



# In the Human Network...

## Security is Everywhere



**Colin Bradley**  
**Advanced Technologies Lead for Security (ANZ)**  
[cobradle@cisco.com](mailto:cobradle@cisco.com)



# Agenda

- The Changing Threat Landscape
- Cisco's Security Strategy – the Self Defending Network
- Threat Control & Containment
- Technology & Solutions Update
- Summary

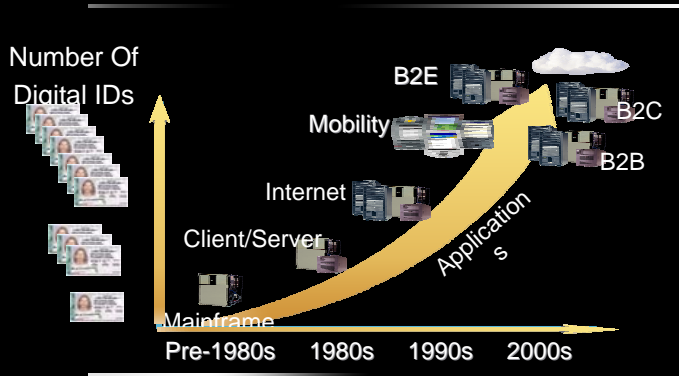


# Threat Trends...

## Why security is still a No.1 Business Priority

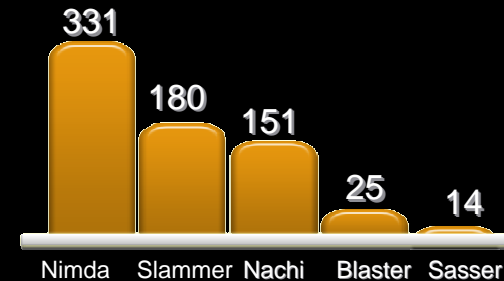
### Exponential growth of IDs

*Identity and access management challenging*



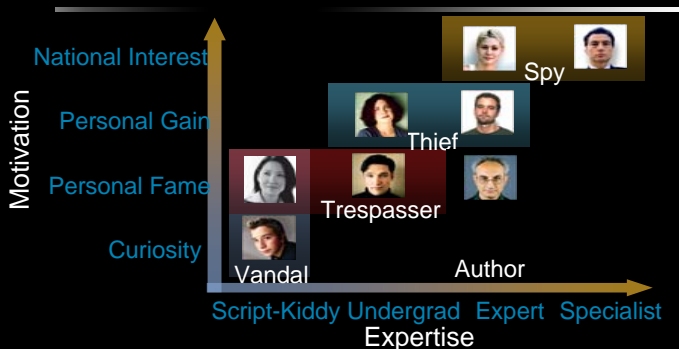
### Days from update to exploit decreasing

*Updating alone is not sufficient*



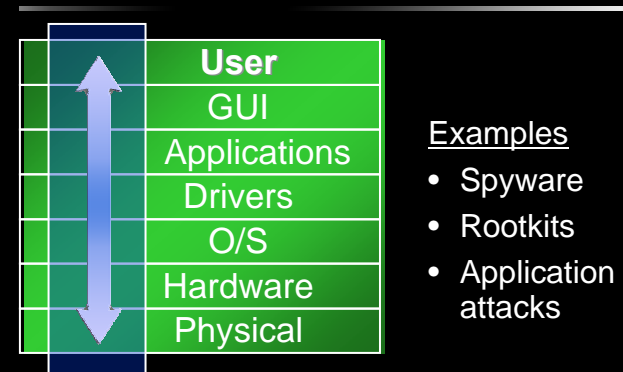
### Organized crime on the rise

*IP protection is critical*



### Attacks getting more sophisticated

*Traditional defenses are inadequate*



# Convergence, not a question of if but when! However, it does pose a new conundrum...



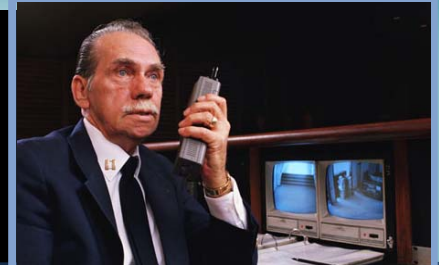
**Data**



**Voice**



**Video**



**Mobility**

**Infrastructure**

**Need to  
Balance  
Security**

**Security**

**IP**

**With  
QoS and  
Availability**

# Business Security Challenges



**Minimize Business  
Disruption and  
Information Asset  
Vulnerability**



**Meet Regulatory  
Compliance  
Requirements**



**Maximize the  
Efficiency of Limited  
IT Staff and  
Resources**

# The market is at an inflexion point:

- **New threats are being targeted at the application layer and specific individuals [Spear-Phishing etc]. So, greater need to re-focus on what's leaving the organisation and not what's coming in!)**
- **Convergence**
- **Consolidation & the “Microsoft Effect”**

# Spyware for Sale

## The New Corporate Espionage



- Ruth and Michael Haephrati charged with writing custom spyware for corporate intelligence gathering
- Michael Haephrati began developing the Trojan in 2000
- Wife Ruth Haephrati marketed it to three private investigation companies in 2004
- Leveraged both known and unannounced vulnerabilities on Windows systems
- Captured various data using standard behaviors: keystroke logging, screen capture, file transmissions, etc.

**"Organized criminals are hell bent on stealing information and making a profit. This case sends out a strong message that the menace of spyware is growing, and that companies need to realize that it's not just home users who are at risk."**

Source: TechWeb



# Doubt consolidation...

"The value of security as a standalone solution is diminishing."

RSA president Art Coviello said he was simply expressing the need for security "to be built more and more into an infrastructure....If I'm proven wrong about the timing [within three years], I won't be proven wrong in the need for this." but he did acknowledge, "There will always be a place for innovative startups."

RSA Conference, San Francisco, 7<sup>th</sup> February 2007



# Dispelling a Myth?

Is it more secure to use firewalls from two different vendors?

***“Enterprises should standardize on one firewall platform to minimize self-inflicted configuration errors. It's not more secure to use firewalls from different vendors instead of one to protect enterprise networks”*** – Greg Young, John Pescatore in Gartner Research Note (published 5<sup>th</sup> February 2007)

- \* Having two platforms greatly increases configuration and management problems
- \* The increasingly complex DMZ is increasing the complexity in the firewall rule base
- \* More than 99% of breaches are caused by firewall misconfigurations, not firewall flaws

# So, its time to change thinking. Its time to change the model....

- **Security solutions must have relevancy to convergence**
- **Increased productivity and return on investment must be leveraged from existing infrastructure solutions**
- **Eco-system will be proactive, anticipate, learn and adapt....become “Self-Defending”.**
- **Market trends are towards consolidation – Cisco and Microsoft are best placed to deliver in the new market**
- **Confidence and Trust are the only barriers!!!!**

# Agenda

- The Changing Threat Landscape
- **Cisco's Security Strategy – the Self Defending Network**
- Threat Control & Containment
- Technology & Solutions Update
- Summary



# Secure Everything



# Cisco Self-Defending Network

A systems approach leveraging the Network Platform



## Integrated

Enabling every element to be a point of defense and policy enforcement



## Collaborative

Collaboration among the services and devices throughout the network to thwart attacks



## Adaptive

Proactive security technologies that automatically prevent threats

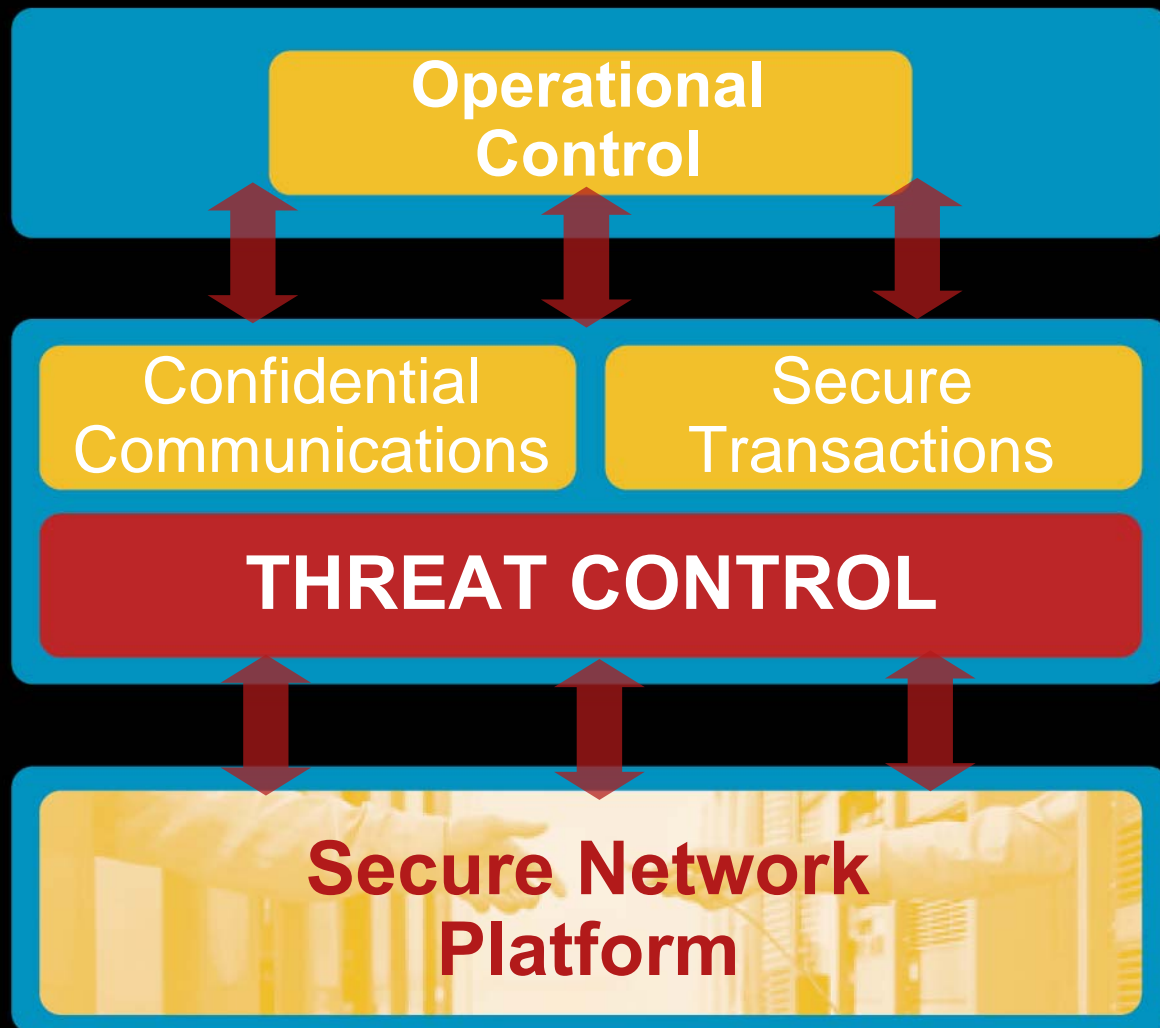
# Self-Defending Network Defined

**“You can’t do Security without understanding Networking”**

Efficient security  
management, control,  
and response

Technologies and  
security services to:

- Mitigate the effects of outbreaks
- Protect critical assets
- Ensure privacy
- Security as an integral, fundamental network capability
- Embedded security leverages network investment



# Agenda

- The Changing Threat Landscape
- Cisco's Security Strategy – the Self Defending Network
- **Threat Control & Containment**
- Technology & Solutions Update
- Summary

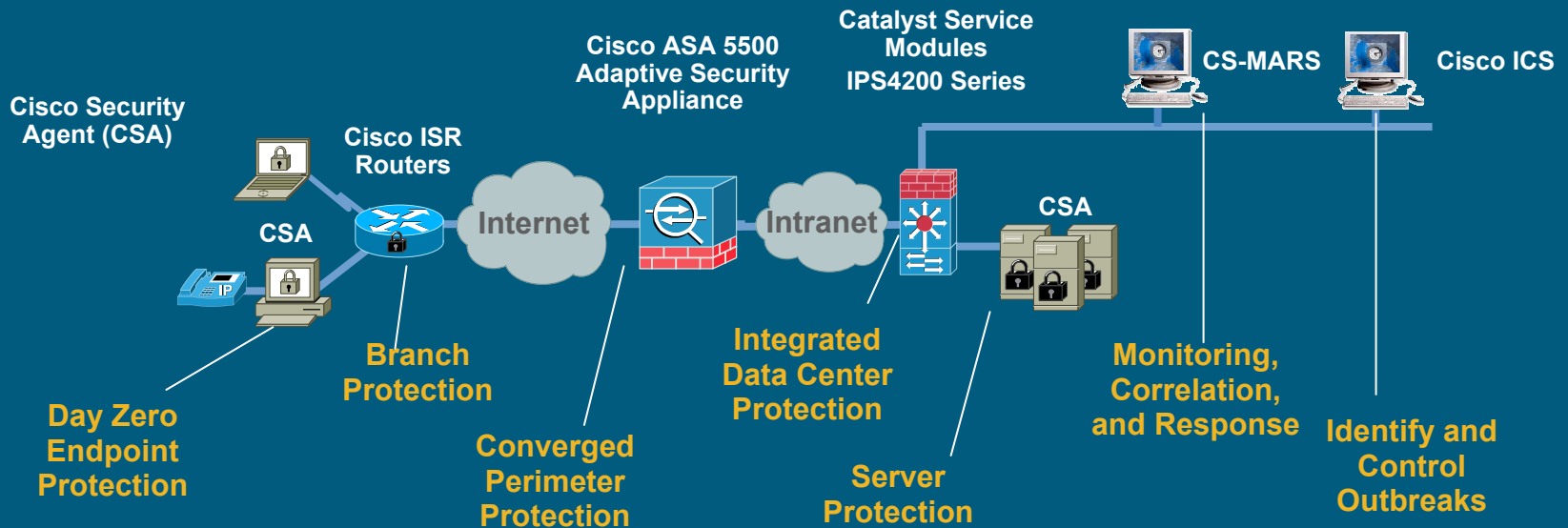




# Comprehensive Threat Protection

## Integrated

Multi-vector protections at all points in the Network, and Desktop and Server Endpoints



## Collaborative

- Cross-solution Feedback Linkages
- Common Policy Management
- Multi-vendor Event Correlation
- Attack path identification
- Passive/Active Fingerprinting
- CSA-IPS Collaboration\*

## Adaptive

- Anomaly Detection with In-Production Learning
- Network Behavioral Analysis
- On-device & Network Event Correlation
- Real-time Security Posture Adjustment
- Dynamic Signature Sets & Recognition
- Rapid Response

# Collaborative Systems Enabling Unparalleled Security

## 360° Visibility and Protection:

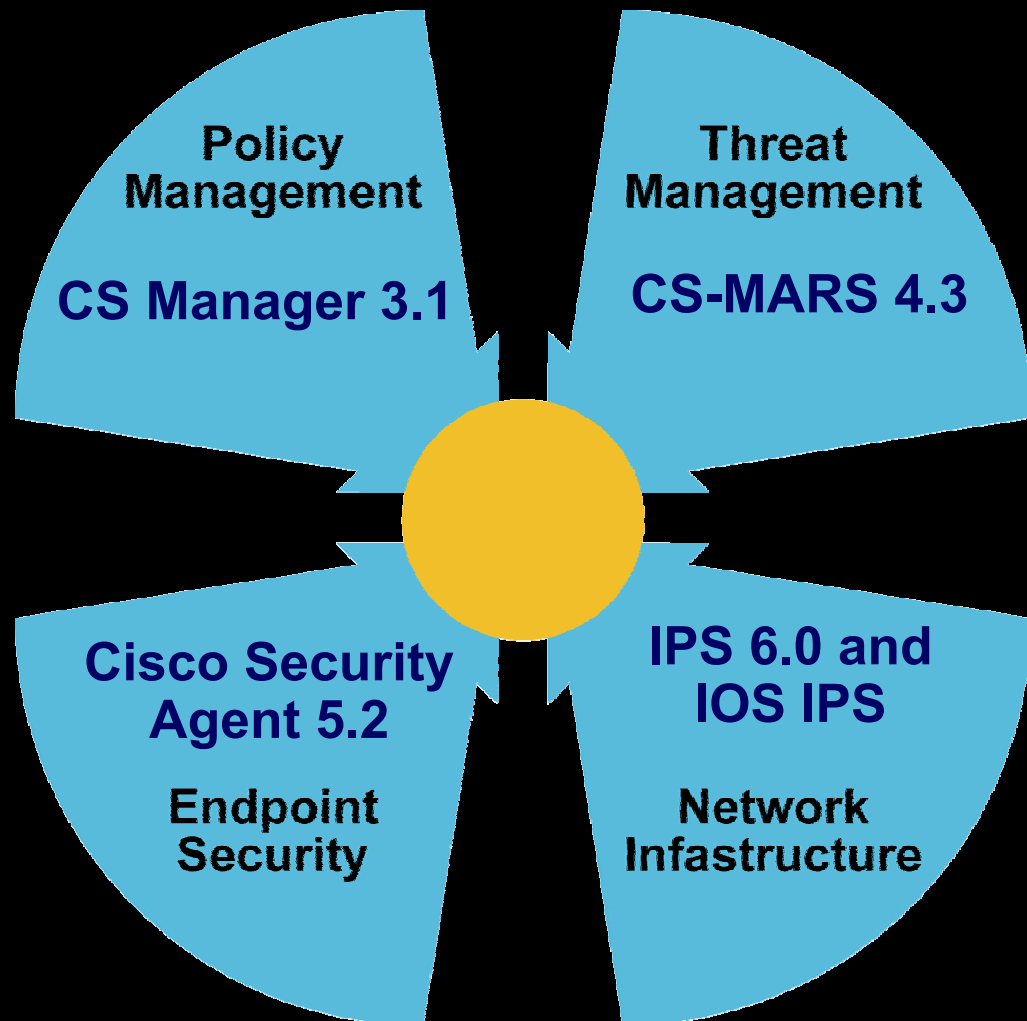
Delivering comprehensive and proactive network defence

## Simplified Control:

Streamlining policy and threat management across the network

## Business Resiliency:

Ensuring the enterprise's operations



# Enhancements in IPS 6.0

## Innovations in Intrusion Prevention

\* New in 6.0  
^ Unique to the Industry

### ■ Integrated

Multi-vector protections across the product portfolio in the Network, Desktop and Server Endpoints\*^

**Visibility into attack relevancy through passive OS fingerprinting\***

Static OS mapping to include environment specific OS assignments\*

Database Protection\*

Insight into user and endpoint credentials\*

### ■ Collaborative

Increased contextual analysis of endpoint\*

**Ability to use CSA Watch Lists to influence IPS actions\*^**

### ■ Adaptive

**Day Zero Anomaly Detection – system learns traffic patterns\***

Dynamic Risk Rating adjustment based on attack relevance\*^

Automated event and action filtering based on OS match\*^

- **Hardware Platforms:** All IPS4200 Sensors, ASA5500 Series AIP modules, Cisco Access Router NM-CIDS modules, and Catalyst IDSM-2 modules



\* New in 5.2  
^ Unique to the Industry

# CSA 5.2 Highlights

## Collaborative Security Enhances Threat Control

**CSA establishes endpoint-network relationship which enhances total network security**

- Application- and user-based QoS tagging ^
- QoS and wireless policy controls provide WIFI optimization and security\*
- Data Protection capabilities provide flexible policy control (eg. What can USB be used for?)
- CSA and IPS: Real-time information sharing providing improved signature fidelity \*^

CSA's QoS markings are specified as Differentiated Services Code Point (DSCP) values. As applied at the source, the host, and managed centrally by the CSA Management Center (CSAMC), enterprise trust boundaries can now be extended to grant conditional trust by posture assessment (via the use of NAC) to mobile stations without the fear of abuse from self-appraising applications (or users!). Cisco recommends the following suggestions for the QoS baseline as outlined in the "Enterprise QoS Solution Reference Network Design Guide" [http://www.cisco.com/application/pdf/en/us/quest/netso/ns432/c649/ccmigration\\_09186a008049b062.pdf](http://www.cisco.com/application/pdf/en/us/quest/netso/ns432/c649/ccmigration_09186a008049b062.pdf)

Application	Layer 3 Classification			Layer 2
	IPP	PHB	DSCP	CoS/MPLS EXP
IP Routing	6	CS6	48	6
Voice	5	EF	46	5
Interactive Video	4	AF41	34	4
Streaming-Video	4	CS4	32	4
Locally-Defined Mission-Critical Data (see note below)	3	—	25	3
Call-Signaling (see note below)	3	AF31/CS3	26/24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1

# Cisco Security Manager 3.1

“It has to be easy to use and flexible.”

