Saudi Expo 2007

Self Defending Networks in Action

Haider Pasha, CISSP

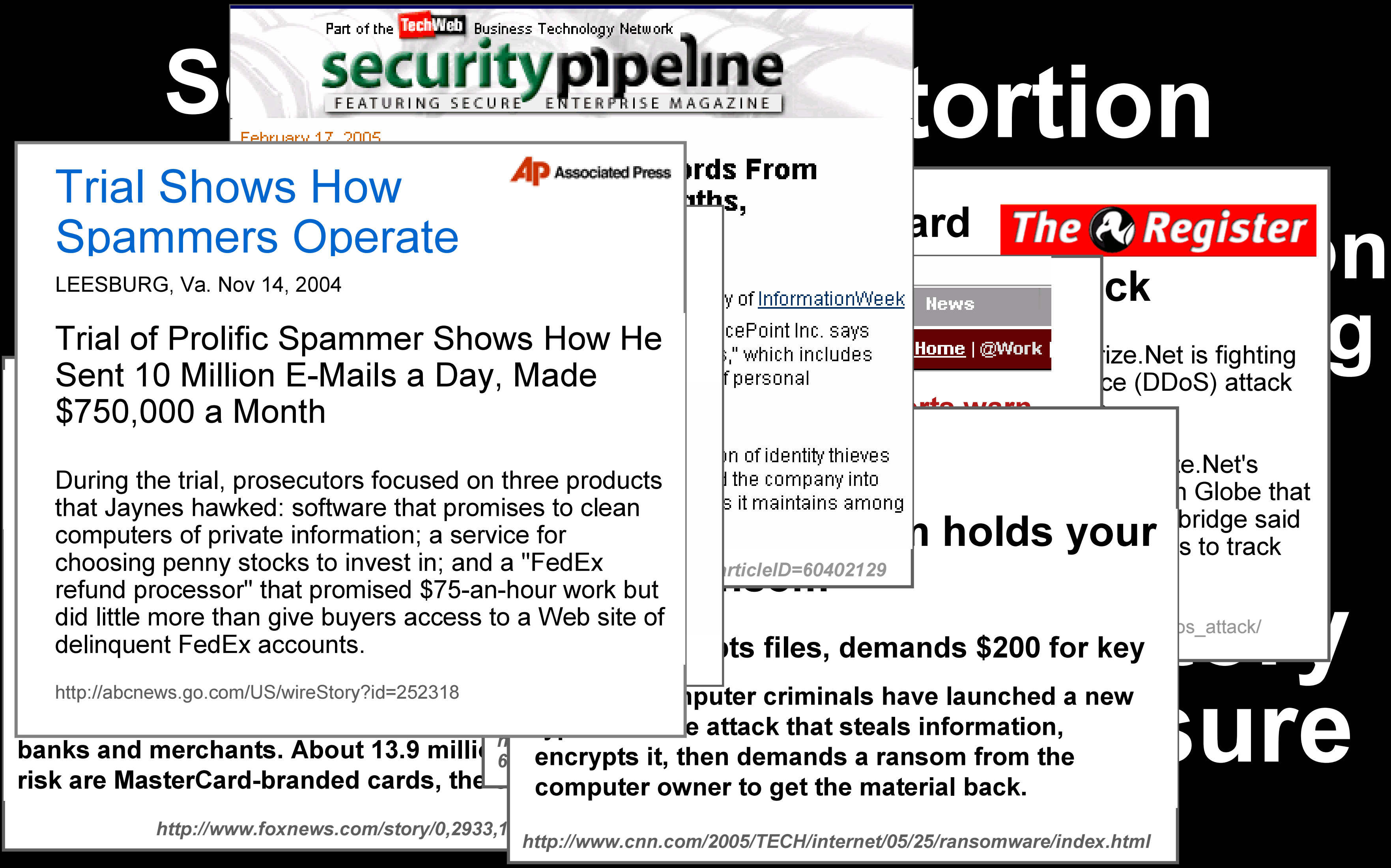
Consulting Systems Engineer, MEA

hpasha@cisco.com

Agenda

- The Need for a Self Defending Network
- What is SDN? What is it made of?
- Examples and Scenarios on Integration, Collaboration and Adaptiveness

An Evolution of Security Threats
Beyond Worms and Viruses



Part of the TechWeb Business Technology Network
securitypipeline
FEATURING SECURE ENTERPRISE MAGAZINE
February 17, 2005

...rds From
...ths,

...y of InformationWeek
...cePoint Inc. says
...," which includes
...f personal

...n of identity thieves
... the company into
...s it maintains among

...rticleID=60402129

Associated Press

Trial Shows How Spammers Operate

LEESBURG, Va. Nov 14, 2004

Trial of Prolific Spammer Shows How He Sent 10 Million E-Mails a Day, Made $750,000 a Month

During the trial, prosecutors focused on three products that Jaynes hawked: software that promises to clean computers of private information; a service for choosing penny stocks to invest in; and a "FedEx refund processor" that promised $75-an-hour work but did little more than give buyers access to a Web site of delinquent FedEx accounts.

http://abcnews.go.com/US/wireStory?id=252318

...ard

The Register

News
Home | @Work

...ck

...ize.Net is fighting
...ce (DDoS) attack

...e.Net's
...n Globe that
...bridge said
...s to track

...s_attack/

...n holds your

...ts files, demands $200 for key

...puter criminals have launched a new
...e attack that steals information,
encrypts it, then demands a ransom from the
computer owner to get the material back.

http://www.cnn.com/2005/TECH/internet/05/25/ransomware/index.html

banks and merchants. About 13.9 milli...
risk are MasterCard-branded cards, the...

http://www.foxnews.com/story/0,2933,1...

Facts on the Ground:
Real Threats Affecting Real Networks

James Ancheta, small time hacker from California

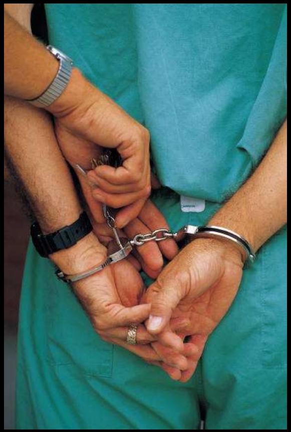
Ancheta used a variety of malware to take control of 400,000 computers globally

