CSO PERSPECTIVES

CSO Perspectives on
Defending Against the Pervasive Attacker

A Regional Seminar

Cyber Security Incident Response: Understanding the Norm in Your Environment

Jeff Wells

Director, Business Development

Lancope

CSO PERSPECTIVES

Lancope

VISION TO SECURE,
INTELLIGENCE TO PROTECT

A Stranger at Dinner: Cyber Security Incidence Response – Are you as Secure as You Think?

Jeffrey M. Wells, CCIE, CISSP

Director of Business Development

jwells@lancope.com

The value of complete visibility…

- How do you protect your important assets?

© 2014 Lancope, Inc. All rights reserved.

Consider your home…

- If someone was sitting at your dinner table who didn't belong there, would you know?

© 2014 Lancope, Inc. All rights reserved.

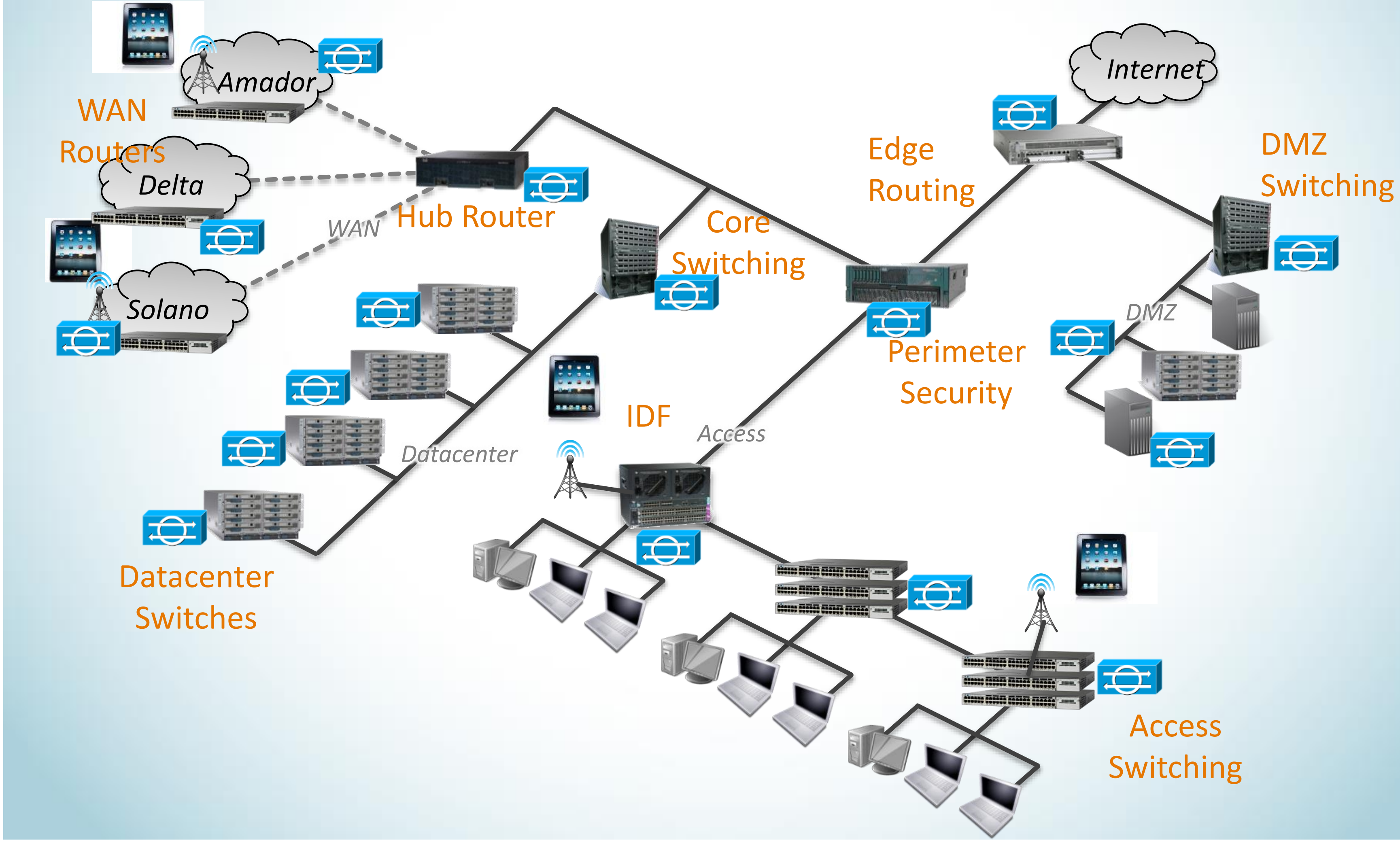
Protecting your home

- We all have walls, doors and locks. We teach our kids to keep doors closed and locked.
  - This is an example of **perimeter defense** and a **security policy**.
- We also pay attention to our surroundings. We have visibility into our environment. We know when something is out of place. And we act accordingly.
  - Security of our home is effective because we know what belongs and what doesn't. We **know what's normal**.
- If your child walked in with a swollen, red arm, **you would notice**. You would act. You would assess the situation and escalate to the appropriate resource if necessary. You would ensure the problem was remediated.
- We could not secure our homes without walls, doors and locks. And we could not secure them if we did not have visibility, nor if we did not know what was normal.
- **We need these things for our electronic asset security as well.**

© 2014 Lancope, Inc. All rights reserved.

What would be the ideal visibility situation?

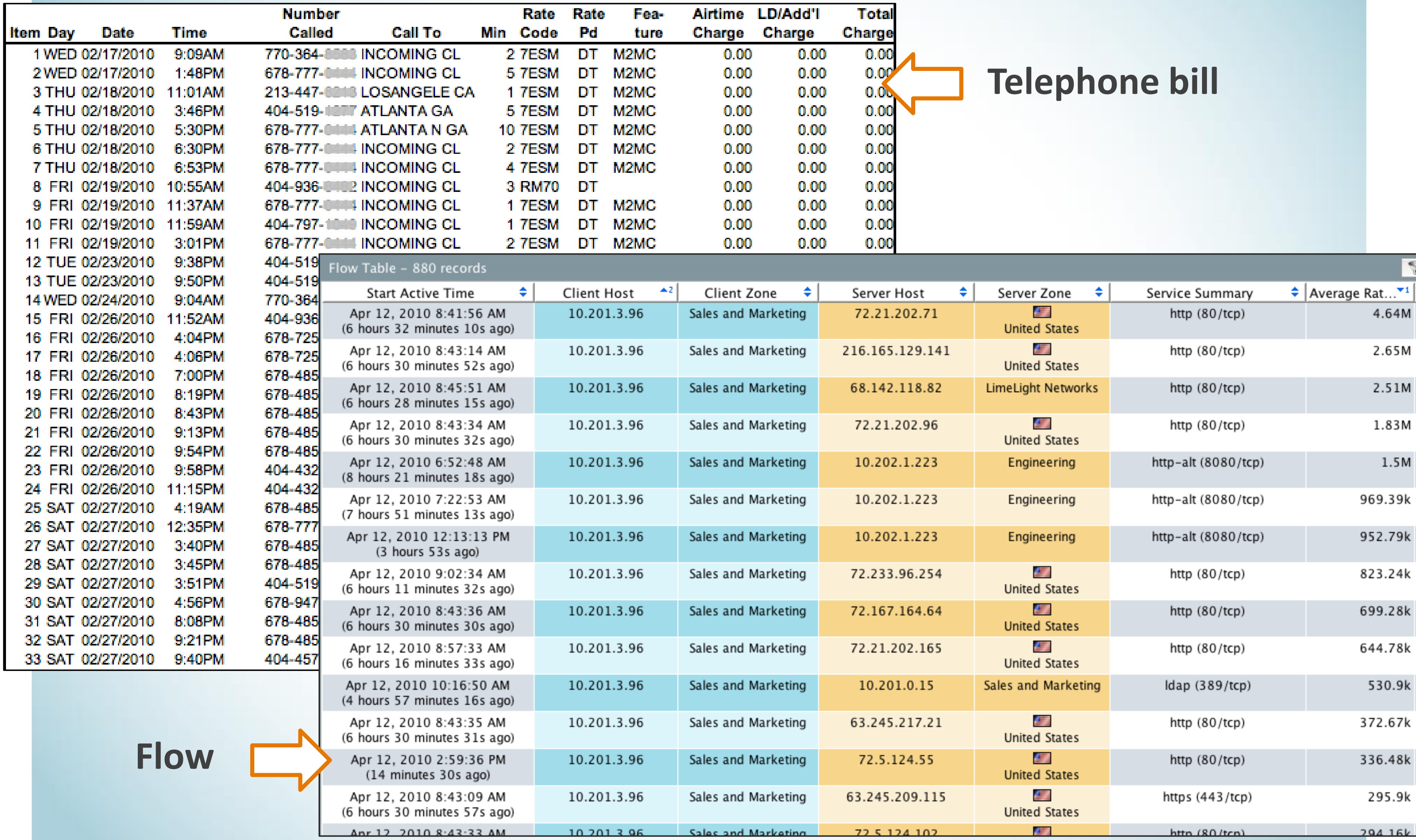
Full packet capture or IDS everywhere…?



© 2014 Lancope, Inc. All rights reserved.

Visibility via Flow Metadata

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT



Telephone bill

Item	Day	Date	Time	Number Called	Call To	Min	Rate Code	Rate Pd	Feature	Airtime Charge	LD/Add'l Charge	Total Charge
1	WED	02/17/2010	9:09AM	770-364-[redacted]	INCOMING CL	2	7ESM	DT	M2MC	0.00	0.00	0.00
2	WED	02/17/2010	1:48PM	678-777-[redacted]	INCOMING CL	5	7ESM	DT	M2MC	0.00	0.00	0.00
3	THU	02/18/2010	11:01AM	213-447-[redacted]	LOSANGELE CA	1	7ESM	DT	M2MC	0.00	0.00	0.00
4	THU	02/18/2010	3:46PM	404-519-[redacted]	ATLANTA GA	5	7ESM	DT	M2MC	0.00	0.00	0.00
5	THU	02/18/2010	5:30PM	678-777-[redacted]	ATLANTA N GA	10	7ESM	DT	M2MC	0.00	0.00	0.00
6	THU	02/18/2010	6:30PM	678-777-[redacted]	INCOMING CL	2	7ESM	DT	M2MC	0.00	0.00	0.00
7	THU	02/18/2010	6:53PM	678-777-[redacted]	INCOMING CL	4	7ESM	DT	M2MC	0.00	0.00	0.00
8	FRI	02/19/2010	10:55AM	404-936-[redacted]	INCOMING CL	3	RM70	DT		0.00	0.00	0.00
9	FRI	02/19/2010	11:37AM	678-777-[redacted]	INCOMING CL	1	7ESM	DT	M2MC	0.00	0.00	0.00
10	FRI	02/19/2010	11:59AM	404-797-[redacted]	INCOMING CL	1	7ESM	DT	M2MC	0.00	0.00	0.00
11	FRI	02/19/2010	3:01PM	678-777-[redacted]	INCOMING CL	2	7ESM	DT	M2MC	0.00	0.00	0.00
12	TUE	02/23/2010	9:38PM	404-519								
13	TUE	02/23/2010	9:50PM	404-519								
14	WED	02/24/2010	9:04AM	770-364								
15	FRI	02/26/2010	11:52AM	404-936								
16	FRI	02/26/2010	4:04PM	678-725								
17	FRI	02/26/2010	4:06PM	678-725								
18	FRI	02/26/2010	7:00PM	678-485								
19	FRI	02/26/2010	8:19PM	678-485								
20	FRI	02/26/2010	8:43PM	678-485								
21	FRI	02/26/2010	9:13PM	678-485								
22	FRI	02/26/2010	9:54PM	678-485								
23	FRI	02/26/2010	9:58PM	404-432								
24	FRI	02/26/2010	11:15PM	404-432								
25	SAT	02/27/2010	4:19AM	678-485								
26	SAT	02/27/2010	12:35PM	678-777								
27	SAT	02/27/2010	3:40PM	678-485								
28	SAT	02/27/2010	3:45PM	678-485								
29	SAT	02/27/2010	3:51PM	404-519								
30	SAT	02/27/2010	4:56PM	678-947								
31	SAT	02/27/2010	8:08PM	678-485								
32	SAT	02/27/2010	9:21PM	678-485								
33	SAT	02/27/2010	9:40PM	404-457								

Flow

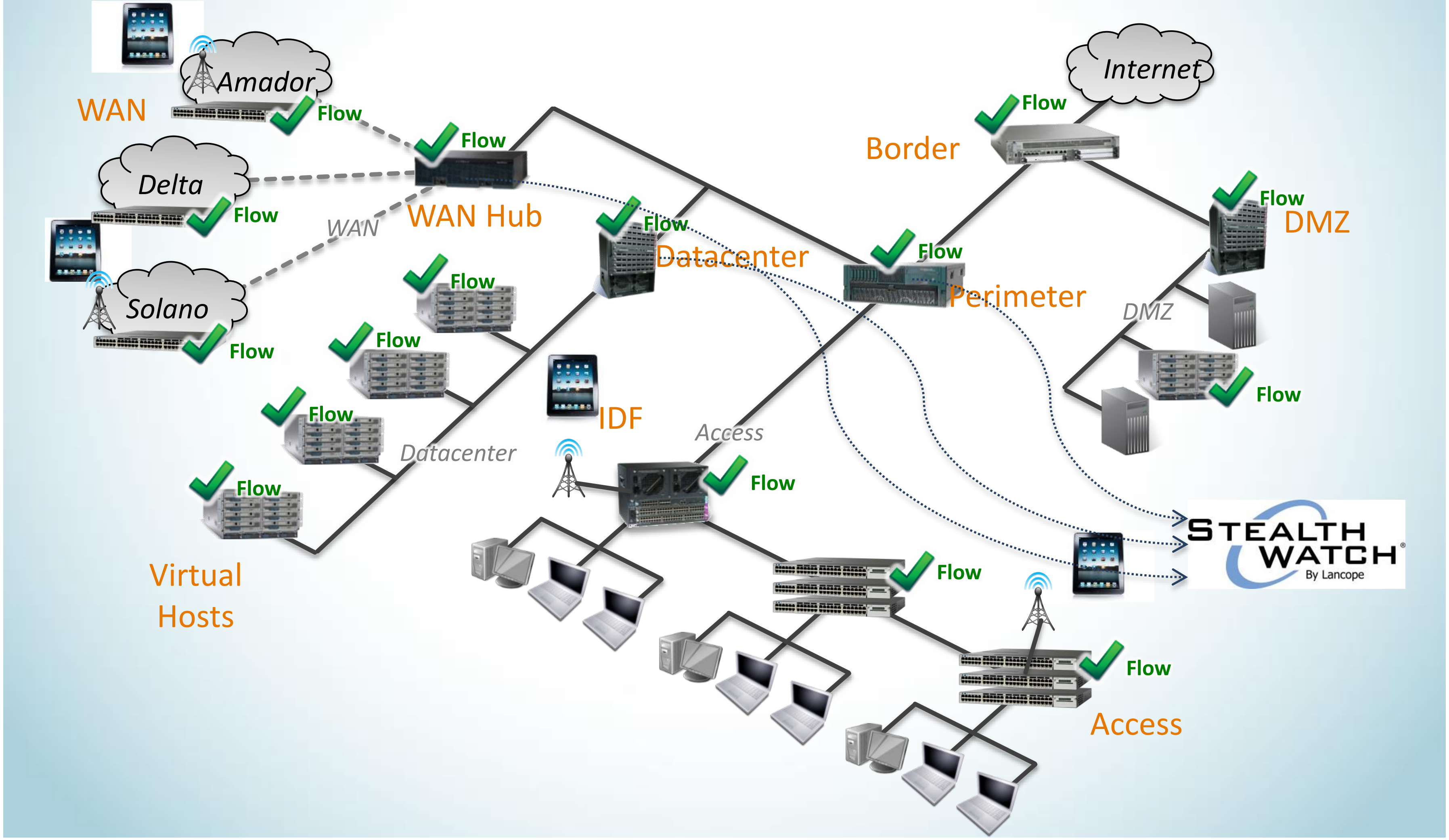
Flow Table – 880 records

Start Active Time	Client Host	Client Zone	Server Host	Server Zone	Service Summary	Average Rat…
Apr 12, 2010 8:41:56 AM (6 hours 32 minutes 10s ago)	10.201.3.96	Sales and Marketing	72.21.202.71	United States	http (80/tcp)	4.64M
Apr 12, 2010 8:43:14 AM (6 hours 30 minutes 52s ago)	10.201.3.96	Sales and Marketing	216.165.129.141	United States	http (80/tcp)	2.65M
Apr 12, 2010 8:45:51 AM (6 hours 28 minutes 15s ago)	10.201.3.96	Sales and Marketing	68.142.118.82	LimeLight Networks	http (80/tcp)	2.51M
Apr 12, 2010 8:43:34 AM (6 hours 30 minutes 32s ago)	10.201.3.96	Sales and Marketing	72.21.202.96	United States	http (80/tcp)	1.83M
Apr 12, 2010 6:52:48 AM (8 hours 21 minutes 18s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	1.5M
Apr 12, 2010 7:22:53 AM (7 hours 51 minutes 13s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	969.39k
Apr 12, 2010 12:13:13 PM (3 hours 53s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	952.79k
