Behavioral Network Security

Steinþór Bjarnason

Consulting Engineer Security

Cisco Europe

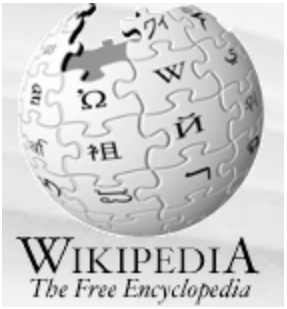
Agenda

- Threats and how to detect them
  - Threat Telemetry
  - Processing Telemetry
- Fighting Threats
  - Responding to a Threat
  - Rapid Threat Mitigation
- The future of Behavioral Network Security

Threat Detection

What is a Threat?

- **Definition:**
  - A probable impending danger or warning of impending danger, e.g. "a terrorist threat"
  - An act of coercion wherein a negative consequence is proposed to elicit response



- Looking at the networking field, a ”Threat” means different things to different people
  - Enterprise/SMB
  - Home user
  - Service Provider

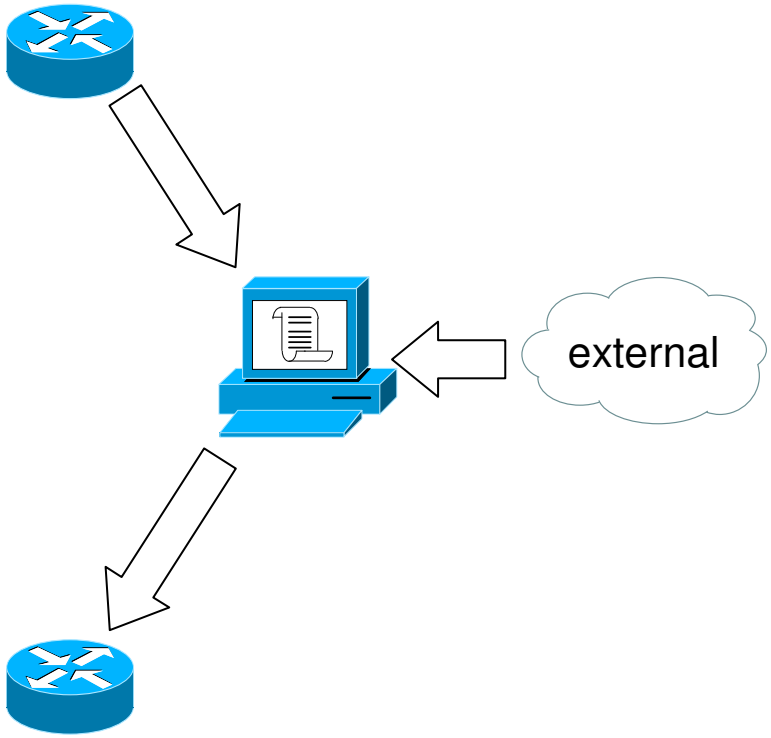
Today's threats

- Modern threats are stealthy and use encryption in order to hide communication
- The main focus is on stealing data and confidential information
- Also, modern bots/trojans often contain attack code in order to defend themselves against active detection
- There have been cases of large Enterprises being down for up to 2 weeks due to persistent trojan infections



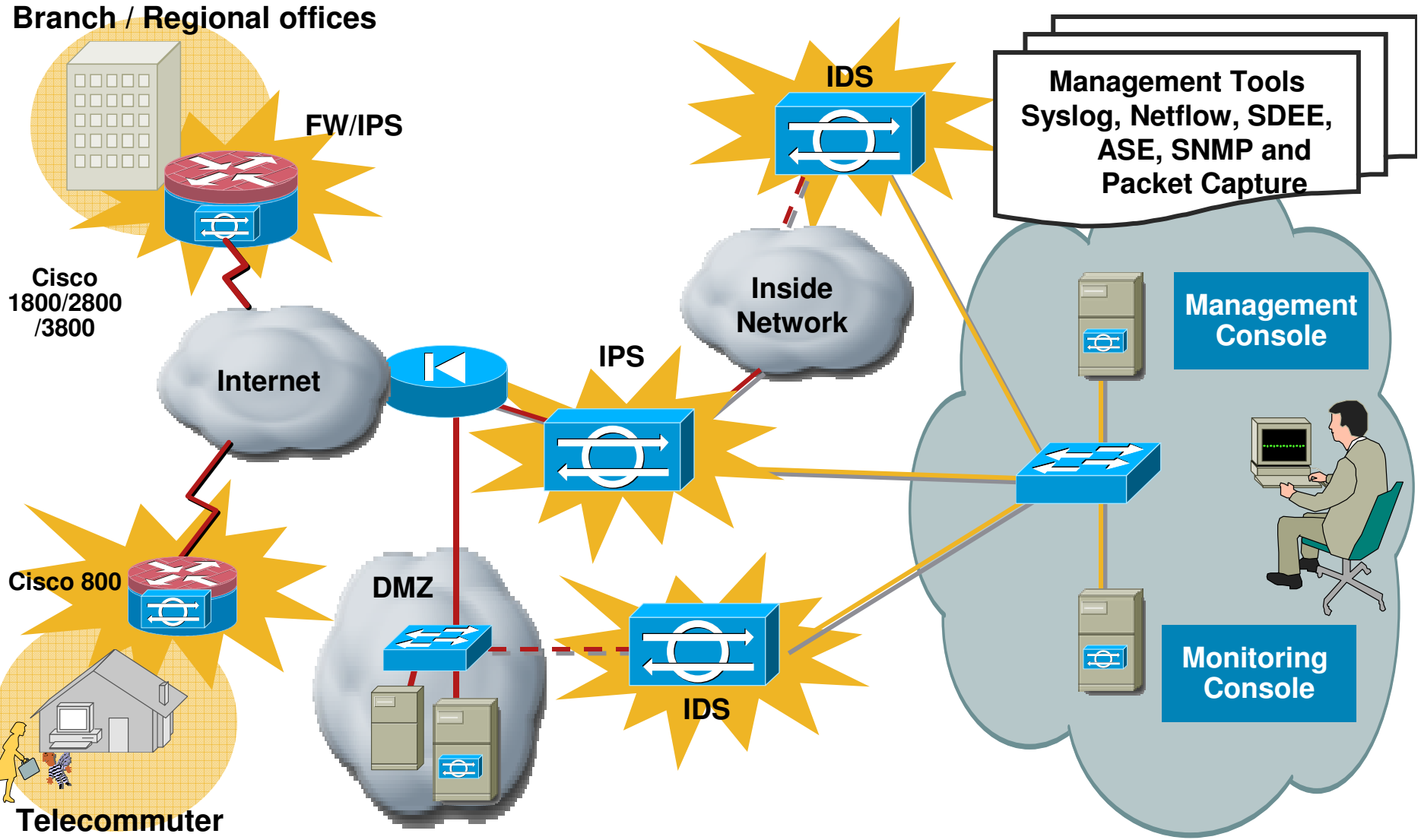

The Threat Picture – High Level Overview

- Learn from the network …
  - Netflow, syslog, SNMP, …
  - IDS events,
  - Signature extraction, …
- … and from external sources …
  - Senderbase, Intellishield, other feeds,
- … to defend the network
  - packet filtering,
  - routing / blackholing,
  - static configs,

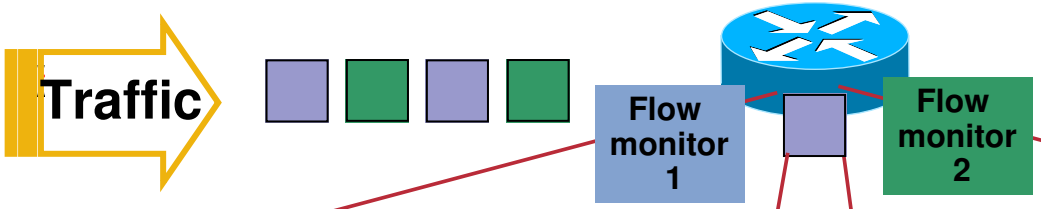


Threat Telemetry

Security Operation
Threat Detection



Netflow:
Keeping a (virtual) finger on the pulse



Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source port	23
Destination port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non Key Fields
Packets
Bytes
Time Stamps
Next-Hop Address

Key Fields	Packet 2
Source IP	3.3.3.3
Dest IP	2.2.2.2
Input Interface	Ethernet 0
Packet Section	1010101

Non Key Fields
Packets
Time Stamps

Traffic Analysis Cache

Source IP	Dest. IP	Dest. I/F	Protocol	TOS	…	Pkts
3.3.3.3	2.2.2.2	E1	6	0	…	11000
1.1.1.1	2.2.2.2	E1	6	0	…	11000

Security Analysis Cache

Source IP	Dest. IP	Dest. I/F	Input I/F	Sec	…	Pkts
3.3.3.3	2.2.2.2	E1	E1	101	…	11000

IronPort SenderBase Network: Using Reputation to enhance Threat detection

First, Biggest, Best Email & Web Traffic Monitoring Network – Data Makes the Difference

View into **over 30%** of global email traffic

20M+ IP addresses tracked globally

Data from **~120,000 sources**; **8 of the 10** largest ISPs

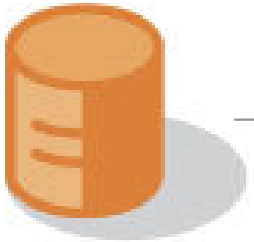
Millions of human reporters & spamtraps

IronPort SenderBase
Data Makes the Difference

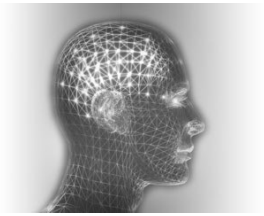
150 Parameters

- Complaint Reports
- Spam Traps
- Message Composition Data
- Global Volume Data
- URL Lists
- Compromised Host Lists
- Web Crawlers
- IP Blacklists & Whitelists
- Additional Data

Threat Prevention in Realtime



SenderBase Data



Data Analysis/ Security Modeling

SenderBase Reputation Scores -10 to +10

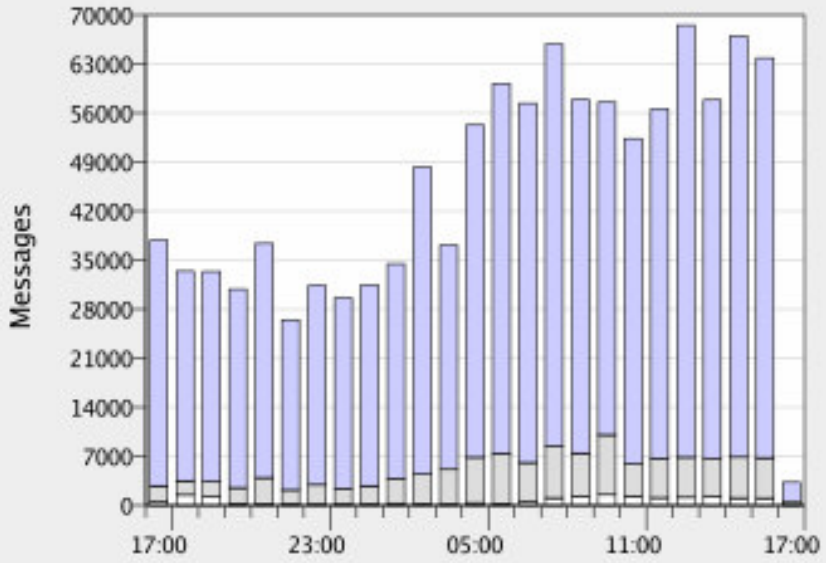
Monitor – Daily Overview
2200 Users

88% of all emails sent to customer domains were stopped by reputation filters alone.

Incoming Mail Overview

Time Range: Past Day

Incoming Mail: **18 Mar 22:00 (GMT)** to **19 Mar 22:00 (GMT)**



Incoming Mail Category	%	# Messages
Total Attempted Messages		**1134180**
Stopped by Reputation Filtering	88.87	1007902
Invalid Recipients	0.01	109
Spam Messages Detected	9.63	109226
Virus Messages Detected*	0.00	53
Total Threat Messages	**98.51**	**1117290**
Clean Messages Accepted	**1.49**	**16890**

98% of all emails sent to customer domains were bogus and thus blocked by the IronPort appliance.

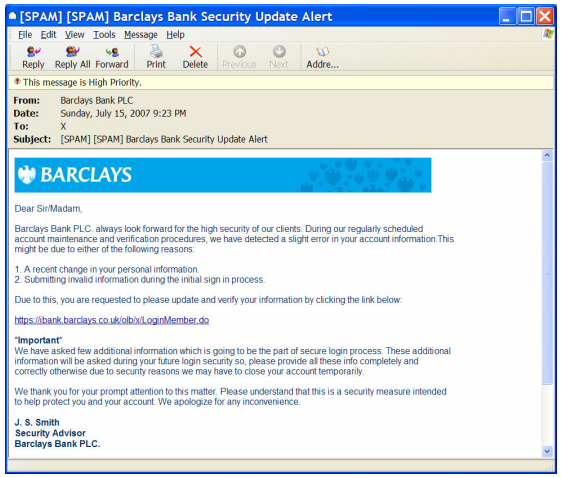
Web Reputation in Action

HOW?

- *Message leaves trace of malware tools*

WHERE?

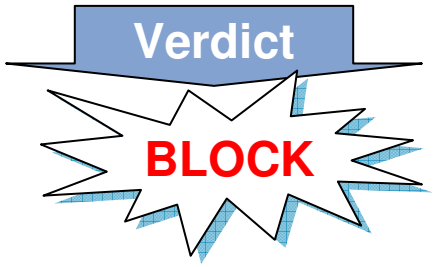
- *URL only just registered*
- *URL already blacklisted*
- *URL seeing large traffic spikes*
- *Hosts many unique sites (rock phish kit)*



WHO?

- *IP address recently started sending email*
- *Message originated from dial-up IP address*
- *Sending IP address located in Ukraine*

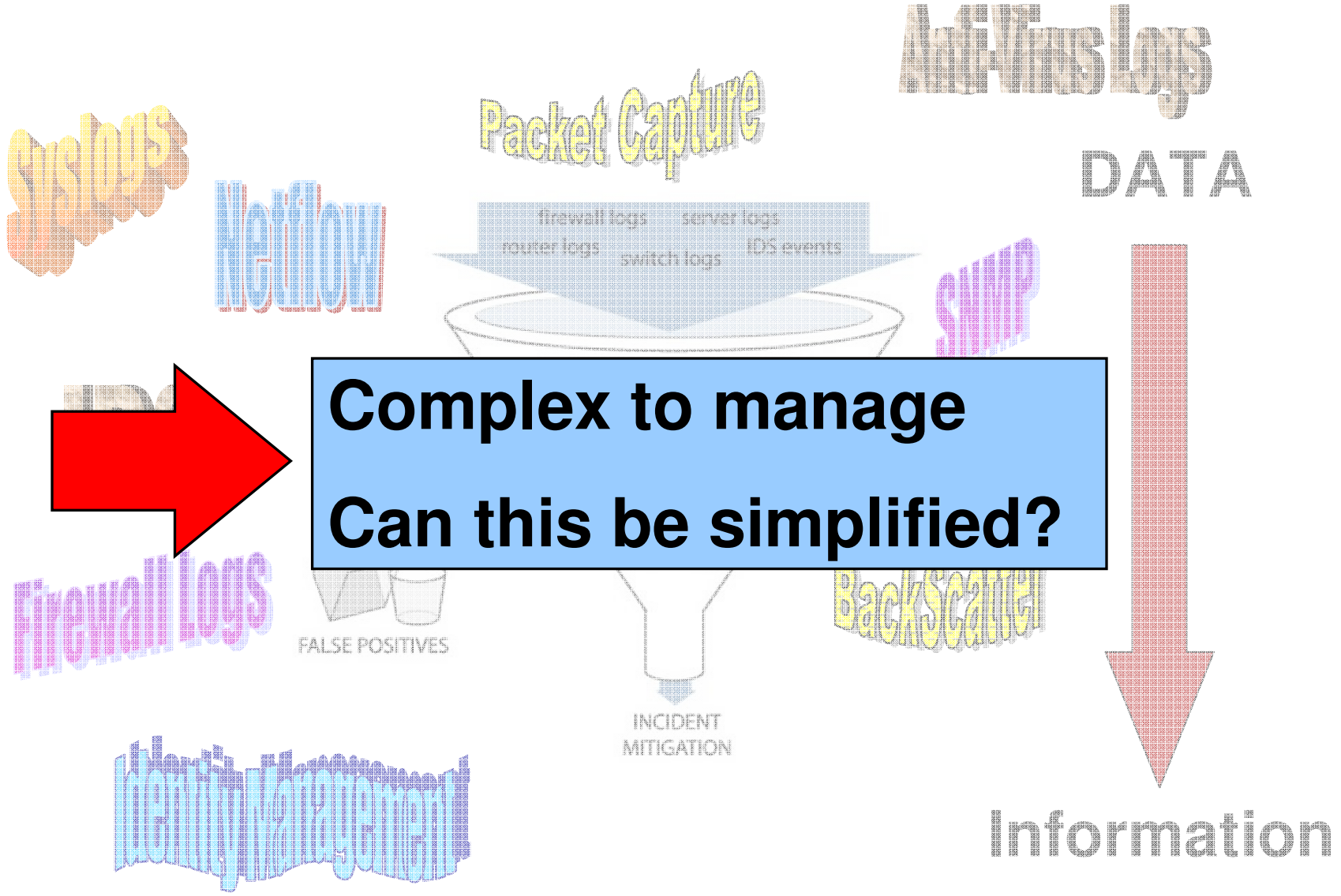
Network Owner	DataNet
Domain	dnet.pl
Date of first message seen from this address	2006-06-18
CIDR range	unknown
# of domains controlled by this network owner	500
Geography data	
Country	RU
State	48
City	Moscow



Processing Telemetry

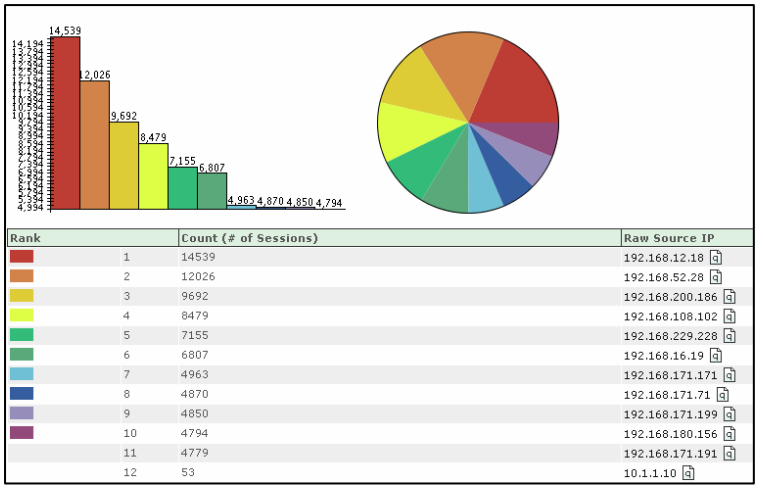
SIM's and NBA

Correlating the Data



Security Information Management (SIM)

- A SIM consists of 5 major elements:
  - Topology awareness
  - Log consolidation
  - Threat correlation
  - Incident management
  - Reporting



Rank	Count (# of Sessions)	Raw Source IP
1	14539	192.168.12.18
2	12026	192.168.52.28
3	9692	192.168.200.186
4	8479	192.168.108.102
5	7155	192.168.229.228
6	6807	192.168.16.19
7	4963	192.168.171.171
8	4870	192.168.171.71
9	4850	192.168.171.199
10	4794	192.168.180.156
11	4779	192.168.171.191
12	53	10.1.1.10

Compliance is often an orthogonal process to correlation

HIPAA.ORG

The Gramm-Leach Bliley Act

PRIVACY INITIATIVES

PCI Security Standards Council

"By year-end 2007, 25 percent of large enterprises will employ NBA as part of their network security strategy (0.8 probability)"

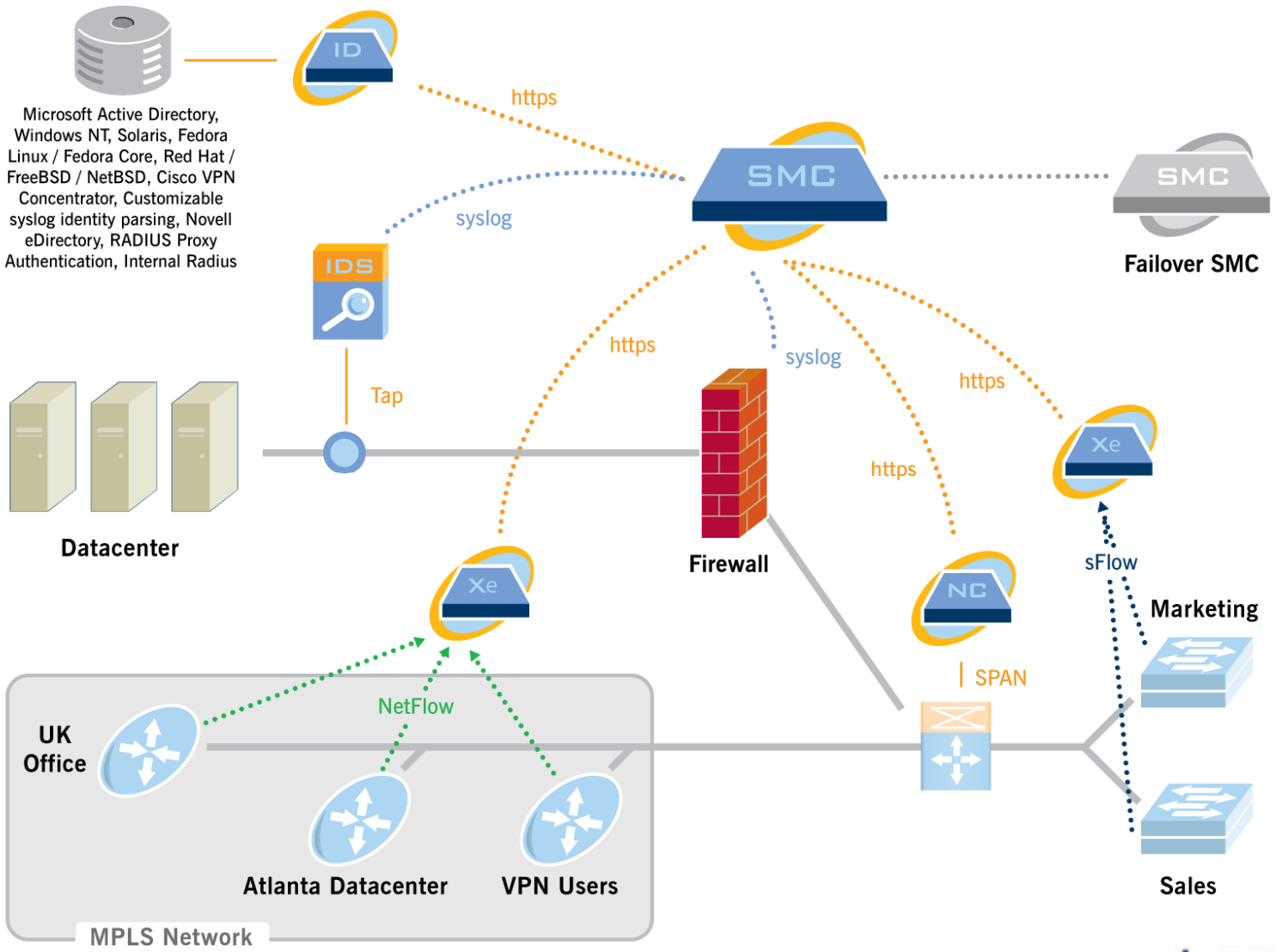
Gartner Research

Publication Date: 9 December 2005 ID Number: G00134030

Use Network Behavior Analysis for Better Visibility Into Security and Operations Events

Paul E. Proctor

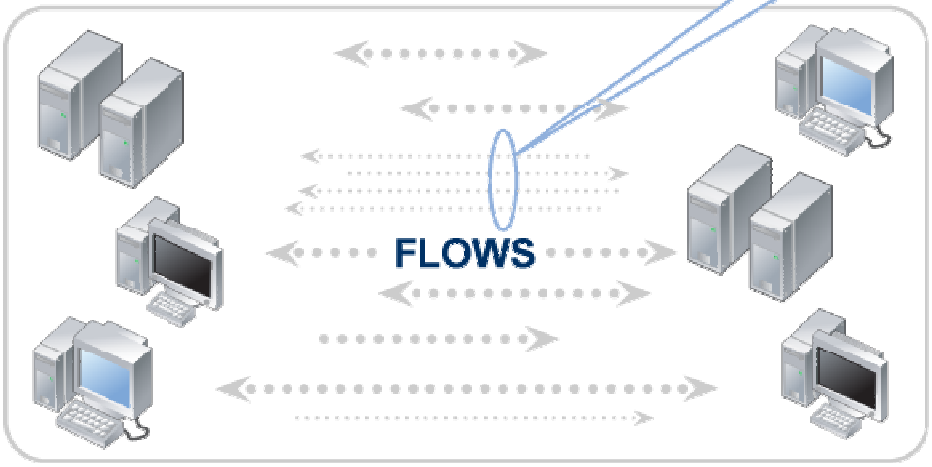
Network Behavioral Analysis (NBA)

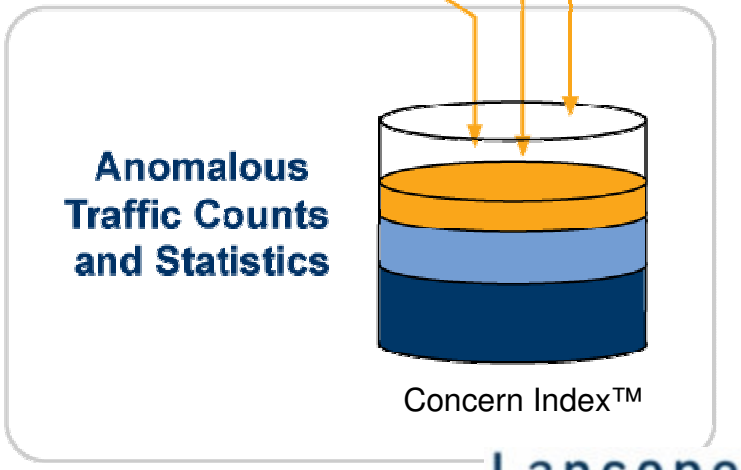


Lancope.
Optimizing Security and Network Operations

NBA Algorithmic Analysis

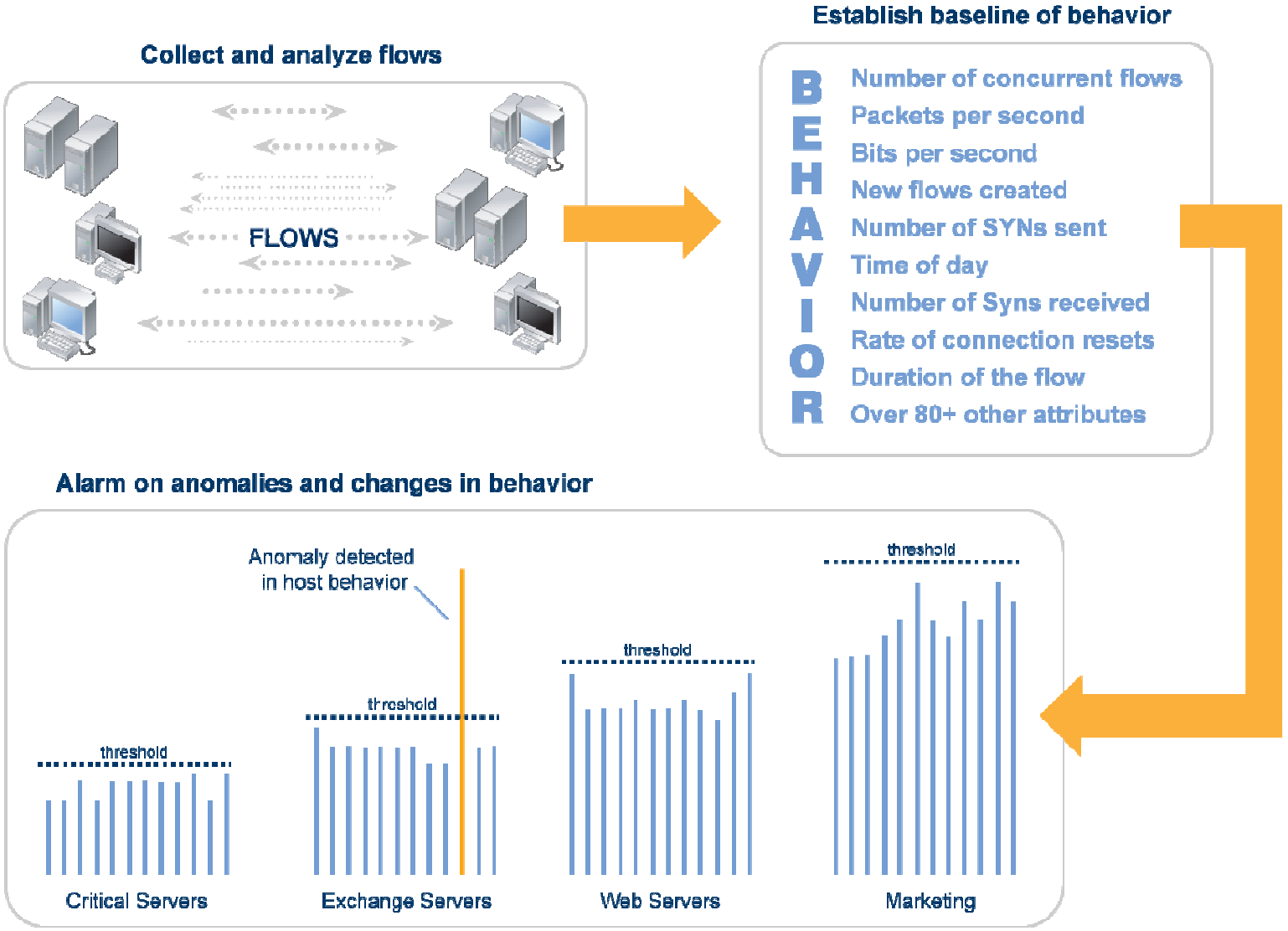
Client Host	Server Host	Service Summary	Server Total Bytes	Client Total Bytes
222.36.40.139	209.182.176.214	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.212	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.216	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.208	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.213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





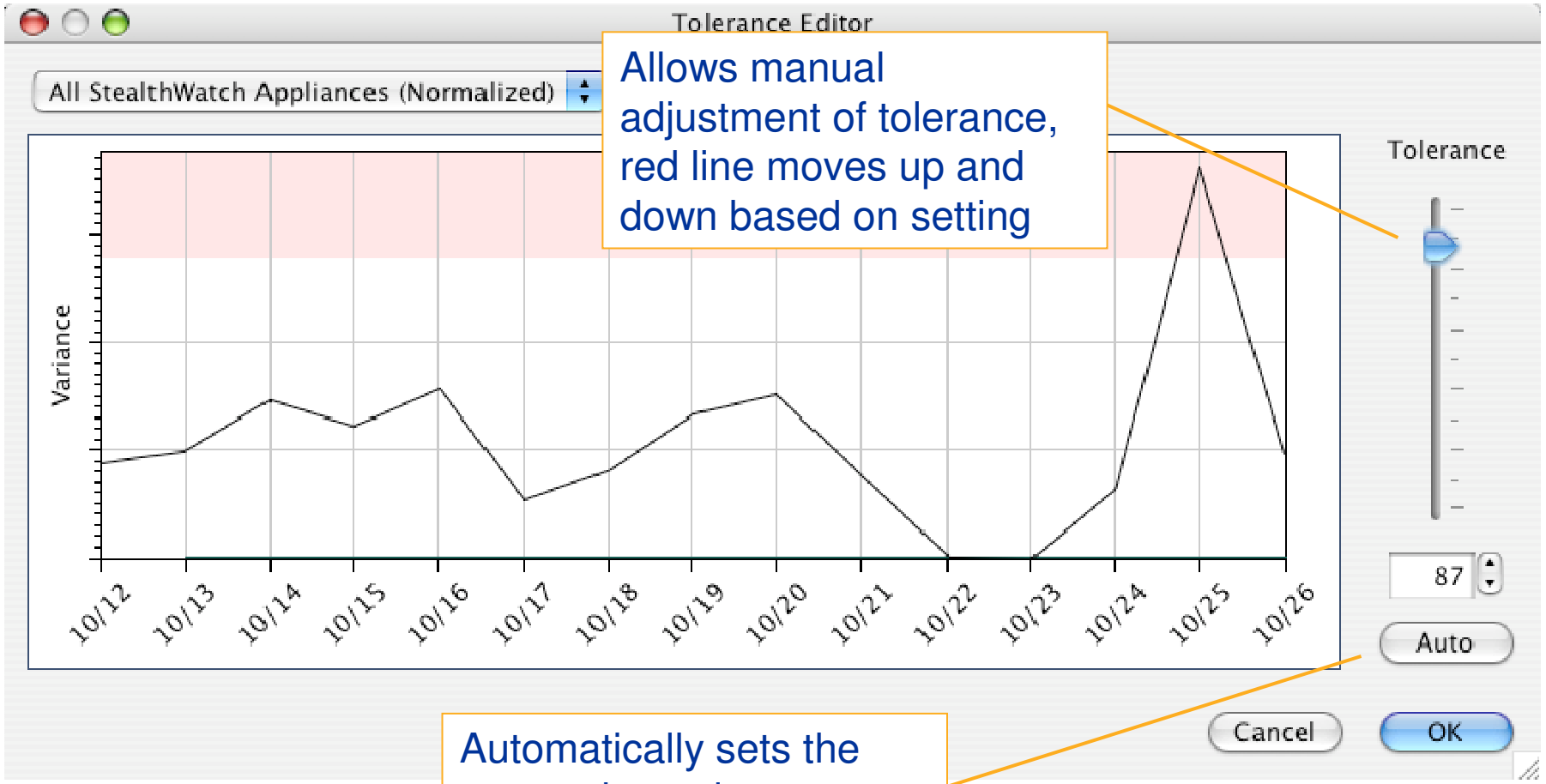
Lancope.
Optimizing Security and Network Operations

NBA Behavior-based Analysis



Lancope.
Optimizing Security and Network Operations

Configuring Tolerance to Behavioral Change

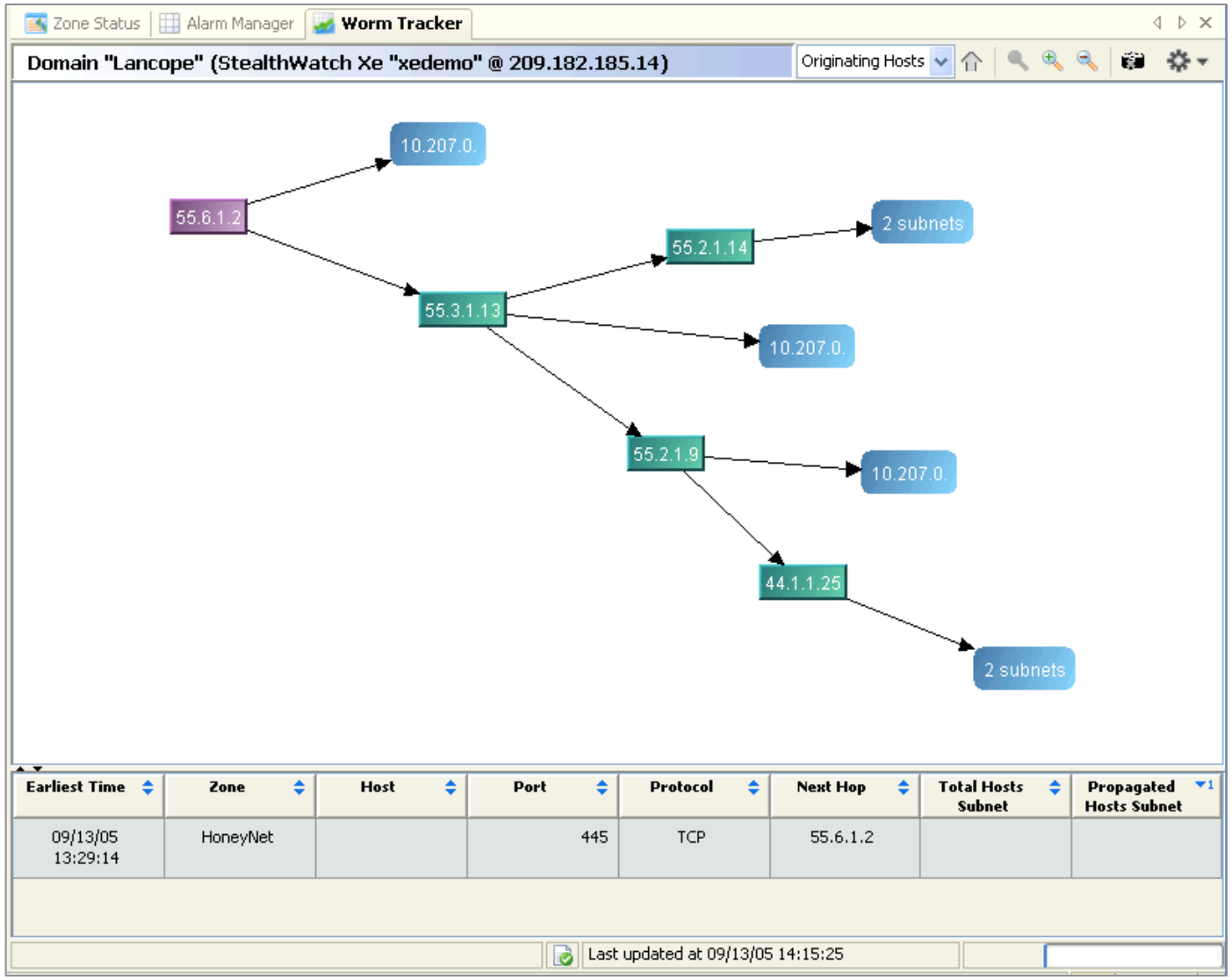


Allows manual adjustment of tolerance, red line moves up and down based on setting

Automatically sets the appropriate tolerance based on historical values

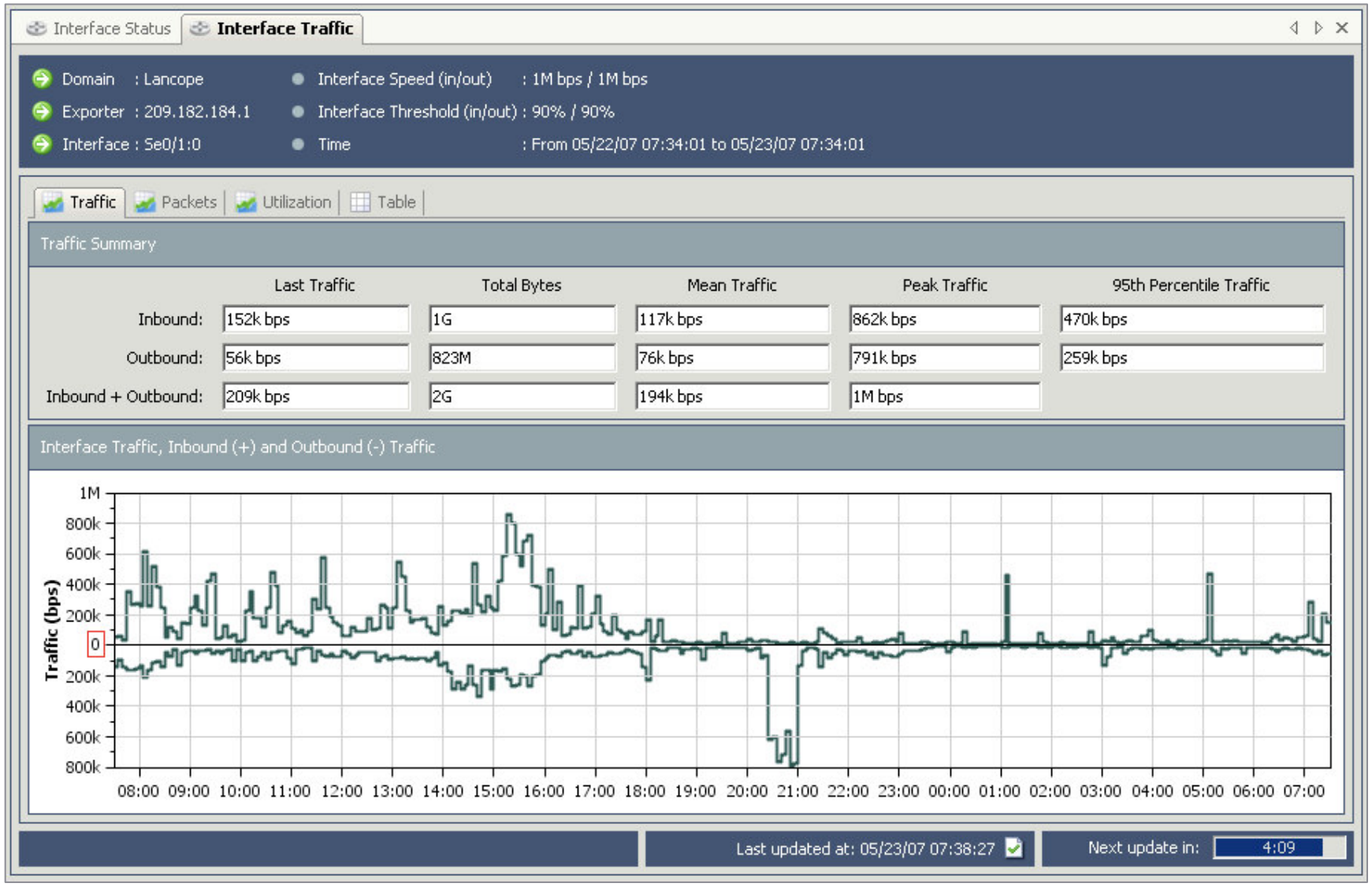
Lancope.
Optimizing Security and Network Operations

NBA Visualization of a Worm Outbreak



Lancope.
Optimizing Security and Network Operations

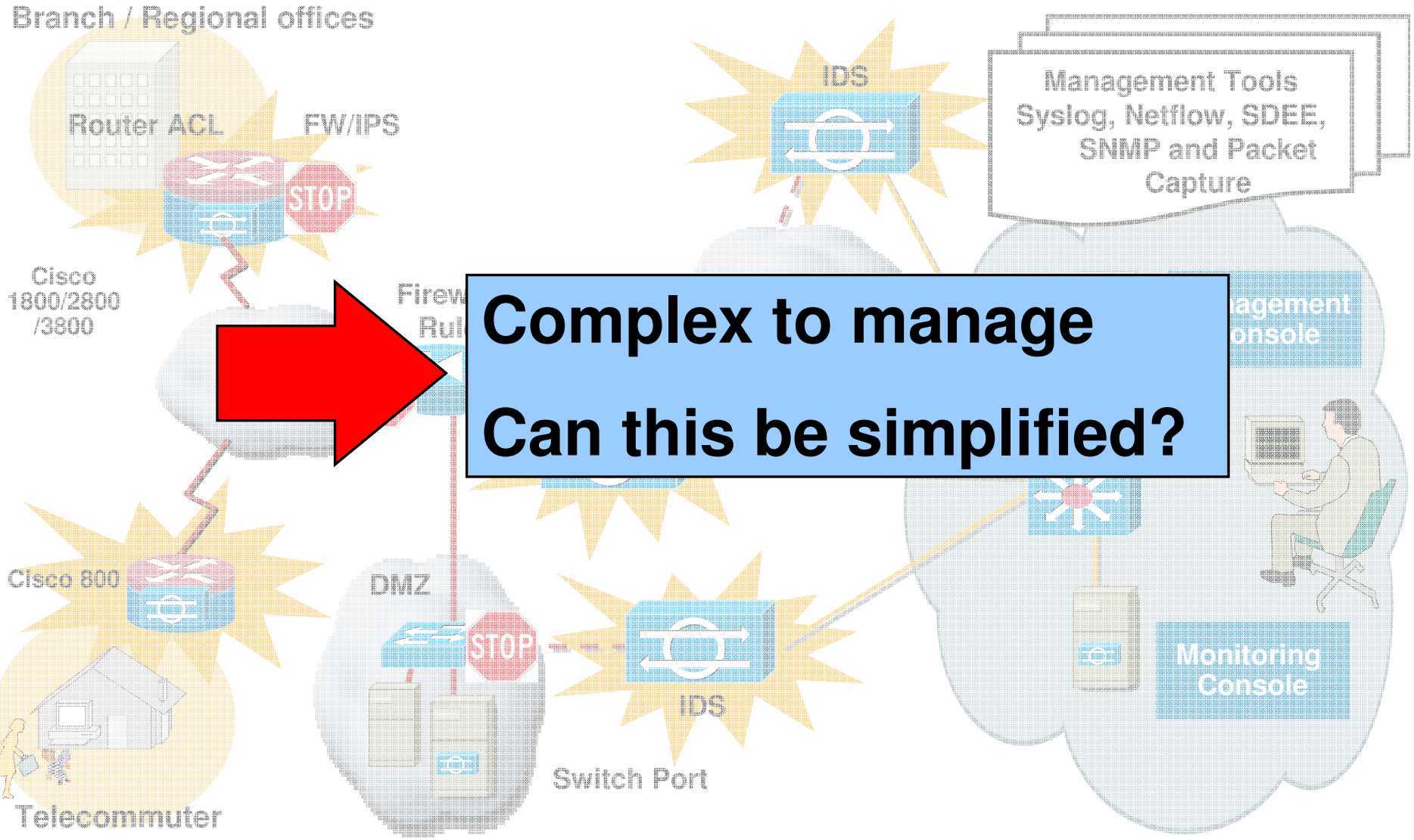
NBA for Traffic Analysis



Lancope.
Optimizing Security and Network Operations

Threat Mitigation

Security Operation
Now I know → Mitigate



Rapid Threat Mitigation

Problem Statement

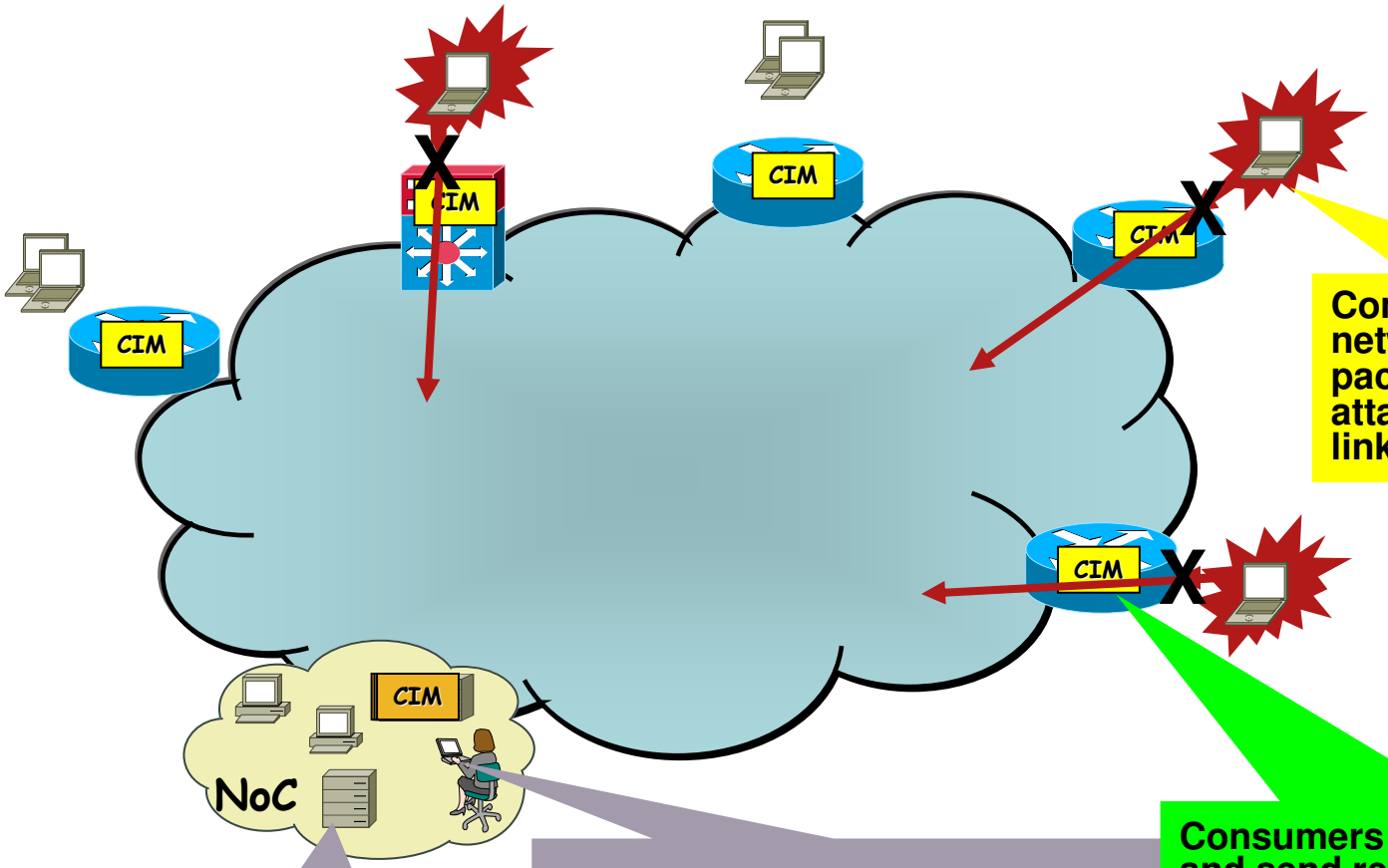
Maintain Network Availability

Need a secure and reliable communication mechanism to immediately propagate network changes for dynamic requirements

- **Sample Use Cases**
  - Rapid and reliable changes in response to an attack
  - Facilitate troubleshooting, detailed data analysis
  - Network analysis tools that take action in the network

Use Case 1: Responding to a Threat

Rapid Threat Mitigation



Compromised hosts plug into network and start sending packets to the network to attack servers or congest links

Consumers receive CIMs, act on them and send responses back to the controller

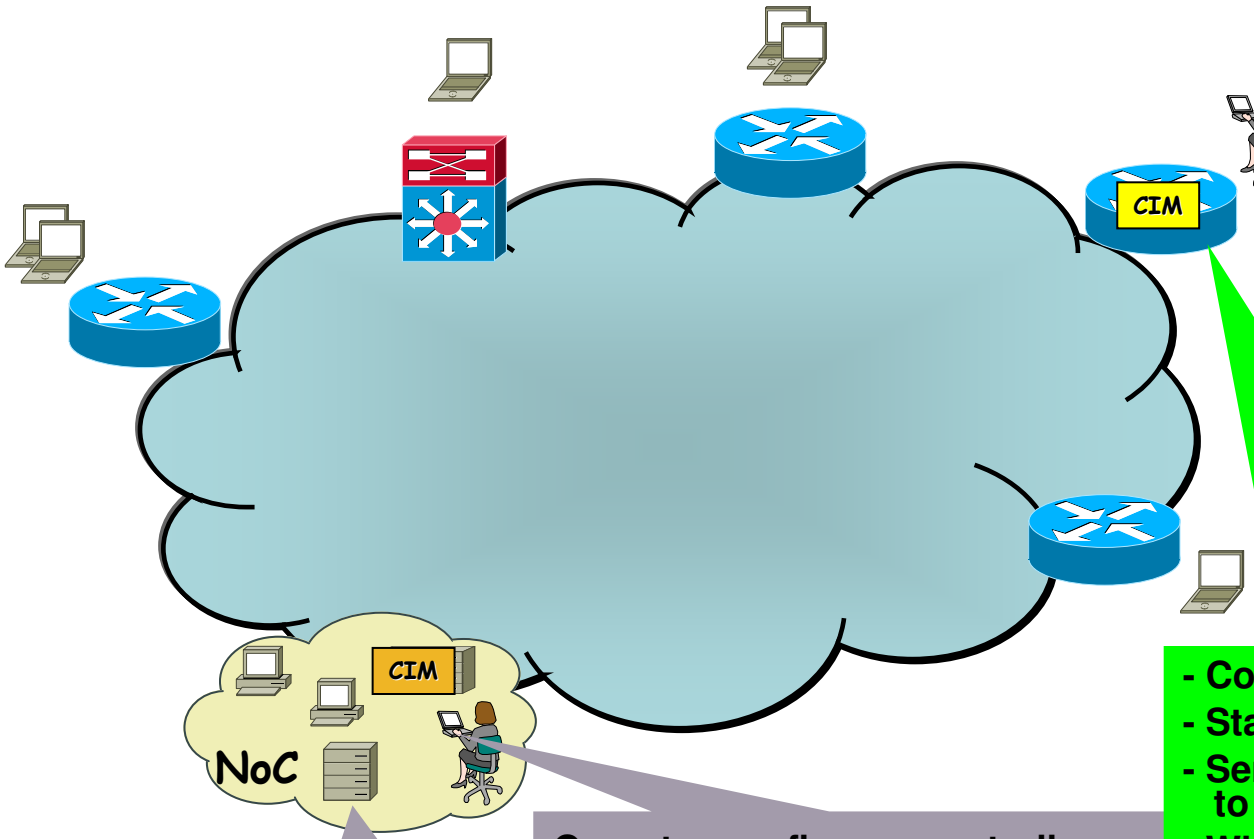
Threat detected by threat correlation and detection tools

Operator configures controller:

- Create Control Information Message
  e.g. *block* udp port 1434, all source and destination addresses, on all routers, switches, all Interfaces
- Send CIM to network

Use Case 2: Troubleshooting and Analysis

Distributed Sniffing Through Central Console



- Users call NOC to complain of slow application response
- NOC suspects there is a problem, but needs more information to troubleshoot

- Consumer receive CIM
- Starts capturing packets
- Sends CIM acknowledgement back to controller
- When capture completes, sends packet capture to NOC Sniffer

Operator configures controller:

- Create Control Information Messa
  e.g. Capture 5 MB of traffic flow and transfer via tftp to NoC with sniffer for further analysis
- Send CIM to select targets

Operator receives packet capture, analyzes it and takes corrective actions

Solution Requirements

Maintain Network Availability

Solution Requirements Summary

Need a secure and reliable communication mechanism to immediately propagate network control and policy changes throughout the network to provide rapid security remediation and to facilitate troubleshooting and analysis

- **Required Attributes of Solution**
  - Simple to use, especially in rapid response situations
  - Scaleable (speed, number of devices)
  - Ability to apply policies to various network device types
  - Reliable & Predictable: Immediate feedback on the status of actions
  - Will not conflict with provisioning system

Solution Overview

- **Controller**

  Centrally located server; distributes Control Information Messages (CIMs) throughout the network, listens for responses, provides 'state of play' in real-time

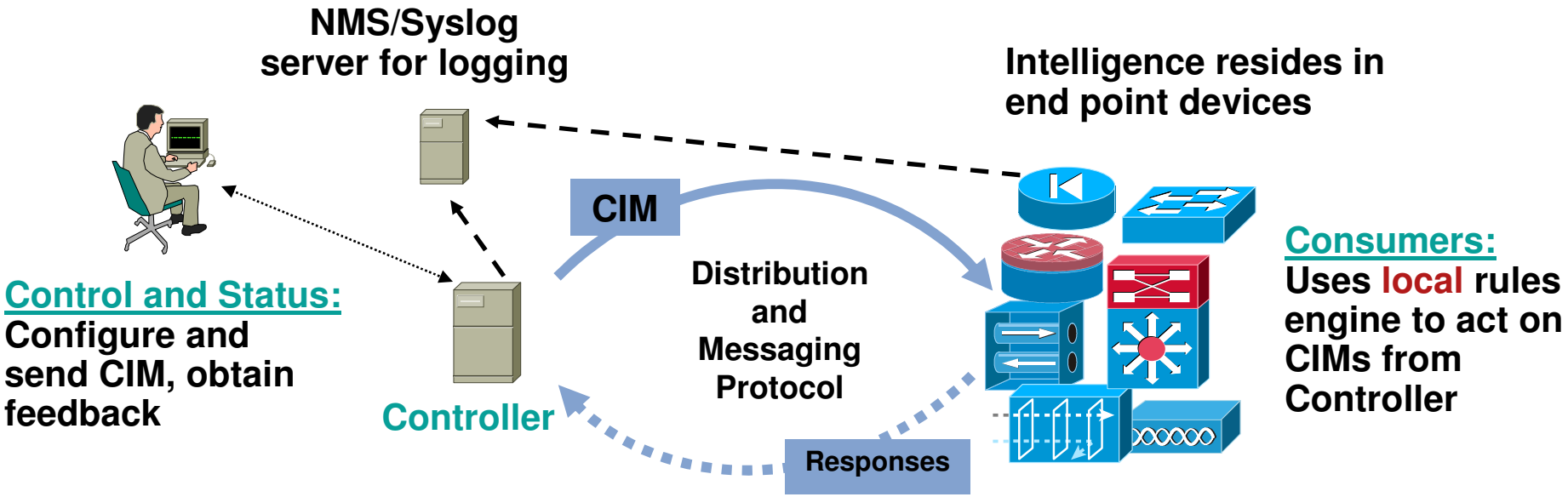
- **Consumer**

  Cisco routers and switches; receives CIMs, acts on them, and informs controller of action taken

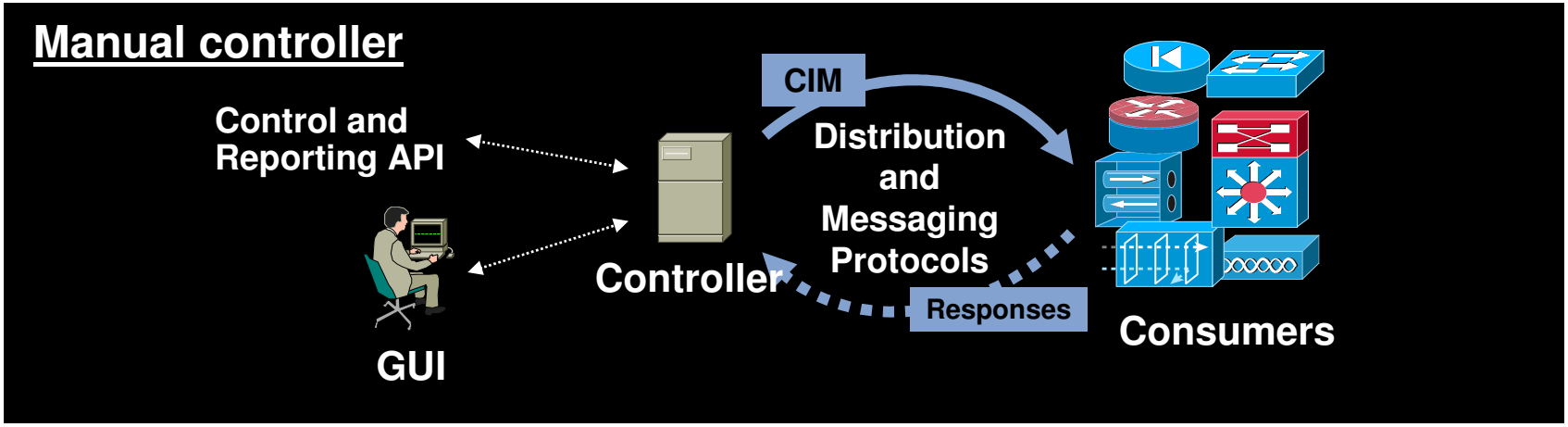
  Uses pre-configured policies which determine responses to CIMs (i.e. block using ACL)

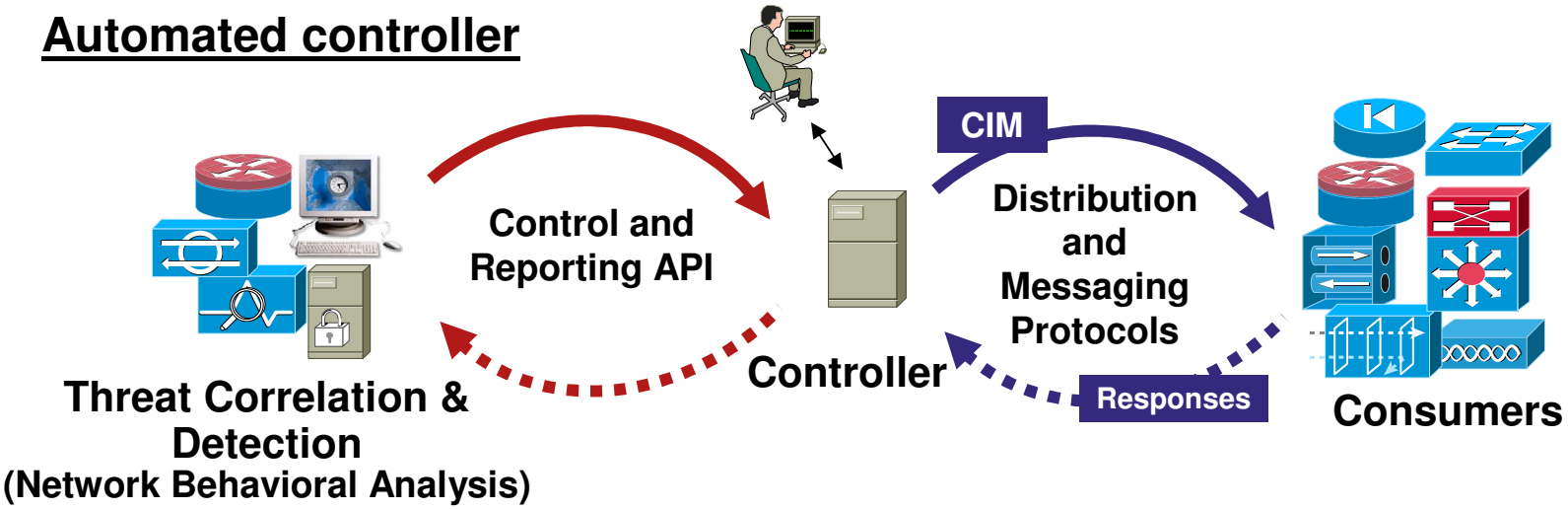
- **Integrated distribution and messaging protocol**

  Rapidly and securely distributes device independent CIMs throughout the network

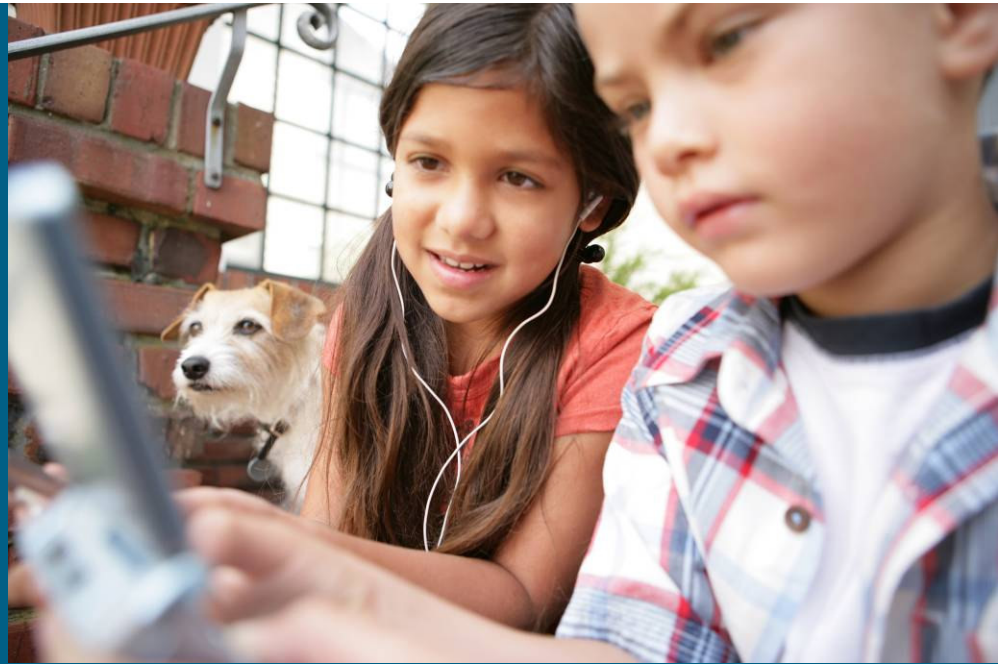


Manual and Automated





The Future of Behavioral Network Security



The Future of Behavioral Network Security

- We will see more use of NBA solutions in addition to traditonal SIM solutions as both technologies have their specific advantages
- Inter-device security communication will increase dramatically, both in order to enhance detection and also in order to speed up mitigation
- Sharing of security information and threat fingerprints will increase (ref. Ironport Senderbase)
- Threat Defense and Mitigation will need to become more rapid as human reaction times are no longer sufficient. This includes fully automated threat defense....