Ancheta used these machines to make over One Hundred Thousand dollars

- **Renting the machines to spammers**
- **Installing adware on the machines**

He got caught while infecting computers used in weapons research by the US Gov't

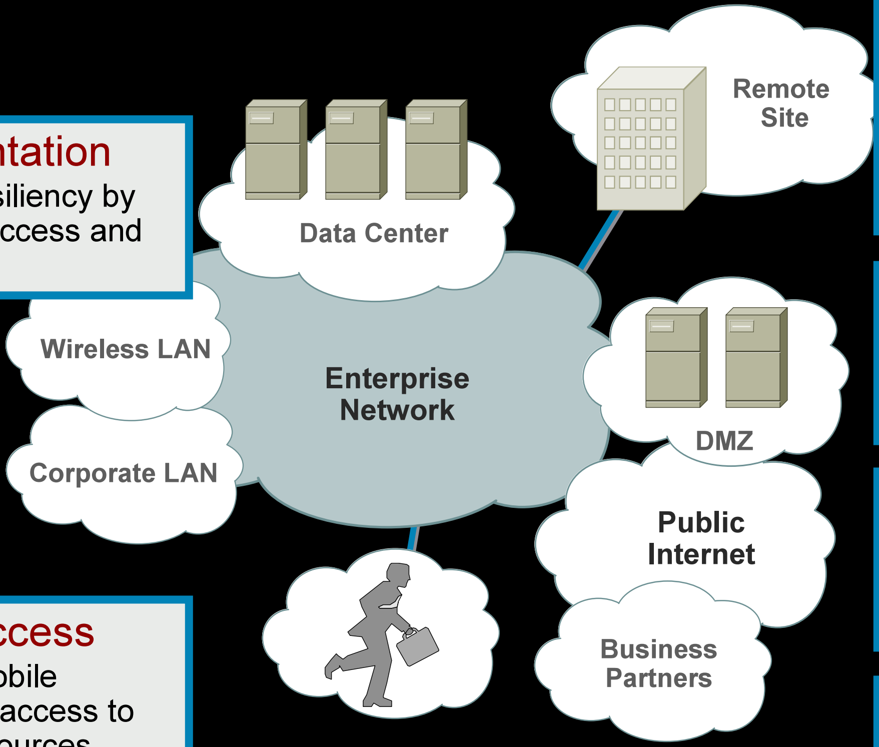
Sentenced to 5 years in jail in May 2006



The Need for a New Paradigm
Enterprise Security Business Needs Evolving

Internal Segmentation
Increase business resiliency by controlling resource access and containing outbreaks

Remote User Access
Road warriors and mobile workers need secure access to internal corporate resources



Remote Site with Internet Access
Sites with local Internet access require a comprehensive set security services in a small footprint

DMZ
Internet presence and eCommerce sites must be secured against hackers

User Internet Access
Internal users need protection when accessing the public Internet

Extranet
The networked business requires secure connections with partners

Multiple Environments, each with specific business drivers and organizational needs

Meeting Needs Requires Many Services

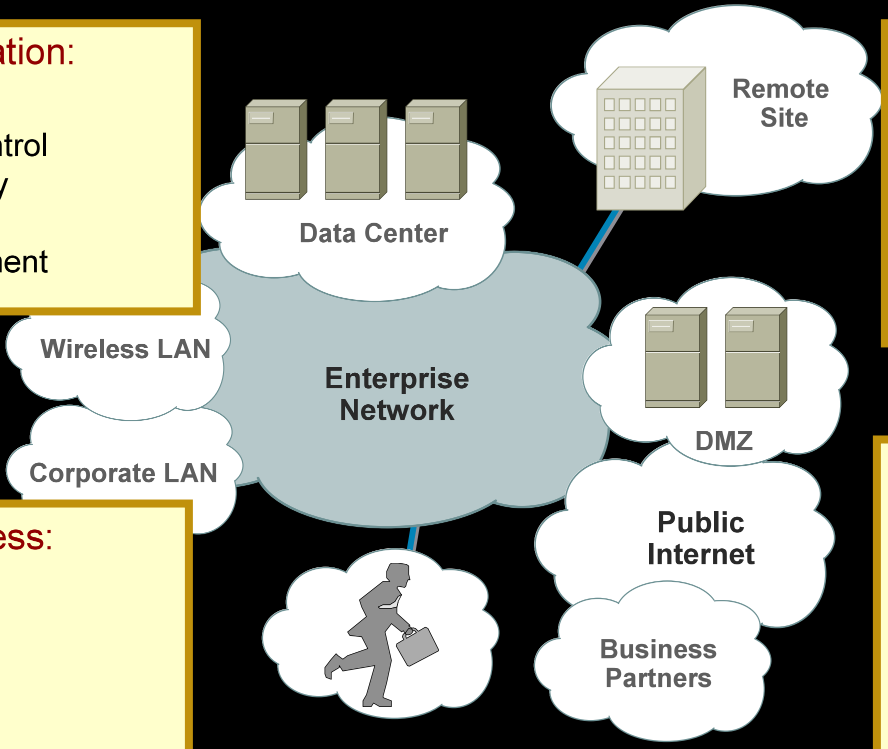
Complex Location-specific Requirements

Internal Segmentation: Requirements

- Robust access control
- Application security
- Worm protection
- Outbreak containment

Remote Site with Internet Access: Requirements

- Enterprise-grade firewall
- Anti-virus
- Anti-spyware
- Web security services
- Site to site VPN



Remote User Access: Requirements

- SSL VPN
- IPSec VPN
- Client Protections
- Threat Defense

DMZ – Internet Access – Extranet: Requirements

- Trusted firewall
- Application controls
- Sophisticated logging
- Intrusion Detection
- Intrusion Prevention
- Analysis and Correlation

Operational Inefficiencies from Multiple Platforms and Consoles

May Require Compromise on Protection

Complex Design and Configuration

Agenda

- The Need for a Self Defending Network
- What is SDN? What is it made of?
- Examples and Scenarios on Integration, Collaboration and Adaptiveness

Comprehensive Security Strategy

Keeping Outsiders Out, Insiders Honest, Endpoints Safe

Threat Defense

Defend the Edge:

- **Integrated Network FW+IPS**

  Detects and Prevents External Attacks

Protect the Interior:

- **Catalyst Integrated Security**

  Protects Against Internal Attacks

Guard the Endpoints:

- **Cisco Security Agent (CSA)**

  Protects Hosts Against Infection

Trust and Identity

Verify the User and Device:

