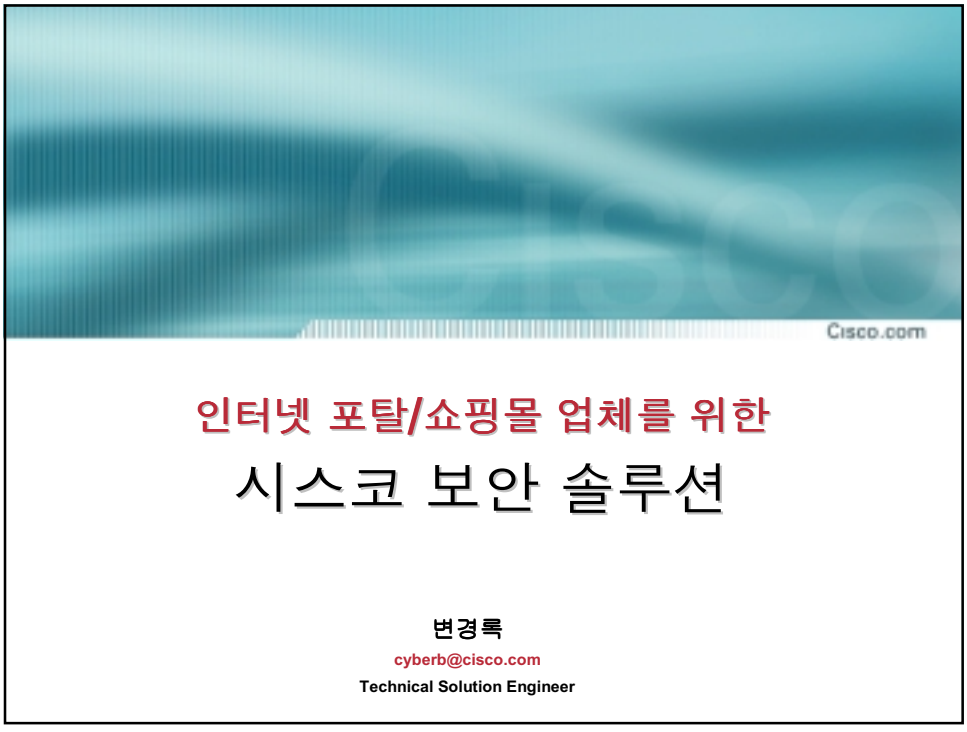

CISCO SYSTEMS
Presentation_ID
© 2001, Cisco Systems, Inc. All rights reserved.
1


Cisco.com
인터넷 포탈/쇼핑몰 업체를 위한
시스코 보안 솔루션
변경록
cyberb@cisco.com
Technical Solution Engineer

목 차

1. Internet Security Challenges
2. Cisco Security Solution
3. Cisco SAFE Desgin overview

3

The Code Red & NIMDA Worms What Happened??

Code Red
- **July 19-20/2001**
- **359,104 Hosts in 13 hours**
- **$2.0 Billion in Damages!**

Estimates from Computer Economics (Carlsbad, CA)

NIMDA
- **September 18, 2001**
- **100K+ Hosts.**
- **Damage still being assessed**

4

The Code Red Worm
How It Works

- **Conceals itself in HTTP Packets. Firewalls alone cannot safeguard against the virus**
- **The worm exploits vulnerabilities found in Microsoft's Internet Information Server (IIS) v4&5 via a buffer overflow attack**
- **It then exploits arbitrary code and installs a copy of itself into the infected computer's memory – which infects other host.**

5

The NIMDA Worm
How It Works

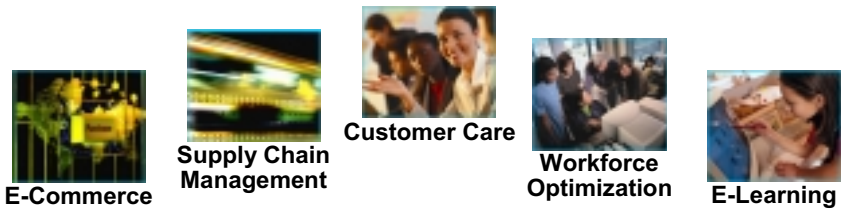
- **Hybrid of Worm & Virus**
- **Spread by:**
  - **E-mail attachment (virus)**
  - **Network Shares (worm)**
  - **Javascript by browsing compromised web site (virus)**
  - **Infected hosts scanning for exploitable hosts (worm)**
  - **Infected hosts scanning for backdoors created by Code-Red and sadmind/IIS worms (worm)**

6

The E-Business Challenge

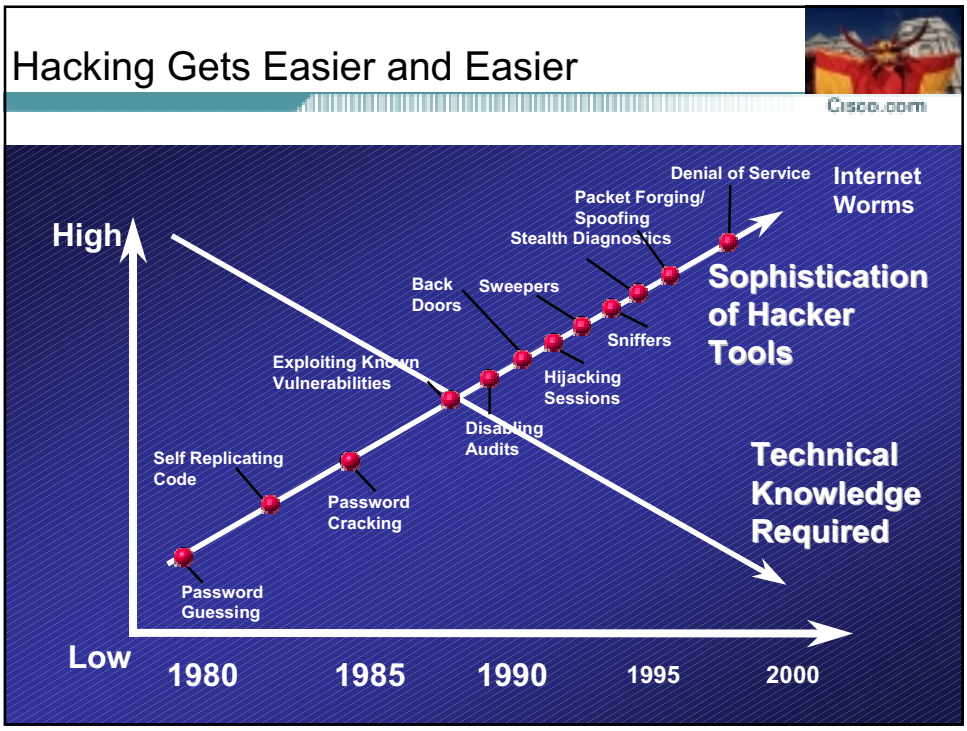
7

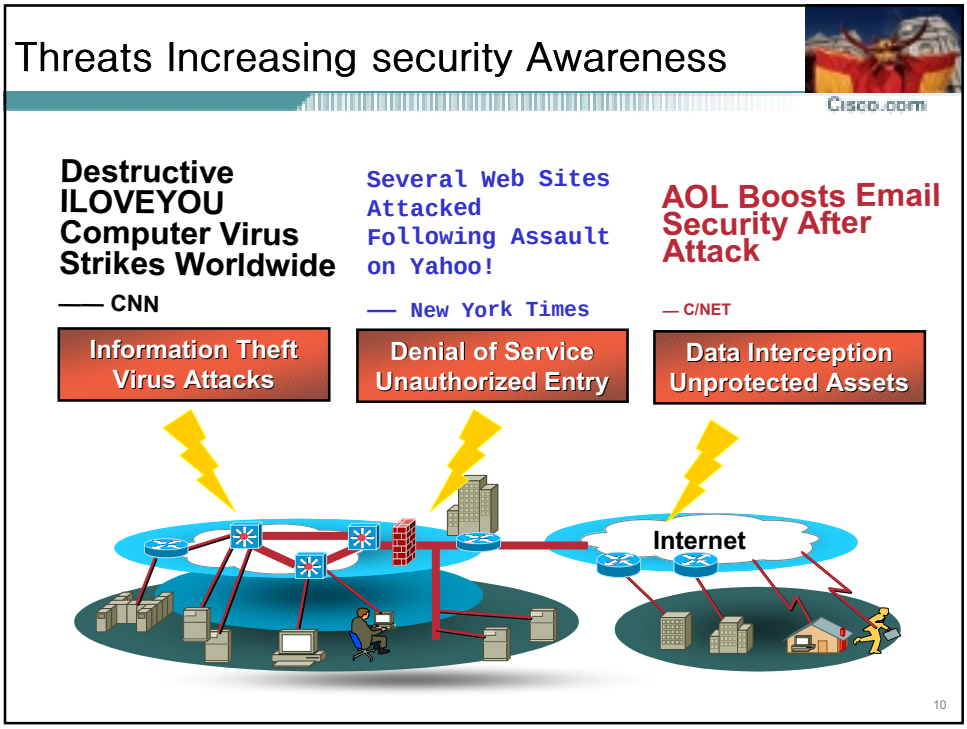
Security Critical Enabler for E-Business



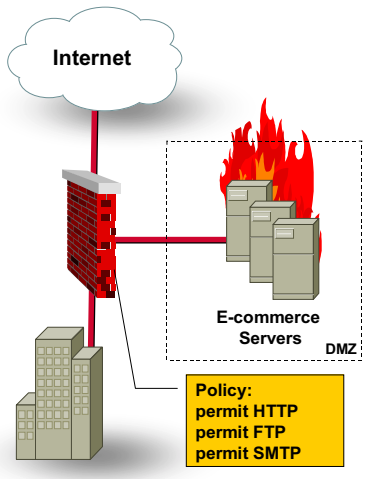
- Requires defense in depth
- Requires multiple and cohesive components
- Integration into e-business infrastructure
- Compatibility with technology initiatives
- Requires comprehensive blueprint

8


Hacking Gets Easier and Easier
Cisco.com
High
Low
1980
1985
1990
1995
2000
Password Guessing
Self Replicating Code
Password Cracking
Exploiting Known Vulnerabilities
Disabling Audits
Back Doors
Sweepers
Hijacking Sessions
Sniffers
Stealth Diagnostics
Packet Forging/ Spoofing
Denial of Service
Internet Worms
Sophistication of Hacker Tools
Technical Knowledge Required


