L2TP sur IPsec

Ce chapitre décrit comment configurer L2TP sur IPsec/IKEv1 sur l'ASA.

À propos des VPN L2TP sur IPsec/IKEv1

Le protocole de tunnelisation pour la couche 2 (L2TP) est un protocole de tunnelisation VPN qui permet aux clients distants d'utiliser le réseau IP public pour communiquer en toute sécurité avec les serveurs de réseau privés d'entreprise. L2TP utilise PPP sur UDP (port 1701) pour tunneliser les données.

Le protocole L2TP est basé sur le modèle client/serveur. La fonction est répartie entre le serveur de réseau L2TP (LNS) et le concentrateur d'accès L2TP (LAC). Le LNS s'exécute généralement sur une passerelle réseau telle qu'un routeur, tandis que le LAC peut être un serveur d'accès réseau (NAS) commuté ou un périphérique terminal doté d'un client L2TP intégré, comme Microsoft Windows, Apple iPhone ou Android.

Le principal avantage de la configuration de L2TP avec IPsec/IKEv1 dans un scénario d'accès à distance est que les utilisateurs distants peuvent accéder à un VPN sur un réseau IP public sans passerelle ni ligne dédiée, ce qui permet un accès à distance à partir de pratiquement n'importe où avec le service POTS. Un autre avantage est qu'aucun logiciel client supplémentaire, comme le logiciel client VPN Cisco, n'est requis.

Remarque L2TP sur IPsec ne prend en charge que IKEv1. IKEv2 n'est pas pris en charge.

La configuration de L2TP avec IPsec/IKEv1 prend en charge l'authentification par certificats ainsi que les méthodes par clé prépartagée ou signature RSA, ainsi que l'utilisation de cartes de chiffrement dynamiques (par opposition à statiques). Ce résumé des tâches suppose l'achèvement d'IKEv1, ainsi que la configuration des clés prépartagées ou de la signature RSA. Consultez le chapitre 41, « Certificats numériques », dans le guide de configuration des opérations générales pour connaître les étapes à suivre pour configurer les clés prépartagées, le RSA et les cartes de chiffrement dynamiques.

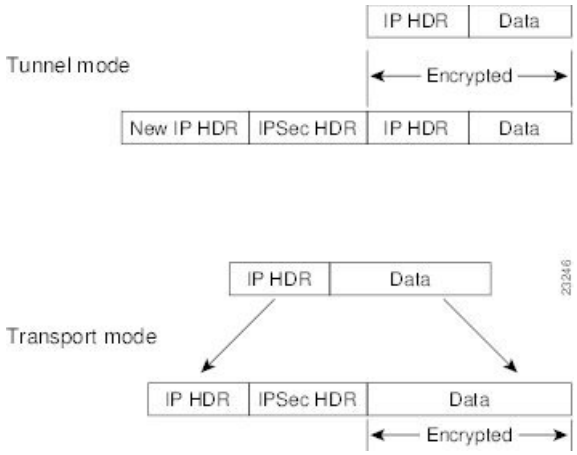
Remarque L2TP avec IPsec sur l'ASA permet au LNS d'interopérer avec des clients VPN natifs intégrés à des systèmes d'exploitation tels que Windows, Mac OS X, Android et Cisco IOS. Seul L2TP avec IPsec est pris en charge ; L2TP natif lui-même n'est pas pris en charge sur l'ASA. La durée de vie minimale d'une association de sécurité IPsec prise en charge par le client Windows est de 300 secondes. Si la durée de vie configurée sur l'ASA est inférieure à 300 secondes, le client Windows l'ignore et la remplace par une durée de vie de 300 secondes.

Modes de transport et de tunnel IPsec

Par défaut, l'ASA utilise le mode tunnel IPsec : l'ensemble du datagramme IP d'origine est chiffré et devient la charge utile d'un nouveau paquet IP. Ce mode permet à un périphérique réseau, comme un routeur, de servir de proxy IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination. Le principal avantage du mode de tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Le mode tunnel offre également une protection contre l'analyse du trafic; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

Cependant, le client Windows L2TP/IPsec utilise le mode transport IPsec—seule la charge utile IP est chiffrée, et les en-têtes IP d'origine demeurent inchangés. Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. La figure suivante illustre les différences entre les modes de tunnel IPsec et de transport.

Illustration 1 : IPsec en modes tunnel et transport



Pour que les clients Windows L2TP et IPsec se connectent à l'ASA, vous devez configurer le mode transport IPsec pour un ensemble de transformation à l'aide de la commande **crypto ipsec transform-set trans_name mode transport**. Cette commande est utilisée dans la procédure de configuration**.**

Remarque L'ASA ne peut pas pousser plus de 28 ACE dans la liste d'accès de tunnel fractionné.

Grâce à ce mode transport, vous pouvez activer un traitement spécifique (par exemple, QoS) sur le réseau intermédiaire en fonction des informations contenues dans l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet. Cependant, si l'en-tête IP est transmis en clair, le mode transport permet à un attaquant d'effectuer une analyse du trafic.

Exigences de licence pour L2TP sur IPsec

Remarque Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Le VPN d'accès à distance IPsec utilisant IKEv2 nécessite une licence AnyConnect Plus ou Apex, disponible séparément. Le VPN d'accès à distance IPsec utilisant IKEv1 et le VPN de site à site IPsec utilisant IKEv1 ou IKEv2 utilise la licence Autre VPN fournie avec la licence Essentials. Consultez Licences de fonctionnalités de la gamme Cisco ASA pour connaître les valeurs maximales par modèle.

Conditions préalables à la configuration de L2TP sur IPsec

La configuration de L2TP sur IPsec nécessite les conditions préalables suivantes :

- Stratégie de groupe : vous pouvez configurer la stratégie de groupe par défaut, DfltGrpPolicy, ou une stratégie de groupe définie par l'utilisateur pour les connexions L2TP/IPsec. Dans les deux cas, la stratégie de groupe doit être configurée pour utiliser le protocole de tunnellisation L2TP/IPsec. Si le protocole de tunnellisation L2TP/IPsec n'est pas configuré pour votre stratégie de groupe définie par l'utilisateur, configurez DfltGrpPolicy pour le protocole de tunnellisation L2TP/IPsec et permettez à votre stratégie de groupe définie par l'utilisateur d'hériter de cet attribut.
- Profil de connexion : vous devez configurer le profil de connexion par défaut (groupe de tunnels), DefaultRAGroup, si vous effectuez une authentification par « clé prépartagée ». Si vous effectuez une authentification basée sur des certificats, vous pouvez utiliser un profil de connexion défini par l'utilisateur qui peut être choisi en fonction des identifiants de certificat.
- La connectivité IP doit être établie entre les homologues. Pour tester la connectivité, essayez d'effectuer un ping vers l'adresse IP de l'ASA depuis votre terminal, puis vers l'adresse IP de votre terminal depuis l'ASA.
- Assurez-vous que le port UDP 1701 n'est pas bloqué le long du chemin de la connexion.
- Si un terminal Windows 7 s'authentifie à l'aide d'un certificat qui spécifie un type de signature SHA, le type de signature doit correspondre à celui de l'ASA, soit SHA1 ou SHA2.

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

Directives relatives au mode contextuel

Pris en charge en mode contexte unique

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode transparent n'est pas pris en charge.

Directives en matière de basculement

Les sessions L2TP sur IPsec ne sont pas prises en charge par le basculement avec état.

Directives IPv6

Il n'y a pas de prise en charge native de la configuration de tunnel IPv6 pour L2TP sur IPsec.

Limitation logicielle sur toutes les plateformes

Nous prenons actuellement en charge uniquement 4 096 tunnels L2TP sur IPsec.

Directives d'authentification

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

Types d'authentification PPP pris en charge

Les connexions L2TP sur IPsec sur l'ASA prennent en charge uniquement les types d'authentification PPP, comme indiqué :

Tableau 1 : Prise en charge des serveurs AAA et types d'authentification PPP

Type de serveur AAA	Types d'authentification PPP pris en charge
LOCAL	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

Tableau 2 : Caractéristiques du type d'authentification PPP

Mot-clé	Type d'authentification	Caractéristiques
chap	CHAP	En réponse au défi du serveur, le client renvoie le [challenge plus password] chiffré avec un nom d'utilisateur en texte clair. Ce protocole est plus sécurisé que le PAP, mais il ne chiffre pas les données.

Mot-clé	Type d'authentification	Caractéristiques
eap-proxy	EAP	Active EAP, ce qui permet au périphérique de sécurité de relayer le processus d'authentification PPP vers un serveur d'authentification RADIUS externe.
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP, version 1 Microsoft CHAP, version 2	Similaire à CHAP, mais plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. Ce protocole génère également une clé pour le chiffrement des données par MPPE.
pap	PAP	Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé.

