



*TOMORROW  
starts here.*

Cisco *live!*



# Cisco CSIRT: Security Analytics and Forensics with NetFlow

BRKSEC-2073

Michael Scheck – CSIRT Investigations Manager

Paul Eckstein – CSIRT Engineering Manager

#clmel

Cisco *live!*

# Agenda

- Heartbleed Use Case
- Netflow Growth
- Deployment
- Problems Solved
- Use Cases
- Conclusion





# Heartbleed

# April 8, 2014: Heartbleed Vulnerability

- The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by SSL



# Cisco CSIRT Response to Heartbleed



- Preparation
  - Scanned 1.2M vulnerable servers - 300 needed repair
  - Helped develop signatures for Sourcefire and Cisco IDS
  - Deployed signatures to IDS
- Monitoring and response
  - Discovered 25 attacks: 21 benign, 4 malicious
  - Researched attack via NetFlow analysis to discern normal connections from those that were anomalous and malicious

# Heartbleed Benign Host

The screenshot displays the Cisco Security Center interface. The main window shows a table with the following columns: Target Host Groups, Target Host, and Concern In. The table is currently empty. On the left side, there is a sidebar with a filter section showing 'Domain : cisco' and 'Host : 200.32.68.4'. Below the filter, there are tabs for 'Table' and 'Short List', and a 'Flow Table - 438 records' section. A small table is visible in the bottom left corner of the sidebar:

Client...	Client Host
	200.32.68.
	200.32.68.
	200.32.68.
	200.32.68.

On the right side, there is a table with the following columns: Server Bytes, First C..., and Ser. The table contains the following data:

Server Bytes	First C...	Ser
852.64k	53922	
684.89k	55555	
561.57k	57011	
287.01k	36962	

# Heartbleed Benign Host

Filter Domain : cisco Time : April 9, 2014  
Host : 82.221.105.7

Identification Alarms Security **CI Events** Top Active Flows Identity, DHCP & Host Notes Exporter Interfaces

Host is Source of CI Events - 43 records

Target Host Groups	Target Host	Concern Index	
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.5.0/24	12,032	Addr_Scan/tcp-443(32)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.4.0/24	6,016	Addr_Scan/tcp-443(16)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.8.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.6.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.10.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.193.0/24	6,012	Addr_Scan/tcp-443(12)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	173.38.2.0/24	3,027	Addr_Scan/tcp-443(27)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.102.4.0/24	3,022	Addr_Scan/tcp-443(22)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.0.0/24	3,011	Addr_Scan/tcp-443(11)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.199.0/24	3,006	Addr_Scan/tcp-443(6)
IPv4, ACL103	192.133.192.0/24	24,048	Addr_Scan/tcp-443(48)
IPv4, ACL103	192.133.190.0/24	18,054	Addr_Scan/tcp-443(54)
IPv4, ACL103	64.104.3.0/24	15,055	Addr_Scan/tcp-443(55)
IPv4, ACL103	64.104.194.0/24	12,024	Addr_Scan/tcp-443(24)
IPv4, ACL103	64.104.192.0/24	12,024	Addr_Scan/tcp-443(24)
IPv4, ACL103	173.39.4.0/24	9,048	Addr_Scan/tcp-443(48)
IPv4, ACL103	64.104.195.0/24	9,018	Addr_Scan/tcp-443(18)
IPv4, ACL103	173.39.14.0/24	6,032	Addr_Scan/tcp-443(32)
IPv4, ACL103	64.104.2.0/24	6,022	Addr_Scan/tcp-443(22)
IPv4, ACL103	72.163.16.0/24	6,016	Addr_Scan/tcp-443(16)
IPv4, ACL103	72.163.1.0/24	6,016	Addr_Scan/tcp-443(16)
IPv4, ACL103	173.37.9.0/24	3,035	Addr_Scan/tcp-443(35)

Client Ratio (%)

66.67%

66.67%

66.67%

66.67%





# Netflow Growth

# NetFlow Overview



Source IP: Port	Destination IP: Port	Packets	Date / Time
192.168.15.7:2068	211.160.17.195:8080	7	3/12/2015 08:15:02 GMT
192.168.21.5:1042	72.18.45.223:21	219	3/12/2015 09:02:51 GMT
192.168.6.22:3161	172.18.15.188:80	1	3/12/2015 09:12:42 GMT

# NetFlow Collection and Analysis Solutions

	OSU FlowTools	Nfdump	Lancope StealthWatch
License	OpenSource from Ohio State	OpenSource from SourceForge	Commercial
NetFlow Versions	V5 and up	V5 and up	V5 and up
IPv6?	Yes	Yes	Yes
Syntax	Command-line, like ACLs	Command-line, like tcpdump	GUI, API
Support	Ad-hoc via Google Code	Up-to-date	Up-to-date

# NetFlow at Cisco Before StealthWatch

- OSU FlowTools
  - 25+ systems running in parallel
    - Speeds up query time, but routers have to point at each collector
- 20+ Tb of physical storage
  - Files were stored in native nfdump/flowtools compressed format
- No flow aggregation
  - Some connections passed through multiple devices, causing **duplicate** flows
  - Routers splitting up long running flows
  - Exporter information obscured by fanout tool

# NetFlow Challenge: Support

- Support of open source tools
- OS support
- Training staff
- Feature requests
- Protocol changes (NetFlow and IP)
- Difficult to monitor for flow loss

# NetFlow Investigation with OSU FlowTools

## Query

```
[myanfchost]$ head bot.acl
ip access-list standard bot permit host 69.50.180.3
ip access-list standard bot permit host 66.182.153.176
```

```
[myanfchost]$ flow-cat /var/local/flows/data/2007-02-12/ft* | flow-filter -Sbot -o -...
```

Start	End	Sif	SrcIPAddress	SrcP	DIf	DstIPAddress	DstP
0213.08:39:49.911	0213.08:40:34.519	58	10.10.71.100	8343	98	69.50.180.3	31337
0213.08:40:33.590	0213.08:40:42.294	98	69.50.180.3	31337	58	10.10.71.100	83

# NetFlow Investigation with OSU FlowTools

## Custom NetFlow report generator

### Netflow Report Generator

click on any of the links above the forms for help, or visit the [FAQ](#).

**Source IP:**   
 Use File for Source

**Time:**

**DNS Resolve:**

**Netflow Collector:**  
all  
charybdis (San Jose)  
rtp-nfc  
ams-nfc  
syd-nfc

**Email address**

**Source Port:**      **Destination IP:**      **Destination Port:**

SOURCE:PORT	(HOSTNAME:DOMAIN:USER)	DESTINATION:PORT	(HOSTNAME:DOMAIN:USER)	PACKETS	TIMESTAMP
64.102.53.34[xianshield.cisco.com]:10872		60.190.23.153 [unknown]:7000		1	1205.21:35:59.
64.102.53.34[xianshield.cisco.com]:48472		61.158.119.94 [unknown]:7000		1	1206.00:18:04.
64.102.53.34[xianshield.cisco.com]:10872		61.152.107.59 [unknown]:7000		1	1206.00:23:00.
64.102.53.34[xianshield.cisco.com]:10872		60.190.23.153 [unknown]:7000		1	1206.03:20:57.
64.102.53.34[xianshield.cisco.com]:48472		61.152.107.59 [unknown]:7000		1	1206.11:15:58.
64.102.53.34[xianshield.cisco.com]:48472		60.190.23.153 [unknown]:7000		1	1206.12:42:48.
64.102.53.34[xianshield.cisco.com]:48472		60.190.23.153 [unknown]:7000		1	1206.12:58:27.



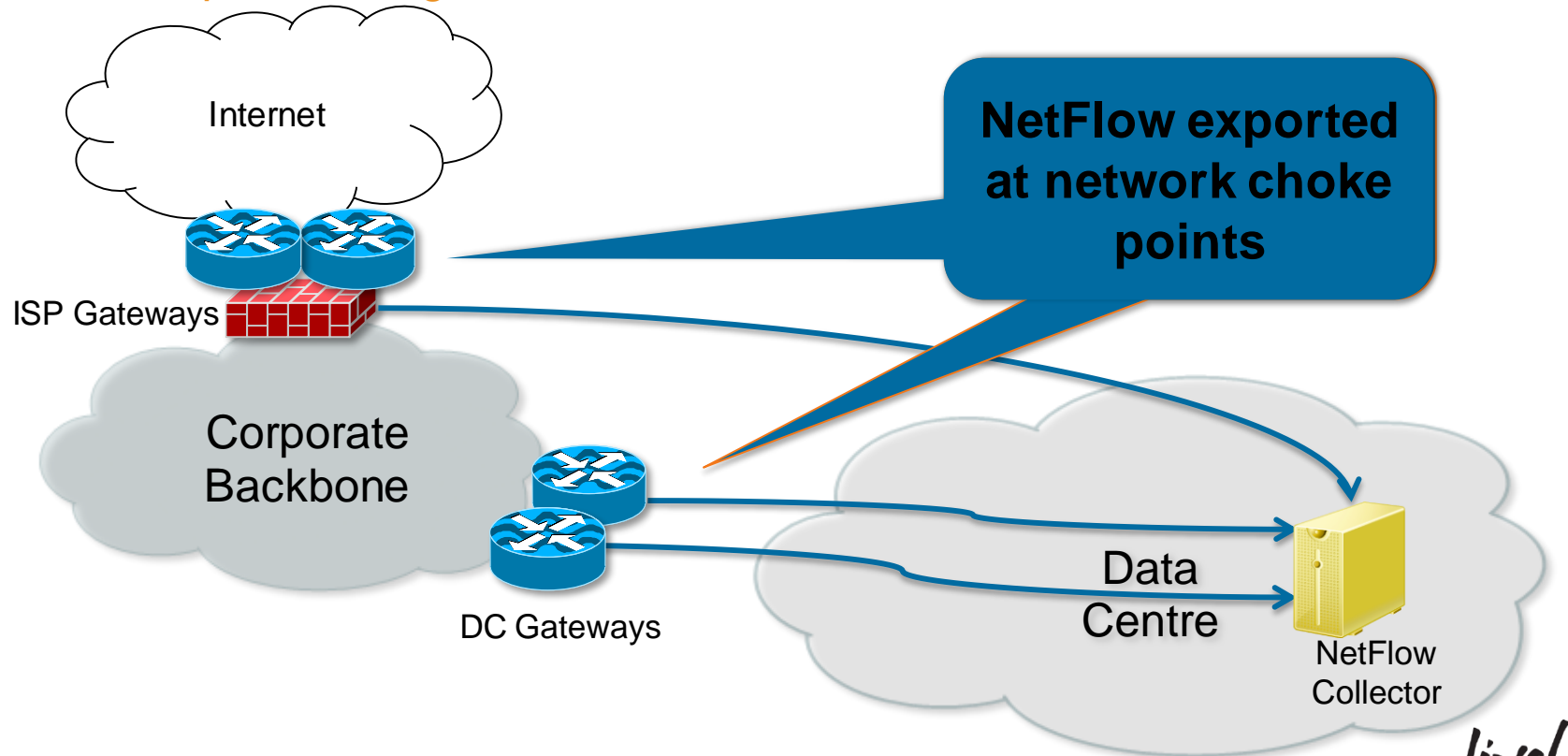
Deployment

Cisco *live!*



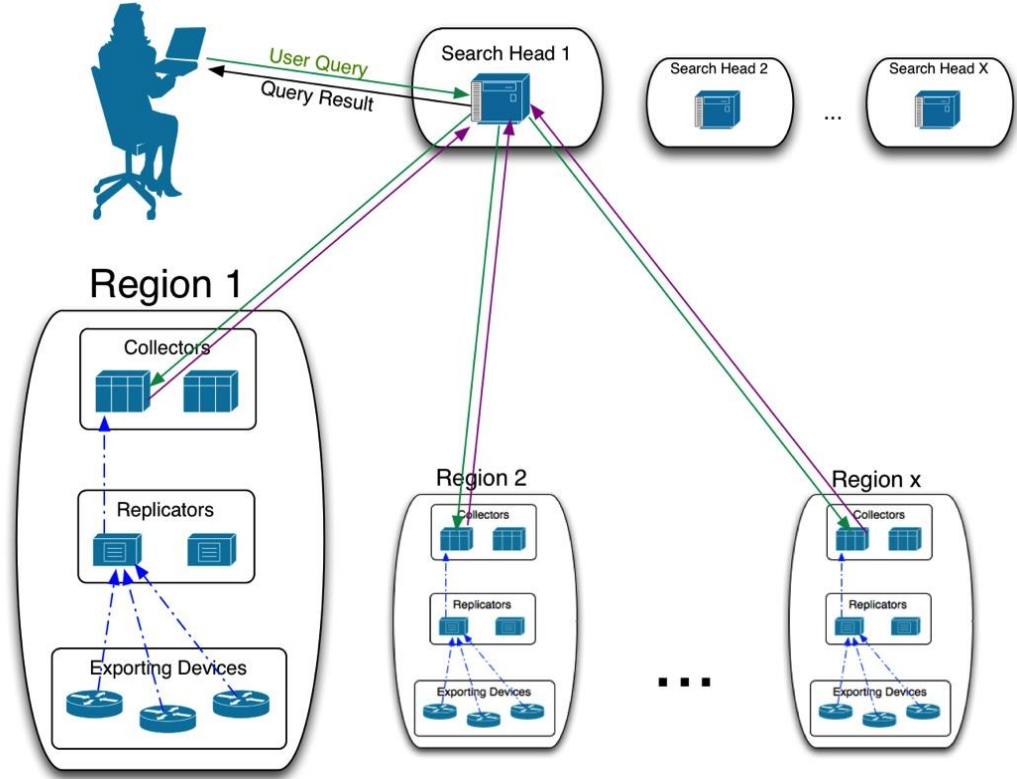
# NetFlow Export at Cisco

Collect at chokepoints for egress detection



# NetFlow Architecture

- Redundant forwarding
- Regional storage
- Global search



# Lancope Devices and Count



Stealthwatch Management Console



FlowSensor

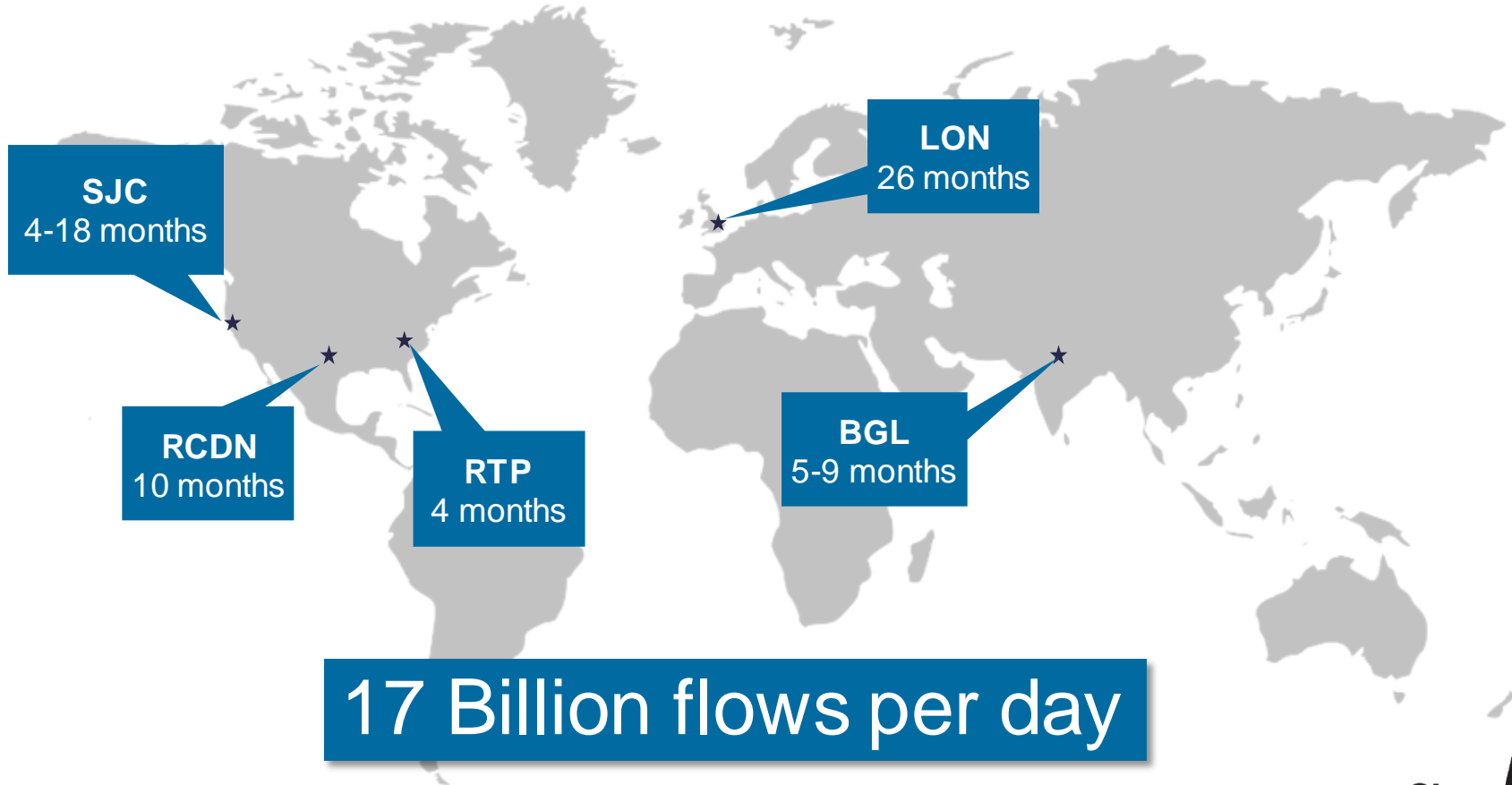


UDP Director



FlowCollector

# NetFlow Retention



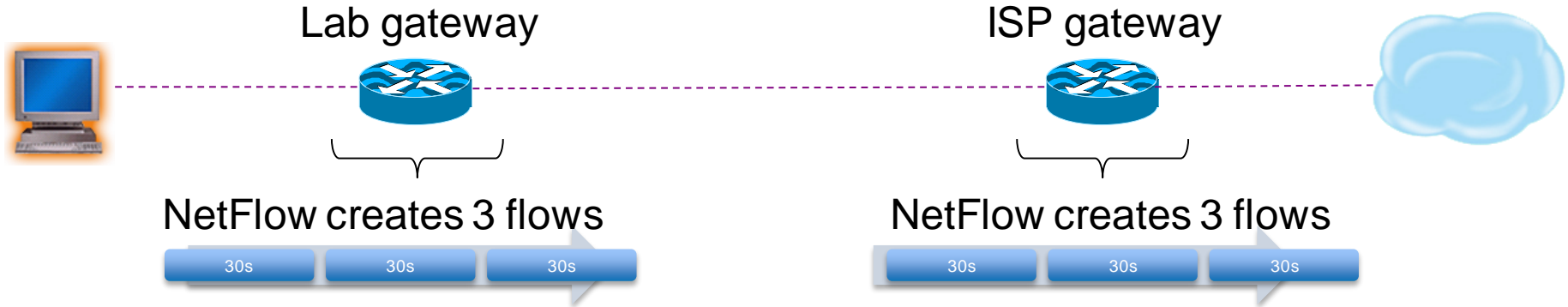


Problems Solved

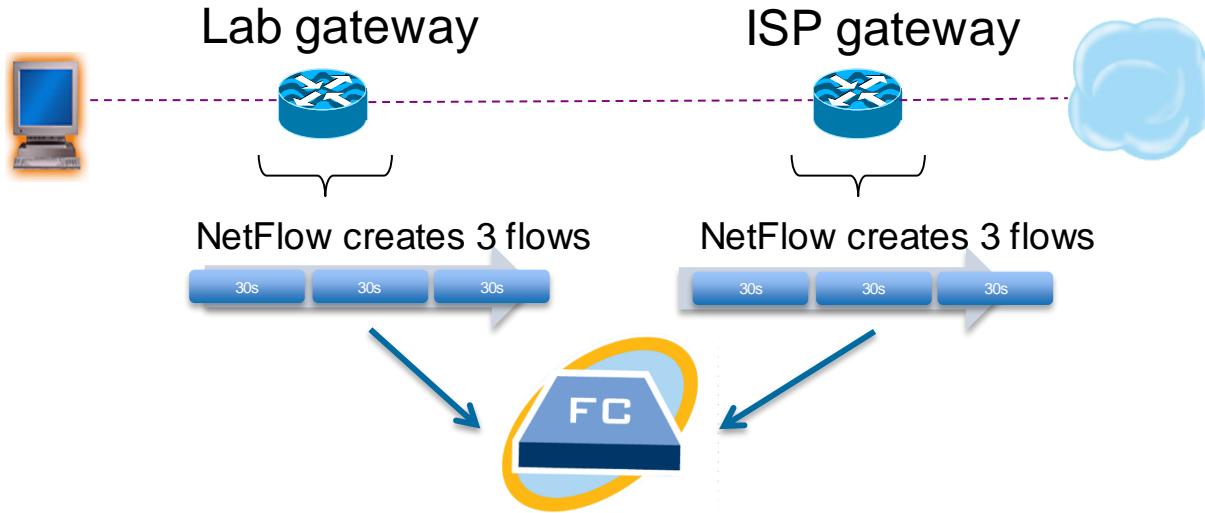
# NetFlow Challenge: Flow Timeouts

**One** 90s flow creates **6 flows**

*30s timeout  $90/30 = 3 \times 2$  collectors*



# Business Benefit #1 Storage Capacity



Exporter	Exporter T...	Interface	Direction	TTL	DSCP	Flow Action
gwy03-dc-gw1.cisco.com (10.53.41.4)	Exporter	ifIndex-1	Outbound			
gwy03-dc-gw1.cisco.com (10.53.41.4)	Exporter	ifIndex-61	Inbound		best_effort	

Exporter	Exporter T...	Interface	Direction	TTL	DSCP	Flow Action
gwy03-dc-gw2.cisco.com (10.53.41.5)	Exporter	ifIndex-2	Inbound		best_effort	
gwy03-dc-gw2.cisco.com (10.53.41.5)	Exporter	ifIndex-61	Outbound			

# Business Benefit #2 Ease of Support

- IPv4/IPv6 both supported
- Netflow v5/v9 both supported
- All supported on the same system, on the same port!
- No system administration required
- Alarms built in for monitoring of lost flows

Filter Domain : cisco Time : Today  
Appliances : 16 Devices

Summary

	Interface Count	Current NetFlow Traffic (bps)	Average NetFlow Traffic (bps)	Maximum NetFlow Traffic (bps)	Average Flow Rate (fps)	Total Flows
sjc12-swath-1:	81	3.39k	4.21M	8.57M	10.37k	497.04M
sjc12-swath-2:	782	0	1.39M	5.44M	2.19k	104.55M