Threats Increasing security Awareness
Cisco.com
Destructive ILOVEYOU Computer Virus Strikes Worldwide
— CNN
Several Web Sites Attacked Following Assault on Yahoo!
— New York Times
AOL Boosts Email Security After Attack
— C/NET
Information Theft Virus Attacks
Denial of Service Unauthorized Entry
Data Interception Unprotected Assets
Internet
10

Typical E-business Security Challenges



Firewalls = Access Control

Attack Scenario:

Step 1: Penetrate Perimeter

Exploit "permitted" conduits to pass attacks

Step 2: Decommission or Compromise Device

Launch buffer overflow attack to plant Trojan horse

Step 3: Escalate Privileges

Use compromised system to access internal network

Provides Perimeter Security That:

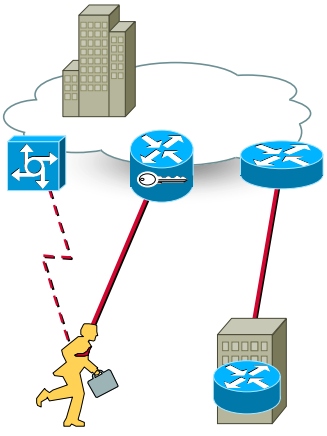
- *Blocks specific unwanted protocols*
- *Blocks communication over specific ports*

Cannot Provide Security For:

- *Malicious attacks contained within "permitted" traffic*
- *Threats including cgi-bin attacks, buffer overflows, fragmented, or Unicode attacks*

11

Typical VPN Security Challenges



VPN = Privacy

Attack Scenario:

Step 1: Compromise Extranet

Attack "weak-link" in extranet chain to gain back door access to corporate network

Step 2: Compromise Remote Access

Exploit weakness in remote access or dial-up devices to gain "trusted" access

Provides Data Privacy By:

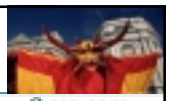
- *Encrypting contents of traffic*
- *Ensuring basic authentication of user*

Cannot Provide Security For:

- *Insider threat – 80% of attacks come from "trusted" sources*
- *Malicious content embedded in encrypted traffic*
- *Site-to-Site VPNs do not authenticate users or traffic*

12

What's the Impact?



- **COST- Directly Affects Bottom Line**
  - According to CSI, out of 645 respondents, 273 willingly reported hack attempts totaling $265,549,940
  - Average loss per respondent nearly $1,000,000
- **CREDIBILITY- End User Perception**
  - Can your end-user trust your network?
- **PRODUCTIVITY- Ability To Use Your System**
  - Downtime is lost time and revenue
- **VIABILITY- Can ultimately affect your business**
  - Where will your company be in 1 year…5 years?
- **LIABILITY – Are you responsible?**
  - If you don't take actions to stop outbound attacks, are you liable for damages inflicted on others?

13

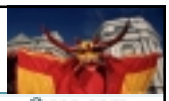
The Problem

" We security folks have got to stop treating security like it's a separate problem from network management. Error detection, intrusion detection, and link outages - these are all aspects of the same network management problem"

Marcus J. Ranum
CEO of Network Flight Recorder
One of the Fathers of the Modern Firewall

14

Conclusion



- **A layered defense is the best defense "Defense in Depth"**
- **Perhaps you need another weapon in your security arsenal**
- **Traditional security technology focus on prevention NOT detection and response**

Protection = Prevention + Detection + Response

15

CISCO SECURITY SOLUTION

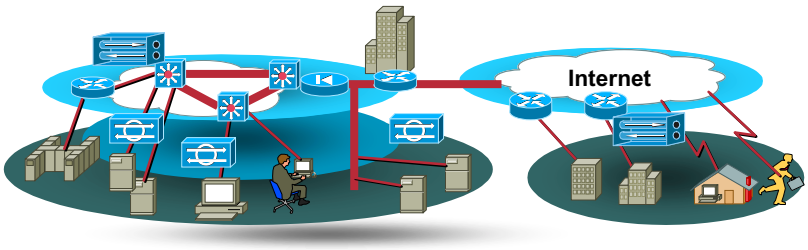
- **Network Security Componet**
- **PIX Firewall**
- **VPN**
- **IDS Sensors**
- **Management**

16

General Trends in Security Solutions

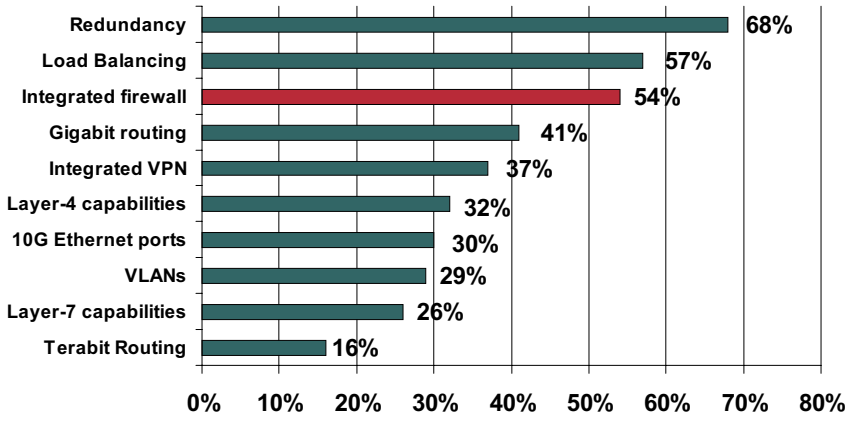
Migration to:

- Out-sourced security services
- Tighter coupling of technologies and services
- Scalable, high-performance platforms
- Self-defending intelligent elements
- Extended security perimeters



17

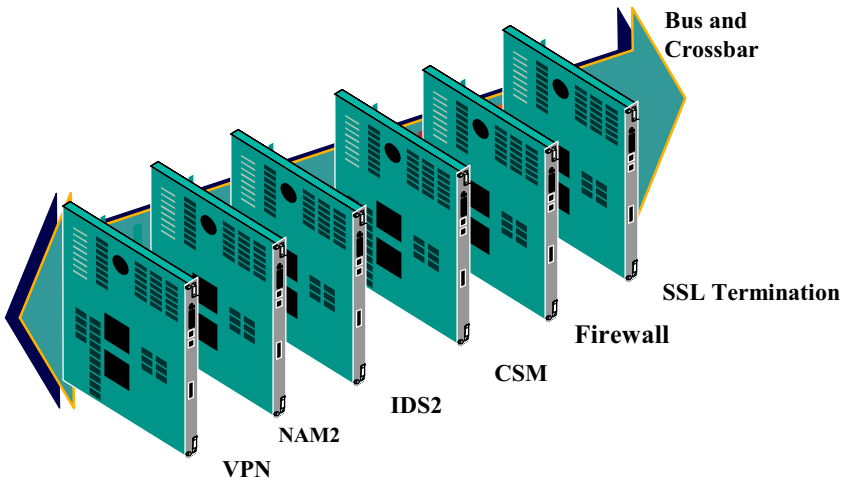
E-commerce respondents feedback



Source: Infonetics 2001

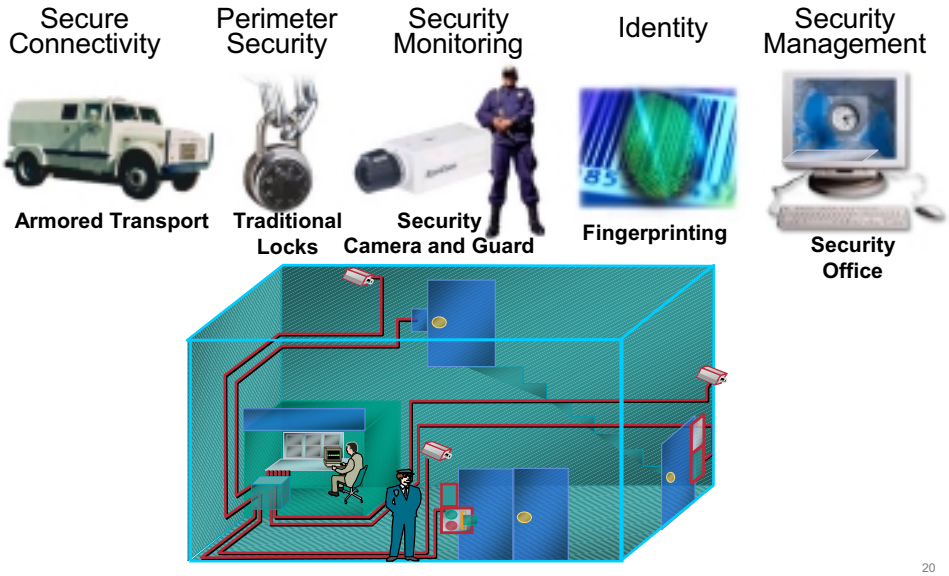
18

Services Cards Portfolio

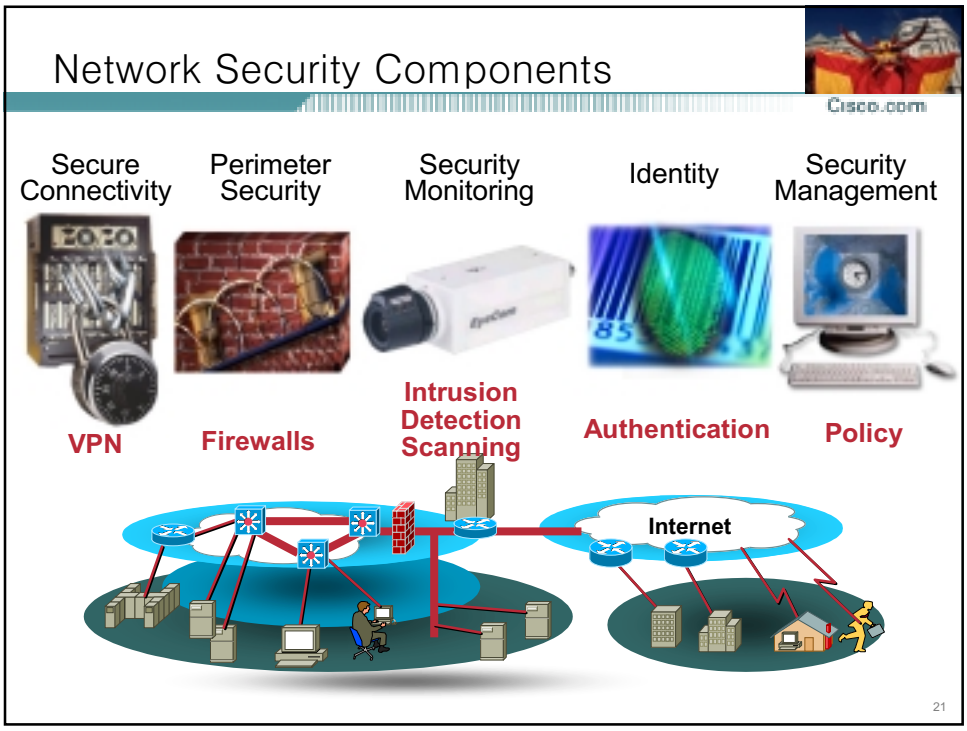


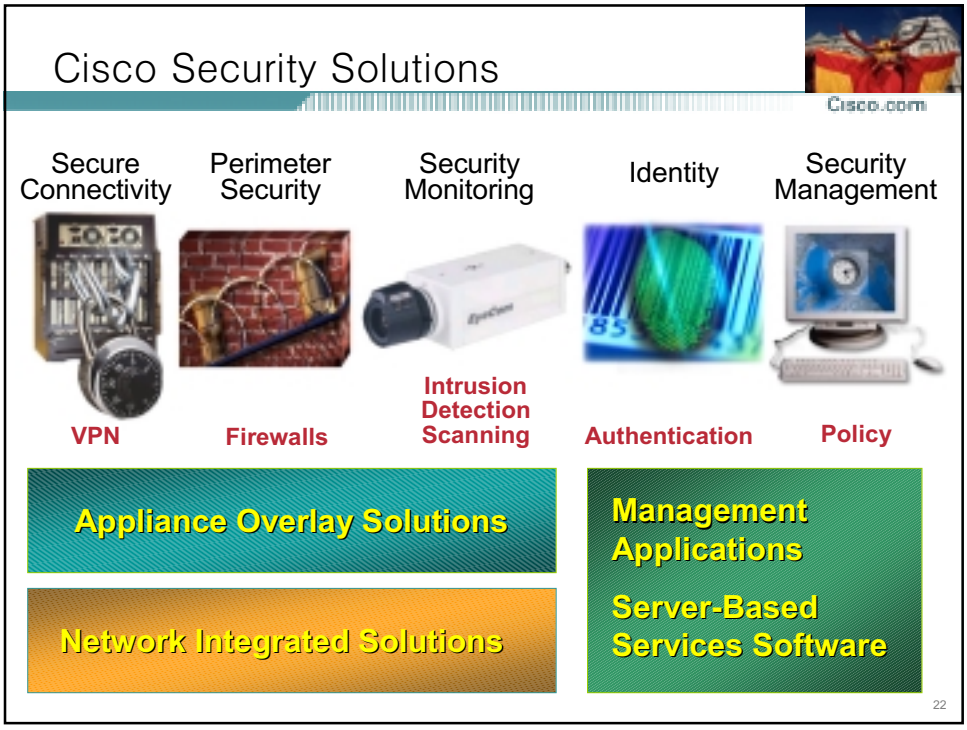
19

Physical Security Components



20


Network Security Components
Cisco.com
Secure Connectivity
Perimeter Security
Security Monitoring
Identity
Security Management
VPN
Firewalls
Intrusion Detection Scanning
Authentication
Policy
Internet
21

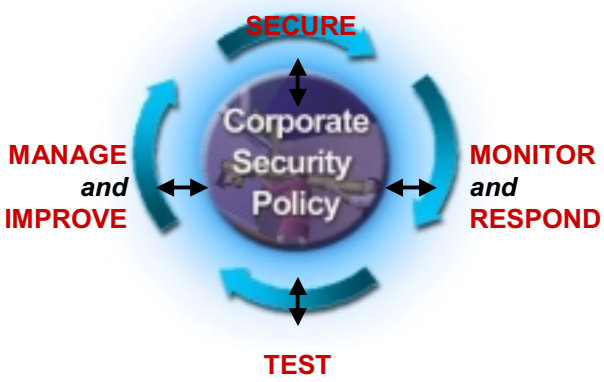

Cisco Security Solutions
Cisco.com
Secure Connectivity
Perimeter Security
Security Monitoring
Identity
Security Management
VPN
Firewalls
Intrusion Detection Scanning
Authentication
Policy
Appliance Overlay Solutions
Network Integrated Solutions
Management Applications
Server-Based Services Software
22

Cisco Security Solutions

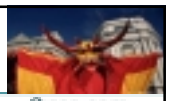
Cisco Security Philosophy: *The Security Wheel*

– **A Continual, multistage process focused on incremental improvement**

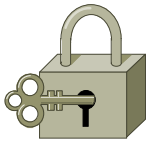
– **Each or all of the functions can be outsourced**



Security Policy



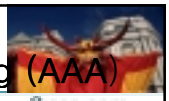
A Security Policy Is More than Just Buying a Firewall



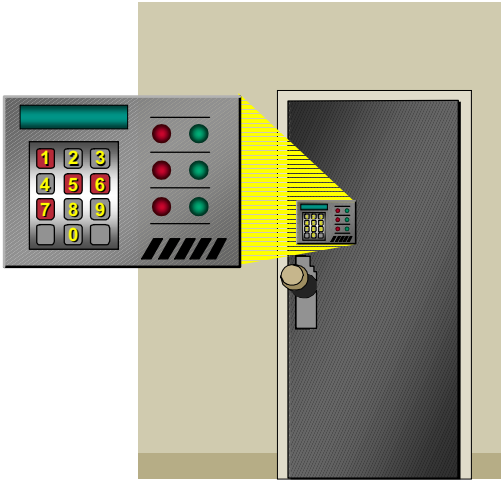
- What assets do I need to protect?
- What services do I plan to offer?
- What security risks does that create?
- What tools or methods are available to reduce my security risks to near zero?
- What is my "acceptable level of risk?"

25

Identity–Authentication/Authorization/ Accounting (AAA)



- Tool for controlling network and system access
- Authentication
  - Verifies identity—who are you?
- Authorization
  - Configures integrity—what are you permitted to do?
- Accounting
  - Assists with audit—what did you do?



26

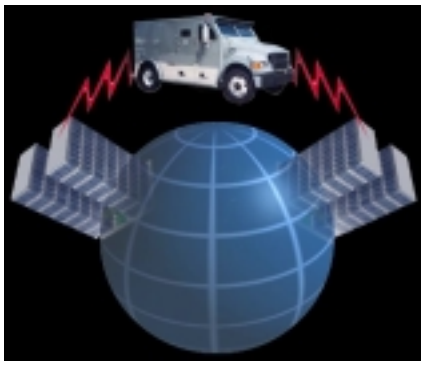
Perimeter Security

- Control access to critical network applications, data, and services
  - Router access control lists
  - DoS protection
  - Firewall
    - Router based
    - Appliance
    - Software
  - Content filtering
  - Intrusion detection

27

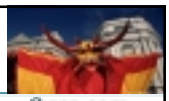
Secure Connectivity

- Data privacy/ encryption/VPN
  - Protecting data through untrusted environments
- Extending network reach and services (QoS, etc.)
- Cost savings
- Enhanced performance
  - 10 Mbps from your hotel room!
- Includes
  - Site-to-site
  - Remote access
  - Firewall based



28

Security Monitoring



- Monitors behavior, like a security camera
- Alarms on unusual 'stuff'
- Analyze behavior
  - Trusted user hacking
  - Denial-of-Service attacks!
- Take immediate action
- Appliance
- Switch
  - Line Card
- Host
  - E-servers (buffer overflow, trojan, etc.)

29

Security Monitoring

- Holes created when network grows/changes
- Hackers are patient and persistent
- Use a security scanner to find holes, prioritize importance, and obtain information on how to repair

30

Security Management

- Different tools for different purposes
- Policy-based tool appropriate for "business-level" IS administrators
- Complements other Cisco network management applications
- User chooses solution that best fits company processes

Staging and Initial Configuration	Multi-Device Management	Policy Management
Embedded Firewall Manager Embedded Web Server ConfigMaker CLI	Management Suite LAN Manager, Routed WAN Manager, and more	Security Policy Manager QoS Policy Manager

