Global Information Assurance Certification Paper

Visual Baselines – Maximizing Economies of Scale Using Round Robin Databases

GIAC Certified Intrusion Analyst (GCIA)

Gold Practical

Kirsten Hook

Table of Contents

Abstract 3
Document Conventions 4
Introduction 5
Round Robin Databases 6
RRDTool 6
Cacti 6
Network Architecture 7
Cacti Install 8
Monitoring MySql 4.0 with Cacti 11
Graph Creation 12
Analysis 13
Scenario 1 14
Scenario 2 15
Scenario 3 16
Scenario 4 17
Scenario 5 18
Scenario 6 19
Scenario 7 20
Bonus Cacti 21
Conclusion 22
References 23
Appendix A 24
Appendix B 27
Appendix C 30

Abstract

The scope of this paper is to demonstrate how using visual baselines can effectively increase your capabilities of discovering anomalies on your network. This paper will discuss Round Robin Databases and how to implement them in your environment as well as installing RRDtool and Cacti as tools to utilize in your environment. They will be installed in a fictitious environment belonging to a company called Canadian Maple Designs. This company has patented a specialized treatment for wood products and understands the need to protect its information assets.

Document Conventions

For the purpose of this document the following conventions will be used:

`command`	**Operating systems commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.**
`filename`	**Filenames, paths and directory names are represented in this style.**
`computer output`	**The results of a command and other computer output.**
URL	**Web URL's are shown in this style.**
Quotation	**A citation or quotation from a book or web site is in this style.**
>>	**Continuation of a single line that would not fit the width of this paper.**

Introduction

In general most people can easily relate to a pictorial or graphical representation rather than a bunch of 1's and 0's of raw data. In the security domain we are often overwhelmed with raw data and a fundamental tool to prevent this is the visual baseline. Visual baselines allow the analyst to have a focused view innumerable network statistics.

How are you going to know if something doesn't quite look "right" when you don't know what "right" is supposed to look like? This paper is designed to give the security professional a solid understanding of some of the tools that are available for them to use in assisting them in creating visual baselines including RRDtool, and Cacti. This paper will discuss the advantages of using Round Robin Databases to collect and display network statistics and how to use this information to create a clear picture of what is actually happening on your network.

One of the most critical aspects of any security professional's job is to have a solid understanding of their network. This is where creating a baseline of your network becomes vital. Essentially you need to actually read and understand the information you are gathering, not just glance at it and say "I'm not sure what that is so I will ignore it". One you have developed a good understanding of the way your network communicates you will feel much more comfortable with the everyday events on the network. This will assist you greatly when it comes time to tune your environment and determine which events are false positives.

Round Robin Databases

A Round Robin Database contains a store of information that holds a fixed amount of data. The size of the database is determined when the database is first set up and will never exceed the maximum size as defined. When determining the size of the database it is important to know exactly what you are measuring and how long you would like to have this data for as it will be written over after a certain defined time period. How this works is that when the database reaches its maximum size the oldest data record is written over by the newest data record, or if you want to think of it in data bytes, the very oldest byte is written over by the newest byte. The data collected and stored can consist of data such as CPU counters, disk space, memory counters, logged in users, bandwidth, temperature values and the list goes on.

The benefits of using round robin databases are that they allow you to compare your data in a time-based manner. You can compare data by the second, minute, hour, day and even yearly depending on the data store you have defined.

RRDtool

RRDtool which stands for Round Robin Database Tool was written by Tobias Oetiker and can be downloaded here: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/download.en.html.

RRDtool is an application that logs and graphs data collected from devices on your network and stores it in a database.

Cacti

Cacti is a powerful php driven front end component for RRDTool. It gathers data the data collected by RRDtool and organizes it in to very easy to read graphs. It can be downloaded here: http://cacti.net/download_cacti.php.

Network Architecture

The network environment that these tools will be running in will be a fictitious company called Canadian Maple Designs, which specializes in unique wood treatments. They have patented a number of treatments for wood products and are quite aware of the need for protection of their informational assets. All addressing information pertaining to the network has been sanitized. The following hardware will be used

Firewall – Cisco PIX 506E
Switch – Cisco Catalyst 2900 XL
Sensor – 600MHz Pentium III, 256 MB of RAM running Centos 4.1
Workstations - Variety

The following is a diagram of the network:

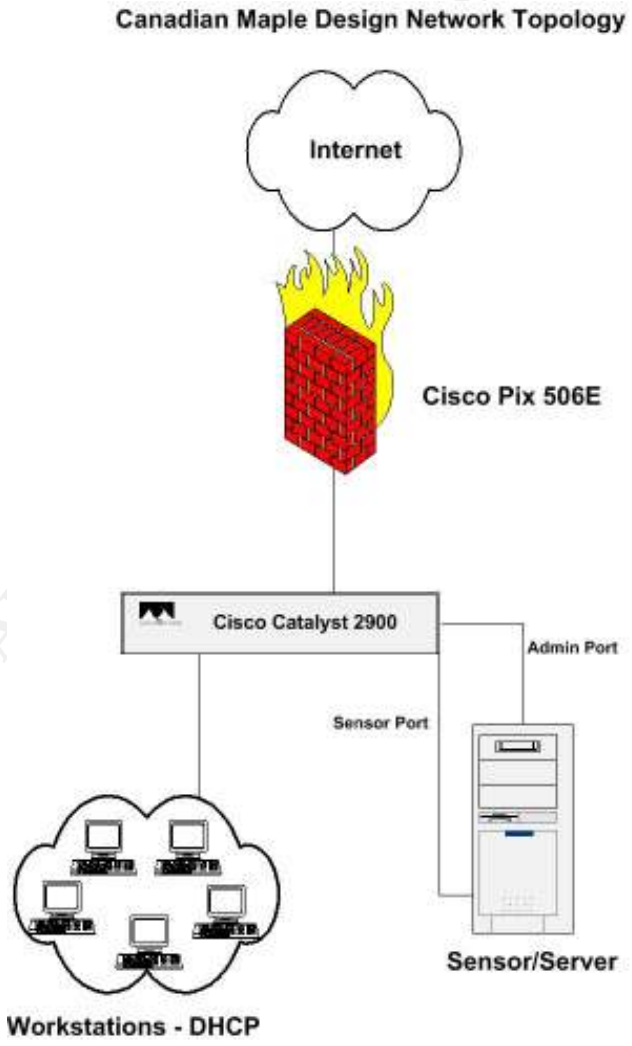


Figure 1

Cacti Install

To install Snort, MySql and Base as a platform for this paper I used Patrick Harper's Snort Enterprise Install document found at http://www.internetsecurityguru.com. By following this document step by step you will have a basic Snort installation, using Base as a front end and MySql database as a backend. Please understand that this is the basic setup and in order for this implementation to be effective in your environment you will need to tune Snort to meet your organization's needs. You may also have reservations of the install of Centos 4.1 according to the paper and the packages that are required and this is up to your discretion. Each environment is different and you may have a certain security standard in place that does not require all of the packages listed in the paper to be installed.

