TOMORROW starts here.

cisco

Cisco live!

Advanced Threat Defence using NetFlow

BRKSEC-2073

Matthew Robertson

Security Technical Marketing Engineer

Cisco live!

"The whole art of war consists of guessing at what is on the other side of the hill."

Arthur Wellesley, 1st Duke of Wellington

Evolution of Cyber Conflict

Manual Attacks *(1980s)*

War Dialing, Phone Phreaking …

Mechanised Attacks *(1988)*

Viruses, Worms …

Google, RSA …

Talented Human / Mechanised Attackers *(2009)*

APT, Multi-Step Attacks…

Target, Neiman Marcus …

DIY Human / Mechanised Attackers *(2011)*

Cyrptocurrency Ransoms, Store-bought Credentials …

Manual Defences

Unplug

Mechanised Defences

Firewall, IDS/IPS

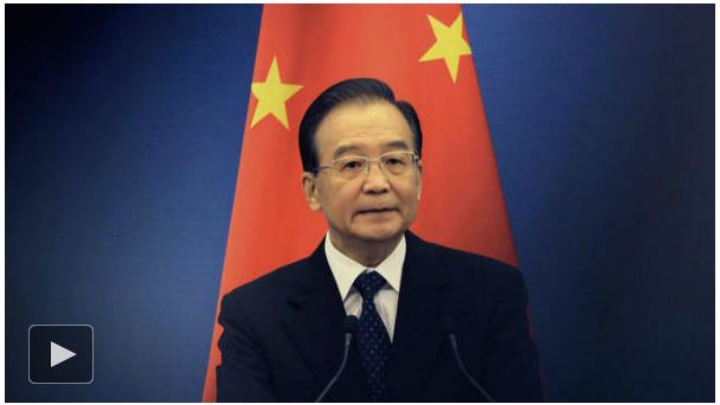
Targeted Human/Mechanised

Reputation, App-aware Firewall

Intelligence Driven Human Defenders

Defending against Humans

Hackers in China Attacked The Times for Last 4 Months



A Cyberattack From China: TimesCast: Chinese hackers infiltrated The New York Times's computer systems, getting passwords for its reporters and others.

By NICOLE PERLROTH
Published: January 30, 2013 | 391 Comments

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

点击查看本文中文版

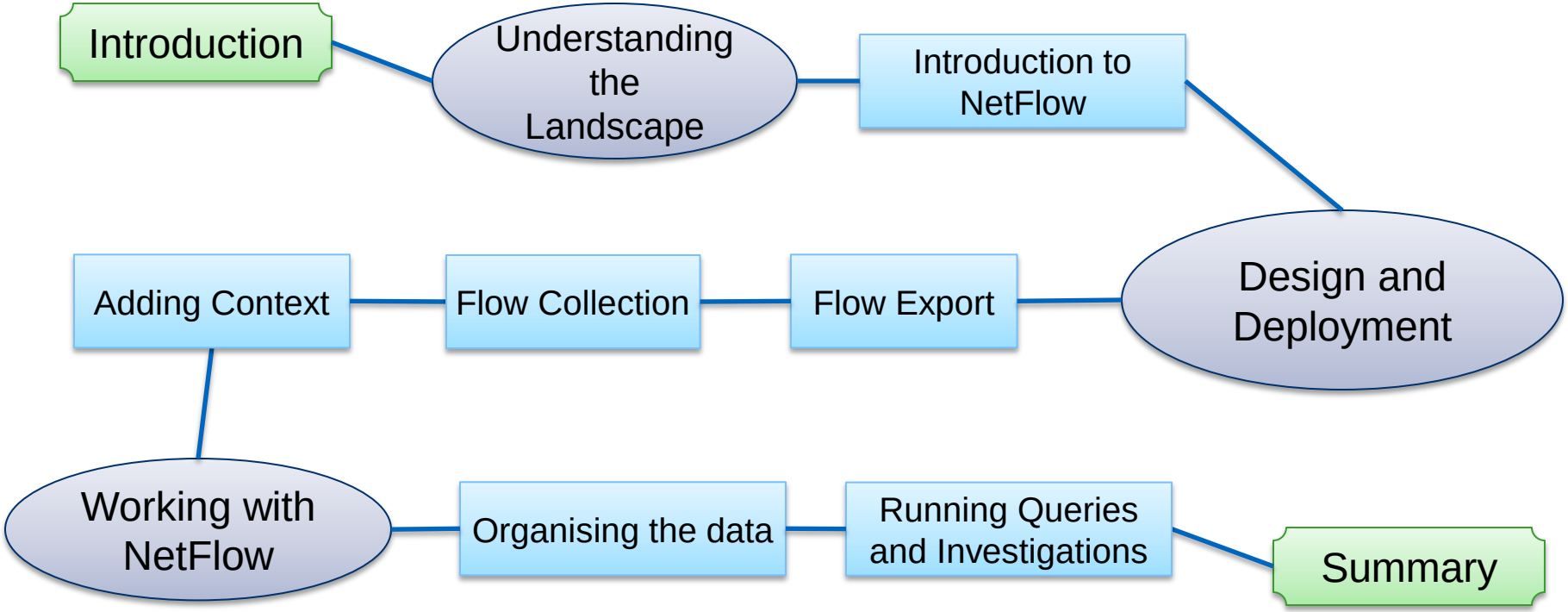
After surreptitiously tracking the intruders to study their movements security experts have expelled the attackers and kept them from breaking back in.

Readers shared their thoughts on this article.
Read All Comments (391) »

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL
PRINT
REPRINTS

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

Agenda



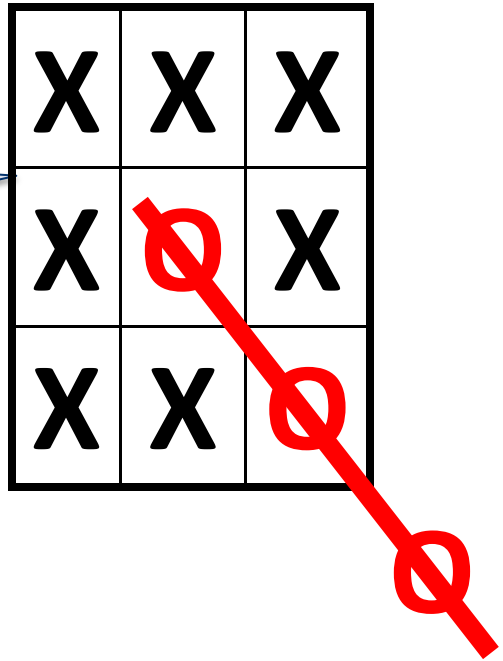
About the Speaker

Matthew Robertson

- Security Technical Marketing Engineer
- ½ year at Lancope
- 5½ years at Cisco
  - Development and Technical Marketing
- Focused on advanced threat detection
- I am Canadian!

Thinking Beyond the Perimeter

Modern threats are consistently bypassing the security perimeter as they redraw the map



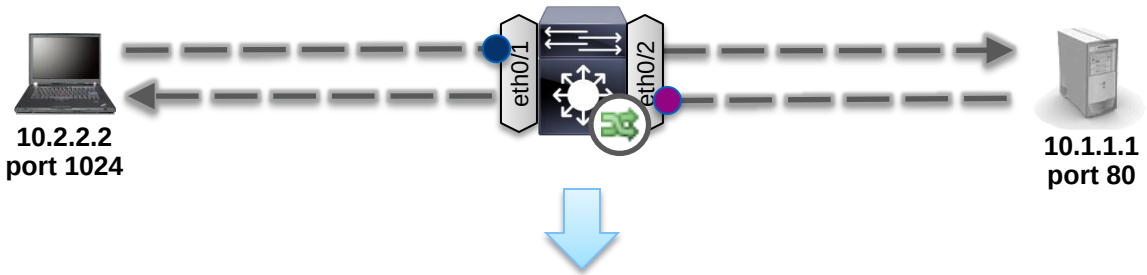
Hiding in plain sight

Signals Intelligence

Traffic Analysis:

- Deduce information from communication patterns

NetFlow



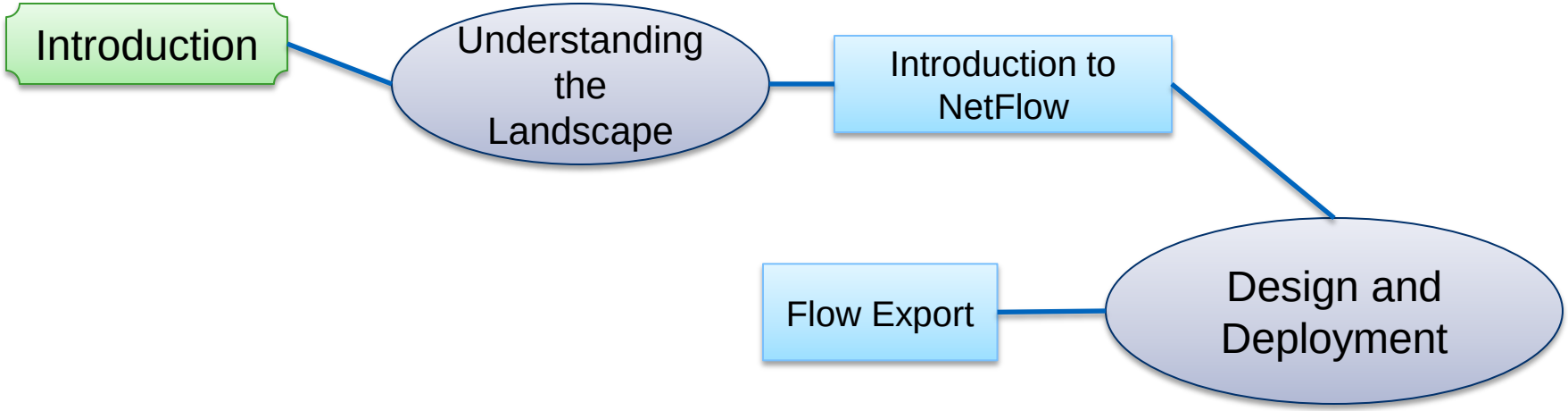
Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	SYN,ACK,FIN

NetFlow = Visibility

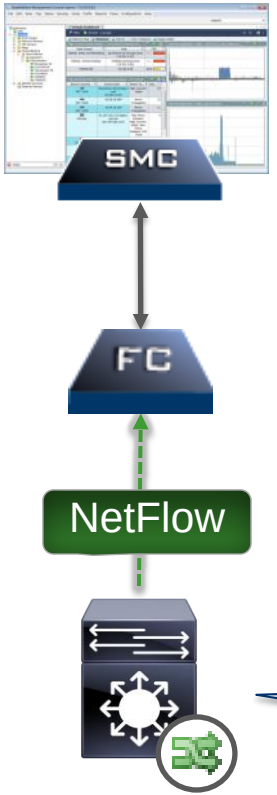
A single NetFlow Record provides a wealth of information


```
Router# show flow monitor CYBER-MONITOR cache
...
IPV4 SOURCE ADDRESS:        192.168.100.100
IPV4 DESTINATION ADDRESS:   192.168.20.6
TRNS SOURCE PORT:           47321
TRNS DESTINATION PORT:      443
INTERFACE INPUT:            Gi0/0/0
IP TOS:                     0x00
IP PROTOCOL:                6
ipv4 next hop address:      192.168.20.6
tcp flags:                  0x1A
interface output:           Gi0/1.20
counter bytes:              1482
counter packets:            23
timestamp first:            12:33:53.358
timestamp last:             12:33:53.370
ip dscp:                    0x00
ip ttl min:                 127
ip ttl max:                 127
application name:           nbar secure-http
...
```

Agenda



NetFlow Deployment Architecture



Management/Reporting Layer:

- Run queries on flow data
- Centralise management and reporting

Flow Collection Layer:

- Collection, storage and analysis of flow records

Flow Exporting Layer:

- Enables telemetry export
- As close to the traffic source as possible

Considerations: Flow Exporting Layer

1. NetFlow support
2. Which version of NetFlow to use
3. How to configure/what to measure
4. Where in the network to enable NetFlow export

Cisco NetFlow Support

Versions of NetFlow

Version	Major Advantage	Limits/Weaknesses
V5	Defines 18 exported fields Simple and compact format Most commonly used format	IPv4 only Fixed fields, fixed length fields only Single flow cache
V9	Template-based IPv6 flows transported in IPv4 packets MPLS and BGP nexthop supported Defines 104 fields, including L2 fields Reports flow direction	IPv6 flows transported in IPv4 packets Fixed length fields only Uses more memory Slower performance Single flow cache
Flexible NetFlow (FNF)	Template-based flow format (built on V9 protocol) Supports flow monitors (discrete caches) Supports selectable key fields and IPv6 Supports NBAR data fields	Less common Requires more sophisticated platform to produce Requires more sophisticated system to consume
IP Flow Information Export (IPFIX) AKA NetFlow V10	Standardised – RFC 5101, 5102, 6313 Supports variable length fields, NBAR2 Can export flows via IPv4 and IPv6 packets	Even less common Only supported on a few Cisco platforms
NSEL (ASA only)	Built on NetFlow v9 protocol State-based flow logging (context) Pre and Post NAT reporting	Missing many standard fields Limited support by collectors

Configuring Flexible NetFlow

1. Configure the Exporter

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

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

Best Practice: include all v5 fields

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
```

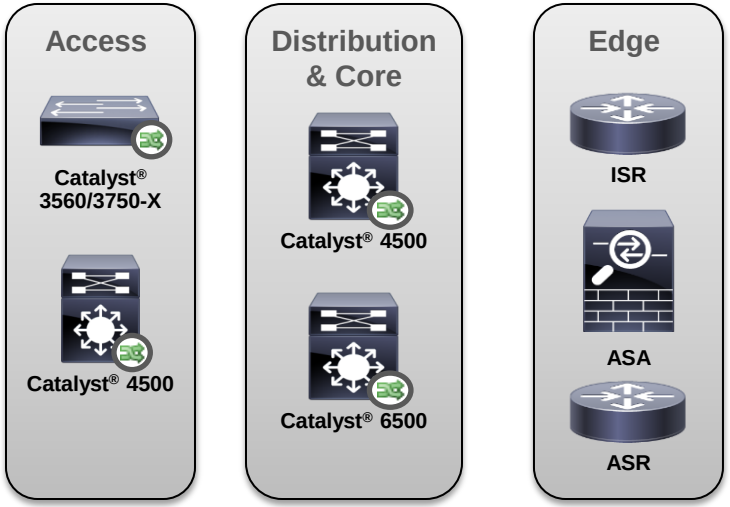
4. Apply to an Interface

```
Router(config)# interface s3/0

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

NetFlow Deployment

Each network layer offers unique NetFlow capabilities



NetFlow Deployment

Access:

- New network edge
  - Detect threats as the enter the network
- Detect threats inside the switch
  - east-west
  - Layer 2 traffic
- Fewer false positives
  - Higher-granular visibility
- Identify the endpoint
  - collect MAC Address

Catalyst 3650-X,3750-X Flow Record

```
!
flow record CYBER_3KX_FLOW_RECORD   match datalink mac source-address
 match datalink mac destination-address
 match datalink mac source-vlan-id
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port   collect interface input snmp   collect interface output snmp   collect counter bytes   collect counter packets   collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

For Your Reference

Catalyst 4500 Flow Record

```
!
flow record CYBER_4K_FLOW_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address   match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

For Your Reference

NetFlow Deployment - Converged Access

Converged Access:

- NetFlow for the first time on Wireless
- Visibility in BYOD environments
- Consistent configuration for wired and wireless
  - Single flow monitor can be applied to wired ports and SSID
- Natively available in the UADP ASIC
- Can monitor East-West and North-South flows
  - 48k flows on the 48 port model

NetFlow Deployment

Distribution & Core:

- Traditional deployment
  - Minimal recommended deployment
- Enable at critical points/bottle necks
- Typically done on a Layer 3 boundary
- Detect threats internal to the VLAN
  - When deployed on an SVI interface
- Detect threats as they traverse the internal network
  - Move between subnets

Catalyst 6500 (Sup 2T) Flow Record

For Your Reference

```
!
flow record CYBER_6K_FLOW_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

NetFlow Deployment

Edge:

- Detect threats as they enter and leave the network
- Monitor communication between branches
- Gain context from edge devices
  - Application - NBAR
  - Events & User-ID - NSEL

ISR Flow Record

For Your Reference

```
!  flow record CYBER_ISR_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
```

Enable NBAR

ASA NSEL Configuration

For Your Reference

```
!
flow-export destination management <ip-address> 2055
!
policy-map global_policy
 class class-default
  flow-export event-type all destination <ip-address>
!
flow-export template timeout-rate 2
logging flow-export syslogs disable
!
```

Flow Monitor Configuration

```
!
flow monitor CYBER_MONITOR    record CYBER_RECORD
  exporter CYBER_EXPORTER
  cache timeout active 60
  cache timeout inactive 15
!
```

Inactive Timeout:

- How long a flow can be inactive before being removed from cache
- Recommended 15 seconds
- All exporters should have the same timeout

Active Timeout:

- Longest amount of time a flow can be in cache without exporting a Flow Record
- Recommended 60 seconds
- All exporters should have the same timeout

Aside: Myths about NetFlow Generation

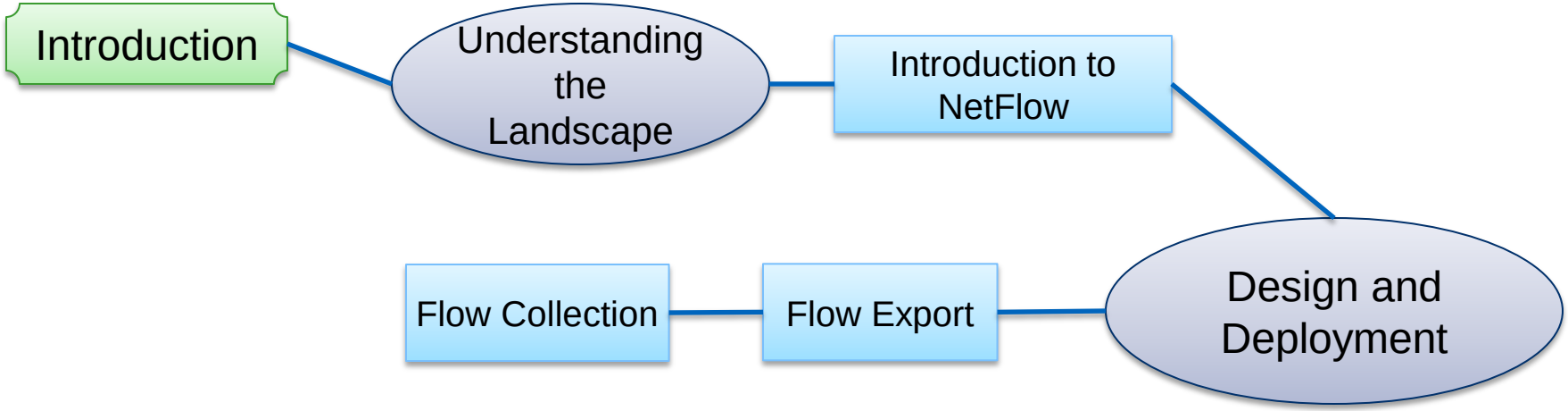
Myth #1: NetFlow impacts performance

- Hardware implemented NetFlow has no performance impact
- Software implementation is typically significantly <15% processing overhead

Myth #2: NetFlow has bandwidth overhead

- NetFlow is a summary protocol
- Traffic overhead is typically significantly <1% of total traffic per exporting device

Agenda



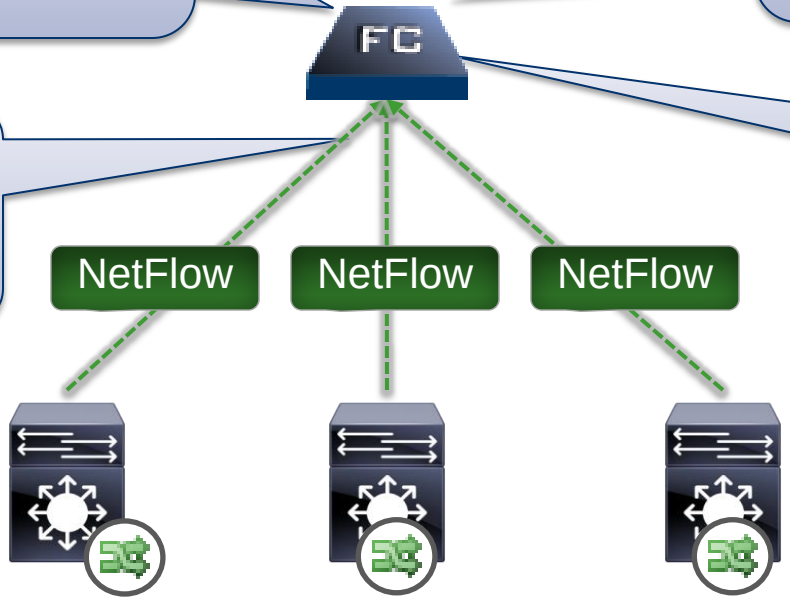
Flow Collection Considerations

Feature set
- Reporting
- Drill down
- Retention
- Analysis

Scalability & Performance
- # of NetFlow sources
- # of users
- Flows per second
  - Sustained vs. burst

Flow Handling
- De-duplication
- Stitching
- Replication

Your **time**, **resources** and **budget**



Components for NetFlow Security Monitoring

StealthWatch Management Console
- Management and reporting
- Up to 25 FlowCollectors
- Up 3 million fps globally

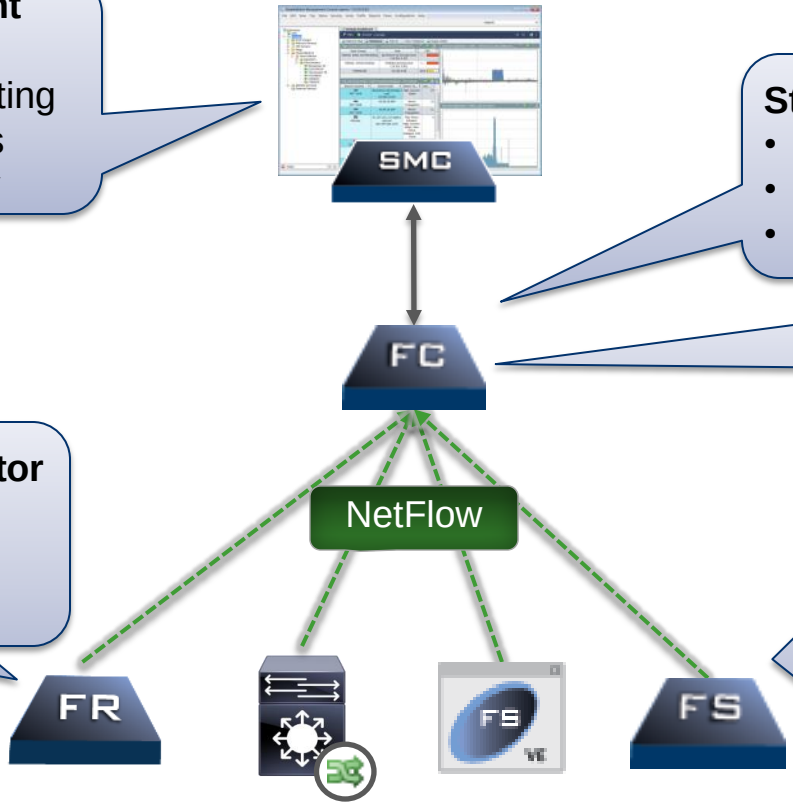
StealthWatch FlowCollector
- Collect and analyse
- Up to 2000 sources
- Up to sustained 120,000 fps

Best Practice: Centralise collection globally

StealthWatch FlowReplicator
- UDP Packet copier
- Forward to multiple collection systems

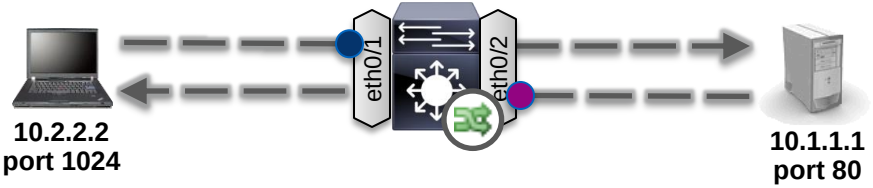
StealthWatch FlowSensor
- Generate NetFlow data

StealthWatch FlowSensor VE
- Virtual environment
- Visibility into ESX



NetFlow Collection: Flow Stitching

Uni-directional flow records



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	eth0/1 eth0/2

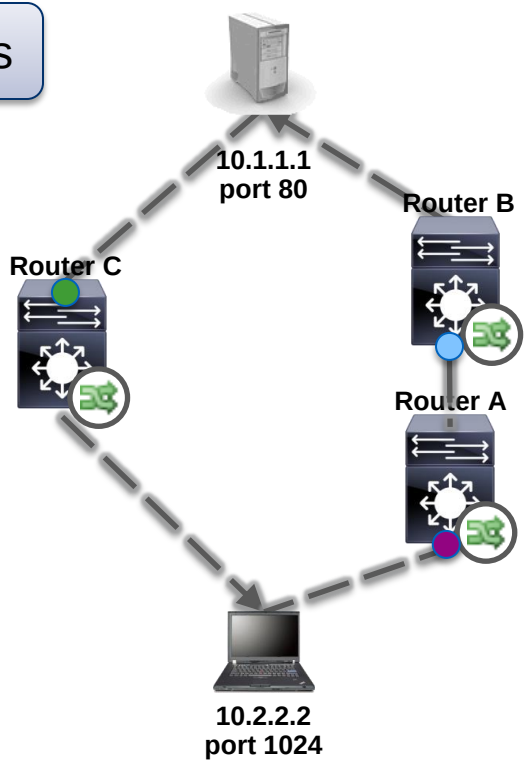
Bi-directional:

- Conversation flow record
- Allows easy visualisation and analysis

NetFlow Collection: De-duplication

Duplicates

- Router A: 10.2.2.2:1024 -> 10.1.1.1:80
- Router B: 10.2.2.2:1024 -> 10.1.1.1:80
- Router C: 10.1.1.1:80 -> 10.2.2.2:1024



- Without de-duplication:
  - Traffic volume can be misreported
  - False positive would occur
- Allows for the efficient storage of flow data
- Necessary for accurate host-level reporting
- Does not discard data

Conversational Flow Record

Who

What

How

Who

Start: 01/10 - 08:12:59 AM
End: 01/10 - 08:14:59 AM
Duration: 2m 0s

10.201.3.179
RFC 1918
charlene
64:80:99:5b:22:84

61488/TCP

69.17MB | 56.08K packets

HTTP

67.74MB | 54.92K packets

80/TCP

77.109.171.10
Switzerland

When

Search Subject Details	Totals	Peer Details
Packets: 56.08K	**Packets:** 111K	**Packets:** 54.92K
Packet Rate: 467.32pps	**Packet Rate:** 924.96pps	**Packet Rate:** 457.64pps
Bytes: 69.17MB	**Bytes:** 136.91MB	**Bytes:** 67.74MB
