# Safe & Secure Environments for School

**Ricky Elias**

**Security Architect**

**Advanced Technologies (Security)**

**relias@cisco.com**

# Agenda

- Current Challenges
- Cisco Solutions
- Case Studies
- Q and A

# Online Security: A Story in Two Parts

- Outside coming in
  - Probing
  - Viruses
  - Attacks on student resources
  - …
- Inside going out
  - What students and visitors bring to schools
  - DDoS launching pads and

# From Fame to Monetary Gain

Jeanson James Ancheta

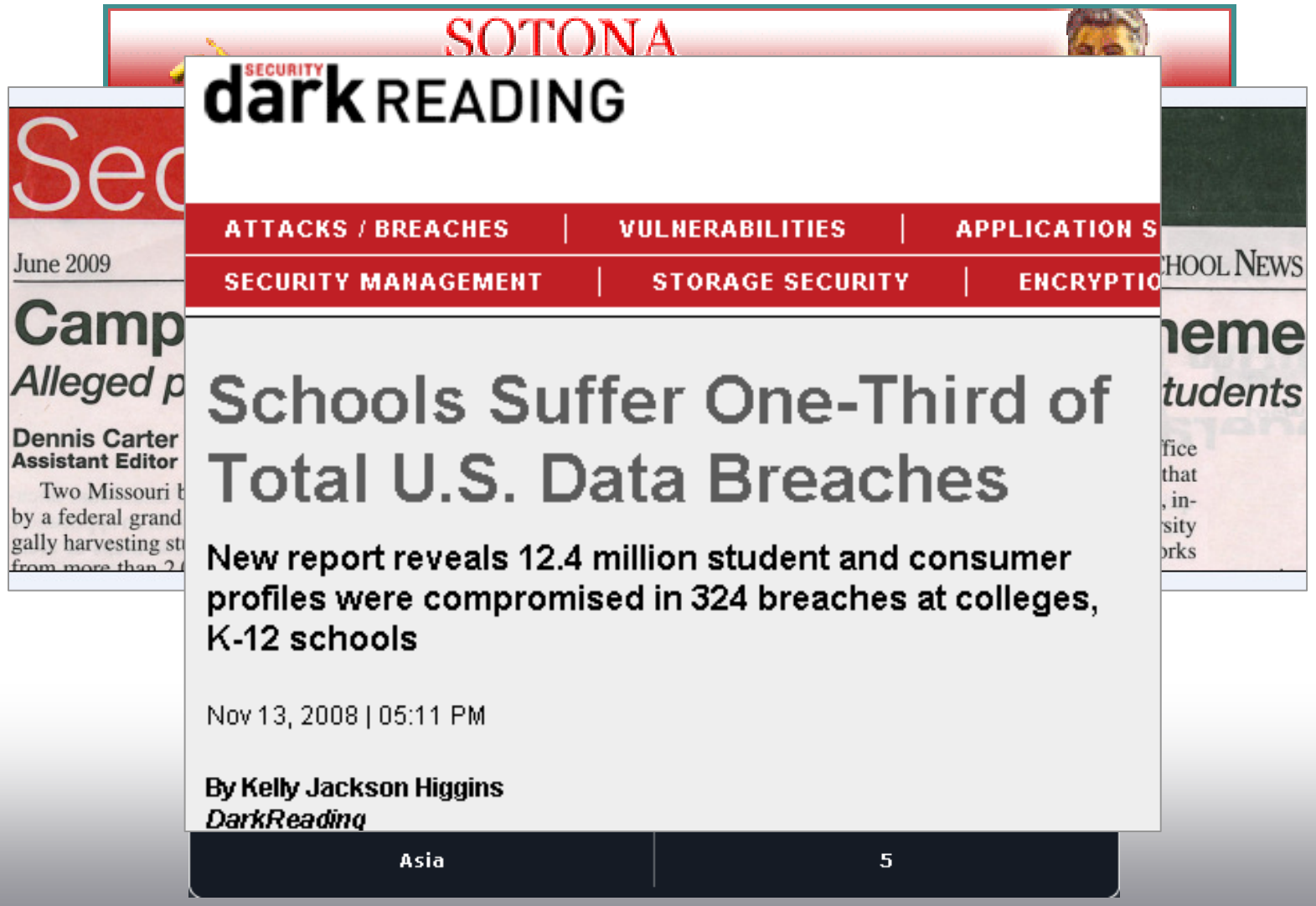
Downey, Calif., Police

But instead of setting up a websi
permission to install ads — a co
used his bots to install adware o
connected PCs, court records sh
each piece of adware installed ra
cents.