- Different views for different administration preference
  - Device view
  - Topology view
  - Policy view
- One-stop shop for VPN discovery, creation and customization (IPSEC and SSL)
- Native IPS Policy Management on 4200, Catalyst, ASA, and ISR platforms
- Device manager cross-launch capability

The image displays three overlapping screenshots of the Cisco Security Manager 3.1 interface, each with a blue callout box identifying the view:

- Topology View:** Shows a network map with green areas representing networks. A callout box labeled "Topology View" is positioned over the top right of this screenshot.
- Policy View:** Shows a table of firewall rules for "FW-Policy - Default (29 Rules)". A callout box labeled "Policy View" is positioned over the top right of this screenshot.
- Device View:** Shows a table of firewall rules for "ASAS520-L3" assigned to 7 devices. A callout box labeled "Device View" is positioned over the top right of this screenshot.

The Policy View and Device View screenshots include the following tables:

No.	Permit	Category	Source	Destination	Service	Direction		
1	None	any	EngNet	dmz	tcp/588	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	any	SSH	outside	in	
8	✓	Cat-C	any	any	EngNet	Telnet	outside	in
9	✓	any	any	any	HTTP	outside	in	
10	✓	Cat-B	any	any	AB-ICMP	outside	in	
11	✓	any	any	any	ICMP-Echo-Reply	outside	in	
12	✓	any	any	any	PPTP-Control	outside	in	
13	None	133.2.6.0/28	10.2.2.2	10.1.1.100	H323-H225	outside	in	
14	✓	None	10.4.3.0/26	10.1.1.100	HTTP	outside	in	

No.	Permit	Category	Source	Destination	Service	Direction		
1	None	any	EngNet	dmz	tcp/588	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	any	SSH	outside	in	
8	✓	Cat-C	any	any	EngNet	Telnet	outside	in
9	✓	any	any	any	HTTP	outside	in	
10	✓	Cat-B	any	any	AB-ICMP	outside	in	
11	✓	any	any	any	ICMP-Echo-Reply	outside	in	
12	✓	any	any	any	PPTP-Control	outside	in	
13	None	133.2.6.0/28	10.2.2.2	10.1.1.100	H323-H225	outside	in	
14	✓	None	10.4.3.0/26	10.1.1.100	HTTP	outside	in	

# The Security Monitoring Challenge

*Always Too Late*

Network Operations



Security Operations



Action Steps:

1. Alert
2. Investigate
3. Mitigate

Collect Network Diagram  
Read and Analyze  
TONS of Data...  
Repeat

Firewall

10K Win,  
100s UNIX

IDS/IPS

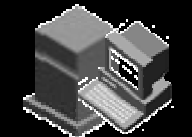
Antivirus

VPN

Router/Switch

Vulnerability  
Scanners

Authentication  
Servers



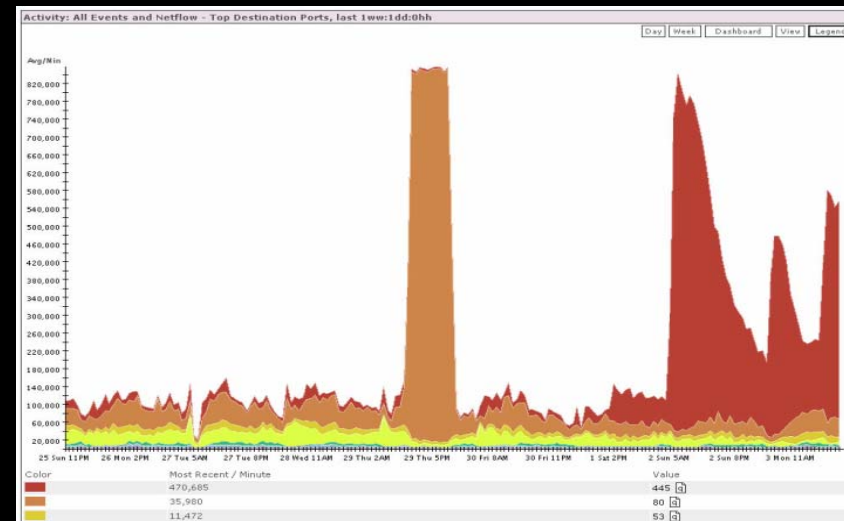
Security  
Knowledge-  
Base

# CS-MARS 4.3 (Monitoring, Analysis, and Response System)

## Operationalizing Threat Management

CS-MARS Transforms Raw Network and Security Data into Actionable Intelligence Used to Subvert Real Security Incidents, as Well as Maintain Corporate Compliance

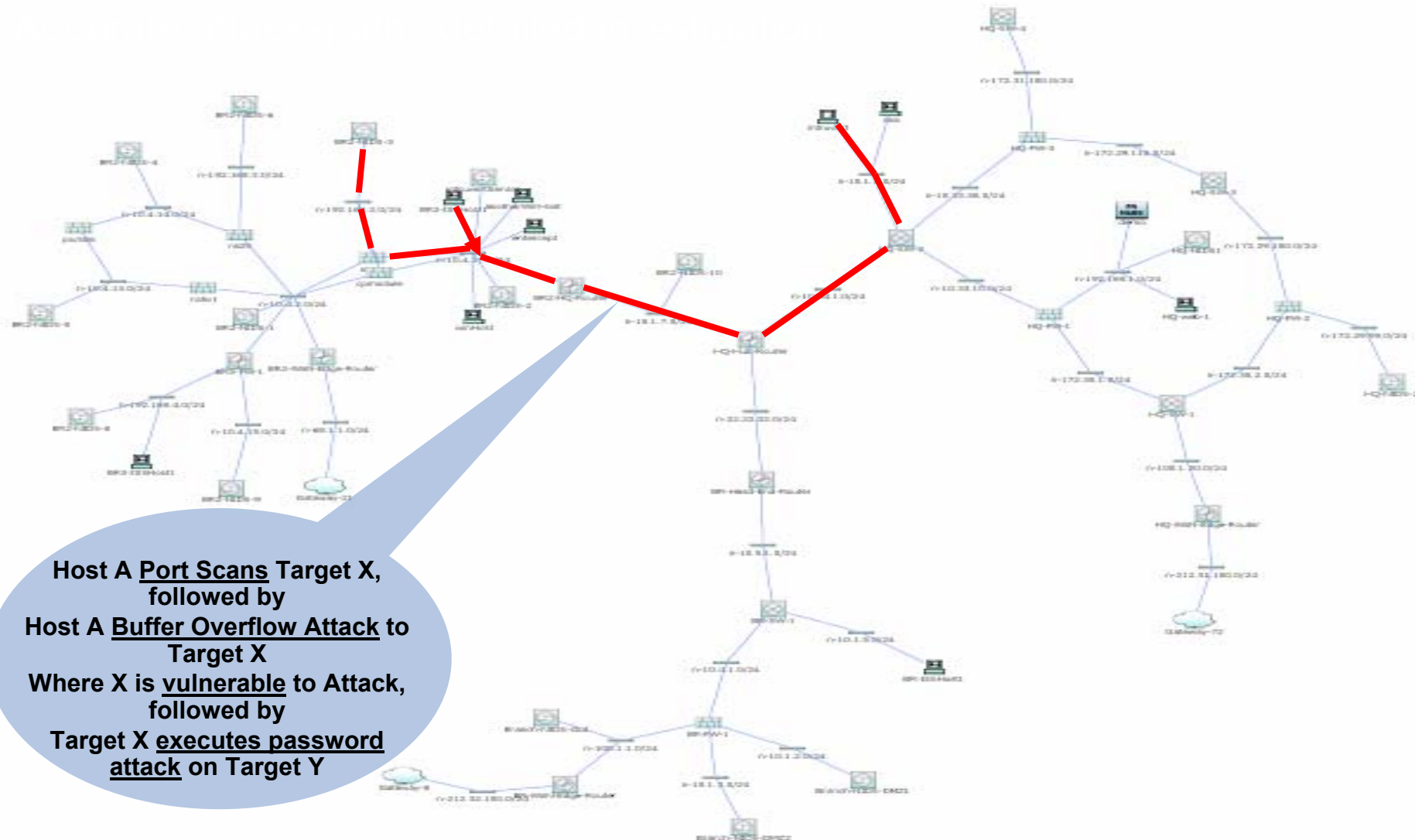
- Network-intelligent correlation
- Incident validation
- Attack visualization
- Automated investigation
- Leveraged mitigation
- Compliance management
- High performance
- Low TCO



Sasser Detection—  
Dynamic Visual Snapshot



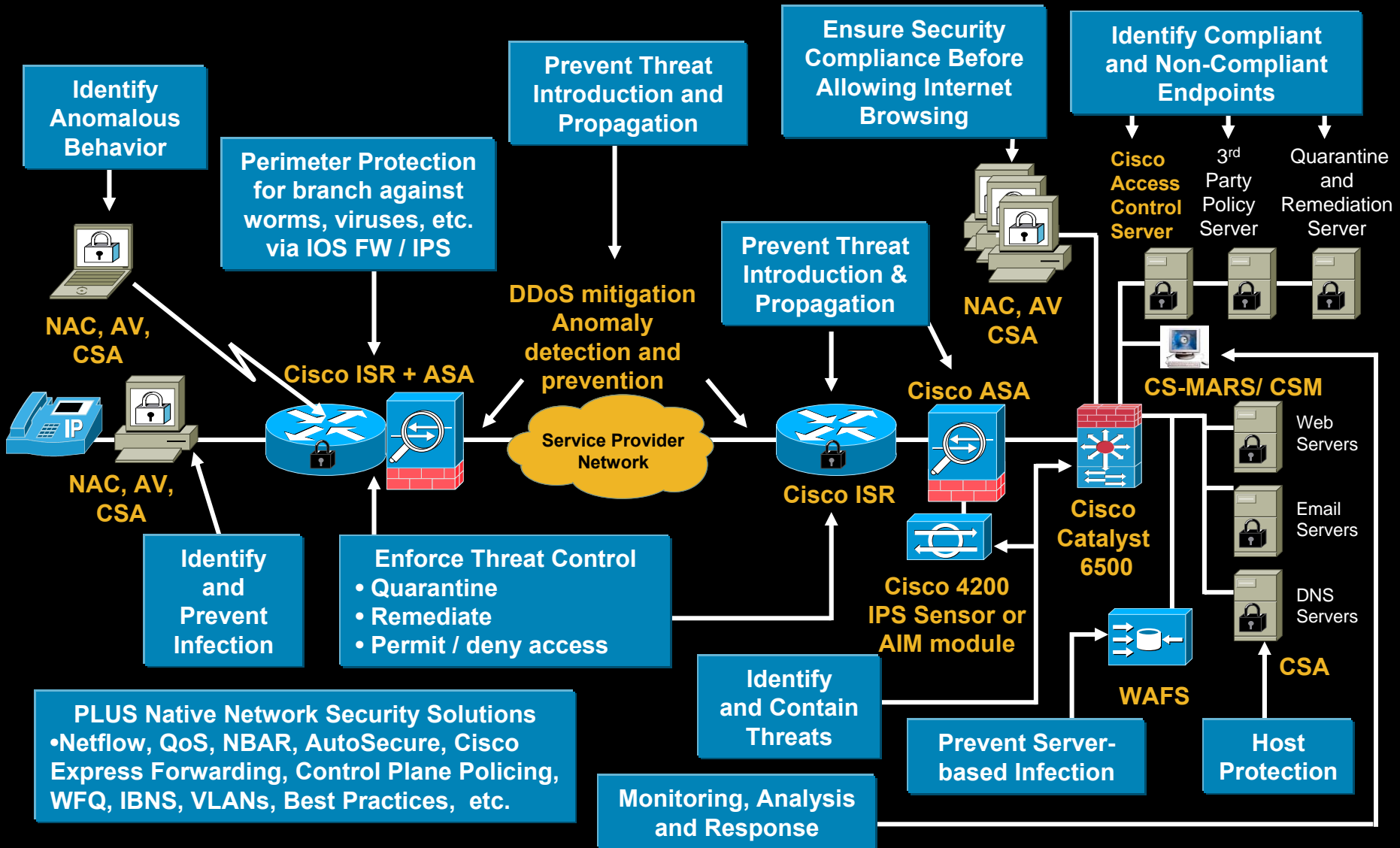
# CS-MARS: “Connect the Dots”



