进程单个数据流大会话(大象流)由Firepower服务

目录

简介

本文描述单个流为什么不能消耗思科Firepower设备的整个额定吞吐量。

背景信息

任何带宽速度测试网站结果或者任何带宽测量工具输出(例如， iperf)也许不陈列思科Firepower设备的通告的吞吐率。同样地，一个非常大文件的转移过渡任何传输协议不展示Firepower设备的通告的吞吐率。因为Firepower服务不使用一个单个网络流为了确定其最大吞吐量，它发生。

由喷鼻息的进程流量

Firepower服务的基础检测技术是喷鼻息。喷鼻息的实施在思科Firepower设备的是单个线索进程为了处理流量。设备为根据通过设备的总吞吐量的一种特定费率是额定的所有流。在边界边缘附近通常预计设备部署在公司网络，并且与千位连接一起使用。

Firepower服务流量使用负载均衡对一定数量的另外喷鼻息进程的与在设备的每个CPU运行的一喷鼻息进程。理论上来讲，系统负载在所有喷鼻息进程间均匀地平衡流量。喷鼻息需要能为下一代防火墙(NGFW)，入侵防御系统(IPS)和先进的恶意软件保护(AMP)检查提供适当的上下文分析。为了保证喷鼻息最有效，从单个流的所有流量是负载被均衡对一个喷鼻息实例。 如果从单个流的所有流量未被平衡对单个喷鼻息实例，系统可能被逃避，并且流量会溢出，在这种情况下喷鼻息规则也许是不太可能匹配或文件的片段为AMP检查不是连续。所以，负载均衡算法根据能独特识别一给的连接的连接信息。

在虚拟ASA与Firepower服务和的NGIPS的2元组算法

在可适应安全工具(ASA)上有Firepower虚拟服务平台和下一代的入侵防御系统的(NGIPS)，流量是被均衡的负载为了打鼾与使用2元组算法。此算法的datapoints是：

- 源 IP
- 目的 IP

在软件版本5.3的3元组算法或在Firepower和FTD设备降低

在所有以前的版本(5.3或降低)，流量是使用3元组算法被均衡的负载打鼾。此算法的datapoints是：

- 源 IP
- 目的 IP
- IP 协议

与同样的所有流量来源、目的地和IP协议是负载被均衡对喷鼻息同一实例。

在软件版本5.4，6.0和极大的5元组算法在Firepower和FTD设备

在版本5.4，6.0或者更加极大，流量是balaned的负载打鼾与5元组算法。被考虑到的datapoints是：

- 源 IP
- 源端口
- 目的 IP
- 目的端口
- IP 协议

算法的目的添加端口是均匀平衡流量，当有占流量的大部分的特定源及目的地对时。由端口的新增内容，高位短暂源端口一定是不同的每个流，并且必须均匀地添加平衡流量对不同的喷鼻息实例的另外的熵。

总吞吐量

设备的总吞吐量被测量根据工作对他们的全部潜在的总吞吐量所有喷鼻息实例。工业标准运作为了测量吞吐量是为与多种对象大小的多个HTTP连接。例如，NSS NGFW测试方法测量设备的总吞吐量有44k、21k、10k、4.4k和1.7k对象的。这些翻译对范围从在1k附近的平均信息包大小&字节对128个字节由于在HTTP连接涉及的其他数据包。

您能预计一个单个喷鼻息实例的性能速率。采取设备的额定吞吐量并且由的喷鼻息实例数量运行分开那。例如，如果设备是额定的在IPS的10Gbps与平均信息包大小1k字节和该设备有喷鼻息20个实例，单个实例的近似最大吞吐量是500 Mbps每个喷鼻息。不同类型的流量，网络协议，数据包的大小与差异一起的在整体安全策略能所有影响设备的被观察的吞吐量。

第三方工具测试结果

当您用所有速度测试网站，或者任何带宽测量工具测试，例如，iperf，一个大单个数据流TCP流时生成。此种大TCP流呼叫大象流。大象流是单个会话，相对消耗大或不成比例的数量带宽的长期的网络连接。此种流分配到一个喷鼻息实例，因此测试结果显示吞吐量单个喷鼻息实例，不是总吞吐量分级设备。

补救

智能应用程序旁路(IAB)

软件版本6.0介绍呼叫IAB的新特性。当Firepower设备达到一个预定义的性能门限值时， IAB功能寻找满足特定标准为了智能绕过缓和在检测引擎的压力的流。

提示：可以找到关于IAB的配置的更多信息此处。

识别并且委托大流

大流与高使用低检查值流量，备份、例如数据库复制等等经常涉及。许多这些应用程序不可能从检查有益于。为了避免与大流的问题，您能识别大流和创建访问控制他们的信任规则。这些规则能独特识别大流，允许那些流通过未经检查和不由单个喷鼻息实例行为限制。

Note:为了识别信任规则的大流，请与思科Firepower TAC联系。

相关信息

- 访问控制使用智能应用程序旁路
- **技术支持和文档 - Cisco Systems**