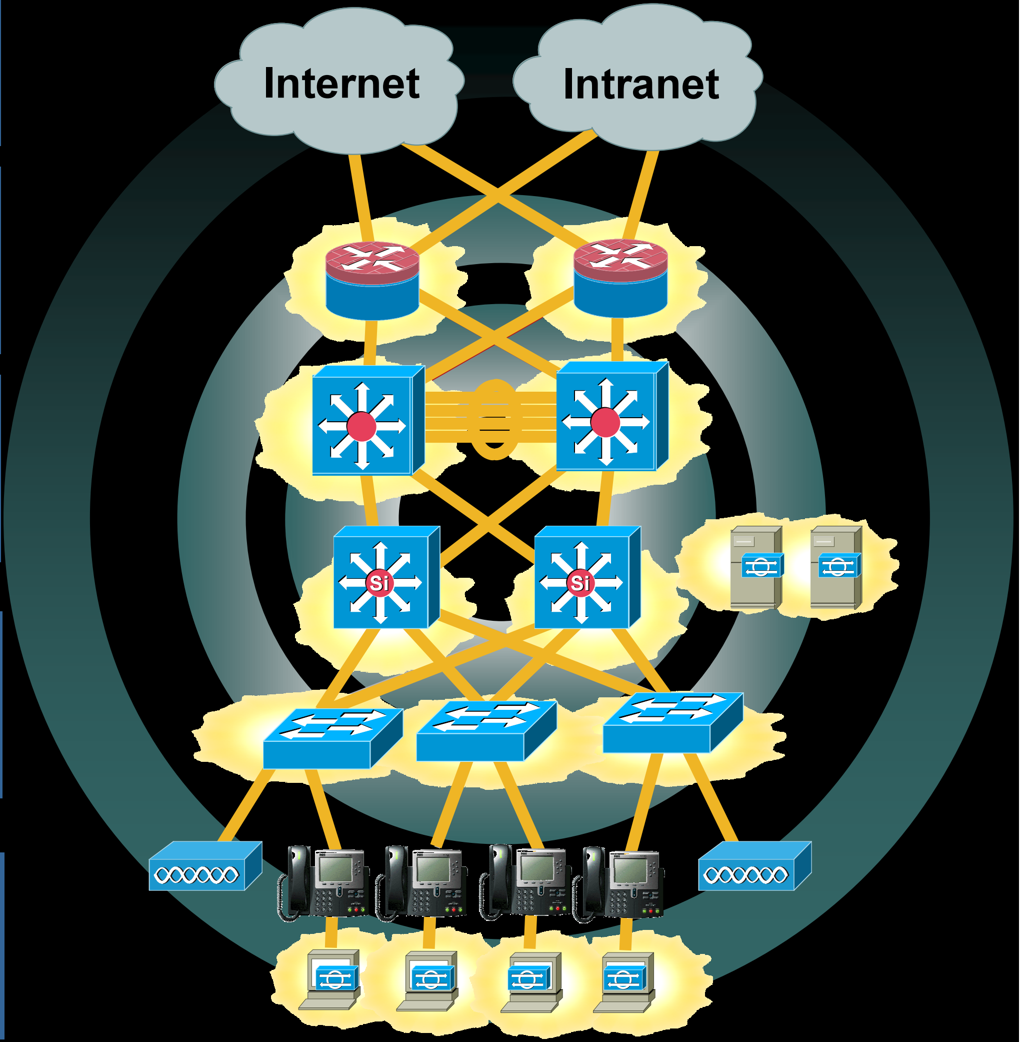
- **Identity-Based Networking/NAC**

  Control Who/What Has Access

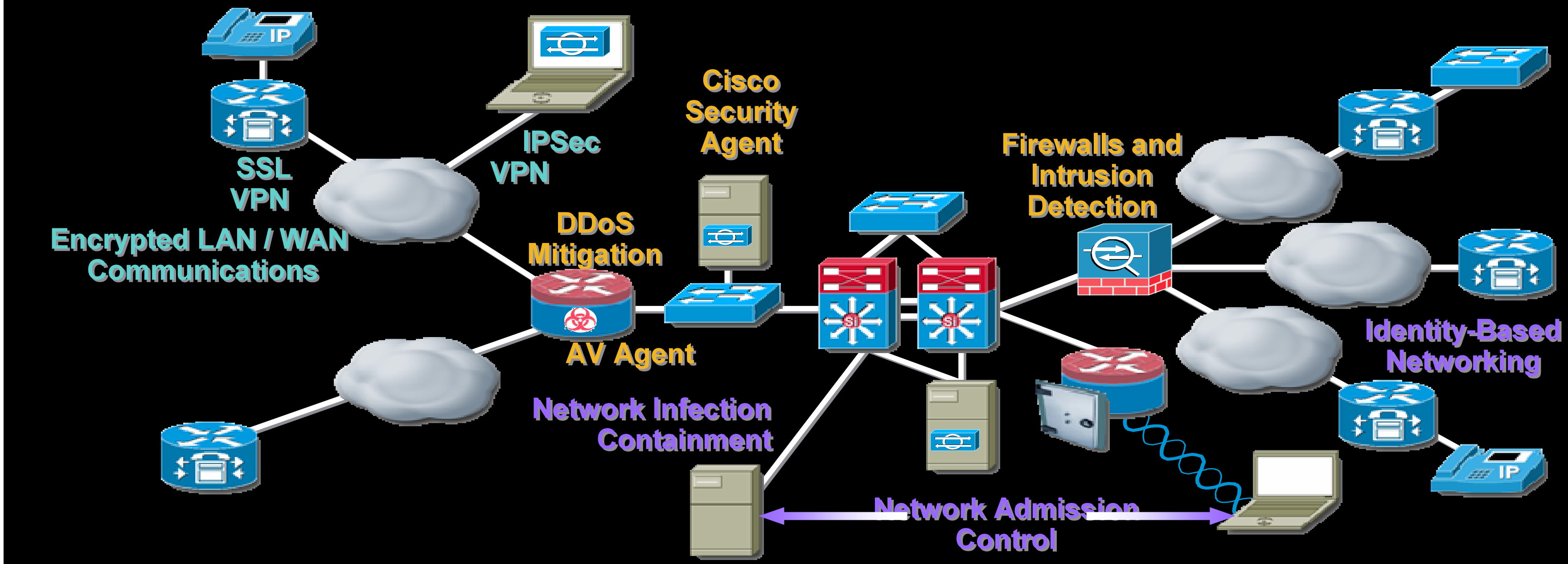
Secure Comm.

Secure the Transport:

