Debuggen von IKEv2-Paketen und Protokollebene

Inhalt

Einführung

Dieses Dokument beschreibt die Vorteile der neuesten Version von Internet Key Exchange (IKE) und die Unterschiede zwischen Version 1 und Version 2.

IKE ist das Protokoll zum Einrichten einer Sicherheitszuordnung (Security Association, SA) in der IPsec-Protokoll-Suite. IKEv2 ist die zweite und neueste Version des IKE-Protokolls. Die Annahme dieses Protokolls begann bereits 2006. Die Notwendigkeit und der Zweck einer Überarbeitung des IKE-Protokolls wurden in Anhang A des *IKEv2-Protokolls* in RFC 4306 beschrieben.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

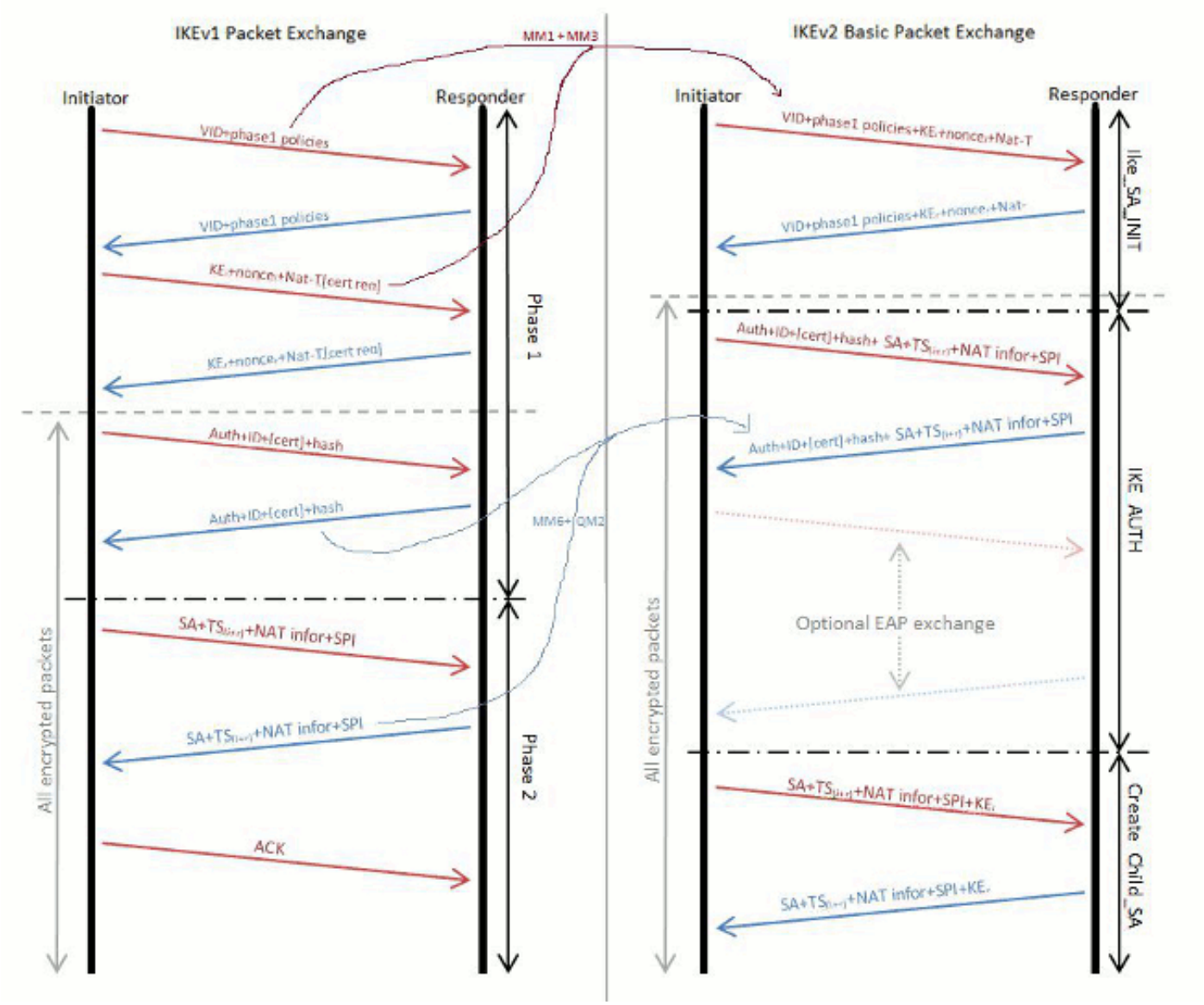
Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Unterschiede zwischen IKEv1 und IKEv2

