AnyConnect ：配置IOS路由器头端的基本SSLVPN与使用CLI

目录

简介

本文描述Cisco IOS路由器的基本配置作为AnyConnect SSLVPN头端。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco互联网操作系统(IOS)
- AnyConnect安全移动性客户端
- 一般安全套接字协议层(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：

- 运行15.3(3)M5的思科892W路由器
- AnyConnect安全移动性客户端3.1.08009

不同的IOS版本的许可授权的信息

- securityk9特性组要求使用SSLVPN功能， IOS版本使用。
- IOS 12.x - SSLVPN功能集成到从12.4(6)T开始有至少一个安全许可证的所有12.x镜像(IE。advsecurityk9， adventerprisek9，等等)。
- IOS 15.0 -更早版本要求在将允许10， 25或者100用户连接的路由器将安装的LIC文件。对Use*许可证的权利在15.0(1)M4实现
- IOS 15.1 -更早版本要求在将允许10， 25或者100用户连接的路由器将安装的LIC文件。对Use*许可证的权利在15.1(1)T2、15.1(2)T2、15.1(3)T和15.1(4)M1实现
- IOS 15.2 -全部15.2版本提供权利对SSLVPN的Use*许可证
- IOS 15.3和以远-更早版本提供权利对Use*许可证。在您启动到securityk9技术包后，开始在15.3(3)M， SSLVPN功能是可用的

对于许可授权的RTU，评估许可证将启用，当第一个WebVPN功能配置(即webvpn gateway GATEWAY1)，并且终端用户许可权协定(EULA)接受。在60天之后，此评估许可证变为永久许可证。这些许可证是基于的荣誉称号并且要求纸许可证采购为了使用功能。另外，而不是对一定数量的用途被限制， RTU允许路由器平台可以同時支持同时连接的最大。

重大软件增强

这些Bug ID导致重大的功能或修正AnyConnect的：

- CSCti89976 ： AnyConnect的3.x已添加支持对IOS
- CSCtx38806 ： 野兽漏洞的修正， Microsoft KB2585542

配置

步骤1.确认许可证启用

第一步，当AnyConnect在IOS路由器头端时配置将确认许可证正确地安装(如果适用)并且启用。参考在前面部分的许可授权的信息在不同的版本的许可授权的特定的。它取决于编码版本，并且平台是否请显示许可证列出一个SSL_VPN或securityk9许可证。不管版本和许可证， EULA将需要接受，并且许可证将显示作为激活。

步骤2.加载和安装AnyConnect安全移动性在路由器的客户端包

上载AnyConnect镜像到VPN头端服务两个目的。首先，安排AnyConnect镜像在AnyConnect头端仅的操作系统允许连接。例如， Windows客户端需要在头端将安装的Windows包， 64位客户端需要Linux 64位包的Linux，等等。其次，在头端安装的AnyConnect镜像将自动地增加到在连接的客户端机器。连接的用户第一次能下载返回能升级从Web门户的客户端和用户，假设在头端的AnyConnect包新比什么在他们的客户端机器安装。

AnyConnect包可以通过Cisco软件下载网站的AnyConnect安全移动性客户端部分得到。当有许多选项联机时，将安装在头端的包将标志操作系统和首端部署(PKG)。AnyConnect包为这些操作系统平

台是现在可以得到的：Windows、Mac OS X、64位Linux (32位)和的Linux。注意Linux的，有两32和64位包。每个操作系统要求在头端将安装的适当的包为了能将允许的连接。

一旦AnyConnect包下载，可以上传到路由器闪存用**copy命令**通过TFTP、FTP、SCP，或者一些个其它选项。示例如下：

```
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)
```

在您复制AnyConnect镜像对路由器的闪存后，必须通过line命令安装。当您指定序号在安装命令结束时时，多个AnyConnect包可以安装;这将允许路由器作为多个客户操作系统的头端。当您安装AnyConnect包，也将移动它向**flash: /webvpn/目录，**如果最初未复制那里。

```
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前发布的编码版本，命令安装PKG是有些不同的。

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

步骤3.启用在路由器的HTTP服务器

```
ip http server
ip http secure-server
```

步骤4.生成RSA密钥对和自签名证书

当您配置SSL或实现公共密钥基础设施(PKI)和数字证书的所有功能时， Rivest Shamir Adelman (RSA)密钥对为签署证书要求。跟随命令将生成然后将使用的RSA密钥对，当自已签署的PKI证书生成。当您利用2048个位时的模数，它不是需求，推荐使用最大的模数联机高级安全和兼容性用AnyConnect客户端机器。要使用，因为将允许密钥管理，方便一个说明性标签也推荐。密钥生成可以用**show crypto key mypubkey rsa命令**确认。

> **注意**：尽管有许多安全风险关联与进行的RSA锁上可导出，是默认的推荐的方法是保证密钥配置不可导出。是包含的风险，当您做时RSA在本文锁上可导出讨论：部署在PKI内的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 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 exportable.
Key Data&colon;
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 2EAFA936 5C866DE8 5184D2D3
6D020301 0001
```

一旦RSA密钥对顺利地生成，必须配置Pki trustpoint与我们的路由器信息和RSA密钥对。应该配置在的共同名称(CN) subject-name用用户使用连接到AnyConnect网关的IP地址或全双工合格的域名(FQDN);在本例中，当他们尝试连接时，客户端使用fdenofa-SSLVPN.cisco.com FQDN。当不是必须时，当您在CN时正确地输入，帮助减少的证书错误数量被提示在登录。

> **注意**：而不是使用路由器生成的自签名证书，使用第三方CA发出的证书是可能的。这可以通过一些不同的说法执行如本文所述： 配置PKI的证书登记。

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

在信任点正确地定义后，路由器必须生成证书通过使用**crypto pki登记**命令。使用此进程，指定一些个其他参数例如序列号和IP地址是可能的。然而，这没有要求。证书生成可以用**显示crypto pki证书**命令确认。

```
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]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

```
show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
```

```
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
    end   date: 20:00:00 EDT Dec 31 2019
  Associated Trustpoints: SSLVPN_CERT
```

步骤5.配置本地VPN用户帐户

当使用外部验证、授权和核算(AAA)时是可能的服务器，为了此示例本地认证使用。这些命令将创建用户名VPNUSER并且建立名为SSLVPN_AAA的AAA认证列表。

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

步骤6.定义客户端将使用的地址池和分割隧道访问列表

本地IP地址池必须创建为了AnyConnect客户端适配器能获取IP地址。保证您配置一个足够大池支持同时AnyConnect客户端连接最大。

默认情况下， AnyConnect在意味着的全通道模式将运行客户端机器生成的所有流量在通道间将发送。因为这不典型地是理想，配置访问控制表(ACL)然后定义了流量应该或不应该在通道间发送的是可能的。如同其他ACL实施，隐式拒绝在末端排除需要对于明确拒绝;因此，配置应该以隧道传输的流量的permit语句只是必要的。

```
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
```

步骤7.配置虚拟模板接口(VTI)

动态VTIs 为允许高度安全和可扩展连接远程访问VPN的每VPN会话提供一个根据要求分开的虚拟访问接口。DVTI技术替换动态加密映射和帮助建立通道的动态星型网方法。 由于DVTIs功能类似他们允许更加复杂的远程Accesss部署的其他真正的接口，因为他们支持QoS、防火墙、每用户attribtues和其他安全服务，当通道是活跃的。

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

步骤8.配置Webvpn gateway

Webvpn gateway是什么定义了将由AnyConnect头端使用的IP地址和端口，以及Ssl encryption算法和将被提交给客户端的PKI证书。默认情况下，网关将支持所有可能的加密算法，根据在路由器的IOS版本变化。

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

步骤9.配置WebVPN上下文并且分组策略

WebVPN上下文和组策略定义了将使用AnyConnect客户端连接的一些另外的参数。对于一基本AnyConnect配置，上下文担当用于的机制呼叫将使用AnyConnect的默认组策略。然而，上下文可以用于进一步定制WebVPN飞溅页和WebVPN操作。在定义的策略组中， SSLVPN_AAA列表配置作为用户是成员的AAA认证列表。**功能svc启用的**命令是允许用户连接AnyConnect **SSL VPN客户端**而不是WebVPN通过浏览器配置的片段。最后，与SVC连接是仅相关的其他SVC define命令参数：**svc地址池**通知网关对在ACPool的赠送品地址对客户端， **svc split包括**定义了分割隧道策略每个1定义的ACL以上，并且**svc dns-server**定义了DNS服务器哪些将使用域名解决方法。使用此配置，所有DNS查询将被发送到指定的DNS服务器。在查询答复接收的地址指明流量是否在通道间发送。

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

步骤10 (可选)。配置客户端配置文件

