The Latest on Securing Your Customers’ Networks

Cisco Business Solutions Workshop for Resellers Canada 2004
What Are We Going to Talk about…

• Threat Evolution and Security Challenges
• Cisco’s Security Vision
• Cisco’s Integrated Security Strategy
• Cisco Security in Action
• Channel Partner Programs and Tools
• Cisco SMB Portfolio of Products and Services
• Cisco Key Differentiators
• Q&A
Security Challenges
Threat Evolution

1980s
1st Gen
- Boot viruses

1990s
2nd Gen
- Macro viruses
- E-mail
- DoS
- Limited hacking

Today
3rd Gen
- Network DoS
- Blended threat (worm + virus+ trojan)
- Turbo worms
- Widespread system hacking

Future
Next Gen
- Infrastructure hacking
- Flash threats
- Massive worm driven
- DDoS
- Damaging payload viruses and worms

Target and Scope of Damage
- Global Infrastructure Impact
- Regional Networks
- Multiple Networks
- Individual Networks
- Individual Computer

Weeks
- Boot viruses

Days
- Macro viruses
- E-mail
- DoS
- Limited hacking

Minutes
- Network DoS
- Blended threat (worm + virus+ trojan)
- Turbo worms
- Widespread system hacking

Seconds
- Infrastructure hacking
- Flash threats
- Massive worm driven
- DDoS
- Damaging payload viruses and worms
“Slammer” or the Sapphire Worm

Infected 75,000 hosts in first 11 minutes

- Infections doubled every 8.5 seconds
- Infected 75,000 hosts in first 11 minutes
- Caused network outages, cancelled airline flights and ATM failures

At Peak,
Scanned 55 Million Hosts per Second

11 Minutes after Release
Top 3 SMB IT initiatives over the next 12-18 months

- Network infrastructure: 34%
- Application software upgrades: 31%
- Hardware upgrades/consolidation: 21%
- CRM: 14%
- Security/antivirus/disaster recovery: 13%
- Training: 13%
- Storage/storage management: 12%
- System software upgrades: 9%
- General communication: 8%
- ERP: 6%
- Inventory management/asset tracking: 5%

Source: IDC Canada Sept 2003
SMB Business Issues and Network Security

Top Challenges

- Making effective use of scarce IT resources
- Improving employee collaboration and productivity
- Protecting network investment
- Safeguarding valuable information
- Gaining a competitive edge without driving up network operations cost
- Reducing the cost of securing and managing the network infrastructure
Drivers of Cisco SMB Class Security

- Everything is a target
  - Routers, switches, desktops, hosts, networks, applications, information, management tools
  - Some of these can be turned into weapons
  - New breed of network attacks have multiple vectors that cannot be blocked by one device

- Network security requires an integrated system
  - Layers of security are required
  - Embedded security is required throughout the network
  - Integrated security in network devices is required
  - Network management and reporting must be secure
Cisco SMB Class Security Solutions

- Integrated security throughout IP networks
  Ease of security deployment and management
  Efficient operations with touchless administration
  Consistent user experience
  Combining IP networking and security technologies offers best means of protection ex. QoS and VLAN roles in mitigating internet worms.

- Convergence of security services within platforms
  Scalable security services for routers and switches
  Convergence of multiple security services on dedicated platforms

- Collaboration of security functions
  Increased performance and efficiency
  Price/performance and scalability
  Offer a consistent security service profile (e.g. combined IDS, FW, VPN and AAA)
Why Sell Cisco SMB Class Security?

• Compete on differentiated value
  
  Trusted advisor

  Protect and enhance your margins

  Clear value proposition for working with Cisco now and in the future

  Cisco provides a complete network solution

  Network security enables you to build and keep long-term relationships

• Increase your revenue

  Improving network security requires new network equipment

  Security, as a process, needs regular re-evaluation

• SAFE—security products, infrastructure, new network services, consulting, design, and implementation
Customer Qualifications

Hot buttons:

– Damage to company image after a security breach
– Legal liabilities resulting from a breach
– Lost revenues resulting from a breach
– Need for customer/supplier confidence in doing e-business with the company
– Fear of theft
– Fear of fraud
– Loss of employee morale
– Wireless security
Cisco Security Vision

Create Self Defending Networks with Auto-Response Capabilities

- Migration of security features into the network infrastructure
- A presence on the endpoint as well as the network edge
- Complimentary anomaly-based (coarse-grained) and signature-based (fine-grained) detection methods
- A proper trust and identity infrastructure
- Services
System-based Security Solution Required…

“Anyone can build a stop sign – or even a traffic light – but it takes a different mind-set entirely to conceive of a city-wide traffic control system.”

-Bruce Schneier, “Beyond Fear”

Cisco is Building it…
This is the Power of the Network. NOW.
Deploy Security as an Integrated System

- Secured Doors and Vaults
- Firewalls and Router ACLs
- Surveillance and Alarms
- Network and Host-based Intrusion Detection
- Patrolling Security Guard Scanner
- Security Room CCTV
- Centralized Security and Policy Management
- Card Readers
- Identity, AAA, Access Control Servers and Certificate Authorities
- Secure Transport
- Encryption and Virtual Private Networks (VPN’s)
Cisco Integrated Security Strategy

**Secure the Transport:**
- IPSec VPN
  Protects Data/Voice Confidentiality

**Defend the Edge:**
- Integrated Network FW+IDS
  Detects and Prevents External Attacks

**Protect the Interior:**
- Catalyst Integrated Security
  Protects Against Internal Attacks

**Guard the Endpoints:**
- Cisco Security Agent (CSA)
  Protects Hosts Against Infection

**Verify the User and Device:**
- Identity-Based Networking
  Control Who/What Has Access
Integrated Security Systems and Technologies

** PRIVACY **

**SECURE CONNECTIVITY SYSTEM**
Secure transport of applications across numerous network environments

** PROTECTION **

**THREAT DEFENSE SECURITY SYSTEM**
Collaboration of security and network intelligence services to minimize effects of known and unknown threats

** CONTROL **

**TRUST & IDENTITY MANAGEMENT SYSTEM**
Contextual identity required for entitlement and trust

**Management and Analysis**
## Cisco VPN: Brodest Solution Set

<table>
<thead>
<tr>
<th>VPN Family</th>
<th>Large Enterprises</th>
<th>Medium Enterprise</th>
<th>SMB Office</th>
<th>SOHO</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN 3000 Concentrators</td>
<td>3080 3060</td>
<td>3060 3030</td>
<td>3015 3005</td>
<td>3002</td>
</tr>
<tr>
<td>IOS VPN Routers and Switches</td>
<td>7600, 7300 7200, Cat6500</td>
<td>3600 3700</td>
<td>2600 1700</td>
<td>800 900</td>
</tr>
<tr>
<td>PIX Security Appliance</td>
<td>Cisco VPN Client</td>
<td>515E</td>
<td>506E</td>
<td>501</td>
</tr>
<tr>
<td>VPN Client</td>
<td>Cisco VPN Client</td>
<td>Cisco VPN Client</td>
<td>Cisco VPN Client</td>
<td>Cisco VPN Client</td>
</tr>
</tbody>
</table>

- Complete end-to-end solution for all applications
- Best VPN Client software for all popular platforms
- Best technical support anywhere—Cisco TAC
# Hot Topic: SSL VPN and IPSec VPN

Deployment Flexibility = Comprehensive Solutions

<table>
<thead>
<tr>
<th>SSL VPN</th>
<th>IPSec VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Anywhere access to a specific</td>
<td>• Robust remote access extending all applications</td>
</tr>
<tr>
<td>application set using a web browser</td>
<td>available in the office to remote users</td>
</tr>
<tr>
<td>All applications accessed through</td>
<td>All applications, all traffic types</td>
</tr>
<tr>
<td>browser portal</td>
<td>Client software allows for application transparency</td>
</tr>
<tr>
<td>Easy firewall traversal</td>
<td></td>
</tr>
<tr>
<td>Enables extranets/B2B commerce</td>
<td></td>
</tr>
<tr>
<td>• Client/server support requires</td>
<td>• Maximum functionality for managed computers</td>
</tr>
<tr>
<td>application specific applets</td>
<td>• Robust voice/video convergence</td>
</tr>
</tbody>
</table>
Web VPN Announcement