bgl11-swath-1:	342	2.83M	5.89M	10.49M	14.57k	698.24M
rcdn9-swath-1:	389	10.5M	9.7M	16.44M	24.57k	1.18G
rt5-swath-2:	852	891.59k	1.15M	2.41M	2.89k	138.1M
bgl11-swath-2:	586	4.4M	5.5M	9.23M	8.62k	412.72M
sjc12-swath-3:	864	0	3.2M	7.51M	8.42k	378.15M
rcdn9-swath-2:	1.63k	10.48M	4.2M	18.12M	10.38k	496.19M
webex-swath-1:	418	15.76M	6.1M	27.27M	13.01k	621.96M
nap4-swath-1:	65	1.64M	1.18M	2.52M	3.28k	137.56M
mtv5-swath-1:	550	21.87M	21.39M	51.58M	64.49k	3.09G
nds-bgl43-dmz-lcfc-1:	1	17.33k	17.96k	31.03k	24	1.11M
sv4-swath-1:	21	50	16	249	2	2.06k
lon3idc-dc-swath-1:	5	11.83M	14.45M	18.08M	9.4k	448.86M
rt5-swath-1:	503	11.02M	8.06M	15.78M	20.25k	969.14M
nds-jrsm01-dmz-lcfc-1:	1	415.38k	595.6k	907.2k	731	35M

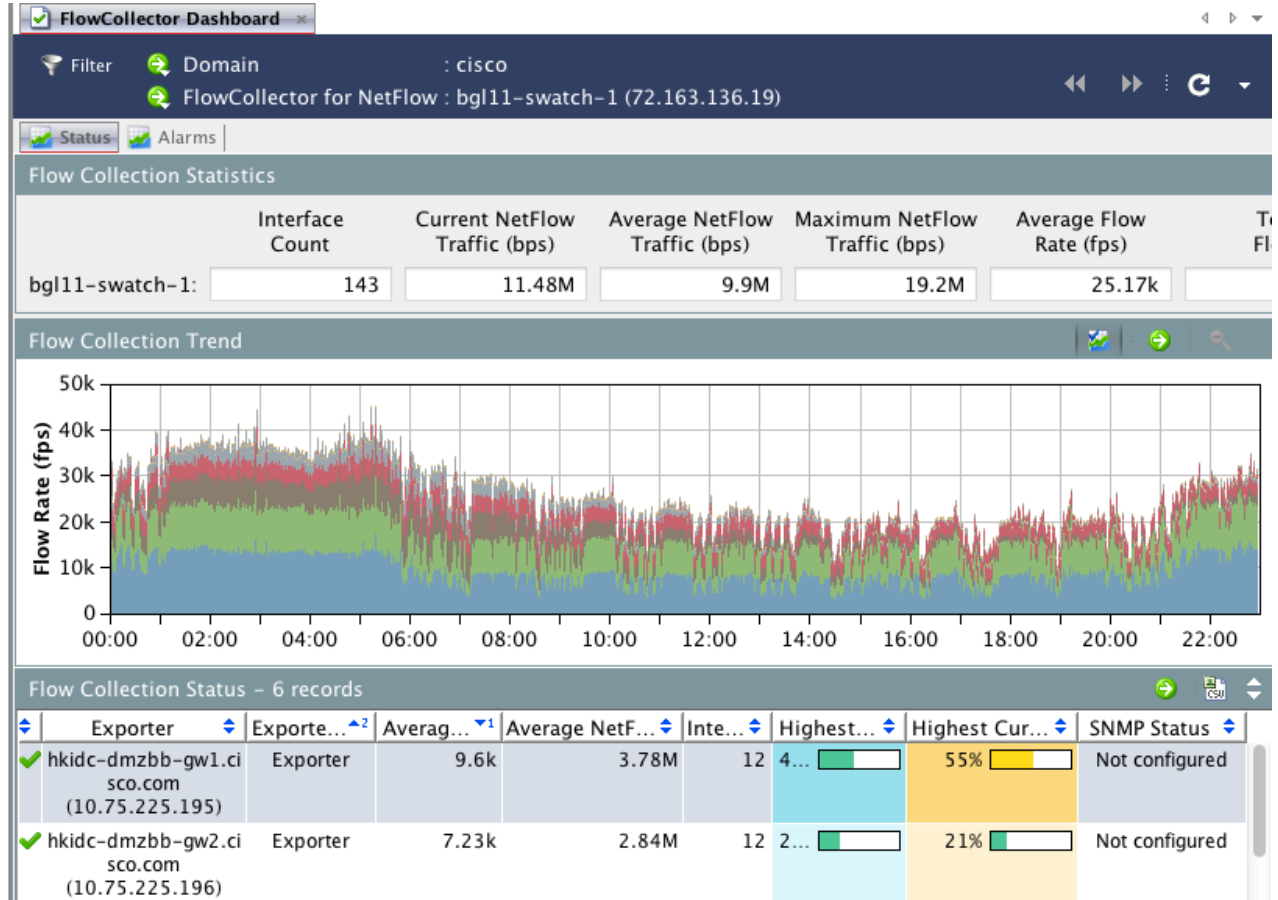
Details - 514 records

...	Exporter	Exporter Type	Flow Type	Average Flo...	Average NetFlow...	Interfa...	Highest Cur...	Highest Current...	SNMP Status
!	Unknown Exporter (10.53.35.91)	Unknown	IPFIX	9.4k	14.45M	3	21%	0%	
!	shnidc-wbb-gw2.cisco.co	Exporter	NetFlow v9	8.35k	2.52M	6	29%	0%	Not configured



# Business Benefit #3 Ease of Use

- Enterprise
  - SMC (Primary)
  - SMC Failover (Secondary)
  - cisco
    - Host Groups
      - Inside Hosts
      - Outside Hosts
      - jbolling-test2
    - Network Devices
    - VM Servers
    - Maps
    - FlowCollectors
      - bgl11-swatch-1**
      - bgl11-swatch-2
      - lon3idc-dc-swatch-1
      - mtv5-swatch-1
      - rcdn9-swatch-1
      - rcdn9-swatch-2
      - rtp5-swatch-1
      - rtp5-swatch-2
      - sjc12-swatch-1
      - sjc12-swatch-2
      - sjc12-swatch-3
      - webex-swatch-1
    - Identity Services
    - External Devices
  - Mobile Monitoring