Working at home, Ancheta nurtur
during a workday that usually beg
stretched non-stop until 5 a.m., a
of the case says. He hired an ass

- **Hijacked more than 400,000 PCs, used them to build a botnet, then rented out the system to spyware distributors, hackers, and spammers**
- **Made $3,000 from renting the botnet to others, who used it to launch denial-of-service (DoS) attacks and spew spam**
- **Pocketed an additional $107,000 by seeding the botnet's PCs with adware and raking in affiliate fees**
- **Pleaded guilty to federal charges, sentenced to 57 months**

# “Installs” for Sale — Monetizing Botnets



# Cisco Education Solution Portfolios

## Safe & Secure Environments for Education

- Provide enforcement and accountability
- Secure the web and school network
- Protect critical resources and data

# Layered Security

| Security Needs | Goals | Technologies |
| --- | --- | --- |
|  Student records and personal data | Protect critical resources and data | ▪ Firewall<br>▪ Web security<br>▪ Network admission control |
|  Safe online learning environment | Secure the web and school network | |
|  Policy and control | Provide enforcement and accountability | |

# Provide Enforcement & Accountability

## Cisco Network Admission Control (NAC) for Education

# Keeping Schools Safe and Secure

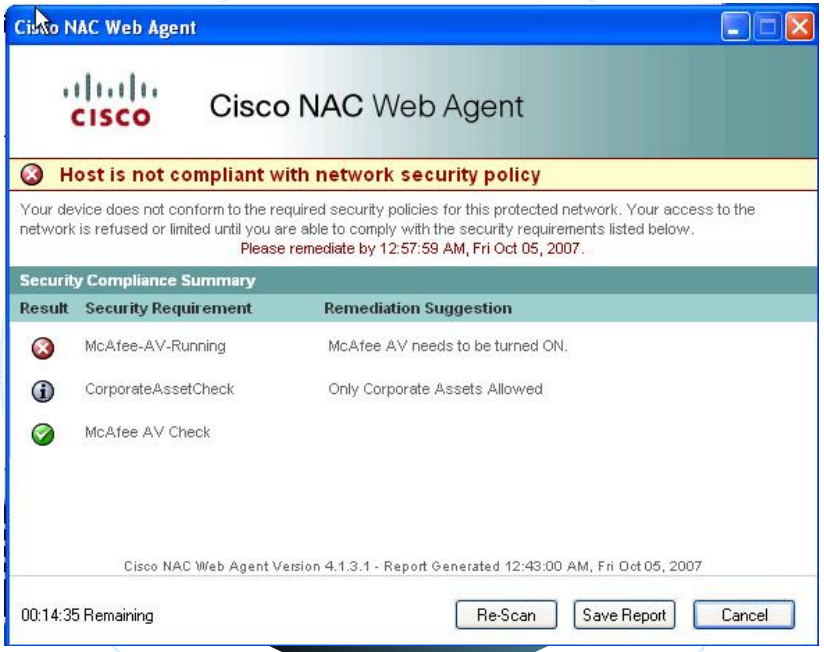
- Secure access to school network
- Protect against viruses and other network infections
- Prevent unauthorized access to personal data and academic records
- Assist in compliance with regulatory requirements

