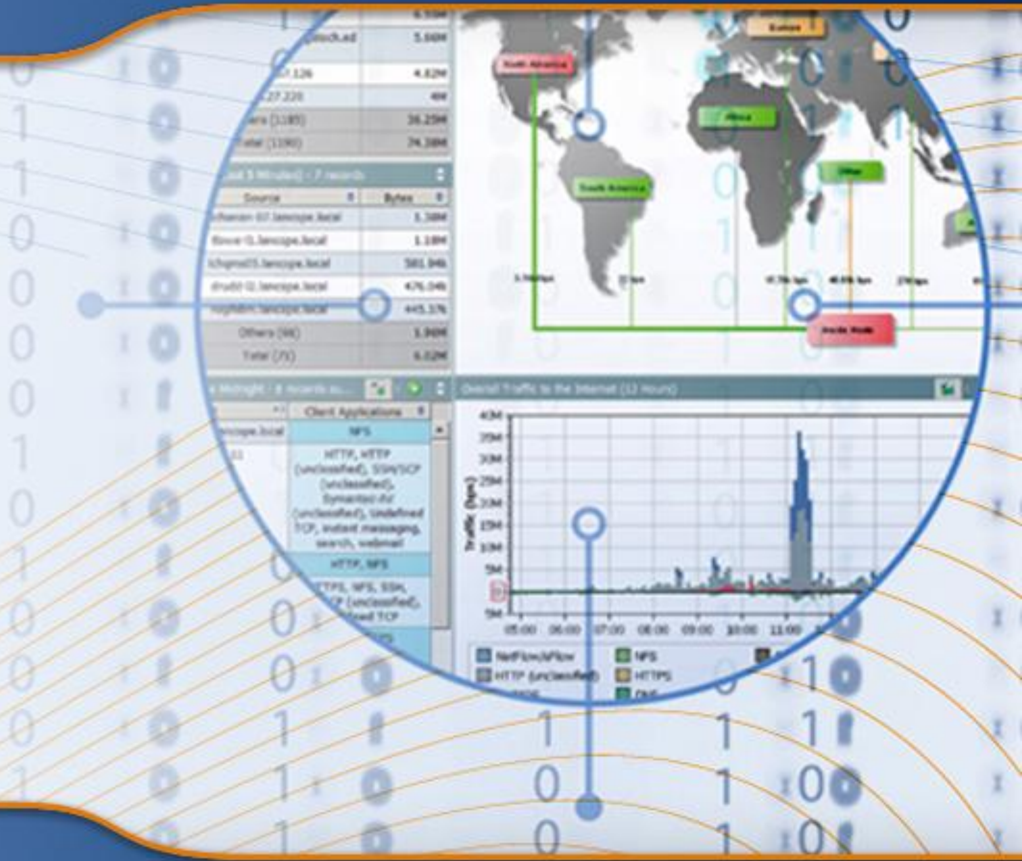
Lancope
Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™



NetFlow 101 Seminar Series, 2012

An Introduction to Cisco’s NetFlow Technology

Know Your Network, Run Your Business

Agenda

- **Introduction to NetFlow**

  how it works, what it is
- **Why is NetFlow so popular?**

  NetFlow costs less and works better
- **How is NetFlow used?**

  what can we do with NetFlow?
- **Configuring and Working with NetFlow**

  a glimpse into the power of NetFlow
- **Cisco Flexible NetFlow Lab**

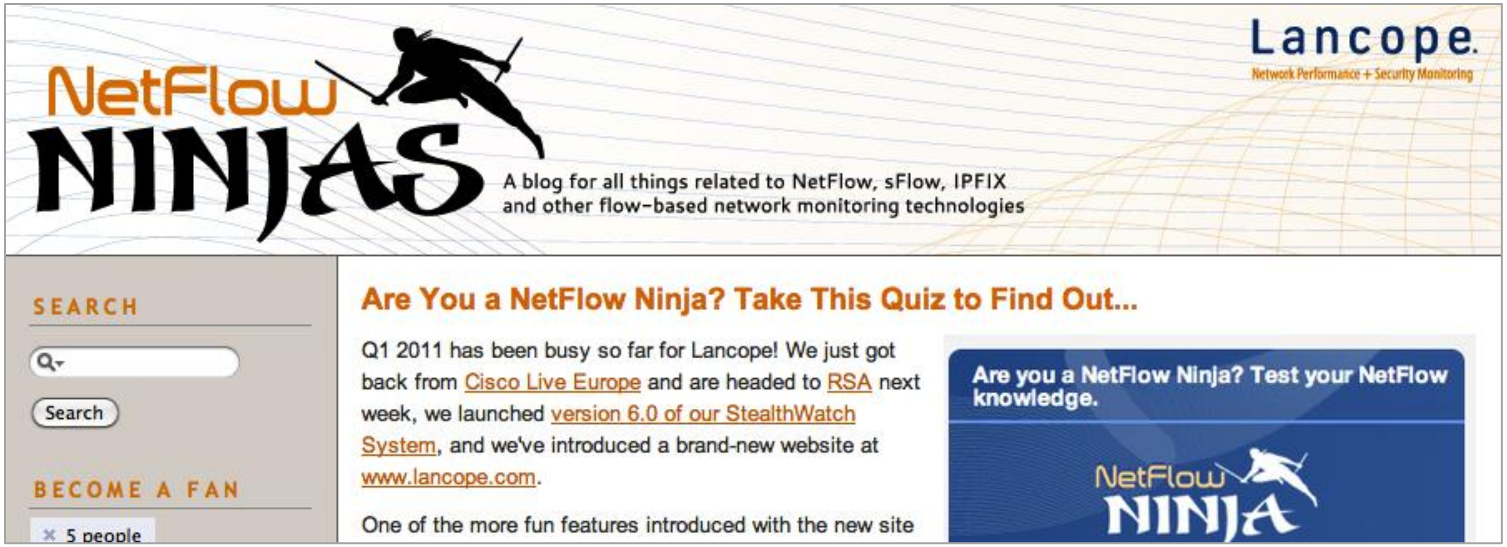
  set up and work with NetFlow
- **Lancope's StealthWatch System**

  premium NetFlow collection and analysis

Science of Flow Analysis

- Lancope specializes in Behavior-based Network Flow Analysis
- Detects attacks by baselining and analyzing network traffic patterns
- Excellent defense in depth strategy to aid in defense of critical assets
- Over 600 customers world-wide
- Operational since 2002, located in Atlanta, GA

http://netflowninjas.lancope.com



A blog for all things related to NetFlow, sFlow, IPFIX and other flow-based network monitoring technologies

Are You a NetFlow Ninja? Take This Quiz to Find Out...

Q1 2011 has been busy so far for Lancope! We just got back from Cisco Live Europe and are headed to RSA next week, we launched version 6.0 of our StealthWatch System, and we've introduced a brand-new website at www.lancope.com.

One of the more fun features introduced with the new site

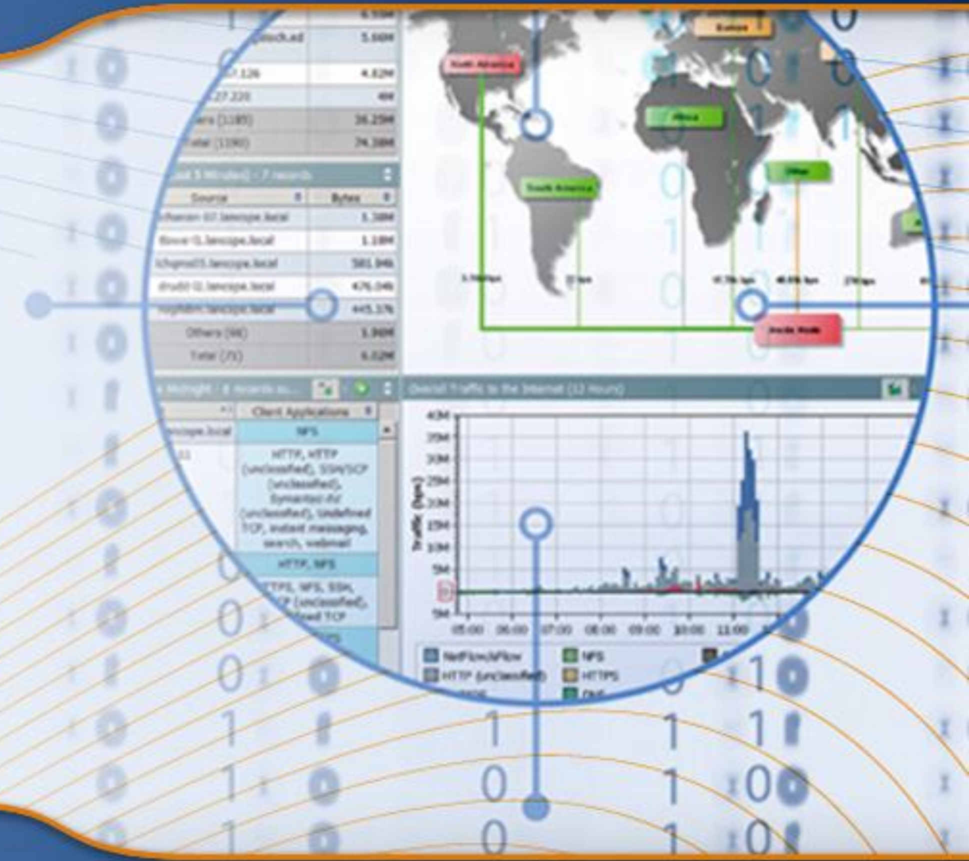
Are you a NetFlow Ninja? Test your NetFlow knowledge.

Lancope

Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

Introduction to NetFlow

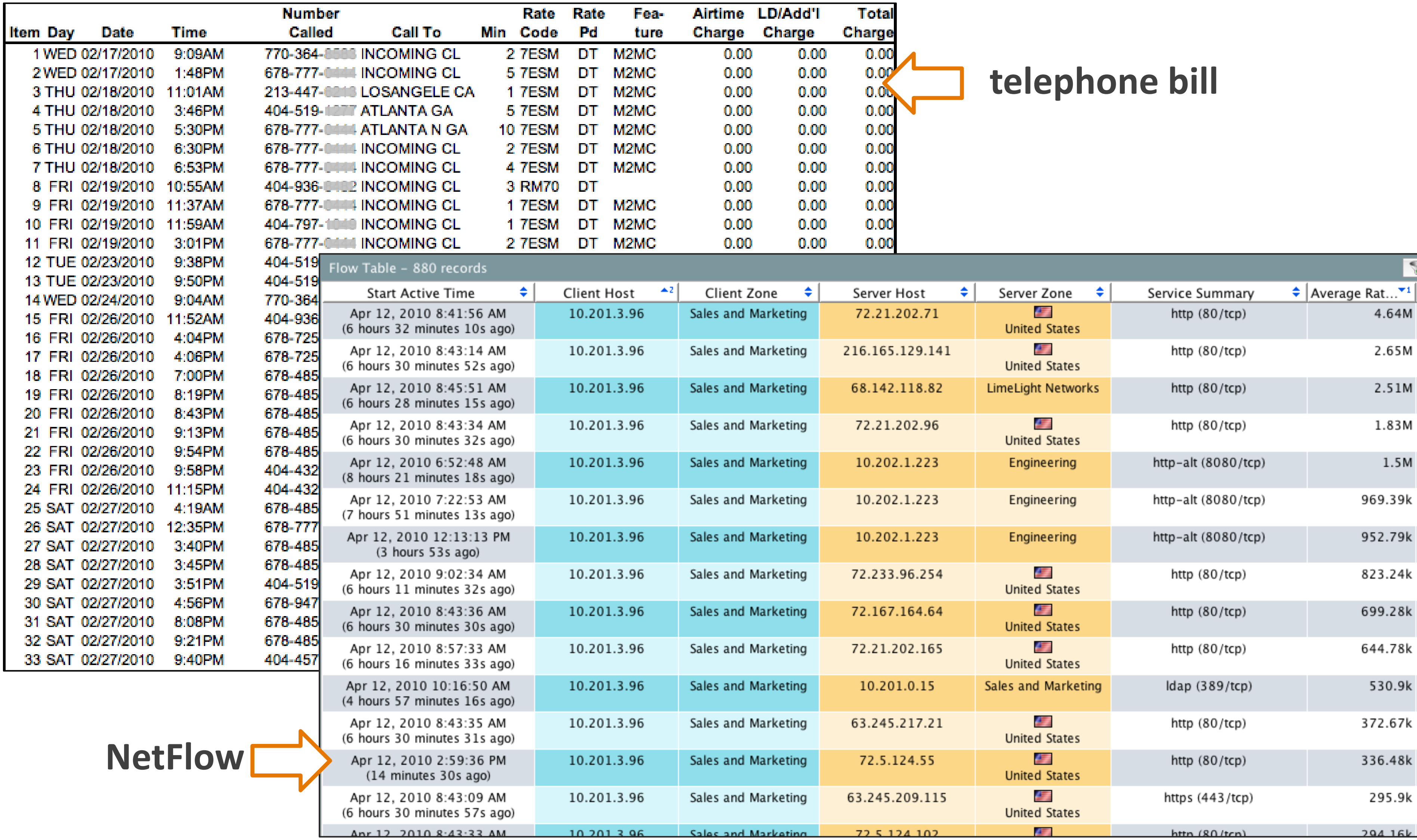


Know Your Network, Run Your Business

Recap: The OSI Model

Uppe	**Layer-7:** *Application*	• HTTP Browser, FTP, Telnet
	Layer-6: *Presentation*	• JPEG, GIF, MPEG-2
	Layer-5: *Session*	• WinSock, RPC, SQL, NFS
Lower	**Layer-4:** *Transport*	• TCP, UDP, SPX
	Layer-3: *Network*	• IP, ICMP, IPX
	Layer-2: *Data-Link*	• Ethernet (Mac Addresses)
	Layer-1: *Physical*	• Hub, Cat-5 Cable

Introducing NetFlow Technology



telephone bill

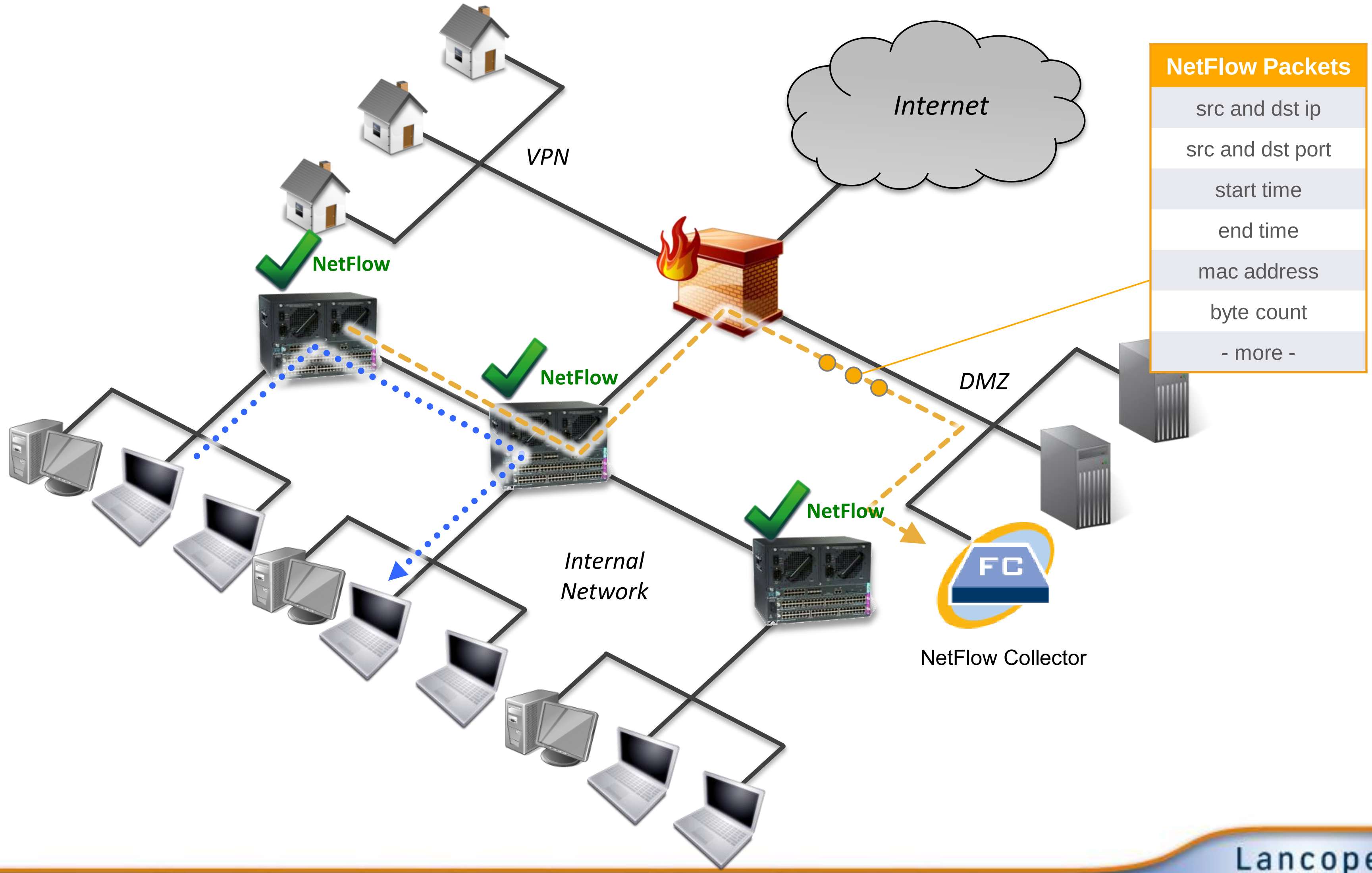
Item	Day	Date	Time	Number Called	Call To	Min	Rate Code	Rate Pd	Fea-ture	Airtime Charge	LD/Add'l Charge	Total Charge
1	WED	02/17/2010	9:09AM	770-364-[redacted]	INCOMING CL	2	7ESM	DT	M2MC	0.00	0.00	0.00
2	WED	02/17/2010	1:48PM	678-777-[redacted]	INCOMING CL	5	7ESM	DT	M2MC	0.00	0.00	0.00
3	THU	02/18/2010	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								

NetFlow

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

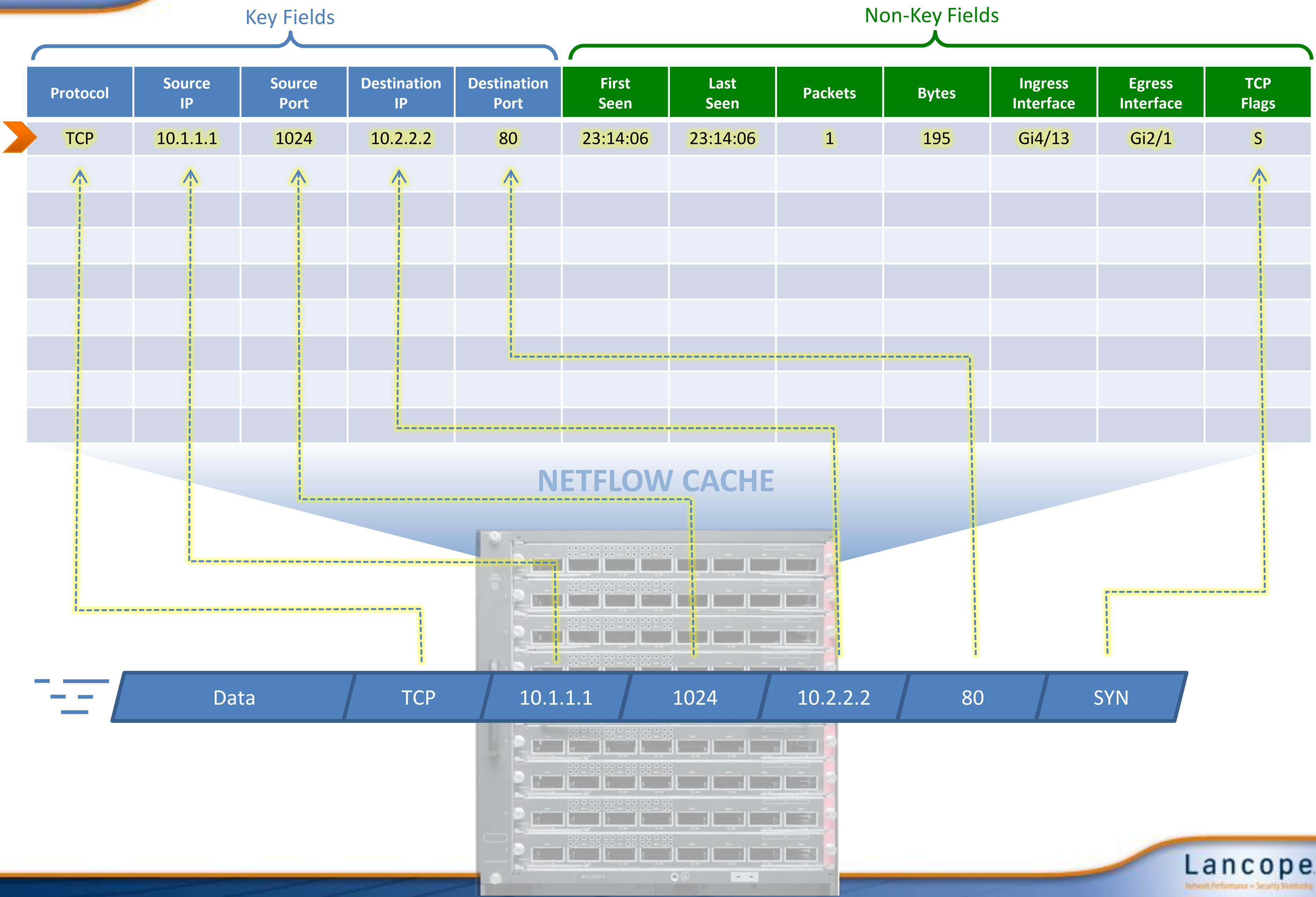
Internal Visibility Through NetFlow



NetFlow Packets

- src and dst ip
- src and dst port
- start time
- end time
- mac address
- byte count
- - more -

Create New TCP Flow



Key Fields

Non-Key Fields

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:06	1	195	Gi4/13	Gi2/1	S

NETFLOW CACHE

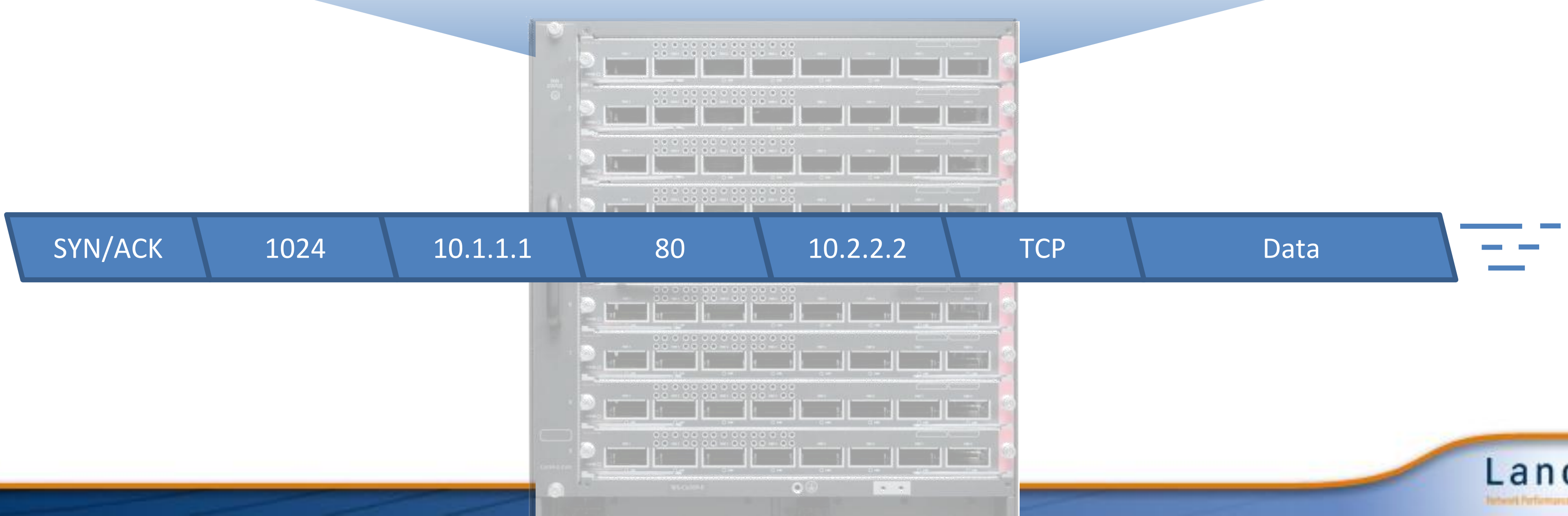
Data	TCP	10.1.1.1	1024	10.2.2.2	80	SYN

Create New TCP Flow

Ingress and Egress ports are based on the interface on which the packets entered and left the router

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:06	1	195	Gi4/13	Gi2/1	S
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.07	1	132	Gi2/1	Gi4/13	SA

NETFLOW CACHE

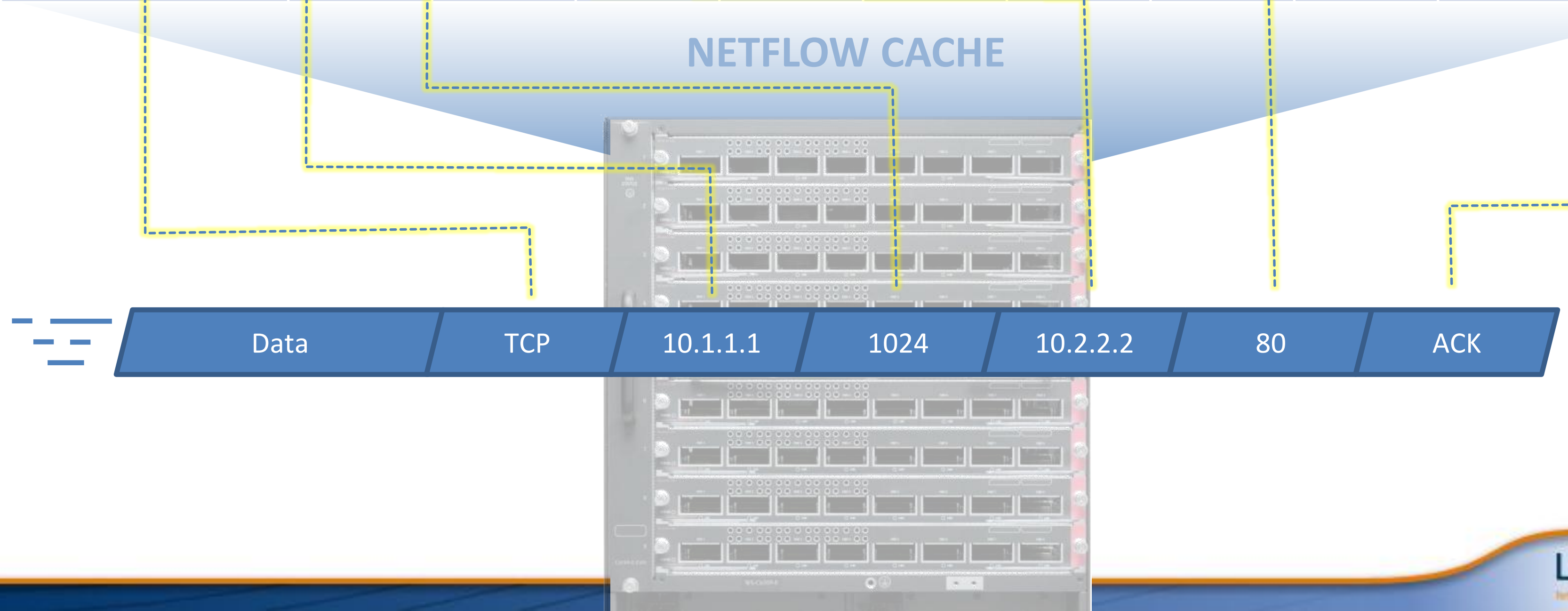


SYN/ACK | 1024 | 10.1.1.1 | 80 | 10.2.2.2 | TCP | Data

Update Existing TCP Flow

Packet and Byte counts are incremented accordingly. Last Seen is also updated.

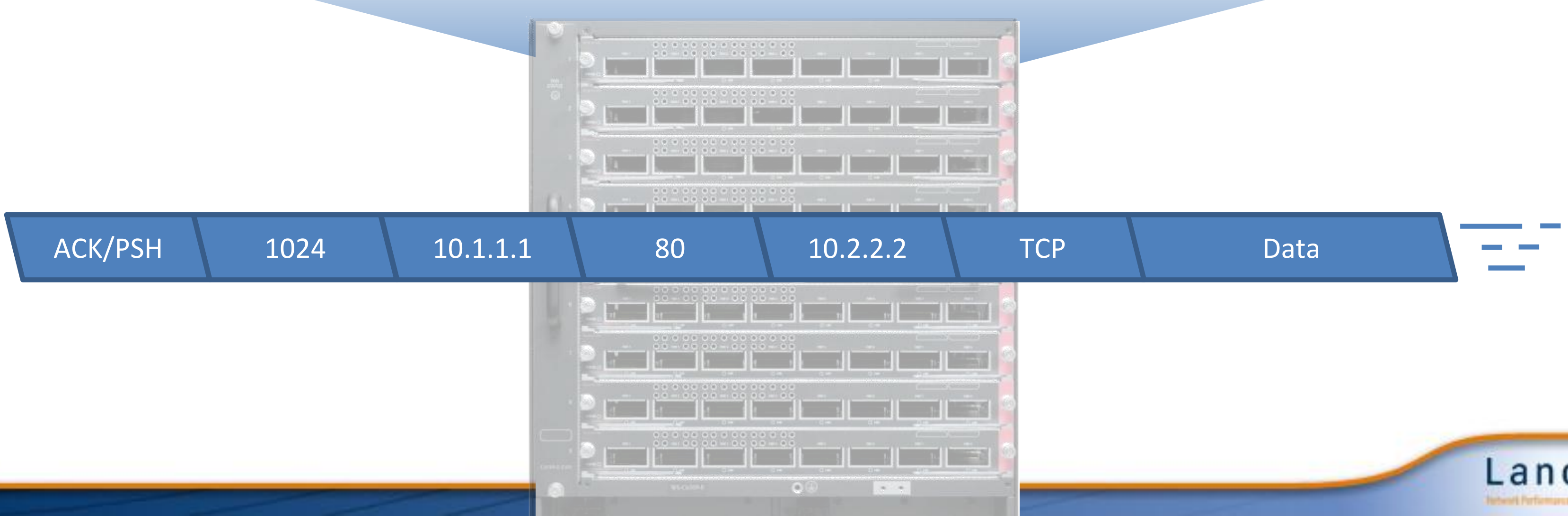
Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.07	1	132	Gi2/1	Gi4/13	SA



Update Existing TCP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP

NETFLOW CACHE

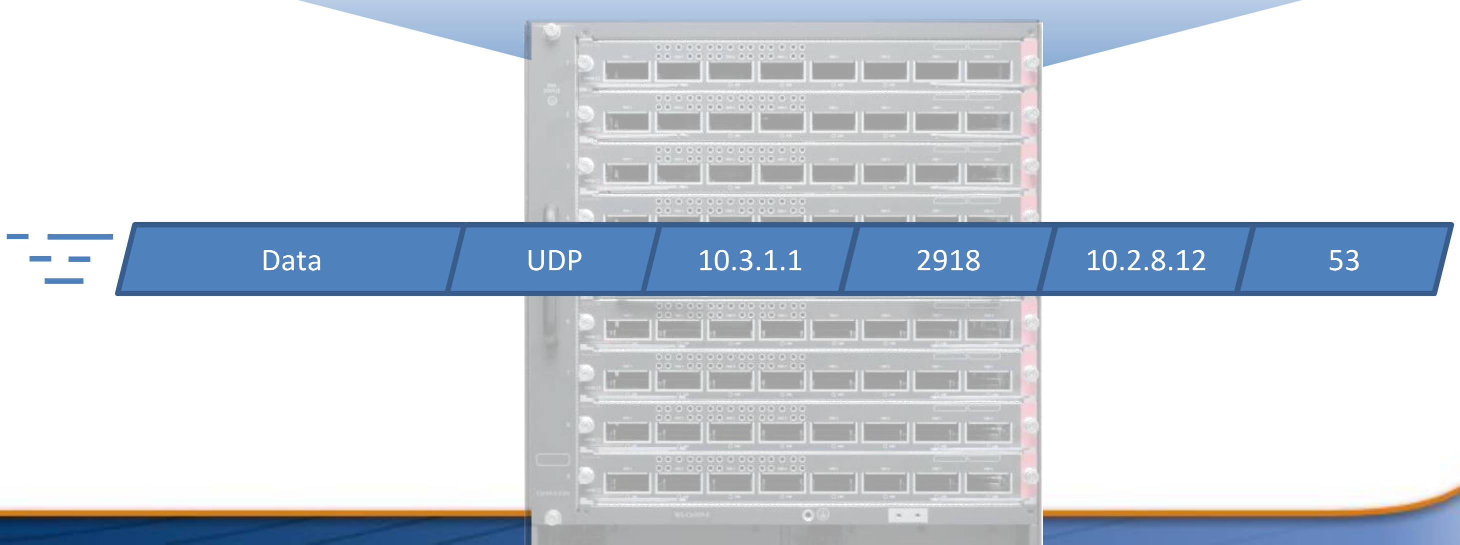


ACK/PSH | 1024 | 10.1.1.1 | 80 | 10.2.2.2 | TCP | Data

Create New UDP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-

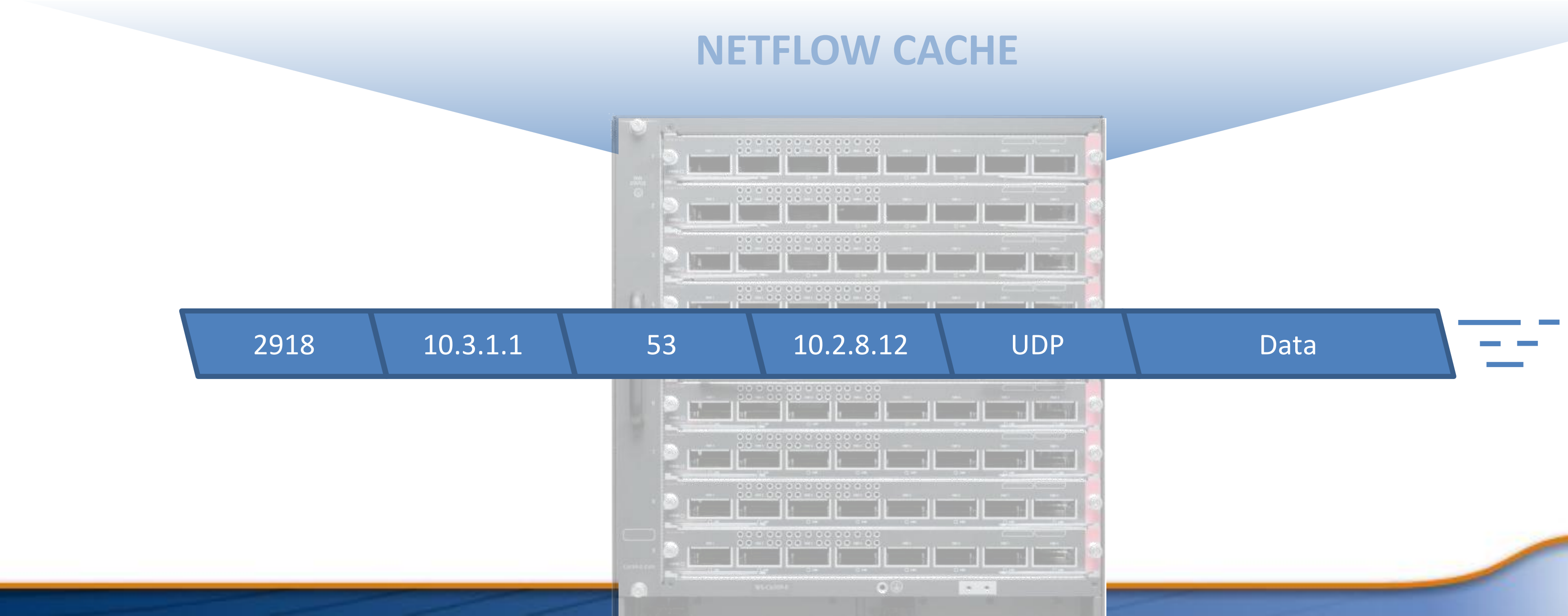
NETFLOW CACHE



Data | UDP | 10.3.1.1 | 2918 | 10.2.8.12 | 53

Create New UDP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-

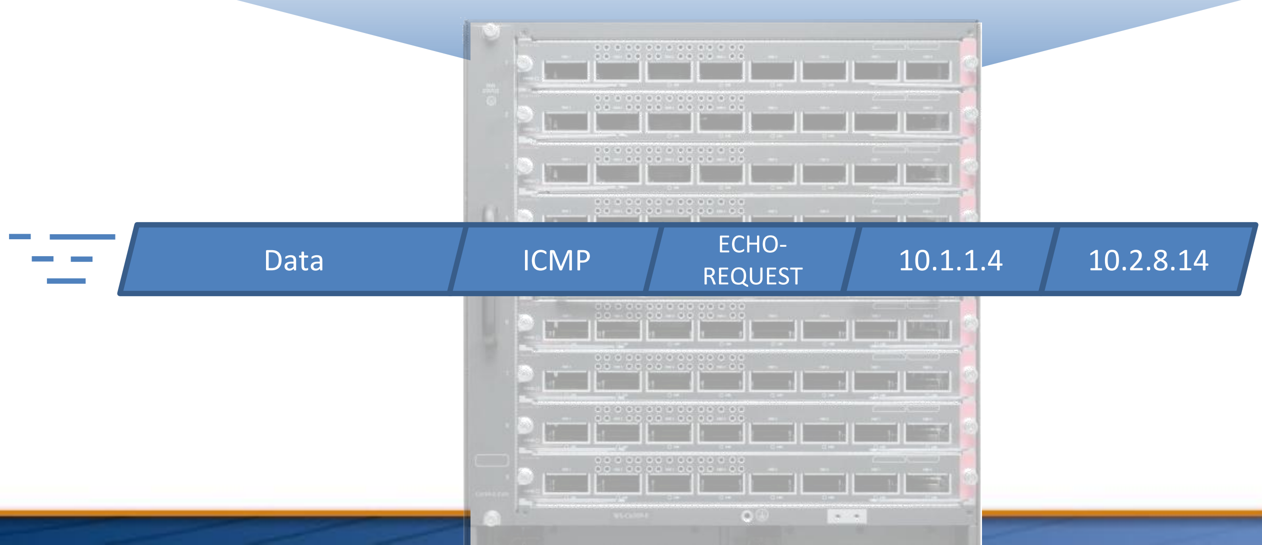


Create New ICMP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.12	1	96	Gi4/19	Gi2/1	-

Most NetFlow caches do not offer ICMP type and code fields so the Destination Port column is overloaded with with ICMP information.

