在IOS路由器上有CCP的AnyConnect VPN (SSL)客户端配置示例

目录

简介

本文描述如何设置Cisco IOS路由器执行在忠心于的安全套接字协议层(SSL) VPN使用Cisco Configuration Professional (CCP)的Cisco AnyConnect VPN客户。此设置适用于在路由器的AnyConnect配置与分割隧道的一个特定案件，并且允许对公司资源的客户端安全访问并且提供不安全的访问给互联网。

多数路由器平台支持SSL VPN或WebVPN技术例如集成业务路由器(ISR)生成1，生成2 (ISR产品列表的参考的ISR产品)。客户被劝告参考功能导航指南为了得到支持AnyConnect VPN Cisco IOS平台的完整列表(SSL)客户端(或任何其它功能技术就此而言)。此信息是可用的在功能导航。

CCP是允许您配置基于Cisco IOS的接入路由器的一个基于GUI的设备管理管理工具。CCP在PC安装并且通过基于GUI的，易用向导简单化路由器、安全、统一通信、无线、广域网和基本LAN配置

。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 适当的客户端操作系统。参考支持的操作系统的AnyConnect版本注释。
- 与SUN JRE版本1.4或以上的Web浏览器或者ActiveX控制浏览器
- 客户端的本地管理权限
- 安装了高级安全镜像 12.4(20)T 或更高版本的 Cisco IOS 路由器
- Cisco Configuration Professional版本1.3或以上

如果Cisco Configuration Professional在您的计算机已经没有装载，您能得到软件的赠送阅本和从软件下载安装.exe (cisco-config-pro-k9-pkg-2_8-en.zip)文件。有关 CCP 安装和配置的详细信息，请参阅"Cisco Configuration Professional 快速入门指南"。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS有软件版本的15.1(4)M8系列CISCO2811路由器
- CCP版本2.8
- 思科AnyConnect Windows的3.1.05160 SSL VPN客户端版本

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图

本文档使用以下网络设置：

配置前的任务

1. 配置CCP的路由器。

有适当的安全套件许可证的路由器已经安排CCP应用程序装载在闪存。参考的Cisco Configuration Professional快速入门指南为了得到和配置软件。

2. 将 Anyconnect VPN .pkg 文件副本下载至管理 PC。

配置

在此部分，您提交以必要步骤为了配置在本文描述的功能。此配置示例使用CCP向导为了启用Anyconnect VPN的操作在IOS路由器的。

要在 Cisco IOS 路由器上配置 Anyconnect VPN，完成以下步骤：

1. 设置CCP并且发现Cisco IOS路由器。
2. 安装并且启用在Cisco IOS路由器的Anyconnect VPN软件。
3. 配置SSL VPN上下文和SSL VPN网关用CCP向导。
4. 配置Anyconnect VPN用户的用户数据库。
5. 配置AnyConnect全通道。

