ASA和本地L2TP-IPSec Android客户端配置示例

目录

简介

通过IPSec的第2层隧道协议(L2TP)，可以在单个平台中部署和管理L2TP VPN解决方案以及IPSec VPN和防火墙服务。在远程访问场景中配置L2TP over IPSec的主要优势是远程用户可以通过公共IP网络访问VPN，而无需网关或专用线路，这使远程访问几乎可以从任何位置通过普通老式电话服务(POTS)进行。 另一个好处是，VPN访问的唯一客户端要求是使用Windows和Microsoft拨号网络(DUN)。 无需其他客户端软件，如Cisco VPN客户端软件。

本文档提供本地L2TP/IPSec Android客户端的配置示例。它将引导您完成思科自适应安全设备(ASA)上所需的所有必要命令，以及Android设备本身需要执行的步骤。

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：

- Android L2TP/IPSec需要Cisco ASA软件版本8.2.5或更高版本、版本8.3.2.12或更高版本，或版本8.4.1或更高版本。
- 当使用L2TP/IPSec协议时，ASA支持Microsoft Windows 7和Android本地VPN客户端的安全散列算法2(SHA2)证书签名支持。
- 请参阅使用CLI、8.4和8.6的Cisco ASA 5500系列配置指南：配置L2TP over IPSec:L2TP over IPSec的许可要求。

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

本节介绍配置本文档中描述的功能所需的信息。

在Android上配置L2TP/IPSec连接

此过程介绍如何在Android上配置L2TP/IPSec连接：

1. 打开菜单，然后选择**“设置”**。
2. 选择**Wireless and Network(无线和网**络)**或Wireless Controls(无线控**制)。可用选项取决于您的Android版本。
3. 选择**VPN Settings**。
4. 选择**Add VPN**。
5. 选择**Add L2TP/IPsec PSK VPN**。
6. 选择**VPN Name**，然后输入描述性名称。
7. 选择**Set VPN Server**，然后输入描述性名称。
8. 选择**Set IPSec pre-shared key**。
9. 取消选**中Enable L2TP secret**。
10. [可选]将IPSec标识符设置为ASA隧道组名称。无设置意味着它将落入ASA上的DefaultRAGroup。
11. 打开菜单，然后选择**保存**。

在ASA上配置L2TP/IPSec连接

以下是必需的ASA互联网密钥交换版本1(IKEv1)（互联网安全关联和密钥管理协议[ISAKMP]）策略设置，当使用基于IPSec的L2TP协议时，允许与终端上的操作系统集成的本地VPN客户端与ASA建立VPN连接：

- IKEv1第1阶段 — 使用SHA1哈希方法的三重数据加密标准(3DES)加密
- IPSec第2阶段 — 3DES或高级加密标准(AES)加密，采用消息摘要5(MD5)或SHA散列方法
- PPP身份验证 — 密码身份验证协议(PAP)、Microsoft质询握手身份验证协议第1版(MS-CHAPv1)或MS-CHAPv2（首选）
- 预共享密钥

注意：ASA仅支持本地数据库上的PPP身份验证PAP和MS-CHAP（版本1和2）。可扩展身份验证协议(EAP)和CHAP由代理身份验证服务器执行。因此，如果远程用户属于使用**authentication eap-proxy或authentication chap** 命令配置的隧道组，并且如果ASA配置为使用本地数据库，则该用户将无法连接。

此外，Android不支持PAP，而且，由于轻量目录访问协议(LDAP)不支持MS-CHAP，LDAP不是可行的身份验证机制。唯一的解决方法是使用RADIUS。有关MS-CHAP和LDAP问题的详细信息，请参阅Cisco Bug ID CSCtw58945，“L2TP over IPSec connections fail with ldap authorization and mschapv2”。

此过程介绍如何在ASA上配置L2TP/IPSec连接：

1. 定义本地地址池或为自适应安全设备使用dhcp服务器，以便为组策略的客户端分配IP地址。
2. 创建内部组策略。 将隧道协议定义为l2tp-ipsec。配置要由客户端使用的域名服务器(DNS)。
3. 创建新隧道组或修改现有DefaultRAGroup的属性。(如果IPSec标识符在电话上设置为group-name，则可使用新隧道组；请参阅步骤10了解电话配置。)
4. 定义所用隧道组的常规属性。 将定义的组策略映射到此隧道组。映射要由此隧道组使用的已定义地址池。如果要使用除LOCAL以外的其他功能，请修改身份验证服务器组。
5. 在要使用的隧道组的IPSec属性下定义预共享密钥。
6. 修改所使用的隧道组的PPP属性，以便仅使用chap、ms-chap-v1和ms-chap-v2。
7. 使用特定封装安全负载(ESP)加密类型和身份验证类型创建转换集。
8. 指示IPSec使用传输模式而非隧道模式。
9. 使用3DES加密和SHA1哈希方法定义ISAKMP/IKEv1策略。
10. 创建动态加密映射，并将其映射到加密映射。
11. 将加密映射应用于接口。
12. 在该接口上启用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。

此示例显示了确保ASA与任何操作系统上的本地VPN客户端兼容的配置文件命令。

ASA 8.2.5或更高版本配置示例

```
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或更高版本配置示例

```
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。

此步骤介绍如何设置连接：

1. 打开菜单，然后选择“**设置**”。
2. 选择**无线和网络**或无**线控制**。（可用选项取决于您的Android版本。）
3. 从列表中选择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Connect。

此过程描述如何断开连接：

1. 打开菜单，然后选择“**设置**”。

2. 选择**无线和网络**或无**线控制**。（可用选项取决于您的Android版本。）
3. 从列表中选择VPN配置。
4. 选择**Disconnect**。

使用这些命令确认连接是否正常工作。

- **show run crypto isakmp** — 用于ASA版本8.2.5
- **show run crypto ikev1** — 用于ASA 8.3.2.12或更高版本
- **show vpn-sessiondb ra-ikev1-ipsec** — 用于ASA 8.3.2.12或更高版本
- **show vpn-sessiondb remote** — 用于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。**使用输出解释器工具来查看 show 命令输出的分析。

已知问题说明

- Cisco Bug ID CSCtq21535，“ASA traceback when connecting with Android L2TP/IPsec client”
- Cisco Bug ID CSCtj57256，“L2TP/IPSec connection from Android does not establish to the ASA55xx”
- Cisco Bug ID CSCtw58945，“L2TP over IPSec connections fail with ldap authorization and mschapv2”

相关信息

- **使用CLI、8.4和8.6的Cisco ASA 5500系列配置指南：配置L2TP over IPsec**
- **Cisco ASA 5500系列版本说明，版本8.4(x)**
- **使用CLI的Cisco ASA 5500系列配置指南8.3:有关NAT的信息**
- **ASA 8.3版到8.3版NAT配置示例**
- **技术支持和文档 - Cisco Systems**