Während das *IKEv2-Protokoll* in RFC 4306 die Vorteile von IKEv2 gegenüber IKEv1 ausführlich beschreibt, ist zu beachten, dass der gesamte IKE-Austausch überholt wurde. Dieses Diagramm bietet einen Vergleich der beiden Austauschvorgänge:



In IKEv1 gab es einen klar abgegrenzten Phase-1-Austausch, der sechs Pakete enthält, gefolgt von einem Phase-2-Austausch, der aus drei Paketen besteht. Der IKEv2-Austausch ist variabel. Bestenfalls können maximal vier Pakete ausgetauscht werden. Je nach Komplexität der Authentifizierung, der Anzahl der verwendeten EAP-Attribute und der Anzahl der erstellten SAs kann dies auf höchstens 30 Pakete (wenn nicht sogar mehr) steigen. IKEv2 kombiniert die Phase-2-Informationen in IKEv1 in den IKE_AUTH-Austausch und stellt sicher, dass nach Abschluss des IKE_AUTH-Austauschs beide Peers bereits über einen SA verfügen, der zur Verschlüsselung des Datenverkehrs bereit ist. Diese SA ist nur für die Proxy-Identitäten konzipiert, die mit dem Triggerpaket übereinstimmen. Jeder nachfolgende Datenverkehr, der mit anderen Proxy-Identitäten übereinstimmt, löst dann den CREATE_CHILD_SA-Austausch aus, der der Phase-2-Austausch in IKEv1 entspricht. Es gibt keinen aggressiven Modus oder Hauptmodus.

Erste Phasen in IKEv2 Exchange

IKEv2 verfügt im Prinzip nur über zwei anfängliche Verhandlungsphasen:

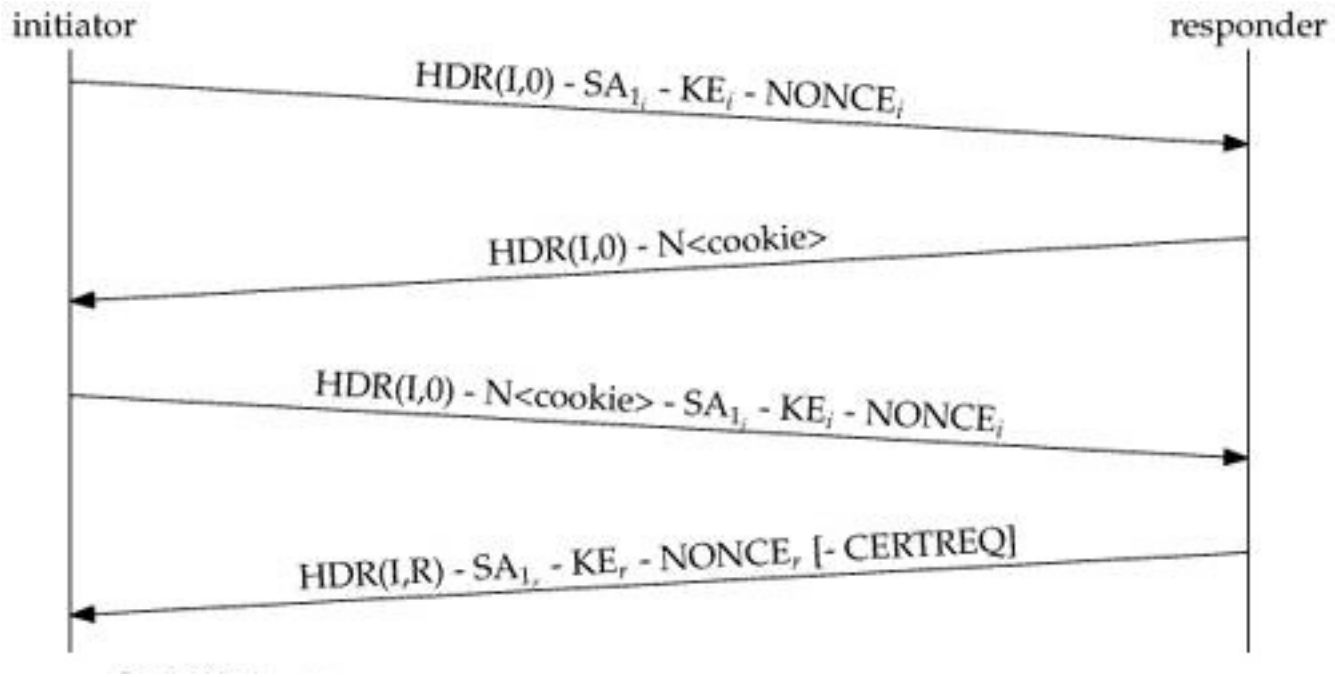
- IKE_SA_INIT-Exchange
- IKE_AUTH-Exchange