# Secure School Network

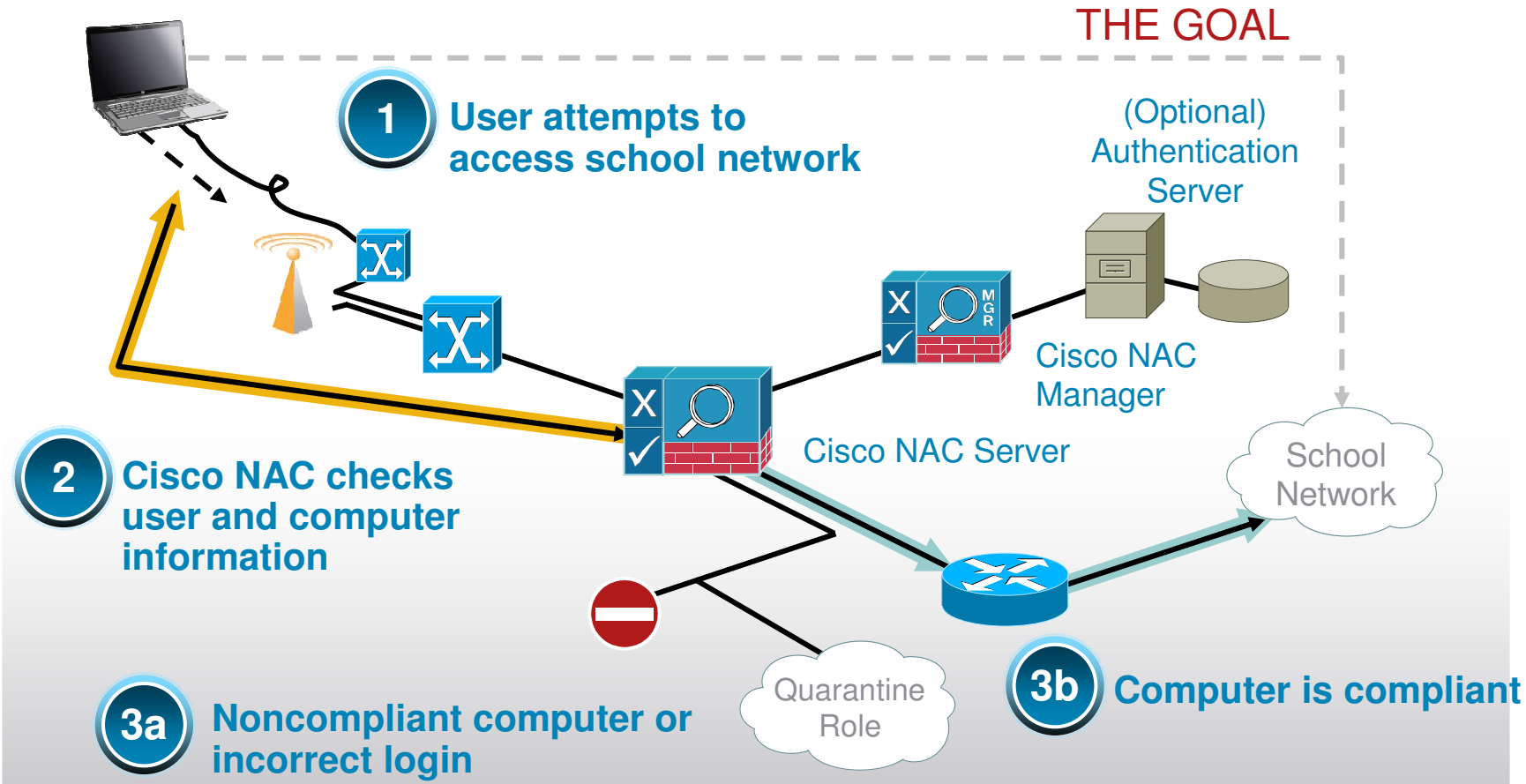
List of Roles | New Role | Traffic Control | Bandwidth

| Role Name | IPSec | Roam | VLAN | Description |
|---|---|---|---|---|
| Unauthenticated Role | deny | deny | | Role for unauthenticated users |
| Temporary Role | deny | deny | | Role for users to download requirements |
| Quarantine Role | deny | deny | | Role for quarantined users |
| Allow All | deny | deny | | Full Access |
| Guest Access | deny | deny | :666 | guest privileges |
| consultant access | deny | deny | :55 | consultant privileges |

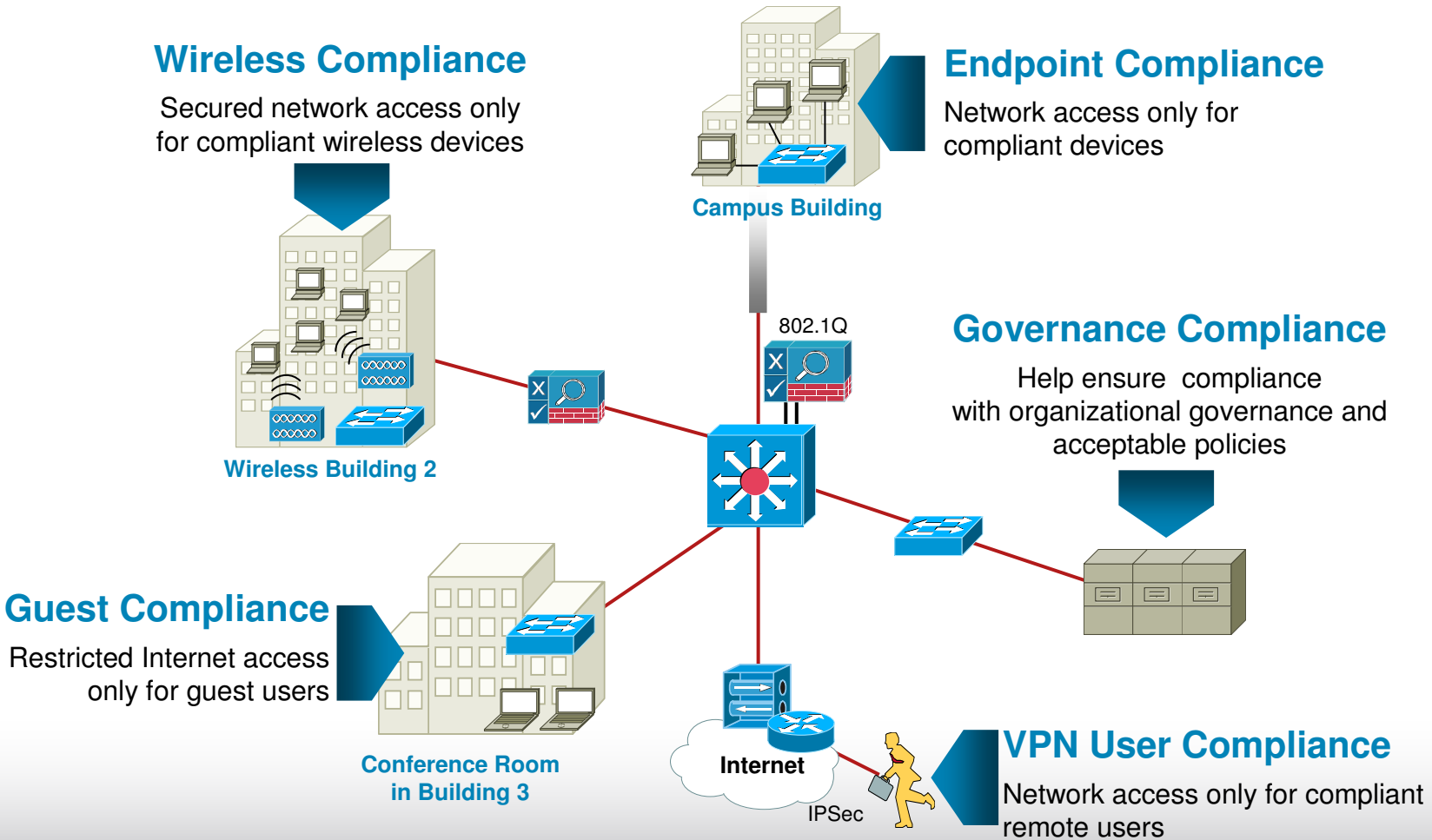
# Prevent Network Infections

# How Network Admission Control Works



# Meeting Student and Faculty Needs



# Network Admission Control Benefit

| Cisco NAC Benefits | Schools Gain |
| --- | --- |
| Threat containment | ▪ Fewer infections<br>▪ Reduced interruptions to education<br>▪ More resilient school network |
| Access control | ▪ Decline in incidents<br>▪ Less loss of personal data and school records |
| Compliance | ▪ Improved security<br>▪ More reliable audit and enforcement |

# Case Study: Virginia Commonwealth University

## Protect Students, Faculty and Staff

| | |
|---|---|
| **Situation / Challenge** | ▪ Balance need for academic openness with need to protect information and assets<br>▪ Government laws/regulations and industry requirements to be met |
| **Solution/** | ▪ Provide secure online access while thwarting threats<br>▪ Implement a campus network access and enforcement policy to minimize incident and virus outbreaks<br>▪ Retain logs, audit/tracking information, and reports to meet compliance requirements, and demonstrate compliance with P2P/RIAA regulations<br>▪ Video monitor school events, and validate students with their own RFID cards as they enter the site |
| **Technology** | ▪ Cisco Security Solutions, Cisco Network Admission Control (NAC) Profiler, Cisco NAC Guest Server, Cisco Physical Access Control, Cisco Video Surveillance Manager |

*"Since the Cisco NAC solution has been in place, we have seen an approximately 90 percent drop in infections on the student resident network."*

— Jesse Crim, Information Security Analyst, Virginia Commonwealth University

# Secure the Web and School Network

## Cisco IronPort Web Security Appliance (WSA) for Education

# Protecting Students from Harmful Content

- Secure and control access to the Internet
- Protect against malware, spyware, and zero-day threats
- Enforce acceptable-use policies for Internet use, including role-based administration and access

# Cisco IronPort WSA Protects School Users



Layer 4 Traffic Monitor

Web Reputation Filters

Dynamic Vectoring and Streaming Engine

- Detects malicious botnet traffic across all ports
- Blocks 70% of known and unknown malware traffic at connection time
- Blocks malware based on deep content analysis

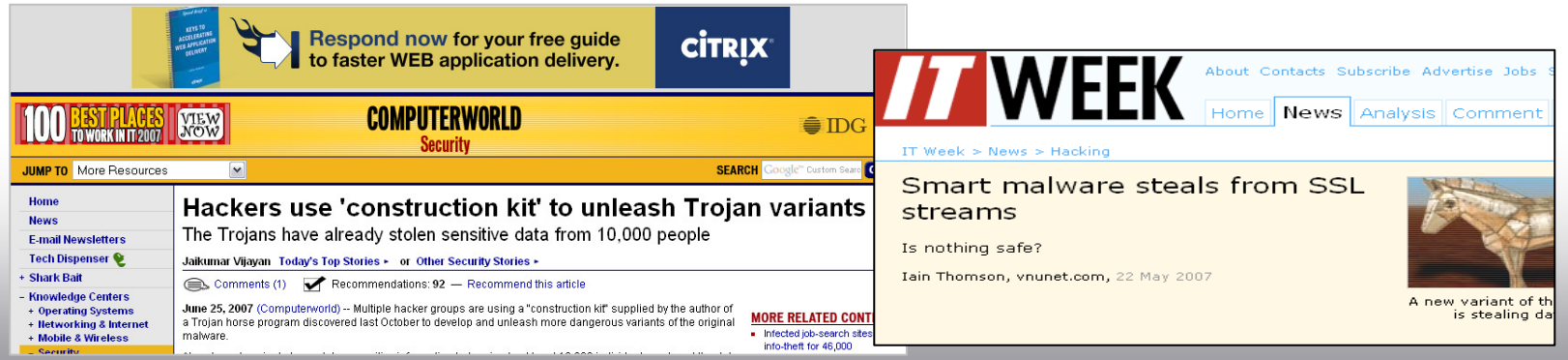
# Detect Existing Client Infections

*Threat Spotlight – Gozi Trojan Exploit*

- Trojan program designed to steal data from encrypted Secure Sockets Layer (SSL) stream.
- Undetected for more than 50 days has stolen more than **10,000 records** containing confidential information.

  2,000 SSN, account numbers, usernames/ passwords tied bank accounts and retail/ e-commerce sites.

  The black market street value of the stolen data: $2 million.
- Took advantage of a vulnerability in the iFrame tags of Microsoft Corp.'s Internet Explorer



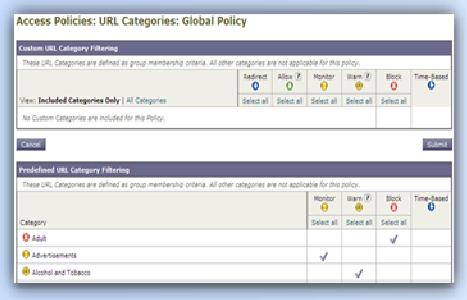
# Acceptable Internet Use Policy
## Example

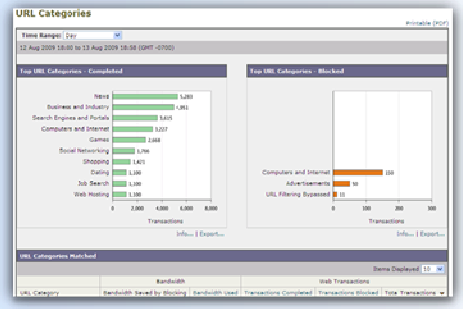
Prohibited uses and activities include, without limitation, any use of the Services in a manner that involves, facilitates, or attempts any of the following:

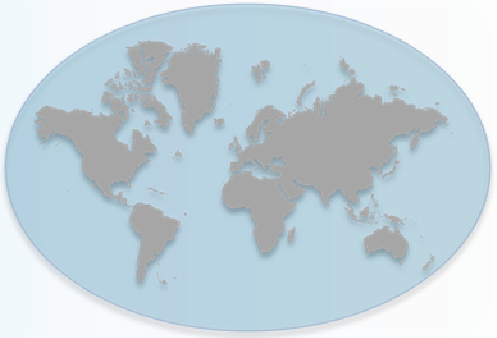
- gambling activities;
- displaying, performing, sending, receiving or storing any content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful;
- advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful;
- accessing, sending, receiving, displaying, performing, disclosing, storing, or executing any content a) in violation of any copyright, right of publicity, patent, trademark, service mark, trade name, trade secret or other intellectual property right, b) in violation of any applicable agreement, or c) without authorization

# Cisco IronPort Web Usage Controls

## Leading Efficacy, Rich Controls, Comprehensive Visibility



### Control

- Per user, per group policies
- Multiple actions: block, warn, monitor
- Time-based policies
- Unlimited custom categories
- Custom end-user notifications

### Visibility

- Easy to understand reports
- Extensive logging
- Comprehensive alerting

### Efficacy

- 200+ countries
- 50+ languages
- 65 categories
- Less than 1 in 1 million false positives

# Case Study: Enumclaw School District

- **Enumclaw School District's challenge:**
  - 5 elementary schools, 2 middle schools, 1 high schools
  - Ensure students, teachers and administrators make the most of its computing technology – while receiving only appropriate Internet content
  - Previous filtering solution provided inadequate integration with user directories,
- **IronPort's solution:**

  Since deploying the Cisco IronPort S160, the district reports a daily average of:
  - 200 suspicious URLs blocked by Cisco IronPort Web Reputation Filters
  - 45,500 URLs stopped by Cisco IronPort URL Filters
  - At least 10 malware or spyware downloads blocked

Enumclaw SCHOOL DISTRICT
*all students achieving at high levels*

*If there's an identified threat, it's blocked at the gateway – rather than on the desktop after the threat is already inside the network.*

*The ability to dynamically block webpages is very powerful. This is something we were not able to do previously. The Cisco IronPort S160 is like a firewall for web traffic.*

Chad Marlow
Technology Coordinator
Enumclaw School District

| USERS PROTECTED | 4000+ |
|---|---|

# Protect Critical Resources and Data

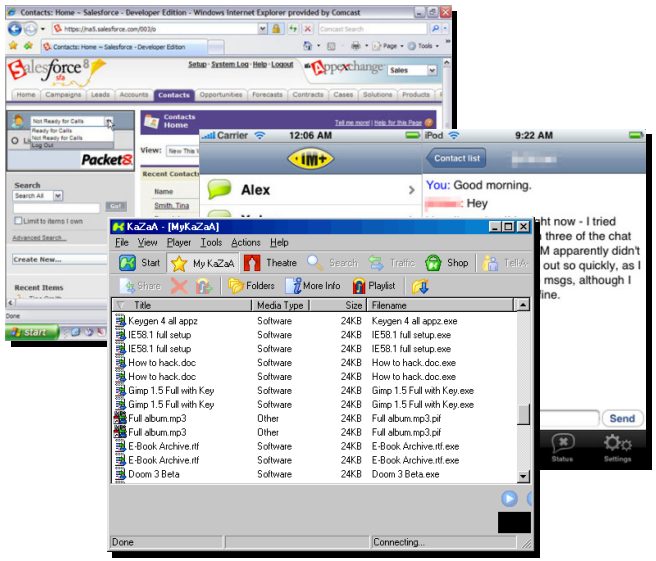
## Cisco Adaptive Security Appliance (ASA) for Education