Once you have installed the software and have snort and Base running properly it's time to install Cacti and RRDtool

For the purpose of this paper we will be using a yum repository to install the required software. A yum repository is a collection of updates, tools and applications that use RPM's. There are many different repositories out there, for this paper we will be using the one located on Dag Wieers site http://dag@wieers.com. To set up your system to use this repository copy and paste the following in your /etc/yum.conf file:

```
[dag] name=Dag RPM Repository for Red Hat Enterprise Linux
baseurl=http://apt.sw.be/redhat/el$releasever/en>>
/$basearch/dag
gpgcheck=1
enabled=1
```

Download http://www.cacti.net/downloads/cacti-0.8.6f.tar.gz

Install the following required packages:

```
yum install net-snmp-devel php-snmp net-snmp net-snmp-utils
rrdtool
```

The following installation guide is courtesy of http://www.cacti.net and can be found at http://www.cactgi.net/downloads/docs/html/install_unix.html. There is also an excellent How To guide written by Lee Carter that can be found at http://www.cacti.net/downloads/docs/contrib/Cacti-Linux-How-To.pdf

Extract the distribution tarball:

```
shell> tar xzvf cacti-version.tar.gz
```

Create the MySQL database:

```
shell> mysqladmin --user=root -p create cacti
```

Import the default cacti database:

```
shell> mysql -u root -p cacti < cacti.sql
```

Optional: Create a MySQL username and password for Cacti.

```
shell> mysql --user=root -p mysql

mysql> GRANT ALL ON cacti.* TO cactiuser@localhost>>

IDENTIFIED BY 'somepassword;

mysql> flush privileges;
```

Edit include/config.php and specify the MySQL user, password and database for your Cacti configuration.

```
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "cacti";
```

Create Cacti User

```
shell> adduser cactiuser
shell> passwd cactiuser
```

Set the appropriate permissions on cacti's directories for graph/log generation. You should execute these commands from inside cacti's directory to change the permissions.

```
shell> chown -R cactiuser rra/log/
```

(Enter a valid username for cactiuser; this user will also be used in the next step for data gathering.)

```
shell> adduser newuser
```

```
shell> passwd  *******
```

Add a line to your /etc/crontab file similar to:

```
*/5 * * * * newuser php /var/www/html/cacti>>
/poller.php > /dev/null 2>&1
```

Replace cactiuser with the valid user specified in the previous step.

Point your web browser to:

http://whatever_your_server_is/cacti/

Log in with both the username and password of admin. You will be required to change this password immediately. Make sure to fill in all of the path variables carefully and correctly on the following screen.

Cacti – Enabling NetSNMP

Using the editor of your choice and add the following to your:

```
emacs /etc/snmp/snmpd.conf
```

```
# First, map the community name "public" into a>>
"security name"
# sec.name  source          community >>
com2sec notConfigUser  default       thisismystring
/sbin/chkconfig snmpd on
```

For the purpose of this paper a Cisco PIX 506E is used in the lab. This requires the Cacti PIX monitoring templates. Cacti provides a variety of templates for many devices that are used in most environments. They are available…….

Monitoring MySQL 4.0 with Cacti

mysql_stats.php
version 2.0
enables cacti to read mysql statistics
by berger@hk-net.de 2005/01/18

Installation

The cacti templates for MySQL graphs can be downloaded from http://forums.cacti.net/about6108.html&highlight=mysql.

Put the mysql_stats.php file inside the cacti/scripts/ directory

Import the Xml-Files using the cacti web interface

```
cacti_graph_template_mysql_command_statistics.xml
cacti_graph_template_mysql_connections.xml
cacti_graph_template_mysql_handler_statistics.xml
cacti_graph_template_mysql_querycache_statistics.xml
cacti_graph_template_mysql_questions.xml
cacti_graph_template_mysql_single_statistics.xml
cacti_graph_template_mysql_thread_statistics.xml
cacti_graph_template_mysql_traffic.xml
```

Usage

Configure the mysql-server you want to graph. To enable access from the cacti-machine to the mysql-status information, you must have the "process" right. Use for example the following mysql-command to set the process-right for the mysql-user "cactiuser" with the password "cactipasswd":

```
GRANT PROCESS ON * TO cactiuser@'localhost' IDENTIFIED >>
by 'cactipasswd';
GRANT PROCESS ON * TO cactiuser@'127.0.0.1' IDENTIFIED >>
by 'cactipasswd';
```

To monitor a foreign host, fill in the hostname where you came from, for example:

```
GRANT PROCESS ON * TO cactiuser@'cactihost.com'>>
IDENTIFIED by 'cactipasswd';
```

Graph Creation

Click inside cacti on "New Graphs"

Choose host and a mysql-template

Click create

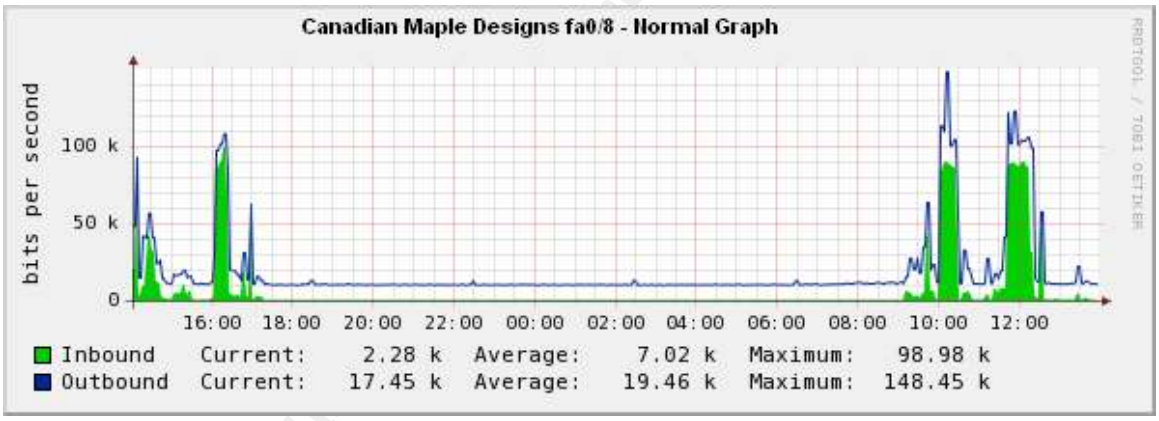
Fill in the MySQL-username and password as specified above.

Analysis

In this section of the paper we will review some of the cacti graphs collected from Canadian Maple Design's network. Some of the main features of the graphs that we will focus on are:

- Amount of traffic
- Large Spikes
- Traffic occurring during after hours
- Unusual amounts of incoming or outgoing traffic
- Traffic on unused ports

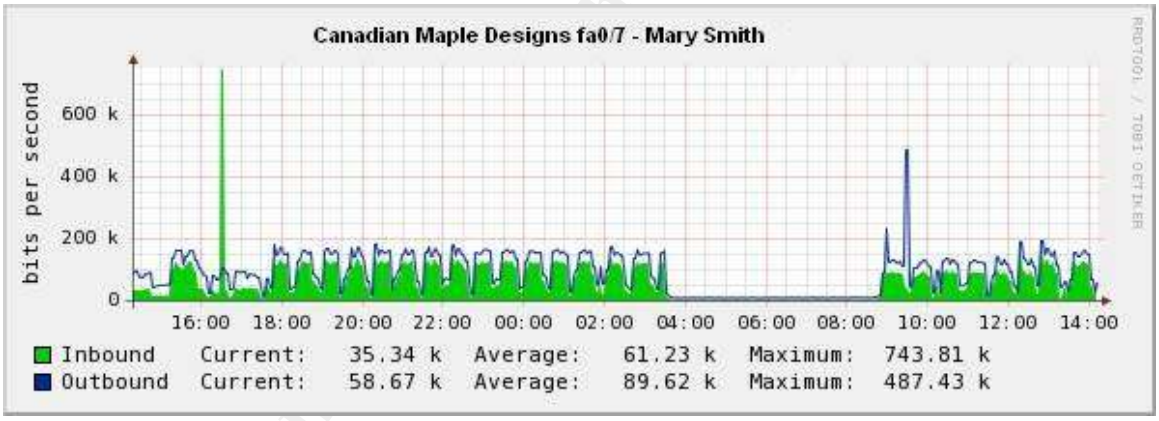
The graph pictured below is essentially a normal workday for one of the employees. Note that the traffic does not seem unreasonably high and there are no real patterns that catch our eye. Notice the time stamps on the bottom of this graph, obviously the person does not work until wee hours of the night and that is why there is no activity throughout the evening



Scenario 1

A user named Mary thinks that if she downloads a desktop indexing tool she will save time and money by being able to find her documents that much quicker. What she doesn't realize is the overhead of these programs. The graph below represents what's really happening after she installs that program. Mary configured it to index her files in her home folder which resides on the corporate file server, and scheduled it to run almost 24 hours a day. We can see by the graph that it stops indexing around 4:00 a.m and starts to index again at 9:00 a.m. The IT Department advised Mary to implement a more organized file structure and to remove the indexing program.

