NetFlow Analysis

Jonzy
Data Security Analysis, Sr.

Information Security Office

NetFlow Analysis
Intrusion Detection, Protection, and Usage Reporting

NetFlow is a cornucopia of information that allows for: Intrusion Detection, Bandwidth usage, and network problem resolution, to name a few. The University of Utah has been using this information for the past 8 years, to automatically block problematic traffic, manually block malicious sites, and generate traffic reports for local Administrators, as well as generate reports on local subnets, or Departments, for the percentage of bandwidth being used. My presentation shows how to use NetFlow data to: block on known patterns, generate reports, and allow administrators the ability to view information about their local networks. The problem with implementing automatic blocking, is the need for 0 false positives. Pattern matching is the key here. Not only must a pattern be observed, other thresholds must be exceeded, to ensure a block is not falsely implemented. Slow probes are difficult to identify, but the obvious patterns are easy to process. By breaking the time frame down for specific searches, problematic traffic, both Inbound and Outbound, can be addressed. Inbound analysis protects the local environment, while the Outbound analysis is being a good net citizen. Some patterns are relevant to both Inbound and Outbound traffic, such as mail-bombs or excessive SMTP, bot-nets, icmp attacks, and virus propagation. Inbound attacks have their own concerns such as: denial of services attacks, distributed attacks are harder to identify and whack-a-mole is not a solution. Using automation to identify and react to problematic network traffic is essential in todays computing environment. There is information available via NetFlow Analysis to help secure your local network. With NetFlow Analysis, a Firewall, and the ability to identify problematic traffic quickly, one can sleep well at night knowing their network is better protected.

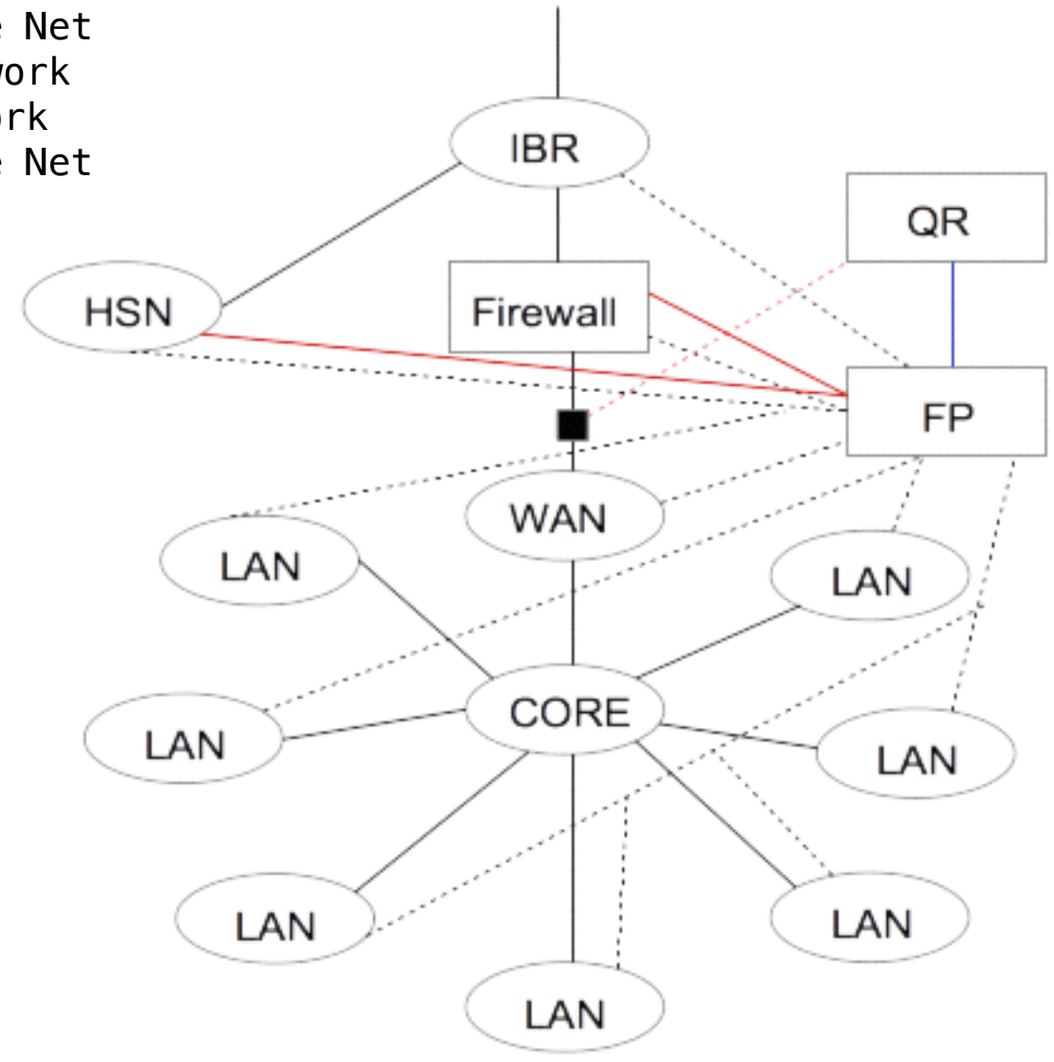
THE UNIVERSITY OF UTAH

Information Security Office

Network Layout / Flow Collection

IBR - 2 routers, with a 100 Gb/s channel to the Net
WAN - 2 routers, with a 10 Gb/s commodity network
LAN - 28 routers, with a 10 Gb/s internal network
HSN - 1 router, with a 100 Gb/s channel to the Net
FP - Flow Processor

