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 Threshold s页面:

Fotal filters: 0							
Filter Name:	Segment:	Action: Protocol:	Src Address:	Src Port:	Dest Address:	Dest Port:	State: Functions:
None							

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

	rs:					
Name:						
Traffic thresho continuously mo	Id filters detect abnormally high or low volum intored and updated.	es of network traffic	compare	ed to historical b	aselines. Th	ese baselines are
Segment:	Segment 1 💌					
Direction:	 From Port A to Port B From Port B to Port A 					
Units per Second	Packets M based on last hour	×				
Monitoring	 Monitor only Monitor with thresholds 					
Thresholds:						
Thresholds: Up to 4 thresh major drop belov	ods can be configured for each filter, minor in v normal. Each threshold is a percentage cha	norease over normal nge from "normal".	l, major in	crease over nor	mal, minor d	rop below normal, ar
Thresholds: Up to 4 thresh major drop belov Above Normal	ods can be configured for each filter, minor in v normal. Each threshold is a percentage cha Enabled Major Threshold	ncrease over normal nge from "normal". % of normal	l, major in Action	crease over nor Permit + Notify	mal, minor d	rop below normal, er
Thresholds: Up to 4 thresh major drop belov Above Normal	ods can be configured for each filter: minor in v normal. Each threshold is a percentage cha Enabled Major Threshold Enabled Minor Threshold	norease over normal nge from "hernsi". % of normal % of normal	I, major in Action Action	crease over nor Permit + Notify Permit + Notify	mal, minor d	rop below normal, ar
Thresholds: Up to 4 threshi major drop belov Above Normal Below Normal	ods can be configured for each filter, minor ir v normal. Each threehold is a percentage cha Enabled Major Threehold Enabled Minor Threehold Enabled Minor Threehold	norease over normal nge from "hormsi". % of normal % of normal % of normal	l, major in Action Action Action	Perinit + Notify Perinit + Notify Perinit + Notify	mal, minor d	rop below normal, ar
Thresholds: Up to 4 thresh Insjor drop belov Above Normal Below Normal	ods can be configured for each filter, miner ir rormal. Each threehold is a percentage cha Ensibled Major Threshold Ensibled Minor Threshold Ensibled Minor Threshold Ensibled Major Threshold	ncrease over normal nge from "horms!" % of norms! % of norms! % of norms! % of norms!	I, major in Action Action Action Action	Pernit + Notify Pernit + Notify Pernit + Notify Pernit + Notify	mal, minor d	rop below normal, ar
Thresholds: Up to 4 thresh najor drop belov Above Normal Below Normal	ods can be configured for each filter, miner ir v normal. Each threshold is a percentage chai Enabled Minor Threshold Enabled Minor Threshold Enabled Minor Threshold	ncrease over normal nge from "horns!" % of normal % of normal % of normal % of normal	I, major in Action Action Action Action	Permit + Notify Permit + Notify Permit + Notify Permit + Notify Permit + Notify	mal, mihor d	rop below normal, er
Thresholds: Up to 4 thresh major drop belov Above Normal Below Normal Fype:	ods can be configured for each filler: minor ir vnormal. Each threshold is a percentage cha Ensbled Major Threshold. Ensbled Minor Threshold. Ensbled Minor Threshold. Ensbled Major Threshold.	ncrease over normal nge from "hornsi". % of normal % of normal % of normal % of normal	I, major In Action Action Action Action	Permit + Notify Permit + Notify Permit + Notify Permit + Notify Permit + Notify	mal, mihor d	rop below normal, er
Ihresholds: Up to 4 thresh major drop belov Above Normal Below Normal Below Normal	ods can be configured for each filer: minor ir vinormal. Each threshold is a percentage cha Ensbled Major Threshold. Ensbled Minor Threshold. Ensbled Minor Threshold. Ensbled Minor Threshold.	ncrease over normal nge from 'hornsi'. % of normal % of normal % of normal % of normal	l, major in Action Action Action Action	Permit + Notify Permit + Notify Permit + Notify Permit + Notify Permit + Notify	msl, mihor d	rop below normal, er

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

流量相比的百分比变化:

- ◆ 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 Nor mal 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.**