Host A Port Scans Target X,  
followed by  
Host A Buffer Overflow Attack to  
Target X  
Where X is vulnerable to Attack,  
followed by  
Target X executes password  
attack on Target Y

# Cisco Threat Control & Containment

## An End-to-End Security Architecture



# Cisco Threat Control and Containment



# Agenda

- The Changing Threat Landscape
- Cisco's Security Strategy – the Self Defending Network
- Threat Control & Containment
- **Technology & Solutions Update**
- Summary

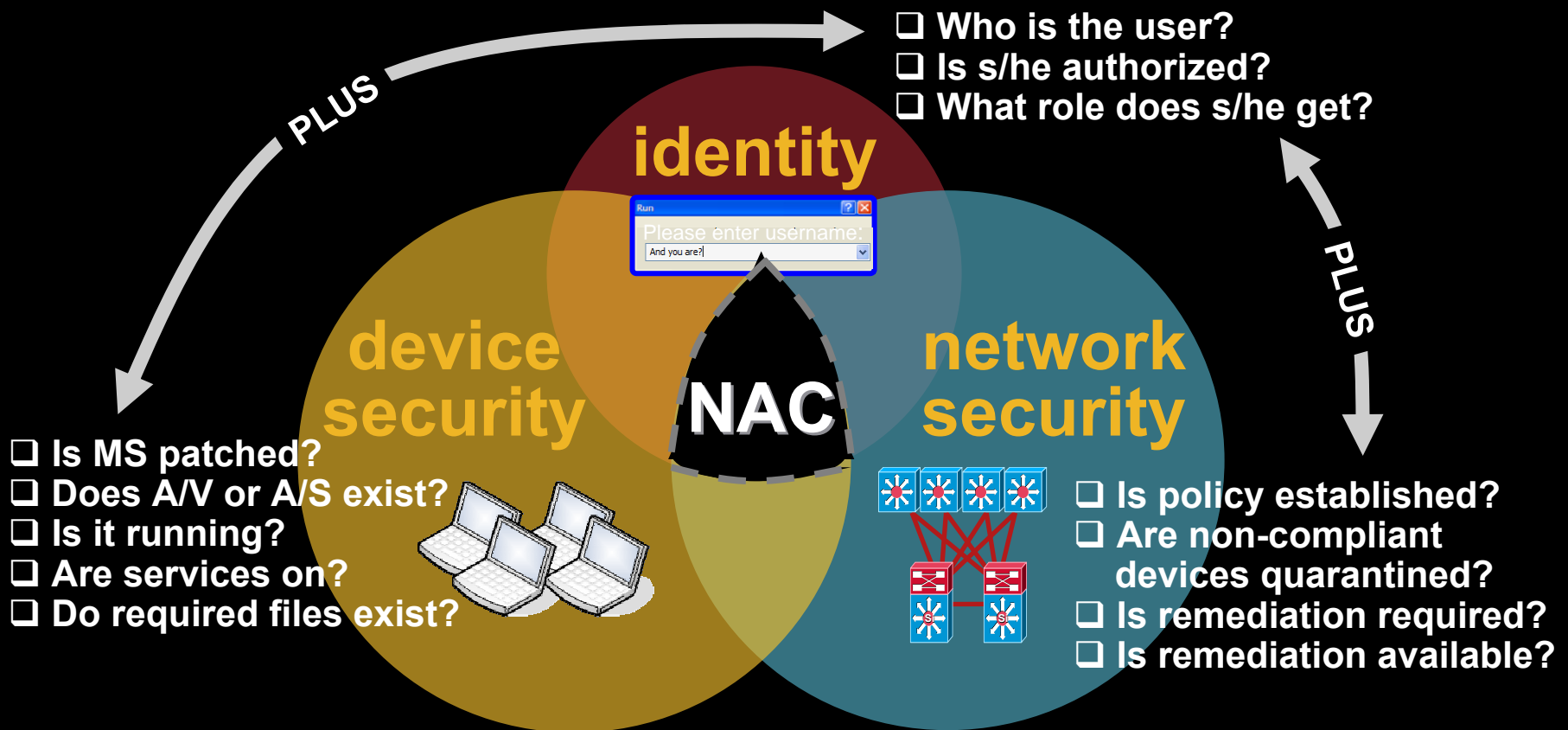


# Cisco NAC



# What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



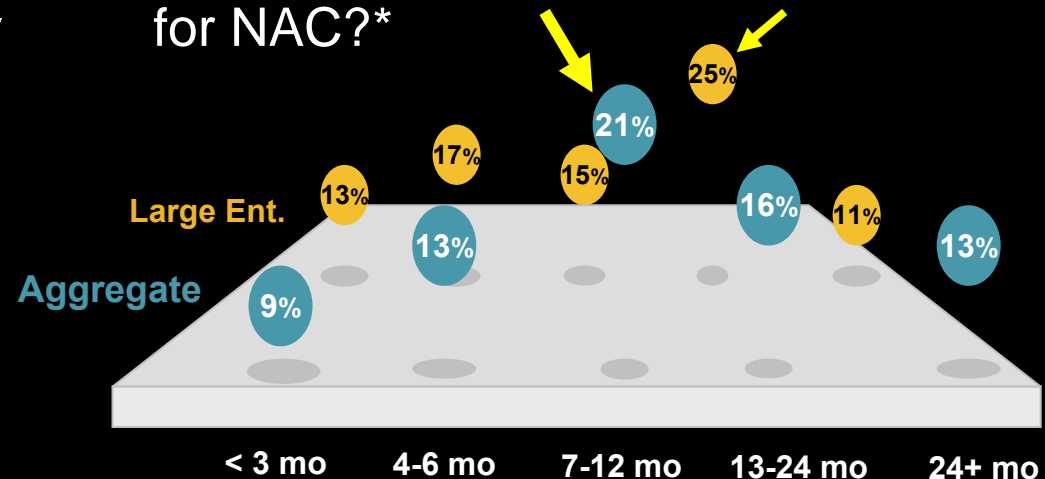
# 2007 Will Be the Year of Cisco NAC

## The Market Is Heating Up

- Now over **30 competitors**, includes many major security companies
- Infonetics estimates a **\$3.9 billion** market by 2008
- NAC is increasingly a **priority budget item**

## Customers Will Choose Soon

What Is Your Investment Horizon for NAC?\*



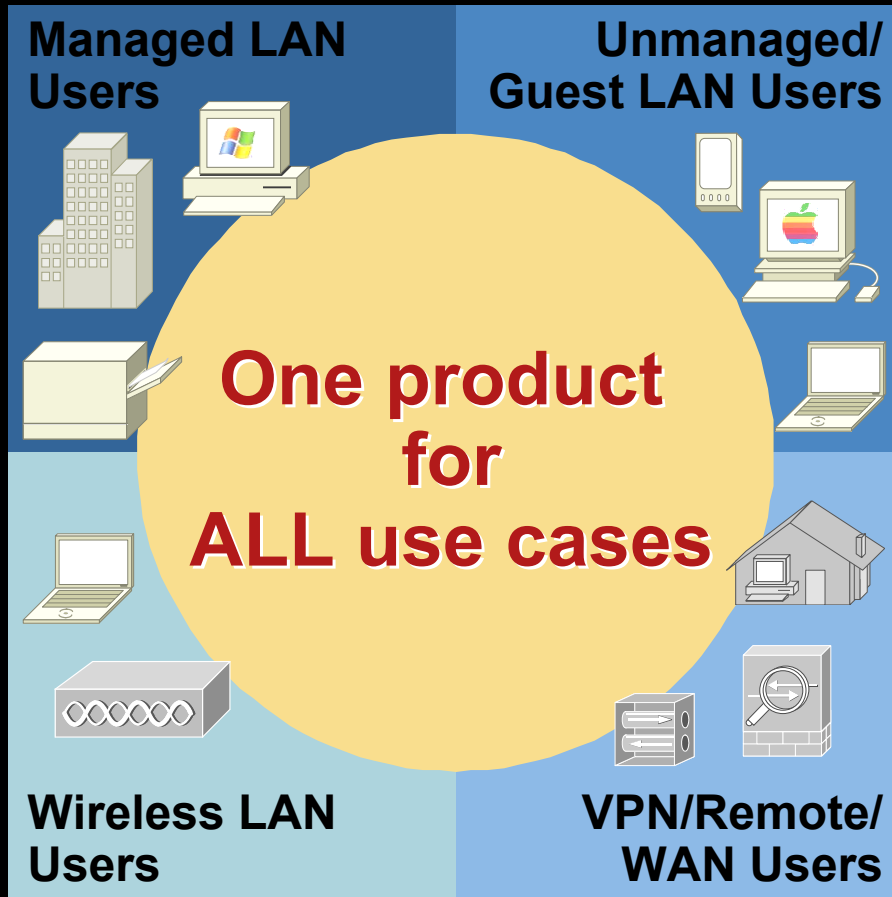
\* Source: Current Analysis, July 2006

## Capture Your Customer's NAC Budget



# The Cisco NAC Appliance Advantage

1.