Null-route / Blockage
Netflow Collection
QR to FP link
QR Tap



THE UNIVERSITY OF UTAH

Information Security Office

Flow Collection Hardware and Stats

The Collector

HP ProLiant DL380p Gen8

Processor:	2x Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz 6/6 cores; 12 threads 64-bit Capable
Memory:	98 GB DDR3 1333 MHz RAM
Storage:	12x HP 600GB 15K RPM 6GBs SAS Drives configured RAID 5
NIC:	3x 1Gbs copper NIC connected full duplex
Average Load:	less then 1.5, but has been as high as 22.

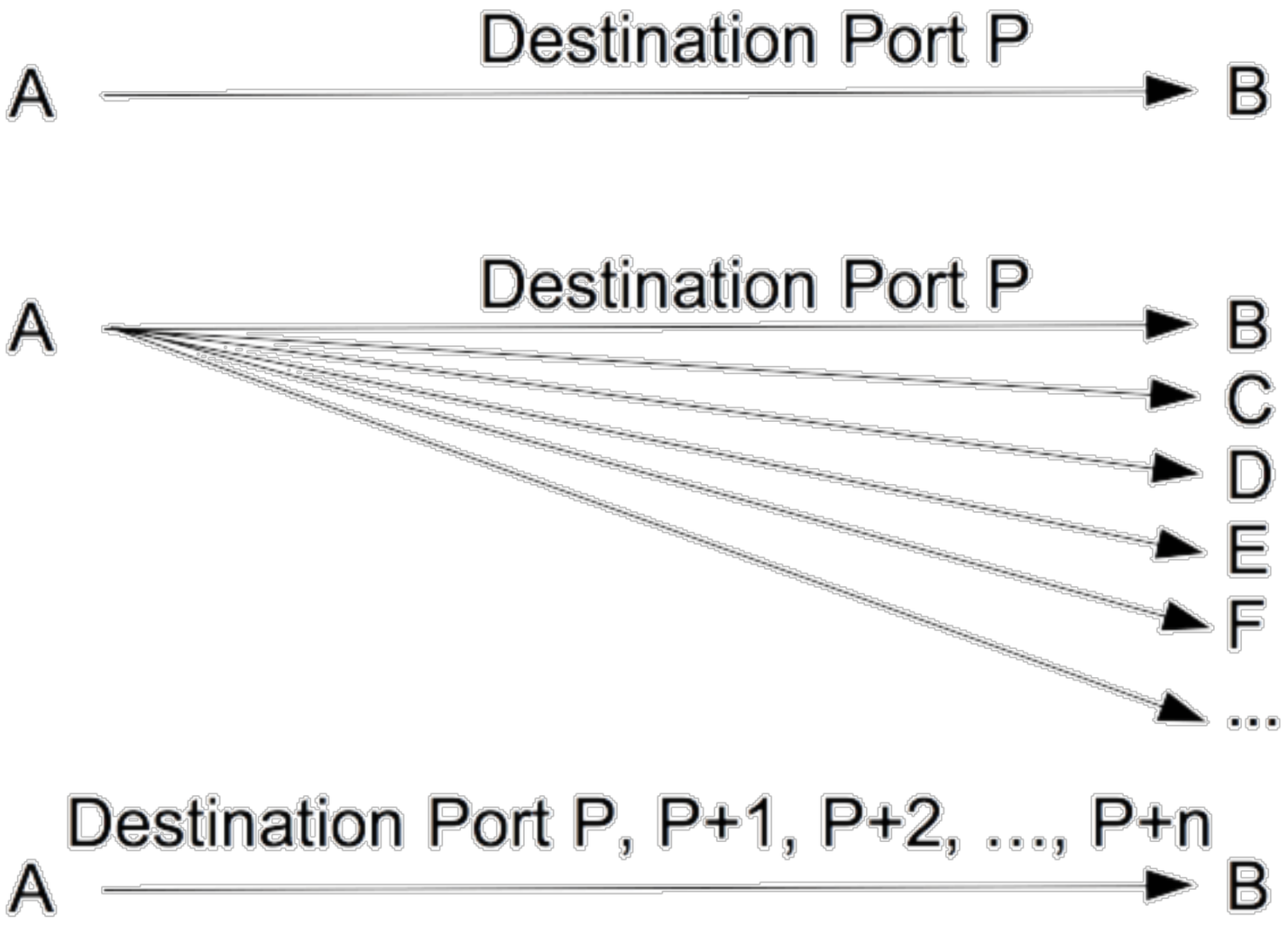
Flow Collection Statistics

COLLECTOR	AVERAGE/DAY NUM_FLOW_RECORDS	AVERAGE_TIME TO_PROCESS_24_HOURS
IBR	685,527,940	11 seconds
WAN	654,118,979	11 seconds
LAN	1,336,572,438	24 seconds
HSN	1,899,668	less then a second