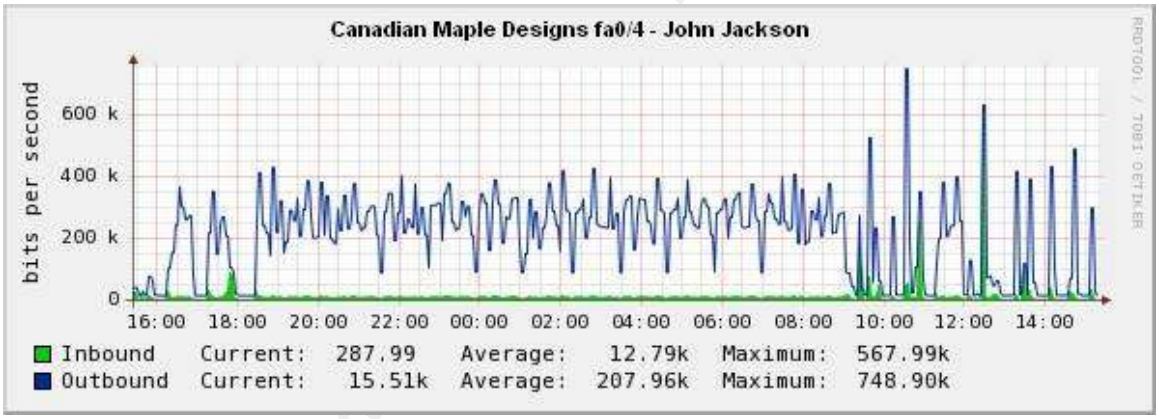
Daily



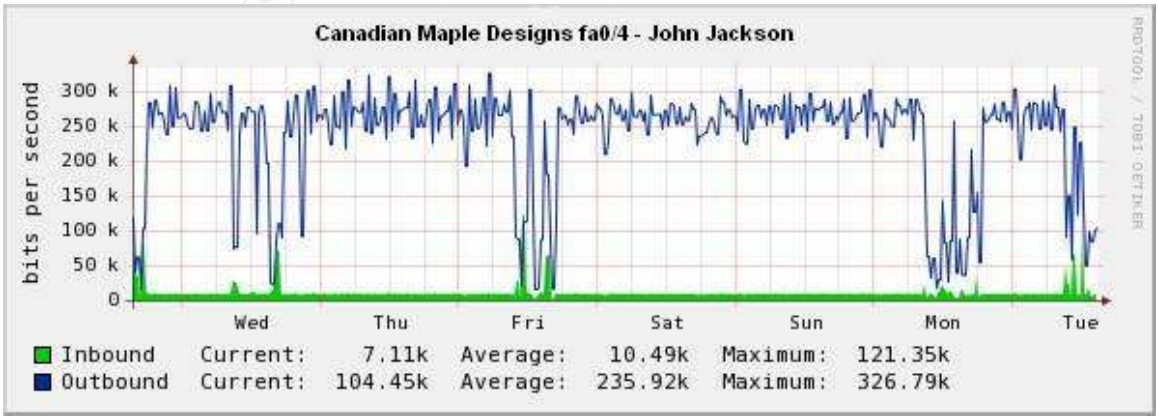
Scenario 2

The next graph we will look at is a daily and weekly graph from a user named John. The IT department was a little perplexed by John's cacti graph and decided to find out what was causing all of this traffic from his port. It turned out John was quite paranoid about viruses on his computer. He had had bad luck in the past with spyware and viruses on his home computer and will take any precaution to avoid losing his work. He decided to run a virus scan of his home folder every night using the antivirus client he had been provided, just to make sure that his files are clean. What John didn't know was that his home folder resides on the main file server, which is scanned nightly by a corporate antivirus program configured by the IT Department. It turns out John not only is scanning his home folder on the file server but he is also scanning all of his mapped drives to the file server, which actually contain about 160 GB of data. John is reassured by the IT department that his files are safe on the file server and the scan is unnecessary.

Daily Graph:



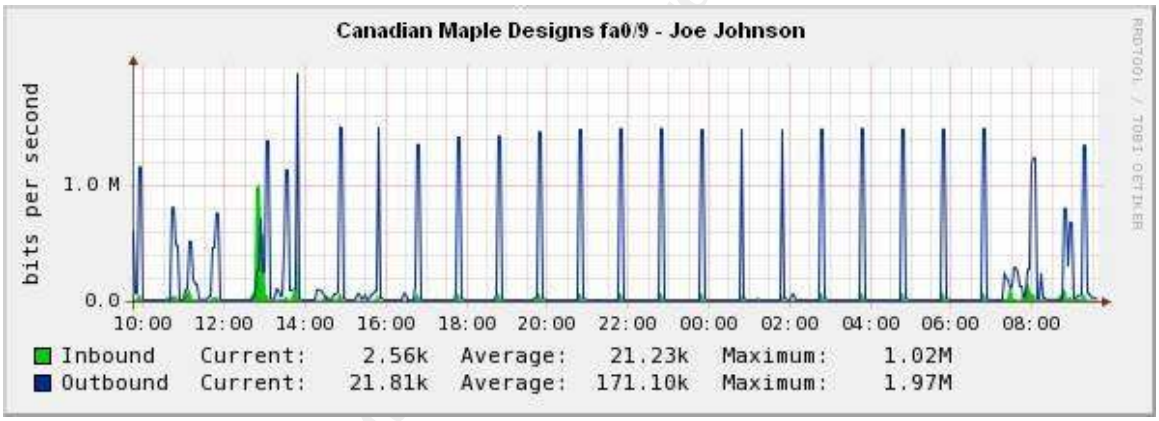
Weekly Graph:



Scenario 3

The next graph we will examine belongs to a user named Joe. Joe is a dangerous computer user. He believes that clicking anywhere on a website is ok, he actually doesn't mind pop ups at all, he finds them informational. Joe has decided that he needs to install a weather toolbar that showed up on his screen after he visited a website. He found the weather toolbar to be very cool, now he knows what the weather is all of the time! He is confused, as his home page changed to a site he doesn't recognize. He also found his computer a bit slow after installing the toolbar. The IT staff had noticed his cacti graph and decided to pay him a visit. They ask Joe what could be on his computer that would be going to the Internet exactly every hour. He informs them of his new weather toolbar he installed. Obviously the sheer size of the spikes indicates that it's probably not just going back to the site to get weather statistics, there is most likely some kind of malware installed on this computer.

