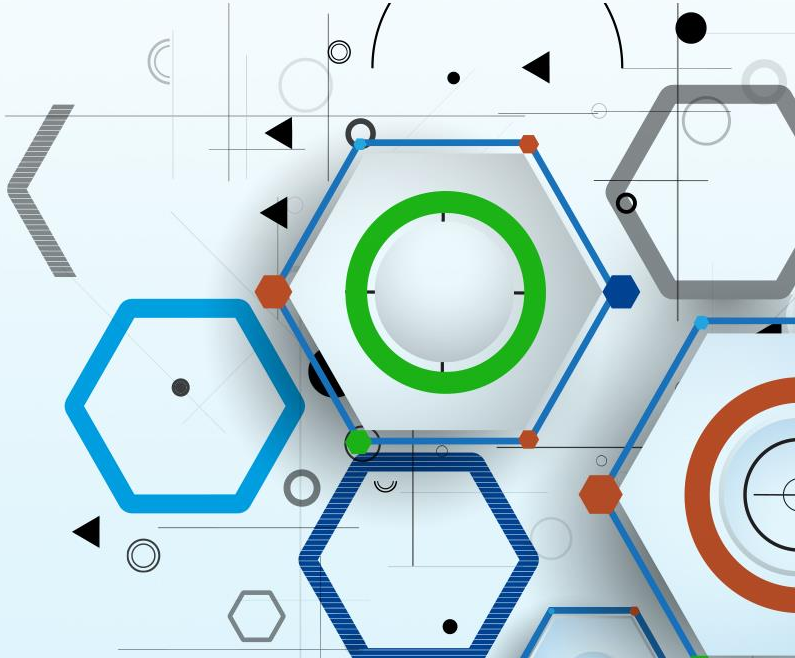
Monitorování chování sítě a detekce bezpečnostních incidentů

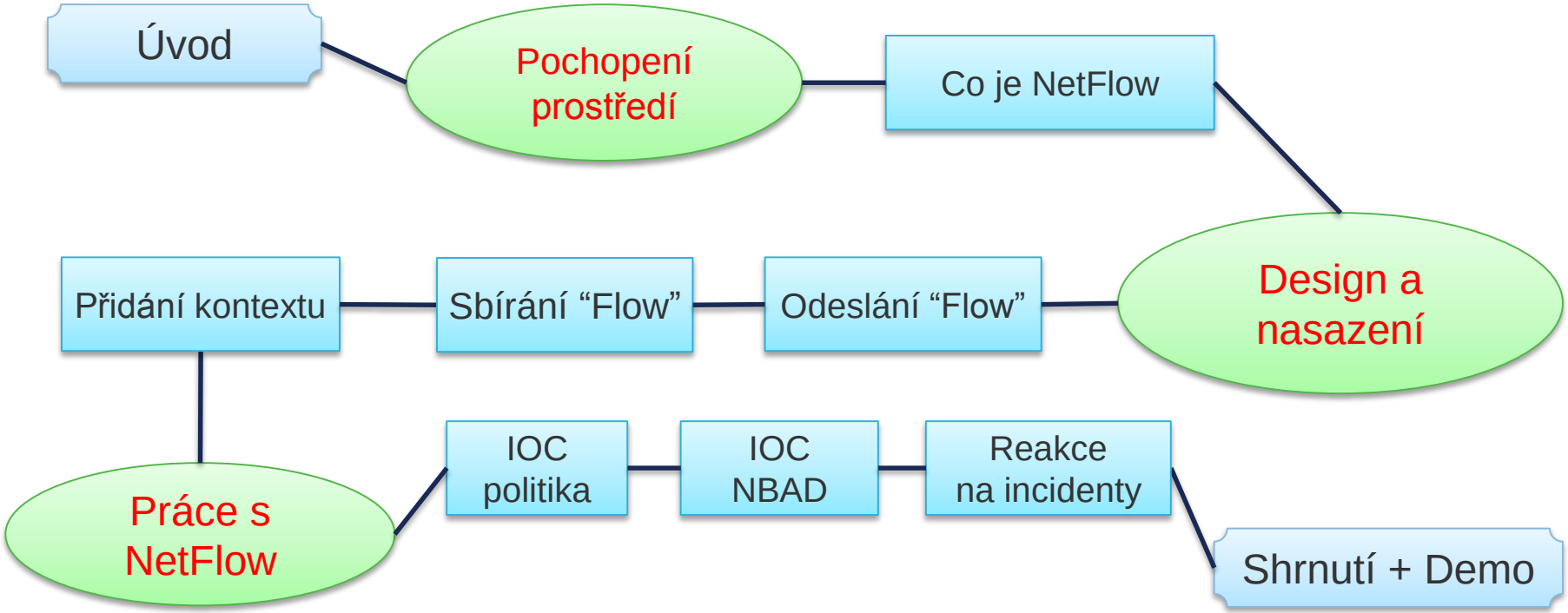
- **SEC4** DETAIL/L2

Andrej Jeleník - Systems Engineer



Agenda

1. Prostředí a co je NetFlow?
2. Jak získat údaje / důkazy (D & D)
3. Hodnota dat / důkazů (analýza NetFlow)



Na co se zaměříme?

Hrozby uvniř sítě

Zvládnutí hrozeb uvnitř sítě

Kontrola přístupu
- Kdo a co se snaží dostat do sítě

Jste kdo tvrdíte že jste, a to jsou zdroje, ke kterým máte povolen přístup na základě Vašich přihlašovacích údajů.

Segmentace
- Definuj co mohou dělat

Zvládnutí hrozeb uvnitř sítě

Kontrola pohybu škodlivého obsahu prostřednictvím kontrolních bodů

To je to, co je dovoleno vnášet do bezpečné zóny / sítě.

Kontrola obsahu

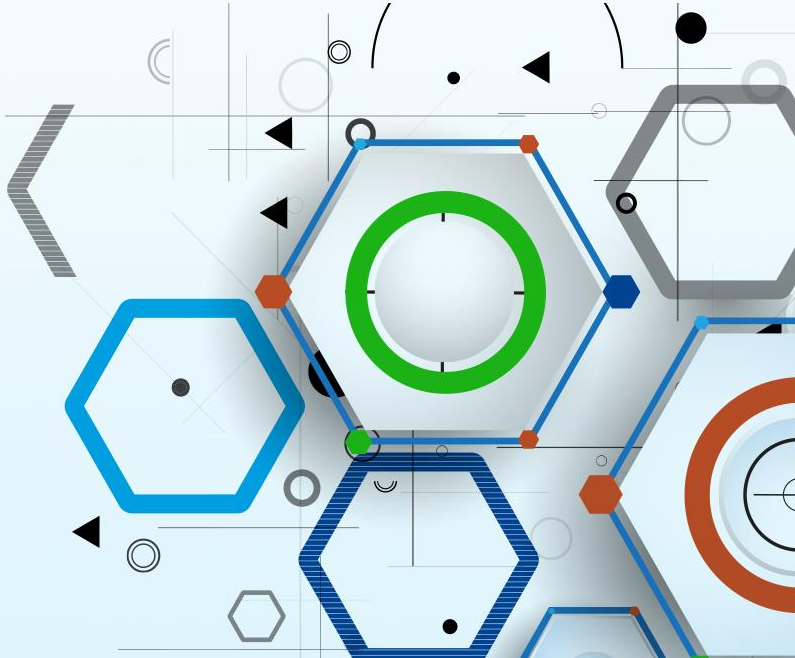
- Hluboká viditelnost obsahu na kontrolních bodech

Zvládnutí hrozeb uvnitř sítě

A teď sledovat činnost uvnitř kontrolované a zabezpečené zóny.

Monitorovaný prostor poskytuje viditelnost a vyšší bezpečnost.

NetFlow



Introduction to NetFlow

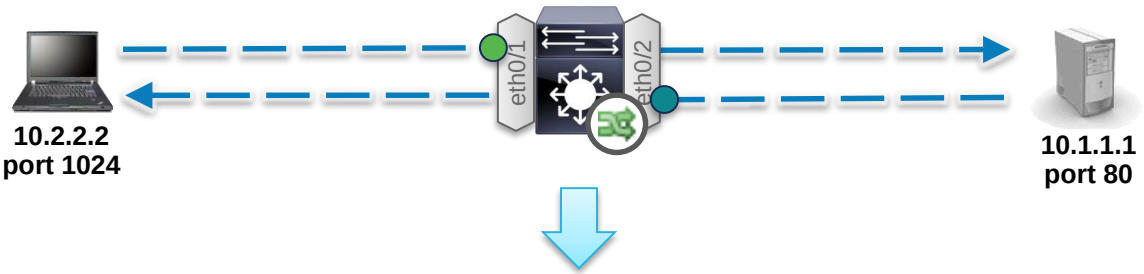
- Developed by Cisco in 1996 as a packet forwarding mechanism
  - Uses a fixed seven tuples of IP information to identify a flow
  - Reporting is based on Flow and not necessarily per-packet

- Various versions exist version 1 through 9, with 5 being the most popular and 9 being the most functional
  - Traditional NetFlow (TNF) – fixed info to identify a flow
  - Flexible Netflow (FNF) – user defines how to identify a flow

- NetFlow will let you understand who, what, when, where, and how network traffic is flowing

