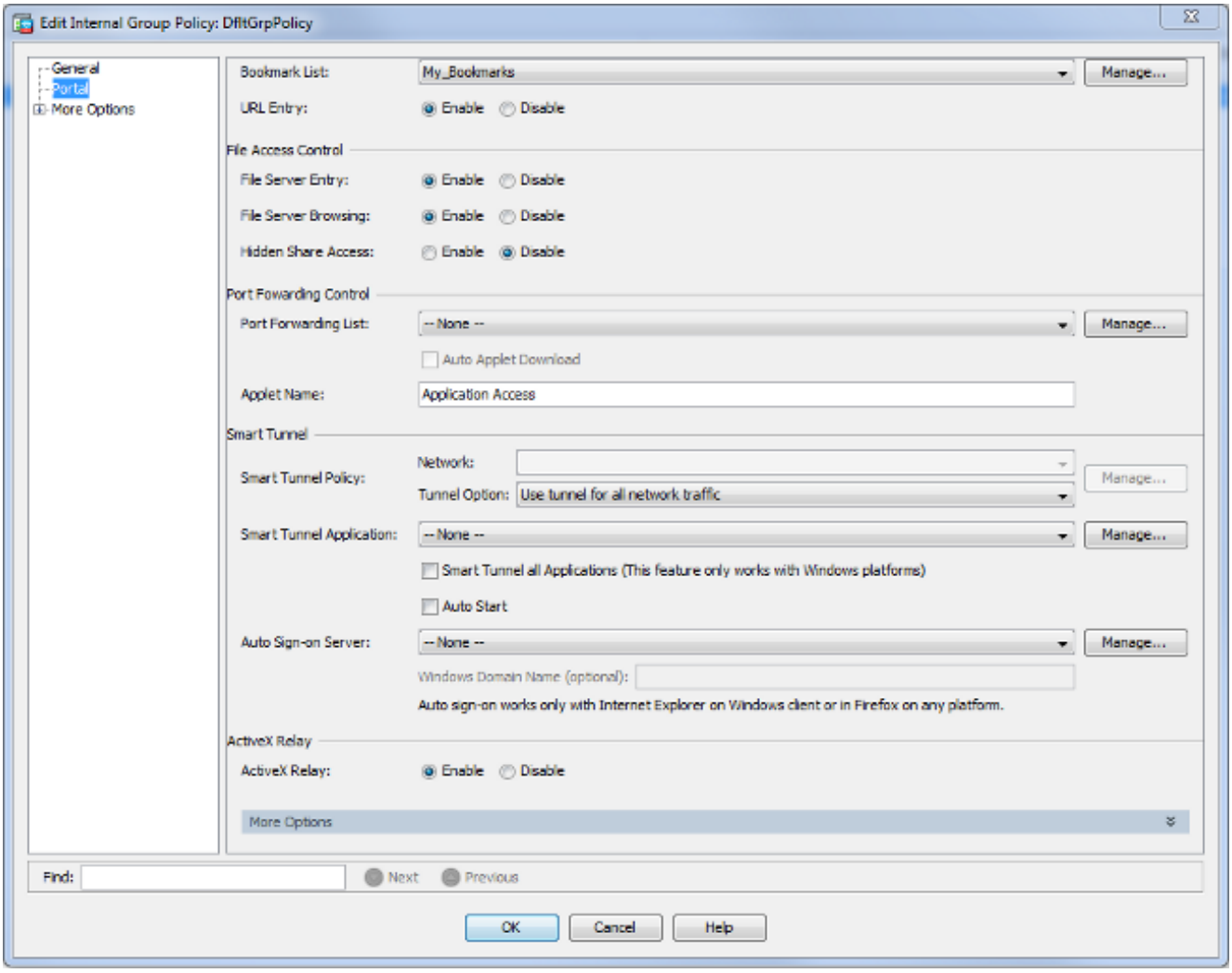


選擇**Add**以新增特定書籤。



CLI:無法通過CLI建立書籤，因為它們是作為XML檔案建立的。

8. （可選）為特定組策略分配書籤。選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Portal > Bookmark List**。

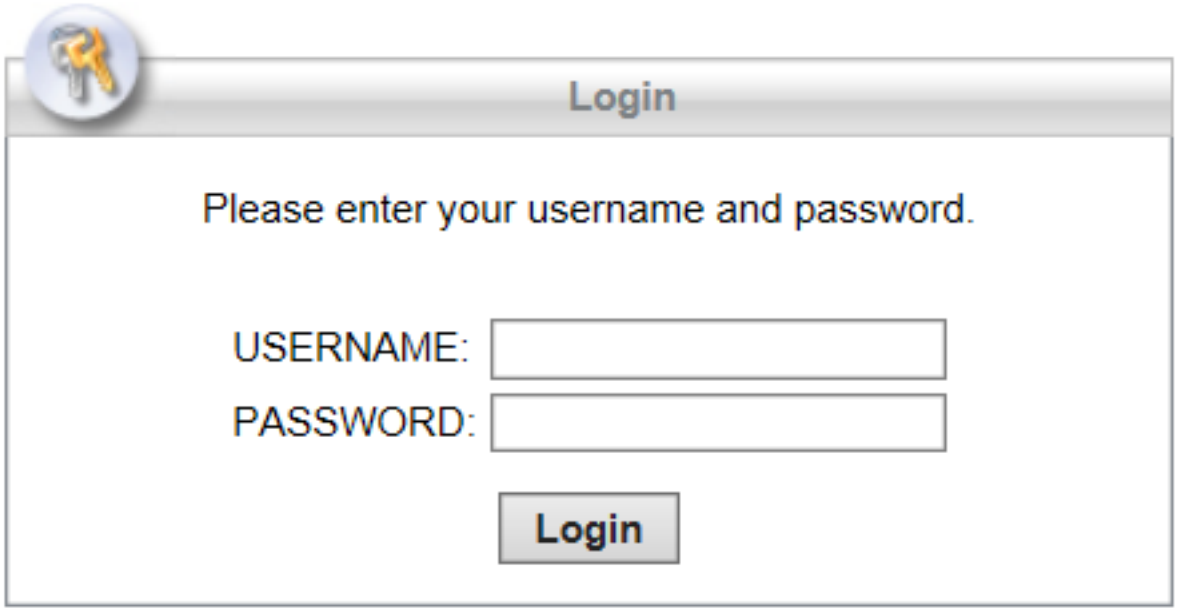


CLI:

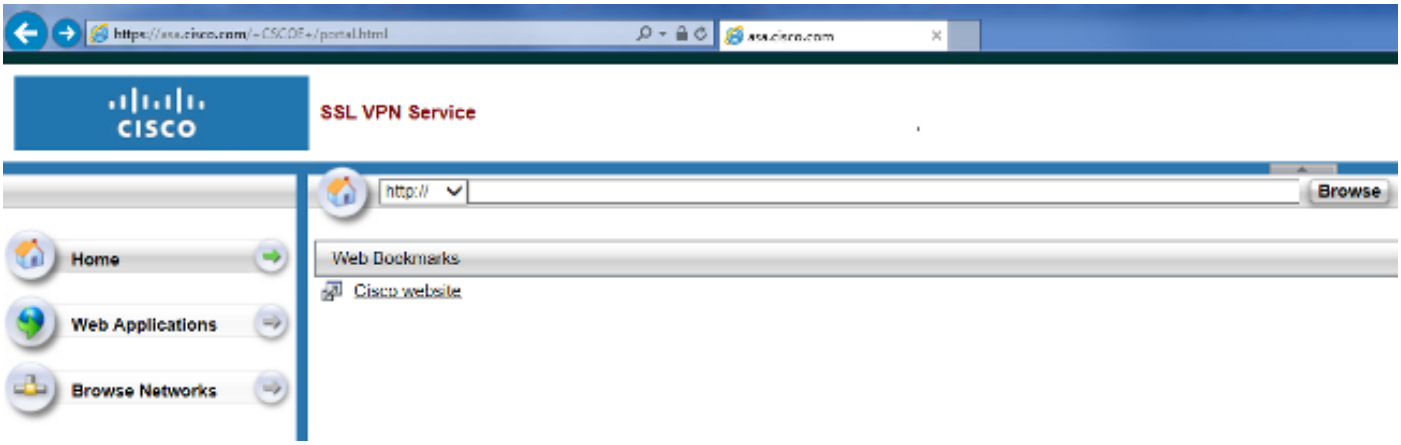
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

驗證

配置WebVPN後，在瀏覽器中使用*地址https://*<ASA的FQDN>。



登入後，您應該能夠看到用於導航到網站的位址列和書籤。



疑難排解

用於排除故障的程式

請依照以下說明進行操作，對組態進行疑難排解。

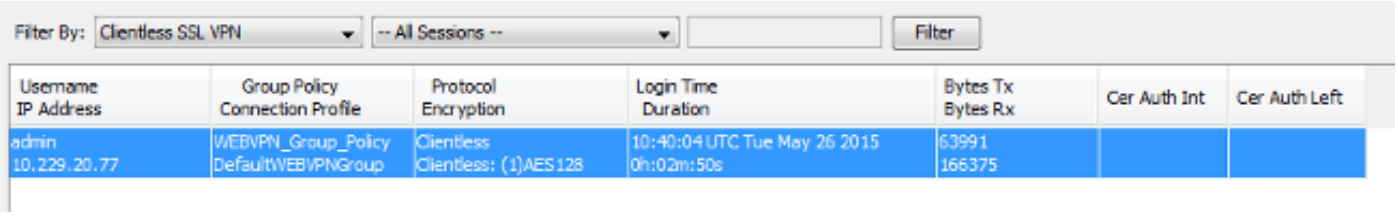
在ASDM中，選擇**Monitoring > Logging > Real-time Log Viewer > View**。當客戶端連線到ASA時，請注意建立TLS會話、選擇組策略以及成功驗證使用者。

```
Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session
```

CLI:

```
ASA(config)# logging buffered debugging
ASA(config)# show logging
```

在ASDM中，選擇**Monitoring > VPN > VPN Statistics > Sessions > Filter by:無客戶端SSL VPN**。查詢新的WebVPN會話。請務必選擇WebVPN過濾器，然後按一下**Filter**。如果出現問題，請暫時繞過ASA裝置，以確保客戶端可以訪問所需的網路資源。檢視本文檔中列出的配置步驟。



CLI:

```
ASA(config)# show vpn-sessiondb webvpn

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none
```

用於排除故障的命令

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。

- **show webvpn** — 有許多與**WebVPN**關聯的show命令。要詳細瞭解**show**命令的用法，請參閱思科安全裝置的命令參考部分。
- **debug webvpn -** 使用**debug**指令可能會對ASA造成負面影響。要詳細瞭解**debug**命令的用法，請參閱思科安全裝置的命令參考部分。

常見問題

使用者無法登入

問題

消息「不允許無客戶端（瀏覽器）SSL VPN訪問」。 登入嘗試失敗後顯示在瀏覽器中。AnyConnect Premium許可證未安裝在ASA上，或未使用，如「Premium AnyConnect license is not enabled on the ASA」所示。

解決方案

使用以下命令啟用高級AnyConnect許可證：

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

問題

登入嘗試失敗後，瀏覽器中將顯示消息「登入失敗」。已超過AnyConnect許可證限制。

解決方案

在日誌中查詢此消息：

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>
Session could not be established: session limit of 2 reached.
```

此外，請驗證您的許可證限制：

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

問題

登入嘗試失敗後，瀏覽器中會顯示消息「AnyConnect is not enabled on the VPN server」。組策略中未啟用無客戶端VPN協定。

解決方案

在日誌中查詢此消息：

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>
WebVPN session terminated: Client type not supported.
```

確保已為所需的組策略啟用無客戶端VPN協定：

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

無法將三個以上的WebVPN使用者連線到ASA

問題

只有三個WebVPN客戶端可以連線到ASA。第四個客戶端的連線失敗。

解決方案

在大多數情況下，此問題與組策略中的同時登入設定有關。使用此圖解可配置所需的同時登入數。在此示例中，所需的值為20。

```
ASA(config)# group-policy Cisco attributes
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

WebVPN客戶端無法命中書籤且呈灰色顯示

問題

如果這些書籤是為使用者登入無客戶端VPN配置的，但在主螢幕的「Web應用程式」下，它們顯示為灰色，如何啟用這些HTTP連結以便使用者能夠按一下它們並進入特定URL?

解決方案

您應該首先確保ASA可以通過DNS解析網站。嘗試按名稱ping網站。如果ASA無法解析名稱，則鏈路將呈灰色顯示。如果DNS伺服器位於您的網路內部，請配置DNS域查詢專用介面。

通過WebVPN的Citrix連線

問題

錯誤訊息「ica client received a corrupted ica file.」。 適用於Citrix over WebVPN。

解決方案

如果通過WebVPN對Citrix連線使用*安全網關*模式，則ICA檔案可能會損壞。由於ASA與此操作模式不相容，請在直接模式（非安全模式）下建立一個新的ICA檔案。

如何避免使用者進行第二次身份驗證

問題

當您訪問無客戶端WebVPN門戶上的CIFS連結時，在按一下書籤後，系統將提示您輸入憑據。輕量型目錄訪問協定(LDAP)用於驗證資源和使用者已輸入LDAP憑證以登入到VPN會話。

解決方案

在這種情況下，您可以使用自動登入功能。在正在使用的特定組策略及其WebVPN屬性下配置以下內容：

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

其中X.X.X.X=CIFSIP和*=/。

配置片段示例如下所示：

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

有關此問題的詳細資訊，請參閱使用HTTP基本或NTLM身份驗證配置SSO。

相關資訊

- ASA:使用ASDM的智慧隧道配置示例
- 技術支援與文件 - Cisco Systems