- Clientless SSL VPN on Cisco VPN 3000 Series Concentrator
- Software release in January (v4.1)
- Free upgrade for SMARTnet™ customers
- No additional hardware required
Integrated Security Systems and Technologies

**PRIVACY**
SECURE CONNECTIVITY SYSTEM
Secure transport of applications across numerous network environments

**PROTECTION**
THREAT DEFENSE SECURITY SYSTEM
Collaboration of security and network intelligence services to minimize effects of known and unknown threats

**CONTROL**
TRUST & IDENTITY MANAGEMENT SYSTEM
Contextual identity required for entitlement and trust

Management and Analysis
## Threat Defense System Technologies

<table>
<thead>
<tr>
<th>Category</th>
<th>Products/Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall</strong></td>
<td>PIX Security Appliance, IOS FW, Catalyst 6500 FWSM</td>
</tr>
<tr>
<td><strong>Network IDS</strong></td>
<td>IDS Appliances, Catalyst IDS Module, Router IDS Module, IOS-IDS</td>
</tr>
<tr>
<td><strong>Endpoint Agent Protection</strong></td>
<td>Cisco Security Agent (CSA)</td>
</tr>
<tr>
<td><strong>Network Services Security</strong></td>
<td>NetFlow, NBAR, CAR, Private VLANS, DHCP Snooping, Dynamic ARP Inspection, ACLs, QoS Features, CPU/Memory Limiting</td>
</tr>
<tr>
<td><strong>Intelligent Investigation</strong></td>
<td>Cisco Threat Response (CTR)</td>
</tr>
<tr>
<td><strong>Content Security</strong></td>
<td>Content Engines, Router Network Modules</td>
</tr>
<tr>
<td><strong>Security Management</strong></td>
<td>Device Managers, CiscoWorks VMS, ISC, CiscoWorks SIMS</td>
</tr>
</tbody>
</table>
Threat Defense System in Action

Endpoint Security
- Protects servers/desktops
  - Thwart buffer overflow
  - Control port connection
  - Validate access policy to ensure patch/AV compliance
  - Lock down system

Firewall/Access Control
- Limit worm propagation
- Control connection attempts
- Limit inbound to server (ingress)
- Disallow outbound to limit infection (egress)
- Validate protocol adherence

Network IDS/IPS
- Detects worm and propagation
- Attack identification
- Attack mitigation
- Forensics analysis

Content Security
- Proxy cache and web security
- Port 80 filtering
- URL filtering
- Store and serve clean content

L3-L7 Services
- Traffic classification/response
- Classify and control traffic (NBAR)
- Deploy CAR to rate limit traffic
- Prioritize traffic (QoS)
- Use “sink hole” routing to detect/drop worm propagation
- CPU/memory thresholding
- Autosecure

L2 Services
- Minimize infection
- Segment network (Private VLANs)
- DHCP snooping
- Dynamic ARP inspection
- PortFast BPDU Guard
- Port Flood Blocking

Management
- TDSS system management
- Unified security monitoring
- Coordinated device configuration
CSA: Single Agent Endpoint Protection

Cisco Security Agent offers a Common and Consolidated Solution for BOTH Desktops and Servers

CSA Desktop Protection:
- Distributed Firewall
- Day Zero Virus/Worm Protection
- File Integrity Checking
- Microsoft Office protection
- Instant Messenger security
- Security for other applications

CSA Server Protection:
- Host-based Intrusion Prevention
- Buffer Overflow Protection
- Day Zero Virus/Worm Protection
- Operating System Hardening
- Web Server Protection
- Security for other applications
Endpoint Protection with Cisco Security Agent – “MyDoom” Virus

Screen Shot – Desktop

Default action will be taken in 4 minutes:10 seconds

Cisco Security Agent. A problem was detected, press one of the action buttons below.