Daily

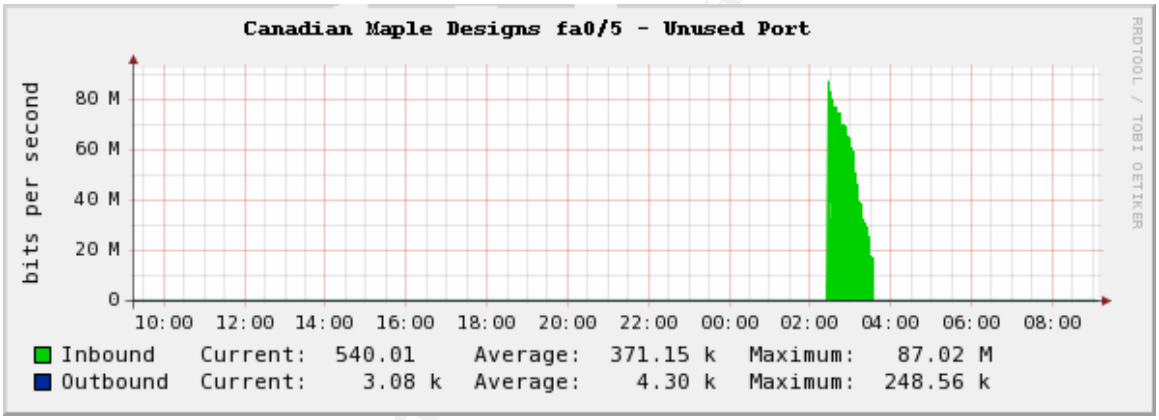


Now that we have reviewed some of the Cacti graphs from the daily events on Canadian Maple Design's network, let's start to explore how we could use these graphs as Security Analysts to aid in our detection of suspicious events.

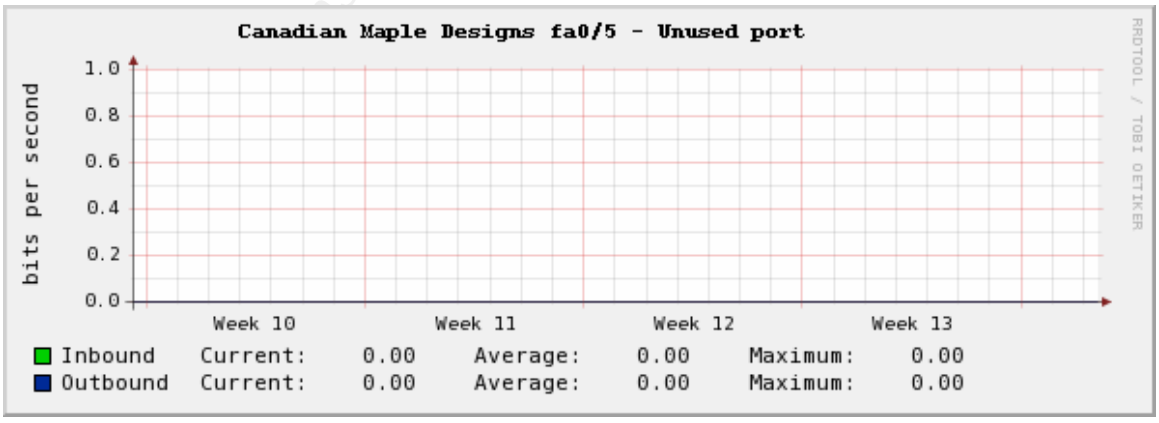
Scenario 4

What is the first thing that catches your eye on the graph pictured below? Obviously there is a large spike that occurred on the network at around 2:20 a.m. What is unusual about this graph is the lack of activity on the port as indicated by the daily and weekly graphs pictured below. We can see that on the label of the graph it says "Unused Port". This is considered suspicious as the port has been inactive for months, yet all of a sudden at around 2:00 in the morning we are seeing large volumes of traffic on the port.

Daily

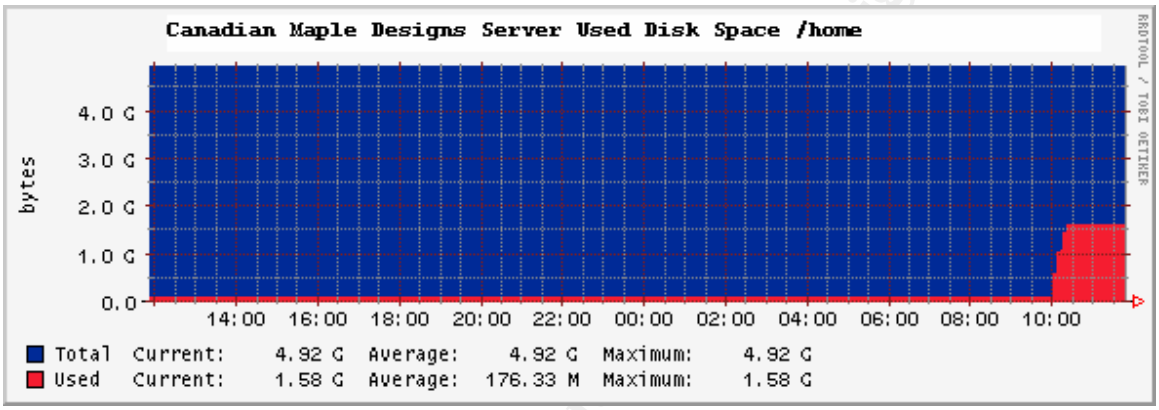


Weekly



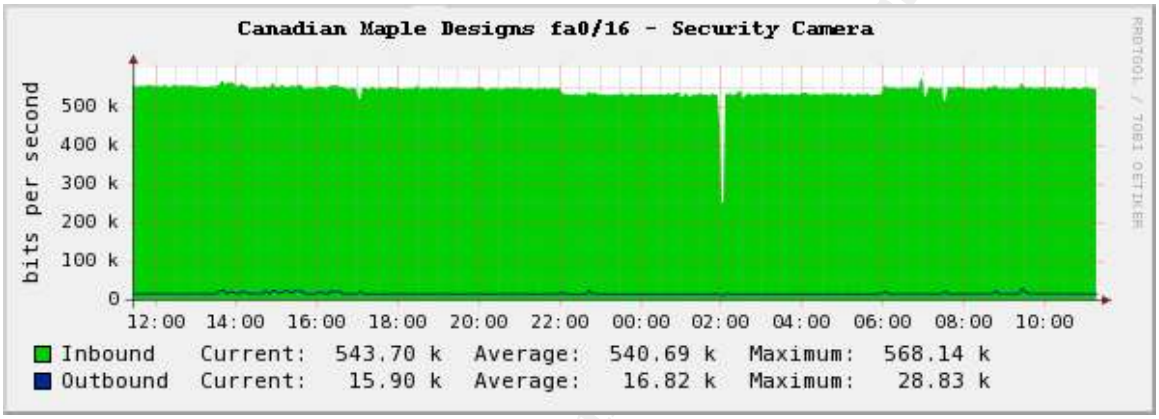
Scenario 5

Let's take a look at another cacti graph. This graph represents used disk space for Canadian Maple Designs main Server. The thing that really jumps out is the large increase in disk space usage towards the end of the day. This is very suspicious as this is a restricted box that only two System Administrators have access to.