2.

**1,200+ customers across all use cases: No. 1 NAC solution**

3.

**Most deployments ready under 5 days**

4.

**Scales from 100 users to 100,000+ user, across 150+ locations**

5.

**Does not require infrastructure upgrade**

## In September 2006, Cisco & Microsoft

- **Unveiled a NAC-NAP Joint Interoperable Architecture**
- **Provided a related technical white paper**
- **Outlined a general roadmap for when customers can implement interoperable components**
- **Demonstrated the interoperability at the Security Standards Conference**
- **Limited betas started late in calendar year 2006**
- **General production deployments to be supported by both Cisco and Microsoft when Windows Server “Longhorn” ships 2H 2007**

# ANZ NAP / NAC Delivery Strategy **Microsoft**

- Nirvana

Running Vista on all desktop devices and NAP / NAC framework components available across the entire infrastructure

Question: how quickly can you have all devices running Vista and have the whole network on 65xx/37xx/ISR etc from Cisco

- Stepping Stones

Use NAC Appliance to solve immediate pain points

Cisco Security Agent to protect and integrate legacy NT4 systems into an agreed NAP / NAC customer centric strategy

Use a combination of MSFT agents for Vista/XPSP2, Cisco Trust Agent for other devices (W2K, Linux, Solaris...)

IBNS (through 802.1x) as option to progress to NAC Framework implementation (Recognise, Assess, Enforce and Remediate).

- Will progress over time from stepping stone to Nirvana

# Router Security - Cisco ISR

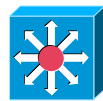


# All-in-One Security for the WAN

Only Cisco® Security Routers  
Deliver All This

Now with  
EAL4  
Certification

## Secure Network Services



Secure  
LAN



Secure  
Voice



Secure  
Wireless

## Perimeter Defense



URL  
Filtering



Application  
Firewall



IPS



Network  
Admission Control



NetFlow

## Secure Connectivity



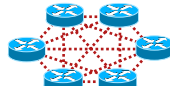
SSL  
VPN



IPsec  
VPN



DMVPN



GET  
VPN

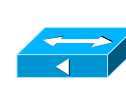
## Business Continuity



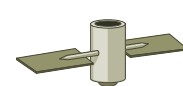
DSL



ISDN



Cable

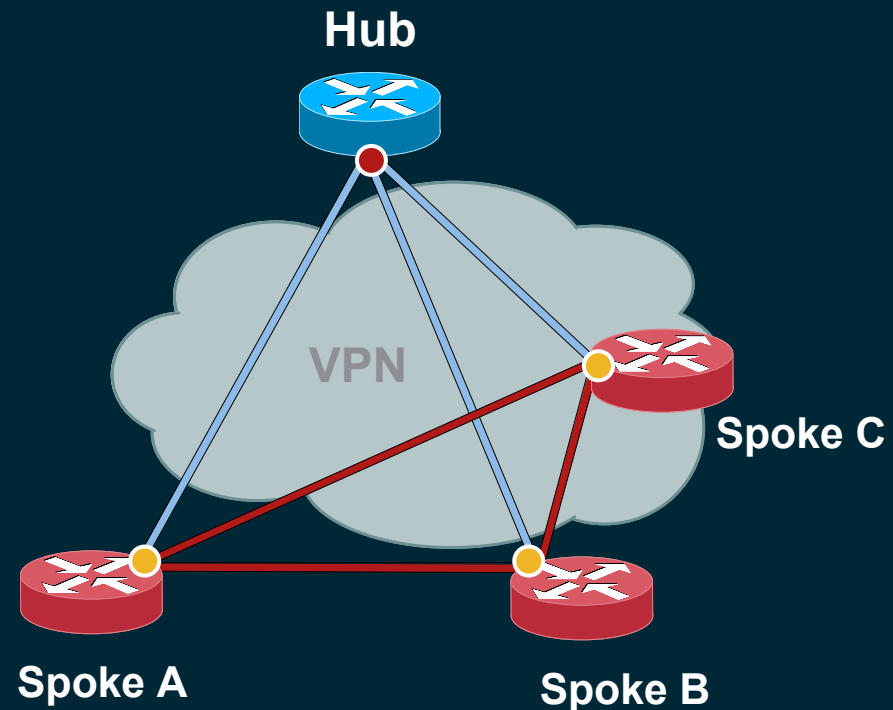


Satellite

# Dynamic Multipoint VPN (DMVPN) Secure Meshed Tunnels – Automatically!

## Dynamic Multipoint VPN Benefits:

- Fully Meshed connectivity with the configuration simplicity of hub and spoke VPN
- Preserves (central) bandwidth, minimizes latency



- = DMVPN Tunnels
- = Traditional Static Tunnels
- = Static Known IP Addresses
- = Dynamic Unknown IP Addresses

# IPS Overview on the ISR

- **Cost effective** IPS solutions for:
  - Branch offices & Telecommuters
  - SMB & Commercial customers
  - Managed Service offerings
- Can inspect traffic passing through any combination of LAN/WAN interfaces in both directions
- Closely integrated with other Cisco security solutions to deliver “Distributed Threat Mitigation”
- IOS-IPS supports / shares a subset of the signatures available on our dedicated IPS appliance & modules