# Flow Table Query

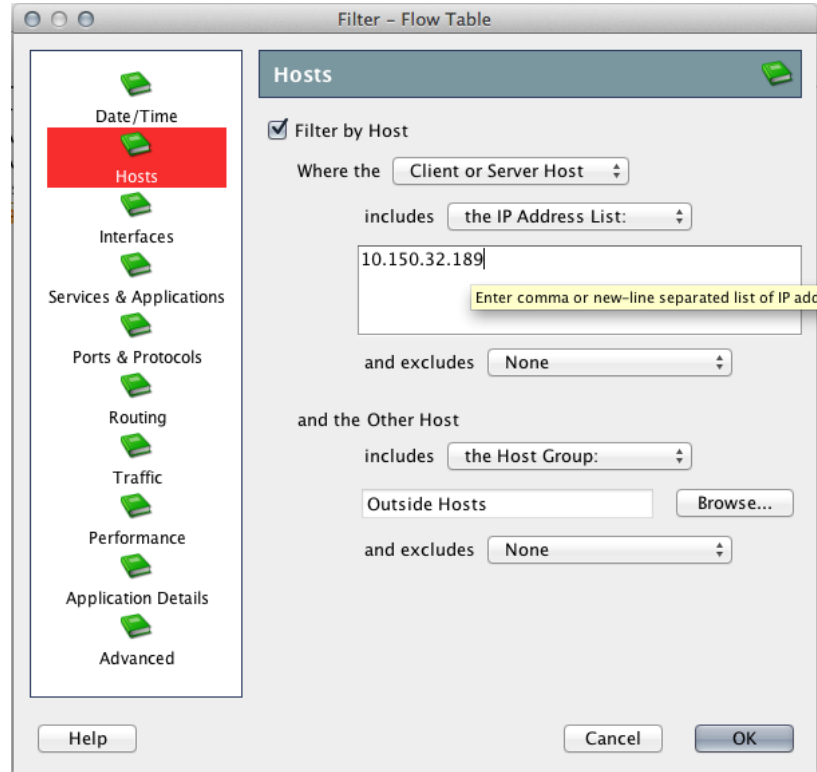
- Other variables: host groups, time range, interfaces, ports
- Defaults to 2000 flow records returned
- Much simpler than syntax for CLI (example below)

## 1. Create a file called 'flow.acl' with a named access list:

```
linux-machine# cat ip access-list standard botnet permit ip 10.31.33.7 >flow.acl
```

## 2. Run a query for the time period you are interested in using the ACL

```
linux-machine# flow-cat /var/local/flows/data/2006-12-01/ft*  
| flow-filter -f ~/flow.acl -Sbotnet -o -Dbotnet | flow-  
print -f5
```



# Flow Table Output

Filter Domain : cisco ● Time : Last 2 hours 5 minutes  
 Client or Server Host : dhcp-10-150-32-189.cisco.com (10.150.32.189)  
 Client or Server Host Group : Outside Hosts

Table  Short List

Flow Table – 148 records

Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application	Service Summary	Total Tr...	Total Bytes
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	74.125.228.33	United States	5 minutes 11s	HTTP (unclassified)	http (80/tcp)	4.21k	159.95k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	69.171.237.16	United States	17 minutes 50s	HTTP (unclassified)	http (80/tcp)	1.03k	134.28k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	199.47.216.147	United States	2 hours 8 minutes 3s	HTTP (unclassified)	http (80/tcp)	101	91.39k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	31.13.76.26	Ireland, IANA Reserved	5 minutes 11s	HTTP (unclassified)	http (80/tcp)	1.99k	75.53k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	74.125.228.44	United States	5 minutes 10s	HTTP (unclassified)	http (80/tcp)	1.92k	72.56k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	23.67.250.154	IANA Reserved, United States	8 minutes 21s	HTTP (unclassified)	http (80/tcp)	1.13k	69.35k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	lad23s05-in-f12.1e100.net (74.125.228.12)	United States	5 minutes 4s	HTTP (unclassified)	http (80/tcp)	1.81k	67.12k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	205.188.7.243	United States	2 hours 9 minutes 12s	HTTPS (unclassified)	https (443/tcp)	68	62.01k



# FlowTable Results

Flow Summary x Security and Traffic Overview x Flow Summary

Domain: cisco Active Time: From Jun 7, 2010 5:10:00 PM to Jun 7, 2010 5:11:00 PM

Client or Server Zone: Inside Zones

Client Hosts Server Hosts Services Conversations

Conversation - 2,000 records

Client Zone	Client Host	Server Zone	Server Host	Flow Count	From Server (bps)	To Client (bps)	Server Traffic (bps)	Adjusted Total (bps)
IN	rtp5-dmz-wsa-1.cisco.com (64.102.249.6)	United States	rdc-024-025-026-041.southeast.st.rr.com (24.25.26.41)	1	855.25k	21.96k	833.29k	41.6M
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States	rdc-024-025-026-032.southeast.st.rr.com (24.25.26.32)	1	789.79k	38.16k	751.63k	40.38M
IN	rtp10-dmz-wsa-2.cisco.com (64.102.249.9)	United States	208.111.161.254	1	757.32k	35.25k	722.07k	39.47M
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States	rdc-024-025-026-116.southeast.st.rr.com (24.25.26.116)	1	705.75k	77.99k	627.76k	35.95M
IN	lwr02-00-acns-ce1.cisco.com (64.100.144.8)	United States	rdc-024-025-026-049.southeast.st.rr.com (24.25.26.49)	1	855.25k	21.96k	833.29k	30.59M
IN	rtp5-dmz-wsa-1.cisco.com (64.102.249.6)	United States	rdc-024-025-026-032.southeast.st.rr.com (24.25.26.32)	1	789.79k	38.16k	751.63k	28.24M
IN	rtp10-dmz-wsa-2.cisco.com (64.102.249.9)	United States	208.111.161.254	1	757.32k	35.25k	722.07k	27.08M
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States	rdc-024-025-026-116.southeast.st.rr.com (24.25.26.116)	1	705.75k	77.99k	627.76k	25.24M
IN	lwr02-00-acns-ce1.cisco.com (64.100.144.8)	United States	rdc-024-025-026-049.southeast.st.rr.com (24.25.26.49)	1	855.25k	21.96k	833.29k	25.24M
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States	rdc-024-025-026-032.southeast.st.rr.com (24.25.26.32)	1	789.79k	38.16k	751.63k	25.24M
IN	rtp-ksalhoff-8719.cisco.com (10.116.34.74)	IANA Reserved	184.50.211	1	456.77k	23.83k	432.93k	17.44M
IN	dhcp-64-102-220-150.cisco.com (64.102.220.150)	United States	184.50.211	1	456.77k	23.83k	432.93k	17.26M
IN	smokehouse.cisco.com (64.102.19.208)	IANA Reserved	184.50.211	1	456.77k	23.83k	432.93k	17.05M
IN	rtp10-dmz-wsa-2.cisco.com (64.102.249.9)	United States	rdc-024-025-026-049.southeast.st.rr.com (24.25.26.49)	1	855.25k	21.96k	833.29k	16.95M
IN	rtp5-dmz-wsa-2.cisco.com (64.102.249.9)	United States	rdc-024-025-026-049.southeast.st.rr.com (24.25.26.49)	1	855.25k	21.96k	833.29k	16.95M

Server, DNS, and Country

United States

rdc-024-025-026-041.southeast.st.rr.com  
(24.25.26.41)

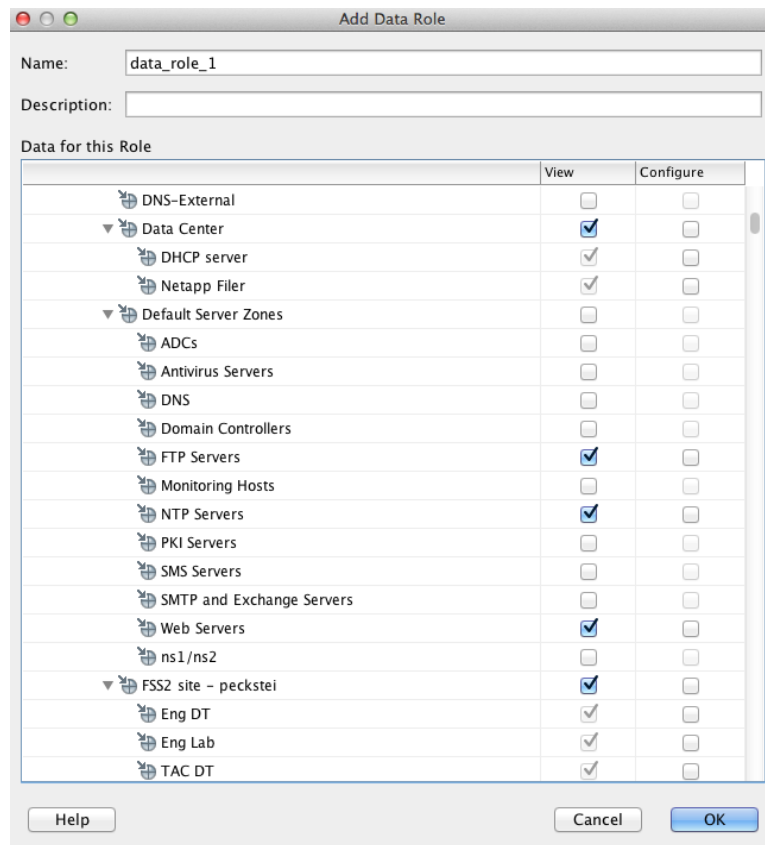
Service Summary	Flow Count	Total Traffic (bps)
http (80/tcp)	1	1.16M

Traffic Type & Volume



# Role Based Access

- Twofold restriction
  - Functional roles: configure appliances, policies, etc.
  - Data roles: view/edit x, y, z host groups
- Notes
  - Granular data restriction
  - No audit log of configuration changes!
  - CSIRT manages all SMC access and privileges



# NetFlow Challenge: Limited Detection Capability

- No concept of host groups for query
- Effective for forensics
- Can do basic DOS detection
- Any other queries required writing algorithms



# Business Benefit #4: Analytics

**Suspected Data Loss**

**High File Sharing Index**

**Max Flows Served**

Start Active Time	Alarm	Source	Source Host Groups	Details	Target	Target Host Groups
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	Suspected Data Loss	[Redacted]	Private Addresses, CRDC-VPN, CRDC-LAB	Observed 40.62M bytes. Expected 2.99M bytes, tolerance of 50 allows up to 10M bytes.	Multiple Hosts	
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	New Flows Served	Multiple Hosts		Observed 2.05k flows. Expected 1 flows, tolerance of 50 allows up to 1k flows.	83.218.20.202	United Kingdom
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	High File Sharing Index	[Redacted].cisco.com	Private Addresses, [Redacted]	Observed 61.75k points. Expected 24.96k points, tolerance of 50 allows up to 58.71k points. (Double-click for details)	Multiple Hosts	
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	High File Sharing Index	[Redacted].cisco.com	Private Addresses, [Redacted]	Observed 58.25k points. Expected 7.62k points, tolerance of 50 allows up to 50k points. (Double-click for details)	Multiple Hosts	
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	New Flows Served	Multiple Hosts		Observed 4.28k flows. Expected 16 flows, tolerance of 50 allows up to 4.09k flows.	91.205.41.182	United Kingdom
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	Max Flows Served	Multiple Hosts		Observed 4.13k flows. Expected 14 flows, tolerance of 50 allows up to 4.12k flows.	91.205.41.182	United Kingdom
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	Max Flows Served	Multiple Hosts		Observed 2.94k flows. Expected 2.05k flows, tolerance of 50 allows up to 2.91k flows.	[Redacted].cisco.com	ACL103, IPv4
Apr 13, 2012 11:30:09 AM (2 minutes 11s ago)	Suspect Data Loss	[Redacted]	Private Addresses, CRDC-VPN, CRDC-LAB	Observed 44.51M bytes. Expected 3.27M bytes, tolerance of 50 allows up to 13.67M bytes.	Multiple Hosts	
Apr 13, 2012 11:30:04 AM (2 minutes 16s ago)	High File Sharing Index	[Redacted].cisco.com	[Redacted], IPv4	Observed 114.61k points. Expected 30.6k points, tolerance of 50 allows up to 114.61k points.	Multiple Hosts	



# Use Cases

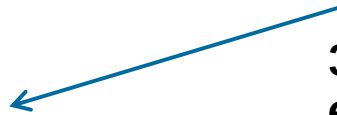


# NetFlow CNC Discovery

**1. Detect host communicating with external Command-and-Control**

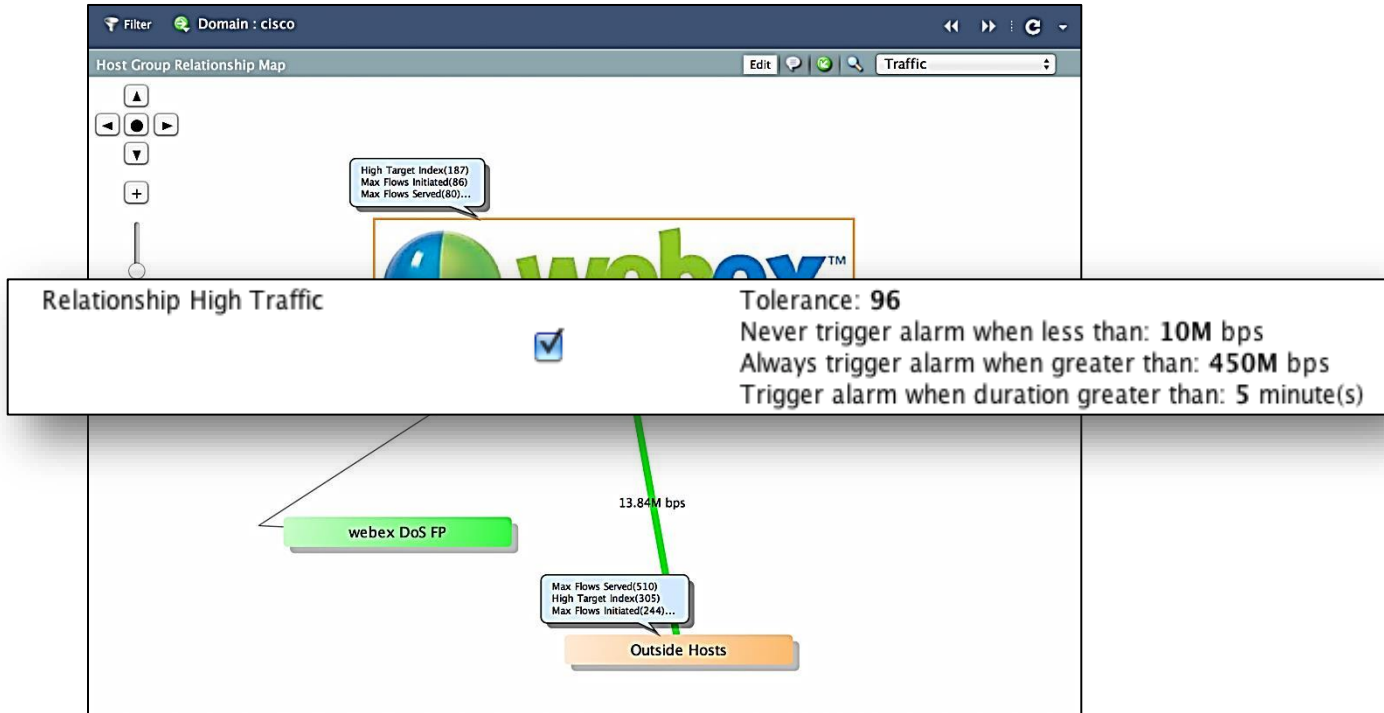


**2. Investigate other internal hosts communicating with the same CnC**

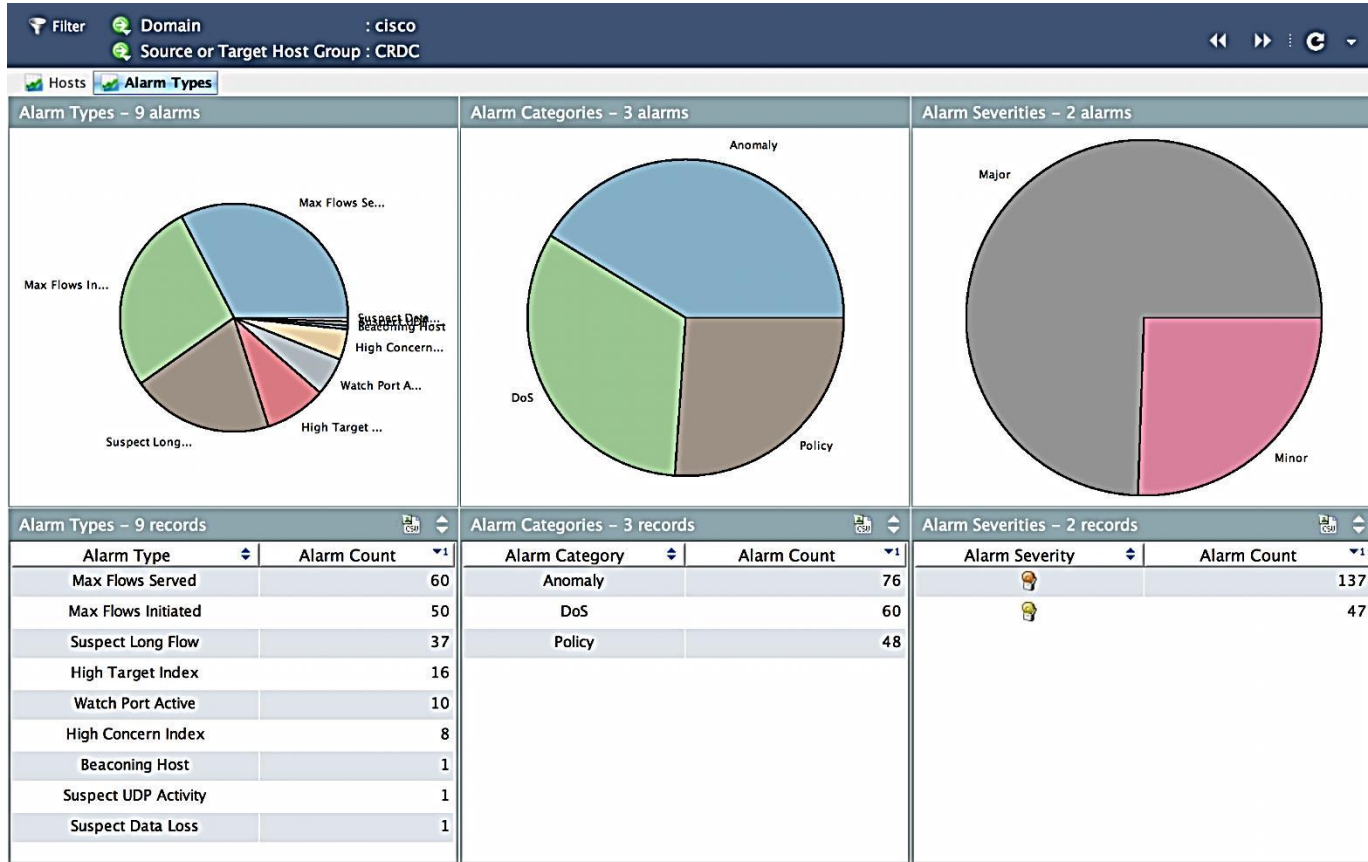


**3. Uncover other malicious, external entities from the compromised hosts**

# Targeted Monitoring: DoS Detection

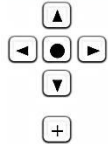


# Targeted Monitoring: DoS Detection



# Targeted Monitoring – Data Loss

Host Group Relationship Map Edit 🗨 🟢 🔍 Traffic



Max Flows Served(59)  
Max Flows Initiated(50)  
Watch Port Active(19)...

CRDC

Alarm <span>▲1</span>	Enabled <span>⬇</span>	Settings	Mitigation <span>⬇</span>
Suspect Data Loss	<input checked="" type="checkbox"/>	Tolerance: 50 Never trigger alarm when less than: <b>10M</b> client payload bytes in 24 hours Always trigger alarm when greater than: <b>500M</b> client payload bytes in 24 hours	None

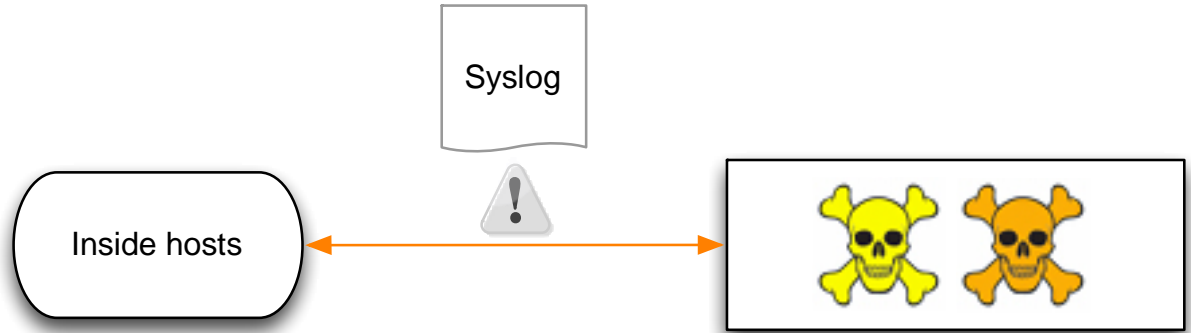
28.28M bps

Max Flows Served(510)  
High Target Index(309)  
Max Flows Initiated(244)...

Outside Hosts

# StealthWatch Host Locking

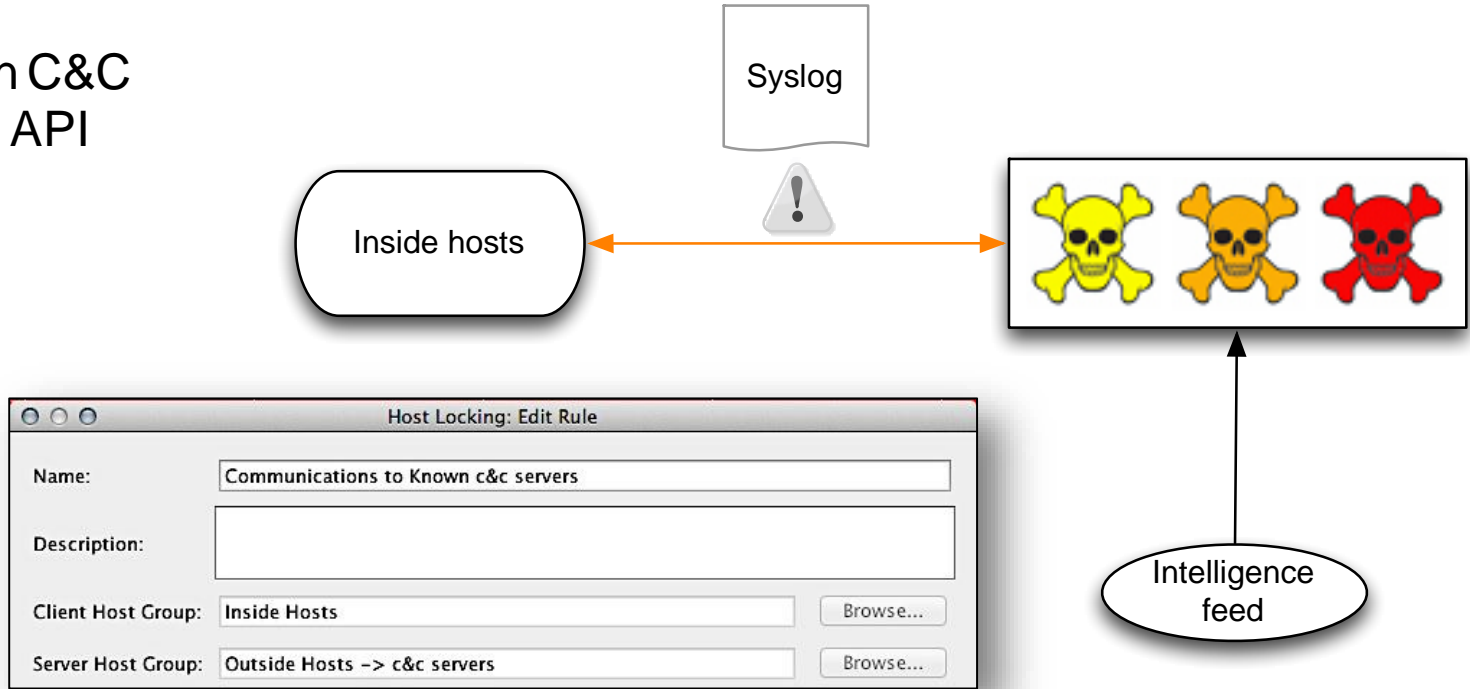
Send syslog for any traffic seen between inside hosts and known C&C servers



The screenshot shows the "Host Locking: Edit Rule" configuration window. The "Name" field is set to "Communications to Known c&c servers". The "Description" field is empty. The "Client Host Group" is set to "Inside Hosts" with a "Browse..." button. The "Server Host Group" is set to "Outside Hosts -> c&c servers" with a "Browse..." button.

# StealthWatch Host Locking

Modify known C&C server list via API



### Top Backdoors

Name	Samples
<a href="#">DPD</a>	1
<a href="#">PIVY</a>	

### Top Campaigns

Name	Emails	Indicators	Samples
<a href="#">Group 3</a>	0	2067	1
<a href="#">Group 17</a>	0	818	11
<a href="#">Group 16</a>	0	68	0
<a href="#">Group 13</a>	0	13	0
<a href="#">Group 10</a>	0	0	0