- IPSec VPN
- SSL VPN
- MPLS



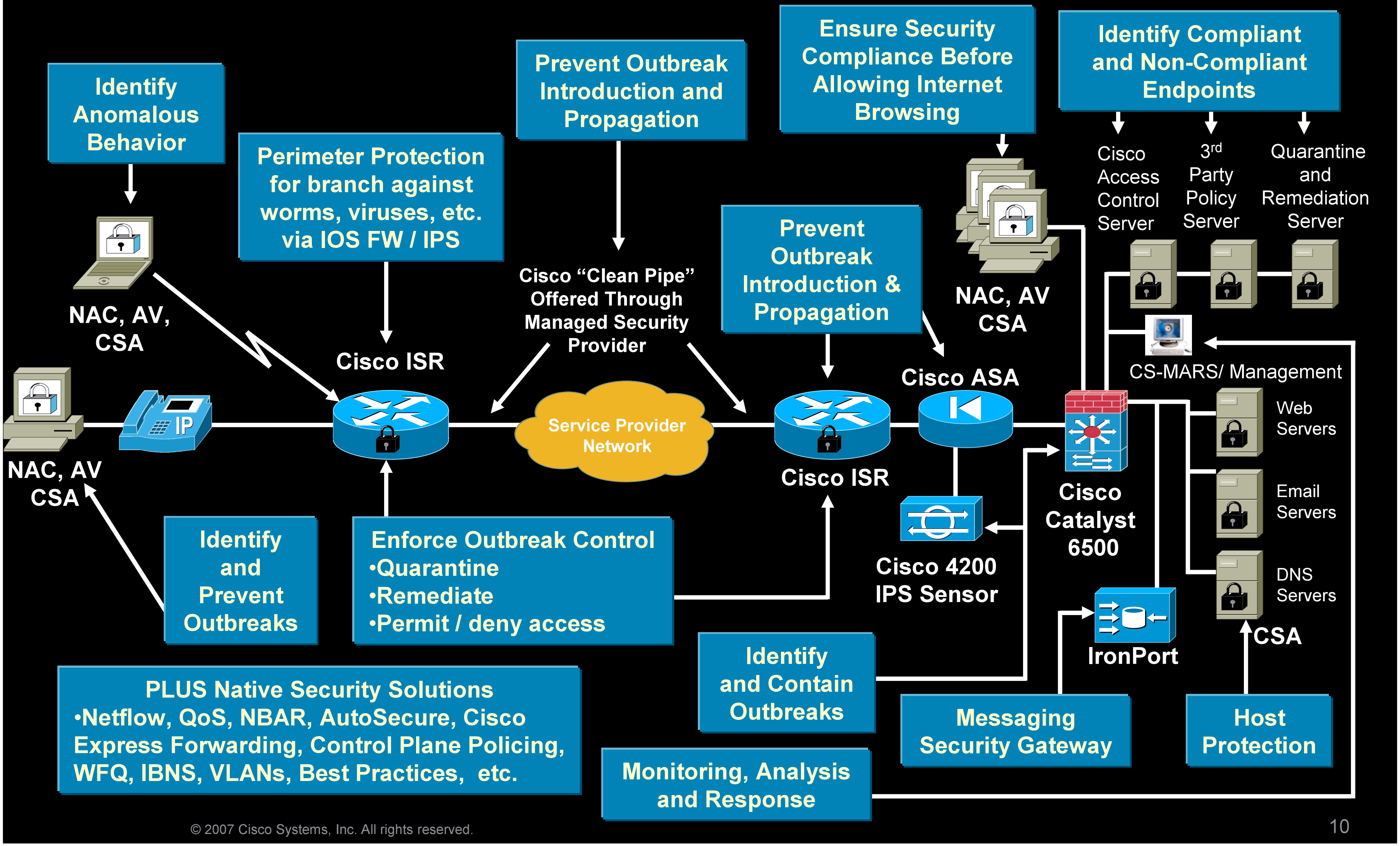
Properties of a Self-Defending Network



IP
SSL VPN
Encrypted LAN / WAN Communications
IPSec VPN
Cisco Security Agent
DDoS Mitigation
AV Agent
Network Infection Containment
Firewalls and Intrusion Detection
Identity-Based Networking
Network Admission Control
SI
IP

- *Network Availability*: remain active when under attack
- *Ubiquitous Access*: provide secure access from any location
- *Admission Control*: authenticate all users, devices, and posture
- *Application Intelligence*: enable network-based application visibility
- *Day-Zero Protection*: ensure endpoints are immune to new threats
- *Infection Containment*: rapidly identify & contain virulent attacks

Self Defending Network (SDN) in Action



Identify Anomalous Behavior

Perimeter Protection for branch against worms, viruses, etc. via IOS FW / IPS

Prevent Outbreak Introduction and Propagation

Ensure Security Compliance Before Allowing Internet Browsing

Identify Compliant and Non-Compliant Endpoints

Prevent Outbreak Introduction & Propagation

Cisco "Clean Pipe" Offered Through Managed Security Provider

Identify and Prevent Outbreaks

Enforce Outbreak Control
- Quarantine
- Remediate
- Permit / deny access

PLUS Native Security Solutions
- Netflow, QoS, NBAR, AutoSecure, Cisco Express Forwarding, Control Plane Policing, WFQ, IBNS, VLANs, Best Practices, etc.