Byte Rate: 604.4Kbps	**Byte Rate:** 1.2Mbps	**Byte Rate:** 591.91Kbps
Percent Transfer: 50.5%	**Search Subject/Peer Ratio:** 1.02	**Percent Transfer:** 49.5%
NAT: 209.182.184.8	**TCP Connections:** 3	**Host Groups:** Switzerland
Host Groups: Sales and Marketing, End User Devices, Atlanta	**RTT:** 306ms	**Payload:** HEAD http://au.download.windowsupdate.com/msdownload/update/software/crup/2012/12/proof-en-us_82ec984db73a712e4b54cb1fe93738c82afde551.cab
Payload: 200 OK	**SRT:** 3ms	

More Details

Integrating with a SIEM

Log alarms and summary info to SIEM
- Complete visibility throughout network
- Leverage specialty data handling

SIEM

Security Events

STEALTH WATCH By Lancope

API

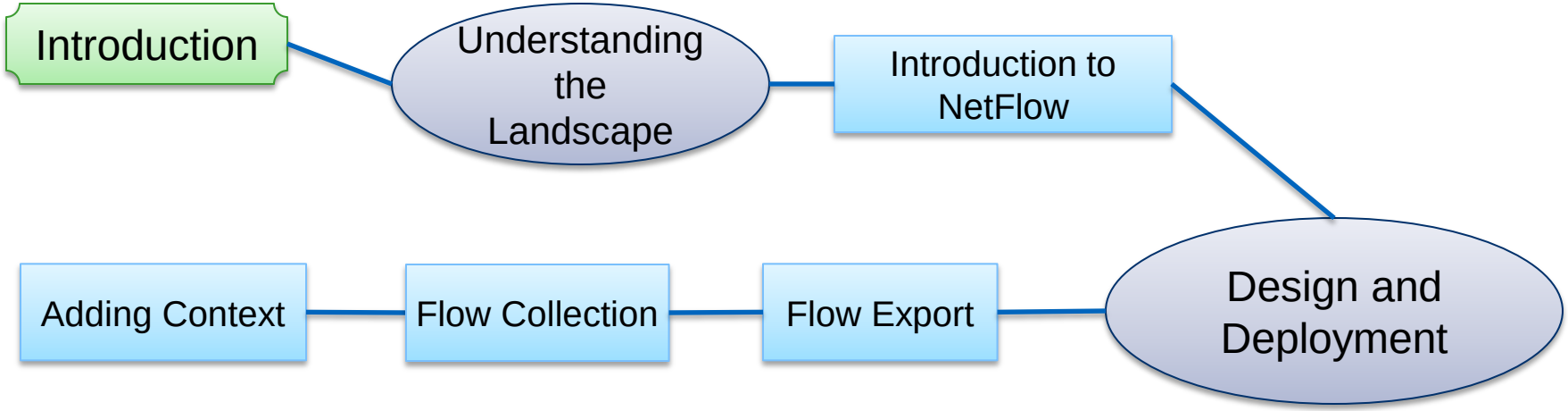
Syslog

SDEE

API's to access database
- Directly access flow data (ex. *getFlows*)
- Improved scale - collection and retention
- Decreased cost

NetFlow

Agenda



Context is Critical

ISE as a Telemetry Source

Monitor Mode

- Open Mode, Multi-Auth
- Unobstructed Access
- No impact on productivity
- Profiling, posture assessment
- Gain Visibility

syslog

- Maintain historical session table
- Correlate NetFlow to username
- Build User-centric reports

SMC

Start Active Time	End Active Ti...	User Name	Host	Device Type	MAC Address
Apr 15, 2013 2:08:33 PM (17 minutes 3s ago)	Current	student01	192.168.103.101	VMWare-Device	00:50:56:85:5c:3d (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student04	192.168.104.100	WindowsXP-Workstation	00:50:56:85:13:c4 (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod08-mgmt.demo.local	192.168.108.100	WindowsXP-Workstation	00:50:56:85:13:cc (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod09-mgmt.demo.local	192.168.109.100	WindowsXP-Workstation	00:50:56:85:13:ce (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student05	192.168.105.100	WindowsXP-Workstation	00:50:56:85:13:c6 (VMware, Inc.)

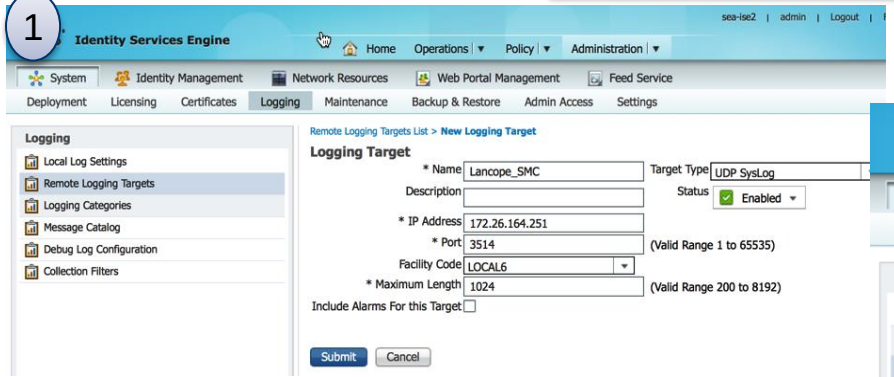
Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Apr 15,13 02:08:33.241 PM	✓		student01	00:50:56:85:5C:3D	192.168.103.1...	sw1	GigabitEthernet0/4	PermitAccess
Apr 15,13 02:08:21.241 PM	✓		DEMO\student04	00:50:56:85:13:C4	192.168.104.1...	sw1	GigabitEthernet0/5	PermitAccess
Apr 15,13 02:08:21.219 PM	✓		host/pod08-mgmt.demo.local	00:50:56:85:13:CC	192.168.108.1...	sw1	GigabitEthernet0/9	PermitAccess
Apr 15,13 02:08:21.192 PM	✓		host/pod09-mgmt.demo.local	00:50:56:85:13:CE	192.168.109.1...	sw1	GigabitEthernet0/10	PermitAccess
Apr 15,13 02:08:21.144 PM	✓		DEMO\student05	00:50:56:85:13:C6	192.168.105.1...	sw1	GigabitEthernet0/6	PermitAccess
Apr 15,13 02:08:21.082 PM	✓		DEMO\stu	00:50:56:85:13:CA	192.168.107.1...	sw1	GigabitEthernet0/8	PermitAccess

Authenticated Session Table

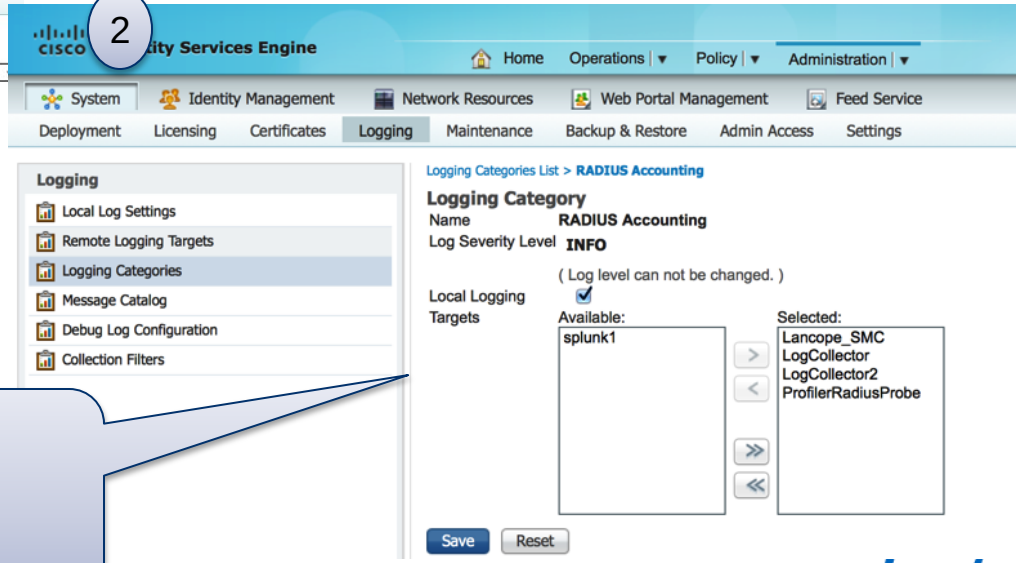
Configuration: Logging on ISE

1. Create Remote Logging Target on ISE
2. Add Target to Logging Categories

1



2

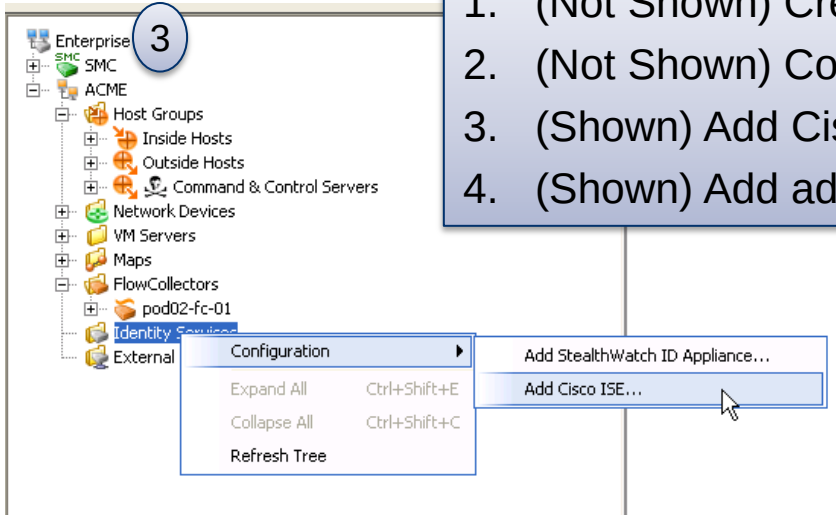


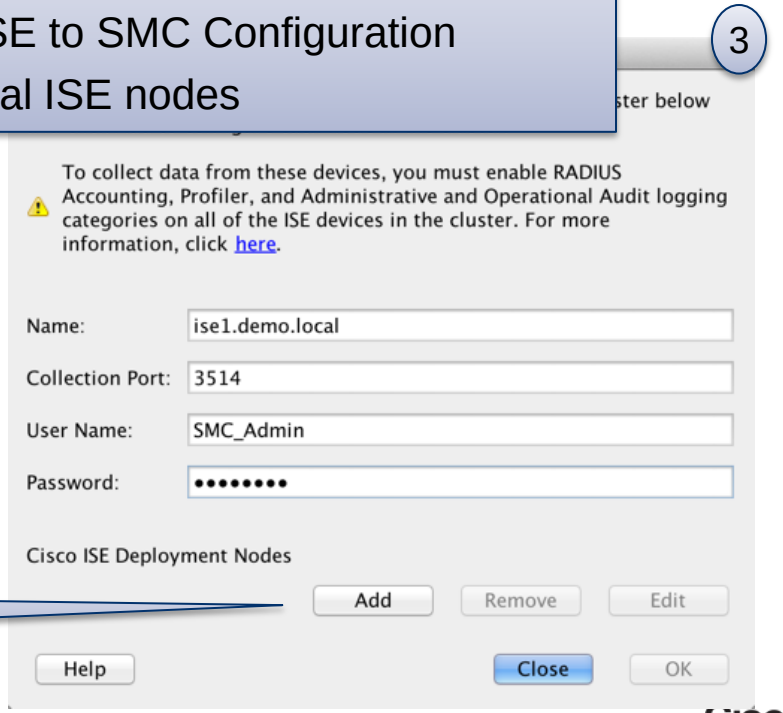
Required Logging categories:

- RADIUS Accounting
- Profiler
- Administrative and Operational Audit

Configuration: Add ISE to SMC

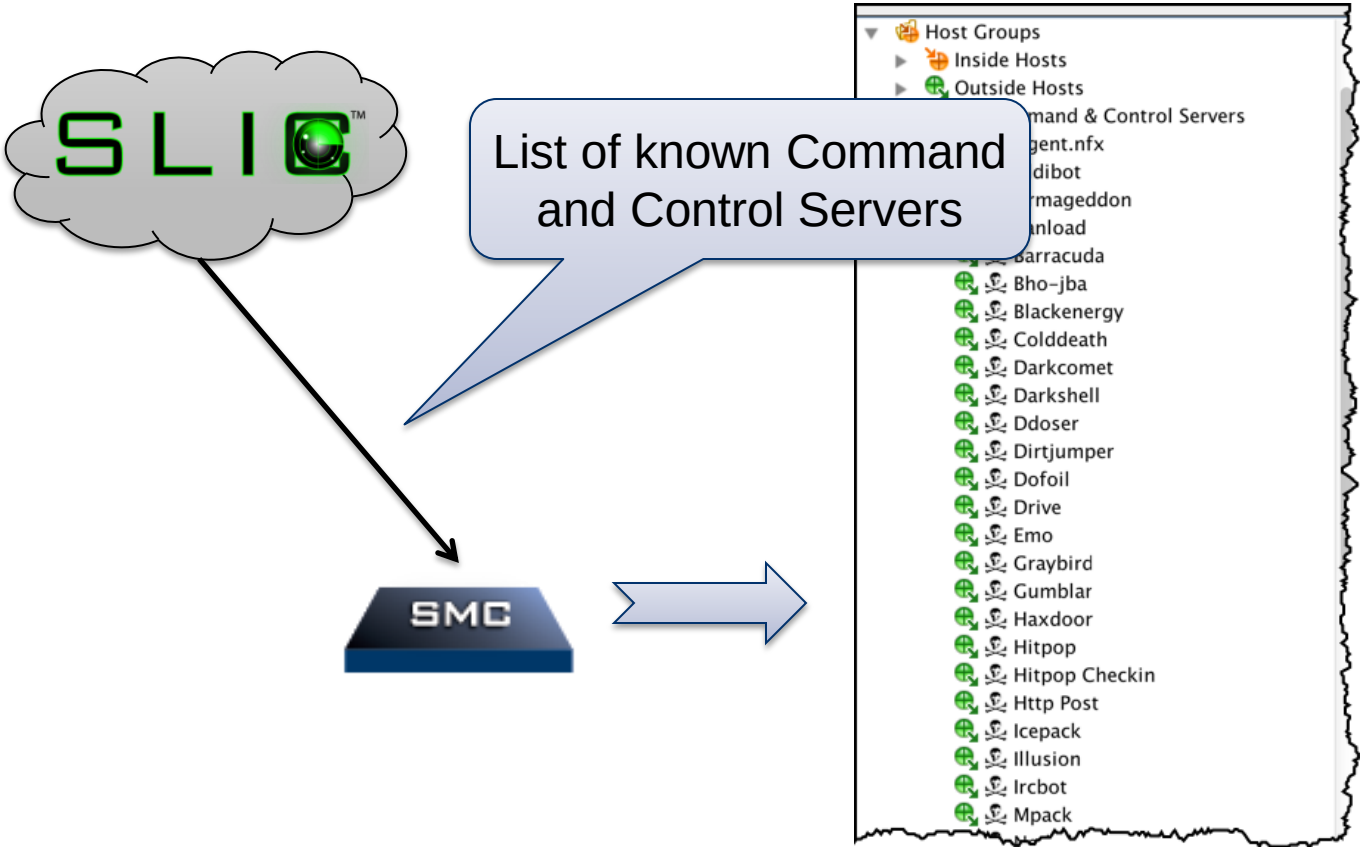
1. (Not Shown) Create Admin User on ISE
2. (Not Shown) Configure ISE or CA certificate on SMC
3. (Shown) Add Cisco ISE to SMC Configuration
4. (Shown) Add additional ISE nodes





4. Add additional ISE nodes

Global Intelligence



Adding Situational Awareness

Flow Table – 29 records

Client Host	Client Host Groups	Server Host	Server Host Groups	Application	Duration	Total Traffic...	Start Active Time
10.201.3.149	Sales and Marketing, End User Devices, Atlanta	89.108.67.143	Russian Federation	HTTP	23s	256.56k	Jan 11, 2014 3:44:20 PM (9 hours 1 minute 26s ago)

Client Host	Client Host Group	Server Host	Server Host Groups	Application	Duratio n	Total Traffic	Start Active Time
10.201.3.149	Sales and Marketing, End User Devices	89.108.67.143	Russian Federation	HTTP	23s	256.56K	Jan 11, 2014

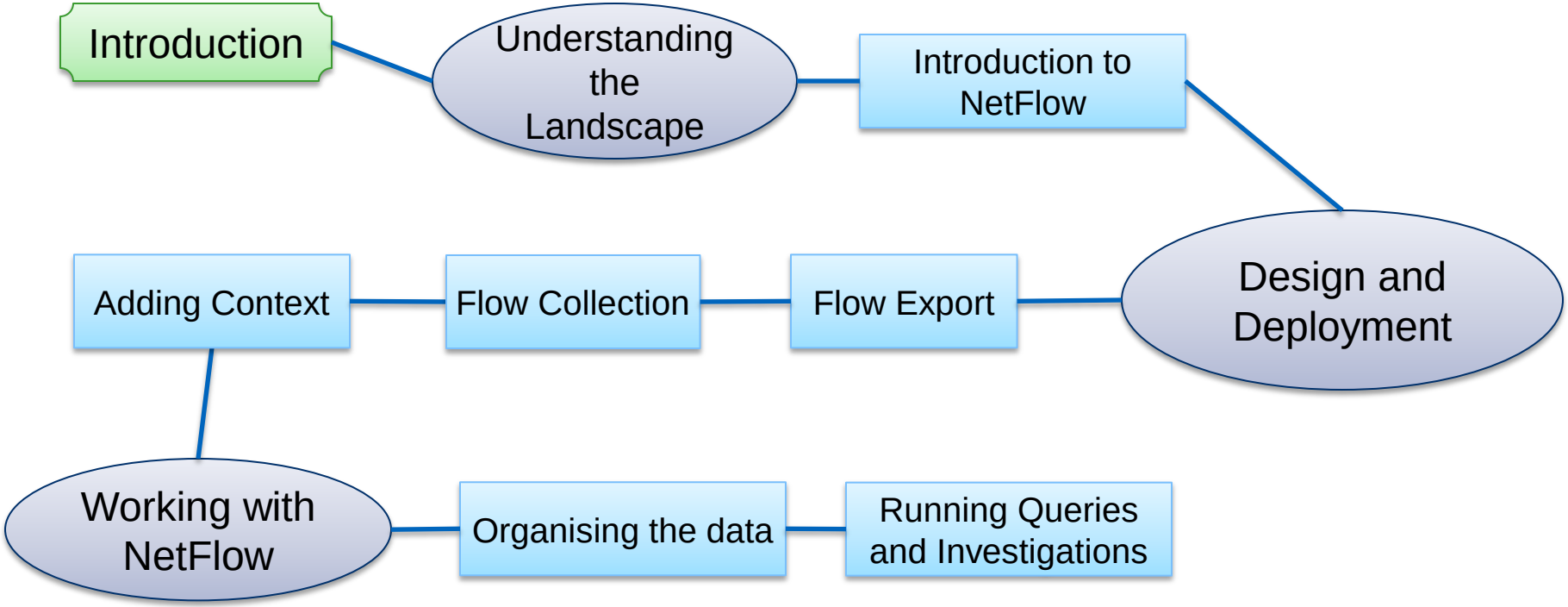
Adding Situational Awareness

Flow Table – 29 records

Client User Name	Client Host	Client Host Groups	Server Host	Server Host Groups	Application	Duration	Total Traffic...	Start Active Time