这些步骤中的每一个在本文的以下部分较详细地描述。

步骤 1：设置CCP并且发现Cisco IOS路由器

1. 点击在CCP窗口的**路由器状态**为了查看路由器设备信息。

2. 单击**配置**为了开始配置。

步骤 2：安装并且启用在IOS路由器的Anyconnect VPN软件

完成这些步骤为了安装和启用在IOS路由器的Anyconnect VPN软件：

1. 打开CCP应用程序，导航**配置> Security**和然后单击**VPN**。
2. 展开 **SSLVPN**，并选择 **Packages**。

保证SSL VPN功能许可证在设备安装，否则您也许获得在前一个镜像显示的警告。参考的功能许可证链路为了查看订购信息信息部分。

3. 在 Cisco SSL VPN 客户端软件中，单击 **Browse**。

   此时将显示 Select SVC location 对话框。

4. 指定Cisco AnyConnect VPN客户镜像的位置(请选择两选项联机之一)。

   如果Cisco AnyConnect VPN客户镜像在路由器闪存，请点击**路由器文件系统**单选按钮对话框，并且单击**浏览。**

   如果Cisco AnyConnect VPN客户镜像不在路由器闪存，请点击**我的计算机**无线电对话框，并且单击**浏览**。

5. 选择您希望安装和点击OK键的客户端镜像。

6. 指定客户端镜像的位置后，单击 **Install**。

7. 点击**是**然后点击OK键。

8. 一旦客户端镜像顺利地安装，您收到成功消息。单击 **OK** 以继续。

9. 一旦安装，请查看安装的程序包详细信息在**安全> VPN > SSL下VPN >包**。

步骤 3：配置一个SSLVPN上下文和SSLVPN网关用CCP向导

完成这些步骤为了配置SSL VPN上下文和SSL VPN网关：

1. 选择 **Configure > Security > VPN**，然后单击 **SSL VPN**。

2. 点击**SSL VPN管理器**然后单击**创建SSL VPN选项**。

3. 跟随提示符为了启用认证、授权和核算(AAA)，如果已经没有启用。

4. 检查**创建一个新的SSL VPN**单选按钮然后单击**启动选定的任务**。

   此时将出现 SSL VPN Wizard 对话框。

5. 单击 **Next**。

   注意：如果SSL VPN配置在思科CP被调用的接口下，也许导致思科CP从路由器的disconnet。当一更加好的实践，您能通过从内部接口(在本例中， 10.106.44.141)或其他接口的CCP访问Cisco IOS路由器，而SSL VPN配置在外部接口FastEthernet0/0下(在本例中，10.105.130.149)。

6. 输入新的SSL VPN网关的IP地址并且输入一唯一的名称对于此SSL VPN上下文。

   您可以为同一个 IP 地址（SSL VPN 网关）创建不同的 SSL VPN 上下文，但每个名称都必须唯一。本示例使用以下 IP 地址： **https://10.105.130.149/**

7. 单击**其次**，并且继续对下一部分。

步骤 4：配置 Anyconnect VPN 用户的用户数据库

您可以使用 AAA 服务器、本地用户或同时使用两者进行身份验证。此配置示例使用本地创建的用户验证。

要配置 Anyconnect VPN 用户的用户数据库，完成以下步骤：

1. 在您完成步骤3后，请点击在SSL VPN向导用户认证对话框查找的**本地此路由器**单选按钮。

   可以使用此对话框向本地数据库添加用户。

2. 单击**添加**并且输入用户信息。

3. 点击OK键并且如所需要添加另外的用户。

4. 在您添加必要的用户后，**其次请**单击，并且继续对下一部分。

步骤5.配置Anyconnect通道

完成这些步骤为了配置IP地址的Anyconnect通道和池用户的：

1. 由于Anyconnect提供直接访问给企业内部网资源， URL列表不是需要的为了配置。单击 Configure Intranet Websites 对话框中的 **Next** 按钮。

2. 确认 **Enable Full Tunnel** 复选框已勾选。

3. 创建此 SSL VPN 上下文客户端可使用的 IP 地址池。

   地址池必须对应于地址联机和可路由的在您的内联网。

4. 点击椭圆(...)在IP地址旁边请缓冲字段，并且选择**创建一个新的IP池**。

5. 在 Add IP Local Pool 对话框中，输入地址池的名称（例如，*new*），然后单击 **Add**。

6. 在添加IP地址范围对话框中，请输入Anyconnect VPN客户端的地址池范围并且点击OK键。

   注意：在**版本12.4(20)T前**， IP地址池应该是在接口的范围直接地连接对路由器。如果要使用一个不同的池范围，您能创建环回地址关联以您的新池为了满足此要求。

7. 单击 **Ok**。

8. configure提前通道选项，例如分割隧道、分割DNS、浏览器代理设置和域名系统(DNS)和WINDOWS互联网名称服务(WINS)服务器。

   注意：思科建议您配置至少DNS和WINS服务器。

   完成这些步骤为了配置先进的通道选项，例如分割隧道：

   单击 **Advanced Tunnel Options** 按钮。

   点击**DNS和WINS服务器**选项卡并且输入DNS和WINS服务器的主要IP地址。

   点击**分割隧道**选项卡为了配置分割隧道。

   使用同一个接口同时传输安全数据流和非安全数据流的功能称为分割隧道。分割隧道要求明确指定哪个是安全数据流以及该数据流的目标是什么，这样只有指定的数据流进入隧道，而其余数据流则以未加密形式通过公共网络 (Internet) 进行传输。

