Cisco Router Security Solutions

Today's Security Concerns

Collaboration and Communication

- TelePresence / Video / IM / Email
- Mobility
- Web 2.0 / Web Services / SOA

The New Threat Environment

- The Eroding Perimeter
- Spam / Malware / Profit-Driven Hacking
- Data Loss and Theft

The Business Impact of Security

- IT Risk Management
- Regulatory Compliance
- Security as Business Enabler

The Branch Transformation

Today's Branch	Empowered Branch
Aging, Disparate Data/ Voice Networks	Unified Voice/Data/Video Network Platform
Saturated WAN, Poor Response Time	Optimized WAN, Accelerated Applications
Blended Security Threats, Compliance	Self-Defending Networks
Limited Mobility, Limited Disaster Recovery	High Availability, Unified Wireless—Wireline Business
Inconsistent Branches and Branch-HQ solutions	Consistent Branches and Branch-HQ Services

The Evolution of Intent
From Hobbyists to Professionals

Threats becoming increasingly difficult to detect and mitigate

THREAT SEVERITY

FINANCIAL:
Theft & Damage

FAME:
Viruses and Malware

TESTING THE WATERS:
Basic Intrusions and Viruses

| 1990 | 1995 | 2000 | 2005 | 2008 | WHAT'S NEXT? |
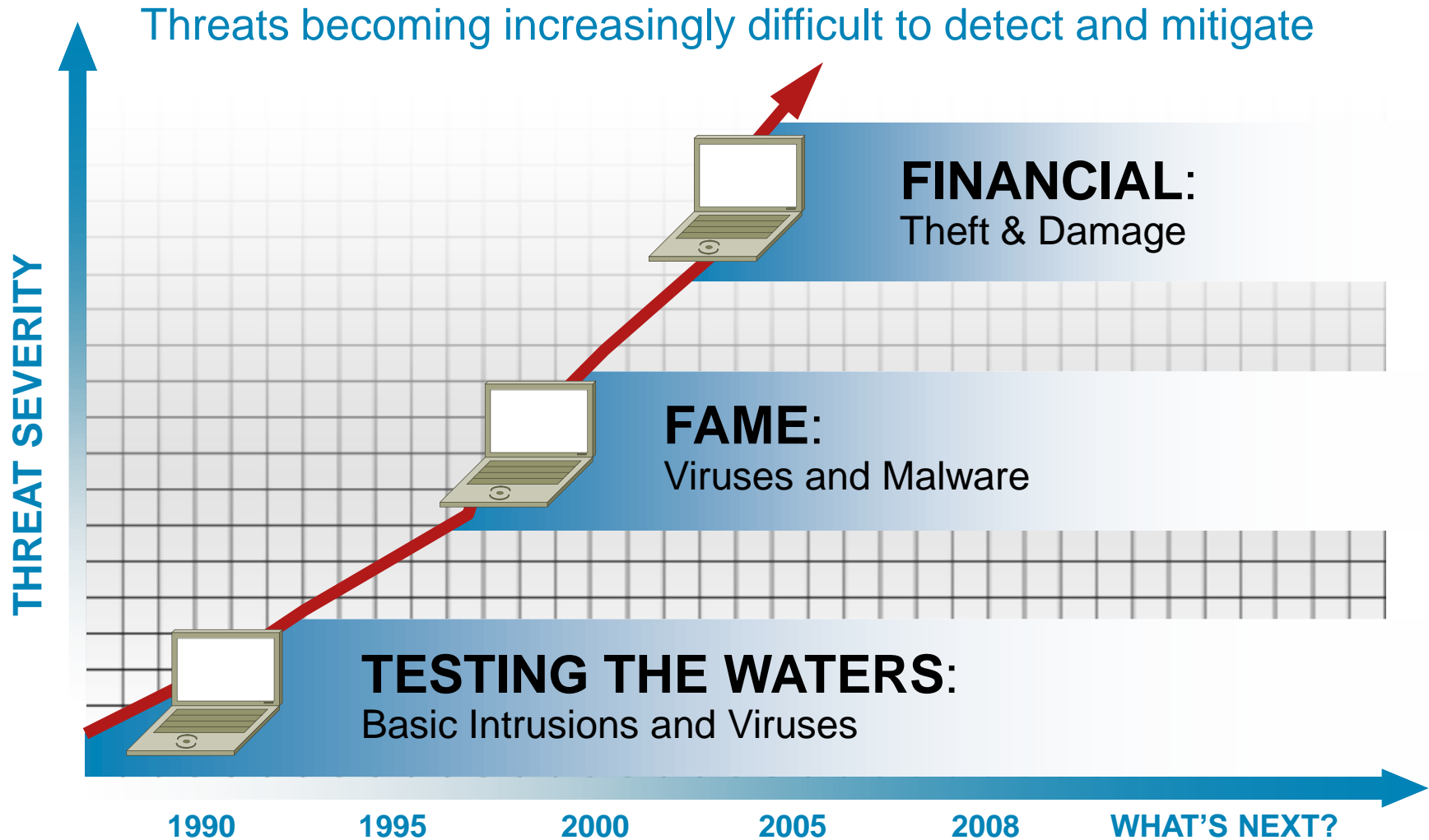
Cisco Self-Defending Network
Solutions for Business Security

