ASA和本地L2TP-IPSec Android客戶端配置示例

目錄

簡介

使用IPSec的第2層通道通訊協定(L2TP)能夠在單一平台中部署和管理L2TP VPN解決方案以及IPSec VPN和防火牆服務。在遠端訪問場景中通過IPSec配置L2TP的主要優點是，遠端使用者可以通過公共IP網路訪問VPN，而無需網關或專用線路，這樣幾乎可以從任何位置使用普通舊式電話服務(POTS)進行遠端訪問。 另一個好處是，VPN接入的唯一客戶端要求是使用Windows和Microsoft撥號網路(DUN)。 不需要額外的客戶端軟體，如Cisco VPN客戶端軟體。

本文檔提供了本機L2TP/IPSec Android客戶端的配置示例。它將帶您瞭解思科自適應安全裝置(ASA)上所需的所有命令，以及在Android裝置本身上要採取的步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Android L2TP/IPSec需要Cisco ASA軟體版本8.2.5或更高版本、版本8.3.2.12或更高版本、版本8.4.1或更高版本。
- 在使用L2TP/IPSec協定時，ASA支援對Microsoft Windows 7和Android本地VPN客戶端的安全雜湊演算法2(SHA2)證書簽名支援。
- 請參閱使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南：配置L2TP over IPSec:L2TP over IPSec的許可要求。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本節介紹設定本檔案所述功能所需的資訊。

在Android上配置L2TP/IPSec連線

以下過程介紹如何在Android上配置L2TP/IPSec連線：

1. 開啟選單，然後選擇**設定**。
2. 選擇**Wireless and Network**或**Wireless Controls**。可用選項取決於您的Android版本。
3. 選擇**VPN Settings**。
4. 選擇**Add VPN**。
5. 選擇**Add L2TP/IPsec PSK VPN**。
6. 選擇**VPN名稱**，然後輸入描述性名稱。
7. 選擇**Set VPN Server**，然後輸入描述性名稱。
8. 選擇**Set IPSec pre-shared key**。
9. 取消選中**Enable L2TP secret**。
10. [可選]將IPSec識別符號設定為ASA隧道組名稱。無設定表示它將進入ASA上的DefaultRAGroup。
11. 開啟選單，然後選擇**儲存**。

在ASA上配置L2TP/IPSec連線

以下是所需的ASA網際網路金鑰交換版本1(IKEv1)（網際網路安全關聯和金鑰管理協定[ISAKMP]）策略設定，允許本地VPN客戶端與終端上的作業系統整合，以便在使用L2TP over IPSec協定時與ASA建立VPN連線：

- IKEv1第1階段 — 使用SHA1雜湊方法的三重資料加密標準(3DES)加密
- IPSec第2階段 — 3DES或採用消息摘要5(MD5)或SHA雜湊方法的高級加密標準(AES)加密
- PPP身份驗證 — 密碼身份驗證協定(PAP)、Microsoft質詢握手身份驗證協定版本1(MS-CHAPv1)或MS-CHAPv2（首選）
- 預共用金鑰

附註：ASA僅支援本地資料庫上的PPP身份驗證PAP和MS-CHAP（版本1和2）。可擴展身份驗證協定(EAP)和CHAP由代理身份驗證伺服器執行。因此，如果遠端使用者屬於使用**authentication eap-proxy** 或**authentication chap** 命令配置的隧道組，並且ASA配置為使用本地資料庫，則該使用者將無法連線。

此外，Android不支援PAP，並且由於輕量級目錄訪問協定(LDAP)不支援MS-CHAP，LDAP不是可行的身份驗證機制。唯一的解決方法是使用RADIUS。有關MS-CHAP和LDAP問題的更多詳細資訊，請參閱Cisco錯誤ID CSCtw58945，「L2TP over IPSec connections fail with ldap authorization and mschapv2」。

以下過程介紹如何在ASA上配置L2TP/IPSec連線：

1. 為自適應安全裝置定義本地地址池或使用dhcp-server，以便將IP地址分配給組策略的客戶端。
2. 建立內部組策略。 將隧道協定定義為l2tp-ipsec。配置客戶端使用的域名伺服器(DNS)。
3. 建立新的隧道組或修改現有DefaultRAGroup的屬性。(如果IPSec識別符號在電話上設定為group-name，則可以使用新的隧道組；有關電話配置，請參閱步驟10。)
4. 定義所使用的隧道組的一般屬性。 將定義的組策略對映到此隧道組。對映此隧道組要使用的已定義地址池。如果要使用LOCAL以外的其他內容，請修改authentication-server組。
5. 在要使用的隧道組的IPSec屬性下定義預共用金鑰。
6. 修改所用隧道組的PPP屬性，以便僅使用chap、ms-chap-v1和ms-chap-v2。
7. 使用特定封裝安全負載(ESP)加密型別和身份驗證型別建立轉換集。
8. 指示IPSec使用傳輸模式而不是隧道模式。
9. 使用3DES加密和SHA1雜湊方法定義ISAKMP/IKEv1策略。
10. 建立動態加密對映，並將其對映到加密對映。
11. 將加密對映應用於介面。
12. 在該介面上啟用ISAKMP。

適用於ASA相容性的配置檔案命令

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

此示例顯示了確保ASA與任何作業系統上的本地VPN客戶端相容的配置檔案命令。

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

以下過程介紹了如何設定連線：

1. 開啟選單，然後選擇**設定**。
2. 選擇**Wireless and Network**或**Wireless Controls**。（可用選項取決於您的Android版本。）
3. 從清單中選擇VPN配置。
4. 輸入您的使用者名稱和密碼。
5. 選擇**Remember username**。
6. 選擇**Connect**。

以下過程介紹了如何斷開連線：

1. 開啟選單，然後選擇**設定**。

2. 選擇**Wireless and Network**或**Wireless Controls**。（可用選項取決於您的Android版本。）
3. 從清單中選擇VPN配置。
4. 選擇**Disconnect**。

使用這些命令可確認您的連線是否正常工作。

- **show run crypto isakmp** - For ASA 8.2.5
- **show run crypto ikev1** — 適用於ASA 8.3.2.12版或更高版本
- **show vpn-sessiondb ra-ikev1-ipsec -** 用於ASA 8.3.2.12或更高版本
- **show vpn-sessiondb remote -** ASA 8.2.5版

附註：輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

已知警告

- 思科錯誤ID CSCtq21535，「Android L2TP/IPsec客戶端連線時的ASA回溯」
- 思科錯誤ID CSCtj57256，「L2TP/IPSec connection not established to the ASA55xx（從Android到ASA55xx的L2TP/IPSec連線無法建立）」
- 思科錯誤ID CSCtw58945，「L2TP over IPSec連線失敗，帶ldap授權和mschapv2」

相關資訊

- **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8.4(x)版發行說明**
- **使用CLI的Cisco ASA 5500系列配置指南8.3:有關NAT的資訊**
- **ASA 8.3版到8.3版NAT配置示例**
- **技術支援與文件 - Cisco Systems**