ken	10.201.3.149	Sales and Marketing, End User Devices, Atlanta	89.108.67.143	Russian Federation, Zeus	HTTP	23s	256.56k	Jan 11, 2014 3:44:20 PM (9 hours 1 minute 26s ago)

Client User Name	Client Host	Client Host Group	Server Host	Server Host Groups	Application	Duration	Total Traffic	Start Active Time
Ken	10.201.3.149	Sales and Marketing, End User Devices	89.108.67.143 	Russian Federation, **Zeus**	HTTP	23s	256.56K	Jan 11, 2014

Agenda



Behavioural Analysis & Anomaly Detection

Behavioural Analysis:

- Leverages knowledge of known bad behaviour

Anomaly Detection:

- Identify a change from “normal”

StealthWatch: Indices

Concern Index: Track hosts that appear to compromising network integrity

Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops, Atlanta	10.10.101.118	313,624,542	3,136%	High Concern Index	Ping, Ping_Scan, TCP_Scan
New York, Desktops	10.50.100.83	190,075,544	1,901%	High Concern Index, High File Sharing Index, High Total Traffic	Ping, Rejects, TCP_Scan

Target Index: Track hosts that appear to be victims of the suspicious behaviour of other hosts

Host Groups	Host	TI	TI%	Alarms	Alerts
Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.15	118,019,003	11,802%		Excess_Clients, Rejects

File Sharing Index: Tracks behaviour that is indicative of peer-to-peer activity

Host Groups	Host	FSI	FSI%	Alarms	Alerts
Atlanta, Trusted Wireless	10.10.200.59	180,385	361%	High Concern Index, High File Sharing Index, High Total Traffic	Ping, Ping_Scan, Port_Scan, TCP_Scan, TCP_Stealth

StealthWatch: Alarms

Alarms

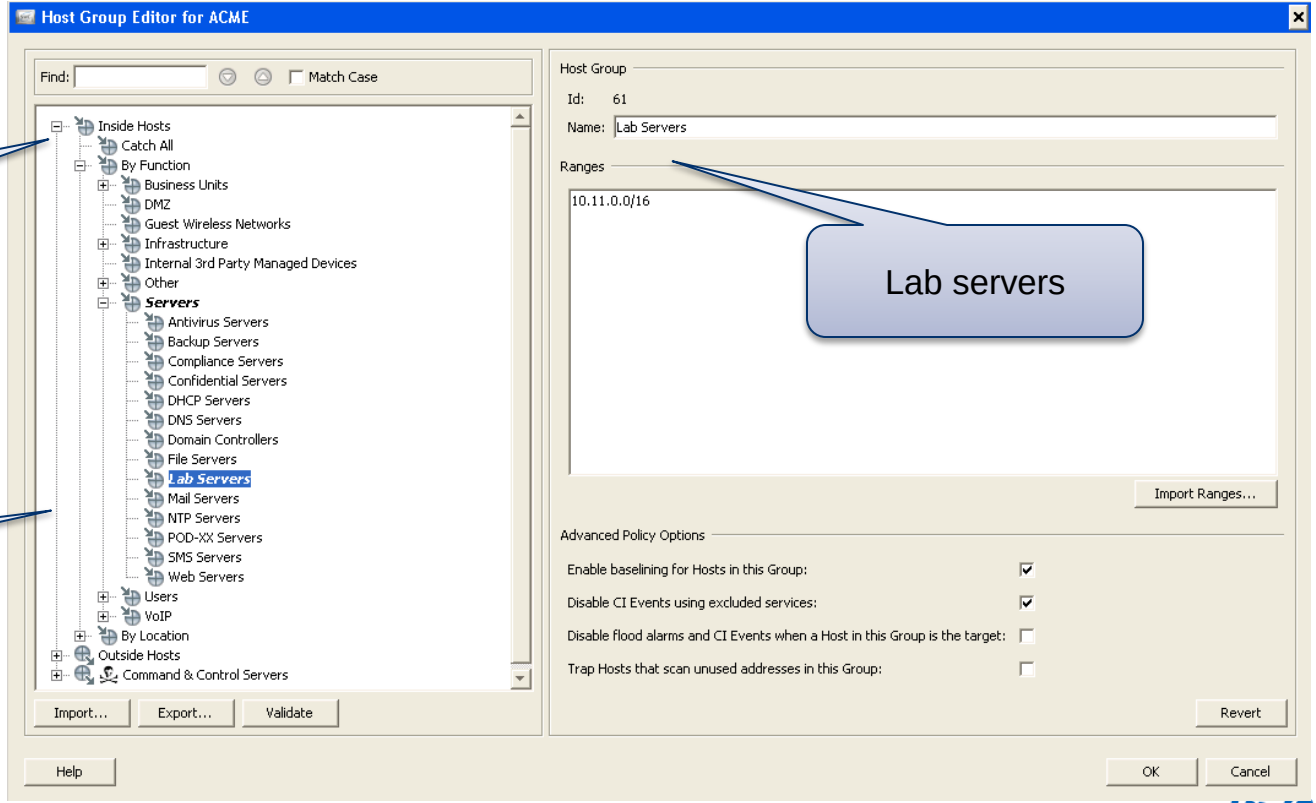
- Indicate significant behaviour changes and policy violations
- Known and unknown attacks generate alarms
- Activity that falls outside the baseline, acceptable behaviour or established policies

Policy	Start Active Time	Alarm	Source	Source Host Groups	Source Use...	Target	Details
Desktops & Trusted Wireless	Apr 15, 2013 4:20:00 PM (7 minutes 7s ago)	Suspect Data Loss	10.10.101.89	Desktops, Atlanta	ud0158	Multiple Hosts	Observed 1.87G bytes. Policy maximum allows up to 500M bytes.

Host Groups

Virtual container of multiple IP Addresses/ranges that have similar attributes

Best Practice: classify all known IP Addresses in one or more host groups



Lab servers

Policy Tuning

Role Policies

Name	Description	Assigned to Host Groups	Assigned to Ranges
Antivirus & SMS Servers	Suppress Scanning Activity	SMS Servers Antivirus Servers	
Backup Servers		Backup Servers	
Desktops & Trusted Wirele		End User Devices Trusted Wireless	
rs	Increases Traffic Values for File Server Alarms	Web Servers File Servers	
Devices		Proxy	
		Mail Servers	
tems &		Network Scanners	
Servers		Servers	
Trusted Internet Hosts	Suppress High Total Traffic, Suspect Data Loss, Suspect Long Flow	Trusted Internet Hosts	

Add... Duplicate... Remove Edit...

Default Policies

Name	Description
Inside Hosts	All hosts in Inside Hosts
Outside Hosts	All hosts in Outside Hosts

Edit...

Policies can be created for individual host groups

Tune alarm thresholds

Default policy for Inside and Outside hosts

Flow Query Basics – The Flow Table

Flow Table

Filter

Filter conditions

Filter | Domain : ACME | Time : Last 5 minutes

Client or Server Host Group : Inside Hosts

Table | Short List

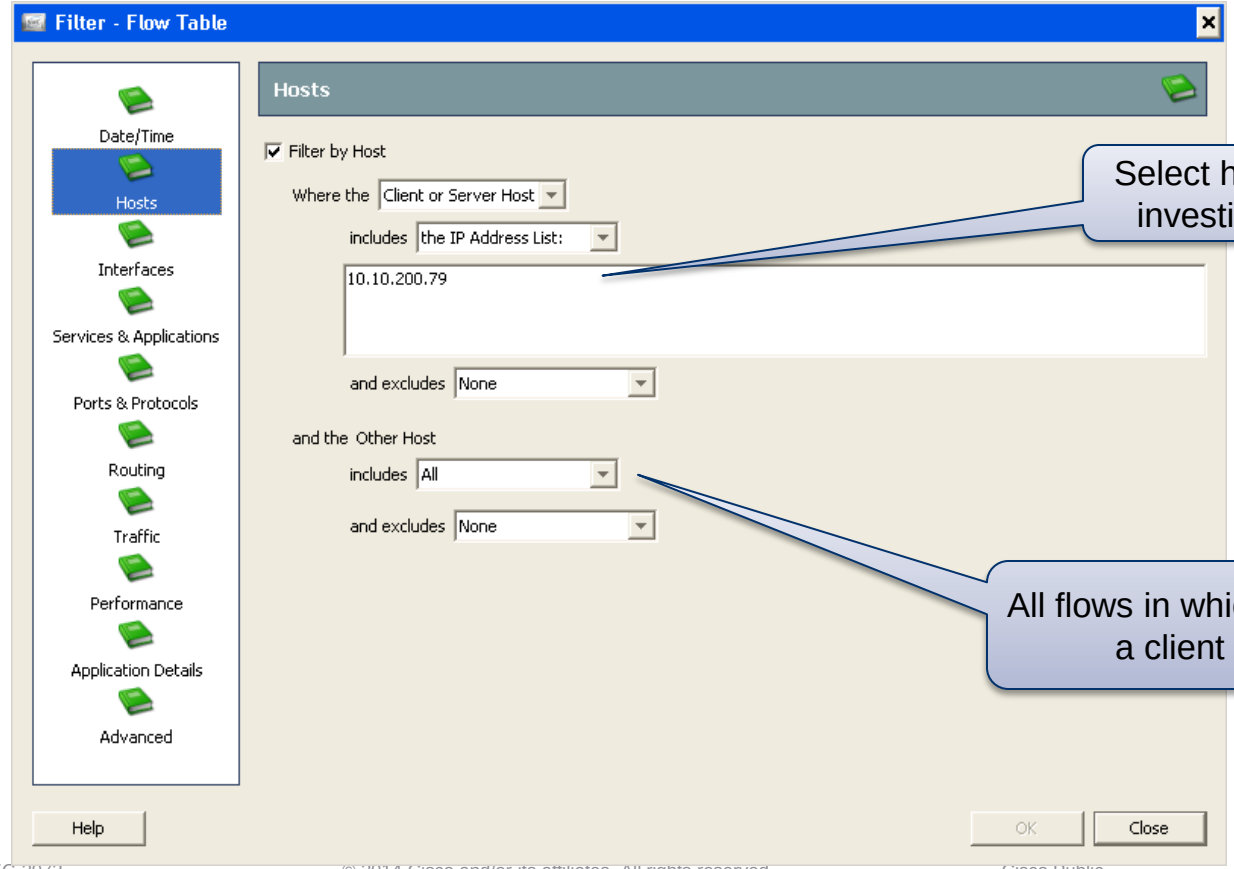
Flow Table - 2,000 records

Client Host	Client Host Groups	Server Host	Server Host Groups	Application	Service Summary	Duration	To
10.10.101.89	Desktops, Atlanta	4.27.11.253	United States	streaming audio/video	http (80/tcp)	4 hours 2 minutes 39s	
10.10.1.31	Atlanta	10.10.99.21	Atlanta	NetFlow/sFlow	netflow (2055/udp)	3 hours 30 minutes 27s	
10.10.101.43	Desktops, Atlanta	10.203.0.207	Atlanta, Engineer	HTTPS	https (443/tcp)	33 days 4 hours 4 minutes	
10.10.101.23	tops, Atlanta	10.202.30.126	Atlanta, Engineer	HTTPS	https (443/tcp)	33 days 4 hours 4 minutes	
10.10.31.48		0.3.1.104		SSH/SCP (unclassified)	ssh (22/tcp)	33 days 4 hours 4 minutes	
10.10.101.159	Desktops, Atlanta	10.202.3.110	Atlanta, Engineer	HTTPS	https (443/tcp)	8 hours 14 minutes 45s	
10.10.30.23	Domain Controllers, Atlanta	10.10.30.16	Domain Controllers, Atlanta, DNS Servers, NTP Servers	authentication	Undefined TCP (3268/tcp)	33 days 4 hours 5 minutes	
10.10.30.23	Domain Controllers, Atlanta	10.10.30.16	Domain Controllers, Atlanta, DNS Servers, NTP Servers	authentication	ldap (389/tcp)	33 days 4 hours 4 minutes	

Details

More details

Flow Query Basics - Filtering



Select host to investigate

All flows in which this host was a client or server

Flow Query Basics - Filtering

All flows for 10.10.200.79 in the last hour

Filter | Domain : ACME | Time : Last 1 hour

Client or Server Host : 10.10.200.79

Table | Short List

Flow Table - 68 records

Client User Name	Client Host	Client Host Groups	Server Host	Server C...	Server Host Groups	Duration	Application
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.32.24	RFC 1918	End User Devices, Atlanta, New York, Mail Servers	22 hours 50 minutes 25s	Undefined TCP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.32.24	RFC 1918	End User Devices, Atlanta, New York, Mail Servers	6 minutes 21s	HTTPS
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.31.33	RFC 1918	End User Devices, Atlanta, New York, File Servers	27s	HTTP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.30.12	RFC 1918	End User Devices, Domain Controllers, Atlanta, New York	1 minute 23s	HTTP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	38.109.139.142	United States	United States	1 minute 15s	HTTP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.200.1	RFC 1918	End User Devices, Atlanta, New York, Trusted Wireless	22 hours 50 minutes 55s	Undefined UDP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	10.10.30.12	RFC 1918	End User Devices, Domain Controllers, Atlanta, New York	9s	HTTP
billy	10.10.200.79	End User Devices, Atlanta, New York, Trusted Wireless	208-80-58-74.clickability.com (208.80.58.74)	United States	United States	1 minute 15s	HTTP

Flow Table: Visibility across NAT

Filter | Domain : demo.local | Time : From Sep 11, 2012 9:00:15 AM to Sep 11, 2012 9:20:15 AM

Cisco ASA : 192.168.200.6

Table | Short List

Flow Table - 11 records

User

Client Host	Translated Host	Client User Name	Server Host	Service Summary	Server Host Groups
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States

Inside local

Outside global

Server

Querying Events - Leveraging NSEL

Flow Action	Client Host	Client Host Groups	Server Host	Server Host Groups	Service Summary
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (90/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (900/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (648/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (720/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (100/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (1022/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (19/tcp)
Denied	168.192.200.22	United States			Undefined TCP (32/tcp)
Denied	168.192.200.22	United States			Undefined TCP (512/tcp)

Flow denied events over many ports

Flow Table – IPv6

Flow Table - 504 records

Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application
2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	2000:1:1:0:213:72ff:fe56:20e9	Atlanta IPv6	4 minutes 58s	SSH/SCP (unclassified)
2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	2000:1:1:0:213:72ff:fe56:20e9	Atlanta IPv6	6s	Undefined TCP
2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	2000:1:1:0:213:72ff:fe56:20e9	Atlanta IPv6	6s	Undefined TCP
2000:1:1:0:213:72ff:fe56:20e9	Atlanta IPv6	2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	50s	Undefined
2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	2000:1:2:0:204:23ff:feb4:eb25	Atlanta IPv6	< 1s	HTTP (unclassified)
2000:1:4:0:204:23ff:fe9e:f16e	Atlanta IPv6	2000:1:1:0:213:72ff:fe56:20e9	Atlanta IPv6	4 minutes 58s	HTTP (unclassified)

Host Groups – Targeted Monitoring

Host Group Dashboard for Engineers

Host Group Dashboard

Filter | Domain : ACME | Host Group : Engineer

Network | Security | Alarm Summary

Active High Concern Hosts - 1 Record

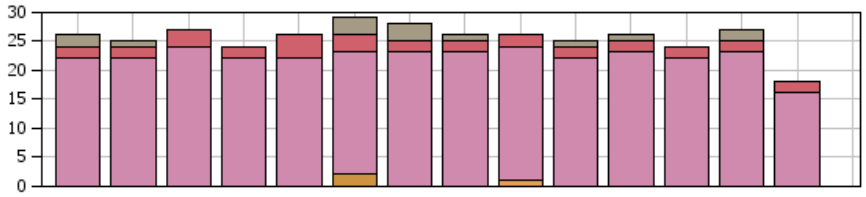
Host	CI	CI%
10.202.1.122	584,942	62%

Suspiciously behaving hosts

