

使用AnyConnect透過CLI為路由器頭端配置基本SSL VPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[不同IOS版本的許可證資訊](#)

[重要的軟體增強功能](#)

[設定](#)

[步驟 1. 確認許可證已啟用](#)

[步驟 2. 上傳和安裝AnyConnect安全移動客戶端資料包到路由器](#)

[步驟 3. 生成RSA金鑰對和自簽名證書](#)

[步驟 4. 配置本地VPN使用者帳戶](#)

[步驟 5. 定義客戶端要使用的地址池和分割隧道訪問清單](#)

[步驟 6. 設定虛擬樣板介面\(VTI\)](#)

[步驟 7. 配置WebVPN網關](#)

[步驟 8. 配置WebVPN情景和組策略](#)

[步驟 9. 配置客戶端配置檔案 \(可選\)](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹Cisco IOS®路由器作為AnyConnect安全套接字層VPN (SSL VPN)頭端的基本配置。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS
- AnyConnect安全移動客戶端
- 一般SSL作業

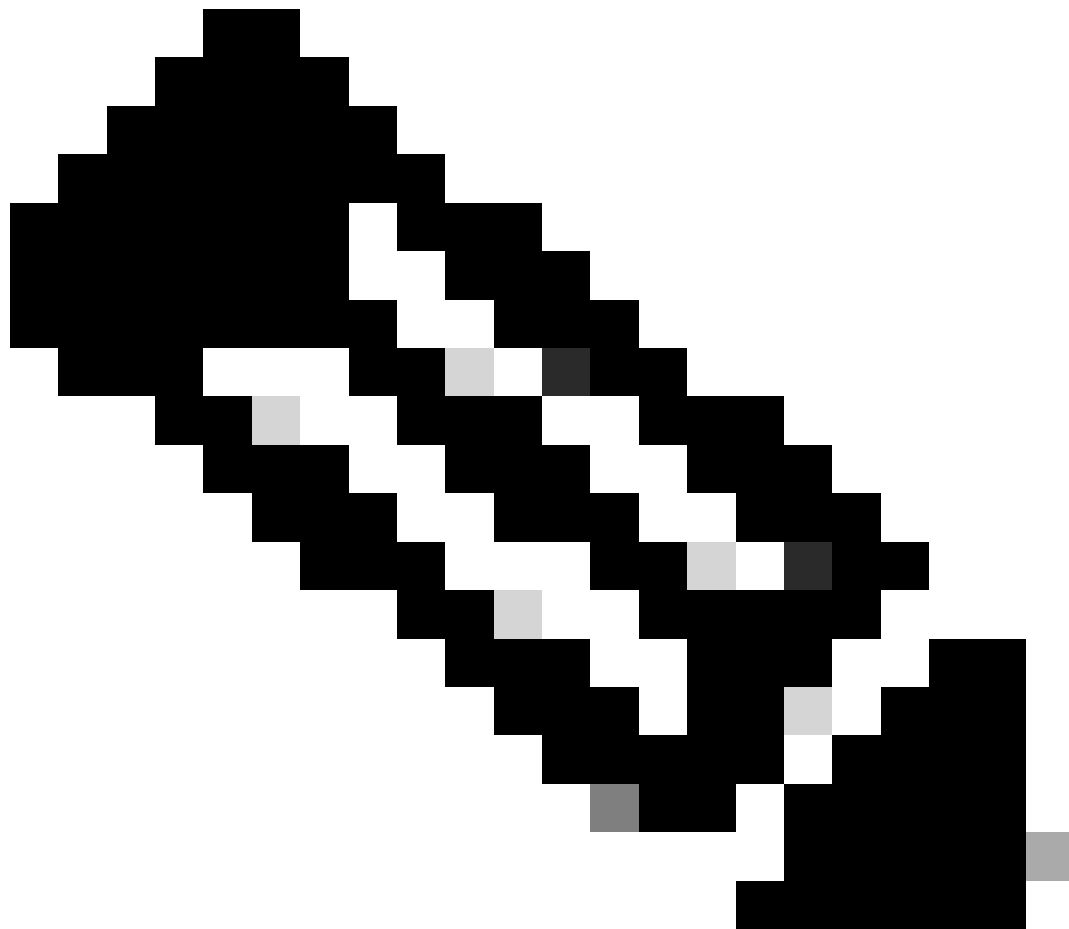
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 892W路由器，帶15.3(3)M5版
- AnyConnect安全行動化使用者端3.1.08009

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



注意：AnyConnect已重新命名為Cisco Secure Client。沒有更改其他內容，僅更改名稱，並且安裝程式相同。

不同IOS版本的許可證資訊

- 無論使用Cisco IOS版本如何，使用SSL VPN功能均需要securityk9功能集。
- Cisco IOS 12.x - SSL VPN功能整合到所有以12.4(6)T開頭的至少具有安全許可證（即advsecurityk9、adventerprisek9等）的12.x映像中。
- Cisco IOS 15.0 -較早版本需要在路由器上安裝LIC檔案，從而允許10、25或100個使用者連線。使用權*許可證在15.0(1)M4中實施。
- Cisco IOS 15.1 -較早版本需要在路由器上安裝LIC檔案，從而允許10、25或100個使用者連線。使用權*許可證在15.1(1)T2、15.1(2)T2、15.1(3)T和15.1(4)M1中實施。
- Cisco IOS 15.2 -所有15.2版本均提供SSL VPN的Right to Use*許可證。
- Cisco IOS 15.3及更高版本-早期版本提供使用權*許可證。自15.3(3)M起，SSL VPN功能在引導到securityk9技術包後可用。

對於RTU許可，當配置第一個webvpn功能（即webvpn網關1）並且已接受終端使用者許可協定(EULA)時，將啟用評估許可證。60天後，此評估許可證成為永久許可證。這些許可證基於榮譽，需要購買紙質許可證才能使用該功能。此外，RTU允許路由器平台可同時支援的最大併發連線數，而不是限制使用次數。

重要的軟體增強功能

這些錯誤ID為AnyConnect帶來了重要的功能或修復：

- 思科漏洞ID [CSCti89976](#)增加了對AnyConnect 3.x到IOS的支援。
- 用於BEAST漏洞的思科漏洞ID [CSCtx38806](#)修復，Microsoft KB2585542。

設定

步驟 1. 確認許可證已啟用

在IOS路由器頭端上配置AnyConnect的第一步是確認許可證已正確安裝（如果適用）並啟用。有關不同版本的許可證詳細資訊，請參閱上一節中的許可資訊。這取決於代碼和平台的版本，show license是否列出SSL_VPN或securityk9許可證。無論版本和許可證如何，都需要接受EULA，然後許可證將顯示為活動。

步驟 2. 在路由器上上傳和安裝AnyConnect安全移動客戶端軟體套件

為了將AnyConnect映像上傳到VPN，頭端有兩個用途。首先，只允許在AnyConnect頭端上存在AnyConnect映像的作業系統進行連線。例如，Windows客戶端要求在前端安裝Windows軟體套件，Linux 64位客戶端要求安裝Linux 64位軟體套件，等等。第二，在連線時，安裝在頭端上的AnyConnect映像會自動向下推到客戶端電腦。如果頭端上的AnyConnect軟體套件比其客戶端電腦上安裝的軟體套件新，則首次連線的使用者可以從入口網站下載客戶端，而返回的使用者可以升級。

可以透過[Cisco軟體下載網站](#)的「AnyConnect安全移動客戶端」部分獲取AnyConnect軟體套件。雖然有許多可用選項，但要在頭端安裝的軟體套件會標有作業系統和頭端部署(PKG)。AnyConnect軟

體套件當前可用於以下作業系統平台：Windows、Mac OS X、Linux (32位) 和Linux 64位。對於Linux，同時有32位和64位軟體套件。每個作業系統都需要在前端安裝適當的套件，才能允許連線。

下載AnyConnect軟體套件後，您可以透過TFTP、FTP、SCP或其他一些選項使用copy命令將其上傳到路由器快閃記憶體。以下是範例：

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0): !!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]

37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

將AnyConnect映像複製到路由器的快閃記憶體後，必須透過命令列進行安裝。在安裝命令結束時指定序列號時，可以安裝多個AnyConnect軟體套件。這樣，路由器就可以充當多個客戶端作業系統的頭端。在安裝AnyConnect軟體套件時，如果最初未將其複製到flash:/webvpn/ directory，它也會將其移到。

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1 SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

在15.2(1)T之前發佈的代碼版本中，安裝PKG的命令略有不同。

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

步驟 3.生成RSA金鑰對和自簽名證書

當您配置SSL或實施公鑰基礎架構(PKI)和數位證書的任何功能時，需要使用Rivest-Shamir-Adleman (RSA)金鑰對來簽署證書。此命令生成RSA金鑰對，然後在生成自簽名PKI證書時使用該金鑰對。使用2048位的模數並非必要條件，但建議使用最大模數，以增強安全性並增強與AnyConnect客戶端電腦的相容性。此外，建議使用與金鑰管理一起分配的描述性金鑰標籤。可使用show crypto key mypubkey rsa 命令確認金鑰的生成。



註：由於RSA金鑰是可導出的，因此建議採用的方法是確保金鑰配置為不可導出（這是預設設定）。本文檔中討論了將RSA金鑰導出到可導出的產品時涉及的風險：[在PKI中部署RSA金鑰](#)。

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048
```


The name for the keys will be: SSLVPN_KEYPAIR

```
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)
```

```
show crypto key mypubkey rsa SSLVPN_KEYPAIR
```

```
% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AEC AA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAE EB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAF A936 5C866DE8 5184D2D3
6D020301 0001
```

成功生成RSA金鑰對後，必須使用此路由器資訊和RSA金鑰對配置PKI信任點。使用者名稱中的一般名稱(CN)可設定使用者用來連線AnyConnect閘道的IP位址或完整網域名稱(FQDN)。在本示例中，客戶端在嘗試連線時使用 fdenofa-SSLVPN.cisco.com 的FQDN。雖然這不是強制性的，但當您正確輸入CN時，它有助於減少登入時提示的證書錯誤數量。

 **注意：**可以使用第三方CA頒發的證書，而不是使用路由器生成的自簽名證書。這可以透過幾種不同的方法完成，如本文檔中的[配置PKI的證書註冊](#)中所述。

```
<#root>
```

```
crypto pki trustpoint SSLVPN_CERT enrollment selfsigned subject-name CN=fdenofa-SSLVPN.cisco.com rsakeypair SSLVPN_KEYPAIR
```

正確定義信任點後，路由器必須使用**crypto pki enroll** 命令生成證書。透過此過程，可以指定一些其他引數，如序列號和IP地址；但這不是必需的。可以使用**show crypto pki certificates** 命令確認證書生成。

```
<#root>
```

```
crypto pki enroll SSLVPN_CERT % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]:
```

步驟 4. 配置本地VPN使用者帳戶

雖然可以使用外部身份驗證、授權和記帳(AAA)伺服器；例如，使用本地身份驗證。這些命令將建立使用者名稱VPNUSER，並建立名為SSLVPN_AAA的AAA身份驗證清單。

```
<#root>
```

```
aaa new-model aaa authentication login SSLVPN_AAA local username VPNUSER password TACO
```

步驟 5. 定義客戶端要使用的地址池和分割隧道訪問清單

必須建立本地IP地址池，AnyConnect客戶端介面卡才能獲取IP地址。確保配置足夠大的池，以支援最大數量的併發AnyConnect客戶端連線。

預設情況下，AnyConnect以全隧道模式運行，這意味著客戶端電腦生成的任何流量將透過隧道傳送。由於這通常是不希望出現的，因此可以配置定義流量的訪問控制清單(ACL)，該流量可以或不能透過隧道傳送。與其他ACL實現一樣，末端的隱式deny無需顯式拒絕；因此，只需為可以隧道傳輸的流量配置permit語句。

