

使用AnyConnect通过CLI为路由器头端配置基本SSL VPN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[不同IOS版本的许可证信息](#)

[重要的软件增强功能](#)

[配置](#)

[步骤1:确认许可证已启用](#)

[第二步：在路由器上上传和安装AnyConnect安全移动客户端包](#)

[第三步：生成RSA密钥对和自签名证书](#)

[第四步：配置本地VPN用户帐户](#)

[第五步：定义供客户端使用的地址池和拆分隧道访问列表](#)

[第六步：配置虚拟模板接口\(VTI\)](#)

[步骤 7.配置WebVPN网关](#)

[步骤 8配置WebVPN上下文和组策略](#)

[步骤 9配置客户端配置文件（可选）](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍Cisco IOS®路由器作为AnyConnect安全套接字层VPN (SSL VPN)头端的基本配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS
- AnyConnect 安全移动客户端
- 一般SSL操作

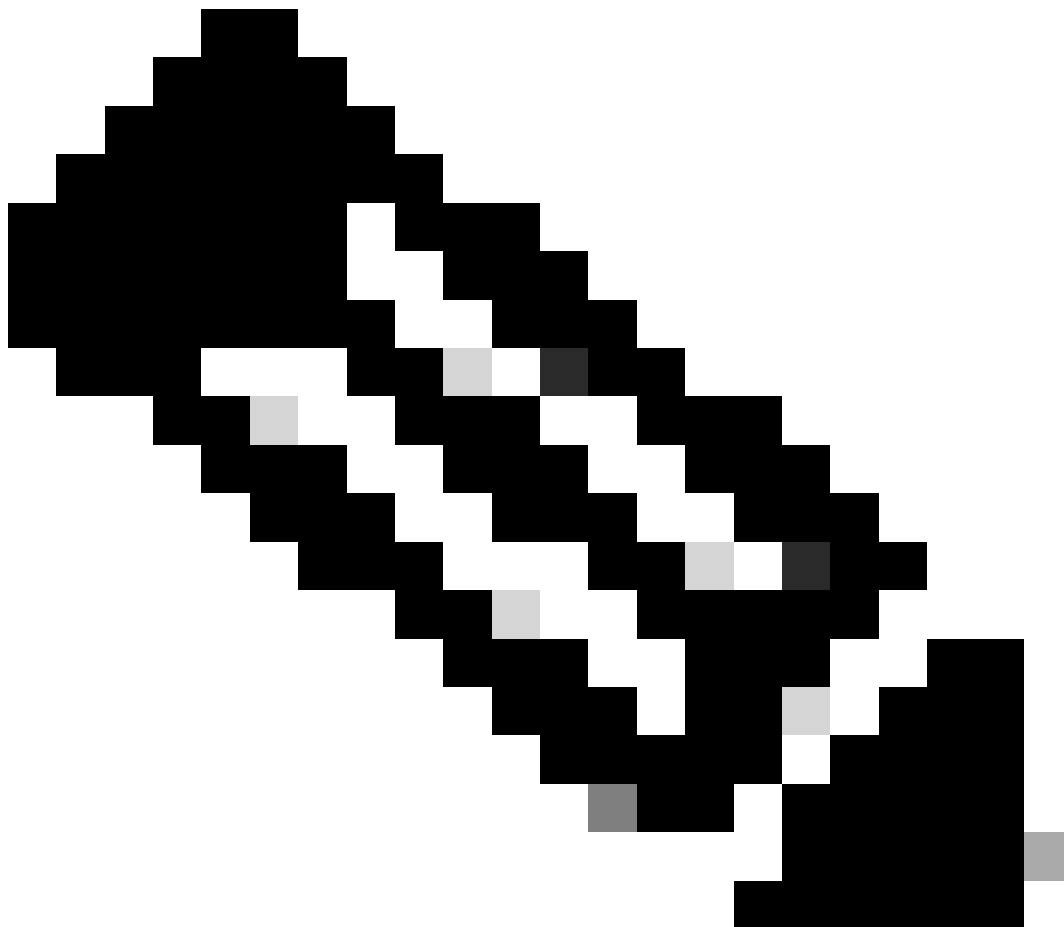
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科892W路由器，带版本15.3(3)M5
- AnyConnect安全移动客户端3.1.08009

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息



注意：AnyConnect已更名为Cisco Secure Client。没有其他任何更改，只有名称，并且安装过程是相同的。

不同IOS版本的许可证信息

- 无论使用何种思科IOS版本，使用SSL VPN功能都需要使用securityk9功能集。
- Cisco IOS 12.x - SSL VPN功能集成到所有以12.4(6)T开头的12.x映像，这些映像至少具有安全许可证（即advsecurityk9、adventerprisek9等）。
- Cisco IOS 15.0 -早期版本需要在路由器上安装LIC文件，该文件支持10、25或100个用户连接。使用权*许可证在15.0(1)M4中实施。
- Cisco IOS 15.1 -早期版本需要在路由器上安装一个LIC文件，该文件支持10、25或100个用户连接。使用权*许可证在15.1(1)T2、15.1(2)T2、15.1(3)T和15.1(4)M1中实施。
- Cisco IOS 15.2 -所有15.2版本均提供SSL VPN的使用权*许可证。
- Cisco IOS 15.3及以上版本-早期版本提供使用权*许可证。从15.3(3)M开始，SSL VPN功能在引导到securityk9技术包后可用。

对于RTU许可，当配置第一个webvpn功能（即webvpn网关1）并且已接受最终用户许可协议(EULA)时，将启用评估许可证。60天后，此评估许可证成为永久许可证。这些许可证基于荣誉，需要购买纸质许可证才能使用该功能。此外，RTU没有限制一定数量的使用，而是允许路由器平台同时支持的最大并发连接数。

重要的软件增强功能

这些Bug ID为AnyConnect带来了重要的功能或修复：

- Cisco bug ID [CSCti89976](#)（仅限注册用户）添加了对IOS中AnyConnect 3.x的支持。
- BEAST漏洞的思科漏洞ID [CSCtx38806](#)修复，Microsoft KB2585542。

配置

步骤1:确认许可证已启用

在IOS路由器头端上配置AnyConnect的第一步是确认许可证已正确安装（如果适用）并启用。有关不同版本的许可证详细信息，请参阅上一节中的许可信息。这取决于代码和平台的版本，即show license列出SSL_VPN或securityk9许可证。无论版本和许可证如何，都需要接受EULA，然后许可证将显示为活动。

第二步：在路由器上上传和安装AnyConnect安全移动客户端软件包

要将AnyConnect映像上传到VPN，头端有两个用途。首先，仅允许在AnyConnect头端上存在AnyConnect映像的操作系统进行连接。例如，Windows客户端要求在头端安装Windows程序包，Linux 64位客户端要求安装Linux 64位程序包，等等。第二，在连接时，安装在头端上的AnyConnect映像会自动下推到客户端计算机。如果头端上的AnyConnect软件包比其客户端计算机上安装的软件包要新，则首次连接的用户可以从Web门户下载客户端，而返回的用户可以升级。

您可以通过[Cisco软件下载网站](#)的“AnyConnect安全移动客户端”部分获取AnyConnect软件包。尽管有许多选项可用，但要在头端安装的软件包标有操作系统和头端部署(PKG)。AnyConnect软件包目前可用于以下操作系统平台：Windows、Mac OS X、Linux（32位）和Linux 64位。对于Linux，有

32位和64位软件包。每个操作系统都需要在头端安装适当的软件包，以便允许连接。

下载AnyConnect软件包后，可以通过TFTP、FTP、SCP或其他一些选项使用copy命令将其上传到路由器闪存。例如：

```
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)
```

将AnyConnect映像复制到路由器的闪存后，必须通过命令行进行安装。如果在安装命令结束时指定了序列号，则可以安装多个AnyConnect软件包。这样，路由器就可以充当多个客户端操作系统的前端。在安装AnyConnect软件包时，如果最初没有将其复制到flash:/webvpn/ directory，它也会将其移动到。


```
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之前发布的代码版本中，安装PKG的命令略有不同。

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

第三步：生成RSA密钥对和自签名证书

当您配置SSL或实施公钥基础设施(PKI)和数字证书的任何功能时，证书签名需要Rivest-Shamir-Adleman (RSA)密钥对。此命令生成RSA密钥对，然后生成自签名PKI证书时使用该密钥对。使用2048位的模数是不必要的，但建议使用最大模数来增强安全性并与AnyConnect客户端计算机兼容。还建议使用通过密钥管理分配的描述性密钥标签。使用show crypto key mypubkey rsa命令可确认密钥生成。

 **注意：**由于RSA密钥可导出存在许多安全风险，因此建议的做法是确保密钥配置为不可导出（这是默认设置）。本文档讨论了将RSA密钥导出时所涉及的风险：[在PKI内部署RSA密钥](#)。

```
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 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAF9A936 5C866DE8 5184D2D3
6D020301 0001
```

成功生成RSA密钥对后，必须使用此路由器信息和RSA密钥对配置PKI信任点。Subject-Name中的公用名(CN)可以使用用户用于连接AnyConnect网关的IP地址或完全限定域名(FQDN)进行配置。在本示例中，客户端在尝试连接时使用 fdenofa-SSLVPN.cisco.com 的 FQDN。虽然这不是必需的，但当您正确输入CN时，它有助于减少登录时提示的证书错误数量。

 **注意：**可以使用第三方CA颁发的证书，而不是使用路由器生成的自签名证书。这可以通过几种不同的方法完成，如本[文档配置PKI的证书注册](#)中所述。

<#root>

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

在正确定义信任点后，路由器必须使用 `crypto pki enroll` 命令生成证书。通过此过程，可以指定一些其他参数，如序列号和IP地址；但是，这不是必需的。使用 `show crypto pki certificates` 命令可确认证书生成。

<#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]:
```

第四步：配置本地VPN用户帐户

虽然可以使用外部身份验证、授权和记帐(AAA)服务器；在本例中，使用本地身份验证。这些命令将创建用户名VPNUSER，并创建名为SSLVPN_AAA的AAA身份验证列表。

```
<#root>
```

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

第五步：定义供客户端使用的地址池和拆分隧道访问列表

必须创建本地IP地址池，AnyConnect客户端适配器才能获取IP地址。确保配置足够大的池以支持最大数量的并发AnyConnect客户端连接。

默认情况下，AnyConnect在全隧道模式下运行，这意味着客户端计算机生成的任何流量都会通过隧道发送。由于这通常是不理想的，因此可以配置定义流量的访问控制列表(ACL)，该流量可以或不能通过隧道发送。与其他ACL实现一样，末尾的隐式deny不需要显式deny；因此，只需为可以隧道传输的流量配置permit语句。

```
<#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
```

第六步：配置虚拟模板接口(VTI)

[动态VTI](#)为每个VPN会话提供按需独立虚拟访问接口，允许远程访问VPN实现高度安全且可扩展的连接。DVTI技术取代了动态加密映射和帮助建立隧道的动态中心辐射型方法。由于DVTI的功能与任何其他实际接口类似，因此它们允许更复杂的远程访问部署，因为它们支持隧道一旦激活时的QoS、防火墙、每用户属性和其他安全服务。

```
<#root>
```

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

步骤 7.配置WebVPN网关

WebVPN网关是定义AnyConnect头端使用的IP地址和端口，以及提供给客户端的SSL加密算法和PKI证书的来源。默认情况下，网关支持所有可能的加密算法，具体取决于路由器上的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
```

步骤 8配置WebVPN上下文和组策略

WebVPN情景和组策略定义用于AnyConnect客户端连接的一些其他参数。对于基本AnyConnect配置，情景仅用作一种机制，用于调用用于AnyConnect的默认组策略。但是，上下文可用于进一步自定义WebVPN启动页和WebVPN操作。在定义的策略组中，SSLVPN_AAA列表配置为用户所属的AAA身份验证列表。functions svc-enabled 命令是允许用户通过浏览器连接AnyConnect SSL

VPN客户端 (而不仅是WebVPN) 的配置片段。最后, 其他SVC命令定义仅与SVC连接相关的参数: `svc address-pool` 告知网关将SSLVPN_POOL中的地址分发给客户端, 根据上面定义的ACL 1定义svc split include 义拆分隧道策略, 以及svc dns-server定义用于域名解析的DNS服务器。使用此配置, 所有DNS查询都将发送到指定的DNS服务器。查询响应中接收的地址指示是否通过隧道发送流量。

```
<#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 s  
default-group-policy SSLVPN_POLICY
```

步骤 9配置客户端配置文件 (可选)

与ASA不同, Cisco IOS没有内置GUI界面, 无法帮助管理员创建客户端配置文件。AnyConnect客户端配置文件需要使用[独立配置文件编辑器](#)单独创建/编辑。



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

要让路由器部署配置文件, 请执行以下步骤:

- 使用ftp/tftp将其上传到IOS闪存。
- 使用此命令识别刚刚上传的配置文件:

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




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

在情景下, 使用此命令将配置文件链接到该情景:

<#root>

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

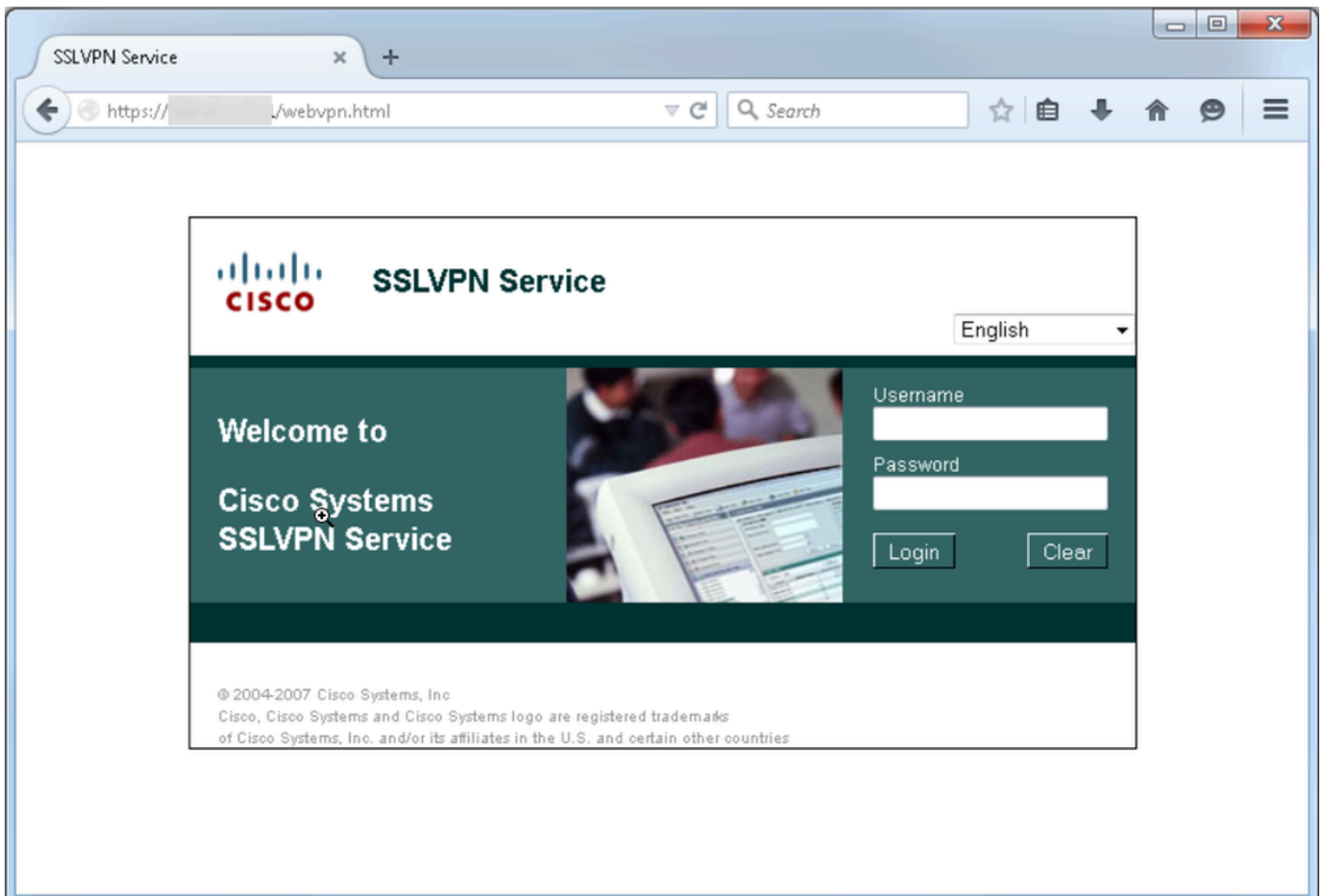
 **注意：**请使用[命令查找工具](#)获取有关此部分使用的命令的详细信息。

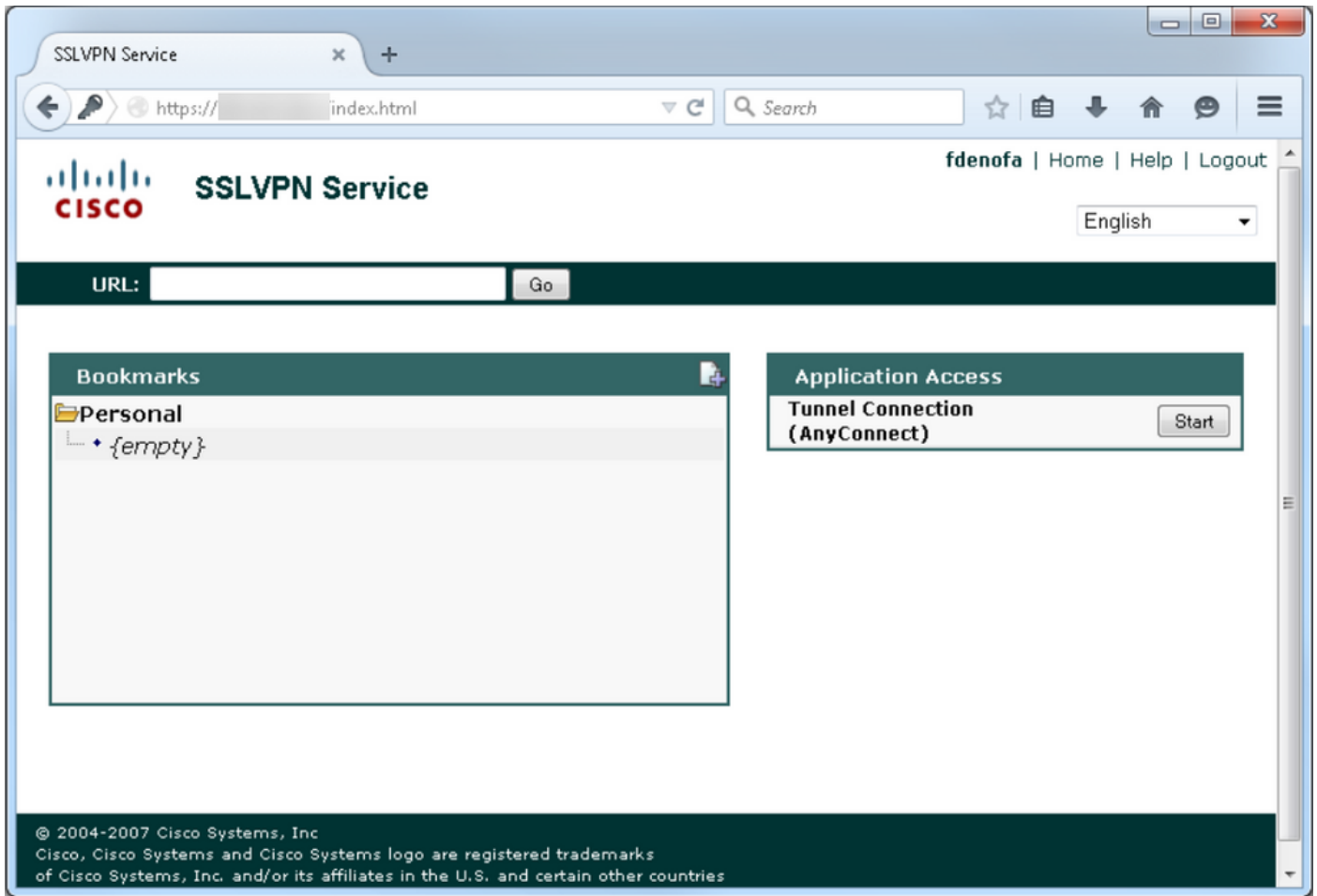
验证

使用本部分可确认配置能否正常运行。

配置完成后，当通过浏览器访问网关地址和端口时，它将返回到WebVPN启动页：

登录后，将显示WebVPN主页。从此处单击Tunnel Connection (AnyConnect)。使用Internet Explorer时，ActiveX用于向下推送和安装AnyConnect客户端。如果未检测到，则改为使用Java。所有其他浏览器立即使用Java。





安装完成后，AnyConnect会自动尝试连接到WebVPN网关。由于自签名证书用于网关标识自身，因此在尝试连接期间会出现多个证书警告。这些应为预期值，必须接受它们才能继续连接。为了避免这些证书警告，提供的自签名证书必须安装在客户端计算机的受信任证书库中，或者如果使用第三方证书，则证书颁发机构证书必须位于受信任的证书库中。



当连接完成协商时，点击AnyConnect左下角的gear 图标，将显示有关连接的一些高级信息。在此页上，可以查看从组策略配置中的拆分隧道ACL获得的一些连接统计信息和路由详细信息。



AnyConnect Secure Mobility Client



Virtual Private Network (VPN)

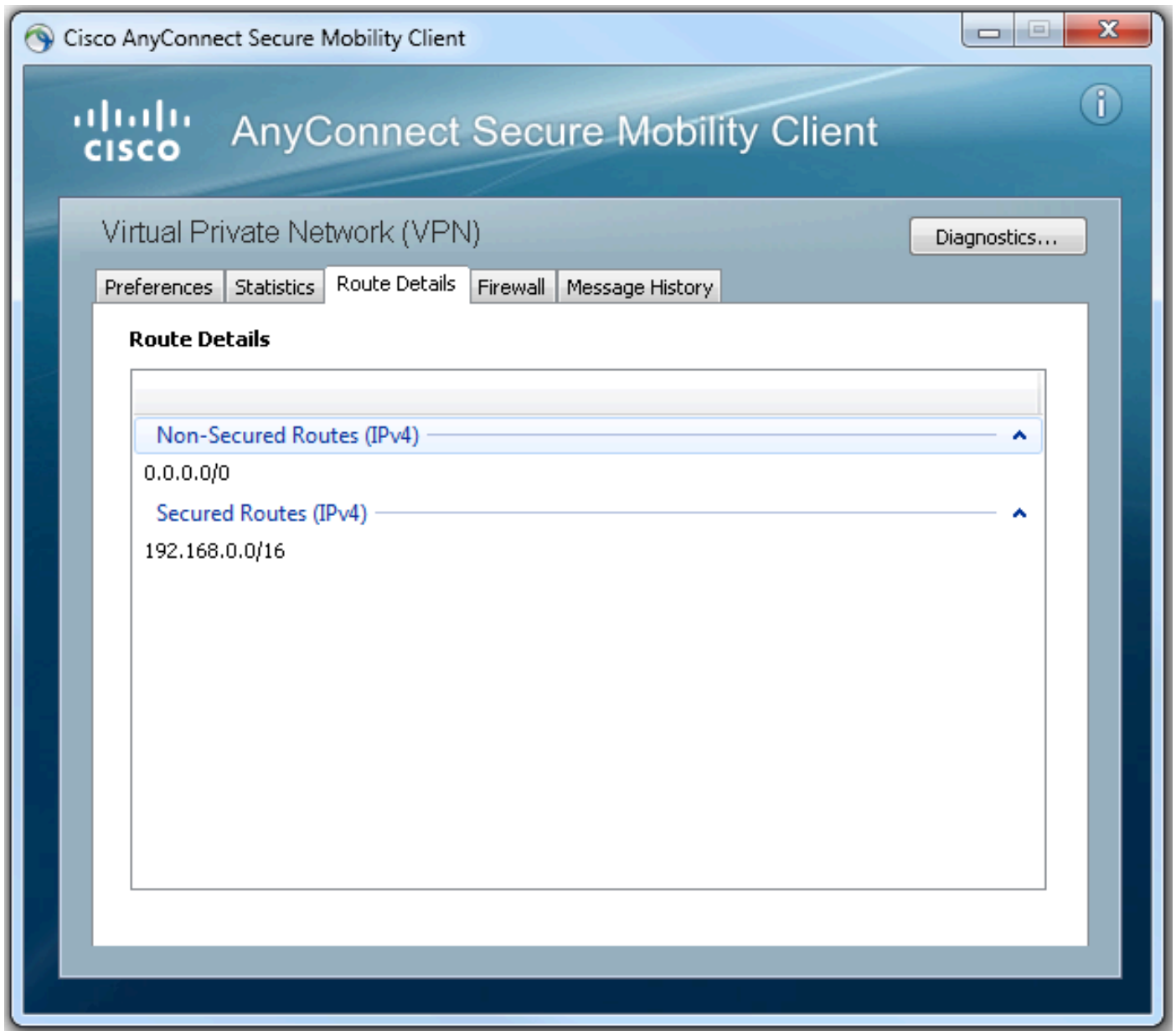
Diagnostics...

- 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...



以下是配置步骤的最终运行配置结果：

```
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 192.168.0.1 192.168.0.254
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

当您排除AnyConnect连接故障时，可以检查一些常见组件：

- 由于客户端必须提供证书，因此WebVPN网关中指定的证书必须有效。发出show crypto pki certificate命令将显示与路由器上所有证书相关的信息。
- 每当更改WebVPN配置时，最佳做法是在网关和上下文中都发出 **no inservice** 和 **inservice**。这可确保更改正确生效。
- 如前所述，连接到此网关的每个客户端操作系统都需要一个AnyConnect PKG。例如，Windows客户端需要Windows PKG，Linux 32位客户端需要Linux 32位PKG，等等。
- 如果将AnyConnect客户端和基于浏览器的WebVPN都视为使用SSL，则访问WebVPN启动页通常表示AnyConnect能够连接（假设相关AnyConnect配置正确）。

Cisco IOS提供可用于排除连接故障的各种调试WebVPN选项。以下是debug WebVPN aaa、debug WeVPN tunnel和show WebVPN session upon a successful connection attempt生成的输出：

```
<#root>
```

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

相关信息

- [SSL VPN配置指南，Cisco IOS版本15M&T](#)
- [在IOS路由器上有CCP的AnyConnect VPN \(SSL\)客户端配置示例](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。