IKEv2数据包交换和协议级调试

目录

简介

本文档介绍最新版本的互联网密钥交换(IKE)的优点以及版本1和版本2之间的差异。

IKE是用于在IPsec协议簇中设置安全关联(SA)的协议。IKEv2是IKE协议的第二个和最新版本。此协议最早于2006年开始采用。RFC 4306中的Internet密钥交换(IKEv2)协议附录A*中介绍了全面检查IKE协议的需*要和意图。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

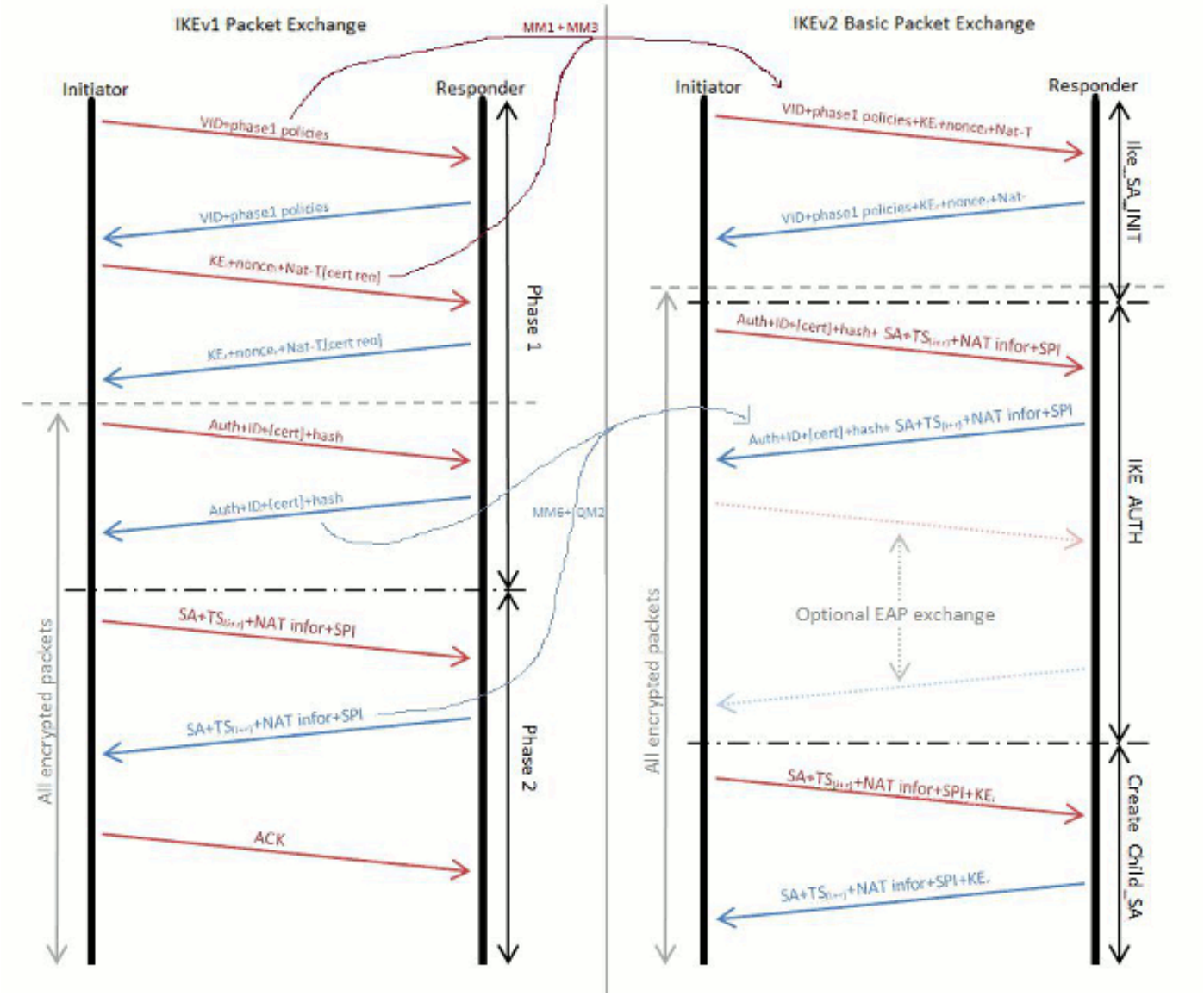
本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

IKEv1和IKEv2之间的区别

虽*然RFC 4306中的Internet密钥交换(IKEv2)协*议详细描述了IKEv2相对于IKEv1的优势，但必须注意的是，整个IKE交换已进行了全面修改。此图提供了两种交换的比较：



在IKEv1中，有一个明确分界的第1阶段交换，包含6个数据包，然后第2阶段交换由3个数据包组成；IKEv2交换是可变的。最多只能交换四个数据包。最坏情况下，这可能会增加多达30个数据包（如果不是更多），具体取决于身份验证的复杂性、使用的可扩展身份验证协议(EAP)属性的数量以及形成的SA的数量。IKEv2将IKEv1中的第2阶段信息合并到IKE_AUTH交换中，并确保在IKE_AUTH交换完成后，两个对等体已经构建了一个SA并准备好加密流量。此SA仅针对与触发数据包匹配的代理身份而构建。任何与其他代理身份匹配的后续流量都会触发CREATE_CHILD_SA交换，该交换相当于IKEv1中的第2阶段交换。没有主动模式或主模式。

