Échange de paquets IKEv2 et débogage au niveau du protocole

Contenu

Introduction

Ce document décrit les avantages de la dernière version d'Internet Key Exchange (IKE) et les différences entre les versions 1 et 2.

IKE est le protocole utilisé pour configurer une association de sécurité (SA) dans la suite de protocoles IPsec. IKEv2 est la deuxième et dernière version du protocole IKE. L'adoption de ce protocole a commencé dès 2006. La nécessité et l'intention d'une révision du protocole IKE ont été décrites à l'annexe A du *protocole IKEv2 (Internet Key Exchange)* dans la RFC 4306.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

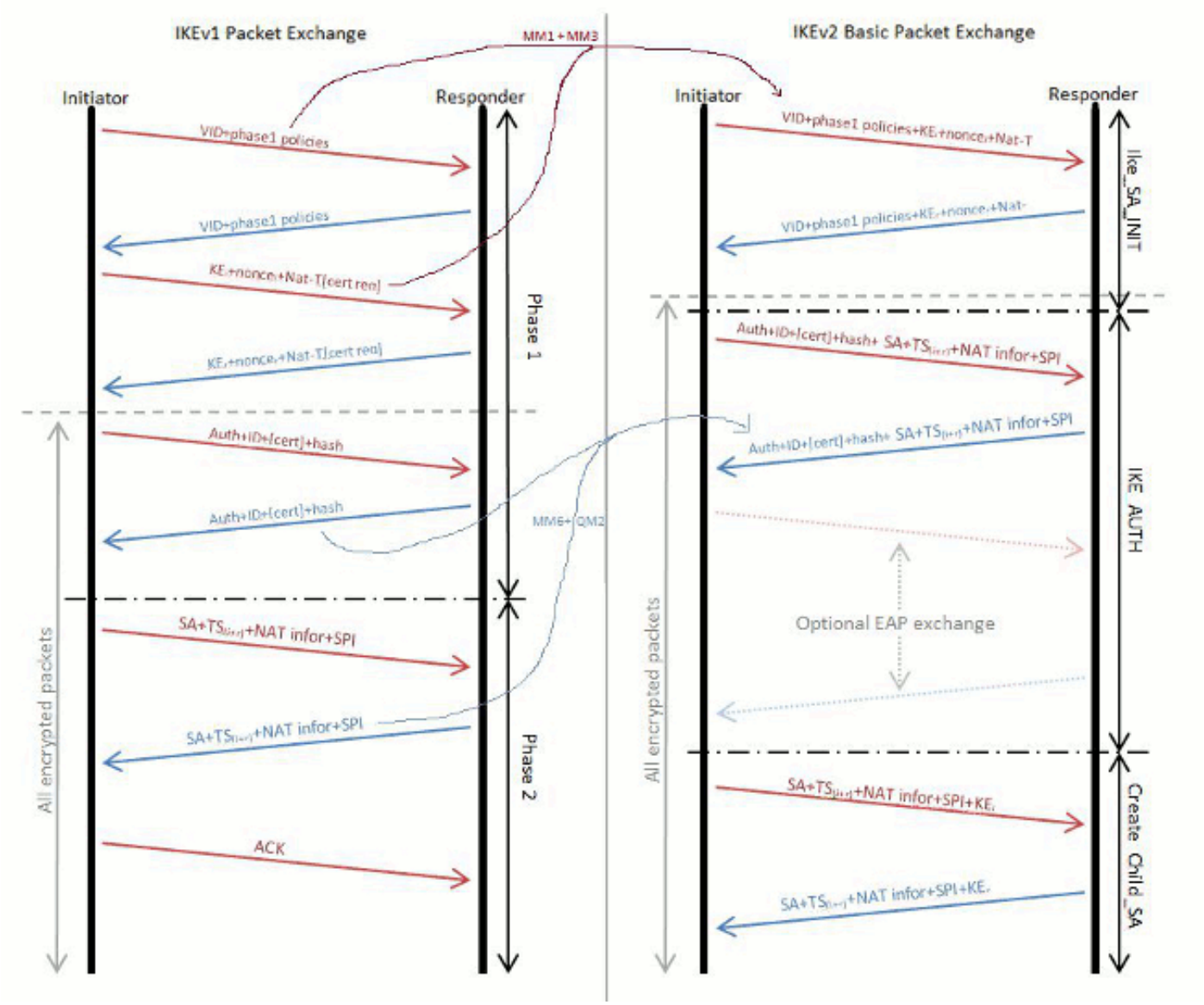
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Alors que *le protocole IKEv2 (Internet Key Exchange)* dans la RFC 4306 décrit en détail les avantages d'IKEv2 par rapport à IKEv1, il est important de noter que l'ensemble de l'échange IKE a été remanié. Ce diagramme fournit une comparaison des deux échanges :