在示例中，分割隧道配置为了包括流量。

9. 完成必要选项配置后，单击 **Next**。选择适当的SSL VPN隧道接口选项并且**其次**单击。

10. 自定义 SSL VPN 门户页或选择默认值。

    通过 Customize SSL VPN Portal Page 可以自定义向客户显示 SSL VPN 门户页的方式。

11. 完成自定义 SSL VPN 门户页后，单击 **Next**。

12. 单击 **完成**。

13. 单击**传送**为了保存您的配置然后点击OK键。

    SSL VPN向导提交您的命令到路由器。

基本上这些是从CCP传送到路由器的命令：

AAA commands:

```
aaa new-model
aaa authorization exec default local
aaa authentication login default local
line vty 0 4
login authentication default
authorization exec default
exit
```

Remaining commands:

```
aaa authentication login ciscocp_vpn_xauth_ml_1 local
ip local pool IP_Pool 192.168.1.10 192.168.1.15
interface Virtual-Template1
exit
default interface Virtual-Template1
interface Virtual-Template1
no shutdown
ip unnumbered FastEthernet0/0
exit
webvpn gateway gateway_1
ip address 10.105.130.149 port 443
http-redirect port 80
inservice
```

```
ssl trustpoint TP-self-signed-1878971148
exit
webvpn context Test
aaa authentication list ciscocp_vpn_xauth_ml_1
gateway gateway_1
virtual-template 1
max-users 1000
inservice
secondary-color white
title-color #FF9900
text-color black
policy group policy_1
svc split include 10.106.44.0 255.255.255.0
svc keep-client-installed
functions svc-enabled
svc address-pool IP_Pool netmask 255.255.255.255
svc default-domain cisco.com
svc dns-server primary 10.106.44.10
svc wins-server primary 10.106.44.12
exit
default-group-policy policy_1
exit
! IP address / user account command
username user1 privilege 1 secret 0 *********
```

注意：如果收到错误消息， SSL VPN许可证也许不正确。

完成这些步骤为了更正许可问题：

1. 选择 **Configure > Security > VPN**，然后单击 **SSL VPN**。
2. 点击**SSL VPN管理器**然后单击在右边的**编辑SSL VPN选项**。
3. 突出显示您新建立的上下文并且点击**编辑按钮**。
4. 在 Maximum Number of users 字段中，输入许可证允许的正确用户数。
5. 单击 **OK**，然后单击 **Deliver**。

   命令写入到配置文件。

CLI 配置

CCP 创建以下命令行配置：

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
```

```
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
redundancy
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
```

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
  functions svc-enabled
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...

Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

建立 AnyConnect VPN 客户端连接

完成这些步骤为了建立AnyConnect VPN连接用路由器。

> **注意**：添加一个路由器到可信的站点列表Internet Explorer的。有关详细信息，请参考"将安全设备/路由器添加至受信任的站点列表 (IE)"。

1. 输入路由器WebVPN接口的URL或IP地址在您的Web浏览器的在格式如显示。

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
```

```
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
```

```
redundancy
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
```

```
 policy group policy_1
  functions svc-enabled
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...

Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

或者

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
```

```
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
redundancy
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
```

```
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
  functions svc-enabled
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...
```

```
Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

2. 输入您的用户名和密码。

3. 点击**开始**为了首次Anyconnect VPN隧道连接。

   在 SSL VPN 连接建立之前，将会出现以下窗口。

   注意：在您下载Anyconnect VPN前，在您的计算机必须安装ActiveX软件。

4. 成功建立连接后，单击 **Statistics** 选项卡。

   Statistics 选项卡将显示关于 SSL 连接的信息。

   统计信息Details对话框显示详细的连接统计信息，包括隧道状态和模式、连接持续时间，发送和接收的字节数和帧，地址信息，传输信息和Cisco Secure Desktop状态评估状态。通过该选项卡上的 Reset 按钮可重置传输统计数据。**出口统计**按钮允许您导出当前统计信息、接口和路由表到文本文件。AnyConnect 客户端将提示您输入文本文件的名称和位置。默认名称是*A*nyConnect-ExportedStats.txt，并且默认位置在桌面。

5. 检查路由详细信息(根据分割隧道配置)在**路由详细信息选项卡下**。

6. 在Cisco AnyConnect VPN客户对话框中，**请**单击选项卡为了显示Cisco AnyConnect VPN客户版本信息。

验证

使用本部分可确认配置能否正常运行。

命令

> **注意**：命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

有若干 **show** 命令与 WebVPN 关联。您能执行这些at命令CLI为了show statistics和其他信息。有关 **show** 命令的详细信息，请参阅验证 WebVPN 配置。

显示webvnp会话上下文全部

