Campus Security

Cisco Self-Defending Network

2004.7.8

Cisco Systems, Korea

Bang, Hang Mo (banha@cisco.com)

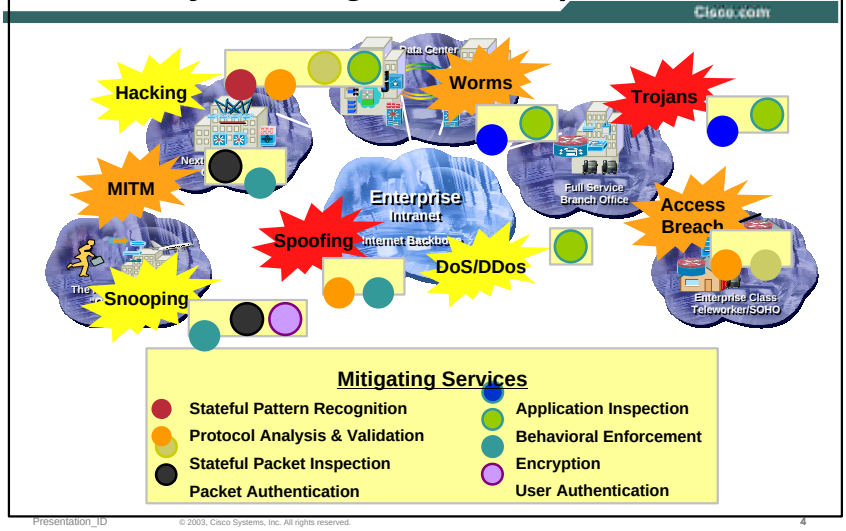
Agenda

Cisco.com

- Evolution of Security Challenge
- Cisco Self-Defending Network
- Cisco Security Agent
- Network Admission Control
- Cisco DDoS prevention Solution
- Summary

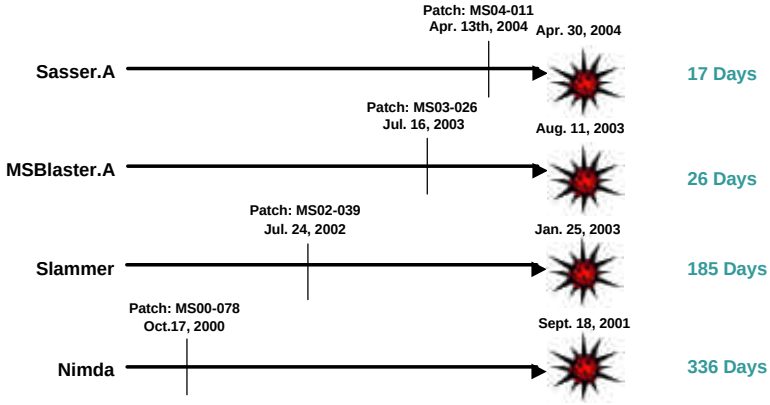
Evolution of Security Challenge

Security Challenges Are Complex



Window of Time from Patch Availability to Outbreak Getting Shorter

Cisco.com



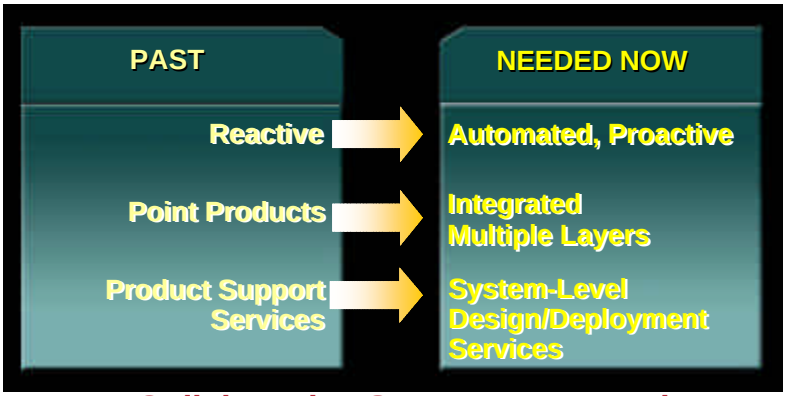
Customers need an innovative systems approach to preventing and containing infections

The Security Situation

Cisco.com

- **Threat environment has reached unprecedented levels of complexity**
  - **Multiple types of security threats**
  - **Fast spreading**
- **No single technology or device stops everything**
  - **Security functions are compartmentalized**

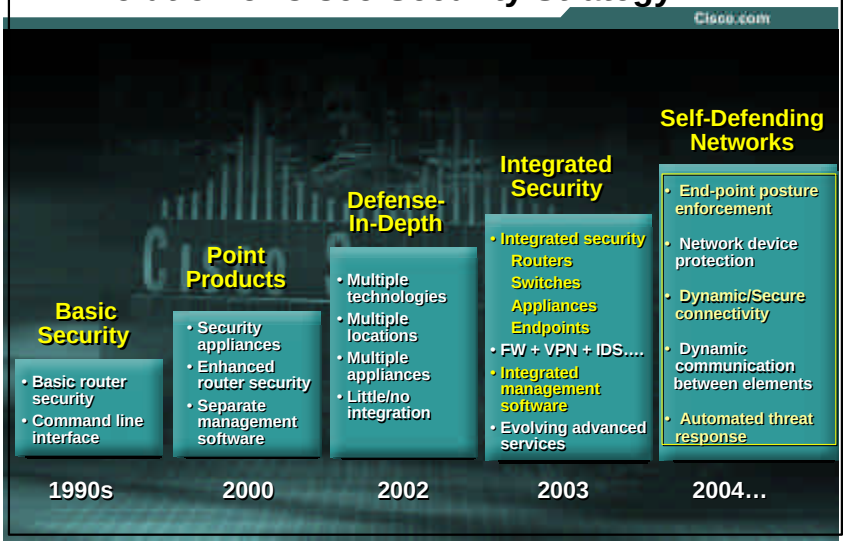
What Worked in the Past Can't Meet Today's Threats