IKEv2交换的初始阶段

实际上，IKEv2只有两个初始协商阶段：

- IKE_SA_INIT交换
- IKE_AUTH交换

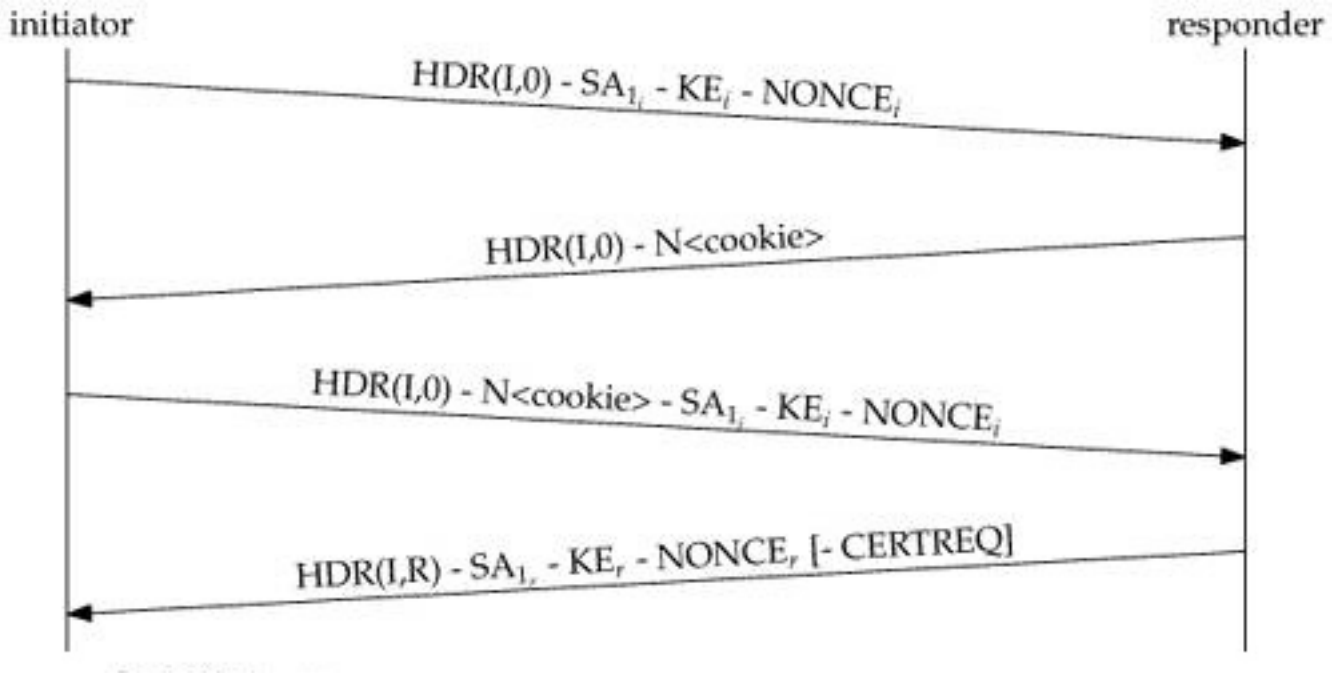
IKE_SA_INIT交换

IKE_SA_INIT是对等体在其中建立安全信道的初始交换。完成初始交换后，所有进一步的交换都将加密。交换仅包含两个数据包，因为它将IKEv1中通常在MM1-4中交换的所有信息合并在一起。因此，响应方处理IKE_SA_INIT数据包的计算成本很高，可以离开以处理第一个数据包；它使协议对

欺骗地址的DOS攻击保持开放。

为了防止此类攻击，IKEv2在IKE_SA_INIT内有一个可选交换，以防止欺骗攻击。如果达到不完整会话的特定阈值，响应方不会进一步处理数据包，而是使用cookie向发起方发送响应。要使会话继续，发起方必须重新发送IKE_SA_INIT数据包并包括其收到的cookie。

