Cisco Self Defending Network

Louis Senecal

November 2007

Why Cisco?
We Are Committed to Security

- Product and Technology Innovation
  - $500M in Security R&D Investment
  - 1500 security-focused engineers
  - Eight acquisitions added to our solution portfolio in last two years
  - 64+ 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®

Security Acquisitions

Riverhead networks — 2004, DDOS Protection

Twingo Systems — 2004, SSL VPN Client

OKENA — 2003, HIPS

PSIONIC — 2002, CTR (Technology)

Allegro Systems, Inc. — 2001, VPN (Technology)

ALTIGA NETWORKS — 2000, VPN (Enterprise)

Compatible Systems — 2000, VPN (SP)

WheelGroup — 1998, IDS

nti — 1995, PIX

NETSOLVE — 2004, Security Mgmt.

perfigo™ — 2004, NAC addition

PROTEGO NETWORKS — 2004, Event Correlation MARS

IntelliShield — 2005, Customer Advocacy

MaSecure — 2005, VPN Technology

FineGround — 2005, Application-Acceleration and Security

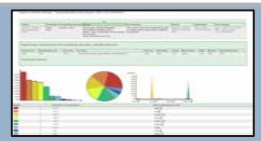
Meetinghouse Network Access Security — 2006

SyPixx NETWORKS — 2006

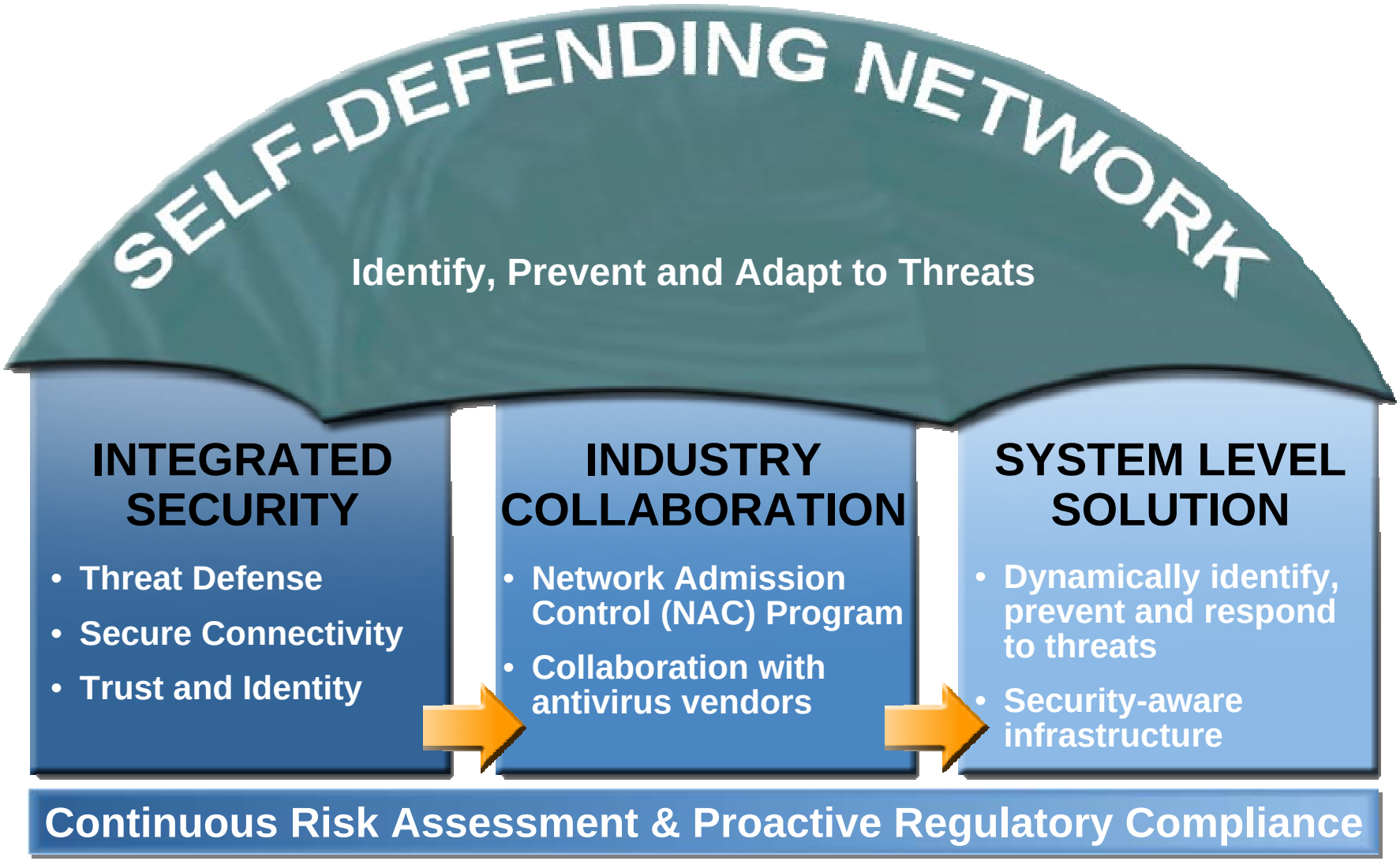
IRONPORT — 2007, Messaging and Web Security Appliance