IKE_SA_INIT-Exchange

IKE_SA_INIT ist der erste Austausch, bei dem die Peers einen sicheren Kanal einrichten. Nach Abschluss des ersten Austauschs werden alle weiteren Austauschvorgänge verschlüsselt. Der Datenaustausch enthält nur zwei Pakete, da er alle Informationen enthält, die normalerweise in MM1-4 in IKEv1 ausgetauscht werden. Das Ergebnis ist, dass der Responder das IKE_SA_INIT-Paket rechnerisch verarbeiten muss und das erste Paket verarbeiten kann. es lässt das Protokoll einem DOS-Angriff von gefälschten Adressen offen.

Zum Schutz vor solchen Angriffen verfügt IKEv2 über einen optionalen Austausch innerhalb von IKE_SA_INIT, um Spoofing-Angriffe zu verhindern. Wenn ein bestimmter Grenzwert für unvollständige Sitzungen erreicht wird, verarbeitet der Responder das Paket nicht weiter, sondern sendet stattdessen eine Antwort mit einem Cookie an den Initiator. Damit die Sitzung fortgesetzt werden kann, muss der Initiator das IKE_SA_INIT-Paket erneut senden und das von ihm empfangene Cookie einfügen.

Der Initiator sendet das ursprüngliche Paket zusammen mit der Benachrichtigungs-Payload vom Responder erneut, um zu belegen, dass der ursprüngliche Austausch nicht gesaugt wurde. Im folgenden Diagramm wird der Austausch IKE_SA_INIT mit Cookie-Herausforderung dargestellt:



IKE_AUTH-Exchange

Nach Abschluss des IKE_SA_INIT-Austauschs wird die IKEv2 SA verschlüsselt. Der Remote-Peer wurde jedoch nicht authentifiziert. Der IKE_AUTH-Austausch dient zur Authentifizierung des Remote-Peers und zur Erstellung der ersten IPsec-SA.

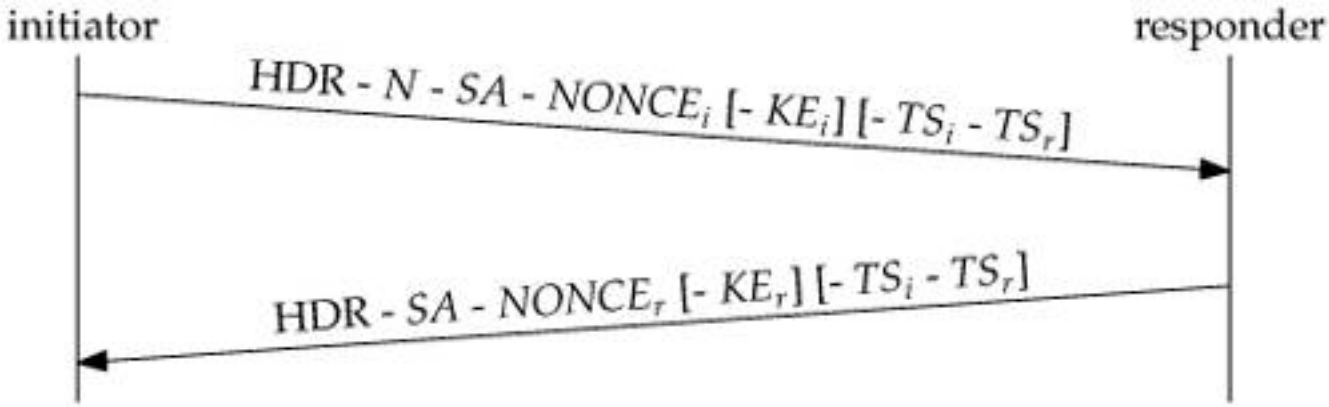
Der Austausch enthält die ISAKMP-ID (Internet Security Association and Key Management Protocol) sowie eine Authentifizierungs-Payload. Der Inhalt der Authentifizierungs-Payload hängt

von der Authentifizierungsmethode ab, die Pre-Shared Key (PSK), RSA-Zertifikate (RSA-SIG), Elliptic Curve Digital Signature Algorithm Certificates (ECDSA-SIG) oder EAP sein kann. Zusätzlich zu den Authentifizierungs-Payloads enthält der Austausch die SA- und Traffic Selector-Payloads, die die zu erstellende IPsec SA beschreiben.

Spätere IKEv2-Austausche

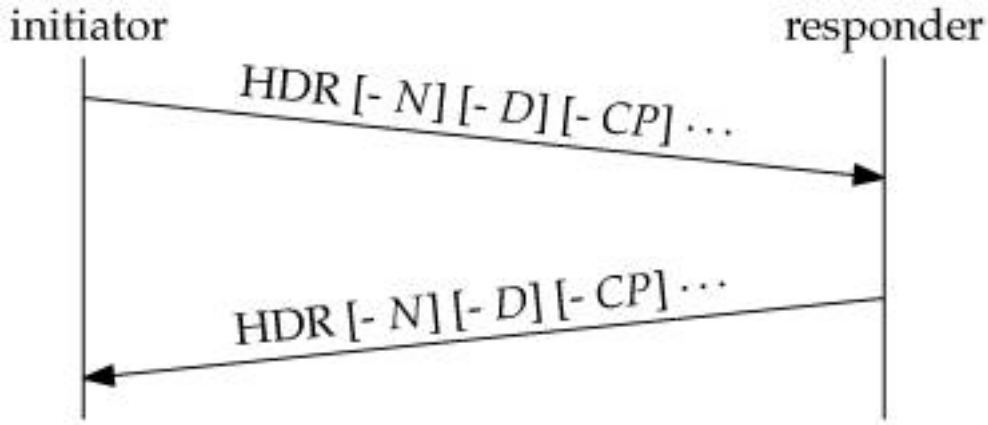
CREATE_CHILD_SA Exchange

Wenn zusätzliche untergeordnete SAs erforderlich sind oder wenn die IKE SA oder eine der untergeordneten SAs neu codiert werden muss, erfüllt sie dieselbe Funktion wie der Quick-Mode-Austausch in IKEv1. Wie in diesem Diagramm gezeigt, befinden sich in diesem Austausch nur zwei Pakete. Der Austausch wiederholt sich jedoch für jeden Schlüssel oder jede neue SA:



Informationsaustausch

Wie bei allen IKEv2-Austauschen erwartet jede Anforderung des Informationsaustauschs eine Antwort. Drei Arten von Payloads können in einem INFORMATIONALEN Austausch enthalten sein. Es können beliebig viele verschiedene Kombinationen von Payloads enthalten werden, wie im folgenden Diagramm gezeigt:



- Die Notify Payload (N) wurde bereits in Verbindung mit Cookies erkannt. Es gibt auch mehrere andere Typen. Sie enthalten Fehler- und Statusinformationen wie in IKEv1.
- Die Delete Payload (D) informiert den Peer, dass der Absender eine oder mehrere seiner eingehenden SAs gelöscht hat. Der Responder muss diese SAs löschen und normalerweise die Payloads löschen, die für die SAs in der anderen Richtung in der Antwortnachricht übereinstimmen.

- Die Configuration Payload (CP) dient zur Aushandlung von Konfigurationsdaten zwischen den Peers. Ein wichtiger Zweck des CP besteht darin, eine Adresse in einem Netzwerk anzufordern (anzufordern) und zuzuweisen (zu antworten), das durch ein Sicherheits-Gateway geschützt ist. In der Regel richtet ein mobiler Host ein Virtual Private Network (VPN) mit einem Sicherheits-Gateway im Heimnetzwerk ein und fordert, dass ihm eine IP-Adresse im Heimnetzwerk zugewiesen wird.**Hinweis:** Dadurch entfällt eines der Probleme, die durch die gleichzeitige Verwendung von Layer 2 Tunneling Protocol (L2TP) und IPsec gelöst werden sollen.

Zugehörige Informationen

- ASA IKEv2-Debugger für Site-to-Site-VPN mit PSKs - Technische Anmerkung
- ASA IPsec- und IKE-Debug (IKEv1-Hauptmodus) Fehlerbehebung TechHinweis
- IOS IPSec- und IKE-Debug - IKEv1 Main Mode Troubleshooting TechNote
- ASA IPSec- und IKE-Debug - IKEv1 Aggressive Mode TechNote
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Software-Downloads für Cisco Adaptive Security Appliances der Serie ASA 5500
- IPSec-Aushandlung/IKE-Protokolle
- Cisco IOS-Firewall
- Cisco IOS-Software
- Secure Shell (SSH)
- IPSec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems