IKEv2信息包交换和协议级调试

目录

简介

本文描述Internet Key Exchange (IKE)新版本的优点和在版本1和版本2之间的区别。

IKE是用于的协议设置安全关联(SA)在IPSec协议套件。IKEv2是IKE协议的第二和新版本。此协议的采用开始早在2006年。IKE协议的检修的需要和目的在*互联网密钥交换(IKEv2)协*议附录A描述在RFC 4306的。

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。

在IKEv1和IKEv2之间的区别

当在RFC 4306的*互联网密钥交换(IKEv2)时协*议在了不起的详细信息描述IKEv2优点在IKEv1的，请注意整个IKE交换被翻修了。此图表提供两交换的比较：

在IKEv1中，有清楚地被标定的阶段1交换，包含第2阶段交换跟随的六数据包由三数据包制成;IKEv2交换可变。最好，它能交换只有四数据包。在最坏情况下，这能增加到多达30数据包(如果不是更多)，根据验证复杂性，可扩展的认证协议(EAP)属性数量使用的，以及SAS编号形成了。IKEv2结合在IKEv1的第2阶段信息到IKE_AUTH交换，并且保证，在IKE_AUTH交换完成后，两对等体已经安排一个SA被构件并且准备加密流量。此SA为匹配触发数据包的代理身分只被构件。匹配其他代理身分然后的所有后续的流量触发CREATE_CHILD_SA交换，是第2阶段交换等同在IKEv1的。没有积极模式或主模式。

在IKEv2 Exchange的初期阶段

实际上， IKEv2只有两个初期阶段协商：

- IKE_SA_INIT Exchange
- IKE_AUTH Exchange

IKE_SA_INIT Exchange

IKE_SA_INIT是对等体设立一条安全信道的初始交换。在它完成初始交换后，所有进一步交换加密。因为它结合在IKEv1的MM1-4通常交换的所有信息交换只包含两数据包。结果，响应方计算上昂贵处理IKE_SA_INIT数据包，并且能离开处理第一数据包;它打开协议对从被伪装的地址的一次DOS攻击。

为了从这种攻击保护， IKEv2有在防止的IKE_SA_INIT内的可选交换欺骗攻击。如果不完整会话一特定的阈值达到，响应方进一步不处理数据包，反而发送对发起者的一答复与Cookie。为了使继续的会话，发起者必须再发出接收的IKE_SA_INIT数据包和包括Cookie。

发起者与从证明的响应方的通知有效负载一起再发出初始数据包原始交换未被伪装。这是IKE_SA_INIT交换图表与Cookie挑战的：

IKE_AUTH Exchange

在IKE_SA_INIT交换完成后， IKEv2 SA加密;然而，远端对等体未验证。IKE_AUTH交换用于验证远端对等体和创建第一IPsec SA。

交换与验证有效负载一起包含互联网安全协会和密钥管理协议(ISAKMP) ID。验证有效负载的内容依靠验证方法，可以是预先共享密钥(PSK)， RSA证书(RSA-SIG)，椭圆曲线数字签名算法证书(ECDSA-SIG)，或者EAP。除描述SA将创建的IPsec的验证有效载荷之外，交换包括SA和流量选择器有效载荷。

最新IKEv2交换

CREATE_CHILD_SA Exchange

如果另外的孩子SAS要求，或者，如果孩子SAS的IKE SA或一需要键变更，供应快速模式交换在IKEv1执行的同一种功能。如此图表所显示，只有在此交换的两数据包;然而，每交换重复重新生成密钥或新建的SA ：

信息性Exchange

当它在所有IKEv2交换，每信息性Exchange请求预计一答复。有效载荷的三种类型在信息性交换可以包括。如此图表所显示，有效载荷的任何数量的所有组合可以包括， ：

- 通知有效负载(n)与Cookie一道已经看见。有几个其他类型。他们传播错误和状态信息，他们在IKEv1执行。
- 删除有效负载(d)通知对等体发送方删除一个或很多其流入SAS。响应方预计删除那些SAS和通常包括在其响应消息的另一个方向对应SAS的删除有效载荷。
- 配置有效负载(CP)用于协商在对等体之间的配置数据。一重要使用CP是请求(请求)和分配(答复)在安全网关保护的网络的一个地址。在典型的案件中，一台移动主机设立一个虚拟专用网络(VPN)用在其家庭网络的一个安全网关，并且该的请求给在家庭网络的一个IP地址。**注意：** 这消除复合使用第2层隧道协议和IPsec打算解决的其中一问题。

相关信息

- 站点到站点VPN的ASA IKEv2调试与PSKs TechNote
- 主模式)排除故障TechNote的ASA IPsec和IKE调试(IKEv1
- IOS IPSec和IKE调试- IKEv1排除故障TechNote的主模式
- ASA IPSec和IKE调试- IKEv1积极模式TechNote
- 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