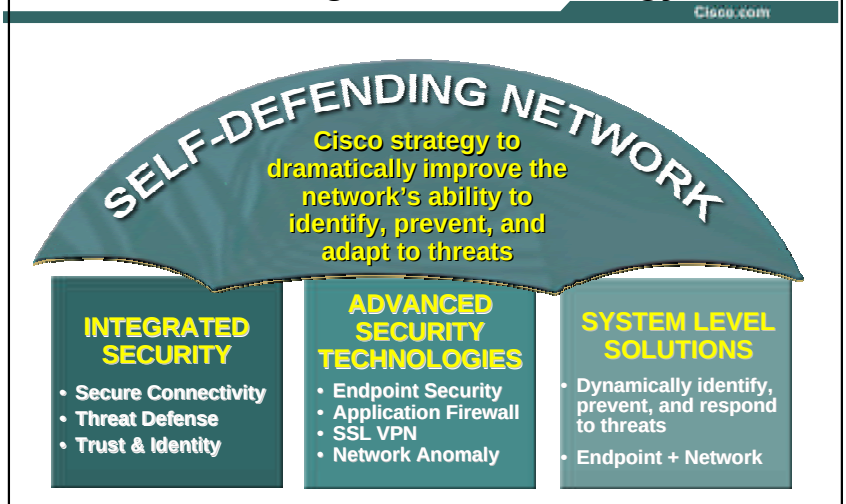
A Collaborative Systems Approach

Cisco Self-Defending Network

Evolution of Cisco Security Strategy



Self Defending Network Strategy



Security Architecture
Defense in Depth : Self-Defending Architecture

Cisco.com

Enforce **who has access** to the network

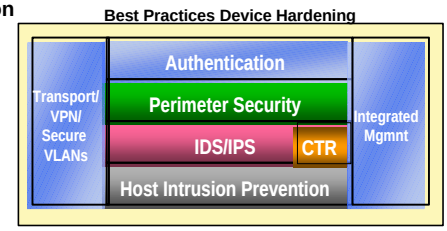
Enforce **what network services can be accessed**, DDoS protection

Look into the packet, make sure traffic is valid, alarm or respond

Evaluate server and host behavior to ensure an attack has not circumvented the first three layers

Encrypt/VLAN critical traffic to to ensure Data security

Effective security is accomplished via an "defense in depth" approach. If one layer is bypassed by an attacker they still face other layers before they reach critical network resources.



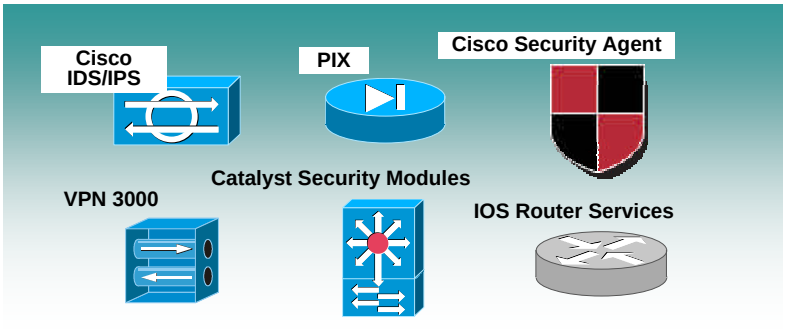
Self Defending Network:
A Network-Based Systems Approach

Cisco.com

- An **automated** security system to address **"Day Zero" threats**
- Security is applied at **multiple layers** to defend against multiple avenues of attack
- **Flexible deployment of integrated security** enables **defense-in-depth** and reduces cost
- **Proactive and adaptive** system protects against a new breed of threats

Cisco Security Solutions

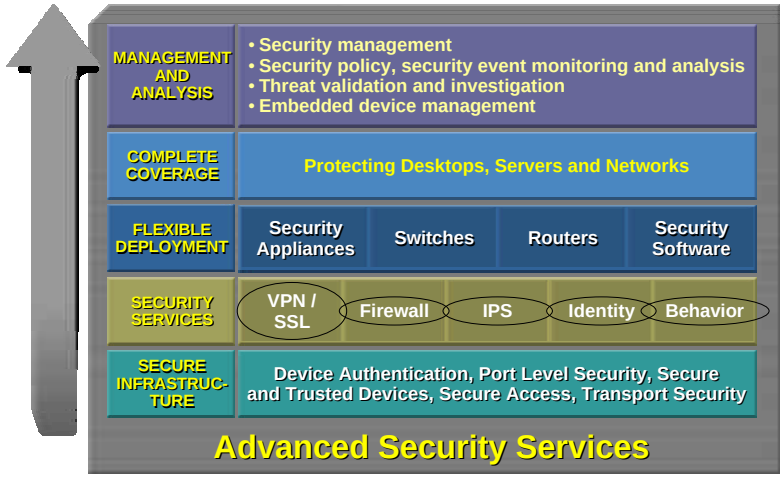
Comprehensive Threat Defense and Secure Connectivity



Mitigating Services

- Stateful Pattern Recognition
- Protocol Analysis & Validation
- Stateful Packet Inspection
- Packet Authentication
- Application Inspection
- Behavioral Enforcement
- Encryption
- User Authentication

Cisco Integrated Security Portfolio



Cisco Delivers Integrated Security Systems

Threat Defense, Secure Connectivity, Trust & Identity

Cisco.com

Threat Defense

Infrastructure Security
- Network Fabric Protection

Protect device, mitigation & availability

Patrol the Edge:
- Intrusion Detection and Prevention

Detects Network Attacks

Protect the Interior:
- Firewalling

Protects Against Network Attacks

Guard the Endpoints:
- Cisco Security Agent (CSA)

Protects Hosts Against Threats

Trust & Identity

Verify the User and Device:
- Identity and Policy Servers

Control Who/What Has Access

Secure Comm.

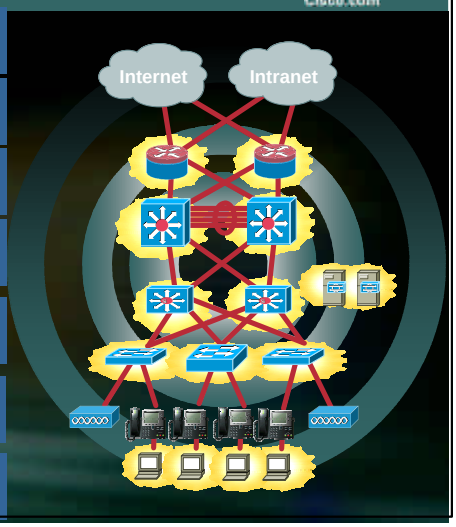
Secure Transport:
- IPSec and SSL VPN

Protects Data/Voice Confidentiality

Mgm't

Integrated Management:
- CiscoWorks VMS

Operational Integration Across Services



Cisco.com

Endpoint Security
Cisco Security Agent

Security Challenges for the Enterprise

Cisco Security Agent for Zero-Day Protection

Cisco.com

Business Challenge	Cisco Security Agent takes you…
• **Day Zero attacks**	✓ **To Zero-Update Protection**
Rapidly propagating attacks evade signature recognition	Stops new attacks with no signatures to manage
• **Point product challenges**	✓ **To a Single Agent**
Reactive products (PFW, etc.) fail to address the problem	Aggregates multiple security functionality in one agent
Requires multiple agents and management paradigms	HIPS, Day-zero protection, firewalling and OS lockdown
• **Reactive Patching & Patch Management**	✓ **To Scheduled Maintenance**
Increasing # of vulnerabilities makes the task of patching systems an 'update race' without end	Wait for 'roll-ups' and Service Packs, which come better qualified from vendor
	Testing and implementation of updates can be scheduled without undue change control interruption

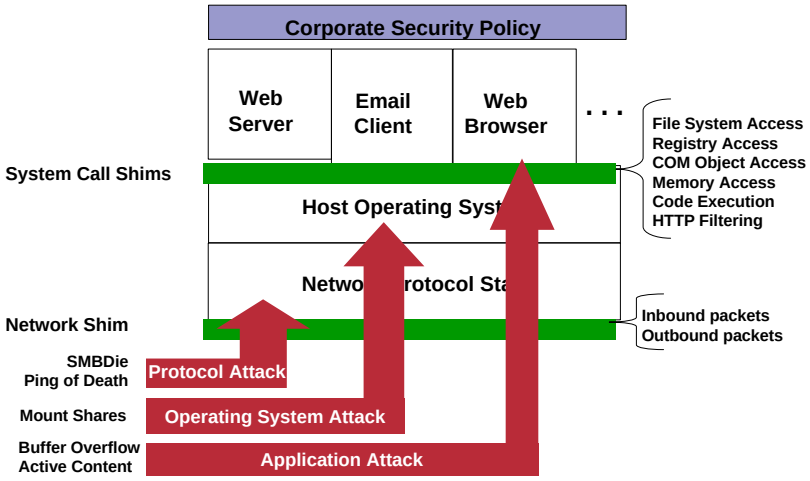
Cisco Security Agent

Cisco.com

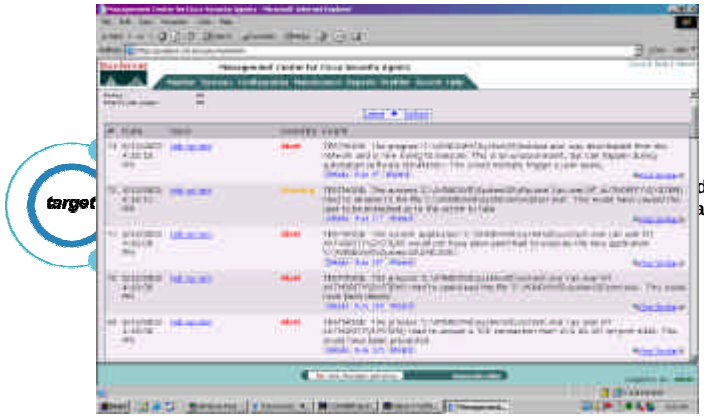
- **Next-generation security solution**
  - **Threat protection for servers and desktops**
- **Identifies and prevents malicious behavior before it occurs**
- **Unique behavior analysis addresses known and unknown threats**
- **Protected against:**
  - Mydoom
  - Fizzer
  - Sobig.E
  - Sircam.A
  - Nimda
  - W32.Blaster
  - Bugbear
  - SQL Slammer
  - CodeRed
  - W32.Netsky

  and more, with NO signature updates!

CSA (Cisco Security Agent)
Behavior Control Protects End Points

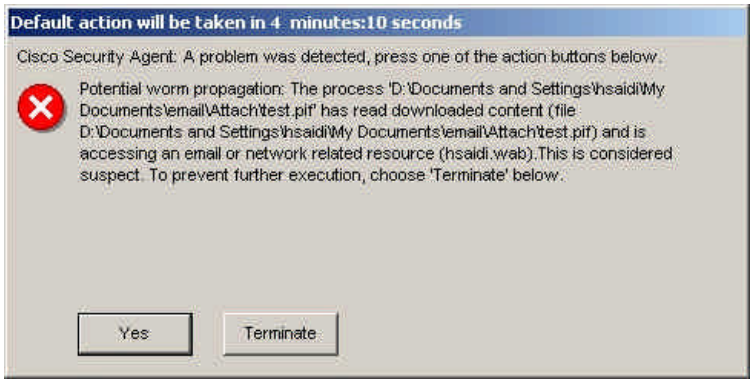


2003: MSBlast/LovSan



d'.
age is

Cisco Security Agent
"MYDOOM" Screen Shot – Desktop Device

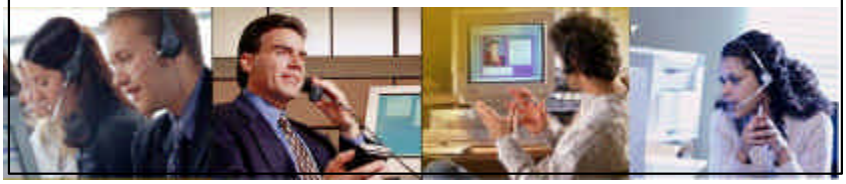


Network Admission Control
(Phase 1 of SDN)

Customer Problems with Host Security

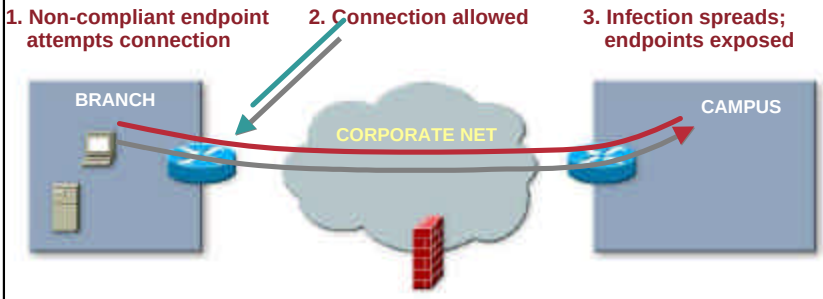
Cisco.com

- **Viruses and worms continue to disrupt business**
- **Day-zero attacks make reactive solutions less effective**
- **Point technologies preserve host rather than network availability and enterprise resiliency**
- **Non-compliant servers and desktops common, difficult to detect and contain**
- **Locating and isolating infected systems time and resource intensive**



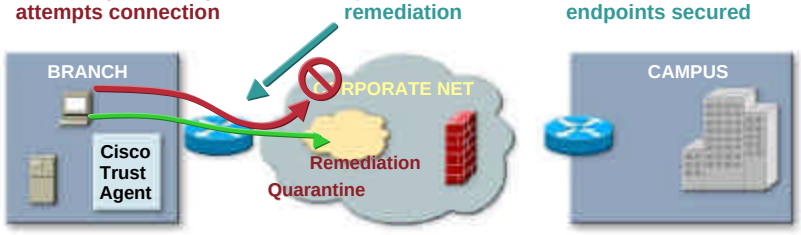
Why Network Admission Control?

Cisco.com

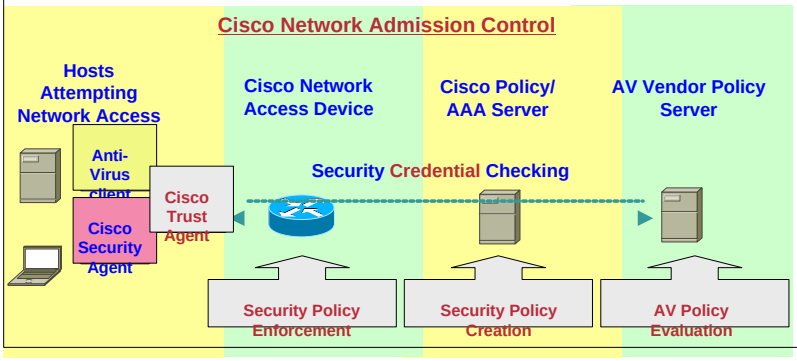


Cisco Network Admission Control

1. Non-compliant endpoint attempts connection
2. Quarantine/ remediation
3. Infection containment; endpoints secured



Cisco Network Admission Control (NAC)

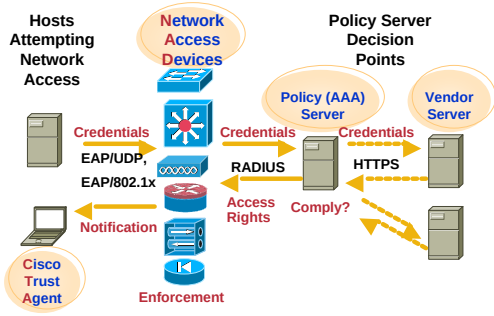


- Based on endpoint security posture, appropriate admission policy will be enforced in the network
- Cisco & NAC co-sponsors to deliver this collaborative solution

Cisco NAC Solution

Cisco.com

NAC Solution: Leverages the network to intelligently enforce access privileges based on endpoint security posture



NAC Characteristics:

- Ubiquitous solution for *all* connection methods
- Validates *all* hosts
- Leverages customer investments in Cisco network and AV solutions
- Supports Multiple AV vendors & Cisco Security Agent
- Quarantine & remediation services
- Deployment scalability

NAC Deployment Scenarios

Comprehensive Compliance Validation

Cisco.com

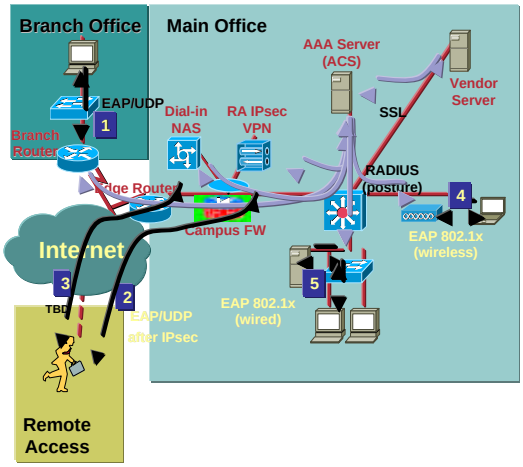
1: Branch office compliance
- Enforce on L3 router and firewall

2: Remote access compliance
- Extension of "Are You There"

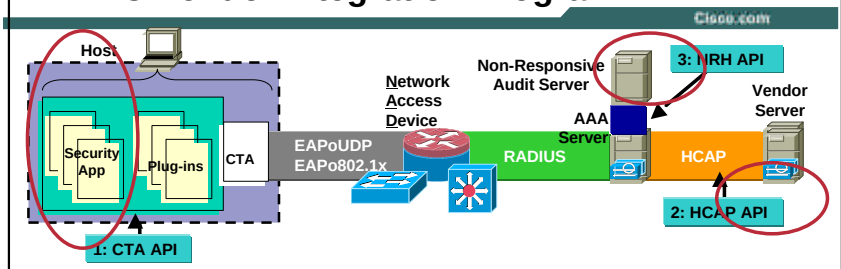
3: Dial-in access compliance

4: Wireless campus protection
- Quarantine with ACLs/VLANS
- Extension of 802.1x

5: Campus Access and data center protection
- Quarantine with ACLs/ VLANS
- Extension of wired 802.1x

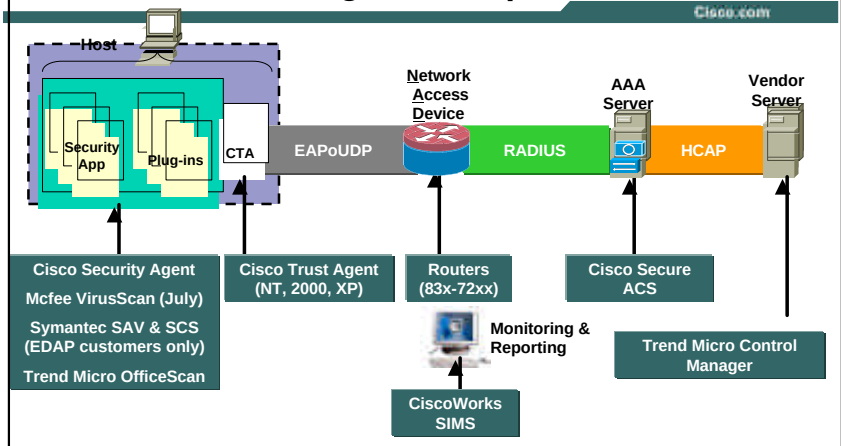


NAC Vendor Integration Program

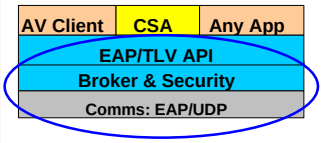


- Broad NAC licensing program for vendor integration
  - Standard, open process, boilerplate licensing agreement
  - Non-royalty & no-cost distribution of CTA
- Phased API availability to vendors through 2004
  - CTA API: host applications tie into posture analysis
  - HCAP API: vendor policy servers assist posture assessment
  - NRH API: audit servers assess non-responsive devices

NAC Phase 1 Logical Components



Cisco Trust Agent (CTA)

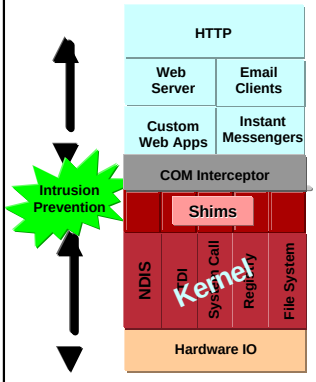


Cisco Trust Agent

- Endpoint agent for communications
  - Windows NT, XP, 2000
- Performs three primary functions
  - Network comms (EAPoUDP)
  - Application comms (EAP/TLV broker)
  - Authenticate ACS & encrypt comms
- Application integration
  - Initial focus: OS & AV patches
  - Co-sponsors: NAI, Symantec, Trend Micro
  - Muxes & demuxes EAP posture reqs between registered application (vendor & app type = ID)
- Availability
  - No charge component, available from CCO
  - Licensees *may* redistribute for free

CSA Integration

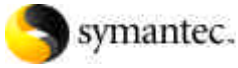
Kernel Shim Wrappers



- CSA a valuable optional component
  - CSA receives no special privileges vs vendor apps
- Offers OS credentials & endpoint integrity
  - Provides OS info including patch & hotfix
  - Hardens endpoint, more immune to attack
  - Protects CTA from application spoofing
- NAC Support
  - CSA 4.0.2 integrated with CTA/NAC
  - CSA 4.5 bundles CTA for distribution

Vendor Integration

Cisco.com



- **NAI / Mcfee**
  - VirusScan 8.0i integration (July), and 7.0, 7.1
  - ePO integration & CTA bundling timeline TBD
- **Symantec**
  - Enterprise Development Alliance Program (EDAP) support in 2004, commercial in 2005
  - SAV 9.0 [AV] & SCS 2.0 [AV, FW, HIDS] integration (June)
  - Policy manager integration (target Nov)
  - CTA bundling timeline TBD
- **Trend Micro**
  - OfficeScan Corporate Edition & Trend Micro Control Manager integration (June) -- OfficeScan CE 6.5
  - CTA bundled in OfficeScan
- **IBM**
  - Tivoli integration planned, timeline TBD

Credentials Validated

Cisco.com

FROM CISCO AGENTS

- **CTA 1.0**
  - CTA version
  - Operating system name
  - Operating system version
- **CSA 4.0.2**
  - Installed Service Packs
  - Installed hotfixes
  - CSA version
  - CSA enabled or disabled
  - FQDN of CSA-MC (VMS)
  - CSA status
  - Last poll of CSA-MC (VMS)

FROM VENDORS

- **Anti-Virus**
  - AV software name or identifier
  - Software version
  - Scan engine version
  - DAT/pattern file version
  - AV enabled or not
  - On-access scan enabled
  - DAT/pattern file release date
- **Other Software**
  - Varies by vendor
  - E.g. SYMC SCS 2.0 includes FW & HIDS

Other Required Credentials Not Recognized By ACS Can Be Forwarded to Vendor Policy Server for Validation

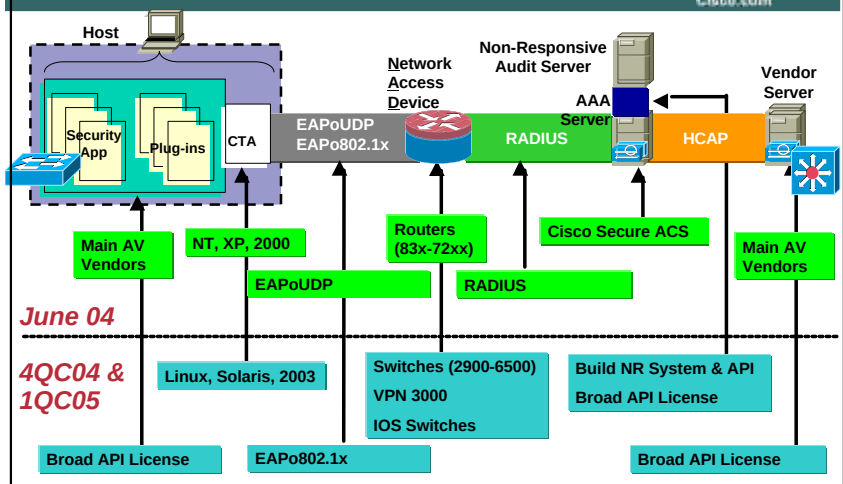
CiscoWorks Security Information Management Solution (CW SIMS)

- Collects and interprets IOS syslog and ACS events
- Real-time monitoring
  - NAC dashboard
  - Summary and detailed drill-down views
- NAC reporting
  - Compliance reports by network device, group, user
  - Enforcement actions
  - Rejected hosts and host remediation time
  - Application posture
  - Application credential posture
  - Administrative responsibility

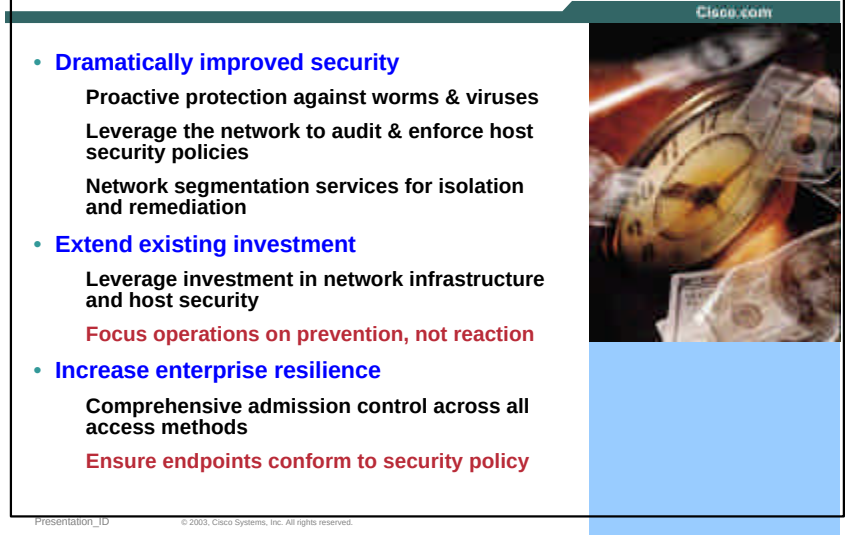
Switch Support (NAC Phase 2)

- Differentiated LAN access based on host policy compliance
  - L2 port support
  - 802.1x and non-802.1x based environments
  - Single host, IP phone, and shared media scenarios
- L3 aggregation switches provide gateway router NAC support
- 802.1x supplicants
  - LAN 802.1x will require supplicant support

NAC Phase 2 Logical Components

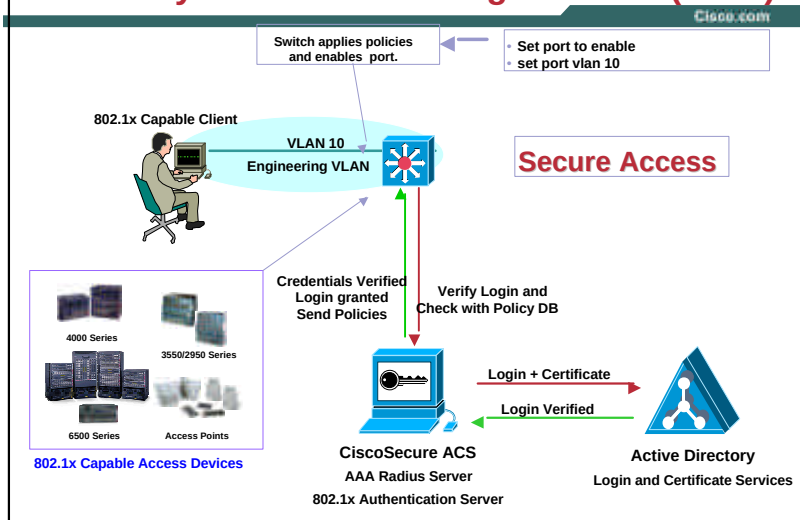


NAC Customer Benefits



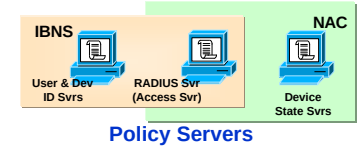
- **Dramatically improved security**
  - Proactive protection against worms & viruses
  - Leverage the network to audit & enforce host security policies
  - Network segmentation services for isolation and remediation
- **Extend existing investment**
  - Leverage investment in network infrastructure and host security
  - Focus operations on prevention, not reaction
- **Increase enterprise resilience**
  - Comprehensive admission control across all access methods
  - Ensure endpoints conform to security policy

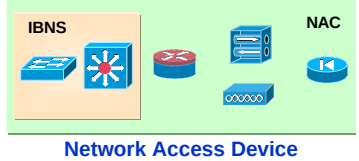
Identity Based Networking Services (IBNS)

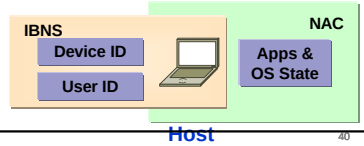


Ties to User & Device ID (IBNS)

- **IBNS**
  - Focused in access layer
  - Leverages 802.1x (L2)
  - Access based on user & device ID
  - Enforces with VLANs
- **NAC**
  - Covers all access methods
  - Leverages IP & 802.1x (L2 & 3)
  - Device state (OS & app)
  - Enforces with VLANs, PACLs, ACLs
- **Convergence**
  - L2 switch ports using 802.1x
  - Provide combined access policy
  - User ID, device ID, & device state







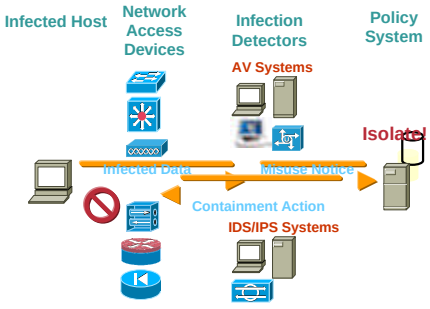
Cisco NAC Roadmap

	Phase 1 Current	Phase 2 2H CY04	Phase 3 1H CY05
Network Devices	IOS Routers 17xx – 72xx	Switches Wireless APs VPN 3000	Security Devices
Cisco Trust Agent Support	Windows NT, 2000, XP	Windows 2003 Red Hat Linux Solaris	IP Phones Cisco Appliances MAC OS, HPUX, AIX
Partner Integration	AV Vendors	OS Vendors Mgmt Vendors	Broadly expand partners
Device Communications	Layer 3 EAP/UDP	Layer 2 EAP/802.1x	HTTP/SSL
Non-Responsive Endpoints	Exception List Single Policy	Differentiated Policy	Download Applet
Quarantine Method	Layer 3 ACLs	VLANs, PACLs, 802.1X DHCP, Layer 3 ACLs	QoS

Network Infection Containment (NIC)

Objective: Greatly improve the ability to quickly contain virus infections

Strategy: Leverage the network to dynamically enforce access privileges based on endpoint behavior



- **Detect virus infections** leveraging multiple sensing technologies
- **Determine policy to apply:** isolate, content filter, re-route, adjust QoS
- **Appropriate and closest network access device dynamically enforce new policy**

Cisco DDoS Prevention Solution

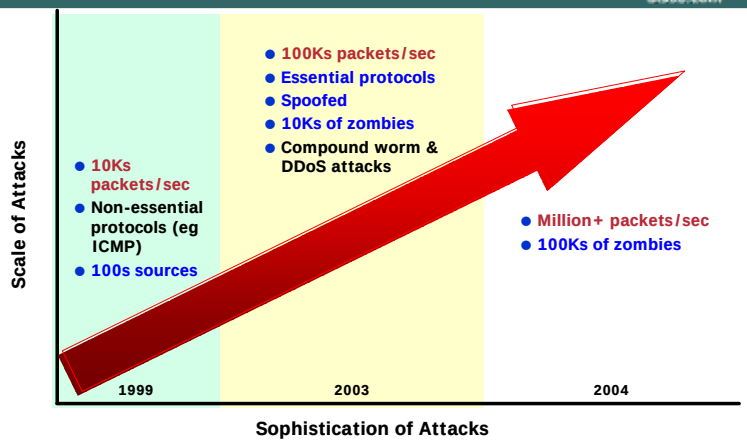
DDoS Problem Getting Worse

- **Frequency of attacks is increasing**
  - **Only cyber attack to grow in 2003***
  - **Second-most common security breach in 2003****
  - **Matches intrusion as the greatest concern of security executives†**
- **Specific sites & industries targeted to disrupt operations**
  - **E-commerce**
  - **Online betting**
  - **Online retail**
  - **Service providers**
- **Power of attacks is unprecedented - Not just SYN floods anymore**
  - **Hybrid and dynamically morphing attacks**
  - **100ks of Zombies**

* 2003 CSI/FBI Computer Crime & Security Survey ** *InformationWeek* U.S. Security Survey 2003 † *CSO Magazine* Security Sensor III & IV Research

Attack Evolution

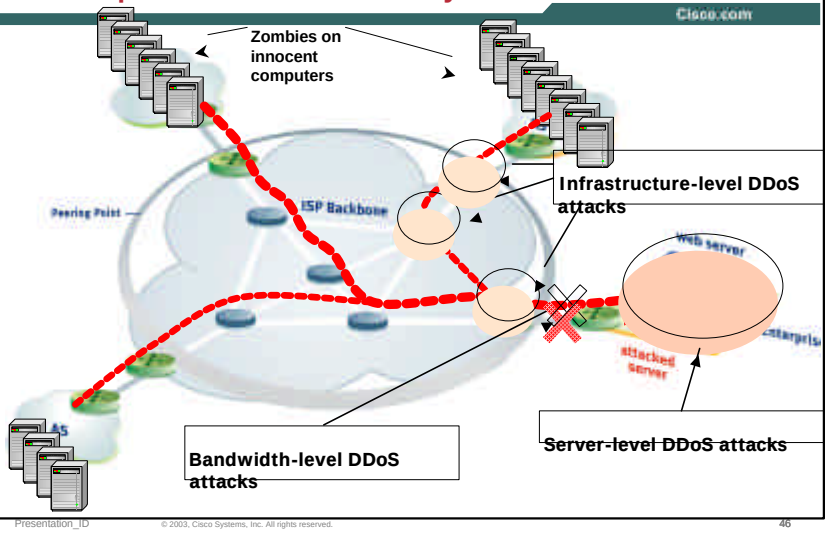
Cisco.com



Distributed Denial of Service

Multiple Points of Vulnerability

Cisco.com



Cisco Networks Purpose-built Solutions

Cisco.com

Cisco Guard XT 5650:

- Attack analysis & mitigation
- Diverts traffic for on-demand protection
- 2 GE Fiber/Copper
- 10/100/GE Copper Mgmt