Apr 12, 2010 9:02:34 AM (6 hours 11 minutes 32s ago)	10.201.3.96	Sales and Marketing	72.233.96.254	United States	http (80/tcp)	823.24k
Apr 12, 2010 8:43:36 AM (6 hours 30 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.167.164.64	United States	http (80/tcp)	699.28k
Apr 12, 2010 8:57:33 AM (6 hours 16 minutes 33s ago)	10.201.3.96	Sales and Marketing	72.21.202.165	United States	http (80/tcp)	644.78k
Apr 12, 2010 10:16:50 AM (4 hours 57 minutes 16s ago)	10.201.3.96	Sales and Marketing	10.201.0.15	Sales and Marketing	ldap (389/tcp)	530.9k
Apr 12, 2010 8:43:35 AM (6 hours 30 minutes 31s ago)	10.201.3.96	Sales and Marketing	63.245.217.21	United States	http (80/tcp)	372.67k
Apr 12, 2010 2:59:36 PM (14 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http (80/tcp)	336.48k
Apr 12, 2010 8:43:09 AM (6 hours 30 minutes 57s ago)	10.201.3.96	Sales and Marketing	63.245.209.115	United States	https (443/tcp)	295.9k
Apr 12, 2010 8:43:33 AM	10.201.3.96	Sales and Marketing	72.5.124.102		http (80/tcp)	294.16k

© 2014 Lancope, Inc. All rights reserved.