Potential worm propagation: The process 'D:\Documents and Settings\hsaidi\My Documents\email\Attach\test.pif' has read downloaded content (file D:\Documents and Settings\hsaidi\My Documents\email\Attach\test.pif) and is accessing an email or network related resource (hsaidi.wab). This is considered suspect. To prevent further execution, choose 'Terminate' below.

Yes

Terminate
Integrated Security Systems and Technologies

**PRIVACY**

**SECURE CONNECTIVITY SYSTEM**
Secure transport of applications across numerous network environments

**PROTECTION**

**THREAT DEFENSE SECURITY SYSTEM**
Collaboration of security and network intelligence services to minimize effects of known and unknown threats

**CONTROL**

**TRUST & IDENTITY MANAGEMENT SYSTEM**
Contextual identity required for entitlement and trust

Management and Analysis
Identity Is a Growing Requirement

- Too easy for an unsecured individual to gain physical and logical access to a network
- A network port is either enabled or disabled
- Dynamic configuration (DHCP) is plug and play
Trust & Identity
Controlling “Who” gets access and “What” they can do

Identity Based Networking Services and Management

Controls “who” has Access to the Network

Controlling “what” users can access (User/Device Policies)

Today

Available Q2 CY04

Detects And Isolates Non Complaint Users & Devices

Future
802.1x

- Key component of IBNS
  Identifies who can access what
  Focused primarily on switches
- Restricts unauthorized devices from connecting to a LAN through publicly accessible ports
  Key technology in IBNS for authentication and access control
- Works between supplicant (client) and authenticator (network device)
- Maintains backend communication to an authentication (RADIUS) server

802.1x are supported on all Cisco Catalyst switches, including Catalyst 6500, 4500, 3550, and 2950 Series switches, Cisco ACS Server as well as Cisco Aironet 1100 and 1200 Series products
IEEE 802.1x

802.1x is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

1. User activates link (ie: turns on the PC)
2. Switch requests authentication server if user is authorized to access LAN
3. Authentication server responds with authority access
4. Switch opens controlled port (if authorized) for user to access LAN
Cisco Network Admission Control (NAC)

- Cisco-led, multi-partner program
  Limits damage from viruses, worms, etc.
- Limits network access to compliant, trusted endpoints; restricts access by non-compliant devices
  - Endpoint device interrogated for policy compliance
  - Network determines appropriate admission enforcement: *permit*, *deny*, *quarantine*, *restrict*
- Phase I of Cisco Self-Defending Network Initiative
  Dramatically improves network’s ability to identify, prevent, and adapt to threats
Integrated Security Systems and Technologies

**PRIVACY**

**SECURE CONNECTIVITY SYSTEM**
Secure transport of applications across numerous network environments

**PROTECTION**

**THREAT DEFENSE SECURITY SYSTEM**
Collaboration of security and network intelligence services to minimize effects of known and unknown threats

**CONTROL**

**TRUST & IDENTITY MANAGEMENT SYSTEM**
Contextual identity required for entitlement and trust

Management and Analysis
Embedded Device Managers for Security
Small Network Management (1–5 Devices)

- Each platform offers a web-based embedded device manager

  Cisco VPN 3000 Device Manager
  Cisco PIX Device Manager
  Cisco Security Device Manager
Cisco Management Overview

- **Embedded Device Managers**
  Web-based management suitable for remote access and small site-to-site environments

- **Management Applications**
  Element-centric packages for homogenous platform deployments
  Network-centric, policy-based applications for heterogeneous and more complex networks and topologies

- **AVVID Security Partner Management Applications**
  Certified partners leverage advanced Cisco device manageability for multi-vendor environments

- **Traditional Management Interfaces**
  CLI, Telnet, SSH, etc.
Securing the Smaller Office Example