NETFLOW CACHE

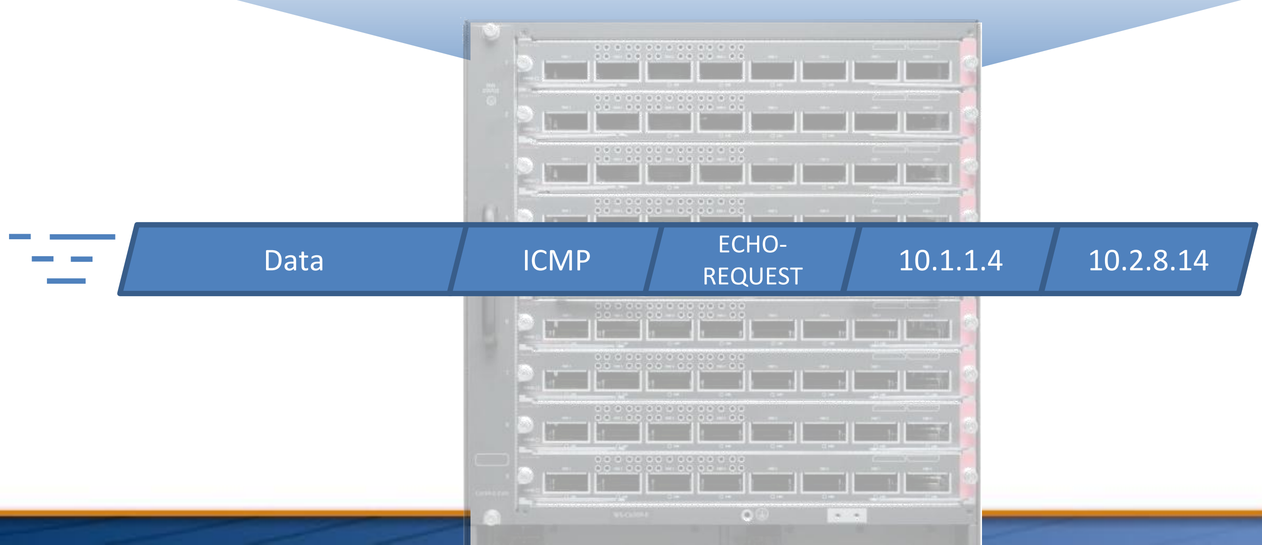


Data | ICMP | ECHO-REQUEST | 10.1.1.4 | 10.2.8.14

Update Existing ICMP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-

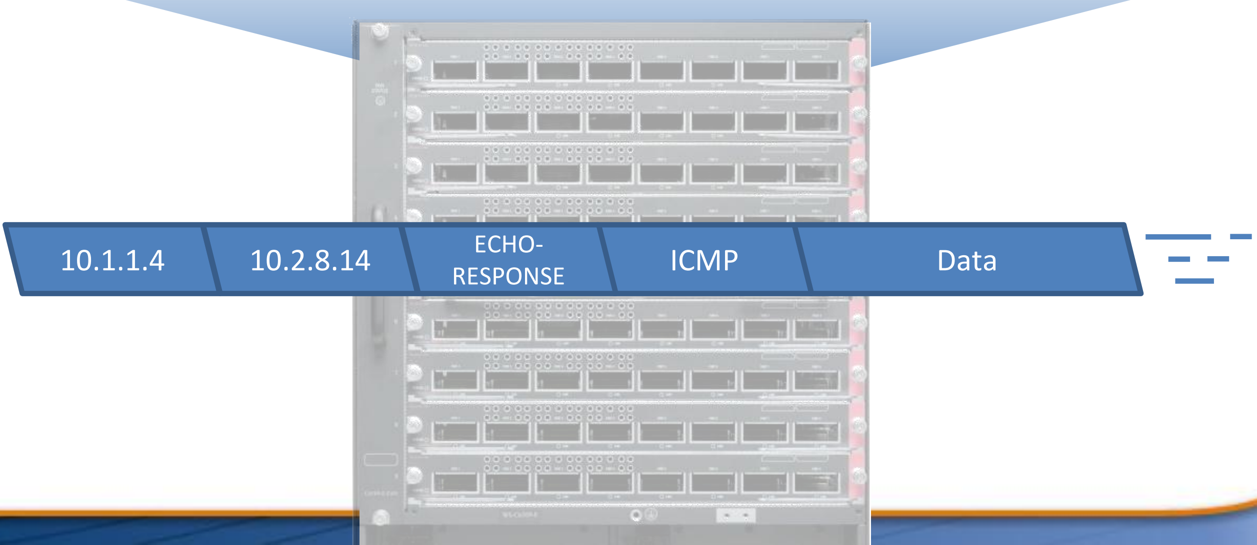
NETFLOW CACHE



Create New ICMP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-
ICMP	10.2.8.14	-	10.1.1.4	ECHO-RESPONSE	23.14.13	23.14.13	1	92	Gi2/1	Gi4/19	-

NETFLOW CACHE



10.1.1.4

10.2.8.14

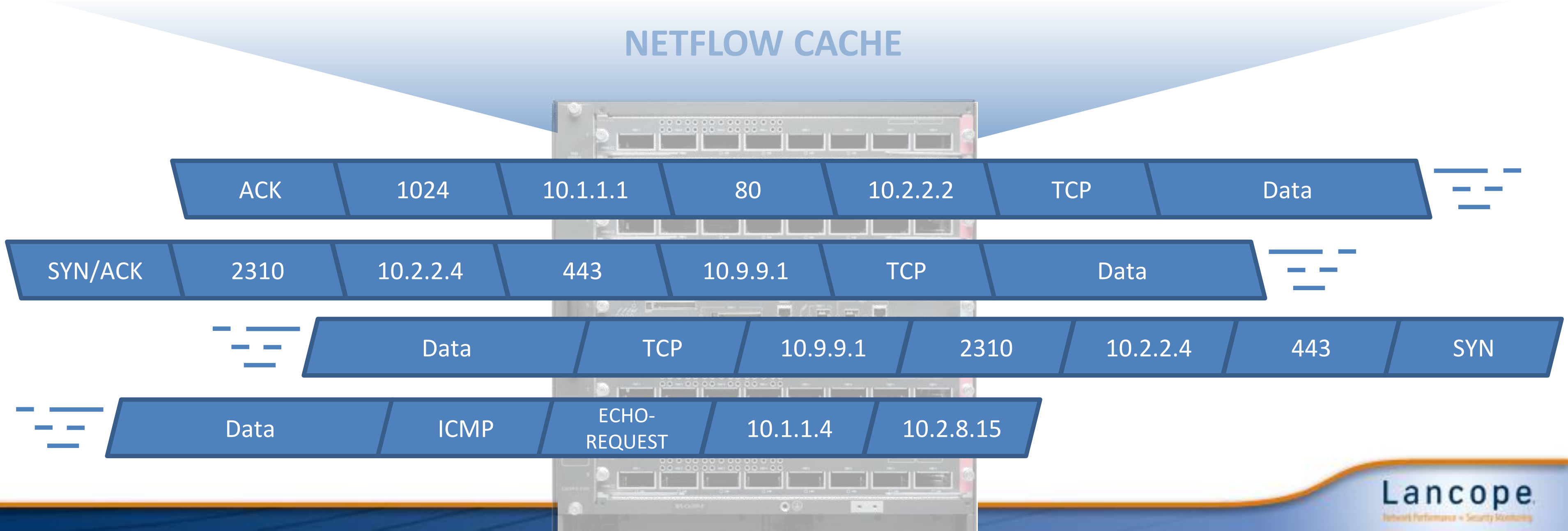
ECHO-RESPONSE

ICMP

Data

Continued Operation

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-
ICMP	10.2.8.14	-	10.1.1.4	ECHO-RESPONSE	23.14.13	23.14.13	1	92	Gi2/1	Gi4/19	-



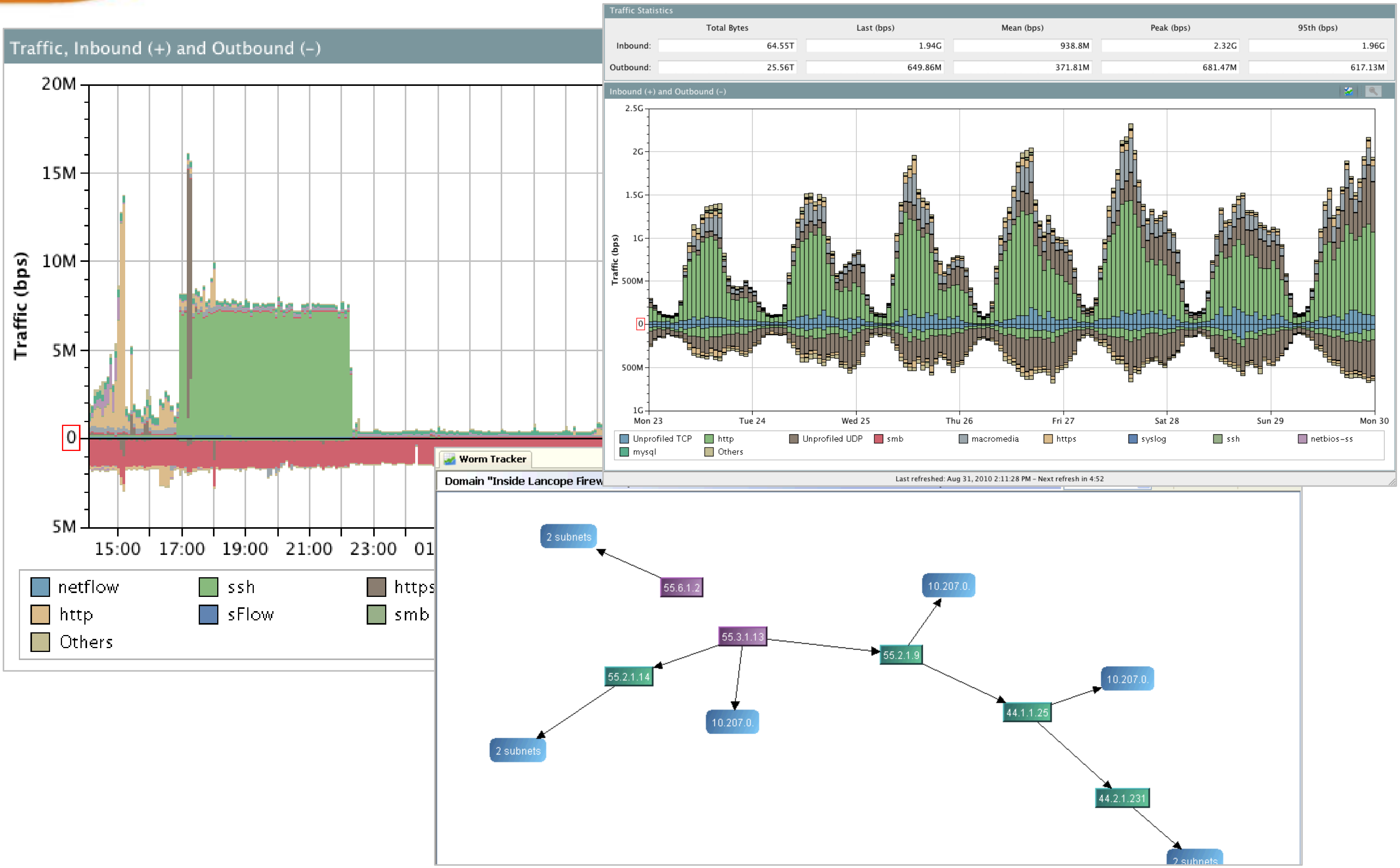
ACK | 1024 | 10.1.1.1 | 80 | 10.2.2.2 | TCP | Data

SYN/ACK | 2310 | 10.2.2.4 | 443 | 10.9.9.1 | TCP | Data

Data | TCP | 10.9.9.1 | 2310 | 10.2.2.4 | 443 | SYN

Data | ICMP | ECHO-REQUEST | 10.1.1.4 | 10.2.8.15

NetFlow In Action



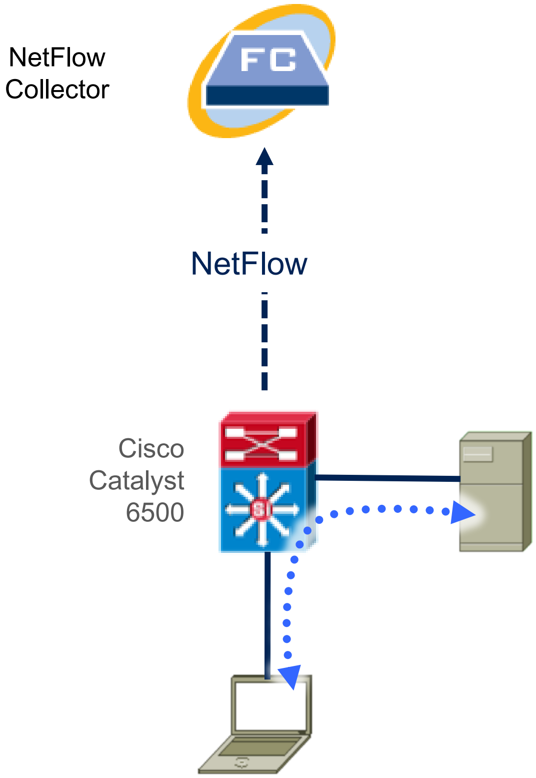
Traffic Statistics

	Total Bytes	Last (bps)	Mean (bps)	Peak (bps)	95th (bps)
Inbound:	64.55T	1.94G	938.8M	2.32G	1.96G
Outbound:	25.56T	649.86M	371.81M	681.47M	617.13M

Last refreshed: Aug 31, 2010 2:11:28 PM - Next refresh in 4:52

Flow Collection Methods

- **Traditional NetFlow**
  - Provides router interface statistics
  - Very easy to deploy; available for "free" almost anywhere Cisco equipment is found
  - No packet-level visibility or response time information
- **FlowSensor Appliance**
  - Enables flow monitoring where traditional NetFlow is not available
  - Provides flow performance information such as round-trip time and server response time
  - URL information in Flows
  - Requires SPAN port or Ethernet tap
- **FlowSensor Virtual Edition (VE)**
  - Installs into VMware ESX to monitor VM2VM communications
  - Software only, no hardware required



Cisco NetFlow Support

Cisco ASA

Cisco 2900

Cisco 2800

Cisco 1700

Cisco 7600

Cisco 7200 VXR

Cisco ISR G2

Cisco XR 12000

Hardware Supported

Cisco Nexus 7000

Cisco ASR

Cisco 3560/3750-X

Cisco Catalyst 4500

Cisco Catalyst 6500

Wide Support for NetFlow

Exinda 2060

Palo Alto
Firewalls

Huawei Quidway

Juniper Networks

BlueCoat PacketShaper

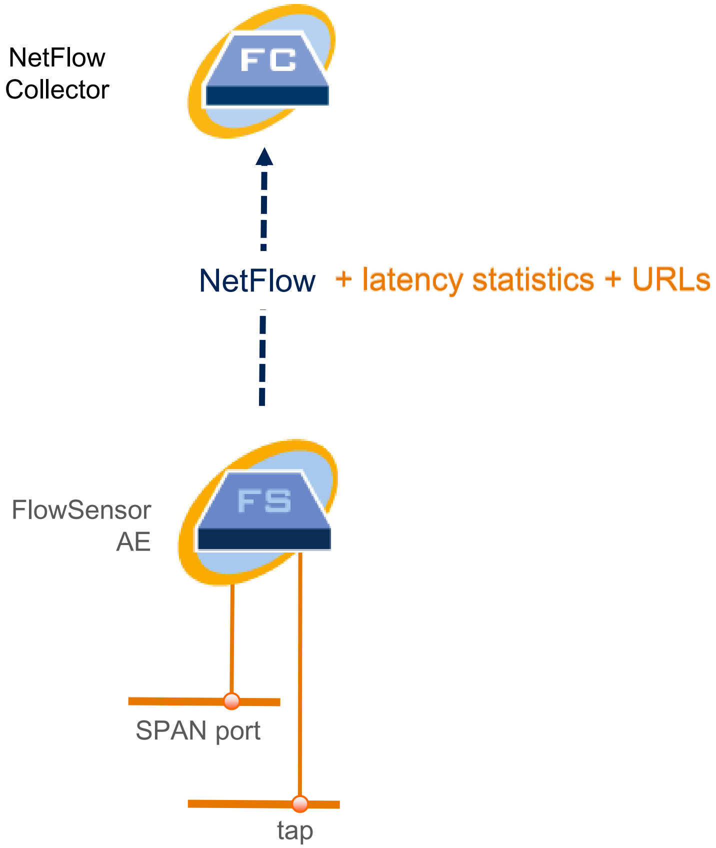
SonicWall 3500

Nortel Networks

Citrix NetScaler

Flow Collection Methods

- Traditional NetFlow
  - Provides router interface statistics
  - Very easy to deploy; available for "free" almost anywhere Cisco equipment is found
  - No packet-level visibility or response time information
- **FlowSensor Appliance**
  - Enables flow monitoring where traditional NetFlow is not available
  - Provides flow performance information such as round-trip time and server response time
  - URL information in Flows
  - Requires SPAN port or Ethernet tap
- FlowSensor Virtual Edition (VE)
  - Installs into VMware ESX to monitor VM2VM communications
  - Software only, no hardware required



Flow Collection Methods

- **Traditional NetFlow**
  - Provides router interface statistics
  - Very easy to deploy; available for “free” almost anywhere Cisco equipment is found
  - No packet-level visibility or response time information
- **FlowSensor Appliance**
  - Enables flow monitoring where traditional NetFlow is not available
  - Provides flow performance information such as round-trip time and server response time
  - URL information in Flows
  - Requires SPAN port or Ethernet tap
- **FlowSensor Virtual Edition (VE)**
  - Installs into VMware ESX to monitor VM2VM communications
  - Software only, no hardware required

FlowSensor VE: How It Works

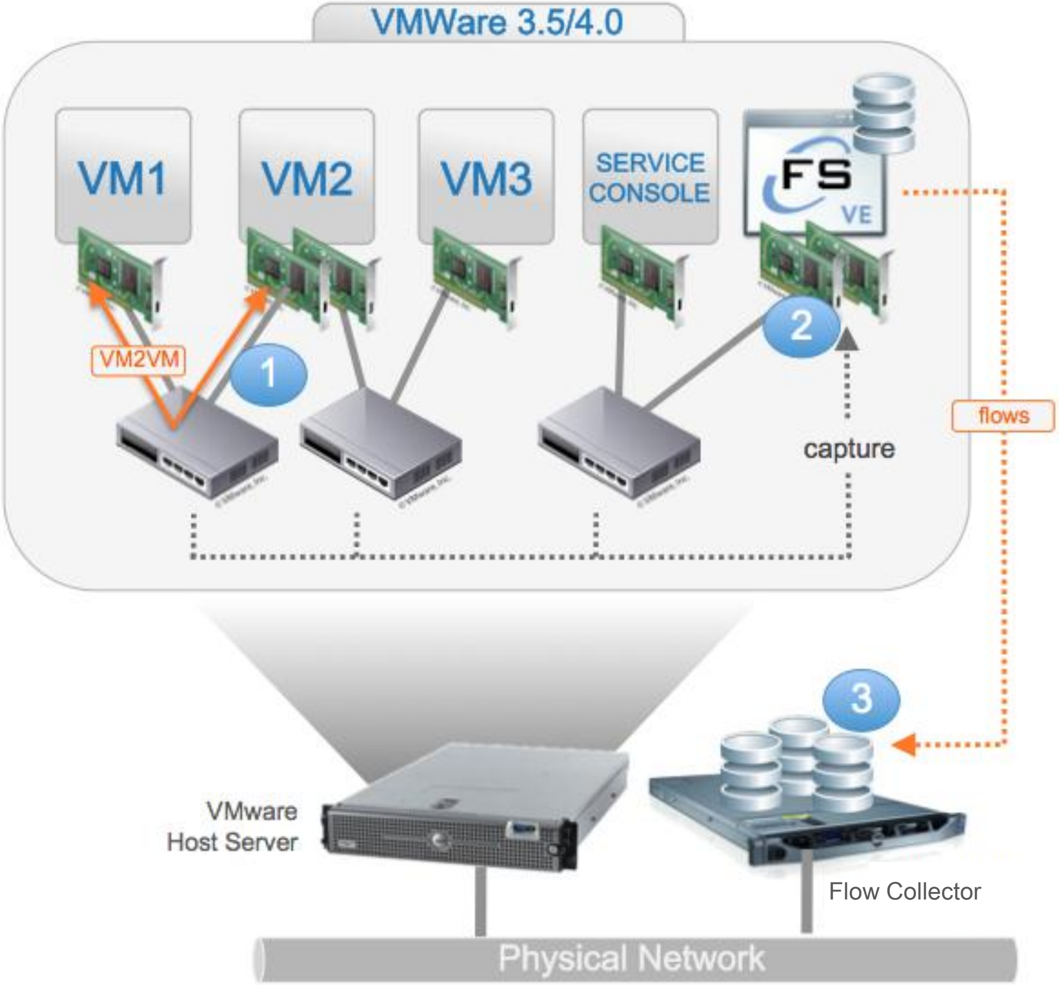
1 VM to VM communications captured by the FlowSensor

2 Virtualized FlowSensor creates NetFlow v9 packets just like a router

3 External Flow Collector has complete visibility into the virtual network backplane *(layer-2!)*

✱ Other virtual NetFlow enablement mechanisms:

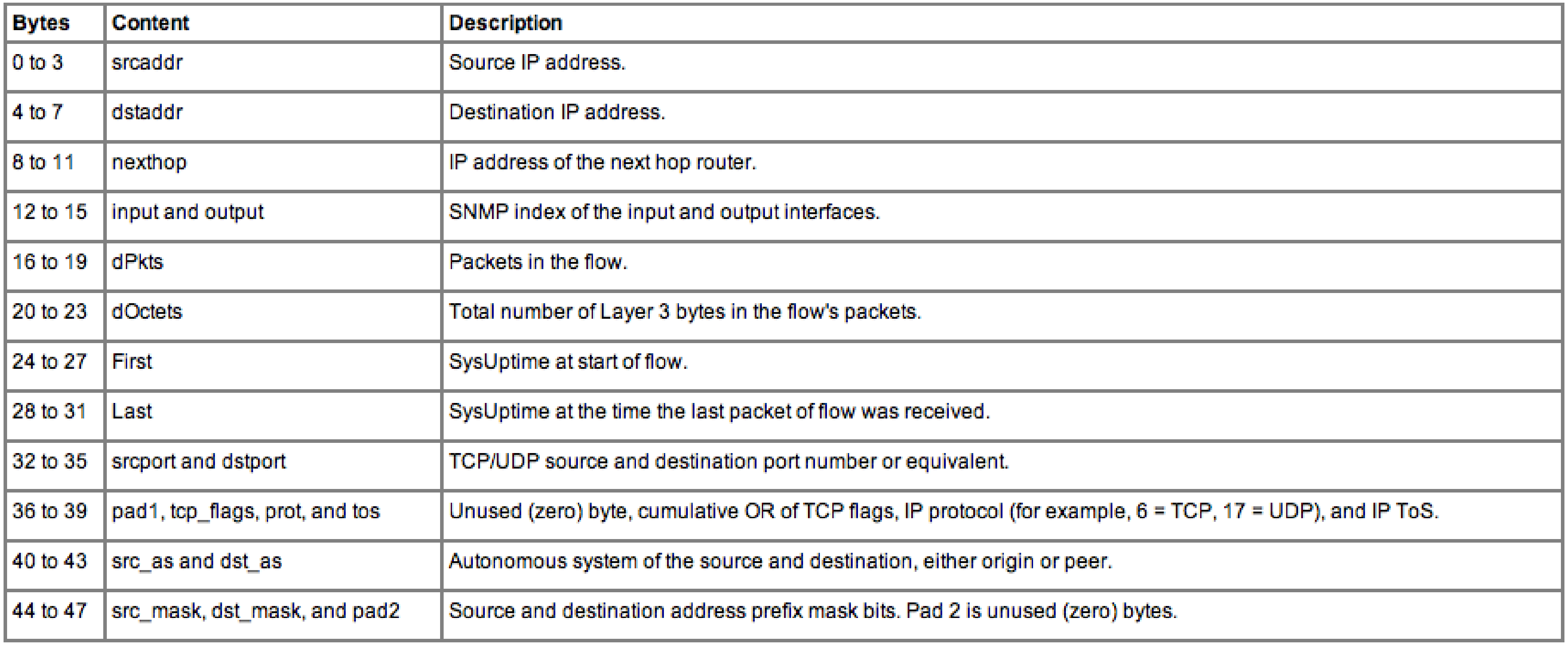
- *Cisco Nexus-1000v*
- *Xen Open vSwitch*



NetFlow Versions

Version	Status
v1	Similar to v5 but without sequence numbers or BGP info
v2	Never released
v3	Never released
v4	Never released
v5	Fixed format, most common version found in production
v6	Never released
v7	Similar to v5 but without TCP flags, specific to Cat5k and Cat6k
v8	Aggregated formats, never gained wide use in the enterprise
v9	“Next Gen” flow format found in most modern NetFlow exporters, supports IPv6, MPLS, Multicast, many others
IPFIX	Similar to v9 but standardized and with variable length fields

NetFlow v5* (most common)



Bytes	Content	Description
0 to 3	srcaddr	Source IP address.
4 to 7	dstaddr	Destination IP address.
8 to 11	nexthop	IP address of the next hop router.
12 to 15	input and output	SNMP index of the input and output interfaces.
16 to 19	dPkts	Packets in the flow.
20 to 23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24 to 27	First	SysUptime at start of flow.
28 to 31	Last	SysUptime at the time the last packet of flow was received.
32 to 35	srcport and dstport	TCP/UDP source and destination port number or equivalent.
36 to 39	pad1, tcp_flags, prot, and tos	Unused (zero) byte, cumulative OR of TCP flags, IP protocol (for example, 6 = TCP, 17 = UDP), and IP ToS.
40 to 43	src_as and dst_as	Autonomous system of the source and destination, either origin or peer.
44 to 47	src_mask, dst_mask, and pad2	Source and destination address prefix mask bits. Pad 2 is unused (zero) bytes.

* fixed format, cannot be extended to include new fields

NetFlow Version 9: Key Fields

Flow
Sampler ID
Direction

Interface
Input
Output

Layer 2
Source VLAN
Dest VLAN
Dot1q VLAN
Dot1q priority
Source MAC address
Destination MAC address

IPv4	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	TTL
Protocol	Options bitmap
Fragmentation Flags	Version
Fragmentation Offset	Precedence
Identification	DSCP
Header Length	TOS
Total Length	

IPv6	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	DSCP
Protocol	Extension Headers
Traffic Class	Hop-Limit
Flow Label	Length
Option Header	Next-header
Header Length	Version
Payload Length	

NetFlow Version 9: Key Fields

Routing
src or dest AS
Peer AS
Traffic Index
Forwarding Status
IGP Next Hop
BGP Next Hop
Input VRF Name

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type*	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

Application
Application ID

Multicast
Replication Factor*
RPF Check Drop*
Is-Multicast

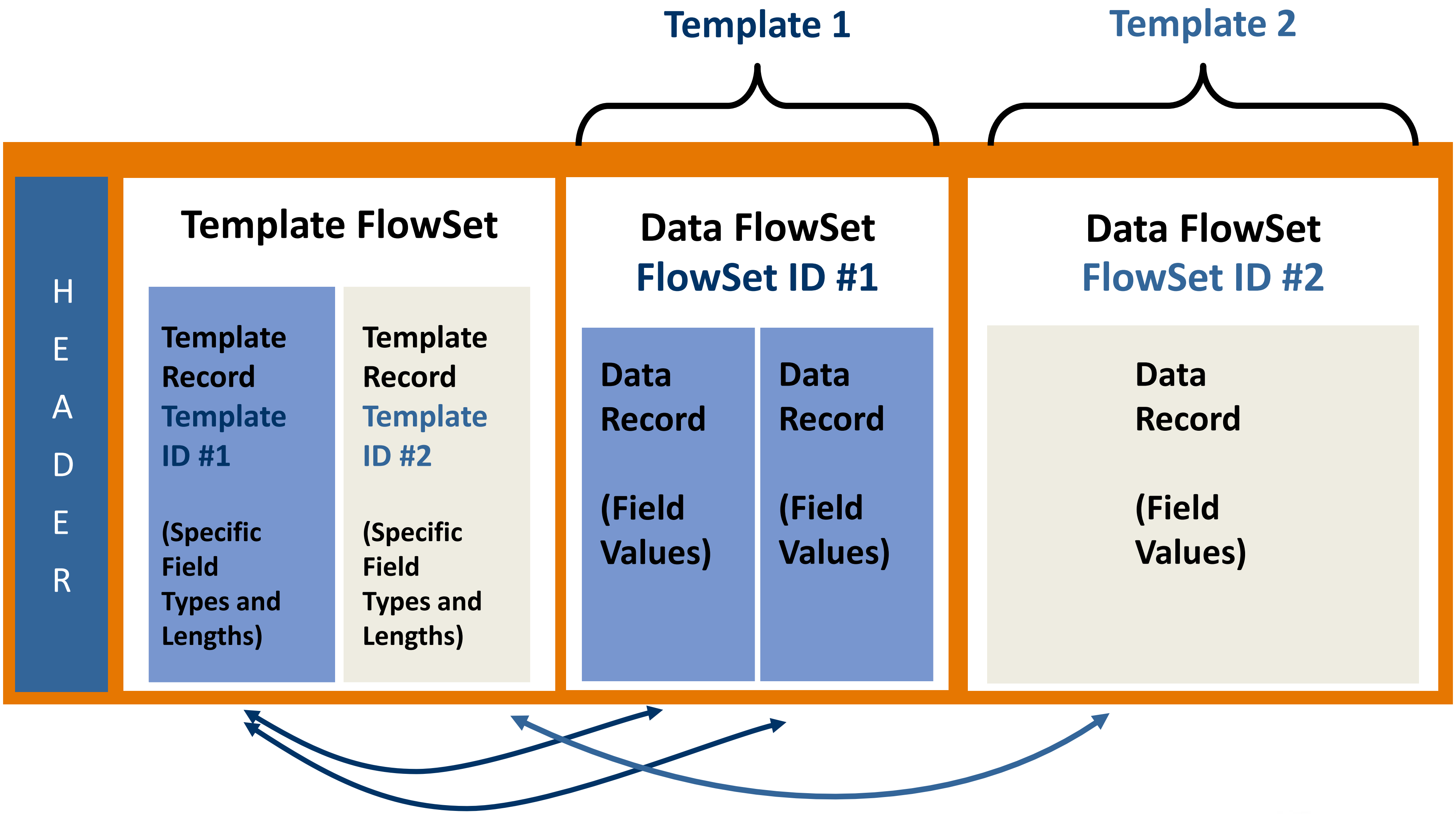
NetFlow Version 9: Non-Key Fields

Counters	Timestamp	IPv4	IPv4 and IPv6
Bytes	sysUpTime First Packet	Total Length Minimum (*)	Total Length Minimum (**)
Bytes Long	sysUpTime First Packet	Total Length Maximum (*)	Total Length Maximum (**)
Bytes Square Sum		TTL Minimum	
Bytes Square Sum Long		TTL Maximum	
Packets			
Packets Long			

- Plus any of the potential “key” fields: will be the value from the first packet in the flow

(*) IPV4_TOTAL_LEN_MIN, IPV4_TOTAL_LEN_MAX
(**)IP_LENGTH_TOTAL_MIN, IP_LENGTH_TOTAL_MAX

NetFlow Version 9 Export Packet


Template 1
Template 2
H E A D E R
Template FlowSet
Template Record Template ID #1 (Specific Field Types and Lengths)
Template Record Template ID #2 (Specific Field Types and Lengths)
Data FlowSet FlowSet ID #1
Data Record (Field Values)
Data Record (Field Values)
Data FlowSet FlowSet ID #2
Data Record (Field Values)

NetFlow v9: Application Aware NetFlow

Exinda

Palo Alto
Firewalls

SonicWall NSA

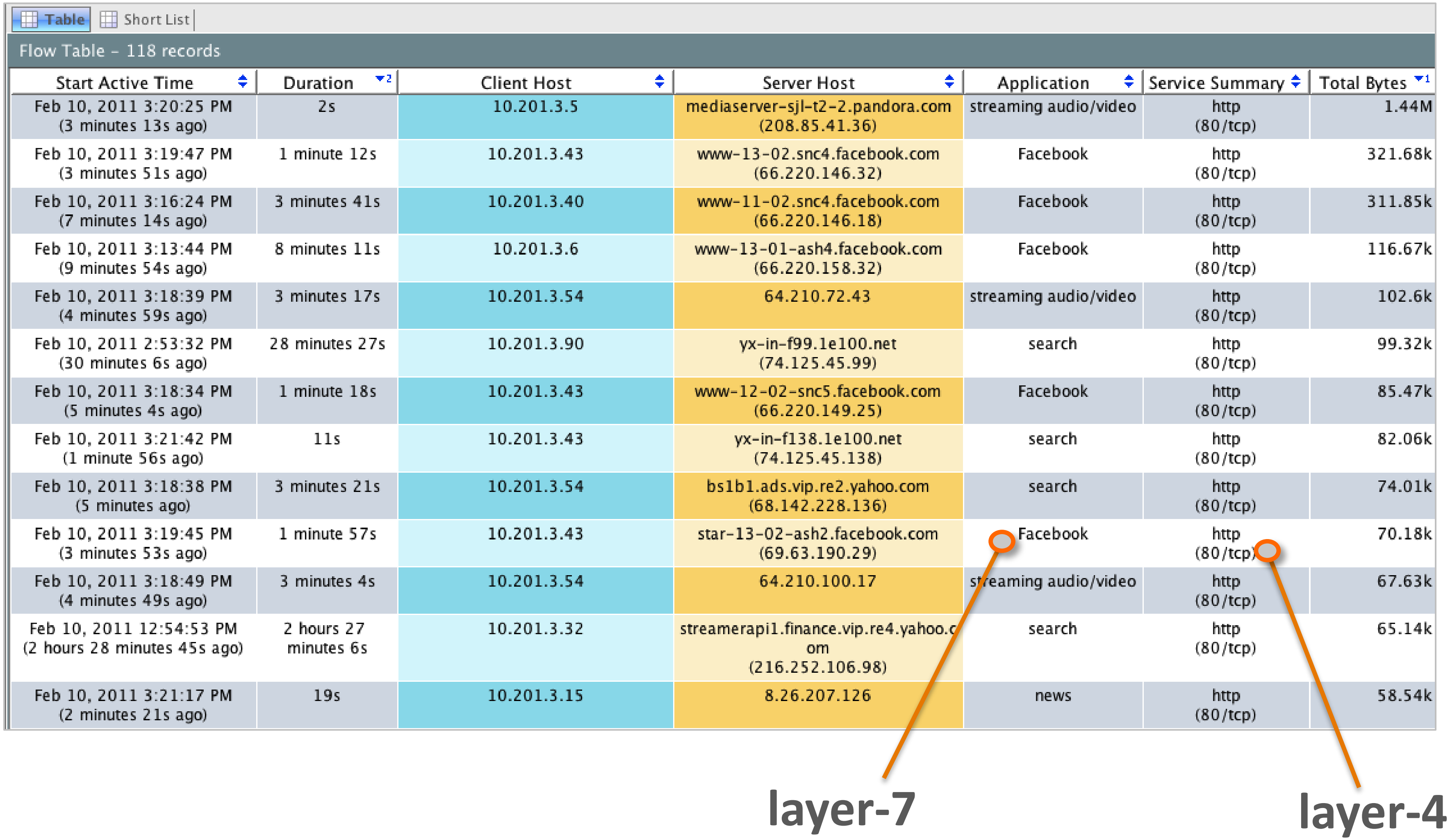
Lancope FlowSensor

BlueCoat PacketShaper

Cisco ASR

Cisco ISR G2

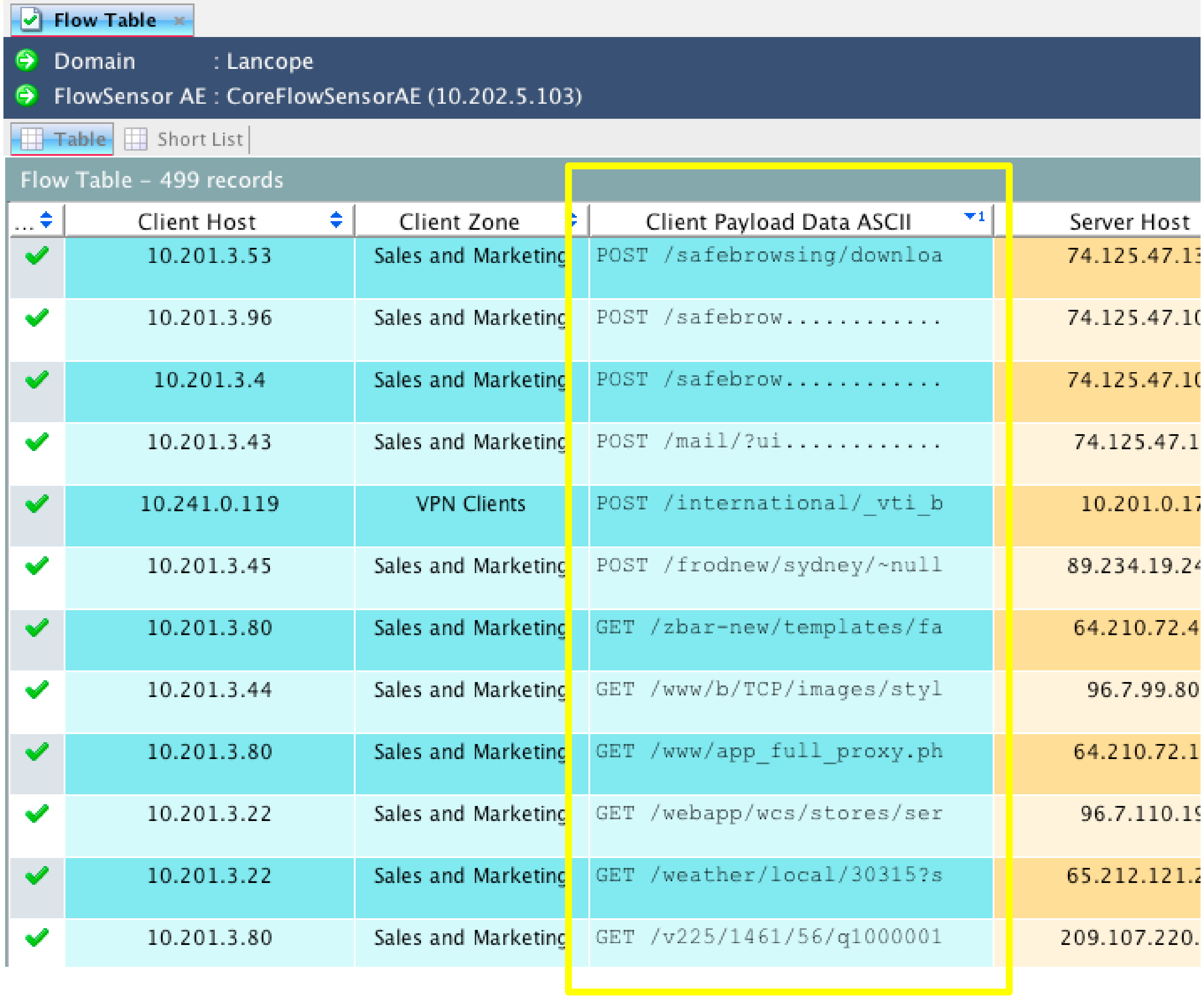
Application Awareness



Flow Table - 118 records

Start Active Time	Duration	Client Host	Server Host	Application	Service Summary	Total Bytes
Feb 10, 2011 3:20:25 PM (3 minutes 13s ago)	2s	10.201.3.5	mediaserver-sjl-t2-2.pandora.com (208.85.41.36)	streaming audio/video	http (80/tcp)	1.44M
Feb 10, 2011 3:19:47 PM (3 minutes 51s ago)	1 minute 12s	10.201.3.43	www-13-02.snc4.facebook.com (66.220.146.32)	Facebook	http (80/tcp)	321.68k
Feb 10, 2011 3:16:24 PM (7 minutes 14s ago)	3 minutes 41s	10.201.3.40	www-11-02.snc4.facebook.com (66.220.146.18)	Facebook	http (80/tcp)	311.85k
Feb 10, 2011 3:13:44 PM (9 minutes 54s ago)	8 minutes 11s	10.201.3.6	www-13-01-ash4.facebook.com (66.220.158.32)	Facebook	http (80/tcp)	116.67k
Feb 10, 2011 3:18:39 PM (4 minutes 59s ago)	3 minutes 17s	10.201.3.54	64.210.72.43	streaming audio/video	http (80/tcp)	102.6k
Feb 10, 2011 2:53:32 PM (30 minutes 6s ago)	28 minutes 27s	10.201.3.90	yx-in-f99.1e100.net (74.125.45.99)	search	http (80/tcp)	99.32k
Feb 10, 2011 3:18:34 PM (5 minutes 4s ago)	1 minute 18s	10.201.3.43	www-12-02-snc5.facebook.com (66.220.149.25)	Facebook	http (80/tcp)	85.47k
Feb 10, 2011 3:21:42 PM (1 minute 56s ago)	11s	10.201.3.43	yx-in-f138.1e100.net (74.125.45.138)	search	http (80/tcp)	82.06k
Feb 10, 2011 3:18:38 PM (5 minutes ago)	3 minutes 21s	10.201.3.54	bs1b1.ads.vip.re2.yahoo.com (68.142.228.136)	search	http (80/tcp)	74.01k
Feb 10, 2011 3:19:45 PM (3 minutes 53s ago)	1 minute 57s	10.201.3.43	star-13-02-ash2.facebook.com (69.63.190.29)	Facebook	http (80/tcp)	70.18k
Feb 10, 2011 3:18:49 PM (4 minutes 49s ago)	3 minutes 4s	10.201.3.54	64.210.100.17	streaming audio/video	http (80/tcp)	67.63k
Feb 10, 2011 12:54:53 PM (2 hours 28 minutes 45s ago)	2 hours 27 minutes 6s	10.201.3.32	streamerapi1.finance.vip.re4.yahoo.com (216.252.106.98)	search	http (80/tcp)	65.14k
Feb 10, 2011 3:21:17 PM (2 minutes 21s ago)	19s	10.201.3.15	8.26.207.126	news	http (80/tcp)	58.54k

HTTP Application Awareness – Flow Payload Sampling



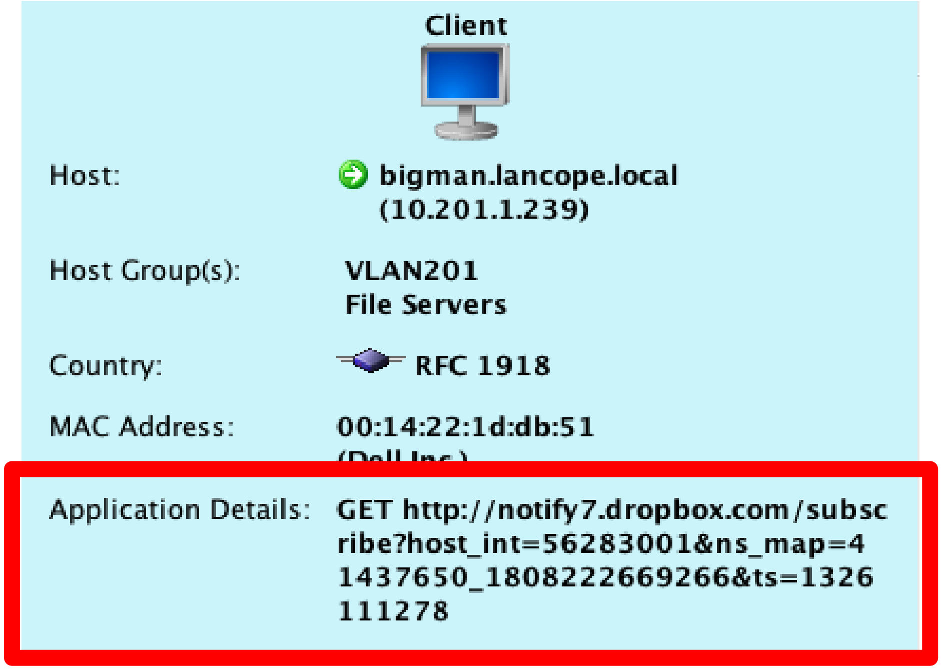
Domain : Lancope
FlowSensor AE : CoreFlowSensorAE (10.202.5.103)

Flow Table – 499 records

...	Client Host	Client Zone	Client Payload Data ASCII	Server Host
✓	10.201.3.53	Sales and Marketing	POST /safebrowsing/downloa	74.125.47.13
✓	10.201.3.96	Sales and Marketing	POST /safebrow............	74.125.47.10
✓	10.201.3.4	Sales and Marketing	POST /safebrow............	74.125.47.10
✓	10.201.3.43	Sales and Marketing	POST /mail/?ui............	74.125.47.1
✓	10.241.0.119	VPN Clients	POST /international/_vti_b	10.201.0.17
✓	10.201.3.45	Sales and Marketing	POST /frodnew/sydney/~null	89.234.19.24
✓	10.201.3.80	Sales and Marketing	GET /zbar-new/templates/fa	64.210.72.4
✓	10.201.3.44	Sales and Marketing	GET /www/b/TCP/images/styl	96.7.99.80
✓	10.201.3.80	Sales and Marketing	GET /www/app_full_proxy.ph	64.210.72.1
✓	10.201.3.22	Sales and Marketing	GET /webapp/wcs/stores/ser	96.7.110.19
✓	10.201.3.22	Sales and Marketing	GET /weather/local/30315?s	65.212.121.2
✓	10.201.3.80	Sales and Marketing	GET /v225/1461/56/q1000001	209.107.220.

