IKEv2封包交換和通訊協定層級偵錯

目錄

簡介

本文檔介紹最新版本的Internet Key Exchange(IKE)的優點以及版本1和版本2之間的差異。

IKE是用於在IPsec協定簇中設定安全關聯(SA)的協定。IKEv2是IKE協定的第二個也是最新版本。該協定早在2006年開始採用。RFC 4306的*Internet Key Exchange(IKEv2)協定的附錄A中介紹了對IKE協定進行大修*的必要性和意圖。

必要條件

需求

本文件沒有特定需求。

採用元件

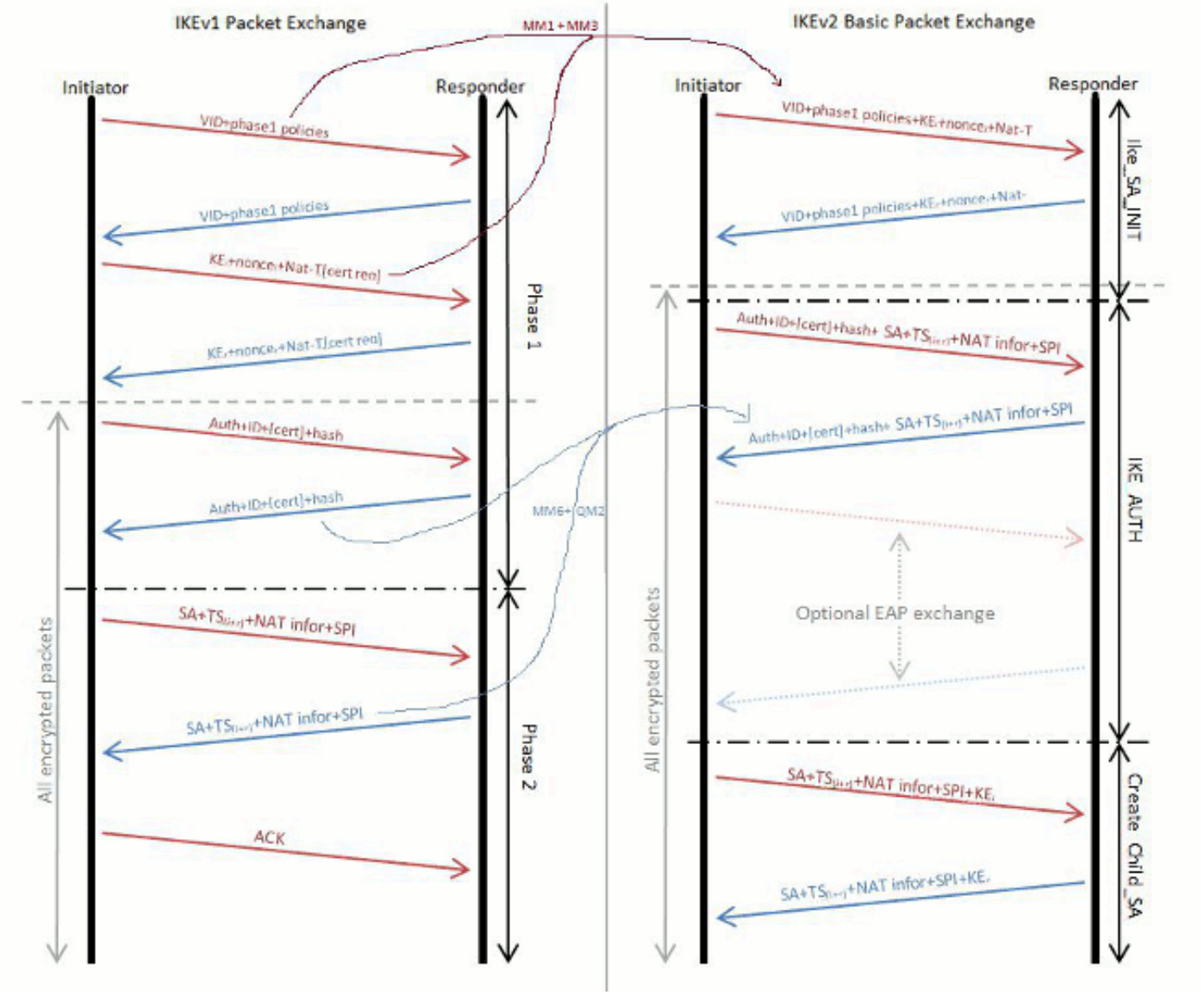
本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IKEv1和IKEv2之間的差異

