Securing the Data Center:
Technologies and Best Practices

Timothy Snow
Consulting System Engineer (Security)
Asia Region
snow@cisco.com

The Need for Security

A DC Security Strategy

Data Center Infrastructure

Secure Management

“ The biggest challenge we have is keeping the door open during a [security] event.”

Large Global Financial Customer, NYC

The Security Challenge: Disruption, Loss, and Damage

Disruption affects Productivity (The CIO Problem)

1. External source (e.g. DDoS)
2. Internal source (e.g. virus breakout)
3. Accidental source (e.g. configuration mistake)

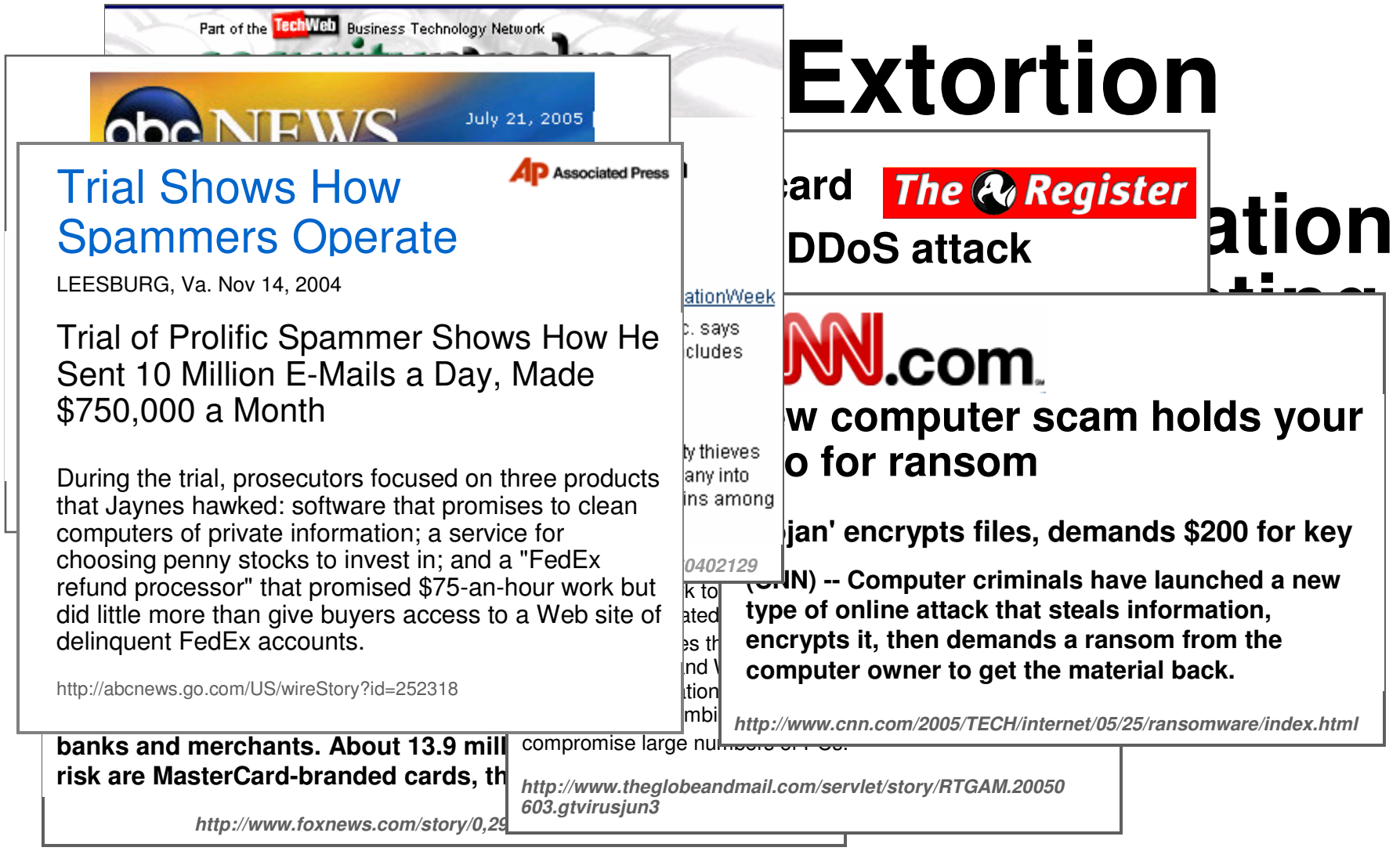
Loss affects Value (The CFO Problem)

1. Random theft (e.g. break-in, no coordination)
2. Directed theft (e.g. espionage)
3. Accidental loss (e.g. email inadvertently sent)

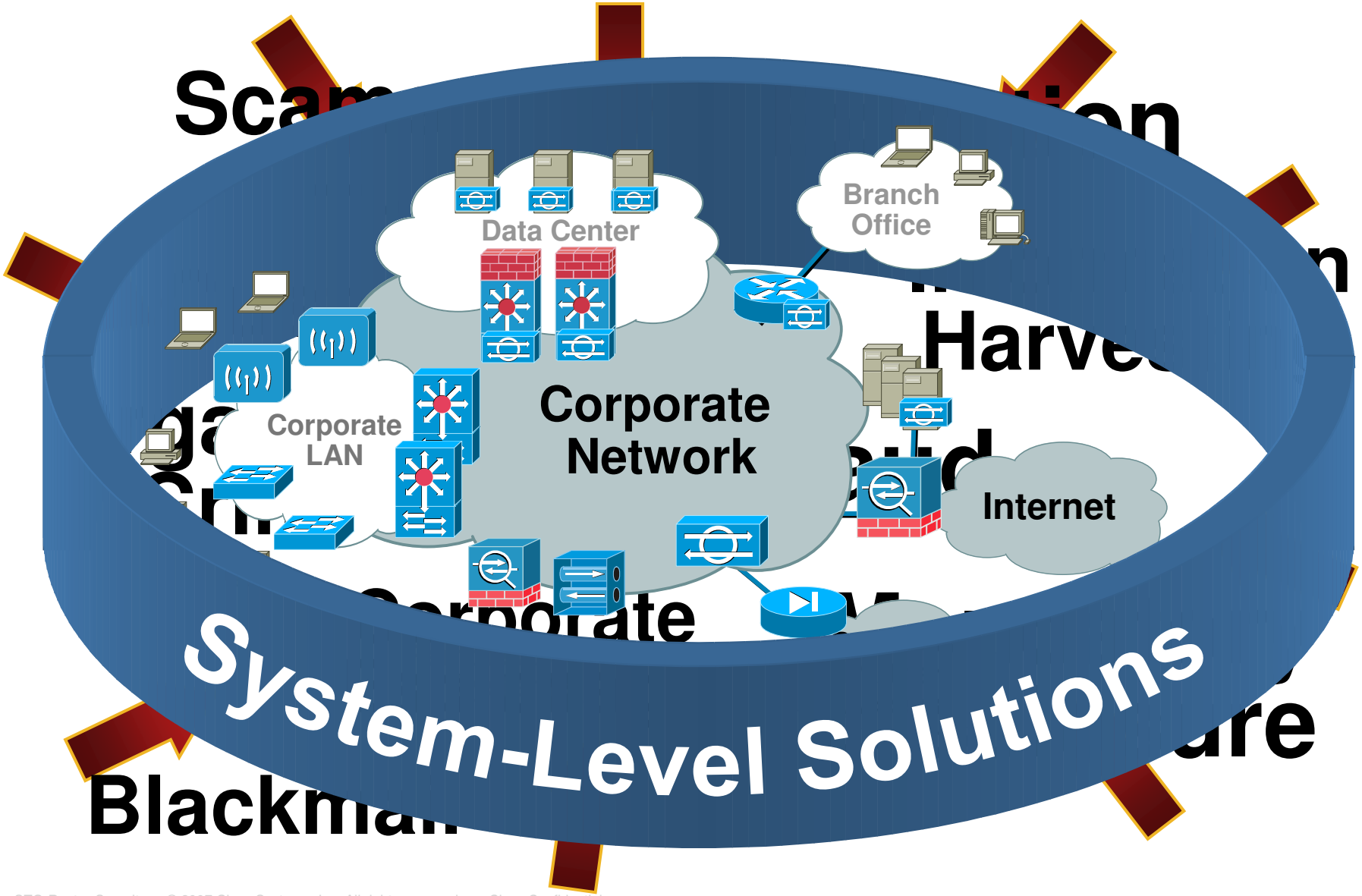
Damage affects Reputation (The CEO Problem)

1. Public visage (e.g. web site defacement)
2. Shareholder confidence (e.g. loss of information)
3. Accidental damage (e.g. a misstep in industry)

Evolution of Security Challenges



Beyond Worms and Viruses



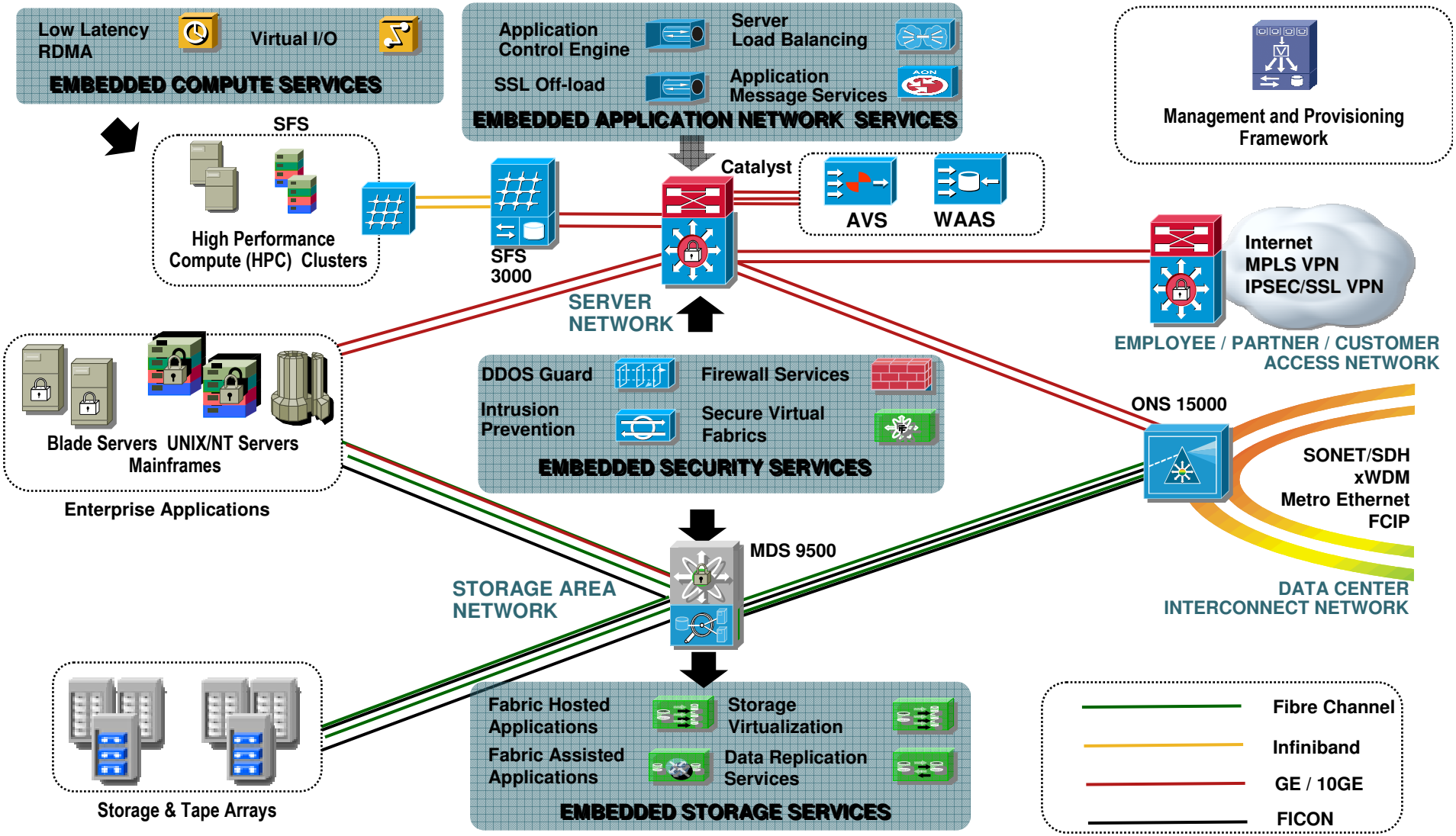
The Need for Security

A DC Security Strategy

Data Center Infrastructure

Secure Management

Services Embedded in the Fabric



The Need for Security
A DC Security Strategy
- IDS
- Host IDS (CSA)
- FWSM
- DDOS

Data Center Infrastructure
Secure Management

Intrusion Management
What a Typical Hacker Will Do?

- Perform RECONNAISSANCE

  Scan ports and systems to find out your network topology, PCs, servers, operating systems, etc.

- Find VULNERABILITIES in your network

  What desktop/servers are running vulnerable services or OS

- Attacker EXPLOITS a known VULNERABILITY to gain access to servers, change data, steal information or cause denial of service

  Known vulnerabilities

  CGI-Scripts

  Buffer overflows

  Trojan horses

  Traffic flooding

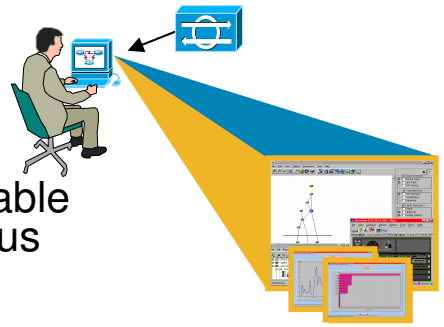
Intrusion Management
How do I detect malicious behavior?

How do I know when something is wrong?

- Network IDS collects and analyzes data from the network
- When activity matches a predefined signature and alert is sent to the management system
- Several methods are available for stopping malicious activity once detected: TCP reset, shunning, manual intervention

BENEFITS

- Alerts are given when an attack occurs and manual or automatic action can be taken against it
- Resets can be sent to systems trying to spawn a virus or attack
- You know what is going on in your network in real time!



Why Cisco:

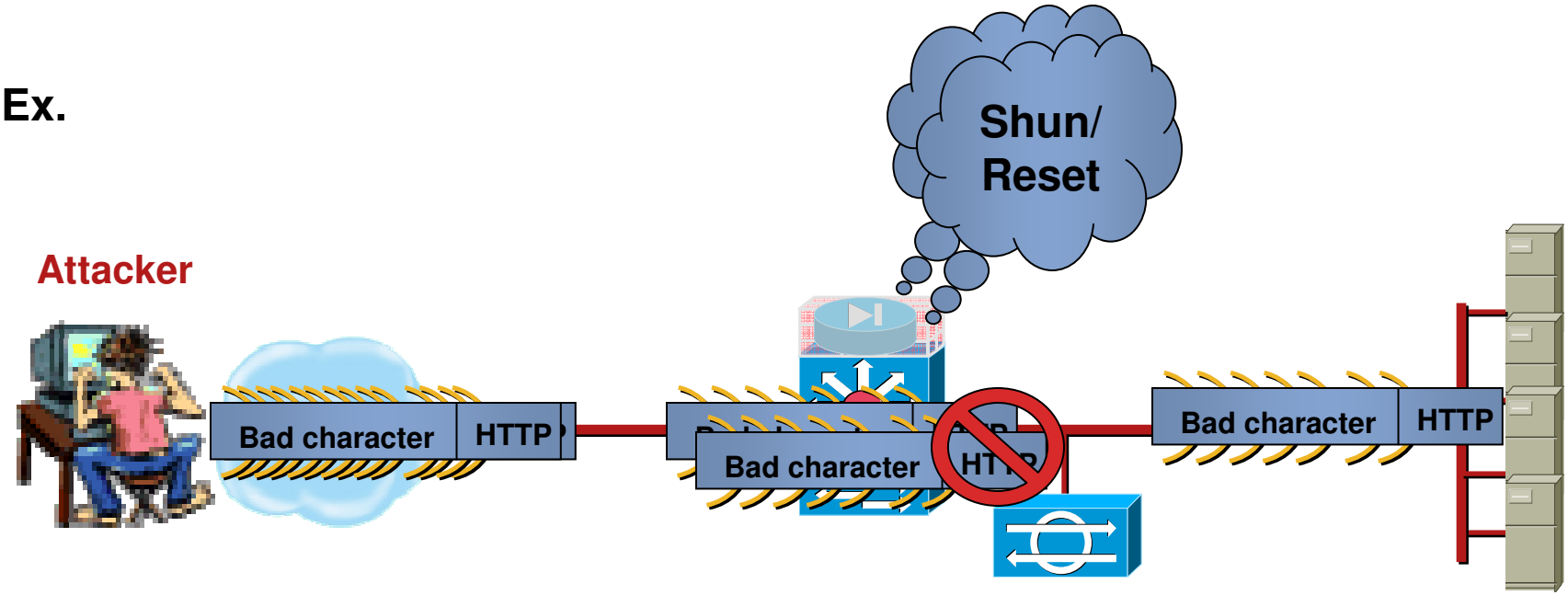
Cisco Network IDS provides an easily deployable and manageable solution for detecting, logging and taking action against malicious network traffic (Inband or OOB)

Intrusion Management
Why Network IDS?

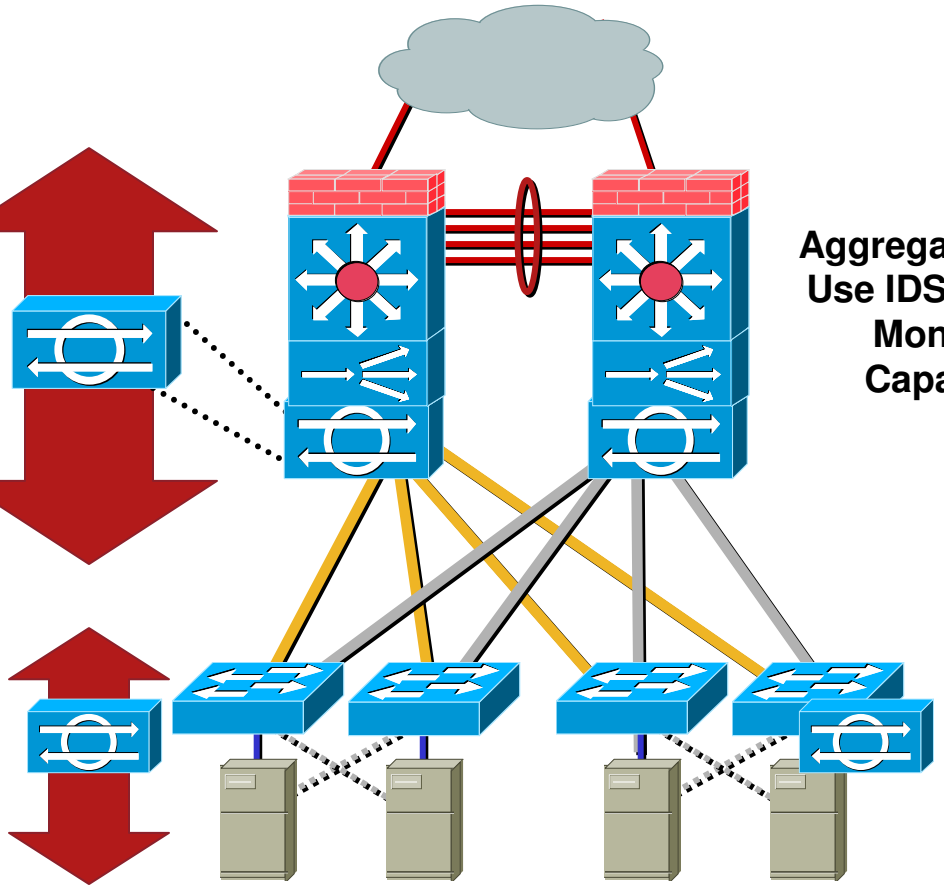
Because Firewalls are no longer enough

- Network IDS goes beyond firewall capabilities by providing network and application protection through the use of signatures, anomalies, pattern matching, etc
- Guards against fragmentation, flooding (needle in a hay stack), buffer overflows
- IDS uses shuns and resets to stop an attack once the attack has been detected

Ex.



Intrusion Management
Network IDS in the Data Center



Predictable Traffic Path Allows IDS to Monitor Synchronous Flows

Aggregation Layer: Use IDS L3 and L4 Monitoring Capabilities

Access Layers: Use IDS L2 and L7 Monitoring Capabilities

Ex. Signatures to Stop Layer 2 Attacks

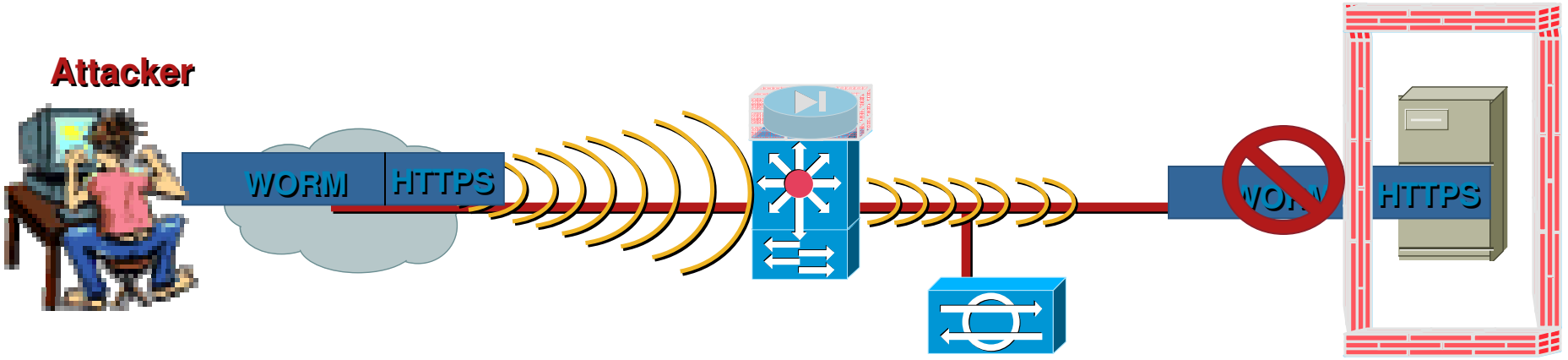
- 7101—ARP Source Broadcast
- 7102—ARP Reply-to-Broadcast
- 7104—ARP MacAddress-Flip-Flop-Response
- 7105—ARP Imbalance-of-Requests

Intrusion Management
Why Host IPS?

- Patching isn't always the easiest solution; sometimes requires service pack upgrades etc…
- Patches only work after the virus or worm has been discovered
- The behavior-based IPS feature protects the servers and applications without any updating at all
- Only uses a maximum of 3–4% server CPU

Intrusion Management
Host IPS for the Server Farm

- Server hardening
  - File system/OS lockdown and baseline
  - Controlled registry access
  - Buffer overflow and network attack protection
- Application security policies
  - IIS/Apache, SQL Server, Exchange, Sendmail, DHCP, DNS, Microsoft Office, Instant Messenger, custom applications
- Cisco Security Agent does not require reboot of server post install



Endpoint Security Must:

- Protect the integrity of desktops and servers, on and off the corporate network, from worms, viruses and spyware
- Identify data from critical or important applications, so the network can prioritize it
- Cooperate with the network infrastructure to establish required levels of trust and auditability, and to react to threats in real-time
- CSA default behavioral rules protect against Zero-Day virii, worms, spyware, etc. 'sight unseen'
- CSA with Trusted QoS control ensures that traffic is marked so that the network can apply correct handling
- CSA integration into Cisco NAC establishes endpoint-network trust relationship which enhances total network security and report on health

Intrusion Management
Why Host IPS?

- Patching isn't always the easiest solution; sometimes requires service pack upgrades etc…
- Patches only work after the virus or worm has been discovered
- The behavior-based IPS feature protects the servers and applications without any updating at all
- Only uses a maximum of 3–4% server CPU

Zero-Day Protection

- Cisco defines Host-Based Intrusion Prevention as the ability to stop Zero-Day malicious code without reconfiguration or update.
- CSA has the industry's best record of stopping Zero Day exploits, worms, and viruses over past 4 years:
  - 2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debploit, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability, Zotob

No signatures, reconfiguration or binary updates required

Day-Zero Protection

- Traditional issue: vulnerable to day-zero attacks, often resource intensive patching effort
- SDN Solution: assets protected against new and unknown attacks via behavioral-based technology

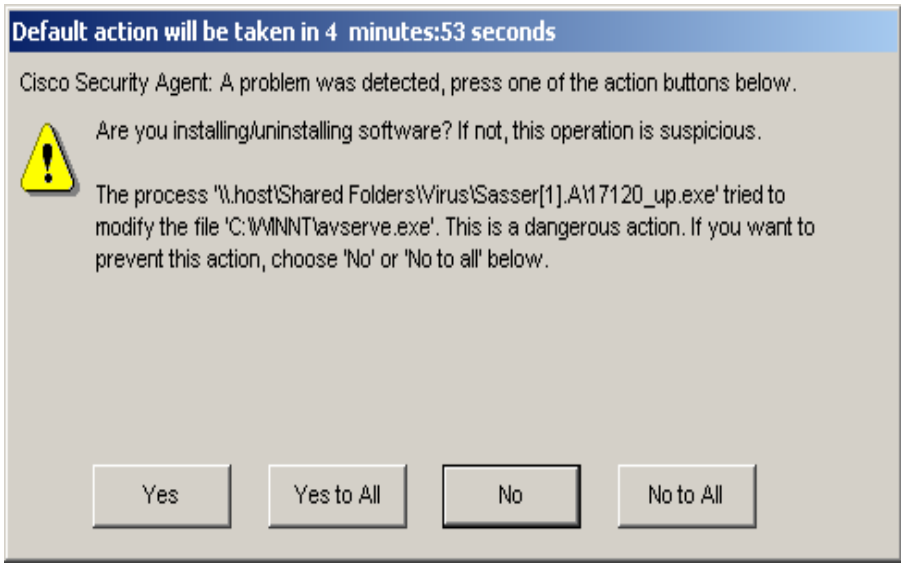
Sasser vs Cisco Security Agent

Randomly scans IP addresses on port 445/tcp. Can scan up to 1,024 addresses simultaneously

Creates remote shell on port 9996/tcp. It then starts an FTP server listening on port 5554/tcp

Victim system connects back to attacking system on port 5554/tcp to retrieve copy of worm

Crashes infected devices
Causes systems to reboot continuously

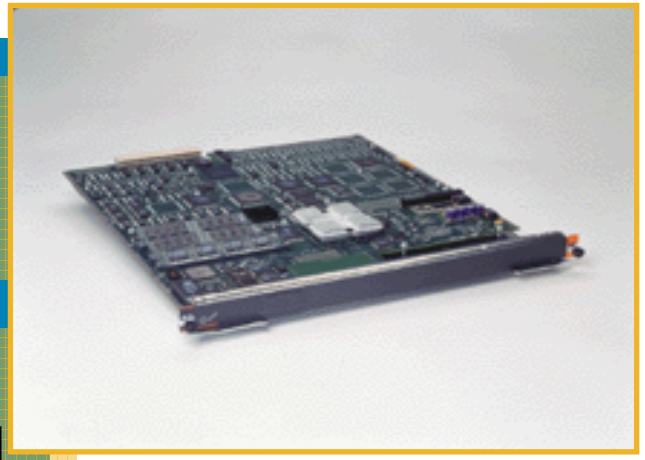


The Need for Security
A DC Security Strategy
- IDS
- Host IDS (CSA)
- FWSM
- DDOS

Data Center Infrastructure
Secure Management

Catalyst 6500 / 7600 Router Firewall Services Module

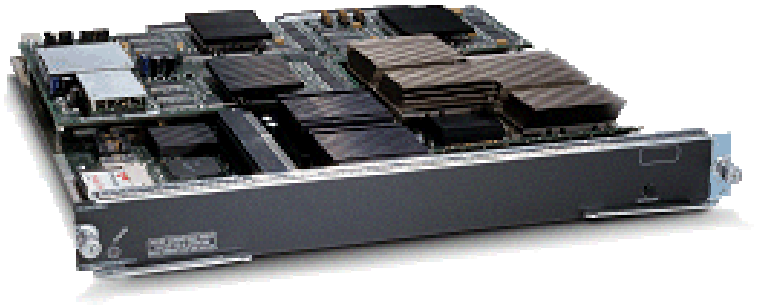
- High performance and scalability firewall up to 5 Gbps per module and 20 Gbps per chassis
- Integrated security module providing superior network infrastructure services and ease of management
- Industry-leading virtualized services allowing consolidation, granular customized control with lower TCO
- Flexible management solutions lower operational costs



Fabric Enabled

Firewall Services Module

Cisco's Highest Performance Firewall



PIX 7.0 base Feature Set

- High Performance Firewall: 5.5Gbps bandwidth
- 2.8 Million pps throughput
- 1 million concurrent connections
- 100K new connections/sec for HTTP, DNS and enhanced SMTP

250 Virtual firewalls/contexts

- Transparent (L2) and Routed (L3) firewalls in the same service module
- Resource Manager: Assign Service Classes, Resource Limits
- 256 VLANs per context with maximum of 1000 VLANs
- LAN failover active/standby and active/active (both intra/inter chassis)
- Dynamic Routing: OSPF and RIP (2 OSPF virtual routers)
- Support multiple blades in the chassis, up to 4 for 20Gbps

80K access-lists enforced in hardware

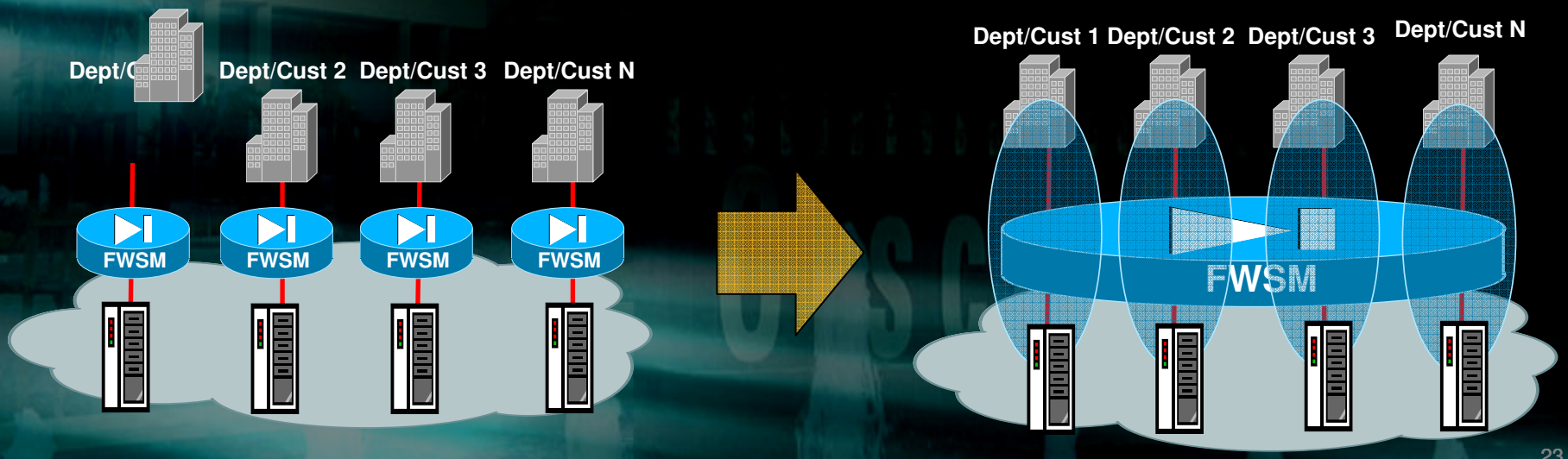
- Supported on Native IOS 12.1(13E) and CatOS 7.5(1) onwards
- Jumbo-ready (8500 bytes)

FWSM v3.1

Virtual Firewall
Highly Scalable Multi-Context Security Services

Security Contexts (Virtual Firewalls) lower operational costs

- Reduce overall management and support costs by hosting multiple virtual firewalls in a single device
- Enables the logical partitioning of a single FWSM into multiple logical firewalls, each with their own unique policies and administration (NAT, ACL, Protocol Inspection, SNMP, Syslog, DHCP)
- Enables multiple DMZs and service differentiation classes (gold, silver, bronze) per context
- Resource Manager limits resource usage on a per context basis, ensuring protection between contexts
- Supports 20, 50, 100 and 250 virtual firewall licenses
- Ideal solution for consolidating multiple firewalls into a single FWSM



Transparent Firewall
Delivers "Drop In" L2-L7 Security Services at L2

Transparent Firewall provides rapid deployment security services

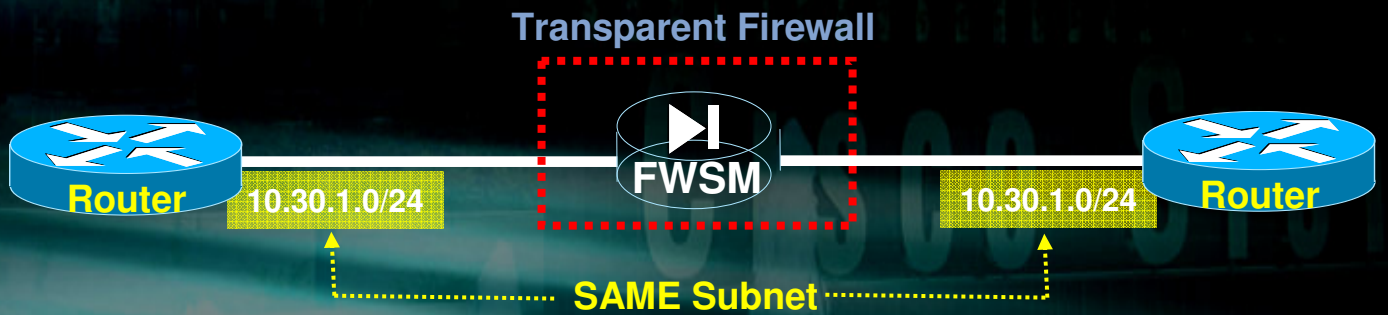
- Simplifies and speeds deployment

  Provides ability to rapidly "drop in" FWSM into existing networks without requiring any addressing changes

  Useful in data center server farm and internal firewall deployments

  Delivers high-performance stealth L2-L7 security services within same subnet and provides protection against network layer attacks

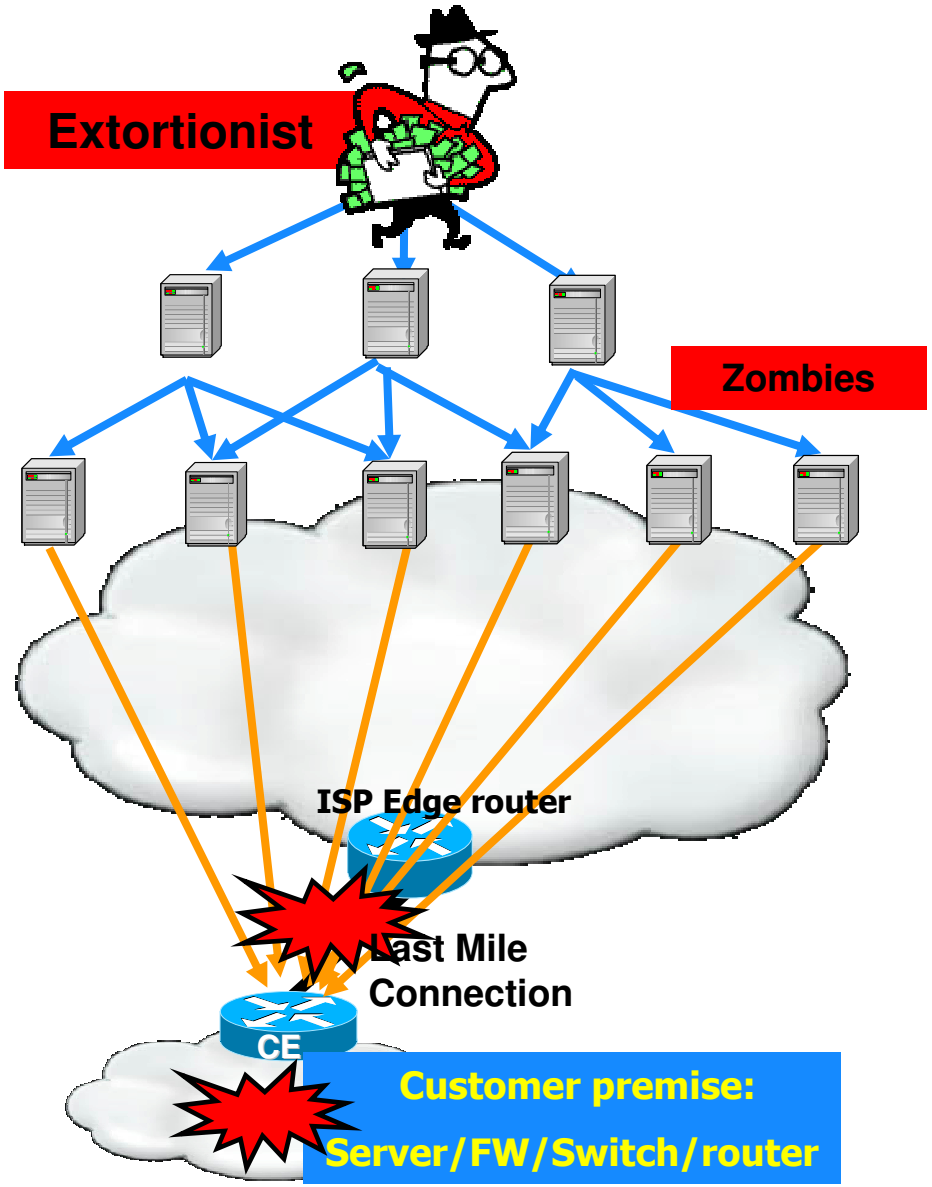
  Leverage L3 features (such as Routing, Multicast, High Availability) supported by IOS and switching platform.



The Need for Security
A DC Security Strategy
- IDS
- Host IDS (CSA)
- FWSM
- DDOS

Secure Management

BOTNETS – Making DDoS Attacks Easy

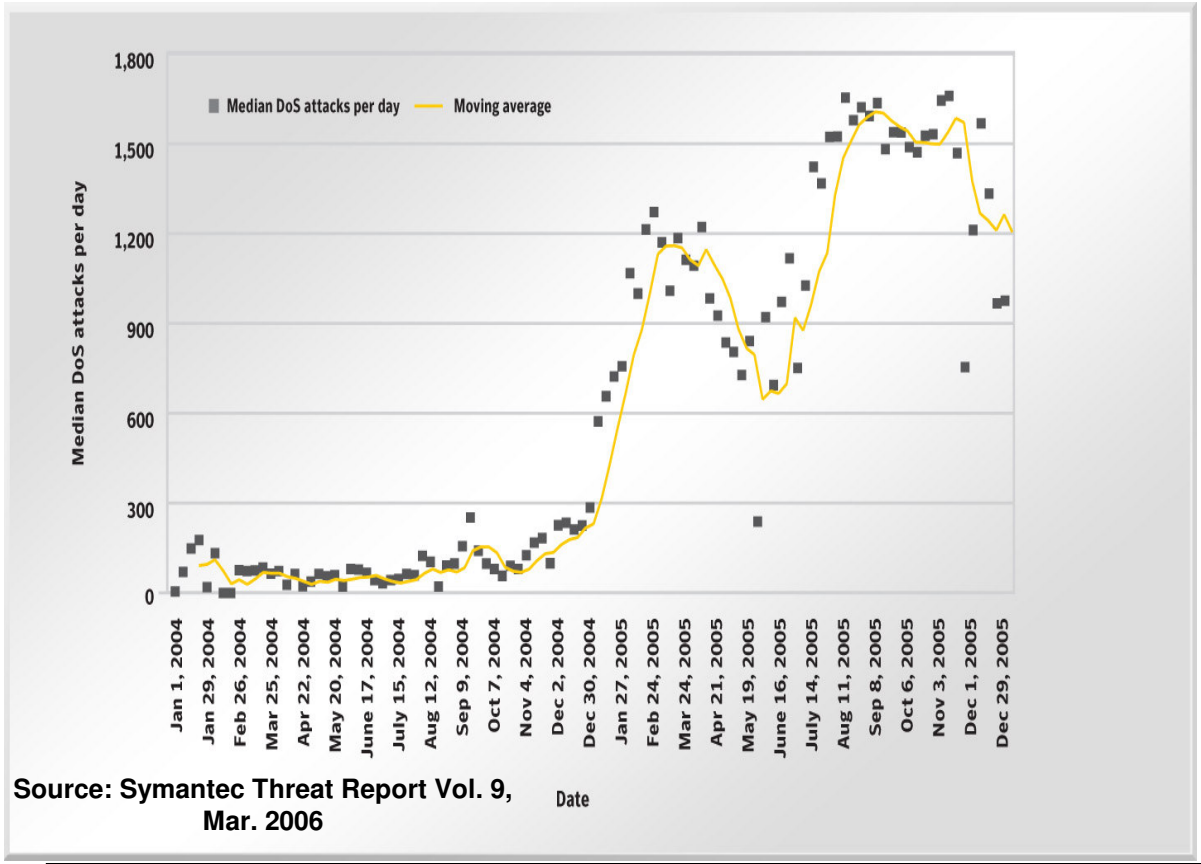


2 for 1 Special

BOTNETs for Rent!

- A BOTNET is comprised of computers that have been broken into and planted with programs (zombies) that can be directed to launch attacks from a central controller computer
- BOTNETs allow for all the types of DDOS attacks: ICMP Attacks, TCP Attacks, and UDP Attacks, http overload
- Options for deploying BOTNETs are extensive and new tools are created to exploit the latest system vulnerabilities
- A relatively small BOTNET with only 1000 zombies can cause a great deal of damage.
- For Example: 1000 home PCs with an average upstream bandwidth of 128KBit/s can offer more than 100MBit/s
- Size of attacks are ever increasing and independent of last mile bandwidth

BOTNETS GROWING TOO FAST



Source: Symantec Threat Report Vol. 9, Mar. 2006

- 10,000+ new bots added everyday
- DoS attacks grow five-fold in 12 months: Dec. 1, 2004-2005
- Large % of DDoS attacks are motivated by extortion demands

CNN: Over 75 Million computers are infected with BOTNET software

http://www.cnn.com/2006/TECH/internet/01/31/furst/

What is Cisco protecting from DDoS Attacks?

- Revenue stream - 93% of revenue booked online via www.cisco.com & related systems.

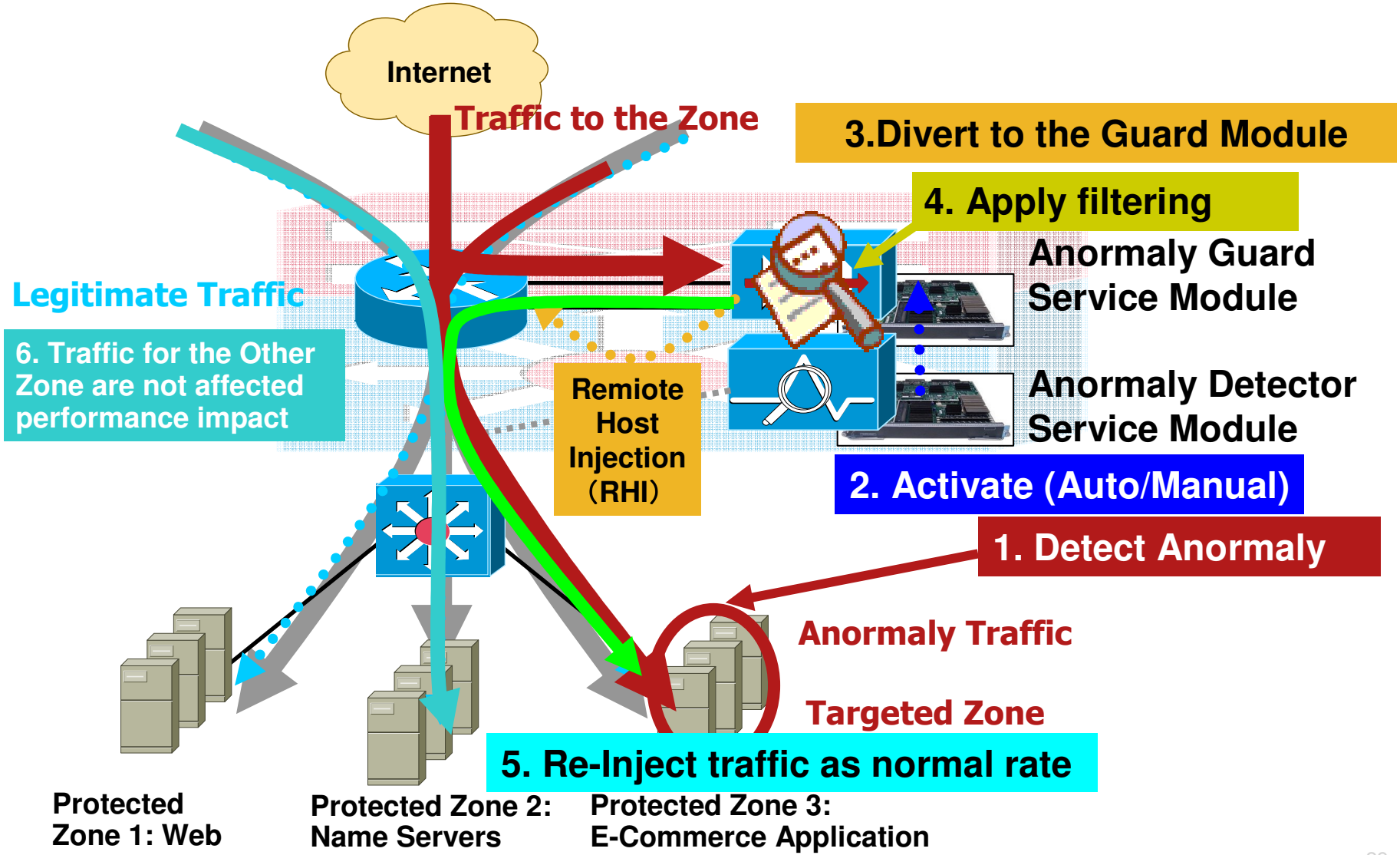
  If there were a DDoS attack, Cisco would lose an ***average of $43,005.05 per minute.***

- Customer support - 80% of TAC cases opened via www.cisco.com

  If there were a DDoS attack, Cisco could not receive the TAC case

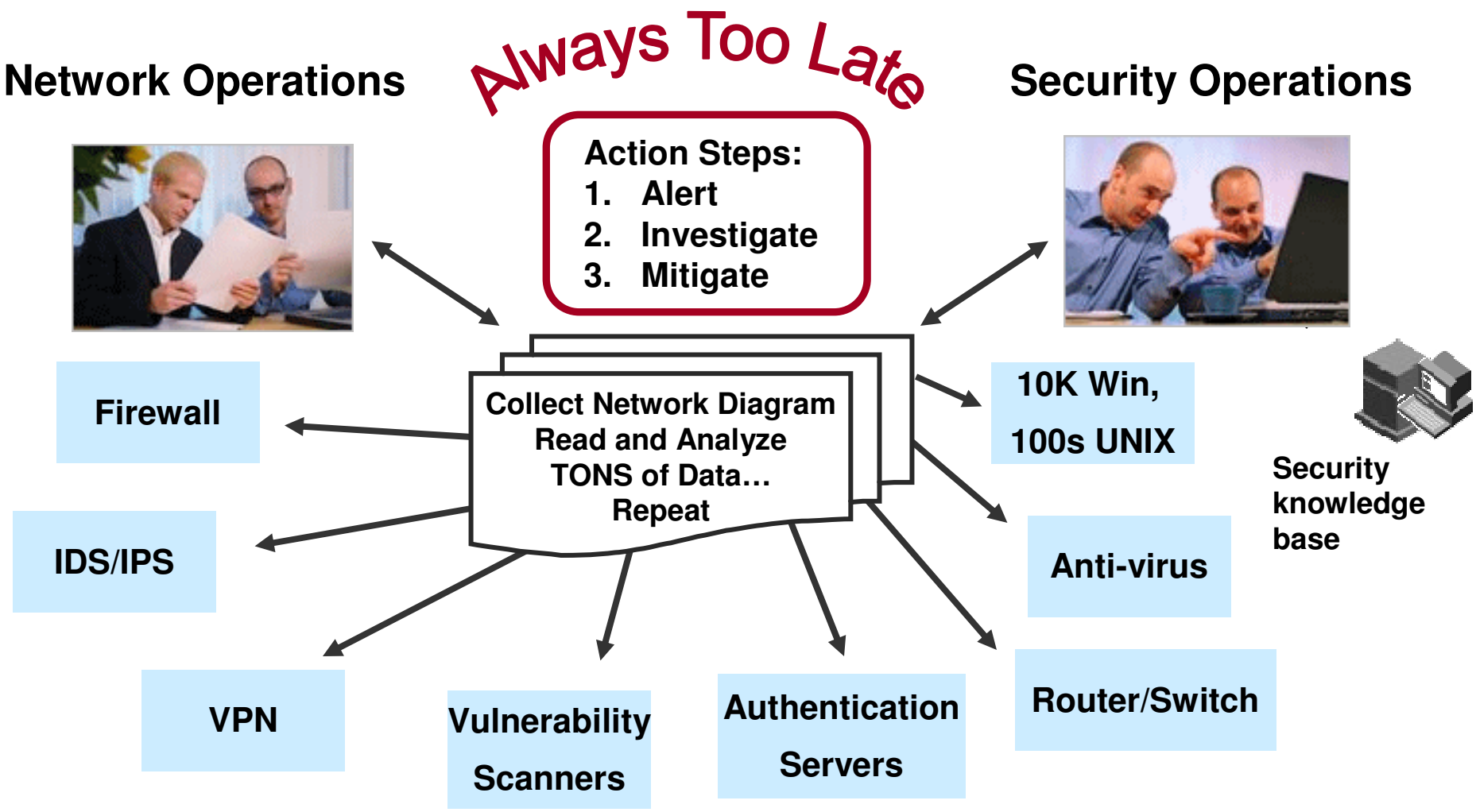
What is the cost of your Data Centre downtime?

Internal Diversion (Integrated Model, Inline Network Configuration)

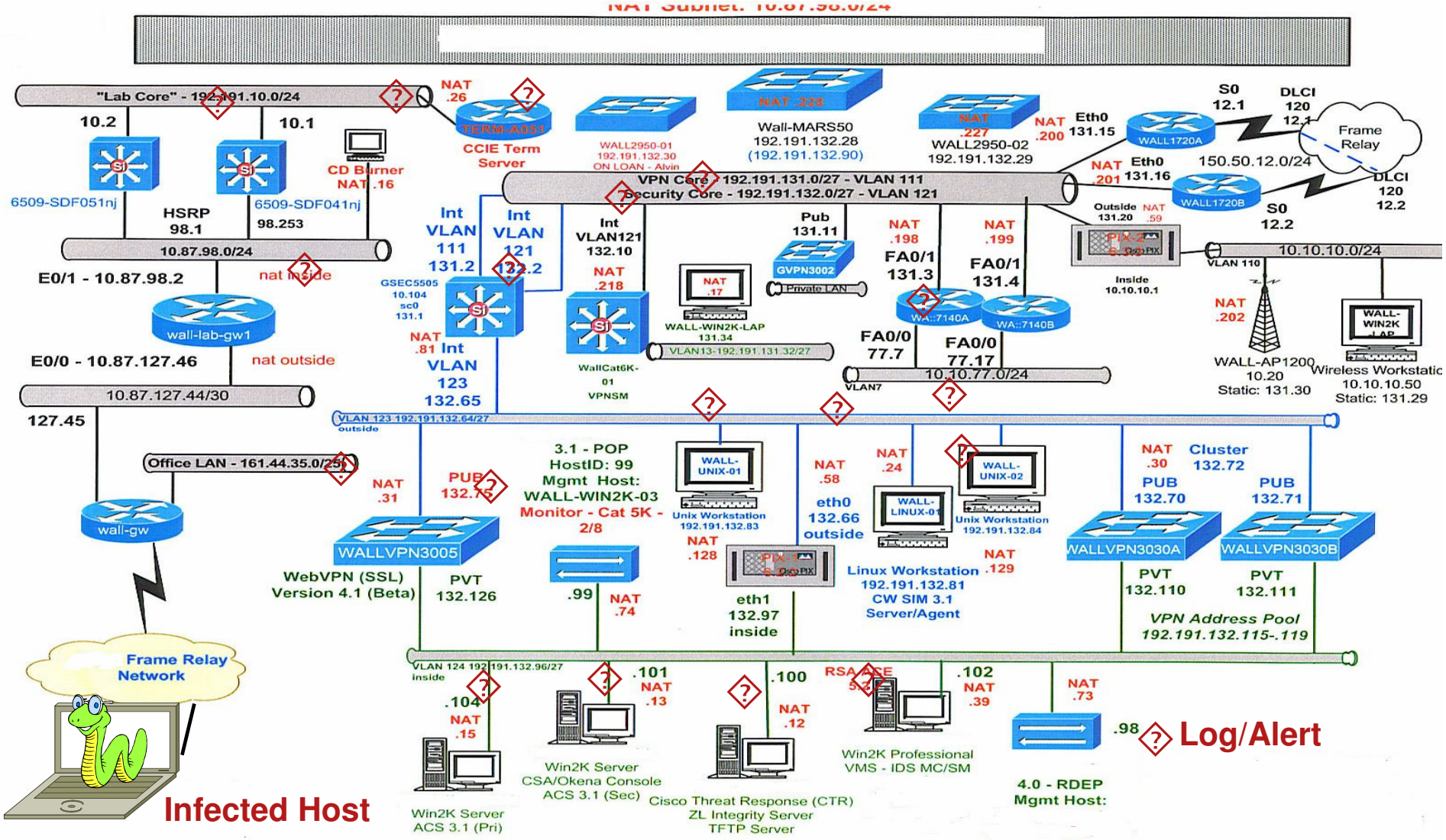


The Need for Security
A DC Security Strategy
Data Center Infrastructure
Secure Management

Security Operations / Reactions Today



Defense-In-Depth = Complexity

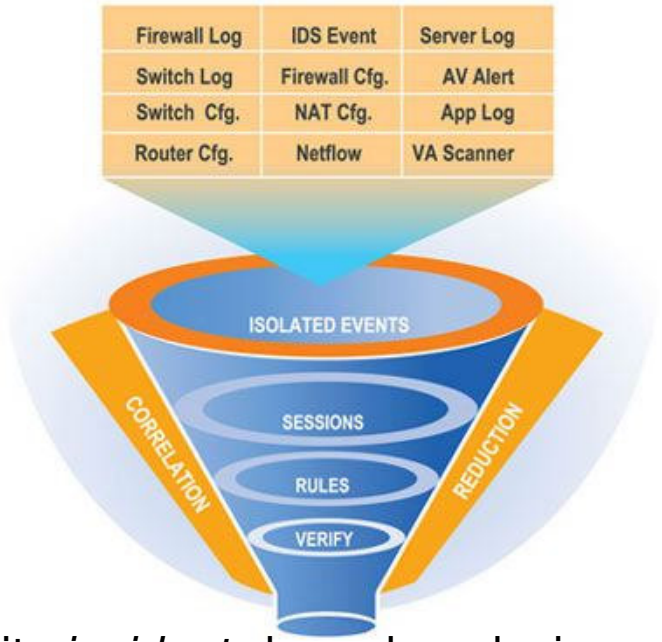


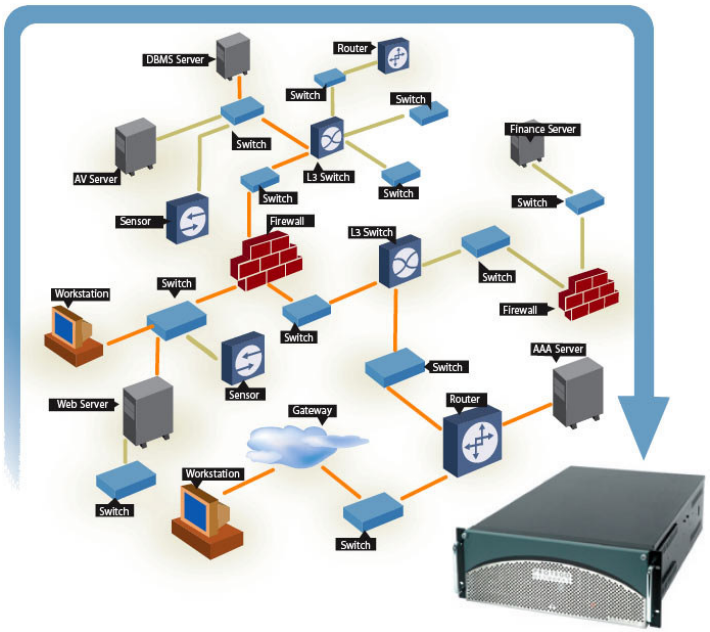
Mitigation, Analysis, and Response System (MARS) *Next Generation SIM/STM*

- Leverage YOUR existing investment to build "pervasive security"
- Correlate data from across the Enterprise

  NIDS, Firewalls, Routers, Switches, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs, Multi-Vendor
- Rapidly locate and mitigate attacks





- Key Features

  Determines security *incidents* based on device *messages*, *events*, and "*sessions*"

  Incidents are topologically aware for visualization and replay

  Mitigation on L2 ports and L3 chokepoints

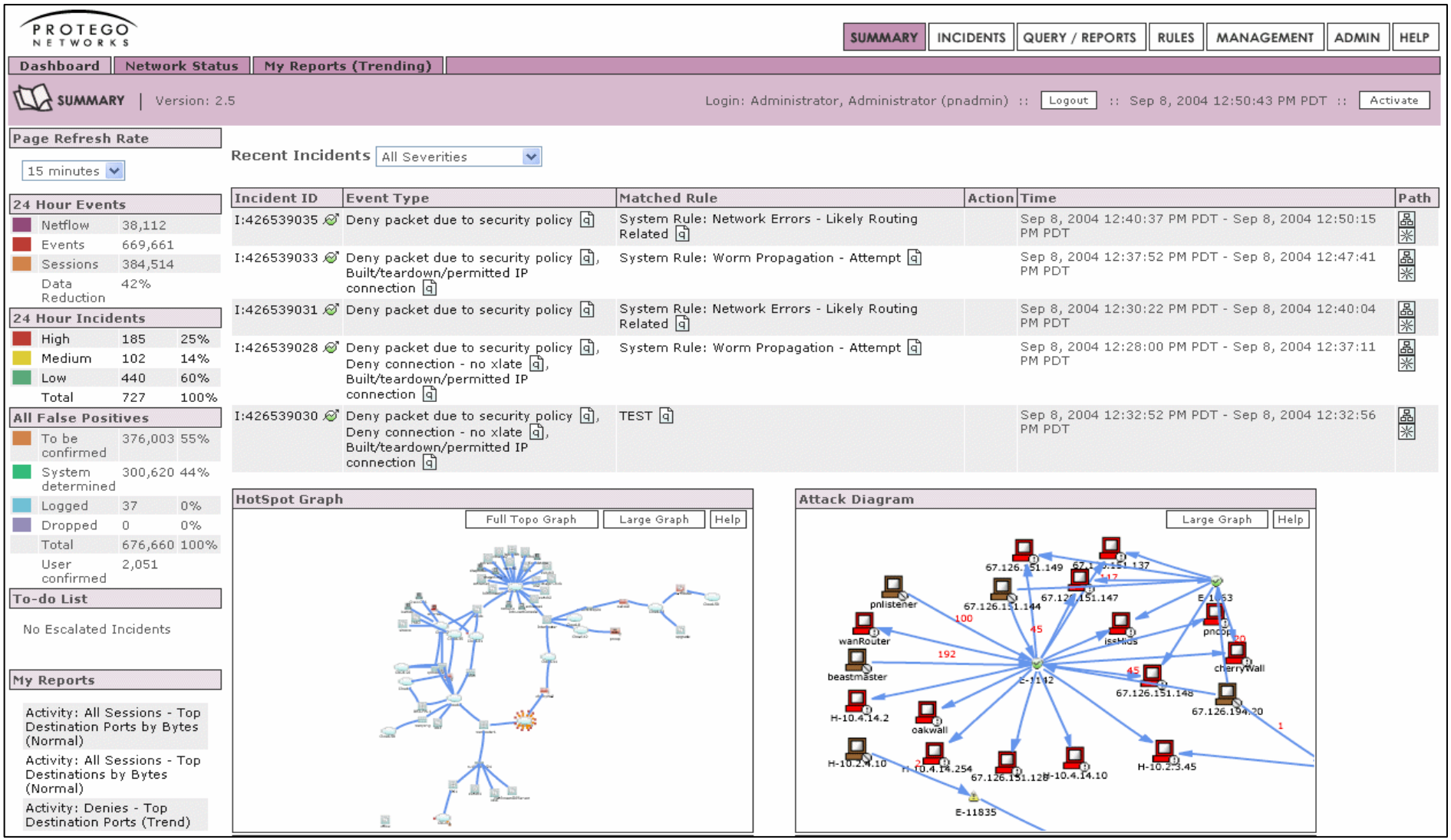
  Efficiently scales for real-time use across the Enterprise

  Onboard Nessus – Verification of Vulnerability

CS-MARS Device Support

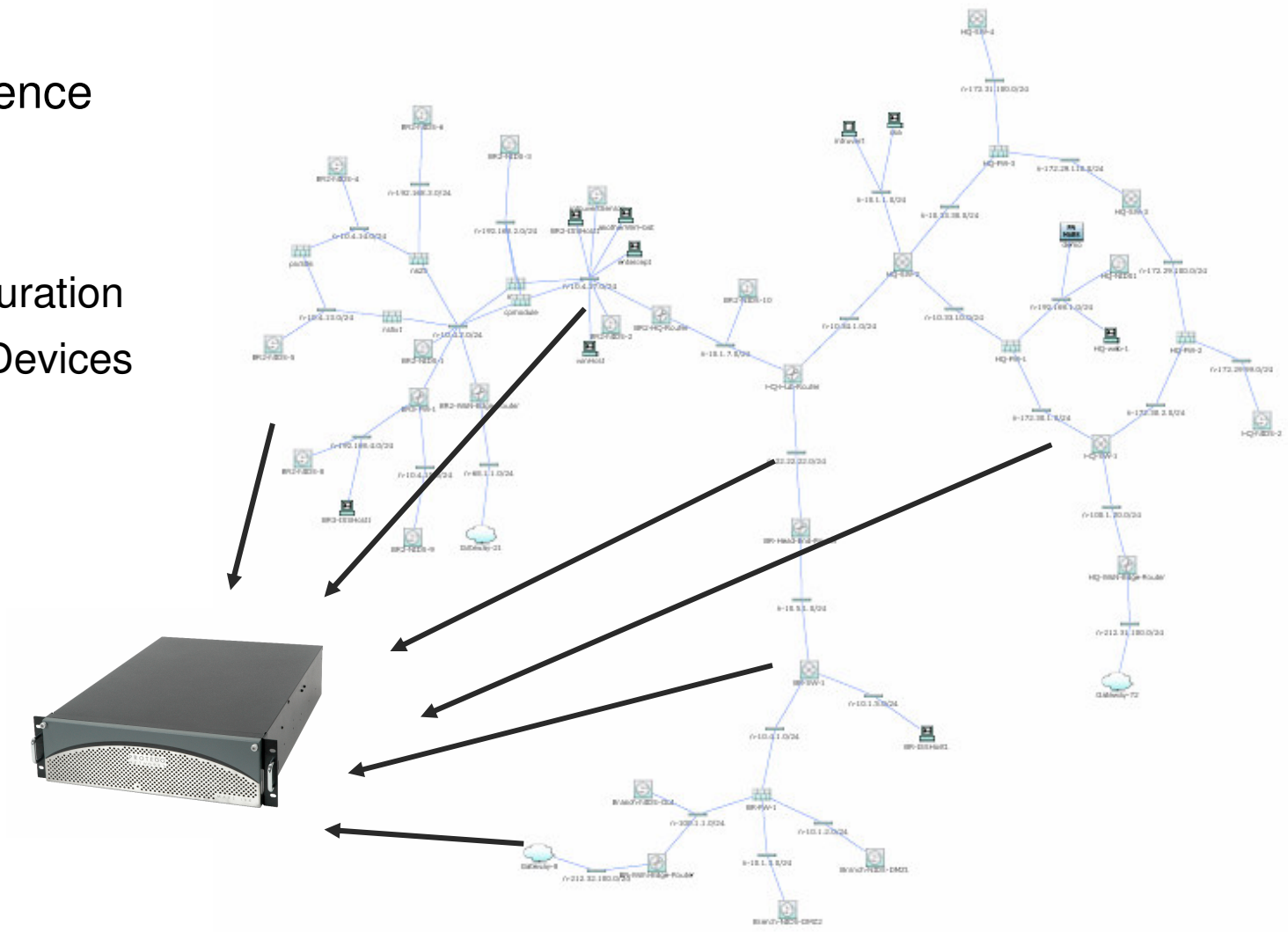
- Networking
  - Cisco IOS 11.x and 12.x, Catalyst OS 6.x
  - NetFlow v5/v7
  - NAC ACS 3.x
  - Extreme Extremeware 6.x
- Firewall/VPN
  - Cisco PIX 6.x, 7.x, ASA, IOS Firewall/IPS, FWSM 1.x, 2.3, 3.1 VPN Concentrator 4.x
  - CheckPoint Firewall-1 NG FPx, VPN-1
  - NetScreen Firewall 4.x, 5.x
  - Nokia Firewall
- IDS
  - Cisco NIDS 4.x, 5.x, IDSM 4.x, 5.x
  - Enterasys Dragon NIDS 6.x
  - ISS RealSecure Network Sensor 6.5, 7.0
  - Snort NIDS 2.x
  - McAfee Intrushield NIDS 1.x
  - NetScreen IDP 2.x
  - Symantec ManHunt 3.x
- Vulnerability Assessment
  - eEye REM 1.x
  - Foundstone FoundScan 3.x
  - Qualys Guard
- Host Security
  - Cisco Security Agent (CSA) 4.x
  - McAfee Entercept 2.5, 4.x
  - ISS RealSecure Host Sensor 6.5, 7.0
  - Symantec AnitVirus 9.x
- Host Log
  - Windows NT, 2000, 2003 (agent/agent-less)
  - Solaris
  - Linux
- Syslog
  - **Universal device support**
- Applications
  - Web servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10i database audit logs
  - Network Appliance NetCache

CS-MARS
“Command and Control”



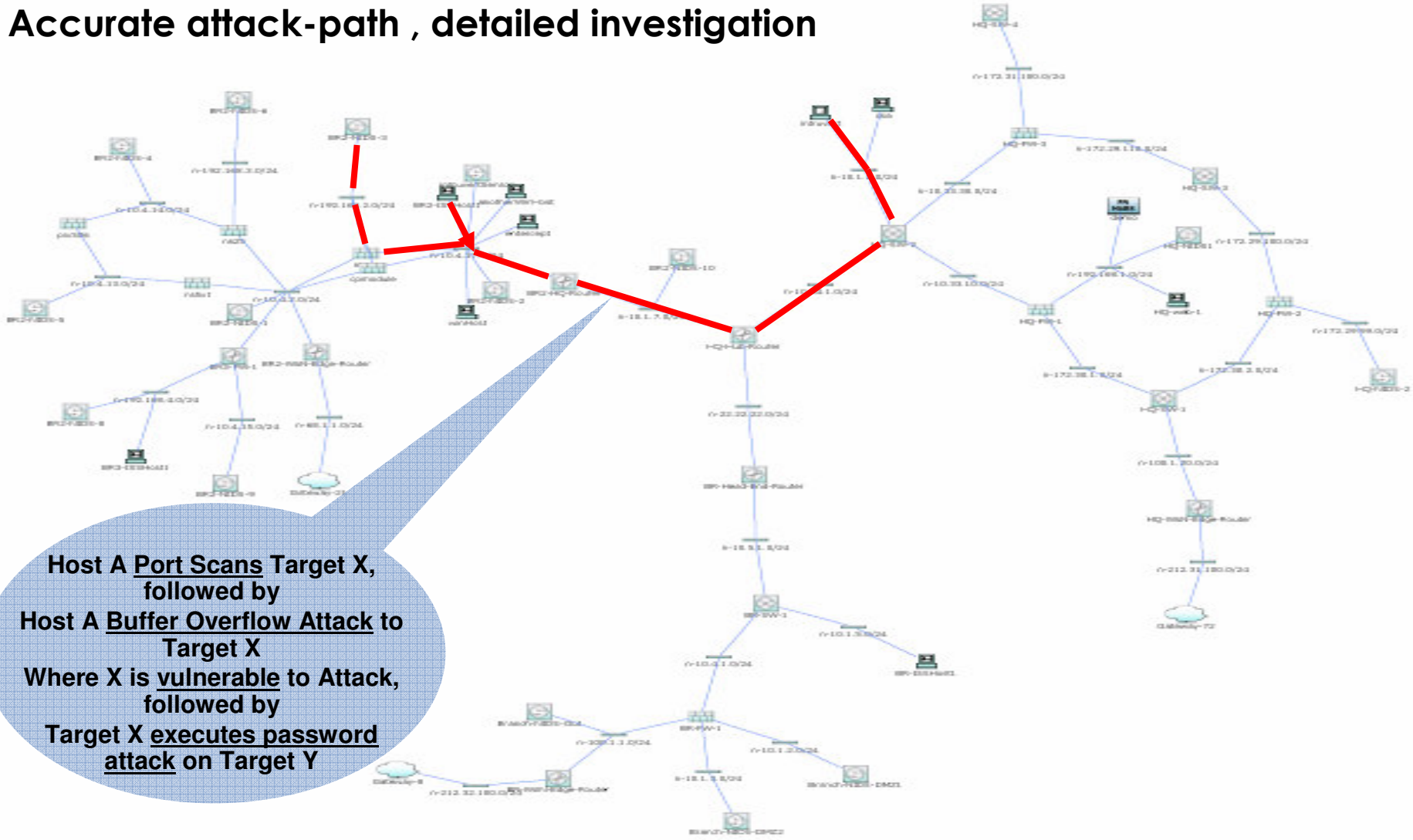
CS-MARS
"The Battlefield"

- Network Intelligence
  - Topology
  - Traffic Flow
  - Device Configuration
  - Enforcement Devices



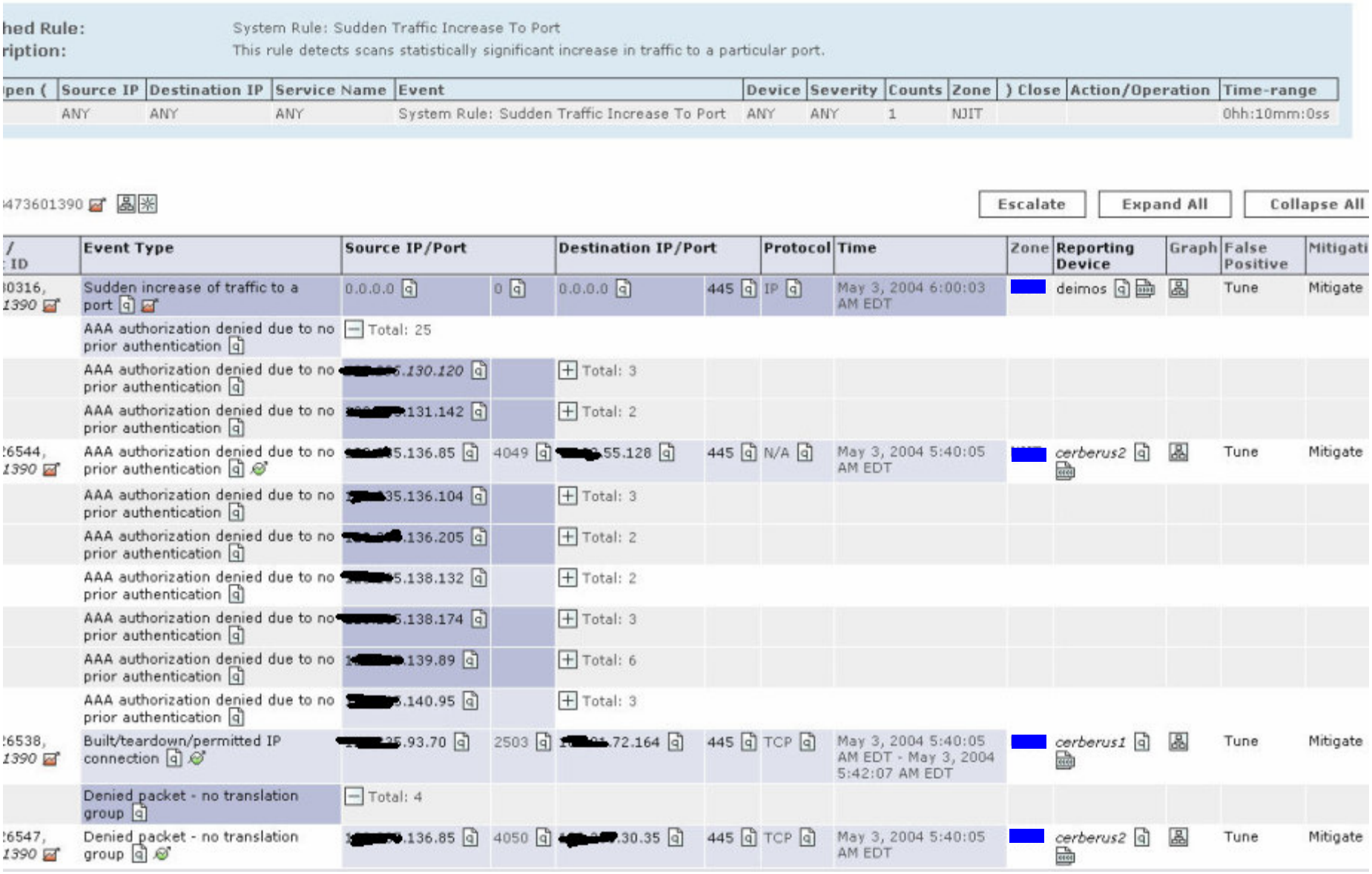
CS-MARS
"Connect the Dots"

Accurate attack-path , detailed investigation



CS-MARS in Action:
Sasser-D in a Northeast University

Incident that Pops Up in the Dashboard



hed Rule: System Rule: Sudden Traffic Increase To Port
ription: This rule detects scans statistically significant increase in traffic to a particular port.

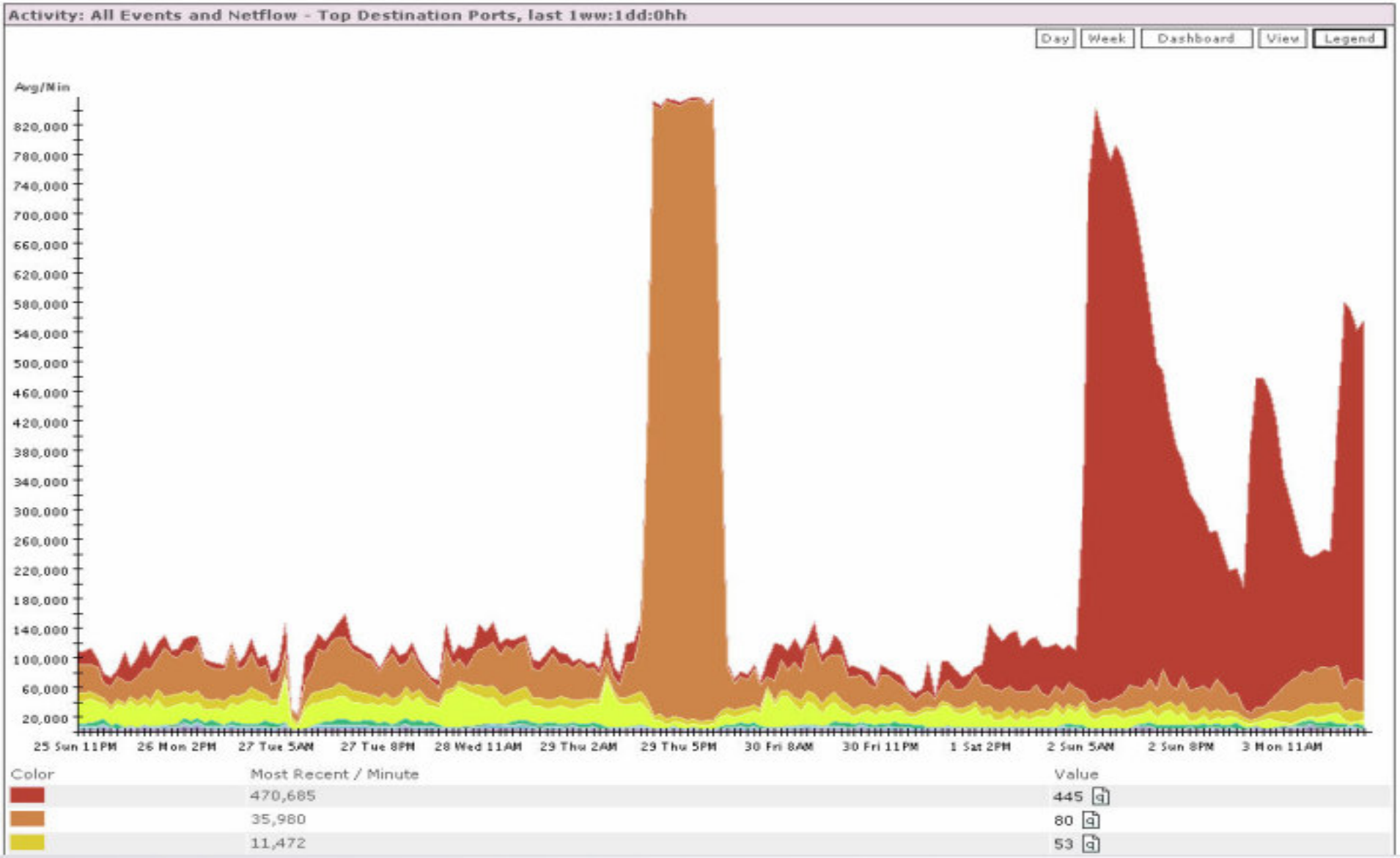
pen (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1	NJIT			0hh:10mm:0ss

473601390

Escalate | Expand All | Collapse All

/ ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigati
0316, 1390	Sudden increase of traffic to a port	0.0.0.0	0	0.0.0.0	445	IP	May 3, 2004 6:00:03 AM EDT		deimos		Tune	Mitigate
	AAA authorization denied due to no prior authentication	Total: 25										
	AAA authorization denied due to no prior authentication	[redacted].130.120		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].131.142		Total: 2								
6544, 1390	AAA authorization denied due to no prior authentication	[redacted]5.136.85	4049	[redacted]55.128	445	N/A	May 3, 2004 5:40:05 AM EDT		cerberus2		Tune	Mitigate
	AAA authorization denied due to no prior authentication	[redacted]35.136.104		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].136.205		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted]5.138.132		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted].138.174		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].139.89		Total: 6								
	AAA authorization denied due to no prior authentication	[redacted].140.95		Total: 3								
6538, 1390	Built/teardown/permitted IP connection	[redacted].93.70	2503	[redacted].72.164	445	TCP	May 3, 2004 5:40:05 AM EDT - May 3, 2004 5:42:07 AM EDT		cerberus1		Tune	Mitigate
	Denied packet - no translation group	Total: 4										
6547, 1390	Denied packet - no translation group	[redacted].136.85	4050	[redacted].30.35	445	TCP	May 3, 2004 5:40:05 AM EDT		cerberus2		Tune	Mitigate

Graph Says It All



Example of Compromised Hosts

Rank		Count (# of Sessions)	Raw Source IP	Defined Hosts
	1	102572	[redacted].130.160	
	2	40339	[redacted].132.44	
	3	36881	[redacted].203.82	dhcp-203-82
	4	36595	[redacted].202.66	dhcp-202-66
	5	35827	[redacted].134.196	
	6	35622	[redacted].134.75	
	7	35428	[redacted].133.80	
	8	35307	[redacted].134.199	
	9	35167	[redacted].138.196	
	10	34070	[redacted].136.118	
	11	33376	[redacted].136.205	
	12	32931	[redacted].203.42	dhcp-203-42
	13	30390	[redacted].133.16	
	14	27682	[redacted].30.120	
	15	22031	[redacted].138.166	
	16	19681	[redacted].140.154	
	17	19135	[redacted].130.82	
	18	18229	[redacted].140.5	

Q&A