THE UNIVERSITY OF UTAH

Information Security Office

Patterns



THE UNIVERSITY OF UTAH

Information Security Office

Detection

Every 5 minutes Inbound Traffic is processed
blocks observed probes and scans.
blocks known malware patterns.
Every 30 minutes Outbound Traffic is processed
Contacts POC's about problematic traffic.

5 minute job: Pattern matches result in an AUTO-BLOCK except those noted.

```
  22       more than X flows per 5 minutes, where more then Y% destination IP's are unique.
  23       more than X flows per 5 minutes, where more then Y% destination IP's are unique.
  25       more than X flows per 5 minutes, destined to any campus MTA. NO-AUTO-BLOCK.
  53       more than X unique destination IP's per 5 minutes. NO-AUTO-BLOCK.
 110       more than X flows per 5 minutes, where more then Y% destination IP's are unique.
Excessive more then X flows per 5 minutes. NO-AUTO-BLOCK.
```

THE UNIVERSITY OF UTAH

Information Security Office

30 minute job: no auto-blocks, ISO and POC notifications.

WAN

0	flows > X source port 0 destined to not UofU IP space single ICMP flow of Y bytes.
22	flows > X, destined to utah.edu port 22, where Y% of the destination IP's are unique.
25	flows > X, source utah.edu destined to port 25, where Y% of the destination IP's are unique.
53	flows > X, destined to utah.edu port 53.
80	flows > X, destined to not UofU IP space, where Y% of destination IP's are unique.
135-139	flows > X, sourced utah.edu destined to tcp ports 135-139.
445	flows > X, destined not utah.edu port 45, where Y% of the destination IP's are unique.
1025	flows > X, sourced utah.edu, destined to port 1025, where Y% of the destination IP's are unique.
1443	flows > X, sourced utah.edu destined port 1433, where Y% of the destination IP's are unique.
1981	flows > X, sourced utah.edu destined port 1981.
2745	flows > X, sourced utah.edu destined port 2745.
3127-3129	flows > X, sourced utah.edu source ports 1-19,21-79,81-65535 destination Ports 3127-3129, where Y% of the destination IP's are unique.
botnet	any flow sourced utah.edu destination known botnet IP's.
ccnips	any flow sourced utah.edu destination known CNC IP's.
icmp-bomb	flows > X, ICMP sourced utah.edu with packets > Y and bytes > Z.
identical	flows > X, sourced utah.edu, with identical source and destination ports of 0-2491,2493-65535.
ludp	flows > X, UDP sourced utah.edu with more than Y packets.
malware	flows > X, source utah.edu source ports 1025-6880,6882-65535 and destination Ports 42,903,1205,2745,3127,3306,3410,5000 with bytes < Y.
outbound	flows > X, sourced utah.edu destined to not UofU IP space to ports 22 and 5900, where Y% of the destination IP's are unique.
sober	any flow sourced utah.edu destined to known SOBER IP's destination port TCP-37.
storm-skype	flows > X, sourced utah.edu, UDP traffic with Y bytes.
warez	any flows destined to known WAREZ IPs with bytes > Y.

LAN

22	flows > X, sourced utah.edu destination port 22.
25	flows > X, sourced utah.edu destination port 25.
53	flows > X destined to utah.edu nameservers port 53.
135-139	flows > X, sourced utah.edu destination TCP ports 135-139.
445	flows > X, sourced utah.edu destination port 445.
3389	flows > X, sourced utah.edu destination port 3389.
5554	any flow sourced utah.edu source port 5554.
9996	any flow sourced utah.edu destination port 9996.

THE UNIVERSITY OF UTAH

Information Security Office

Protection

All blocks result in a block rule at the Firewall, and null-route at the HSN.
The plan is to null-route at the IBR's, and no longer block at the Firewall.

There is a human interface to manually block, or remove a block.

All blocks are automatically removed via the following algorithm:
The last date the IP was blocked is greater than
7 days * 2 ^ (number of times blocked) the block is removed.

Thus the first time an IP is blocked, it will remain so for 7 days,
the second time, 14 days,
the third time, 28 days,
The forth time, 56 days,
and so on.

THE UNIVERSITY OF UTAH

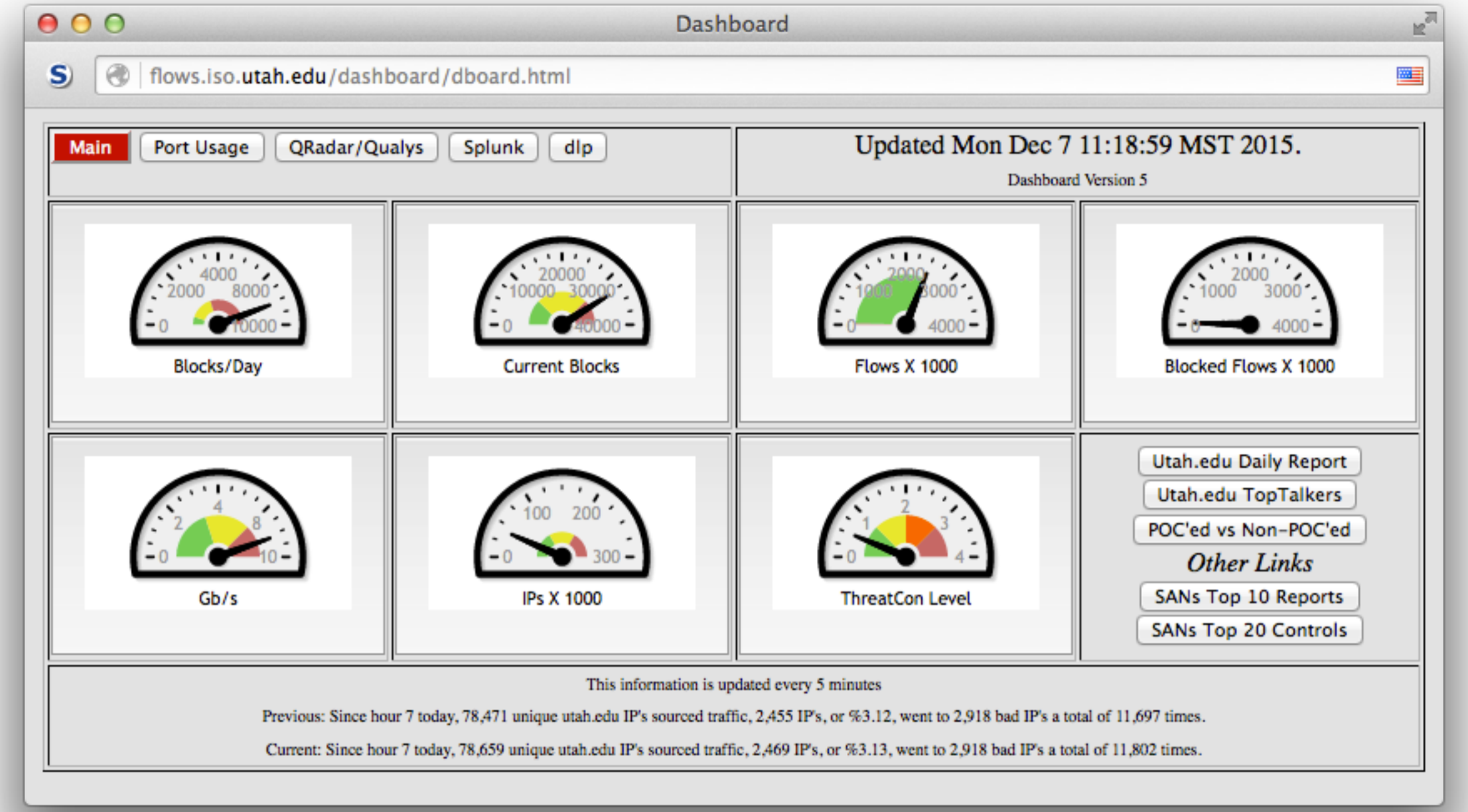
Information Security Office

Reporting

Reports:
- Daily report of Utah utah.edu IP space
- Daily subdomain reports for local admins
- Daily Bandwidth usage reports based on departments

POC (Point of Contact)
- Email is sent to the POC for internal traffic generating potential traffic that may be problematic.