雖然RFC 4306中的*網際網路金鑰交換(IKEv2)通訊協定*詳細描述了IKEv2相對於IKEv1的優勢，但必須注意的是，整個IKE交換已經過全面調整。此圖提供兩種交換的比較：



在IKEv1中，有一個明確劃分的第一階段交換，其中包含六個資料包，然後由三個資料包組成的第二階段交換；ikev2交換是可變的。最多只能交換四個資料包。最差情況下，根據身份驗證的複雜性、使用的可擴展身份驗證協定(EAP)屬性數量以及形成的SA數量，這會增加多達30個資料包（甚至更多）。IKEv2將IKEv1中的第2階段資訊合併到IKE_AUTH交換中，並確保在IKE_AUTH交換完成之後，兩個對等體已建立一個SA，並且已準備好加密流量。此SA僅針對與觸發資料包匹配的代理身份而構建。隨後匹配其他代理標識的任何後續流量都會觸發CREATE_CHILD_SA交換，該交換相當於IKEv1中的第2階段。沒有主動模式或主模式。

IKEv2交換的初始階段

實際上，IKEv2隻有兩個交涉的初始階段：

- IKE_SA_INIT交換
- IKE_AUTH交換

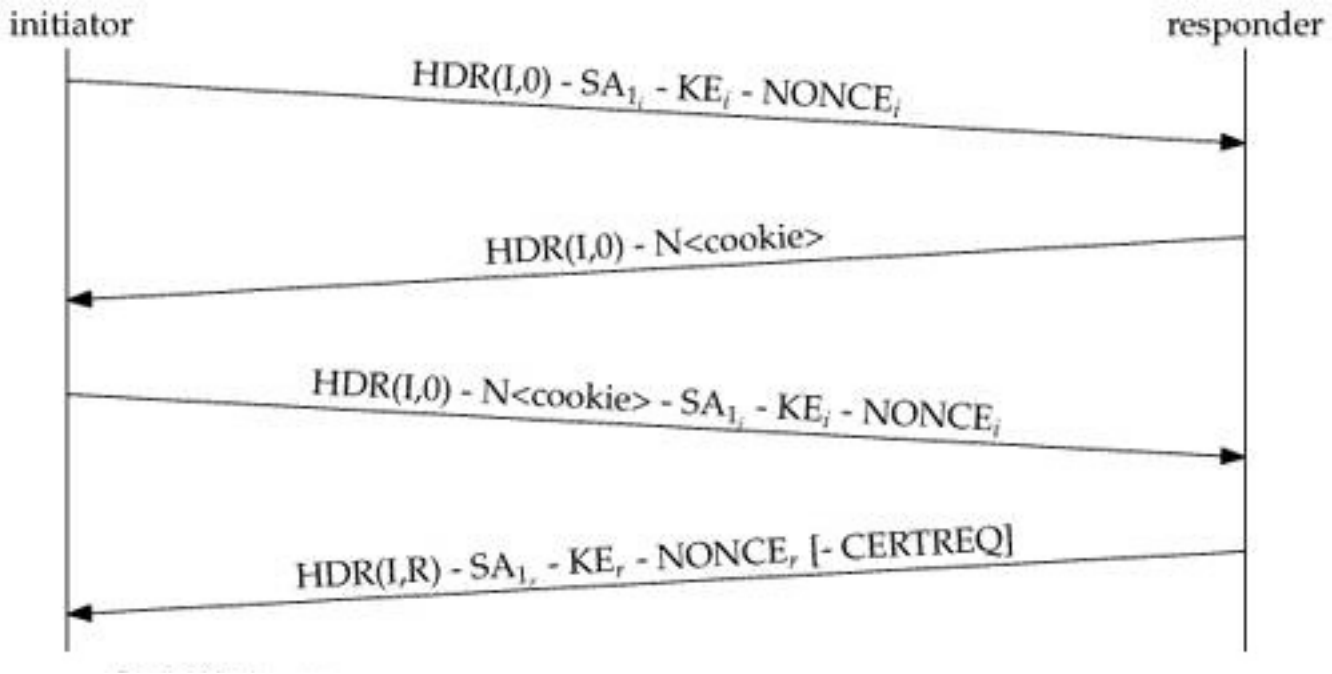
