在IPS的轴向TCP会话跟踪模式

目录

简介

本文描述入侵防御系统(IPS)设备的轴向TCP会话跟踪功能。

先决条件

要求

Cisco 建议您了解以下主题：

- IPS 4200系列设备配置与轴向接口。
- TCP协议和通信流知识。

使用的组件

本文档中的信息基于：

- IPS 4270用软件版本7.1(7)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。 如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

背景信息

在某些轴向IPS部署方案中，从TCP数据流的数据包能乘规整器引擎两次看到，导致丢包由于不正确的数据流跟踪。此情况典型地被看到，当流量通过多个虚拟局域网(VLAN)时或由单个虚拟传感器监控的接口对路由。当任一个方向的流量从不同的VLAN或接口时，接收此问题由必要允许不对称流量进一步复杂化为适当的数据流跟踪合并。

网络图

问题

在此网络拓扑方面，网络内部的一个客户端启动HTTP连接到在外部网络的服务器。两个网段由一可适应安全工具(ASA)防火墙分离。在此设计，单个IPS设备配置轻拍到与两套的两内部和外部VLAN轴向接口对。当客户端启动会话到服务器时， TCP SYN (请同步)数据包通过IPS和ASA采取此路径(出站数据流) ：

Client> IPS G3/0 > *vs0* > IPS G3/1 > ASA G0/0 > ASA G0/1 > IPS G3/2 > *vs0* > IPS G3/3 >Server

在出站数据流，客户端发送的TCP SYN由**vs0**虚拟传感器后看到，当数据包横断往ASA的内部接口的内部接口对，并且再，当数据包横断往Web服务器的外部接口对。 在一个对称方案中，同一个情况在有SYN ACK的(肯定回答)从Web服务器的返回路径和后续信息包发生。 当IPS尝试结合数据流到单个TCP连接时，每数据包重复项在连接的被观察，导致一台混淆的规整器和丢弃的数据包。 为了确认IPS是否遇到此情况，**显示stat virt**命令的输出显示射击的很大数量的1330个TCP规整器签名，以及很大数量的已修改和已拒绝数据包和连接。

解决方案

轴向TCP会话跟踪模式选项可以用于解决情况例如此。 有可以配置的三个可能的模式：

1. **虚拟传感器(默认设置)** -在客户端数据包在一个轴向对被看到的一个不对称部署情况监控，而服务器数据包在一个第二个接口对被看到。 必须一起监控两个接口对发现连接的两边。
2. **接口和VLAN** -这是应急方案对在本文显示的拓扑示例，两个或多个轴向接口对分配到同一个虚拟传感器。 使用启用的此选项， TCP连接可能横断超过一个对，允许规整器为每个轴向对独立地跟踪TCP会话。
3. **仅VLAN** -这是两第一选择的一个非常少见组合和使用您监控多不对称网络的组合。 在左侧接口对的**VLAN1**有客户端数据包，并且必须与在正确的接口对的**VLAN1**一起，有服务器数据包。 在这种情况下，流量在所有接口对间聚集，但是由VLAN分离。 例如，一起放置在所有接口间的VLAN1数据包;一起放置从所有接口的VLAN 2数据包，但是VLAN1和VLAN 2数据包为TCP会话跟踪一起从未被放置。

对于上述拓扑示例，有两种方式问题可以是解决的：

解决方案 1

搬入每个轴向接口对其自己的虚拟传感器。例如，在**vs0的**一个对和在**vs1的**一个对。 通常推荐此方法，当少于四个轴向对时有(由于四个虚拟传感器平台限制)。 规整器对待重复的数据流作为两独立的连接。

解决方案 2

配置轴向TCP会话跟踪模式**建立接口和VLAN**。推荐此方法，当有超过四个轴向对时，在，被迫使放置多个轴向对到单个虚拟传感器情况下。 规整器对待在不同的轴向对的数据包作为在同一个虚拟传感器内的完全不同的连接。

配置

这是分离每轴向接口对的虚拟传感器的配置：

```
IPS4510-01# conf t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Inside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# virtual-sensor vs1

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Outside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

IPS4510-01(config)# exit
```

这是接口和VLAN的配置：

```
IPS4510-01# config t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# inline-tcp-session interface-and-vlan

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

Apply Changes?[yes]: yes

Warning: Change of TCP session tracking mode will not take effect until restart.

IPS4510-01(config)# exit
```

```
IPS4510-01# reset
```

验证

- 请使用**显示stat virt|b TCP statistics命令规整器Dropped、重复项，拒绝**或者**SendAck发送的数据包**非零统计信息的**阶段**和复核在TCP规整器。
- 请使用**显示stat virt|b**与从前面的命令的TCP Normalier统计信息一道射击了的1330个签名的每**签名count命令的SigEvent**和复核。

相关信息

- **思科入侵防御系统传感器IPS的7.0 CLI配置指南-轴向TCP会话跟踪模式**
- **思科入侵防御系统管理器IPS的7.1 Express配置指南-轴向TCP会话跟踪模式**
- **技术支持和文档 - Cisco Systems**