# Supporting 21st-Century Education

- Provides strong protection for the network by quickly detecting and responding to threats and risks
- Keeps sensitive and confidential information safe and prevents financial loss due to data breach or leakage
- Guards valuable assets and intellectual properties
- Prevents unauthorized access to certain website classifications
- Assists in compliance with regulatory requirements

# Application and User-Centric Security

## Access Control for Modern Networks




### Application Access Control

- Integrated HTTP & Port 80
- IM & P2P
- Content type & Active-X

### Authentication Policies

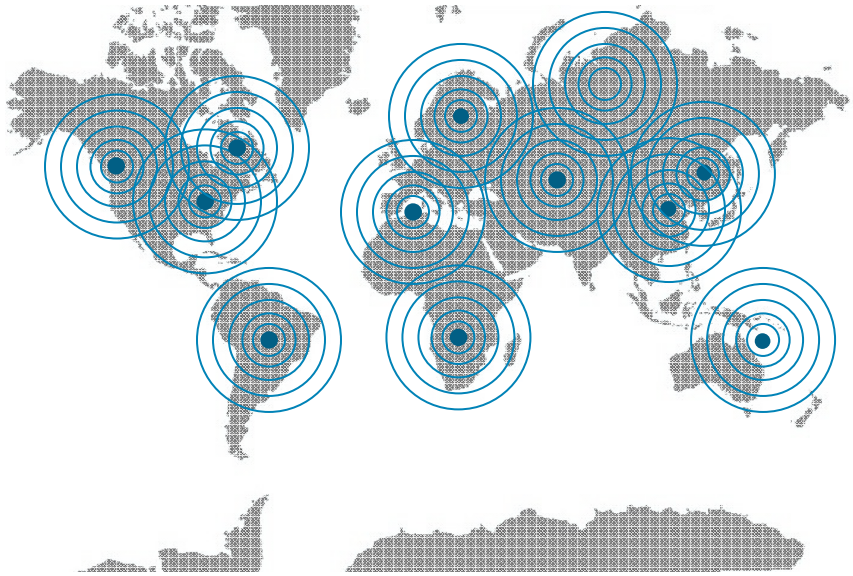
- Selective access to assets
- Track and audit user activity
- Extensive protocol support

# Global Correlation in Action

## Network IPS to Global IPS

### 08:00 GMT

- A sensor in Australia detects new malware
- A sensor in Russia detects a botnet issuing new commands
- A sensor in Korea detects a virus mutating
- A sensor in Florida detects a hacker probing major financial institutions



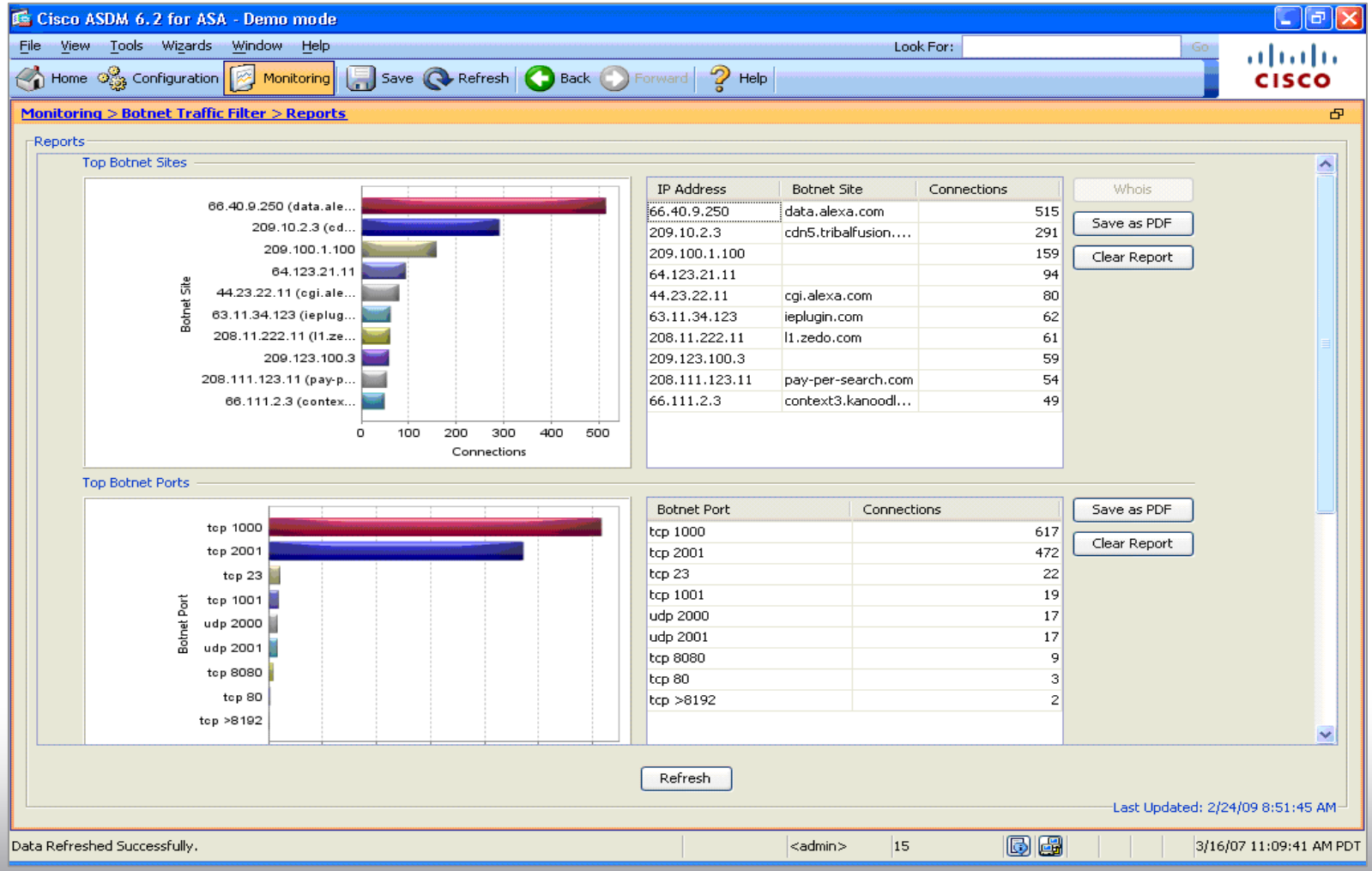
### 08:15 GMT

- All Cisco IPS customers protected

Responsive and Accurate Protection

# Detecting Client Infections

## Botnet Traffic Filters



# Cisco Solutions for Information Security Protect Data and Prevent Attacks

## Features

- Identity-based network security
- Cisco Campus Secure protects wired and wireless networks and endpoints
- Cisco Network Security is embedded in all solutions
- Cisco ASA 5500 Series Adaptive Security Appliances

## Benefits

- Prevent cyber attacks
- Keep records safe
- Protect students from harmful online sites or predators
- Monitor bandwidth

*Indiana State University enables automated bandwidth control*

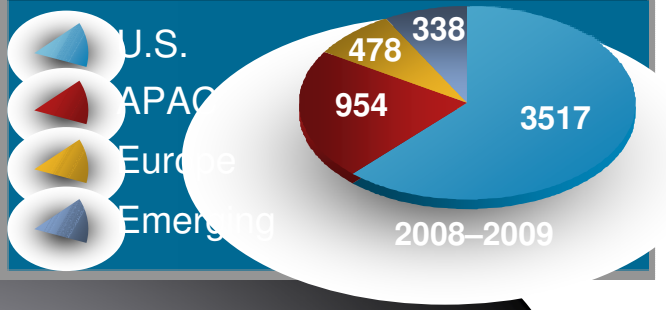
# Cisco's Commitment to Higher Education

Internet and Education: The two great equalizers

## IBSG Higher Education

- Thought Leadership
- Strategy
- Innovation
- Models

## University Recruitment/Interns




## Cisco Research Center

- Funded Research
- Collaboration Projects
- Technology Transfer

## Cisco Networking Academy

- 9000+ Academies
- 760,000+ Students Per Year
- 160+ Countries


CISCO