IKE_SA_INIT交換

IKE_SA_INIT是對等體建立安全通道的初始交換。完成初始交換後，所有進一步的交換均被加密。交換僅包含兩個資料包，因為它組合了IKEv1中通常以MM1-4形式交換的所有資訊。因此，響應方處理IKE_SA_INIT資料包的計算成本很高，並且可以離開處理第一個資料包；它使協定從偽裝地址

對DOS攻擊開放。

為了防範此類攻擊，IKEv2在IKE_SA_INIT內有一個可選的交換以防止欺騙攻擊。如果達到不完整會話的某個閾值，響應方不會進一步處理資料包，而是使用cookie向發起方傳送響應。要使會話繼續，發起方必須重新傳送IKE_SA_INIT資料包並包括收到的cookie。

發起方重新傳送初始資料包以及響應方發出的通知負載，以證明原始交換未被偽裝。以下是具有cookie質詢的IKE_SA_INIT交換的圖表：



IKE_AUTH交換

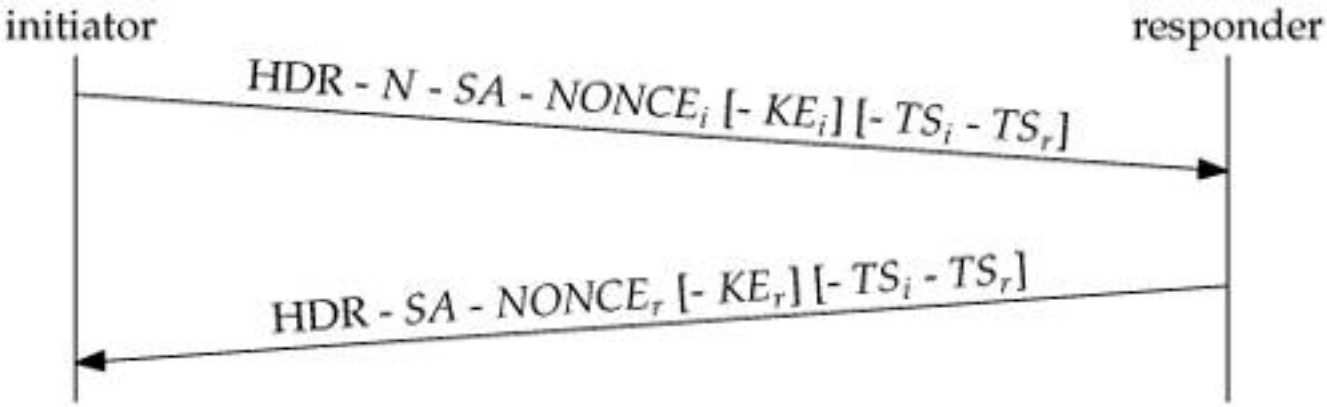
IKE_SA_INIT交換完成後，IKEv2 SA會加密；但是，遠端對等體尚未通過身份驗證。IKE_AUTH交換用於驗證遠端對等體並建立第一個IPsec SA。