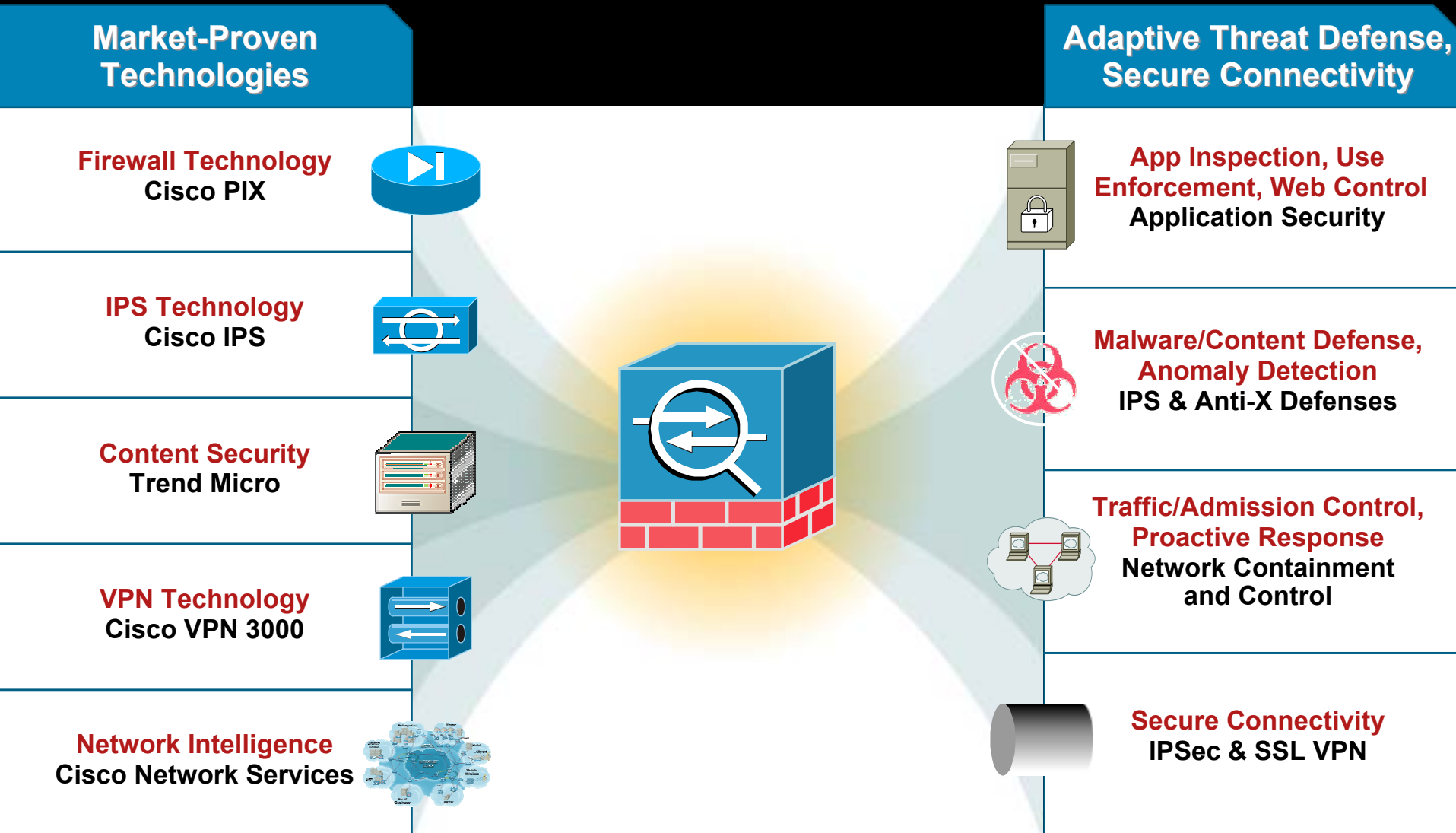


# Confidential Communications - The ASA 5500 Series

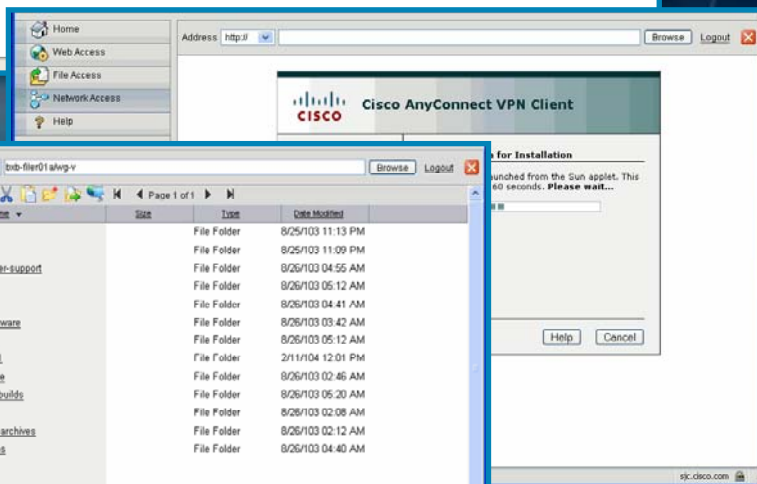
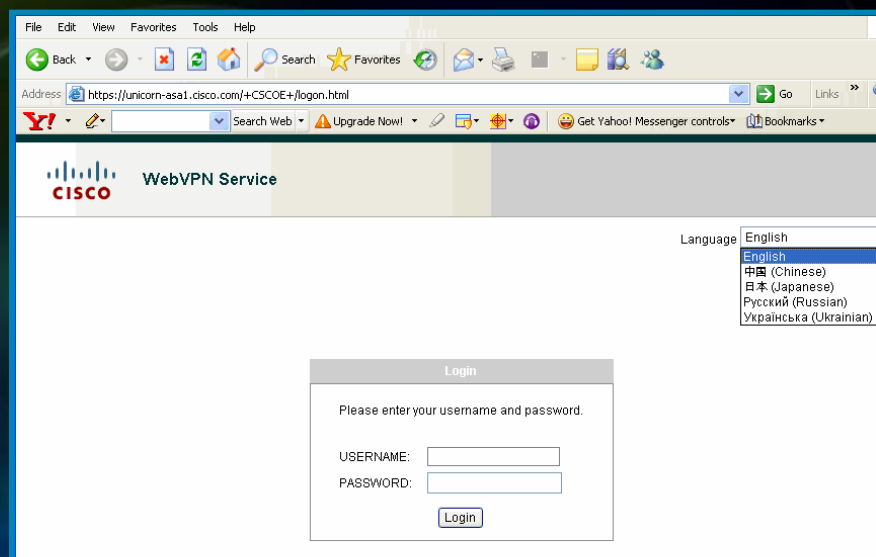


# Cisco ASA 5500 Series

## Convergence of Robust, Market-Proven Technologies



# Cisco ASA 5500 Software v8.0 Introduces Significant Enhancements in Clientless Access



- Precise, granular access control to specific resources

- Enhanced Portal Design

Localizable

RSS feeds

Personal bookmarks

AnyConnect Client access



- Drag and Drop file access and webified file transport

- Transformation enhancements including Flash support

# Cisco AnyConnect Client



- **Next generation VPN client, available on many more platforms including:**

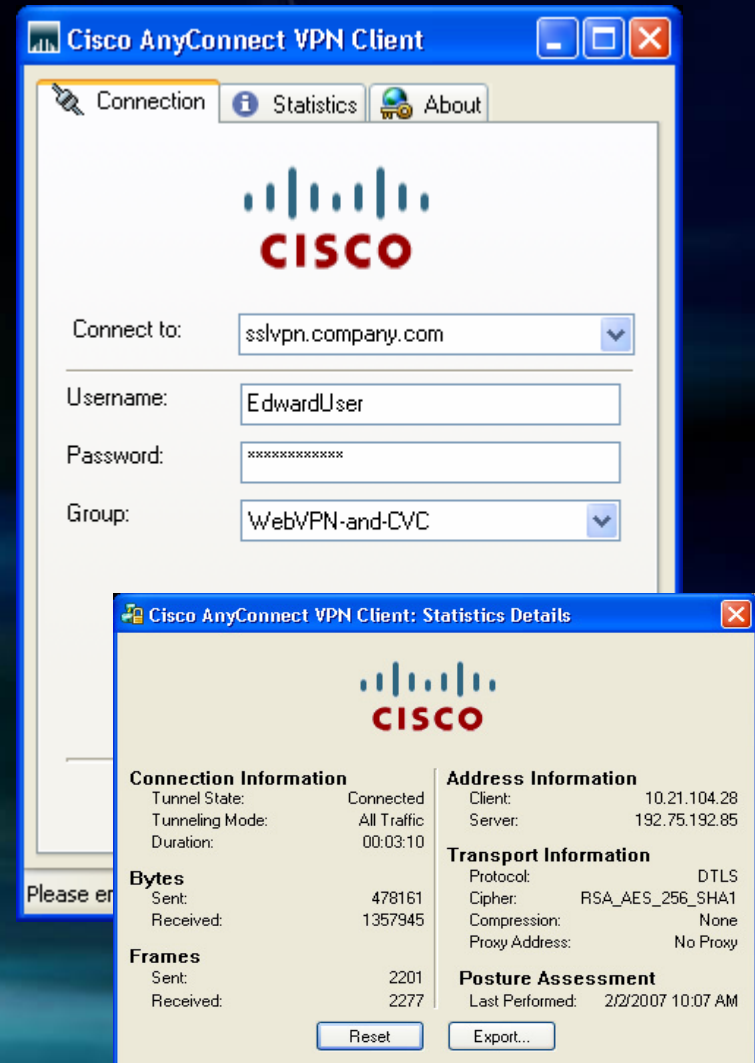
Windows Vista 32-bit, Windows XP 32- and 64-bit, and Windows 2000

Mac OS X 10.4 (Intel and PPC)

Intel-based Linux

Windows Mobile 5 Pocket PC Edition

- **Stand-alone, Web Launch, and Portal Connection Modes**



# Cisco ASA 5500 Series VPN Solutions

Enterprise-Class Site-to-Site VPN Capabilities

## Network-Aware Site-to-Site VPNs

### QoS-Enabled VPN

- Support for low latency queuing for latency-sensitive traffic such as VoIP

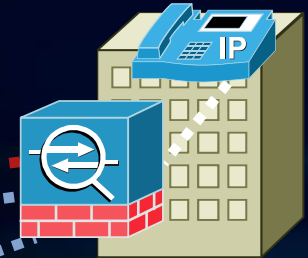
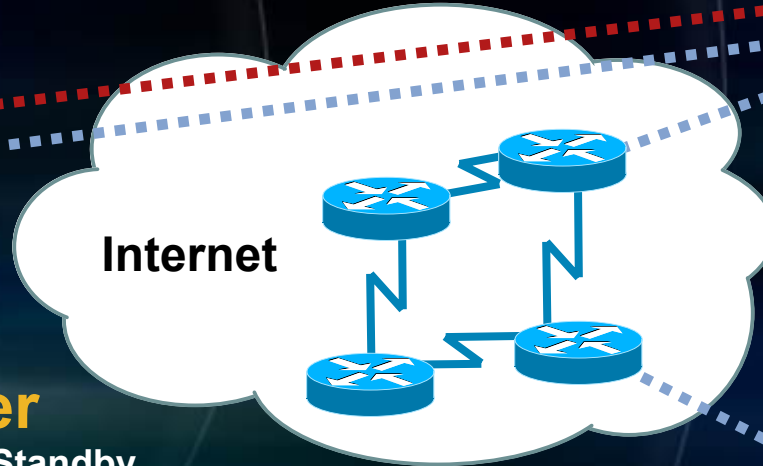


### IPSec Stateful Failover

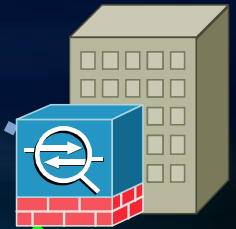
- Provides high performance Active-Standby failover with automatic key and SA information synchronization

### Robust X.509 Certificate Support

- Manual enrollment support (PKCS 7/10)
- n-tiered X.509 certificate chaining support
- 4096-bit RSA keysize support



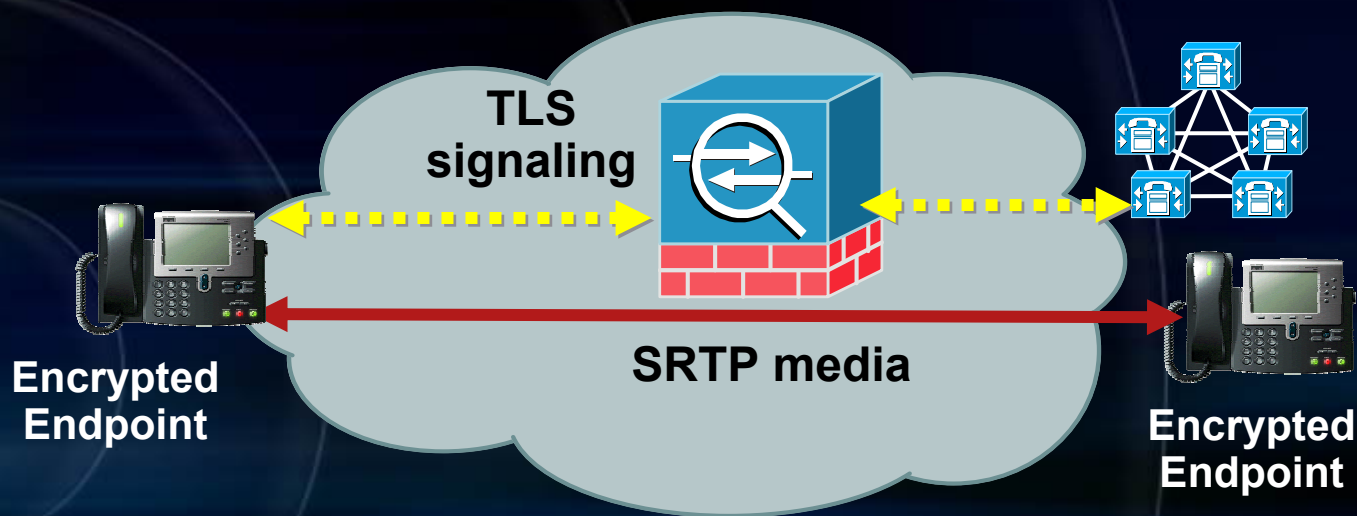
OSPF Routing Over VPN



# Industry-First Encrypted Voice/Video Security Solution

## Now Available with Cisco ASA 5500 Software v8.0

New  
in 8.0!



Any Cisco voice/video communications encrypted with SRTP/TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- **Maintains integrity and confidentiality** of call while enforcing security policy through advanced SIP/SCCP firewall services
- **TLS signaling is terminated and inspected**, then re-encrypted for connection to destination (leveraging integrated hardware encryption services for scalable performance)
- Dynamic port is opened for SRTP encrypted media stream, and automatically closed when call ends



# Cisco Adaptive Security Appliance



# Cisco Secure Wireless





# Cisco Secure Wireless Solution

An architecture that builds on the inherent security of the Cisco Unified Wireless Network to combine best of breed security services for unparalleled control of business resources to meet compliance needs

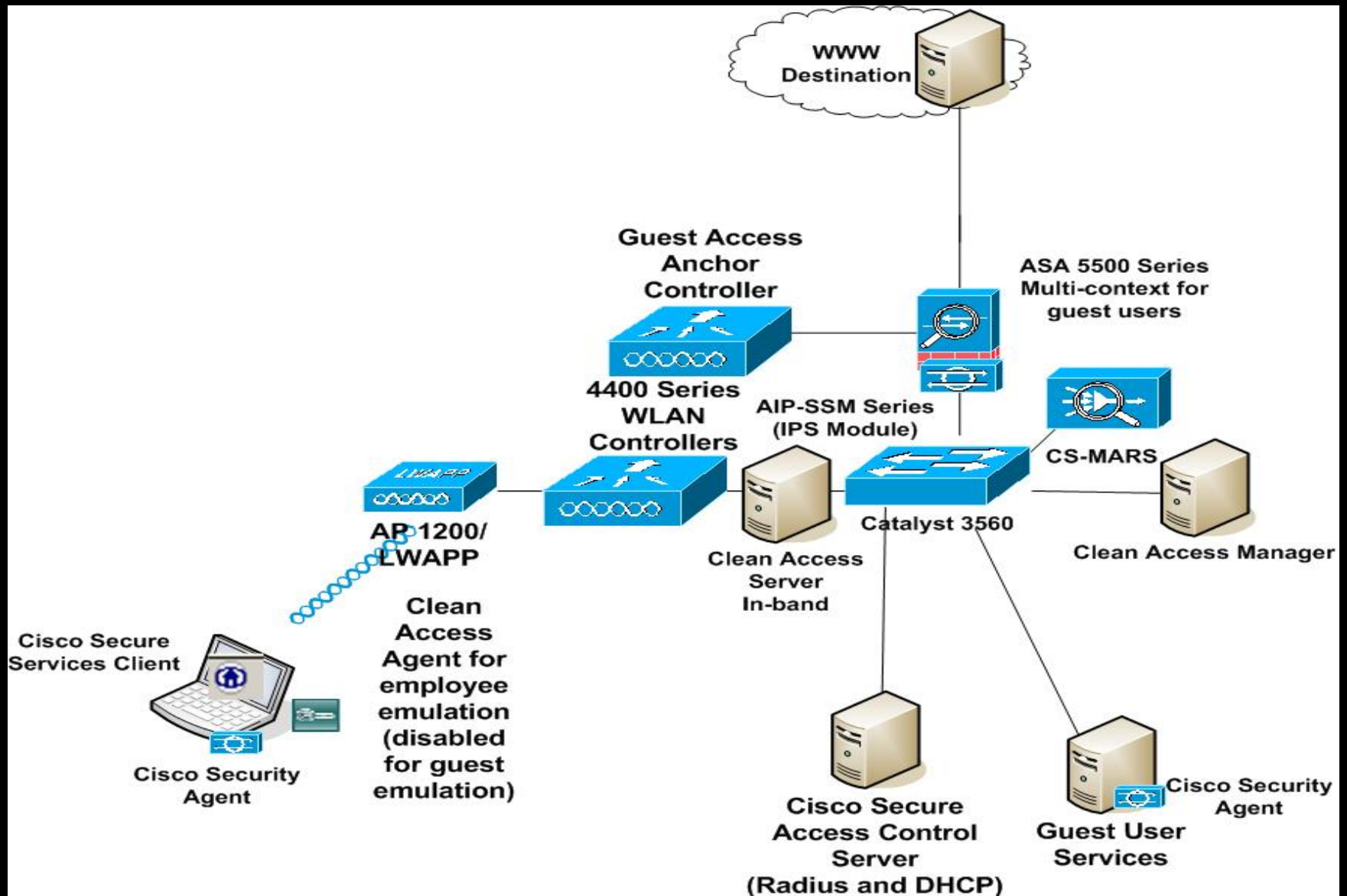
## What's New?

- An end-to-end architecture
- Integration of wireless and security products
- A solution far superior to that of any wireless competitor

## Key Features

- Unified wired & wireless IPS/IDS
- Client validation, posture assessment and remediation
- Wireless single sign on & 802.1X integration
- Can be integrated with firewalls for secure guest access
- L2, L3-7 & Host intrusion prevention
- Automatic rogue detection via RF monitoring

# Secure Wireless Solution Architecture



# Cisco Secure Unified Communications



## Protect Your Most Vital Asset

# The Good News....

1

Included as features in Cisco UC Products (ex: Encryption)



2

Included in networking products (ex: VLAN)



3

Security things you should do anyway (ex: Firewalling, IPS)



# Protect All Levels of IP Communications

**Applications**

**Value-Added Components**



**Messaging, Customer Care,  
and Other Application Software**

**Endpoints**

**User Interfaces**



**IP Phones, Video Terminals,  
and Other Delivery Devices**

**Call Control**

**System Config and Operation**



**Infrastructure and Protocols for  
Call Management and Operation**

**Infrastructure**

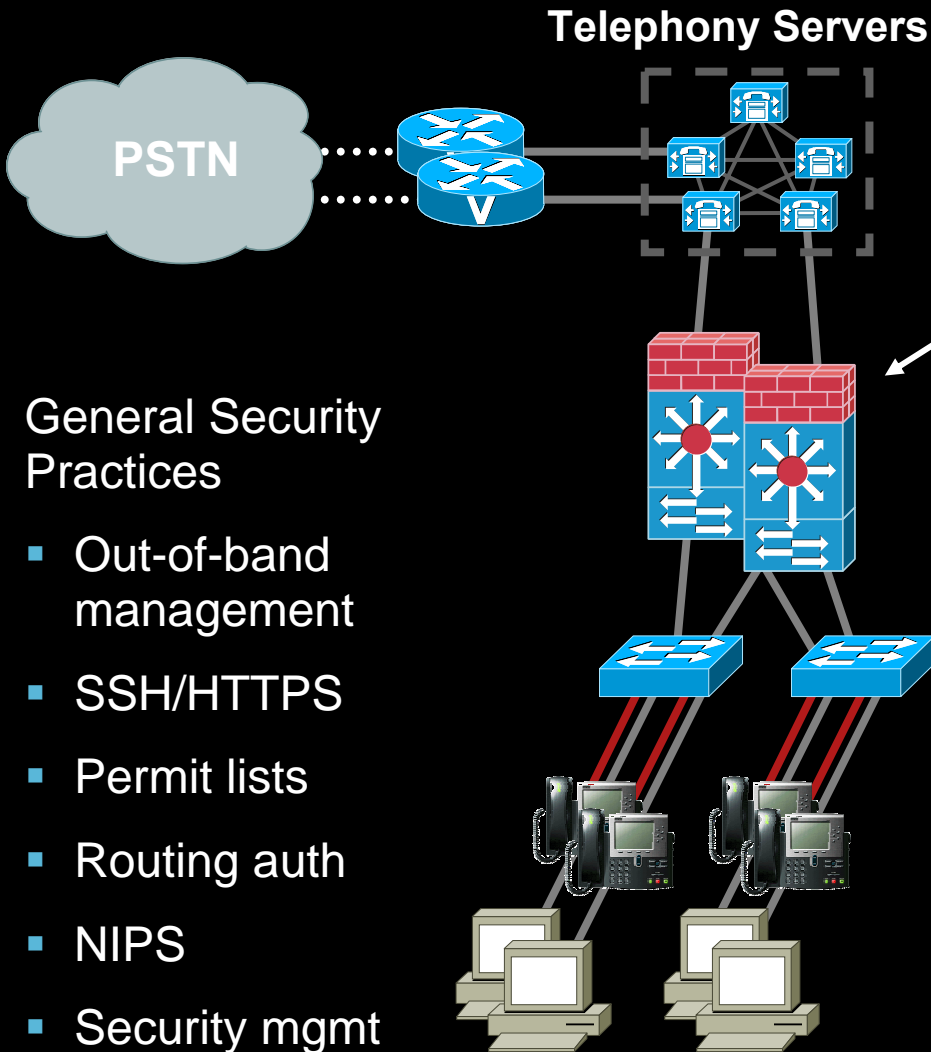
**Transport**



**Secure, Reliable  
Communications that Connects  
All of the Other Components**

**IP  
Communications  
System**

# Secure Voice by First Securing the Network



## General Security Practices

- Out-of-band management
- SSH/HTTPS
- Permit lists
- Routing auth
- NIPS
- Security mgmt

- Firewalls in front of telephony servers
- Rate Limiting in Cat6k

## Catalyst Integrated Security Features (CISF)

- Separate voice & data VLANs
- VLAN ACLs (VACLs)
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- Scavenger-class QoS

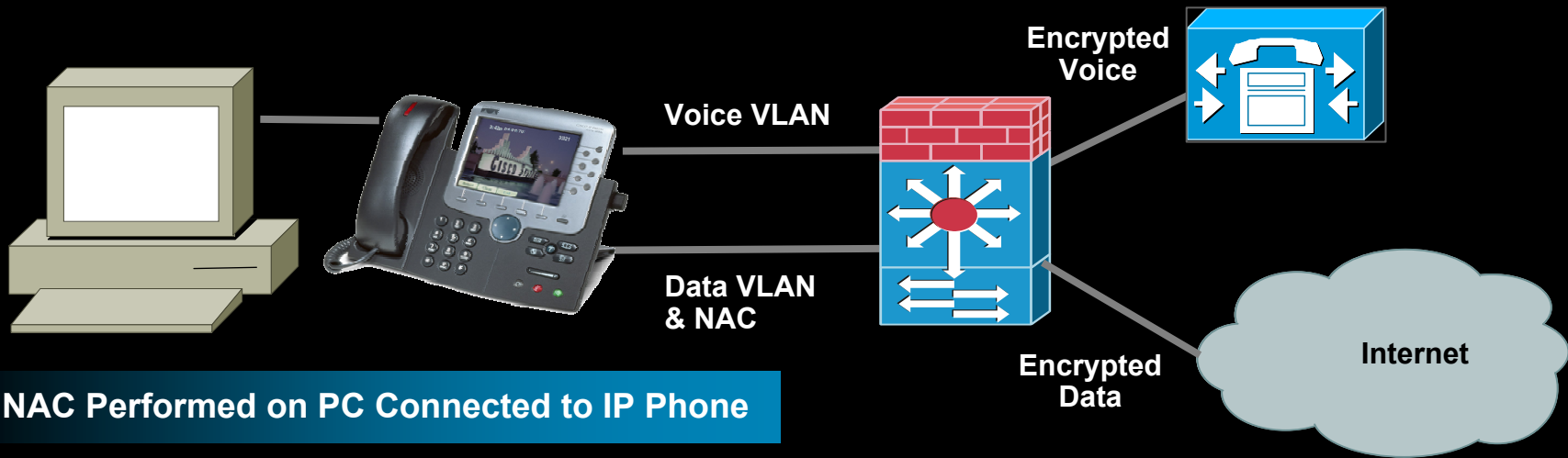
# Deployment of Security Features Is a Balance Between Risk and Cost

