VPN网关已配置设备作为在crypto协商的响应方

目录

简介

本文提供信息关于怎样配置VPN网关设备总是作为在IKE协商的一响应方。设备将回应对其对等体启动的所有crypto协商。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有Cisco IOS软件版本12.4(24)T的Cisco路由器和以后
- Cisco可适应安全工具(ASA)有版本7.0和以上的

相关产品

本文档也可用于以下硬件和软件版本：

- 与软件版本7.0的Cisco PIX防火墙及以后

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

所有crypto协商有双方播放发起者和响应方角色。发起者发送crypto建议到包含关于加密的不同的参数，认证算法，键变更选项和寿命值等等的响应方。响应方选择正确的建议，并且一crypto会话设立。终端设备播放的角色可以由此命令输出查看：

```
Router#show crypto isakmp sa1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no State : MM_ACTIVE ASA(config)#show crypto isakmp sa detailIKE Peer Type Dir Rky State Encrypt Hash Auth Lifetime1 209.165.200.225 User Resp No AM_Active 3des SHA preshrd 86400
```

IKE响应方模式功能的好处

因为的虚拟专用网络(VPN)功能与处理的出现允许同时双向IKE协商(有或没有关注数据流)，数据问题和恢复从重复的IKE SAS的发生。IKE作为协议没有能力比较IKE协商确定是否已经有在发生两的对等体之间的一现有或进行中协商。这些重复的协商可以是昂贵的根据资源和混淆对路由器管理员。当设备配置作为一个响应方设备，不会启动IKE主要，积极或者快速模式(IKE和SA IPSec建立)，亦不将重新生成密钥IKE和IPSec SAS。所以，降低重复项SAS可能性。

此功能的另一个好处是允许受控的支持协商在一个仅方向的连接在负载平衡方案。没有推荐服务器或集线器首次VPN连接往客户端或spoke，因为这些设备是一个单一面对的IP地址访问的全部如通告通过负载平衡器。如果集线器是首次连接，使用一个单个IP地址，他们如此将执行，因而避免负载平衡器的好处。同样是真的重新生成密钥从集线器或服务器来源在负载平衡器背后的请求。

作为在crypto协商的响应方设备将配置的路由器

Cisco IOS软件版本12.4(24)T引入路由器的功能总是响应到其对等体启动的IKE协商。主要限制是此功能是仅可配置在IPSec简档下并且与虚拟接口方案是仅相关的。静态或动态加密映射方案的没有支持。

为了配置您的路由器如响应方，请执行这些步骤：

```
enable configure terminal crypto ipsec profile <name>    responder-only
```

作为在crypto协商的响应方设备将配置的ASA

一般IPSec LAN-to-LAN连接， ASA能功能作为发起者或响应方。在IPSec客户端对LAN连接，ASA仅作用作为响应方。ASA可以配置作为在LAN对LAN VPN连接的响应设备。然而，限制是在VPN通道的另一端设备必须是这些中的一个：

- Cisco ASA 5500系列设备
- Cisco VPN 3000系列集中器
- 运行7.0软件和以后的Cisco PIX 500系列防火墙

为了配置您的ASA作为响应方设备，请发出此命令：

只接听hostname(config)-加密映射mymap 10集合的连接类型

注意： 被建议配置VPN网关设备如响应方广泛VPN对等体终止的地方。

相关信息

- 配置路由器到路由器的 LAN 到 LAN 隧道，从一台路由器发起 IKE 积极模式
- 思科ASA配置示例和TechNotes
- 技术支持和文档 - Cisco Systems