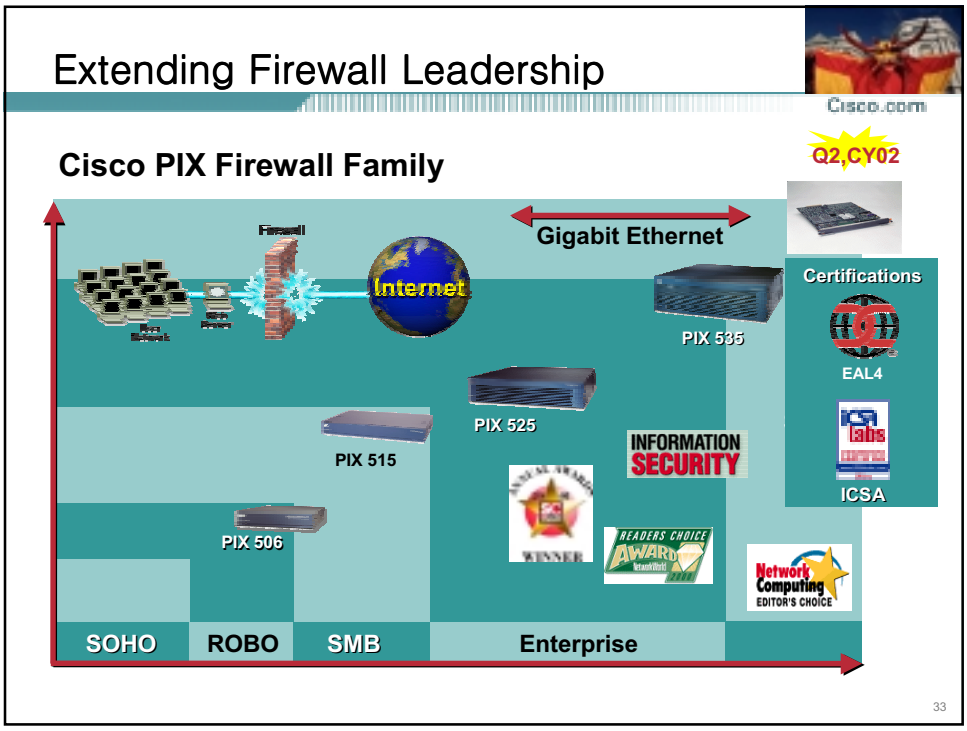
31

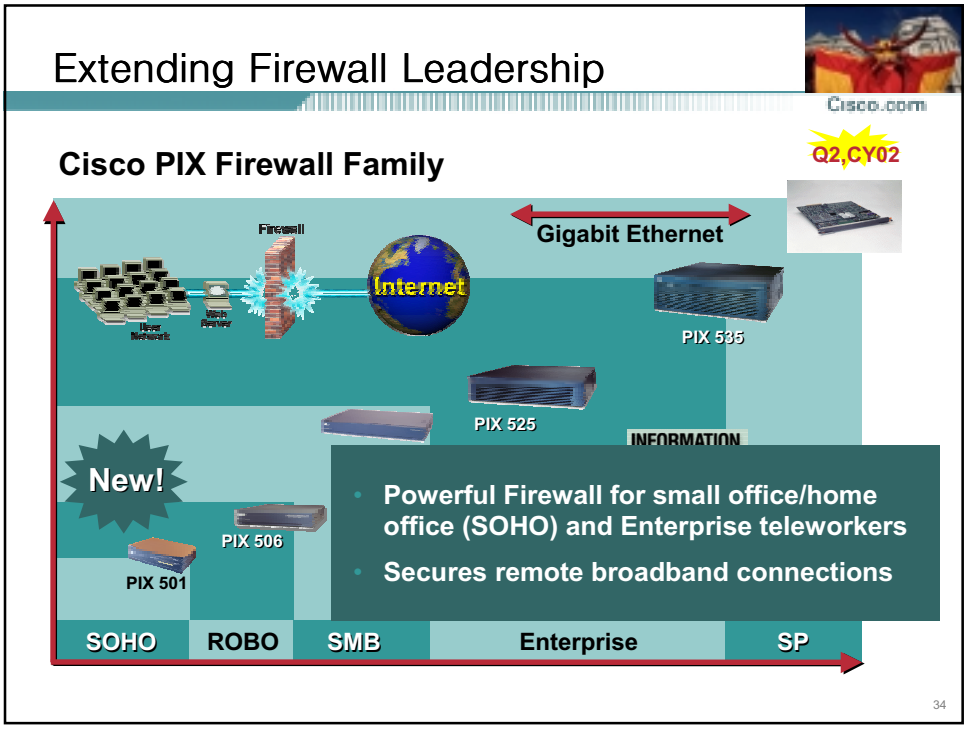
Put Security *IN* the Network

- Static networks are relics of the past
- Network security is more than firewalls
- Leverage your network infrastructure. Don't build a separate network for security
- Like TCP/IP, security has become a basic building block of every network
- A layered defense is the best defense "Defense in Depth"
- Traditional security technology focus on prevention NOT detection and response

Protection = Prevention + Detection + Response

32


Extending Firewall Leadership
Cisco.com
Cisco PIX Firewall Family
Q2,CY02
Gigabit Ethernet
Firewall
Internet
PIX 535
Certifications
EAL4
PIX 525
PIX 515
INFORMATION SECURITY
ICSA
PIX 506
READERS CHOICE AWARD
Network Computing EDITOR'S CHOICE
SOHO
ROBO
SMB
Enterprise
33


Extending Firewall Leadership
Cisco.com
Cisco PIX Firewall Family
Q2,CY02
Gigabit Ethernet
Firewall
Internet
PIX 535
PIX 525
INFORMATION
New!
PIX 506
PIX 501
Powerful Firewall for small office/home office (SOHO) and Enterprise teleworkers
Secures remote broadband connections
SOHO
ROBO
SMB
Enterprise
SP
34

Features Overview

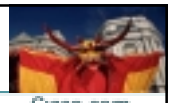
Industry's leading firewall performance!

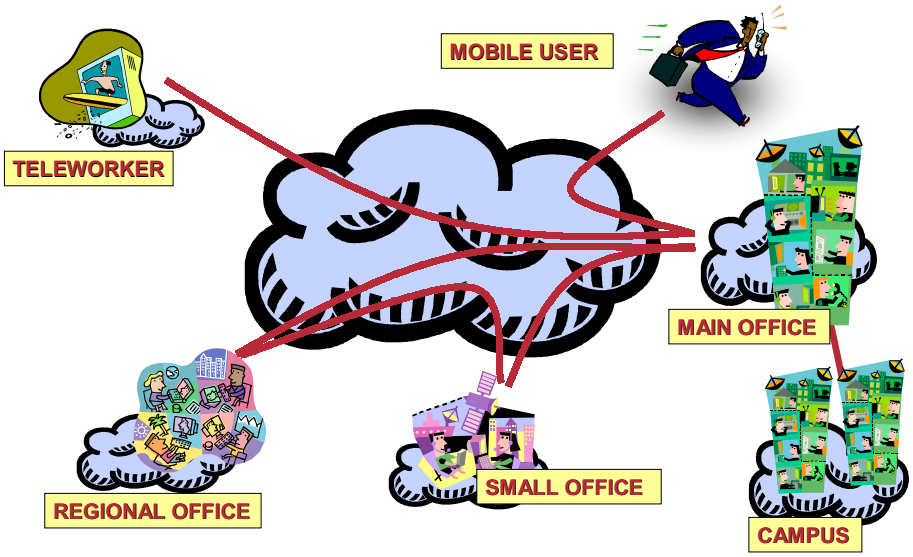
- PIX 6.0 base Feature Set + some feature of 6.2 also
- High Performance Firewall, targeted OC48 or 5GB (full duplex)
- 1 million Concurrent connections
- 3 Million pps
- 100K new connections/sec for HTTP, DNS
- 100 VLANs
- LAN failover active/standby (both intra/inter chassis)
- Dynamic Routing I.e. RIP, OSPF
- Support multiple blades in the chassis
- Supports multiple IN/OUT and DMZs
- IPSEC for management only (IPSEC VPN in macedon)
-

Q2,CY02

35

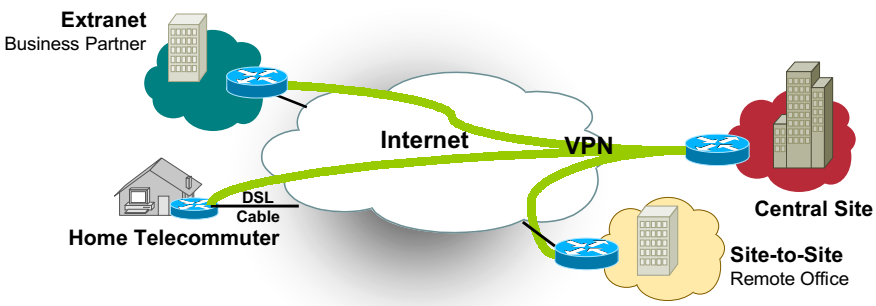
VPN Solutions





36

Site-to-Site VPNs Inherit

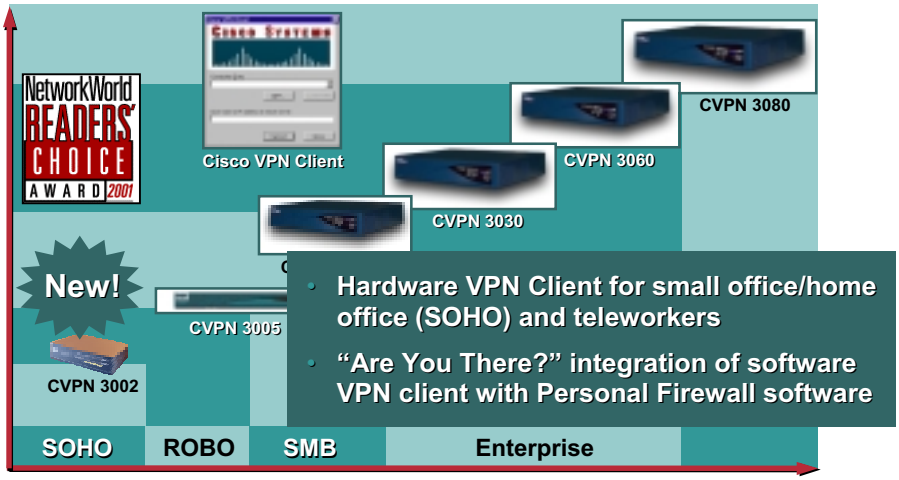


- **Site-to-Site VPNs are the evolution of WANs, but with better security, higher bandwidth, and less expense**
- **Changing the network fabric from frame relay or private lines to IPSec does not change the base network requirements**

37

Extending VPN Leadership

Cisco VPN 3000 Concentrator Family



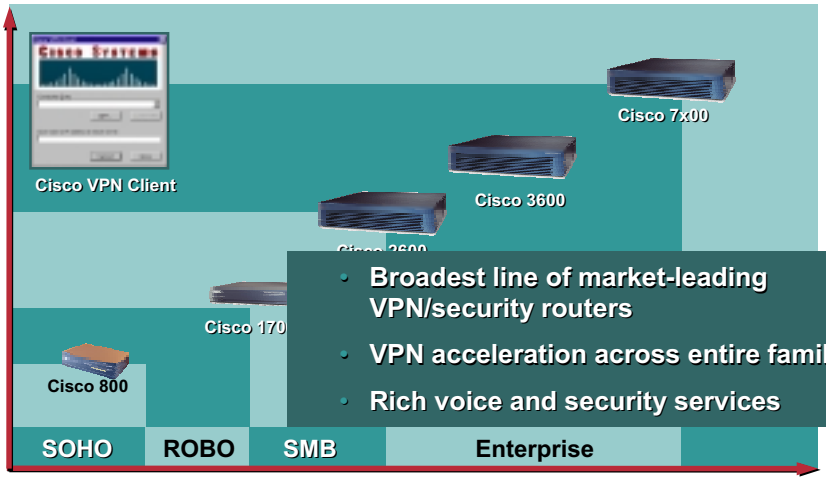
- **Hardware VPN Client for small office/home office (SOHO) and teleworkers**
- **"Are You There?" integration of software VPN client with Personal Firewall software**

38

Extending VPN and Security Leadership

Cisco.com

Cisco Family of VPN/Security Optimized Routers



- Broadest line of market-leading VPN/security routers
- VPN acceleration across entire family
- Rich voice and security services

39

Cisco Home VPN Portfolio

Cisco.com

Cisco PIX 501 Firewall
Integrated security appliance for SOHO environments
- Provides stateful firewalling, VPN and intrusion protection
- Includes integrated 4-port 10/100 switch
- MSRP $695 (10 users+3DES), $1295 (50 users+3DES)

Cisco 806 Broadband Gateway Router
IOS router platform for SOHO environments
- Provides advanced networking features + firewall/VPN
- Includes integrated 4-port 10 Mbps hub
- MSRP $799 (firewall+VPN+memory)

Cisco VPN 3002 Hardware VPN Client
Scalable, seamless hardware VPN client solution
- Provides advanced VPN features including unit/user level auth (incl. tokens) NAT transparency, load balancing, failover
- Optional 8-port 10/100 switch
- MSRP $995 (dual ethernet), $1195 (8 port switch model)

40

Cisco IDS Solution

Total Intrusion Protection

Cisco.com

- **Network Sensors**
  - Overlay network protection
- **Switch Sensors**
  - Integrated switch protection
- **Host Sensors**
  - Server & application protection
- **Router Sensors**
  - Integrated router protection
- **Firewall Sensors**
  - Integrated firewall protection
- **Comprehensive Management**
  - Robust system management and monitoring

41

Why Intrusion Detection

Cisco.com

amazon.com.