- Flexible NetFlow fully supported in IOS 15.0 and up & IOS XE 3.1S and up

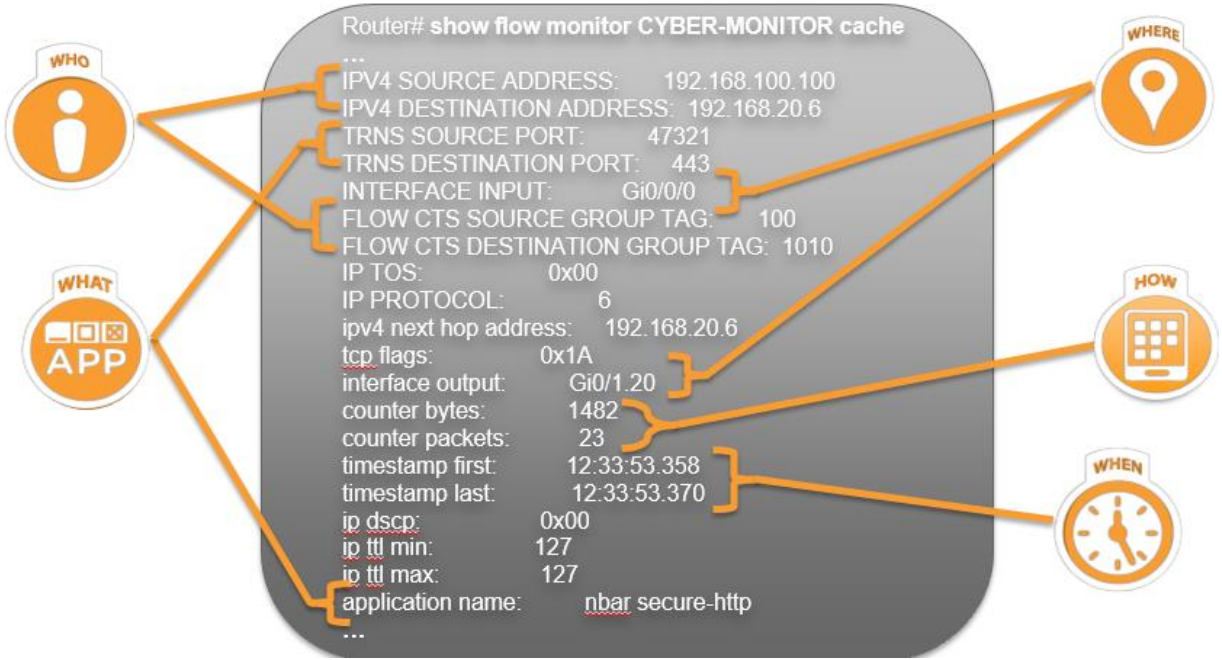
NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100	SYN,ACK,FIN

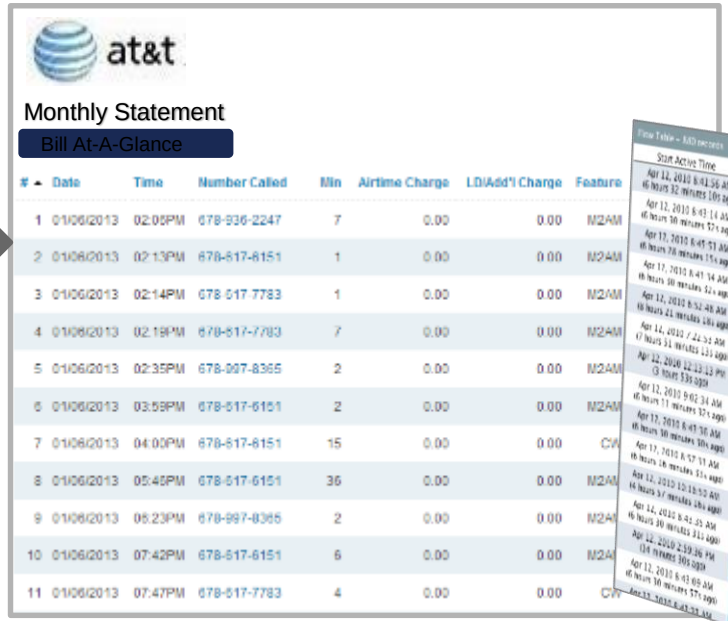
NetFlow = Visibility

A single NetFlow Record provides a wealth of information

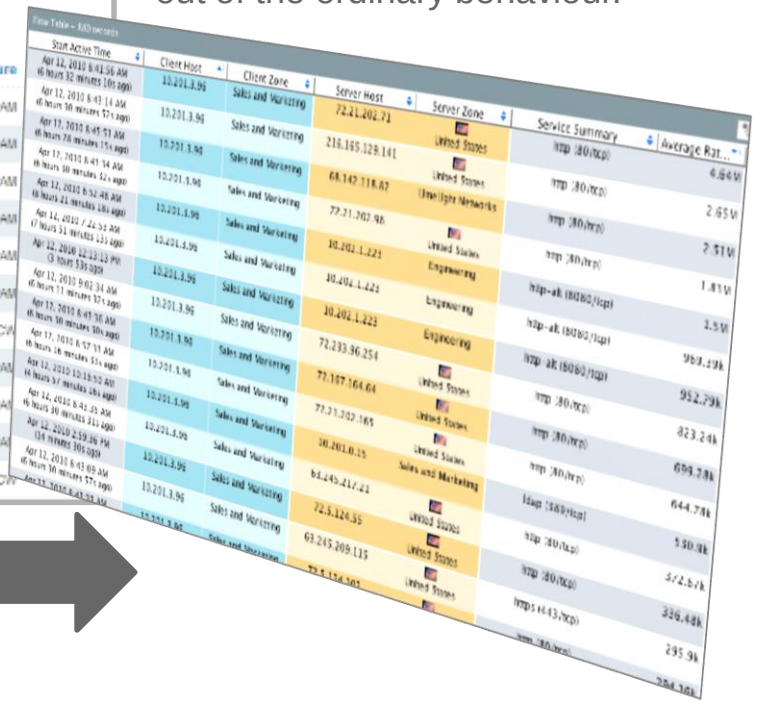


NetFlow - The Network Phone Bill

Telephone Bill



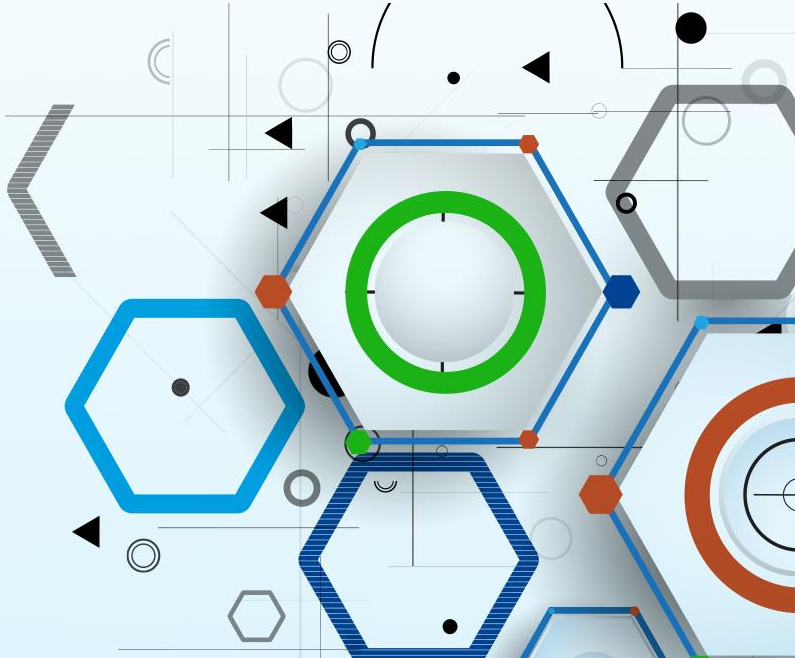
Flow Record



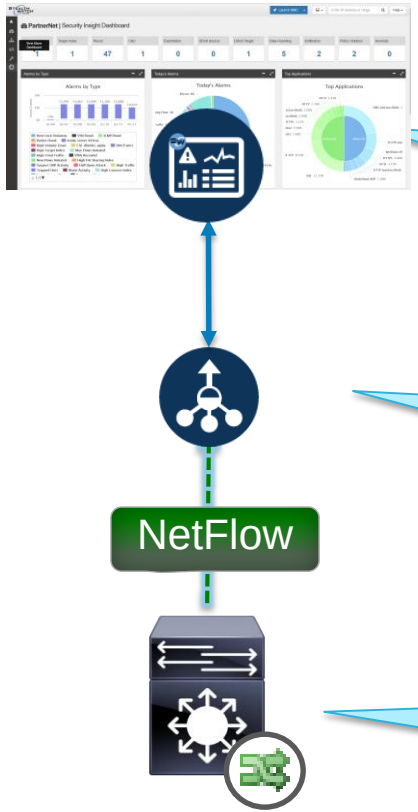
NetFlow = shows you the **who, what, where and when**. It's a phone bill, which we use to look for out of the ordinary behaviour.

Viditelnost

Design a nasazení



NetFlow Deployment Architecture

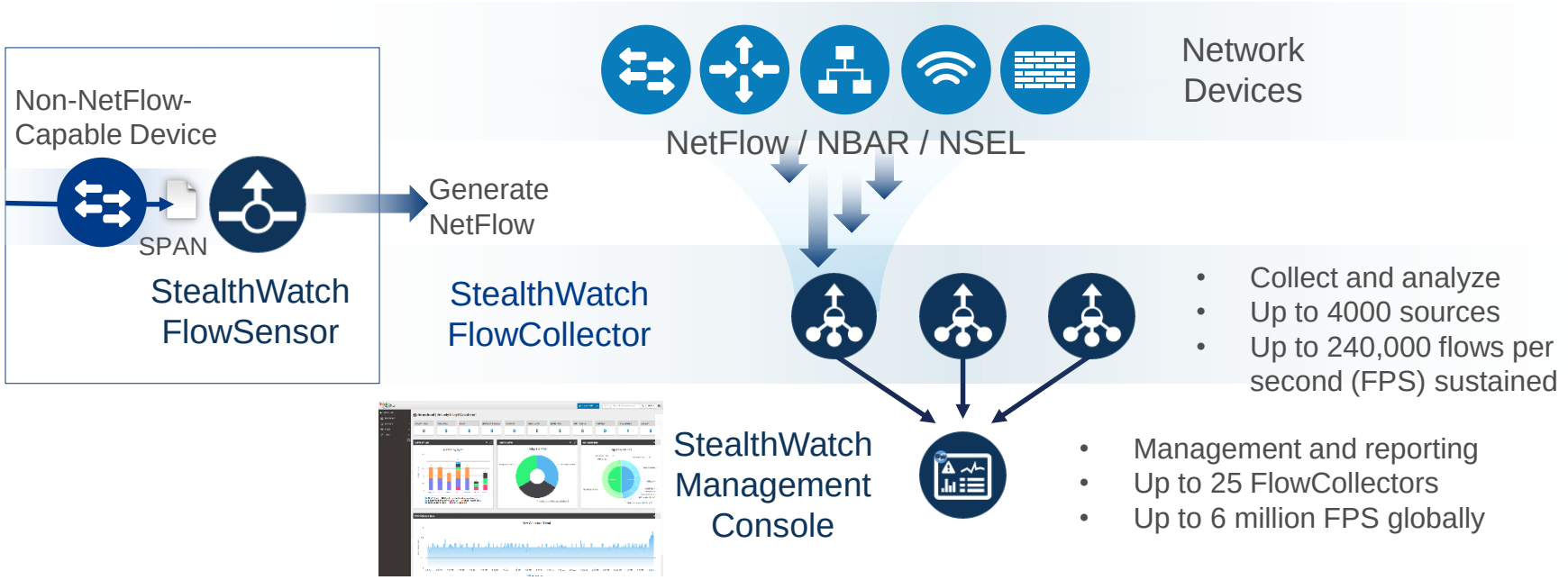


Management/Reporting Layer:
- Run queries on flow data
- Centralize management and reporting

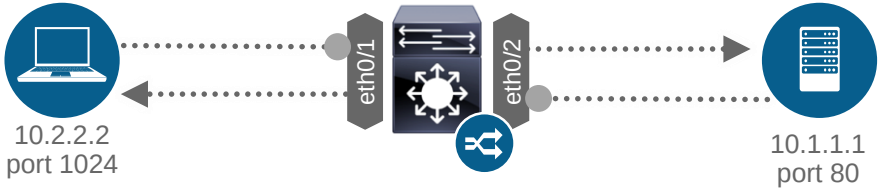
Flow Collection Layer:
- Collection, storage and analysis of flow records

Flow Exporting Layer:
- Enables telemetry export
- As close to the traffic source as possible

StealthWatch System Overview



Scaling Visibility: Flow Stitching



Unidirectional 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

Bidirectional Flow Record

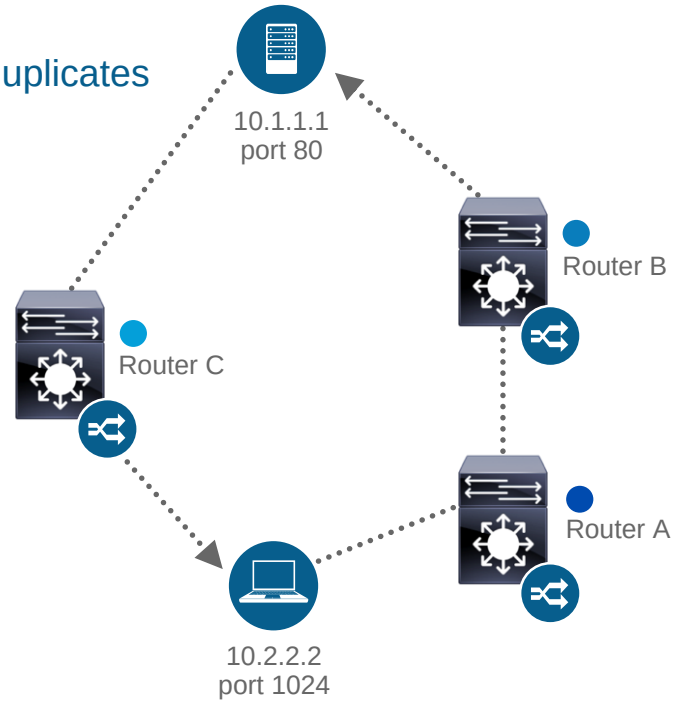
- Conversation flow record
- Allows easy visualization and analysis

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

Scaling Visibility: NetFlow Deduplication

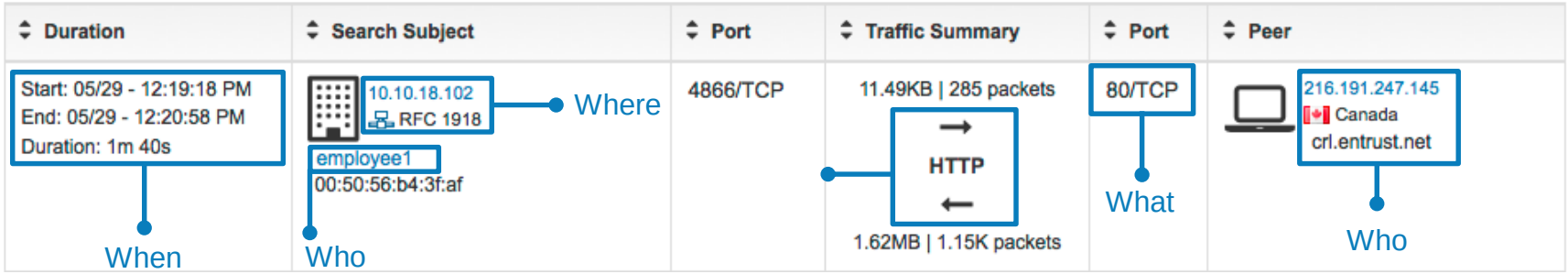
- Router A: 10.2.2.2:1024 -> 10.1.1.1:80
- Router B: 10.2.2.2:1024 -> 10.1.1.1:80
- Router C: 10.1.1.1:80 -> 10.2.2.2:1024

Duplicates

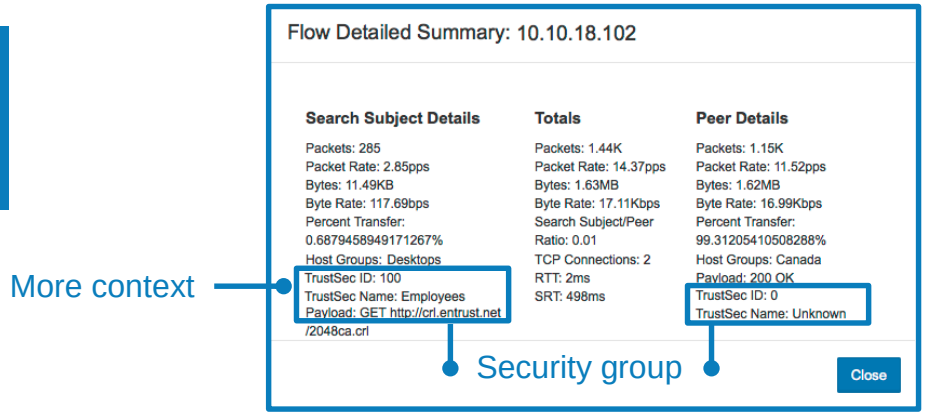


- Without deduplication
  - Traffic volume can be misreported
  - False positives would occur
- Allows for efficient storage of flow data
- Necessary for accurate host-level reporting
- Does not discard data

Conversational Flow Record

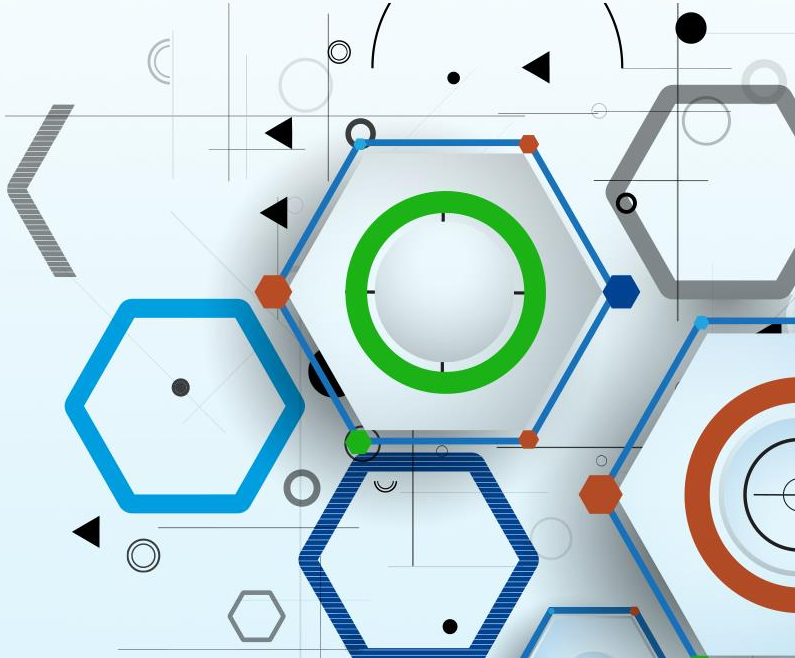


- Highly scalable (enterprise-class) collection
- High compression => long-term storage
  - Months of data retention



Zjišťování

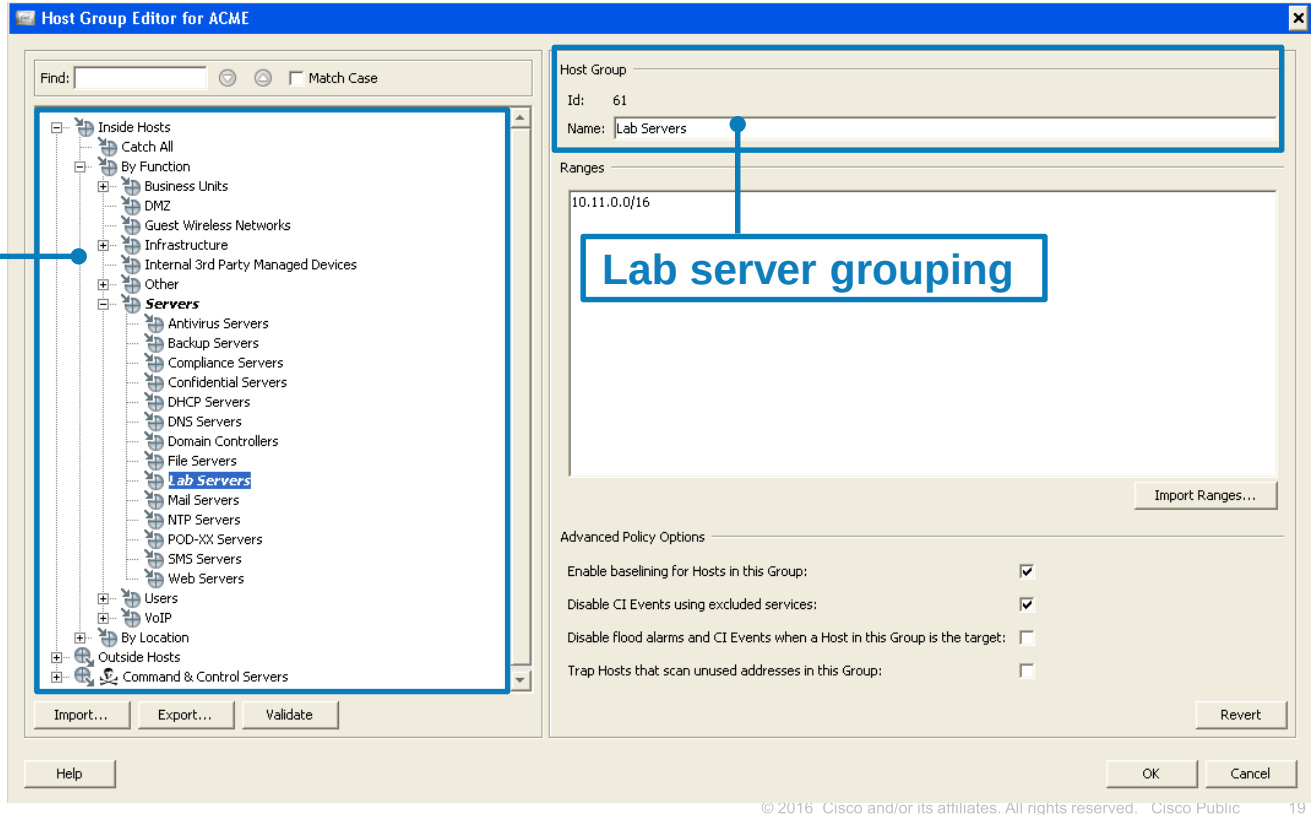
Design a nasazení



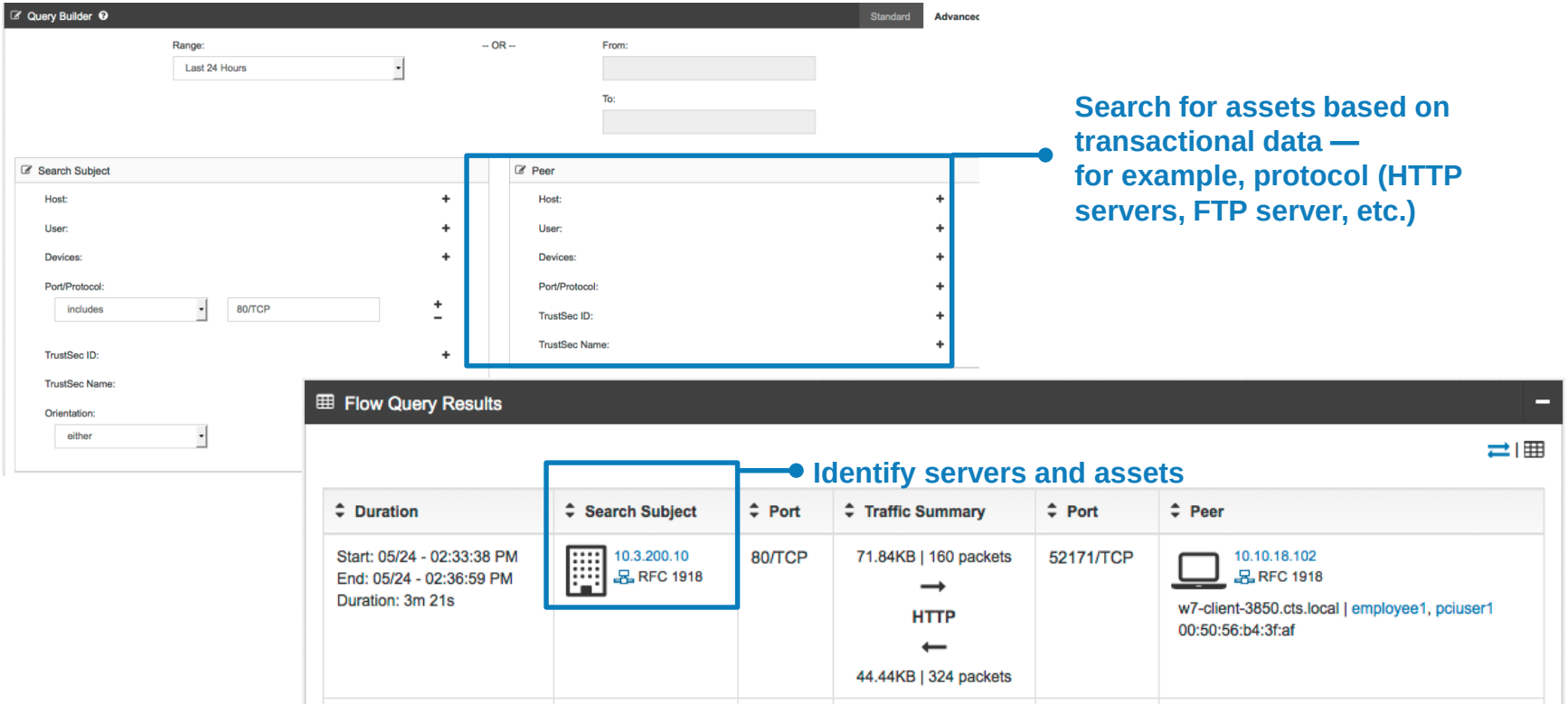
Host Groups: Applied Situational Awareness

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

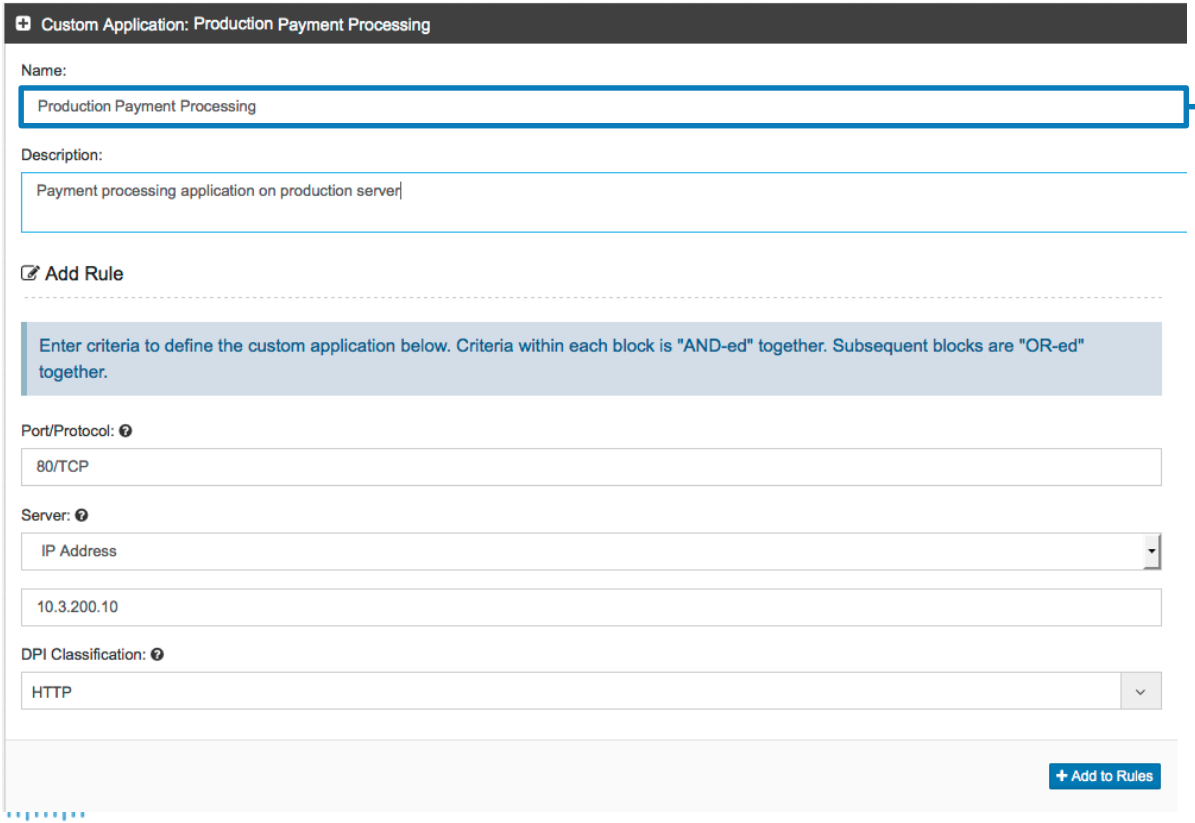
Best practice: Classify all known IP addresses into one or more host groups



Locating Services and Applications

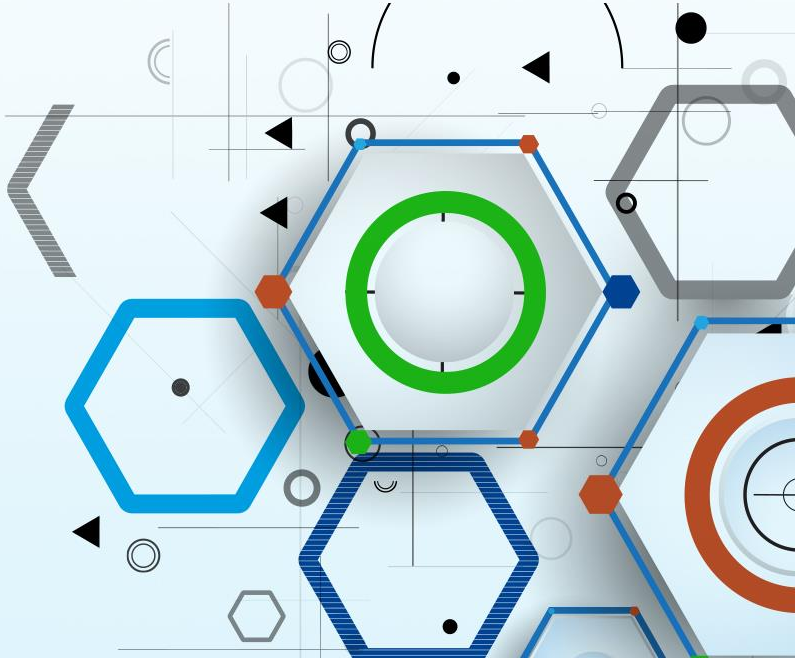


Profile Applications

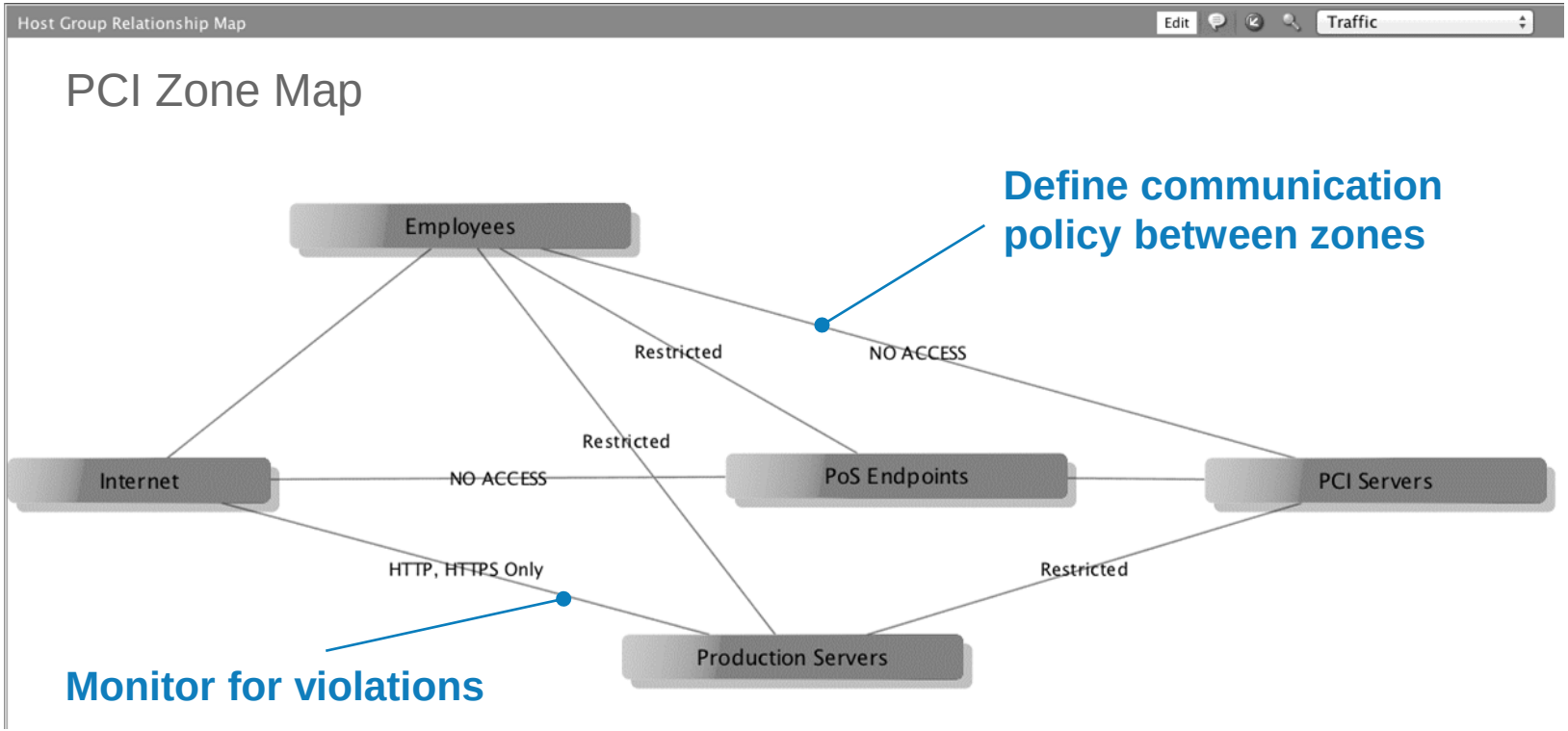


Classify business-critical applications

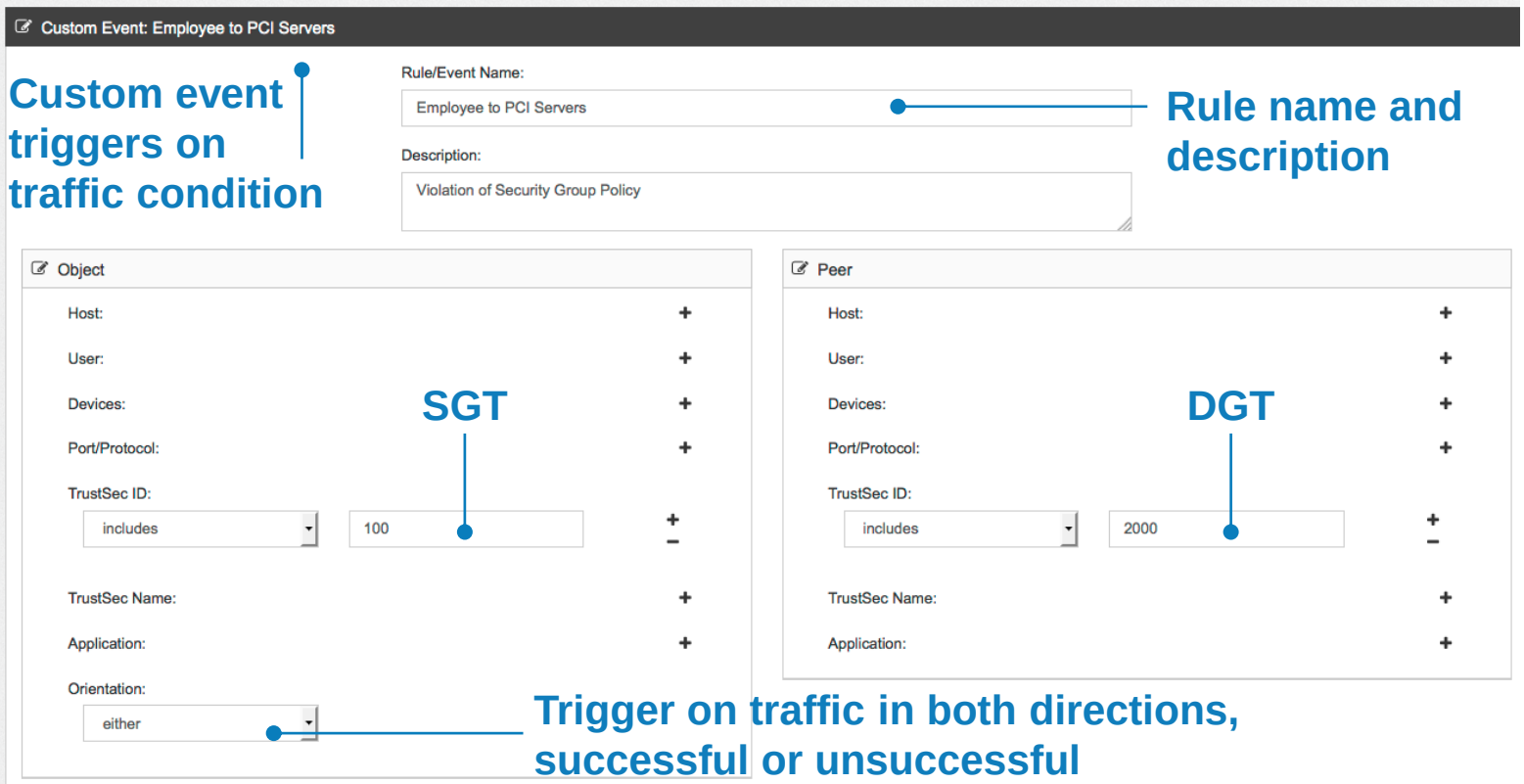
Indication of Compromise: Politika a segmentace



Segmentation Monitoring with StealthWatch

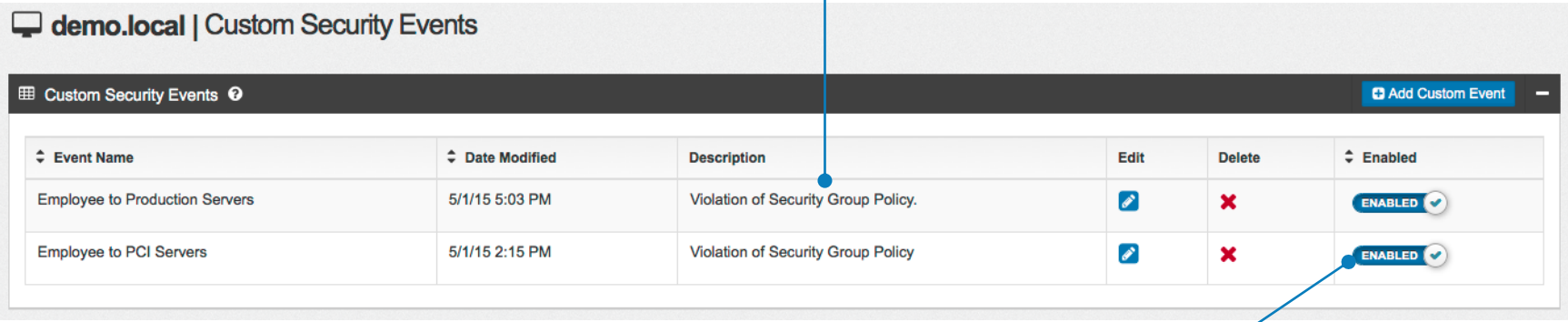


Policy Modeling and Monitoring



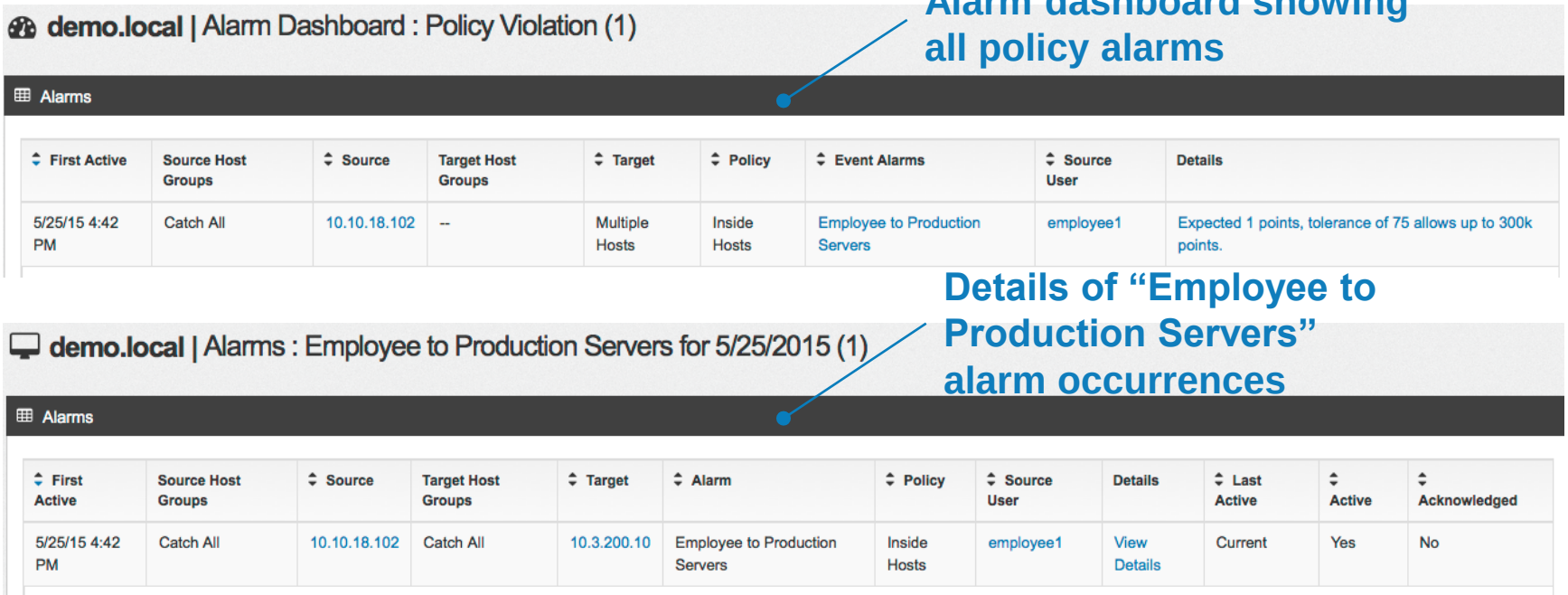
Modeling Policy in StealthWatch

Create flow-based rules for all proposed policy elements



Policy violation alarm will trigger if condition is met.

Modeling Policy: Alarm Occurrence



demo.local | Alarm Dashboard : Policy Violation (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
5/25/15 4:42 PM	Catch All	10.10.18.102	--	Multiple Hosts	Inside Hosts	Employee to Production Servers	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.

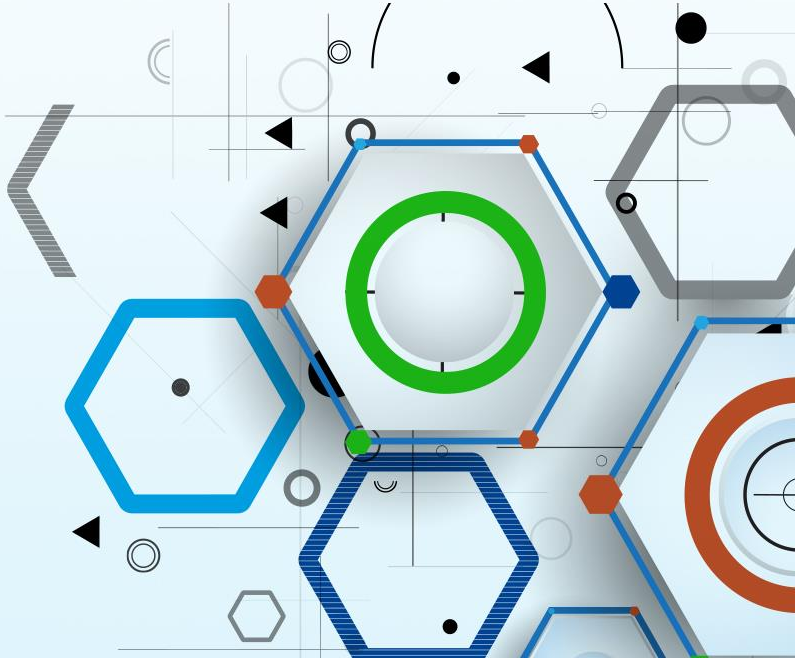
demo.local | Alarms : Employee to Production Servers for 5/25/2015 (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active	Active	Acknowledged
5/25/15 4:42 PM	Catch All	10.10.18.102	Catch All	10.3.200.10	Employee to Production Servers	Inside Hosts	employee1	View Details	Current	Yes	No

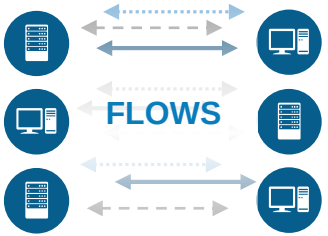
Indication of Compromise: Detekce anomálního chování v síti

Network Behavior Anomaly Detection



Behavioral and Anomaly Detection Model
Behavioral Algorithms Are Applied to Build “Security Events”

COLLECT AND ANALYZE FLOWS



SECURITY EVENTS (94 +)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

ALARM CATEGORY

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

RESPONSE

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

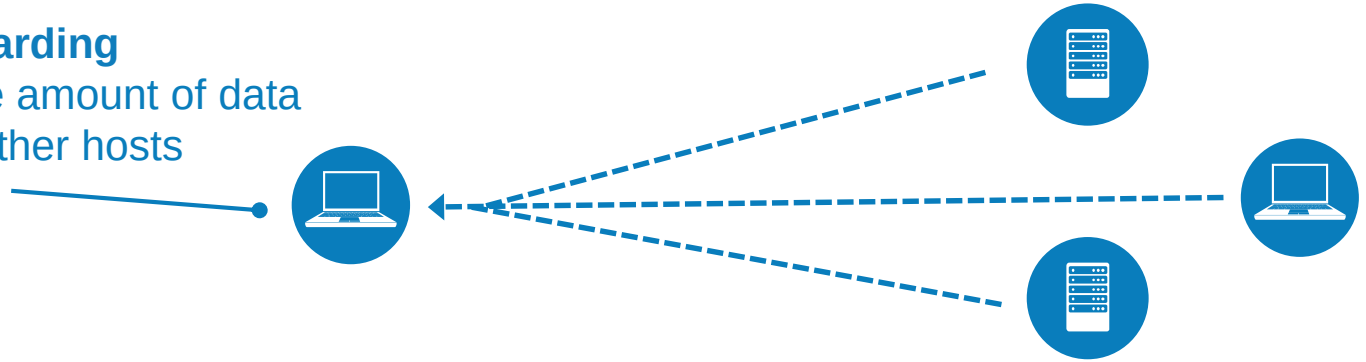
StealthWatch Alarm Categories

Each category accrues points

Example Algorithm: Data Hoarding

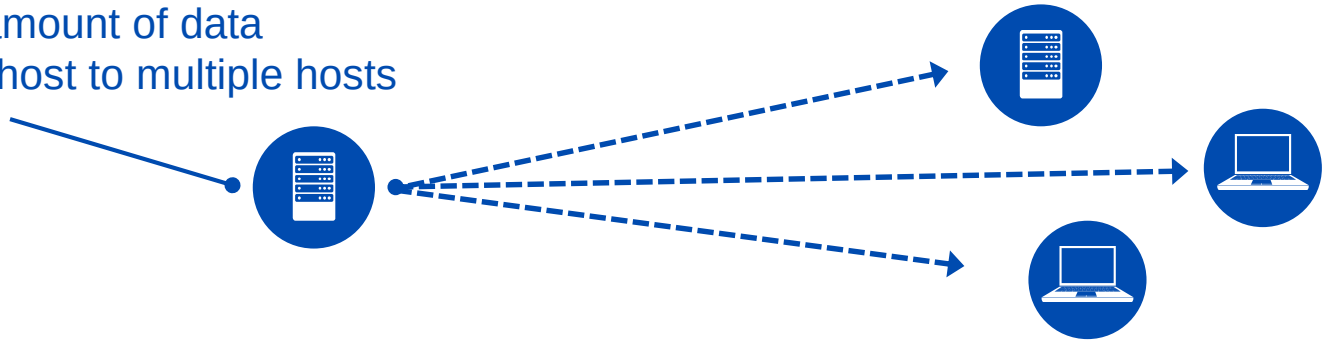
Suspect Data Hoarding

- Unusually large amount of data inbound from other hosts



Target Data Hoarding

- Unusually large amount of data outbound from a host to multiple hosts



Network Behavior and Anomaly Detection

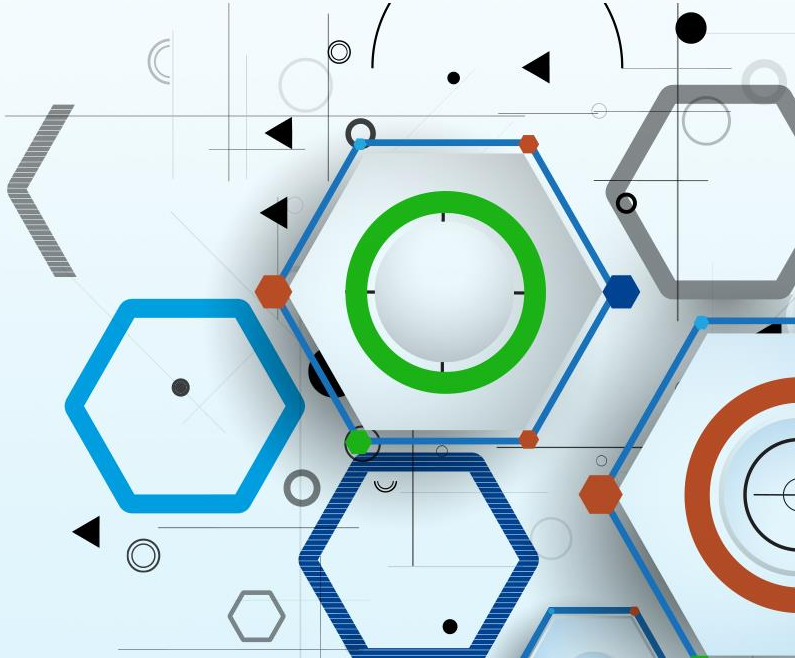
Alarm Model

- Monitor activity and alarm on suspicious conditions
- Policy and behavioral

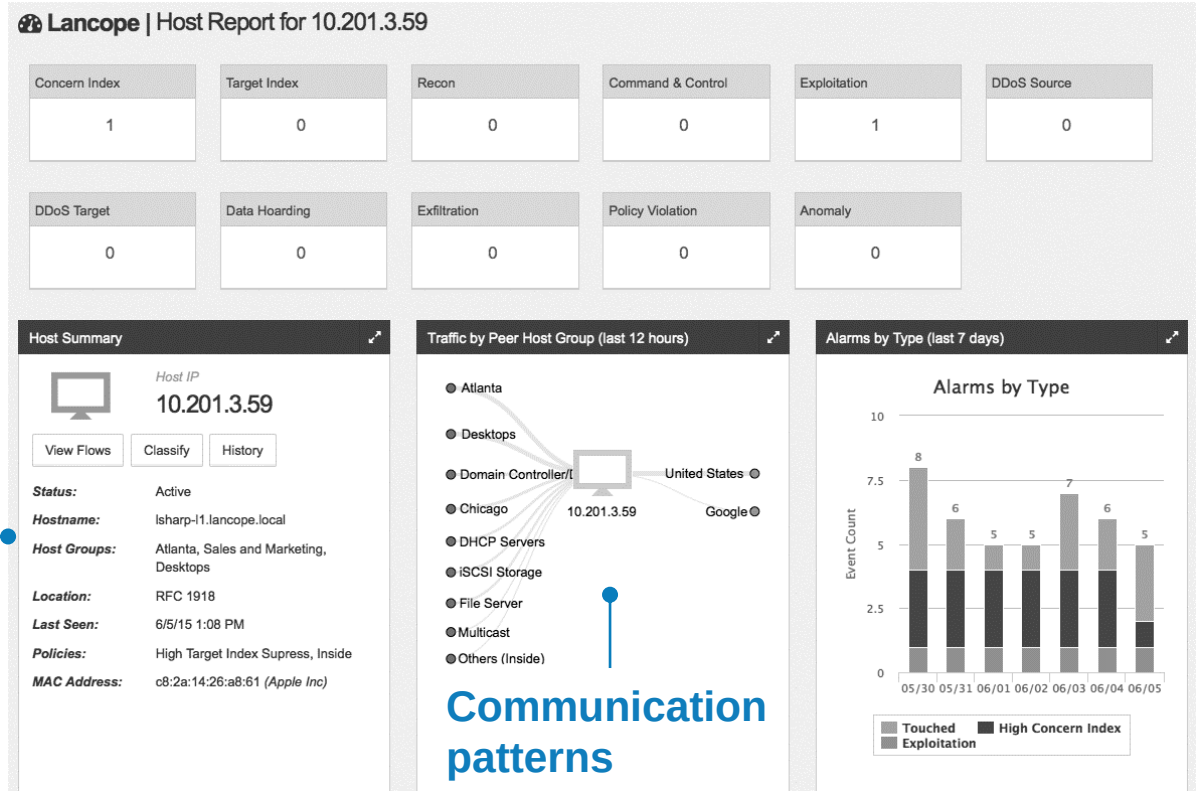
First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active
5/29/15 12:00 PM	Atlanta, Sales and Marketing, Desktops	10.201.3.18	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.18	--	Observed 23.9G bytes. Policy maximum allows up to 50M bytes.	5/29/15 1:05 PM
5/29/15 11:20 AM	Terminal Server, Datacenter	10.201.0.23	--	Multiple Hosts	Suspect Data Hoarding	10.201.0.23	--	Observed 38.45G bytes. Policy maximum allows up to 50M bytes.	5/29/15 2:40 PM

Reakce na incidenty

Incident Response



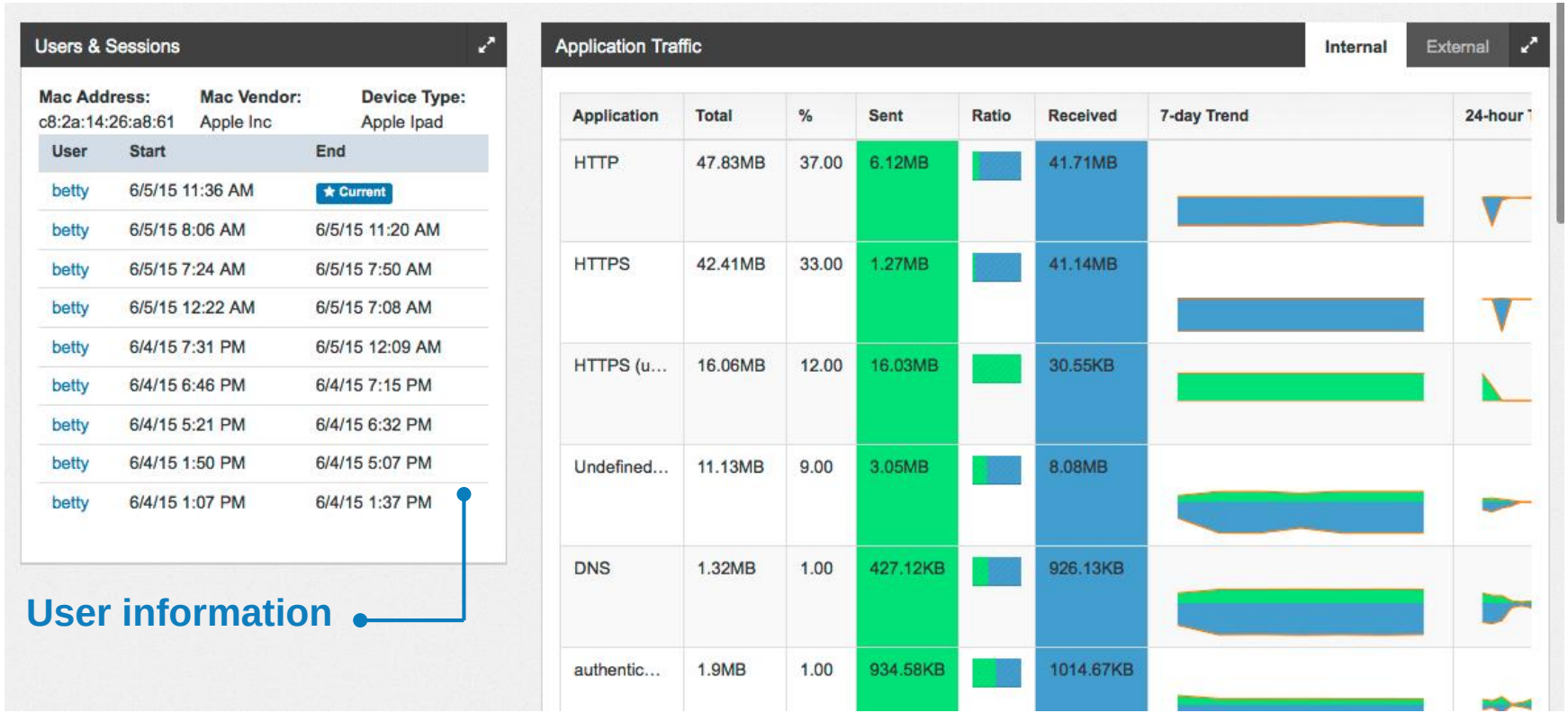
Investigating a Host



Summary

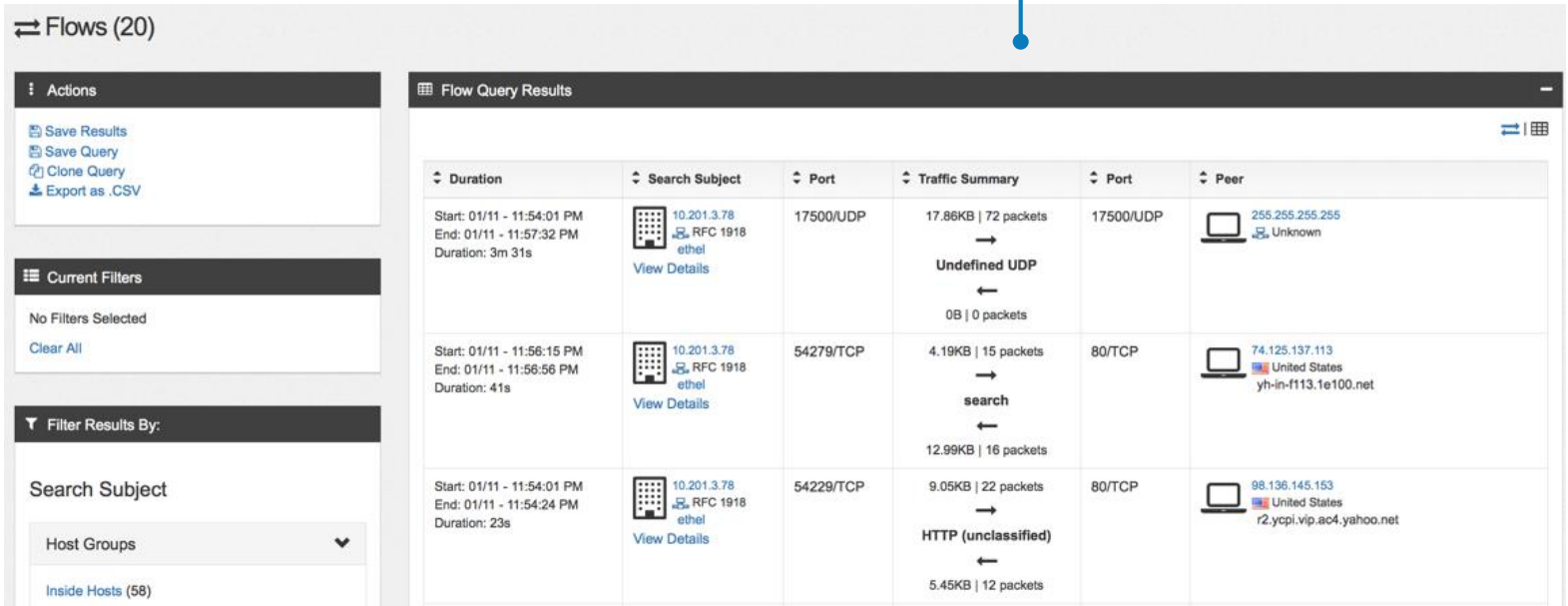
Communication patterns

Investigating: Host Drill-Down

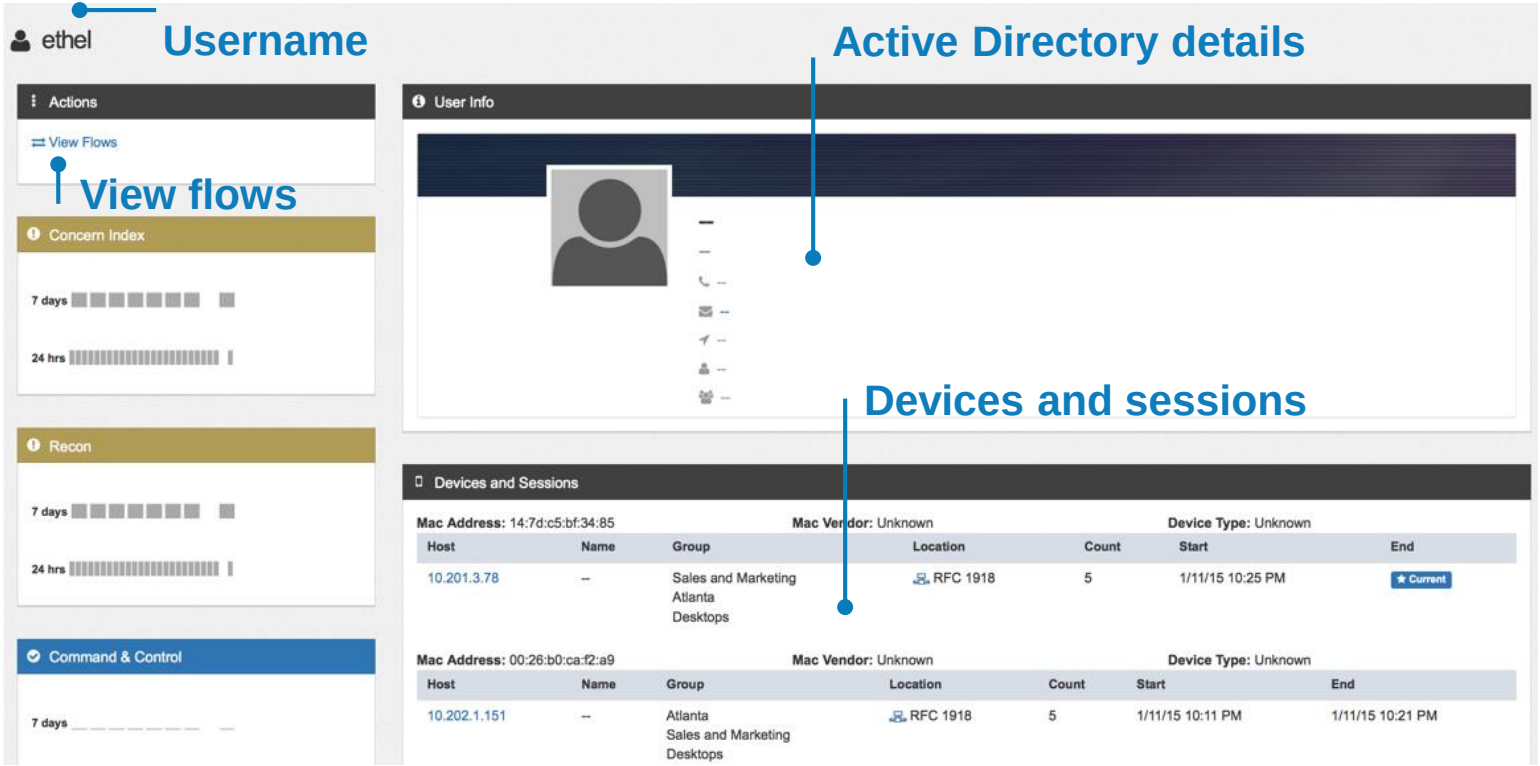


Investigating: Audit Trails

Network behavior retroactively analyzed



Extrapolating to a User



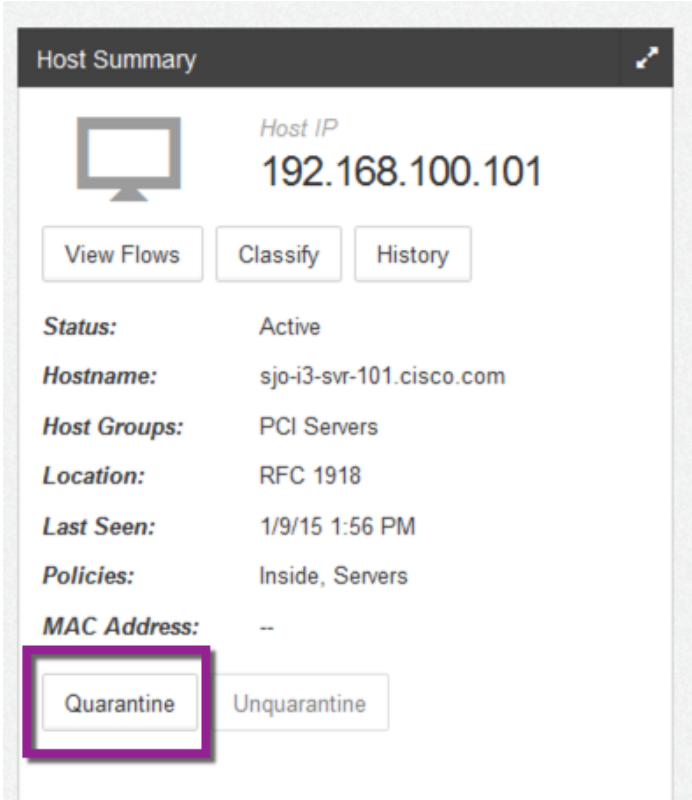
Adaptive Network Control

Cisco® Identity Services Engine

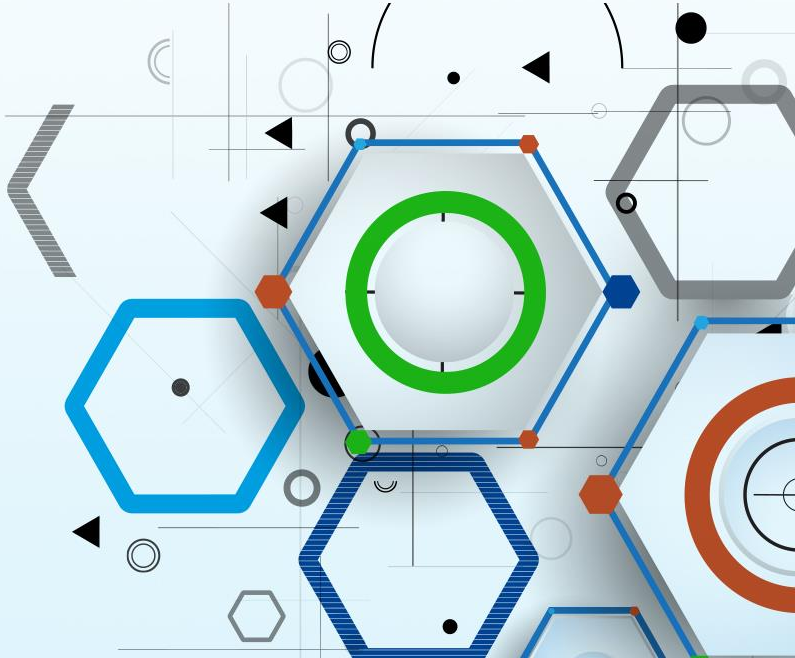
SMC

StealthWatch Management Console

Quarantine or unquarantine via pxGrid

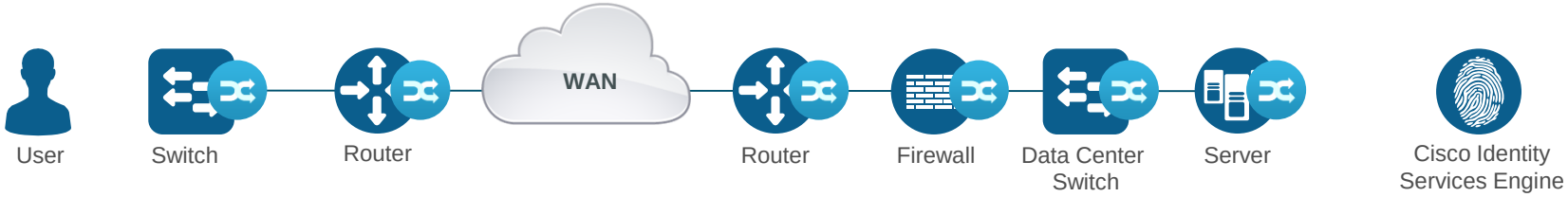


Shrnutí



NetFlow Supported Platforms

NetFlow Capable



NetFlow Exporters

Cisco® Catalyst® 2960-X (NetFlow Lite) - sample only
Cisco Catalyst 3560-X (SM-10G module only)
Cisco Catalyst 3750-X (SM-10G module only)
Cisco Catalyst 3850/3650 (FNF v9 SGT support)
Cisco Catalyst 4500E (Sup7E/7LE)
Cisco Catalyst 4500E (Sup8) (FNF v9 SGT support)
Cisco Catalyst 6500E (Sup2T) (FNF v9 SGT support)
Cisco Catalyst 6800 (FNF v9 SGT support)
Cisco ISR G2 (FNF v9 SGT support)
Cisco 4000 Series ISR (FNF v9 SGT support)
Cisco ASR 1000 Series (FNF v9 SGT support)
Cisco Cloud Services Router 1000v Series (FNF v9 SGT support)
Cisco 5760 Wireless LAN Controller (WLC) (FNF v9)
Cisco 5520, 8510, 8540 WLC (v9)*
Cisco ASA 5500, 5500-X (NSEL)
Cisco Nexus® 7000 Series (M Series I/O modules – FNF v9)
Cisco Nexus 1000v (FNF v9)
Cisco NetFlow Generation Appliance (FNF v9)
Cisco UCS® Virtual Interface Card (VIC) (VIC 1224/1240/1280/1340/1380)

Lancope is now part of Cisco

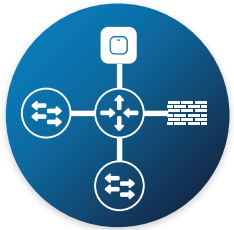
StealthWatch Management Console

StealthWatch FlowCollector

StealthWatch FlowSensor

For more information, visit: http://www.cisco.com/c/en/us/solutions/enterprise-networks/threat-defense/index.html

Key Takeaways



The network is a key asset for threat detection and control

NetFlow and StealthWatch provide visibility and intelligence

Reference:

Lancope is Now Part of Cisco
https://www.lancope.com/partners/lancope-now-part-cisco

StealthWatch Wiki
https://www.lancope.com/wiki

Cisco Cyber Threat Defense Solution
http://cs.co/9004BYtJ8

Cisco Cyber Threat Defense Solution Data Sheet
http://cs.co/9005BYtJ3

Cisco Identity Services Engine and Lancope StealthWatch Integration
http://cs.co/9001BYtJT

Děkujeme za pozornost.

DEMO

https://dcloud-lon-web-1.cisco.com/dCloud/drn.jsp