Web Interface:
- Reports
- Activity



THE UNIVERSITY OF UTAH

Information Security Office

Shuns per Day

flows.iso.utah.edu/dashboard/js/shuns.html

Shuns per Day

Go Back

THE UNIVERSITY OF UTAH

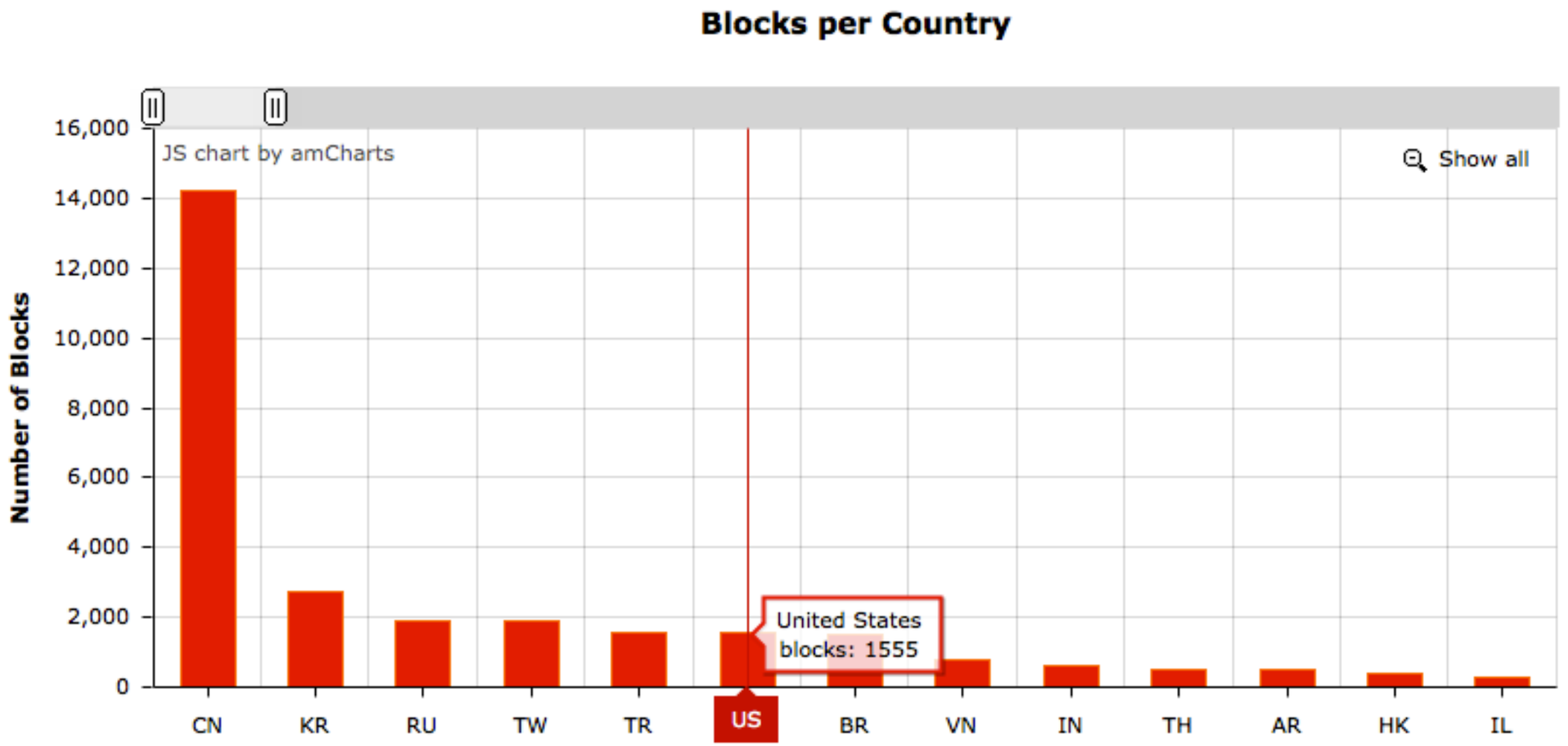
Information Security Office

Blocks per Country

flows.iso.utah.edu/dashboard/blocksbycountry.html

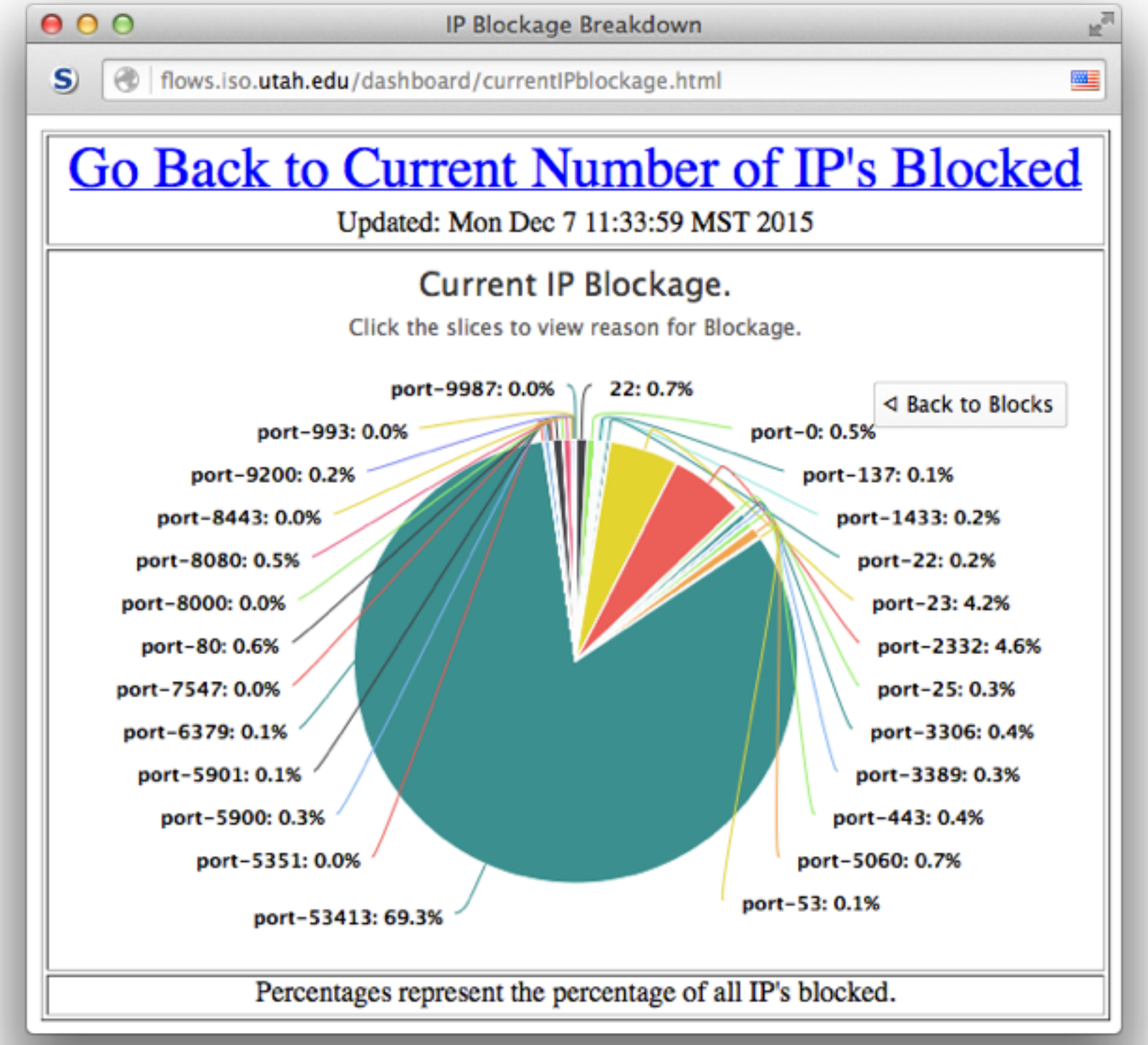
[Go Back]