Reactivity — 2007, XML Firewall

Security Product Portfolio

Integrated Services Router	 800	 1800	 2800	 3800	 7000	
ASA Security appliance	 5505	 5510	 5520	 5540	 5550	 5580
Intrusion Prevention System (IPS) Appliances	 4215	 4240	 4255	 4260	 4270	
Email and WEB Security Appliances	 Ironport C-Series	 Ironport S-Series	POSTX			
Anomaly Detection and Mitigation Appliances	 XT 5600	 XT 5650				
Catalyst® 6500 Series Service Modules and Data Center Security	 Firewall	 VPN	 IPS	 Anomaly Guard, Detector	 ACE	 ACE XML Gateway
Endpoint Protection	 Security Agent	 NAC Appliance: Clean Access	 CSACS & Meetinghouse			
Security Management	 CSM	 MARS	 Device Manager	 Network Compliance Manager		

Cisco Self-Defending Network



SDN Architectural Philosophy

- Technologies must span network from end-to-end including endpoints
  - Different elements have a larger or smaller role in specific locations
- Communication among devices is key to increasing contextual awareness of security entities
  - Host to network communication is critical step
- Support existing standards where mature (IPsec) and innovate where required (NAC)
- Defense-in-depth is key, each threat type needs more than one point of mitigation

Goal is a network security architecture greater than the sum of its parts

SDN = Self-Defending Network – "*The Ability for the **Network** to Identify, Adapt & Respond to Threats*"

Goal: Stop Bad Stuff.

3 Requirements:

1. **Transparency**
2. **Accuracy**
3. **Systems Approach**

3 Pillars of SDN:

Integrated Security

Collaborative Security

Adaptive Security

MARS , CSM and NCM

REMOTE SITE

ISR

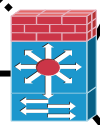
Router
ISR

FW
IPS
VPN

Firewall
PIX?
ASA
FW
VPN
IPS
Anti-X

IPS Appliance

CCA – Cisco Clean Access



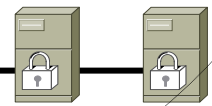
Switch
ACE
AVS

IDS Appliance

PCs

CSA – Cisco Security Agent

Servers



CSA

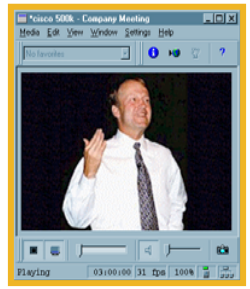
Properties of a Self-Defending Network

E-Commerce

Supply-Chain Management

Customer Care

Workforce Optimization



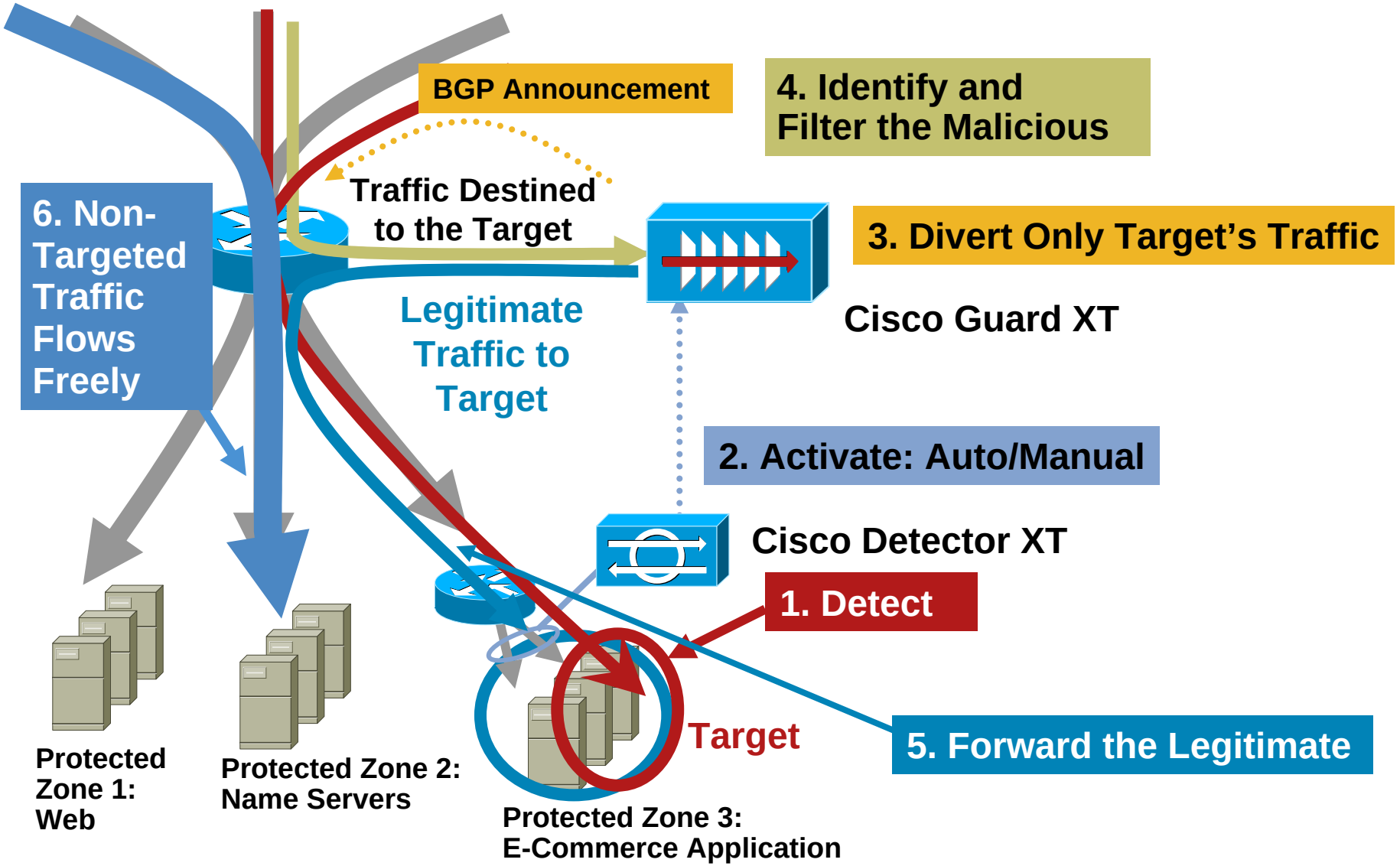
E-Learning

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

Network Availability

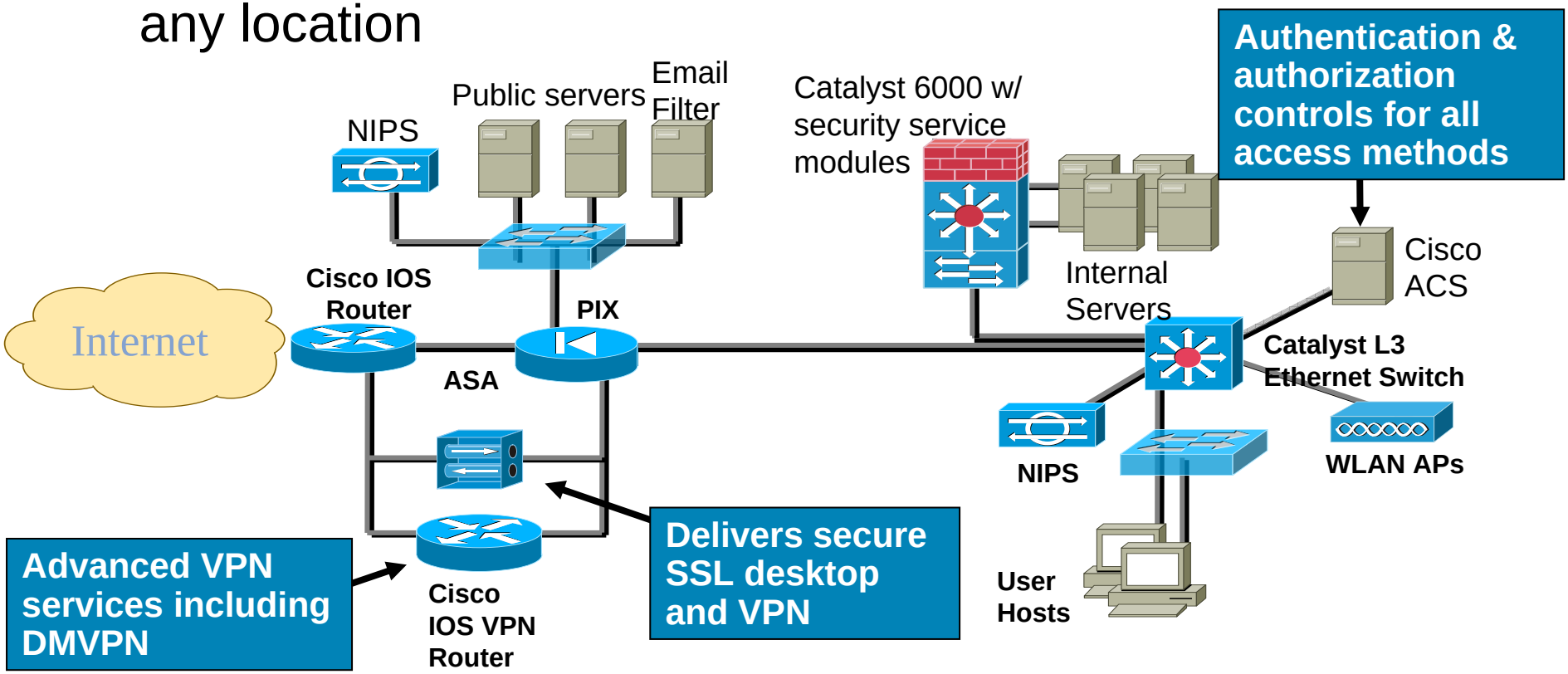
- Traditional issue: attacks consume bandwidth, endpoint, and control plane resources
- SDN solution: use anomaly guards, QoS, dynamic NIPS and firewall controls and CSA to protect these resources