Active High Target Hosts - 4 recor...

Host	TI	TI%
10.202.3.110	62,710	84%
10.202.1.124	108,832	82%
10.202.3.112	138,770	76%
10.202.1.226	20,112	67%

Alarm Trend, Last 2 Weeks

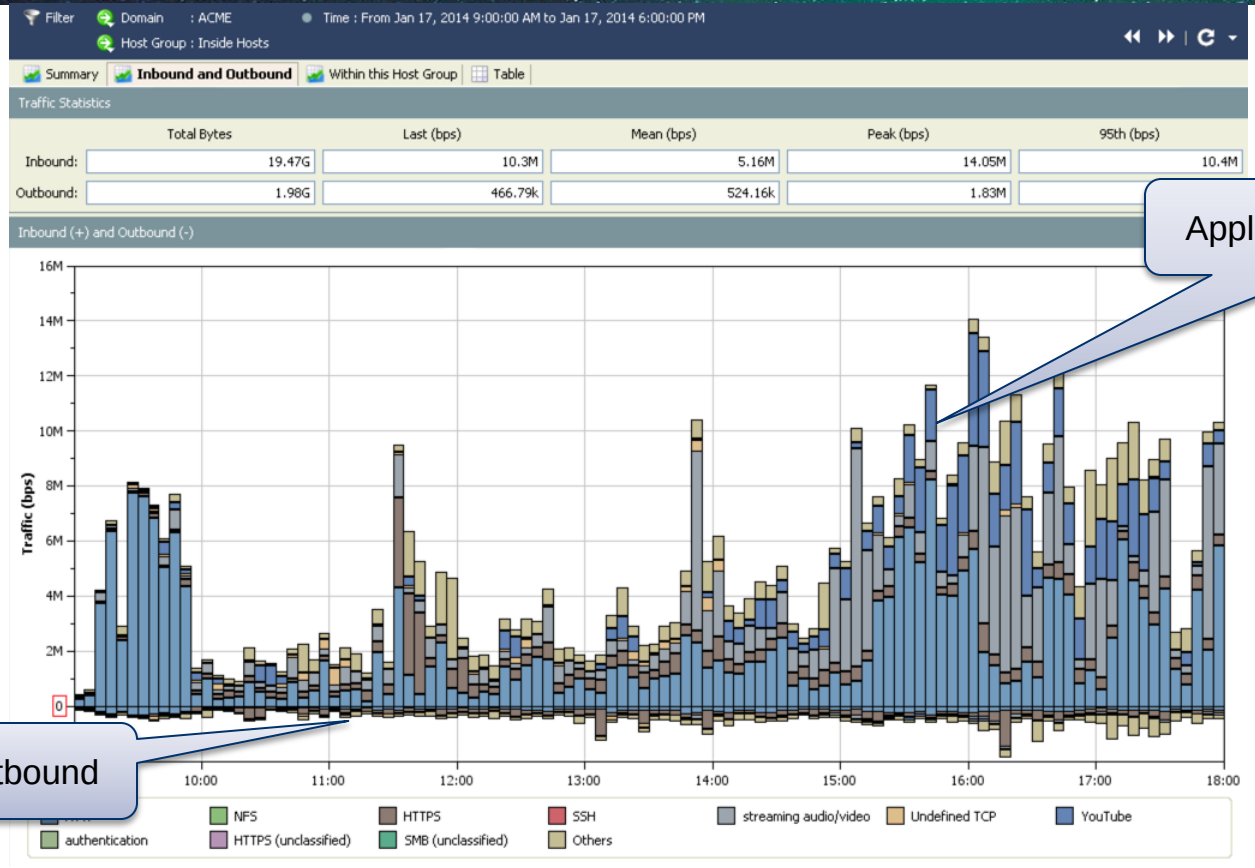


Active Alarms, Today (Unacknowledg...

Alarm	Source	Sourc...	Target	Targe...	Details	Start Active ...
High Volume Email	10.202.1.223	Atlanta, Engineer	Multiple Hosts		Double-click for details.	Apr 25, 2013 5:25:00 PM (8 minutes 58s ago)
High Volume Email	10.202.1.65	Atlanta, Engineer	Multiple Hosts		Double-click for details.	Apr 25, 2013 5:00:00 PM (33 minutes 58s ago)

Alarms

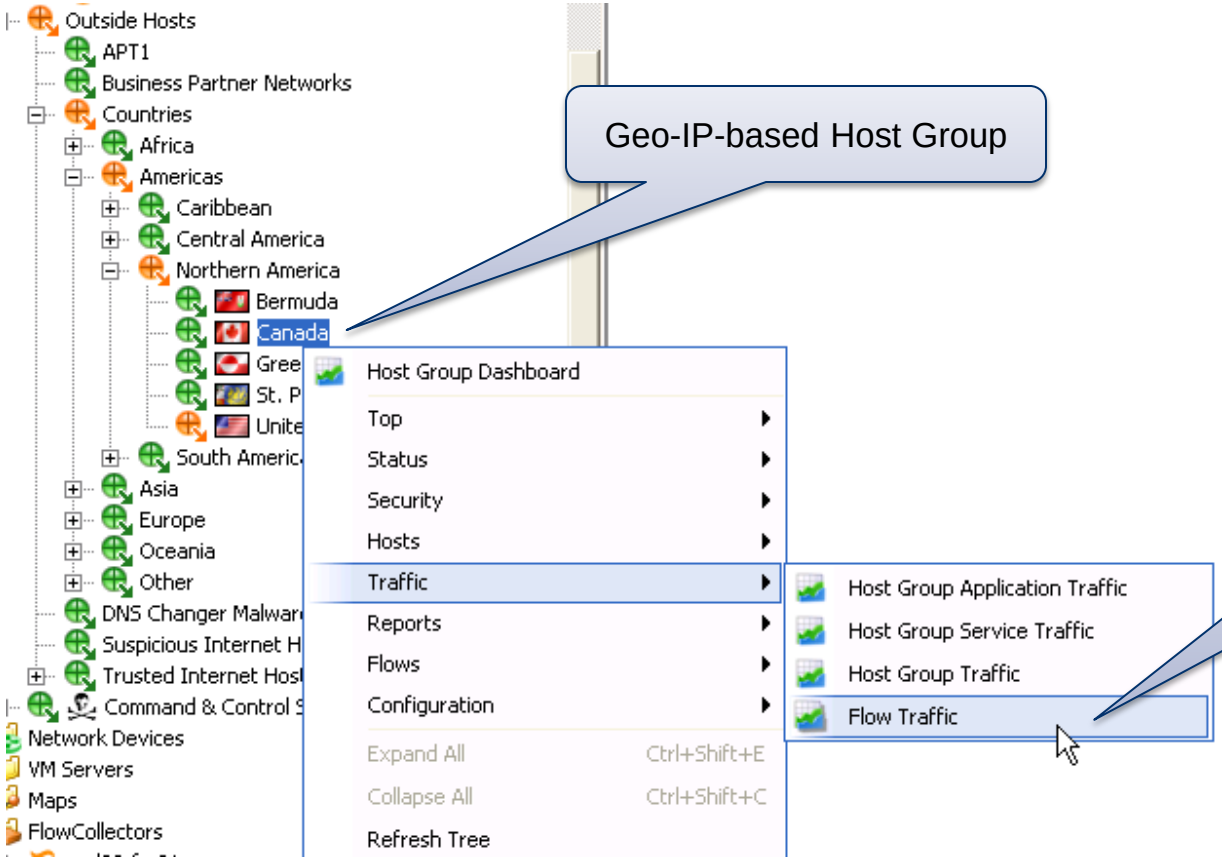
Host Groups – Application Report



Applications inbound

Applications outbound

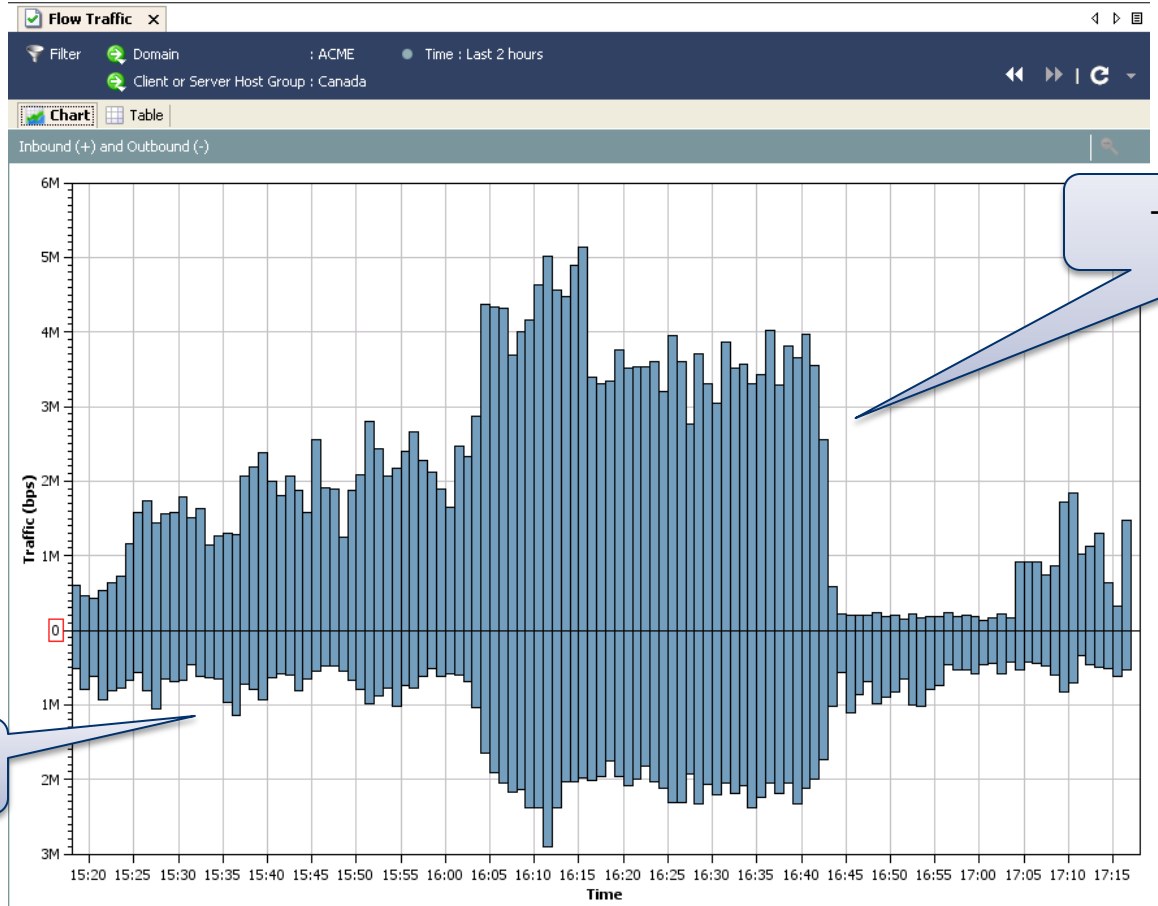
Host Groups – Targeted Reporting



Geo-IP-based Host Group

Summary chart of traffic inbound and outbound from this Host Group

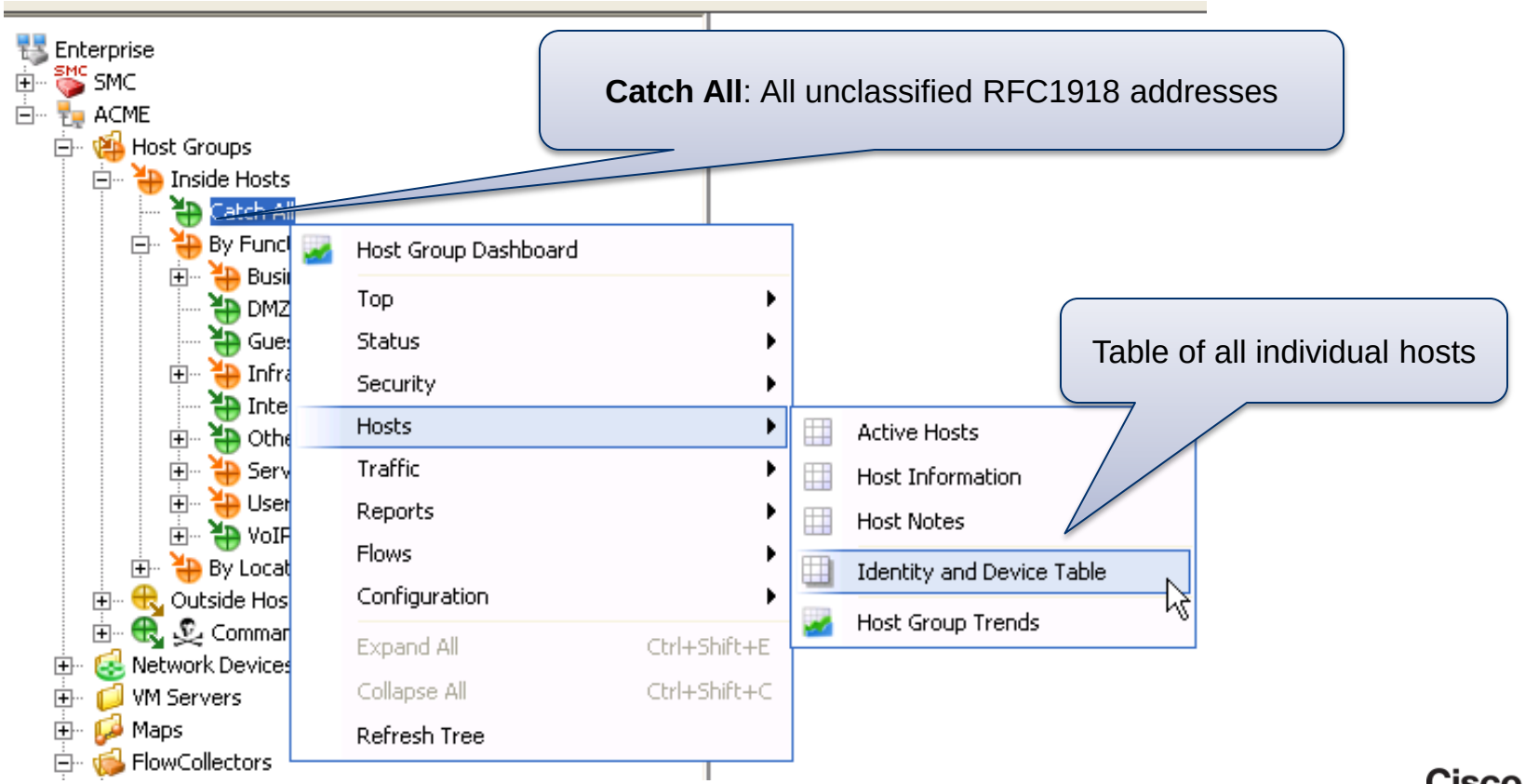
Host Groups – Targeted Reporting



Traffic inbound

Traffic outbound

Host Groups – Discovering Rogue Hosts



Catch All: All unclassified RFC1918 addresses

Table of all individual hosts

Host Groups – Discovering Rogue Hosts

Rogue Hosts

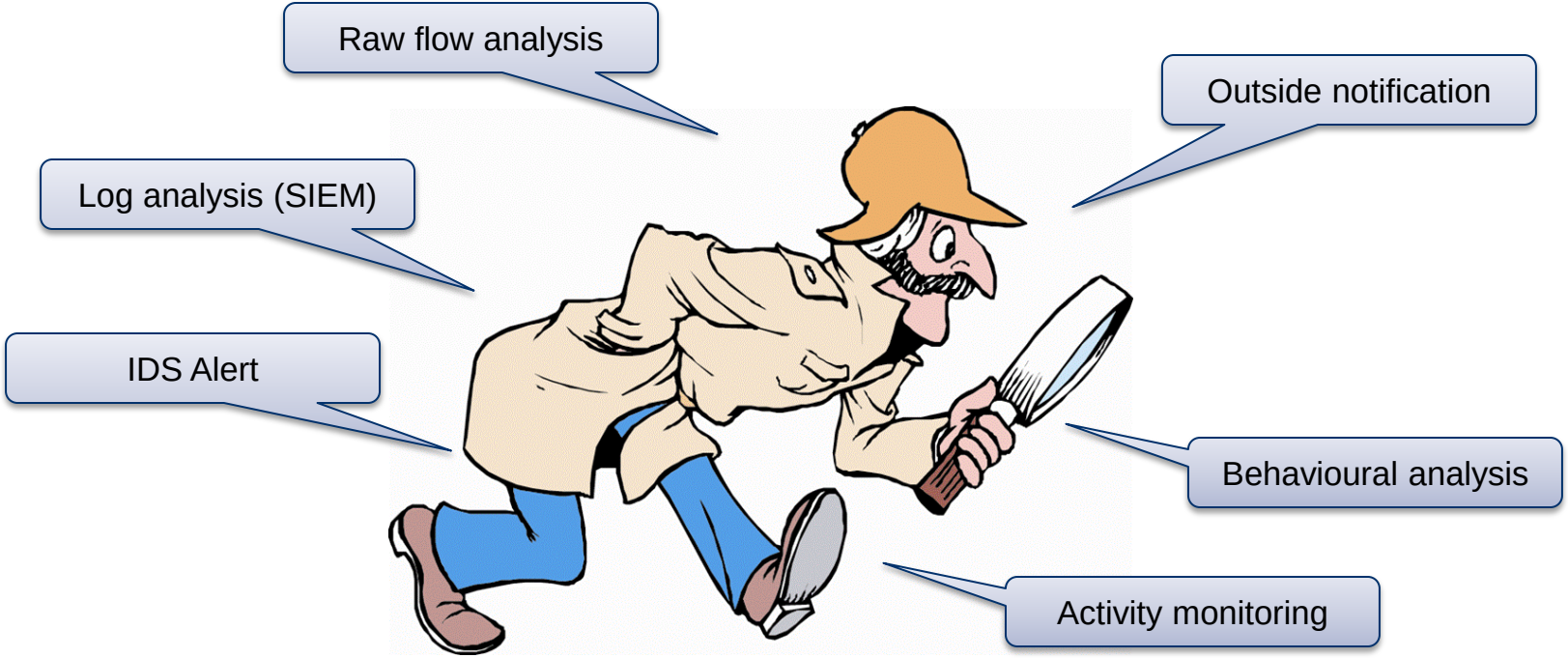
Identity and Device Table

Filter Domain : ACME
Host Group : Catch All

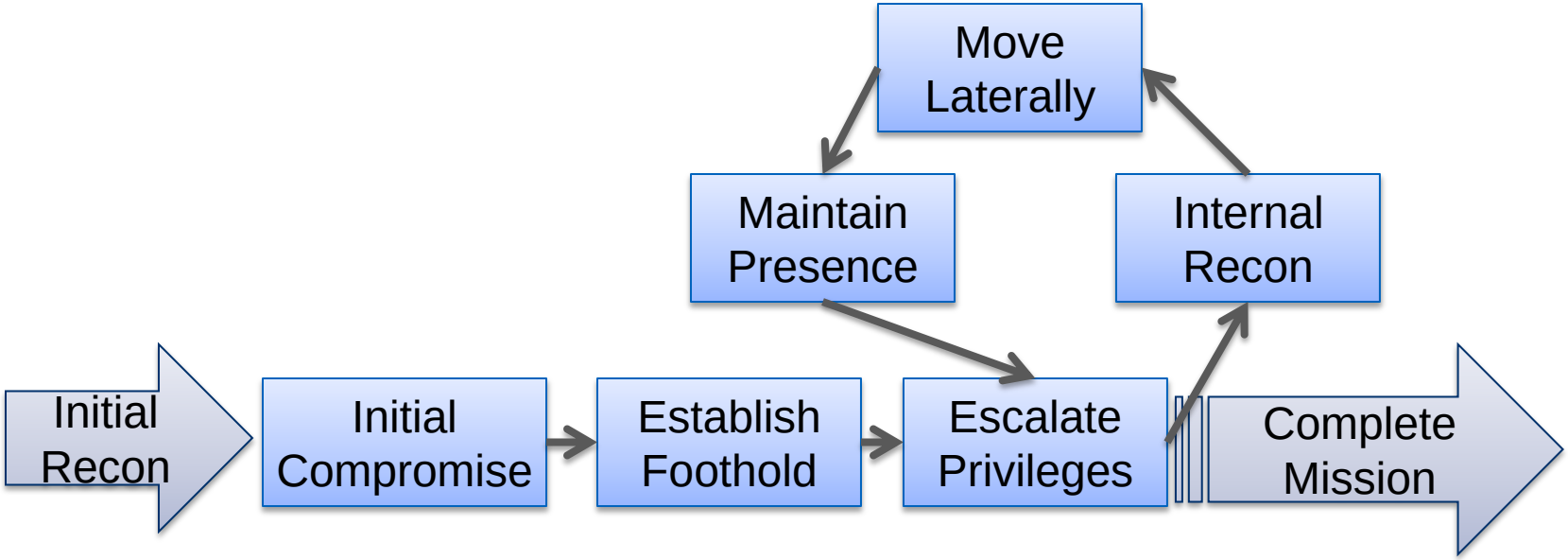
Identity and Device Table - 255 records

Start Active Time	End Active Time	User Name	Host	Host Groups	MAC Address	Device Type
Apr 27, 2013 6:17:41 PM (2 days 18 hours 28 minutes ago)	Current	isesim_user_7944	10.201.3.255	Catch All	f8:1e:df:57:0c:44 (Apple, Inc)	Apple-MacBook
Apr 27, 2013 6:17:41 PM (2 days 18 hours 28 minutes ago)	Current	isesim_user_1148	10.201.3.254	Catch All	f8:1e:df:13:c5:42 (Apple, Inc)	Apple-MacBook
Apr 27, 2013 6:17:41 PM (2 days 18 hours 28 minutes ago)	Current	isesim_user_8109	10.201.3.253	Catch All	f8:1e:df:63:20:4f (Apple, Inc)	Apple-MacBook
Apr 27, 2013 6:17:41 PM (2 days 18 hours 28 minutes ago)	Current	isesim_user_2386	10.201.3.252	Catch All	f8:1e:df:a2:33:4d (Apple, Inc)	Apple-MacBook
Apr 27, 2013 6:17:41 PM (2 days 18 hours 28 minutes ago)	Current	isesim_user_8686	10.201.3.251	Catch All	f8:1e:df:31:71:74 (Apple, Inc)	Apple-MacBook

Indicators of Compromise



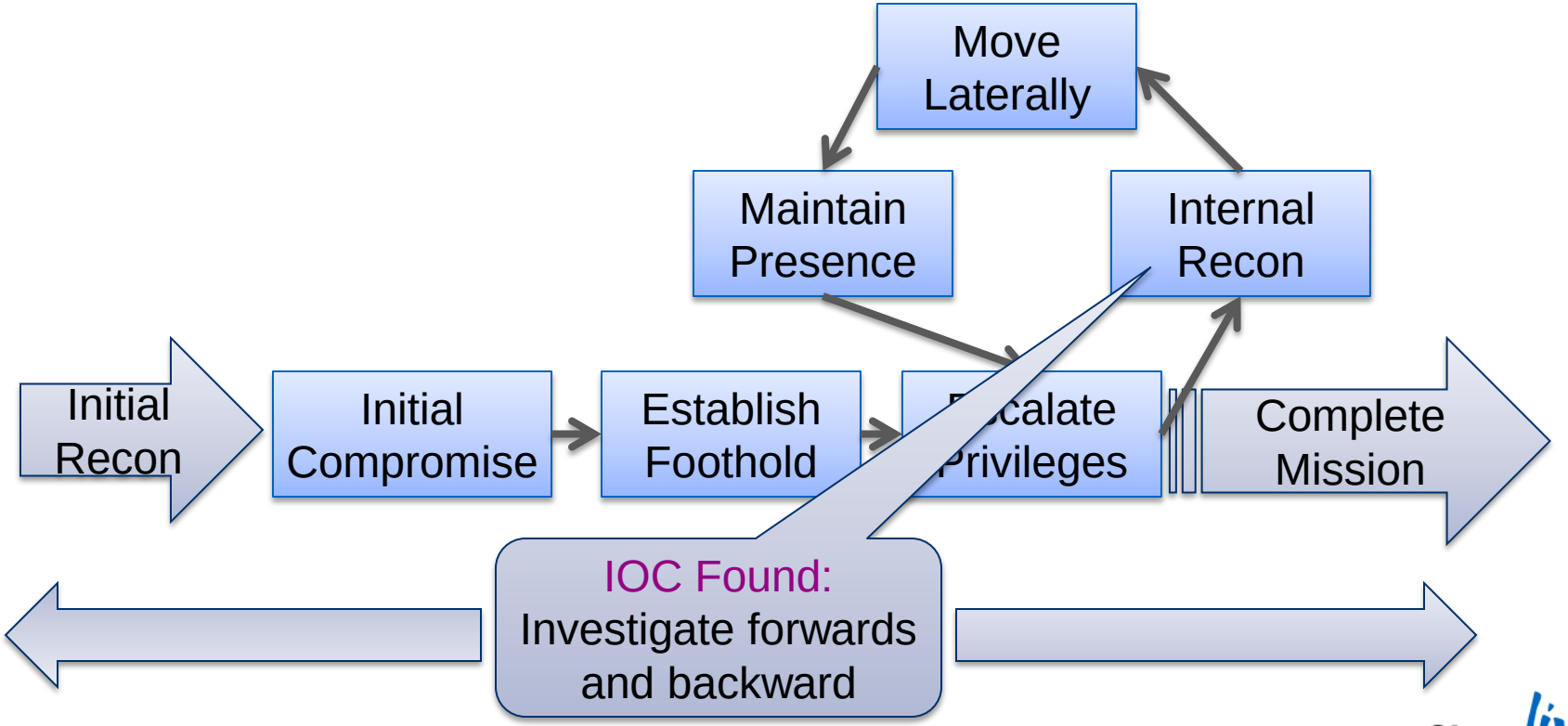
Attack Lifecycle Model (AKA the Kill Chain)



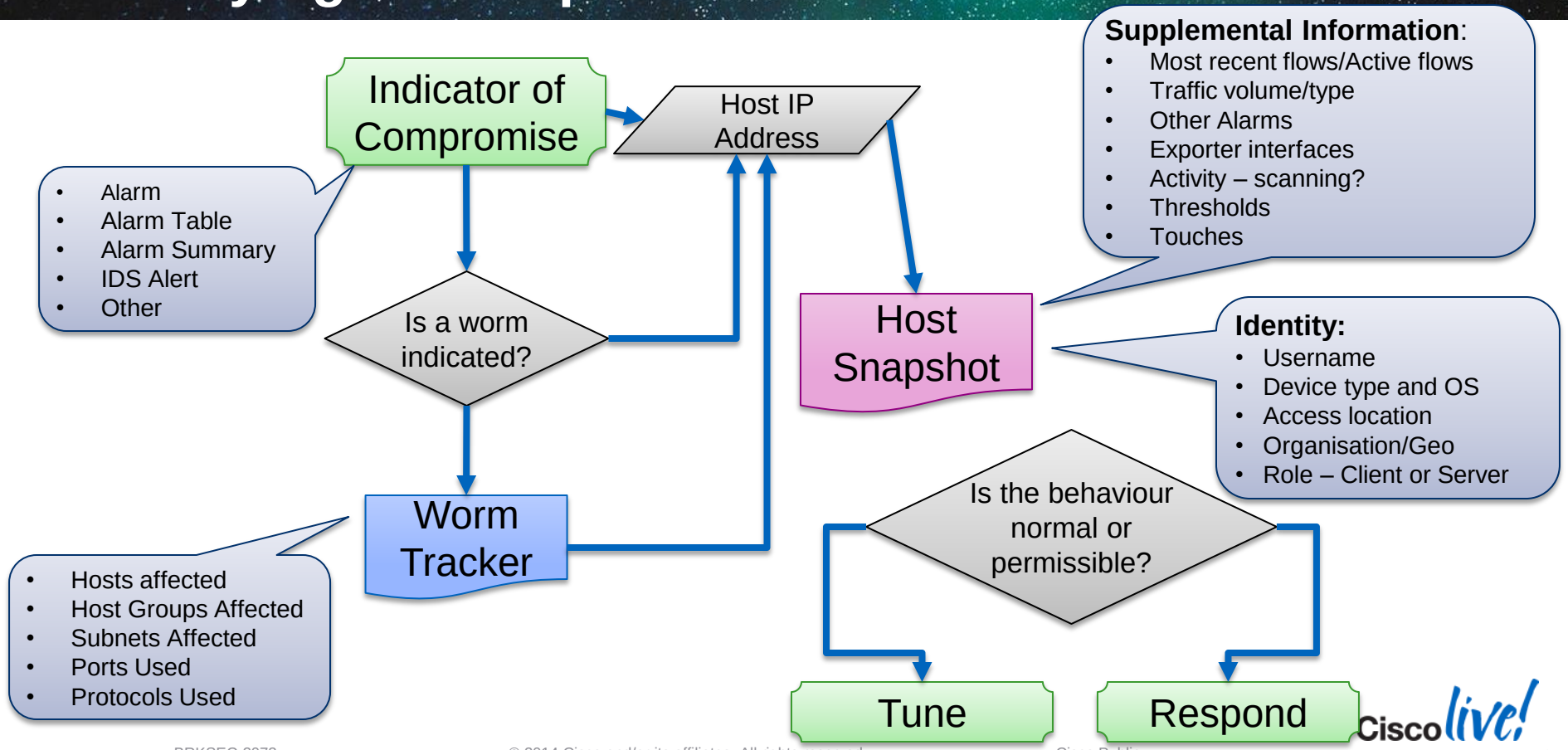
Mandiant APT1 Report: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Kill Chain: http://bit.ly/killchain

Building a Timeline

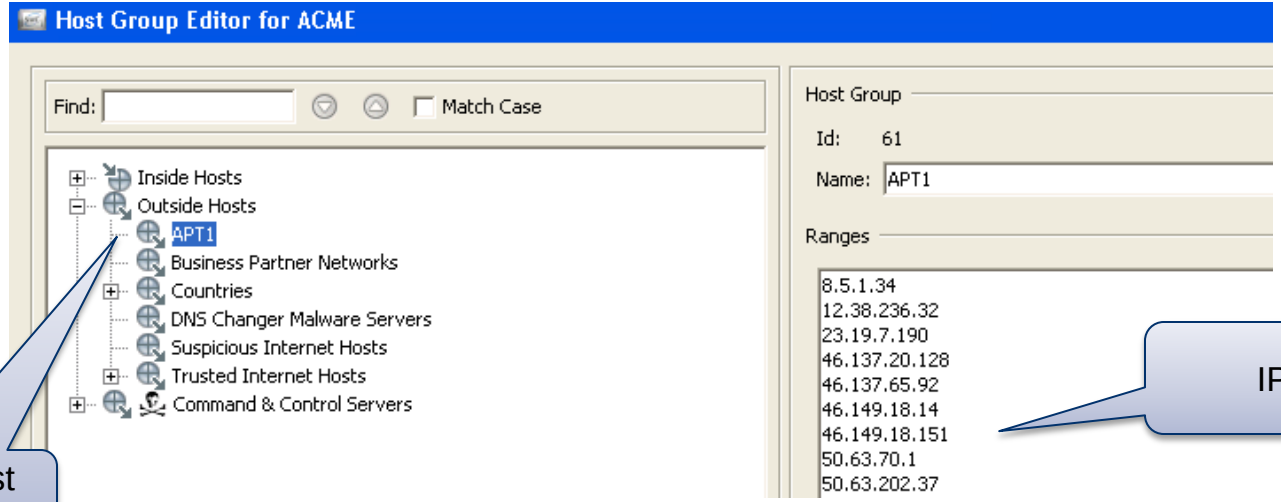


Identifying the Culprit



APT1

IOC: Mandiant publishes list of domain names and IP addresses known to be used by APT1



Create a Host Group for APT1

IP Addresses

APT1 – Host Locking Violation Alarm

Create a Host Lock Violation Alarm for communication to APT1

Set client hosts to all Inside Hosts

Set server hosts to APT1

Disallow all traffic

Trigger alarm on any unidirectional traffic

Host Locking: Add Rule

Name: Communication to APT1

Description:

Client Host Group: Inside Hosts [Browse...]

Server Host Group: Outside Hosts -> APT1 [Browse...]

- (•) Disallow all traffic except
- ( ) Allow all traffic except

☐ Services

- ☐ 0-hop
- ☐ 3pc
- ☐ a/n
- ☐ afs
- ☐ ah
- ☐ aol-im
- ☐ apple-net-assistant
- ☐ appleshare

☐ Applications

- ☐ ActiveX
- ☐ Adobe Connect
- ☐ authentication
- ☐ Blackberry
- ☐ Citrix
- ☐ Clearcase
- ☐ corporate email
- ☐ DHCP

☑ Unidirectional UDP traffic triggers alarm

☑ Unidirectional TCP traffic triggers alarm

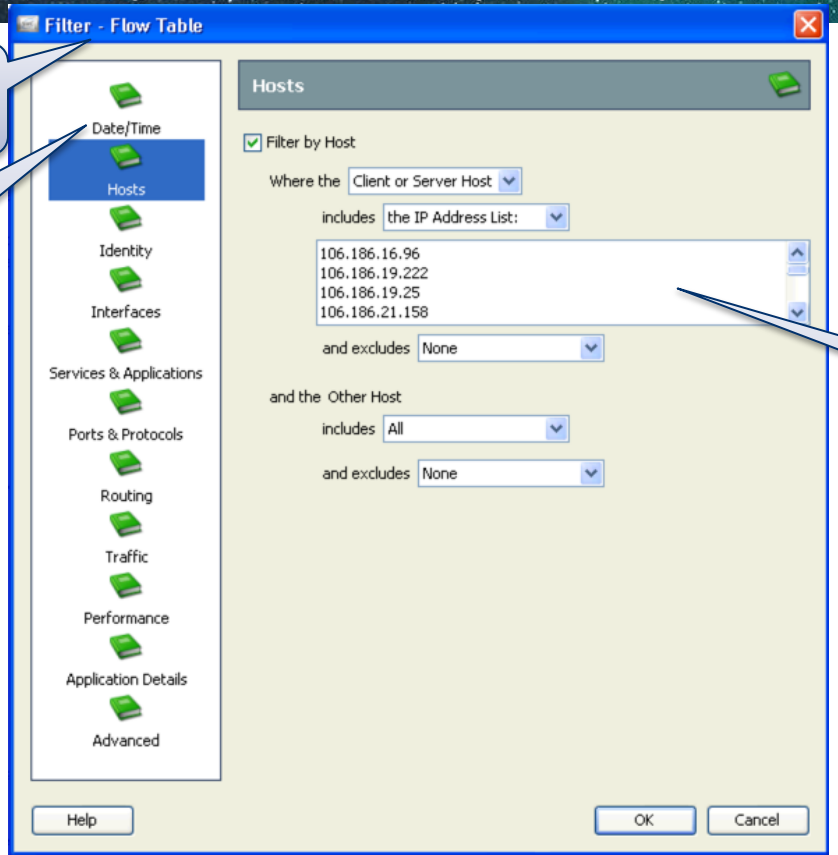
[Help] [OK] [Cancel]

APT1 - Investigate

You know today what you didn't know yesterday

Run a Flow Query

Over the last 90 days



Server or client includes the APT1 IP Address list

APT1 – Returned Flows

Infected hosts

FTP Transfers

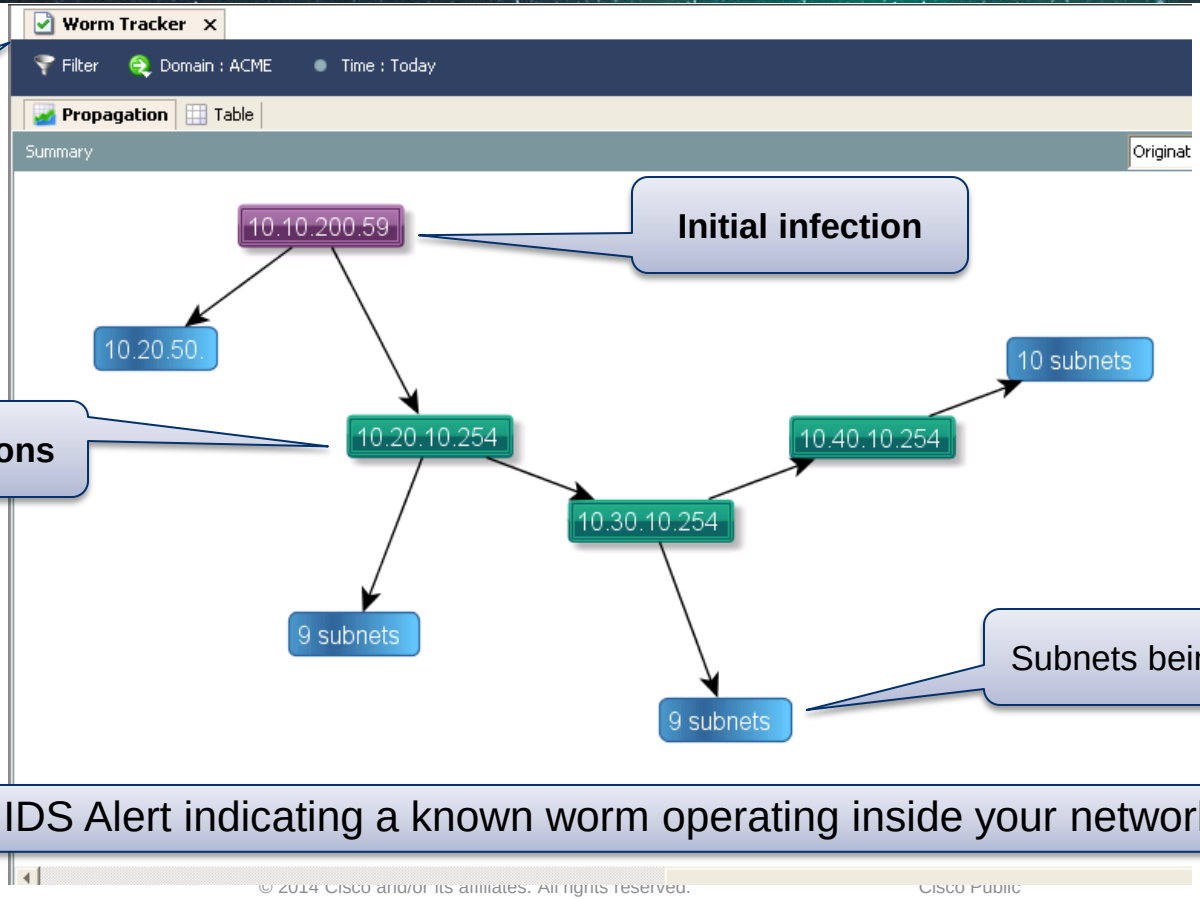
Table | Short List

Flow Table - 32 records

Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application	Total Bytes
10.210.7.38	File Servers	li527-96.members.linode.com (106.186.16.96)	Japan	18 minutes 59s	FTP (unclassified)	1.16G
10.10.31.48	File Servers	161.58.93.33	United States	19 minutes 1s	FTP (unclassified)	1.16G
10.50.100.83	File Servers	161.58.182.205	United States	38s	FTP	2.2k

APT1 Servers

Investigating Malware Spread: Worm Tracker



Worm tracker

Initial infection

Secondary infections

Subnets being scanned

IOC: IDS Alert indicating a known worm operating inside your network

Investigating Malware Spread: Host Snapshot

Everything the system knows about 10.10.200.59

Start with CI Events. We notice significant scanning activity

Domain : ACME Time : April 15, 2013

Host : 10.10.200.59

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

Host is Source of CI Events - 22 records

Start Active Time	Last Active Time	Target Host Groups	Target Host	Concern I...	CI Events
Apr 15, 2013 12:55:37 AM (23 hours 54 minutes 19s ago)	Apr 15, 2013 9:55:46 PM (2 hours 54 minutes 10s ago)	Catch All	10.20.40.0/24	1,767,533	Addr_Scan/tcp-135(3533)
Apr 15, 2013 12:55:37 AM (23 hours 54 minutes 19s ago)	Apr 15, 2013 9:55:46 PM (2 hours 54 minutes 10s ago)	Catch All	10.20.10.0/24	1,620,254	Addr_Scan/tcp-135(3254)
Apr 15, 2013 12:55:37 AM (23 hours 54 minutes 19s ago)	Apr 15, 2013 9:55:46 PM (2 hours 54 minutes 10s ago)	Catch All	10.20.20.0/24	1,602,202	Addr_Scan/tcp-135(3202)
Apr 15, 2013 12:55:37 AM (23 hours 54 minutes 19s ago)	Apr 15, 2013 9:55:46 PM (2 hours 54 minutes 10s ago)	Catch All	10.20.70.0/24	1,596,186	Addr_Scan/tcp-135(3186)
Apr 15, 2013 7:39:59 AM (17 hours 9 minutes 57s ago)	Apr 15, 2013 6:58:18 PM (5 hours 51 minutes 38s ago)	Atlanta, File Servers	10.10.31.0/24	435,904	Ping_Scan(904)
Apr 15, 2013 7:44:19 AM (17 hours 5 minutes 37s ago)	Apr 15, 2013 7:00:49 PM (5 hours 49 minutes 7s ago)	Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.0/24	252,514	Addr_Scan/tcp-27001(6), Addr_Scan/tcp-27009(168), Ping_Scan(340)
Apr 15, 2013 7:44:26 AM (17 hours 5 minutes 30s ago)	Apr 15, 2013 6:58:42 PM (5 hours 51 minutes 14s ago)	Domain Controllers, Atlanta, NTP Servers	10.10.30.19	150,704	Reset/tcp-27000(24), Reset/tcp-27001(1100), Reset/tcp-27002(1091), Reset/tcp-27003(1088), Reset/tcp-27004(1200),

Investigating Malware Spread: Identity

Telemetry from the ISE

Host : 10.10.200.59

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

Identity and Device Table - 1 record

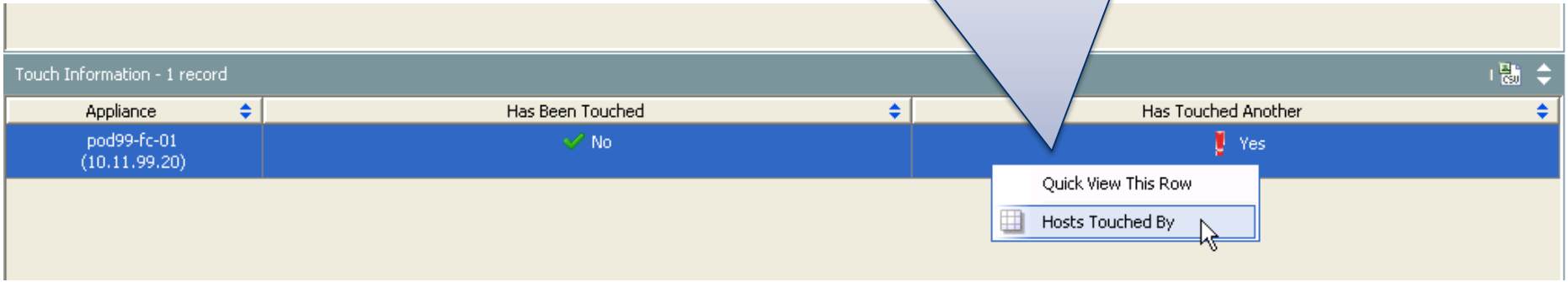
Start Active Time	End Active Time	User Name	MAC Address	Device Type	Domain Name	Network ...	Netwo...	Securi...
Jun 10, 2013 11:27:37 PM (8 days 20 hours 26 minutes ago)	Current	bmcmahon	00:d0:b8:0d:fd:27 (Iomega Corporation)	Windows7-Workstation	LC	Unknown Exporter (10.10.1.1)	GigabitEthernet5/37	

Username

Infected machine

Investigating Malware Spread: Touched Hosts

This infected host has established a connection with another host



Investigating Malware Spread: Touched Hosts

All hosts touched by 10.10.200.59

Filter Domain : ACME Time : April 15, 2013
High CI Host : 10.10.200.59

Summary - 57 records summarized into 14 records

Start Date/Time	End Date/Time	High CI Host Groups	High CI Host	Touched Host Groups	Touched Host
Apr 15, 2013 12:53:21 PM (11 hours 58 minutes 40s ago)	Apr 15, 2013 10:07:36 PM (2 hours 44 minutes 25s ago)	Atlanta, Trusted Wireless	10.10.200.59	Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.17
Apr 15, 2013 9:49:26 AM (15 hours 2 minutes 35s ago)	Apr 15, 2013 9:57:19 PM (2 hours 54 minutes 42s ago)	Atlanta, Trusted Wireless	10.10.200.59	Atlanta, File Servers	10.10.31.33
Apr 15, 2013 9:40:04 AM (15 hours 11 minutes 57s ago)	Apr 15, 2013 7:08:28 PM (5 hours 43 minutes 33s ago)	Atlanta, Trusted Wireless	10.10.200.59	Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.15
Apr 15, 2013 12:53:32 PM (11 hours 58 minutes 29s ago)	Apr 15, 2013 7:02:39 PM (5 hours 49 minutes 22s ago)	Atlanta, Trusted Wireless	10.10.200.59	Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.16
Apr 15, 2013 12:59:26 PM (11 hours 52 minutes 35s ago)	Apr 15, 2013 6:59:56 PM (5 hours 52 minutes 5s ago)	Atlanta, Trusted Wireless	10.10.200.59	Atlanta, File Servers	10.10.31.48
Apr 15, 2013 3:57:55 PM (8 hours 54 minutes 6s ago)	Apr 15, 2013 6:58:29 PM (5 hours 53 minutes 32s ago)	Atlanta, Trusted Wireless	10.10.200.59	Atlanta, File Servers	10.10.31.46
Apr 15, 2013 6:55:46 PM (5 hours 56 minutes 15s ago)	Apr 15, 2013 6:55:46 PM (5 hours 56 minutes 15s ago)	Atlanta, Trusted Wireless	10.10.200.59	Catch All	10.20.10.254

High Concern Index

Baseline deviated by 2,432%!

Concern Index

Filter | Domain : ACME | Time : Toda

Summary - 92 records summarized into 92 records

Host Groups	Host	CI	CI%	Alarms	Alerts
New York, Desktops	10.50.100.83	243,231,761	2,432%		Ping, Rejects, TCP_Scan
Desktops, Atlanta	10.10.101.27	153,644,484	1,536%	High Concern Index	Ping, Ping_Scan
Desktops, Atlanta	10.10.101.24	117,213,499	1,172%		Ping, Ping_Scan, Rejects, TCP_Scan
Domain Controllers, Atlanta	10.10.30.28	32,760,657	328%		High_Volume_Email, Ping, Ping_Scan, Rejects, TCP_Scan, UDP_Scan
Atlanta, Trusted Wireless	10.10.200.59	21,345,906	213%		Ping, Ping_Scan, Port_Scan, Rejects, TCP_Scan, TCP_Stealth

What was this Host up to?

Target – entire subnet?

Filter | Domain : ACME | Time : Today
Host : 10.50.100.83

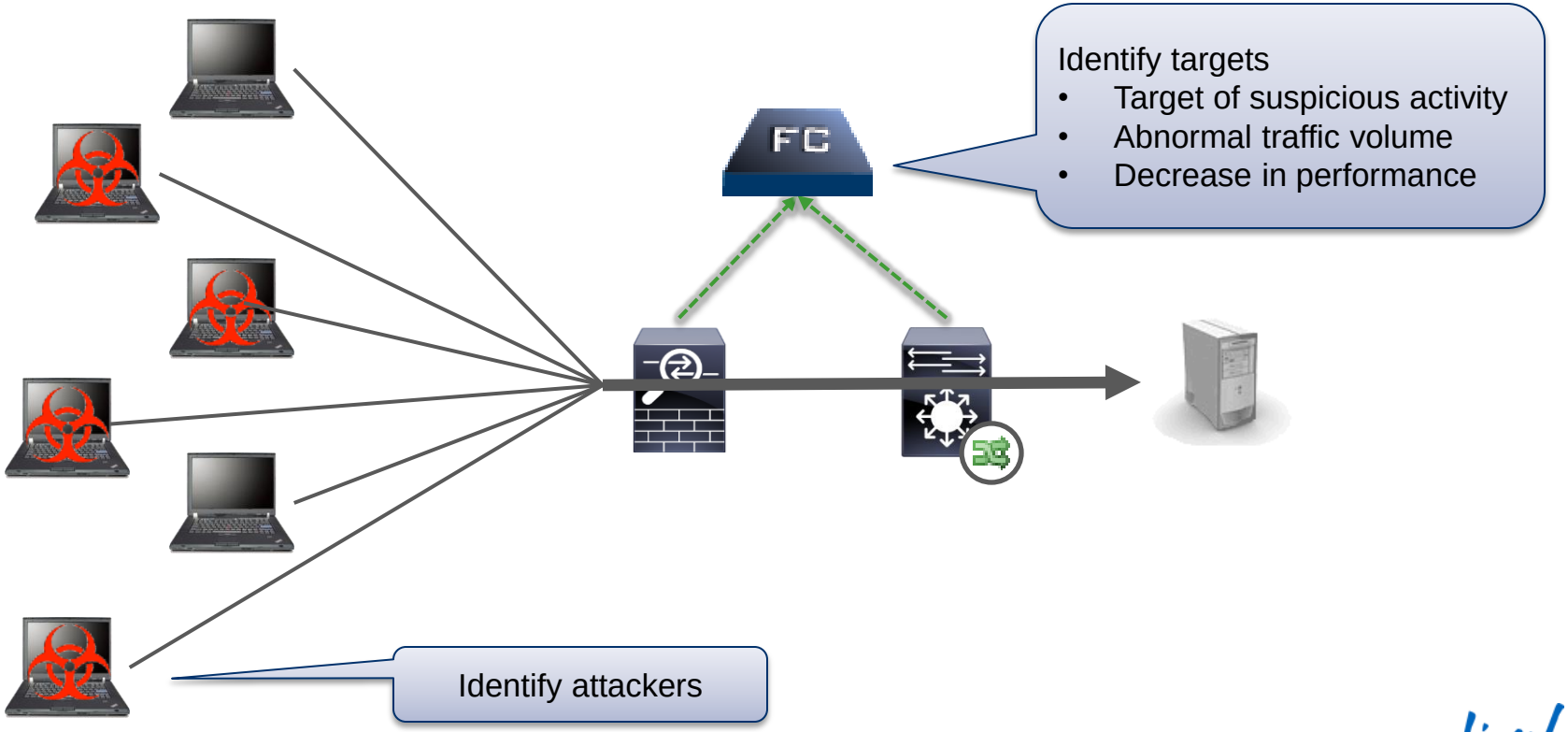
Identification | Alarms | Security | **CI Events** | Top Active Flows | ...w, DHCP & Host Notes | Exporter Interfaces

Host is Source of CI Events (High CI) - 25 records

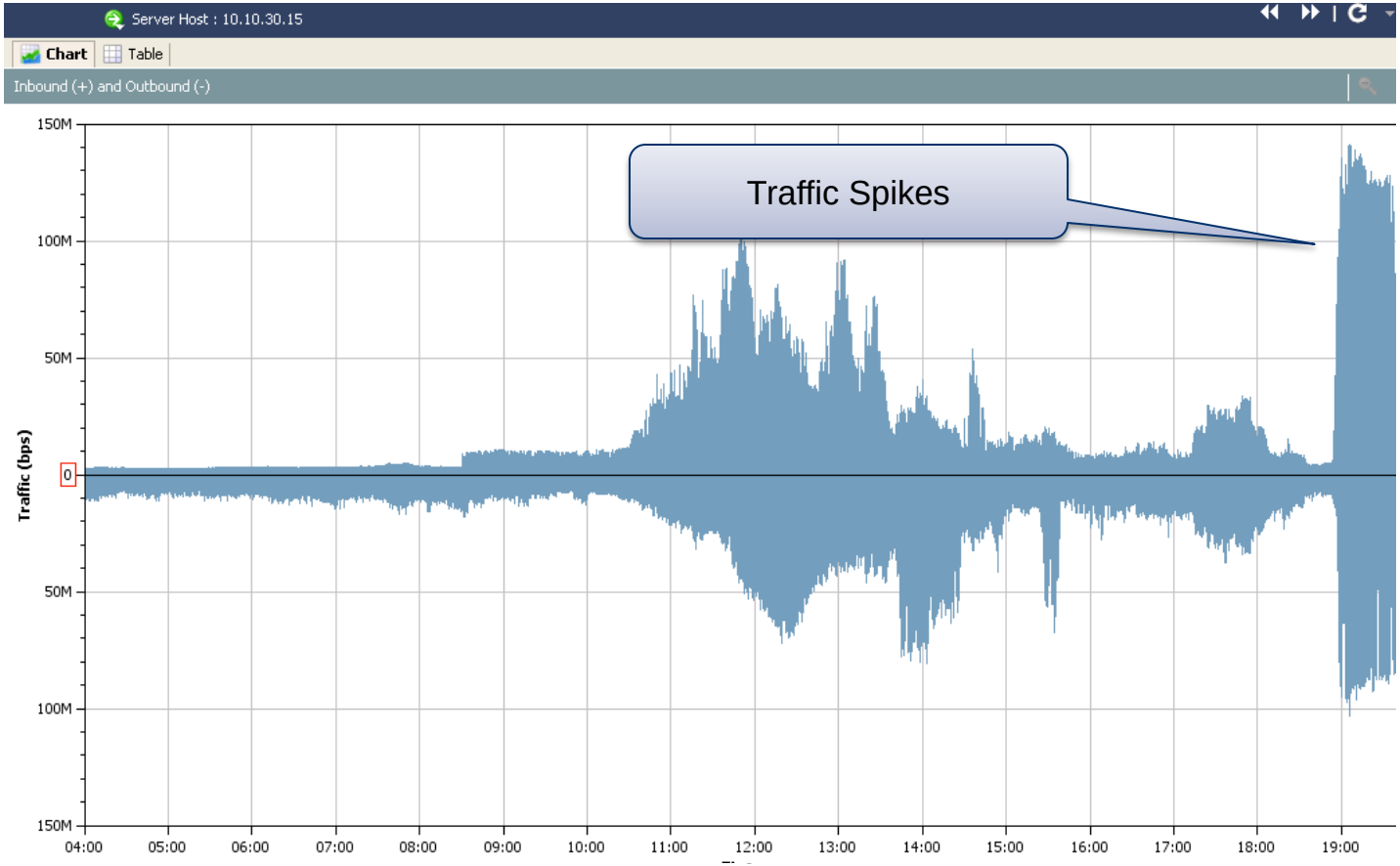
Start Active Time	Last Active Time	Target Host Groups	Target Host	Concer...	CI Events
Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.2.0/24	5,765,795	Addr_Scan/tcp-445(11795)
Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.1.0/24	5,600,479	Addr_Scan/tcp-445(11479)
Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.3.0/24	5,591,328	Addr_Scan/tcp-445(11328)
Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.0.0/24	5,576,380	Addr_Scan/tcp-445(11380)
Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.6.0/24	5,534,438	Addr_Scan/tcp-445(11438)

Scanning on TCP-445

NetFlow and (D)DoS Detection

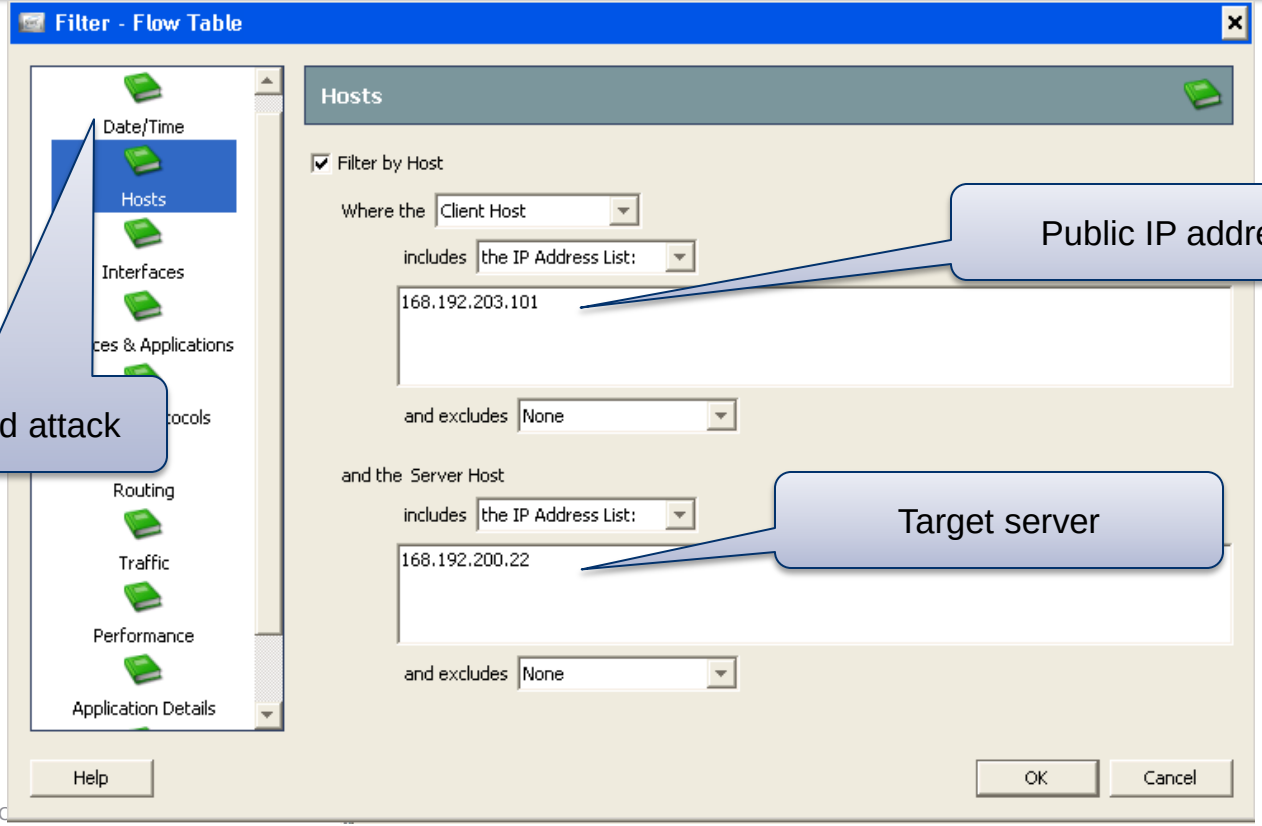


Volumetric DDoS



Identifying a DDoS Participant

IOC: Notification from 3rd party that your IP Address is participating in a DDoS



Time of reported attack

Public IP address

Target server

Identifying a DDoS Participant

Time of reported attack

Filter Domain : demo.local Time : From Sep 11, 2012 9:00:15 AM to Sep 11, 2012 9:20:15 AM

Cisco ASA : 192.168.200.6

Validate attack activity

Table Short List

User

Flow Table - 11 records

Client Host	Translated Host	Client User Name	Server Host	Service Summary	Server Host Groups
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	billy	168.192.200.22	http (80/tcp)	United States

Inside local

Outside global

Target Server

Identify a DDoS Participant

Host snapshot

192.168.201.100

Filter | Domain : demo.local | Time : Today

Host : 192.168.201.100

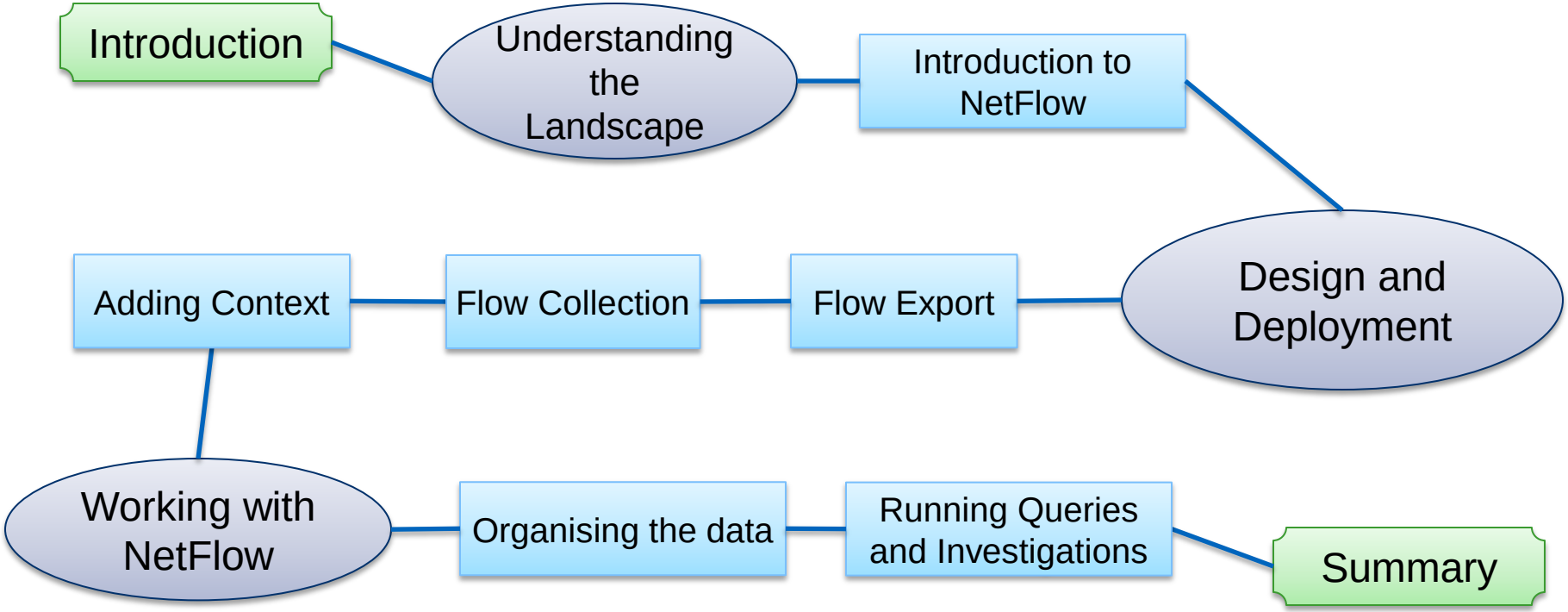
Identification | Alarms | Security | **CI Events** | Top Active Flows | Identity, DHCP & Host Notes | Exporter Interfaces

Host is Source of CI Events (High CI) - 2 records

Start Active Time	Last Active Time	Target Host Groups	Target Host	Concer...	CI Events
Sep 11, 2012 3:40:07 AM (7 hours 10 minutes 32s ago)	Sep 11, 2012 3:44:41 AM (7 hours 5 minutes 58s ago)	United States	65.197.197.0/24	15,066	Addr_Scan/tcp-80(66)
Sep 10, 2012 10:22:36 PM (12 hours 28 minutes 3s ago)	Sep 11, 2012 8:46:20 AM (2 hours 4 minutes 19s ago)	Catch All	192.168.200.10	6	ICMP_Port_Unreach(3)

Other suspicious activity

Agenda



Links and Recommended Reading

More about the Cisco Cyber Threat Defence Solution:

http://www.cisco.com/go/threatdefense

http://www.lancope.com

Recommended Reading

Cyber Threat Defence Cisco Validated Design Guide:

http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber_threat_defense_design_guide.pdf

Key Takeaways

Modern threats are consistently bypassing the security perimeter

Threat Detection requires visibility and context into network traffic

NetFlow and the Lancope StealthWatch System provide actionable security intelligence




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo 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 www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 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

CISCO™