

TRAFFIC ENGINEERING

FURKAN AYAR

Agenda

- Network Goals
- Introduction to Traffic Engineering
- Importance and Benefits
- Process model of Traffic Engineering
- Practical implementations (Tools)
- Optimizations
- Questions & Answers

Network Goals

- Vulnerabilities on the network
- Service outages due to errors, failures and faults
- High visibility and proactive prevention and detection
- Delays, packet loss, throughput

What is Traffic Engineering ?

- Understanding your traffic flows
- How packets move around over the internet
- Most used protocols and ports

Benefits

- Improve connectivity
- Reduce latency
- Reduce cost
- Detecting problems
- Alert on anomalies

Traffic Flows

- Sequence of packets
- Traffic shaping, QoS

Netflow

- Designed by Cisco
- Different versions
- Simple & powerfull information

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	->	192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	->	127.0.0.1:24920	1	80	1

PROCESS MODEL



MONITORING

ANALYSIS

OPTIMIZATION

Monitoring

- High visibility
- Cost effective
- Maintainable
- Classification

Tools

- ntop-ng
- nfdump - nfsen

- MRTG, RRDTool, CflowD, Flowscan, PRTG, Softflowd

ntop-ng

- Next-generation advanced flow analysis and collection suite
- Web based interface
- Authentication and Authorization facilities
- Lightweight

ntop-ng

ntop

ActiveFlows

Home Flows Hosts Admin Search Host

Active Flows

10

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	<div>Server</div>	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	<div>Client Server</div>	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	<div>Client Server</div>	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	<div>Client Server</div>	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	<div>Client Server</div>	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	<div>Client Server</div>	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	<div>Client Server</div>	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	<div>Client Server</div>	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	<div>Client</div>	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	<div>Client</div>	516

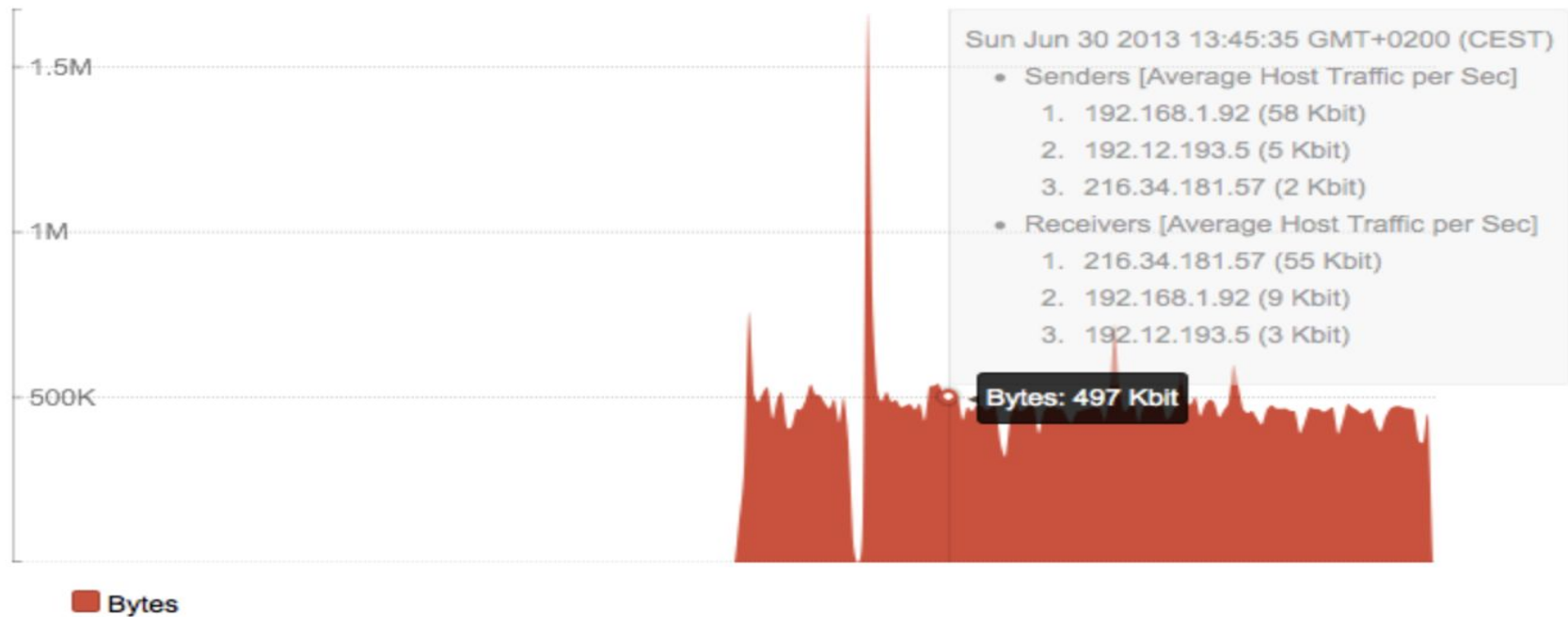
Showing 1 to 10 of 55 rows

← || →


← First Prev 1 2 3 4 5 Next Last →

ntop-ng

5m 10m 1h 3h 6h 12h 1d 1w 2w 1m 6m 1y



ntop-ng



Home ▾ Flows **Hosts ▾** Admin ▾

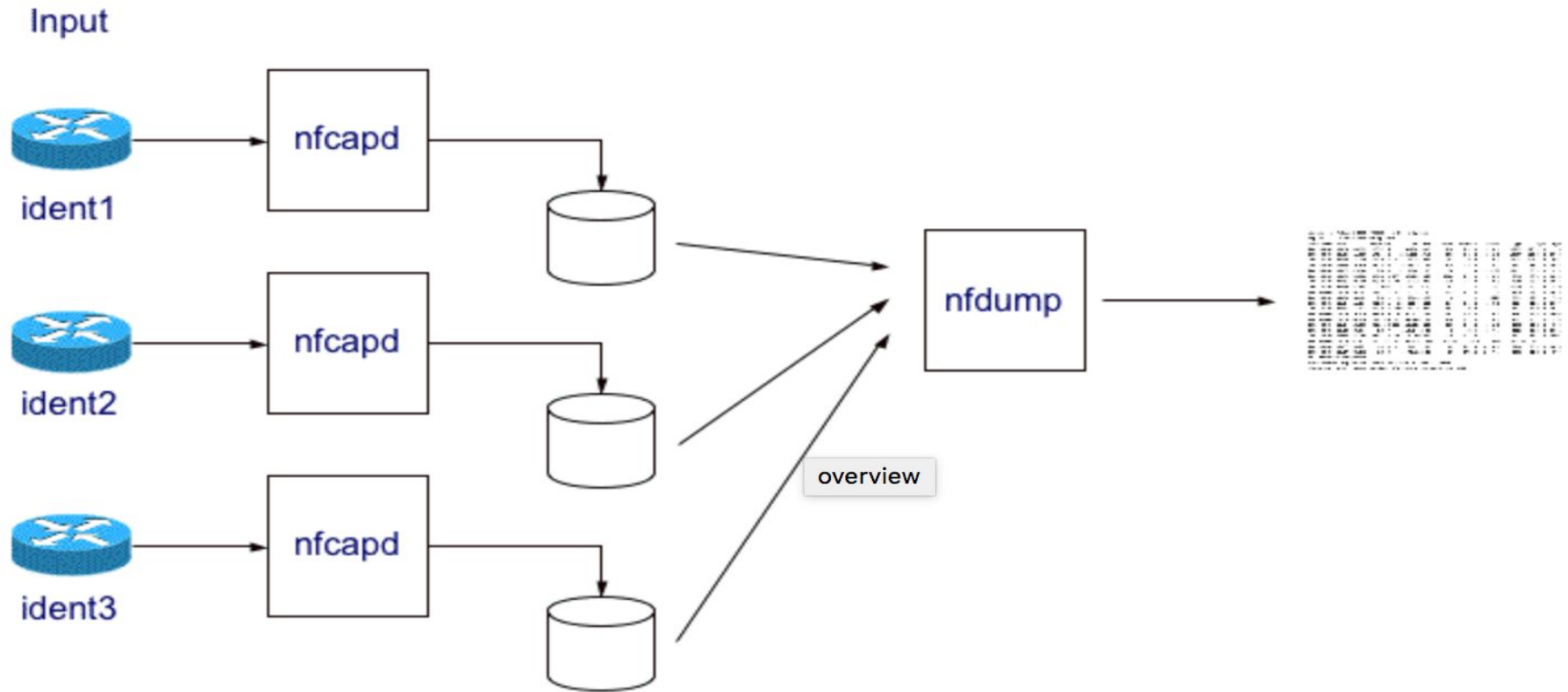
Host: 192.168.1.92 Overview Traffic Protocols Active Flows Talkers Historical Activity

(Router) MAC Address	C4:2C:03:06:49:FE
IP Address	192.168.1.92
Name	192.168.1.92 Local
First Seen	06/30/13 13:44:51 [1 min, 51 sec ago]
Last Seen	06/30/13 13:46:41 [1 sec ago]
Sent vs Received Traffic Breakdown	<div><div>Sent</div><div>Rcvd</div></div>
Traffic Sent	6,192 Pkts / 5.52 MB
Traffic Received	4,116 Pkts / 511.35 KB

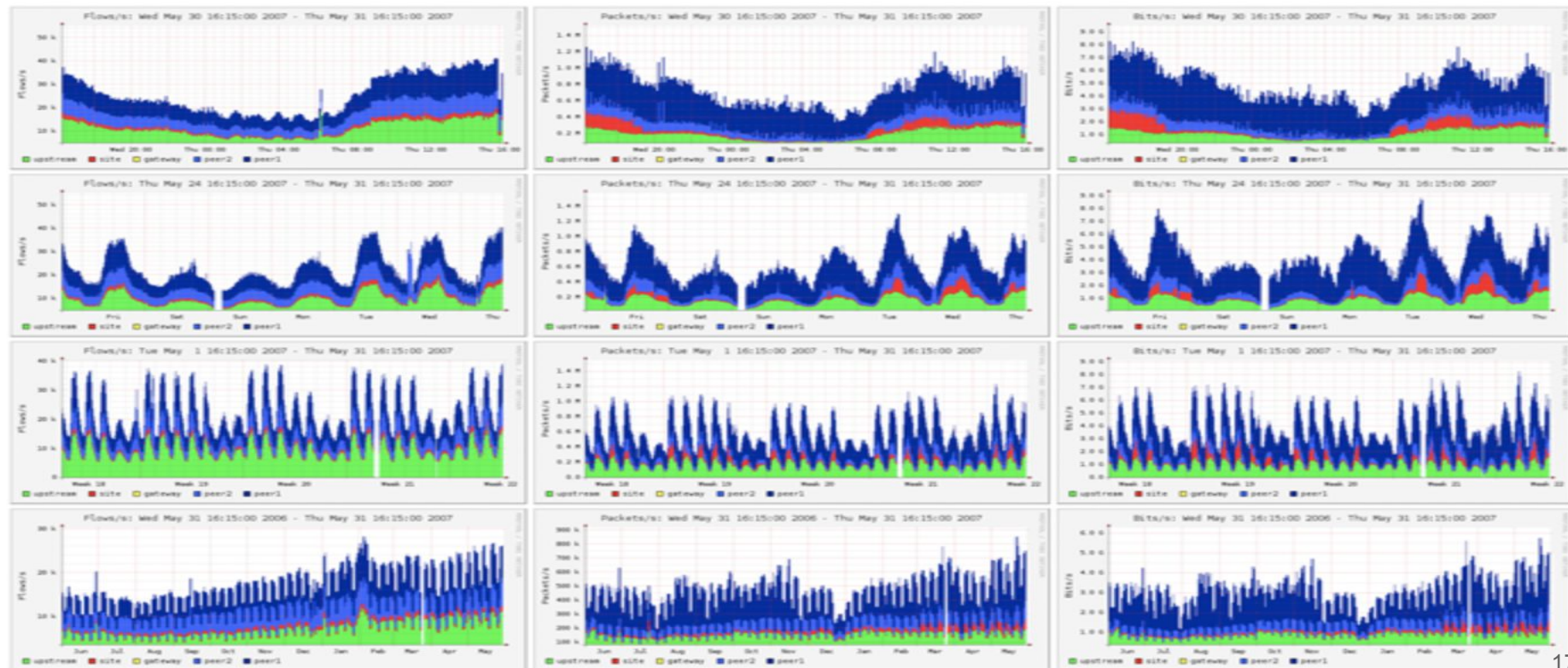
nfdump - nfsen

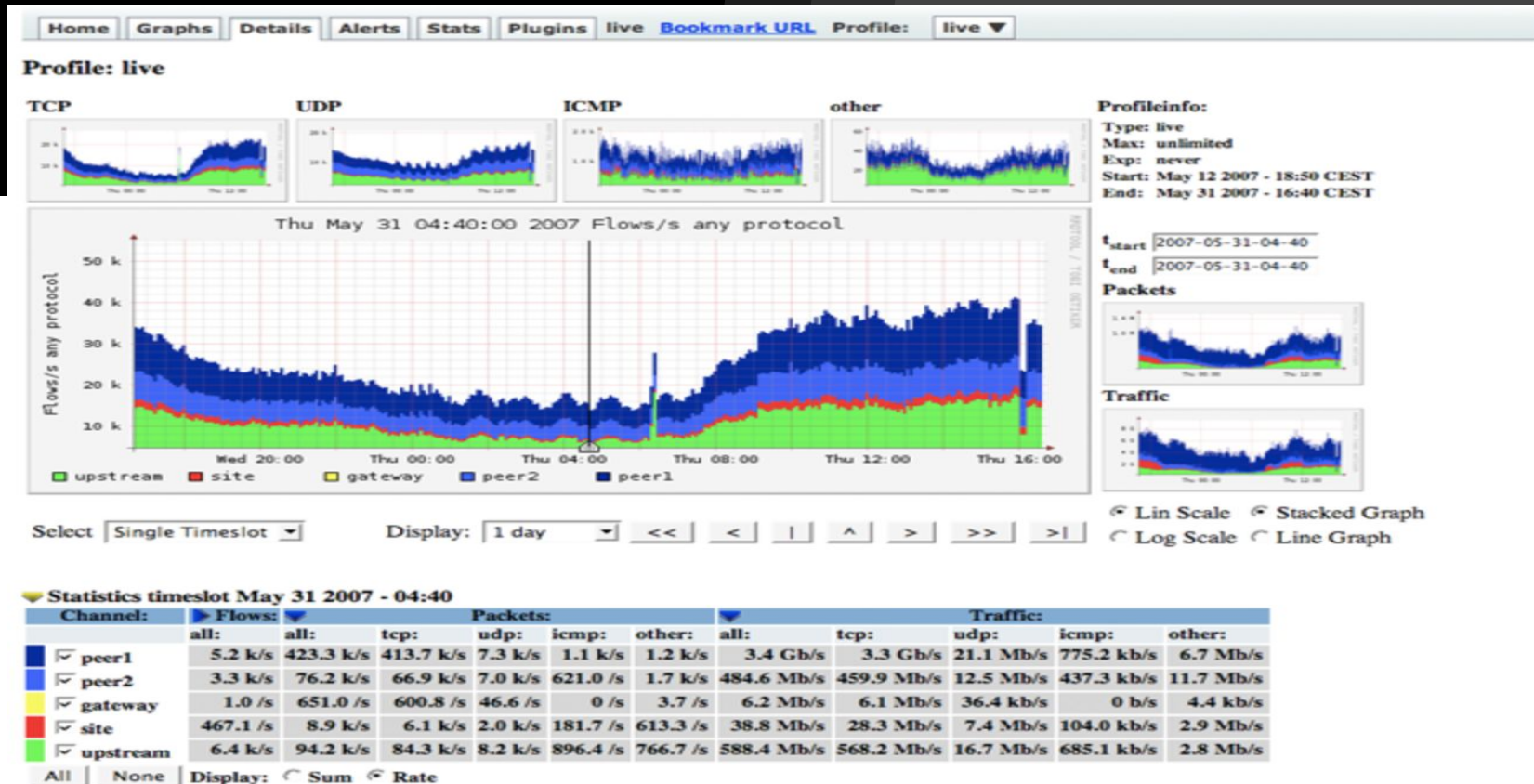
- Nfdump, collects netflow data
- Nfsen is an analytical web interface for netflow data
- Nfsen plugins (SURFmap, SSHcure etc)

nfdump



Overview Profile: live, Group: (nogroup)





nfsen

Netflow Processing

Source:
peer2
gateway
site
upstream

Filter:

All Sources and

Options:

☐ List Flows ☒ Stat TopN

Top:

Stat: order by

Aggregate ☒ proto ☒ srcPort ☒ dstPort

Limit:

Output: ☐ / IPv6 long

```
** nfdump -M /netflow0/nfsen-demo/profile-data/live/peer1:peer2:gateway:site:upstream -T -r 2007/06/26/14/nfcapd.200706261405 -n 20 -s record/flow
```

```
nfdump filter:
```

```
proto TCP
```

```
Aggregated flows 4307432
```

```
Top 20 flows ordered by flows:
```

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2007-06-26 14:04:52.233	304.620	TCP	131.152.7.48:25000 ->	125.252.105.225:80	1276	58696	115
2007-06-26 14:04:47.723	299.707	TCP	84.16.67.133:80 ->	147.86.124.128:3136	6743	9.3 M	62
2007-06-26 14:04:47.661	307.782	TCP	194.97.52.210:8000 ->	131.152.112.160:1476	10491	9.5 M	62
2007-06-26 14:04:47.978	299.454	TCP	212.58.227.86:554 ->	131.152.84.130:44368	7385	3.5 M	61
2007-06-26 14:04:48.108	307.212	TCP	131.152.34.73:4374 ->	85.5.58.34:21	9968	1.0 M	61
2007-06-26 14:04:48.108	305.992	TCP	69.247.93.228:18376 ->	147.87.131.32:49474	5305	2.9 M	61
2007-06-26 14:04:58.195	289.820	TCP	85.158.42.174:5000 ->	129.194.97.180:4516	60	5160	60
2007-06-26 14:04:58.671	289.475	TCP	129.194.97.180:4516 ->	85.158.42.174:5000	60	2760	60
2007-06-26 14:04:48.108	305.866	TCP	131.152.164.93:49751 ->	221.9.241.96:38916	3002	3.6 M	60
2007-06-26 14:04:48.170	305.546	TCP	81.230.33.141:36220 ->	147.87.131.32:36827	9476	12.6 M	58
2007-06-26 14:04:47.981	307.337	TCP	195.176.238.195:19996 ->	69.181.19.32:57396	1887	1.7 M	57
2007-06-26 14:04:47.725	299.899	TCP	24.202.245.190:53736 ->	193.222.247.66:50515	5003	2.4 M	56
2007-06-26 13:50:30.576	1157.759	TCP	195.176.162.19:56413 ->	62.2.243.157:443	1029	71512	56
2007-06-26 14:04:48.489	298.942	TCP	131.152.55.83:4894 ->	84.125.80.128:59143	688	32004	56
2007-06-26 14:04:48.109	307.270	TCP	213.39.148.243:20784 ->	131.152.97.66:1755	7607	3.1 M	56
2007-06-26 14:04:47.978	307.468	TCP	193.222.242.13:53849 ->	205.188.215.226:8012	4057	186790	56
2007-06-26 14:05:00.357	291.634	TCP	193.222.244.196:2206 ->	82.64.151.160:6324	937	46208	55
2007-06-26 14:04:48.045	303.499	TCP	66.222.172.199:44999 ->	131.152.159.32:4164	2356	2.4 M	55
2007-06-26 14:04:47.913	304.015	TCP	193.222.243.153:2659 ->	151.203.244.128:6346	1574	76744	54
2007-06-26 14:04:47.850	299.835	TCP	84.16.67.133:80 ->	129.129.158.98:50420	6767	9.3 M	54

```
Summary: total flows: 6836668, total bytes: 226.6 G, total packets: 269.8 M, avg bps: 932.4 M, avg pps: 142096, avg bpp: 860
```

```
Time window: 2007-06-26 13:36:47 - 2007-06-26 14:09:58
```

```
Total flows processed: 11582548, skipped: 0, Bytes read: 602310700
```

```
Sys: 11.524s flows/second: 1005017.7 Wall: 11.521s flows/second: 1005332.2
```


SURFmap

A network monitoring tool based on the Google Maps API

SURFmap

UNIVERSITY OF TWENTE.



SSHcure

Dashboard

SSHcure
Version 2.2

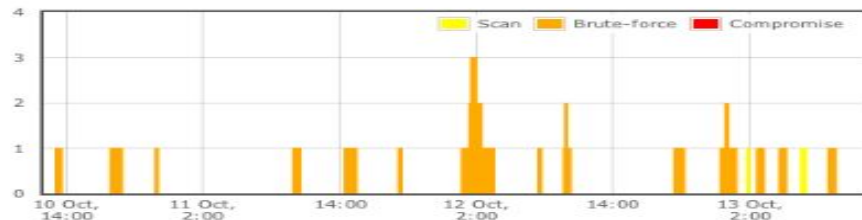
UNIVERSITY OF TWENTE.

[Dashboard](#)

[Search](#) [Help](#) [About](#) [License](#)

Time range: 3 days from Thu. Oct 10, 2013 12:00 Thu. Oct 10, 2013 - Sun. Oct 13, 2013

Attacks



Top attackers - scan

Attacker	Attacks	Targets
192.168.1.100	3	4025
192.168.1.101	2	16641
192.168.1.102	1	65536
192.168.1.103	1	65536
192.168.1.104	1	65144
192.168.1.105	1	57856
192.168.1.106	1	32812
192.168.1.107	1	19905
192.168.1.108	1	16641
192.168.1.109	1	12089

Top targets - brute-force

Target	Attacks	Attack blocked
192.168.1.100	8	×
192.168.1.101	7	×
192.168.1.102	7	×
192.168.1.103	7	×
192.168.1.104	7	×
192.168.1.105	7	×
192.168.1.106	7	×
192.168.1.107	7	×
192.168.1.108	7	×
192.168.1.109	7	×

Date	Ongoing	Phases	Attacker	Targets
Sun. Oct 13, 2013 09:01		Scan	192.168.1.100	65536
Sun. Oct 13, 2013 02:43		Scan	192.168.1.101	12089
Sat. Oct 12, 2013 23:58		Scan	192.168.1.102	437
Sat. Oct 12, 2013 19:29		Scan	192.168.1.103	16641
Sat. Oct 12, 2013 03:02		Scan	192.168.1.104	19905
Sat. Oct 12, 2013 01:38		Scan	192.168.1.105	10422
Sat. Oct 12, 2013 00:46		Scan	192.168.1.106	57856
Fri. Oct 11, 2013 09:57		Scan	192.168.1.107	4025
Thu. Oct 10, 2013 17:59		Scan	192.168.1.108	4562
Thu. Oct 10, 2013 13:06		Scan	192.168.1.109	8090
Sun. Oct 13, 2013 04:45		Brute-force	192.168.1.100	1
Sun. Oct 13, 2013 04:17		Brute-force	192.168.1.101	1

Top attackers - brute-force & compromise

Attacker	Attacks	Targets
192.168.1.100	6	1
192.168.1.101	2	4025
192.168.1.102	1	65536
192.168.1.103	1	57856
192.168.1.104	1	19905
192.168.1.105	1	16641
192.168.1.106	1	12089
192.168.1.107	1	10422
192.168.1.108	1	8090
192.168.1.109	1	437

Top targets - compromise

Target	Attacks	Compromises
No data available for selected time period...		

Analysis

- Traffic type and characterization
- Purposeful reports
- Defining critical resources
- Underlying potential issues

Optimization

- Routing remediations (adaptive, static)
- Mapping remediations
- Routing protocols (ospf, eigrp, bgp)
- Specific parameters (ttl, mtu etc)
- Traffic shaping, Rate limiting, QoS, Schedulers, Queue management etc

Traffic Shaping

- Packet Shaping
- Traffic classification and prioritization
- Limiting resources (rate limiting, source limiting)
- tc utility
- Queue and Scheduling mechanisms

Resources

- <http://nfsen.sourceforge.net>
- <http://nfdump.sourceforge.net>
- <http://www.ntop.org/products/traffic-analysis/ntop/>
- <https://sourceforge.net/projects/surfmap/>
- <https://sourceforge.net/projects/sshcure/>
- https://en.wikipedia.org/wiki/Traffic_shaping
- https://en.wikipedia.org/wiki/Routing_protocol
- https://en.wikipedia.org/wiki/Internet_traffic_engineering
- RFC3272



THANK YOU