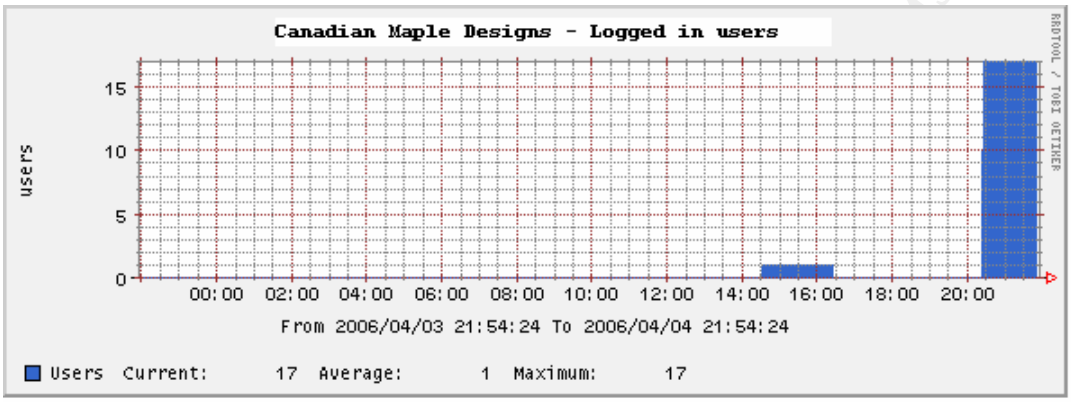
Scenario 6

At first glance this cacti graph is a bit startling. What on earth could be causing that much inbound traffic? Well thank goodness the IT team is so well organized and have all of their ports labeled properly, as we can see this is the video camera that is installed on the floor for security purposes. It is very important when analyzing the cacti graphs to make sure your information is correct and that you don't jump to conclusions before thoroughly researching an event.



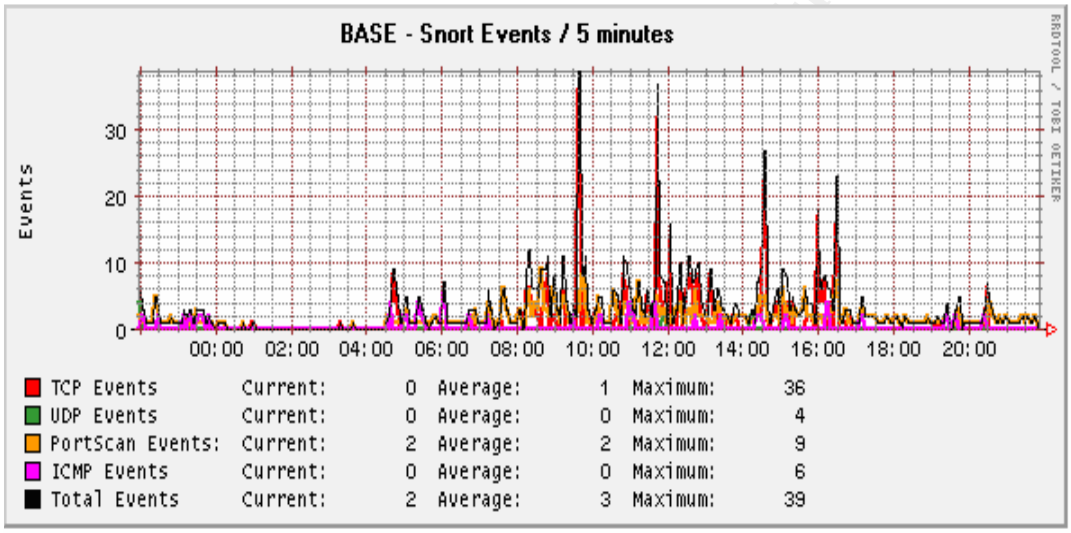
Scenario 7

Here is a graph that shows how many users are logged on at any given time. What is frightening about this graph is that it is indicating that at around 8:30p.m there are 17 users logged on to the server. This is way out of the norm for this server as there are only two System Administrators that have access to this box and neither of them works past 4:30 on any given day.



Bonus Cacti Graph

Here is a bonus graph created by the IT team at Canadian Maple Designs. Instead of pouring through various snort event reports from Base one of the guys decided to create a cacti template for Base based off of the MySql cacti templates. Note the different colors for the different protocols. This graph allows for the analyst to spot large volumes of events or errors much more efficiently. This graph was provided by Shannon McNaught at http://www.chekmate.org/wiki/index.php/Snort-Cacti.



Conclusion

Cacti graphs are very useful tool to aid in the detection of anomalous events on your network. After pouring through thousands of lines of syslogs and hundreds of events triggered by your IDS you can finally take off your loggles (goggles used for reading log files) and feast your eyes on some beautiful looking cacti graphs. They are very easy to implement and give the Security Professional another check and balance in the growing world of security technology. They are by no means a silver bullet in defending your network, but by using visual baselines you are able to catch things that may not have been as noticeable in your logs.

References

Software websites used:

http://www.cacti.net/

http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

http://www.internetsecurityguru.com/ which can also be found at

http://www.snort.org/docs/setup_guides/snort_base_SSL.pdf

http://www.snort.org

http://www.centos.org

http://dag.wieers.com/

Crontab Quick Reference http://www.adminschoice.com/docs/crontab.htm

Creating Round Robin databases
http://www.cuddletech.com/articles/rrd/ar01s02.html

MySQL graph creation http://forums.cacti.net/about6108.html&highlight=mysql

Appendix A

Cisco PIX 506E Configuration

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password ******* encrypted
passwd ******* encrypted
hostname cmdlab
domain-name domain.local
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list   101   permit   ip   172.20.73.0   255.255.255.0
172.14.73.0 255.255.255.0
access-list acl-out permit ip any any
pager lines 24
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500
ip address outside 257.119.160.73 255.255.255.128
ip address inside 172.20.73.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 172.14.73.1-172.14.73.254
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-group acl-out in interface outside
route outside 0.0.0.0 0.0.0.0 257.119.160.1 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client token authentication LOCAL
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
isakmp keepalive 3600
isakmp nat-traversal 20
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup cmdlab address-pool vpnpool
vpngroup cmdlab split-tunnel 101
vpngroup cmdlab idle-time 1800
vpngroup cmdlab password *******
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh 172.20.73.0 255.255.255.0 inside
ssh 172.14.73.0 255.255.255.0 inside
ssh timeout 60
management-access inside
console timeout 0
dhcpd address 172.20.73.10-172.20.73.50 inside
dhcpd dns 257.119.160.4
dhcpd lease 3600
dhcpd ping_timeout 750
```

```
dhcpd enable inside
username student password ******* privilege 15
username pixadmin password ******* privilege 15
terminal width 80
```

Appendix B

Cisco Catalyst 2900 Configuration

```
Using 2012 out of 32768 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cmdlab
!
enable secret *******
!
!
!
!
!
!
ip subnet-zero
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
```

```
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 port monitor FastEthernet0/1
 port monitor FastEthernet0/2
 port monitor FastEthernet0/3
 port monitor FastEthernet0/4
 port monitor FastEthernet0/5
 port monitor FastEthernet0/6
 port monitor FastEthernet0/7
 port monitor FastEthernet0/8
 port monitor FastEthernet0/9
 port monitor FastEthernet0/10
 port monitor FastEthernet0/11
 port monitor FastEthernet0/12
 port monitor FastEthernet0/13
 port monitor FastEthernet0/14
 port monitor FastEthernet0/15
 port monitor FastEthernet0/16
 port monitor FastEthernet0/17
 port monitor FastEthernet0/18
 port monitor FastEthernet0/19
 port monitor FastEthernet0/20
 port monitor FastEthernet0/21
 port monitor FastEthernet0/22
```

```
 port monitor FastEthernet0/23
 port monitor VLAN1
!
interface VLAN1
 ip address 172.20.73.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 172.20.73.1
snmp-server engineID local *******
snmp-server community ******* RW
snmp-server community ******* RO
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 password ******
 login
line vty 5 15
 password ******
 login
!
end
```

Appendix C

Snort Cacti Template