Infection Containment
Cisco DDoS Solution

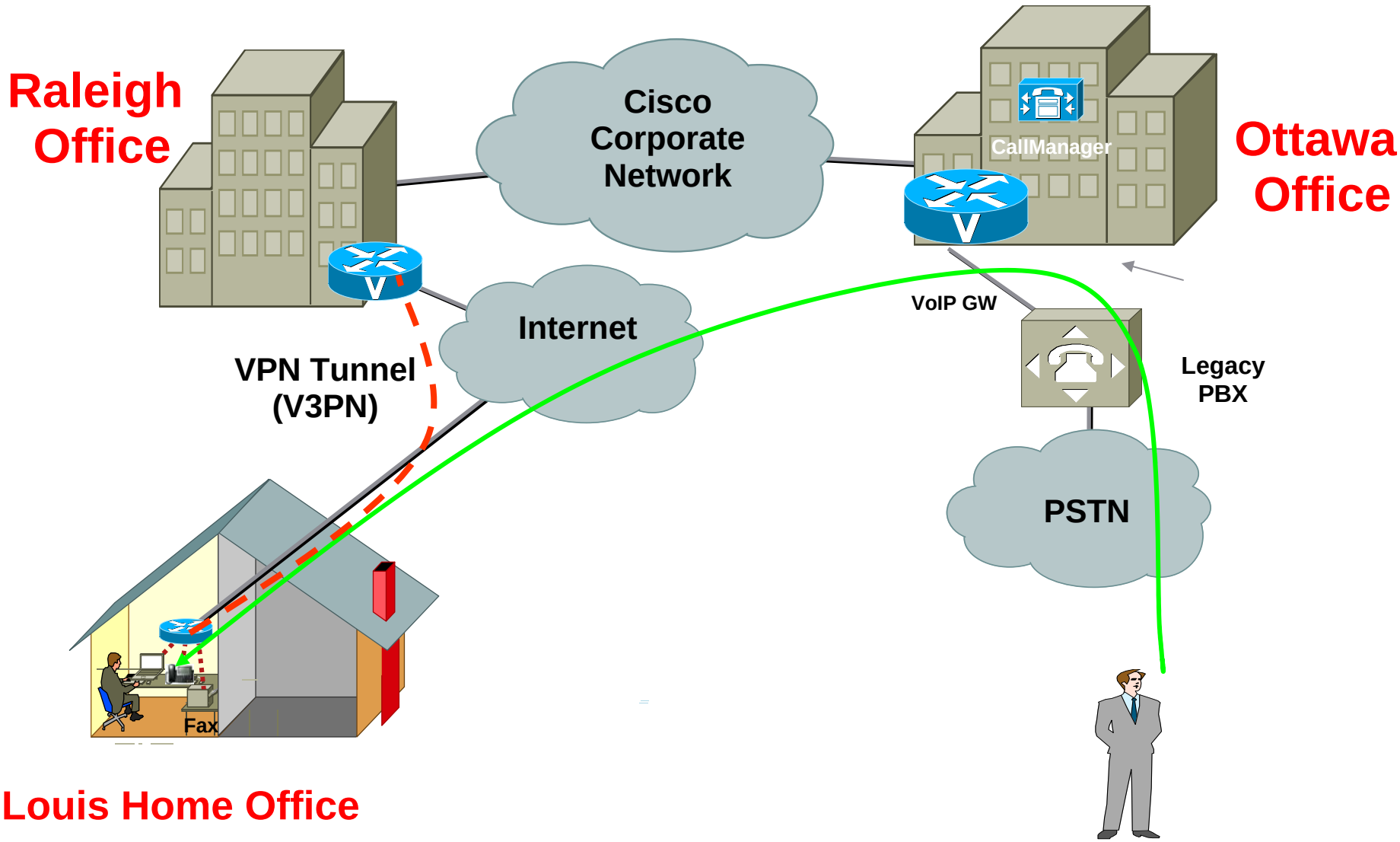


Ubiquitous Access

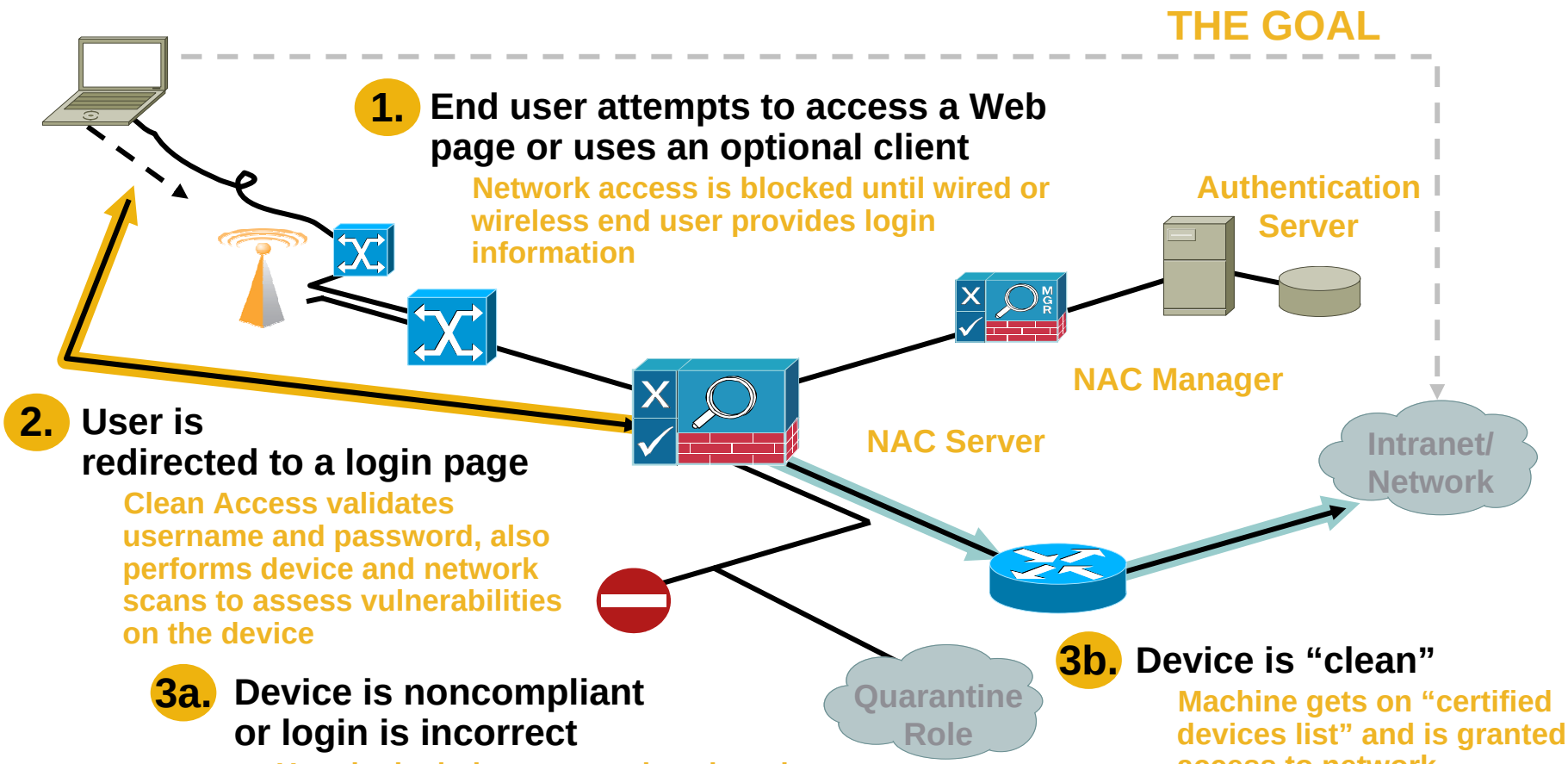
- Traditional issue: access is arbitrarily open or restrictive
- SDN Solution: use authentication, privacy, and isolation facilities to provide secure access for any device from any location



Enterprise Class Teleworker



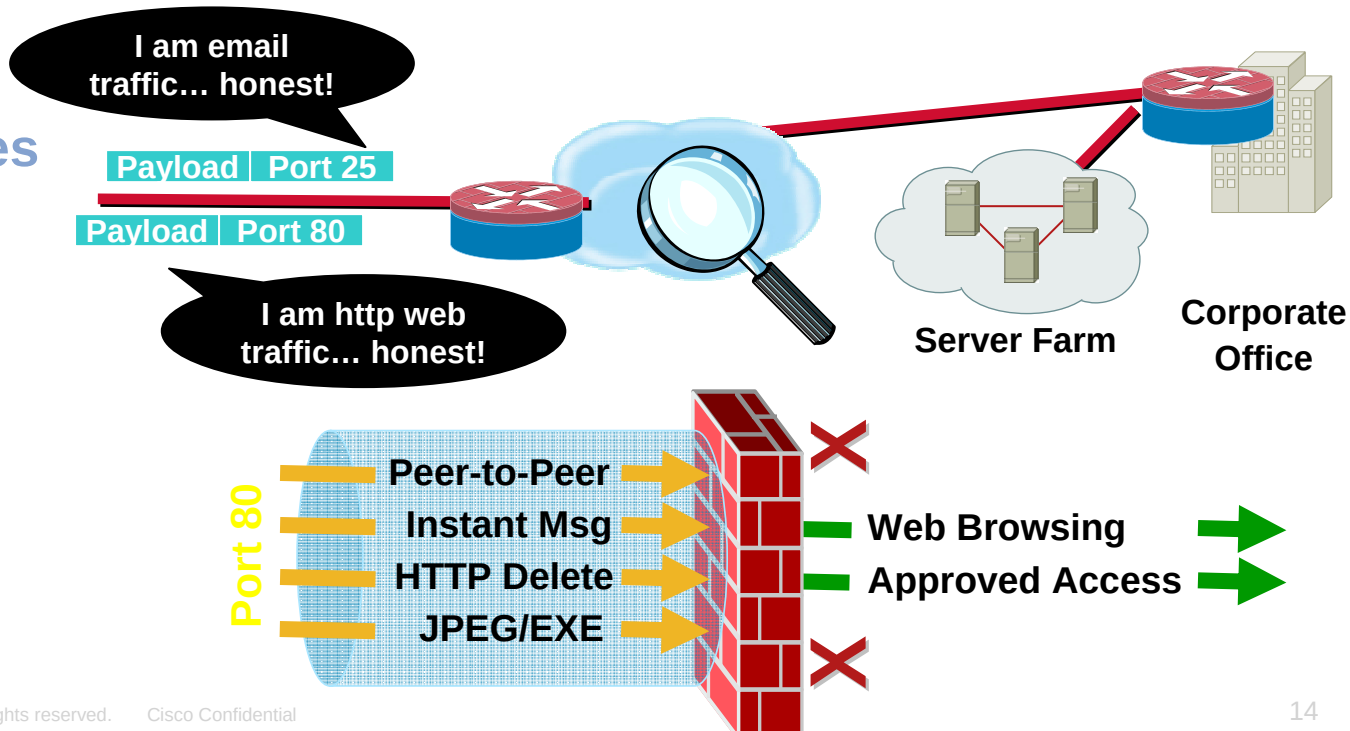
Network Admission Control



Application Intelligence

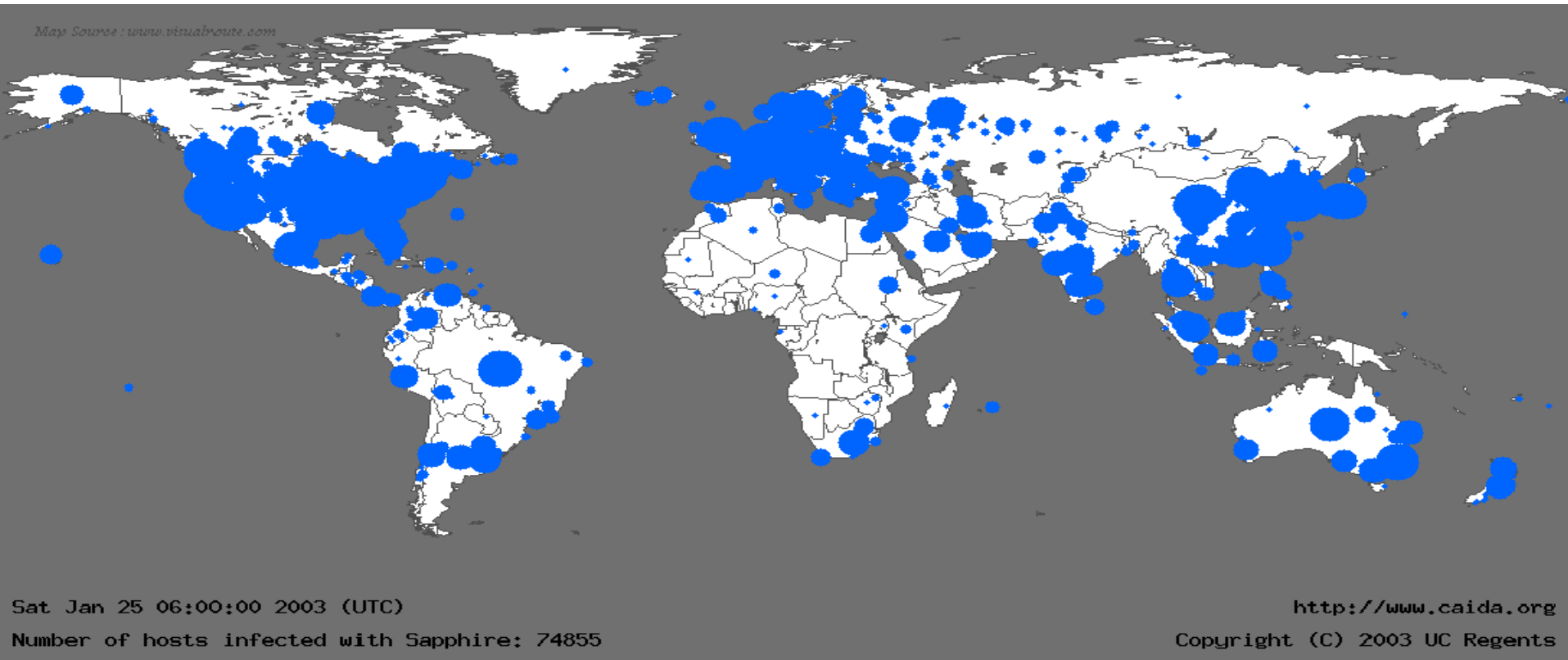
- Traditional issue: difficult to obtain and control application communication flows in a network
- SDN Solution: associates packets to applications, provides control mechanisms to enforce security policies

Inspection Engines in Ironport Appliance



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



Day Zero Protection

- Cisco defines Host-Based Intrusion Prevention as the ability to stop day zero 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
- No reconfiguration of the CSA default configuration, or update to the CSA binaries were required

Infection Containment

- Traditional issue: isolating and dampening effects of outbreaks is a difficult, manual, time and resource intensive process
- SDN Solution: rapid visibility of infected systems, system-wide isolation and response controls