Introduction

Layer 2 Tunneling Protocol (L2TP) over IPSec provides the capability to deploy and administer an L2TP VPN solution alongside the IPSec VPN and firewall services in a single platform. The primary benefit of the configuration of L2TP over IPSec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, which enables remote access from virtually any place with plain old telephone service (POTS). An additional benefit is that the only client requirement for VPN access is the use of Windows with Microsoft Dial-Up Networking (DUN). No additional client software, such as the Cisco VPN client software, is required.

This document provides a sample configuration for the native L2TP/IPSec Android client. It takes you through all the necessary commands required on a Cisco Adaptive Security Appliance (ASA), as well as the steps to be taken on the Android device itself.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the following software and hardware versions:
Configure

This section describes the information one would need in order to configure the features described in this document.

Configure the L2TP/IPSec Connection on the Android

This procedure describes how to configure the L2TP/IPSec connection on the Android:

1. Open the menu, and choose Settings.
2. Choose Wireless and Network or Wireless Controls. The available option depends on your version of Android.
3. Choose VPN Settings.
4. Choose Add VPN.
5. Choose Add L2TP/IPsec PSK VPN.
6. Choose VPN Name, and enter a descriptive name.
7. Choose Set VPN Server, and enter a descriptive name.
8. Choose Set IPSec pre-shared key.
9. Uncheck Enable L2TP secret.
10. [Optional] Set the IPSec identifier as the ASA tunnel group name. No setting means it will fall into DefaultRAGroup on the ASA.
11. Open the menu, and choose Save.

Configure the L2TP/IPSec Connection on ASA

These are the required ASA Internet Key Exchange Version 1 (IKEv1) (Internet Security Association and Key Management Protocol [ISAKMP]) policy settings that allow native VPN clients, integrated with the operating system on an endpoint, to make a VPN connection to the ASA when L2TP over IPSec protocol is used:

- IKEv1 phase 1 - Triple Data Encryption Standard (3DES) encryption with SHA1 hash method
- IPSec phase 2 - 3DES or Advanced Encryption Standard (AES) encryption with Message Digest 5 (MD5) or SHA hash method
- PPP Authentication - Password Authentication Protocol (PAP), Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1), or MS-CHAPv2 (preferred)
- Pre-shared key

- Android L2TP/IPSec requires Cisco ASA software version 8.2.5 or later, version 8.3.2.12 or later, or version 8.4.1 or later.
- ASA supports Secure Hash Algorithm 2 (SHA2) certificate signature support for Microsoft Windows 7 and Android-native VPN clients when the L2TP/IPSec protocol is used.
- See Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring L2TP over IPSec: Licensing Requirements for L2TP over IPSec.

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.
**Note:** The ASA supports only the PPP authentications PAP and MS-CHAP (versions 1 and 2) on the local database. The Extensible Authentication Protocol (EAP) and CHAP are performed by proxy authentication servers. Therefore, if a remote user belongs to a tunnel group configured with the `authentication eap-proxy` or `authentication chap` commands and if the ASA is configured to use the local database, that user will be unable to connect.

Furthermore, Android does not support PAP and, because Lightweight Directory Access Protocol (LDAP) does not support MS-CHAP, LDAP is not a viable authentication mechanism. The only workaround is to use RADIUS. See Cisco Bug ID CSCtw58945, "L2TP over IPSec connections fail with ldap authorization and mschapv2," for further details on issues with MS-CHAP and LDAP.

This procedure describes how to configure the L2TP/IPSec connection on the ASA:

1. Define a local address pool or use a dhcp-server for the adaptive security appliance in order to allocate IP addresses to the clients for the group policy.
2. Create an internal group-policy. Define the tunnel protocol to be l2tp-ipsec. Configure a domain name server (DNS) to be used by the clients.
3. Create a new tunnel group or modify the attributes of the existing DefaultRAGroup. (A new tunnel group can be used if the IPSec identifier is set as group-name on the phone; see step 10 for the phone configuration.)
4. Define the general attributes of the tunnel group that are used. Map the defined group policy to this tunnel group. Map the defined address pool to be used by this tunnel group. Modify the authentication-server group if you want to use something other than LOCAL.
5. Define the pre-shared key under the IPSec attributes of the tunnel group to be used.
6. Modify the PPP attributes of the tunnel group that are used so that only chap, ms-chap-v1 and ms-chap-v2 are used.
7. Create a transform set with a specific encapsulating security payload (ESP) encryption type and authentication type.
8. Instruct IPSec to use transport mode rather than tunnel mode.
9. Define an ISAKMP/IKEv1 policy using 3DES encryption with SHA1 hash method.
10. Create a dynamic crypto map, and map it to a crypto map.
11. Apply the crypto map to an interface.
12. Enable ISAKMP on that interface.

**Configuration File Commands for ASA Compatibility**

**Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

This example shows the configuration file commands that ensure ASA compatibility with a native VPN client on any operating system.

**ASA 8.2.5 or Later Configuration Example**

```
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 mschap-v1
authentication mschap-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 or Later Configuration Example

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 mschap-v1
authentication mschap-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

Verify

Use this section to confirm that your configuration works properly.
This procedure describes how to set up the connection:

1. Open the menu, and choose **Settings**.
2. Select **Wireless and Network** or **Wireless Controls**. (The available option depends on your version of Android.)
3. Select the VPN configuration from the list.
4. Enter your username and password.
5. Select **Remember username**.
6. Select **Connect**.

This procedure describes how to disconnect:

1. Open the menu, and choose **Settings**.
2. Select **Wireless and Network** or **Wireless Controls**. (The available option depends on your version of Android.)
3. Select the VPN configuration from the list.
4. Select **Disconnect**.

Use these commands in order to confirm that your connection works properly.

- **show run crypto isakmp** - For ASA version 8.2.5
- **show run crypto ikev1** - For ASA version 8.3.2.12 or later
- **show vpn-sessiondb ra-ikev1-ipsec** - For ASA version 8.3.2.12 or later
- **show vpn-sessiondb remote** - For ASA version 8.2.5

**Note:** The **Output Interpreter Tool** (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

**Known Caveats**

- Cisco bug ID [CSCtj57256](https://www.cisco.com/c/en/us/support/docs/security/asa/3325836.html), "L2TP/IPSec connection from Android doesn't establish to the ASA55xx"
- Cisco bug ID [CSCtw58945](https://www.cisco.com/c/en/us/support/docs/security/asa/3325836.html), "L2TP over IPSec connections fail with ldap authorization and mschapv2"

**Related Information**

- [Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring L2TP over IPsec](https://www.cisco.com/c/en/us/support/docs/security/asa/3325836.html)
- [ASA Pre-8.3 to 8.3 NAT Configuration Examples](https://www.cisco.com/c/en/us/support/docs/security/asa/3325836.html)