Possible remote site

Security SCALABLE with Business Needs

SECURITY CHALLENGES
- Protect business communications
- Prevent malicious traffic, threats, worms, etc.
- Adopting new network services/apps w/o performance impact
- Little to no remote IT staff

SECURITY SOLUTIONS
- Software agents protect key servers and desktops
- Router embedded security services (FW,VPN,IDS)
- Router integrated VPN, IDS modules for high-performance secure connectivity and threat prevention
- Identity services manage authorized device/user access
- Intuitive and easy to use management
Challenge

- Upgrade from a frame relay network to an IP network to position itself for business in the new century
- Provide security for a leading-edge network that would use the public Internet to save on phone costs and boost productivity by limiting Web browsing to business-related sites

Solution

- Remote Access Solution based on AVVID architecture, PIX Firewall, 3600 Series Routers, 2924 & 3548 XL Switches.
- Users at branch offices are connected through 10 Mbps switched Ethernet, while the head office uses 100 Mbps switched Ethernet.

Results

- Cost savings have started to roll in.
- Employee productivity increase based on a faster and more secure Network

“Cisco AVVID made it easy to implement the firewall with the Cisco switches because all the products are under the same umbrella. Cisco is known; it’s reliable...The PIX Firewall made us feel secure.”

Sheldon Guenther
Network analyst
Lockerbie & Hole.
Graphic Design Agency

Challenge:
- Clients demand aggressive scheduling
- Repeated reviews and changes extended project completion time
- Possibility of loss or damage
- Need to accommodate a continually changing and growing community of partners and customers

Solution:
- Adding VPN capability to its existing Cisco network enabled the agency to exchange creative materials over the public Internet with the same level of security, manageability, and quality of service as a private network — at a fraction of the cost.

Results:
- Reduced courier charges by more than 75%
- Reduced total turnaround time for projects
- VPN access to select major accounts results in closer customer relationships
- Mobile employees connect to the office network
PROGRAMS AND TOOLS FOR CHANNEL PARTNERS

www.cisco.com/ca/smbpartnerconnections
Hot “Security Bundles”

- **Cisco Security Agenda (CSA) bundle**
  - (1) server, (10) desktop licenses and VMS pass-through: C$4350

- **NIDS + CSA bundle**
  - (1) 4215 + CTR+ CSA bundle: C$13043

- **NMIDS + CSA bundle**
  - NMIDS + IOSFW+ CTR+ CSA bundle: C$10143
Ongoing Security Channel Promotions

Cisco Security Agent Special Pricing
- Effective dates: AUG 18, 2003 to JUL 24, 2004
- Cisco VPN/Security Specialized Resellers and those participating in the Value Incentive Program (VIP) under VPN/Security can now receive additional discounts on the Cisco Security Agent product family

CSA Opportunity Registration Page link
- [http://www.cisco.com/cgi-bin/front.x/AppTool/controller.cgi](http://www.cisco.com/cgi-bin/front.x/AppTool/controller.cgi)

Specialized Partner Discount Program (SPD)
- The Specialized Partner Discount gives you up to an additional 7% discount on products included in your VPN Security specialization

Cisco Success Builder Program
- A Program designed to recruit new SMB customers.
- Partners get min. 45% off Canadian product & SMARTnet list prices.

Visit the Channel Programs and Promotions Page for more information: [www.cisco.com/ca/smbpartnerconnections](http://www.cisco.com/ca/smbpartnerconnections)
SMB Solution Designer

- Design a custom network solution for your SMB customer
  Network Foundation
  Security
  IP Communications
  Mobility

- Educate Potential Customers

- Print or Email the network design to your customer.

- Vertical Solutions soon!

www.cisco.com/go/solutiondesigner
SMB Solution Designer - Reseller-customized Versions

- Specialized partners may leverage Solution Designer as a call-to-action in their own demand generation programs.
- All leads generated by this custom version are routed back to the originating partner and that partner’s account manager.
- Users asking to ‘talk to an expert’ are sent to the web location of the partner’s choosing.
- Partners may include their own logo in the tool.