```
- <cacti>
- <hash_000009089329b99b340d968ff88bbfb4555e55>
  <name>BASE - Traffic Profile</name>
- <graph>
  <t_title />
  <title>|host_description| - BASE - Snort Events / 5 Mins</title>
  <t_image_format_id />
  <image_format_id>1</image_format_id>
  <t_height />
  <height>120</height>
  <t_width />
  <width>500</width>
  <t_auto_scale />
  <auto_scale>on</auto_scale>
  <t_auto_scale_opts />
  <auto_scale_opts>2</auto_scale_opts>
  <t_auto_scale_log />
  <auto_scale_log />
  <t_auto_scale_rigid />
  <auto_scale_rigid>on</auto_scale_rigid>
  <t_auto_padding />
  <auto_padding>on</auto_padding>
  <t_export />
  <export>on</export>
  <t_upper_limit />
  <upper_limit>100</upper_limit>
  <t_lower_limit />
  <lower_limit>0</lower_limit>
  <t_base_value />
  <base_value>1000</base_value>
  <t_unit_value />
  <unit_value />
  <t_unit_exponent_value />
  <unit_exponent_value />
  <t_vertical_label />
  <vertical_label>Events</vertical_label>
    </graph>
- <items>
- <hash_100009feff36f01d5e7b8a5ef4cd167729c8b9>
  <task_item_id>hash_08000994426d13bd0129e9c2fcb84fdd214458</task_item_id>
  <color_id>FF0000</color_id>
  <graph_type_id>5</graph_type_id>
  <consolidation_function_id>4</consolidation_function_id>
  <cdef_id>0</cdef_id>
  <value />
  <gprint_id>hash_06000919414480d6897c8731c7dc6c5310653e</gprint_id>
  <text_format>TCP Events</text_format>
  <hard_return />
  <sequence>1</sequence>
    </hash_100009feff36f01d5e7b8a5ef4cd167729c8b9>
```

- <hash_1000096038e9963b300390159bb0dc988b63b2>
  <task_item_id>**hash_08000994426d13bd0129e9c2fcb84fdd214458**</task_item_id>
  <color_id>**0**</color_id>
  <graph_type_id>**9**</graph_type_id>
  <consolidation_function_id>**4**</consolidation_function_id>
  <cdef_id>**0**</cdef_id>
  <value />
  <gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
  <text_format>**Current:**</text_format>
  <hard_return />
  <sequence>**2**</sequence>
    </hash_1000096038e9963b300390159bb0dc988b63b2>
- <hash_100009b6b956b3776cbdbacd8059451235c185>
  <task_item_id>**hash_08000994426d13bd0129e9c2fcb84fdd214458**</task_item_id>
  <color_id>**0**</color_id>
  <graph_type_id>**9**</graph_type_id>
  <consolidation_function_id>**1**</consolidation_function_id>
  <cdef_id>**0**</cdef_id>
  <value />
  <gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
  <text_format>**Average:**</text_format>
  <hard_return />
  <sequence>**3**</sequence>
    </hash_100009b6b956b3776cbdbacd8059451235c185>
- <hash_1000096dd9f63bd89c4fc261bf5d144637b5f8>
  <task_item_id>**hash_08000994426d13bd0129e9c2fcb84fdd214458**</task_item_id>
  <color_id>**0**</color_id>
  <graph_type_id>**9**</graph_type_id>
  <consolidation_function_id>**3**</consolidation_function_id>
  <cdef_id>**0**</cdef_id>
  <value />
  <gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
  <text_format>**Maximum:**</text_format>
  <hard_return>**on**</hard_return>
  <sequence>**4**</sequence>
    </hash_1000096dd9f63bd89c4fc261bf5d144637b5f8>
- <hash_10000903d8679669af481fb5e988725233fbb2>
  <task_item_id>**hash_080009411b641db3c666a232a41a3f7e2baea4**</task_item_id>
  <color_id>**35962B**</color_id>
  <graph_type_id>**5**</graph_type_id>
  <consolidation_function_id>**4**</consolidation_function_id>
  <cdef_id>**0**</cdef_id>
  <value />
  <gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
  <text_format>**UDP Events**</text_format>
  <hard_return />
  <sequence>**5**</sequence>
    </hash_10000903d8679669af481fb5e988725233fbb2>
- <hash_100009b890a7d5c25f31a4d3e05dbbaefbd753>
  <task_item_id>**hash_080009411b641db3c666a232a41a3f7e2baea4**</task_item_id>
  <color_id>**0**</color_id>
  <graph_type_id>**9**</graph_type_id>
  <consolidation_function_id>**4**</consolidation_function_id>
  <cdef_id>**0**</cdef_id>
  <value />
  <gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>

<text_format>**Current:**</text_format>
<hard_return />
<sequence>**6**</sequence>
</hash_100009b890a7d5c25f31a4d3e05dbbaefbd753>
- <hash_100009bd10c8e30c730b6a402e56cfadcb87fb>
<task_item_id>**hash_080009411b641db3c666a232a41a3f7e2baea4**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**1**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Average:**</text_format>
<hard_return />
<sequence>**7**</sequence>
</hash_100009bd10c8e30c730b6a402e56cfadcb87fb>
- <hash_1000096ab595d4ad0ec44f06ccc2cc42705ddb>
<task_item_id>**hash_080009411b641db3c666a232a41a3f7e2baea4**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**3**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Maximum:**</text_format>
<hard_return>**on**</hard_return>
<sequence>**8**</sequence>
</hash_1000096ab595d4ad0ec44f06ccc2cc42705ddb>
- <hash_100009de2421ea8815ac6cf44bfa3bc1ce0506>
<task_item_id>**hash_0800090ecc57565cc0b42da5cf9b22733470d1**</task_item_id>
<color_id>**FF9900**</color_id>
<graph_type_id>**5**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**PortScan Events:**</text_format>
<hard_return />
<sequence>**9**</sequence>
</hash_100009de2421ea8815ac6cf44bfa3bc1ce0506>
- <hash_1000095a476abe1f020da01e5e7871c52df4ef>
<task_item_id>**hash_0800090ecc57565cc0b42da5cf9b22733470d1**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Current:**</text_format>
<hard_return />
<sequence>**10**</sequence>
</hash_1000095a476abe1f020da01e5e7871c52df4ef>
- <hash_100009122285a99673c84f919bcb2dea451d09>
<task_item_id>**hash_0800090ecc57565cc0b42da5cf9b22733470d1**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>