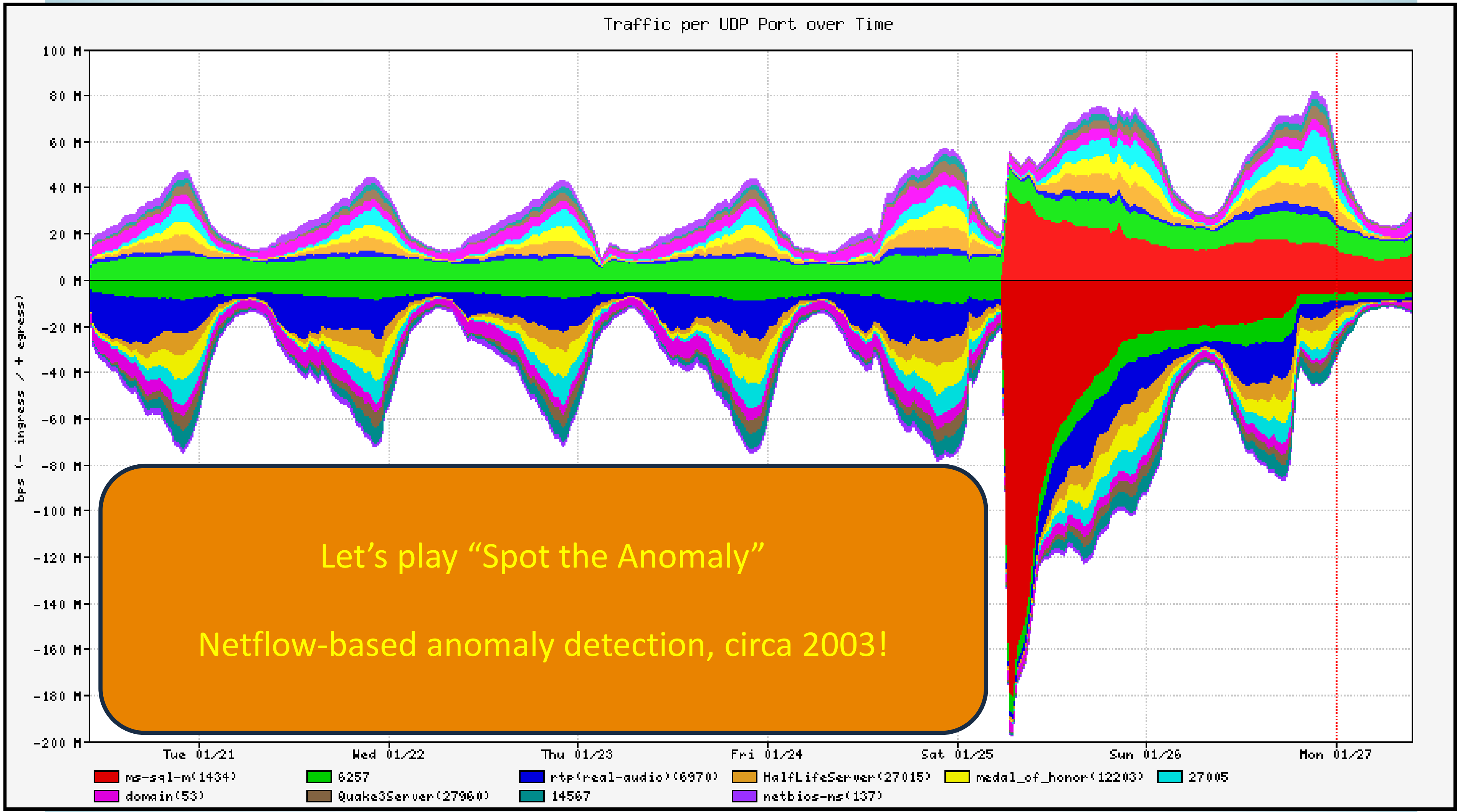
Ubiquitous visibility via flow telemetry …

… your infrastructure is the source:



© 2014 Lancope, Inc. All rights reserved.

Statistical analysis and pattern recognition



Let’s play “Spot the Anomaly”

Netflow-based anomaly detection, circa 2003!

© 2014 Lancope, Inc. All rights reserved.

Thank You

Jeffrey M. Wells, CCIE, CISSP
Director of Business Development
jwells@lancope.com