不同于在ASA， Cisco IOS没有能协助解决在创建客户端配置文件的admins的一个内置的GUI界面。AnyConnect客户端配置文件需要用独立配置文件编辑器分开创建/编辑。

提示：寻找anyconnect-profileeditor-win-3.1.03103-k9.exe

遵从这些步骤安排路由器部署配置文件：

1. 使用ftp/tftp，上传它对IOS闪存
2. 请使用此命令识别上传的配置文件：

1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```
提示：在IOS版本旧比15.2(1)T，需要使用此命令：**WebVPN导入svc配置文件<profile_name> flash: <profile.xml>**

3. 在上下文下，请使用此命令与该上下文连接配置文件：

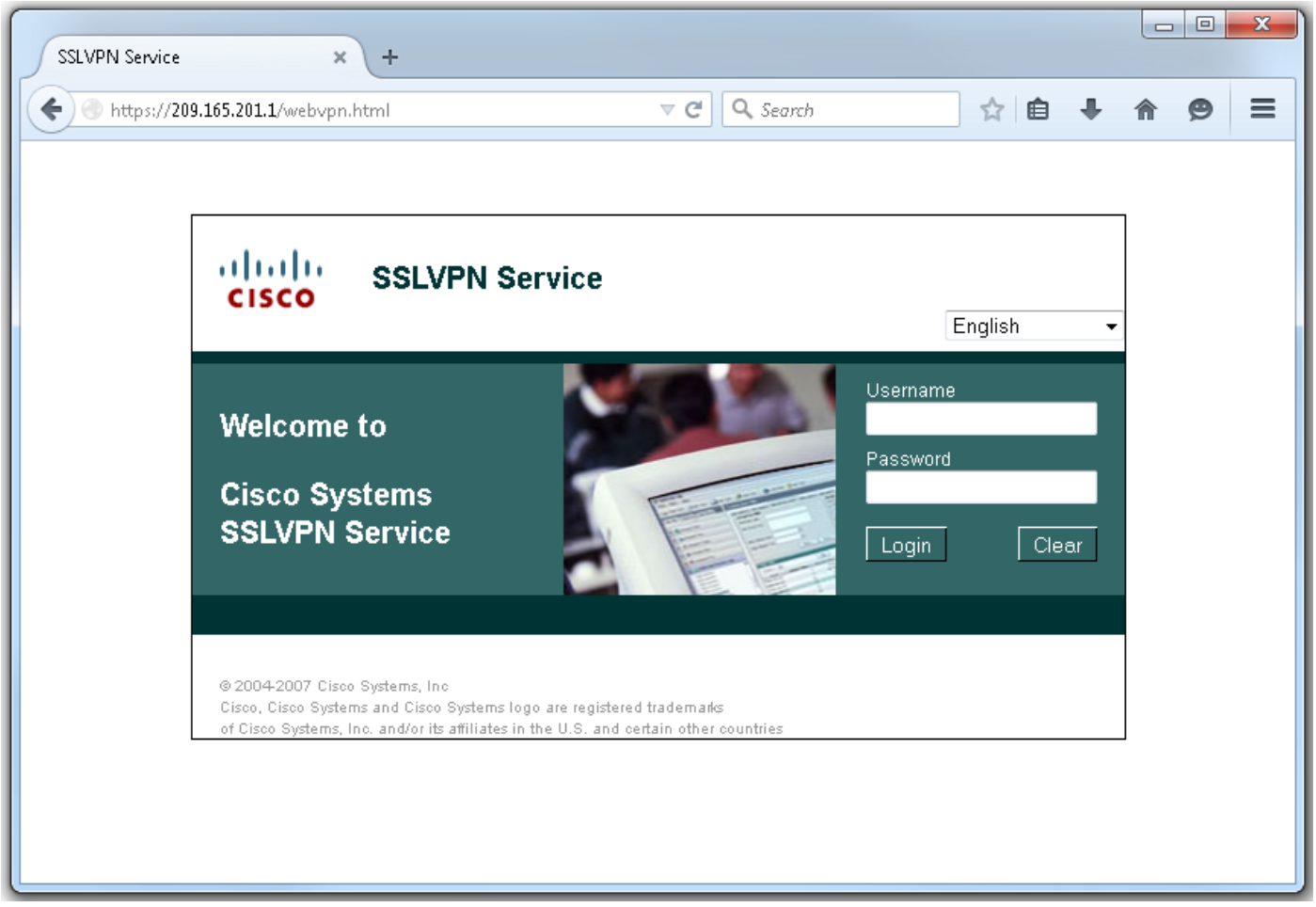
1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
```

```
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

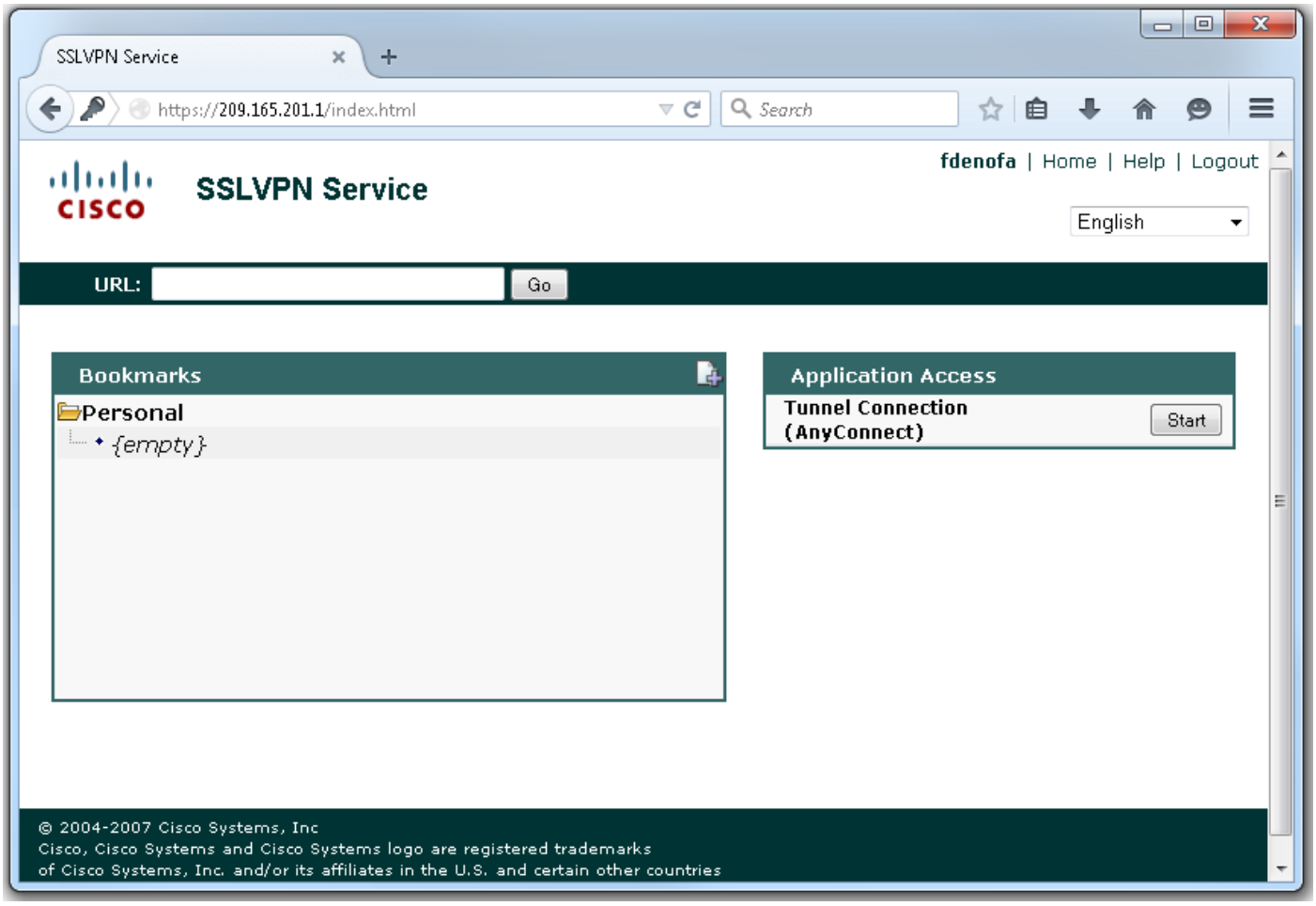
注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

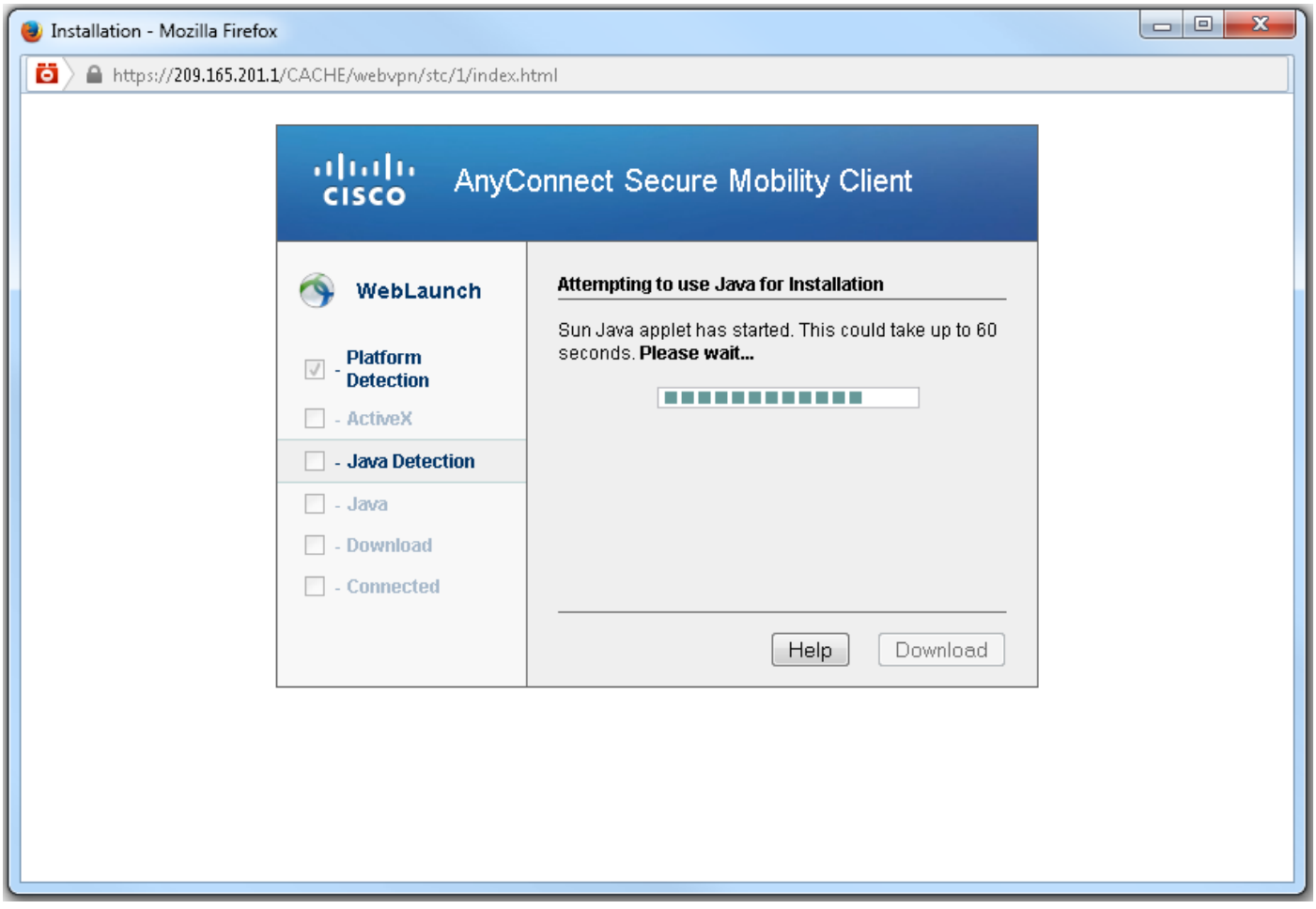
验证

一旦配置完成，当您通过浏览器访问网关地址和端口，将回到WebVPN飞溅页。



在您登陆后，WebVPN主页显示。从这里，请点击**隧道连接(AnyConnect)。** 当使用时Internet Explorer，ActiveX使用增加和安装AnyConnect客户端。如果它没有检测，将使用Java。其他浏览器立即使用Java。

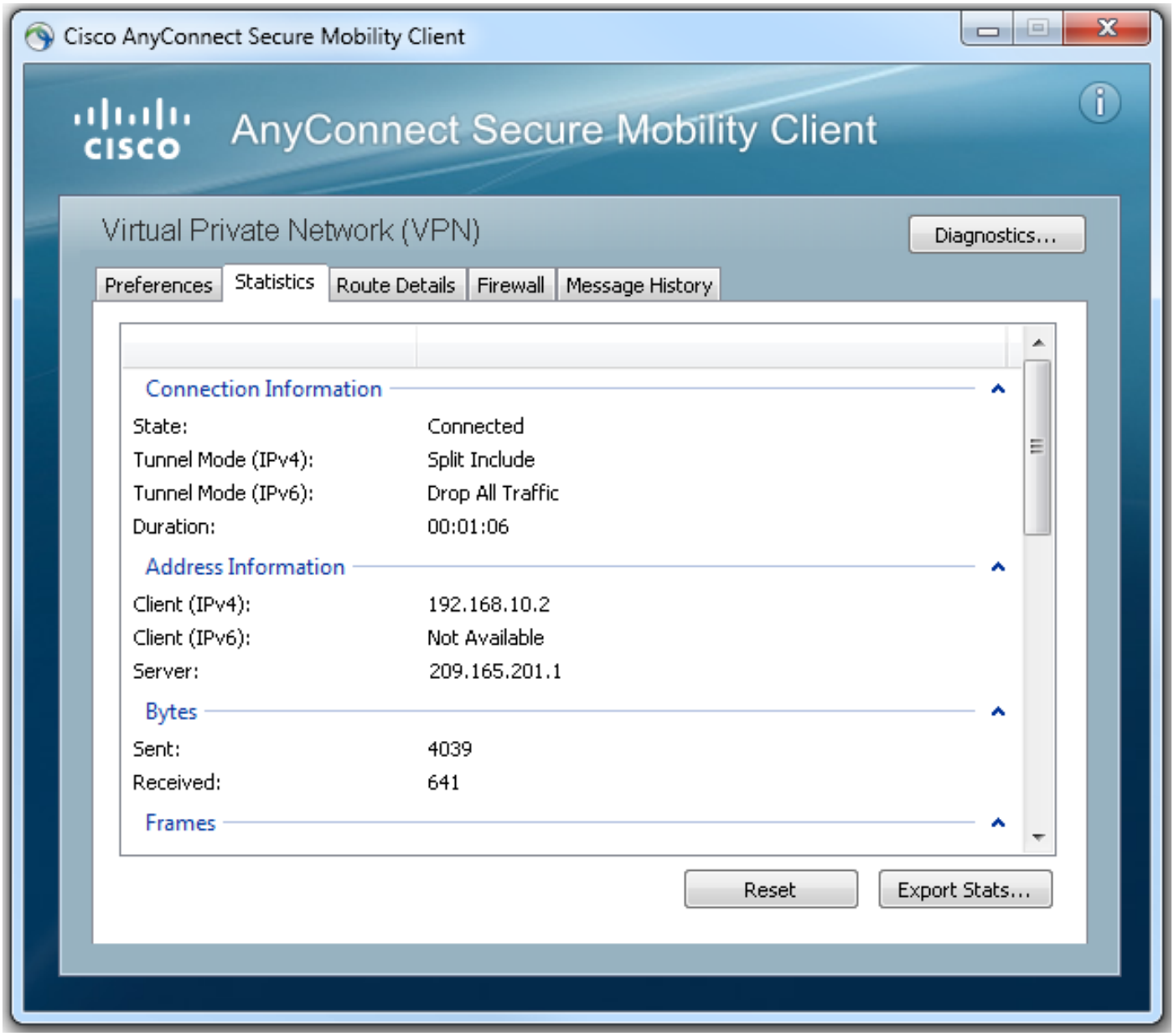


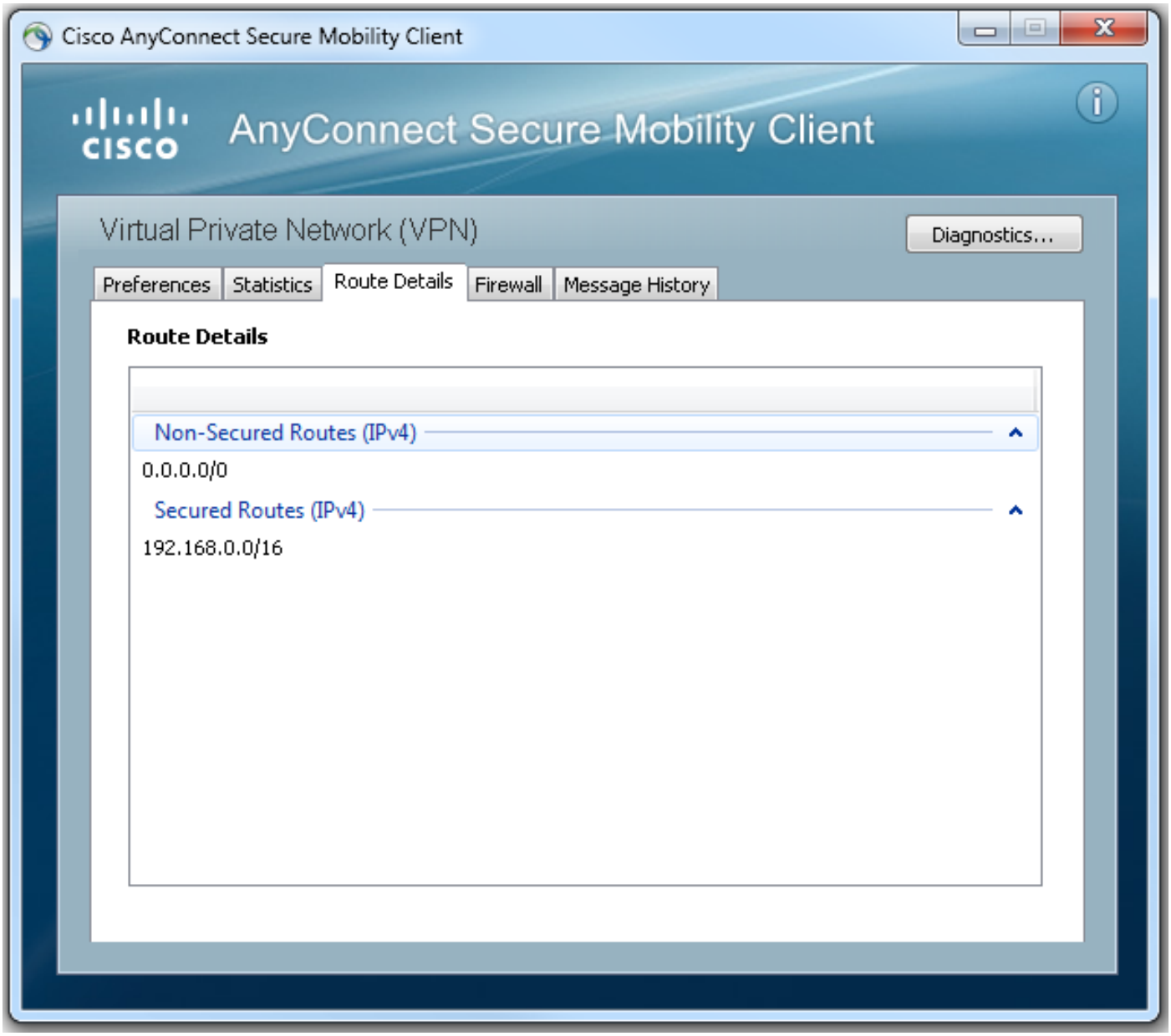


一旦安装完成， AnyConnect将自动地尝试连接到Webvpn gateway。因为自签名证书用于网关识别，在连接尝试期间，多份证书警告将出现。这些预计并且必须接受为了连接能继续。要避免这些证

书警告，在客户端机器的信任证书存储必须安装被提交的自签名证书，或者，如果一第三方证书是然后使用的认证机关证书必须在信任证书存储。

当连接完成协商时，请点击在AnyConnect左下的**齿轮**图标将显示关于连接的若干预先信息。在此页查看从分割隧道ACL和路由详细信息获得的一些连接统计在组策略配置里是可能的。


Cisco AnyConnect Secure Mobility Client
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: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



这是从配置步骤的最终running-configuration结果：

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

故障排除

当您排除故障AnyConnect连接问题时，有检查的一些个普通的组件：

- 客户端必须提交证书，它是证书在Webvpn gateway指定有效的要求。要发行**显示crypto pki证书将**显示适合于对在路由器的所有证书的信息。
- 每当变化做出对WebVPN配置，它是最佳实践发出没有在职和在职在网关和上下文。这将保证

更改适当地生效。

- 如前面提到，它是需求有将连接到此网关的每个客户端操作系统的一AnyConnect PKG。例如，Windows客户端需要Windows PKG，32位客户端需要Linux 32位PKG的Linux，等等。
- 当您考虑AnyConnect客户端时，并且基于浏览器的WebVPN使用SSL，能访问WebVPN飞溅页通常表明AnyConnect能连接(假设，有关AnyConnect配置正确)。

Cisco IOS提供可以用于排除故障失败连接的一些多种调试WebVPN选项。这是从调试WebVPN aaa，调试wevpn通道和show webvpn session生成的输出在成功的连接尝试：

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

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