Identify and Contain Outbreaks

Messaging Security Gateway

Host Protection

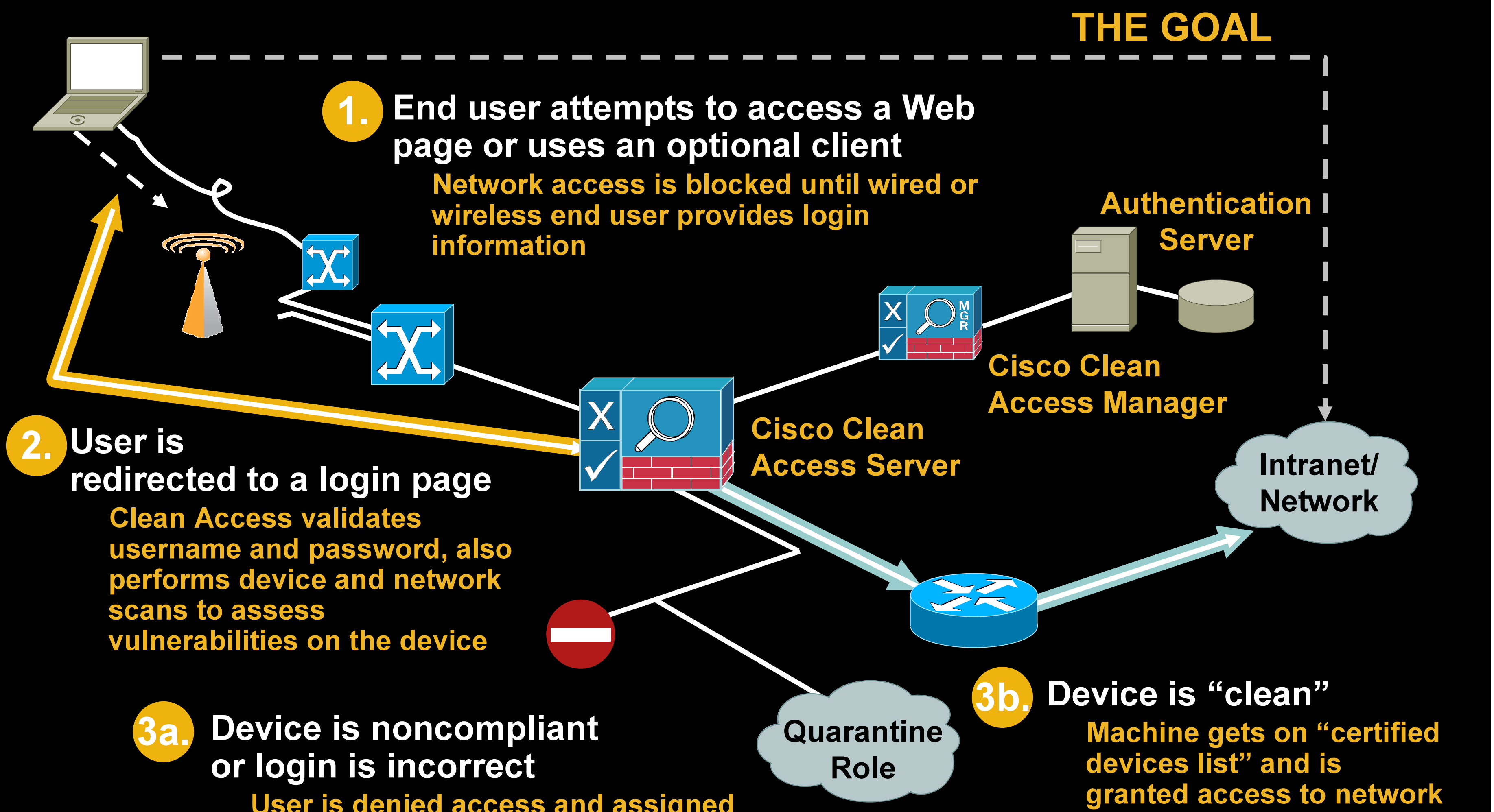
Monitoring, Analysis and Response

Agenda

- The Need for a Self Defending Network
- What is SDN? What is it made of?
- Examples and Scenarios on Integration, Collaboration and Adaptiveness

Self Defending Network (SDN) in Action:

Cisco NAC Appliance



1. End user attempts to access a Web page or uses an optional client

Network access is blocked until wired or wireless end user provides login information

2. User is redirected to a login page

Clean Access validates username and password, also performs device and network scans to assess vulnerabilities on the device

3a. Device is noncompliant or login is incorrect

User is denied access and assigned to a quarantine role with access to online remediation resources

3b. Device is "clean"

Machine gets on "certified devices list" and is granted access to network

SDN in Action

Mitigating Threats through IPS Rate Limiting

- **Rate limiting on routers and switches allows sensors to dynamically throttle traffic at strategic points across the network**

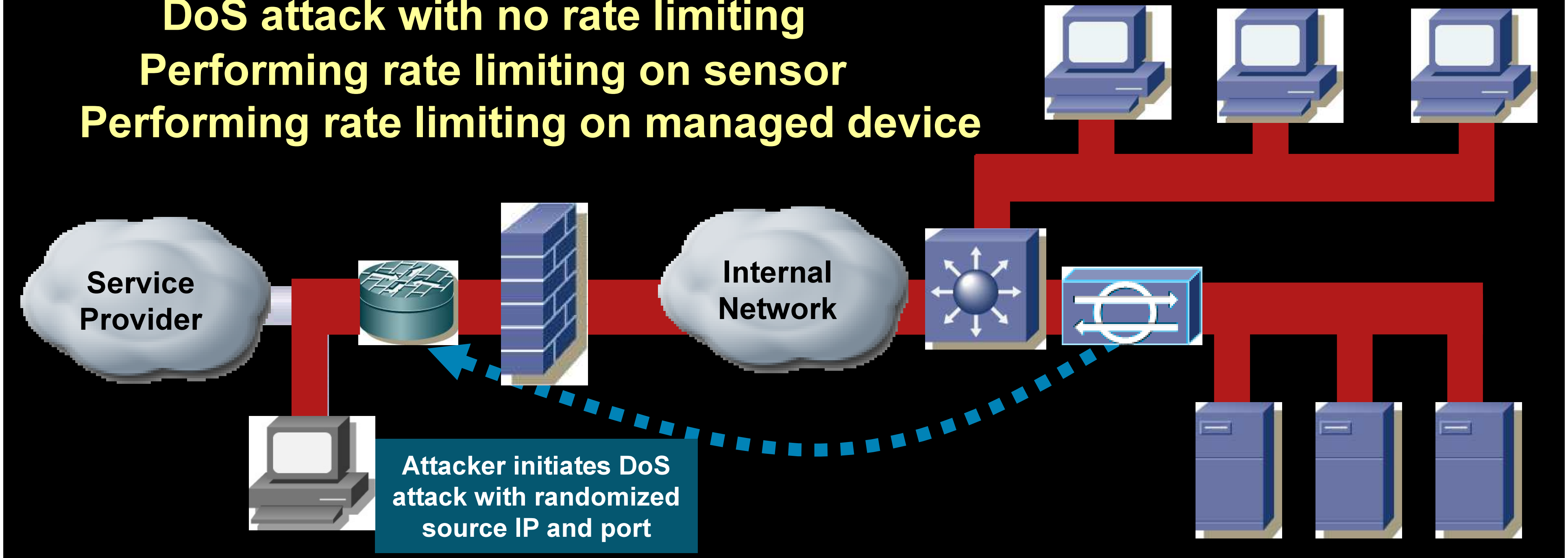
Flexible rate limiting parameters based on source IP, port information, and service type

Device management performed over a secure communications channel

DoS attack with no rate limiting

Performing rate limiting on sensor

Performing rate limiting on managed device

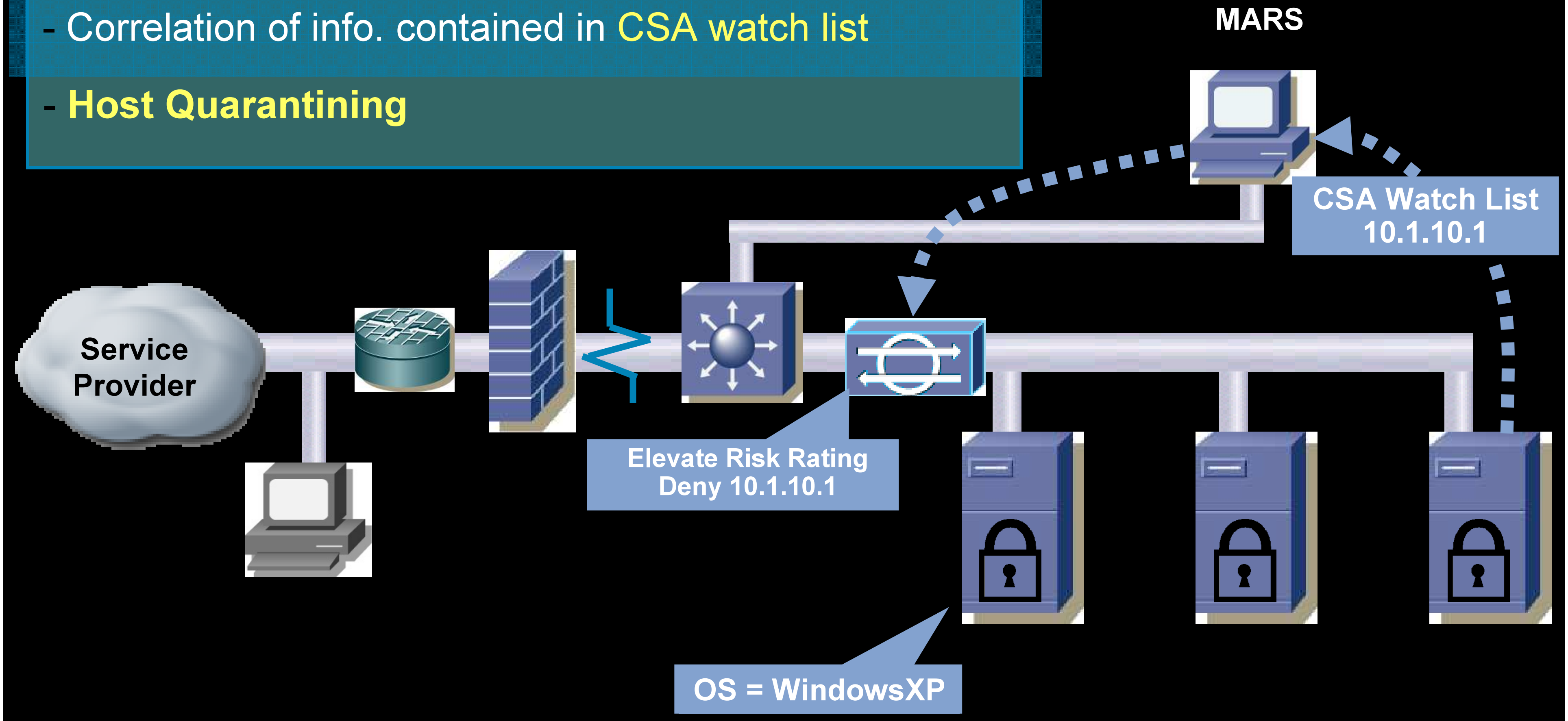


Attacker initiates DoS attack with randomized source IP and port

SDN in Action

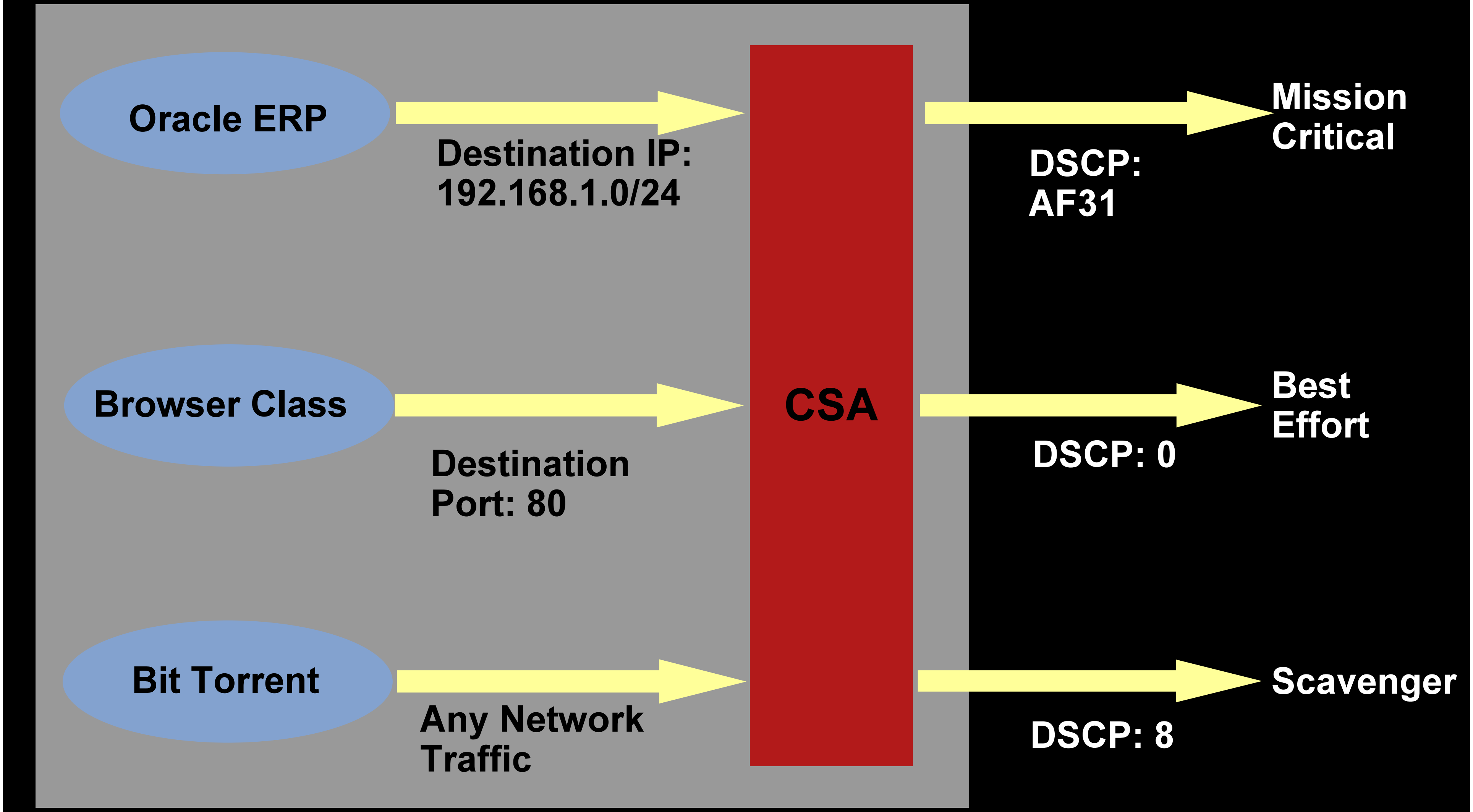
IPS-CSA Collaboration Example

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- **Host Quarantining**



SDN in Action

Cisco Security Agent and Infrastructure Integration



Oracle ERP

Destination IP:
192.168.1.0/24

Browser Class

Destination
Port: 80

Bit Torrent

Any Network
Traffic

CSA

DSCP:
AF31

Mission
Critical

DSCP: 0

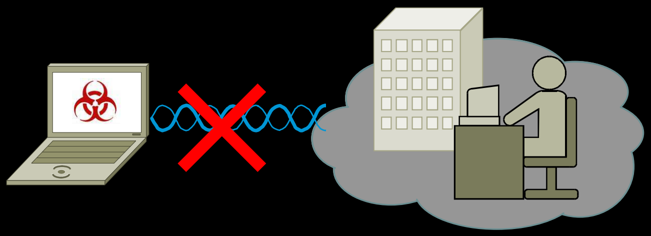
Best
Effort

DSCP: 8

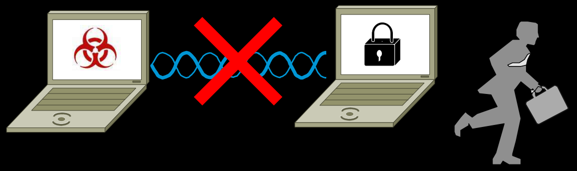
Scavenger

SDN in Action

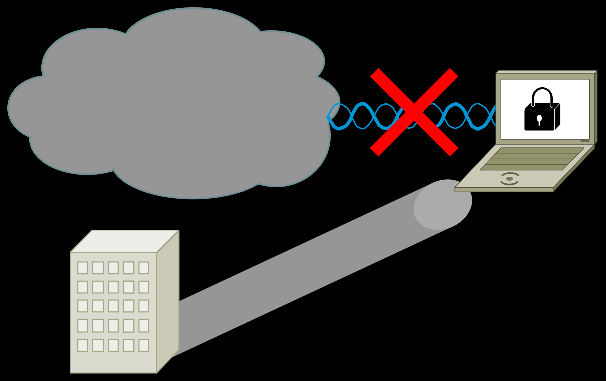
Cisco Security Agent and Infrastructure Integration