```
Router#show webvpn session context all
WebVPN context name: Test
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.106.42.10                1         00:01:22  00:00:01
```

show webvpn session用户user1上下文测验

```
Router#show webvpn session user user1 context Test detail
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.05160

Username          : user1                 Num Connection : 1
Public IP         : 10.106.42.10          VRF Name       : None
Context           : Test                  Policy Group   : policy_1
Last-Used         : 00:00:00              Created        : *06:33:24.505 UTC Sat
Nov 29 2014
Session Timeout   : Disabled              Idle Timeout   : 2100
DNS primary serve : 10.106.44.10          WINS primary s : 10.106.44.12
DPD GW Timeout    : 300                   DPD CL Timeout : 300
Address Pool      : IP_Pool               MTU Size       : 1199
Rekey Time        : 3600                  Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.1.10          Netmask        : 255.255.255.255
Rx IP Packets     : 0                     Tx IP Packets  : 617
CSTP Started      : 00:01:22              Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                     Virtual Access : 2
Msie-ProxyServer  : None                  Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 10.106.44.0 255.255.255.0
Client Ports      : 60304

Detail Session Statistics for User:: user1
-----------------------------------

CSTP Statistics::
Rx CSTP Frames    : 618                   Tx CSTP Frames   : 0
Rx CSTP Bytes     : 46113                 Tx CSTP Bytes    : 0
Rx CSTP Data Fr   : 617                   Tx CSTP Data Fr  : 0
Rx CSTP CNTL Fr   : 1                     Tx CSTP CNTL Fr  : 0
Rx CSTP DPD Req   : 0                     Tx CSTP DPD Req  : 0
Rx CSTP DPD Res   : 0                     Tx CSTP DPD Res  : 0
Rx Addr Renew Req : 0                     Tx Address Renew : 0
Rx CDTP Frames    : 0                     Tx CDTP Frames   : 0
Rx CDTP Bytes     : 0                     Tx CDTP Bytes    : 0
Rx CDTP Data Fr   : 0                     Tx CDTP Data Fr  : 0
Rx CDTP CNTL Fr   : 0                     Tx CDTP CNTL Fr  : 0
Rx CDTP DPD Req   : 0                     Tx CSTP DPD Req  : 0
```

```
Rx CDTP DPD Res   : 0                 Tx CDTP DPD Res  : 0
Rx IP Packets     : 0                 Tx IP Packets    : 617
Rx IP Bytes       : 0                 Tx IP Bytes      : 41122

CEF Statistics::
Rx CSTP Data Fr   : 0                 Tx CSTP Data Fr  : 0
Rx CSTP Bytes     : 0                 Tx CSTP Bytes    : 0
```

show webvpn stats