E*TRADE

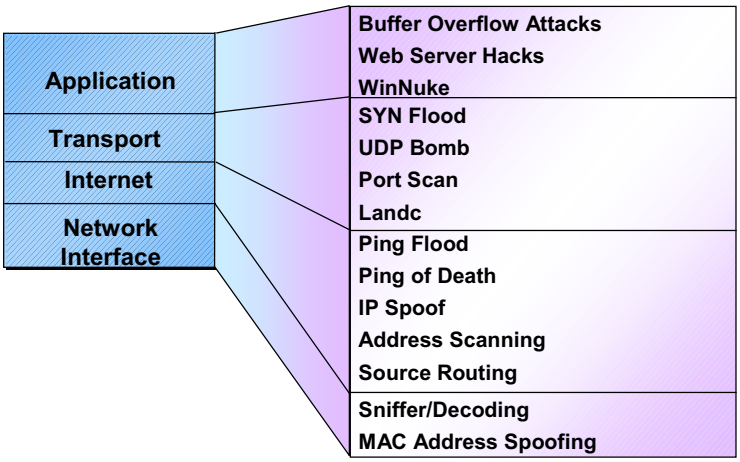
CNN.com

ebay

- 80% of security breaches from insiders—FBI
- 1 in 3 intrusion occur where a firewall exists—Computer Security Inst
- Explosive growth of Denial-of-Service attacks and buffer overflows
- $1.7 trillion WW loss due to downtime—InformationWeek
- $266 billion—damages from viruses and cracking—InformationWeek

42

Demystifying Common Attacks



43

Signature Analysis

Context: (Header)	Ping of Death Land Attack	Port Sweep SYN Attack TCP Hijacking
Content: (Data)	NetBIOS OOB DNS Attacks	Web Server Hacks Buffer Overflows
	"Atomic" Single Packet	"Composite" Multiple Packets

+ plus IP fragmentation reassembly

44

NSDB

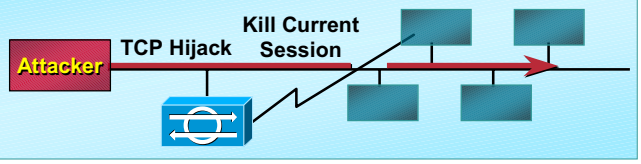
- On-line reference tool
- Contains:
  - Descriptions
  - Severity ratings
  - Benign triggers
  - Hyperlinks to related vulnerability information and patches
- Bi-monthly updates via web

45

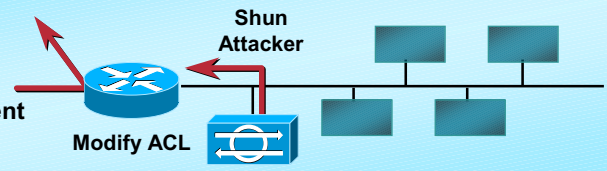
Response Actions

Session Termination and Shunning

Session Termination
Terminates an Active TCP Session



Shunning
Reconfigure Filters With Device Management Option



46

Host Sensor Agent Protection

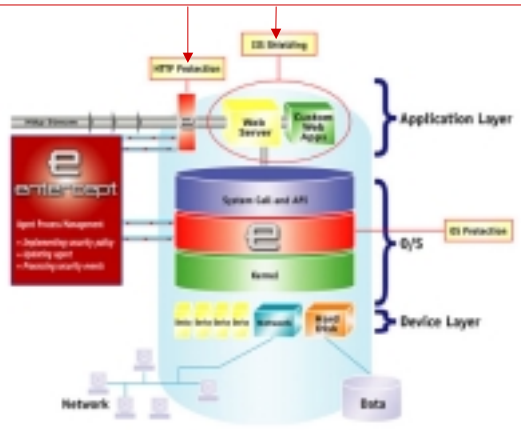
	Standard Edition	Web Server Edition
Individual Signature Protection	X	X
Generic Signature Protection	X	X
Resource Protection	X	X
HTTP Protection		X
Web Server Shielding		X

47

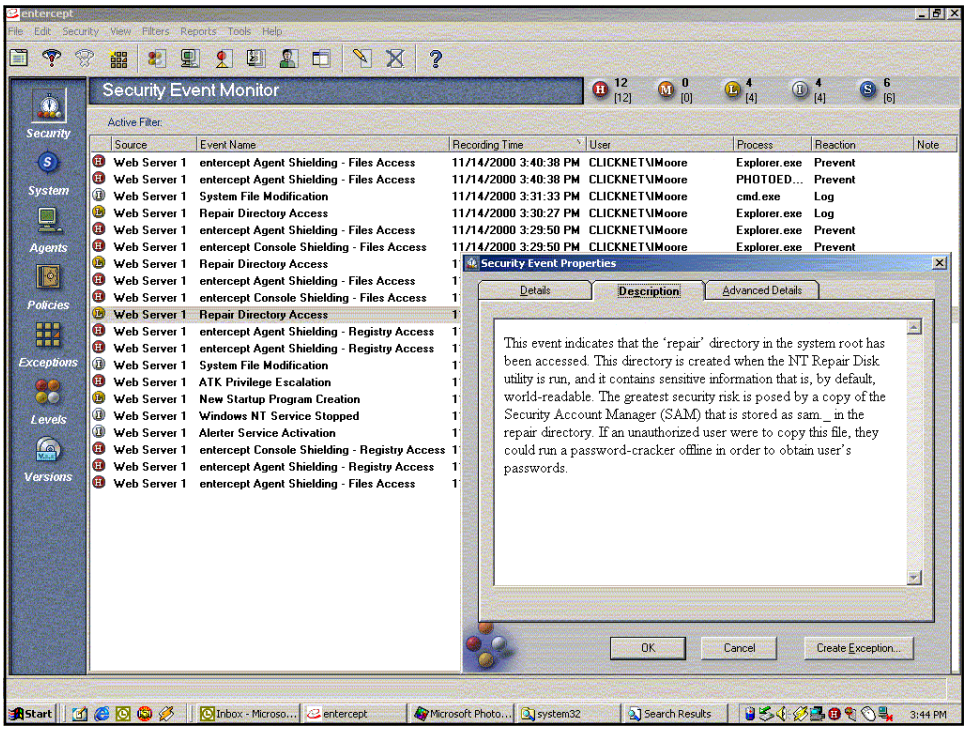
IDS Host WSE Technology

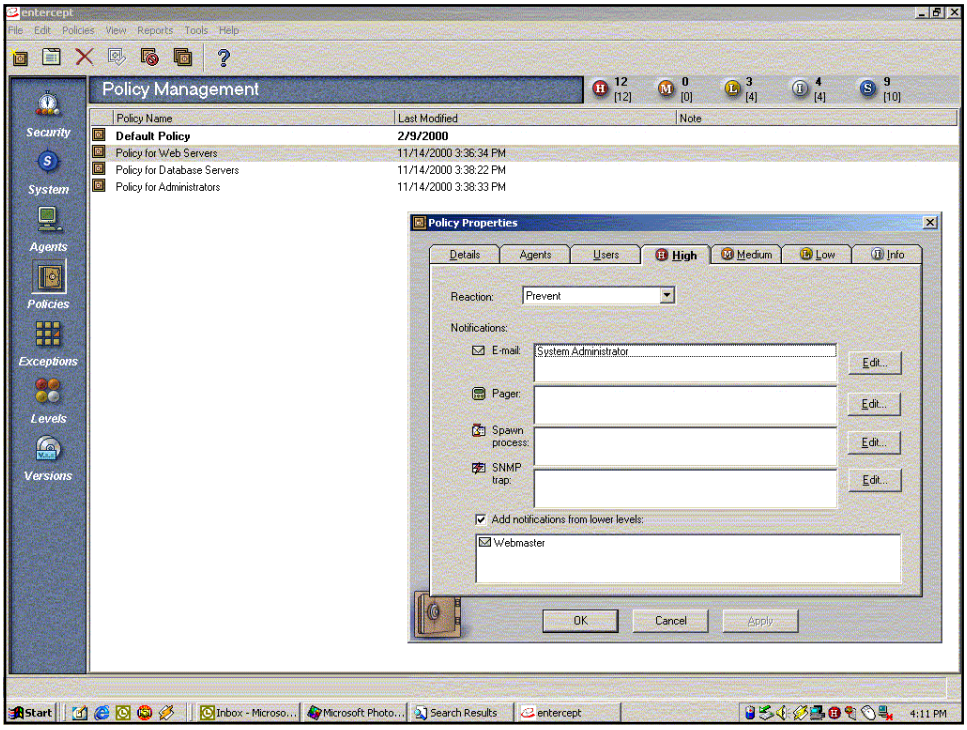
In addition, shielding technology is used to provide a protective envelope around the Web server, ensuring the integrity of the Web server, its applications and files, including customers' valuable data.

This shielding technology enables IDS Host to protect Web servers from both known and unknown attacks.