<consolidation_function_id>**1**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Average:**</text_format>
<hard_return />
<sequence>**11**</sequence>
</hash_100009122285a99673c84f919bcb2dea451d09>
- <hash_100009ce166caadc309632247048865fc2df6f>
<task_item_id>**hash_0800090ecc57565cc0b42da5cf9b22733470d1**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**3**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Maximum:**</text_format>
<hard_return>**on**</hard_return>
<sequence>**12**</sequence>
</hash_100009ce166caadc309632247048865fc2df6f>
- <hash_1000099cf5e4da97e478874a901a8655be192c>
<task_item_id>**hash_080009efe52ed8f1a2ddfb82f987f8fac3a633**</task_item_id>
<color_id>**FF00FF**</color_id>
<graph_type_id>**5**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**ICMP Events**</text_format>
<hard_return />
<sequence>**13**</sequence>
</hash_1000099cf5e4da97e478874a901a8655be192c>
- <hash_100009a85382df80f590b52186bab913c782b4>
<task_item_id>**hash_080009efe52ed8f1a2ddfb82f987f8fac3a633**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Current:**</text_format>
<hard_return />
<sequence>**14**</sequence>
</hash_100009a85382df80f590b52186bab913c782b4>
- <hash_10000956561d9bfac79760a4c65c4b7c00517d>
<task_item_id>**hash_080009efe52ed8f1a2ddfb82f987f8fac3a633**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**1**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Average:**</text_format>
<hard_return />
<sequence>**15**</sequence>
</hash_10000956561d9bfac79760a4c65c4b7c00517d>

- <hash_1000093a9f559376a79a94849b8303ef21ff92>
<task_item_id>**hash_080009efe52ed8f1a2ddfb82f987f8fac3a633**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**3**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Maximum:**</text_format>
<hard_return>**on**</hard_return>
<sequence>**16**</sequence>
</hash_1000093a9f559376a79a94849b8303ef21ff92>
- <hash_100009b52fff359249ba2f4757cfef54c6720d>
<task_item_id>**hash_080009887e94cbde36c02130b437573f6304ca**</task_item_id>
<color_id>**000000**</color_id>
<graph_type_id>**4**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Total Events**</text_format>
<hard_return />
<sequence>**17**</sequence>
</hash_100009b52fff359249ba2f4757cfef54c6720d>
- <hash_1000093cf72c83b7ded615cdbe5cf203d402ef>
<task_item_id>**hash_080009887e94cbde36c02130b437573f6304ca**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**4**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Current:**</text_format>
<hard_return />
<sequence>**18**</sequence>
</hash_1000093cf72c83b7ded615cdbe5cf203d402ef>
- <hash_100009d0bf857d67908de5ad3d2e19f382c28d>
<task_item_id>**hash_080009887e94cbde36c02130b437573f6304ca**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**1**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>
<text_format>**Average:**</text_format>
<hard_return />
<sequence>**19**</sequence>
</hash_100009d0bf857d67908de5ad3d2e19f382c28d>
- <hash_1000090aadd3168741a8644165ac865a0f4619>
<task_item_id>**hash_080009887e94cbde36c02130b437573f6304ca**</task_item_id>
<color_id>**0**</color_id>
<graph_type_id>**9**</graph_type_id>
<consolidation_function_id>**3**</consolidation_function_id>
<cdef_id>**0**</cdef_id>
<value />
<gprint_id>**hash_06000919414480d6897c8731c7dc6c5310653e**</gprint_id>

<text_format>**Maximum:**</text_format>
<hard_return>**on**</hard_return>
<sequence>**20**</sequence>
</hash_1000090aadd3168741a8644165ac865a0f4619>
</items>
- <inputs>
- <hash_090009e065f4d6463b466db12fcf8bde42c838>
<name>**Data Source [portscan]**</name>
<description />
<column_name>**task_item_id**</column_name>

<items>**hash_000009de2421ea8815ac6cf44bfa3bc1ce0506|hash_0000095a476abe1f020da01e5e7871c52df4ef|hash_000009122285a99673c84f919bcb2dea451d09|hash_000009ce166caadc309632247048865fc2df6f**</items>
</hash_090009e065f4d6463b466db12fcf8bde42c838>
- <hash_090009209bfb82d2f2fc41a86d71f333ea5bb3>
<name>**Data Source [total]**</name>
<description />
<column_name>**task_item_id**</column_name>

<items>**hash_000009b52fff359249ba2f4757cfef54c6720d|hash_0000093cf72c83b7ded615cdbe5cf203d402ef|hash_000009d0bf857d67908de5ad3d2e19f382c28d|hash_0000090aadd3168741a8644165ac865a0f4619**</items>
</hash_090009209bfb82d2f2fc41a86d71f333ea5bb3>
- <hash_090009f0656ed0204896dc5e1939efe8307a8a>
<name>**Data Source [icmp]**</name>
<description />
<column_name>**task_item_id**</column_name>

<items>**hash_0000099cf5e4da97e478874a901a8655be192c|hash_000009a85382df80f590b52186bab913c782b4|hash_00000956561d9bfac79760a4c65c4b7c00517d|hash_0000093a9f559376a79a94849b8303ef21ff92**</items>
</hash_090009f0656ed0204896dc5e1939efe8307a8a>
- <hash_090009ff3515018c5ad6463644016ae6d35008>
<name>**Data Source [tcp]**</name>
<description />
<column_name>**task_item_id**</column_name>

<items>**hash_000009feff36f01d5e7b8a5ef4cd167729c8b9|hash_0000096038e9963b300390159bb0dc988b63b2|hash_000009b6b956b3776cbdbacd8059451235c185|hash_0000096dd9f63bd89c4fc261bf5d144637b5f8**</items>
</hash_090009ff3515018c5ad6463644016ae6d35008>
- <hash_0900094313e6ab33bd4c6679fbcf8d582c9123>
<name>**Data Source [udp]**</name>
<description />
<column_name>**task_item_id**</column_name>

<items>**hash_00000903d8679669af481fb5e988725233fbb2|hash_000009b890a7d5c25f31a4d3e05dbbaefbd753|hash_000009bd10c8e30c730b6a402e56cfadcb87fb|hash_0000096ab595d4ad0ec44f06ccc2cc42705ddb**</items>
</hash_0900094313e6ab33bd4c6679fbcf8d582c9123>
</inputs>
</hash_000009089329b99b340d968ff88bbfb4555e55>
- <hash_01000910ca6ad4f48450bf275a5d842e9a2fdc>
<name>**BASE - Traffic Profile**</name>
- <ds>

```
  <t_name />
  <name>BASE - Traffic Profile</name>
  <data_input_id>hash_030009069af24d69a17ff682d3588ef0156e06</data_input_id>
  <t_rra_id />
  <t_rrd_step />
  <rrd_step>300</rrd_step>
  <t_active />
  <active>on</active>

      <rra_items>hash_150009c21df5178e5c955013591239eb0afd46|hash_1500090d9c0af8b8acd
      c7807943937b3208e29|hash_1500096fc2d038fb42950138b0ce3e9874cc60|hash_150009e36f
      3adb9f152adfa5dc50fd2b23337e</rra_items>
    </ds>
- <items>
- <hash_080009efe52ed8f1a2ddfb82f987f8fac3a633>
  <t_data_source_name />
  <data_source_name>icmp</data_source_name>
  <t_rrd_minimum />
  <rrd_minimum>0</rrd_minimum>
  <t_rrd_maximum />
  <rrd_maximum>10000000000</rrd_maximum>
  <t_data_source_type_id />
  <data_source_type_id>1</data_source_type_id>
  <t_rrd_heartbeat />
  <rrd_heartbeat>600</rrd_heartbeat>
  <t_data_input_field_id />
  <data_input_field_id>hash_07000913a961cbbe30928d1a6acf3713971df6</data_input_field_id>
    </hash_080009efe52ed8f1a2ddfb82f987f8fac3a633>
- <hash_080009411b641db3c666a232a41a3f7e2baea4>
  <t_data_source_name />
  <data_source_name>udp</data_source_name>
  <t_rrd_minimum />
  <rrd_minimum>0</rrd_minimum>
  <t_rrd_maximum />
  <rrd_maximum>10000000000</rrd_maximum>
  <t_data_source_type_id />
  <data_source_type_id>1</data_source_type_id>
  <t_rrd_heartbeat />
  <rrd_heartbeat>600</rrd_heartbeat>
  <t_data_input_field_id />
  <data_input_field_id>hash_070009873aed518380d69e309666bd4ac7a5d4</data_input_field_id>
    </hash_080009411b641db3c666a232a41a3f7e2baea4>
- <hash_080009887e94cbde36c02130b437573f6304ca>
  <t_data_source_name />
  <data_source_name>total</data_source_name>
  <t_rrd_minimum />
  <rrd_minimum>0</rrd_minimum>
  <t_rrd_maximum />
  <rrd_maximum>10000000000</rrd_maximum>
  <t_data_source_type_id />
  <data_source_type_id>1</data_source_type_id>
  <t_rrd_heartbeat />
  <rrd_heartbeat>600</rrd_heartbeat>
  <t_data_input_field_id />
  <data_input_field_id>hash_0700095bf540d0bcc1ce5298a1a223423a8ba0</data_input_field_id>
    </hash_080009887e94cbde36c02130b437573f6304ca>
```

- <hash_08000994426d13bd0129e9c2fcb84fdd214458>
  <t_data_source_name />
  <data_source_name>**tcp**</data_source_name>
  <t_rrd_minimum />
  <rrd_minimum>**0**</rrd_minimum>
  <t_rrd_maximum />
  <rrd_maximum>**10000000000**</rrd_maximum>
  <t_data_source_type_id />
  <data_source_type_id>**1**</data_source_type_id>
  <t_rrd_heartbeat />
  <rrd_heartbeat>**600**</rrd_heartbeat>
  <t_data_input_field_id />
  <data_input_field_id>**hash_0700093aebb47180f596bb700361f5ce6356f6**</data_input_field_id>
    </hash_08000994426d13bd0129e9c2fcb84fdd214458>
- <hash_0800090ecc57565cc0b42da5cf9b22733470d1>
  <t_data_source_name />
  <data_source_name>**portscan**</data_source_name>
  <t_rrd_minimum />
  <rrd_minimum>**0**</rrd_minimum>
  <t_rrd_maximum />
  <rrd_maximum>**10000000000**</rrd_maximum>
  <t_data_source_type_id />
  <data_source_type_id>**1**</data_source_type_id>
  <t_rrd_heartbeat />
  <rrd_heartbeat>**600**</rrd_heartbeat>
  <t_data_input_field_id />
  <data_input_field_id>**hash_070009641b22c53f2bc0ae9d31774d4caf7f06**</data_input_field_id>
    </hash_0800090ecc57565cc0b42da5cf9b22733470d1>
    </items>
- <data>
- <item_000>
  <data_input_field_id>**hash_070009558d71ece6bd40ba226c3cf0a2653498**</data_input_field_id>
  <t_value>**on**</t_value>
  <value />
    </item_000>
- <item_001>
  <data_input_field_id>**hash_0700090adc0b7e0dc15675e5b5acac015341eb**</data_input_field_id>
  <t_value>**on**</t_value>
  <value />
    </item_001>
- <item_002>
  <data_input_field_id>**hash_0700096aaf622b92e70da36bdea951a7b73f8d**</data_input_field_id>
  <t_value />
  <value />
    </item_002>
    </data>
    </hash_01000910ca6ad4f48450bf275a5d842e9a2fdc>
- <hash_030009069af24d69a17ff682d3588ef0156e06>
  <name>**BASE - Traffic Profile**</name>
  <type_id>**1**</type_id>
  <input_string>**<path_php_binary> -q <path_cacti>/scripts/BASE.php trafficprofile <hostname> <username> <password>**</input_string>
- <fields>
- <hash_0700096aaf622b92e70da36bdea951a7b73f8d>
  <name>**Database Host**</name>
  <update_rra />

```
  <regexp_match />
  <allow_nulls>on</allow_nulls>
  <type_code>hostname</type_code>
  <input_output>in</input_output>
  <data_name>hostname</data_name>
     </hash_0700096aaf622b92e70da36bdea951a7b73f8d>
- <hash_0700090adc0b7e0dc15675e5b5acac015341eb>
  <name>Database User</name>
  <update_rra />
  <regexp_match />
  <allow_nulls>on</allow_nulls>
  <type_code />
  <input_output>in</input_output>
  <data_name>username</data_name>
     </hash_0700090adc0b7e0dc15675e5b5acac015341eb>
- <hash_070009558d71ece6bd40ba226c3cf0a2653498>
  <name>Database Password</name>
  <update_rra />
  <regexp_match />
  <allow_nulls>on</allow_nulls>
  <type_code />
  <input_output>in</input_output>
  <data_name>password</data_name>
     </hash_070009558d71ece6bd40ba226c3cf0a2653498>
- <hash_0700095bf540d0bcc1ce5298a1a223423a8ba0>
  <name>Total Events</name>
  <update_rra>on</update_rra>
  <regexp_match />
  <allow_nulls />
  <type_code />
  <input_output>out</input_output>
  <data_name>total</data_name>
     </hash_0700095bf540d0bcc1ce5298a1a223423a8ba0>
- <hash_0700093aebb47180f596bb700361f5ce6356f6>
  <name>TCP Events</name>
  <update_rra>on</update_rra>
  <regexp_match />
  <allow_nulls />
  <type_code />
  <input_output>out</input_output>
  <data_name>tcp</data_name>
     </hash_0700093aebb47180f596bb700361f5ce6356f6>
- <hash_070009873aed518380d69e309666bd4ac7a5d4>
  <name>UDP Events</name>
  <update_rra>on</update_rra>
  <regexp_match />
  <allow_nulls />
  <type_code />
  <input_output>out</input_output>
  <data_name>udp</data_name>
     </hash_070009873aed518380d69e309666bd4ac7a5d4>
- <hash_07000913a961cbbe30928d1a6acf3713971df6>
  <name>ICMP Events</name>
  <update_rra>on</update_rra>
  <regexp_match />
  <allow_nulls />
```

```
  <type_code />
  <input_output>out</input_output>
  <data_name>icmp</data_name>
     </hash_07000913a961cbbe30928d1a6acf3713971df6>
- <hash_070009641b22c53f2bc0ae9d31774d4caf7f06>
  <name>PortScan Events</name>
  <update_rra>on</update_rra>
  <regexp_match />
  <allow_nulls />
  <type_code />
  <input_output>out</input_output>
  <data_name>portscan</data_name>
     </hash_070009641b22c53f2bc0ae9d31774d4caf7f06>
     </fields>
     </hash_030009069af24d69a17ff682d3588ef0156e06>
- <hash_150009c21df5178e5c955013591239eb0afd46>
  <name>Daily (5 Minute Average)</name>
  <x_files_factor>0.5</x_files_factor>
  <steps>1</steps>
  <rows>600</rows>
  <timespan>86400</timespan>
  <cf_items>1|2|3|4</cf_items>
     </hash_150009c21df5178e5c955013591239eb0afd46>
- <hash_1500090d9c0af8b8acdc7807943937b3208e29>
  <name>Weekly (30 Minute Average)</name>
  <x_files_factor>0.5</x_files_factor>
  <steps>6</steps>
  <rows>700</rows>
  <timespan>604800</timespan>
  <cf_items>1|2|3|4</cf_items>
     </hash_1500090d9c0af8b8acdc7807943937b3208e29>
- <hash_1500096fc2d038fb42950138b0ce3e9874cc60>
  <name>Monthly (2 Hour Average)</name>
  <x_files_factor>0.5</x_files_factor>
  <steps>24</steps>
  <rows>775</rows>
  <timespan>2678400</timespan>
  <cf_items>1|2|3|4</cf_items>
     </hash_1500096fc2d038fb42950138b0ce3e9874cc60>
- <hash_150009e36f3adb9f152adfa5dc50fd2b23337e>
  <name>Yearly (1 Day Average)</name>
  <x_files_factor>0.5</x_files_factor>
  <steps>288</steps>
  <rows>797</rows>
  <timespan>33053184</timespan>
  <cf_items>1|2|3|4</cf_items>
     </hash_150009e36f3adb9f152adfa5dc50fd2b23337e>
- <hash_06000919414480d6897c8731c7dc6c5310653e>
  <name>Exact Numbers</name>
  <gprint_text>%8.0lf</gprint_text>
     </hash_06000919414480d6897c8731c7dc6c5310653e>
     </cacti>
```