配置AnyConnect有分割隧道的安全移动性客户端在ASA

目录

简介

本文描述如何通过Cisco Adaptive Security Device Manager (ASDM)配置Cisco AnyConnect安全移动客户端Cisco可适应安全工具的(ASA)该运行软件版本9.3(2)。

先决条件

要求

应该下载Cisco AnyConnect安全移动客户端Web部署包到对ASA的ASDM访问是存在的本地桌面。为了下载客户端包，参考Cisco AnyConnect安全移动客户端网页。多种操作系统的(Oss) Web部署包可以同时上传到ASA。

这些是Web部署文件名对于多种Oss ：

- **Microsoft Windows Oss** âÂ Â *AnyConnect-win-<version>-k9.pkg*
- **麦金塔(MAC) Oss** âÂ Â *AnyConnect-macosx-i386-<version>-k9.pkg*
- **Linux Oss** âÂ Â *AnyConnect-linux-<version>-k9.pkg*

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA版本9.3(2)
- ASDM版本7.3(1)101
- AnyConnect版本3.1

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。

背景信息

本文提供关于如何的逐步细节通过ASDM使用思科AnyConnect配置向导为了配置AnyConnect客户端和enable (event)分割隧道。

分割隧道用于仅特定的流量必须建立隧道的方案，被反对方案所有在VPN间的客户端机器产生的通信流，当连接。默认情况下使用AnyConnect配置向导将导致在ASA的通道*所有*配置。必须分开配置分割隧道，在本文的分割隧道部分的更详细的资料解释。

在本例中配置示例，目的将发送10.10.10.0/24子网的流量，是在ASA后的LAN子网，在VPN通道，并且从客户端机器的其他流量通过其自己的互联网电路转发。

AnyConnect许可证信息

这是一些链路对关于Cisco AnyConnect安全移动客户端许可证的有用的信息：

- 参考AnyConnect安全移动性客户端特性、许可证和Oss，版本3.1文档为了确定为AnyConnect安全移动性客户端和相关功能要求的许可证。
- 参考思科AnyConnect订购指南关于AnyConnect尖顶的信息和加上许可证。
- 参考什么ASA许可证为IP电话和移动VPN连接是需要的？关于另外的许可证需求的信息文档IP电话和移动连接的。

配置

此部分描述如何配置ASA的Cisco AnyConnect安全移动客户端。

Note:请使用命令查找工具(仅限注册用户)为了得到关于在此部分使用的命令的更多信息。

网络图

这是使用示例在本文的拓扑：

ASDM AnyConnect配置向导

AnyConnect配置向导可以使用为了配置AnyConnect安全移动性客户端。保证AnyConnect客户端包上传到ASA防火墙的闪存/磁盘，在您继续前。

完成这些步骤为了通过配置向导配置AnyConnect安全移动性客户端：

1. 登录ASDM，启动**配置向导**，并且**其次**单击：

2. 输入*连接配置文件名称*，选择VPN从*VPN访问接口*下拉菜单将终止的接口，并且**其次**单击：

3. 检查**SSL**复选框为了启用安全套接字协议层(SSL)。*设备证书*可以是委托第三方Certificate Authority (CA)已签发证书(例如Verisign或者Entrust)，或者自签名证书。如果证书在ASA已经安装，则可以通过下拉菜单选择。**Note**:此证书是将提供的服务器端认证。如果没有在ASA当前安装的证书，并且必须生成自签名证书，则请单击**管理**。为了安装一第三方证书，请完成在ASA 8.x描述手工安装第三方供应商证书为了用在WebVPN配置示例Cisco文档上的步骤。

4. 单击**添加**：

5. 键入适当的名称到*信任点Name字段*，并且点击**添加一个新的身份证书**单选按钮。如果没有Rivest沙米尔Addleman (RSA)密钥对在设备，请单击**新**为了生成一：

6. 点击**使用DEFAULT键对名称**单选按钮或者点击**回车新密钥对名称**单选按钮并且输入新名字。选择密钥的大小，然后单击**生成现在:**

7. 在RSA密钥对生成后，请选择密钥并且检查**生成自签名证书**复选框。输入希望的附属的域名

(DN)到*证书主题DN*字段，然后单击**添加证书**：

8. 一旦登记完成，**其次请**点击OK键， **OK**，然后：

9. 单击**添加**为了添加AnyConnect客户端镜像(*.pkg*文件)从PC或从闪存。单击**浏览闪存**为了从闪存驱动器添加镜像或者点击**加载**为了从主机直接地添加镜像：

10. 一旦镜像被添加，**其次请**单击：

11. 用户认证可以通过验证、授权和统计(AAA)服务器组完成。如果用户已经配置，则请选择**本地并且其次**单击。 **Note**:在本例中，**本地认证**配置，因此意味着在ASA的本地用户数据库将使用验证。

12. VPN客户端的地址池必须配置。如果一个人已经配置，则请从下拉菜单选择它。否则，请单击**新**为了配置新的。一旦完整，**其次请**单击：

13. 输入域名系统(DNS)服务器和Dns到*DNS*和*域名字段*适当地，**其次**然后单击：

14. 在此方案中，目标将限制在VPN的访问对配置的**10.10.10.0/24**网络，因为在ASA后的*里面*(或LAN)子网。客户端和里面子网之间的流量一定是豁免从所有动态网络地址转换(NAT)。

    检查**从网络地址转换**复选框的**豁免VPN流量**并且配置将使用免税的LAN和广域网接口：

15. 选择一定豁免的本地网络：

16. 单击**其次**，**其次**，然后**完成**。

AnyConnect客户端配置当前完成。然而，当您通过配置向导时配置AnyConnect，默认情况下它配置*分割隧道*策略作为**Tunnelall**。为了建立隧道仅特定的流量，必须实现*分割隧道*。

Note:如果切分通道没有配置，分割隧道策略从默认策略(DfltGrpPolicy)将被继承，默认情况下设置为**Tunnelall。**这意味着，一旦客户端在VPN连接，所有流量(包括流量到Web)在通道发送。

被注定对ASA广域网仅的流量(或*外部*) IP地址将绕过在客户端机器的隧道。这在输出能被看到**route print命令中**在Microsoft Windows机器。

分割隧道配置

分割隧道是您能使用为了定义子网或主机的流量必须加密的功能。这介入将关联与此功能访问控制表(ACL)的配置。在此ACL定义子网或主机的流量在从客户端的通道和这些子网的路由在PC路由表将加密安装。

完成这些步骤为了从通道*所有*配置移动向*独立的隧道*配置：

1. 导航对**Configuration>远程访问VPN >组策略**：

2. 单击**编辑**，并且使用导航结构树为了导航到**先进>分割隧道。**非选定在*策略部分的***继承**复选框，并且从下拉菜单选择**如下隧道网络列表**：

3. 非选定在指定LAN网络客户端需要访问的*网络列表*部分的**继承**复选框，并且单击**设法**为了选择ACL ：

4. 点击**标准ACL**，**添加**，**添加ACL**然后**ACL名称**：

5. 单击**添加ACE**为了增加规则：

6. 单击 **Ok。**

7. 单击 **Apply。**

一旦连接，子网的在已分解ACL的路由或主机被添加到客户端机器的路由表。在Microsoft Windows机器上，这在输出可以查看**route print命令中。**这些路由的下一跳将是从客户端IP池子网(通常第一个IP地址的一个IP地址子网) ：

```
C:\Users\admin>route print
```

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0      255.255.255.0    10.10.11.2  10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1    255.255.255.255     On-link    10.106.44.243  6

!! This is the route for the ASA Public IP Address.
```

在MAC OS机器上，请输入**r命令的netstat -**为了查看PC路由表：

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

下载并且安装AnyConnect客户端

有您能使用为了部署用户计算机的Cisco AnyConnect安全移动客户端的两个方法：

- Web部署
- 独立部署

这两个方法在跟随的部分较详细地解释。

Web部署

为了使用Web部署方法，请输入**https:// <ASA FQDN>or<ASA IP>** URL到在客户端机器的一个浏览器，给*WebVPN*入口页面带来您。

> **Note**:如果使用Internet Explorer (IE)，安装主要通过ActiveX完成，除非被迫使使用Java。其他浏览器使用Java。

一旦登录页，安装在客户端机器应该开始，并且客户端应该连接到ASA，在安装完成后。

> **Note**:也许提示对于权限运行ActiveX或Java。必须允许这为了继续进行安装。

独立部署

完成这些步骤为了使用独立部署方法：

1. 下载从Cisco网站的AnyConnect客户端镜像。为了选择下载的正确镜像，参考Cisco AnyConnect安全移动客户端网页。下载链路在此页提供。 导航对下载页并且选择适当的版本。 执行**全双工安装包的**一搜索**-窗口/独立安装程序(ISO)**。**Note**:ISO安装程序镜像然后下载(例如*anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。
2. 请使用*WinRar*或*7 ZIP*为了解压缩ISO包的内容：

3. 一旦内容解压缩，请运行**Setup.exe文件**并且选择必须与Cisco AnyConnect安全移动客户端一起安装的模块。

   提示：*使用CLI，8.4和8.6*，为了配置VPN的另外的设置，请参考*Cisco ASA 5500系列配置指南的*配置的AnyConnect VPN客户端连接部分。

CLI 配置

此部分为参考目的Cisco AnyConnect安全移动客户端提供CLI配置。

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!**********Split ACL configuration**********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
```

```
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration ****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate***********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
```

```
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
```

```
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

验证

完成关联对该连接的这些步骤为了验证客户端连接和多种参数：

1. 导航对在ASDM的**Monitoring> VPN** ：

2. 您能**由**选项使用**过滤器**为了过滤VPN种类。选择从下拉菜单和所有的**AnyConnect客户端** AnyConnect客户端会话。**提示**：会话可以进一步过滤与其他标准，例如*用户名*和*IP地址*。

3. 双击会话为了得到关于该特定的会话的更详细的资料：

4. 输入**显示vpn-sessiondb anyconnect**命令到CLI为了得到会话详细信息：

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. 您能使用其他过滤器选项为了完善结果：

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

故障排除

您能使用AnyConnect诊断和报告工具(箭)为了收集为排除故障AnyConnect安装和连接问题是有用的数据。 箭向导在运行AnyConnect的计算机使用。箭在客户端机器装配日志、状态和诊断信息Cisco技术支持中心(TAC)分析的，并且不要求管理员权限运行。

安装箭

完成这些步骤为了安装箭：

1. 下载从Cisco网站的AnyConnect客户端镜像。为了选择下载的正确镜像，参考Cisco

AnyConnect安全移动客户端网页。下载链路在此页提供。 导航对下载页并且选择适当的版本。 执行**全双工安装包的**一搜索**-窗口/独立安装程序(ISO)**。**Note**:ISO安装程序镜像然后下载(例如*anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。

2. 请使用*WinRar*或*7 ZIP*为了解压缩ISO包的内容：

3. 浏览到内容解压缩的文件夹。

4. 运行**Setup.exe文件**并且选择仅AnyconnectDiagnostic**和报告工具：**

运行箭

这是要考虑的一些重要信息，在您运行箭前：

- 在您运行箭前，必须至少一次再创问题。
- 当问题被再创时，在用户计算机的日期和时间一定是要注意的。

从在客户端机器的*开始菜单*运行箭：

*默认*或*自定义*模式可以选择。Cisco建议您运行在默认模式的箭，以便所有信息在一次单发射击可以捕获。

一旦完成，工具保存箭套件*.zip*文件到客户端桌面。套件可能然后被发电子邮件给TAC (在您开TAC案例)后进一步分析的。

相关信息

- Cisco AnyConnect安全移动客户端管理员指南，版本3.0 âÂ Â 管理，监控和排除故障AnyConnect塞申斯
- AnyConnect VPN客户端故障排除指南-常见问题
- Java与AnyConnect、CSD/Hostscan和WebVPN的7个问题-故障排除指南
- 技术支持和文档 - Cisco Systems