Cisco Guard XT 5650

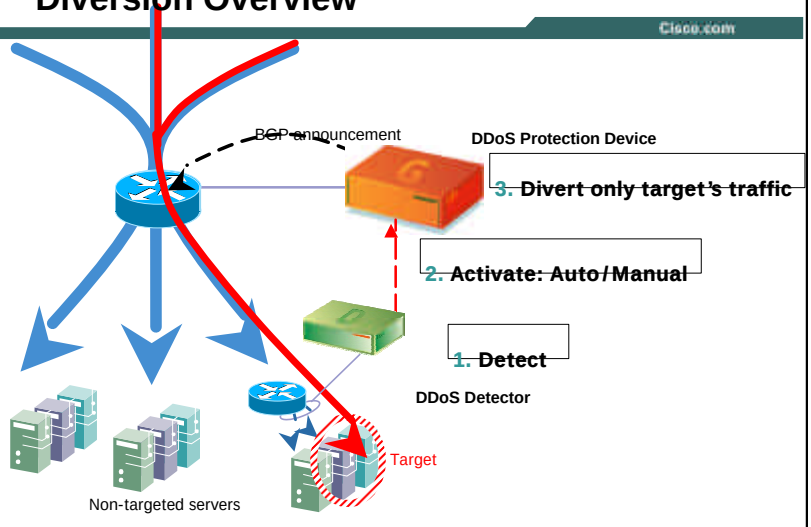
Cisco Traffic Anomaly Detector XT 5600:

- Attack detection & identification
- Monitors copy of traffic
- Same Interfaces as Guard

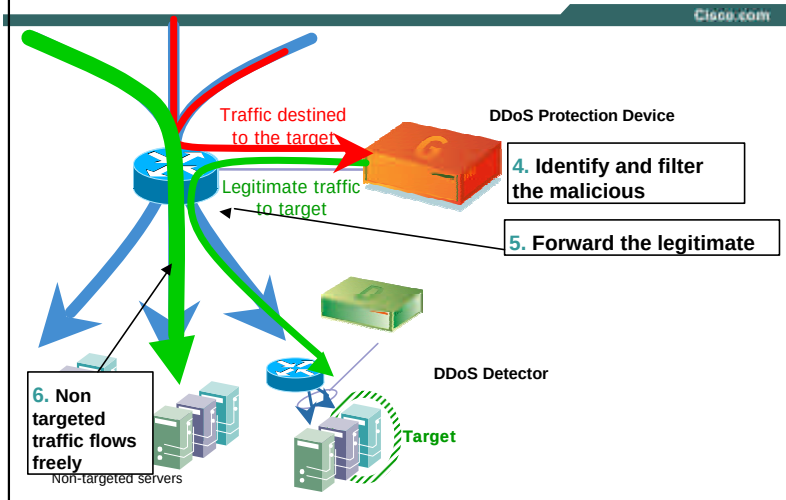
Cisco Traffic Anomaly Detector XT 5600

Diversion Overview

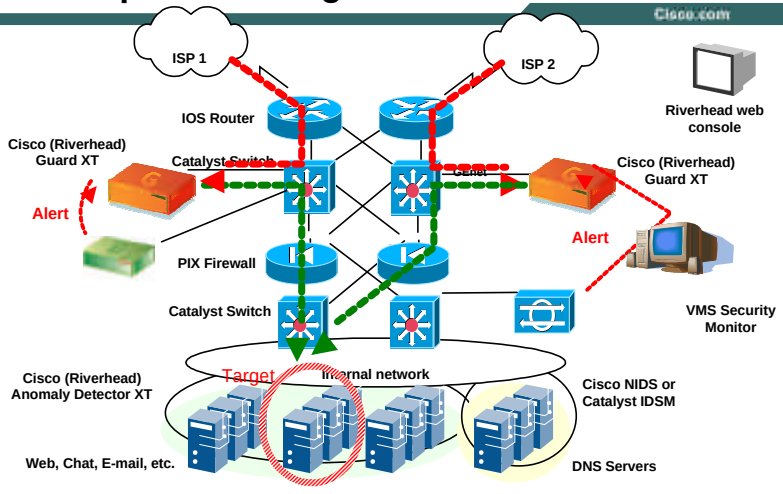
Cisco.com



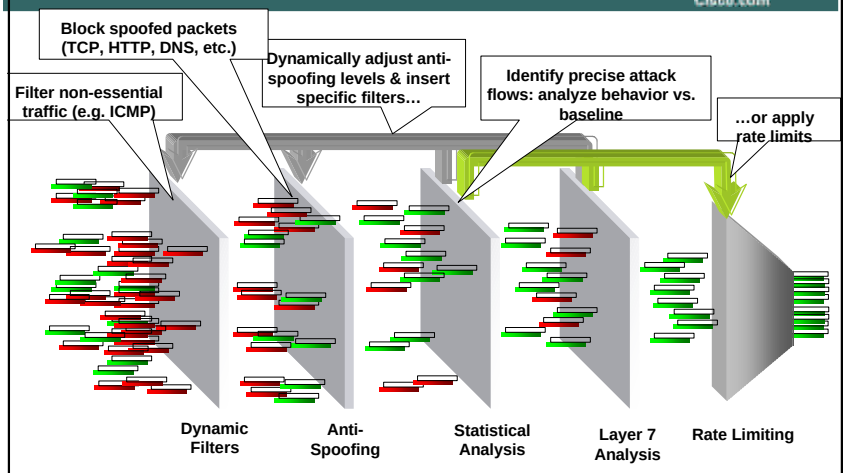
Diversion Overview



Enterprise/Hosting/Data Center



Multiple Layers of Defense

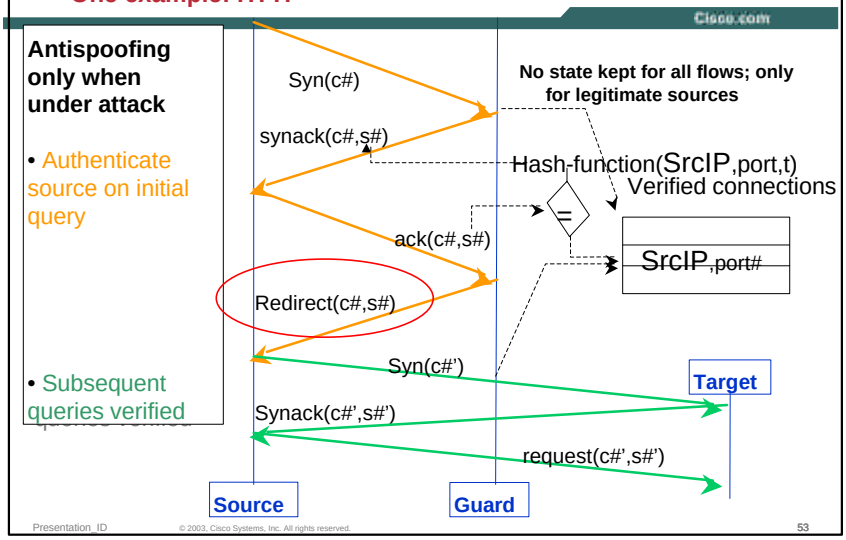


Anti-Spoofing

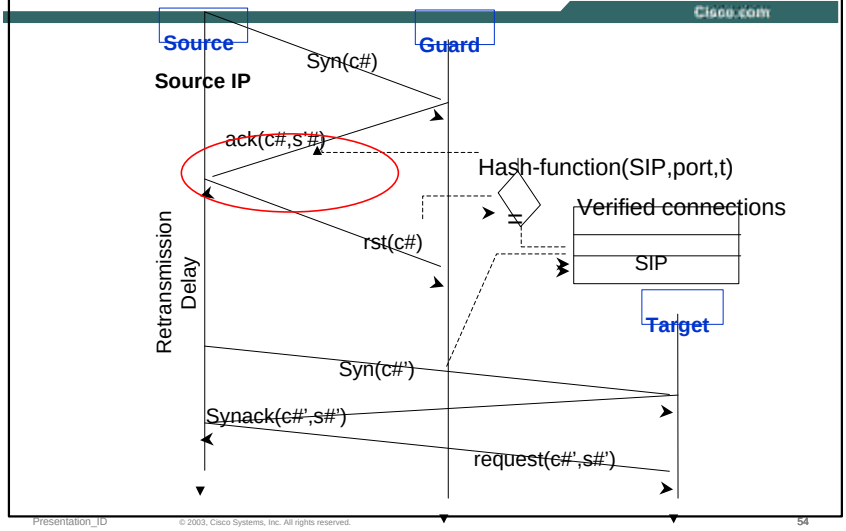
- **Specific support for protocols:**
  - HTTP, DNS, SMTP, IRC
- **Authenticates:**
  - SYNs, SYNACKs, FINs, regular TCP packets
  - DNS requests, DNS replies, Zone transfers
  - UDP traffic via correlated control sessions
- **Menu of techniques to support different protocols**
  - SYN Cookie
  - Reset Cookie
  - TTL
  - DNS authentication techniques
  - Various Redirection methods

Anti-Spoofing Defense

One example: HTTP



Basic safe reset TCP authentication



Baseline & Learning

Cisco.com

- **Templates provide "universal" default values**
  - **Provision closest template**
- **Two phases for customization by on-site learning**
  - **Done for each protected "victim"**
  - **Policy construction**
  - **Threshold tuning**
    - **By service and specific sub-parameter**
    - **Different thresholds established for activation of basic, strong and drop actions**

Anomaly Detection
Against Non-Spoofed Attacks

Cisco.com

- **Extensive profiling**
  - **Hundreds of anomaly sensors/victim**
  - **For global, proxies, discovered top sources, typical source,…**
- **Auto discovery and profiling of services**
  - **Automatically detects HTTP proxies and maintains specific profiles**
  - **Learns individual profiles for top sources, separate from composite profile**
- **Depth of profiles**
  - **PPS rates**
  - **Ratios eg SYNs to FINs**
  - **Connection counts by status**
  - **Protocol validity eg DNS queries**

Other Guard Features

Cisco.com

- **Reporting**
  - Victim statistics: rcvd, dropped, replied, forwarded
  - Detected anomalies (detail: specific thresholds crossed)
  - Mitigation mechanism: static, dynamic, spoof, malform, rate limit
  - Type of attack mitigated
- **Traffic analysis**
  - Shows rates of traffic prior to any anomaly detection or action

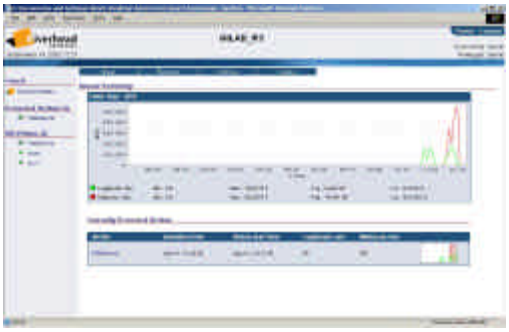
Performance

Cisco.com

- **Cisco Traffic Anomaly Detector XT 5600**
  - Can detect on both GE interfaces
  - 3.0Mpps for detection
- **Cisco Guard XT 5650**
  - 1.25Mpps for most attack conditions
  - Protects 15 concurrently attacked “zones”
  - Minimum 1.5 million concurrent connections
  - 150,000 blocked sources (dynamic filters)
  - < 1 msec latency & jitter

Manageability

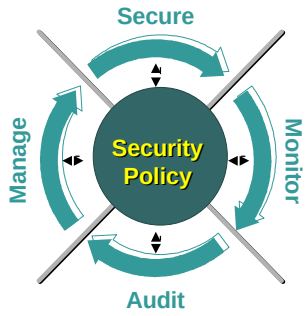
- IOS-Like CLI
- Web based embedded device manager
- Interactive recommendations
- Extensive reporting and data export
- DDoS SNMP MIB and traps
- HW environmental monitoring



Summary

Security Wheel

- **Secure**
  - Identity and authentication
  - Filtering and stateful inspection
  - Encryption and VPNs
- **Monitor**
  - Intrusion detection and response
  - Content-based detection and response
  - Employee monitoring
- **Audit**
  - Security posture assessment
  - Vulnerability scanning
  - Patch verification/application auditing
- **Manage**
  - Secure device management
  - Event/data analysis and reporting
  - Network security intelligence



Security Wheel

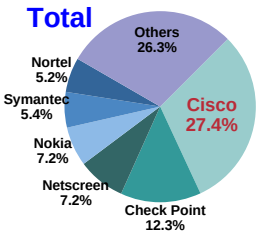
Cisco Security Solutions

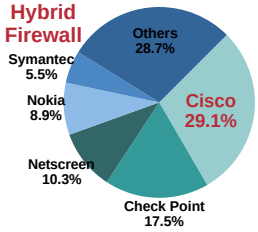
- **Every network device plays a part in security – Cisco spans the entire network**
- **Cisco embeds effective, appropriate security capabilities everywhere for defense in depth – Threat Defense, Secure Connectivity, Trust & Identity**
- **Endpoints must be protected – Cisco security footprint intelligently links endpoints to the network**
- **One size doesn't fit all – Cisco security deployment flexibility is unsurpassed**

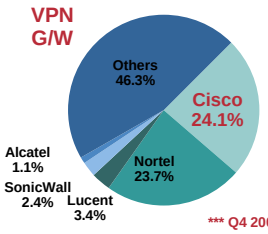
Security is not a single box…it's a collaboration of devices that deliver network-wide sensing and control capabilities!

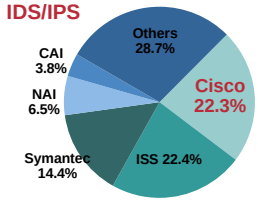
Network Security Market Share
Synergy Research Group,Inc

Cisco.com









*** Q4 2003 Network Security Market Shares

"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"

Q and A

CISCO SYSTEMS