```
<#root>
```

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10 access-list 1 permit 192.168.0.0 0.0.255.255
```

步驟 6. 設定虛擬樣板介面(VTI)

[動態VTI](#)為每個VPN會話提供按需單獨的虛擬訪問介面，可為遠端訪問VPN提供高度安全且可擴展的連線。DVTI技術取代了動態加密對映，以及幫助建立隧道的動態星型方法。由於DVTI的功能與任何其他實際介面相同，因此它們允許更複雜的遠端訪問部署，因為一旦隧道處於活動狀態，它們就會支援QoS、防火牆、每使用者屬性和其他安全服務。

```
<#root>
```

```
interface Loopback0 ip address 172.16.1.1 255.255.255.255
!  
interface Virtual-Template 1 ip unnumbered Loopback0
```

步驟 7. 配置WebVPN網關

WebVPN網關定義AnyConnect前端使用的IP地址和埠，以及向客戶端提供的SSL加密演算法和PKI證書。預設情況下，網關支援所有可能的加密演算法，具體取決於路由器上的Cisco IOS版本。

```
<#root>
```

```
webvpn gateway SSLVPN_GATEWAY ip address 10.165.201.1 port 443 http-redirect port 80 ssl trustpoint SSLVPN_CERT inservice
```

步驟 8. 配置WebVPN情景和組策略

WebVPN情景和組策略定義了一些用於AnyConnect客戶端連線的附加引數。對於基本AnyConnect配置，情景僅用作一種機制，用於呼叫用於AnyConnect的預設組策略。但是，情景可用於進一步自定義WebVPN啟動頁和WebVPN操作。在定義的策略組中，SSLVPN_AAA清單被配置為使用者所屬的AAA身份驗證清單。functions svc-enabled 命令是一種配置，它允許使用者透過瀏覽器連線AnyConnect SSL VPN客戶端，而不僅僅是WebVPN。最後，其他SVC命令定義僅與SVC連線相關的引數：**svc address-pool** 通知網關將SSLVPN_POOL中的地址分發給客戶端，根據上面定義的ACL 1定義分割隧道策略，svc dns-server定義用於域名解析的DNS伺服器。透過此配置，所有DNS查詢都將傳送到指定的DNS伺服器。查詢響應中接收的地址指示是否透過隧道傳送流量。

```
<#root>
```

```
webvpn context SSLVPN_CONTEXT  
virtual-template 1
```

```
aaa authentication list SSLVPN_AAA  
gateway SSLVPN_GATEWAY inservice  
policy group SSLVPN_POLICY functions svc-enabled svc address-pool "SSLVPN_POOL" netmask 255.255.255.0  
default-group-policy SSLVPN_POLICY
```

步驟 9. 配置客戶端配置檔案 (可選)

與ASA不同的是，Cisco IOS沒有內建的GUI介面可以幫助管理員建立客戶端配置檔案。AnyConnect客戶端配置檔案需要使用[獨立配置檔案編輯器](#)單獨建立/編輯。



提示：查詢anyconnect-profileeditor-win-3.1.03103-k9.exe。

請執行這些步驟，讓路由器部署設定檔：

- 使用ftp/tftp將其上傳到IOS快閃記憶體。
- 使用此命令標識剛剛上傳的配置檔案：


```
crypto vpn annyconnect profile SSLVPN_PROFILE flash:test-profile.xml
```

 **提示：**在早於15.2(1)T的Cisco IOS版本上，需要使用此命令：`webvpn import svc profile <profile_name> flash:<profile.xml>`。

在前後關聯下，使用此指令將基本資料連結至該前後關聯：

```
<#root>
```

```
webvpn context SSLVPN_CONTEXT  
policy group SSLVPN_POLICY  
svc profile SSLVPN_PROFILE
```

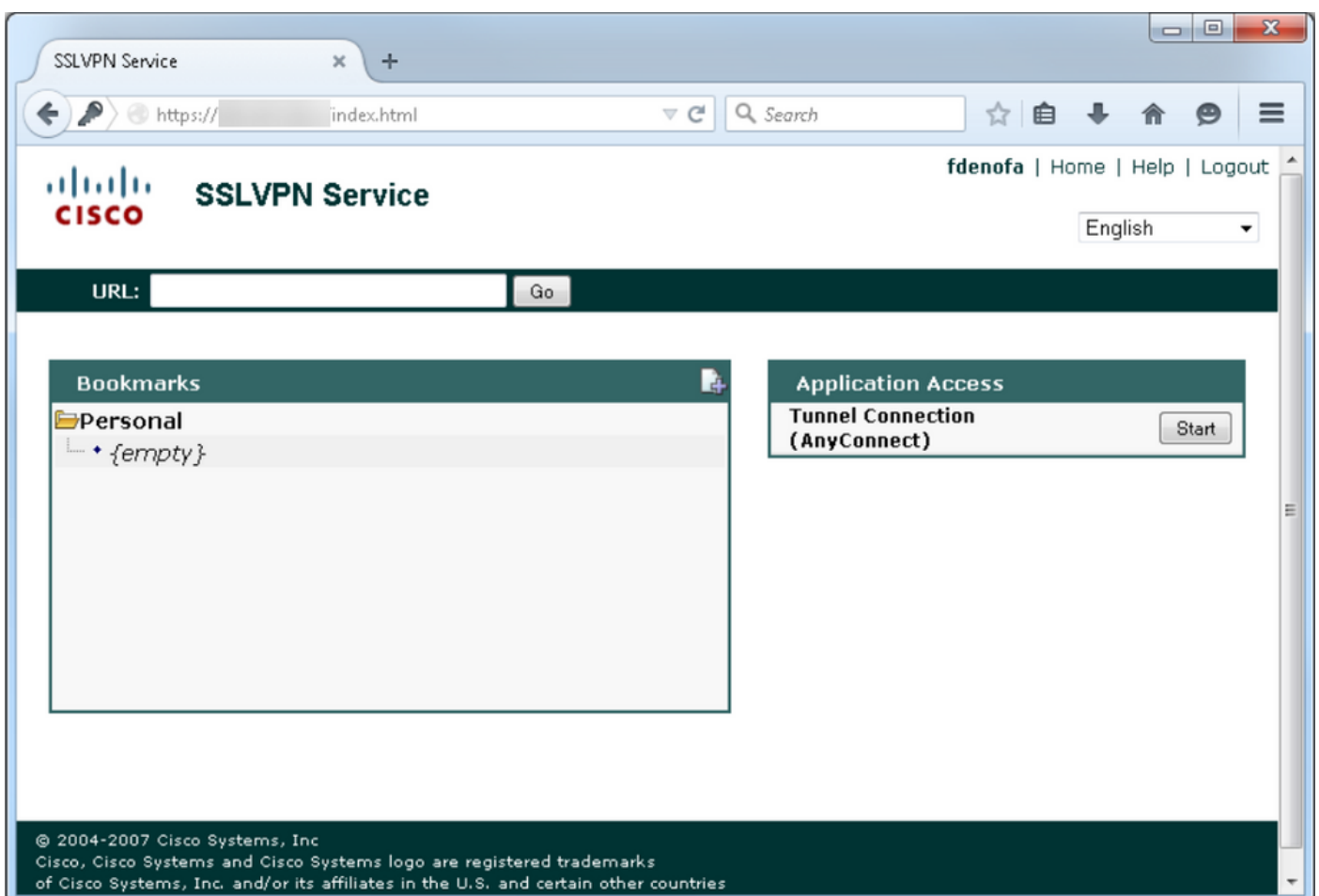
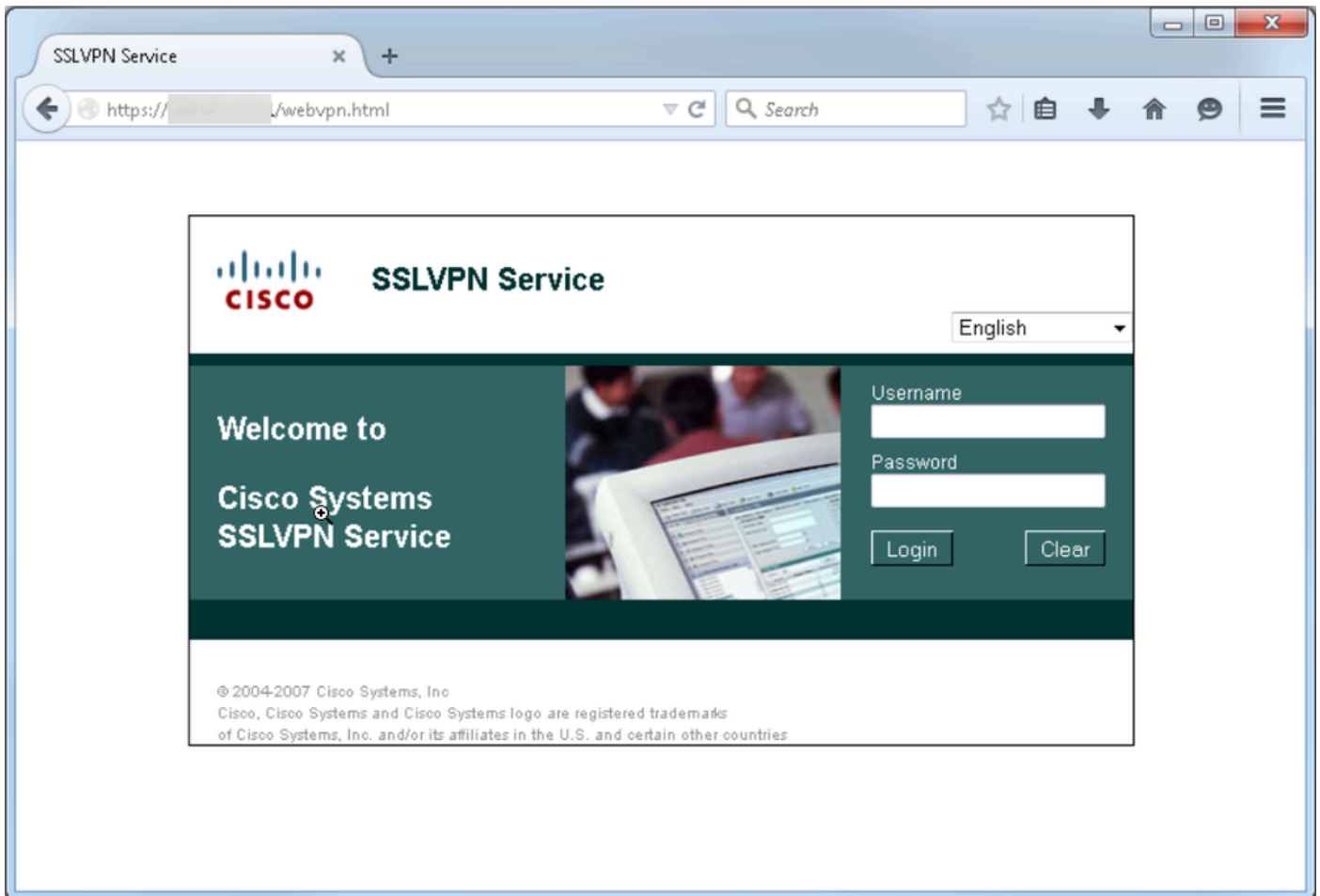
 **注意：**請使用[命令查詢工具](#)獲取有關此部分中所用命令的詳細資訊。