URL Data from the FlowSensor

- Added Application Details (meta-data) by extending existing Payload functionality
  - For HTTP: Host name, path, and response code / error messages
  - For HTTPS: Common name and organization
- Flow Table is only place this information is shown



Client

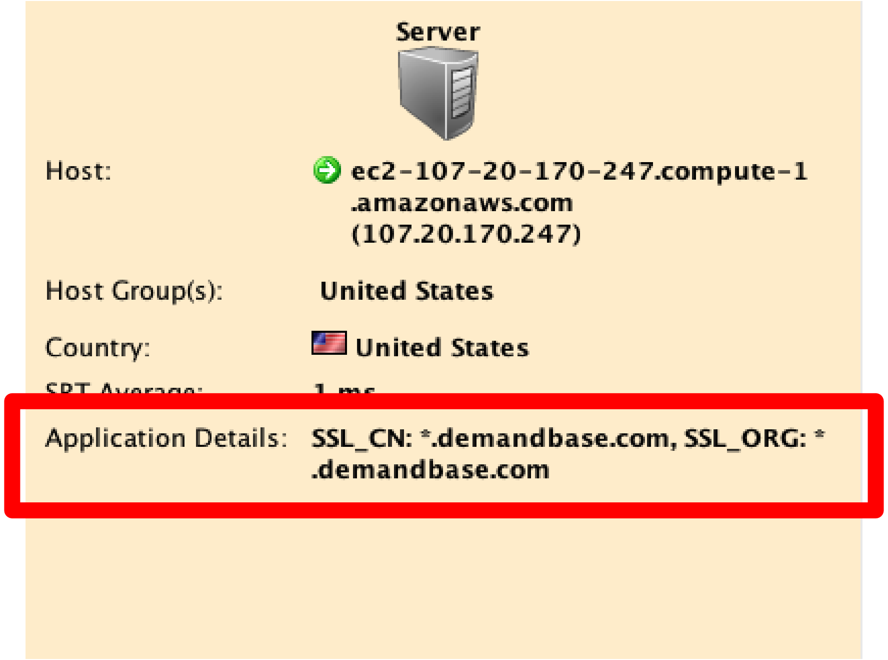
Host: bigman.lancope.local (10.201.1.239)

Host Group(s): VLAN201
File Servers

Country: RFC 1918

MAC Address: 00:14:22:1d:db:51 (Dell Inc.)

Application Details: GET http://notify7.dropbox.com/subscribe?host_int=56283001&ns_map=41437650_1808222669266&ts=1326111278



Server

Host: ec2-107-20-170-247.compute-1.amazonaws.com (107.20.170.247)

Host Group(s): United States

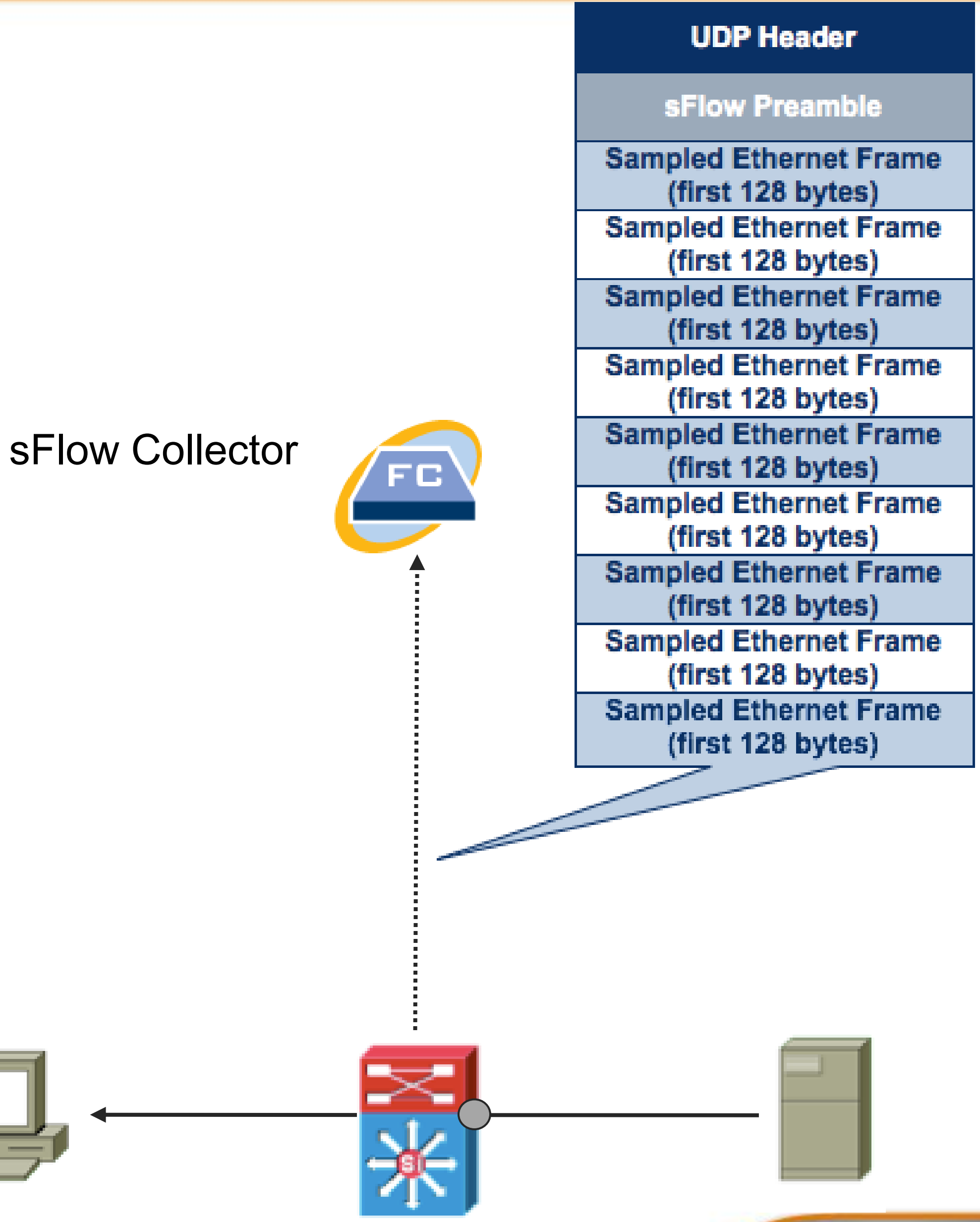
Country: United States

SRT Average: 1 ms

Application Details: SSL_CN: *.demandbase.com, SSL_ORG: *.demandbase.com

A Note on sFlow

- Found in Foundry, Extreme, HP Procurve, etc
- Uses sampling such as "1 in 128" packets
- The first ~100 bytes of the Ethernet frame is extracted and placed into a UDP packet
- 1500 sFlow packets are sent to the sFlow collector
- Collector scales the byte counts based on scaling factor
- Performs poorly in low-bandwidth environment or when full flow details are needed (compliance)



sFlow Collector

UDP Header

sFlow Preamble

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Sampled Ethernet Frame (first 128 bytes)

Lancope.
Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

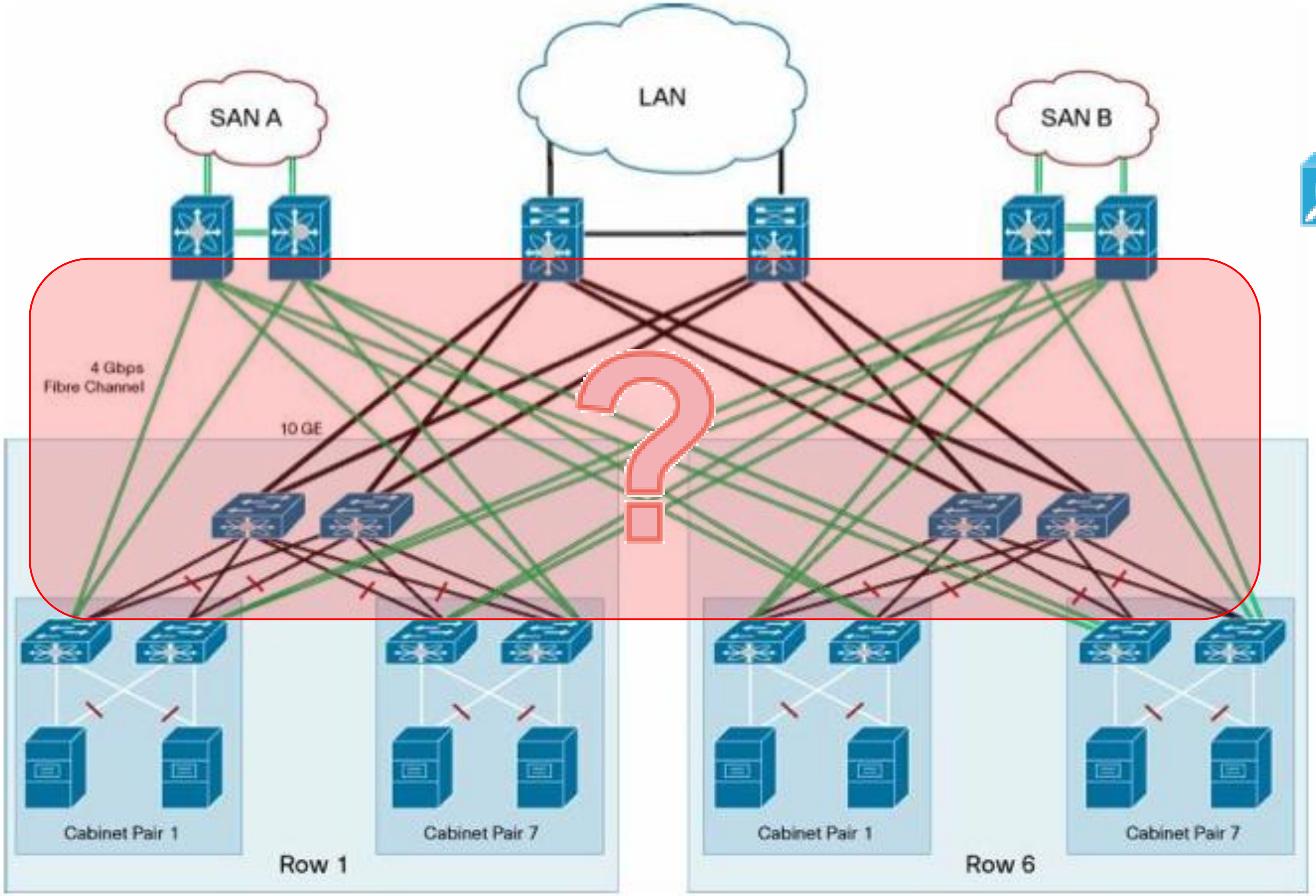
Why NetFlow?

Business Challenges

- High availability and performance of the Network and its Apps
- Constantly evolving networks create gaps in monitoring
  - 10G, 40G, 100G Interfaces
  - MPLS & Multipoint VPN
- Lack of Internal security
  - Gaps left by traditional security technologies
  - High-speed, highly segmented networks
  - IT Consumerization
- Rapidly evolving threats - How do we stay out of the news?
  - Advanced Persistent Threat
  - Denial of Service
  - Data Exfiltration
- Compliance – SOX, PCI, HIPPA, etc
  - Lack of visibility into behaviors across the network
  - User accountability for employees, partners, consultants, customers

10G+ Ethernet

“10G Ethernet is so fast few probe technologies can keep up and those that can are too expensive”

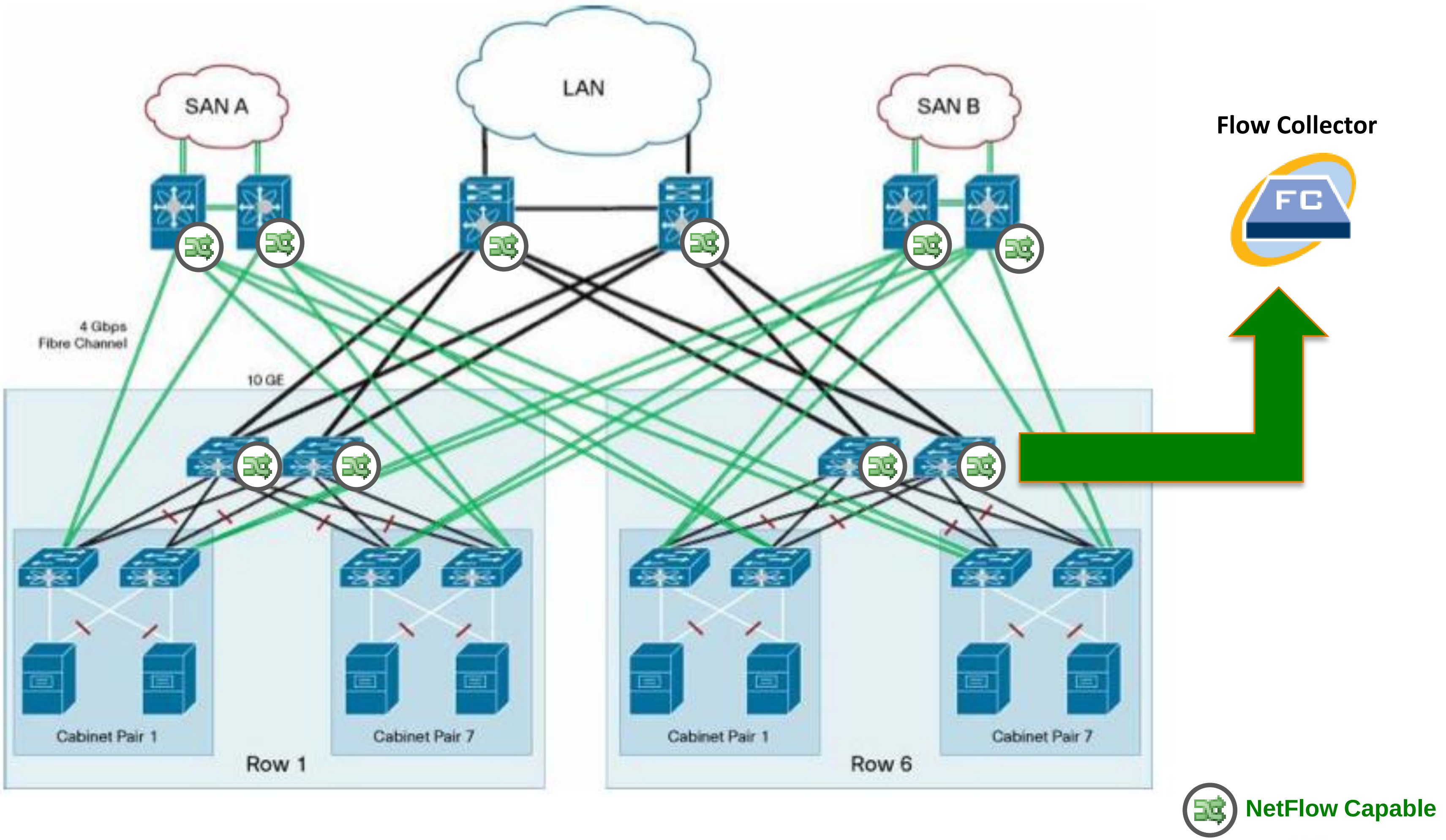


traditional Ethernet sensor

Where to plug in?

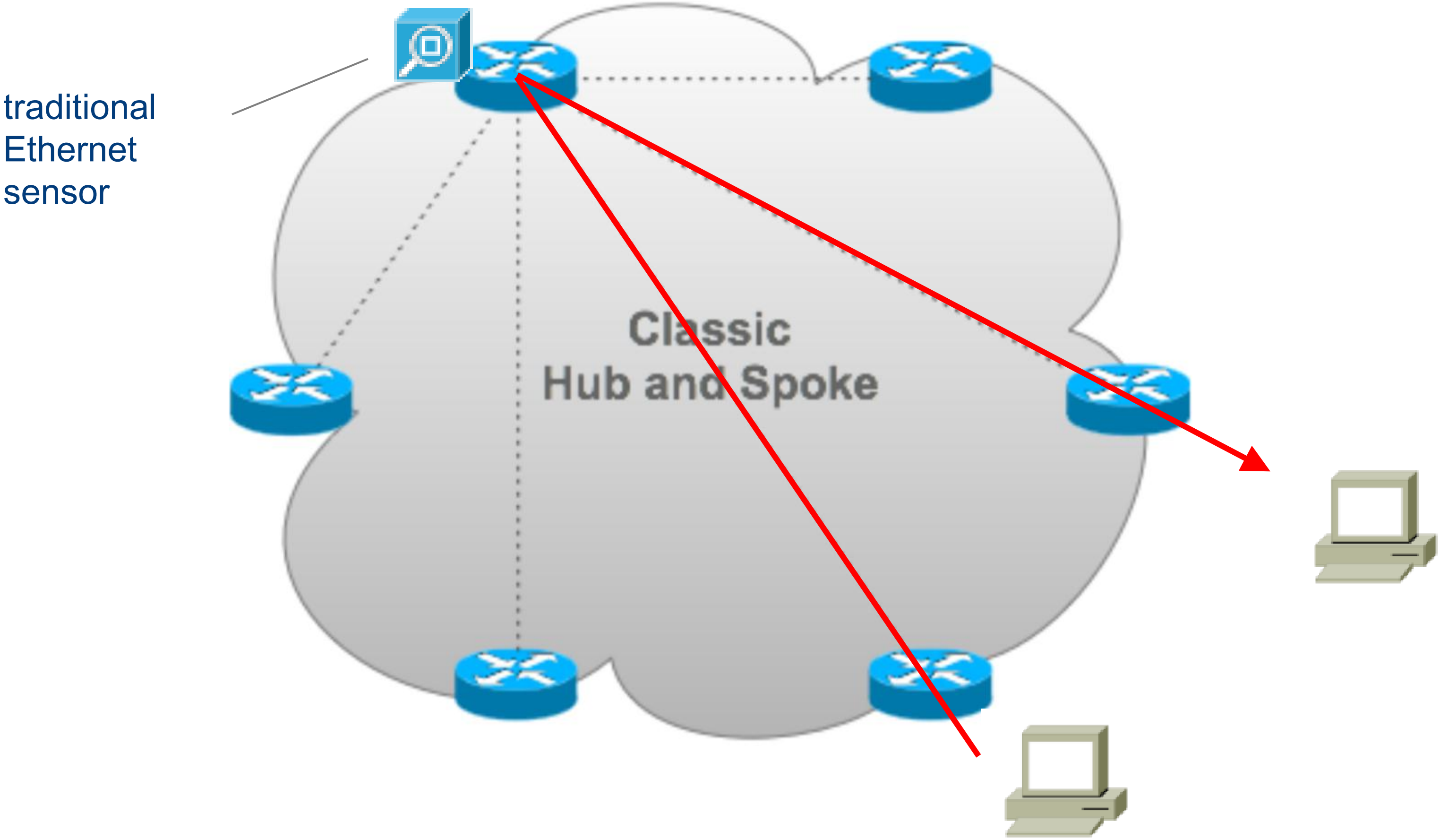
10G+ Ethernet

“NetFlow enables monitoring without the high cost of placing probes throughout the network”



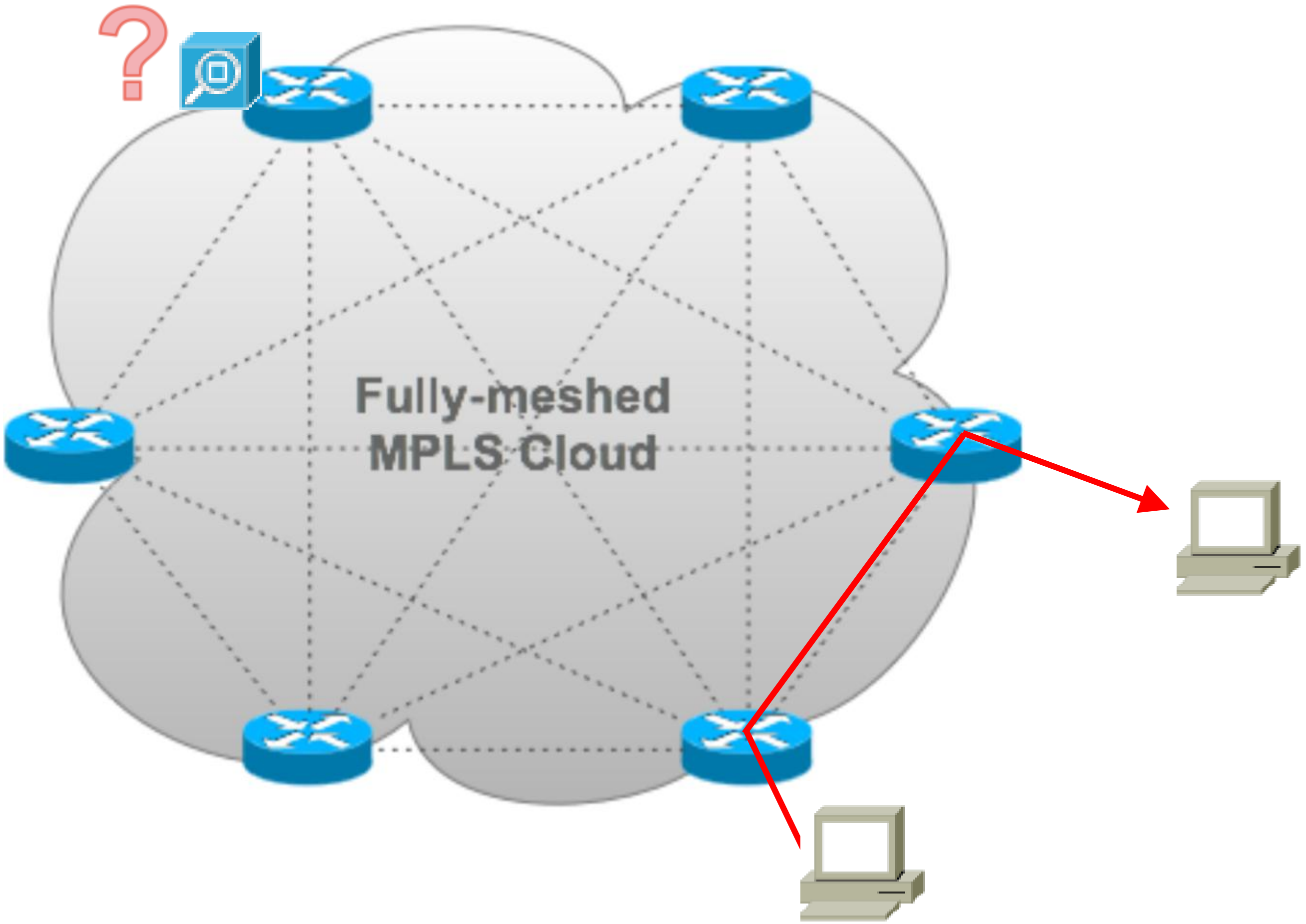
MPLS and Multi-point VPNs

"MPLS and multi-point VPNs create a meshed WAN that's expensive to monitor adequately"



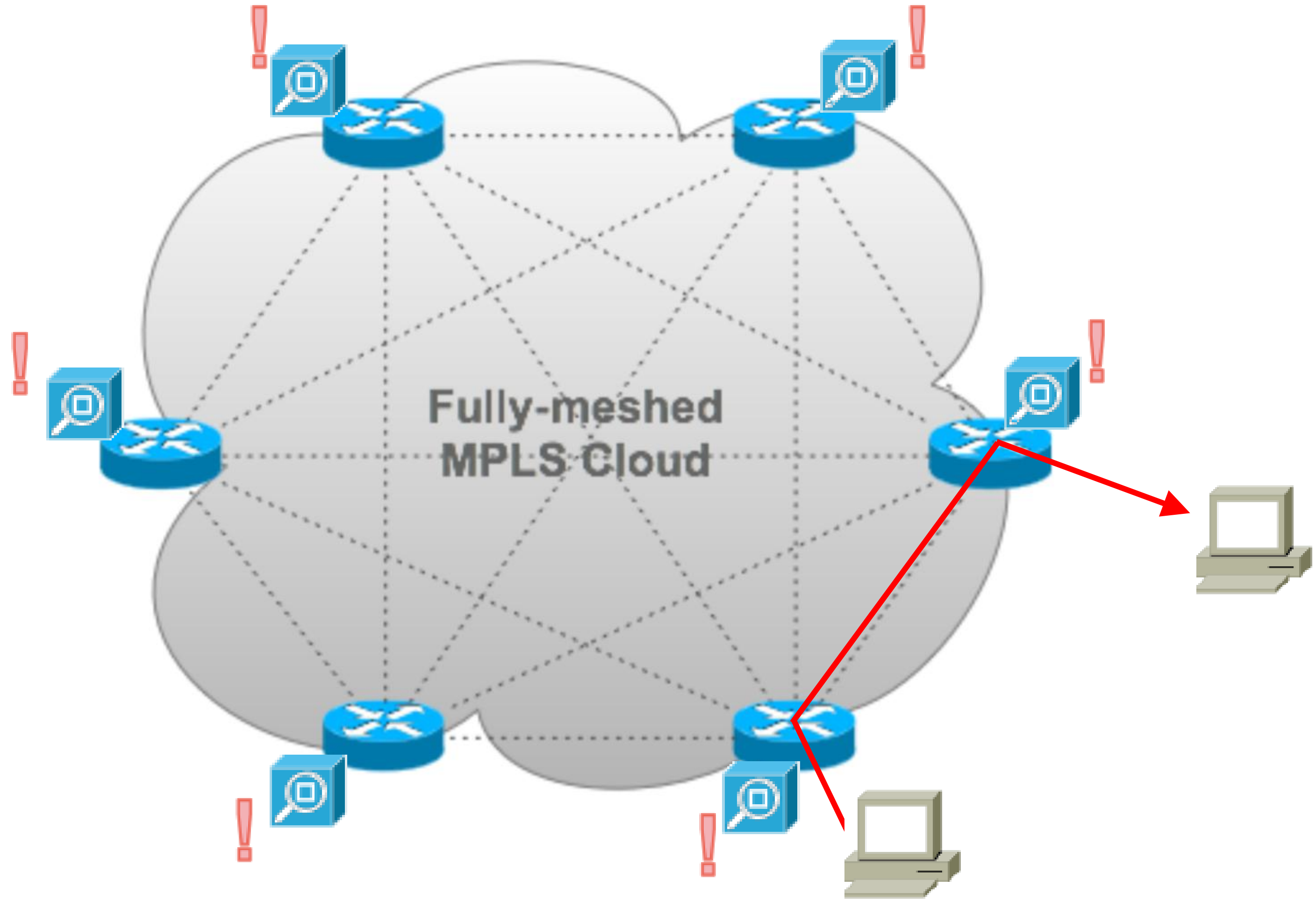
MPLS and Multi-point VPNs

Fully meshed connectivity circumvents network monitoring deployed at the "hub" location…



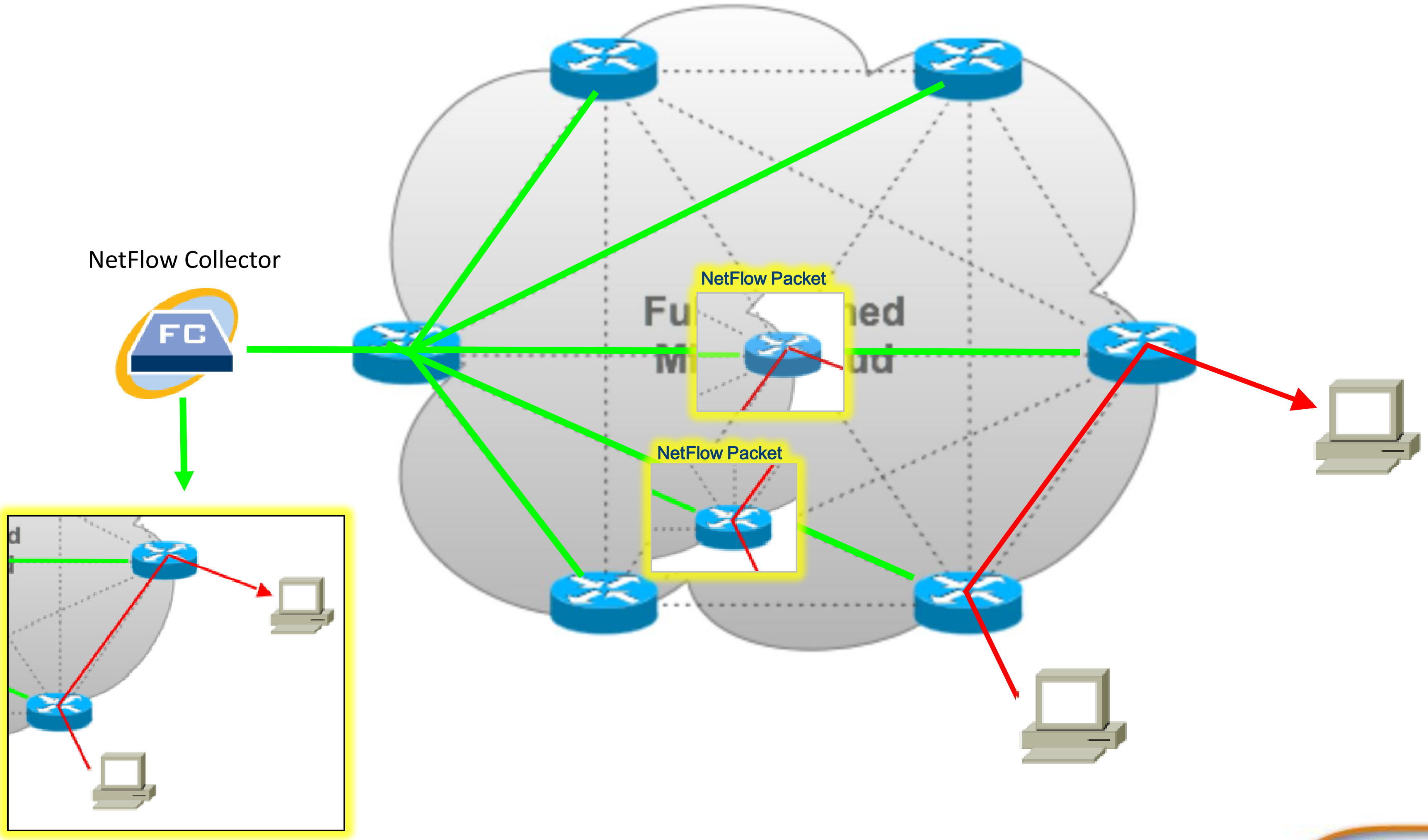
MPLS and Multi-point VPNs

Full visibility requires a probe at each location throughout the WAN…



NetFlow Collection in the WAN

Deploy a StealthWatch NetFlow collector at a central location and enable NetFlow at each remote site…



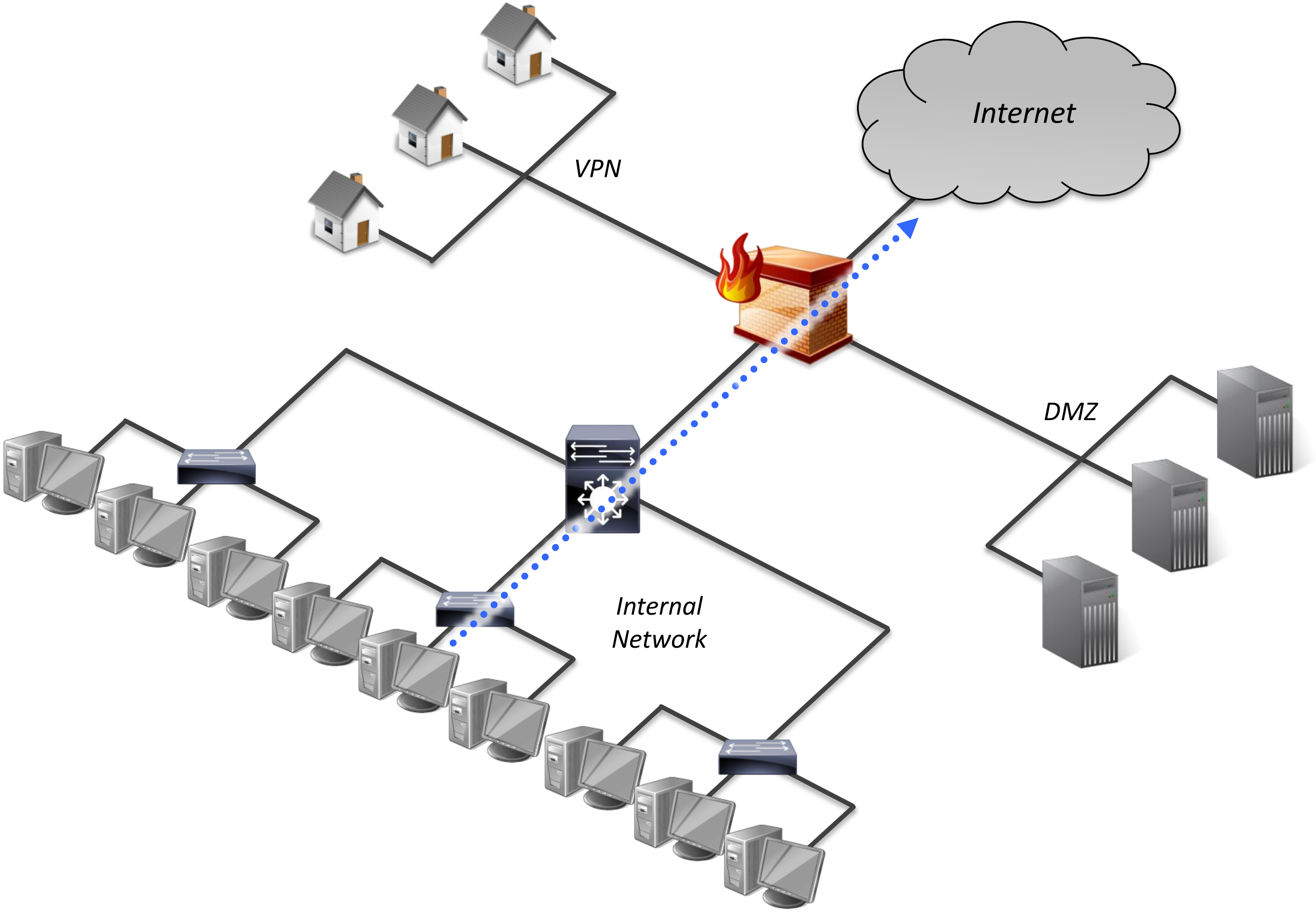
NetFlow Benefits for Network Operations

- Fully integrated view of:
  - Network usage
  - Performance
  - Host integrity
  - User behavior
- Diagnose the source and root cause of a network problem causing response time delays
- Network management and security operations collaboration
- Avoid expensive upgrades and complexity to existing network management and security architectures with fully meshed networks
- Provides extensive historical and trending data to facilitate network performance capacity planning and resource management