```
Router#show webvpn stats
User session statistics:
   Active user sessions     : 1          AAA pending reqs         : 0
   Peak user sessions       : 1          Peak time                : 00:02:29
   Active user TCP conns    : 1          Terminated user sessions : 0
   Session alloc failures   : 0          Authentication failures  : 0
   VPN session timeout      : 0          VPN idle timeout         : 0
   User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 57         Server process rcvd pkts : 0
   Client process sent pkts : 8134       Server process sent pkts : 0
   Client CEF received pkts : 664        Server CEF received pkts : 0
   Client CEF rcv punt pkts : 29         Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 0          Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 0          Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0          SSLVPN eng  bufs inuse   : 0
   Active server TCP conns  : 0

Mangling statistics:
   Relative urls            : 0          Absolute urls            : 0
   Non-http(s) absolute urls: 0          Non-standard path urls   : 0
   Interesting tags         : 0          Uninteresting tags       : 0
   Interesting attributes   : 0          Uninteresting attributes : 0
   Embedded script statement: 0          Embedded style statement : 0
   Inline scripts           : 0          Inline styles            : 0
   HTML comments            : 0          HTTP/1.0 requests        : 0
   HTTP/1.1 requests        : 3          Unknown HTTP version     : 0
   GET requests             : 3          POST requests            : 0
   CONNECT requests         : 0          Other request methods    : 0
   Through requests         : 0          Gateway requests         : 3
   Pipelined requests       : 0          Req with header size >1K : 0
   Processed req hdr bytes  : 844        Processed req body bytes : 0
   HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
   HTML responses           : 0          CSS responses            : 0
   XML responses            : 0          JS responses             : 0
   Other content type resp  : 0          Chunked encoding resp    : 0
   Resp with encoded content: 0          Resp with content length : 0
   Close after response     : 0          Resp with header size >1K: 0
   Processed resp hdr size  : 0          Processed resp body bytes: 0
   Backend https response   : 0          Chunked encoding requests: 0

HTTP Authentication stats :
   Successful NTLM Auth     : 0          Failed NTLM Auth         : 0
   Successful Basic Auth    : 0          Failed Basic Auth        : 0
   Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
   NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
   Oversize NTLM Type3 cred : 0          Internal Error           : 0
   Num 401 responses        : 0          Num non-401 responses    : 0
   Num Basic forms served   : 0          Num NTLM forms served    : 0
   Num Basic Auth sent      : 0          Num NTLM Auth sent       : 0
```

```
CIFS statistics:
 SMB related Per Context:
   TCP VC's                 : 0          UDP VC's                 : 0
   Active VC's              : 0          Active Contexts          : 0
   Aborted Conns            : 0
 NetBIOS related Per Context:
   Name Queries             : 0          Name Replies             : 0
   NB DGM Requests          : 0          NB DGM Replies           : 0
   NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
 SMB related Global:
   Sessions in use          : 0          Mbufs in use             : 0
   Mbuf Chains in use       : 0          Active VC's              : 0
   Active Contexts          : 0          Browse Errors            : 0
   Empty Browser List       : 0          NetServEnum Errors       : 0
   Empty Server List        : 0          NBNS Config Errors       : 0
   NetShareEnum Errors      : 0
 HTTP related Per Context:
   Requests                 : 0          Request Bytes RX         : 0
   Request Packets RX       : 0          Response Bytes TX        : 0
   Response Packets TX      : 0          Active Connections       : 0
   Active CIFS context      : 0          Requests Dropped         : 0
 HTTP related Global:
   Server User data         : 0          CIFS User data           : 0
   Net Handles              : 0          Active CIFS context      : 0
   Authentication Fails     : 0          Operations Aborted       : 0
   Timers Expired           : 0          Pending Close            : 0
   Net Handles Pending SMB  : 0          File Open Fails          : 0
   Browse Network Ops       : 0          Browse Network Fails     : 0
   Browse Domain Ops        : 0          Browse Domain Fails      : 0
   Browse Server Ops        : 0          Browse Server Fails      : 0
   Browse Share Ops         : 0          Browse Share Fails       : 0
   Browse Dir Ops           : 0          Browse Network Fails     : 0
   File Read Ops            : 0          File Read Fails          : 0
   File Write Ops           : 0          File Write Fails         : 0
   Folder Create Ops        : 0          Folder Create Fails      : 0
   File Delete Ops          : 0          File Delete Fails        : 0
   File Rename Ops          : 0          File Rename Fails        : 0
   URL List Access OK       : 0          URL List Access Fails    : 0

Socket statistics:
   Sockets in use           : 1          Sock Usr Blocks in use   : 1
   Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
   Select timers in use     : 1          Sock Select Timeouts     : 0
   Sock Tx Blocked          : 150        Sock Tx Unblocked        : 150
   Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
   Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
   Sock Premature Close     : 0          Sock Pipe Errors         : 13
   Sock Select Timeout Errs : 0

Smart Tunnel statistics:
 Client                              Server
   proc pkts                : 0        proc pkts                : 0
   proc bytes               : 0        proc bytes               : 0
   cef  pkts                : 0        cef  pkts                : 0
   cef  bytes               : 0        cef  bytes               : 0

Port Forward statistics:
 Client                              Server
   proc pkts                : 0        proc pkts                : 0
   proc bytes               : 0        proc bytes               : 0
   cef pkts                 : 0        cef pkts                 : 0
   cef bytes                : 0        cef bytes                : 0

WEBVPN Citrix statistics:
```

```
              Server                    Client
 Packets in   : 0                        0
 Packets out  : 0                        0
 Bytes in     : 0                        0
 Bytes out    : 0                        0

ACL statistics:
   Permit web request       : 0          Deny web request         : 0
   Permit cifs request      : 0          Deny cifs request        : 0
   Permit without ACL       : 0          Deny without match ACL   : 0
   Permit with match ACL    : 0          Deny with match ACL      : 0

Single Sign On statistics:
   Auth Requests            : 0          Pending Auth Requests    : 0
   Successful Requests      : 0          Failed Requests          : 0
   Retranmissions           : 0          DNS Errors               : 0
   Connection Errors        : 0          Request Timeouts         : 0
   Unknown Responses        : 0

URL-rewrite splitter statistics:
   Direct access request    : 0          Redirect request         : 0
   Internal request         : 0

Tunnel Statistics:
   Active connections       : 1
   Peak connections         : 1          Peak time                : 00:01:44
   Connect succeed          : 2          Connect failed           : 0
   Reconnect succeed        : 1          Reconnect failed         : 0
   DPD timeout              : 0
 Client
   in  CSTP frames          : 671        in  CSTP control         : 1
   in  CSTP data            : 670        in  CSTP bytes           : 50002
   out CSTP frames          : 0          out CSTP control         : 0
   out CSTP data            : 0          out CSTP bytes           : 0
   in  CDTP frames          : 0          in  CDTP control         : 0
   in  CDTP data            : 0          in  CDTP bytes           : 0
   out CDTP frames          : 0          out CDTP control         : 0
   out CDTP data            : 0          out CDTP bytes           : 0
   cef in  CSTP data frames : 0          cef in  CSTP data bytes  : 0
   cef out CSTP data frames : 0          cef out CSTP data bytes  : 0
   cef in  CDTP data frames : 0          cef in  CDTP data bytes  : 0
   cef out CDTP data frames : 0          cef out CDTP data bytes  : 0
 Server
   In  IP pkts              : 0          In  IP bytes             : 0
   Out IP pkts              : 670        Out IP bytes             : 44587
```

在CCP中，请选择**Monitoring>安全> VPN状态> SSL VPN (所有上下文)**为了查看在路由器的当前SSL VPN用户列表。

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。

故障排除命令

有若干 **clear** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅“使用 WebVPN Clear 命令”。

有若干 **debug** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

> **注意**：使用 **debug** 命令可能会对 Cisco 设备造成负面影响。使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- Cisco IOS SSLVPN
- AnyConnect VPN 客户端常见问题
- Cisco AnyConnect VPN客户管理员指南
- SSL VPN - WebVPN
- 有 SDM 的 Cisco IOS 的无客户端 SSL VPN (WebVPN) 配置示例
- 使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例
- WebVPN 和 DMVPN 融合部署指南
- 技术支持和文档 - Cisco Systems