Securing Your Enterprise
Realizing the SDN Vision

April 3rd, 2008 Vienna
Connected World with Complex Security Challenges

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 Growing Need for Security Solutions

A Systems Approach to Streamline IT Risk Management for Security and Compliance

- Regulatory Compliance
- Data Loss
- Malware
Solutions for Business Security

- Enforce business policies and protect critical assets
- Decrease IT administrative burden and reduce TCO
- Reduce security and compliance IT risk

**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
Systems Approach Built From A Leadership Product Portfolio

- Emerging Threats
  - Alone Products
  - Coupled Silos
- Pervasive Threats
  - Built from Best of Breed

Level of Integration

Product Leadership
Building Upon the Self-Defending Network Vision

- Identity, Policy and System Management for Improved Enterprise Control
- Protection of Business Applications and Data: Application Security
- Protection Beyond the Perimeter: Content Security for Data in Motion
Foundation of the Self-Defending Network:
Network Security

- Firewall, IDS/IPS, and VPN in ASA, ISR and Catalyst 6500
- 1.4M Routers with Integrated Security
- 3M Switches with Integrated Security

Integrated

Adaptive

- Cisco Security Agent (CSA)
- IPS and Anomaly Detection
- DOS Guard and NetFlow Event Management

Collaborative

- Cisco Security Agent (CSA), Network IPS and MARS
- Cisco Security Manager
- Secure Wireless
- Secure Unified Communications

Success with Systems Based Architectural Solution
Cisco Network and Endpoint Security Innovations/Milestones

- **2003**: DDoS, SSL VPN, Monitoring Technology
- **2004**: Application Security, Intelligence Services
- **2005**: TrustSec
- **2006**: High Performance Firewall
- **2007**: 1.5 Million PIX and ASA Shipped
- **2008**: $100M IPS Revenue, 38% Network Security Market Share, 500K ISR Security Bundles Shipped
Realizing the Self-Defending Network Vision Strategy for Network and Endpoint Security

**Network Security Strategy**
- Integrate security services; seamlessly embed into the network
- Empower security team
  - Less touch points
  - More threat identification granularity
- Scale performance and services to meet real customer deployment needs
- Connect security technology controls to business risk
- Deliver identity networking pervasively

**Endpoint Security Strategy**
- Endpoint Protection & Control
- Data Loss Protection
- Guest Services
- Endpoint Discovery
- Posture Remediation
- Secure Connectivity Services
- Increased business policy enforcement
- Unify endpoint clients
- Seamless transitions for endpoint
Evolutions for Network and Endpoint Security Portfolio

System Management
Policy—Reputation—Identity

Application Security

Content Security

Network Security

Endpoint Security

Enhancements Address PCI, Malware and DLP Solution Needs
Cisco Security Agent: Evolutions

- **Server and desktop endpoint protection**
  - Single client, single management interface, comprehensive security and control
  - Pervasive attack protection with zero-update host intrusion prevention
  - Network collaboration with local threat remediation

- **New Features:**
  - Integrated Anti-virus: Automatic, no-cost updates
  - Data Loss Prevention: Identify and Control Sensitive Information
  - Policy Enforcement: Appropriate use for regulatory compliance

**Business Benefits:**
- Protection from persistent and evolving threats
- Empower IT to address business risks
- Enforce policies and protect business critical assets
- Decrease IT administrative burden and reduce expenses
Cisco ASA 5500 Series Adaptive Security Appliances

Comprehensive Solutions from Desktop to the Data Center

Cisco ASA 5580: Extends Market-leading Family to the Data Center

ASA 5505 (150 Mbps, 4K Conn/s)
ASA 5510 (300 Mbps, 12K conn/s)
ASA 5520 (450 Mbps, 25K conn/s)
ASA 5540 (650 Mbps, 90K conn/s)
ASA 5550 (1.2 Gbps, 36K conn/s)
ASA 5580-20 (5-10 Gbps, 90K conn/s)
ASA 5580-40 (10-20 Gbps, 150K conn/s)

New

Teleworker Branch Office Internet Edge Campus Data Center
Cisco ASA 5580 Series
Extending the ASA Series into the Data Center

- Provides the **highest connection rates in the industry** to secure high capacity Web 2.0 sites and data centers
- Delivers **massive throughput and low latency** to secure the most demanding applications, such as video, data backup, scientific / grid computing, and financial trading systems
- Enables **scalable auditing and event monitoring** to meet compliance requirements

Cisco ASA 5580 Highlights
- Industry-leading connection rates
- Protects demanding Web 2.0 applications
- Enables security auditing of high speed networks
Cisco ASA 5580: Built for Speed
New Solution Offers Dependable, Scalable Performance

- **Unprecedented Scalability**
  
  Sustains up to two million connections and 150K connections/second
  
  Supports up to 750,000 policies, with essentially no performance degradation as the number of firewall policies grow

- **Blazing Fast Performance, Ultra-Low Latency**
  
  Delivers up to 10 Gbps of real world Web 2.0 throughput, scaling up to 20 Gbps for data-intensive applications, such as SAN
  
  Provides strong small packet performance with less than 30 microseconds of latency

- **Dependable Performance**
  
  Offers multiple redundancy options, including Active/Active failover, as well as redundant power, fans and network links
Cisco IPS for Smaller Businesses: Evolutions

- **IPS for SMB**
  - Provisioning, Monitoring, Reporting
- **ASA-IPS Module**
  - Integrated ASA IPS – up to 650 Mbps
- **IPS Software**
  - Enhancing health data, device protection, auto signature updates
- **Services for IPS – expanded protection**
  - UC Protection, MSFT Vulnerabilities, P2P

**Business Benefits:**

- Proactive protection of network assets
- Maintain resource availability
- Decrease IT administrative burden and reduce expenses for SMBs
Cisco Firewall Service Module: Evolutions
Acceleration of Trusted Flow Inspection

**Trusted Flow Acceleration**
- FWSM establishes secure connection between trusted hosts based on policy
- Cisco Catalyst Switch Supervisor 720 accelerates data flow between connections (20-50 Gbps)
- Cut-through processing for same header packets
- After transaction completes, FWSM closes the connection and reestablishes per-packet analysis

**Use Cases**
- Routine high-volume data backups
- High bandwidth requirements for clustered and grid computing
- Bulk FTP transfers
- Transactions between “trusted” zones for app-specific processes
Cisco Router Security: GET VPN on Cisco VSA

- A new paradigm for encrypted any-to-any WAN connectivity

- Secure encrypted MPLS
  - Extends GET VPN performance on mid-range routing platforms
  - 300% performance increase over VAM2+
  - Fits in I/O controller slot on the 7204VXR and 7206VXR
  - Ideal for WAN edge deployments at medium and large sites

Business Benefits:

- Increase ROI: Leverage underlying transport and routing technology
- Reducing OPEX: Simplify administration of overlay VPN tunnels
- Enables scalable, multipoint encrypted communications
Protection Beyond the Perimeter: Content Security

New Forms of Communications and Collaboration Have Become the New Target of Attackers

Spam Volume Grew 100% from ’06-’07
Millions of New Botnets Appear Daily
Cisco Content Security
Innovations/Milestones

- Application Control Engine (ACE)
- IronPort Web Security Appliance
- IronPort Email Encryption
- DomainKey integration into Email Security
- ASA Content Security
- Supervisor-32 PISA on Catalyst 6500
- IronPort Botnet Defense for Web Security Appliance

#1 Market Share Email Security
First integrated DPI in wiring closet
Unprecedented visibility into 25% of global email traffic
Integrated DLP capabilities for data in motion
Realizing the Self-Defending Network Vision:
Cisco’s Strategy for Content Security

- Develop content security where everything is zero day—first time
  - Reputation based analysis vs. signature based
  - Capability to respond to huge number of variants
- Capability to scale to address a myriad of unique attacks
  - Attacks today are all different—not same attack across a population (ie fraud vs. NIMDA)
- Secure all sources of attack - from collaboration software to Web to email
- Manage evolving attack techniques – from self propagating to user propagating
Evolutions for Content Security Portfolio

System Management
Policy—Reputation—Identity

Application Security
Content Security
Network Security
Endpoint

Content Filtering
Voice Security
IronPort Web and Email Security
Cisco Router Security: UC IOS Voice Firewall

- SIP Application Layer Gateway (ALG) Features:
  - SIP signaling and associated media with IOS Firewall pass through
  - IOS Firewall protecting the WAN uplink and the phones
  - Voice pin holing works for SIP

Business Benefits:
- Reduce OPEX for telecommuter, small and branch office deployments
- Helps meet regulations such as HIPAA, FISMA, CIPA
- Protects against new web-based security threats
Cisco Router Security: Content Filtering

- **Cisco Content Filtering**
  
  Block malicious sites and enforce corporate policies
  
  Offers category based security and productivity ratings
  
  Leverages existing content security partnerships

**Business Benefits:**

- Reduce OPEX for telecommuter, small and branch office deployments
- Helps meet regulations such as HIPAA, FISMA, CIPA
- Protects against new web-based security threats
IronPort Enhancements to Email and Web Security

- BITS Security Standard for Email authentication
  - Protection from phishing attacks
  - Point and click SPF and DKIM functionality
  - Integrated TLS connection with IronPort PXE Encryption
- Botsite defense and URL outbreak detection added to web reputation filters

Business Benefits:
- Eases administration through integrated functionality that enforces corporate policy
- Meets compliance requirements: HIPAA, GLB, and other
- Reduces employee downtime and desktop clean-up costs
Realizing the Self-Defending Network Vision: Cisco’s Strategy for System Management with Identity, Policy and Reputation

- “Operationalize” security with automation to optimize resources
- Align monitoring and policy for a closed loop system
- Leverage reputation-based information across security services
- Provide comprehensive view for IT Risk Management
Operational Control and Monitoring: Total Security System Management

- Policy Implementation
- Configuration and Management
- Event Sharing and Collaboration
- Threat Intelligence

Reduced complexity for more effective risk analysis and operational control
Monitoring, Analysis & Response (MARS) : Evolutions

- Device support framework with MARS community enablement
- New Cisco and 3rd party device support
  - High-Performance security logging for ASA 5580 Netflow v9
- Cisco IPS risk and threat rating support
- Policy edit linkages with Cisco Security Manager

Open schema accelerates new device support for more comprehensive monitoring
Cisco Security Manager: Evolutions

- **CSM – MARS collaboration:**
  Rule/Signature ↔ Event

- **Expanded product support**
  5580, IOS-IPS AIM, 4270, and more

- **Support for desktop switches**
  Cat 35xx, 37xx, 4500, 4900

- **Scheduled deployment**

- **Enhanced workflow notification**

Greatly enhances administrative visibility and control while expanding competitive differentiation.
A Systems Approach to Streamline IT Risk Management for Security and Compliance

Data Loss
Regulatory Compliance
Malware
Self-Defending Network

Best of Breed Security in a Systems Approach

ASA, CSA, NAC, IPS, Web Application Firewall, MARS

CSA, IronPort, Cisco SME, Trustsec

IronPort, ASA, CSA, IPS, MARS
Q and A