Updated: Mon Dec 7 15:23:07 MST 2015



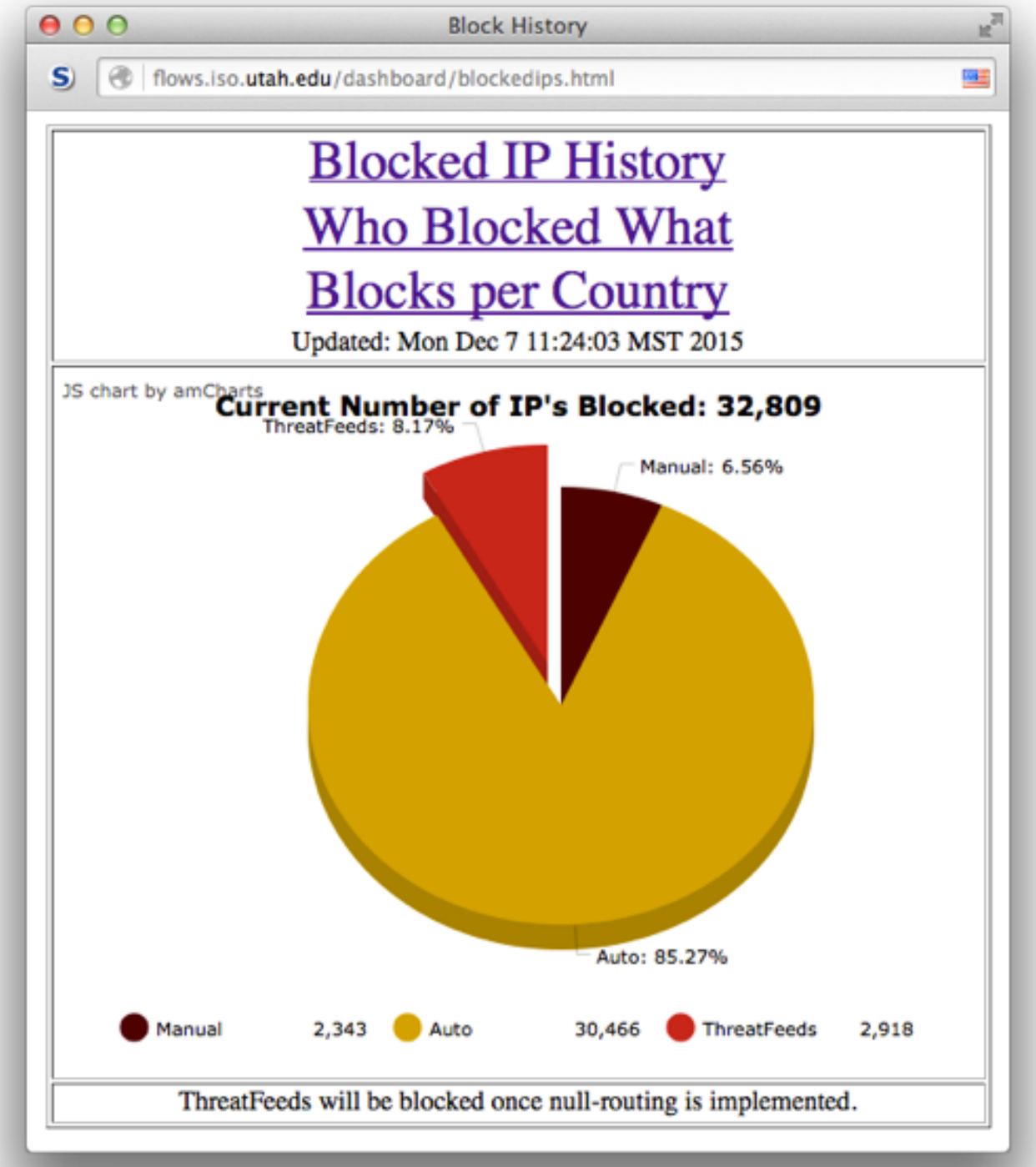
THE UNIVERSITY OF UTAH

Information Security Office



THE UNIVERSITY OF UTAH

Information Security Office



THE UNIVERSITY OF UTAH

Information Security Office

Firewall Blacklist

flows.iso.utah.edu/dashboard/block.log.html

Updated: December 07, 2015, at 11:23

Go Back

The information contained in this file is a description of IP's that have been
automaticly blacklisted per the current algorithm, or manualy blacklisted due
to observed problems or known anomolies.

Automatic blacklisting was implemented Thu Dec 1, 2005 at 08:00:00. As of
February 1, 2006, automatic blocks are removed when the offending IP has not
been seen for 30 days, except those IP's blocked more than once. Manualy