48


entercept
File Edit Security View Filters Reports Tools Help
Security Event Monitor
Active Filter:
Source | Event Name | Recording Time | User | Process | Reaction | Note
Web Server 1 entercept Agent Shielding - Files Access 11/14/2000 3:40:38 PM CLICKNET\JMoore Explorer.exe Prevent
Web Server 1 entercept Agent Shielding - Files Access 11/14/2000 3:40:38 PM CLICKNET\JMoore PHOTOED... Prevent
Web Server 1 System File Modification 11/14/2000 3:31:33 PM CLICKNET\JMoore cmd.exe Log
Web Server 1 Repair Directory Access 11/14/2000 3:30:27 PM CLICKNET\JMoore Explorer.exe Log
Web Server 1 entercept Agent Shielding - Files Access 11/14/2000 3:29:50 PM CLICKNET\JMoore Explorer.exe Prevent
Web Server 1 entercept Console Shielding - Files Access 11/14/2000 3:29:50 PM CLICKNET\JMoore Explorer.exe Prevent
Web Server 1 Repair Directory Access
Web Server 1 entercept Agent Shielding - Files Access
Web Server 1 entercept Console Shielding - Files Access
Web Server 1 Repair Directory Access
Web Server 1 entercept Agent Shielding - Registry Access
Web Server 1 entercept Agent Shielding - Registry Access
Web Server 1 System File Modification
Web Server 1 ATK Privilege Escalation
Web Server 1 New Startup Program Creation
Web Server 1 Windows NT Service Stopped
Web Server 1 Alerter Service Activation
Web Server 1 entercept Console Shielding - Registry Access
Web Server 1 entercept Agent Shielding - Registry Access
Web Server 1 entercept Agent Shielding - Files Access
Security Event Properties
Details Description Advanced Details
This event indicates that the 'repair' directory in the system root has been accessed. This directory is created when the NT Repair Disk utility is run, and it contains sensitive information that is, by default, world-readable. The greatest security risk is posed by a copy of the Security Account Manager (SAM) that is stored as sam._ in the repair directory. If an unauthorized user were to copy this file, they could run a password-cracker offline in order to obtain user's passwords.
OK Cancel Create Exception...
Security System Agents Policies Exceptions Levels Versions
Start Inbox - Microso... entercept Microsoft Photo... system32 Search Results 3:44 PM


entercept
File Edit Policies View Reports Tools Help
Policy Management
Policy Name | Last Modified | Note
Default Policy 2/9/2000
Policy for Web Servers 11/14/2000 3:36:34 PM
Policy for Database Servers 11/14/2000 3:38:22 PM
Policy for Administrators 11/14/2000 3:38:33 PM
Policy Properties
Details Agents Users High Medium Low Info
Reaction: Prevent
Notifications:
E-mail: System Administrator Edit...
Pager: Edit...
Spawn process: Edit...
SNMP trap: Edit...
Add notifications from lower levels:
Webmaster
OK Cancel Apply
Security System Agents Policies Exceptions Levels Versions
Start Inbox - Microso... Microsoft Photo... Search Results entercept 4:11 PM

Advanced Intrusion Protection

Cisco.com

Cisco Intrusion Detection Family



Network Sensor Appliances | Switch Sensor Blades | Host Sensor Software

- Detects intrusions and malicious activities on hosts
- Blocks access to server before damage occurs; stopped Code Red Worm
- Complements market-leading network and switched-based IDS solutions

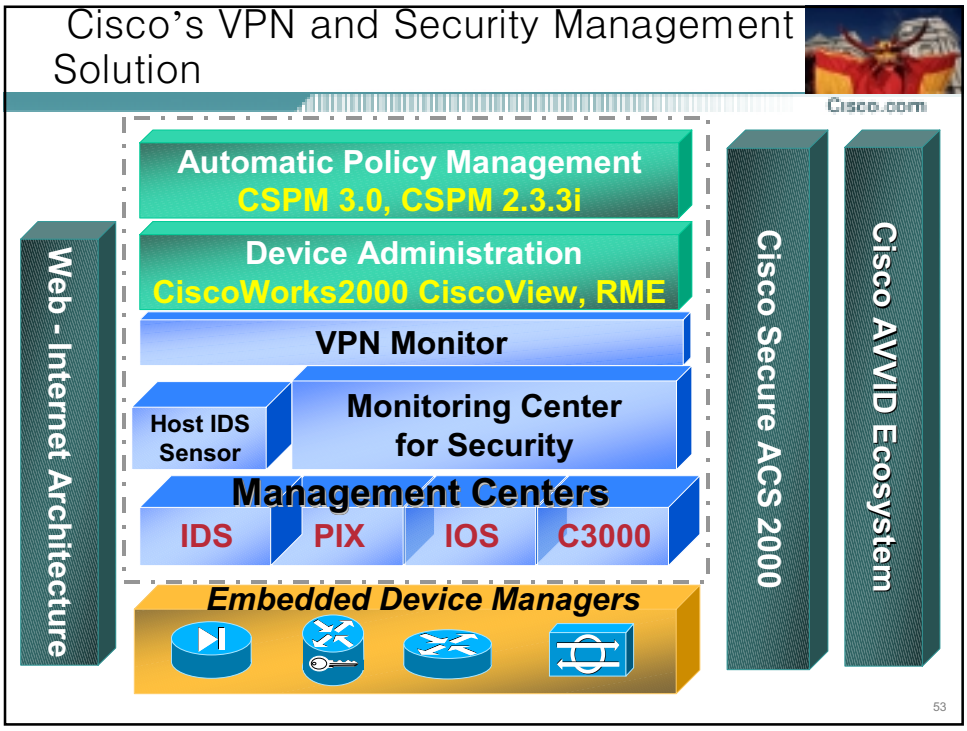
51

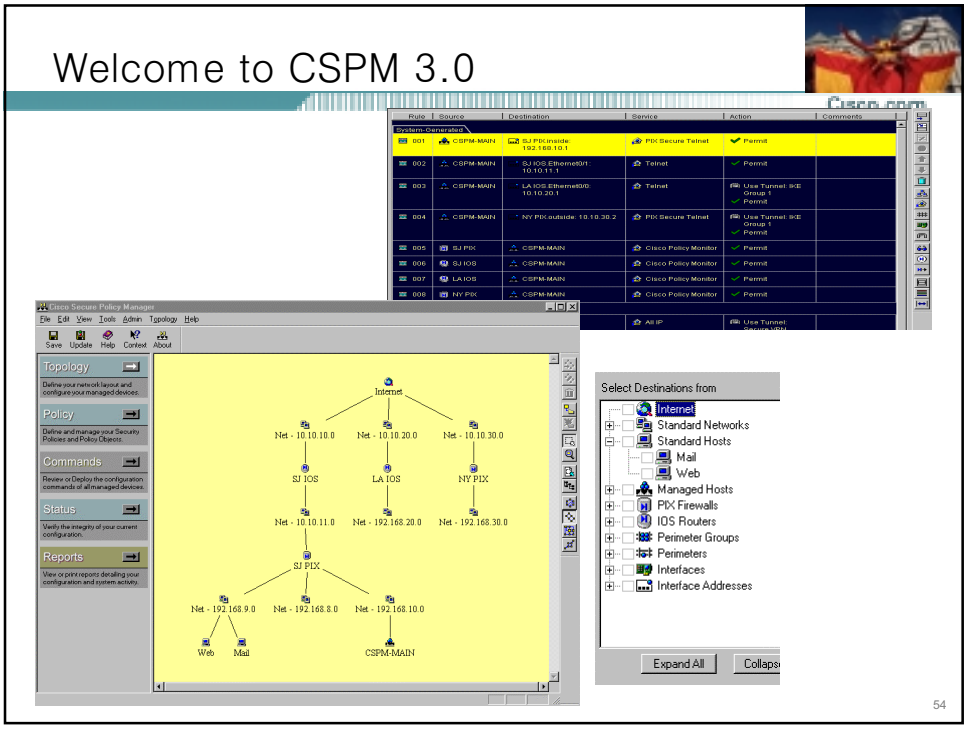
Cisco AVVID Security Product Partners

Cisco.com

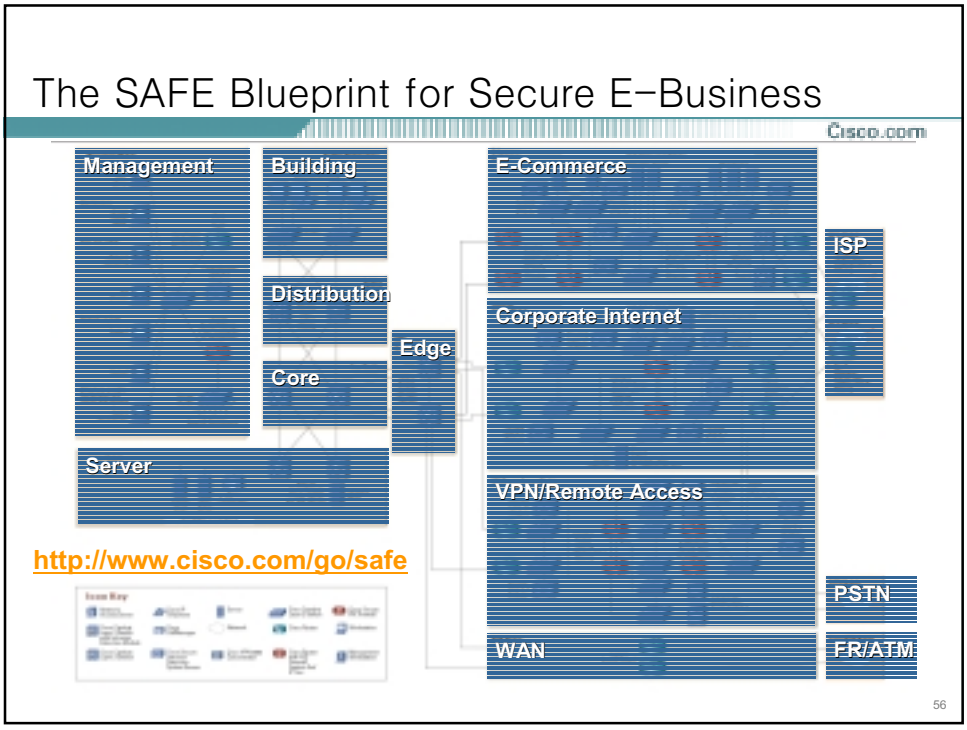
Secure Connectivity	Perimeter Security	Application Monitoring	Identity	Security Management
				
Wired and Wireless VPNs	Content Filtering; Personal F/W	Host and Server Protection	Strong Authentication, PKI	Event Logging, Reporting and Analysis
certicom, F-SECURE, iPass	ZONE LABS, BRIDATE, CONTROL, WEBSENSE, N2H2, BALTIMORE, TREND MICRO, SurfControl	entercept, SANCTUM	SECURE COMPUTING, CRYPTOCard, RSA SECURITY, BALTIMORE, Entrust, VeriSign, VASCO	SOLSOFT, F-SECURE, ARBOR NETWORKS, WEBTRENDS, Security, PENTASAFE

