L2TP over IPsec

本章介绍如何在 ASA 上配置 L2TP over IPsec/IKEv1。

关于 L2TP over IPsec/IKEv1 VPN

第 2 层隧道协议 (L2TP) 是允许远程客户端使用公共 IP 网络安全地与企业专用网络服务器通信的 VPN 隧道协议。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。

L2TP 协议基于客户端/服务器模式。此功能在 L2TP 网络服务器 (LNS) 和 L2TP 访问集中器 (LAC) 之间分配。LNS 通常在路由器等网络网关上运行，而 LAC 可以是拨号网络接入服务器 (NAS) 或有一个捆绑的 L2TP 客户端的终端设备（如 Microsoft Windows、Apple iPhone 或 Android）。

在远程访问场景中，使用 IPsec/IKEv1 配置 L2TP 的主要优势在于远程用户可以通过公共 IP 网络访问 VPN，而无需使用网关或专线，实际上就可以利用 POTS 从任何位置实现远程访问。另一个优势是无需思科 VPN 客户端软件等任何其他客户端软件。

注释 L2TP over IPsec TP 仅支持 IKEv1。不支持 IKEv2。

使用 IPsec/IKEv1 的 L2TP 配置支持使用预共享密钥或 RSA 签名方法的证书，也支持使用动态（相对于静态）加密映射。此任务摘要假设已经完成 IKEv1 以及预共享密钥或 RSA 签名配置。有关配置预共享密钥、RSA 和动态加密映射的步骤，请参阅常规操作配置指南中的第 41 章“数字证书”。

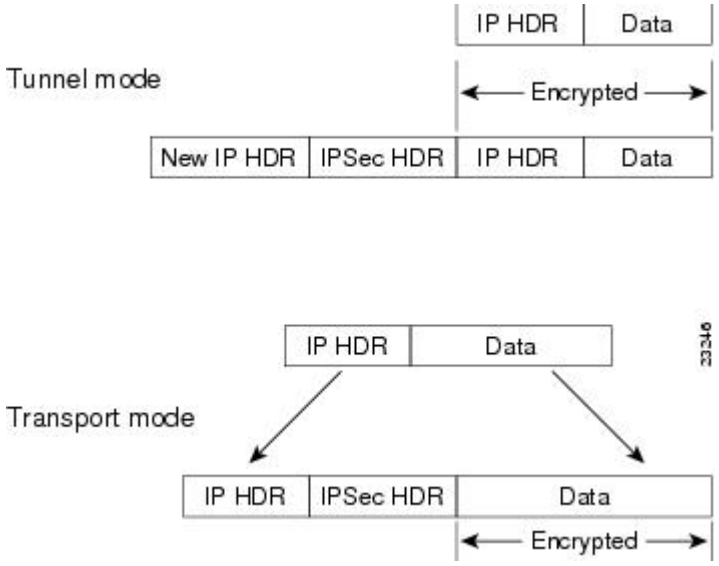
注释 在 ASA 上，使用 IPsec 的 L2TP 允许 LNS 与 Windows、Mac OS X、Android 和思科 IOS 等操作系统中集成的本地 VPN 客户端进行互操作。ASA 上仅支持使用 IPsec 的 L2TP，不支持单独使用本地 L2TP。Windows 客户端支持的最小 IPsec 安全关联生命周期是 300 秒。如果 ASA 上的生命周期设置低于 300 秒，Windows 客户端会忽略此设置并将其替换为 300 秒的生命周期。

IPsec 传输和隧道模式

默认情况下，ASA 使用 IPsec 隧道模式 - 整个原始 IP 数据报都将加密并且将成为新 IP 数据包的负载。此模式允许路由器等网络设备用作 IPsec 代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式的主要优势是不需要修改终端系统即可获得 IPsec 的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

但是，Windows L2TP/IPsec 客户端使用 IPsec 传输模式 - 只加密 IP 负载，而原始 IP 报头保留原封不动。此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。下图说明了 IPsec 隧道和传输模式之间的差异。