Disable wireless NIC when wired is active



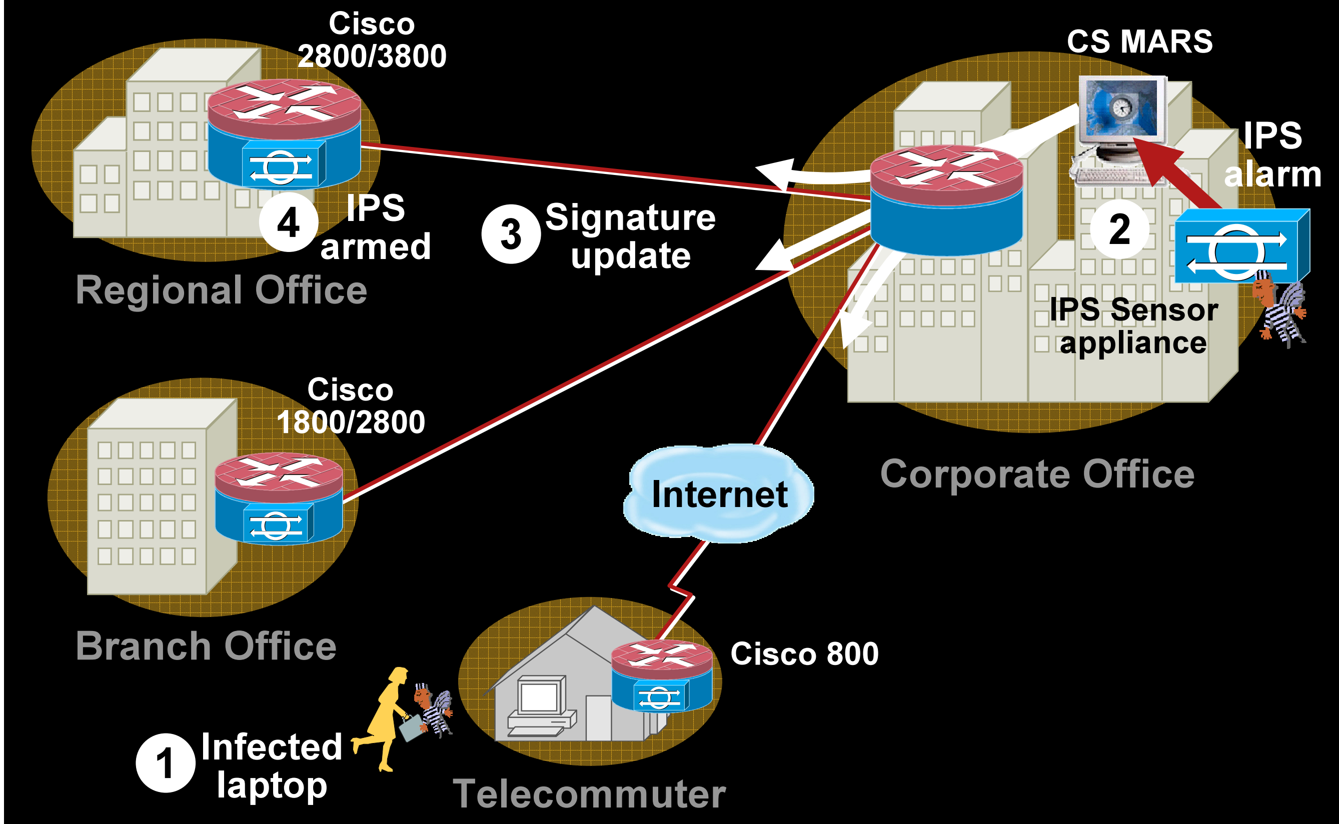
Connection restrictions -
certain SSIDs, encryption, ad-hoc



Require VPN connection when out of the office

SDN in Action:

Distributed Threat Mitigation with IPS



1. Infected telecommuter connects to the corporate network
2. Virus sets off IPS alarm on the sensor appliance at corporate office
3. CS MARS distributes signatures to all security routers
4. Armed routers protect all remote sites

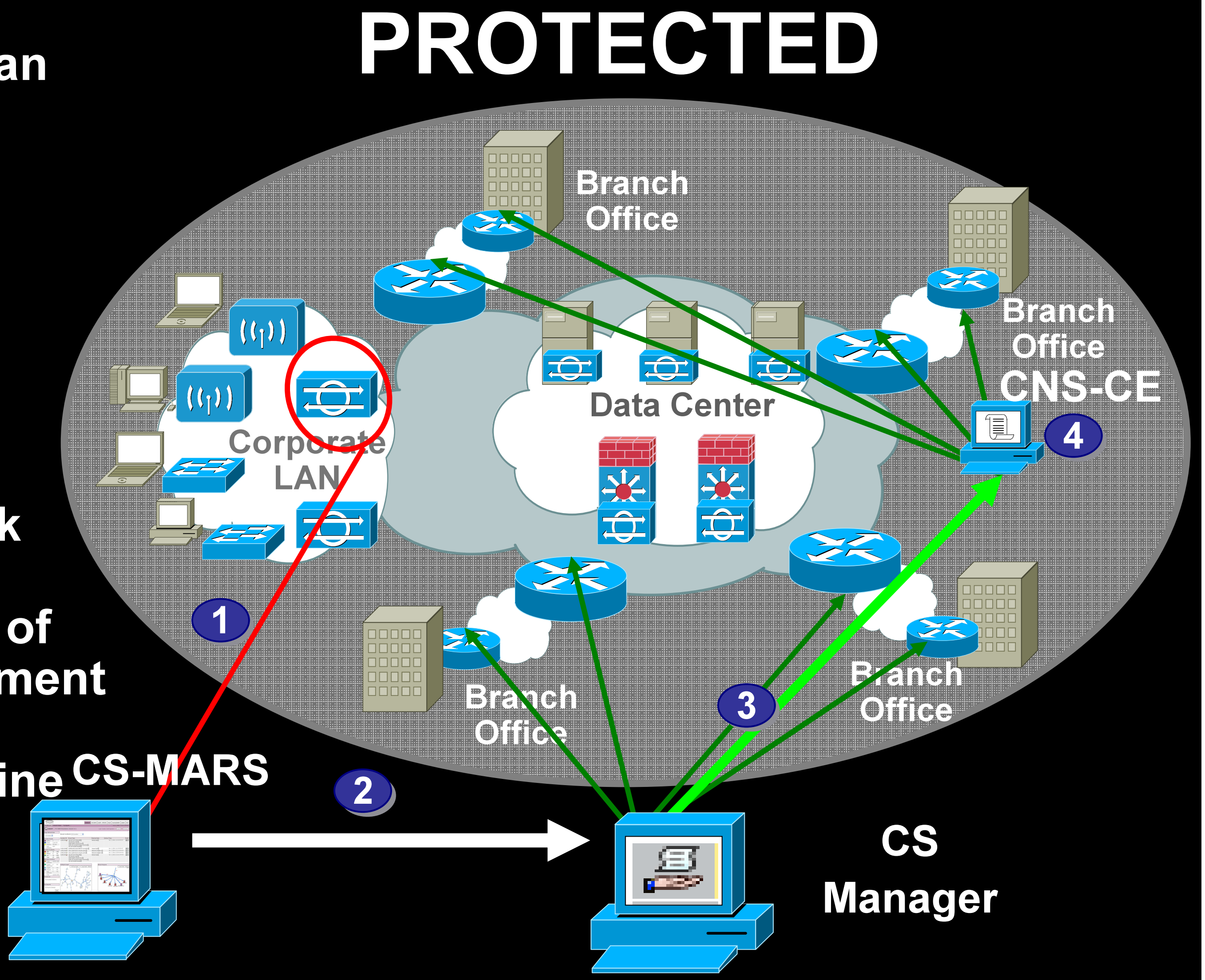
Benefits:

- Automating mitigation reduces administrative costs
- Dropping malicious traffic near source preserves WAN bandwidth & performance
- Adapting to attacks at branch routers uses security resources efficiently

SDN in Action

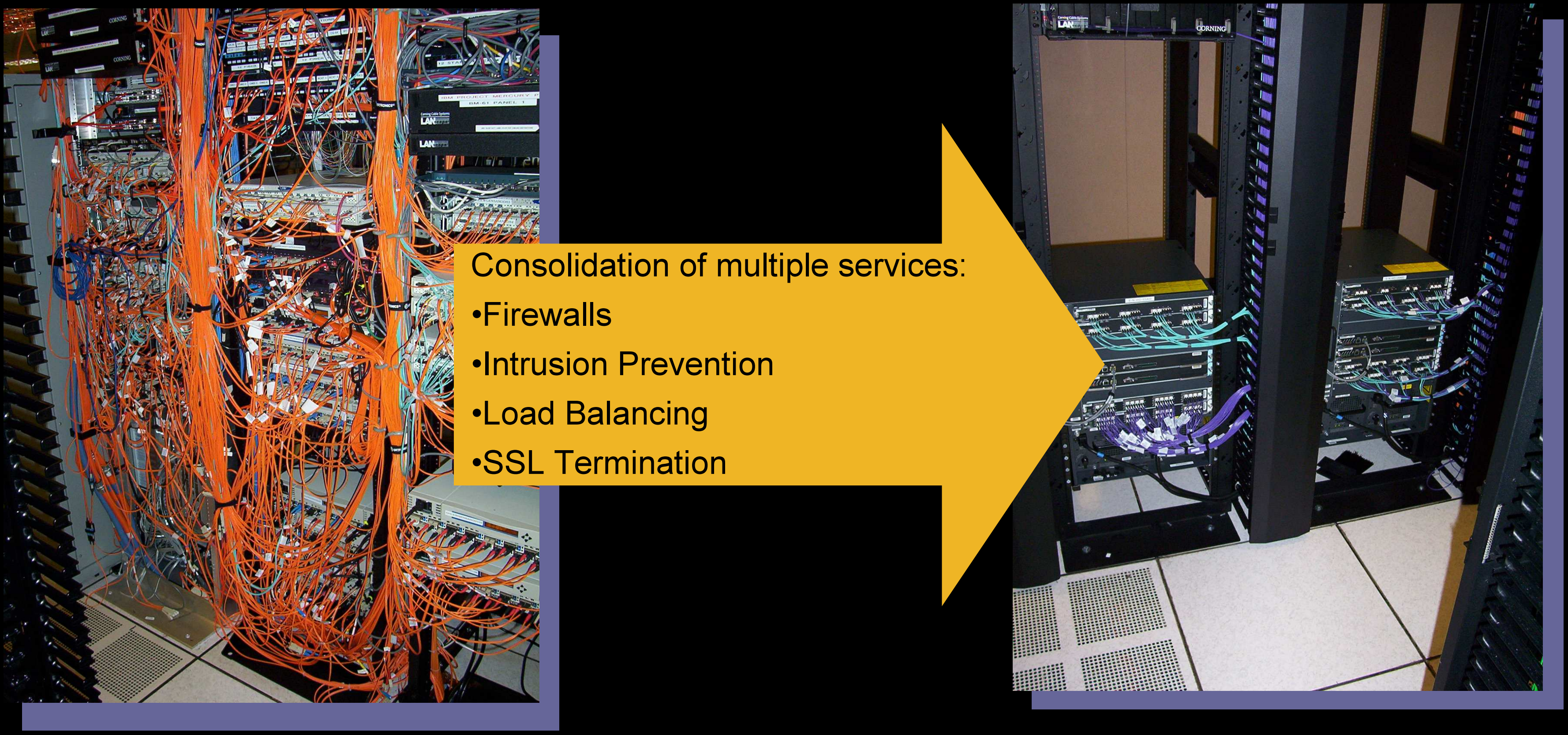
CS MARS and CS Manager Example

1. CS MARS detects an Incident
2. CS Administrator updates a Shared Policy In one place
3. A single deploy to protect the network
4. Scale through use of distributed deployment using CNS Configuration Engine



SDN in Action

Integrated Data Center Services



Consolidation of multiple services:

- Firewalls
- Intrusion Prevention
- Load Balancing
- SSL Termination

Why Cisco?
We Are Committed to Security

Product and Technology Innovation

- 2500 security-focused engineers, $300Mil R&D
- 22 acquisitions added to our solution portfolio
- $1.8 Billion in Security Revenue
- 250+ NAC partners worked collaboratively with us to deliver an unprecedented security vision

Responsible Leadership

- NIAC Vulnerability Framework Committee
- Critical Infrastructure Assurance Group
- PSIRT—responsible disclosure
- MySDN.com—intelligence and best practices sharing

"Because the network is a strategic customer asset, the protection of its business-critical applications and resources is a top priority."

—John Chambers, CEO, Cisco Systems®

References

Good links to visit:

http://www.cisco.com/go/security
http://www.cisco.com/go/sdn
http://www.cisco.com/go/nac
http://www.cisco.com/go/mars

http://www.MySDN.com

http://www.cisco.com/go/intellishield/trial

Live Demo

Questions