ASA和本地L2TP-IPSec机器人客户端配置示例

目录

简介

IPSec上第二层隧道协议(L2TP)在单个平台提供功能部署和管理沿着IPSec VPN的一个L2TP VPN解决方案和防火墙服务。IPSec上的L2TP的配置的主要优点在远程访问方案的是远程用户能访问在公共IP网络的VPN，不用网关或专线，启用从实际上所有地方的远程访问有普通旧式电话服务的。其它好处是VPN访问的唯一的客户端请求是使用Windows与Microsoft Dial-Up Networking (DUN)。另外的客户端软件，例如Cisco VPN客户端软件，没有要求。

本文为本地L2TP/IPsec机器人客户端提供一配置示例。它通过在Cisco可适应安全工具(ASA)的所有必要的required命令在机器人设备采取您，以及步骤被采取。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于下列软件和硬件版本：

- 机器人L2TP/IPsec要求Cisco ASA软件版本8.2.5或以上，版本8.3.2.12或以上或者版本8.4.1或以上。
- ASA支持安全散列算法2 (SHA2)证书Microsoft Windows 7和机器人本地VPN客户端的签名支持，当使用时L2TP/IPsec协议。
- 使用CLI， 8.4和8.6，请参阅Cisco ASA 5500系列配置指南：配置IPSec上的L2TP ：IPSec上的L2TP的许可权要求。

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

此部分描述信息一将需要为了配置在本文描述的功能。

配置在机器人的L2TP/IPsec连接

此步骤描述如何配置在机器人的L2TP/IPsec连接：

1. 打开菜单，并且选择**设置**。
2. 选择**无线和网络**或者**无线控制**。可用的选项取决于机器人您的版本。
3. 选择**VPN设置**。
4. 选择**添加VPN**。
5. 选择**添加L2TP/IPsec PSK VPN**。
6. 选择**VPN命名**，并且输入描述性名称。
7. 选择**集合VPN服务器**，并且输入描述性名称。
8. 选择**集合IPSec预先共享密钥**。
9. 不选定**Enable (event) L2TP机密**。
10. [Optional]设置IPSec标识符作为ASA隧道组组名。设置不意味将落入在ASA的DefaultRAGroup。
11. 打开菜单，并且选择**保存**。

配置在ASA的L2TP/IPsec连接

这些是需要的ASA互联网密钥交换版本1 (IKEv1) (Internet安全连接和密钥管理协议[ISAKMP])允许本地VPN客户端的策略设置，集成用在终端的操作系统，建立对ASA的VPN联系，当使用IPSec上的L2TP协议：

- IKEv1相位1 -与SHA1哈希方法的三重数据加密标准(3DES)加密
- IPSec阶段2 - 3DES或高级加密标准(AES)加密与消息摘要5 (MD5)或SHA哈希方法
- PPP authentication password认证协议(PAP)，微软询问握手认证协议版本1 (MS-CHAPv1)，或者MS-CHAPv2 (首选)
- 预共享密钥

  注意：ASA支持PPP认证仅PAP和MS-CHAP (版本1和2)在本地数据库。可扩展的认证协议(EAP)和CHAP由代理验证服务器执行。所以，如果远程用户属于用**验证EAP代理**或**验证chap**命令配置的隧道组，并且，如果ASA配置使用本地数据库，该用户无法连接。

  此外，机器人不支持PAP，并且，因为轻量级目录访问协议(LDAP)不支持MS-CHAP，

LDAP不是一个可行的认证机制。唯一的应急方案是使用RADIUS。请参阅在IPSec连接失效的Cisco Bug ID CSCtw58945 ， "L2TP与ldap授权和mschapv2,"关于在问题的更详细的资料与MS-CHAP和LDAP。

此步骤描述如何配置在ASA的L2TP/IPsec连接：

1. 定义本地地址池或请使用DHCP服务器可适应安全工具为了分配IP地址到组策略的客户端。
2. 创建一内部组政策。 定义隧道协议是l2tp-ipsec。配置客户端(DNS)将使用的域名服务器。
3. 创建新通道组或修改现有DefaultRAGroup的属性。(A可以使用新通道组，如果IPSec标识符设置作为在电话的组名;请参阅步骤10关于电话配置。)
4. 定义使用隧道组的一般属性。 映射定义的组策略给此隧道组。映射此隧道组将使用的定义地址池。除本地之外，如果要使用某事请修改服务器组。
5. 定义预先共享密钥在隧道组的IPSec属性下将使用。
6. 修改使用隧道组的PPP属性，以便使用chap、仅ms-chap-v1和ms-chap-v2。
7. 创建转换设置一特定封装安全有效载荷(ESP)加密类型和认证类型。
8. 指示IPSec使用传输模式而不是隧道模式。
9. 使用与SHA1哈希方法的3DES加密定义ISAKMP/IKEv1策略。
10. 创建动态加密映射，并且映射它对加密映射。
11. 应用加密映射对接口。
12. 启用在该接口的ISAKMP。

ASA兼容性的配置文件命令

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。

此示例显示保证与一本地VPN客户端的ASA兼容性所有操作系统的配置文件命令。

ASA 8.2.5或以上配置示例

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
```

```
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8.3.2.12或以上配置示例

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

验证

使用本部分可确认配置能否正常运行。

此步骤描述如何设置连接：

1. 打开菜单，并且选择**设置**。
2. 选择**无线和网络**或者**无线控制**。(可用的选项取决于机器人您的版本。)
3. 选择从列表的VPN配置。
4. 请输入您的用户名和密码。
5. 选择**记住用户名**。
6. 选择**连接**。

此步骤描述如何断开连接：

1. 打开菜单，并且选择**设置**。
2. 选择**无线和网络**或者**无线控制**。(可用的选项取决于机器人您的版本。)
3. 选择从列表的VPN配置。
4. 选择**断开**。

请使用这些命令为了确认您的连接适当地运作。

- ASA版本8.2.5的**show run crypto isakmp-**
- **show run crypto ikev1** - ASA版本8.3.2.12或以上
- **显示vpn-sessiondb ra-ikev1-ipsec -** ASA版本8.3.2.12或以上
- **显示vpn-sessiondb远程-** ASA版本8.2.5

注意：命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

已知问题说明

- Cisco Bug ID CSCtq21535， “ASA traceback，当连接与机器人L2TP/IPsec客户端”时
- Cisco Bug ID CSCtj57256，从机器人的"L2TP/IPSec连接不设立到ASA55xx"
- Cisco Bug ID CSCtw58945，在IPSec连接的"L2TP失效与ldap授权和mschapv2"

相关信息

- **Cisco ASA 5500系列配置指南使用CLI， 8.4和8.6 ：配置IPSec上的L2TP**
- **5500系列Cisco的ASA的版本注释，版本8.4(x)**
- **Cisco ASA 5500系列配置指南使用CLI， 8.3 ：关于NAT的信息**
- **对8.3 NAT配置示例的ASA Pre-8.3**
- **技术支持和文档 - Cisco Systems**