发起方重新发送初始数据包以及响应方的通知负载，证明原始交换未欺骗。下面是IKE_SA_INIT交换与cookie质询的图：



IKE_AUTH交换

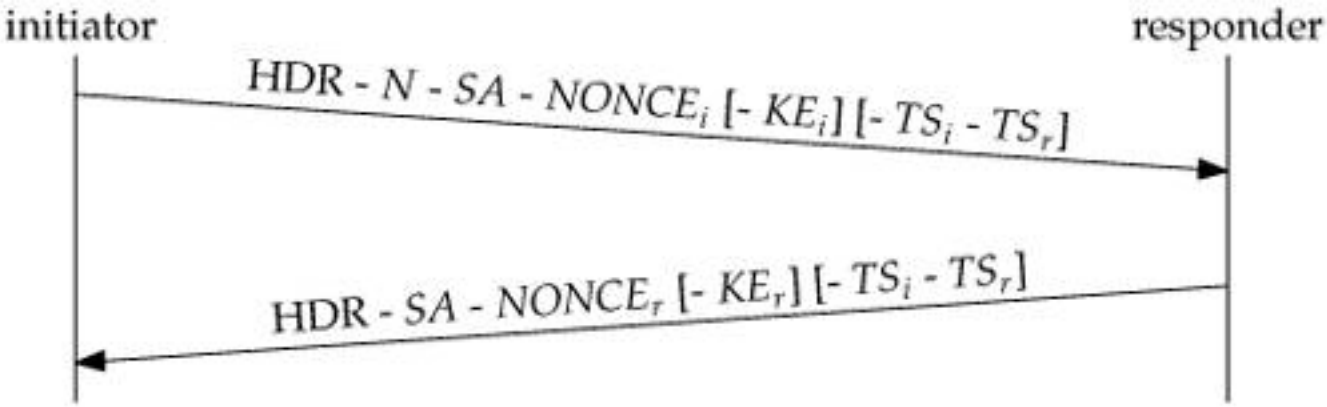
在IKE_SA_INIT交换完成后，IKEv2 SA被加密；但是，远程对等体尚未通过身份验证。
IKE_AUTH交换用于对远程对等体进行身份验证并创建第一个IPsec SA。

交换包含互联网安全关联和密钥管理协议(ISAKMP)ID以及身份验证负载。身份验证负载的内容取决于身份验证方法，身份验证方法可以是预共享密钥(PSK)、RSA证书(RSA-SIG)、椭圆曲线数字签名算法证书(ECDSA-SIG)或EAP。除身份验证负载外，交换还包括描述要创建的IPsec SA的SA和流量选择器负载。

更新IKEv2交换

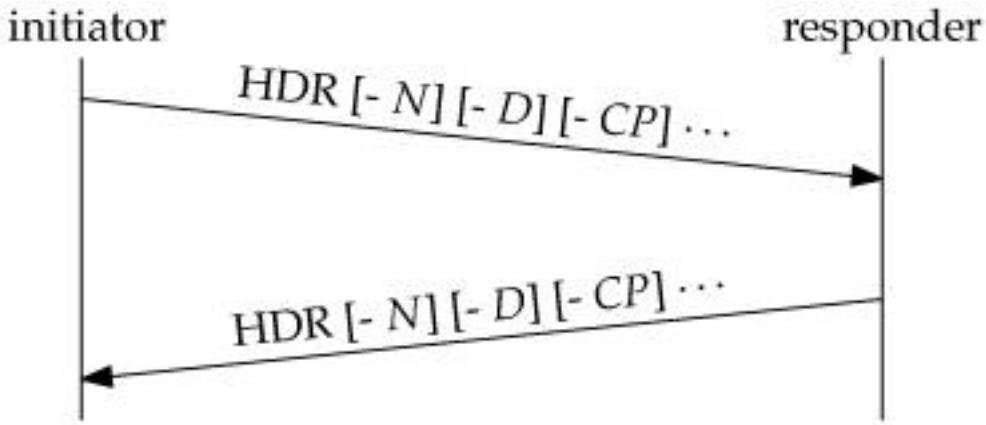
CREATE_CHILD_SA交换

如果需要其他子SA，或者如果需要重新键入IKE SA或其中一个子SA，则它的功能与快速模式交换在IKEv1中的功能相同。如下图所示，此交换中只有两个数据包；但是，每重新生成密钥或新SA都会重复交换：



信息交换

由于它在所有IKEv2交换中，每个信息交换请求都需要响应。信息交换中可包含三种负载类型。可以包括任意数量的负载组合，如下图所示：



- 已将通知负载(N)与cookie一起查看。还有其他几种类型。它们会像在IKEv1中一样传送错误和状态信息。
- 删除负载(D)通知对等体发送方已删除一个或多个传入SA。响应方应删除这些SA，并且通常在响应消息中包括在另一方向对应的SA的删除负载。
- 配置负载(CP)用于在对等体之间协商配置数据。CP的一个重要用途是请求（请求）和在受安全网关保护的网络上分配（响应）地址。在典型情况下，移动主机在其家庭网络上建立具有安全网关的虚拟专用网络(VPN)，并请求在家庭网络上为其分配IP地址。**注意**：这可消除第2层隧道协议(L2TP)和IPsec的组合使用所要解决的问题之一。

相关信息

- 使用PSK的站点到站点VPN的ASA IKEv2调试技术说明
- ASA IPsec和IKE调试（IKEv1主模式）故障排除技术说明
- IOS IPSec和IKE调试 — IKEv1主模式故障排除技术说明
- ASA IPSec和IKE调试 — IKEv1主动模式技术说明
- Cisco ASA 5500 系列自适应安全设备
- Cisco ASA 5500系列自适应安全设备软件下载
- IPsec 协商/IKE 协议
- Cisco IOS 防火墙
- Cisco IOS 软件
- Secure Shell (SSH)

- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems