# Cisco Self-Defending Network - The Global Security Approach

nbennasr@cisco.com

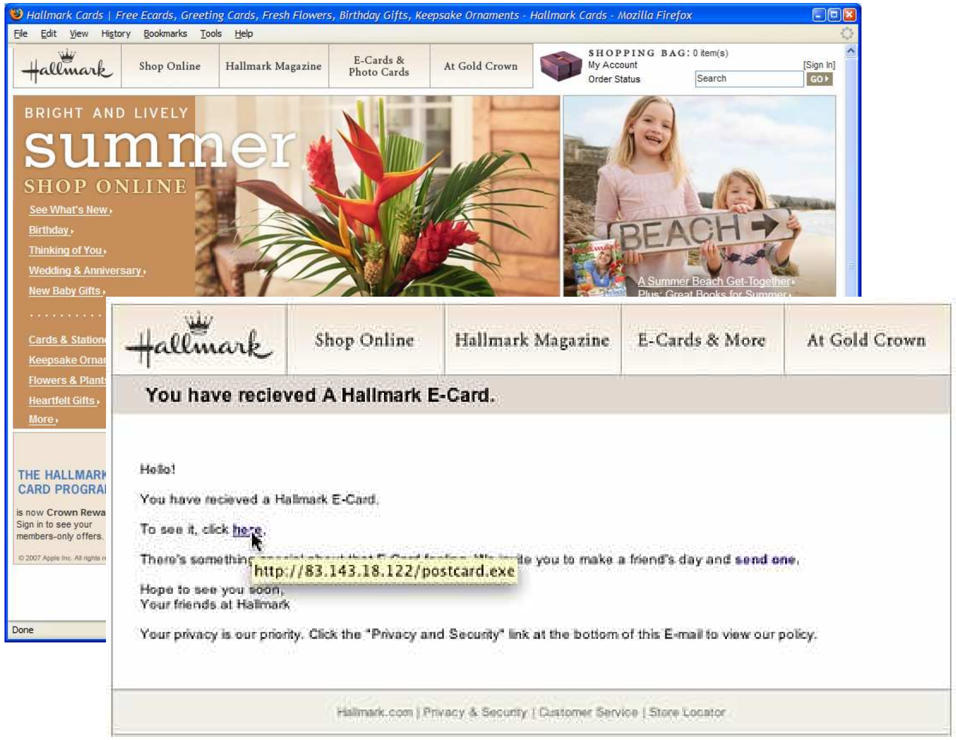
**Cisco Expo 2008**

# Agenda

- Security challenges
- Cisco Self-Defending Network - The Alternative
- Cisco Self-Defending Network - In Action
- Q&A

# Security Challenges

# Blended Threat Targeting E-Mail and Web



You have recieved A Hallmark E-Card.

Hello!

You have recieved a Hallmark E-Card.

To see it, click here.

There's something special about that E-Card feeling. We invite you to make a friend's day and send one.

http://83.143.18.122/postcard.exe

Hope to see you soon,
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.

Hallmark.com | Privacy & Security | Customer Service | Store Locator

- Spam e-mail sent by Botnet
- Directs user to malicious Web server that hosts exploit
- Upon visit, user system is compromised by server, may now be used by botnet
- Moving into enterprises: Spearphishing

## Slide 4

**BH15** the four bullets are not parallel and I'm not sure what their subjects are.  should fix to make them parallel, but i don't know how because not sure what you are trying to say here

Bonnie Hupton, 11/29/2007

# Content Security Required

Port 25

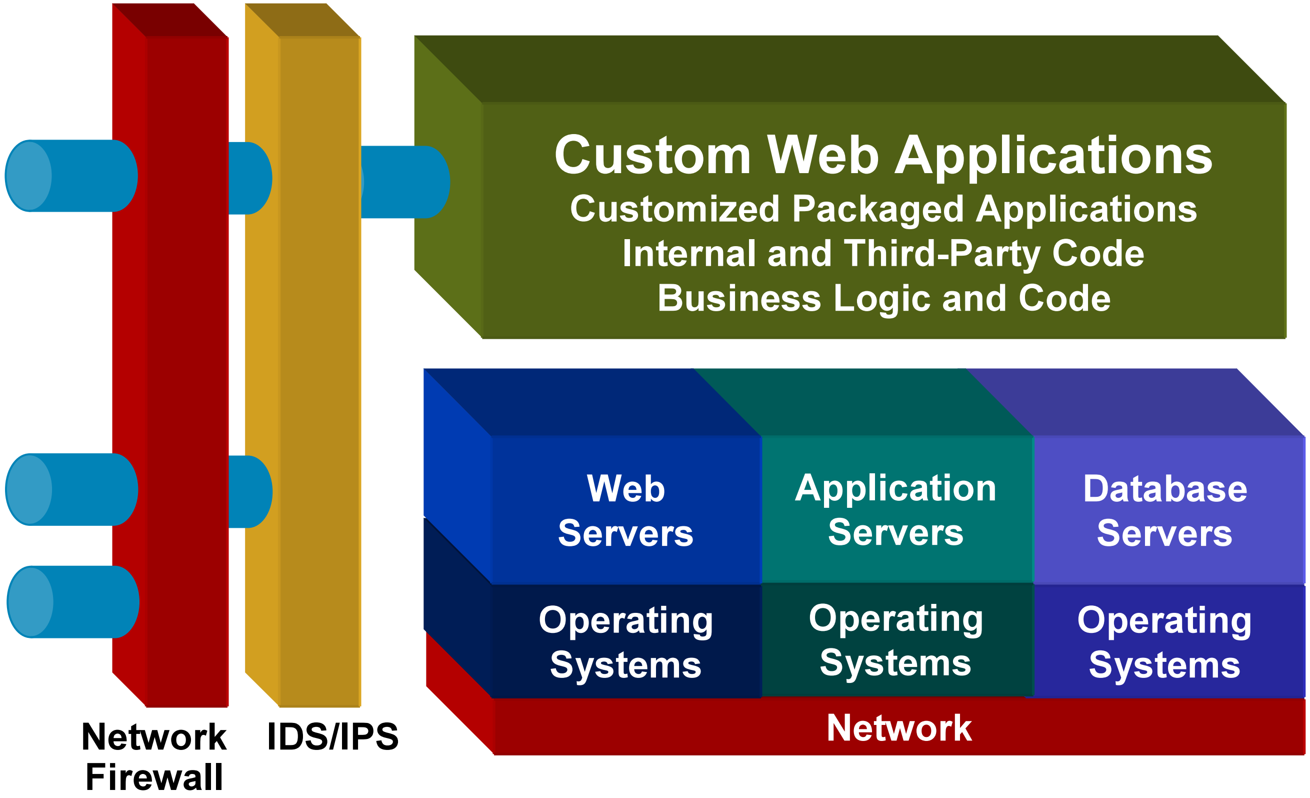
Port 80

Network Security

**Locked the Network Doors, but E-Mail and Web Stayed Open**

# Application Layer Becoming a Target Requiring Protection

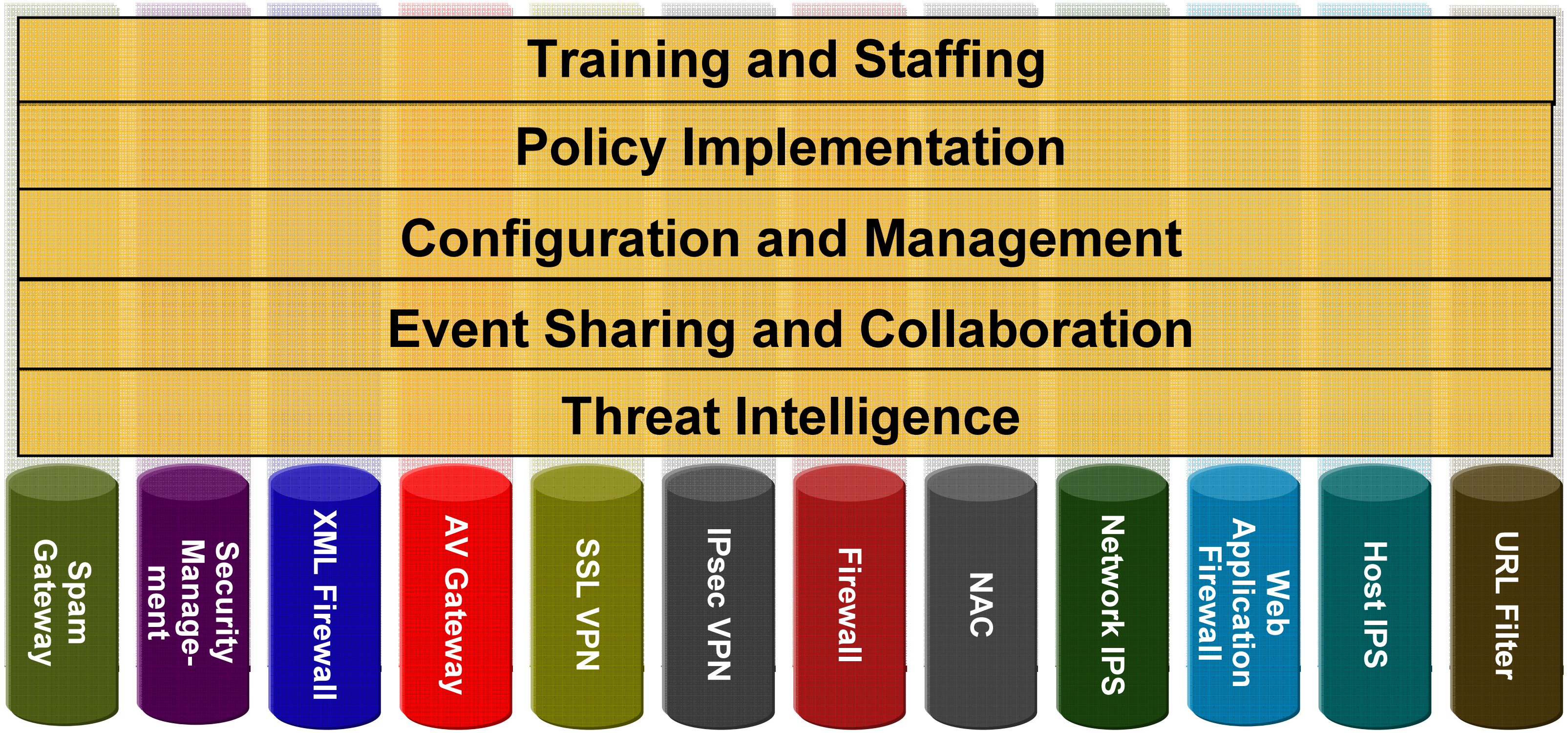
75% of New Application Attacks Focused on Custom Applications