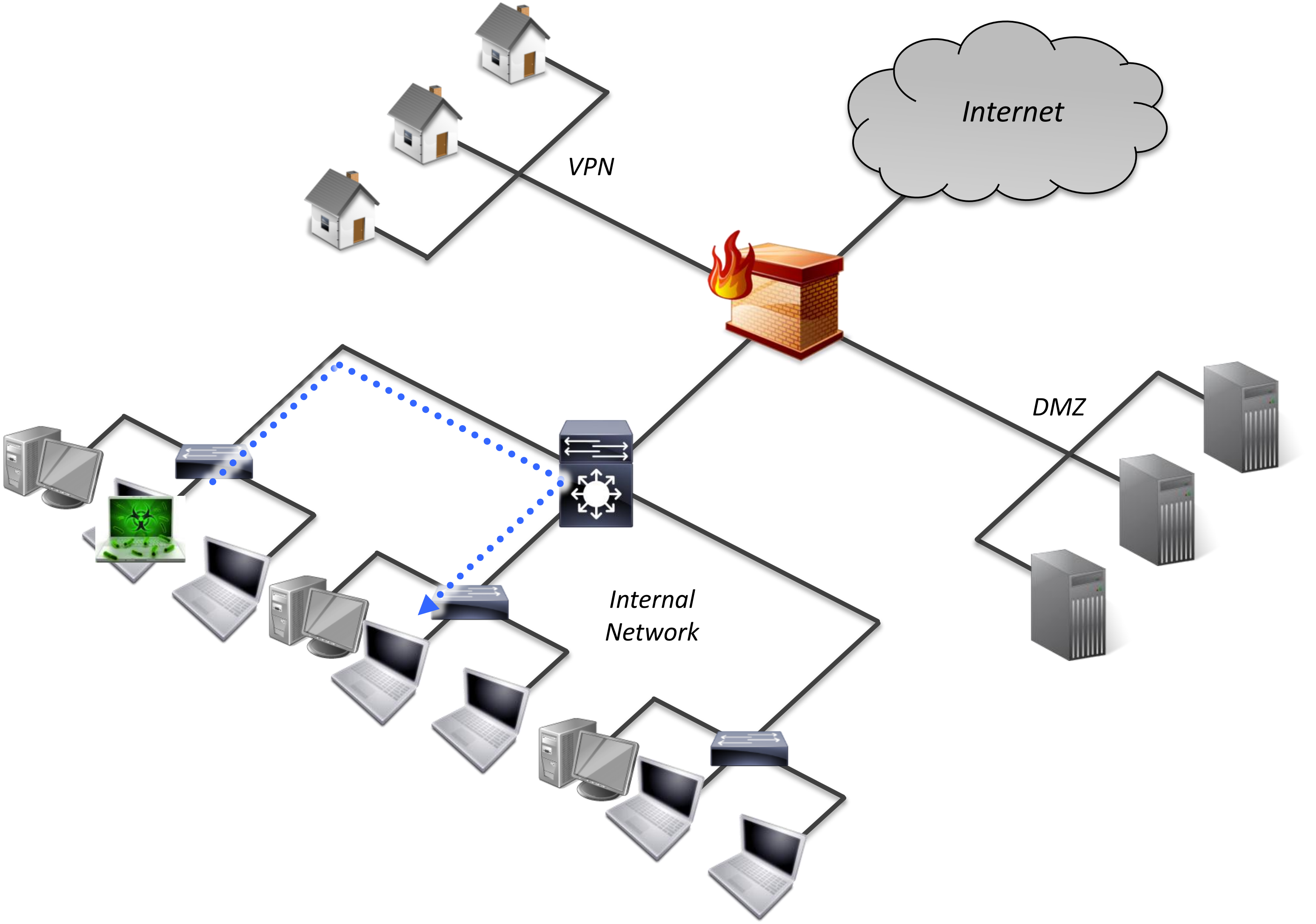
Business Challenges

- High availability and performance of the Network and its Apps
- Constantly evolving networks create gaps in monitoring
  - 10G, 40G, 100G Interfaces
  - MPLS & Multipoint VPN
- Lack of Internal security
  - Gaps left by traditional security technologies
  - High-speed, highly segmented networks
  - IT Consumerization
- Rapidly evolving threats - How do we stay out of the news?
  - Advanced Persistent Threat
  - Denial of Service
  - Data Exfiltration
- Compliance – SOX, PCI, HIPPA, etc
  - Lack of visibility into behaviors across the network
  - User accountability for employees, partners, consultants, customers

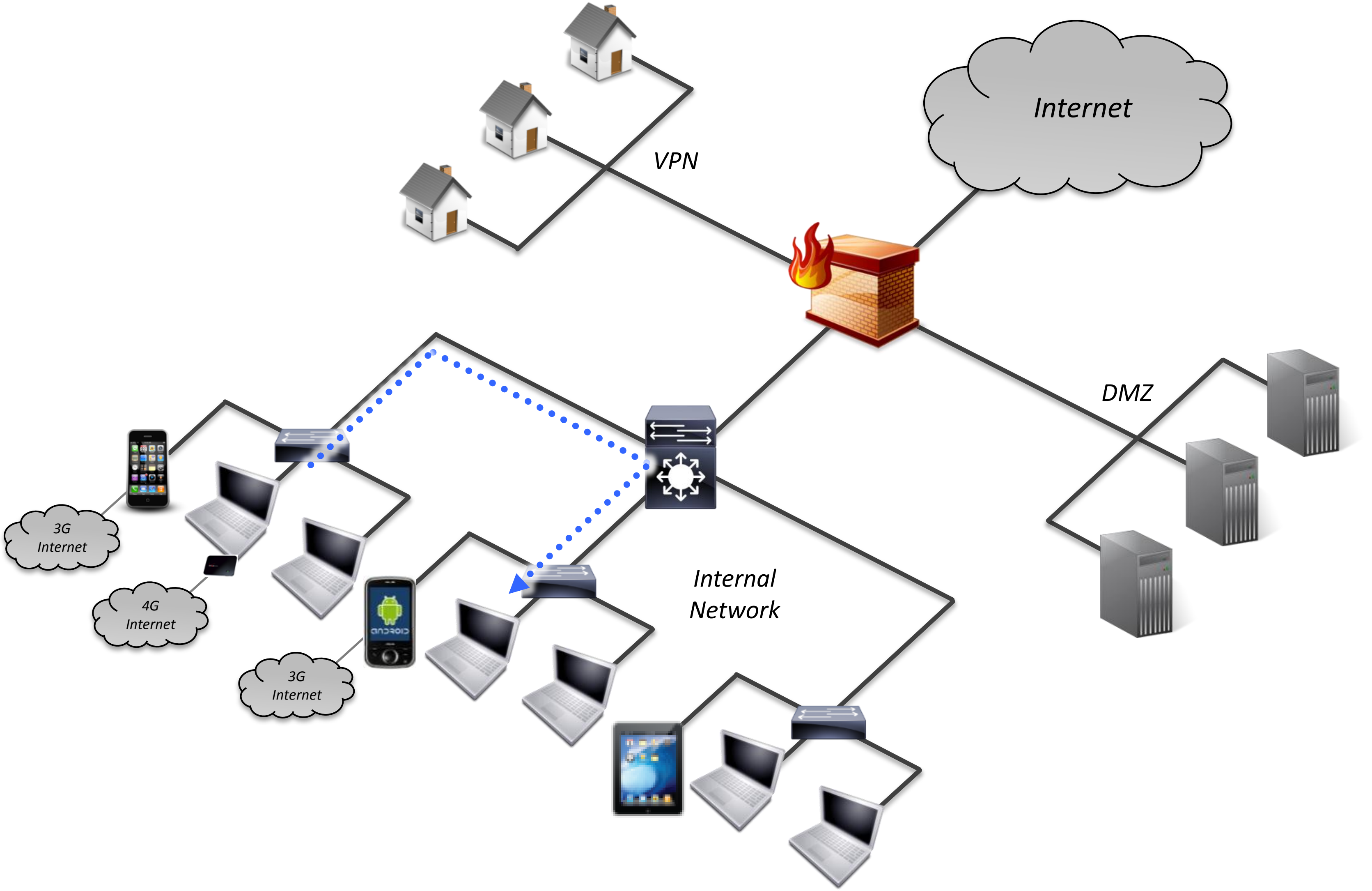
Once upon a time



The Mobile Computing Era



And now BYOD or IT Consumerization



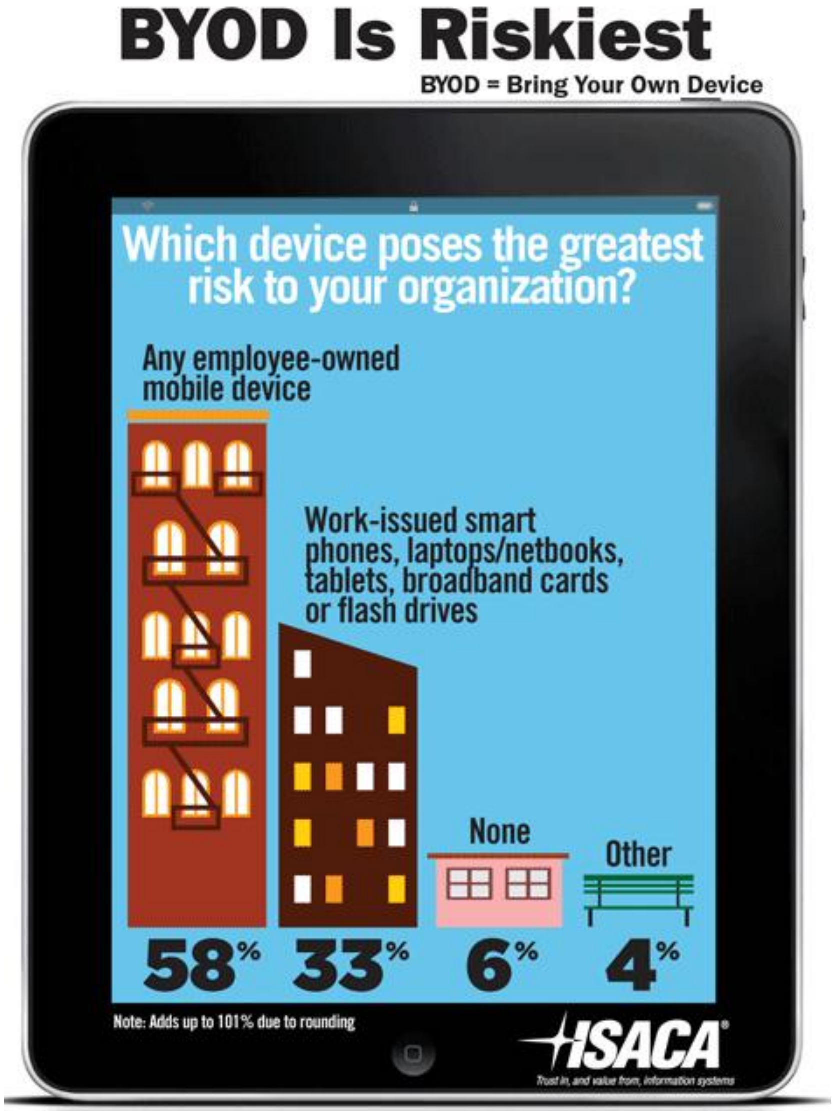
BYOD is Riskiest

- Difficult to find common AV or host based IDS spanning platforms
- Reliant on employees to install them

- Cisco says **70 percent** of young workers ignore IT rules.

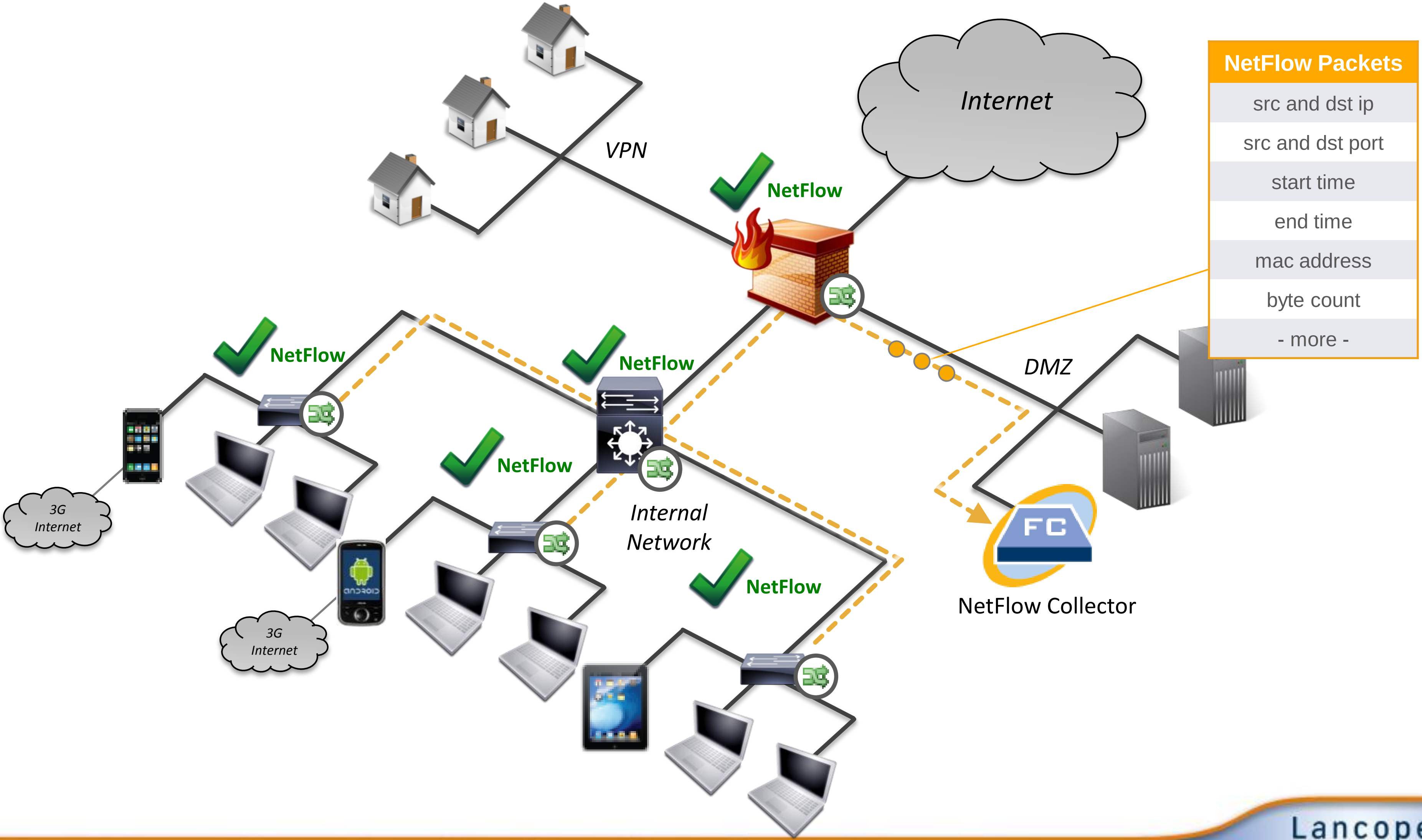
http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=586267

- **Over half** of all IT leaders in the U.S. say that employee-owned mobile devices pose a greater risk to the enterprise than mobile devices supplied by the company.



Source: 2011 ISACA IT Risk/Reward Barometer-US Edition (www.isaca.org/risk-reward-barometer)

Internal Visibility Through NetFlow



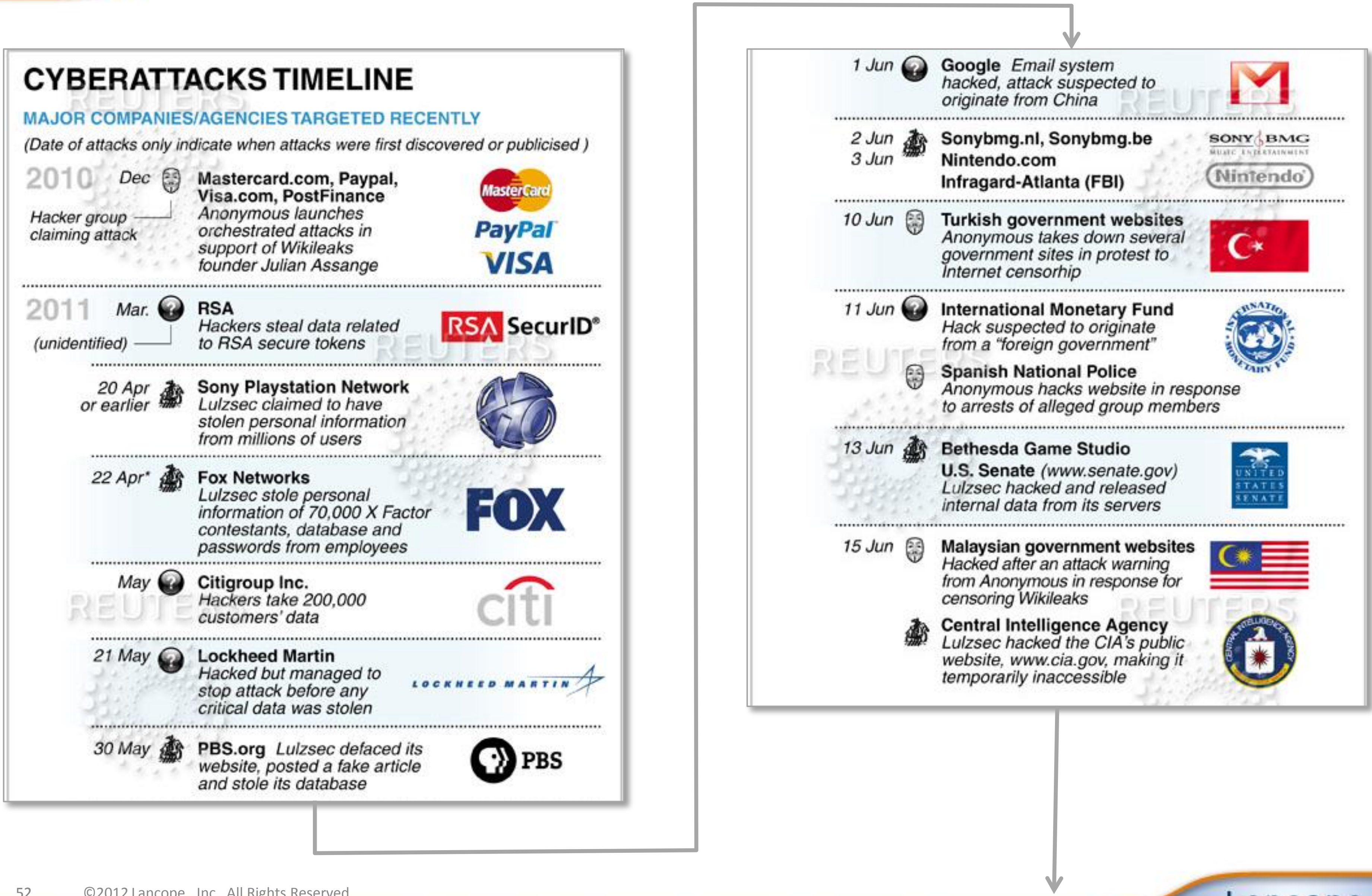
NetFlow Packets

- src and dst ip
- src and dst port
- start time
- end time
- mac address
- byte count
- - more -

Business Challenges

- High availability and performance of the Network and its Apps
- Constantly evolving networks create gaps in monitoring
  - 10G, 40G, 100G Interfaces
  - MPLS & Multipoint VPN
- Lack of Internal security
  - Gaps left by traditional security technologies
  - High-speed, highly segmented networks
  - IT Consumerization
- Rapidly evolving threats - How do we stay out of the news?
  - Advanced Persistent Threat
  - Denial of Service
  - Data exfiltration
- Compliance – SOX, PCI, HIPPA, etc
  - Lack of visibility into behaviors across the network
  - User accountability for employees, partners, consultants, customers

The Threats are Real



CYBERATTACKS TIMELINE

MAJOR COMPANIES/AGENCIES TARGETED RECENTLY

(Date of attacks only indicate when attacks were first discovered or publicised)

2010 *Dec* — *Hacker group claiming attack*

Mastercard.com, Paypal, Visa.com, PostFinance *Anonymous launches orchestrated attacks in support of Wikileaks founder Julian Assange*

2011 *Mar.* — *(unidentified)*

RSA *Hackers steal data related to RSA secure tokens*

20 Apr or earlier **Sony Playstation Network** *Lulzsec claimed to have stolen personal information from millions of users*

*22 Apr** **Fox Networks** *Lulzsec stole personal information of 70,000 X Factor contestants, database and passwords from employees*

May **Citigroup Inc.** *Hackers take 200,000 customers' data*

21 May **Lockheed Martin** *Hacked but managed to stop attack before any critical data was stolen*

30 May **PBS.org** *Lulzsec defaced its website, posted a fake article and stole its database*

1 Jun **Google** *Email system hacked, attack suspected to originate from China*

2 Jun **Sonybmg.nl, Sonybmg.be**

3 Jun **Nintendo.com**

Infragard-Atlanta (FBI)

10 Jun **Turkish government websites** *Anonymous takes down several government sites in protest to Internet censorhip*

11 Jun **International Monetary Fund** *Hack suspected to originate from a "foreign government"*

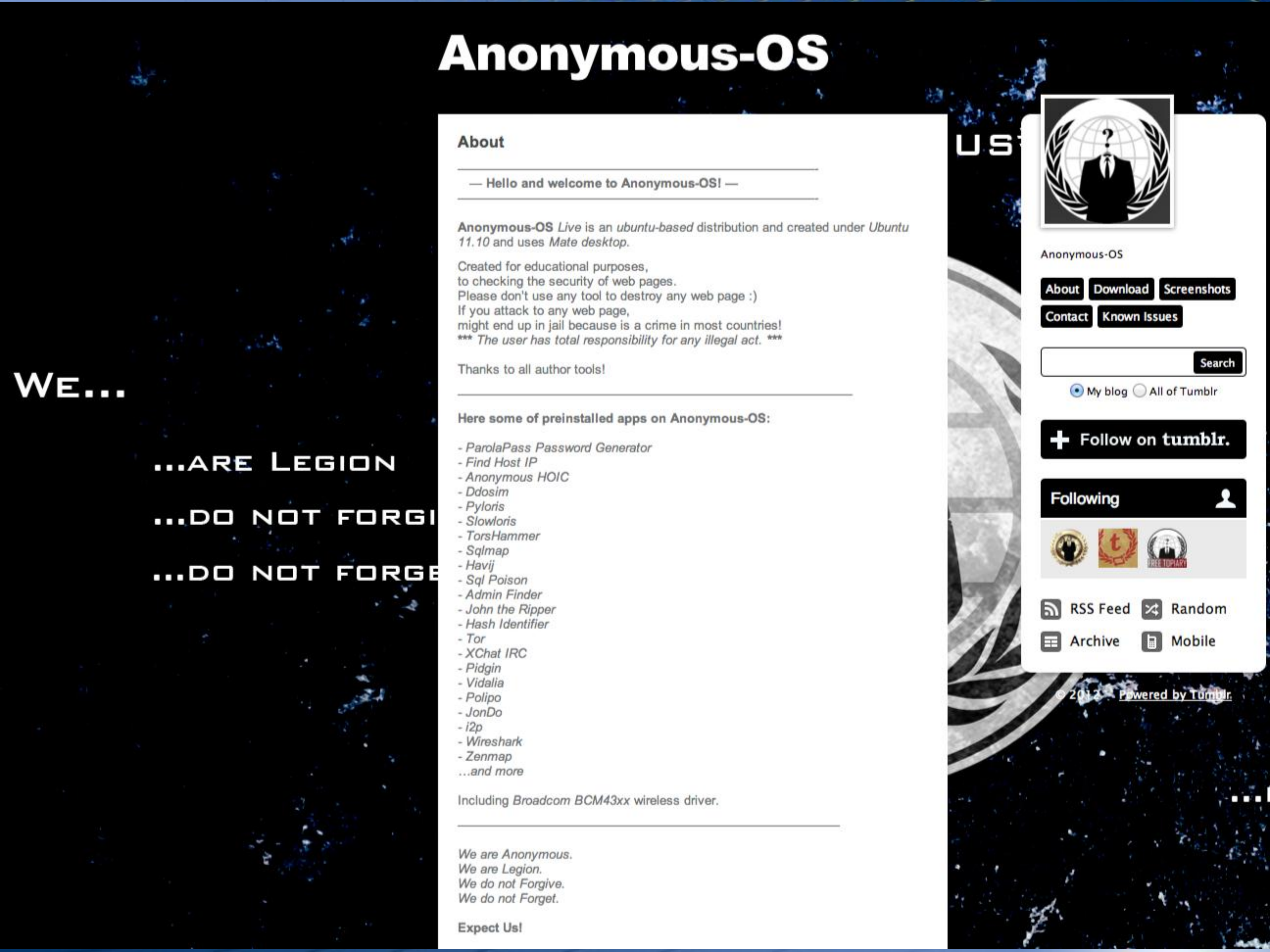
Spanish National Police *Anonymous hacks website in response to arrests of alleged group members*

13 Jun **Bethesda Game Studio**

U.S. Senate *(www.senate.gov)* *Lulzsec hacked and released internal data from its servers*

15 Jun **Malaysian government websites** *Hacked after an attack warning from Anonymous in response for censoring Wikileaks*

Central Intelligence Agency *Lulzsec hacked the CIA's public website, www.cia.gov, making it temporarily inaccessible*



About

— Hello and welcome to Anonymous-OS! —

Anonymous-OS *Live* is an *ubuntu-based* distribution and created under *Ubuntu 11.10* and uses *Mate desktop*.

Created for educational purposes,
to checking the security of web pages.
Please don't use any tool to destroy any web page :)
If you attack to any web page,
might end up in jail because is a crime in most countries!
**** The user has total responsibility for any illegal act. ****

Thanks to all author tools!

Here some of preinstalled apps on Anonymous-OS:

- *ParolaPass Password Generator*
- *Find Host IP*
- *Anonymous HOIC*
- *Ddosim*
- *Pyloris*
- *Slowloris*
- *TorsHammer*
- *Sqlmap*
- *Havij*
- *Sql Poison*
- *Admin Finder*
- *John the Ripper*
- *Hash Identifier*
- *Tor*
- *XChat IRC*
- *Pidgin*
- *Vidalia*
- *Polipo*
- *JonDo*
- *i2p*
- *Wireshark*
- *Zenmap*

...and more

Including *Broadcom BCM43xx* wireless driver.

We are Anonymous.
We are Legion.
We do not Forgive.
We do not Forget.

Expect Us!

Bad Things Will Happen

- HBGary vs. Anonymous: Story by *Ars Technica*

http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars

- HBGary Federal sought to "out" WikiLeaks and associated Anonymous hacker organization
- Anonymous finds out and launches full frontal assault on HBGary
- HBGary website defaced, emails stolen, backups deleted, twitter and LinkedIn accounts hacked, etc.
- Massive damage to HBGary's reputation
- Cleanup could take weeks or months

Business Challenges

- High availability and performance of the Network and its Apps
- Constantly evolving networks create gaps in monitoring
    - 10G, 40G, 100G Interfaces
    - MPLS & Multipoint VPN
- Lack of Internal security
    - Gaps left by traditional security technologies
    - High-speed, highly segmented networks
    - IT Consumerization
- Rapidly evolving threats - How do we stay out of the news?
    - Advanced Persistent Threat
    - Denial of Service
    - Data Exfiltration
- Compliance – SOX, PCI, HIPPA, etc
    - Lack of visibility into behaviors across the network
    - User accountability for employees, partners, consultants, customers

Lancope

Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

How is NetFlow Used? What Can We Do With It?

NetFlow = Visibility

NETWORKING

- Operational troubleshooting
- Capacity planning and optimization
- QoS Monitoring
- Application performance
- Organizational billing

SECURITY

- Remote and data center security
- Internal IDS/IPS
- Network forensics
- Data extrusion detection
- Firewall planning/auditing

COMPLIANCE

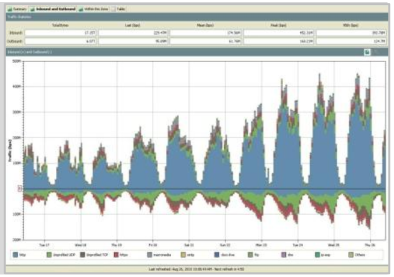
- PCI
- HIPAA, GLB, SOX
- SCADA
- FISMA NIST

How Flows are Used

1

Traffic Analysis and Network Visibility

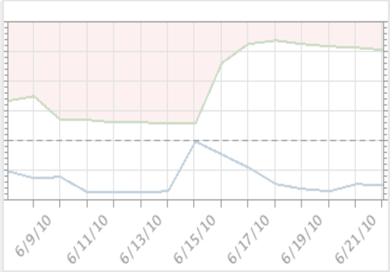
- Bandwidth Trending
- QoS Monitoring
- Network troubleshooting
- Router Capacity



2

Detect Network Anomalies

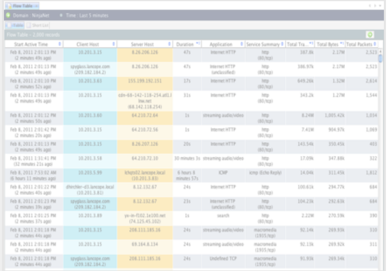
- Internal Monitoring
- Rapid Detection
- Firewall Validation
- DoS Detection



3

Forensics and Incident Response

- Reduce MTTK
- Records *All* Traffic
- Situational Awareness
- Compliments SIEM

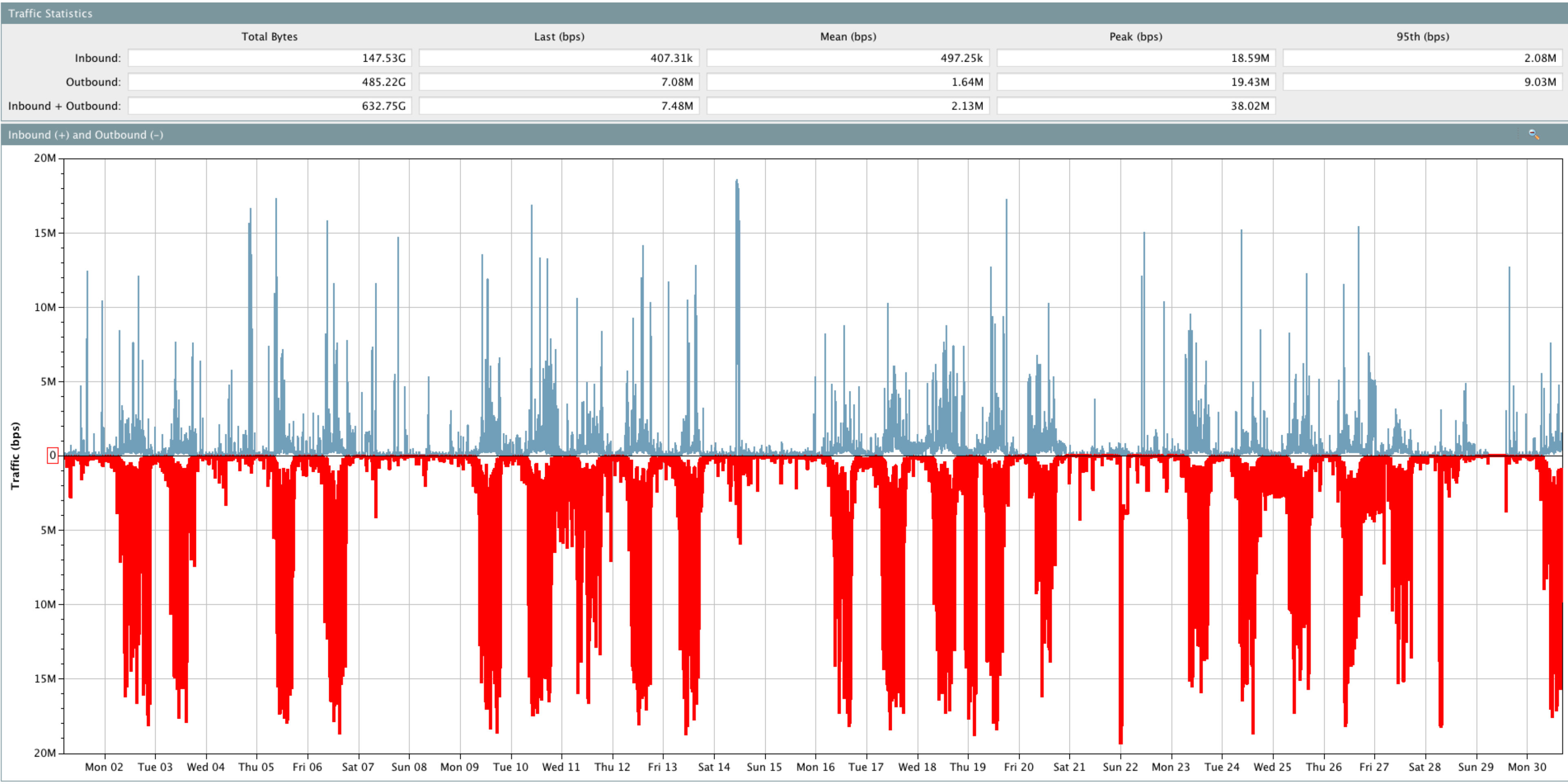


Domain : NinjaNet
Time : Last 5 minutes

Flow Table – 2,000 records

Start Active Time	Client Host	Server Host	Duration	Application	Service Summary	Total Tra...	Total Bytes	Total Packets
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.206.126	47s	Internet HTTP	http (80/tcp)	387.8k	2.17M	2,523
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	spyglass.lancope.com (209.182.184.2)	8.26.206.126	47s	Internet HTTP (unclassified)	http (80/tcp)	386.97k	2.17M	2,523
Feb 8, 2011 2:01:10 PM (2 minutes 52s ago)	10.201.3.63	155.199.192.151	17s	Internet HTTP	http (80/tcp)	649.26k	1.32M	2,614
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	cdn-68-142-118-254.atl1.llnw.net (68.142.118.254)	31s	Internet HTTP	http (80/tcp)	343.2k	1.27M	1,544
Feb 8, 2011 2:01:12 PM (2 minutes 50s ago)	10.201.3.60	64.210.72.64	1s	streaming audio/video	http (80/tcp)	8.24M	1,005.42k	1,034
Feb 8, 2011 2:01:42 PM (2 minutes 20s ago)	10.201.3.15	64.210.72.56	1s	Internet HTTP	http (80/tcp)	7.41M	904.97k	1,069
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.207.126	20s	Internet HTTP	http (80/tcp)	143.54k	350.45k	403
Feb 8, 2011 1:31:41 PM (32 minutes 21s ago)	10.201.3.58	64.210.72.10	30 minutes 3s	streaming audio/video	http (80/tcp)	17.09k	347.88k	322
Feb 8, 2011 7:53:02 AM (6 hours 11 minutes ago)	10.203.5.99	lchqts02.lancope.local (10.201.3.83)	6 hours 8 minutes 57s	ICMP	icmp (Echo Reply)	14.04k	311.45k	1,812
Feb 8, 2011 2:01:22 PM (2 minutes 40s ago)	dhirchler-d1.lancope.local (10.201.3.81)	8.12.132.67	24s	Internet HTTP	http (80/tcp)	100.61k	294.77k	684
Feb 8, 2011 2:01:23 PM (2 minutes 39s ago)	spyglass.lancope.com (209.182.184.2)	8.12.132.67	23s	Internet HTTP (unclassified)	http (80/tcp)	104.23k	292.63k	684
Feb 8, 2011 2:01:25 PM (2 minutes 37s ago)	10.201.3.89	yx-in-f102.1e100.net (74.125.45.102)	1s	search	http (80/tcp)	2.22M	270.59k	390
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	208.111.185.16	24s	streaming audio/video	macromedia (1935/tcp)	92.14k	269.93k	310
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	69.164.8.134	24s	streaming audio/video	macromedia (1935/tcp)	92.13k	269.92k	311
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	spyglass.lancope.com (209.182.184.2)	208.111.185.16	24s	Undefined TCP	macromedia (1935/tcp)	91.93k	269.34k	310

SNMP Monitoring

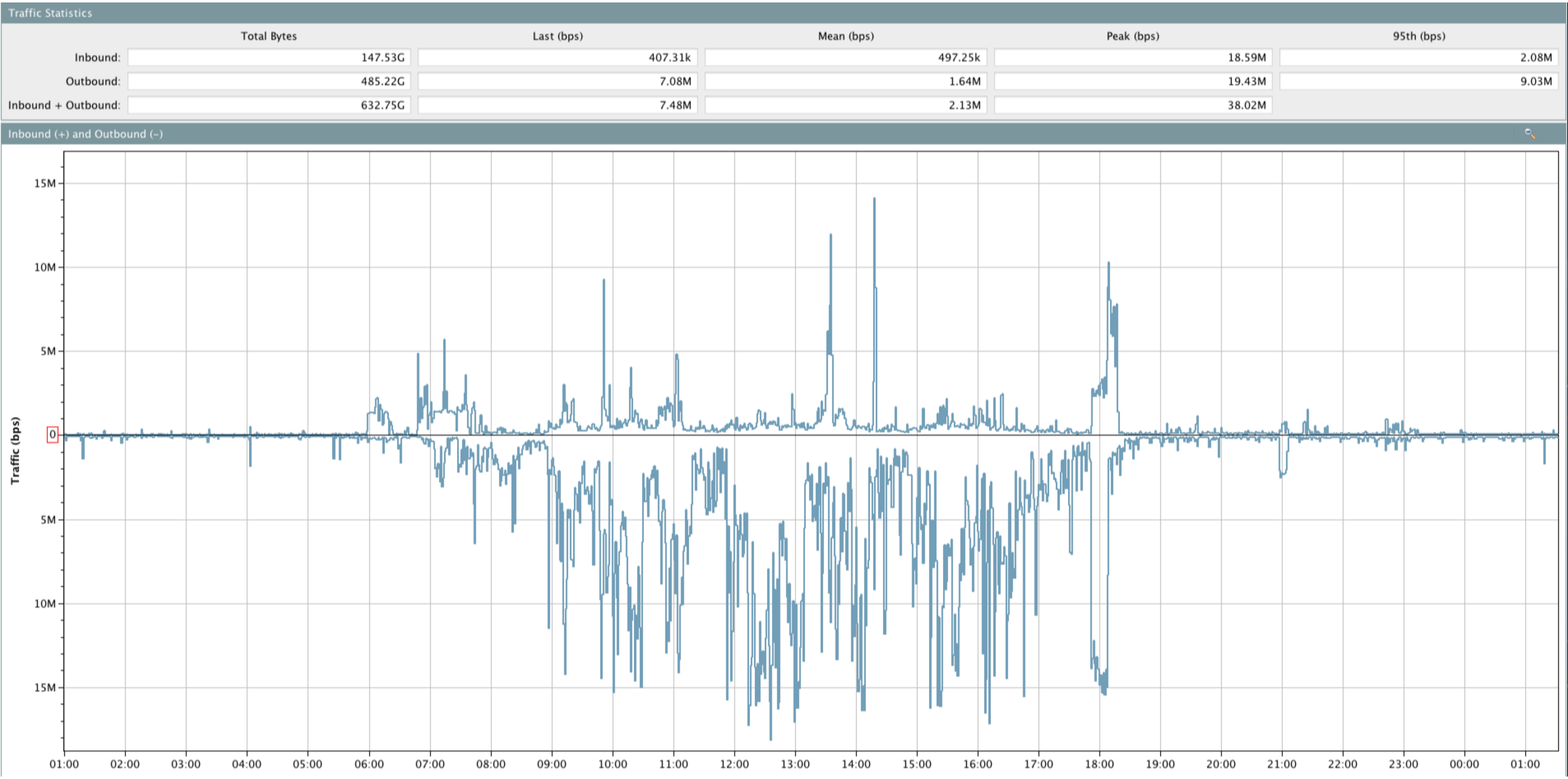


Traffic Statistics

	Total Bytes	Last (bps)	Mean (bps)	Peak (bps)	95th (bps)
Inbound:	147.53G	407.31k	497.25k	18.59M	2.08M
Outbound:	485.22G	7.08M	1.64M	19.43M	9.03M
Inbound + Outbound:	632.75G	7.48M	2.13M	38.02M	

Inbound (+) and Outbound (-)

SNMP Monitoring Cont.

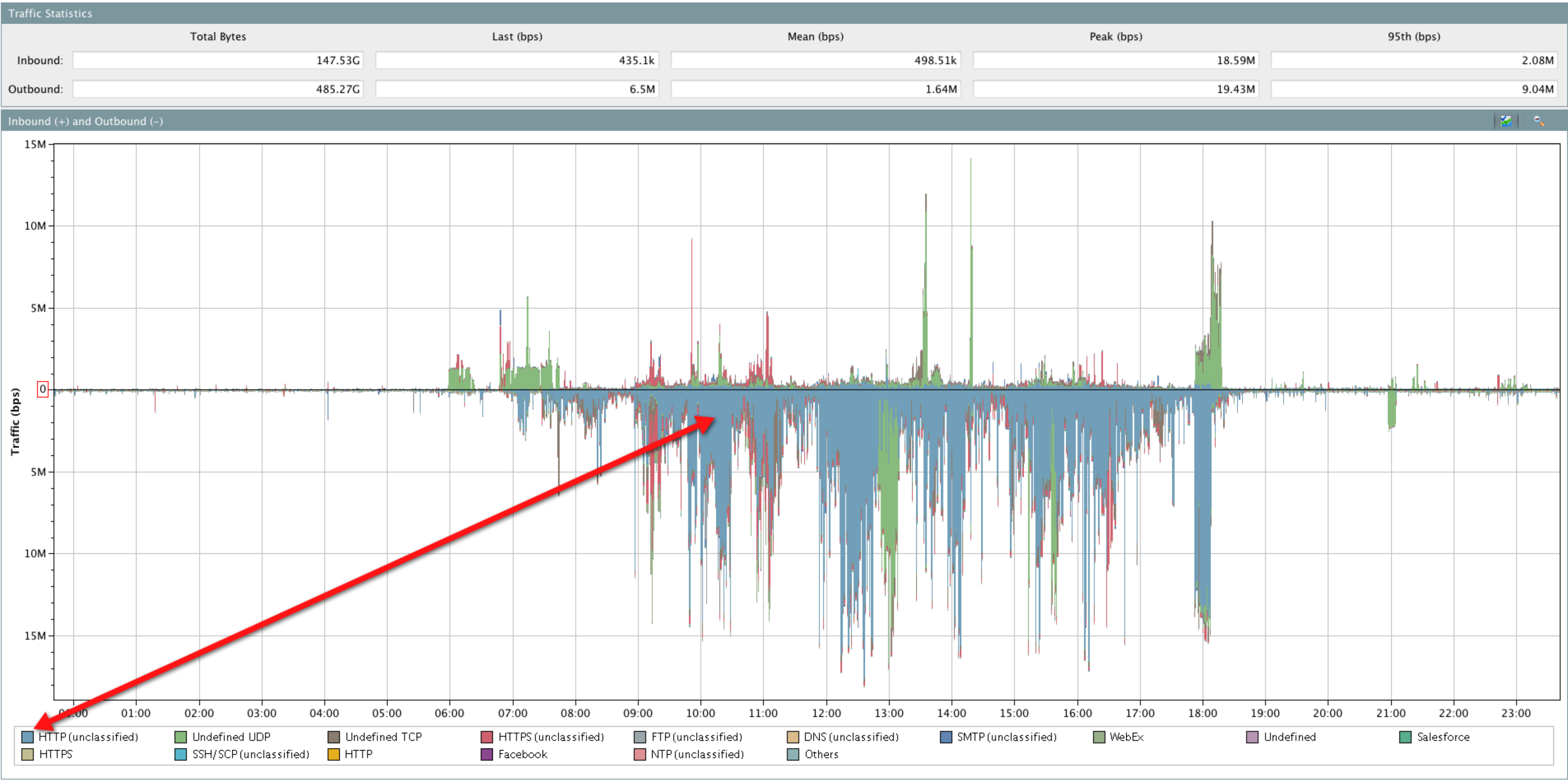


Traffic Statistics

	Total Bytes	Last (bps)	Mean (bps)	Peak (bps)	95th (bps)
Inbound:	147.53G	407.31k	497.25k	18.59M	2.08M
Outbound:	485.22G	7.08M	1.64M	19.43M	9.03M
Inbound + Outbound:	632.75G	7.48M	2.13M	38.02M	

Inbound (+) and Outbound (-)

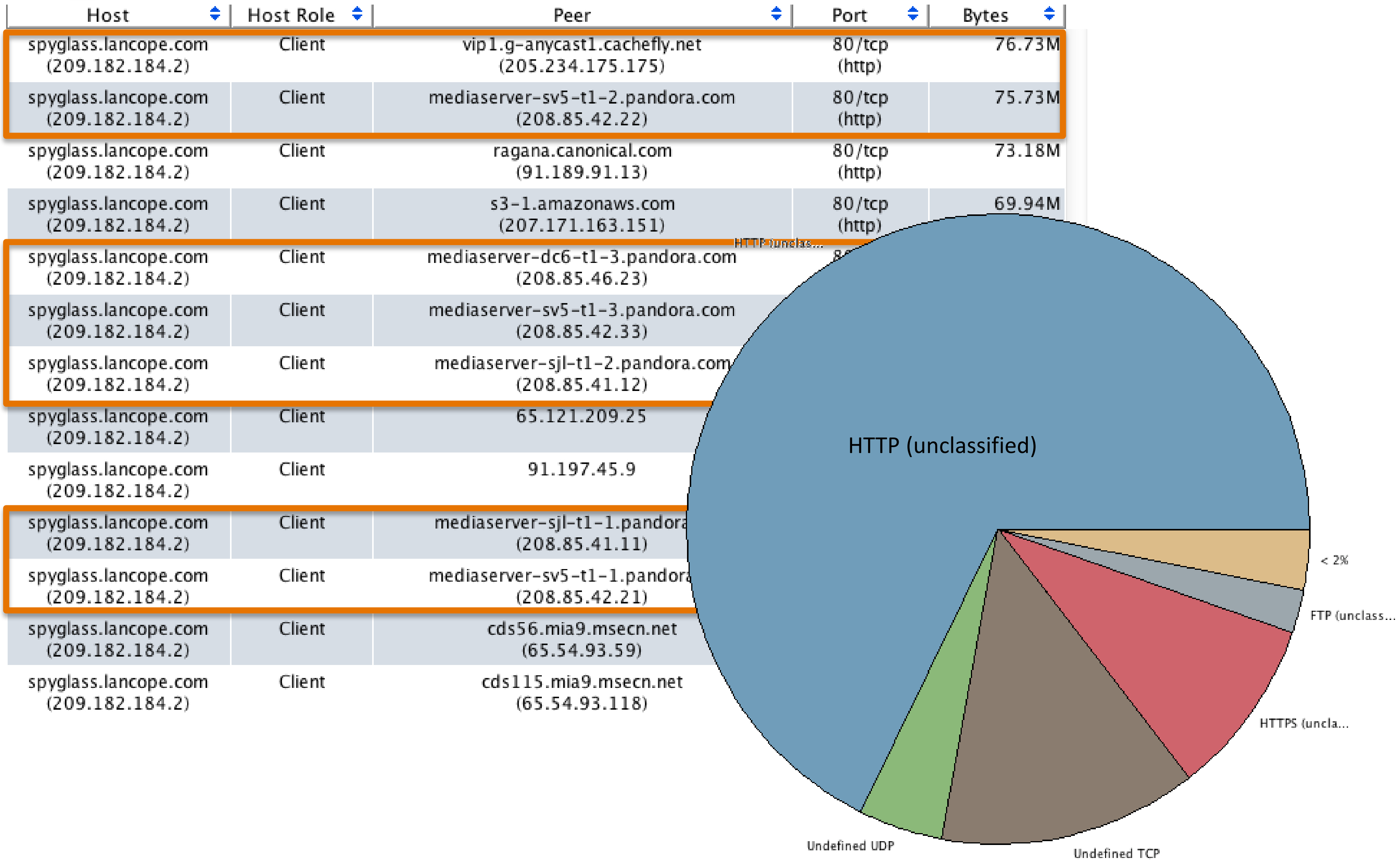
Traffic Visibility with NetFlow and NBAR



Traffic Statistics

	Total Bytes	Last (bps)	Mean (bps)	Peak (bps)	95th (bps)
Inbound:	147.53G	435.1k	498.51k	18.59M	2.08M
Outbound:	485.27G	6.5M	1.64M	19.43M	9.04M

Traffic Visibility with NetFlow and NBAR Cont.



Host	Host Role	Peer	Port	Bytes
spyglass.lancope.com (209.182.184.2)	Client	vip1.g-anycast1.cachefly.net (205.234.175.175)	80/tcp (http)	76.73M
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-sv5-t1-2.pandora.com (208.85.42.22)	80/tcp (http)	75.73M
spyglass.lancope.com (209.182.184.2)	Client	ragana.canonical.com (91.189.91.13)	80/tcp (http)	73.18M
spyglass.lancope.com (209.182.184.2)	Client	s3-1.amazonaws.com (207.171.163.151)	80/tcp (http)	69.94M
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-dc6-t1-3.pandora.com (208.85.46.23)	8	
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-sv5-t1-3.pandora.com (208.85.42.33)		
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-sjl-t1-2.pandora.com (208.85.41.12)		
spyglass.lancope.com (209.182.184.2)	Client	65.121.209.25		
spyglass.lancope.com (209.182.184.2)	Client	91.197.45.9		
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-sjl-t1-1.pandora (208.85.41.11)		
spyglass.lancope.com (209.182.184.2)	Client	mediaserver-sv5-t1-1.pandora (208.85.42.21)		
spyglass.lancope.com (209.182.184.2)	Client	cds56.mia9.msecn.net (65.54.93.59)		
spyglass.lancope.com (209.182.184.2)	Client	cds115.mia9.msecn.net (65.54.93.118)		

How Flows are Used

1

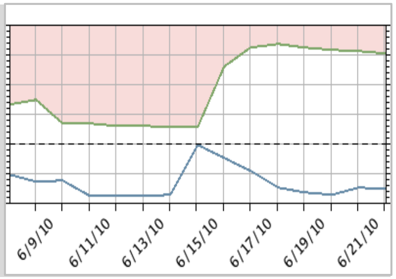
Traffic Analysis and Network Visibility

- Bandwidth Trending
- QoS Monitoring
- Network troubleshooting
- Router Capacity

2

Detect Network Anomalies

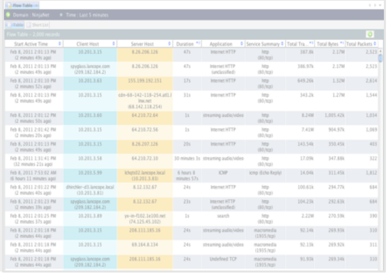
- Internal Monitoring
- Rapid Detection
- Firewall Validation
- DoS Detection



3

Forensics and Incident Response

- Reduce MTTK
- Records *All* Traffic
- Situational Awareness
- Compliments SIEM



Flow Table

Domain : NinjaNet   Time : Last 5 minutes

Table   Short List

Flow Table - 2,000 records

Start Active Time	Client Host	Server Host	Duration	Application	Service Summary	Total Tra...	Total Bytes	Total Packets
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.206.126	47s	Internet HTTP	http (80/tcp)	387.8k	2.17M	2,523
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	spyglass.lancope.com (209.182.184.2)	8.26.206.126	47s	Internet HTTP (unclassified)	http (80/tcp)	386.97k	2.17M	2,523
Feb 8, 2011 2:01:10 PM (2 minutes 52s ago)	10.201.3.63	155.199.192.151	17s	Internet HTTP	http (80/tcp)	649.26k	1.32M	2,614
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	cdn-68-142-118-254.atl1.lnw.net (68.142.118.254)	31s	Internet HTTP	http (80/tcp)	343.2k	1.27M	1,544
Feb 8, 2011 2:01:12 PM (2 minutes 50s ago)	10.201.3.60	64.210.72.64	1s	streaming audio/video	http (80/tcp)	8.24M	1,005.42k	1,034
Feb 8, 2011 2:01:42 PM (2 minutes 20s ago)	10.201.3.15	64.210.72.56	1s	Internet HTTP	http (80/tcp)	7.41M	904.97k	1,069
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.207.126	20s	Internet HTTP	http (80/tcp)	143.54k	350.45k	403
Feb 8, 2011 1:31:41 PM (32 minutes 21s ago)	10.201.3.58	64.210.72.10	30 minutes 3s	streaming audio/video	http (80/tcp)	17.09k	347.88k	322
Feb 8, 2011 7:53:02 AM (6 hours 11 minutes ago)	10.203.5.99	lchqts02.lancope.local (10.201.3.83)	6 hours 8 minutes 57s	ICMP	icmp (Echo Reply)	14.04k	311.45k	1,812
Feb 8, 2011 2:01:22 PM (2 minutes 40s ago)	dhirchler-d3.lancope.local (10.201.3.81)	8.12.132.67	24s	Internet HTTP	http (80/tcp)	100.61k	294.77k	684
Feb 8, 2011 2:01:23 PM (2 minutes 39s ago)	spyglass.lancope.com (209.182.184.2)	8.12.132.67	23s	Internet HTTP (unclassified)	http (80/tcp)	104.23k	292.63k	684
Feb 8, 2011 2:01:25 PM (2 minutes 37s ago)	10.201.3.89	yx-in-f102.1e100.net (74.125.45.102)	1s	search	http (80/tcp)	2.22M	270.59k	390
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	208.111.185.16	24s	streaming audio/video	macromedia (1935/tcp)	92.14k	269.93k	310
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	69.164.8.134	24s	streaming audio/video	macromedia (1935/tcp)	92.13k	269.92k	311
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	spyglass.lancope.com (209.182.184.2)	208.111.185.16	24s	Undefined TCP	macromedia (1935/tcp)	91.93k	269.34k	310

NetFlow security use cases

- **Detecting Sophisticated and Persistent Threats.** Malware that makes it past perimeter security can remain in the enterprise waiting to strike as lurking threats. These may be zero day threats that do not yet have an antivirus signature or be hard to detect for other reasons.

- **Uncovering Network Reconnaissance.** Some attacks will probe the network looking for attack vectors to be utilized by custom-crafted cyber threats.

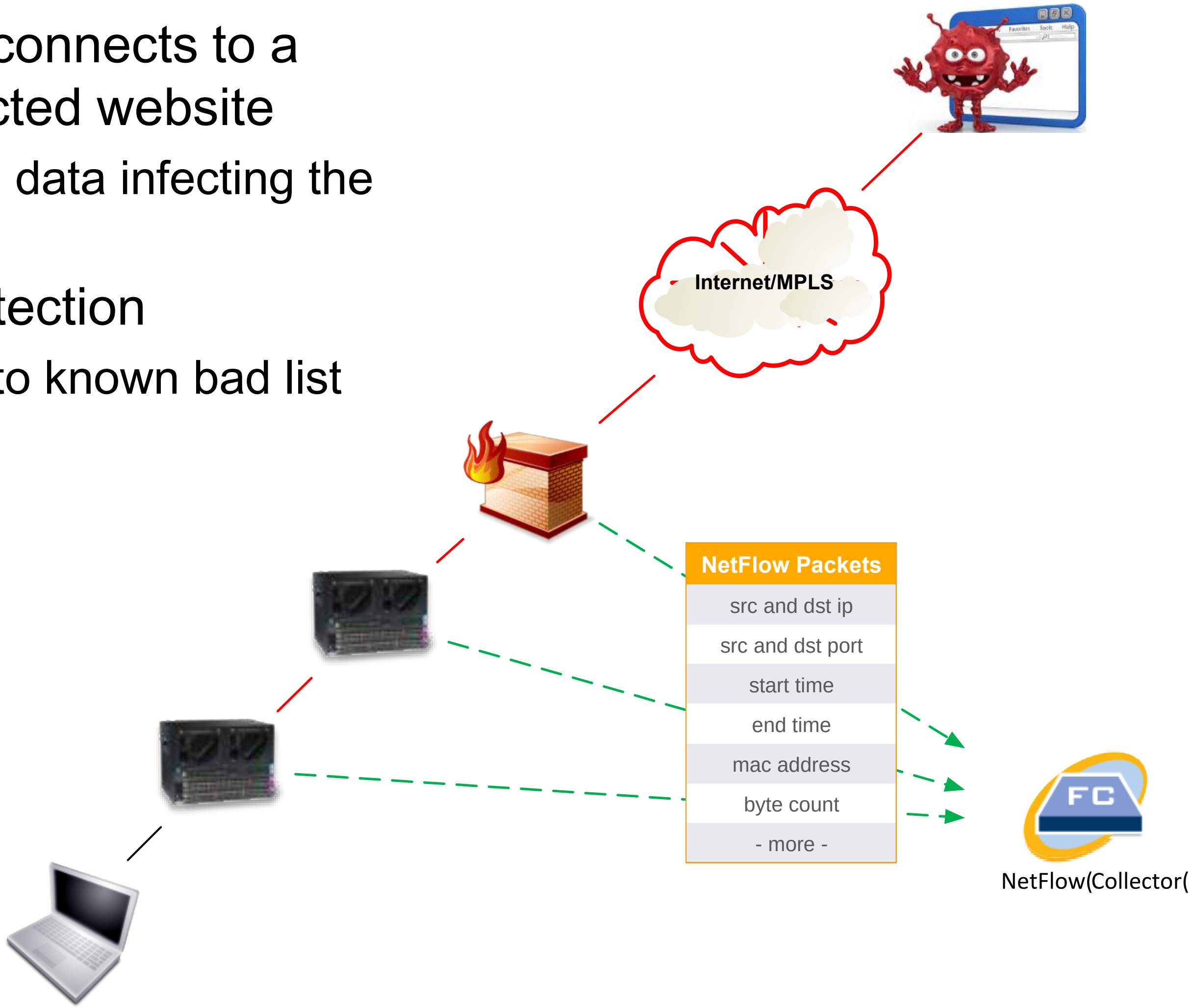
- **Finding Internally Spread Malware.** Network interior malware proliferation can occur across hosts for the purpose gathering security reconnaissance data, data exfiltration or network backdoors.

- **Identifying BotNet Command & Control Activity.** BotNets are implanted in the enterprise to execute commands from their Bot herders to send SPAM, Denial of Service attacks, or other malicious acts.

- **Revealing Data Loss.** Code can be hidden in the enterprise to export of sensitive information back to the attacker. This Data Leakage may occur rapidly or over time.

Host Becomes Infected

- Internal host connects to a malware infected website
  - Downloads data infecting the system
- Method of detection
  - Host Lock to known bad list



Internet/MPLS

NetFlow Packets

src and dst ip

src and dst port

start time

end time

mac address

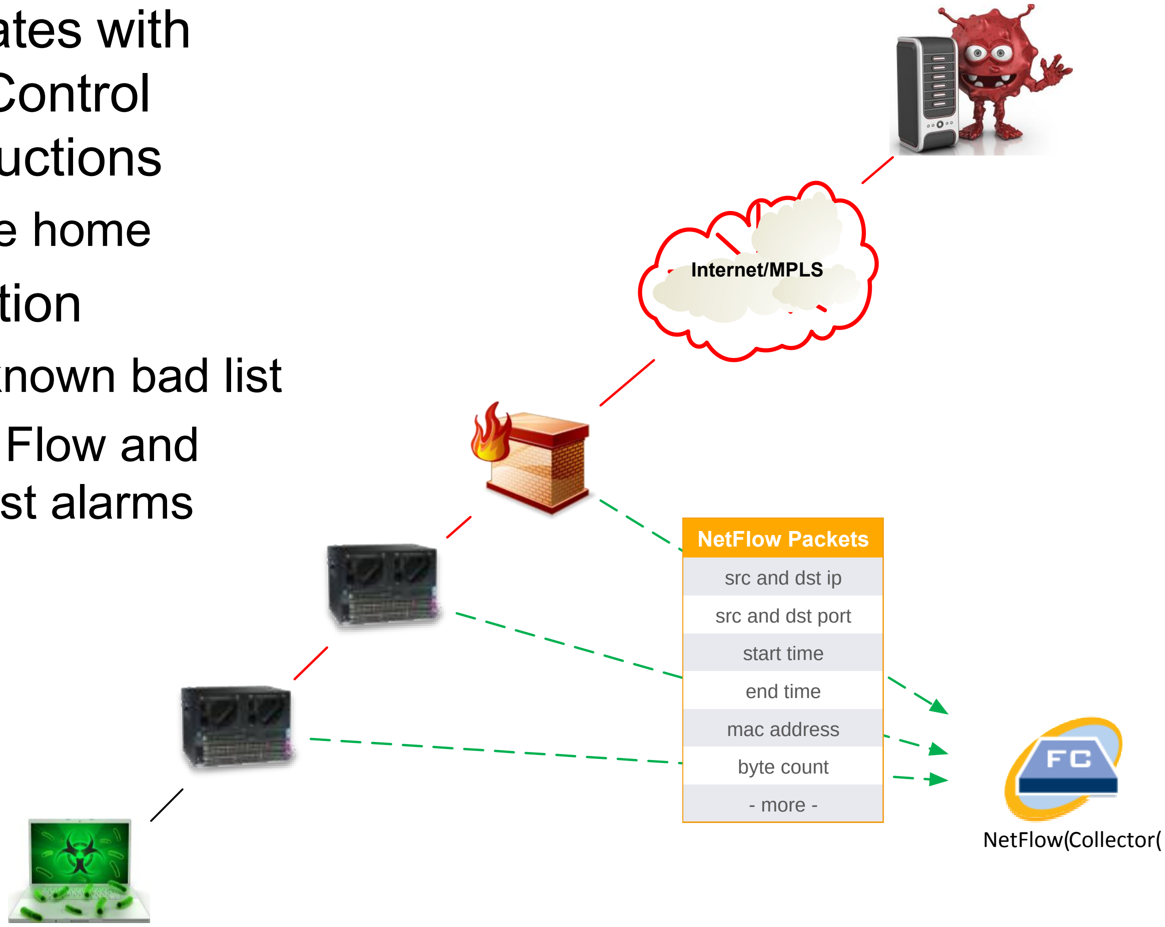
byte count

- more -

NetFlow(Collector(

Communication to CNC

- Host communicates with Command and Control network for instructions
  - Periodic phone home
- Method of detection
  - Host Lock to known bad list
  - Suspect Long Flow and Beaconing Host alarms



NetFlow Packets

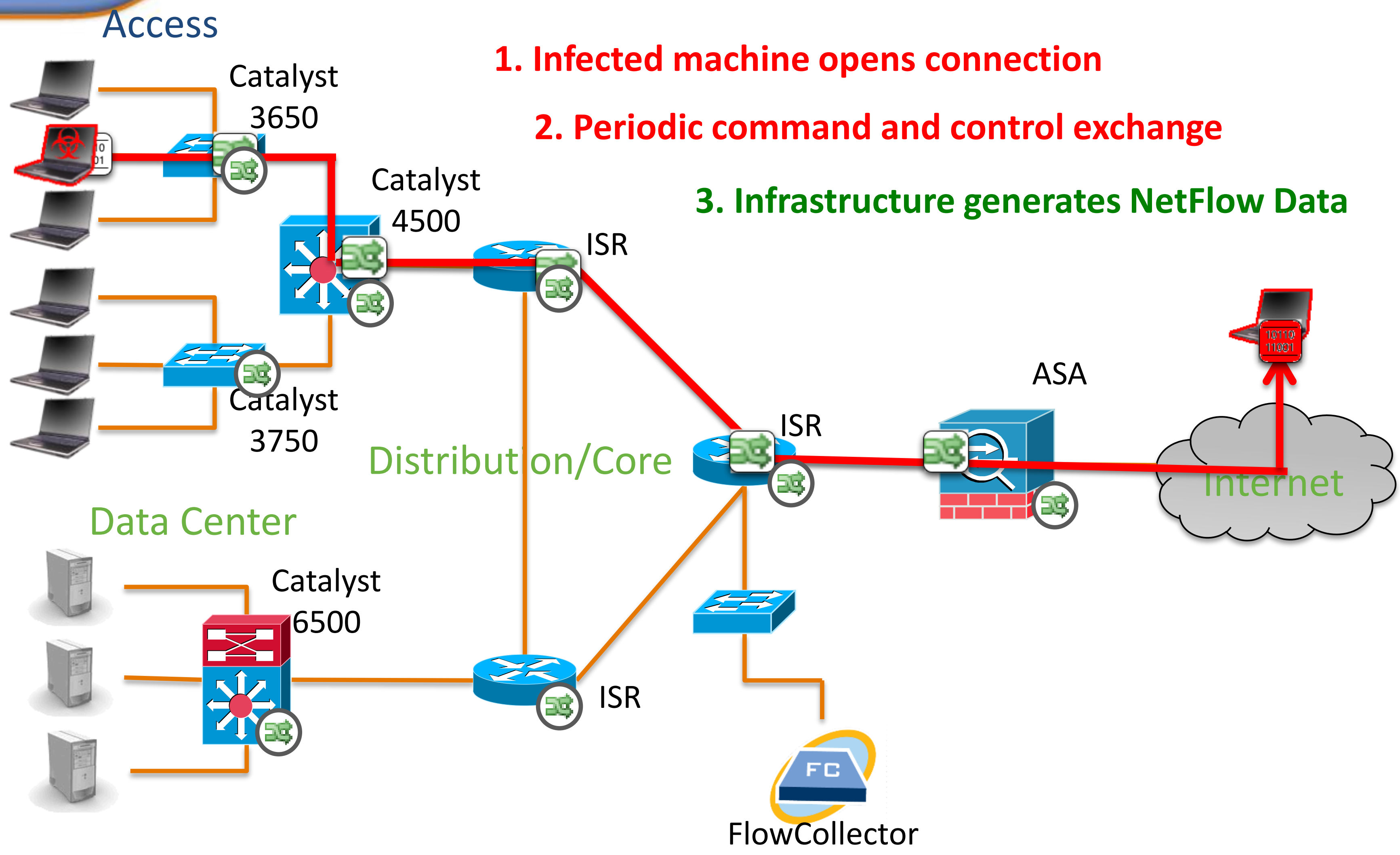
- src and dst ip
- src and dst port
- start time
- end time
- mac address
- byte count
- - more -

Detecting Command and Control

1. Infected machine opens connection

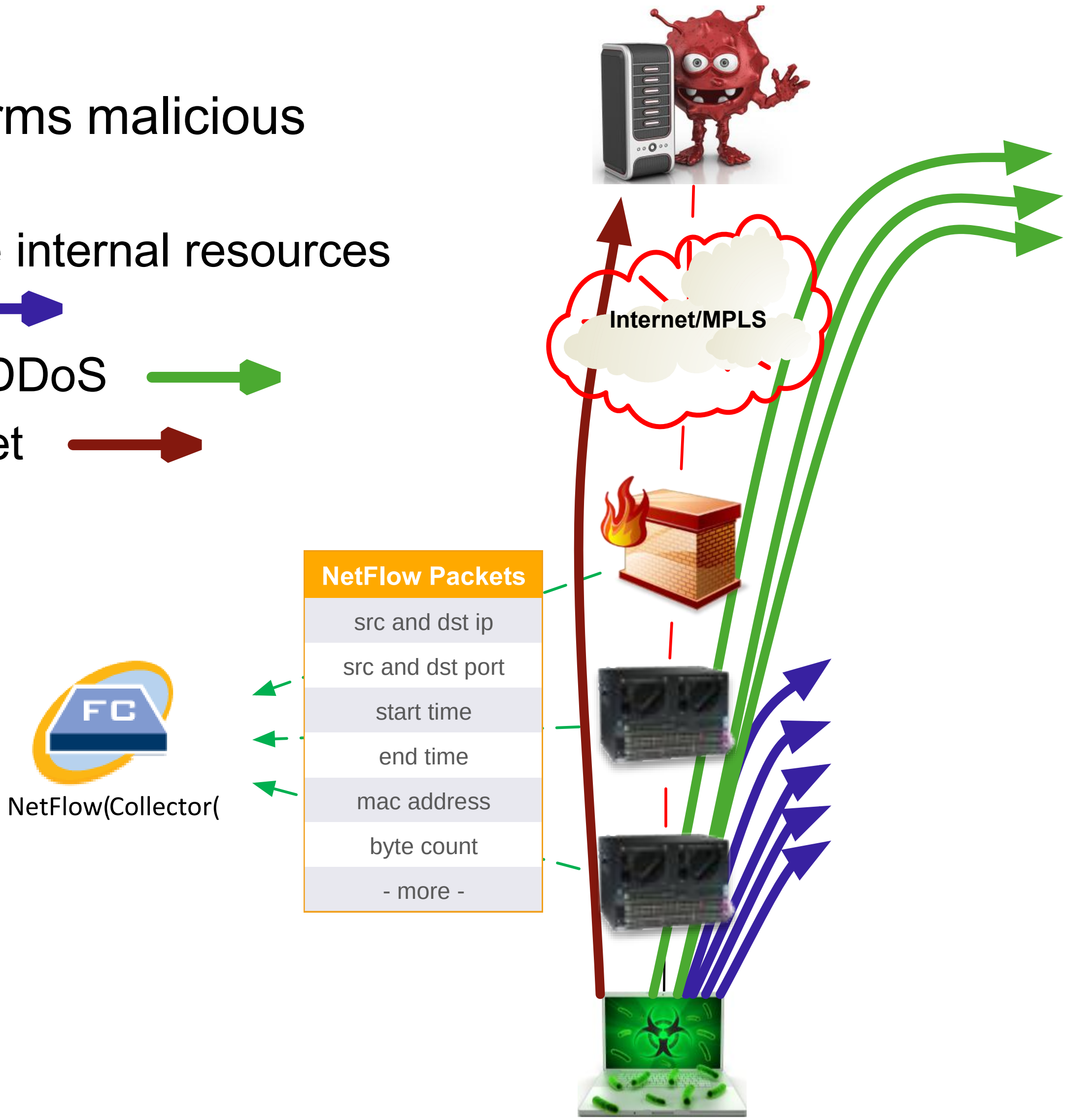
2. Periodic command and control exchange

3. Infrastructure generates NetFlow Data



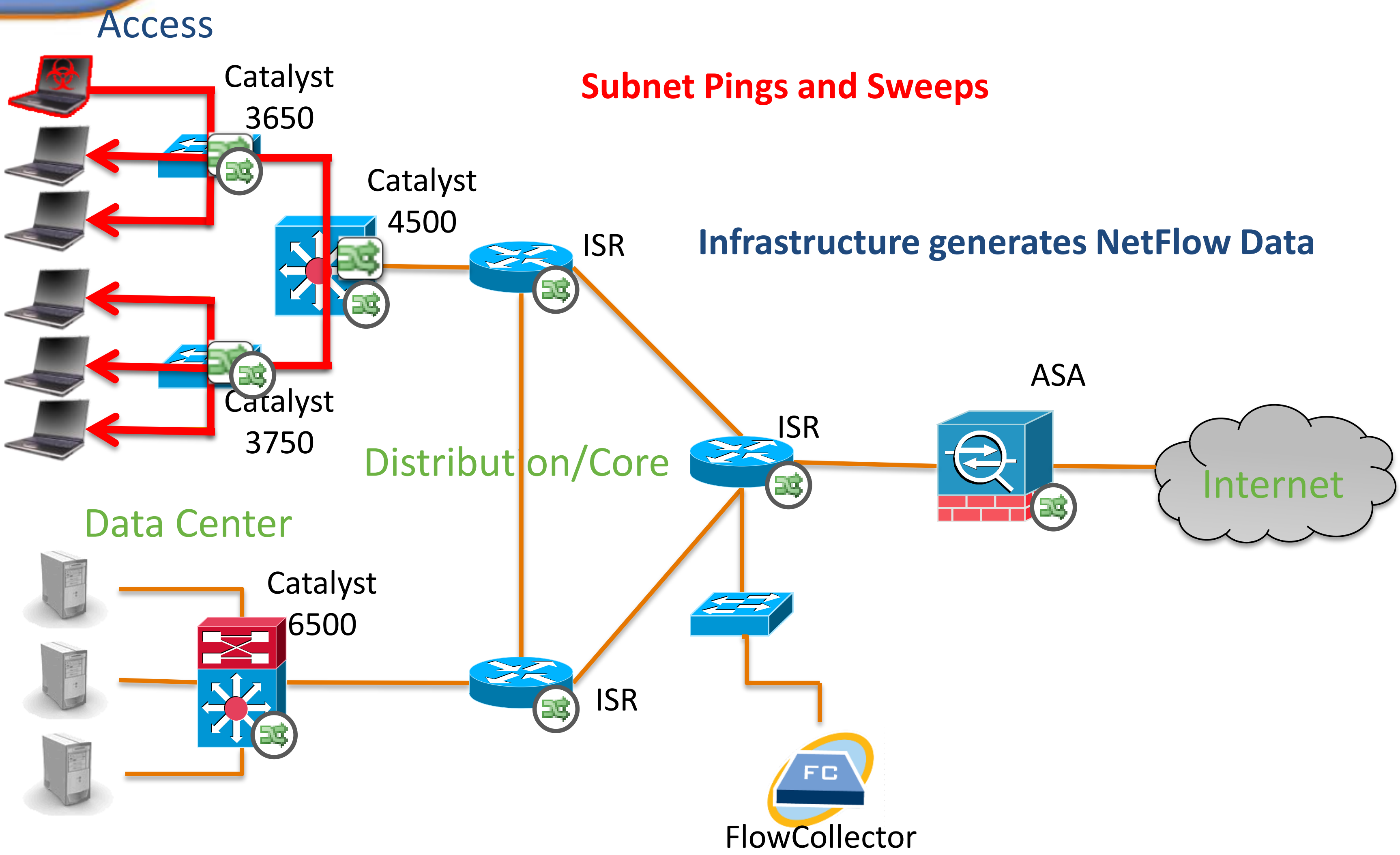
Network activities

- Compromised host performs malicious activities
  - Attempts to compromise internal resources (probing) →
  - Becomes a member of DDoS →
  - Data extrusion to Internet →
- Method of detection
  - Scanning detection (CI)
  - DoS Monitoring
  - Suspect Data Loss



NetFlow Packets
src and dst ip
src and dst port
start time
end time
mac address
byte count
- more -

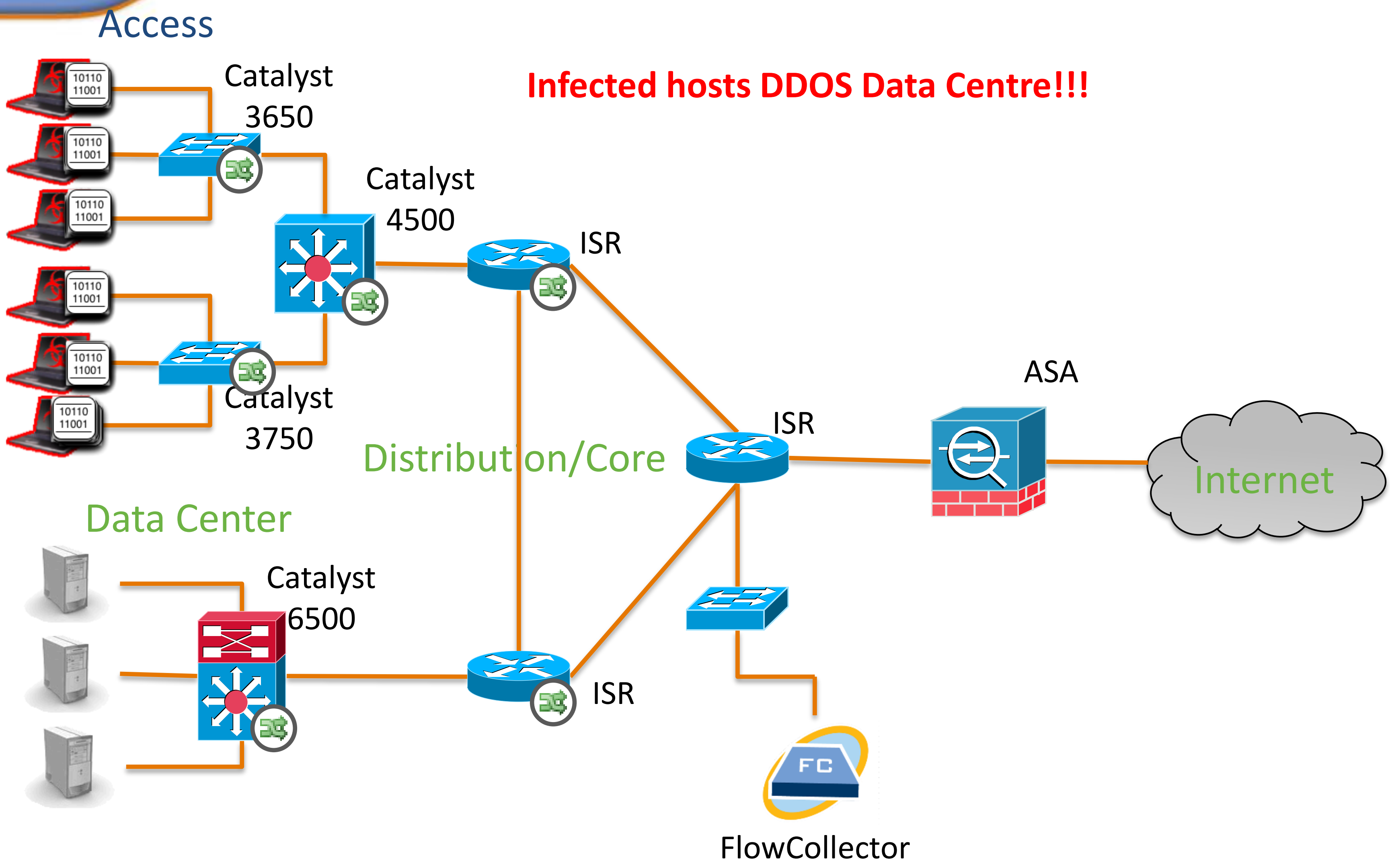
Detecting Network Reconnaissance



Subnet Pings and Sweeps

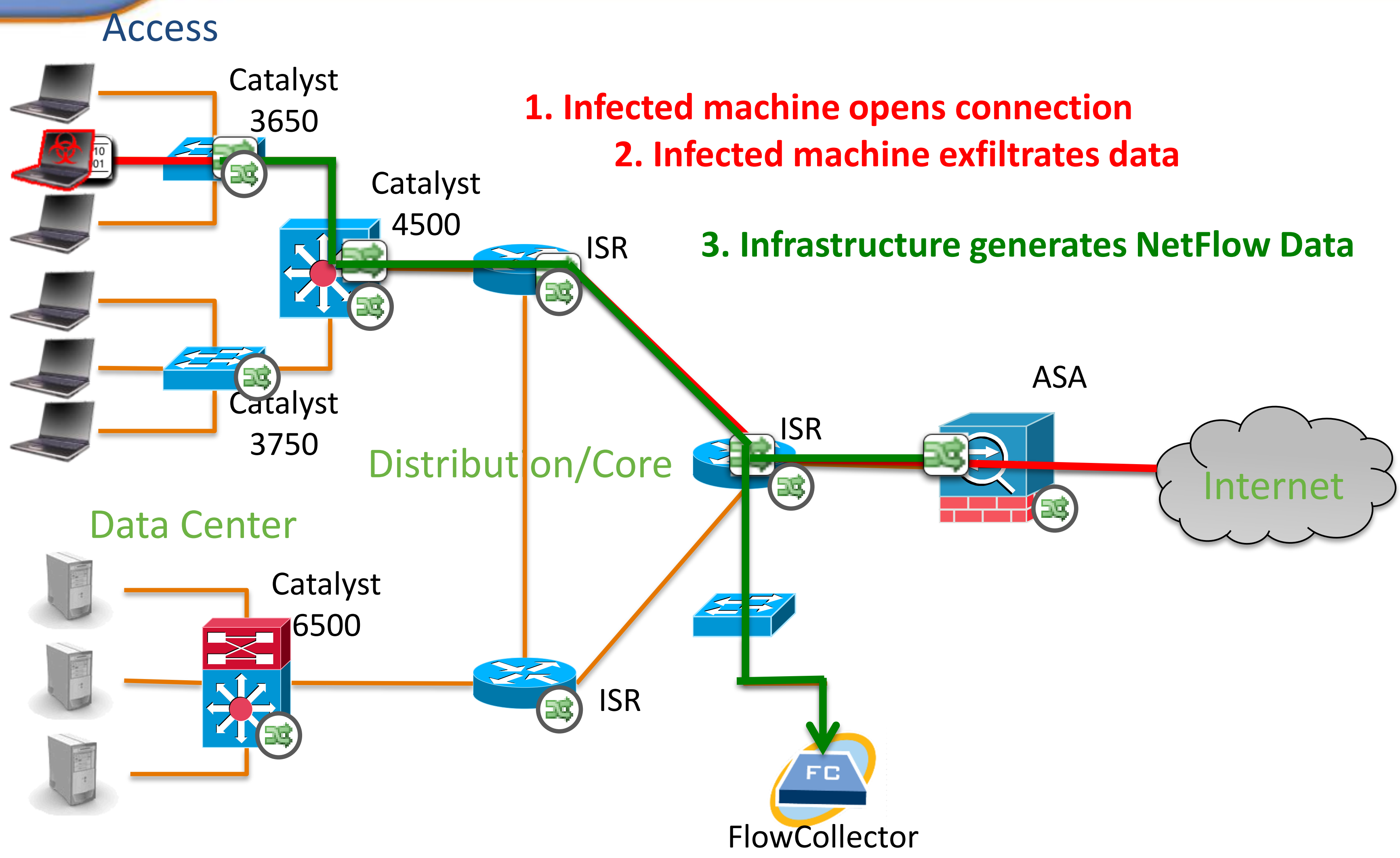
Infrastructure generates NetFlow Data

Distributed Denial of Service



Infected hosts DDOS Data Centre!!!

Detecting Data Exfiltration



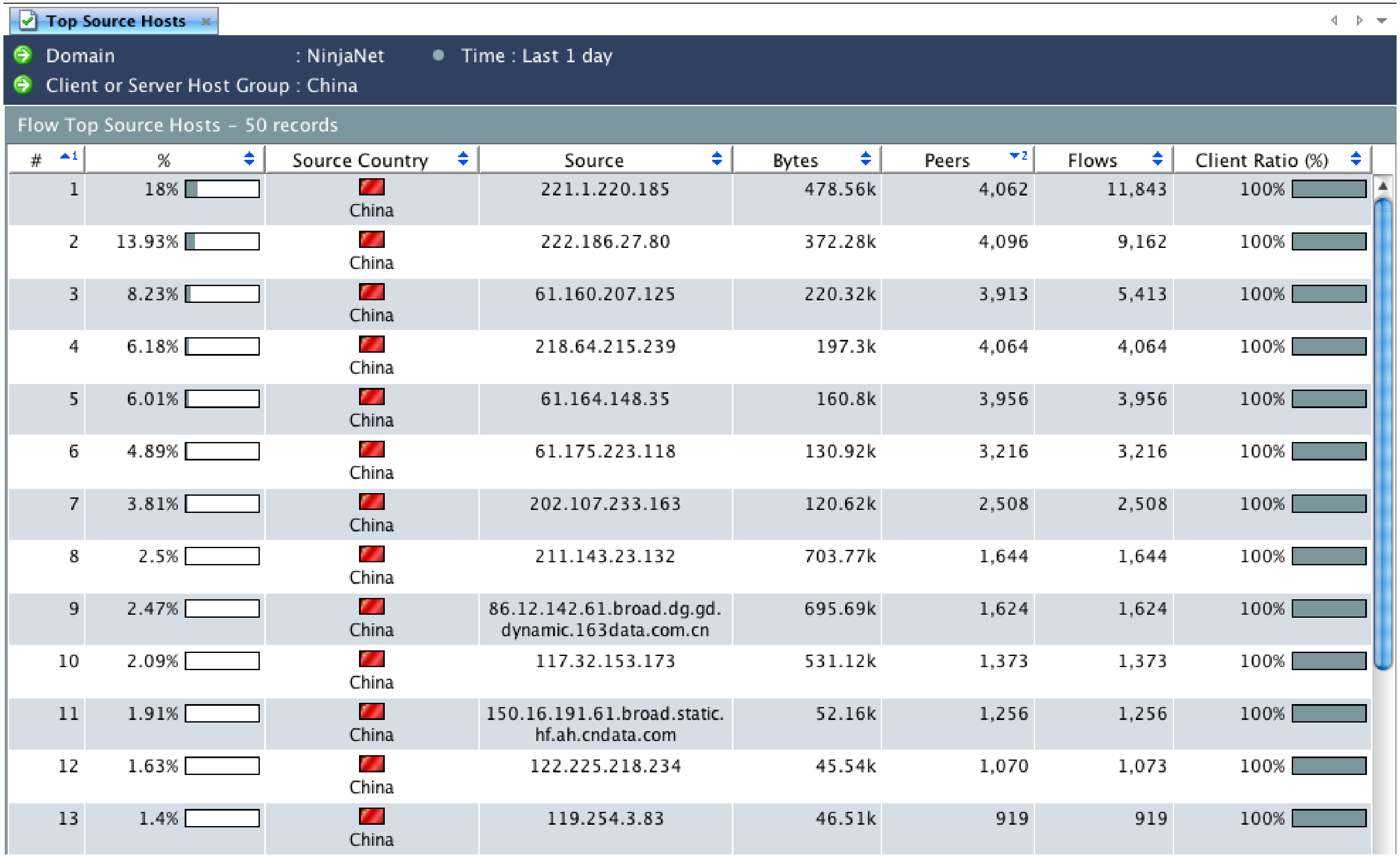
1. Infected machine opens connection

2. Infected machine exfiltrates data

3. Infrastructure generates NetFlow Data

Traffic Analysis and Network Visibility

- Advanced Top N reports showing any time period across any Host Group



Top Source Hosts

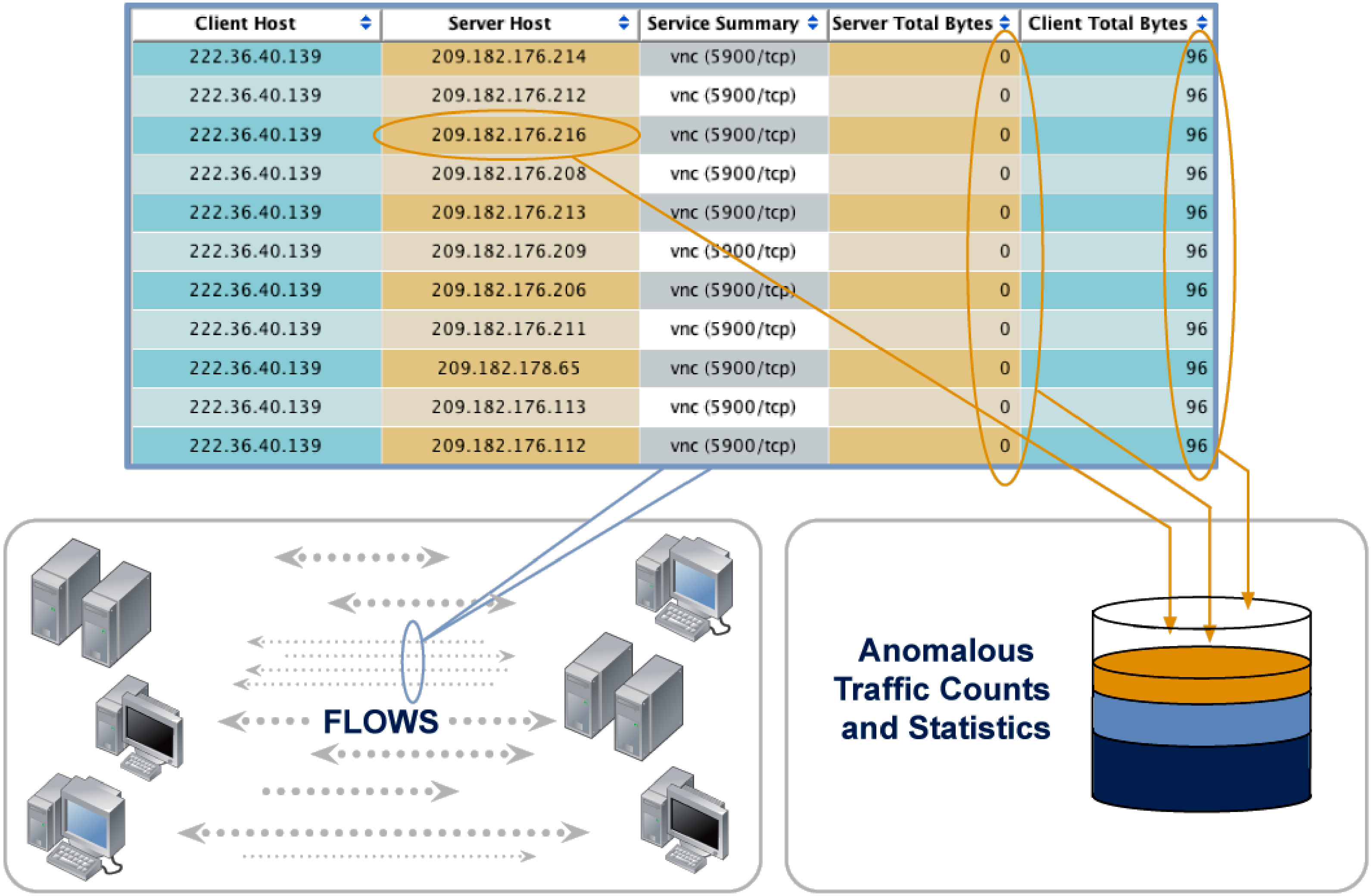
Domain : NinjaNet • Time : Last 1 day

Client or Server Host Group : China

Flow Top Source Hosts – 50 records

#	%	Source Country	Source	Bytes	Peers	Flows	Client Ratio (%)
1	18%	China	221.1.220.185	478.56k	4,062	11,843	100%
2	13.93%	China	222.186.27.80	372.28k	4,096	9,162	100%
3	8.23%	China	61.160.207.125	220.32k	3,913	5,413	100%
4	6.18%	China	218.64.215.239	197.3k	4,064	4,064	100%
5	6.01%	China	61.164.148.35	160.8k	3,956	3,956	100%
6	4.89%	China	61.175.223.118	130.92k	3,216	3,216	100%
7	3.81%	China	202.107.233.163	120.62k	2,508	2,508	100%
8	2.5%	China	211.143.23.132	703.77k	1,644	1,644	100%
9	2.47%	China	86.12.142.61.broad.dg.gd.dynamic.163data.com.cn	695.69k	1,624	1,624	100%
10	2.09%	China	117.32.153.173	531.12k	1,373	1,373	100%
11	1.91%	China	150.16.191.61.broad.static.hf.ah.cndata.com	52.16k	1,256	1,256	100%
12	1.63%	China	122.225.218.234	45.54k	1,070	1,073	100%
13	1.4%	China	119.254.3.83	46.51k	919	919	100%

Flow-based Anomaly Detection

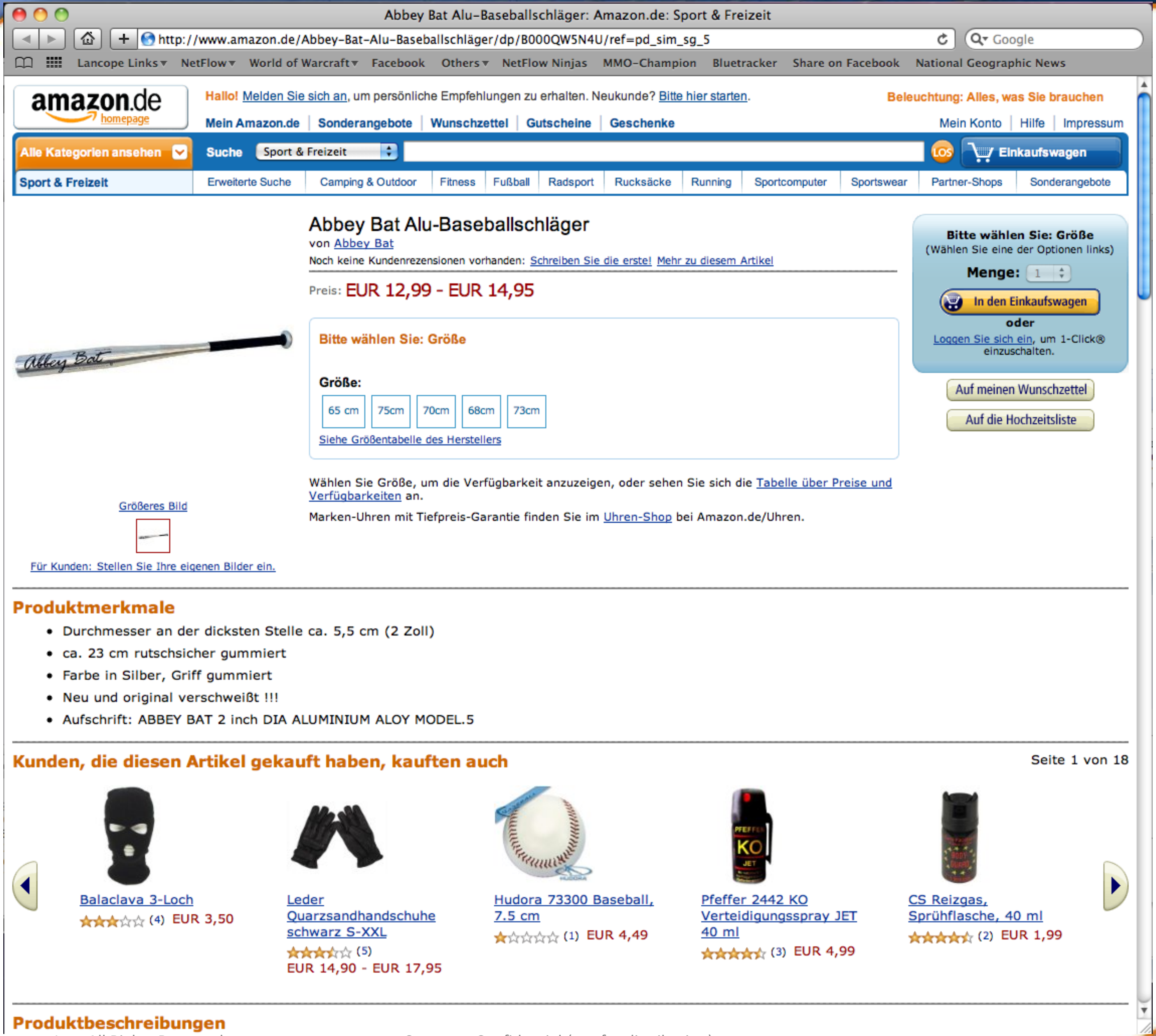


Client Host	Server Host	Service Summary	Server Total Bytes	Client Total Bytes
222.36.40.139	209.182.176.214	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.212	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.216	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.208	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.213	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.209	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.206	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.211	vnc (5900/tcp)	0	96
222.36.40.139	209.182.178.65	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.113	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.112	vnc (5900/tcp)	0	96

Anomalous Traffic Counts and Statistics

Lancope

Expert Systems For Analytics



Hallo! Melden Sie sich an, um persönliche Empfehlungen zu erhalten. Neukunde? Bitte hier starten.

Abbey Bat Alu-Baseballschläger

von Abbey Bat

Noch keine Kundenrezensionen vorhanden: Schreiben Sie die erste! Mehr zu diesem Artikel

Preis: EUR 12,99 - EUR 14,95

Bitte wählen Sie: Größe

Größe:

65 cm | 75cm | 70cm | 68cm | 73cm

Siehe Größentabelle des Herstellers

Bitte wählen Sie: Größe
(Wählen Sie eine der Optionen links)

Menge: 1

In den Einkaufswagen

oder

Loggen Sie sich ein, um 1-Click® einzuschalten.

Auf meinen Wunschzettel

Auf die Hochzeitsliste

Wählen Sie Größe, um die Verfügbarkeit anzuzeigen, oder sehen Sie sich die Tabelle über Preise und Verfügbarkeiten an.

Marken-Uhren mit Tiefpreis-Garantie finden Sie im Uhren-Shop bei Amazon.de/Uhren.

Größeres Bild

Für Kunden: Stellen Sie Ihre eigenen Bilder ein.

Produktmerkmale

- Durchmesser an der dicksten Stelle ca. 5,5 cm (2 Zoll)
- ca. 23 cm rutschsicher gummiert
- Farbe in Silber, Griff gummiert
- Neu und original verschweißt !!!
- Aufschrift: ABBEY BAT 2 inch DIA ALUMINIUM ALOY MODEL.5

Kunden, die diesen Artikel gekauft haben, kauften auch

Seite 1 von 18

Balaclava 3-Loch
★★★☆☆ (4) EUR 3,50

Leder Quarzsandhandschuhe schwarz S-XXL
★★★☆☆ (5)
EUR 14,90 - EUR 17,95

Hudora 73300 Baseball, 7.5 cm
★☆☆☆☆ (1) EUR 4,49

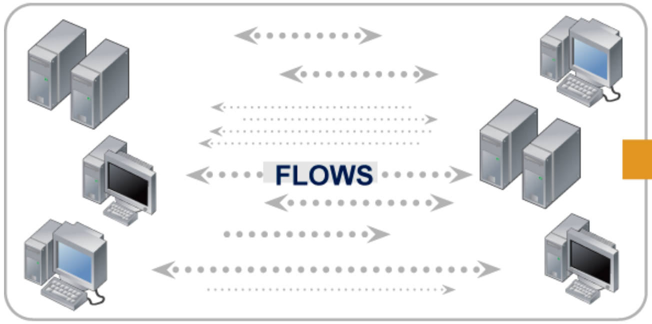
Pfeffer 2442 KO Verteidigungsspray JET 40 ml
★★★★★ (3) EUR 4,99

CS Reizgas, Sprühflasche, 40 ml
★★★★★ (2) EUR 1,99

Produktbeschreibungen

Behavior-based Analysis

Collect and analyze flows

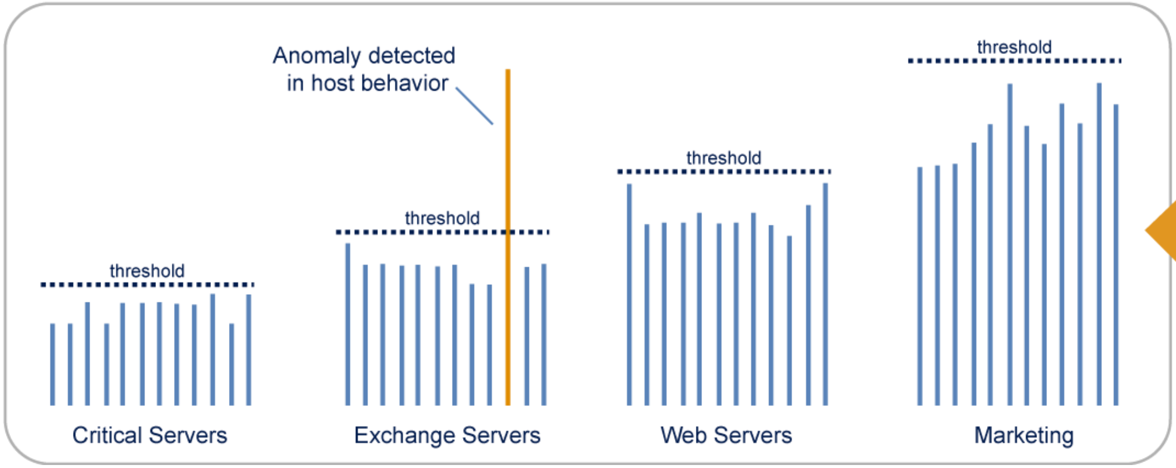


Establish baseline of behavior

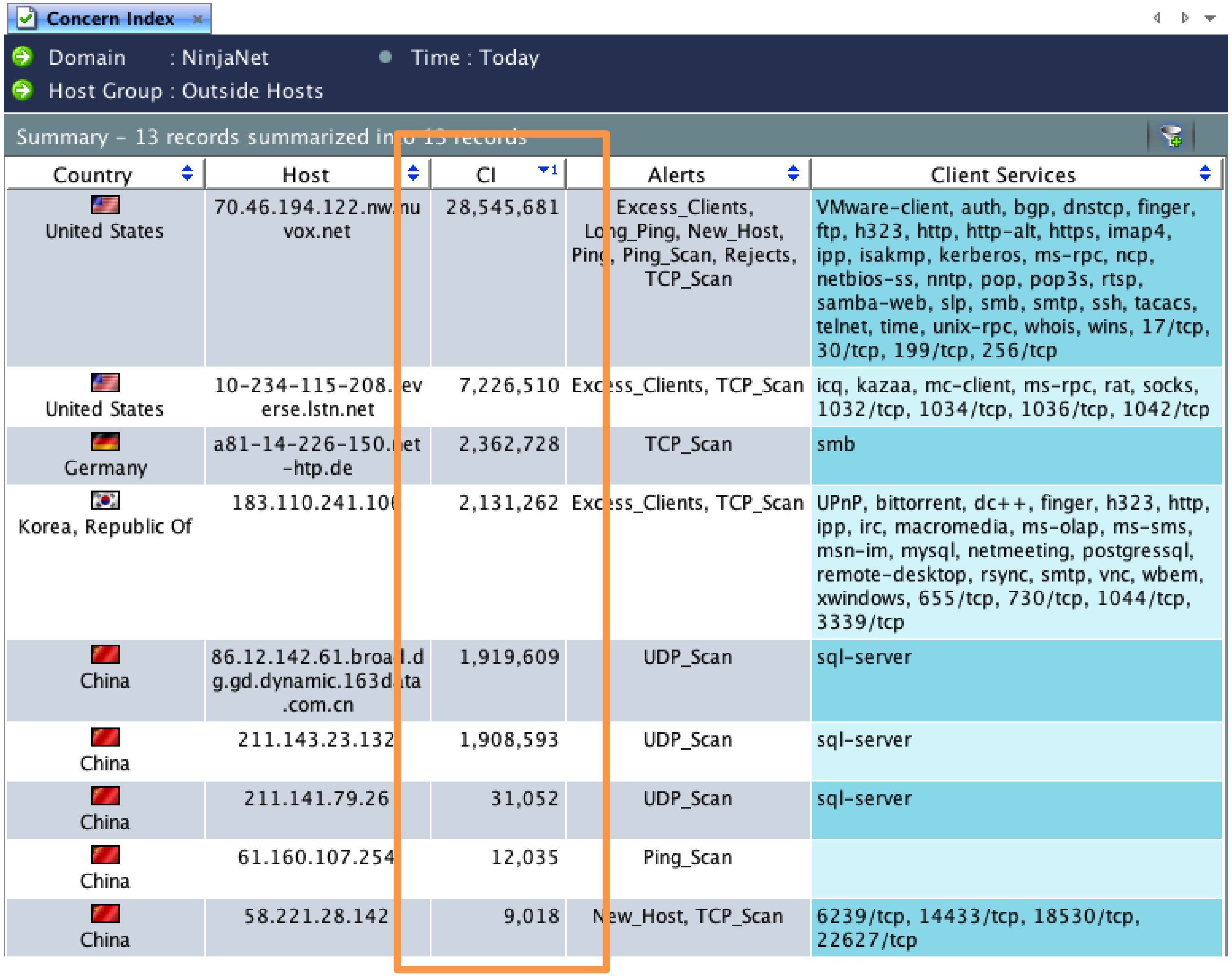
B E H A V I O R

- Number of concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of Syns received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Alarm on anomalies and changes in behavior



StealthWatch Threat Indexes



Domain : NinjaNet

Time : Today

Host Group : Outside Hosts

Summary – 13 records summarized into 13 records

Country	Host	CI	Alerts	Client Services
United States	70.46.194.122.nwnuvox.net	28,545,681	Excess_Clients, Long_Ping, New_Host, Ping, Ping_Scan, Rejects, TCP_Scan	VMware-client, auth, bgp, dnstcp, finger, ftp, h323, http, http-alt, https, imap4, ipp, isakmp, kerberos, ms-rpc, ncp, netbios-ss, nntp, pop, pop3s, rtsp, samba-web, slp, smb, smtp, ssh, tacacs, telnet, time, unix-rpc, whois, wins, 17/tcp, 30/tcp, 199/tcp, 256/tcp
United States	10-234-115-208.reverse.lstn.net	7,226,510	Excess_Clients, TCP_Scan	icq, kazaa, mc-client, ms-rpc, rat, socks, 1032/tcp, 1034/tcp, 1036/tcp, 1042/tcp
Germany	a81-14-226-150.net-htp.de	2,362,728	TCP_Scan	smb
Korea, Republic Of	183.110.241.10	2,131,262	Excess_Clients, TCP_Scan	UPnP, bittorrent, dc++, finger, h323, http, ipp, irc, macromedia, ms-olap, ms-sms, msn-im, mysql, netmeeting, postgressql, remote-desktop, rsync, smtp, vnc, wbem, xwindows, 655/tcp, 730/tcp, 1044/tcp, 3339/tcp
China	86.12.142.61.broad.dg.gd.dynamic.163data.com.cn	1,919,609	UDP_Scan	sql-server
China	211.143.23.132	1,908,593	UDP_Scan	sql-server
China	211.141.79.26	31,052	UDP_Scan	sql-server
China	61.160.107.254	12,035	Ping_Scan	
China	58.221.28.142	9,018	New_Host, TCP_Scan	6239/tcp, 14433/tcp, 18530/tcp, 22627/tcp

How Flows are Used

1

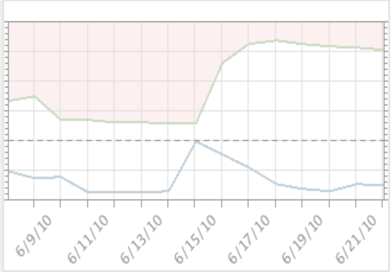
Traffic Analysis and Network Visibility

- Bandwidth Trending
- QoS Monitoring
- Network troubleshooting
- Router Capacity

2

Detect Network Anomalies

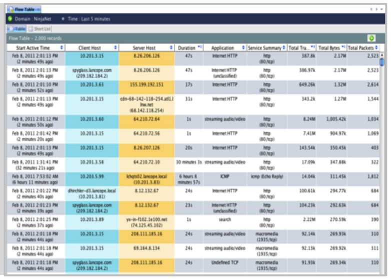
- Internal Monitoring
- Rapid Detection
- Firewall Validation
- DoS Detection



3

Forensics and Incident Response

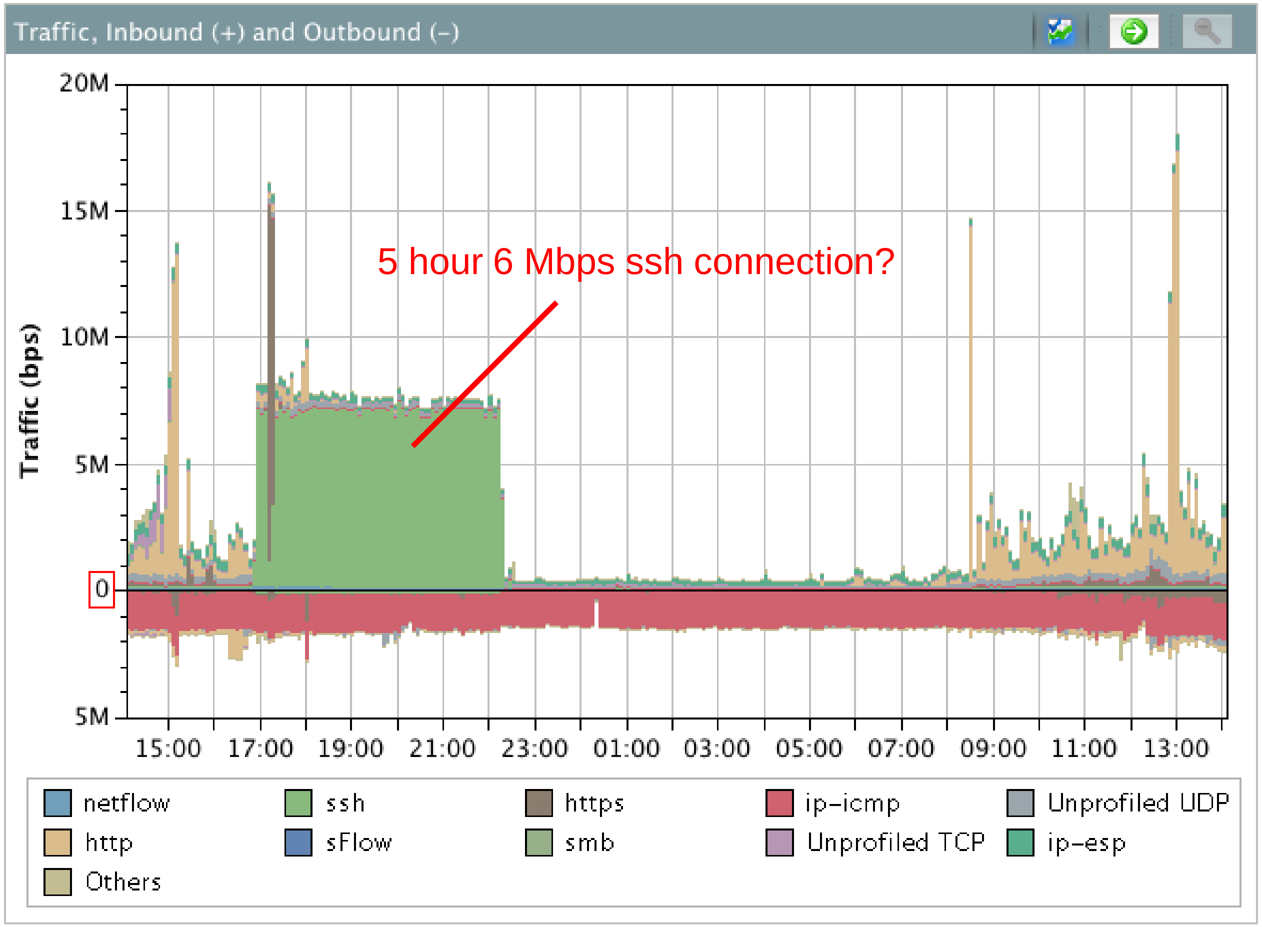
- Reduce MTTK
- Records *All* Traffic
- Situational Awareness
- Compliments SIEM



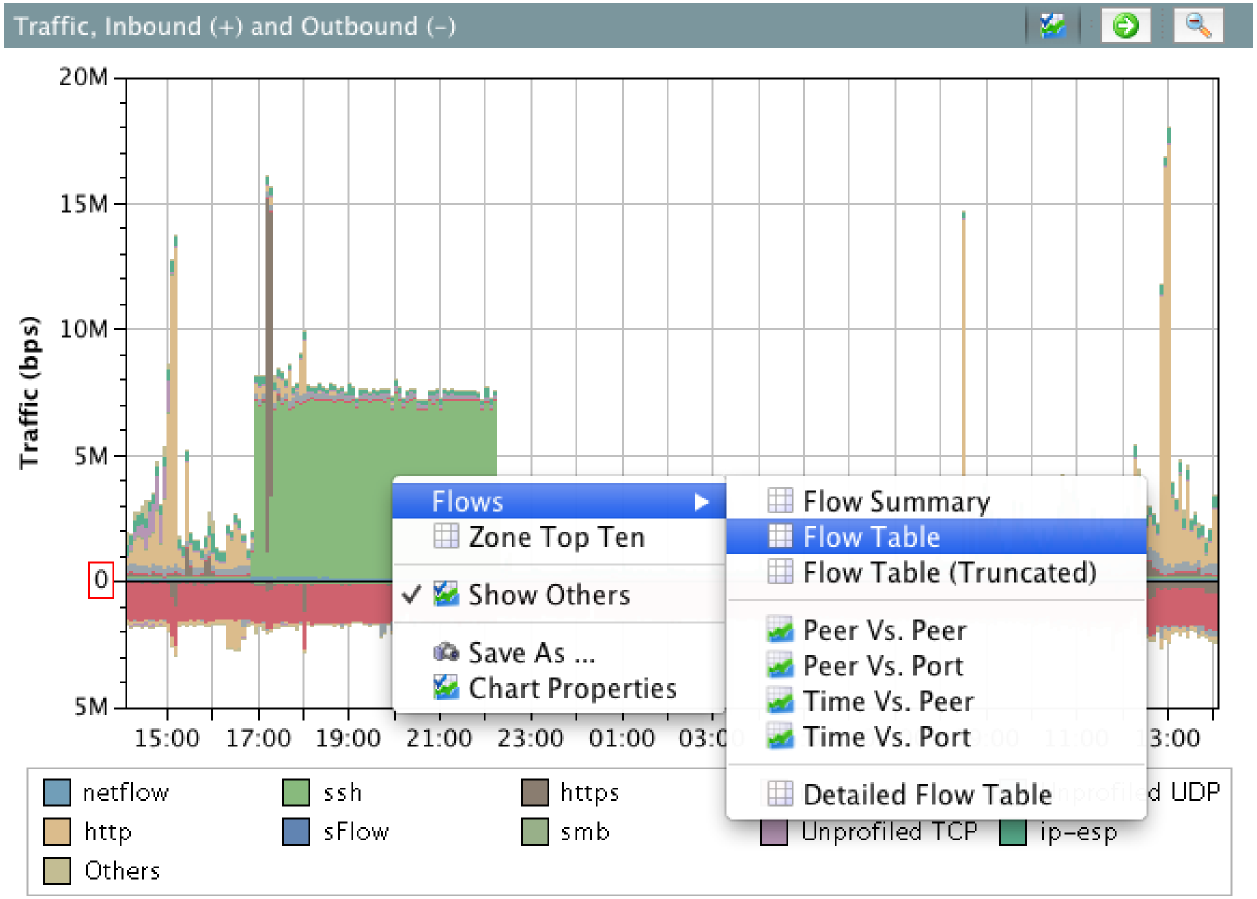
Flow Table - 2,000 records

Start Active Time	Client Host	Server Host	Duration	Application	Service Summary	Total Tra...	Total Bytes	Total Packets
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.206.126	47s	Internet HTTP	http (80/tcp)	387.8k	2.17M	2,523
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	spyglass.lancope.com (209.182.184.2)	8.26.206.126	47s	Internet HTTP (unclassified)	http (80/tcp)	386.97k	2.17M	2,523
Feb 8, 2011 2:01:10 PM (2 minutes 52s ago)	10.201.3.63	155.199.192.151	17s	Internet HTTP	http (80/tcp)	649.26k	1.32M	2,614
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	cdn-68-142-118-254.atl1.lnw.net (68.142.118.254)	31s	Internet HTTP	http (80/tcp)	343.2k	1.27M	1,544
Feb 8, 2011 2:01:12 PM (2 minutes 50s ago)	10.201.3.60	64.210.72.64	1s	streaming audio/video	http (80/tcp)	8.24M	1,005.42k	1,034
Feb 8, 2011 2:01:42 PM (2 minutes 20s ago)	10.201.3.15	64.210.72.56	1s	Internet HTTP	http (80/tcp)	7.41M	904.97k	1,069
Feb 8, 2011 2:01:13 PM (2 minutes 49s ago)	10.201.3.15	8.26.207.126	20s	Internet HTTP	http (80/tcp)	143.54k	350.45k	403
Feb 8, 2011 1:31:41 PM (32 minutes 21s ago)	10.201.3.58	64.210.72.10	30 minutes 3s	streaming audio/video	http (80/tcp)	17.09k	347.88k	322
Feb 8, 2011 7:53:02 AM (6 hours 11 minutes ago)	10.203.5.99	lchqts02.lancope.local (10.201.3.83)	6 hours 8 minutes 57s	ICMP	icmp (Echo Reply)	14.04k	311.45k	1,812
Feb 8, 2011 2:01:22 PM (2 minutes 40s ago)	dhirchler-d3.lancope.local (10.201.3.81)	8.12.132.67	24s	Internet HTTP	http (80/tcp)	100.61k	294.77k	684
Feb 8, 2011 2:01:23 PM (2 minutes 39s ago)	spyglass.lancope.com (209.182.184.2)	8.12.132.67	23s	Internet HTTP (unclassified)	http (80/tcp)	104.23k	292.63k	684
Feb 8, 2011 2:01:25 PM (2 minutes 37s ago)	10.201.3.89	yx-in-f102.1e100.net (74.125.45.102)	1s	search	http (80/tcp)	2.22M	270.59k	390
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	208.111.185.16	24s	streaming audio/video	macromedia (1935/tcp)	92.14k	269.93k	310
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	10.201.3.15	69.164.8.134	24s	streaming audio/video	macromedia (1935/tcp)	92.13k	269.92k	311
Feb 8, 2011 2:01:18 PM (2 minutes 44s ago)	spyglass.lancope.com (209.182.184.2)	208.111.185.16	24s	Undefined TCP	macromedia (1935/tcp)	91.93k	269.34k	310

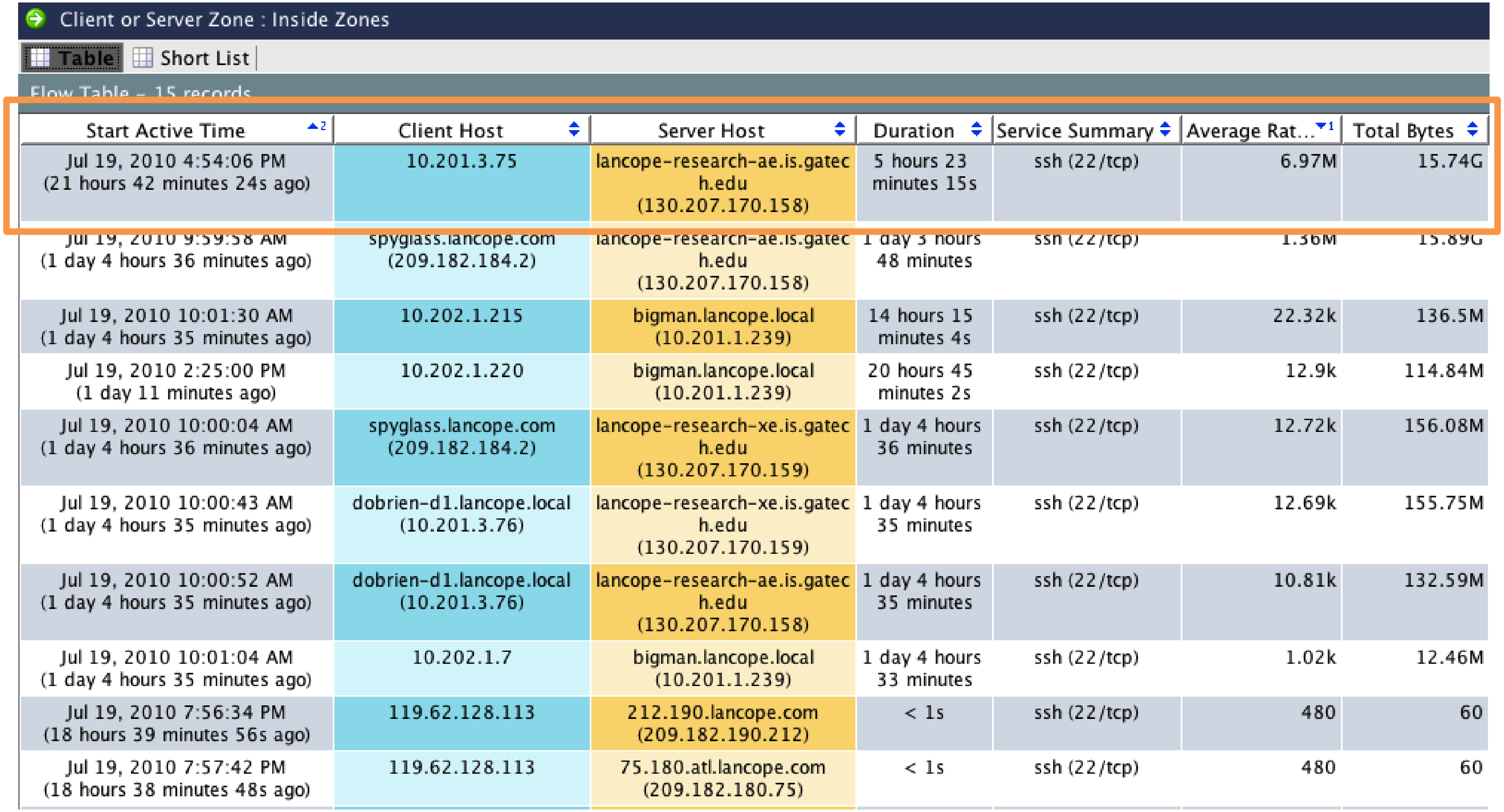
Incident Investigation Using Flows



Incident Investigation Using Flows



Incident Investigation Using Flows

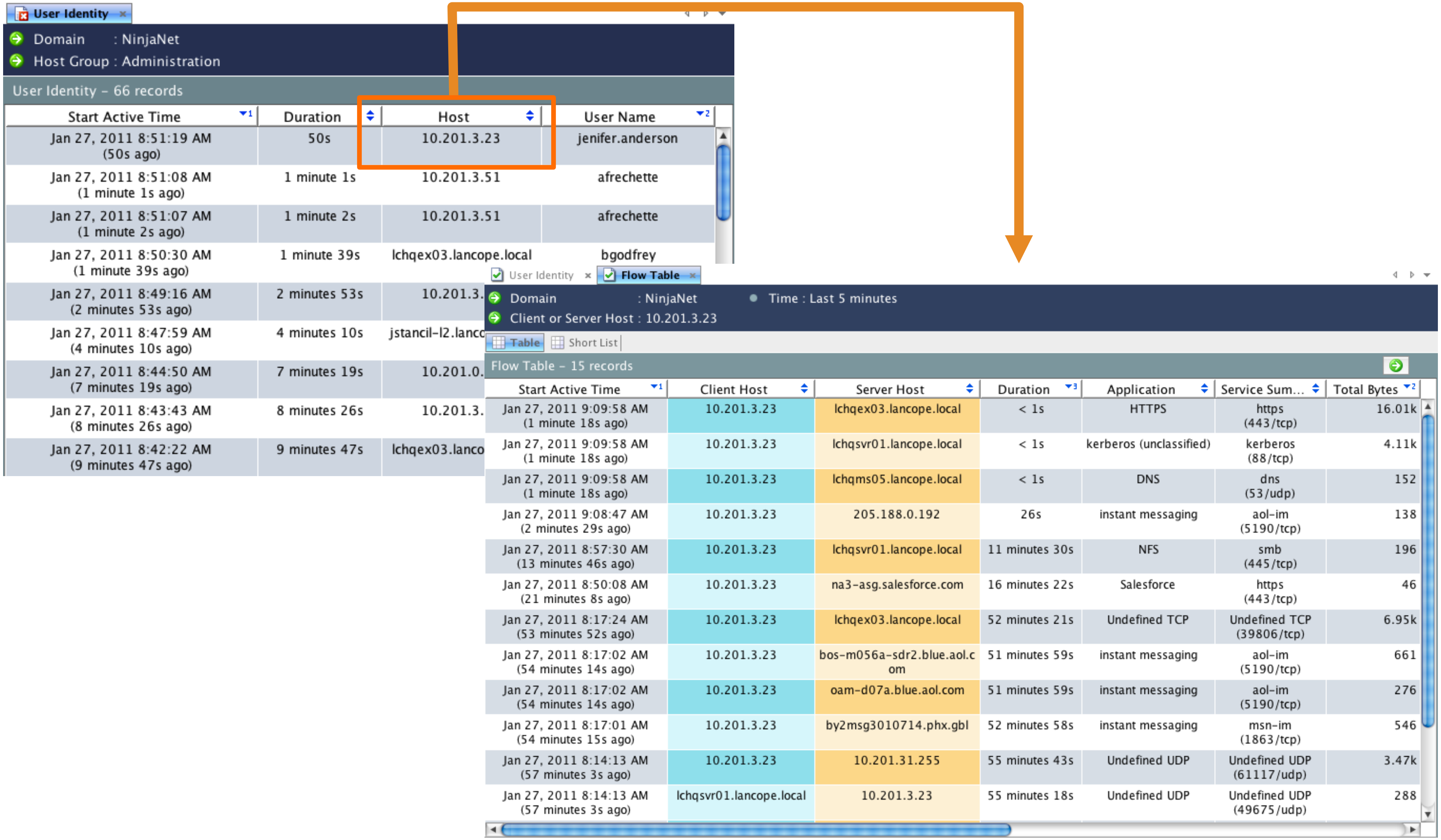


Client or Server Zone : Inside Zones

Flow Table – 15 records

Start Active Time ▲2	Client Host	Server Host	Duration	Service Summary	Average Rat… ▼1	Total Bytes
Jul 19, 2010 4:54:06 PM (21 hours 42 minutes 24s ago)	10.201.3.75	lancope-research-ae.is.gatech.edu (130.207.170.158)	5 hours 23 minutes 15s	ssh (22/tcp)	6.97M	15.74G
Jul 19, 2010 9:59:58 AM (1 day 4 hours 36 minutes ago)	spyglass.lancope.com (209.182.184.2)	lancope-research-ae.is.gatech.edu (130.207.170.158)	1 day 3 hours 48 minutes	ssh (22/tcp)	1.36M	15.89G
Jul 19, 2010 10:01:30 AM (1 day 4 hours 35 minutes ago)	10.202.1.215	bigman.lancope.local (10.201.1.239)	14 hours 15 minutes 4s	ssh (22/tcp)	22.32k	136.5M
Jul 19, 2010 2:25:00 PM (1 day 11 minutes ago)	10.202.1.220	bigman.lancope.local (10.201.1.239)	20 hours 45 minutes 2s	ssh (22/tcp)	12.9k	114.84M
Jul 19, 2010 10:00:04 AM (1 day 4 hours 36 minutes ago)	spyglass.lancope.com (209.182.184.2)	lancope-research-xe.is.gatech.edu (130.207.170.159)	1 day 4 hours 36 minutes	ssh (22/tcp)	12.72k	156.08M
Jul 19, 2010 10:00:43 AM (1 day 4 hours 35 minutes ago)	dobrien-d1.lancope.local (10.201.3.76)	lancope-research-xe.is.gatech.edu (130.207.170.159)	1 day 4 hours 35 minutes	ssh (22/tcp)	12.69k	155.75M
Jul 19, 2010 10:00:52 AM (1 day 4 hours 35 minutes ago)	dobrien-d1.lancope.local (10.201.3.76)	lancope-research-ae.is.gatech.edu (130.207.170.158)	1 day 4 hours 35 minutes	ssh (22/tcp)	10.81k	132.59M
Jul 19, 2010 10:01:04 AM (1 day 4 hours 35 minutes ago)	10.202.1.7	bigman.lancope.local (10.201.1.239)	1 day 4 hours 33 minutes	ssh (22/tcp)	1.02k	12.46M
Jul 19, 2010 7:56:34 PM (18 hours 39 minutes 56s ago)	119.62.128.113	212.190.lancope.com (209.182.190.212)	< 1s	ssh (22/tcp)	480	60
Jul 19, 2010 7:57:42 PM (18 hours 38 minutes 48s ago)	119.62.128.113	75.180.atl.lancope.com (209.182.180.75)	< 1s	ssh (22/tcp)	480	60

Map Flows to Users



Domain : NinjaNet
Host Group : Administration

User Identity – 66 records

Start Active Time	Duration	Host	User Name
Jan 27, 2011 8:51:19 AM (50s ago)	50s	10.201.3.23	jenifer.anderson
Jan 27, 2011 8:51:08 AM (1 minute 1s ago)	1 minute 1s	10.201.3.51	afrechette
Jan 27, 2011 8:51:07 AM (1 minute 2s ago)	1 minute 2s	10.201.3.51	afrechette
Jan 27, 2011 8:50:30 AM (1 minute 39s ago)	1 minute 39s	lchqex03.lancope.local	bgodfrey
Jan 27, 2011 8:49:16 AM (2 minutes 53s ago)	2 minutes 53s	10.201.3.	
Jan 27, 2011 8:47:59 AM (4 minutes 10s ago)	4 minutes 10s	jstancil-l2.lanco	
Jan 27, 2011 8:44:50 AM (7 minutes 19s ago)	7 minutes 19s	10.201.0.	
Jan 27, 2011 8:43:43 AM (8 minutes 26s ago)	8 minutes 26s	10.201.3.	
Jan 27, 2011 8:42:22 AM (9 minutes 47s ago)	9 minutes 47s	lchqex03.lanco	

Domain : NinjaNet
Time : Last 5 minutes
Client or Server Host : 10.201.3.23

Flow Table – 15 records

Start Active Time	Client Host	Server Host	Duration	Application	Service Sum...	Total Bytes
Jan 27, 2011 9:09:58 AM (1 minute 18s ago)	10.201.3.23	lchqex03.lancope.local	< 1s	HTTPS	https (443/tcp)	16.01k
Jan 27, 2011 9:09:58 AM (1 minute 18s ago)	10.201.3.23	lchqsvr01.lancope.local	< 1s	kerberos (unclassified)	kerberos (88/tcp)	4.11k
Jan 27, 2011 9:09:58 AM (1 minute 18s ago)	10.201.3.23	lchqms05.lancope.local	< 1s	DNS	dns (53/udp)	152
Jan 27, 2011 9:08:47 AM (2 minutes 29s ago)	10.201.3.23	205.188.0.192	26s	instant messaging	aol-im (5190/tcp)	138
Jan 27, 2011 8:57:30 AM (13 minutes 46s ago)	10.201.3.23	lchqsvr01.lancope.local	11 minutes 30s	NFS	smb (445/tcp)	196
Jan 27, 2011 8:50:08 AM (21 minutes 8s ago)	10.201.3.23	na3-asg.salesforce.com	16 minutes 22s	Salesforce	https (443/tcp)	46
Jan 27, 2011 8:17:24 AM (53 minutes 52s ago)	10.201.3.23	lchqex03.lancope.local	52 minutes 21s	Undefined TCP	Undefined TCP (39806/tcp)	6.95k
Jan 27, 2011 8:17:02 AM (54 minutes 14s ago)	10.201.3.23	bos-m056a-sdr2.blue.aol.com	51 minutes 59s	instant messaging	aol-im (5190/tcp)	661
Jan 27, 2011 8:17:02 AM (54 minutes 14s ago)	10.201.3.23	oam-d07a.blue.aol.com	51 minutes 59s	instant messaging	aol-im (5190/tcp)	276
Jan 27, 2011 8:17:01 AM (54 minutes 15s ago)	10.201.3.23	by2msg3010714.phx.gbl	52 minutes 58s	instant messaging	msn-im (1863/tcp)	546
Jan 27, 2011 8:14:13 AM (57 minutes 3s ago)	10.201.3.23	10.201.31.255	55 minutes 43s	Undefined UDP	Undefined UDP (61117/udp)	3.47k
Jan 27, 2011 8:14:13 AM (57 minutes 3s ago)	lchqsvr01.lancope.local	10.201.3.23	55 minutes 18s	Undefined UDP	Undefined UDP (49675/udp)	288

Lancope

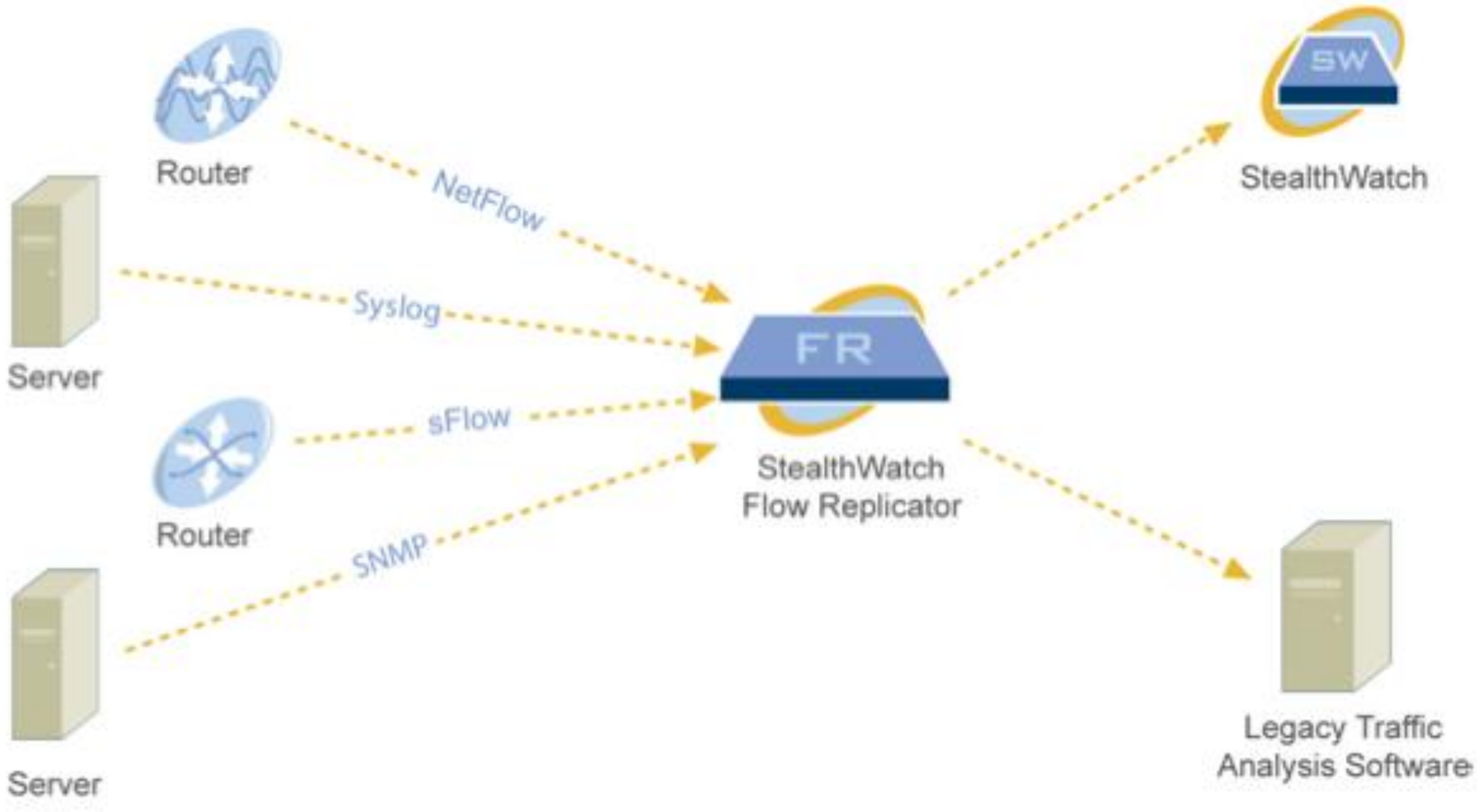
Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

Configuring and Working with NetFlow

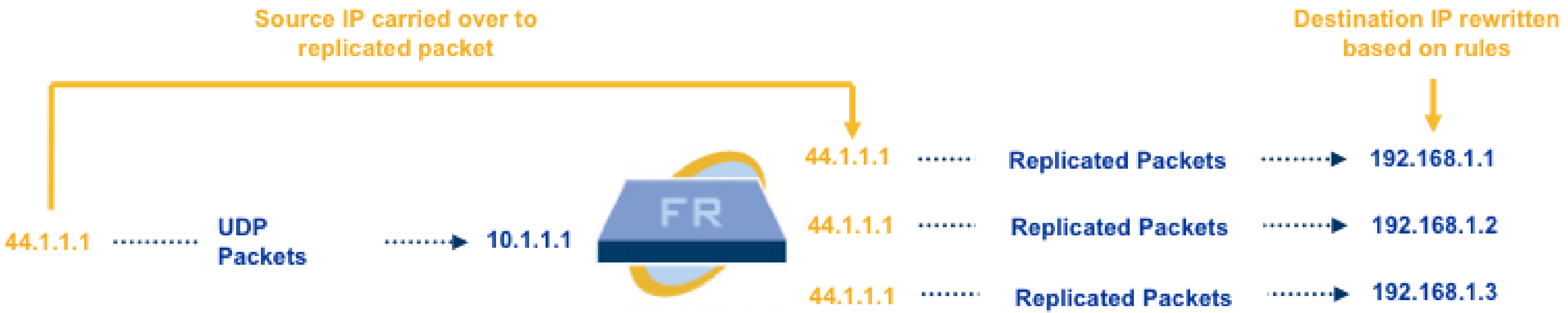
Know Your Network, Run Your Business

Flow Replication

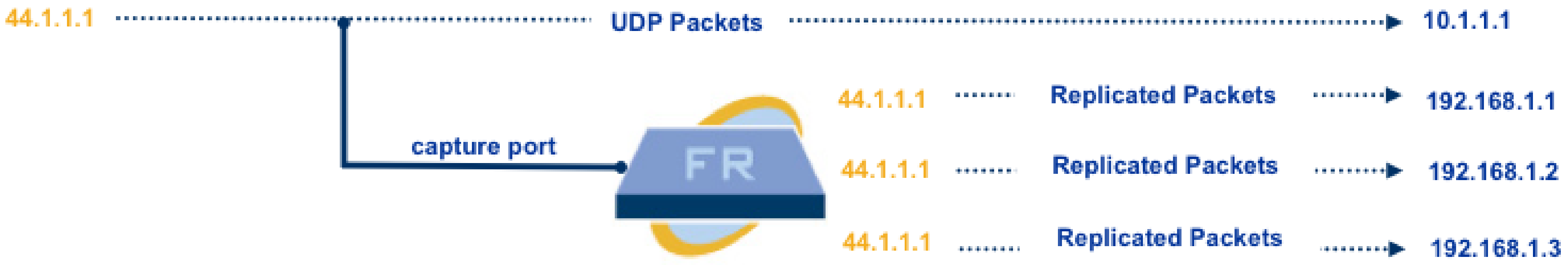


Flow Replication Modes

Unicast Mode

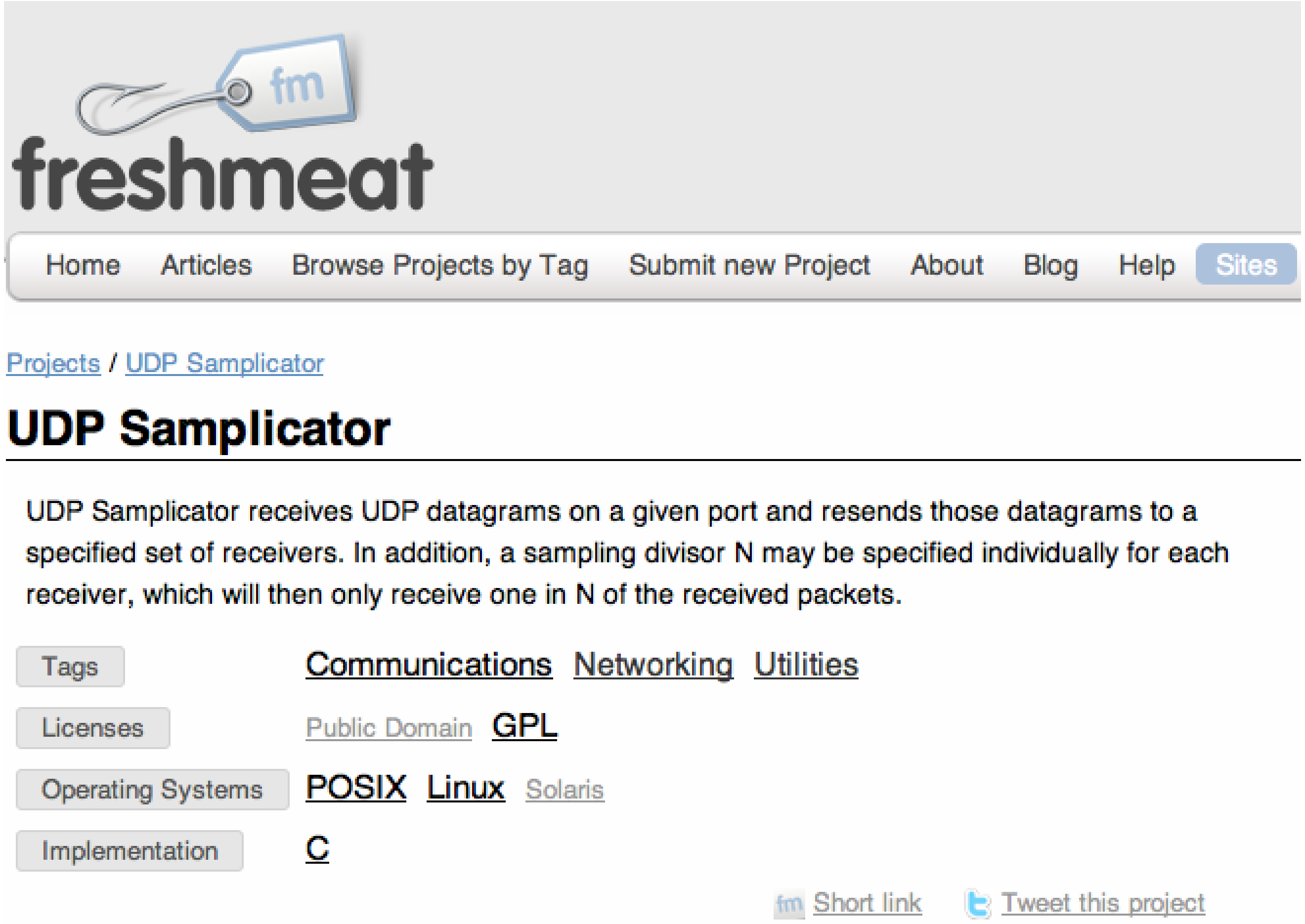


Promiscuous Mode



Flow Replication: UDP Samplicator

http://freshmeat.net/projects/samplicator/



Projects / UDP Samplicator

UDP Samplicator

UDP Samplicator receives UDP datagrams on a given port and resends those datagrams to a specified set of receivers. In addition, a sampling divisor N may be specified individually for each receiver, which will then only receive one in N of the received packets.

Tags	Communications Networking Utilities
Licenses	Public Domain GPL
Operating Systems	POSIX Linux Solaris
Implementation	C

Active vs. Inactive Timeouts

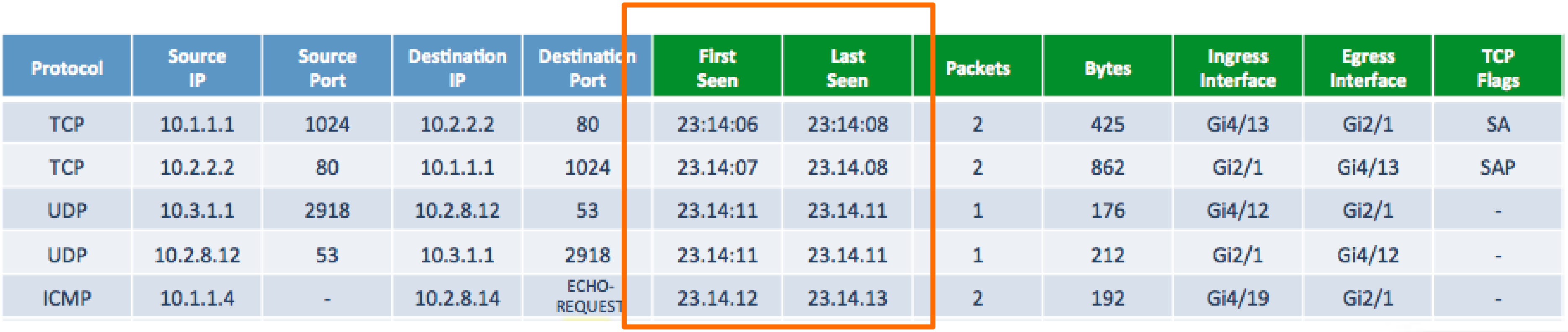
Inactive Timeout

- configures how long a flow can be inactive before it is expired from the cache
- Recommend 15 seconds (which is also the IOS default)
- All exporters should have similar inactive timeouts

Active Timeout

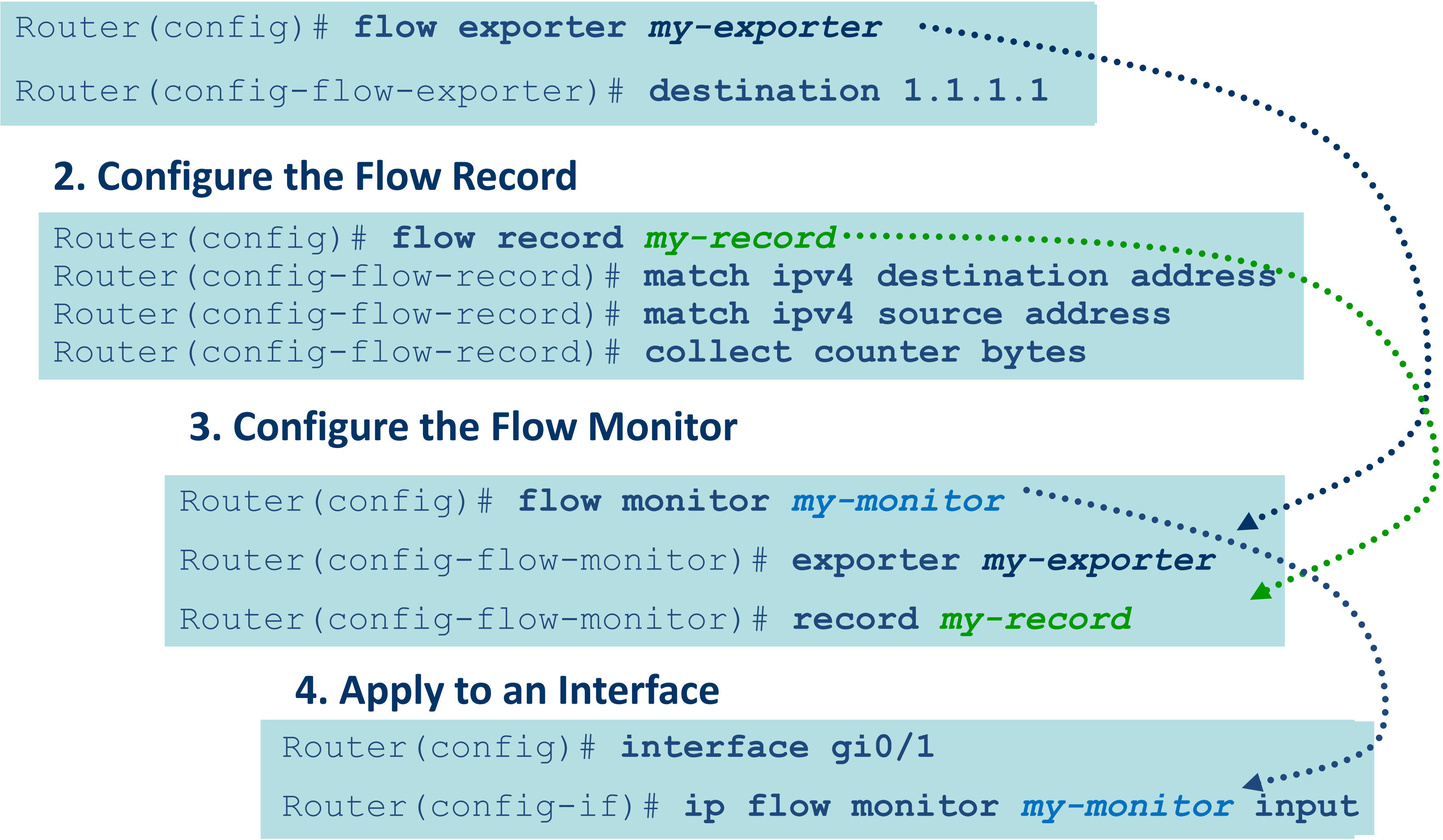
- configures longest amount of time a flow can stay in the cache regardless of activity
- Recommend 1 minute
- All exporters should have similar active timeouts
- Cisco default of 30 minutes is far too long

Last Seen – First Seen == Time Active



Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO- REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-

Configuring Netflow – Flexible NetFlow



1. Configure the Exporter

```
Router(config)# flow exporter my-exporter

Router(config-flow-exporter)# destination 1.1.1.1
```

2. Configure the Flow Record

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

3. Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor

Router(config-flow-monitor)# exporter my-exporter

Router(config-flow-monitor)# record my-record
```

4. Apply to an Interface

```
Router(config)# interface gi0/1

Router(config-if)# ip flow monitor my-monitor input
```

Flexible NetFlow - User-Defined Record Configuration

```
Router(config)# flow record my-record
Router(config-flow-record)# match
Router(config-flow-record)# collect

Router(config-flow-record)# match ?
      application         Application Fields
      datalink            Datalink (layer 2) fields
      flow                Flow identifying fields
      interface           Interface fields
      ipv4                IPv4 fields
      ipv6                IPv6 fields
      routing             routing attributes
      transport           Transport layer field

Router(config-flow-record)# collect ?
      application         Application Fields
      counter             Counter fields
      datalink            Datalink (layer 2) fields
      flow                Flow identifying fields
      interface           Interface fields
      ipv4                IPv4 fields
      ipv6                IPv6 fields
      routing             IPv4 routing attributes
      timestamp           Timestamp fields
      transport           Transport layer fields
```

Specify a Key Field

Specify a Non-Key Kield

Configuring a Flexible NetFlow Flow Record

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 tos
Router(config-flow-record)# match ipv4 protocol
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# match transport source-port
Router(config-flow-record)# match transport destination-port
Router(config-flow-record)# match interface input
Router(config-flow-record)# collect routing destination as
Router(config-flow-record)# collect routing next-hop address ipv4
Router(config-flow-record)# collect ipv4 dscp
Router(config-flow-record)# collect ipv4 ttl maximum
Router(config-flow-record)# collect ipv4 ttl minimum
Router(config-flow-record)# collect transport tcp flags
Router(config-flow-record)# collect interface output
Router(config-flow-record)# collect counter bytes
Router(config-flow-record)# collect counter packets
Router(config-flow-record)# collect timestamp sys-uptime first
Router(config-flow-record)# collect timestamp sys-uptime last
```

Useful Show Commands

- List of all possible information elements

  ```
  show flow exporter export-ids netflow-v9
  ```

- Template assignment

  ```
  show flow exporter template
  ```

- High watermark in the cache

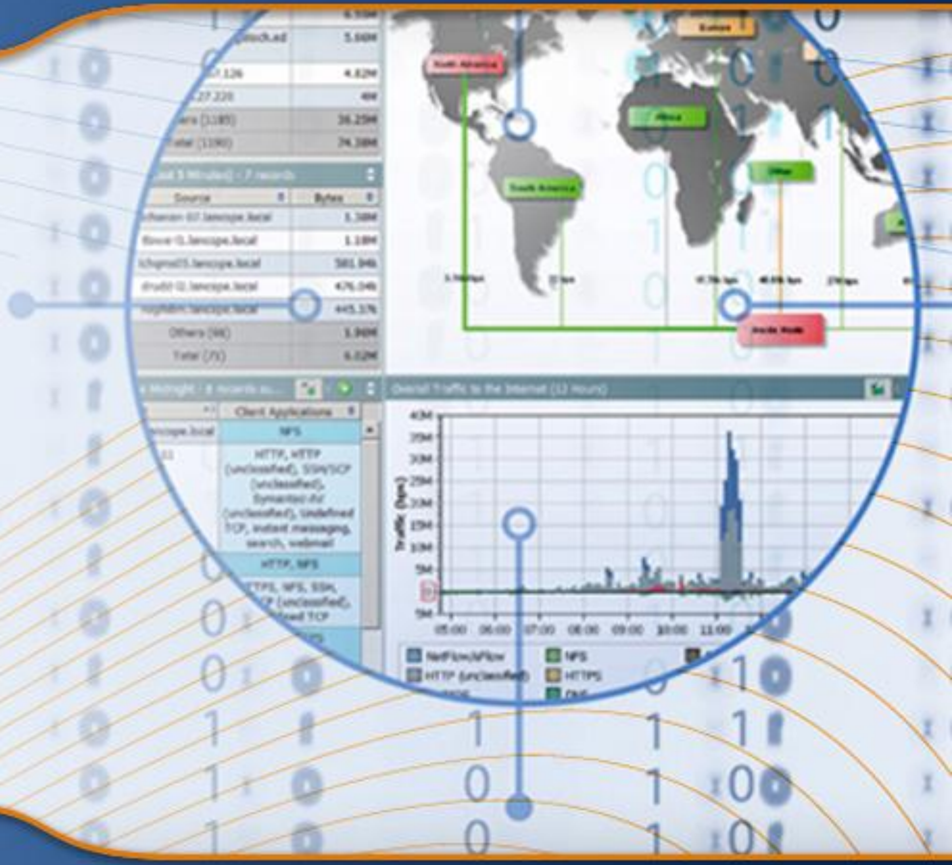
  ```
  show flow monitor <flow-monitor> statistics
  ```

- NetFlow configuration

  ```
  show running flow [exporter | monitor | record]
  ```

Lancope
Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™



Lab Exercise #1, #2

Lancope

Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

Working with NetFlow

Configuring NetFlow on the Cat6k (older)

MSFC (RP)

```
!
ip flow-export destination {collector_ip} 2055          exporter IP and port
ip flow-export source loopback0                         loopback0 usually
ip flow-export version 9                                export in NetFlow v9 format
ip flow-cache timeout active 1                          active timeout in minutes
ip flow-cache timeout inactive 15                       inactive timeout in seconds
ip flow-export version 9 origin-as                      enables BGP AS reporting
ip flow ingress layer2-switched vlan {vlanlist}         enables layer-2 NetFlow
ip flow-capture mac-addresses                                     enables layer-2 MAC addresses
ip flow-capture vlan-id                                 enables vlan ids
snmp-server ifindex persist                             freezes ifindex values
```

Sup (SP)

```
mls nde sender version 7                                sup NetFlow version
mls aging long 64                                                 sup active timeout in seconds
mls aging normal 32
mls nde interface
mls flow ip interface-full
!
interface {interface}
        ip flow ingress
!
```

NetFlow Impact to CPU and Network

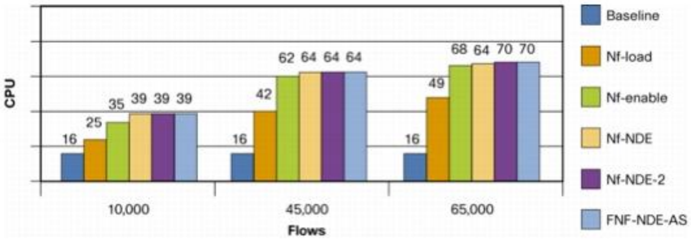
Cisco Whitepaper: NetFlow Performance Analysis

http://www.cisco.com/en/US/tech/tk812/technologies_white_paper0900aecd802a0eb9.shtml

Fully loaded ISR running software IOS ~15% CPU uptick resulting from NetFlow enablement.

Cat6K only runs into issues when TCAM full.

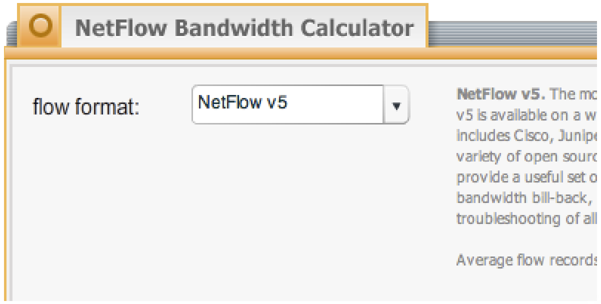
Figure 4. Cisco 2600 Router



Lancope NetFlow Bandwidth Calculator

http://lancope.com/netflowcalculator.aspx

Assume 50 flows per second for each 10Mbps of traffic.



NetFlow Bandwidth Calculator

flow format: NetFlow v5 ▾

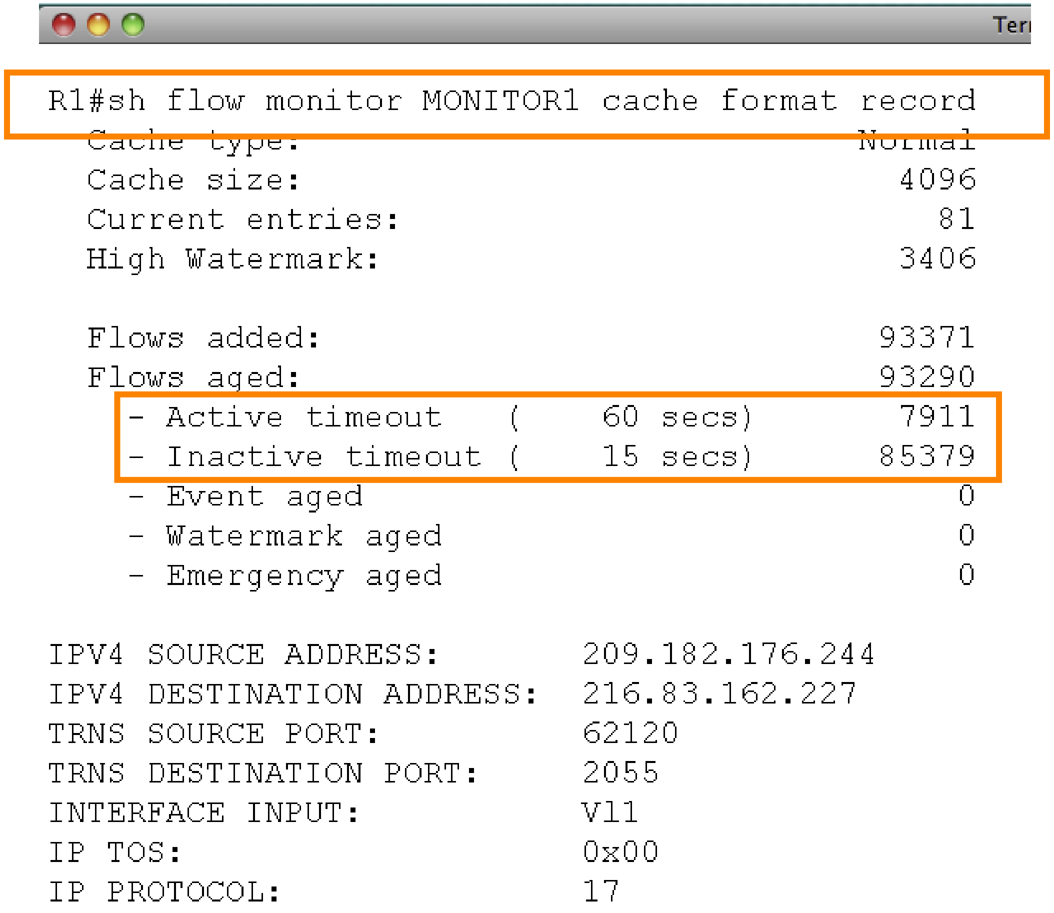
NetFlow v5. The mc
v5 is available on a w
includes Cisco, Junip
variety of open sourc
provide a useful set o
bandwidth bill-back,
troubleshooting of all

Average flow records

Troubleshooting with NetFlow

- Several approaches to working with flow data...
  - Direct router access via CLI
  - Flow-tools, ntop and other open source
  - Commercial NetFlow Collector

Direct access via CLI (Flexible NetFlow)

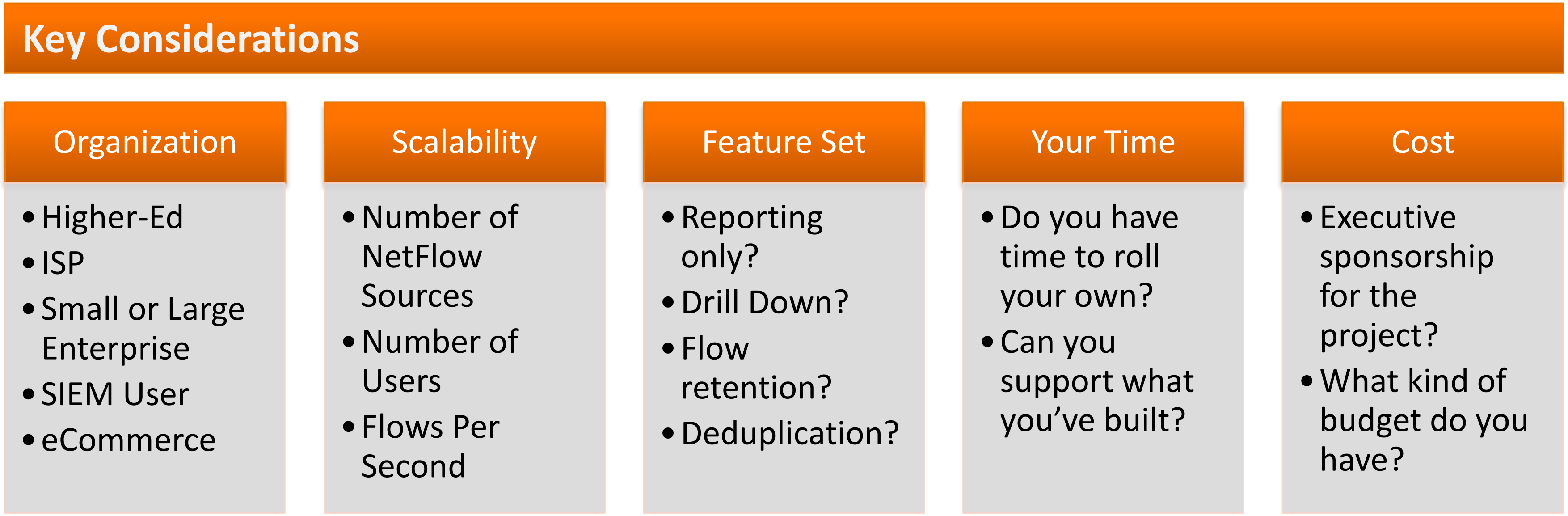


```
R1#sh flow monitor MONITOR1 cache format record
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                              81
  High Watermark:                             3406

  Flows added:                               93371
  Flows aged:                                93290
    - Active timeout    (     60 secs)        7911
    - Inactive timeout  (     15 secs)       85379
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

IPV4 SOURCE ADDRESS:        209.182.176.244
IPV4 DESTINATION ADDRESS:   216.83.162.227
TRNS SOURCE PORT:           62120
TRNS DESTINATION PORT:      2055
INTERFACE INPUT:            Vl1
IP TOS:                     0x00
IP PROTOCOL:                17
```

Choose the Right Collector



Key Considerations

Organization

- Higher-Ed
- ISP
- Small or Large Enterprise
- SIEM User
- eCommerce

Scalability

- Number of NetFlow Sources
- Number of Users
- Flows Per Second

Feature Set

- Reporting only?
- Drill Down?
- Flow retention?
- Deduplication?