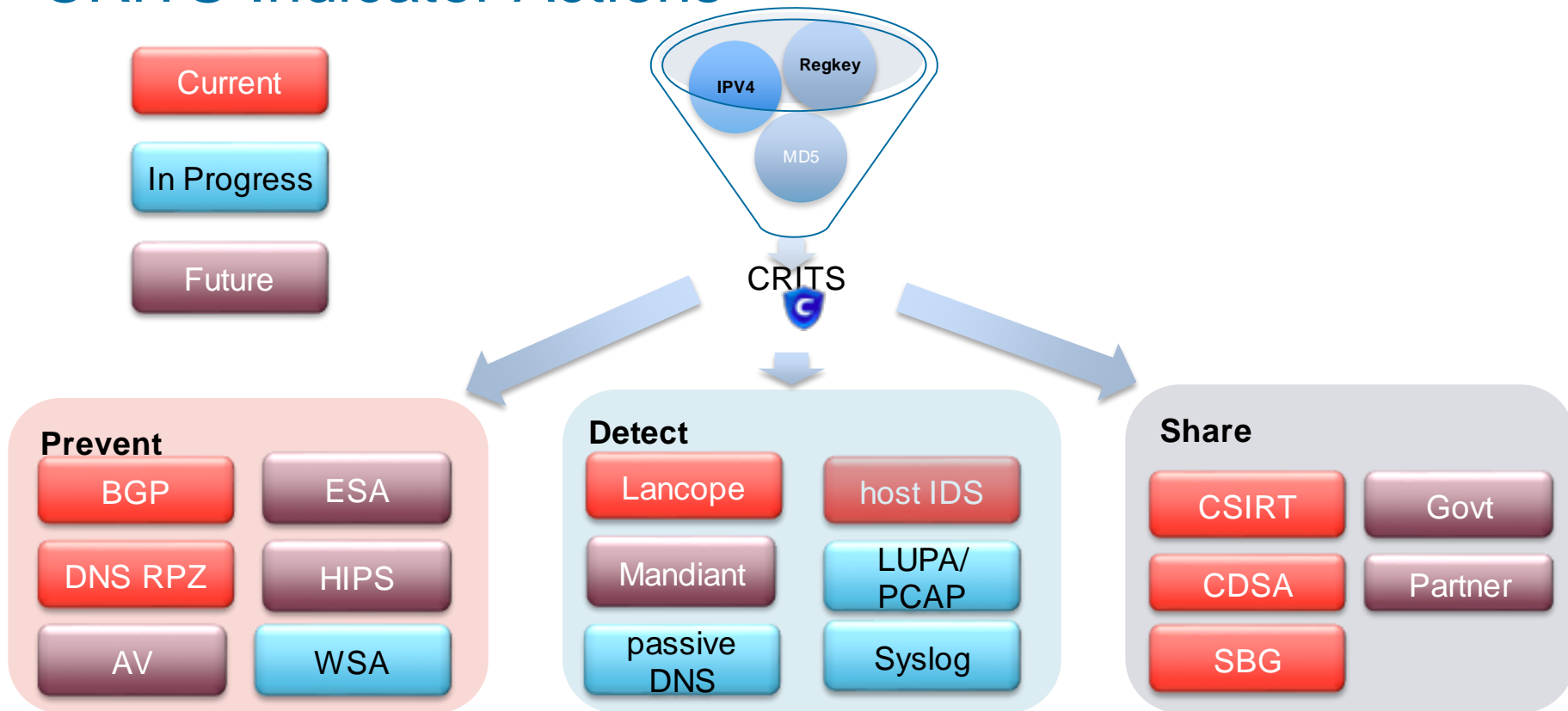
### Latest Indicators

Value	Type	Date Added	Campaign	Source	Status
<a href="#">mx.xmlflash.net</a>	<a href="#">Domain</a>	2013-11-14	<a href="#">Group 3</a>	<a href="#">OTHER</a>	New
<a href="#">www.nbsd.k12.ms.us</a>	<a href="#">Domain</a>	2013-11-14	<a href="#">Group 4</a>	<a href="#">OTHER</a>	New
<a href="#">/serv/pte.exe</a>	<a href="#">Domain</a>	2013-11-14	<a href="#">Group 4</a>	<a href="#">OTHER</a>	New
<a href="#">www.myspace-login.com</a>	<a href="#">Domain</a>	2013-11-14	<a href="#">Group 4</a>	<a href="#">OTHER</a>	New
<a href="#">2014 individual income tax credit policy</a>	<a href="#">String</a>	2013-11-14	<a href="#">Group 4</a>	<a href="#">OTHER</a>	New

### Recently Added/Modified Samples

Filename	Size	Filetype	Receive	Backdoor(v)[C]	CVE
<a href="#">jack246.exe</a>			08/12/2013		
<a href="#">Sample 60eed7a7c5f4f4aeeace594e2e4d180a0.exe_carver</a>			08/12/2013		
<a href="#">c5eb1cff314e4d682b1315dfab44e7dd</a>			08/12/2013		
<a href="#">Sample 68aee94684ba33d1e5d97d7d27d0fe13.exe_carver</a>			08/12/2013		

# CRiTS Indicator Actions





# CRiTs Netflow Alarms

Network Security Alarm Summary

Active High Concern Hosts

Host	CI	CI%

Alarm Trend, Last 2 Weeks

Active Alarms, Today (Unacknowledged) - 1 r...

Alarm	Source	Sourc...	Target	Targe...	Details	Start Active...
High Target Index	Multiple Hosts		69.43.161.170	Australia, IPADDR-CRITS	Observed 30.04k points. Expected 1 points, tolerance of 50 allows up to 30k points. (Double-click for details)	Feb 6, 2014 2:30:00 AM (6 hours 57 minutes 40s ago)

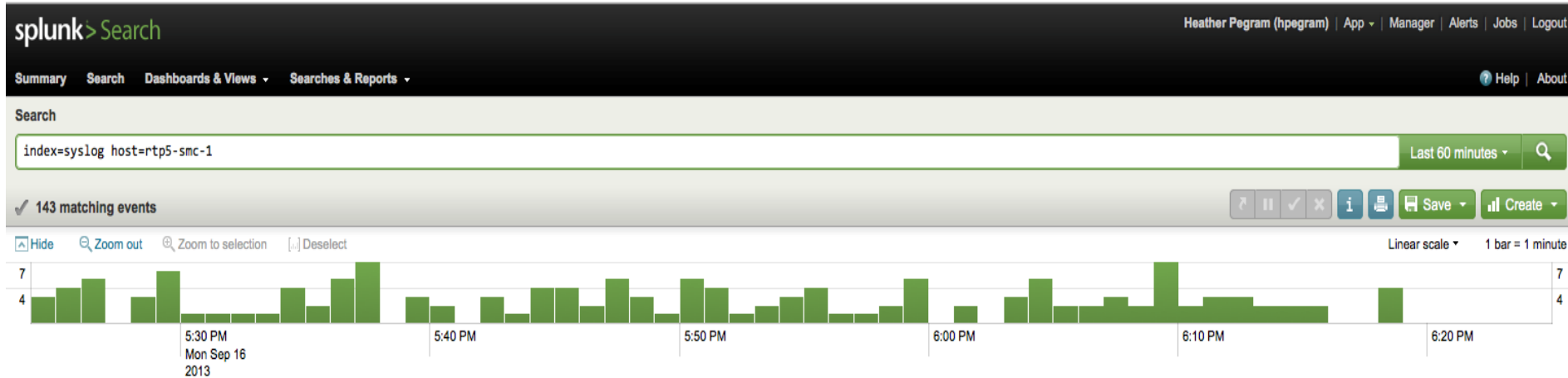
Active High Target Hosts

Host	TI	TI%

# Splunk Integration – SMC Alarms

**Requirement:** integrate flow events with other logs for a single investigation interface

**Solution:** send relevant alarms as syslog messages to in-house Splunk™ architecture



# StealthWatch Splunk Alerts



## Host Snapshot



Flows | Edit Filter | Help

IP Address: **199.59.149.230** Organization: Address: **San Francisco, CA 94107** ISP: Country: **United States**

- Identification
- Alarms**
- Security
- CI Events
- Top Active Flows
- Identity, DHCP and Host Notes
- Exporter Interfaces

Alarm Counts - 1 record

Manage Columns

Alarms - 2 records

			Policy	Alarm ID	Start Active Time	Alarm		Source Host Groups	Source	Target	Target Host Groups	Mitigation	Policy	Details
			Inside Hosts	G7-1906-TS97-SJWE-6	May 9, 2014 1:31:30 PM (52 minutes 43s ago)	Beaconing Host		Private Addresses, ACL103	10.21.70.71	www4.twitter.com	United States (199.59.149.230)		Inside Hosts	Source Host is using https (443/tcp) as client to www4.twitter.com (199.59.149.230)
			Inside Hosts	G7-1906-23UL-WUC9-T	May 9, 2014 8:28:30 AM (5 hours 55 minutes 43s ago)	Beaconing Host		Private Addresses, ACL103	sjc-estein-8917.cisco.com (10.20.221.8)	www4.twitter.com	United States (199.59.149.230)		Inside Hosts	Source Host is using https (443/tcp) as client to www4.twitter.com (199.59.149.230)

Manage Columns

# API Use Cases

Requirement	Problem	API Script Solution
Pull <i>all</i> flows for given time period	SMC $\leftrightarrow$ Flow Collector query limit	Run consecutive, small queries then concatenate
Keep SMC host groups up to date	Manual configuration, old data	Query internal source of truth, push subnet lists to host groups automatically
Look up events for a particular IP for a specific timeframe	No user attribution (yet)	Find IP and lease time from internal source of truth, query StealthWatch for related events

# Network Subnets

Mapped from IPAM

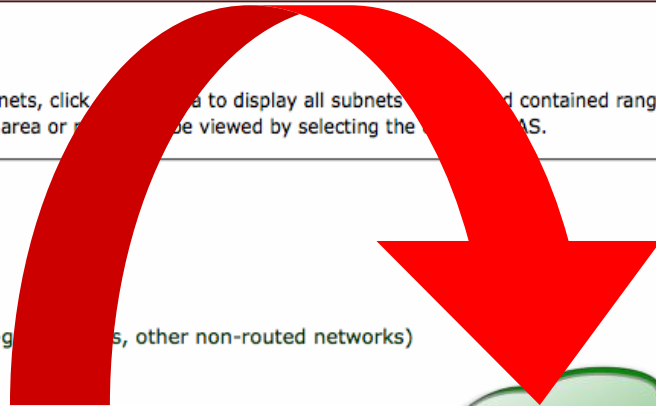
## IPPlan - IP Address Management and Tracking Display subnet information

Main Customers Network DNS Options Admin Help

### Display subnets.

Click on customer/AS to display all associated subnets, click on area to display all subnets and contained ranges associated with that range. Subnets not within an area or range can be viewed by selecting the area/range.

- Blanco Wireless
  - All subnets not part of range
  - 10.0.0.0 (RFC 1918 Space)
    - 10.0.0.0 (Non-routed space for air-gapped networks, other non-routed networks)
  - 10.10.0.0 (Redwood City Campus)
    - 10.10.0.0 (Data Centers)
      - 10.10.0.0 /25 (Windows Server Subnet)
      - 10.10.0.128 /25 (Oracle 10g Subnet)
      - 10.10.1.0 /26 (ESX VMWare Farm)
      - 10.10.1.64 /26 (Web Application Servers)
    - 10.10.32.0 (Site 1 Desktop Networks)
      - 10.10.32.0 /24 (Building 1 1st Floor)
      - 10.10.33.0 /25 (Building 1 2nd Floor)
      - 10.10.33.128 /25 (Building 2)



Internet



DMZ  
172.16.4.0/23



Campus  
172.16.0.0/22



Remote Access  
172.16.32.0/20



Partner  
172.16.8.0/23

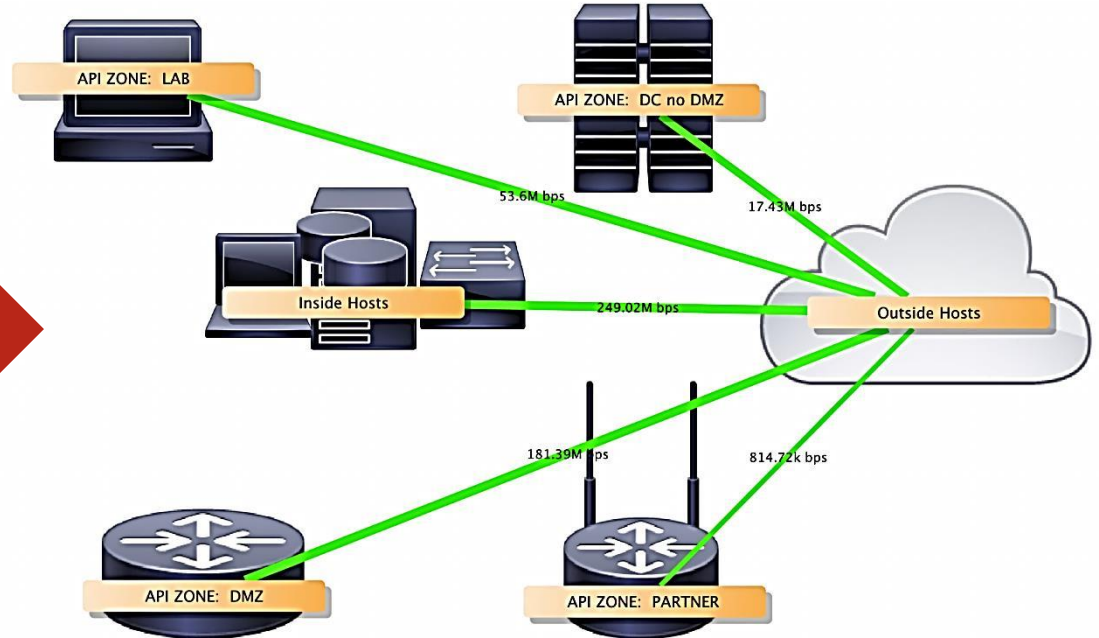
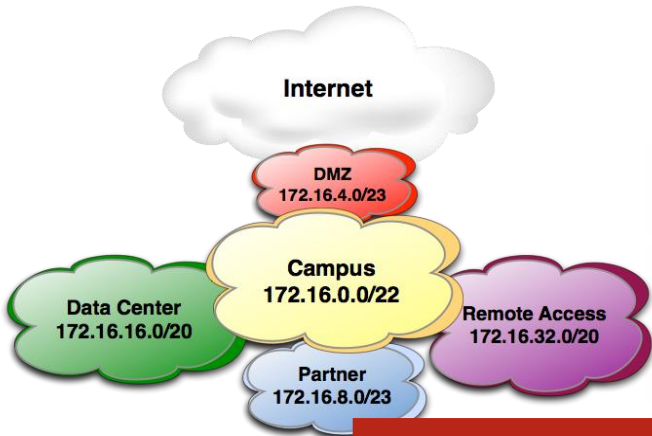


Data Center  
172.16.16.0/20

Cisco *live!*

# Network Subnets

## Map to Lancope Zones



# Splunk Integration - GetFlows

- Find NetFlow Events via Lancope API with the respective src/dst

The screenshot displays the Splunk search results interface. At the top, there is a bar with 'Hide', 'Zoom out', 'Zoom to selection', and 'Deselect' options. Below this is a bar showing '1,400' results and a time range of '6:20 PM Mon Sep 16 2013'. The main search results area shows '9,924 events in the last 15 minutes (from 6:20:00 PM to 6:35:46 PM on Monday)'. On the left, there is a 'Field discovery' section with 'Field discovery is: On' and a 'Hide' button. Below this, there are two lists of fields: '4 selected fields' and '35 interesting fields'. The '4 selected fields' list includes: 'host (≥100)', 'source (1)', 'sourcetype (1)', and 'splunk\_server (11)'. The '35 interesting fields' list includes: 'app\_name (1)', 'appInstanceld (1)', 'attack\_relevance\_rating (1)', 'attacker (≥100)', 'attacker\_locality (4)', 'attacker\_port (≥100)', 'description (3)', 'eventid (≥100)', 'eventtype (8)', 'hostid (1)', and 'index (1)'. The main search results area shows a list of events. The first event is selected, and a context menu is open over it. The context menu options are: 'Build Eventtype', 'Export to CSV', 'Get Flow', 'Get NetFlow Details for 1...20 and 72.163.10.14 on 80', 'Lookup host 183.82.99.20 with DCE', 'Show Source', 'cif\_destip\_query', and 'cif\_srcip\_query'. A red arrow points to the 'Get Flow' option. The event details for the first event are: '9/16/13 1379356076966767000 eventid="682128533416: 6:27:56.966 PM. EXTERNAL HOSTS TO DC" sigDetails="Catches locality="DMZ" target="72.163.10.: " protocol="tcp" trigger\_packet="A: AAGcGoFG3UmMUSKMKCsqeAFBjNkxbAAAAA! rigger\_packet\_details="=00=1F'=C8t: =08=00E=00=000=06c@=00g=06=A0Q=B7R: 00Pc6L [=00=00=00p=02 =00|S=00=04 82.99.20 | sourcetype=cisco\_ips\_syslog'. The event details for the second event are: '9/16/13 076919365000 eventid="682128533416: L HOSTS TO DC" sigDetails="Catches locality="DMZ" target="72.163.10.: " protocol="tcp" gc\_score=" -3.3" g: r\_packet="A89tRnAAACcNrU1ACABFAA8 GkG/IDo1DSKMKCs/OAFBAT1FjAAAAKAC/, AAAMDAAA=" trigger\_packet\_details=' =ADLg=08=00E=00=00<SN=00=003=06=90o=C8=0E: =CF=CE=00P@OQc=00=00=00=A0=02=FF=FF0=C: =9Czu=F7=00=00=00=03=03=00=00" host=200.14.137.67 | sourcetype=cisco\_ips\_syslog'.

# Splunk Integration - GetFlows

1379356076966767000 eventId="6821285334169" hostId="rcdn9-dmz-nms-1" sig\_created="2000101" sig\_type="other" severity="high" app\_name="sensorApp" appInstanceId="25977" signature="64003" subSigId="0" description="INBOUND EXTERNAL HOSTS TO DC" sig\_version="custom" **attacker="183.82.99.20" attacker\_port="51870"** attacker\_locality="OUT" **target="72.163.10.14" target\_port="80"** target\_locality="DMZ" **target="72.163.10.10" target\_port="80"** target\_value\_rating="medium" interface="te0\_1" interface\_group="vs0" vlan="0" protocol="tcp" trigger\_packet="AB8nyHQAACcNrUKACABF AAawBmNAAgGGoFG3UmMUSKMKCsqeAFBjNkxbAAAAAHACIAB8UwAAAgQE7AEB B CA=9E=00Pc6LJ=00=00=00=00p=02 =00S=00=00=02=04=04=EC=01=01=04=02"

Flow of 183.82.99.20 from 2013-09-16 17:57:56 UTC to 2013-09-16 18:57:56 UTC

Start	End	Client IP	Client Name	Client Port	Server IP	Server Name	Server Port	Client Bytes	Server Bytes	Total Bytes
<b>2013-09-16T18:27:56Z</b>	<b>2013-09-16T18:29:46Z</b>	<b>183.82.99.20</b>	<b>183.82.99.20</b>	<b>51870</b>	<b>72.163.10.10</b>	<b>cisco-tags.cisco.com</b>	<b>80</b>	<b>39609</b>	<b>8206</b>	<b>47815</b>
2013-09-16T18:27:56Z	2013-09-16T18:29:46Z	183.82.99.20	183.82.99.20	51865	72.163.10.14	news-tags.cisco.com	80	42298	10206	52504
2013-09-16T18:27:56Z	2013-09-16T18:27:57Z	183.82.99.20	183.82.99.20	51856	173.37.145.8	tools2.cisco.com	80	1012	6748	7760
2013-09-16T18:27:56Z	2013-09-16T18:29:15Z	183.82.99.20	183.82.99.20	51866	72.163.10.14	news-tags.cisco.com	80	42298	0	42298
2013-09-16T18:28:22Z	2013-09-16T18:28:41Z	183.82.99.20	183.82.99.20	51941	173.37.144.208	sso-prod2.cisco.com	443	3340	5217	8557
2013-09-16T18:28:21Z	2013-09-16T18:29:43Z	183.82.99.20	183.82.99.20	51939	173.37.144.208	sso-prod2.cisco.com	80	7716	2732	10448

[Download Report \(CSV format\)](#)

IP Matched logs (highlighted ones are exact matches, ip and port)

Start	End	Client IP	Client Name	Client Port	Server IP	Server Name	Server Port	Client Bytes	Server Bytes	Total Bytes
<b>2013-09-16T18:27:56Z</b>	<b>2013-09-16T18:29:46Z</b>	<b>183.82.99.20</b>	<b>183.82.99.20</b>	<b>51870</b>	<b>72.163.10.10</b>	<b>cisco-tags.cisco.com</b>	<b>80</b>	<b>39609</b>	<b>8206</b>	<b>47815</b>
2013-09-16T18:27:56Z	2013-09-16T18:29:46Z	183.82.99.20	183.82.99.20	51865	72.163.10.14	news-tags.cisco.com	80	42298	10206	52504
2013-09-16T18:27:56Z	2013-09-16T18:29:15Z	183.82.99.20	183.82.99.20	51866	72.163.10.14	news-tags.cisco.com	80	42298	0	42298





# Conclusion

# Conclusion

## NetFlow benefits to Incident Respons teams

- Robust data set
- Due to size and deduplication, significant retention possible
- Ability to integrate NetFlow data with other security tools leveraging API

# Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could be a Winner

- Promote your favorite speaker through Twitter and you could win \$200 of Cisco Press products (@CiscoPress)
- Send a tweet and include
  - Your favorite speaker’s Twitter handle <Speaker – enter your twitter handle here>
  - Two hashtags: #CLUS #MyFavoriteSpeaker
- You can submit an entry for more than one of your “favorite” speakers
- Don’t forget to follow @CiscoLive and @CiscoPress
- View the official rules at <http://bit.ly/CLUSwin>

# Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings



Q & A

Cisco *live!*

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site  
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



### Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. [www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)

**Cisco** *live!*



Thank you.

Cisco *live!*



**CISCO**