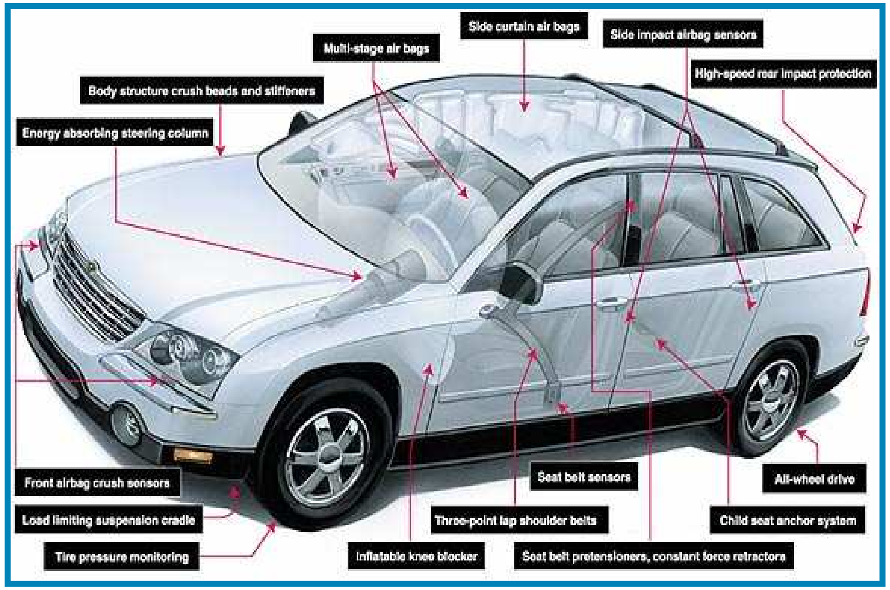
# Many Other Challenges

- **Endpoint Security**: need more then antivirus on the endpoint
- **Non Controlled Access**: access is arbitrarily open or restrictive
- **Rogue Devices** : unmanaged devices connected to the network
- **Policy Compliance & Enforcement** : asset and user identity are inconsistently validated, and endpoint posture is rarely enforced
- **Application Intelligence**: difficult to obtain and control application communication flows in a network
- **Network Availability** : attacks consume bandwidth, endpoint, and control plane resources

# The Challenges of Approaching Security Without an End-to-End, Systems Approach



# The Need for a Systems Approach

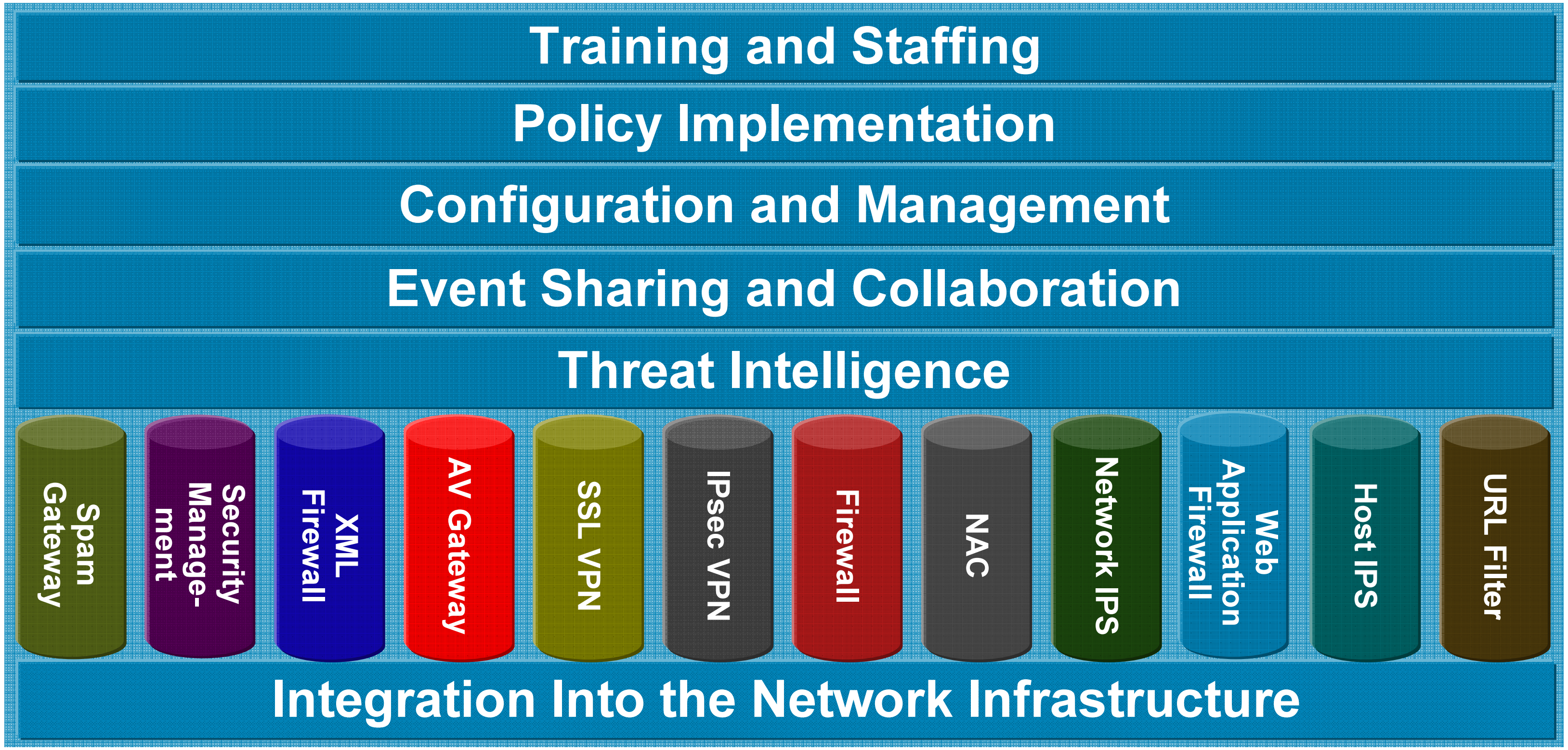

Side curtain air bags
Side impact airbag sensors
Multi-stage air bags
High-speed rear impact protection
Body structure crush beads and stiffeners
Energy absorbing steering column
Front airbag crush sensors
Seat belt sensors
All-wheel drive
Load limiting suspension cradle
Three-point lap shoulder belts
Child seat anchor system
Tire pressure monitoring
Inflatable knee blocker
Seat belt pretensioners, constant force retractors

**Less Complexity, Improved Usability**

**Collaborative Operation, Increased Effectiveness**

**Fewer Devices, Reduced Initial and Ongoing Costs**

# The Advantages of a Systems Approach:
# Lower Cost, Higher Efficiency, Greater Effect



Training and Staffing

Policy Implementation

Configuration and Management

Event Sharing and Collaboration

Threat Intelligence

Spam Gateway

Security Management

XML Firewall

AV Gateway

SSL VPN

IPsec VPN

Firewall

NAC

Network IPS

Web Application Firewall

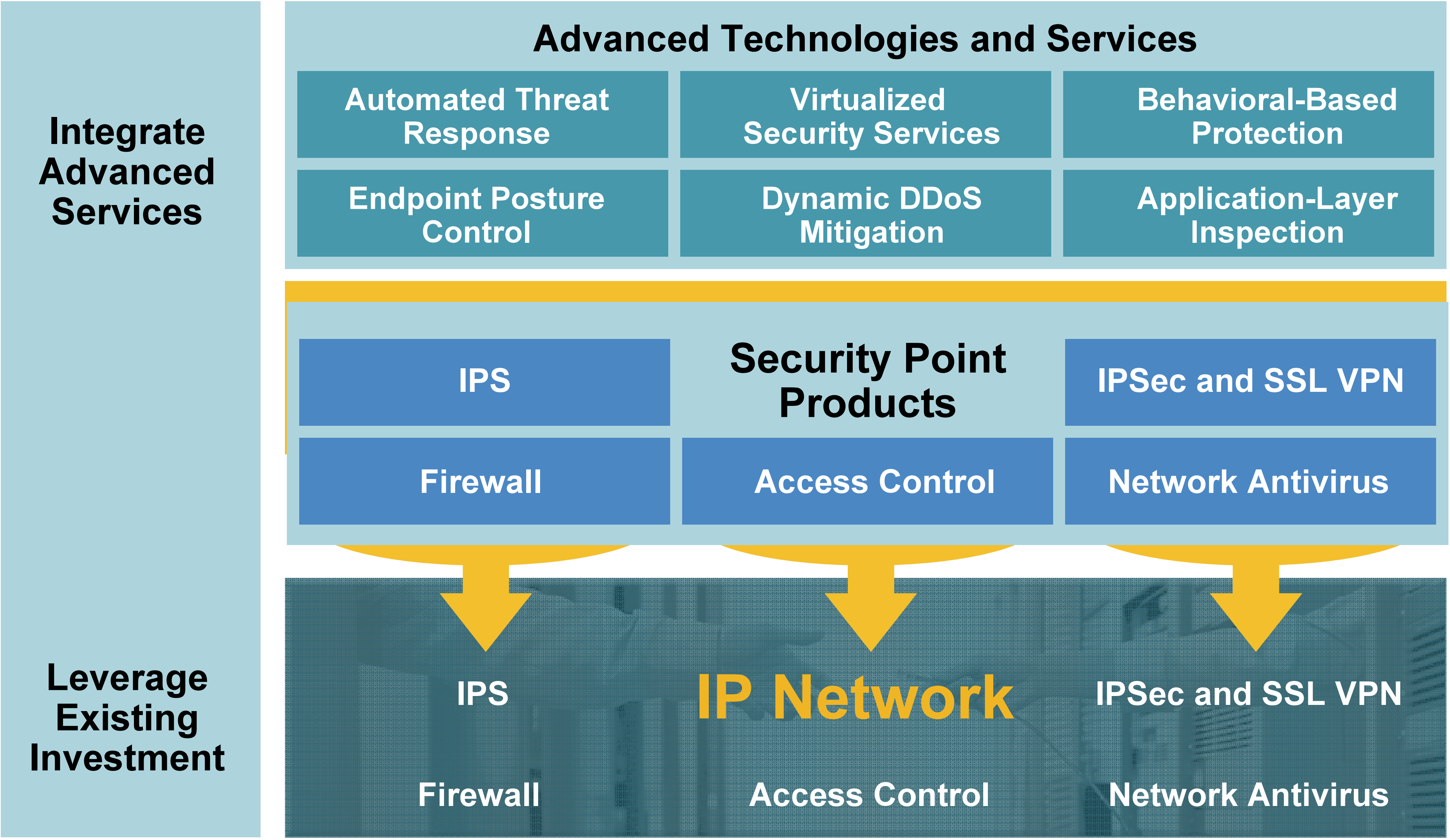
Host IPS

URL Filter

Integration Into the Network Infrastructure

# Cisco Self-Defending Network – The Alternative

# Secure Network Infrastructure
## Security Services Integrated into the Network



Integrate Advanced Services

Advanced Technologies and Services

Automated Threat Response

Virtualized Security Services

Behavioral-Based Protection

Endpoint Posture Control

Dynamic DDoS Mitigation

Application-Layer Inspection

Security Point Products

IPS

IPSec and SSL VPN

Firewall

Access Control

Network Antivirus

Leverage Existing Investment

IP Network

IPS

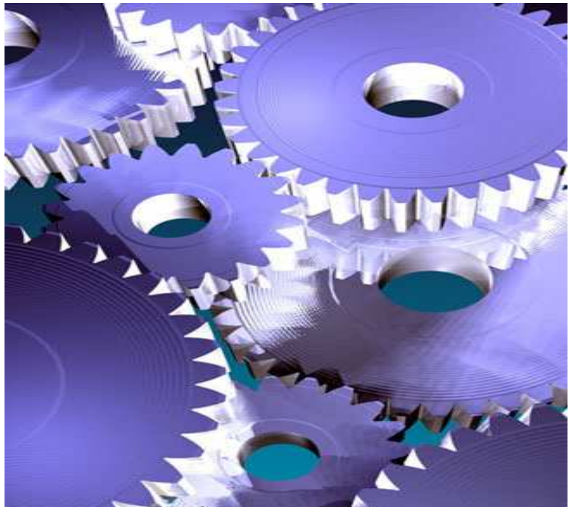
IPSec and SSL VPN

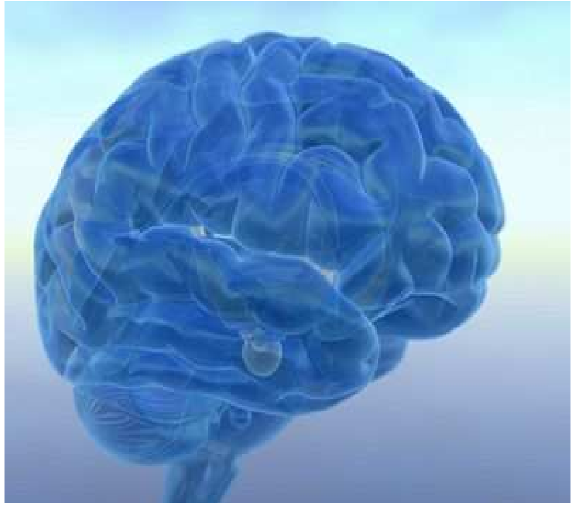
Firewall

Access Control

Network Antivirus

# Cisco Self-Defending Network:
## A Systems Approach to IT Security





### Integrated

Enabling Every Element to Be a Point of Defense and Policy Enforcement

### Adaptive

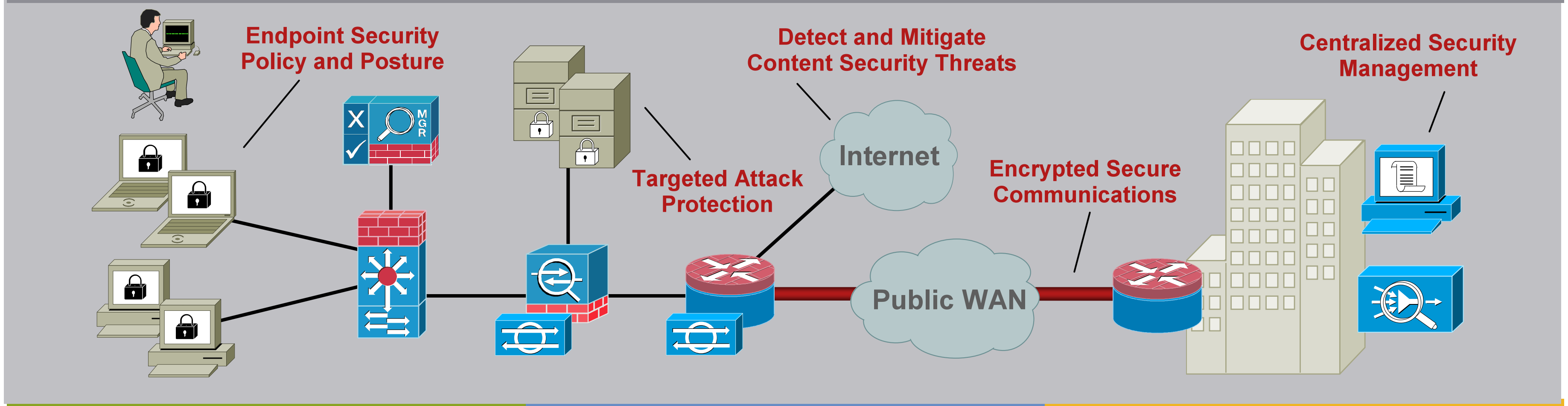
Proactive Security Technologies that Automatically Prevent Threats

### Collaborative

Collaboration Among the Services and Devices Throughout the Network to Thwart Attacks

# Self-Defending Network  Pillars

| Cisco Security Agent | Cisco NAC Appliance | Cisco ASA Adaptive Security Appliance | Cisco Integrated Services Routers | Cisco Intrusion Prevention Systems | Cisco Security Manager | Cisco Security MARS |
|---|---|---|---|---|---|---|


Endpoint Security Policy and Posture
Detect and Mitigate Content Security Threats
Centralized Security Management
Internet
Targeted Attack Protection
Encrypted Secure Communications
Public WAN

## Integrated

- Multivector protections at all points in the network and at desktop and server endpoints
- Branch infrastructure security that enables end-to-end architecture

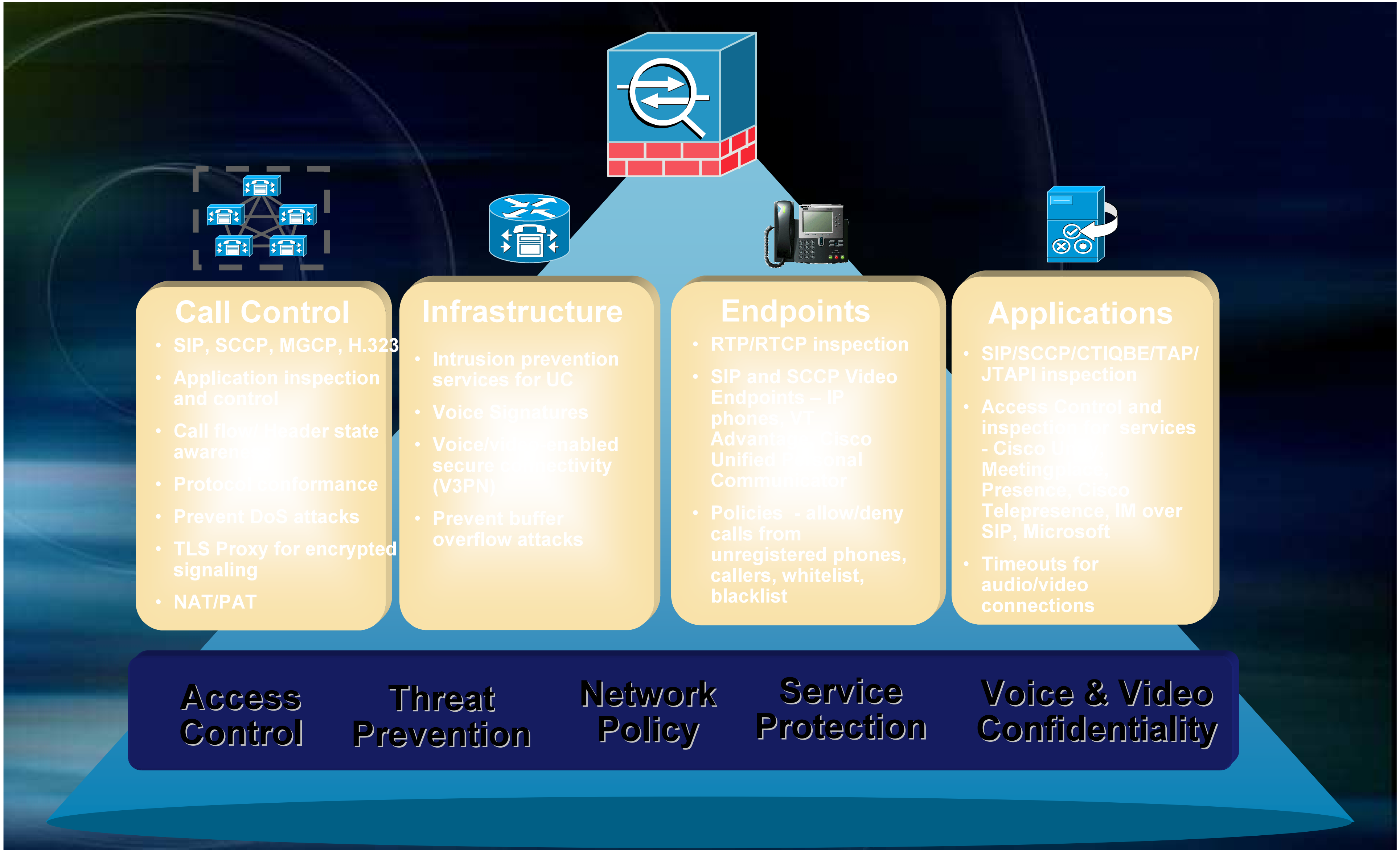
## Adaptive

- Anomaly detection with in-production learning
- Network behavioral analysis
- Visibility and mitigation capabilities for blended content-based threats
- Real-time security posture adjustment

## Collaborative

- Cross-solution feedback linkages
- Common policy management
- Endpoint posture and security policy enforcement
- Passive and active fingerprinting
- Cisco Security Agent IPS collaboration

# Adaptive Application Intelligence
# Unified Communication



### Call Control

- SIP, SCCP, MGCP, H.323
- Application inspection and control
- Call flow/ Header state awareness
- Protocol conformance
- Prevent DoS attacks
- TLS Proxy for encrypted signaling
- NAT/PAT

### Infrastructure

- Intrusion prevention services for UC
- Voice Signatures
- Voice/video-enabled secure connectivity (V3PN)
- Prevent buffer overflow attacks

### Endpoints

- RTP/RTCP inspection
- SIP and SCCP Video Endpoints – IP phones, VT Advantage, Cisco Unified Personal Communicator
- Policies - allow/deny calls from unregistered phones, callers, whitelist, blacklist

### Applications

- SIP/SCCP/CTIQBE/TAP/ JTAPI inspection
- Access Control and inspection for services - Cisco Unified Meetingplace, Presence, Cisco Telepresence, IM over SIP, Microsoft
- Timeouts for audio/video connections

Access Control

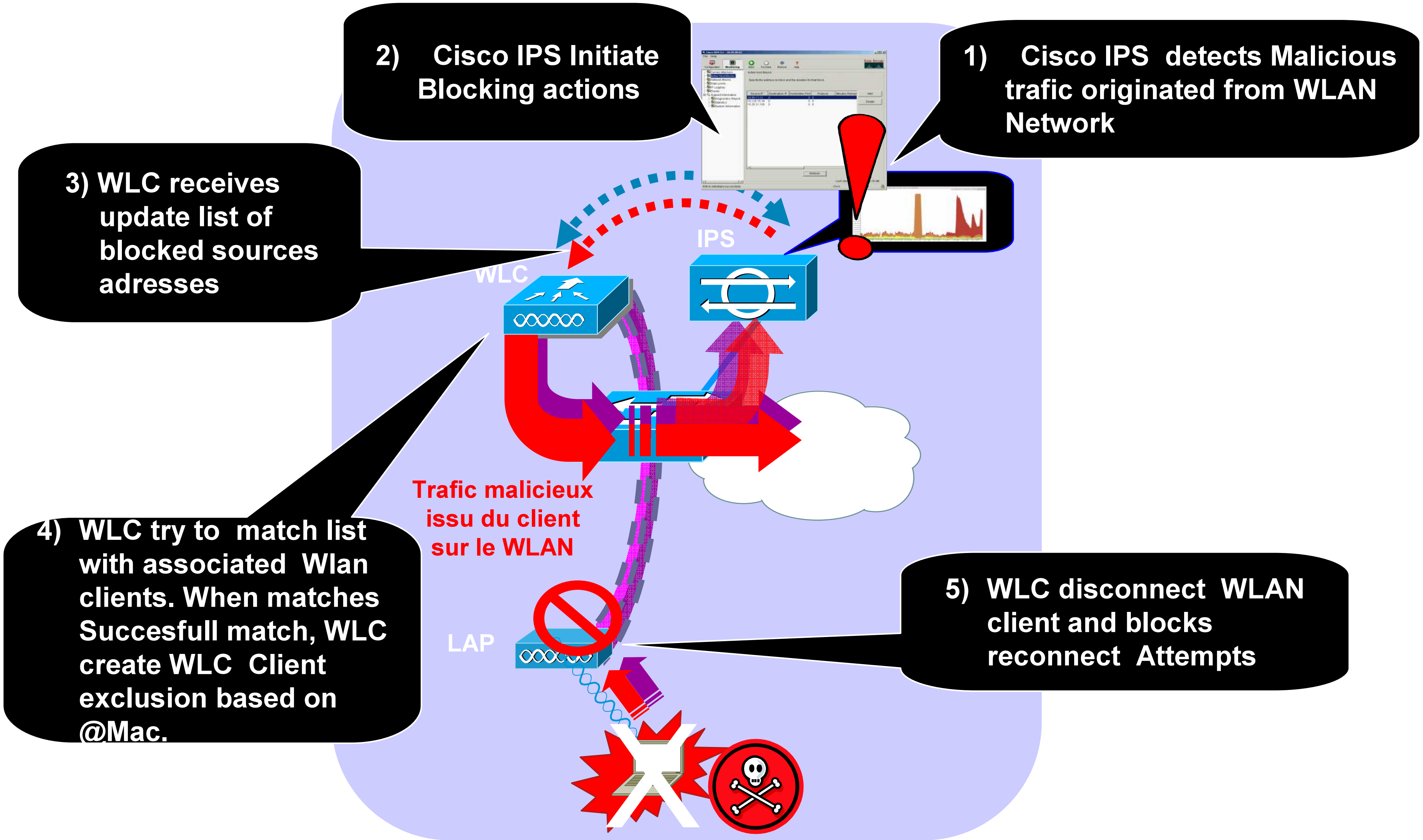
Threat Prevention

Network Policy

Service Protection

Voice & Video Confidentiality

# Collaboration
# WLC & IPS



1) Cisco IPS detects Malicious trafic originated from WLAN Network

2) Cisco IPS Initiate Blocking actions

3) WLC receives update list of blocked sources adresses

Trafic malicieux issu du client sur le WLAN

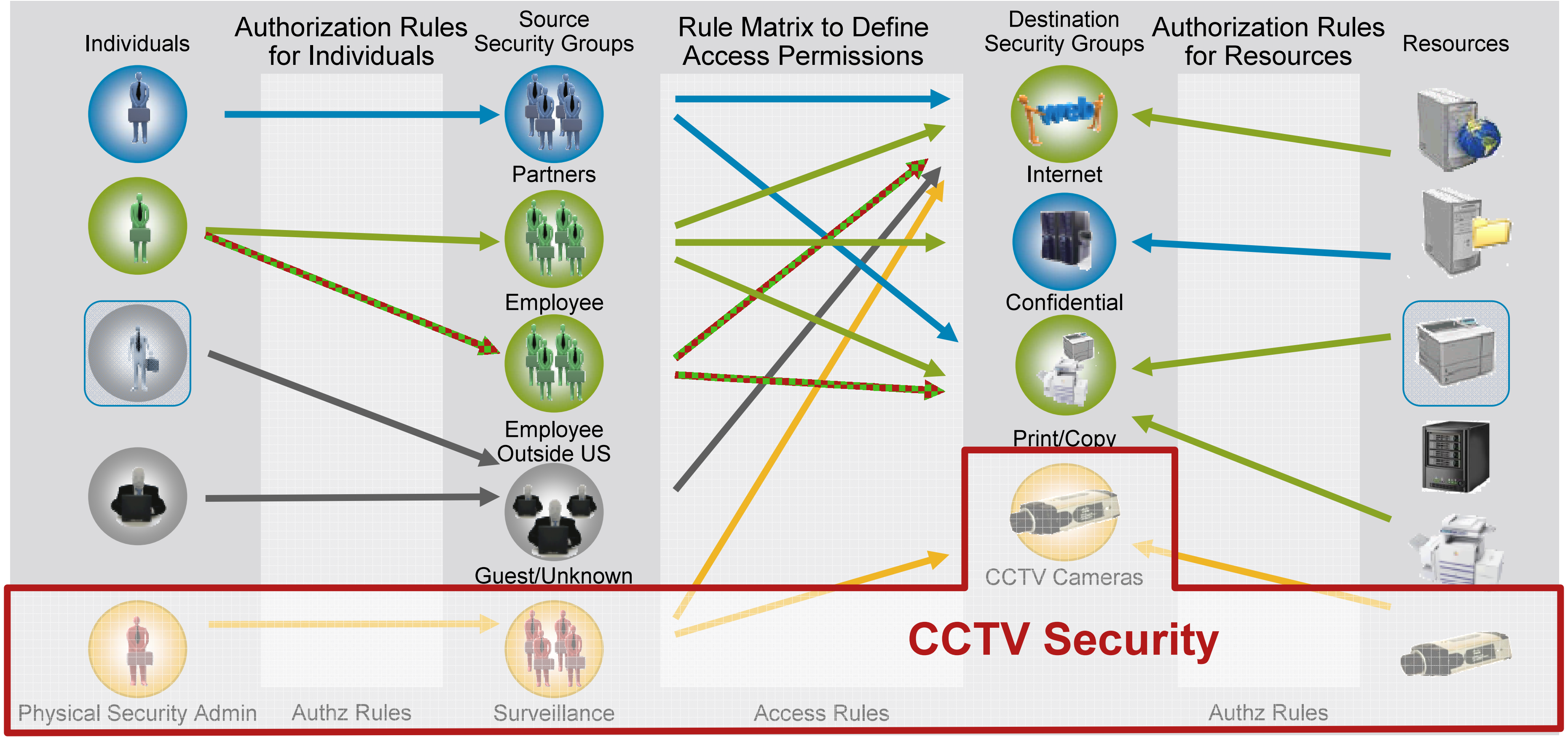
4) WLC try to match list with associated Wlan clients. When matches Succesfull match, WLC create WLC Client exclusion based on @Mac.

5) WLC disconnect WLAN client and blocks reconnect Attempts

# Integrated Security
# Group Tags with Cisco TrustSec

Access Control

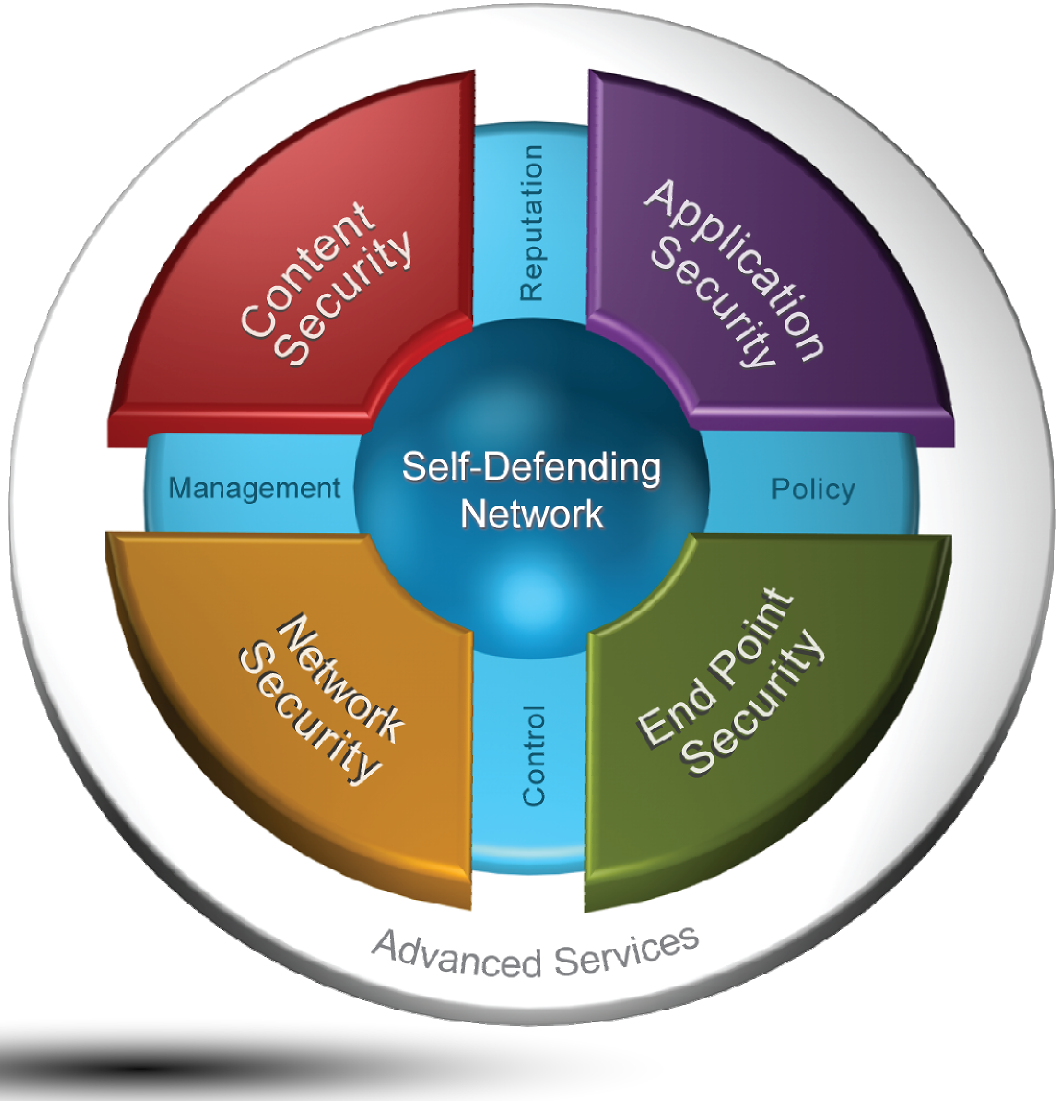
## Multi Network Attributes without Multi ACLs



Source: Ken Hook

- **Example:** Physical security administrators part of surveillance group
- Policy applied on login to restrict access to CCTV cameras

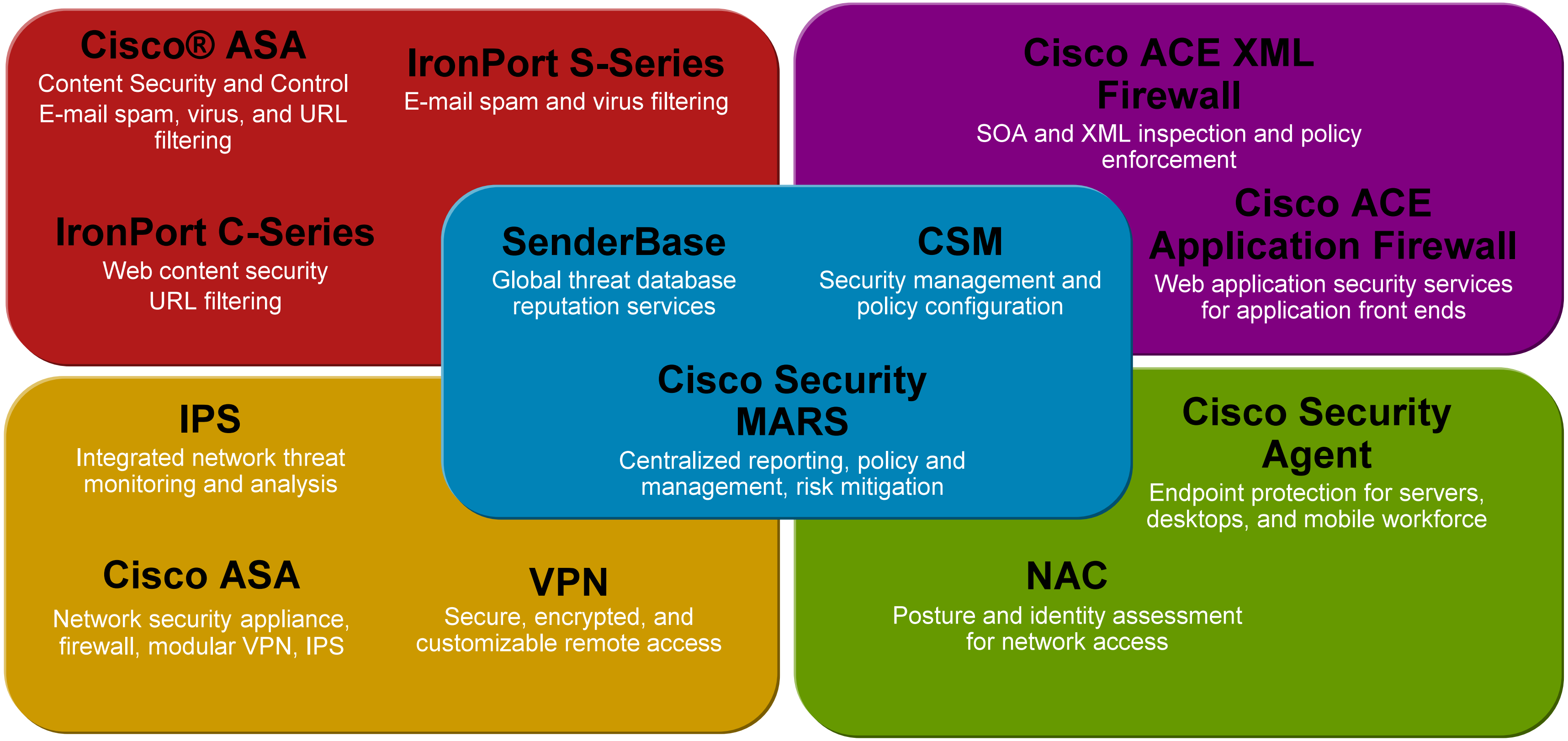
# Cisco Self-Defending Network
## IT Security Solution Components



## Slide 18

**BH21** should be Endpoint in the picture
Bonnie Hupton, 11/29/2007

# Changing the Game
## End-to-End IT Security Solution



**Cisco® ASA**
Content Security and Control
E-mail spam, virus, and URL filtering

**IronPort S-Series**
E-mail spam and virus filtering

**IronPort C-Series**
Web content security
URL filtering

**Cisco ACE XML Firewall**
SOA and XML inspection and policy enforcement

**Cisco ACE Application Firewall**
Web application security services for application front ends

**SenderBase**
Global threat database reputation services

**CSM**
Security management and policy configuration

**Cisco Security MARS**
Centralized reporting, policy and management, risk mitigation

**IPS**
Integrated network threat monitoring and analysis

**Cisco ASA**
Network security appliance, firewall, modular VPN, IPS

**VPN**
Secure, encrypted, and customizable remote access

**Cisco Security Agent**
Endpoint protection for servers, desktops, and mobile workforce

**NAC**
Posture and identity assessment for network access

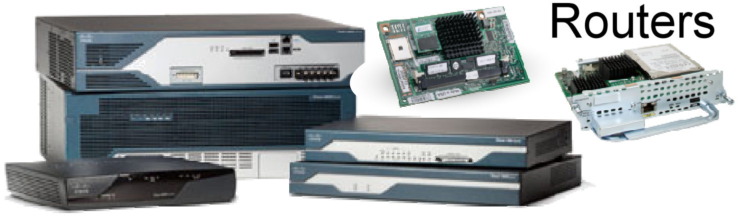
# Advanced Network Security for the SDN

Cisco ASA Adaptive Security Appliance
Firewall, SSL VPN, IPS

Cisco Intrusion Prevention System Sensors

Cisco IDSM and FWSM

Cisco Integrated Services Routers



## Features

- Signature, behavioral- and vulnerability-based detection
- Integrated security policies throughout the network infrastructure infrastructure

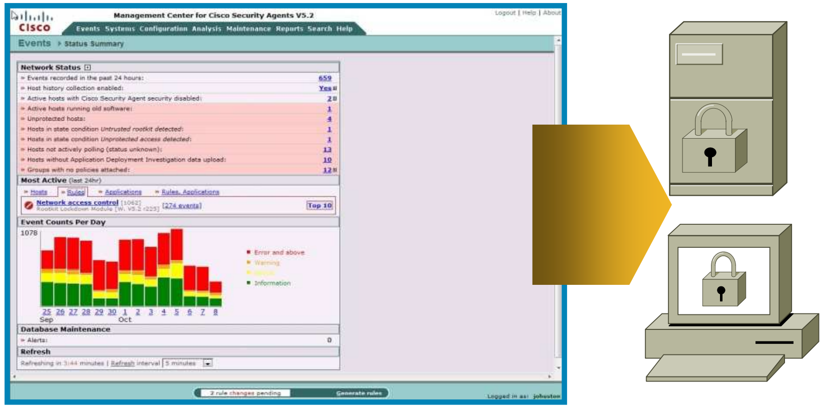
## Benefits

- Helps ensure uptime and asset protection
- Proactively protects against known and unknown threats
- Proactively contains infections and outbreaks
- Maintains privacy and confidentiality
- Cost-effectively extends reach of network
- Increases flexibility and increases employee productivity

# Secure Endpoint Control for the SDN

## Cisco Network Admission Control (NAC)

## Cisco Security Agent



**Network Status**

- Events recorded in the past 24 hours: 659
- Host history collection enabled: Yes
- Active hosts with Cisco Security Agent security disabled: 2
- Active hosts running old software: 1
- Unprotected hosts: 4
- Hosts in state condition *Untrusted rootkit detected*: 1
- Hosts in state condition *Unprotected access detected*: 1
- Hosts not actively polling (status unknown): 13
- Hosts without Application Deployment Investigation data upload: 10
- Groups with no policies attached: 12

**Most Active** (last 24hr)

Network access control [1062] [274 events]
Rootkit Lockdown Module [W, V5.2 r225]

**Event Counts Per Day**

1078

25 26 27 28 29 30 1 2 3 4 5 6 7 8
Sep Oct

**Database Maintenance**

- Alerts: 0

**Refresh**

Refreshing in 3:44 minutes | Refresh interval 5 minutes

2 rule changes pending

Logged in as: johuston

### Features

- Role-based network access control and security policy compliance enforcement
- Full lifecycle: Discovery, assessment, enforcement, and remediation
- Threat protection for desktops, servers, and POS devices

### Benefits

- Securing both managed and unmanaged assets for security policy compliance
- Reducing vulnerability-based exploits to safeguard assets and information
- Minimizing risk by increasing visibility and enforcement

# Content Security for the SDN

**Cisco® IronPort C-Series**
**Cisco IronPort S-Series**

**Cisco ASA Content Security**

Features

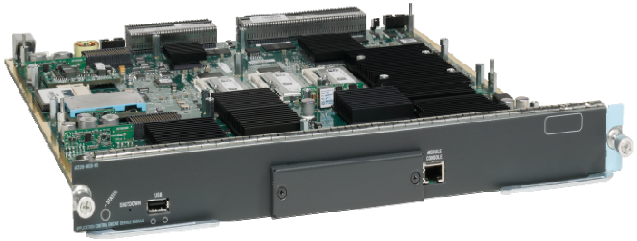
- Blocks incoming e-mail and Web threats
- Controls outbound content
- Filters Web and e-mail with reputation-based filters for granular policy controls

Benefits

- Protects against incoming threats, spam, malware, viruses, and worms with up-to-date technologies
- Protects message privacy
- Meets regulatory compliance
- Consolidates functions

# Application Security for the SDN

Cisco® ACE Application Control Engine Module



Cisco ACE 4710 Appliance

Cisco ACE Web Application Firewall

Features

- Inspects Layer 4–7 applications
- Inspects and secures Web, B2B, and application-to-application traffic
- ACE WAF supports >30,000 transactions per second

Benefits

- Enhances application availability; prevents disruption
- Segments load-balancing and application traffic
- Identifies and prevents application-specific attacks
- Protects business assets from exposure
- Addresses compliance and privacy requirements

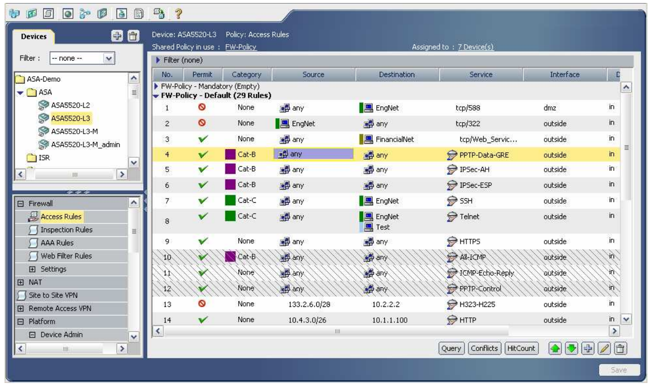
## Slide 23

**BH20** is fifth bullet ok? Segments? trying to make parallel

Bonnie Hupton, 11/29/2007

# Operational Control and Policy Management

## Cisco® Security Manager



Devices

Filter : -- none --

- ASA-Demo
  - ASA
    - ASA5520-L2
    - ASA5520-L3
    - ASA5520-L3-M
    - ASA5520-L3-M_admin
  - ISR

- ⊟ Firewall
  - Access Rules
  - Inspection Rules
  - AAA Rules
  - Web Filter Rules
  - ⊞ Settings
- ⊞ NAT
- Site to Site VPN
- ⊞ Remote Access VPN
- ⊟ Platform
  - ⊟ Device Admin

Device: ASA5520-L3 Policy: Access Rules

Shared Policy in use : FW-Policy Assigned to : 7 Device(s)

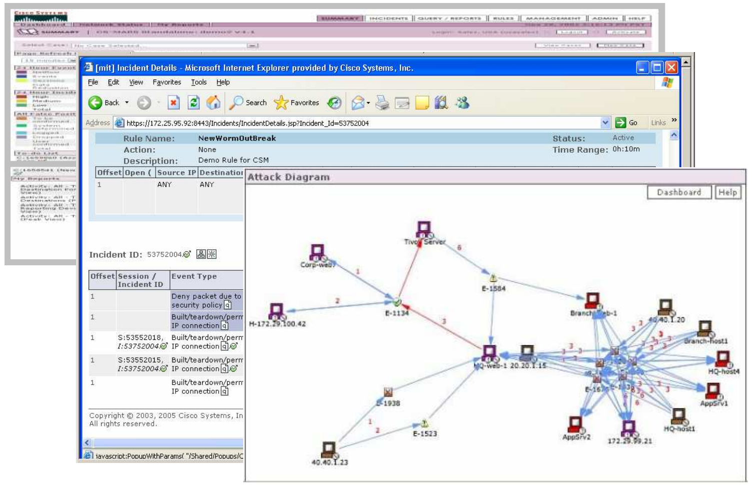
Filter (none)

FW-Policy - Mandatory (Empty)

**FW-Policy - Default (29 Rules)**

| No. | Permit | Category | Source | Destination | Service | Interface | D |
|---|---|---|---|---|---|---|---|
| 1 | ⊘ | None | any | EngNet | tcp/588 | dmz | in |
| 2 | ⊘ | None | EngNet | any | tcp/322 | outside | in |
| 3 | ✓ | None | any | FinancialNet | tcp/Web_Servic... | outside | in |
| 4 | ✓ | Cat-B | any | any | PPTP-Data-GRE | outside | in |
| 5 | ✓ | Cat-B | any | any | IPSec-AH | outside | in |
| 6 | ✓ | Cat-B | any | any | IPSec-ESP | outside | in |
| 7 | ✓ | Cat-C | any | EngNet | SSH | outside | in |
| 8 | ✓ | Cat-C | any | EngNet<br>Test | Telnet | outside | in |
| 9 | ✓ | None | any | any | HTTPS | outside | in |
| 10 | ✓ | Cat-B | any | any | All-ICMP | outside | in |
| 11 | ✓ | None | any | any | ICMP-Echo-Reply | outside | in |
| 12 | ✓ | None | any | any | PPTP-Control | outside | in |
| 13 | ⊘ | None | 133.2.6.0/28 | 10.2.2.2 | H323-H225 | outside | in |
| 14 | ✓ | None | 10.4.3.0/26 | 10.1.1.100 | HTTP | outside | in |

## Cisco Security MARS



[mit] Incident Details - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address https://172.25.95.92:8443/Incidents/IncidentDetails.jsp?Incident_Id=53752004

Rule Name: **NewWormOutBreak**

Action: None

Description: Demo Rule for CSM

Status: Active

Time Range: 0h:10m

| Offset | Open ( | Source IP | Destinatior |
|---|---|---|---|
| 1 | | ANY | ANY |

Incident ID: 53752004

| Offset | Session / Incident ID | Event Type |
|---|---|---|
| 1 | | Deny packet due to security policy |
| 1 | | Built/teardown/perm IP connection |
| 1 | S:53552018, *I:53752004* | Built/teardown/perm IP connection |
| 1 | S:53552015, *I:53752004* | Built/teardown/perm IP connection |
| 1 | | Built/teardown/perm IP connection |

Copyright © 2003, 2005 Cisco Systems, In
All rights reserved.

javascript:PopupWithParams( "/Shared/Popups/C

Attack Diagram

### Features

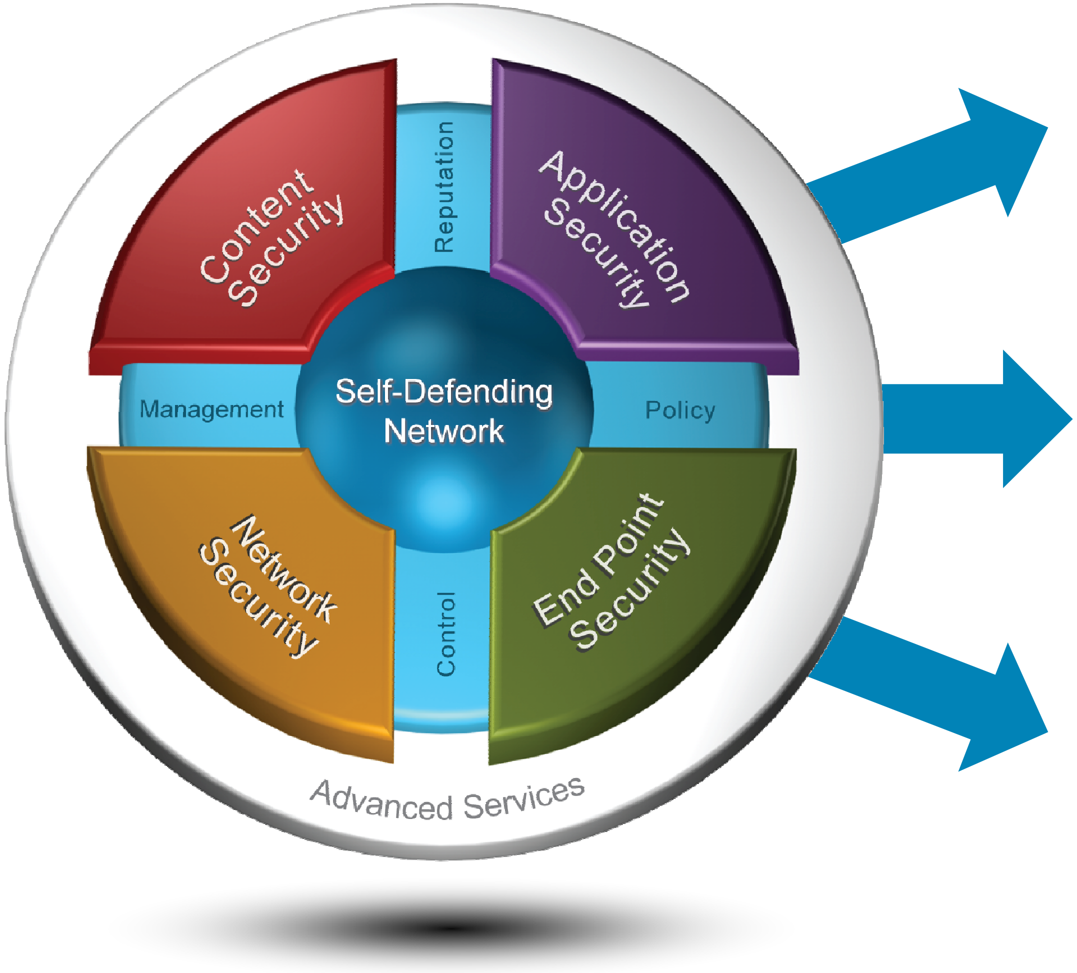
- Unified policy and device management for firewall, IPS, and VPN security services across all Cisco platforms
- Integrated capabilities that link monitored security violations to policy rules
- Multivendor security event monitoring, correlation, and mitigation
- Topology awareness for rapid threat isolation and mitigation

### Benefits

- Simplifies security operations with centralized, hierarchical policy configuration and real-time threat monitoring
- Rapid threat identification minimizes downtime
- Facilitates efficiency with workflow management between security and network operations
- Integrated change management and incident analysis facilitates thorough system auditing