图 *1:* 隧道和传输模式下的 ***IPsec***



要使 Windows L2TP 和 IPsec 客户端连接到 ASA，必须使用 **crypto ipsec transform-set trans_name mode transport** 命令为转换集配置 IPsec 传输模式。此命令用于配置程序。**.**

注释 ASA 在分割隧道访问列表中推送的 ACE 不能超过 28 个。

通过此传输功能，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。遗憾的是，如果 IP 报头以明文传输，传输模式就会允许攻击者执行某些流量分析。

L2TP over IPsec 的许可要求

注释　此功能不适用于无负载加密型号。

使用 IKEv2 的 IPsec 远程访问 VPN 需要 AnyConnect Plus 或 Apex 许可证，可单独购买。使用 IKEv1 的 IPsec 远程访问 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点间 VPN 使用 基础 许可证随附的其他 VPN 许可证。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

配置 L2TP over IPsec 的前提条件

配置 L2TP over IPsec 有以下前提条件：

- 组策略 - 您可以为 L2TP/IPSec 连接配置默认组策略 (DfltGrpPolicy) 或用户定义的组策略。不论是哪种情况，必须将组策略配置为使用 L2TP/IPsec 隧道协议。如果没有为用户定义的组策略配置 L2TP/IPsec 隧道协议，请为 L2TP/IPsec 隧道协议配置 DfltGrpPolicy 并允许用户定义的组策略继承此属性。
- 连接配置文件 - 如果您执行的是“预共享密钥”身份验证，您需要配置默认连接配置文件（隧道组）DefaultRAGroup。如果执行的是基于证书的身份验证，您可以使用用户定义的连接配置文件，可以根据证书标识符选择该配置文件。
- 需要在对等体之间建立 IP 连接。要测试连接、请尝试从您的终端 ping ASA 的 IP 地址并尝试 从 ASA ping 您的终端的 IP 地址。
- 确保连接路径上的任何位置都未阻止 UDP 端口 1701。
- 如果 Windows 7 终端设备使用指定 SHA 签名类型的证书进行身份验证，签名类型必须与 ASA 的签名类型（即 SHA1 或 SHA2）匹配。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景模式中受支持。

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明模式。

故障转移准则

状态故障转移不支持 L2TP over IPsec 会话。

IPv6 准则

对于 L2TP over IPsec，没有本机 IPv6 隧道设置支持。

所有平台上的软件限制

我们目前仅支持 4096 L2TP over IPsec 隧道。

身份验证准则

ASA 在本地数据库上只支持 PPP 身份验证 PAP 和 Microsoft CHAP 版本 1 和 2。EAP 和 CHAP 由代理身份验证服务器执行。因此，如果远程用户属于用 **authentication eap-proxy** 或 **authentication chap** 命令配置的隧道组，而 ASA 被配置为使用本地数据库，则该用户将无法连接。

支持的 PPP 身份验证类型

在 ASA 上，L2TP over IPsec 连接只支持 PPP 身份验证类型，如下所示：

表 *1: AAA* 服务器支持和 *PPP* 身份验证类型

AAA 服务器类型	支持的 PPP 身份验证类型
本地	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

表 *2: PPP* 身份验证类型特征

关键字	身份验证类型	特征
chap	CHAP	客户端响应服务器质询，返回使用明文用户名的加密 [质询以及密码]。此协议比 PAP 更安全，但不加密数据。

关键字	身份验证类型	特征
eap-proxy	EAP	启用 EAP，它允许安全设备代理面向外部 RADIUS 身份验证服务器的 PPP 身份验证过程。
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP 版本 1 Microsoft CHAP 版本 2	与CHAP类似，但更安全，因为服务器仅存储和比较加密密码，而不是像 CHAP 中那样存储和比较明文密码。此协议还通过 MPPE 生成用于数据加密的密钥。
pap	PAP	在身份验证期间传递明文用户名和密码，因此并不安全。

使用 CLI 配置 L2TP over Eclipse

您必须配置 IKEv1 (ISAKMP) 策略设置来允许本地 VPN 客户端使用 L2TP over Eclipse 协议与 ASA 进行 VPN 连接。

- IKEv1 阶段 1 - 使用 SHA1 散列方法的 AES 加密。
- Eclipse 阶段 1 - 使用 SHA 散列方法的 AES 加密。
- PPP 身份验证 — PAP、MS-CHAPv1 或 MSCHAPv2（首选）。
- 预共享密钥（仅适用于 iPhone）。

过程

步骤 1 使用特定 ESP 加密类型和身份验证类型创建转换集。

crypto ipsec ike_version transform-set *transform_name ESP_Encryption_Type ESP_Authentication_Type*

示例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-aes esp-sha-hmac
```

步骤 2 指示 Eclipse 使用传输模式而不是隧道模式。

crypto ipsec ike_version transform-set *trans_name* **mode transport**

示例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

步骤 3 将 L2TP/Eclipse 指定为 VPN 隧道协议。

vpn-tunnel-protocol *tunneling_protocol*

示例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

步骤 4 （可选） 指示自适应安全设备向组策略客户端发送 DNS 服务器 IP 地址。

dns value [**none** | *IP_Primary* | *IP_Secondary*]

示例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2
```

步骤 5 （可选） 指示自适应安全设备向组策略客户端发送 WINS 服务器 IP 地址。

wins-server value [**none** | *IP_primary* [*IP_secondary*]]

示例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4
```

步骤 6 （可选） 创建 IP 地址池。

ip local pool *pool_name starting_address-ending_address* **mask** *subnet_mask*

示例：

```
hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0
```

步骤 7 （可选） 将 IP 地址池与连接配置文件（隧道组）关联。

address-pool *pool_name*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

步骤 8 将组策略的名称与连接配置文件（隧道组）关联。

default-group-policyname

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

步骤 9 指定一个身份验证服务器，以验证尝试通过 IPsec 连接的 L2TP 的用户。如果想在服务器不可用时将身份验证退回到本地身份验证，请在命令末尾添加 LOCAL。

authentication-server-group *server_group* [**local**]

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

步骤 10 为连接配置文件（隧道组）指定对尝试 L2TP over Eclipse 连接的用户进行身份验证的方法。如果目前不是使用 ASA 执行本地身份验证而您想要回退到本地身份验证，请在命令末尾添加 LOCAL。

authentication *auth_type*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

步骤 11 为您的连接配置文件（隧道组）设置预共享密钥。

tunnel-group 隧道组名称 **ipsec-attributes**

示例：

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

步骤 12 （可选） 为连接配置文件（隧道组）生成 L2TP 会话的 AAA 审计开始和停止记录。

accounting-server-group *aaa_server_group*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

步骤 13 配置 hello 消息之间的间隔（单位：秒）。范围是 10 到 300 秒。默认间隔为 60 秒。

l2tp tunnel hello *seconds*

示例：

```
hostname(config)# l2tp tunnel hello 100
```

步骤 14 （可选） 启用 NAT 遍历，从而使 ESP 数据包可以通过一个或多个 NAT 设备。

如果您预计 NAT 设备后面会有多个 L2TP 客户端尝试与自适应安全设备进行 L2TP over Eclipse 连接，则必须启用 NAT 遍历。

crypto isakmp nat-traversal *seconds*

要在全局启用 NAT 遍历，请检查并确保在全局配置模式下启用 ISAKMP（可以使用 **crypto isakmp enable** 命令启用），然后使用 **crypto isakmp nat-traversal** 命令。

示例：

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

步骤 15 （可选） 配置隧道组切换。隧道组切换的目的是在用户使用代理身份验证服务器进行身份验证时为用户提供更好的建立 VPN 连接的机会。隧道组与连接配置文件同义。

strip-group

strip-realm

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

步骤 16 （可选） 使用用户名 **jdoe** 和密码 **j!doe1** 创建用户。mschap 选项指定在您输入密码后，会将密码转换为 Unicode，并使用 MD4 进行散列处理。

只有在使用本地用户数据库时才需要使用此步骤。

username *name* **password** *password* **mschap**

示例：

