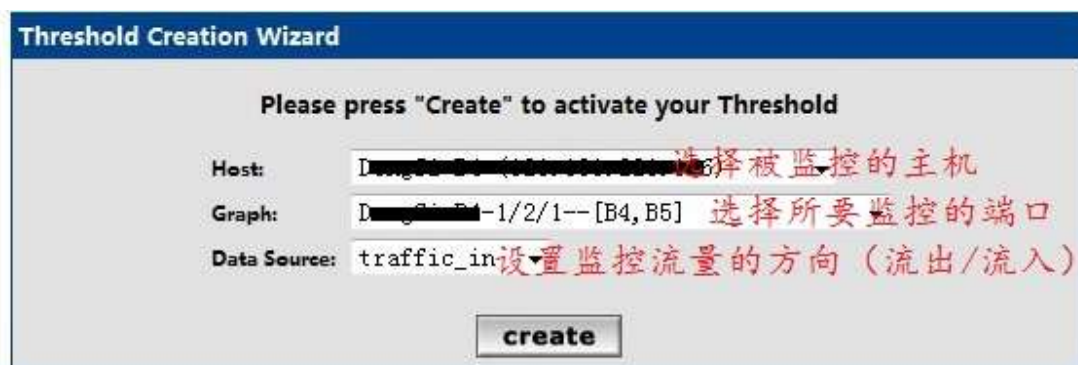


之前笔者介绍过，现在判断网络是否被攻击很多时候是基于流量判断的。比如我们的网络正常情况下使用的带宽在 50-100M，那么带宽到达 200M 的时候就显然很不正常了，造成带宽突然增大的原因有很多种，比如客户在服务器上下载上传数据、对外大量发送恶意数据包、遭受攻击等。所以，及时知道整个网络实时流量状况是非常有必要的。在工作环境中我们不可能专门有人 24 小时盯着显示器监视网络流量大小，而是需要智能化解办法，比如网络正常时带宽为 50-100M，当到达 150M 的时候给管理人员发送预警  
下面我们看一下用 cacti 监控流量是如何实现阈值报警的

新建阈值模板，登录 cacti 后打开 “Console-----Thresholds-----Add”



设置流入阈值报警

1: traffic\_in  
N/A

2: traffic\_out  
N/A

Data Source Item [traffic\_in] - Current value: [187974.4628]

Template settings

**Template Propagation Enabled**  
Whether or not these settings will be propagated from the threshold template. ☐ Template Propagation Enabled

**Mandatory settings**

**Threshold Name**  
Provide the Thold a meaningful name. 5 - Traffic - Ethernet1/2/1 [traf

**Threshold Enabled**  
Whether or not this threshold will be checked and alerted upon. ☒ Threshold Enabled

**Weekend Exemption**  
If this is checked, this Threshold will not alert on weekends. ☐ Weekend Exemption

**Disable Restoration Email**  
If this is checked, Thold will not send an alert when the threshold has returned to normal status. ☐ Disable Restoration Email

**Threshold Type**  
The type of Threshold that will be monitored. High / Low Values ▾

**High / Low Settings**

**High Threshold**  
If set and data source value goes above this number, alert will be triggered. 5242880 当流入流量大于5M或者低于1M是发送报警

**Low Threshold**  
If set and data source value goes below this number, alert will be triggered. 1048576

**Breach Duration**  
The amount of time the data source must be in breach of the threshold for an alert to be raised. 1 Minute ▾

**Data Manipulation**

**Data Type**  
Special formatting for the given data. CDEF ▾ 监控模板类型

**Threshold CDEF**  
Apply this CDEF before returning the data. Turn Bytes into Bits ▾ 流量单位大小

**Other setting**

**Re-Alert Cycle**  
Repeat alert after this amount of time has passed since the last alert. Every Minute ▾ 报警轮询时间

**Notify accounts**  
This is a listing of accounts that will be notified when this threshold is breached.

**Extra Alert Emails**  
13526711@139.com 接收报警地址

设置流出阈值报警

1: traffic\_in  
Hi: 5242880 Lo: 1048576 BL: off

2: traffic\_out  
Hi: 10485760 Lo: 1048576 BL: off

Data Source Item [traffic\_out] - Current value: [4353183.5195]

Template settings

Template Propagation Enabled  
Whether or not these settings will be propagated from the threshold template. ☐ Template Propagation Enabled