# Cisco Self-Defending Network in action

# Cisco SDN Solutions for Secure Communications and Collaboration



Mitigate Targeted Attacks and Malware Propagation

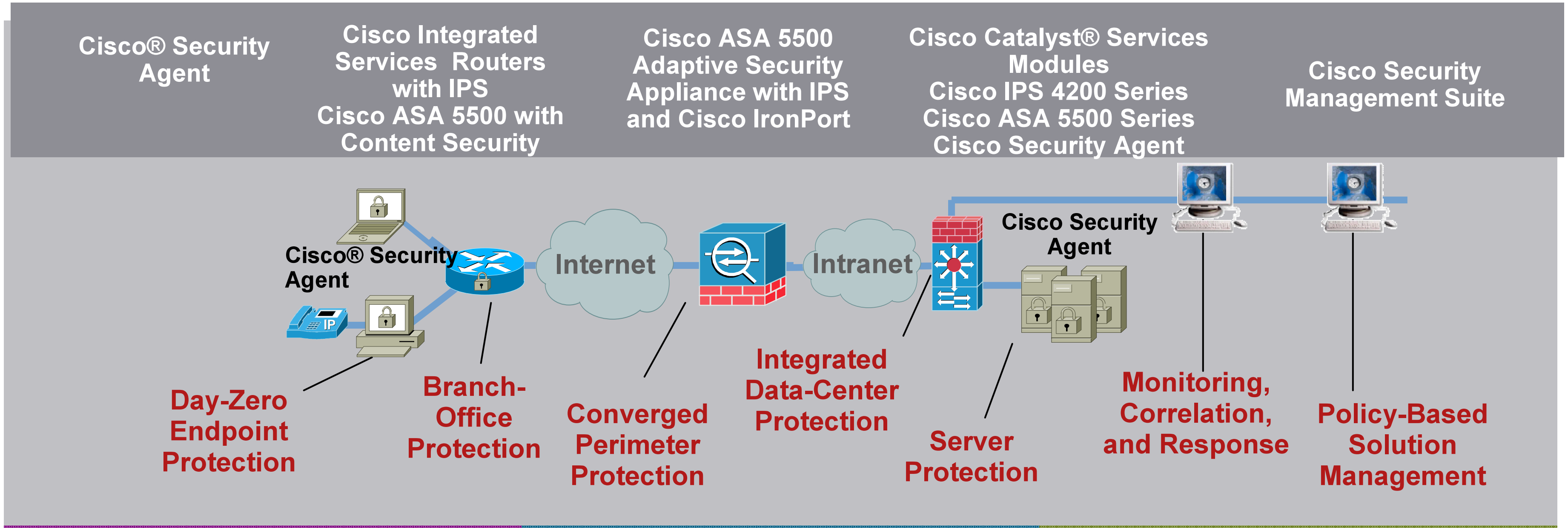
Prevent Data Leakage and Disclosure

Achieve Policy and Regulatory Compliance

## Slide 26

| | |
|---|---|
| **BH7** | should be Endpoint in picture<br>Bonnie Hupton, 11/29/2007 |

# Mitigating Targeted Attacks and Malware
## Self-Defending Network Applied



Cisco® Security Agent

Cisco Integrated Services Routers with IPS
Cisco ASA 5500 with Content Security

Cisco ASA 5500 Adaptive Security Appliance with IPS and Cisco IronPort

Cisco Catalyst® Services Modules
Cisco IPS 4200 Series
Cisco ASA 5500 Series
Cisco Security Agent

Cisco Security Management Suite

Day-Zero Endpoint Protection

Branch-Office Protection

Converged Perimeter Protection

Integrated Data-Center Protection

Server Protection

Monitoring, Correlation, and Response

Policy-Based Solution Management

### Branch

- Converged branch protection
- Local content scanning to mitigate malware introduction
- Network Admission Control to prevent malware and enforce policy
- Router-based IPS to protect local clients and preserve bandwidth

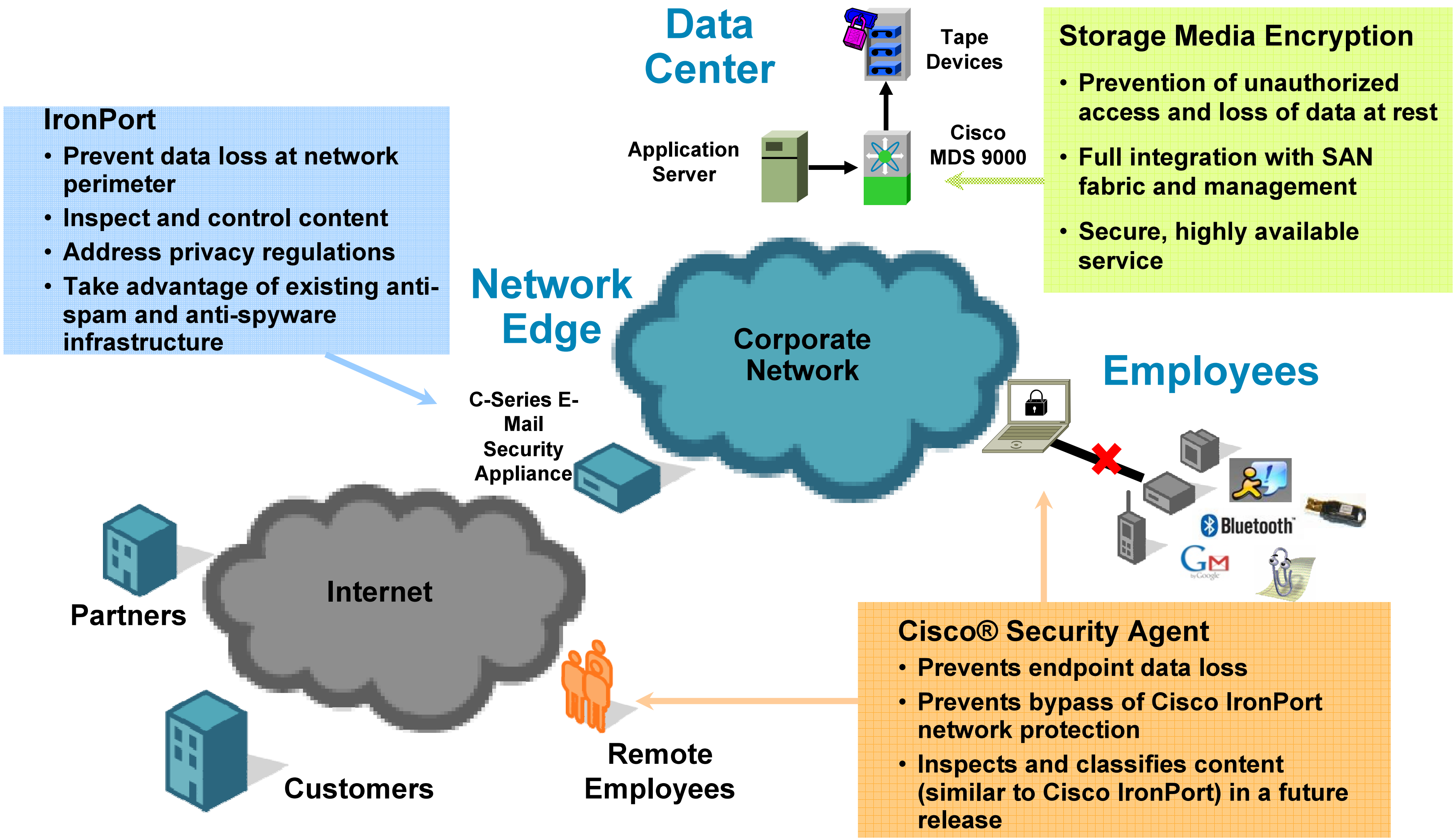
### Campus

- Endpoint protection from spyware, botnets, spam, and Trojan horses
- High-capacity Internet-edge security
- Inbound, outbound, and intra-LAN protection and control
- Content security and Network Admission Control to mitigate malware propagation

### Data Center

- High-capacity protection of servers and applications
- Application and protocol inspection to protect servers and systems
- Local server protection from targeted exploit attempts

# Preventing Data Leakage and Disclosure
## Self-Defending Network Applied



**IronPort**

- Prevent data loss at network perimeter
- Inspect and control content
- Address privacy regulations
- Take advantage of existing anti-spam and anti-spyware infrastructure

**Storage Media Encryption**

- Prevention of unauthorized access and loss of data at rest
- Full integration with SAN fabric and management
- Secure, highly available service

**Cisco® Security Agent**

- Prevents endpoint data loss
- Prevents bypass of Cisco IronPort network protection
- Inspects and classifies content (similar to Cisco IronPort) in a future release

## Slide 28

**BH10** should that C-Series label be: Cisco IronPort C-Series ....?

Bonnie Hupton, 11/29/2007

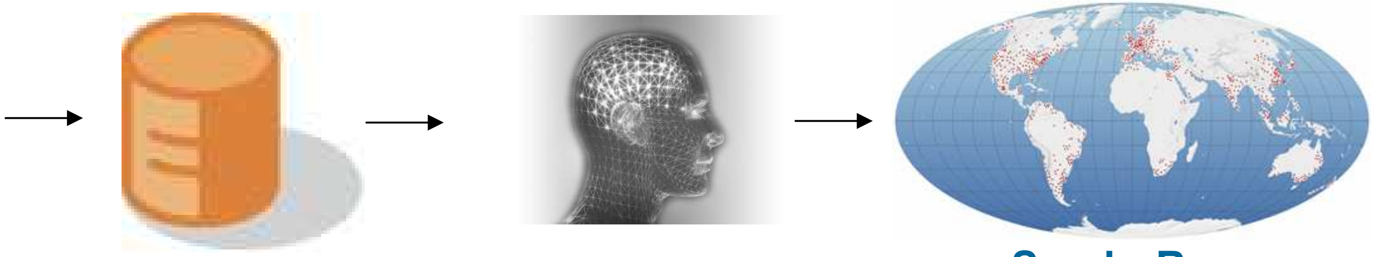
# Wide Traffic Inspection
# Real-Time Knowledge of Threat Environment

**150 Parameters**

- **Complaint reports**
- **Spam traps**
- **Message composition data**
- **Global volume data**
- **URL lists**
- **Compromised host lists**
- **Web crawlers**
- **IP blacklists and whitelists**
- **Additional data**

**The Dominant Force in Global E-Mail and Web Traffic Monitoring…**

- **5B+** queries daily
- **150+** e-mail and Web parameters
- **25%** of the world's e-mail traffic