Registration: www.cisco.com/go/sdpartner
Partner Example: www.ciscowebtools.com/go/praxis
SMB Partner Connections Site for Canadian SMB Resellers

- Portal to help improve your knowledge on Cisco SMB class business & technology solutions and help you better address your customer needs.

- One Stop Shop for:
  - Sales & Technical Resources
  - Canadian Promotions
  - On Line Training & Seminars
  - Key collaterals

www.cisco.com/ca/smbpartnerconnections
Sales Tools for SMB Class Security Solutions

Sales Tools include

- Solution Blueprints
- Solution Overview
- White Paper
- Implementation Guides
- Case Studies
- Scripted “How to Sell” & “Why to Buy” Presentations
- Demand Generation Resources

www.cisco.com/ca/smbpartnerconnections   CLICK ON SMB CLASS!
## Cisco Security and VPN Product Portfolio

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-Site VPN/Firewall Routers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cisco SNMS</td>
</tr>
<tr>
<td>SOHO</td>
<td>501</td>
<td>VPN 3002</td>
<td>New</td>
<td>Identity Appliances</td>
<td>Embedded Device Managers for Security Devices</td>
</tr>
<tr>
<td>800</td>
<td>506E</td>
<td>VPN 3005</td>
<td>New IDSM-2</td>
<td></td>
<td>Security Device Manager 1.0</td>
</tr>
<tr>
<td>1700</td>
<td>515E</td>
<td>VPN 3015</td>
<td>New 2600, 3600, 3700series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2600</td>
<td>525</td>
<td>VPN 3030</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3600</td>
<td>535</td>
<td>VPN 3060</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3700</td>
<td></td>
<td>VPN 3080</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New! 830</td>
<td>New!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New! 1760</td>
<td>New!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New! 2600 XM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Cisco Security Strategy: Key Differentiators

<table>
<thead>
<tr>
<th>COLLABORATION BETWEEN NETWORK AND SECURITY TECHNOLOGIES</th>
<th>FLEXIBLE, CUSTOMIZABLE DEPLOYMENT</th>
<th>COMPREHENSIVE COVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seamless integration into IP Services: Data, Voice, Video, Wireless, Storage</td>
<td>Leverage Existing Investments: Platform Options: Dedicated Security Appliances, Router-Based, Switch-Based Security Technology Options: VPN, Firewall, Threat Protection, AAA, URL Filtering, 802.1x, Behavioral</td>
<td>Security Integrated into All Platforms: Including PCs and Servers Across all of the Network: Wireless, LANs, Campus, Metro, Edge, Service Providers, Branch Offices…</td>
</tr>
</tbody>
</table>
Trust Cisco to Provide Leadership

Cisco Spent $200M on Security R&D (FY '03)

We’re a Partner You Can Trust

- Free software fix and workaround to minimize risk of potential network attacks
- 24x7 support from Cisco’s Technical Assistance Center
- Honest and responsible communication with all Cisco channel partners and customers
Many Vendors

Customers’ Current Environment
One Vendor

ONE VENDOR HELD ACCOUNTABLE
In Closing…

GOAL: ALIGN COMPANY’S SECURITY STRATEGY WITH THE BUSINESS STRATEGY

• The threats are here to stay, are changing, and we must evolve
• Our connected world is the target, not one piece or one company
• Cisco remains committed to help protect our customers with its security vision, and product channel partners
• Integrated Security Strategies are how to approach these issues…
  Integrated Security Strategy aligns security investments with the business requirements
  Knowledgeable people, business processes, and the application of technology all form a system solution…all three are key
  Architecting an Integrated Security Strategy begins with a current security posture and evolves with continuous improvements
More Information

- www.cisco.com/go/smbpartnerconnections
- www.cisco.com/security
- www.cisco.com/go/safe
- www.cisco.com/go/netpro
- www.cisco.com/go/securitypartner
- www.nsa.gov
  (Cisco router recommendation guide)
- www.cisco.com/go/aironet/security
Q AND A