ASA et exemple indigène de configuration de client L2TP-IPSec Android

Contenu

Introduction

Le Layer 2 Tunneling Protocol (L2TP) au-dessus d'IPSec fournit la capacité pour déployer et gérer une solution VPN L2TP à côté de l'IPSec VPN et des services de Pare-feu dans une plate-forme unique. L'avantage primaire de la configuration de L2TP au-dessus d'IPSec dans un scénario d'Accès à distance est que les utilisateurs distants peuvent accéder à un VPN au-dessus d'un réseau IP public sans passerelle ou ligne dédiée, qui active l'Accès à distance de pratiquement n'importe quel endroit avec le réseau téléphonique public commuté (POTS). Une allocation complémentaire est que la seule exigence de client pour l'accès VPN est l'utilisation de Windows avec le réseau commuté de Microsoft (DUN). Aucun logiciel client supplémentaire, tel que le logiciel de Client VPN Cisco, n'est exigé.

Ce document fournit une configuration d'échantillon pour le client indigène L2TP/IPSec Android. Il prend vous par toutes les commandes nécessaires exigées sur une appliance de sécurité adaptable Cisco (ASA), aussi bien que les mesures à prendre sur le périphérique d'Android lui-même.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le logiciel et les versions de matériel suivants :

- L2TP/IPSec androïde exige la version de logiciel 8.2.5 de Cisco ASA ou plus tard, la version 8.3.2.12 ou ultérieures, ou la version 8.4.1 ou ultérieures.
- Soutien de signature de certificat du Secure Hash Algorithm 2 de supports ASA (SHA2) de Microsoft Windows 7 et des clients vpn Android-indigènes quand le protocole L2TP/IPSec est utilisé.
- Voir le guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6 : Configurer L2TP au-dessus d'IPSec : Conditions d'autorisation pour L2TP au-dessus d'IPSec.

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Cette section décrit les informations une devrait afin de configurer les caractéristiques décrites dans ce document.

Configurez la connexion L2TP/IPSec sur Android

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

1. Ouvrez le menu, et le sélectionnez Settings.
2. Choisissez les **contrôles de radio et de réseau** ou de **radio**. L'option disponible dépend de votre version d'Android.
3. Choisissez les **configurations VPN**.
4. Choisissez **ajoutent le VPN**.
5. Choisissez **ajoutent L2TP/IPsec PSK VPN**.
6. Choisissez le **nom VPN**, et écrivez un nom descriptif.
7. Choisissez le **serveur VPN réglé**, et écrivez un nom descriptif.
8. Choisissez la **clé pré-partagée réglée d'IPSec**.
9. Décochez le **secret de l'enable L2TP**.
10. [Facultatif] placez l'identifiant d'IPSec comme nom de groupe de tunnel ASA. Aucune configuration ne signifie qu'elle tombera dans DefaultRAGroup sur l'ASA.
11. Ouvrez le menu, et choisissez la **sauvegarde**.

Configurez la connexion L2TP/IPSec sur l'ASA

Ce sont la version exigée 1 (IKEv1) d'échange de clés Internet (IKE) ASA (association de sécurité internet et protocole de gestion de clés [ISAKMP]) les paramètres de la stratégie qui permettent les clients vpn indigènes, intégrés avec le système d'exploitation sur un point final, pour établir une connexion VPN à l'ASA quand L2TP au-dessus de protocole IPsec est utilisé :

- IKEv1 phase 1 - Cryptage de Norme 3DES (Triple Data Encryption Standard) avec la méthode des informations parasites SHA1
- Phase 2 d'IPSec - Cryptage 3DES ou de Norme AES (Advanced Encryption Standard) avec la méthode de Message Digest 5 (MD5) ou d'informations parasites de SHA
- Version 1 (MS-CHAPv1) d'authentification Protocol (PAP), de Microsoft Challenge Handshake Authentication Protocol de mot de passe d'authentification de PPP, ou MS-CHAPv2 (préférés)
- Clé pré-partagée

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

  En outre, Android ne prend en charge pas le PAP et, parce que le Protocole LDAP (Lightweight Directory Access Protocol) ne prend en charge pas MS-CHAP, le LDAP n'est pas un mécanisme d'authentification viable. Le seul contournement est d'utiliser le RAYON. Voir l'ID de bogue Cisco CSCtw58945, "L2TP au-dessus de l'échouer de connexions d'IPSec avec l'autorisation de LDAP et mschapv2," pour d'autres détails sur des questions avec MS-CHAP et LDAP.

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

1. Définissez un groupe d'adresse locale ou employez un dhcp-server pour l'appliance de sécurité adaptable 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 pour être l2tp-ipsec.Configurez un serveur de noms de domaines (DN) à utiliser par les clients.
3. Créez un nouveau groupe de tunnel ou modifiez les attributs du DefaultRAGroup existant. (Le nouveau groupe de tunnel A peut être utilisé si l'identifiant d'IPSec est placé comme groupe-nom au téléphone ; voir l'étape 10 pour la configuration de téléphone.)
4. Définissez les attributs généraux du groupe de tunnel qui sont utilisés. Tracez la stratégie de groupe définie à ce groupe de tunnel.Tracez le pool d'adresses défini à utiliser par ce groupe de tunnel.Modifiez le groupe d'authentification-serveur si vous voulez utiliser quelque chose autre que des GENS DU PAYS.
5. Définissez la clé pré-partagée sous les attributs d'IPSec du groupe de tunnel à utiliser.
6. Modifiez les attributs de PPP du groupe de tunnel qui sont utilisés de sorte que seulement le CHAP, les ms-chap-v1 et les ms-chap-v2 soient utilisés.
7. Créez un jeu de transformations avec un type spécifique de cryptage de Protocole ESP (Encapsulating Security Payload) et le type d'authentification.
8. Demandez à IPSec pour utiliser le mode de transport plutôt que le tunnel mode.
9. Définissez une stratégie ISAKMP/IKEv1 utilisant le cryptage 3DES avec la méthode des informations parasites SHA1.
10. Créez une crypto-carte dynamique, et tracez-la à un crypto map.

11. Appliquez le crypto map à une interface.
12. ISAKMP d'enable sur cette interface.

Commandes de fichier de configuration pour la compatibilité ASA

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

Cet exemple affiche les commandes de fichier de configuration qui assurent la compatibilité ASA avec un client vpn indigène sur n'importe quel système d'exploitation.

ASA 8.2.5 ou exemple de configuration plus récente

```
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 ou exemple de configuration plus récente

```
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
```

Vérifiez

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

Cette procédure décrit comment installer la connexion :

1. Ouvrez le menu, et le sélectionnez Settings.
2. **Contrôles** choisis de **radio et de réseau** ou de **radio**. (L'option disponible dépend de votre version d'Android.)
3. Sélectionnez la configuration du VPN de la liste.
4. Saisissez votre nom d'utilisateur et votre mot de passe.
5. Choisi **souvenez-vous le nom d'utilisateur**.
6. Choisi **connectez**.

Cette procédure décrit comment déconnecter :

1. Ouvrez le menu, et le sélectionnez Settings.
2. **Contrôles** choisis de **radio et de réseau** ou de **radio**. (L'option disponible dépend de votre version d'Android.)
3. Sélectionnez la configuration du VPN de la liste.
4. Sélectionnez le **débranchement**.

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

- **affichez le crypto isakmp de passage** - Pour la version 8.2.5 ASA
- **affichez le passage ikev1 crypto** - Pour la version 8.3.2.12 ou ultérieures ASA
- **affichez VPN-sessiondb ra-ikev1-ipsec -** Pour la version 8.3.2.12 ou ultérieures ASA
- **affichez le distant de VPN-sessiondb -** Pour la version 8.2.5 ASA

  Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Mises en garde connues

- ID de bogue Cisco CSCtq21535, « retour arrière ASA en se connectant au client d'Android L2TP/IPsec »
- L'ID de bogue Cisco CSCtj57256, connexion "L2TP/IPSec d'Android n'établit pas à l'ASA55xx"
- L'ID de bogue Cisco CSCtw58945, "L2TP au-dessus des connexions d'IPSec échouent avec l'autorisation et mschapv2" de LDAP

Informations connexes

- Guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6 : Configurer le L2TP sur IPsec
- Notes en version pour la gamme de Cisco ASA 5500, version 8.4(x)
- Guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, 8.3 : Informations sur NAT
- ASA Pre-8.3 à 8.3 exemples NAT de configuration
- Support et documentation techniques - Cisco Systems