52


Cisco's VPN and Security Management Solution
Cisco.com
Automatic Policy Management
CSPM 3.0, CSPM 2.3.3i
Device Administration
CiscoWorks2000 CiscoView, RME
VPN Monitor
Host IDS Sensor
Monitoring Center for Security
Management Centers
IDS
PIX
IOS
C3000
Embedded Device Managers
Web - Internet Architecture
Cisco Secure ACS 2000
Cisco AVVID Ecosystem
53


Welcome to CSPM 3.0
Cisco.com
Topology
Policy
Commands
Status
Reports
Internet
Net - 10.10.10.0
Net - 10.10.20.0
Net - 10.10.30.0
SJ IOS
LA IOS
NY PIX
Net - 10.10.11.0
Net - 192.168.20.0
Net - 192.168.30.0
SJ PIX
Net - 192.168.9.0
Net - 192.168.8.0
Net - 192.168.10.0
Web
Mail
CSPM-MAIN
Select Destinations from
Internet
Standard Networks
Standard Hosts
Mail
Web
Managed Hosts
PIX Firewalls
IOS Routers
Perimeter Groups
Perimeters
Interfaces
Interface Addresses
Expand All
54


Cisco.com
SAFE Design Overview
55


The SAFE Blueprint for Secure E-Business
Cisco.com
Management
Building
Distribution
Core
Edge
Server
E-Commerce
ISP
Corporate Internet
VPN/Remote Access
PSTN
WAN
FR/ATM
http://www.cisco.com/go/safe
56

Routers are Targets

- **Potentially a hacker's best friend**
- **Protection should include:**
  - **constraining telnet access**
  - **SNMP read-only**
  - **administrative access with TACACS+**
  - **turning off unneeded services**
  - **logging unauthorized access attempts**
  - **authentication of routing update**

57

Administrative Authentication

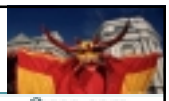

```
aaa new-model
aaa authentication login use_tacacs group tacacs+
aaa authentication login use_line line
aaa authorization exec default group tacacs+
aaa authorization network default group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting network default start-stop group tacacs

tacacs-server host 192.168.253.54 single-connection
tacacs-server key SJj)j~t]6-

line con 0
 exec-timeout 2 0
 login authentication use_line
line vty 0 4
 login authentication use_tacacs
```

58

Administrative Authentication




```
!Turn on NTP
!
clock timezone PST -8
clock summer-time PST recurring
ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 192.168.254.57 key 1
access-l 96 permit host 192.168.254.57
access-l 96 deny any log
!
!turn on logging
!
service timestamp log datetime
localtime
logging 192.168.253.56
logging 192.168.253.51
```

59

Administrative Authentication


```
! turn off un-needed services
!
no ip domain-lo
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-s
no service tcp-small-s
!
access-l 99 permit 192.168.253.0 0.0.0.255
access-l 99 deny any log
!
line vty 0 4
access-class 99 in
login
password 0 X)[^j+#T98
```

60

Switches are Targets

- **Protection needs are similar to routers**
- **VLANs are an added vulnerability:**
  - **remove user ports from auto-trunking**
  - **use non-user VLANs for trunk ports**
  - **set unused ports to a non-routed VLAN**
  - **do not depend on VLAN separation**

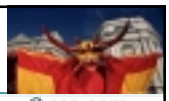
61

Networks are Targets

- **DDoS attacks cannot be stopped by the victim network alone**
- **RFC1918 addresses or local addresses should originate locally**
- **IP address spoofing can mitigated by filtering non-registered addresses**

62

Hosts are Targets



- **High Visibility makes them easy target**
- **Ensure that various host components are compatible and at the latest version**
  - **hardware platform/devices**
  - **operating system and updates**
  - **standard applications and patches**
  - **shareware scripts**

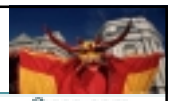
63

Applications are Targets

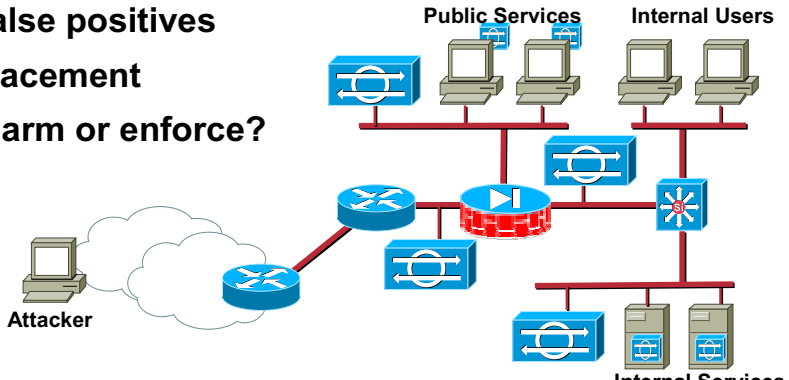
- **Complexity of applications makes them open to human error vulnerabilities**
- **Host and Network based IDS focus on recognizing attack signatures and taking action:**
  - **shunning/blocking**
  - **alarm/warning**
  - **simply logging**

64

Mitigating Application Attacks

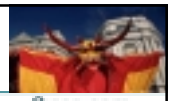


- **Host and Network Intrusion Detection Systems**
  - **HIDS and NIDS; both have their place**
- **False positives**
- **Placement**
- **Alarm or enforce?**



65

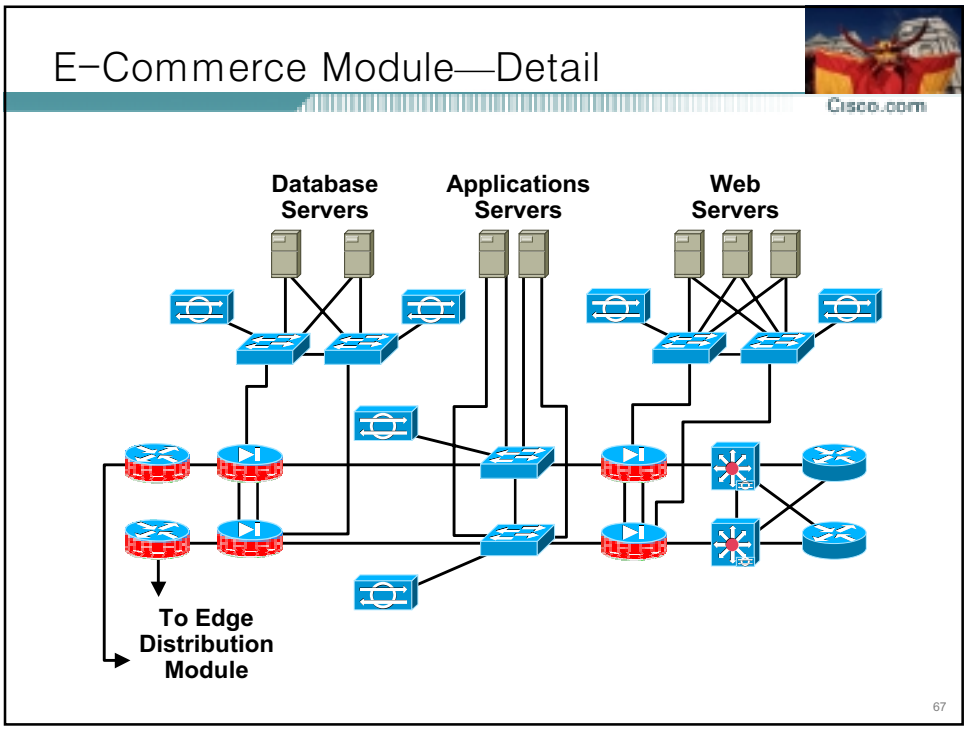
Good System Administration

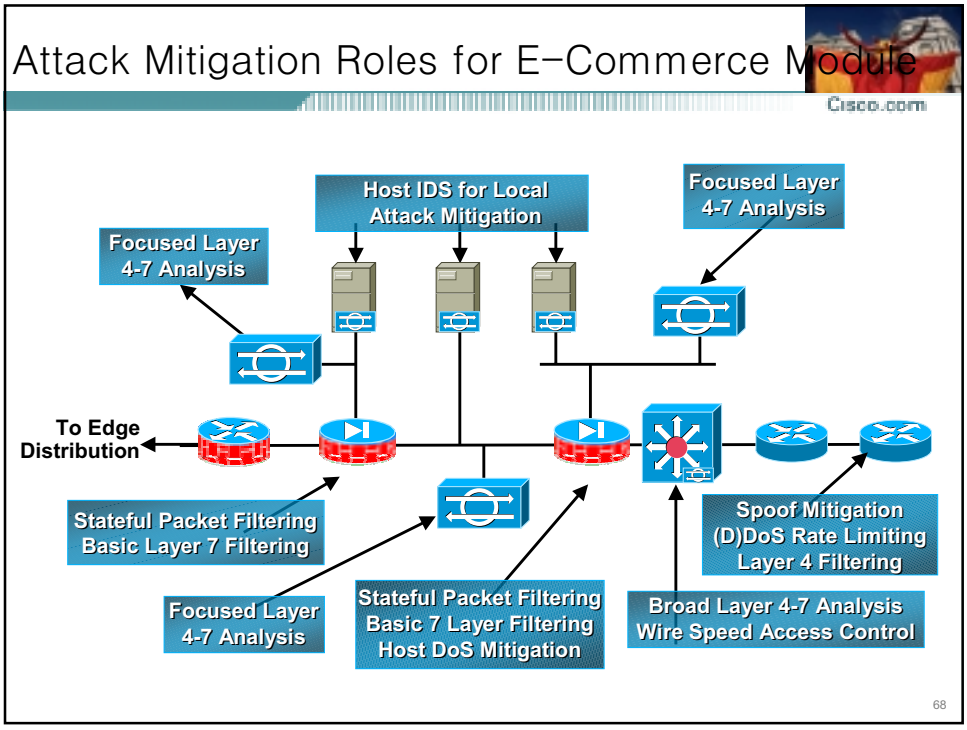


"A new study by Cisco Secure Consulting Services offers some insight into where many common vulnerabilities exist in IT network systems. The study, which analyzed 33 midsize and large customer sites over a period of six months, found vulnerabilities in all the customer sites, but almost all the vulnerabilities could be traced to outdated software or lax system administration maintenance, not to inherent flaws in the systems. While the need for careful system administration and continual system security analysis has been well-understood, Cisco's study indicates that most businesses, especially those that are conducting E-commerce activities over the Internet, aren't being careful enough."