交換包含網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)ID以及驗證負載。身份驗證負載的內容取決於身份驗證方法，可以是預共用金鑰(PSK)、RSA證書(RSA-SIG)、橢圓曲線數位簽章演算法證書(ECDSA-SIG)或EAP。除了身份驗證負載之外，交換還包括描述要建立的IPsec SA的SA和流量選擇器負載。

更高版本的IKEv2交換

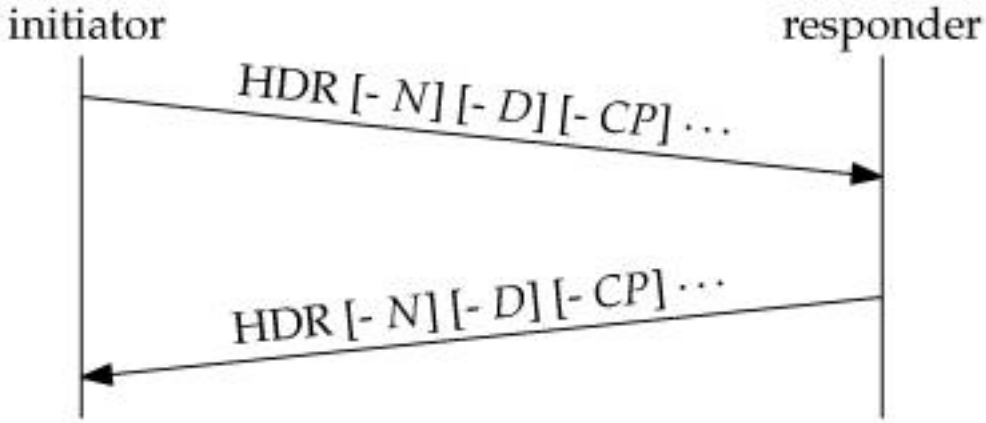
CREATE_CHILD_SA Exchange

如果需要額外的子SA，或者需要重新鍵入IKE SA或其中一個子SA，則其功能與Quick mode exchange在IKEv1中執行的功能相同。如下圖所示，此交換中只有兩個資料包；但是，對於每個重新生成金鑰或新SA，交換會重複：



資訊交換

正如在所有IKEv2交換中一樣，每個INFORMATIONAL Exchange請求都需要響應。資訊交換中可以包含三種型別的負載。可以包含任意數量的任意負載組合，如下圖所示：



- 通知負載(N)已經與cookie一起看到。也有幾種其他型別。它們帶有錯誤和狀態資訊，就像在IKEv1中一樣。
- 刪除負載(D)通知對等體，傳送方已刪除其傳入SA中的一個或多個地址。響應方應刪除這些SA，並且通常在其響應消息中包含在另一個方向對應的SA的刪除負載。
- 配置負載(CP)用於在對等體之間協商配置資料。CP的一個重要用途是在受安全網關保護的網路上請求（請求）和分配（響應）地址。在典型情況下，移動主機在其家鄉網路上建立具有安全網關的虛擬專用網路(VPN)，並請求向其提供家鄉網路上的IP地址。**注意**：這樣可以消除結合使用第2層通道通訊協定(L2TP)和IPsec所要解決的問題之一。

相關資訊

- 適用於採用PSK的站點到站點VPN的ASA IKEv2調試技術說明
- ASA IPsec和IKE調試（IKEv1主模式）故障排除技術說明
- IOS IPSec和IKE調試 — IKEv1主模式故障排除技術說明
- ASA IPSec和IKE調試 — IKEv1主動模式技術說明
- Cisco ASA 5500系列調適型安全裝置
- Cisco ASA 5500系列自適應安全裝置軟體下載
- IPSec 協商/IKE 通訊協定
- Cisco IOS 防火牆
- Cisco IOS軟體
- 安全殼層 (SSH)

- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems