在无线局域网环境中配置 Cisco VPN 客户端的自动 VPN 初始化

目录

简介

本文描述如何配置Cisco VPN Client自动地首次对Cisco VPN 3000集中器的IPSec VPN连接在一个有线的/无线局域网(WLAN)环境。

在WLAN环境，无线客户端首先关联到无线接入点(AP)。基于IP地址范围它从无线连接接收，在无线安装的VPN客户端自动地启动VPN连接请求到在站点的对应的VPN集中器。IPSec VPN连接然后用于为了巩固无线802.11x流量。没有思科VPN连接的成功的建立，无线客户端不得以进入对网络资源的。

此配置示例显示VPN客户端的配置为了启用自动初始化功能。

先决条件

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

要求

在您尝试此配置前，请保证您熟悉这些概念：

- 知道如何设立和配置Cisco VPN Client和Cisco VPN 3000集中器为了设立IPSec VPN通道
- 了解与无线LAN涉及的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco VPN客户端软件版本4.x
- Cisco VPN 3000集中器版本3.6
- Cisco Aironet 340系列接入点
- Cisco Aironet 350系列无线LAN适配器(版本5.0.1)

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。

注意： 在本例中， Cisco Network Registrar用于，动态主机配置协议(DHCP)服务器为了提供IP地址给无线客户端和VPN客户端。

配置

本部分提供有关如何配置本文档所述功能的信息。

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。

网络图

本文档使用以下网络设置：

注意： 在此设置， SJ DHCP服务器用于为了提供IP地址给无线连接和VPN连接。它安排两个IP地址范围定义：

- 对于无线连接，无线用户收到在范围的一个IP地址从200.1.1.50到200.1.1.250。
- 对于VPN连接， VPN客户端收到在范围的一个IP地址从50.1.1.1到50.1.1.254。

配置

在本例中，根据哪些站点用户漫游到，无线客户端自动地启动二者之一在VPN拨号程序预定义两VPN连接的之一(即SJWireless或RTPWireless)。特别地，如果无线用户有IP地址在200.1.1.0/24范围内从无线关联SJ AP，它启动从VPN拨号程序的SJWireless连接。如果它有IP地址在150.1.1.0/24范围内从无线关联RTP AP，启动从VPN拨号程序的RTPWireless连接。

在此部分， VPN连接是第一配置在VPN拨号程序下，然后vpnclient.ini文件是编辑的添加自动初始化配置。一旦这些步骤在一VPN客户端完成，生成的VPN配置文件(.pcf文件)和已配置的vpnclient.ini可以与VPN客户端镜像一起包，为了分配对最终用户。VPN连接启动是透明对最终用户在VPN客户端安装以后。

VPN拨号程序配置

完成这些配置步骤：

1. 选择Start > Programs > Cisco Systems VPN Client > VPN客户端。单击 **New** 以启动 Create New VPN Connection Entry 窗口。
2. 输入 Connection Entry 的名称与说明。进入VPN集中器的外部IP地址在主机方框的。然后输入 VPN 组名称和口令，并单击 **Save**。
3. 重复步骤1和2为了创建与命名**RTPWireless的**另一VPN连接从思科VPN拨号程序。当第二配置过程完成时，名为SJWireless.pcf和RTPWireless.pcf的两个VPN连接配置文件在客户端PC生成。
4. 完成这些步骤为了编辑在客户端PC找到的默认vpnclient.ini文件为了启用自动初始化功能：启用与**AutoInitiationEnable关键字的**自动初始化功能在[main]部分下。定义**AutoInitiationList**。在列表的每个项目对应于部分， VPN连接和无线IP地址范围名称关联。在本例中， SJWireless VPN连接对应到200.1.1.0/24，并且RTPWireless连接对应到150.1.1.0/24。当步骤a和b完成时，文件vpnclient.ini如下所示:
```
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=3
[LOG.PPP]
LogLevel=2
[LOG.CM]
LogLevel=1
[LOG.IPSEC]
LogLevel=3
[main]
AutoInitiationEnable=1 AutoInitiationRetryInterval=3 AutoInitiationList=SJVPN,RTPVPN
EnableLog=1 [SJVPN] Network=200.1.1.0 Mask=255.255.255.0 ConnectionEntry=SJWireless
[RTPVPN] Network=150.1.1.0 Mask=255.255.255.0 ConnectionEntry=RTPWireless RunAtLogon=0
EnableLog=1 XAuthHandler=ipsxauth.exe IsNoTrayIcon=0 StatefulFirewall=0 [LOG.DIALER]
LogLevel=2 [LOG.IKE] LogLevel=3 [LOG.XAUTH] LogLevel=3 [LOG.CLI] LogLevel=1 [LOG.FIREWALL]
LogLevel=1
```
5. 在步骤1 - 3完成在一VPN客户端后， vpnclient.ini和VPN连接配置文件(.pcf)可以收集和被分配对安装包的最终用户。参考的VPNClient管理员指南，关于如何的版本3.6预先配置远程用户的VPN客户端的信息。

Cisco VPN 3000 集中器配置

完成这些配置步骤：

1. 在VPN 3000集中器上， VPN组需要配置建立与VPN客户端的一个IPSec连接。在示例中，无线用户能连接到根据他们漫游的站点的不同的VPN集中器。这里，在SJ VPN集中器的仅必需的配置任务突出显示。VPN组呼叫**SJVPNusers**，匹配在客户端的VPN组名称，创建。
2. 选择**Configuration > User Management > Groups**并且从当前组列表选择**SJVPNusers**。请选择从Actions选项的**修改组，**如果组已经创建，或者**添加组**然后**修改组，**如果组必须创建。
3. 单击**标识**选项卡。Identity Parameters窗口出现。验证在此窗口显示的信息为您的配置是正确。
4. 点击常规选项卡然后检查**IPSec**方框隧道协议属性。
5. 点击IPSec选项，然后指定IPSec安全关联(SA)和认证方法属性用提供的下拉菜单和复选框。在这种情况下， VPN用户在VPN 3000集中器定义本地，因此认证方法内部。
6. 点击Client Config Tab，然后指定在Client Configuration Parameters窗口的模式配置参数。单击 **Apply**。在这种情况下，从VPN客户端的所有流量加密并且发送到IPSec隧道。这指定在普通的客户端参数下。
7. 选择**Configuration > System > Address Management > Assignment**。从Address Assignment options窗口，请指定与提供的复选框的IP地址分配方法。在这种情况下， VPN客户端从DHCP服务器获得IP地址在IKE协商时，因此Use DHCP选项被检查。单击 **Apply**。

8. 请使用DHCP服务器配置窗口为了设置DHCP服务器参数，并且点击**"Save"**为了保存设置。如被提及，一个DHCP服务器在VPN 3000集中器背后使用无线连接和VPN连接。对于无线连接，集中器担当DHCP中继代理中继DHCP信息在无线AP和DHCP服务器之间。

验证

使用本部分可确认配置能否正常运行。

从 VPN 拨号程序验证自动初始化配置

完成这些步骤为了验证从VPN拨号程序的自动初始化配置：

1. 从在VPN客户端工作站的Cisco VPN Dialer窗口，请点击**选项**并且选择**自动VPN开始**。
2. 在Automatic VPN Initiation窗口，请验证Enable复选框被检查。如果它不是，请检查它。点击ok键关闭窗口为了。

在 WLAN 环境中验证自动初始化功能

完成这些步骤为了验证在WLAN环境的自动初始化功能：

1. 插入无线LAN适配器到PC，并且等待关联对无线AP。为了验证无线关联，开始Aironet Client Utility软件和检查Aironet Client窗口的底部。在图上显示的无线客户端能联合到IP地址是200.1.1.2的无线AP。
2. 一旦无线关联完成， VPN客户端自动地启动根据IP地址的连接接收从无线连接。在这种情况下，无线客户端接收从无线AP的200.1.1.52，并且VPN客户端启动根据在vpnclient.ini的配置的SJWireless连接。一旦VPN连接被建立，客户端能访问网络资源在IPSec VPN安全服务保护下，如显示。

检查 VPN 客户端事件日志

此部分显示如何检查VPN客户端事件登录顺序验证自动初始化适当地继续。

打开Cisco VPN Client日志查看器，并且您看到信息类似于此在自动初始化时。正如你看到的VPN客户端收到从无线关联的200.1.1.52 IP地址，落入在vpnclient.ini定义的200.1.1.0/24网络列表。VPN客户端相应地然后开始SJWireless连接。在IKE协商时， Cisco VPN Client收到50.1.1.8的IP地址。它使用此IP地址作为来源IP访问内部网络在Cisco VPN 3000集中器背后。

```
222 17:26:05.019 11/19/02 Sev=Info/6 CM/0x63100036 autoinitiation condition detected: Local IP
200.1.1.52 Network 200.1.1.0 Mask 255.255.255.0 Connection Entry "SJWireless" 223 17:26:06.071
11/19/02 Sev=Info/6 DIALER/0x63300002 Initiating connection. 224 17:26:06.081 11/19/02
Sev=Info/4 CM/0x63100002 Begin connection process 225 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100004 Establish secure connection using Ethernet 226 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100026 Attempt connection with server "200.1.1.1" 227 17:26:06.091 11/19/02 Sev=Info/6
IKE/0x6300003B Attempting to establish a connection with 200.1.1.1. 228 17:26:06.131 11/19/02
Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
200.1.1.1 229 17:26:06.131 11/19/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 230
17:26:06.281 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 231
17:26:06.281 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID,
HASH, VID, VID, VID, VID, VID) from 200.1.1.1 232 17:26:06.281 11/19/02 Sev=Info/5
IKE/0x63000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 233 17:26:06.281 11/19/02
```

Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 234 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 09002689DFD6B712 235 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 236 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 237 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000001 Peer supports DPD 238 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000 239 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500306 240 17:26:06.301 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 200.1.1.1 241 17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 242 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 243 17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 244 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 245 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 246 17:26:06.321 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 247 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 248 17:26:06.321 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 249 17:26:06.321 11/19/02 Sev=Info/4 CM/0x63100015 Launch xAuth application 250 17:26:10.397 11/19/02 Sev=Info/4 CM/0x63100017 xAuth application returned 251 17:26:10.397 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 252 17:26:10.697 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 253 17:26:10.697 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 254 17:26:10.697 11/19/02 Sev=Info/4 CM/0x6310000E Established Phase 1 SA. 1 Phase 1 SA in the system 255 17:26:10.707 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 256 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 257 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Protection Policy). 258 17:26:11.779 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 259 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 260 17:26:11.809 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 **261 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 50.1.1.8 262 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.100 263 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.101** 264 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 265 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 266 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./ VPN 3000 Concentrator Version 3.6.Rel built by vmurphy on Aug 06 2002 10:41:35 267 17:26:11.819 11/19/02 Sev=Info/4 CM/0x63100019 Mode Config data received 268 17:26:11.839 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 200.1.1.1, GW IP = 200.1.1.1 269 17:26:11.839 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 270 17:26:11.849 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 200.1.1.1 271 17:26:11.849 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 272 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 273 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 274 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 275 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 5 seconds, setting expiry to 86395 seconds from now 276 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 277 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 278 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 279 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 200.1.1.1 280 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA (Message ID = 0xF9D733A7 OUTBOUND SPI = 0x1AD0BBA1 INBOUND SPI = 0xA99C00B3) 281 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x1AD0BBA1 282 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xA99C00B3 283 17:26:11.859 11/19/02 Sev=Info/4 CM/0x6310001A One secure connection established 284 17:26:11.879 11/19/02 Sev=Info/6 DIALER/0x63300003 Connection established. 285 17:26:11.889 11/19/02 Sev=Info/6 DIALER/0x63300008 MAPI32 Information - Outlook not default mail client 286 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 287 17:26:11.929 11/19/02 Sev=Info/4

```
IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME)
from 200.1.1.1 288 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has
value of 28800 seconds 289 17:26:11.929 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP
OAK QM *(HASH) to 200.1.1.1 290 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA
(Message ID = 0x0660AF57 OUTBOUND SPI = 0x5E6E8676 INBOUND SPI = 0xF5EAA827) 291 17:26:11.939
11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x5E6E8676 292 17:26:11.939 11/19/02
Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xF5EAA827 293 17:26:11.939 11/19/02
Sev=Info/4 CM/0x63100022 Additional Phase 2 SA established. 294 17:26:12.891 11/19/02 Sev=Info/4
IPSEC/0x63700014 Deleted all keys 295 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created
a new key structure 296 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0xa1bbd01a into key list 297 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 298 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0xb3009ca9 into key list 299 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 300 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x76866e5e into key list 301 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 302 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x27a8eaf5 into key list 303 17:26:21.904 11/19/02 Sev=Info/6 IKE/0x6300003D Sending DPD
request to 200.1.1.1, seq# = 2877451244 304 17:26:21.904 11/19/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 200.1.1.1
```

验证其它自动初始化状态

参考使用自动关于自动初始化的其他状态的VPN开始前面信息。

相关信息

- VPN 3000系列集中器参考音量我：配置
- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- 技术支持和文档 - Cisco Systems