```
asa2(config)# username jdoe password j!doe1 mschap
```

步骤 17 为阶段 1 创建 IKE 策略，并为其分配编号。

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

您可以为 IKE 策略配置几种不同的参数。您还可以为该策略指定一个 Diffie-Hellman 群。ASA 使用 isakamp 策略来完成 IKE 协商。

示例：

```
hostname(config)# crypto ikev1 policy 14
hostname(config-ikev1-policy)# group14
```

创建响应 Windows 7 提议的 IKE 策略

Windows 7 L2TP/IPsec 客户端发送多个 IKE 策略提议来与 ASA 建立 VPN 连接。请定义以下任意一个 IKE 策略，以便从 Windows 7 VPN 本地客户端建立连接。

请按照为 ASA 配置 L2TP over IPsec 的程序进行操作。如要为 Windows 7 本地 VPN 客户端配置 IKE 策略，需在本任务中增加其他步骤。

过程

步骤 1 显示属性和所有现有 IKE 策略的数量。

示例：

```
hostname(config)# show run crypto ikev1
```

步骤 2 配置 IKE 策略number 参数指定您配置的 IKE 策略的编号。此编号已列于 **show run crypto ikev1** 命令的输出中。

crypto ikev1 policy *number*

步骤 3 设置 ASA 用于为每个 IPSec 对等体使用预共享密钥确定身份的身份验证方法。

示例：

```
hostname(config-ikev1-policy)# authentication pre-share
```

步骤 4 选择保护两个 IPSec 对等体之间传输的数据的对称加密方法。对于 Windows 7，请选择适用于 128 位 AES 的 **aes**，或者选择 **aes-256**。

encryption {|**aes**|**aes-256**}

步骤 5 选择确保数据完整性的散列算法。对于 Windows 7，请为 SHA-1 算法指定 **sha**。

示例：

```
hostname(config-ikev1-policy)# hash sha
```

步骤 6 选择 Diffie-Hellman 群标识符。您可以为 aes,aes-256 加密类型指定 14 。

示例：

```
hostname(config-ikev1-policy)# group 14
```

步骤 7 指定 SA 生命周期（以秒为单位）。对于 Windows 7，请指定 86400 秒（即 24 小时）。

示例：

```
hostname(config-ikev1-policy)# lifetime 86400
```

L2TP over IPsec 的配置示例

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

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
 default-group-policy sales_policy
 address-pool sales_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 trans esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set trans mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
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 aes
 hash sha

 group 14
 lifetime 86400
```

L2TP over IPsec 功能历史记录

功能名称	版本	功能信息
L2TP over IPsec	7.2(1)	L2TP over IPsec 在单一平台上提供部署和管理 L2TP VPN 解决方案以 VPN 和防火墙服务的功能。 在远程访问场景中，配置 L2TP over IPsec 的主要优势在于远程用户 过公共 IP 网络访问 VPN，而无需使用网关或专线，实际上就可以利 从任何位置实现远程访问。另一个优势是 VPN 访问的唯一客户端 用带 Microsoft 拨号网络 (DUN) 的 Windows。不需要思科 VPN 客户 等任何其他客户端软件。 引入或修改了以下命令：authentication eap-proxy、authentication ms-c authentication ms-chap-v2、authentication pap、l2tp tunnel hello、 vpn-tunnel-protocol l2tp-ipsec。
弃用 IKE/IPsec 加密和完整性/PRF 密码 对 IKEv1 的 DH 组 14 支持	9.13(1)	以下加密/完整性/PRF 密码已弃用，并将在后续版本 - 9.14(1) 中删 • 3DES 加密 • DES 加密 • MD5 完整性 添加了对 IKEv1 的 DH 组 14（默认）支持。group 2 和 group 5 命令 弃用，并将在后续版本 9.14(1) 中删除。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。