UnityOne IPS流量传输限制过滤器配置案例

谷会波 2006-11-14 发表

UnityOne IPS流量传输限制过滤器配置案例

一、前言

Traffic threshold filters使IPS设备能够统计静态网络传输流量。TippingPoint会统计一定时间的网络正常流量为标准，如果网络中的某种流量与正常流量有较大差异，Traffic threshold filters会报警给管理员。并通过这些过滤器整形、休整系统和网络的带宽。

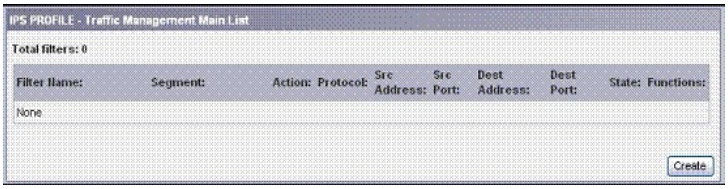
每一个过滤器可以设置4种类型：

- **minor increase —** 流量稍微超过规定的流量限制
- **major increase —** 流量极大超过规定的流量限制
- **minor decrease —** 流量稍微低于规定的流量限制
- **major decrease —** 流量极大低于规定的流量限制

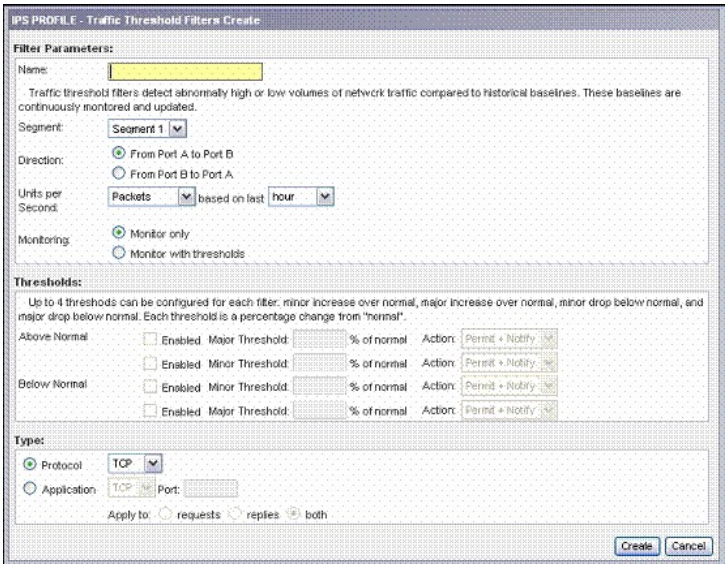
上限和下限用“% of normal”形式来表示。例如，一个极限为120%表示如果流量数值超过正规流量20%，TP会做出响应；一个极限为80%表示如果传输的流量低于标准流量20%，TP将会做出响应。

二、操作步骤

1、点击**IPS —> Filters —> Traffic Thresholds**，进入**IPS PROFILE - FILTERS - Traffic Thresholds**页面：



2、点击**create,**进入**IPS PROFILE - Traffic Threshold Filters Create** 页面：



3、输入**Traffic Threshold Filter Name**.

4、在**Filter Parameters**部分，修改过滤器的属性参数：

- 选择过滤器保护的网段（**Segment**）
- 选择被保护流量的方向（**Direction**）：**A to B** or **B to A**.
- 选择每秒统计的单位 **Units per Second**，可以选择的单位 **packets, bytes, and connections**
- 选择统计的标准时间，可以选择的单位为上一分钟、一小时、一天、一周、三十天和三十五天
- **Monitor**分为**Monitor only** 和 **Monitor with thresholds**两种情况：**Monitor only**只是检测系统流量产生报告，并不触发流量极限的响应动作；**Monitor with thresholds**根据用户设置的响应动作来整形网络流量

5、在参数**Thresholds**设置中，对于每种规则，可以修改四种极限（见前言），每种限制都是与标准

流量相比的白分比变化：

- **Above Normal Major —** 选择激活enable,输入百分比数值略高于标准流量值（大于100%），并选择响应动作action
- **Above Normal Minor —** 选择激活enable,输入百分比数值较多的高于标准流量值（大于**Above Normal Major**数值），并选择响应动作action
- **Below Normal Major —** 选择激活enable,输入百分比数值略低于标准流量值（小于100%），并选择响应动作action
- **Below Normal Minor —** 选择激活enable,输入百分比数值较多低于标准流量值（小于**Below Normal Minor**数值），并选择响应动作action 数值

6、对于 **Type**,选择和修改如下的参数：

协议**Protocol** — 可以选择的协议类型包括**TCP**, **ICMP**，**UDP**和**Other**

应用**Application** — 选择协议的类型和对应的端口；选择应用的类型如下：**requests**, **replies**, **both**

7、点击 **Save.**