Monitoring settings

Threshold Name  
Provide the Thold a meaningful name Traffic - Ethernet1/2/1 [traf

Threshold Enabled  
Whether or not this threshold will be checked and alerted upon. ☒ Threshold Enabled

Weekend Exemption  
If this is checked, this Threshold will not alert on weekends. ☐ Weekend Exemption

Disable Restoration Email  
If this is checked, Thold will not send an alert when the threshold has returned to normal status. ☐ Disable Restoration Email

Threshold Type  
The type of Threshold that will be monitored. High / Low Values

High / Low Settings

High Threshold  
If set and data source value goes above this number, alert will be triggered 10485760 当流出流量大于10M小于1M时

Low Threshold  
If set and data source value goes below this number, alert will be triggered 1048576 发送报警

Breach Duration  
The amount of time the data source must be in breach of the threshold for an alert to be raised. 1 Minute

Data Manipulation

Data Type  
Special formatting for the given data. CDEF

Threshold CDEF  
Apply this CDEF before returning the data. Turn Bytes into Bits

Other setting

Re-Alert Cycle  
Repeat alert after this amount of time has passed since the last alert. Every Minute

Notify accounts  
This is a listing of accounts that will be notified when this threshold is breached.

135285...@139.com

下图为流量没有超过或低于我们设置的阈值，所以显示时为蓝色

console

graphs

thold

monitor

settings

Console -> Thresholds

Logged in as jcmde (Logout)

Thresholds

Host Status

Threshold Status

Template: Interface - Traffic

Status: All

Rows: 30

Search:

go

clear

<< Previous

Showing Rows 1 to 2 of 2 [1]

Next >>

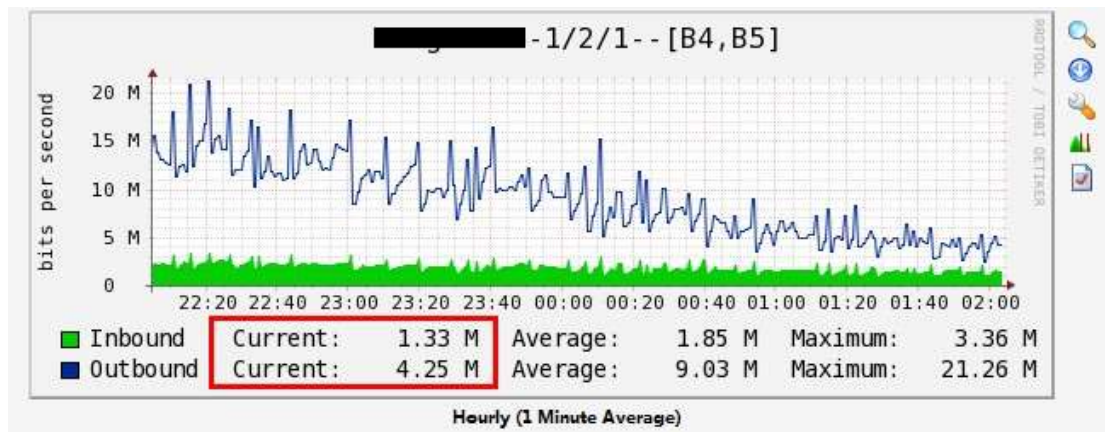
Actions	Name**	ID	Type	High	Low	Current	Enabled
	Traffic - Ethernet1/2/1 [traffic_in]	6	High/Low	5242880	1048576	1484664.9333	Enabled
	Traffic - Ethernet1/2/1 [traffic_out]	7	High/Low	10485760	1048576	4201861.3333	Enabled

<< Previous

Showing Rows 1 to 2 of 2 [1]

Next >>

我们还可以点击阈值左边的小图标查看当前端口的流量曲线图



下图显示的为某端口流出流量已经超过我们所设置的阈值，当超过或者低于我们设置的阈值时，显示呈红色。这个时候我们就可以收到报警邮件通知了

1352 - Traffic - Ethernet1/2/1 [traffic_in]	6	High/Low	5242880	1048576	4543771.3333	Enabled
1352 - Traffic - Ethernet1/2/1 [traffic_out]	7	High/Low	10485760	1048576	15884518.8	Enabled

下图为阈值报警的邮件内容