Configuration de L2TP sur Eclipse avec l'interface de ligne de commande

Vous devez configurer les paramètres de politique IKEv1 (ISAKMP) pour permettre aux clients VPN natifs d'établir une connexion VPN avec l'ASA à l'aide du protocole L2TP sur Eclipse.

- IKEv1 phase 1 : chiffrement AES avec méthode de hachage SHA1.
- Eclipse phase 2 : chiffrement AES avec méthode de hachage SHA.
- Authentification PPP : PAP, MS-CHAPv1 ou MSCHAPv2 (préféré).
- Clé partagée (uniquement pour iPhone).

Procédure

Étape 1 Créez un ensemble de transformation avec un type de chiffrement ESP et un type d'authentification spécifiques.

crypto ipsec ike_version transform-set *transform_name ESP_Encryption_Type ESP_Authentication_Type*

Exemple :

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

Étape 2 Configurez Eclipse pour utiliser le mode transport plutôt que le mode tunnel.

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

Exemple :

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

Étape 3 Précisez L2TP/Eclipse comme protocole de tunnelisation VPN.

vpn-tunnel-protocol *tunneling_protocol*

Exemple :

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

Étape 4 (Facultatif) Demandez à l'appareil de sécurité adaptatif d'envoyer les adresses IP du serveur DNS au client pour la stratégie de groupe.

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

Exemple :

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

Étape 5 (Facultatif) Demandez à l'appareil de sécurité adaptatif d'envoyer les adresses IP du serveur WINS au client pour la stratégie de groupe.

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

Exemple :

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

Étape 6 (Facultatif) Créer un ensemble d'adresses IP.

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

Exemple :

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

Étape 7 (Facultatif) Associez l'ensemble d'adresses IP au profil de connexion (groupe de tunnels).

address-pool *pool_name*

Exemple :

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

Étape 8 Associez le nom d'une stratégie de groupe au profil de connexion (groupe de tunnels).

default-group-policy name

Exemple :

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

Étape 9 Précisez un serveur d'authentification pour vérifier les utilisateurs tentant L2TP sur les connexions IPsec. Si vous souhaitez que l'authentification revienne à l'authentification locale lorsque le serveur n'est pas disponible, ajoutez LOCAL à la fin de la commande.

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

Exemple :

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

Étape 10 Précisez une méthode pour authentifier les utilisateurs tentant des connexions L2TP sur les connexions Eclipse, pour le profil de connexion (groupe de tunnels). Si vous n'utilisez pas l'ASA pour effectuer l'authentification locale et que vous souhaitez revenir à l'authentification locale, ajoutez LOCAL à la fin de la commande.

authentication *auth_type*

Exemple :

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

Étape 11 Définissez la clé prépartagée pour votre profil de connexion (groupe de tunnels).

tunnel-group *tunnel group name* **ipsec-attributes**

Exemple :

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

Étape 12 (Facultatif) Générez des enregistrements de début et de fin de comptabilité AAA pour une session L2TP pour le profil de connexion (groupe de tunnels).

accounting-server-group *aaa_server_group*

Exemple :

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

Étape 13 Configurez l'intervalle (en secondes) entre les messages hello. La plage est de 10 à 300 secondes. L'intervalle par défaut est de 60 secondes.

l2tp tunnel hello *seconds*

Exemple :

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

Étape 14 (Facultatif) Activez la traversée NAT pour que les paquets ESP puissent passer par un ou plusieurs périphériques NAT.

Si vous vous attendez à ce que plusieurs clients L2TP derrière un périphérique NAT tentent des connexions L2TP sur des connexions Eclipse avec l'appareil de sécurité adaptatif, vous devez activer la traversée NAT.

crypto isakmp nat-traversal *seconds*

Pour activer la traversée NAT globalement, vérifiez qu'ISAKMP est activé (vous pouvez l'activer avec la commande **crypto isakmp enable**) en mode de configuration globale, puis utilisez la commande **crypto isakmp nat-traversal**.

Exemple :

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

Étape 15 (Facultatif) Configurez la commutation de groupe de tunnels. L'objectif de la commutation de groupe de tunnels est de donner aux utilisateurs davantage de chances d'établir une connexion VPN lorsqu'ils s'authentifient à l'aide d'un proxy d'authentification. Le groupe de tunnels est synonyme de profil de connexion.

strip-group

strip-realm

Exemple :

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

Étape 16 (Facultatif) Créez un utilisateur avec le nom d'utilisateur **jdoe**, le mot de passe **j!doe1**. L'option mschap spécifie que le mot de passe est converti en Unicode et haché à l'aide de MD4 après sa saisie.

Cette étape est nécessaire uniquement si vous utilisez une base de données d'utilisateurs locale.

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

Exemple :

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

Étape 17 Créez la politique IKE pour la phase 1 et attribuez-y un numéro.

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

Il existe plusieurs paramètres de la politique IKE que vous pouvez configurer. Vous pouvez également spécifier un groupe Diffie-Hellman pour la politique. La politique isakmp est utilisée par l'ASA pour terminer la négociation IKE.

Exemple :

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

Créer des politiques IKE pour répondre aux propositions Windows 7

Les clients Windows 7 L2TP/IPsec envoient plusieurs propositions de politique IKE pour établir une connexion VPN avec l'ASA. Définissez l'une des politiques IKE suivantes pour faciliter les connexions depuis les clients VPN natifs Windows 7.

Suivez la procédure Configuring L2TP over IPsec for ASA. Ajoutez les étapes supplémentaires dans cette tâche pour configurer la politique IKE pour les clients VPN natifs de Windows 7.

Procédure

Étape 1 Affichez les attributs ainsi que le nombre de politiques IKE existantes.

Exemple :

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

Étape 2 Configurez une politique IKE. L'argument number spécifie le numéro de la politique IKE que vous configurez. Ce numéro figurait dans la sortie de la commande **show run crypto ikev1**.

crypto ikev1 policy *nombre*

Étape 3 Définissez la méthode d'authentification que l'ASA utilise pour établir l'identité de chaque homologue IPsec afin d'employer des clés prépartagées.

Exemple :

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

Étape 4 Choisissez une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Pour Windows 7, choisissez **aes** pour AES 128 bits, ou **aes-256**.

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

Étape 5 Choisissez l'algorithme de hachage qui garantit l'intégrité des données. Pour Windows 7, spécifiez **sha** pour l'algorithme SHA-1.

Exemple :

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

Étape 6 Choisissez l'identifiant de groupe Diffie-Hellman. Vous pouvez spécifier 14 pour les types de chiffrement aes et aes-256.

Exemple :

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

Étape 7 Précisez la durée de vie de la SA en secondes. Pour Windows 7, spécifiez 86 400 secondes pour représenter 24 heures.

Exemple :

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

Exemple de configuration pour L2TP sur IPsec

L'exemple suivant montre les commandes de fichier de configuration qui assurent la compatibilité de l'ASA avec un client VPN natif sur n'importe quel système d'exploitation :

```
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
```

Historique des fonctionnalités pour L2TP sur IPsec

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
L2TP sur IPsec	7.2(1)	L2TP sur IPsec permet de déployer et d'utiliser une solution VPN L2TP des services de VPN et de pare-feu IPsec sur une plateforme unique. Le principal avantage de la configuration de L2TP sur IPsec dans un sc d'accès à distance est que les utilisateurs distants peuvent accéder à un un réseau IP public sans passerelle ni ligne dédiée, ce qui permet l'accès depuis pratiquement n'importe quel endroit disposant du réseau télépho commuté (POTS). Un avantage supplémentaire est que la seule exigence pour l'accès au VPN est l'utilisation de Windows avec la mise en réseau Dial-Up Networking (DUN). Aucun logiciel client supplémentaire, tel logiciel client VPN Cisco, n'est requis. Les commandes suivantes ont été introduites ou modifiées : authenticat eap-proxy, authentication ms-chap-v1, authentication ms-chap-v2, auth pap, l2tp tunnel hello, vpn-tunnel-protocol l2tp-ipsec.
Dépréciation des chiffrements IKE/IPsec et des chiffrements d'intégrité/PRF Prise en charge du groupe DH 14 pour IKEv1	9.13(1)	Les chiffrements/intégrité/PRF suivants sont obsolètes et seront suppri la version ultérieure 9.14(1) : • Chiffrement 3DES • Chiffrement DES • Intégrité MD5 Ajout de la prise en charge du groupe DH 14 (par défaut) pour IKEv1. L de commande groupe 2 et groupe 5 sont obsolètes et seront supprimées version ultérieure 9.14(1).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.