blacklisted IP's are periodicly reviewed and removed as neccessary.

At this time there are 30466 IP's automaticly blocked,
2343 IP's manualy blocked,
for a total of 32809 blocked IP's.

There has been 5930 block(s) during the preceeding 24 hours.
There has been 1 block(s) during the preceeding 5 minutes.

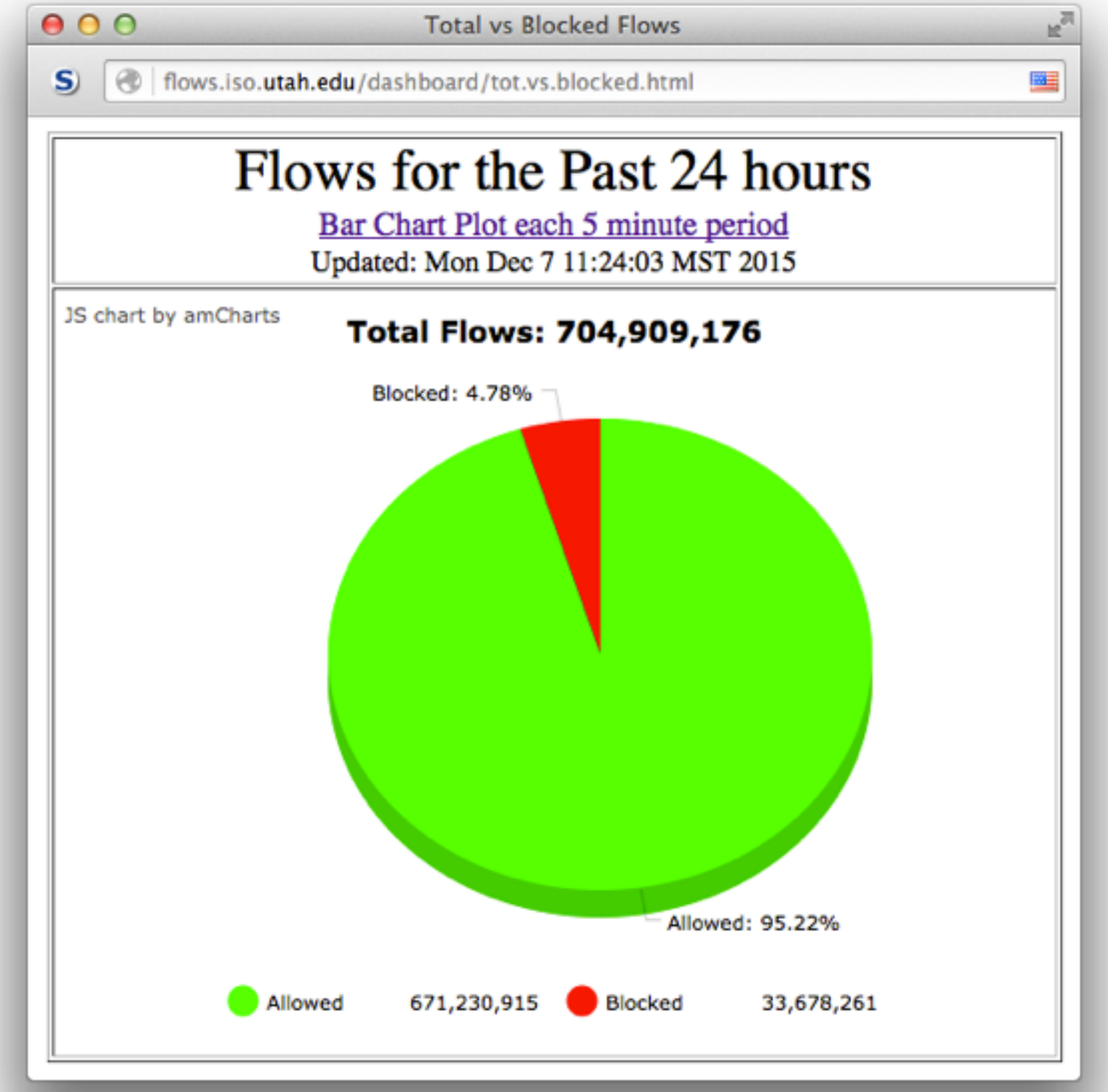
Note: **_____HOSTNAME** may be **IP_NOT_FOUND_IN_DNS**, because its only looked up once, and may not be discoverable,
and is truncated 19 characters from the right.
The **REASON_FOR_BLOCK** field has the following format:
port **PORT:HITS/UNIQUE**
PORT = The port **IP** scanned/probed
HITS = Total utah.edu machines **IP** hit, a single machine may have multiple hits.
UNIQUE = Unique utah.edu machines **IP** hit.
and may be [?] if not known.

Data is listed in the order an IP was blocked:

DATE_TIME_STAMP_IP_BLOCKED__	IP_ADDRESS___	_____HOSTNAME	BLOCK_TYPE	REASON_FOR_BLOCK_____
Fri Dec 19 08:33:02 MST 2014	220.178.78.138	IP_NOT_FOUND_IN_DNS	automatic	QR_BLOCK:port-22:SSH_Slow_Scanner:2/1
Sun Dec 21 05:50:01 MST 2014	61.174.51.214	amic.163data.com.cn	automatic	QR_BLOCK:port-22:SSH_Scanner:/0
Sun Dec 21 10:33:04 MST 2014	71.6.165.200	census12.shodan.io	manual	port-22:?/?
Mon Dec 22 01:20:02 MST 2014	128.9.168.98	nger-w3.ant.isi.edu	automatic	port-0:331/330
Tue Dec 23 04:11:04 MST 2014	222.219.187.9	IP_NOT_FOUND_IN_DNS	automatic	QR_BLOCK:port-22:SSH_Scanner:/0
Thu Dec 25 08:33:04 MST 2014	14.63.217.97	IP_NOT_FOUND_IN_DNS	automatic	port-8080:510/510
Fri Dec 26 01:55:02 MST 2014	125.65.245.146	IP_NOT_FOUND_IN_DNS	automatic	QR_BLOCK:port-22:SSH_Scanner:/0
Fri Dec 26 02:23:02 MST 2014	61.174.51.218	amic.163data.com.cn	automatic	QR_BLOCK:port-22:SSH_Scanner:/0
Fri Dec 26 17:00:01 MDT 2014	146.148.91.120	ogleusercontent.com	automatic	QR_BLOCK:port-22:SSH_Scanner:113/61
Fri Dec 26 17:30:02 MST 2014	61.174.51.215	amic.163data.com.cn	automatic	QR_BLOCK:port-22:SSH_Slow_Scanner:/0
Sat Dec 27 01:53:01 MST 2014	222.35.16.27	IP_NOT_FOUND_IN_DNS	automatic	port-7778:5418/5418
Sat Dec 27 08:40:02 MST 2014	218.24.113.2	IP_NOT_FOUND_IN_DNS	automatic	QR_BLOCK:port-22:SSH_Slow_Scanner:/0
Sat Dec 27 20:33:02 MST 2014	61.174.51.220	amic.163data.com.cn	automatic	QR_BLOCK:port-22:SSH_Scanner:/0
Tue Dec 30 04:15:01 MST 2014	82.221.105.6	census10.shodan.io	automatic	QR_BLOCK:port-22:SSH_Slow_Scanner:2/2
Wed Dec 31 20:24:01 MST 2014	220.226.22.210	IP_NOT_FOUND_IN_DNS	automatic	QR_BLOCK:port-22:SSH_Scanner:35/35

THE UNIVERSITY OF UTAH

Information Security Office



THE UNIVERSITY OF UTAH

Information Security Office

Conclusion

Detection and Protection is possible via the following reports and automated actions:

5 minute inbound processor.
30 minute outbound processor and associated report to the POC's.
Daily Report
Daily Admin Report
Bandwidth usage Report
IP usage Report

Additionally the Web Interface allows for almost real time observations.