# Échange du paquet IKEv2 et élimination des imperfections de niveau de Protocol

## Contenu



# Introduction

Ce document décrit les avantages de la dernière version de l'Échange de clés Internet (IKE) et les différences entre la version 1 et la version 2.

L'IKE est le protocole utilisé pour installer une association de sécurité (SA) dans la suite de protocole IPsec. IKEv2 est la deuxième et dernière version du protocole d'IKE. Adoption pour ce protocole commencé dès 2006. Le besoin et l'intention d'une révision du protocole d'IKE ont été décrits dans l'annexe A de l'*échange de clés Internet (IKE) (IKEv2) Protocol* dans RFC 4306.

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

# Différences entre IKEv1 et IKEv2

Tandis que l'*échange de clés Internet (IKE) (IKEv2) Protocol* dans RFC 4306 décrit en détail les avantages d'IKEv2 au-dessus d'IKEv1, il est important de noter que l'échange entier d'IKE a été révisé. Ce diagramme fournit une comparaison des deux échanges :

Dans IKEv1, il y avait un échange clairement délimité de Phase 1, qui contient six paquets suivis d'un échange de Phase 2 se compose de trois paquets ; l'échange IKEv2 est variable. Au mieux, il peut permuter seulement quatre paquets. Au pis aller, ceci peut grimper jusqu'à l'autant de pendant que 30 paquets (sinon plus), selon la complexité de l'authentification, le nombre d'attributs de Protocole EAP (Extensible Authentication Protocol) utilisés, aussi bien que le nombre de SAS formaient. IKEv2 combine les informations de Phase 2 dans IKEv1 dans l'échange IKE_AUTH, et il s'assure qu'après que l'échange IKE_AUTH soit complet, les deux pairs font déjà construire une SA et prépare pour chiffrer le trafic. Cette SA est seulement construite pour les identités de proxy qui apparient le paquet de déclencheur. N'importe quel trafic ultérieur qui apparie d'autres identités de proxy puis déclenche l'échange CREATE_CHILD_SA, qui est l'équivalent de l'échange de Phase 2 dans IKEv1. Il n'y a aucun mode agressif ou mode principal.

# Phases initiales dans l'échange IKEv2

En effet, IKEv2 a seulement deux phases initiales de négociation :

- Échange IKE_SA_INIT
- Échange IKE_AUTH

## Échange IKE_SA_INIT

IKE_SA_INIT est l'échange initial dans lequel les pairs établissent un canal de sécuriser. Après qu'il se termine l'échange initial, tout permute plus loin est chiffré. Les échanges contiennent seulement deux paquets parce qu'il combine toutes les informations habituellement permutées dans MM1-4 dans IKEv1. En conséquence, le responder est de calcul cher de traiter le paquet IKE_SA_INIT et peut partir pour traiter le premier paquet ; il laisse le protocole ouvert d'attaque DoS des adresses charriées.

Afin de se protéger contre ce genre d'attaque, IKEv2 a un échange facultatif dans IKE_SA_INIT à empêcher contre des attaques de détournement de trafic. Si un certain seuil des sessions inachevées est atteint, le responder ne traite pas le paquet plus loin, mais envoie à la place une réponse au demandeur avec un Témoin. Pour que la session continue, le demandeur doit renvoyer le paquet IKE_SA_INIT et inclure le Témoin qu'il a reçu.

Le demandeur renvoie le paquet initial avec la charge utile de notification du responder qui s'avère que l'échange d'origine n'a pas été charrié. Voici un diagramme d'échange IKE_SA_INIT avec le défi de Témoin :

## Échange IKE_AUTH

Après que l'échange IKE_SA_INIT soit complet, IKEv2 SA est chiffré ; cependant, le pair distant n'a pas été authentifié. L'échange IKE_AUTH est utilisé pour authentifier le pair distant et pour créer premier IPsec SA.

L'échange contient l'ID de Protocole ISAKMP (Internet Security Association and Key Management Protocol) avec une charge utile d'authentification. Le contenu de la charge utile d'authentification dépend de la méthode d'authentification, qui peut être la clé pré-partagée (PSK), les Certificats RSA (RSA-SIG), les Certificats elliptiques d'algorithme de signature numérique de curve (ECDSA-SIG), ou l'EAP. En plus des charges utiles d'authentification, l'échange inclut les charges utiles SA et de sélecteur du trafic qui décrivent IPsec SA à créer.

### De plus défunts échanges IKEv2

#### Échange CREATE_CHILD_SA

Si l'enfant supplémentaire SAS sont priés, ou si IKE SA ou un de l'enfant SAS doit être réintroduit, il remplit la même fonction que l'échange rapide de mode fait dans IKEv1. Suivant les indications du ce diagramme, il y a seulement deux paquets dans cet échange ; cependant, les répétitions d'échange pour chaque rekey ou nouvelle SA :

#### Échange INFORMATIONNEL

Pendant qu'il est dans tous les échanges IKEv2, chaque demande INFORMATIONNELLE d'échange s'attend à une réponse. Trois types de charges utiles peuvent être inclus dans un échange INFORMATIONNEL. Un certain nombre de n'importe quelle combinaison des charges utiles peut être incluse, suivant les indications du ce diagramme :

- La charge utile de notification (n) a été déjà vue en même temps que des Témoins. Il y a plusieurs autres types aussi bien. Ils diffusent l'erreur et les informations d'état, comme ils font dans IKEv1.
- La charge utile d'effacement (d) informe le pair que l'expéditeur a supprimé un ou plusieurs de sa SAS entrante. On s'attend à ce que supprime ces SAS et inclut habituellement le responder les charges utiles d'effacement pour SAS qui correspondent dans l'autre direction dans son message de réponse.
- La charge utile de configuration (CP) est utilisée pour négocier des données de configuration entre les pairs. Une importante utilisation du CP est de demander (demande) et d'assigner (réponse) une adresse sur un réseau protégé par une passerelle de sécurité. Dans le cas typique, un hôte mobile établit un réseau privé virtuel (VPN) avec une passerelle de sécurité sur son réseau domestique et demande qu'il soit donné une adresse IP sur le réseau domestique.**Remarque:** Ceci élimine un des problèmes qui l'utilisation combinée du Layer 2 Tunneling Protocol (L2TP) et IPsec est destiné pour le résoudre.

## Informations connexes

- Debugs ASA IKEv2 pour le site à site VPN avec PSKs TechNote
- ASA IPsec et IKE met au point (mode IKEv1 principal) dépannage de TechNote
- IOS IPSec et IKE met au point - Mode IKEv1 principal dépannant TechNote
- ASA IPSec et IKE met au point - IKEv1 mode agressif TechNote
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Téléchargements logiciels de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Négociation IPSec/Protocoles IKE

- Cisco IOS Firewall
- Logiciel Cisco IOS
- Secure Shell (SSH)
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems