# Exemple de configuration du client Android ASA et L2TP natif-IPSec

## Contenu



## Introduction

Le protocole L2TP (Layer 2 Tunneling Protocol) sur IPSec permet de déployer et d'administrer une solution VPN L2TP parallèlement aux services VPN IPSec et de pare-feu dans une plate-forme unique. Le principal avantage de la configuration de L2TP sur IPSec dans un scénario d'accès à distance est que les utilisateurs distants peuvent accéder à un VPN sur un réseau IP public sans passerelle ou ligne dédiée, ce qui permet un accès à distance depuis pratiquement n'importe quel endroit avec un service téléphonique traditionnel (POTS). Un autre avantage est que la seule condition requise pour l'accès VPN est l'utilisation de Windows avec la mise en réseau à distance Microsoft (DUN). Aucun logiciel client supplémentaire, tel que le logiciel client VPN Cisco, n'est requis.

Ce document fournit un exemple de configuration pour le client Android L2TP/IPSec natif. Il vous présente toutes les commandes nécessaires sur un appareil de sécurité adaptatif Cisco (ASA), ainsi que les étapes à suivre sur le périphérique Android lui-même.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Android L2TP/IPSec nécessite le logiciel Cisco ASA version 8.2.5 ou ultérieure, version 8.3.2.12 ou ultérieure, ou version 8.4.1 ou ultérieure.
- ASA prend en charge la signature de certificat SHA2 (Secure Hash Algorithm 2) pour les clients VPN natifs de Microsoft Windows 7 et d'Android lorsque le protocole L2TP/IPSec est utilisé.
- Reportez-vous au Guide de configuration de la gamme Cisco ASA 5500 à l'aide de la CLI, 8.4 et 8.6 : Configuration de L2TP sur IPSec : Exigences de licence pour L2TP sur IPSec.

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. 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.

## Configuration

Cette section décrit les informations nécessaires pour configurer les fonctionnalités décrites dans ce document.

### Configurer la connexion L2TP/IPSec sur l'Android

Cette procédure décrit comment configurer la connexion L2TP/IPSec sur Android :

1. Ouvrez le menu, puis sélectionnez **Paramètres**.
2. Choisissez **Wireless and Network** ou **Wireless Controls**. L'option disponible dépend de votre version d'Android.
3. Choisissez **VPN Settings**.
4. Choisissez **Add VPN**.
5. Choisissez **Add L2TP/IPsec PSK VPN**.
6. Choisissez **VPN Name**, puis entrez un nom descriptif.
7. Choisissez **Set VPN Server**, puis entrez un nom descriptif.
8. Choisissez **Définir la clé pré-partagée IPSec**.
9. Désélectionnez **Activer le secret L2TP**.
10. [Facultatif] Définissez l'identificateur IPSec comme nom de groupe de tunnels ASA. Aucun paramètre ne signifie qu'il tombera dans DefaultRAGroup sur l'ASA.
11. Ouvrez le menu et choisissez **Enregistrer**.

### Configurer la connexion L2TP/IPSec sur ASA

Il s'agit des paramètres de stratégie ASA Internet Key Exchange Version 1 (IKEv1) (Internet Security Association and Key Management Protocol [ISAKMP]) requis qui permettent aux clients VPN natifs, intégrés au système d'exploitation sur un terminal, d'établir une connexion VPN à l'ASA lorsque le protocole L2TP sur IPSec est utilisé :

- Phase 1 d'IKEv1 - Chiffrement 3DES (Triple Data Encryption Standard) avec méthode de hachage SHA1
- Cryptage IPSec phase 2 - 3DES ou AES (Advanced Encryption Standard) avec la méthode MD5 (Message Digest 5) ou SHA
- Authentification PPP - Protocole d'authentification par mot de passe (PAP), Protocole d'authentification à échanges confirmés Microsoft version 1 (MS-CHAPv1) ou MS-CHAPv2 (préféré)
- Clé pré-partagée

  **Note**: L'ASA prend uniquement en charge les authentifications PPP PAP et MS-CHAP (versions 1 et 2) sur la base de données locale. Les protocoles EAP (Extensible Authentication Protocol) et CHAP sont exécutés par des serveurs d'authentification proxy. Par conséquent, si un utilisateur distant appartient à un groupe de tunnels configuré avec les commandes **authentication eap-proxy** ou **authentication chap** et si l'ASA est configuré pour utiliser la base de données locale, cet utilisateur ne pourra pas se connecter.

  En outre, Android ne prend pas en charge PAP et, comme LDAP (Lightweight Directory Access Protocol) ne prend pas en charge MS-CHAP, LDAP n'est pas un mécanisme d'authentification viable. La seule solution de contournement est d'utiliser RADIUS. Reportez-vous à l'ID de bogue Cisco CSCtw58945, « L2TP sur les connexions IPSec échouent avec l'autorisation ldap et mschapv2, » pour plus de détails sur les problèmes avec MS-CHAP et LDAP.

Cette procédure décrit comment configurer la connexion L2TP/IPSec sur l'ASA :

1. Définissez un pool d'adresses locales ou utilisez un serveur dhcp pour l'appliance de sécurité adaptative afin d'allouer des adresses IP aux clients pour la stratégie de groupe.
2. Créez une stratégie de groupe interne. Définissez le protocole de tunnel à l2tp-ipsec.Configurez un serveur de noms de domaine (DNS) à utiliser par les clients.
3. Créez un nouveau groupe de tunnels ou modifiez les attributs du groupe DefaultRAGroup existant. (Un nouveau groupe de tunnels peut être utilisé si l'identificateur IPSec est défini comme nom de groupe sur le téléphone ; voir l'étape 10 pour la configuration du téléphone.)
4. Définissez les attributs généraux du groupe de tunnels utilisé. Mapper la stratégie de groupe définie à ce groupe de tunnels.Mapper le pool d'adresses défini à utiliser par ce groupe de tunnels.Modifiez le groupe authentication-server si vous voulez utiliser autre chose que LOCAL.
5. Définissez la clé pré-partagée sous les attributs IPSec du groupe de tunnels à utiliser.
6. Modifiez les attributs PPP du groupe de tunnels qui sont utilisés de sorte que seuls chap, ms-chap-v1 et ms-chap-v2 soient utilisés.
7. Créez un jeu de transformation avec un type de cryptage et d'authentification ESP (encapsulating security payload) spécifique.
8. Demandez à IPSec d'utiliser le mode transport plutôt que le mode tunnel.
9. Définissez une stratégie ISAKMP/IKEv1 à l'aide du chiffrement 3DES avec la méthode de hachage SHA1.
10. Créez une crypto-carte dynamique et mappez-la sur une crypto-carte.
11. Appliquez la crypto-carte à une interface.
12. Activez ISAKMP sur cette interface.

## Commandes de fichier de configuration pour la compatibilité ASA

**Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Cet exemple montre les commandes du fichier de configuration qui garantissent la compatibilité ASA avec un client VPN natif sur n'importe quel système d'exploitation.

### Exemple de configuration d'ASA 8.2.5 ou version ultérieure

```
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
```

### Exemple de configuration d'ASA 8.3.2.12 ou version ultérieure

```
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
```

# Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Cette procédure décrit comment configurer la connexion :

1. Ouvrez le menu, puis sélectionnez **Paramètres**.
2. Sélectionnez **Wireless and Network** ou **Wireless Controls**. (L'option disponible dépend de votre version d'Android.)
3. Sélectionnez la configuration VPN dans la liste.
4. Saisissez votre nom d'utilisateur et votre mot de passe.
5. Sélectionnez **Mémoriser le nom d'utilisateur**.
6. Sélectionnez **Connect**.

Cette procédure décrit comment se déconnecter :

1. Ouvrez le menu, puis sélectionnez **Paramètres**.
2. Sélectionnez **Wireless and Network** ou **Wireless Controls**. (L'option disponible dépend de votre version d'Android.)
3. Sélectionnez la configuration VPN dans la liste.
4. Sélectionnez **Déconnecter**.

Utilisez ces commandes afin de confirmer que votre connexion fonctionne correctement.

- **show run crypto isakmp** - Pour ASA version 8.2.5
- **show run crypto ikev1** - Pour ASA version 8.3.2.12 ou ultérieure
- **show vpn-sessiondb ra-ikev1-ipsec -** Pour ASA version 8.3.2.12 ou ultérieure
- **show vpn-sessiondb remote -** Pour ASA version 8.2.5

  **Note**: L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

# Caveats connus

- ID de bogue Cisco CSCtq21535, « Traceback ASA lors de la connexion avec le client Android L2TP/IPsec »
- ID de bogue Cisco CSCtj57256, « La connexion L2TP/IPSec d'Android n'est pas établie à l'ASA55xx »

- ID de bogue Cisco CSCtw58945, « Échec des connexions L2TP sur IPSec avec autorisation ldap et mschapv2 »

## Informations connexes

- Guide de configuration de la gamme Cisco ASA 5500 à l'aide de la CLI, 8.4 et 8.6 : Configuration de L2TP sur IPsec
- Notes de version de la gamme Cisco ASA 5500, version 8.4(x)
- Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, version 8.3 : Informations sur NAT
- Exemples de configuration NAT ASA Pre-8.3 à 8.3
- Support et documentation techniques - Cisco Systems