驗證

使用本節內容，確認您的組態是否正常運作。

設定完成後，當您透過瀏覽器存取閘道位址和連線埠時，它會返回WebVPN啟動顯示頁面：

登入後，將顯示WebVPN首頁。從此處按一下Tunnel Connection (AnyConnect)。使用Internet Explorer時，ActiveX用於下推和安裝AnyConnect客戶端。如果未檢測到，則改用Java。所有其他瀏覽器會立即使用Java。



安裝完成後，AnyConnect將自動嘗試連線到WebVPN網關。由於自簽名證書用於網關辨識自身，因此在連線嘗試期間出現多個證書警

告。這些是預期的，必須接受，連線才能繼續。為了避免這些憑證警告，顯示的自簽憑證必須安裝在使用者端電腦的受信任憑證存放區中，或者如果使用協力廠商憑證，則憑證授權機構憑證必須位於受信任的憑證存放區中。



當連線完成協商時，點選AnyConnect左下方的gear 圖示，將顯示有關連線的一些高級資訊。您可以在此頁面檢視群組原則組態中分割通道ACL所提供的一些連線統計資料和路由詳細資訊。



AnyConnect Secure Mobility Client



Virtual Private Network (VPN)

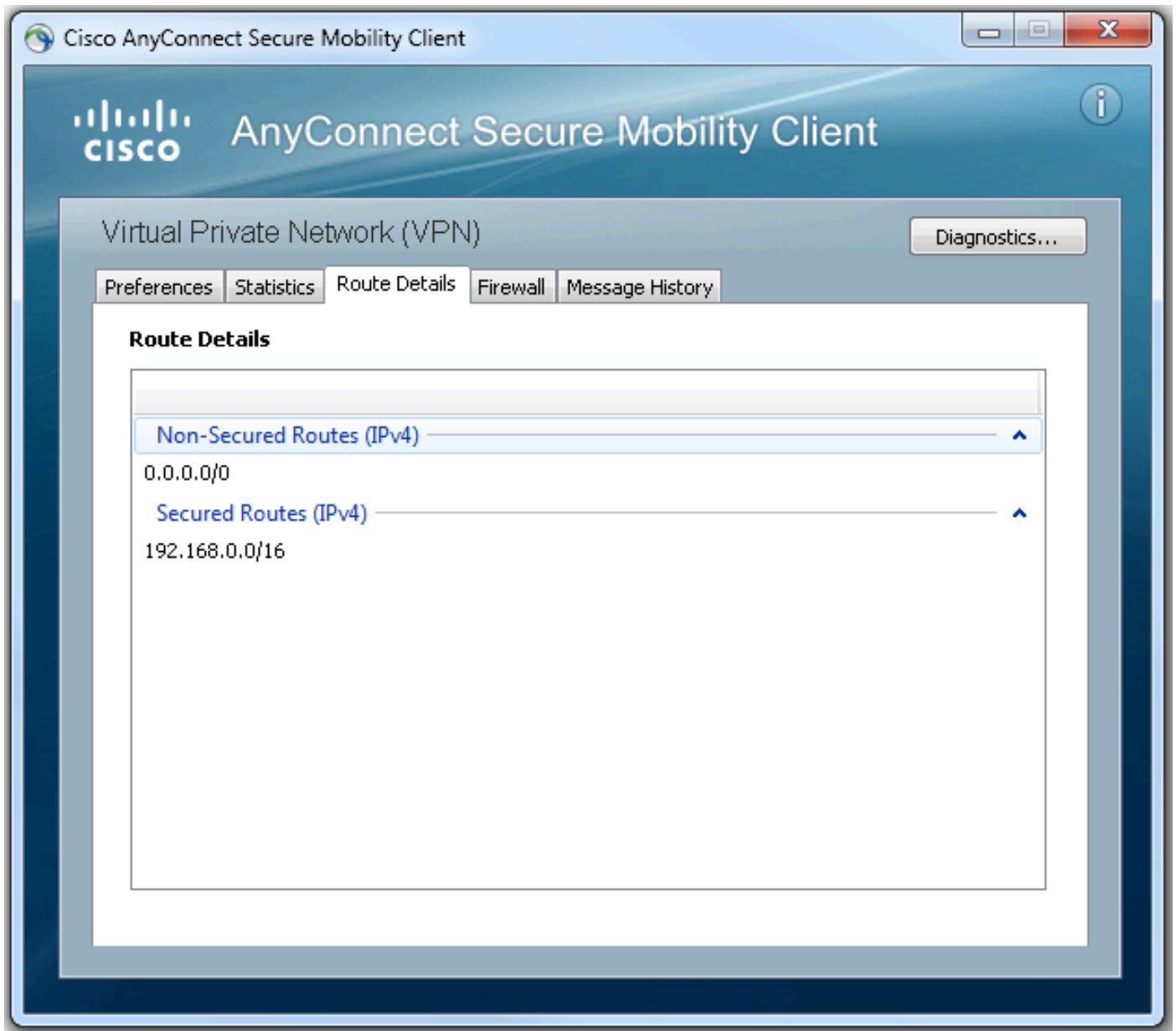
Diagnostics...

- Preferences
- Statistics
- Route Details
- Firewall
- Message History

Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Duration:	00:01:06
Address Information	
Client (IPv4):	192.168.10.2
Client (IPv6):	Not Available
Server:	
Bytes	
Sent:	4039
Received:	641
Frames	

Reset

Export Stats...



以下是組態步驟的最終執行組態結果：

```
crypto pki trustpoint SSLVPN_TP_SELFSIGNED enrollment selfsigned serial-number subject-name cn=892_SELF_SIGNED_CERT revocation-check no
crypto vpn anyconnect profile SSLVPN_PROFILE flash:test-profile.xml ! access-list 1 permit 192.168.0.0 0.0.255.255 ! ip local pool SSLVPN_POOL 192.168.0.1
aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY
! ssl authenticate verify all inservice ! policy group SSLVPN_POLICY functions svc-enabled svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
svc profile SSLVPN_PROFILE default-group-policy SSLVPN_POLICY
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

當您排除AnyConnect連線故障時，需要檢查一些常見元件：

- 由於客戶端必須提供證書，因此WebVPN網關中指定的證書必須有效。發出show crypto pki certificate可顯示關於路由器上所有證書的資訊。
- 每當更改WebVPN配置時，最佳做法是在網關和上下文中都發出 **no inservice** 和 **inservice**。這可確保變更正確生效。
- 如前所述，需要為每個連線到此網關的客戶端作業系統配備AnyConnect PKG。例如，Windows客戶端需要Windows PKG，Linux 32位客戶端需要Linux 32位PKG，等等。
- 當您考慮AnyConnect客戶端和基於瀏覽器的WebVPN都使用SSL時，要訪問WebVPN啟動顯示頁，通常表示AnyConnect能夠連線（假設相關AnyConnect配置正確）。

Cisco IOS提供可用於排除連線故障的各種調試WebVPN選項。以下是debug WebVPN aaa、debug WeVPN tunnel和show WebVPN session在成功嘗試連線時生成的輸出：

```
<#root>
```

```
fdenofa-892#show debugging WebVPN Subsystem: WebVPN AAA debugging is on WebVPN tunnel debugging is on WebVPN Tunnel Events debugging
```

相關資訊

- [SSL VPN組態設定指南，Cisco IOS版本15M&T](#)
- [使用CCP的IOS路由器上的AnyConnect VPN \(SSL\)客戶端配置示例](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。