System Management

Policy—Reputation—Identity

Application Security
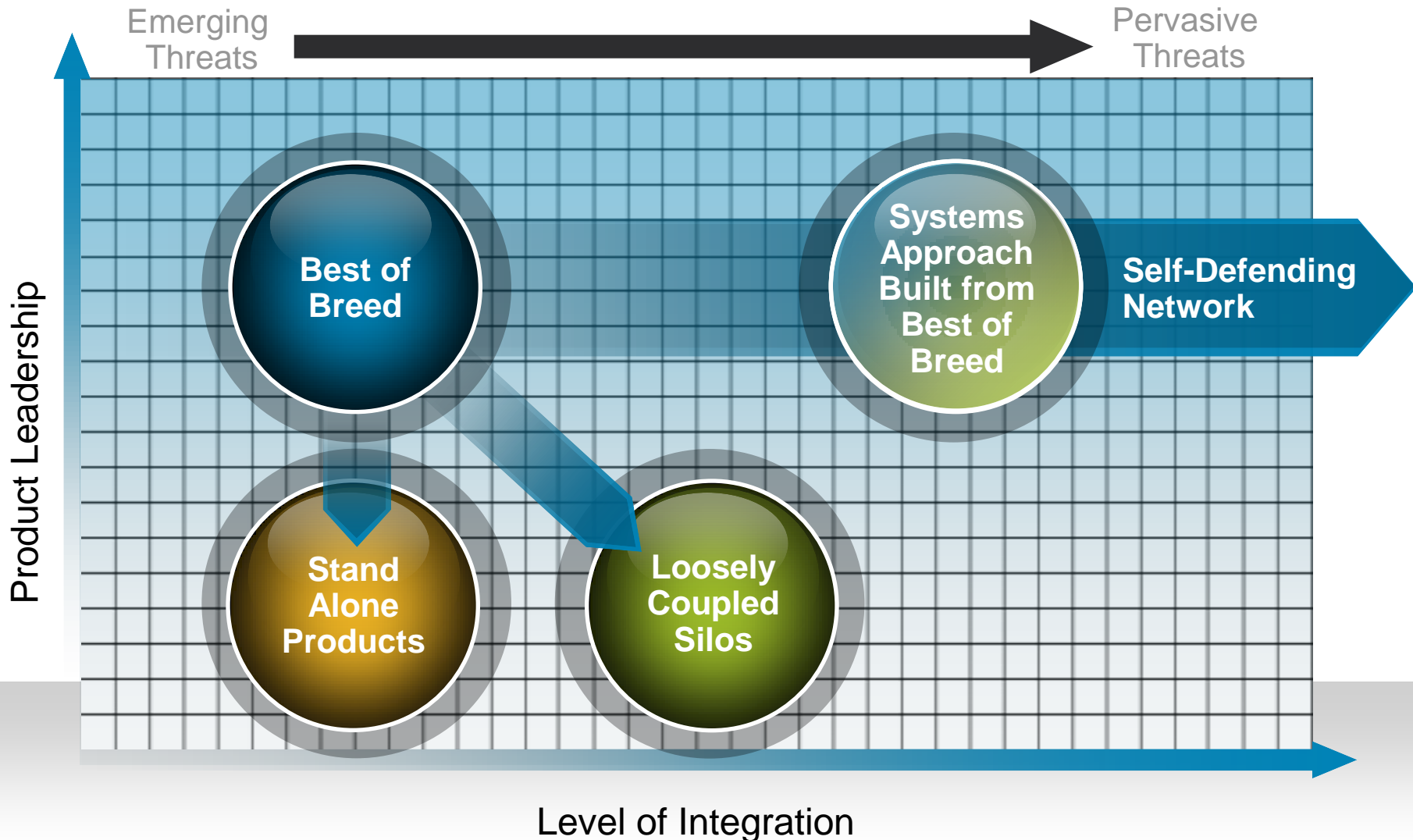
Content Security

Network Security

Endpoint Security

Cisco Self-Defending Network:

Best of Breed Security in a Systems Approach

- Enforce business policies and protect critical assets

- Decrease IT administrative burden and reduce TCO

- Reduce security and compliance IT risk

# Systems Approach Built from a Leadership Product Portfolio

Emerging Threats → Pervasive Threats

Product Leadership

- Best of Breed
- Stand Alone Products
- Loosely Coupled Silos
- Systems Approach Built from Best of Breed
- Self-Defending Network

Level of Integration

"Cisco has developed a vision and strategy for a network security platform that places their customers on a journey. Cisco promises that the security posture of this company will improve as they move through this journey."

Nick Lippis

Special Edition Lippis Report: Network Security 2.0: A Systems Approach to Threat Mitigation Emerges

Market Acceptance: Reaching 5 Million

Overlay Appliances

3G Modem
Router
Switch
Wireless LAN
WAN/App Optimization
Security Appliance
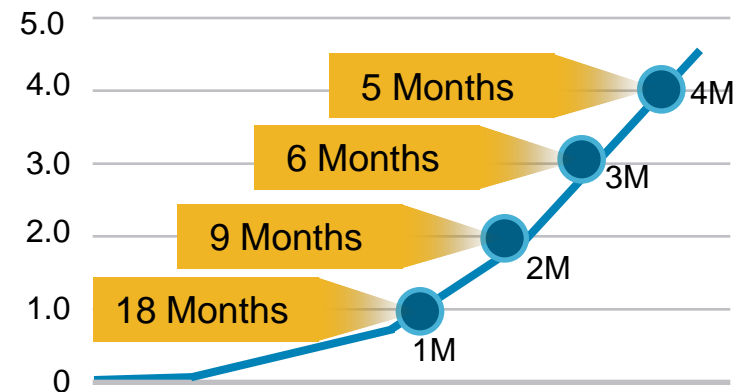**Voice Appliance**
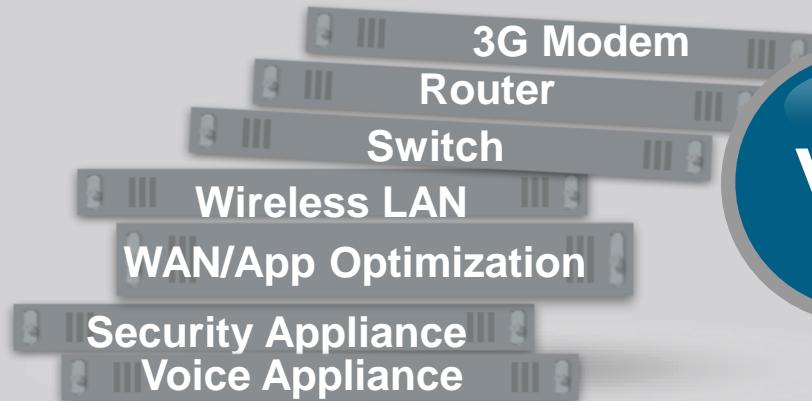
VS.

Integrated Services Router

Cisco ISR 3845

With Voice, Wireless, Video, WAN Optimization, Switch

- 4 Millionth ISR at Coke-Cola Enterprises
- UC, data, video to 30,000 CCE employees
- Greater employee collaboration
- Business innovation

Millions of Routers Sold

5.0

4.0 — 5 Months — 4M

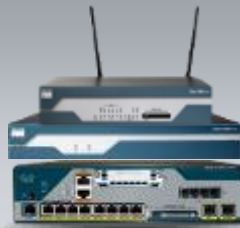3.0 — 6 Months — 3M

2.0 — 9 Months — 2M

1.0 — 18 Months — 1M

0

Cisco Router Security Portfolio

**Service Integration
Scaled to Fit Every Size Branch Office**

Performance and Services Density

3800 Series

3200 Series

High Density and Performance for Concurrent Services

2800 Series

1800 Series

Rugged and Mobile Applications

800 Series

Embedded, Advanced Voice, Video, Data, and Security Services

Embedded Wireless, Security, and Data

| Small Office and Teleworker | Small Branch | Medium Branch | Mobile/Rugged Branch | Medium to Large Branch |

Cisco Router Security

Leadership in Innovation

Industry First

Cisco Integrated Services Router Innovations in Security

- Industry-leading integration of VPN, routing, and QoS: DMVPN, GET VPN, SSL VPN, and Easy VPN

- Router-embedded security services: Application firewall, IPS, and URL filtering

- Cisco® Router and Cisco Configuration Professional (CCP) with one-touch lockdown and security audit

- Router-integrated voice and security

- Router-integrated wireless with advanced security

- Router-integrated switching; Layer 2/3 security

- Secure WAN backup over DSL, cable, 3G, or satellite
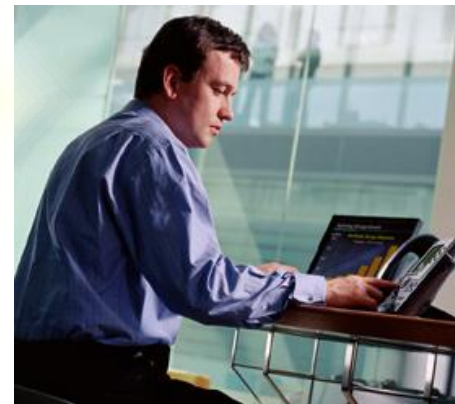
Cisco Router Security Certifications

	FIPS	Common Criteria	
	140-2, Level 2	IPSec (EAL4)	Firewall (EAL4)
Cisco® 870 ISR	✓	✓	✓
Cisco 1800 ISR	✓	✓	✓
Cisco 2800 ISR	✓	✓	✓
Cisco 3800 ISR	✓	✓	✓
Cisco 7200 VAM2+	✓	✓	✓
Cisco 7200 VSA	✓	✓	---
Cisco 7301 VAM2+	✓	✓	✓
Cisco 7600 IPSec VPN SPA	✓	✓	---
Catalyst 6500 IPSec VPN SPA	✓	✓	---
Cisco 7600	✓	✓	✓

cisco.com/go/securitycert

Only Cisco Router Security Delivers All This
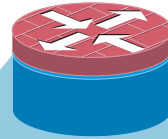
Secure Network Solutions
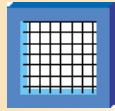- Business Continuity
- Secure Voice
- Secure Mobility
- Compliance

Integrated Threat Management
- Advanced Firewall
- Content Filtering
- Intrusion Prevention
- Flexible Packet Matching
- Network Admission Control
- 802.1x
- Network Foundation Protection

Secure Connectivity
- GET VPN
- DMVPN
- Easy VPN
- SSL VPN

Management and Instrumentation
- CCP
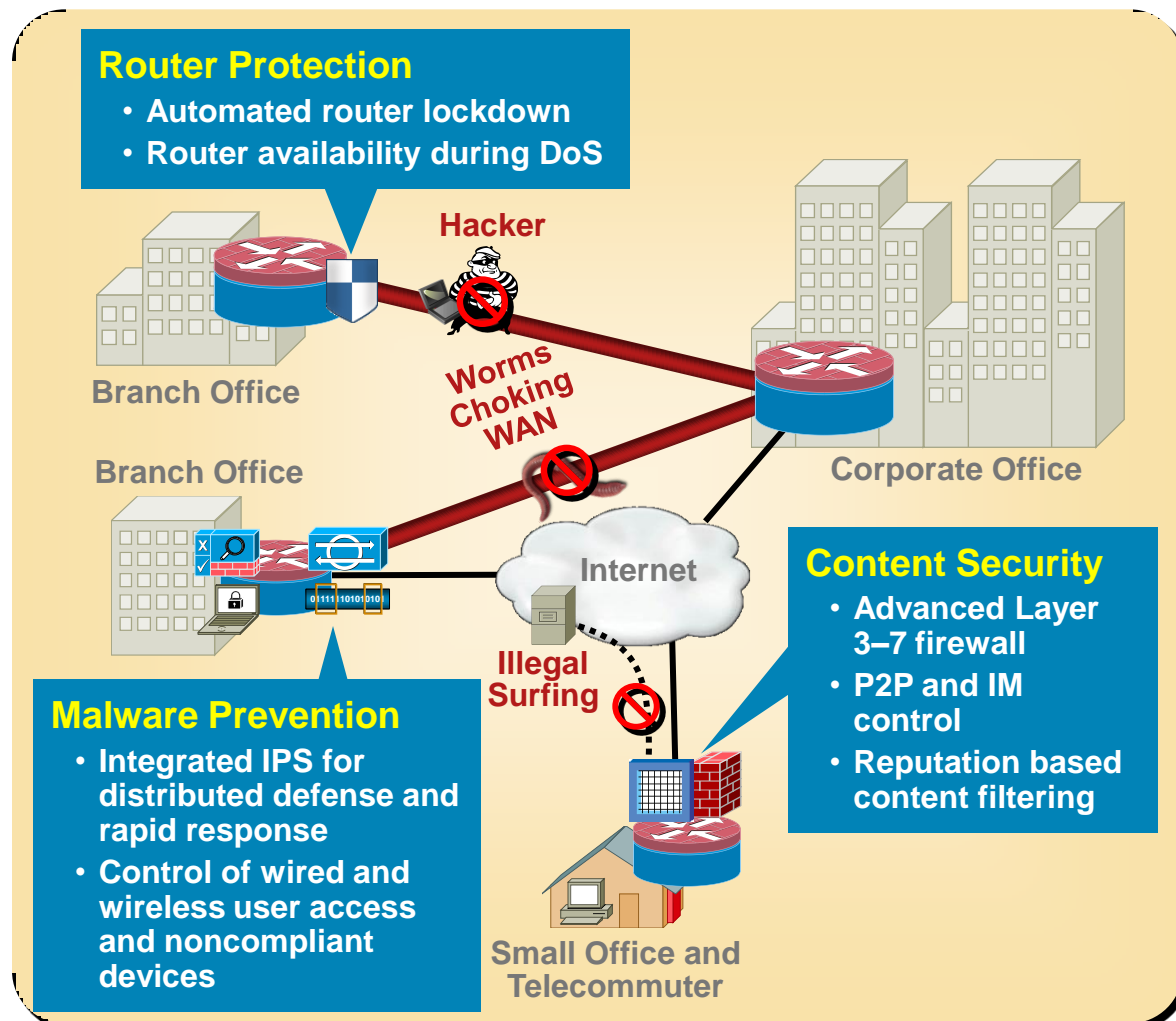- Role-Based Access
- NetFlow
- IP SLA

Integrated Threat Control Overview
Industry-Certified Security Embedded Within the Network

- Access branch office has secure Internet access and no need for additional devices

- Solution controls worms, viruses, and spyware right at the remote site; conserves WAN bandwidth

- Solution protects the router itself from hacking and DoS attacks

Router Protection
- Automated router lockdown
- Router availability during DoS

Hacker

Branch Office

Worms Choking WAN

Branch Office

Corporate Office

Internet

Content Security
- Advanced Layer 3–7 firewall
- P2P and IM control
- Reputation based content filtering

Illegal Surfing

Malware Prevention
- Integrated IPS for distributed defense and rapid response
- Control of wired and wireless user access and noncompliant devices

Small Office and Telecommuter

Integrated Threat Control ROI

Loss of Data and Time

- **Average cost of a security incident in UK:**
    - £17,000 for overall
    - £130,000 for large business

- **Biggest effect:**
    - Availability of information

- **Additional costs:**
    - Disruption to business
    - Time spent responding to the incident
    - Direct financial loss
    - Damage to reputation

Source: UK Department of Trade and Industry Information Security Survey, 2006

Annual Loss from Unauthorized Access to Information

Survey Year	Loss per Respondent
2007	$345,005
2006	$167,713
2005	$204,000

Source: CSI/FBI Computer Crime Survey, 2007

ValueClick Case Study

> "If we were not able to use an integrated solution, the networks at all of our remote sites would become much more complicated, and our staffing requirements would substantially increase."
>
> - Kevin Graham, Director of Networks, Security, and Storage, ValueClick

Business Challenge:

- Protect against malware and Internet threats
- Provide robust security with no disruptions
- Maintain simplicity for remote locations

Network Solution:

- Cisco Router Security solutions for integrated firewall and VPN services
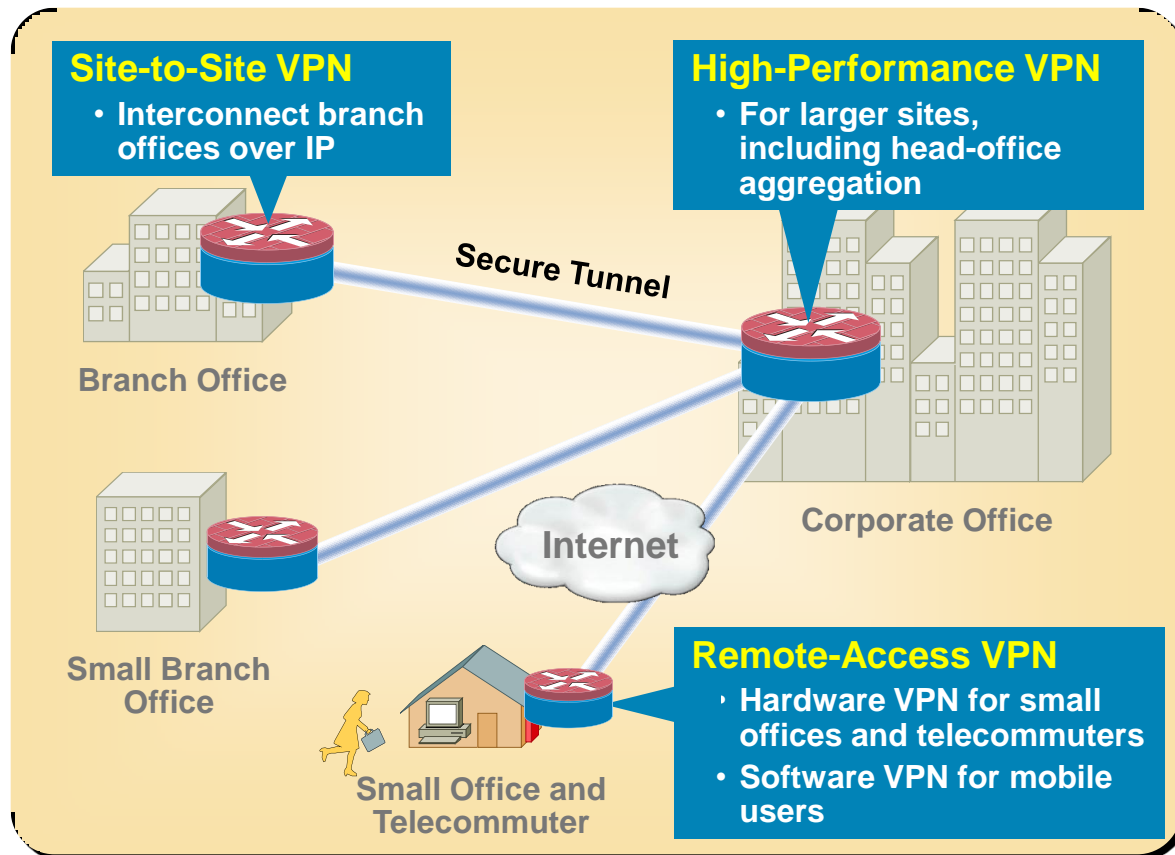
Business Results:

- Strong, integrated defense
- Simple, efficient security management
- Helps meet auditing and regulatory compliance requirements

Secure Connectivity Overview

VPN and High Availability for the WAN

- Encrypted VPN connectivity between sites or partners

- Secure remote access

- High ROI of leased line or Frame Relay to VPN migration

Site-to-Site VPN
- Interconnect branch offices over IP

High-Performance VPN
- For larger sites, including head-office aggregation

Secure Tunnel

Branch Office

Small Branch Office

Internet

Corporate Office

Small Office and Telecommuter

Remote-Access VPN
- Hardware VPN for small offices and telecommuters
- Software VPN for mobile users

Network Integration is the Key

Secure Connectivity ROI

Compelling ROI for VPN Migration

Before – Frame Relay

1.5M (512,000 CIR) Port Speed

30 Sites

Access Charge per Site	=	$350
Total Branch Access	=	$10,150
Headend Access	=	$3,800
Total Cost per Month	=	$13,950

Frame charge based on service provider's average T1 services

After – Broadband IP VPN *

1.5M Port Speed

30 Sites

Cost of 2811 x 29 Sites	=	$78,760
Cost of 3845 Headends	=	$12,700
Total Nonrecurring Cost	=	$91,460
Access Charge per Site	=	$80
Total Branch Access	=	$2,320
Headend Access	=	$3,800
Total Cost per Month	=	$6,120

•Broadband based on DSL or cable Internet business services (average)

$8,000 per Month Savings
Equipment Paid Off in Less than a Year

Secure Connectivity Case Study

## Data Encryption for Frame Relay or Leased Lines

Business Problem

- Reduce risk of exposing customer data (e.g., credit card); avoid painful disclosure and negative publicity

Real-Life Example

- Online retailer with WAN connectivity through Frame Relay

- The service provider misprovisioned a DLCI change

- Another company's network overlapped into the retailer's network…

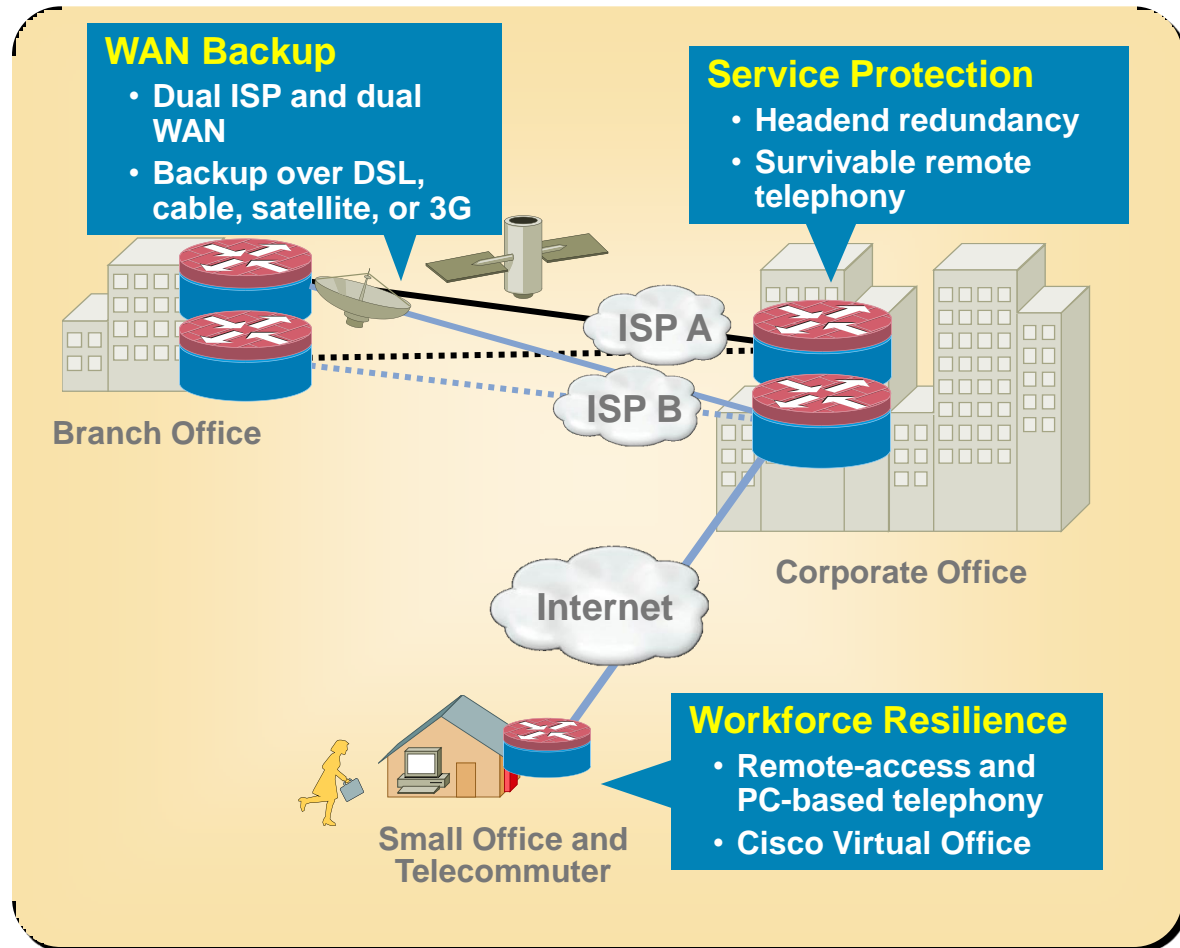- Notification of Risk to Personal Data (NORPDA) mandates that all customers be notified of breach

Solution

- Customer now encrypts all traffic over its WAN

  Unencrypted traffic is denied entrance to the customer's Frame Relay network

- Security of customer data is ensured
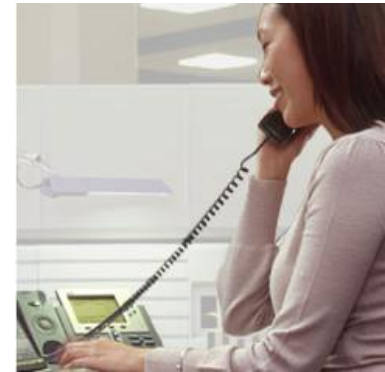
Business Continuity Overview

- Network availability during attacks and disasters

- Employee communications during disasters

- Uninterrupted operation of business-critical applications

- Office-caliber resources to the remote workforce

WAN Backup
- Dual ISP and dual WAN
- Backup over DSL, cable, satellite, or 3G

Service Protection
- Headend redundancy
- Survivable remote telephony

Branch Office

ISP A

ISP B

Corporate Office

Internet

Workforce Resilience
- Remote-access and PC-based telephony
- Cisco Virtual Office

Small Office and Telecommuter

Business Continuity

Cost of Risk as Measured by Downtime

- Costs for downtime are high
  - One day cost of lost productivity = $1,640 per employee
- More than just a data network outage
- More than just revenue affected:
  - o Revenue loss
  - o Productivity loss
  - o Impaired financial performance
  - o Damaged reputation
  - o Recovery expenses

Industry Sector	Revenue/Hour	Revenue/ Employee- Hour
Energy	$2,817,846	$ 569
Telecommunications	$2,066,245	$ 186
Manufacturing	$1,610,654	$ 134
Financial Institution	$1,495,134	$1,079
Insurance	$1,202,444	$ 370
Retail	$1,107,274	$ 244
Transportation	$ 668,586	$ 107
Average	$1,010,536	$ 205

Source: Meta Group

20

Secure Voice Overview

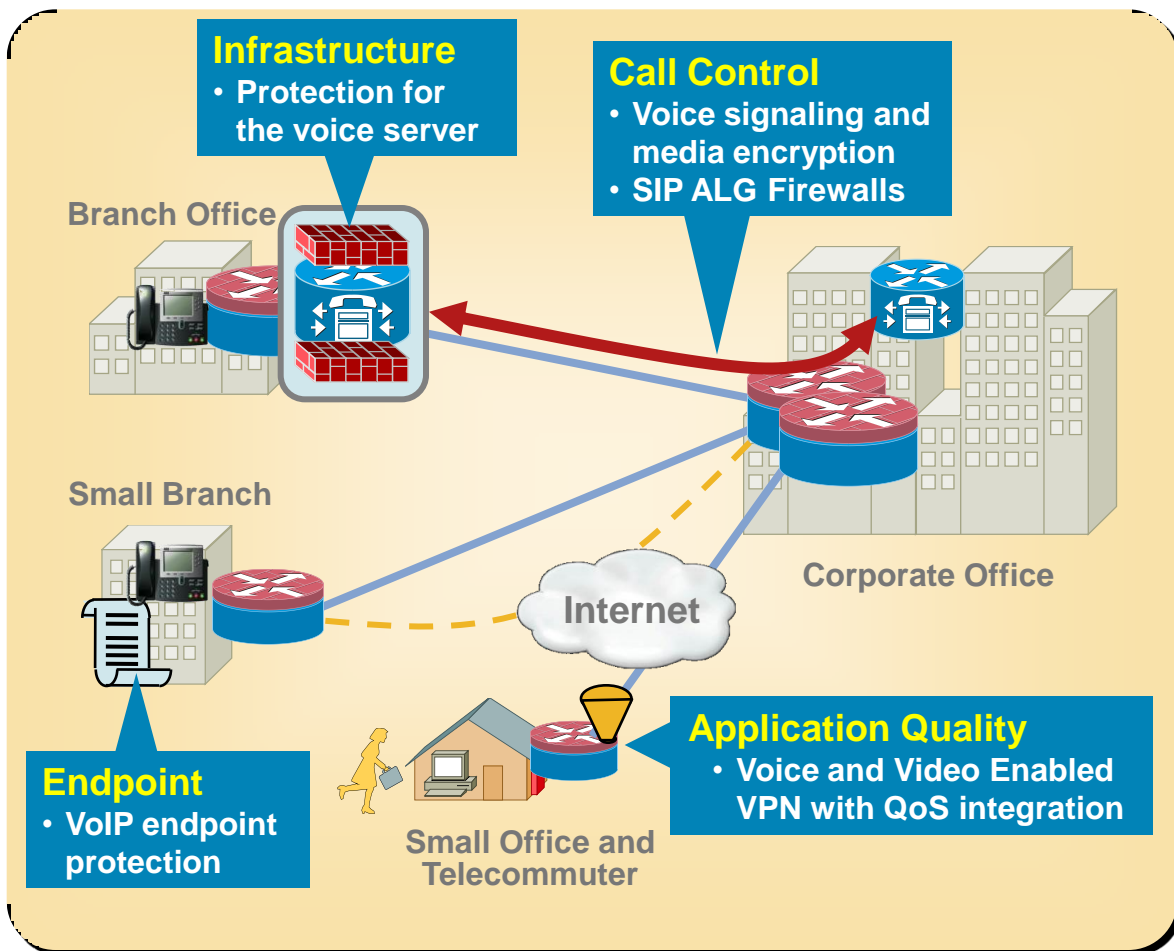- Traditional threats remain in the converged world of IP communications

  Eavesdropping

  Toll fraud

  Denial of service

- Integrated security reduces the total cost of ownership

Infrastructure
- **Protection for the voice server**

Call Control
- **Voice signaling and media encryption**
- **SIP ALG Firewalls**

Branch Office

Small Branch

Corporate Office

Internet

Endpoint
- **VoIP endpoint protection**

Small Office and Telecommuter

Application Quality
- **Voice and Video Enabled VPN with QoS integration**

Secure Voice Bundles TCO

Cheaper to Buy Now vs. Later

Product	Router Only	Secure Voice Bundle (VSEC-CCME)	Savings
Cisco 2801	$5,745	$4,095	$1,650
Cisco 2811	$5,995	$4,695	$1,300
Cisco 2821	$8,445	$6,395	$2,050
Cisco 2851	$12,895	$9,595	$3,300
Cisco 3825	$17,800	$13,795	$4,005
Cisco 3845	$22,500	$17,795	$4,705

Bundles with part number VSEC-CCME include:

- Cisco IOS® Advanced IP Services feature set

- DSP (PVDM) and memory

- Cisco® Unified CallManager Express Feature License

Secure Voice Case Study

Business Problem: Real-Life Example

- ePlus: Financial solutions and enterprise software

- Need: To unify dispersed nationwide workforce

- Requirement: Secure voice and data for remote sites

Solution

- Voice functions integrated into Cisco® integrated services routers

    Routers replaced 35 disparate phone systems.

    Now employees reach coworkers anywhere with four-digit extension.

- Connectivity costs cut by $840,000 per year by migrating from Frame Relay to DMVPN

- Future video conferencing, content caching, intrusion prevention, and NAC services

- Quick business expansion: Cookie-cutter deployment; phones for new sites up in 2 hours
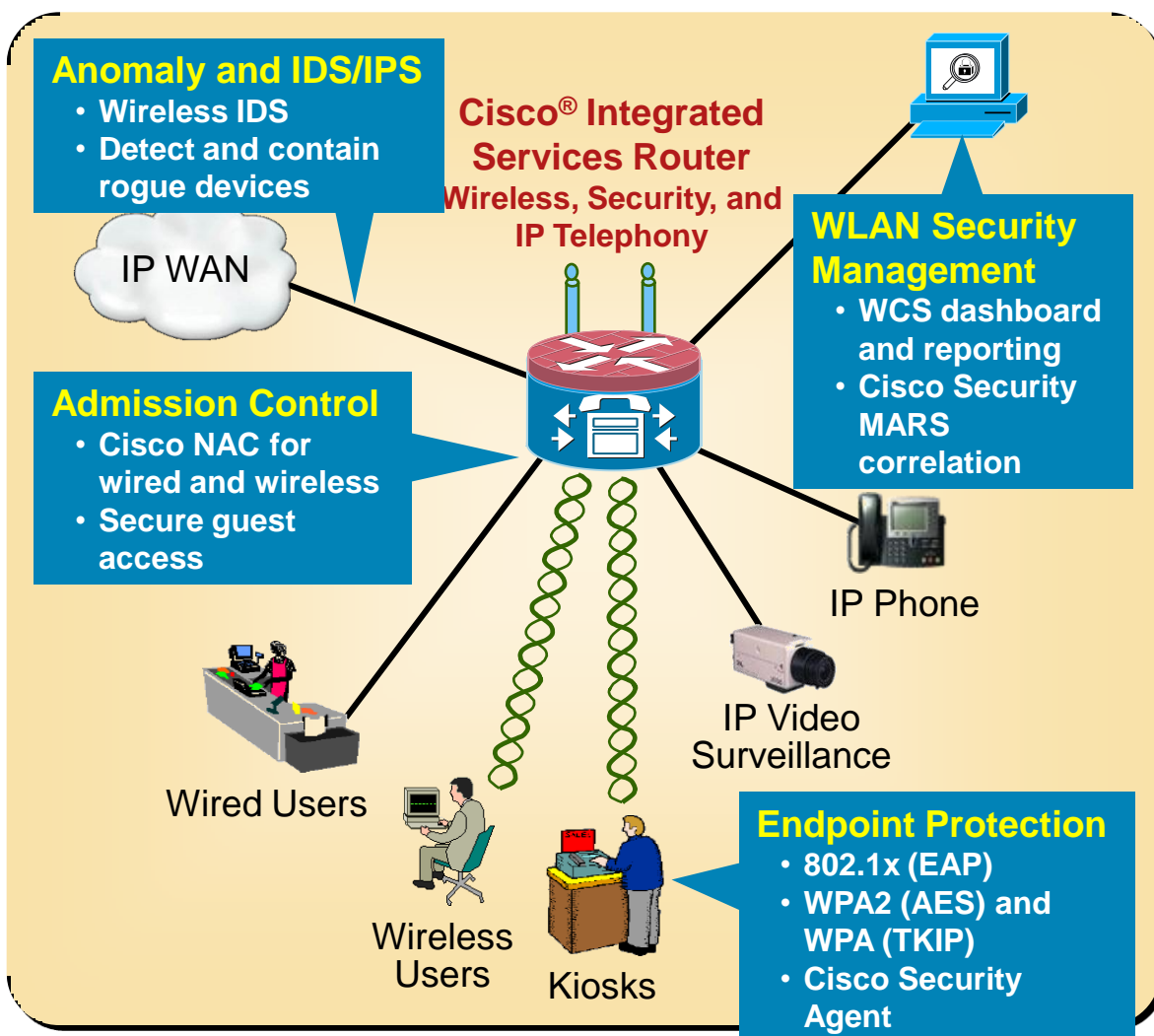
"The Cisco integrated services routers allow us to centralize everything into a router. By the time we have completed our deployment, we will have doubled …our organization, while reducing maintenance and circuit costs."

Chris Fairbanks, Principal Network Architect, ePlus Inc.

Secure Mobility Overview

- Mobile access to critical applications and data throughout the site, while maintaining security

- Ease of deployment; interoperation with wide range of client devices

- Reliable, scalable, centralized security management

Anomaly and IDS/IPS
- **Wireless IDS**
- **Detect and contain rogue devices**

IP WAN

Cisco® Integrated Services Router
Wireless, Security, and IP Telephony

WLAN Security Management
- **WCS dashboard and reporting**
- **Cisco Security MARS correlation**

Admission Control
- **Cisco NAC for wired and wireless**
- **Secure guest access**

IP Phone

IP Video Surveillance

Wired Users

Wireless Users

Kiosks

Endpoint Protection
- **802.1x (EAP)**
- **WPA2 (AES) and WPA (TKIP)**
- **Cisco Security Agent**

Secure Mobility
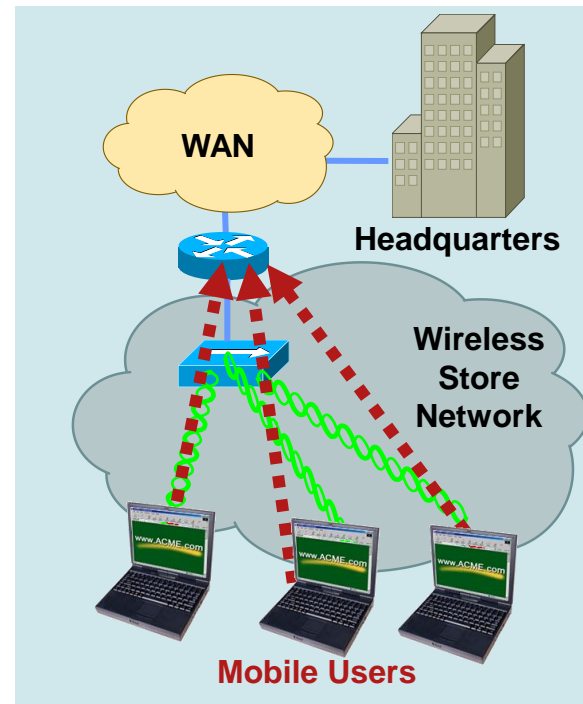
Secure Mobility Case Study

Mobile Retail Application

Business Problem: Real-Life Example

- One of the largest U.S. retailers

- Mobile Windows PC application being delivered to every site

- Basic wireless security of mobile device failed during security audit (deemed vulnerable)

- Requirement: Converge separate systems and data networks into a single solution that is easier to manage and lowers operating costs

Solution

- Mobile devices now use IPsec and AES with L2TP and Microsoft AES from the store wireless network back to the router and WAN.

- Cisco® integrated services routers have built-in AES 128, 192, and 256 – the strongest commercial encryption available today.

WAN

Headquarters

Wireless Store Network

Mobile Users

> "The Cisco 2800 Series Router will become the 'communications hub' of our new stores."
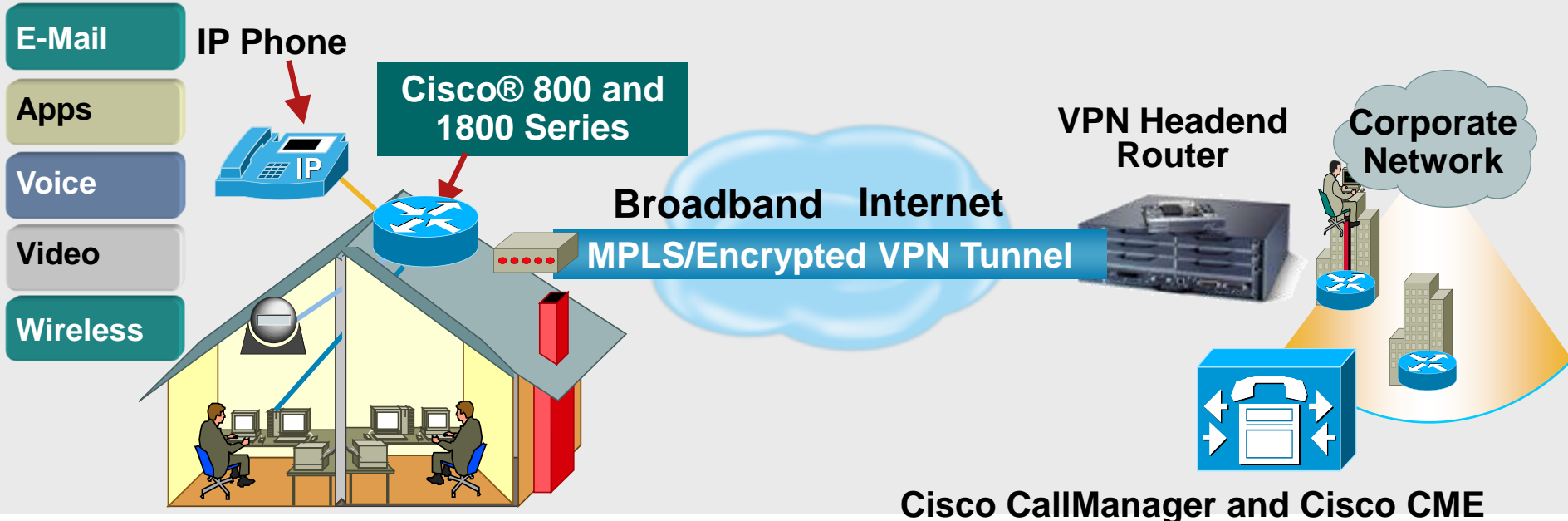
Secure Mobility Case Study

Small Remote Office or Teleworker

Advanced Application Support (voice and video)

Centralized Management: IT-Managed Security Policies

E-Mail

Apps

Voice

Video

Wireless

IP Phone

Cisco® 800 and 1800 Series

IP

Broadband Internet

MPLS/Encrypted VPN Tunnel

VPN Headend Router

Corporate Network

Cisco CallManager and Cisco CME

Corporate Pushed Security Policies (not user-managed)

Corporate Phone, Toll-Bypass, Centralized Voicemail

Integrated Security and Identity Services

Optional Secure Wireless LAN

Compliance Regulations Overview

Compliance

Regulation	Information Protected	Date of Enforcement
HIPAA	Health information of patients	1996
GLBA	Consumer financial information	1999
SOX	Business financial and accounting information	2002
CA SB 1386*	Consumer personal information	2003
PCI	Credit card information	2008**

*As of July, 2008, 44 states had passed security breach notification laws
** PCI DSS version 1.2 (October)

The Payment Card Industry (PCI)
Data Security Standard

- Published January 2005

- Impacts ALL who **process, transmit, or store** cardholder data

- Also applies to 3rd-party hosting companies, information storage companies, etc.

- Monthly fines ranging from $5,000 to $50,000 for missed deadlines

- **Has global reach**

Theater	Level 1	Level 2	Level 3
US	SEP 2007	DEC 2007	DEC 2008
Western Europe	Negotiated individually	MAR-DEC 2008	MAR-DEC 2008
Asia	DEC 2009	DEC 2009	DEC 2009
Canada	2008 TBD	2008 TBD	2008 TBD
Latin American CEMEA	Not Published yet		

Source: pcisecuritystandards.org

Compliance Case Study

Securing Customer Credit Card Information

Business Problem: Real-Life Example

- Leading specialty retail chain

- Requirement: Compliance with government regulations; maximum security for customer credit card information

Solution

- Cisco® Integrated Services Router with voice security (VSEC) bundle

    Provides required level of security and compliance

    Reduces cost of ownership

    Offers security for voice and wireless

- Platform for future capabilities

    Enhanced wireless, e-learning, RFID and location services, and PS system

Total Security System Management

Ease of Configuration and Setup

Policy Administration

Event Sharing and Collaboration

Threat Intelligence

Policy

Monitoring

Reduced complexity for more effective risk analysis and operational control

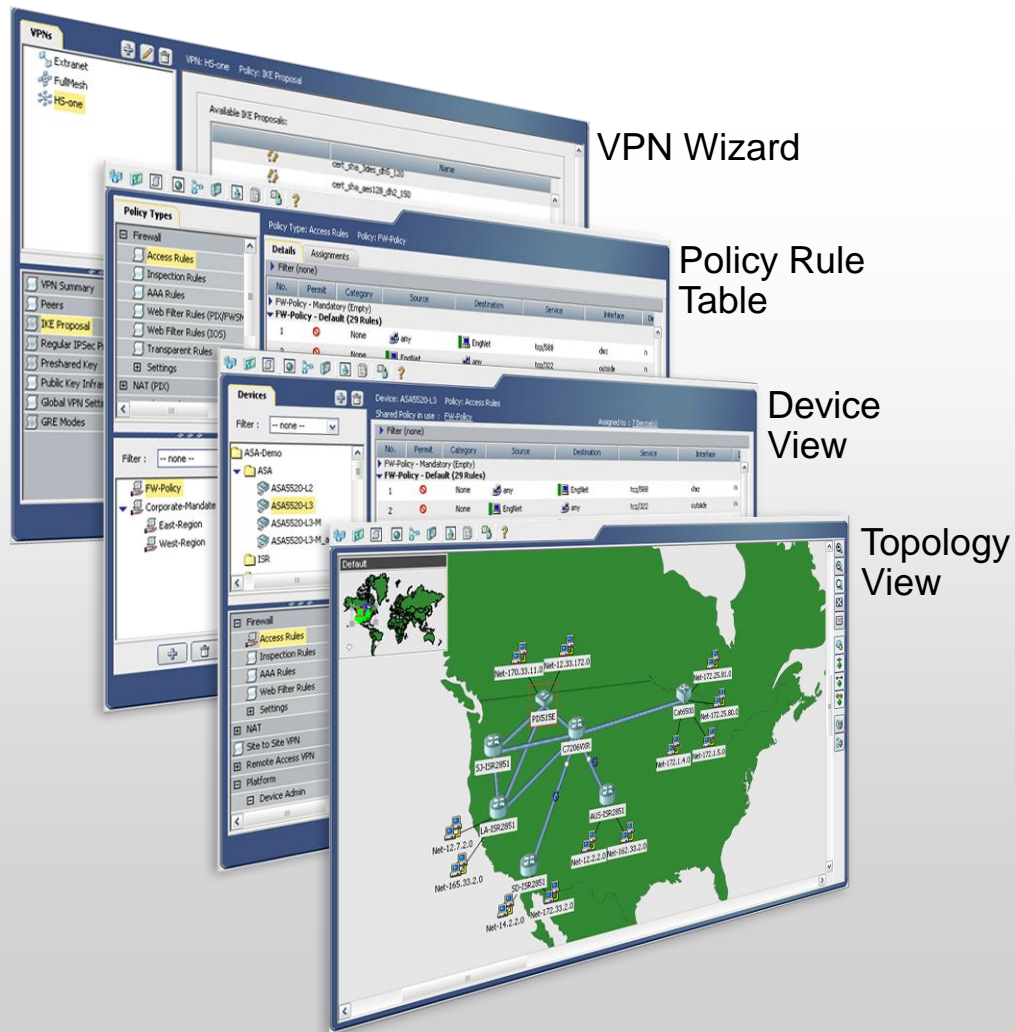# Cisco Configuration Professional

- Unified GUI
  - Routing
  - Security
  - Unified Communications
- Wizard led configuration
  - LAN, WLAN, and WAN
  - Firewall, IPS, and VPN
  - QoS, ACLs

- Voice Gateway, SRST or CME Configuration
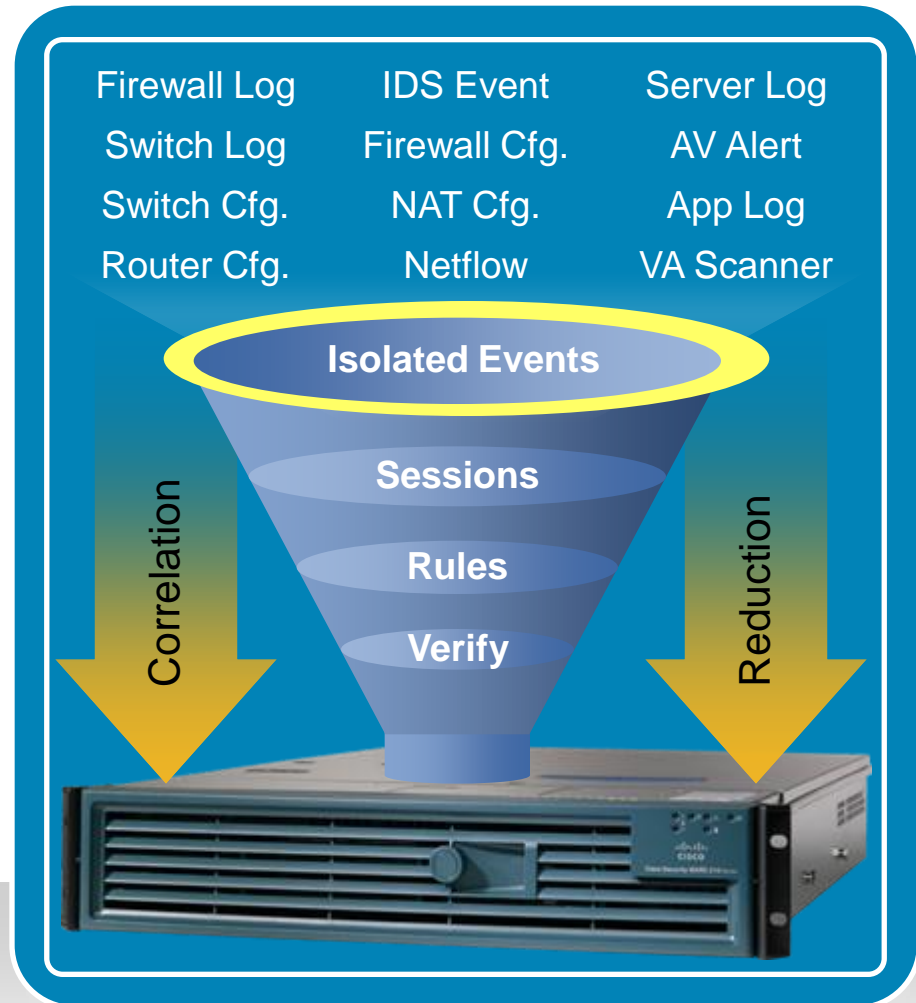
Free Download:
http://www.cisco.com/go/ciscocp

Cisco Security Manager

VPN Wizard

Policy Rule Table
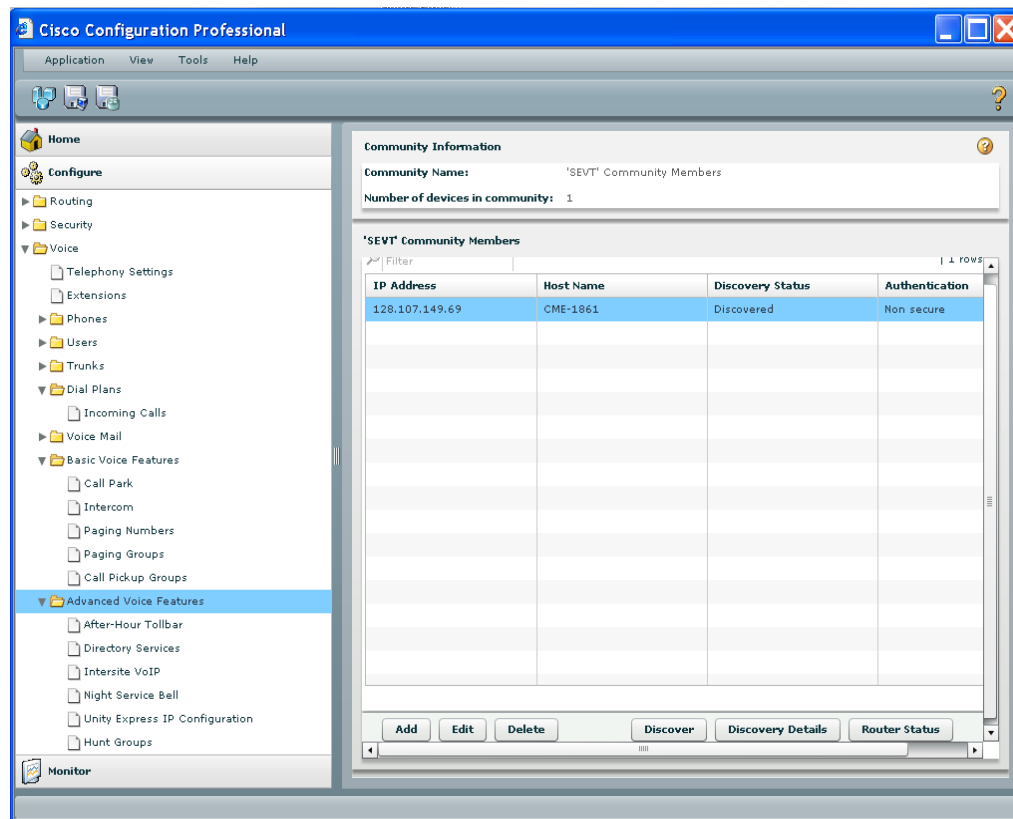
Device View

Topology View

- Unified services management for security including firewall, VPN, and IPS

- Intuitive, feature-rich user interface

- Different views for different administrative preferences

  Device View

  Topology View

  Policy View

- Efficient management architecture for large-scale security deployments

Cisco Security MARS

- MARS is an acronym = Monitoring, Analysis, and Response System

- Security threat mitigation appliance

- Rapid threat detection, isolation and mitigation, topologically aware

- Command and control for your existing network security

- Correlates data from across disparate multi-vendor security devices and applications

Firewall Log	IDS Event	Server Log
Switch Log	Firewall Cfg.	AV Alert
Switch Cfg.	NAT Cfg.	App Log
Router Cfg.	Netflow	VA Scanner

Correlation

Reduction

Isolated Events

Sessions

Rules

Verify

Summary

- Complex security challenges are increasing the need for a solutions approach

- Cisco Router Security is a critical element of Self-Defending Networks.

- Cisco Router Security delivers proven, secure solutions for business continuity, compliance, voice, and wireless

- An integrated approach reduces operations complexity and costs

- Cisco Router Security solutionscan maximize your ROI

www.cisco.com/go/routersecurity