**SenderBase Data**

**Data Analysis/ Security Modeling**

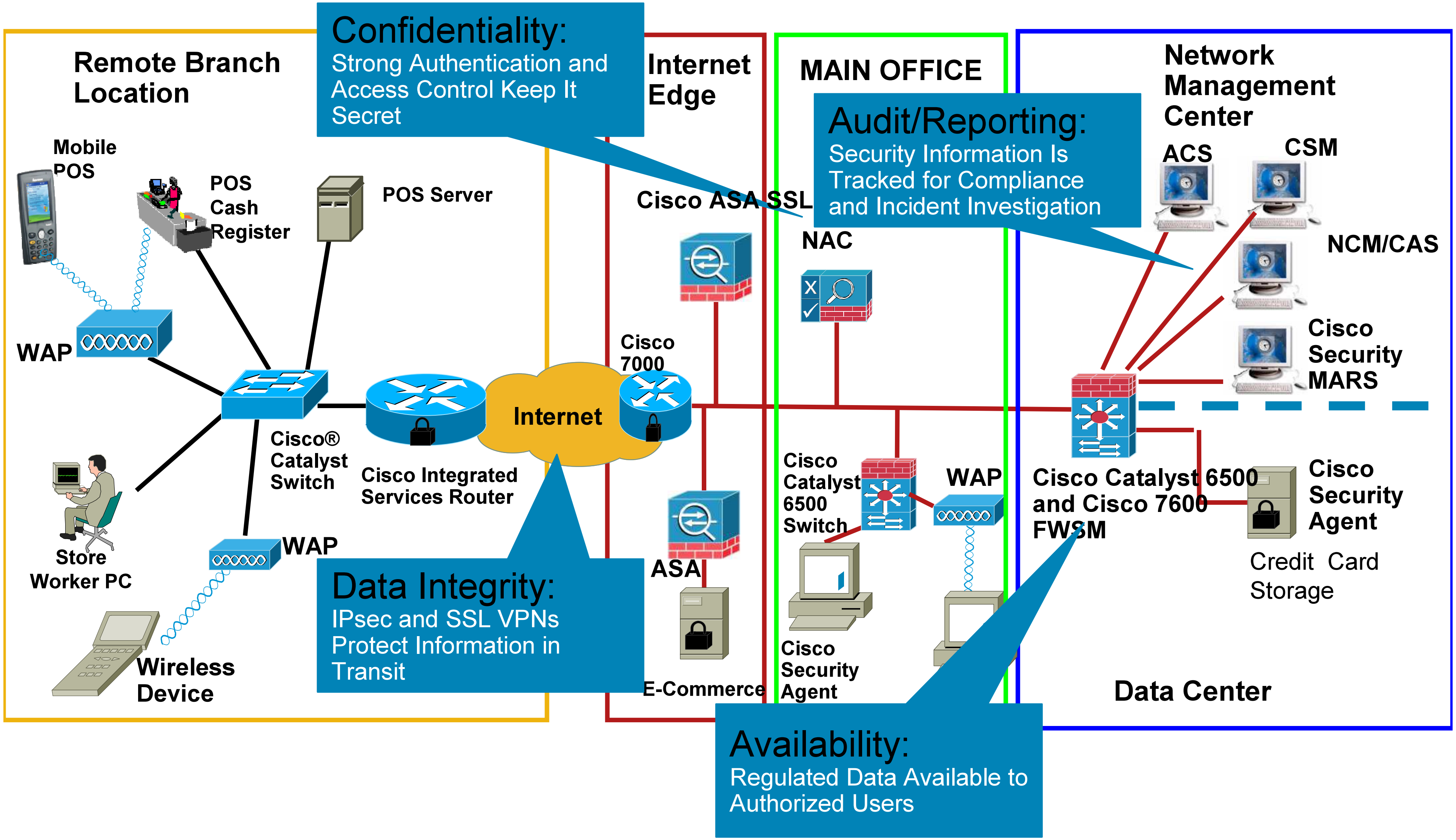
**SenderBase Reputation Scores –10 to +10**

## Slide 29

**BH23** is SenderBase correct? no space?

Bonnie Hupton, 11/29/2007

# Achieving Policy and Regulatory Compliance
## Self-Defending Network Applied



**Confidentiality:**
Strong Authentication and Access Control Keep It Secret

**Audit/Reporting:**
Security Information Is Tracked for Compliance and Incident Investigation

**Data Integrity:**
IPsec and SSL VPNs Protect Information in Transit

**Availability:**
Regulated Data Available to Authorized Users

# Securing the DataCenter

## Self-Defending Network Applied

### Data-Center Edge

- Firewall and IPS
- DoS protection
- Application protocol inspection
- Web Services security
- VPN termination
- E-mail and Web access control

### Web Access

- Web security
- Application security
- Application isolation
- Content inspection
- SSL encryption and offload
- Server hardening

### Applications and Database

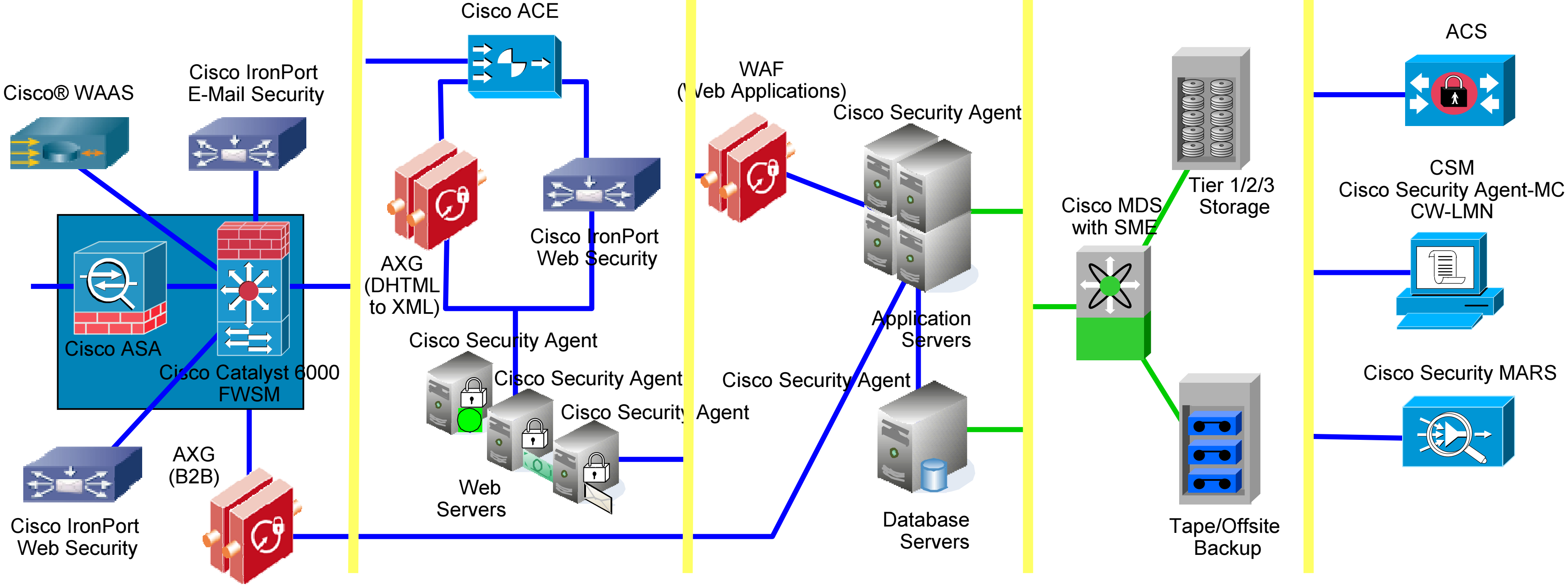
- XML, SOAP, and AJAX security
- DoS prevention
- Application-to-application security
- Server hardening

### Storage

- Data encryption
  - o In motion
  - o At rest
- Stored data access control
- Segmentation

### Management

- Tiered access
- Monitoring and analysis
- Role-based access
- AAA access control



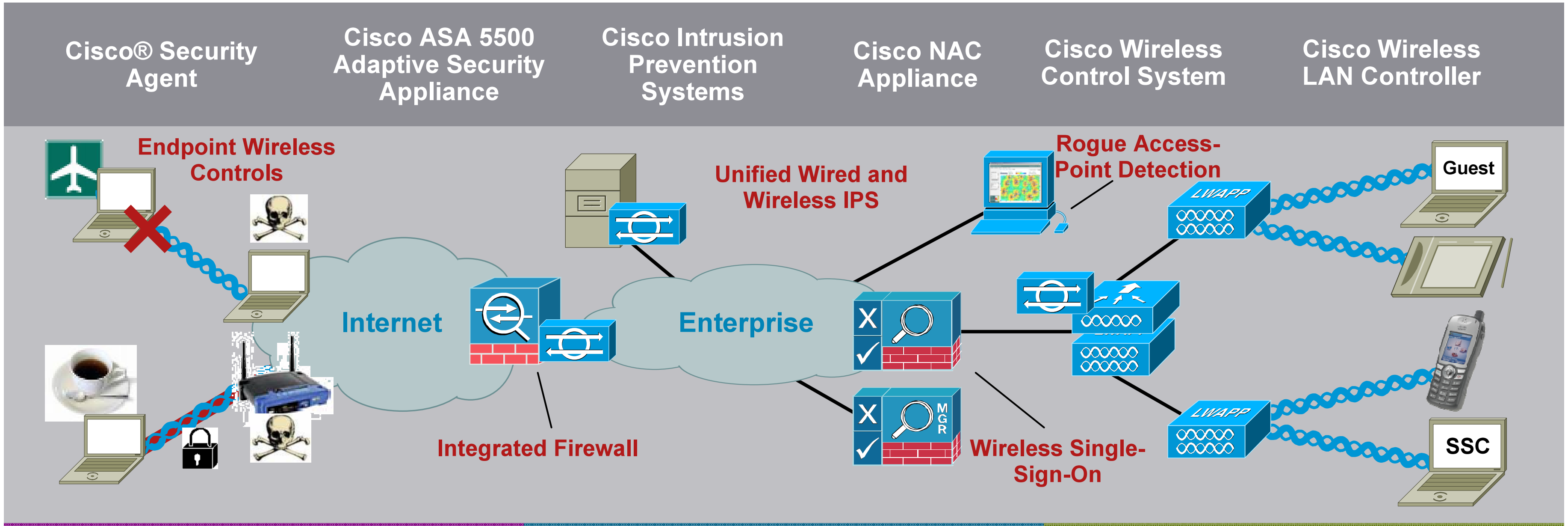
## Slide 31

**BH24** if CW stands for CiscoWorks, need to write it out. if CSM stands for Cisco S... M...... need to write that out, too.  Cannot use C for Cisco in acronyms for legal reasons

Bonnie Hupton, 11/29/2007

# Cisco Secure Wireless Solution

## Self-Defending Network Applied


Cisco® Security Agent
Cisco ASA 5500 Adaptive Security Appliance
Cisco Intrusion Prevention Systems
Cisco NAC Appliance
Cisco Wireless Control System
Cisco Wireless LAN Controller
Endpoint Wireless Controls
Unified Wired and Wireless IPS
Rogue Access-Point Detection
LWAPP
Guest
Internet
Enterprise
M G R
LWAPP
SSC
Integrated Firewall
Wireless Single-Sign-On

### Integrated

- Integrated baseline security capabilities into the wireless LAN infrastructure
- Built-in security intelligence and threat protection specific to wireless security threats

### Adaptive

- Anomaly detection with unified wired and wireless IPS/IDS architecture
- Real-time rogue-access-point detection and mitigation through automatic RF monitoring
- Host-based IPS wireless controls for mobile laptops

### Collaborative

- Unified wired and wireless IPS/IDS
- Enforced wireless security policy through single sign-on with NAC appliance

## Slide 32

**BH14** if RF stands for something besides radio frequency, pls write out

Bonnie Hupton, 11/29/2007

# Summary

- Threat evolution requires new thinking, new approach
- Network and Security Services: Works “better together”
- Cisco® SDN: Defining the System Solution for IT security