Your Time

- Do you have time to roll your own?
- Can you support what you’ve built?

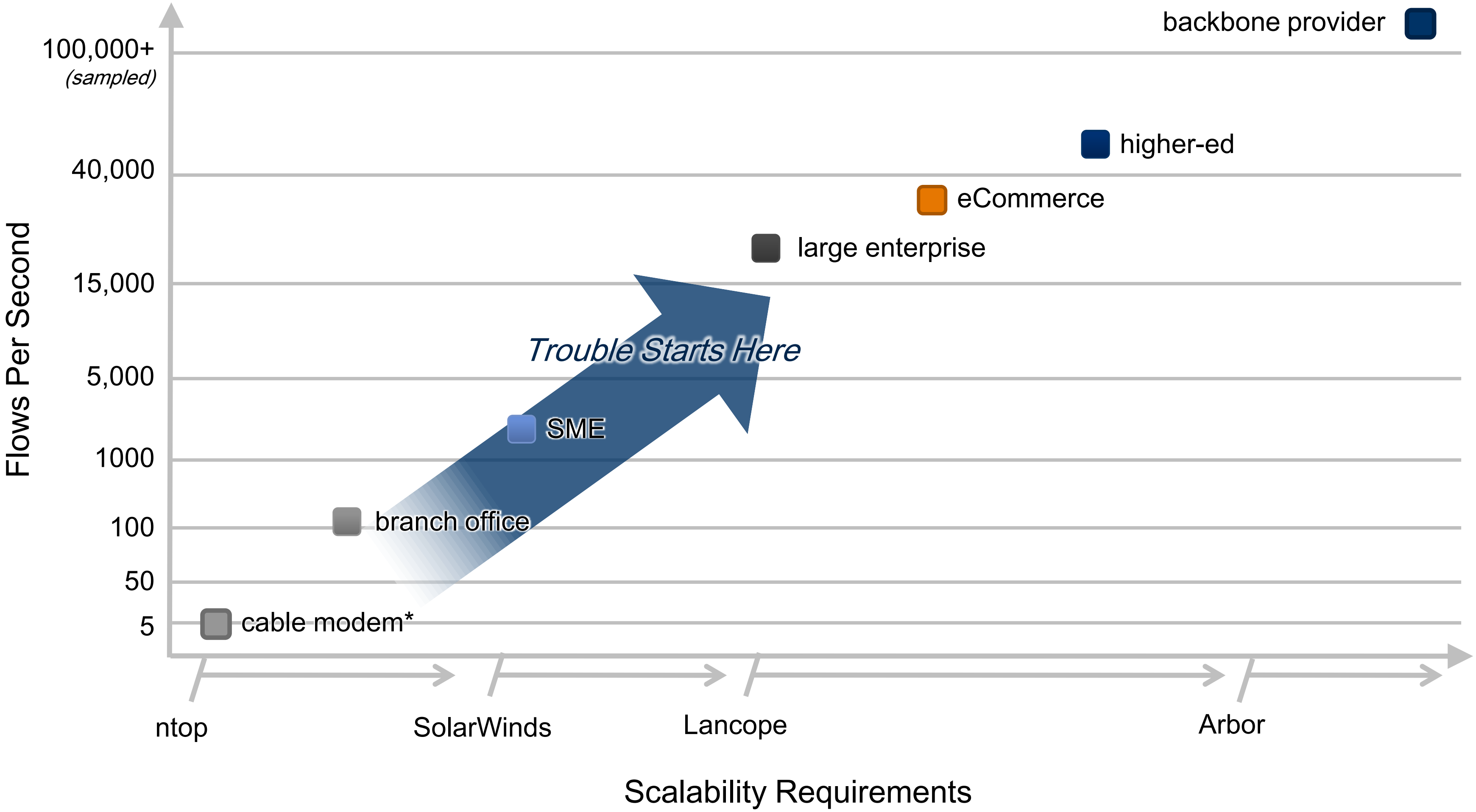
Cost

- Executive sponsorship for the project?
- What kind of budget do you have?

Choose the Right Collector

Collector Type	Example	Price	Target Audience	Scalability	Feature Set
Open Source	nfdump, ntop	Labor + Hardware	Power Users, Enthusiasts	Medium (varies with effort)	Low (varies with effort)
Small Business Commercial	SolarWinds Orion	< $50K	Small Networks, < 500 users	Very Low	Medium
SIEM	ArcSight Express	Varies	Security Administrators	Low	Very Low
Enterprise Commercial	Lancope StealthWatch	$50K+	Fortune 5000, DoD, Higher Ed eCommerce	High	Very High
Carrier Grade and ISP	Arbor PeakFlow SP	$100K+	Internet Service Providers	Very High	High

NetFlow Collector Types



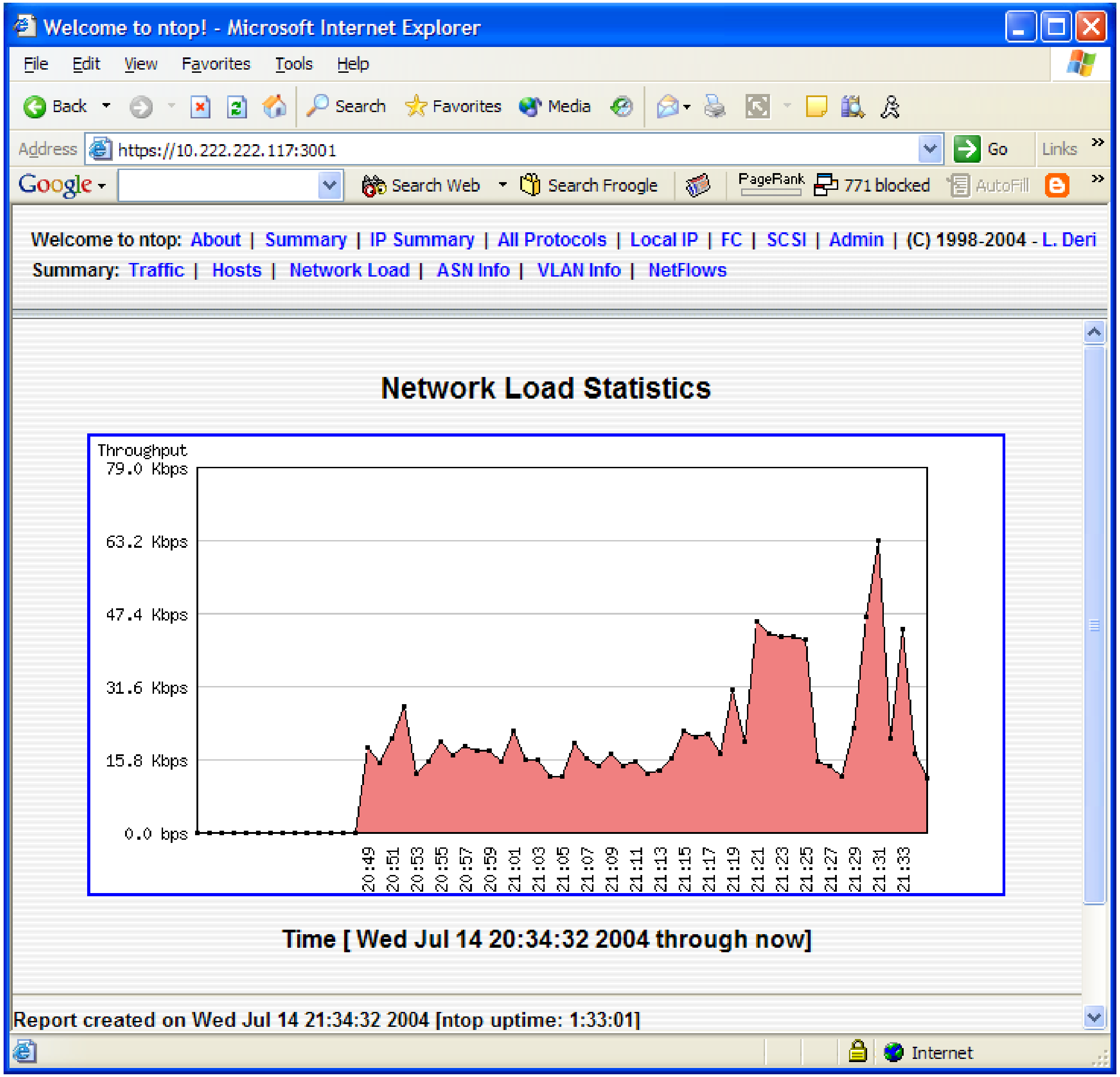
* check out "dd-wrt" for NetFlow support in your Linksys or D-Link home office router

NetFlow Open Source Tools

Product Name	Primary Use	Comment	OS
Cflowd	Traffic Analysis	No longer supported	UNIX
Flow-tools	Collector Device	Scalable	UNIX
Flowd	Collector Device	Support V9	BSD, Linux
FlowScan	Reporting for Flow-Tools		UNIX
IPFlow	Traffic Analysis	Support V9, IPv4, IPv6, MPLS, SCTP, etc..	Linux, FreeBSD, Solaris
NetFlow Guide	Reporting Tools		BSD, Linux
NetFlow Monitor	Traffic Analysis	Supports V9	UNIX
Netmet	Collector Device	V5, support v9	Linux
NTOP	Security Monitoring		UNIX
Stager	Reporting for Flow-Tools		UNIX
Nfdump/nfsen	Traffic Analysis	Supprot V5 and v9	UNIX

Different costs: implementation and customization

ntop web-UI



Welcome to ntop! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.222.222.117:3001
Go Links
Google Search Web Search Froogle PageRank 771 blocked AutoFill
Throughput
79.0 Kbps
63.2 Kbps
47.4 Kbps
31.6 Kbps
15.8 Kbps
0.0 bps
20:49
20:51
20:53
20:55
20:57
20:59
21:01
21:03
21:05
21:07
21:09
21:11
21:13
21:15
21:17
21:19
21:21
21:23
21:25
21:27
21:29
21:31
21:33
Internet

Welcome to ntop: About | Summary | IP Summary | All Protocols | Local IP | FC | SCSI | Admin | (C) 1998-2004 - L. Deri

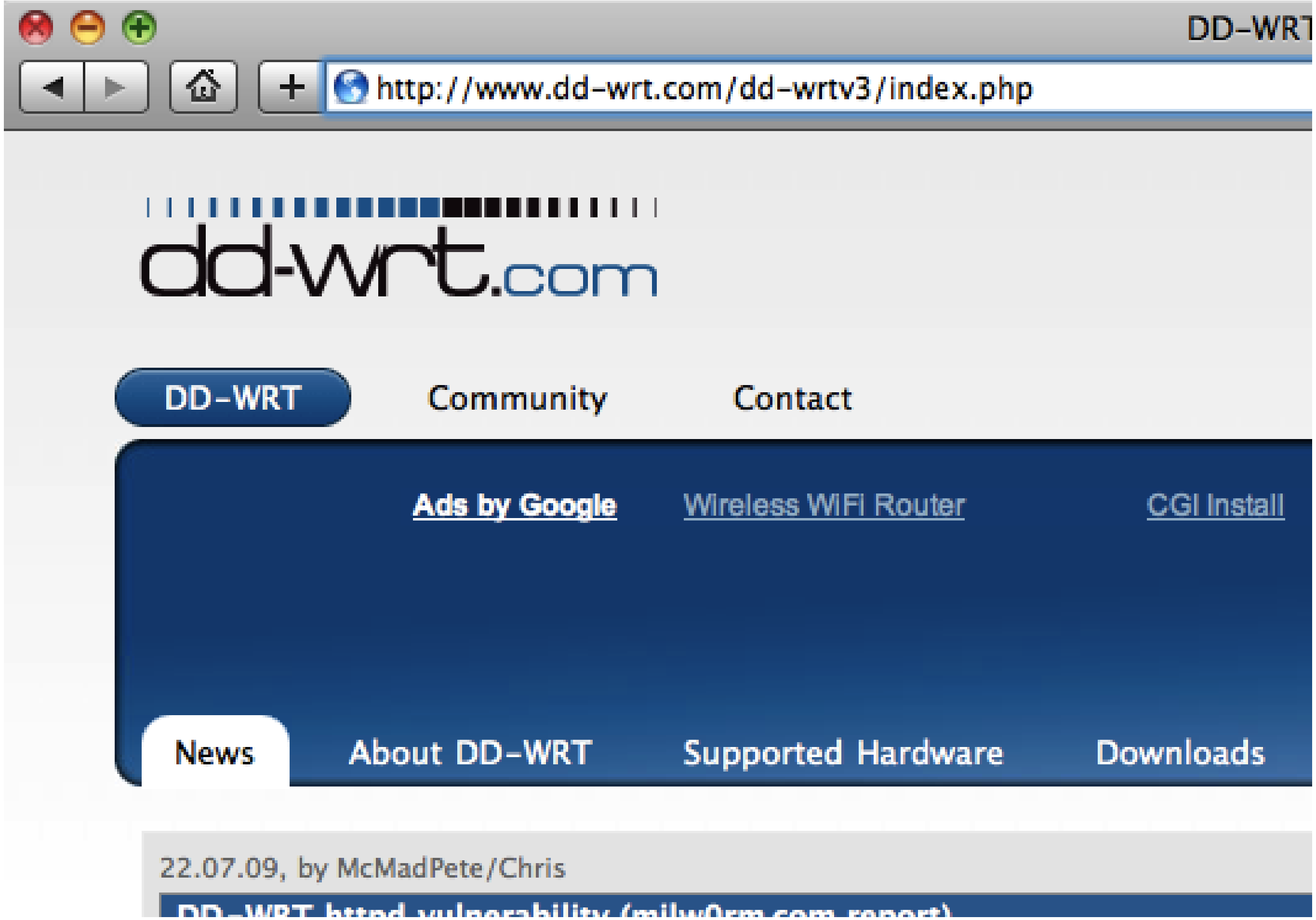
Summary: Traffic | Hosts | Network Load | ASN Info | VLAN Info | NetFlows

Network Load Statistics

Time [Wed Jul 14 20:34:32 2004 through now]

Report created on Wed Jul 14 21:34:32 2004 [ntop uptime: 1:33:01]

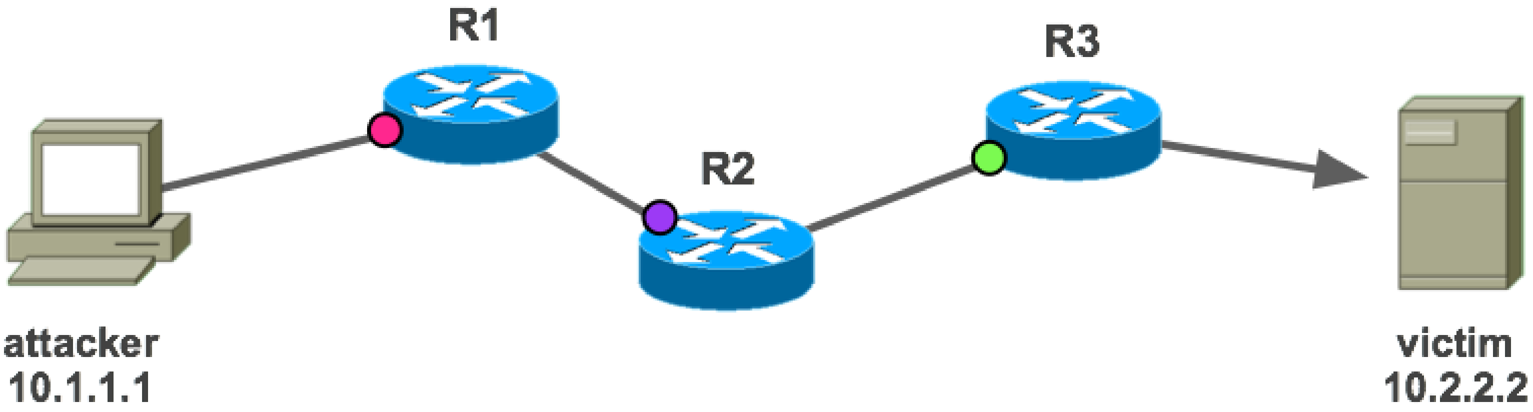
Enable NetFlow on your Linksys router!



22.07.09, by McMadPete/Chris

DD-WRT httpd vulnerability (milw0rm.com report)

Importance of Flow Deduplication



Resulting Duplicate Flows:

● R1: 10.1.1.1 > 10.2.2.2
~~● R2: 10.1.1.1 > 10.2.2.2~~
~~● R3: 10.1.1.1 > 10.2.2.2~~

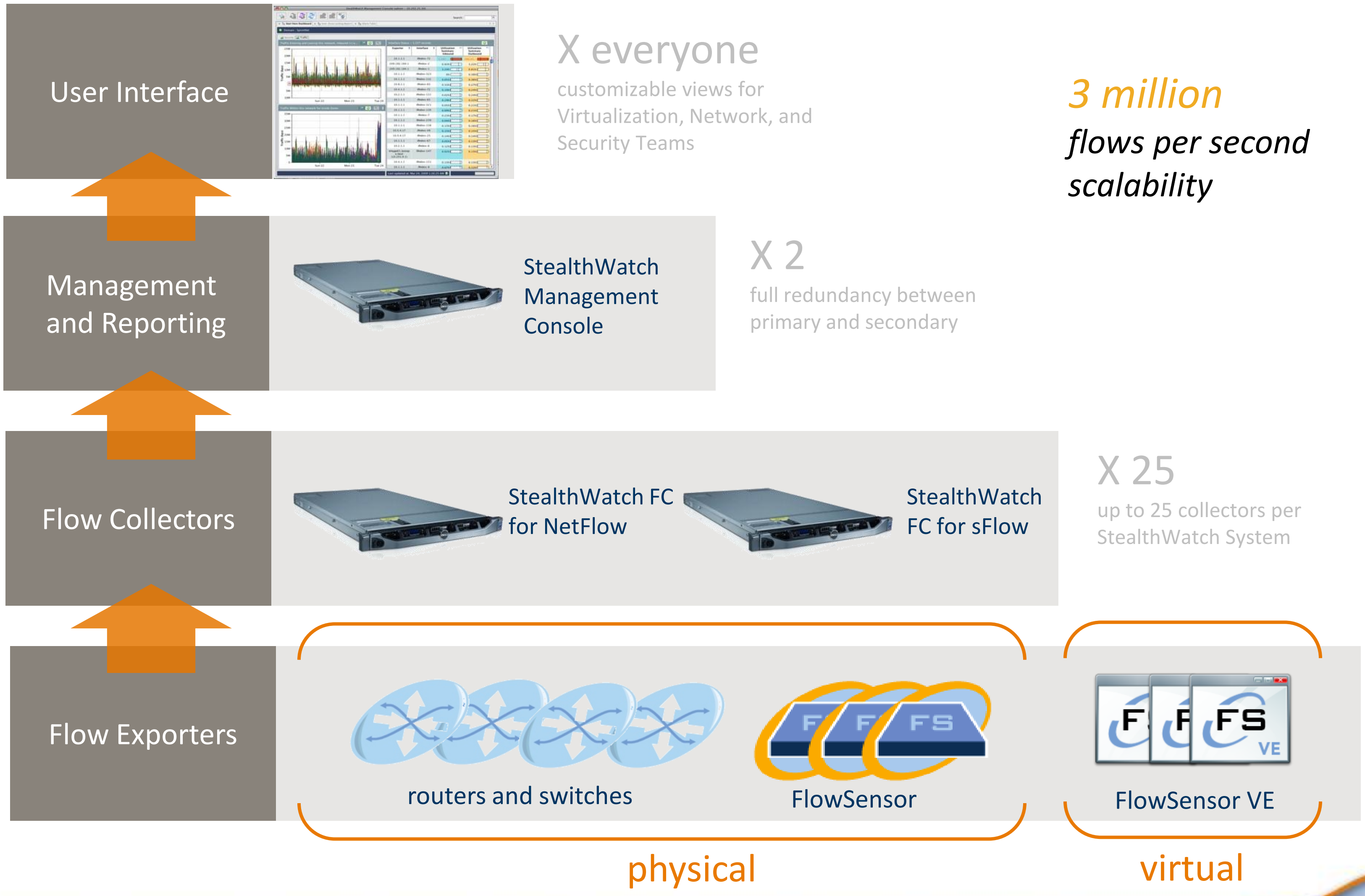
- Deduplication is key in large networks with multiple ingress/egress points
- Without deduplication traffic rates would be misstated and false positives would occur due to the duplicate flows received by the collector

Lancope
Network Performance + Security Monitoring

KNOW YOUR NETWORK.
RUN YOUR BUSINESS.™

Lancope’s StealthWatch NetFlow Collection System

Scalability



User Interface

X everyone
customizable views for Virtualization, Network, and Security Teams

3 million
flows per second scalability

Management and Reporting

StealthWatch Management Console

X 2
full redundancy between primary and secondary

Flow Collectors

StealthWatch FC for NetFlow

StealthWatch FC for sFlow

X 25
up to 25 collectors per StealthWatch System

Flow Exporters

routers and switches

FlowSensor

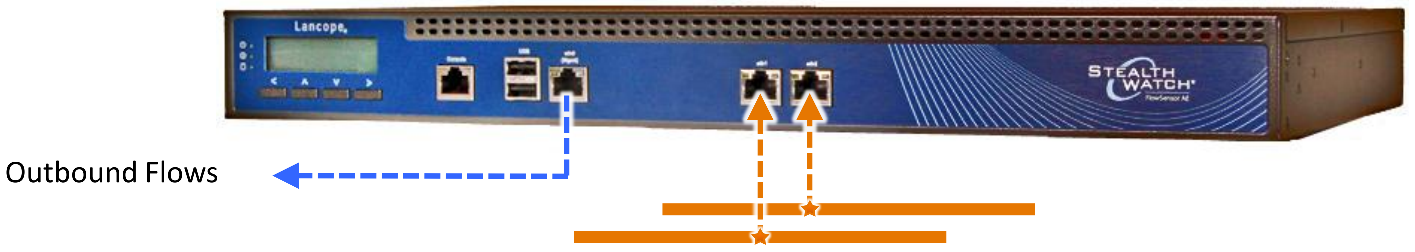
FlowSensor VE

physical

virtual

X 2000
up to 2000 exporters and/or 120,000 flows per second

FlowSensors Work at Layer-2



StealthWatch
FlowSensor

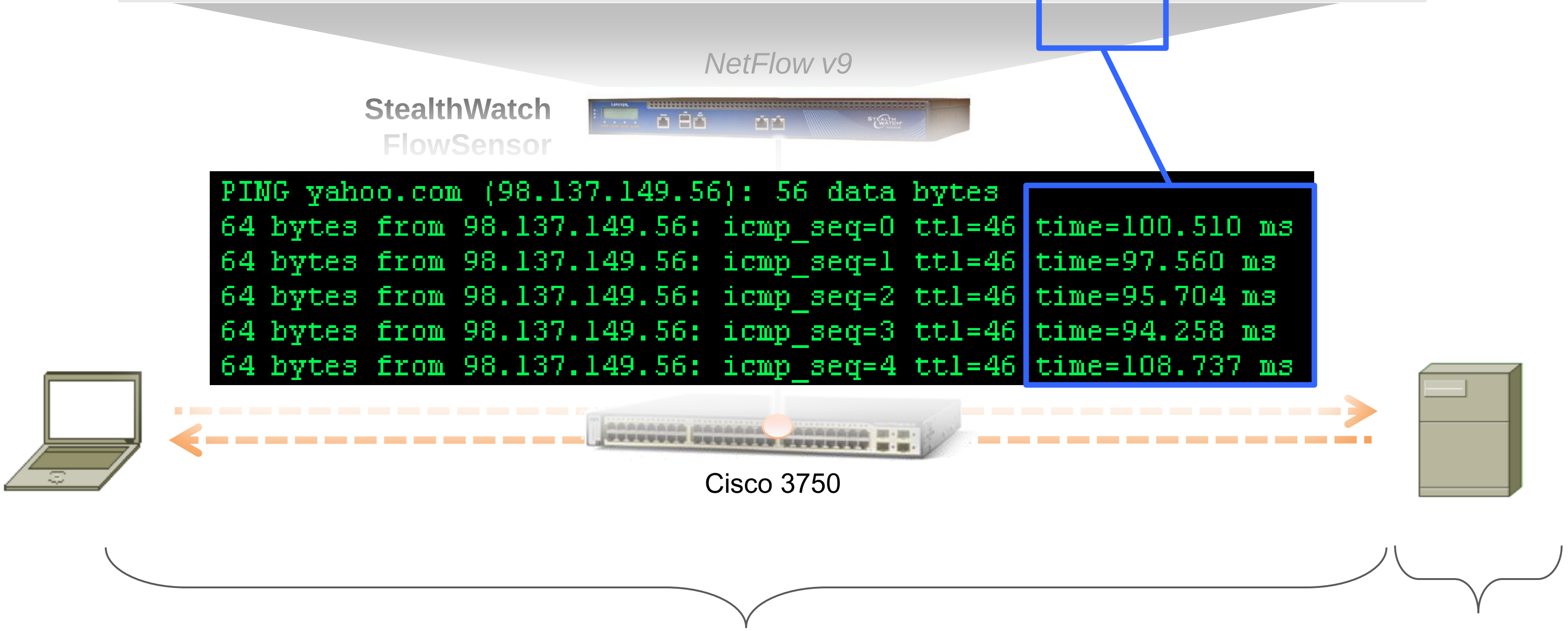
10/100/1000Mbps monitor
ports for mirror/tap/SPAN

- Removes the burden of flow generation from network devices
- Provides NetFlow visibility in areas of the network that don't support NetFlow
- Adds additional details (layer-7 info, latency stats) not found in traditional NetFlow sources

Model	Capacity	Disk	Interfaces
FS-250	100 Mbps	160GB	2
FS-1000	1 Gbps	160GB	3
FS-2000	2.5 Gbps	160GB	3 or 5
FS-3000	5.0 Gbps	160GB	2
FS-VE	-	-	16 vnics

Track Flow Performance Statistics

SRCIP	DSTIP	PROTO	DPORT	SPORT	PKTS	BYTES	RTT	SRT	...
💻	🖥	TCP	80	5749	73	9,092	97ms	2230ms	...
🖥	💻	TCP	5749	80	103	78,020	97ms	2230ms	...



```
PING yahoo.com (98.137.149.56): 56 data bytes
64 bytes from 98.137.149.56: icmp_seq=0 ttl=46 time=100.510 ms
64 bytes from 98.137.149.56: icmp_seq=1 ttl=46 time=97.560 ms
64 bytes from 98.137.149.56: icmp_seq=2 ttl=46 time=95.704 ms
64 bytes from 98.137.149.56: icmp_seq=3 ttl=46 time=94.258 ms
64 bytes from 98.137.149.56: icmp_seq=4 ttl=46 time=108.737 ms
```

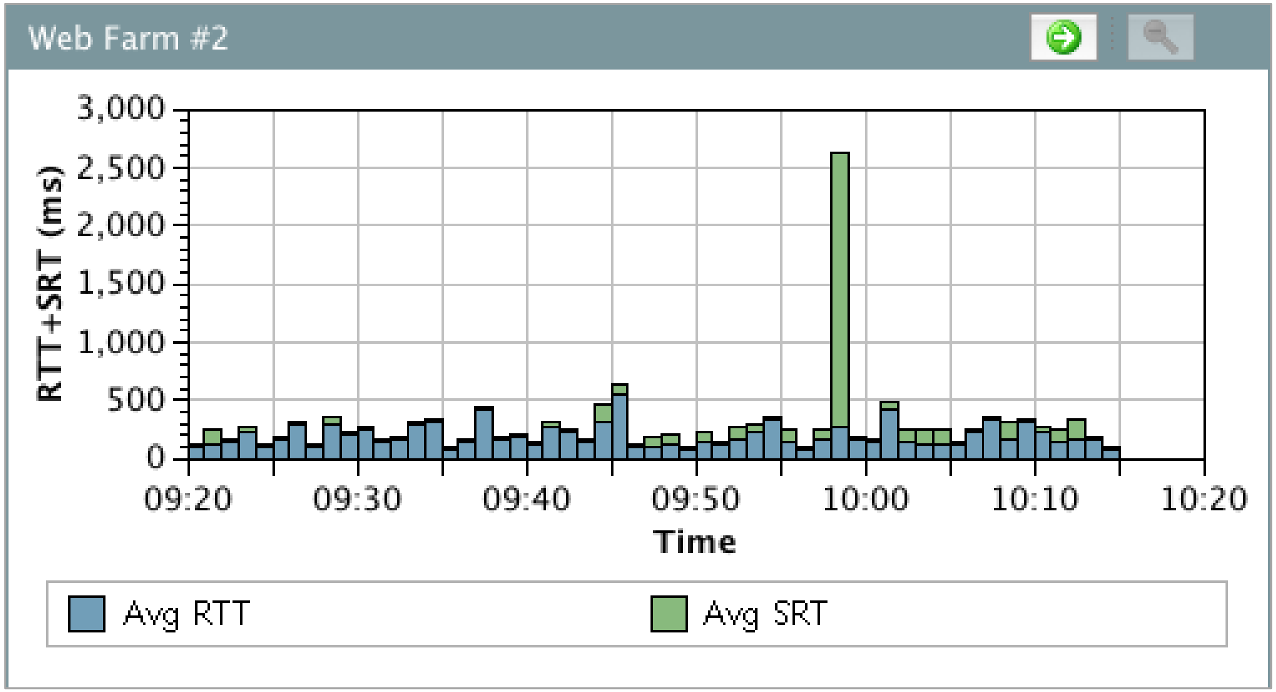
Round Trip Time (RTT): 97ms

Server Response Time (SRT): 2230ms

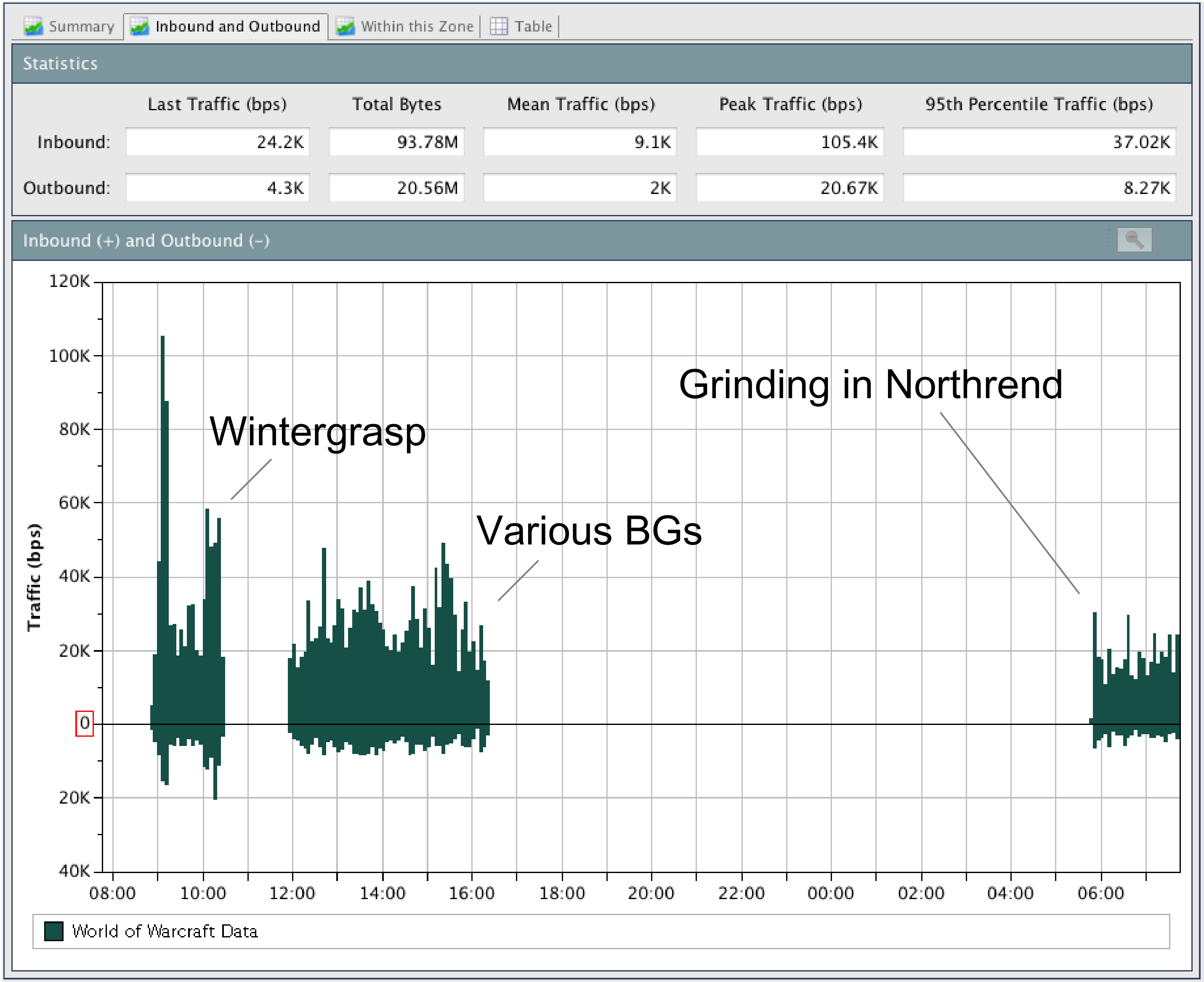
The network or the application?

GARTNER:

> "Through 2012, more than 80% of application performance and availability failures will be blamed on network problems, but the network will represent less than 20% of the root cause."



On a Related Note: World of Warcraft



Statistics

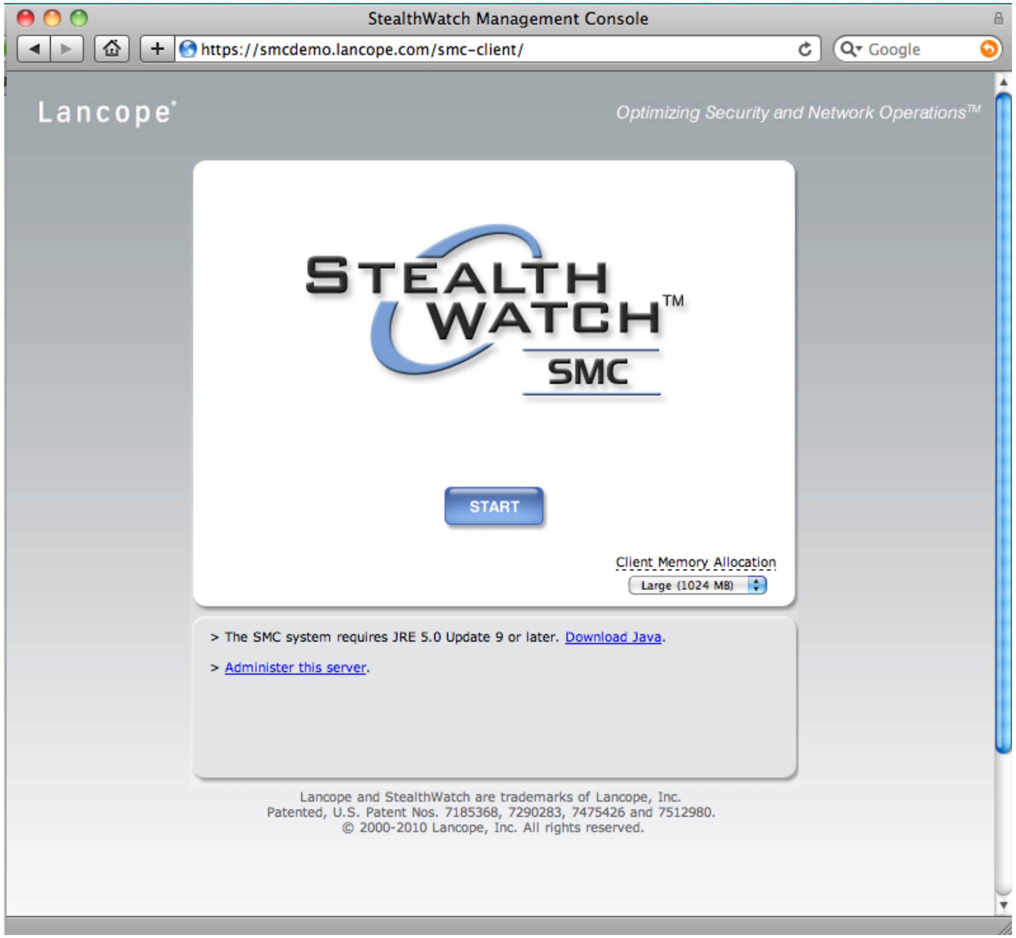
	Last Traffic (bps)	Total Bytes	Mean Traffic (bps)	Peak Traffic (bps)	95th Percentile Traffic (bps)
Inbound:	24.2K	93.78M	9.1K	105.4K	37.02K
Outbound:	4.3K	20.56M	2K	20.67K	8.27K

Wintergrasp

Various BGs

Grinding in Northrend

StealthWatch Lab – Exercises #3, #4, #5



StealthWatch Management Console
https://smcdemo.lancope.com/smc-client/
Google
Lancope
Optimizing Security and Network Operations™
STEALTHWATCH™ SMC
START

Client Memory Allocation

Large (1024 MB)

> The SMC system requires JRE 5.0 Update 9 or later. Download Java.

> Administer this server.

Lancope and StealthWatch are trademarks of Lancope, Inc.
Patented, U.S. Patent Nos. 7185368, 7290283, 7475426 and 7512980.
© 2000-2010 Lancope, Inc. All rights reserved.

Questions and Contact

Sales

sales@lancope.com

Marketing

marketing@lancope.com