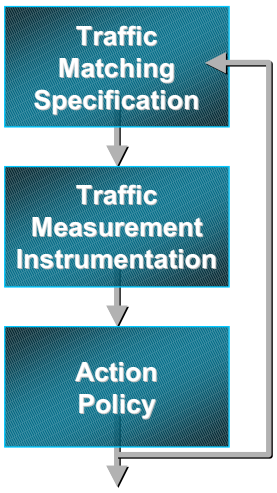
Information Week
February 21, 2000,
Issue: 774

66

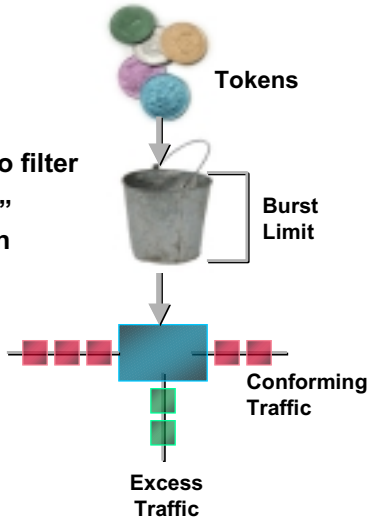

E-Commerce Module—Detail
Cisco.com
Database Servers
Applications Servers
Web Servers
To Edge Distribution Module
67


Attack Mitigation Roles for E-Commerce Module
Cisco.com
Host IDS for Local Attack Mitigation
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
To Edge Distribution
Stateful Packet Filtering Basic Layer 7 Filtering
Focused Layer 4-7 Analysis
Stateful Packet Filtering Basic 7 Layer Filtering Host DoS Mitigation
Broad Layer 4-7 Analysis Wire Speed Access Control
Spoof Mitigation (D)DoS Rate Limiting Layer 4 Filtering
68

Committed Access Rate



- Rate limiting
- Several ways to filter
- "Token bucket" implementation



69

CAR Rate Limiting

Limit outbound ping to 256 Kbps

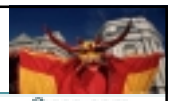
```
interface xy
     rate-limit output access-group 102 256000 8000 8000
          conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

Limit inbound TCP SYN packets to 8 Kbps

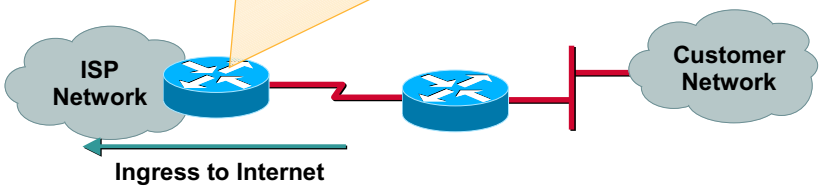
```
interface xy
     rate-limit input access-group 103 8000  8000 8000
          conform-action transmit exceed-action drop
!
access-list 103 deny tcp any host 142.142.42.1 established
access-list 103 permit tcp any host 142.142.42.1
```

70

RFC 1918 Filtering

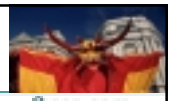



```
interface Serial n
  ip access-group 101 in
!
access-list 101 deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any
```



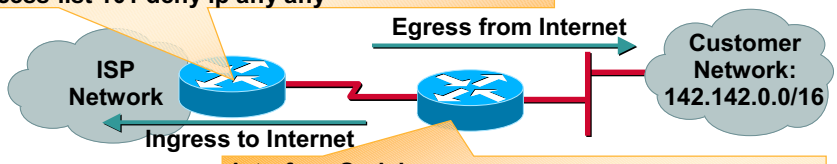
71

RFC 2267 Filtering




```
interface Serial n
  ip access-group 101 in
!
access-list 101 permit 142.142.0.0  0.0.255.255 any
access-list 101 deny ip any any
```

- Ingress packets must be from customer addresses

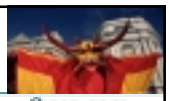


- Egress packets cannot be from and to customer
- Ensure ingress packets are valid

```
interface Serial n
  ip access-group 120 in
  ip access-group 130 out
!
access-list 120 deny ip 142.142.0.0  0.0.255.255 any
access-list 120 permit ip any any
!
access-list 130 permit 142.142.0.0  0.0.255.255 any
access-list 130 deny ip any any
```

72

Verify Unicast Reverse-Path



- **Mitigates source address spoofing by checking that a packets' return path uses the same interface it arrives on**
- **Best Implemented at your ISP**
- **Requires CEF**
- **Not appropriate where asymmetric paths exist**

```
ip cef distributed
!
interface Serial n
  ip verify unicast reverse-path
```

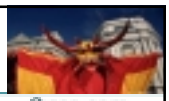
73

Implementing SAFE: Where do I start?

- **Develop a security policy based on business requirements and likely threats.**
- **Use modular blueprint for designing and deploying an all-encompassing security solution.**
- **Use Security Associate products to complement Cisco products and features.**
- **Perform a Network Vulnerability Analysis**
- **Maintain security posture through disciplined system/network administration.**

74

Threat Mitigation



Cisco.com

	Application Layer Attacks	Root Kits	DDoS Source	DDoS Victim	Password Cracking	Port Redirection
Good System Administration	●	●	●		●	●
Intrusion Detection	●				●	
Proper Trust Model	●	●	●		●	●
Committed Access Rate			●	●		
RFC 1918 Filtering			●	●		
RFC 2267 Filtering			●	●		

75

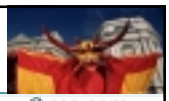
Threat Mitigation (Cont.)

Cisco.com

	Application Layer Attacks	Root Kits	DDoS Source	DDoS Victim	Password Cracking	Port Redirection
Verify Unicast RP forwarding			●	●		
SP Filtering			●	●		
Private VLANs	●	●	●			●
VMPS VLANs			●			
Network Audit						
Specific Filtering			●			●

76

Trends/Predictions



- **Security is going Mainstream**
  - Fundamental to E-business – not an afterthought
- **Security is going to Mainstreet**
  - Every small business will be an e-business
- **Security extends everywhere**
  - The Internet home and the Mobile Office
- **The Bar will continue to be raised**
  - Criticality of e-business applications
  - Increased exposure and regulation
- **Comprehensive solutions will win!**
  - Security integrated into voice, video, wireless infrastructures

77

Top Twenty Most Critical Internet Security Vulnerabilities

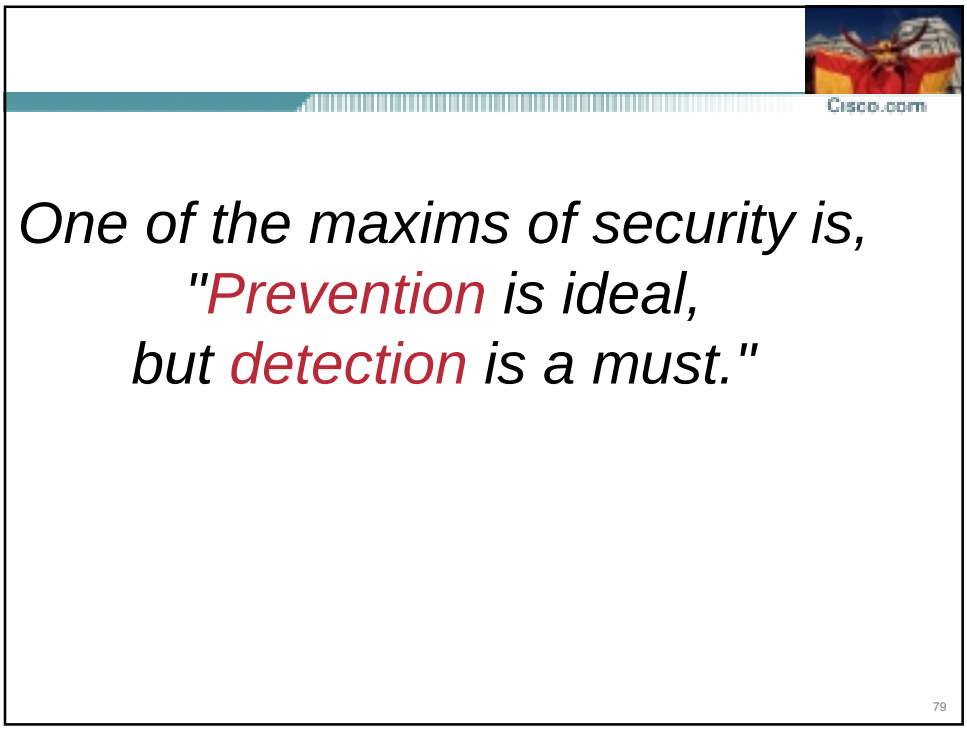
http://www.sans.org/top20.htm (SAN/FBI)

Top Vulnerabilities In Windows Systems (W)
- W1 - Unicode Vulnerability (Web Server Folder Traversal)
- W2 - ISAPI Extension Buffer Overflows
- W3 - IIS RDS exploit (Microsoft Remote Data Services)
- W4 - NETBIOS - unprotected Windows networking shares
- W5 - Information leakage via null session connections
- W6 - Weak hashing in SAM (LM hash)

Top Vulnerabilities In Unix Systems (U)
- U1 - Buffer Overflows in RPC Services
- U2 - Sendmail Vulnerabilities (Buffer Overflow Exploit)
- U3 - Bind Weaknesses (Buffer Overflow Exploits)
- U4 - R Commands
- U5 - LPD (remote print protocol daemon) Buffer Overflow Exploit
- U6 – sadmind and mountd (Buffer Overflow Exploits)
- U7 - Default SNMP Strings

Top Vulnerabilities That Affect All Systems (General)
- G1 - Default installs of operating systems and applications
- G2 - Accounts with No Passwords or Weak Passwords
- G3 - Non-existent or Incomplete Backups
- G4 - Large number of open ports
- G5 – Not filtering packets for correct incoming and outgoing addresses
- G6 - Non-existent or incomplete logging

78


Cisco.com
One of the maxims of security is,
"Prevention is ideal,
but detection is a must."
79


Together we will ..
Achieve all
that's possible
on the Internet
© 2001, Cisco Systems, Inc.
Cisco.com
80


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION
TS-300A
3902_11_2001_c1
© 2001, Cisco Systems, Inc. All rights reserved.
81