Cost—Complexity—Manpower—Overhead

Bronze	Silver	Gold
Default, Easy, No-Brainer	Moderate, Reasonable	Increasing Complexity
Basic Layer 3 ACLs	Simple Firewalls	Application Firewalls
Standard OS Hardening	Rate Limiting	NAC / 802.1X
Unmanaged CSA	Catalyst® Integrated Security	Network Anomaly Detection
Antivirus	VPN—SOHO/Mobile	Security Info Management
HTTPS	Optional OS Hardening	Trusted Endpoint QoS
SLDAP	Managed CSA/VMS	
Signed Firmware and Configs	Directory Integration	
Phone Security Settings	TLS / SRTP to Phones	
	IPSec / SRTP to Gateways	



# The Power of Cisco Integration



**NAC Performed on PC Connected to IP Phone**

**Phone authenticated with X.509  
Phone provides automatic VLAN segmentation (Voice, Data)  
Firewall functionality within the switch  
Traffic prioritized with QoS on the network**

**Encrypted voice and data routed on network**

**Call Management and Operation for Encrypted Voice**

**Only Cisco offers a comprehensive systems approach to unified communications security.**



# Partner Enablement



# Partner Enablement Today

## *Demands Continue to Accelerate...*



# FY'07 Priorities and Strategies

## Selling & Marketing

- Consistent & Complete Launch Packages
- Across Sales Cycle
- PE Engagement Playbook
- Building a Practice Playbooks
- Managed Services

## Training

- Consistent Framework & Learning Roadmaps
  - Sales, Technical & Lifecycle Services
- Efficient & Consistent Infrastructure
- Best Practice Sharing
- Global Reach

## Tools & Methodologies

- Close AT & Commercial Tool Gaps
  - Quoting
  - Implementation
  - Support
- Methodologies:
  - Assessment
  - Gap Analysis
  - Project Plan

# 'Must Have' Partner Enablement Tools

## ▶ Pre/Sales Tools

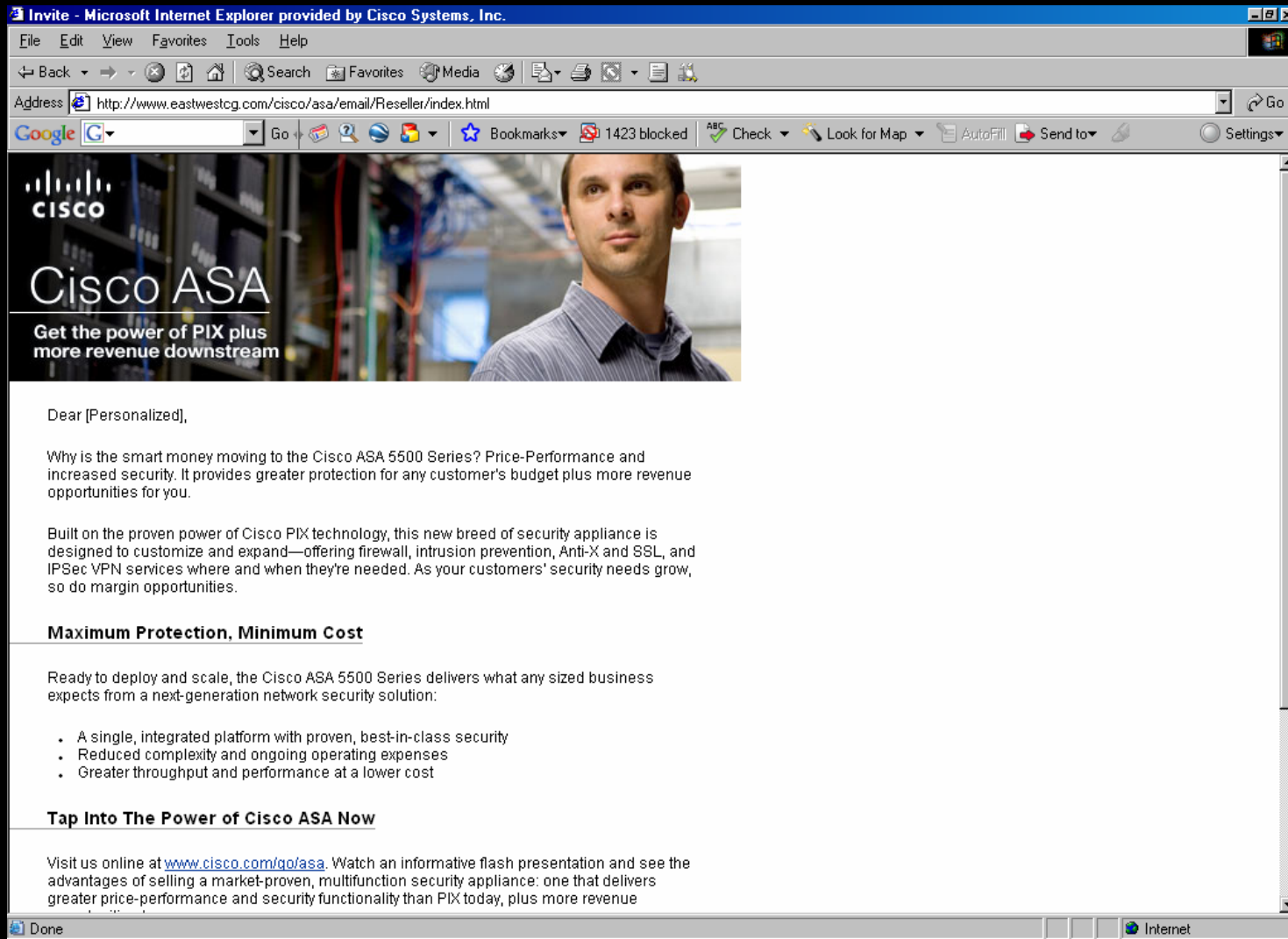
- Discovery
- Solution Expert
- Quote Builder
- Step-to-Success
- PDI Help Desk
- Partner Presales
- PEC (E-Learning)

## ▶ Marketing Tools

- Sales Accelerator
- Competitive Edge Portal
- Customized Partner Intelligence (CPI)
- Collateral-on-Demand



# The Power of PIX...PLUS




Invite - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address <http://www.eastwestcg.com/cisco/asa/email/Reseller/index.html>

Google  Go

Bookmarks 1423 blocked Check Look for Map AutoFill Send to Settings

 **Cisco ASA**  
Get the power of PIX plus more revenue downstream

Dear [Personalized],

Why is the smart money moving to the Cisco ASA 5500 Series? Price-Performance and increased security. It provides greater protection for any customer's budget plus more revenue opportunities for you.

Built on the proven power of Cisco PIX technology, this new breed of security appliance is designed to customize and expand—offering firewall, intrusion prevention, Anti-X and SSL, and IPSec VPN services where and when they're needed. As your customers' security needs grow, so do margin opportunities.

**Maximum Protection, Minimum Cost**

Ready to deploy and scale, the Cisco ASA 5500 Series delivers what any sized business expects from a next-generation network security solution:

- A single, integrated platform with proven, best-in-class security
- Reduced complexity and ongoing operating expenses
- Greater throughput and performance at a lower cost

**Tap Into The Power of Cisco ASA Now**

Visit us online at [www.cisco.com/go/asa](http://www.cisco.com/go/asa). Watch an informative flash presentation and see the advantages of selling a market-proven, multifunction security appliance: one that delivers greater price-performance and security functionality than PIX today, plus more revenue

Done Internet

# Q4 - AIM Sales Tools & Resources Kit

Kit to be provided for channel partners to leverage after training. Contents include:

## -Learning Resources

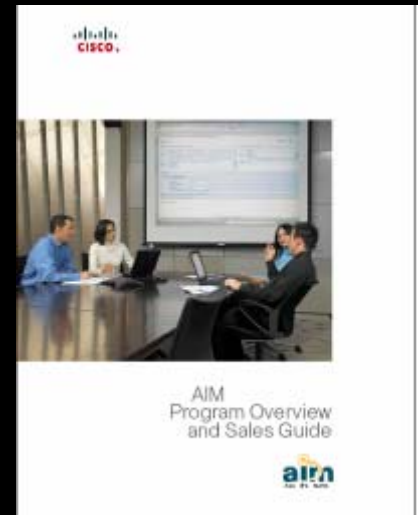
- Program Overview & Sales Guide
- Solutions Demo Guide (how to set up, walk through)

## -Sales Tools

- Solution overview flash demo
- Product flash demos MARS/ASA/IPS
- Presentations
- Product collateral (At a glance, data sheets, FAQ, etc)

## -Additional Resources

- Other collateral (white papers, case studies)
- CD with files and collateral



# Agenda

- The Changing Threat Landscape
- Cisco's Security Strategy – the Self Defending Network
- Threat Control & Containment
- Technology & Solutions Update
- **Summary**



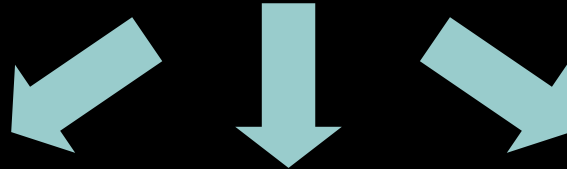


# So Why Cisco? (We are our own best reference!)

Versatility



**Internally, We Face  
Many of the Same  
Challenges as You and  
Your Customer's Do**



Functionality



Performance



Cost of Ownership



Security



Ease of Operation  
and Maintenance



# Security Products – Growth Acceleration

## ASA/PIX

Shipped  
Millionth Unit  
in FY'07




## ISRs

2,000,000+ Units  
Shipped, more  
than 500,000  
with Security



## IPS

Surpassed  
\$100M in  
Revenue in  
FY'06




## CS-MARS

Achieved over  
\$50M Annual  
Booking Run  
Rate in FYQ4



## CS-M

Over 70% Are  
CS-Manager Pro  
Licenses



## NAC Appliance

200% Y/Y Growth  
with 300 New  
Customers in Q4



# Get Mobile, Integrate into UC, but be Secure!



# So Why Cisco? (Our commitment starts at the top)

- **Product and Technology Innovation**

  - >1500 security-focused engineers

  - Nine acquisitions added to our security solution portfolio in last two years

  - 60+ NAC partners work collaboratively with us to deliver on 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®**