Dans IKEv1, il y a eu un échange de phase 1 clairement délimité, qui contient six paquets suivis d'un échange de phase 2 est composé de trois paquets ; l'échange IKEv2 est variable. Au mieux, il peut échanger jusqu'à quatre paquets. Au pire, cela peut augmenter jusqu'à 30 paquets (voire plus), selon la complexité de l'authentification, le nombre d'attributs EAP (Extensible Authentication Protocol) utilisés, ainsi que le nombre de SA formées. IKEv2 combine les informations de phase 2 dans IKEv1 dans l'échange IKE_AUTH et garantit qu'une fois l'échange IKE_AUTH terminé, les deux homologues ont déjà une SA créée et prête à chiffrer le trafic. Cette SA est créée uniquement pour les identités proxy qui correspondent au paquet de déclenchement. Tout trafic ultérieur qui correspond à d'autres identités proxy déclenche alors l'échange CREATE_CHILD_SA, qui est l'équivalent de l'échange de phase 2 dans IKEv1. Il n'existe ni mode agressif ni mode principal.

Phases initiales dans IKEv2 Exchange

En effet, IKEv2 ne comporte que deux phases initiales de négociation :

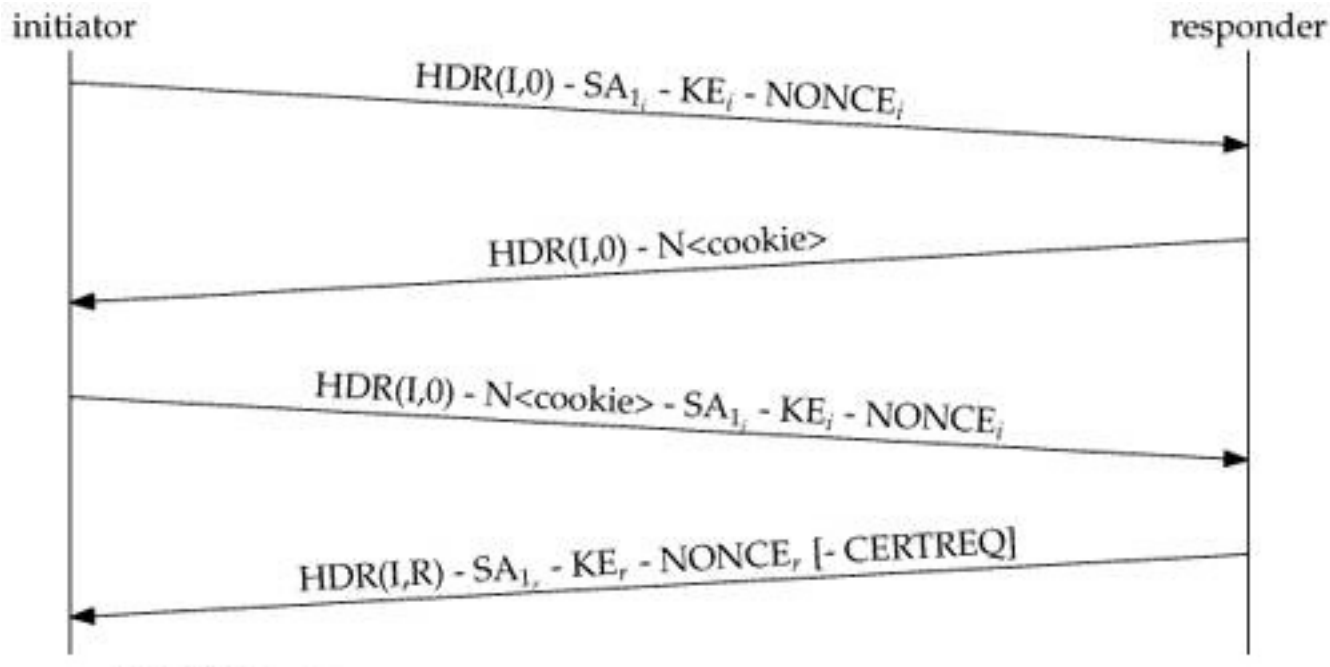
- Échange IKE_SA_INIT
- Échange IKE_AUTH

Échange IKE_SA_INIT

IKE_SA_INIT est l'échange initial dans lequel les homologues établissent un canal sécurisé. Une fois l'échange initial terminé, tous les autres échanges sont chiffrés. Les échanges ne contiennent que deux paquets, car ils combinent toutes les informations généralement échangées dans MM1-4 dans IKEv1. En conséquence, le répondeur est coûteux en calcul pour traiter le paquet IKE_SA_INIT et peut laisser traiter le premier paquet ; il laisse le protocole ouvert à une attaque DOS à partir d'adresses usurpées.

Afin de se protéger de ce type d'attaque, IKEv2 dispose d'un échange optionnel au sein d'IKE_SA_INIT pour empêcher les attaques de mystification. Si un certain seuil de sessions incomplètes est atteint, le répondeur ne traite pas le paquet plus loin, mais envoie une réponse à l'initiateur avec un cookie. Pour que la session continue, l'initiateur doit renvoyer le paquet IKE_SA_INIT et inclure le cookie reçu.

L'initiateur renvoie le paquet initial avec la charge utile Notify du répondeur, ce qui prouve que l'échange initial n'a pas été usurpé. Voici un diagramme de l'échange IKE_SA_INIT avec le défi des cookies :



Échange IKE_AUTH

Une fois l'échange IKE_SA_INIT terminé, la SA IKEv2 est chiffrée ; cependant, l'homologue distant n'a pas été authentifié. L'échange IKE_AUTH sert à authentifier l'homologue distant et à créer la première SA IPsec.

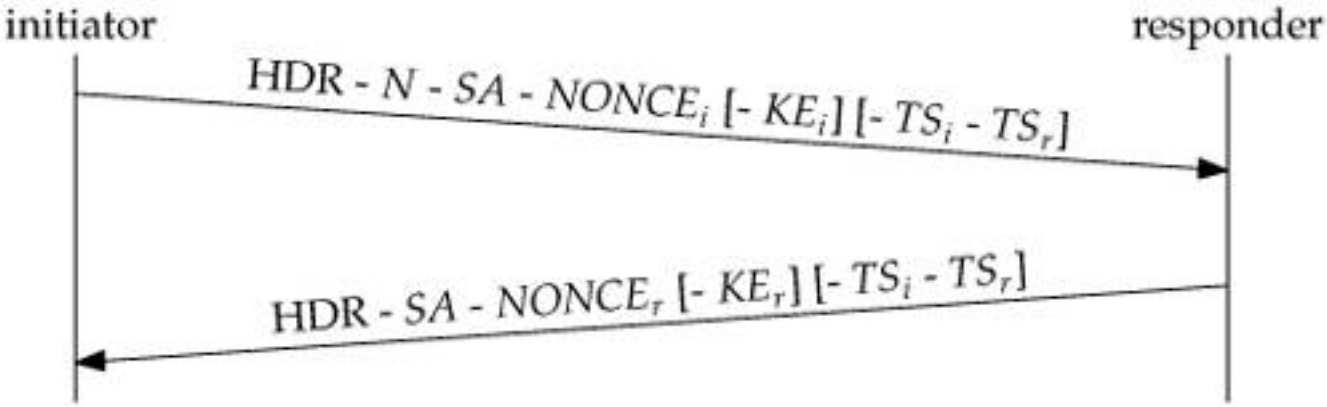
L'échange contient l'ID ISAKMP (Internet Security Association and Key Management Protocol) ainsi qu'une charge utile d'authentification. Le contenu de la charge utile d'authentification dépend de la méthode d'authentification, qui peut être Pre-Shared Key (PSK), RSA Certificats (RSA-SIG),

Elliptic Curve Digital Signature Algorithm Certificats (ECDSA-SIG) ou EAP. Outre les charges utiles d'authentification, l'échange inclut les charges utiles SA et Traffic Selector qui décrivent la SA IPsec à créer.

Échanges IKEv2 ultérieurs

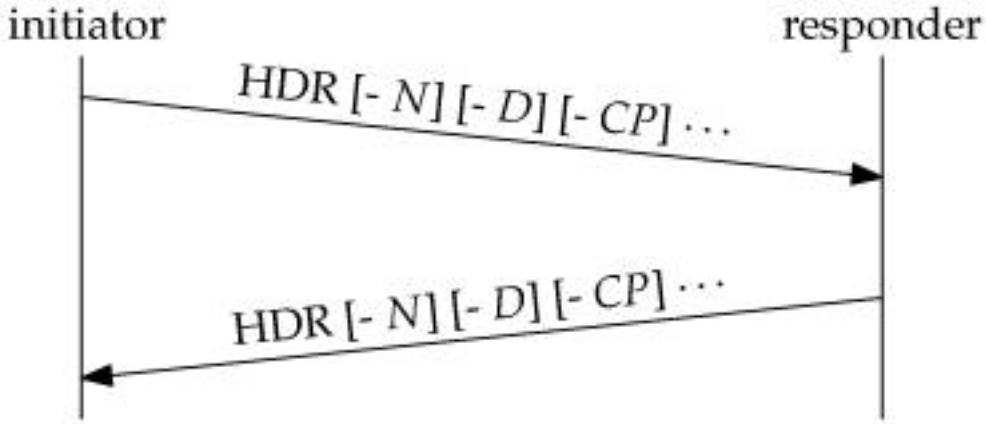
Échange CREATE_CHILD_SA

Si des SA enfant supplémentaires sont nécessaires, ou si l'SA IKE ou l'une des SA enfant doit être recréée, elle sert la même fonction que l'échange en mode rapide dans IKEv1. Comme le montre ce schéma, il n'y a que deux paquets dans cet échange ; cependant, l'échange se répète pour chaque nouvelle SA ou nouvelle SA :



Échange d'informations

Comme dans tous les échanges IKEv2, chaque requête d'échange d'informations attend une réponse. Trois types de charges utiles peuvent être inclus dans un échange d'informations. N'importe quelle combinaison de charges utiles peut être incluse, comme illustré dans ce schéma :



- La charge utile Notify (N) a déjà été vue en conjonction avec les cookies. Il en existe plusieurs autres. Ils transportent des informations d'erreur et d'état, comme dans IKEv1.
- La charge utile Supprimer (D) informe l'homologue que l'expéditeur a supprimé une ou plusieurs de ses SA entrantes. Le répondeur est censé supprimer ces SA et inclut généralement les charges utiles Supprimer pour les SA qui correspondent dans l'autre direction dans son message de réponse.
- La charge utile de configuration (CP) est utilisée pour négocier les données de configuration

entre les homologues. L’une des utilisations importantes du protocole CP consiste à demander (demander) et à attribuer (réponse) une adresse sur un réseau protégé par une passerelle de sécurité. En règle générale, un hôte mobile établit un réseau privé virtuel (VPN) avec une passerelle de sécurité sur son réseau domestique et demande qu'une adresse IP lui soit attribuée sur le réseau domestique.**Remarque :** Ceci élimine l'un des problèmes que l'utilisation combinée du protocole L2TP (Layer 2 Tunneling Protocol) et d'IPsec est censée résoudre.

Informations connexes

- Débogues ASA IKEv2 pour VPN site à site avec PSKs TechNote
- Dépannage des débogages ASA IPsec et IKE (IKEv1 Main Mode) TechNote
- Débogues IOS IPSec et IKE - IKEv1 Main Mode Trouver TechNote
- Débogues ASA IPSec et IKE - IKEv1 Aggressive Mode TechNote
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Téléchargements de logiciels des appareils de sécurité adaptatifs 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