

OVERVIEW OF NETWORK SECURITY

Mohammad S. Hasan

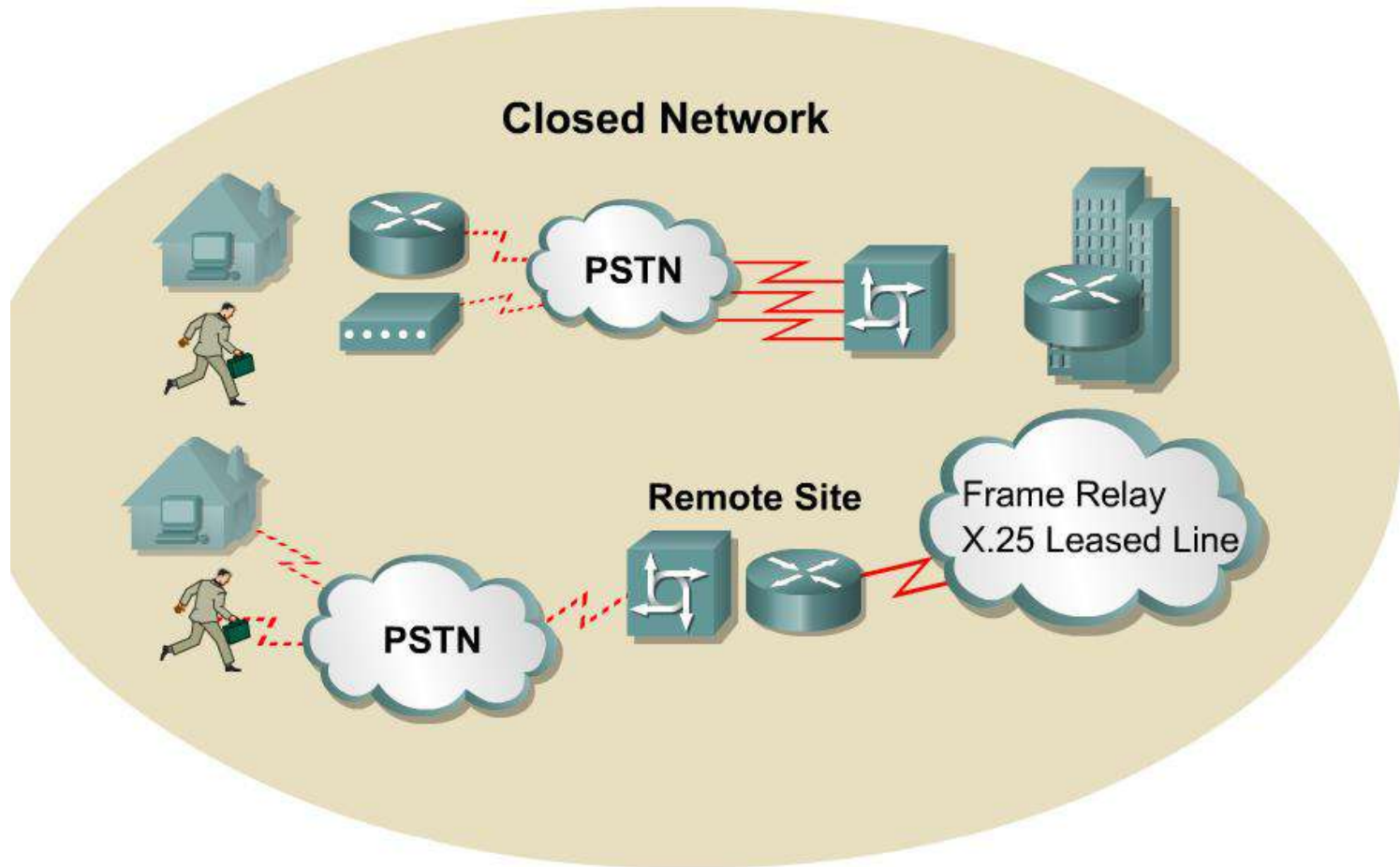
Key Terms

2

- Confidentiality
- Integrity
- Availability
- Vulnerability
- Threat
- Reconnaissance
- Access
- Denial of Service
- Encryption
- Security Wheel

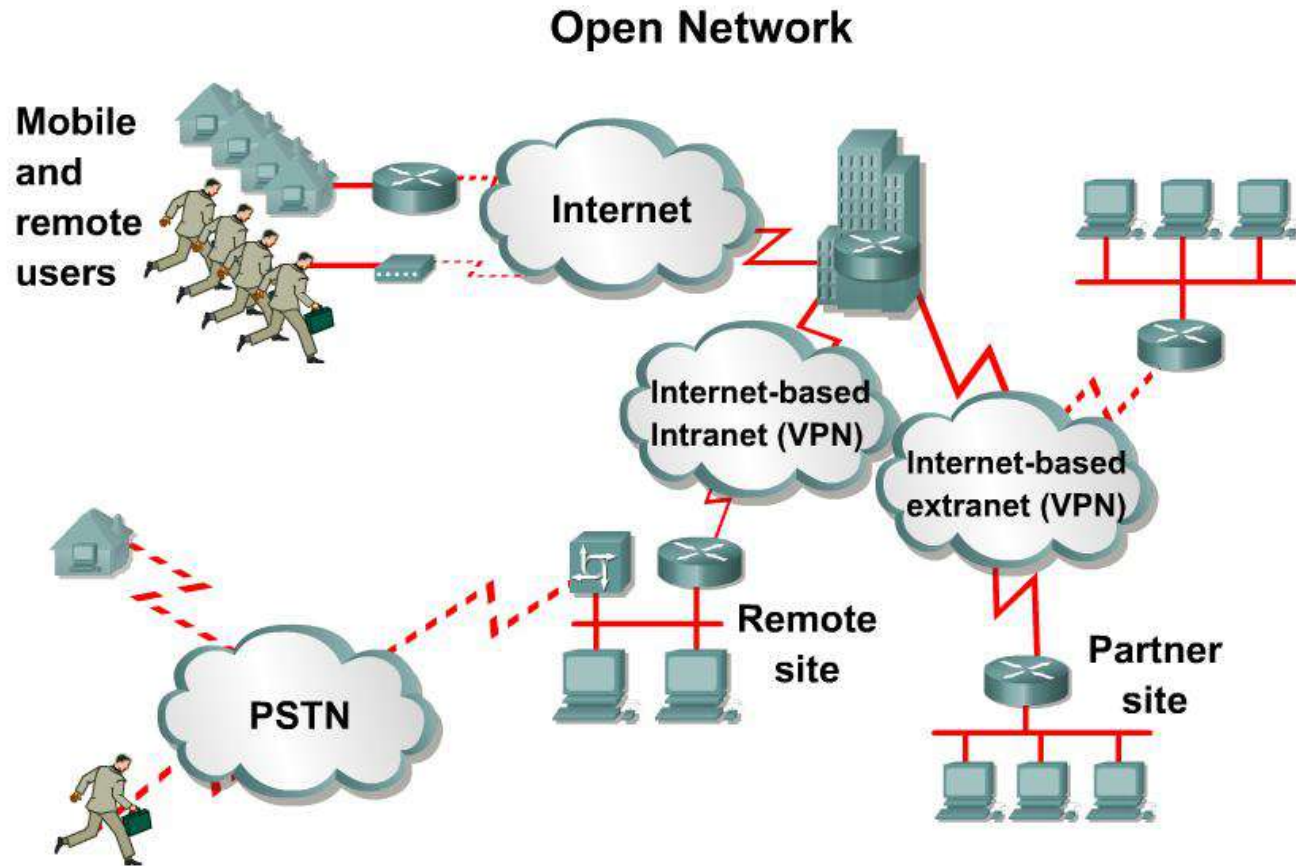
The Closed Network

3



The Network Today

4



Overview of network Security

Trends that Affect Security

5

- Increase of network attacks
- Increased sophistication of attacks
- Increased dependence on the network
- Lack of trained personnel
- Lack of awareness
- Lack of security policies
- Wireless access
- Legislation
- Litigation

Legal and Governmental Policy Issues

6

- Organizations that operate vulnerable networks will face increasing and substantial liability.
- US Federal legislation mandating security includes the following:
 - ▣ GLB financial services legislation
 - ▣ Government Information Security Reform Act
 - ▣ HIPAA
 - ▣ CIPA



The Goals of Network Security

7

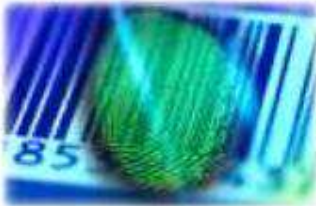
- Availability
- Confidentiality
- Integrity



Key Elements of Network Security

8

Identity



**Perimeter
Security**



Data Privacy



**Security
Monitoring**



**Security
Management**



**Authentication
Authorization
Accounting**

Firewalls

**Virtual Private
Network**

**Intrusion
Detection
Systems**

**Policy
Management
Tools**

Overview of network Security

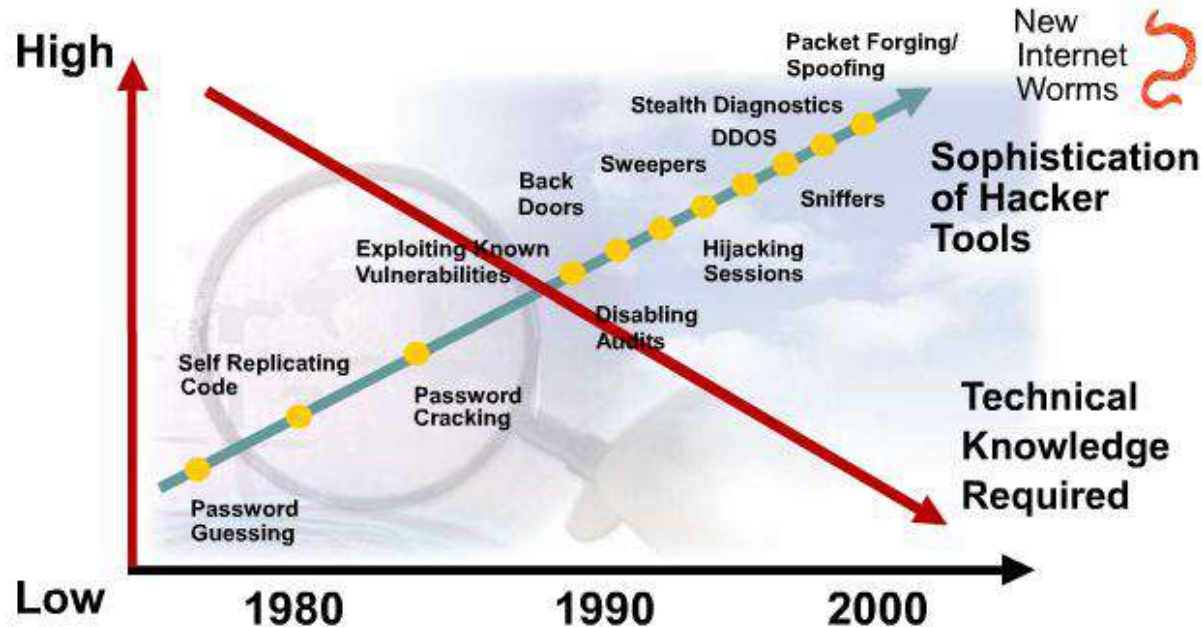
Network Vulnerabilities, Threats, and Attacks

9

- ❑ Technology
- ❑ Configuration
- ❑ Policy

Threat Capabilities—More Dangerous and Easier to Use

10

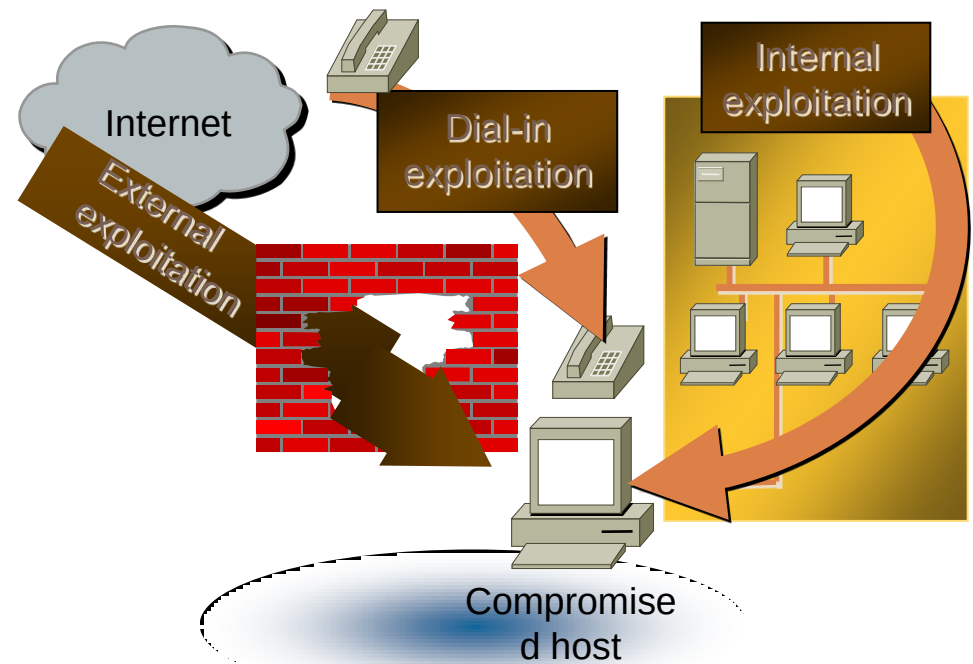


Threats continue to become more sophisticated as the technical knowledge required to implement attacks diminishes.

Network Threats

11

- Four general categories of security threats
 - ▣ Unstructured threats
 - ▣ Structured threats
 - ▣ External threats
 - ▣ Internal threats



Four Classes of Network Attacks

12

- ❑ Reconnaissance attacks
- ❑ Access attacks
- ❑ Denial of service attacks
- ❑ Worms, viruses, and Trojan horses

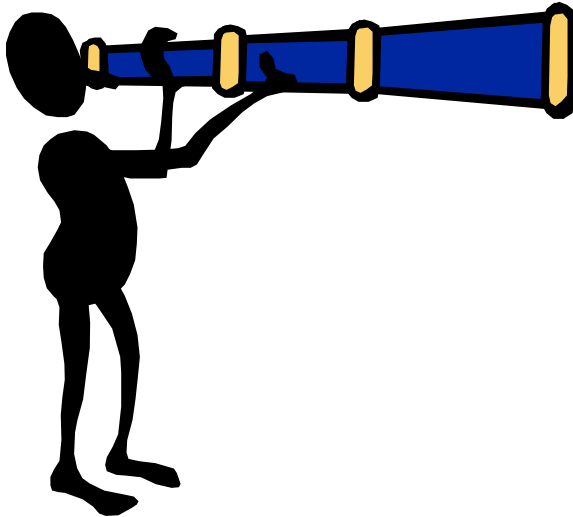
Specific Attack Types

13

- ❑ Packet sniffers
- ❑ IP weaknesses
- ❑ Password attacks
- ❑ DoS or DDoS
- ❑ Man-in-the-middle attacks
- ❑ Application layer attacks
- ❑ Trust exploitation
- ❑ Port redirection
- ❑ Virus
- ❑ Trojan horse
- ❑ Operator error
- ❑ Worms

Reconnaissance Attacks

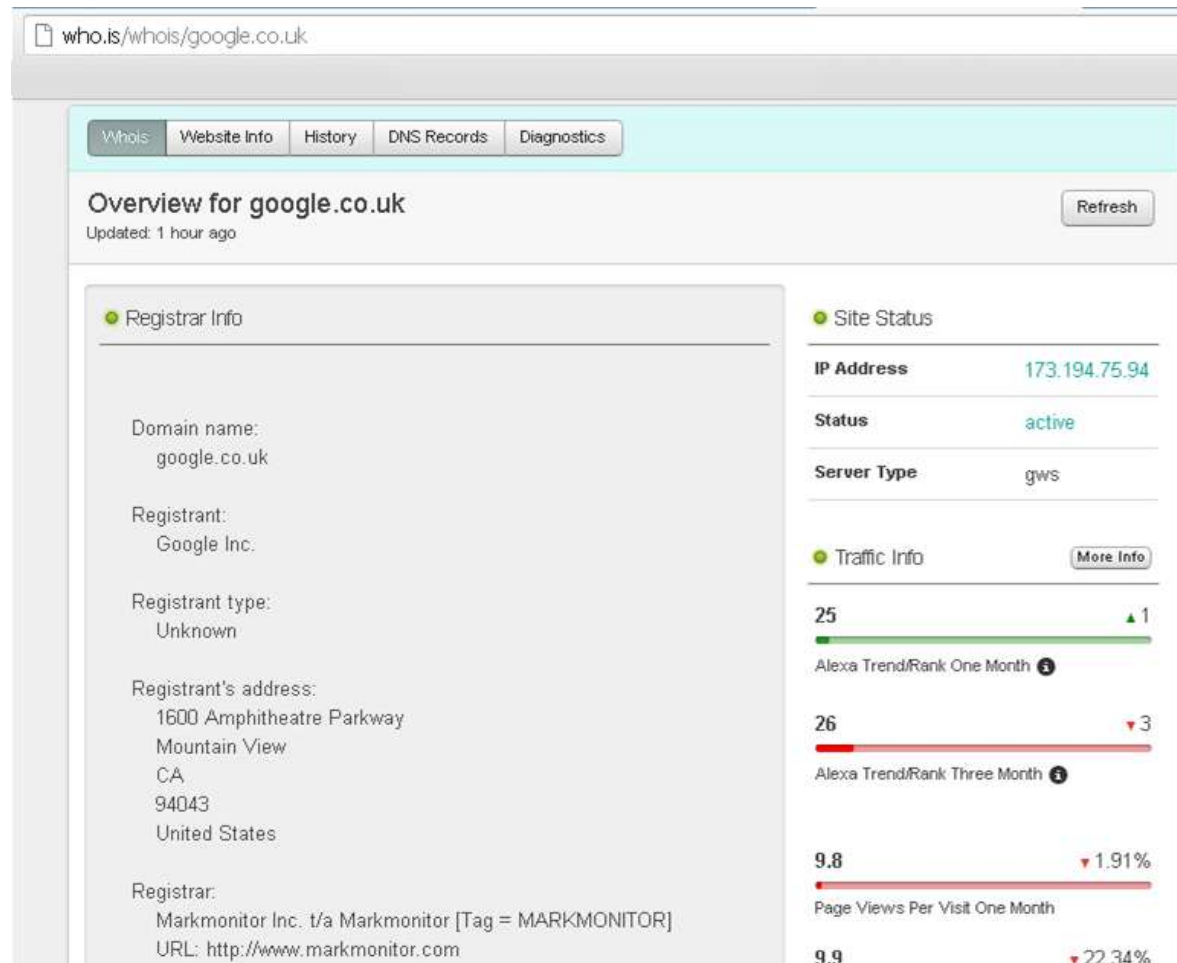
14



- The overall act of learning information about a target network.
- Uses publicly available information and applications.
 - ▣ IP address
 - ▣ Port number etc.

Reconnaissance Attack Example

15



Overview of network Security

Reconnaissance Attack Mitigation

16

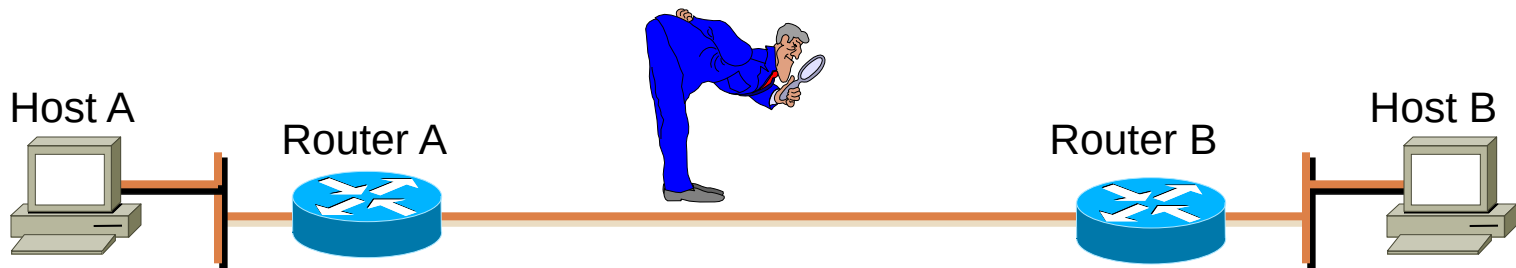


- Network reconnaissance can NOT be prevented entirely.
- Intrusion Detection System (IDS)
 - ▣ can usually notify an administrator about a reconnaissance at the network and host levels
 - ▣ ping sweeps, port scan etc.

Packet Sniffers

17

- A software application that uses a network adapter card in promiscuous mode to capture all network packets.
- Packet sniffers exploit information passed in clear text.
 - Telnet, FTP, SNMP, POP
- Packet sniffers must be on the same collision domain.



Packet Sniffer Mitigation

18

- ❑ Authentication—Using strong authentication, such as one-time passwords (OTP), is a first option for defense against packet sniffers.
- ❑ Switched infrastructure—Deploy a switched infrastructure to counter the use of packet sniffers in your environment.
- ❑ Antisniffer tools—Use these tools to employ software and hardware designed to detect the use of sniffers on a network.
- ❑ Cryptography—The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant.



IP Spoofing

19

- IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.
- Two general techniques used during IP spoofing
 - ▣ A hacker uses an IP address that is within the range of trusted IP addresses.
 - ▣ A hacker uses an authorized external IP address that is trusted.
- Uses for IP spoofing include the following:
 - ▣ IP spoofing is usually limited to the injection of malicious data or commands into an existing stream of data.
 - ▣ A hacker changes the routing tables to point to the spoofed IP address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

IP Spoofing Mitigation

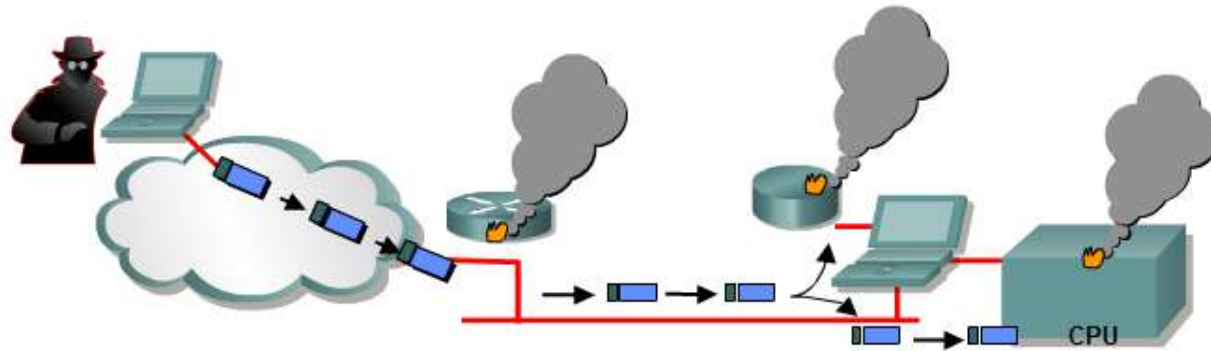
20

- The threat of IP spoofing can be reduced, but not eliminated.
 - ▣ Access control—The most common method for preventing IP spoofing is to properly configure access control.
 - ▣ RFC 2827 filtering—You can prevent users of your network from spoofing other networks (and be a good Internet citizen at the same time) by preventing any outbound traffic on your network that does not have a source address in your organization's own IP range.
 - ▣ Additional authentication that does not use IP-based authentication—Examples of this include the following:
 - Cryptographic (recommended)
 - Strong, two-factor, one-time passwords

DoS Attacks

21

DoS attacks prevent authorized people from using a service by using up system resources.



Resource overloads

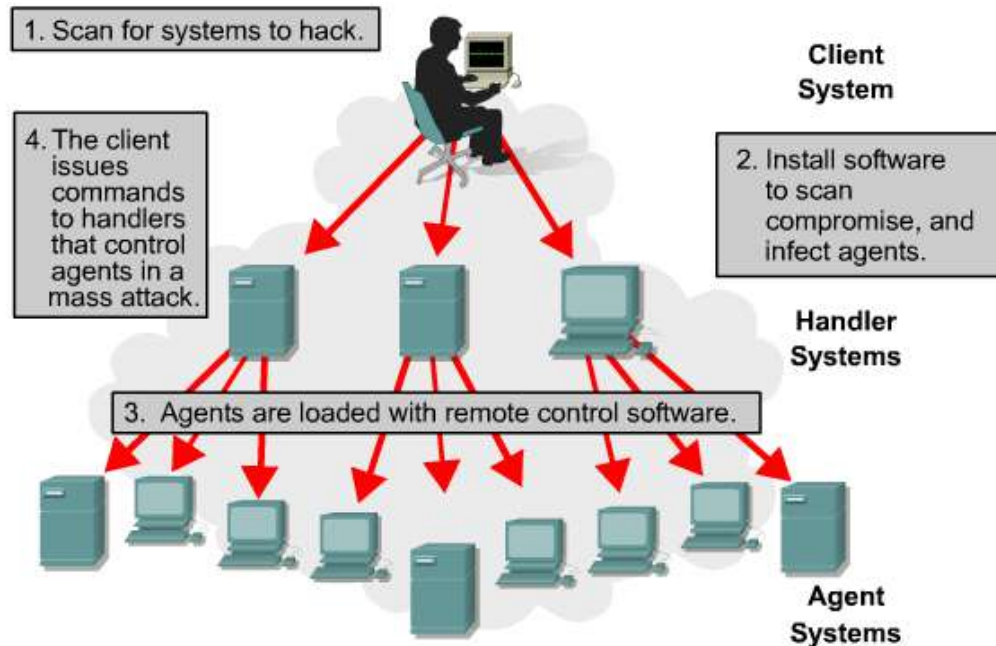
- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

Malformed data

- Oversized packets: ping of death, and so on.
- Overlapping packets: winuke, and so on.
- Un-handled data: teardrop, and so on.

DDoS Attack Example

22



In a Distributed Denial of Service attack (DDoS) a hacker tricks other machines into flooding the target machine with nuisance traffic that robs system performance.

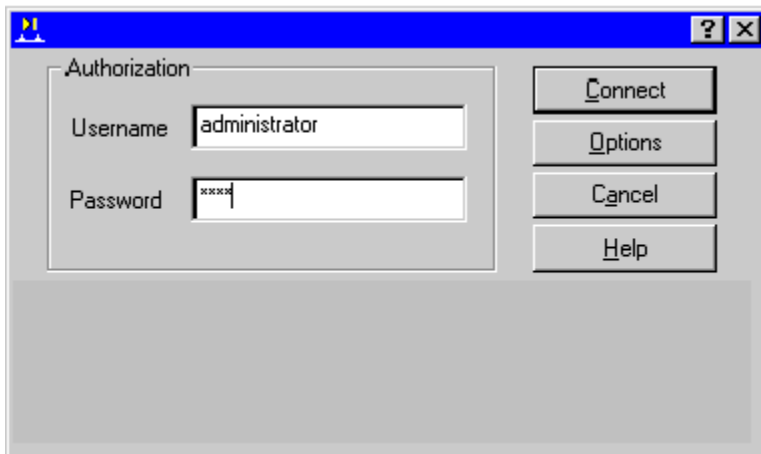
DoS Attack Mitigation

23

- The threat of DoS attacks can be reduced through the following three methods:
 - ▣ Antispoof features—Proper configuration of antispoof features on your routers and firewalls
 - ▣ Anti-DoS features—Proper configuration of anti-DoS features on routers and firewalls
 - ▣ Traffic rate limiting—Implement traffic rate limiting with the networks ISP

Password Attacks

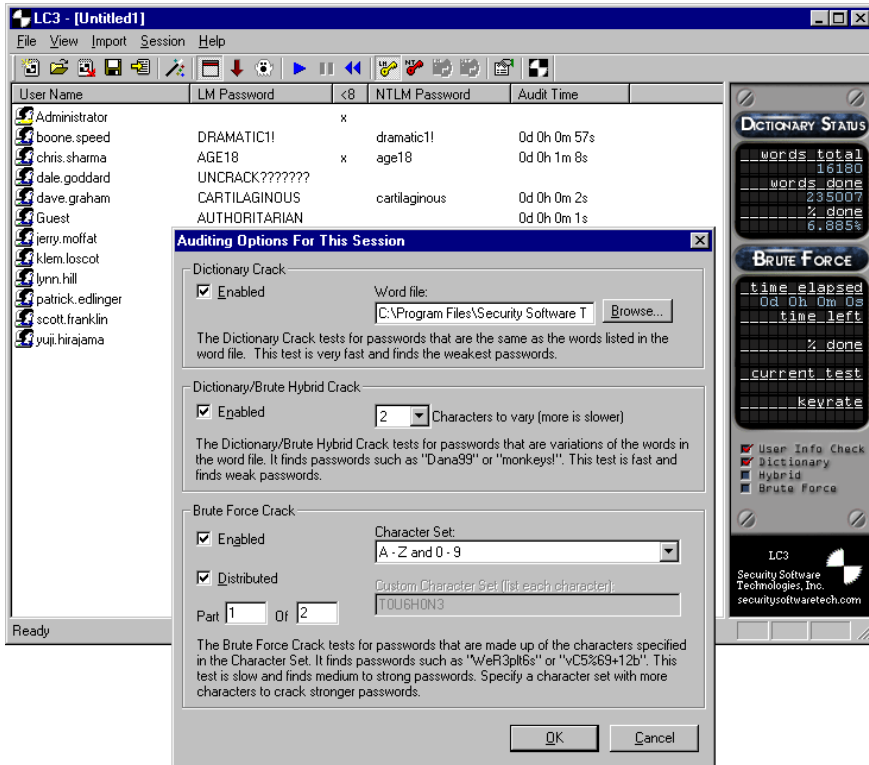
24



- ❑ Brute-force attacks
- ❑ Dictionary Attacks
- ❑ Trojan horse programs
- ❑ IP spoofing
- ❑ Packet sniffers

Password Attack Example

25



- L0phtCrack
 - A password Auditing and recovery tool
 - Can take the hashes of passwords and generate the clear text passwords from them.
- Password computation methods
 - Dictionary cracking
 - Brute force computation

Password Attacks Mitigation

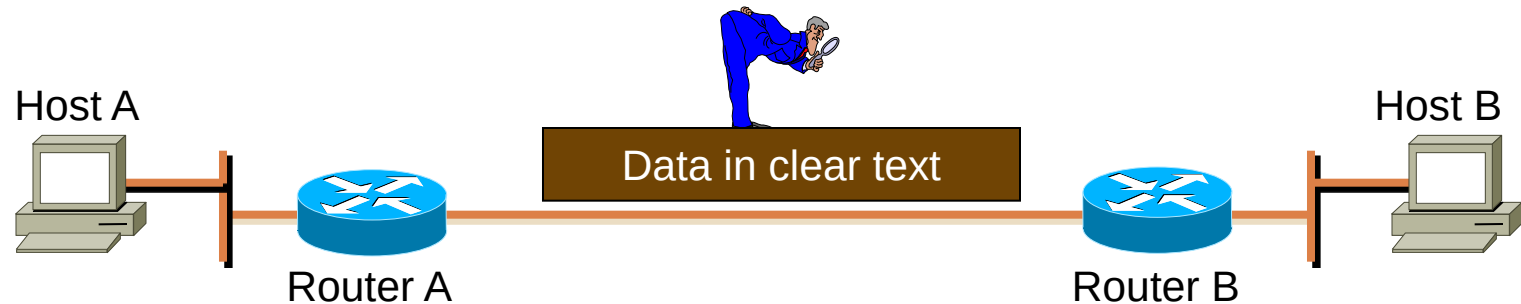
26

- ❑ Do not allow users to use the same password on multiple systems.
- ❑ Disable accounts after a certain number of unsuccessful login attempts.
- ❑ Do not use plain text passwords. OTP or a cryptographic password is recommended.
- ❑ Use “strong” passwords.
 - ❑ at least eight characters long
 - ❑ uppercase and lowercase letters, numbers, and special characters.

Man-in-the-Middle Attacks

27

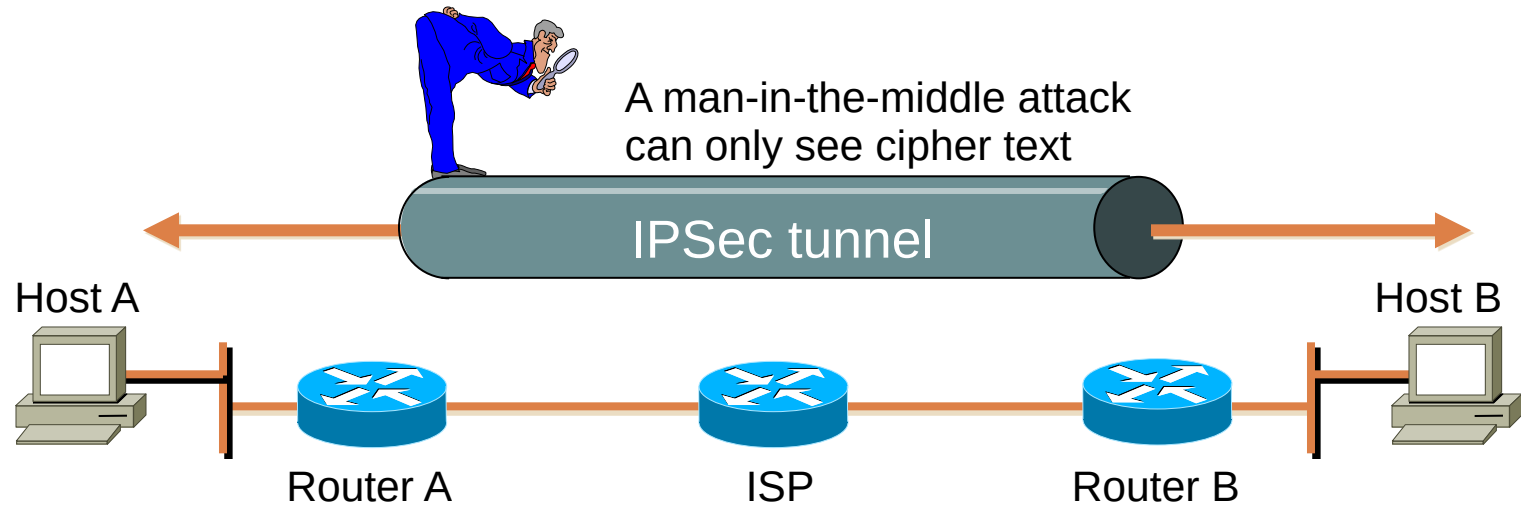
- The hacker needs to have access to network packets that come across a network.
 - ▣ Theft of information, Hijacking of an ongoing session
 - ▣ Traffic analysis, DoS
 - ▣ Corruption of transmitted data
 - ▣ Introduction of new information into network sessions
- A man-in-the-middle attack is implemented using the following:
 - ▣ Network packet sniffers
 - ▣ Routing and transport protocols



Man-in-the-Middle Mitigation

28

- Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography (encryption).



SSL and IPsec

29

	SSL	IPsec
Applications	Web-enabled applications, file sharing, Email	All IP-based applications
Encryption	Moderate to Strong Key lengths from 40 bits to 256 bits	Strong Key lengths from 56 bits to 256 bits
Authentication	Moderate One-way or two-way authentication	Strong Two-way authentication using shared secrets or digital certificates
Connection Complexity	Low Requires only a web browser	Moderate Can be challenging to nontechnical users
Connection Options	Any device can connect	Only specific devices with specific configurations can connect

Application Layer Attacks

30

- ❑ Exploit well known weaknesses, such as protocols, that are intrinsic to an application or system (for example, sendmail, HTTP, and FTP)
- ❑ Often use ports that are allowed through a firewall (for example, TCP port 80 used in an attack against a web server behind a firewall)
- ❑ Can never be completely eliminated, because new vulnerabilities are always being discovered

Application Layer Attacks Mitigation

31

- Measures that can be taken to reduce the risks
 - ▣ Read operating system and network log files, or have them analyzed by log analysis applications.
 - ▣ Subscribe to mailing lists that publicize vulnerabilities.
 - ▣ Keep your operating system and applications current with the latest patches.
 - ▣ IDSs can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks.

Trust Exploitation

32

- A hacker leverages existing trust relationships

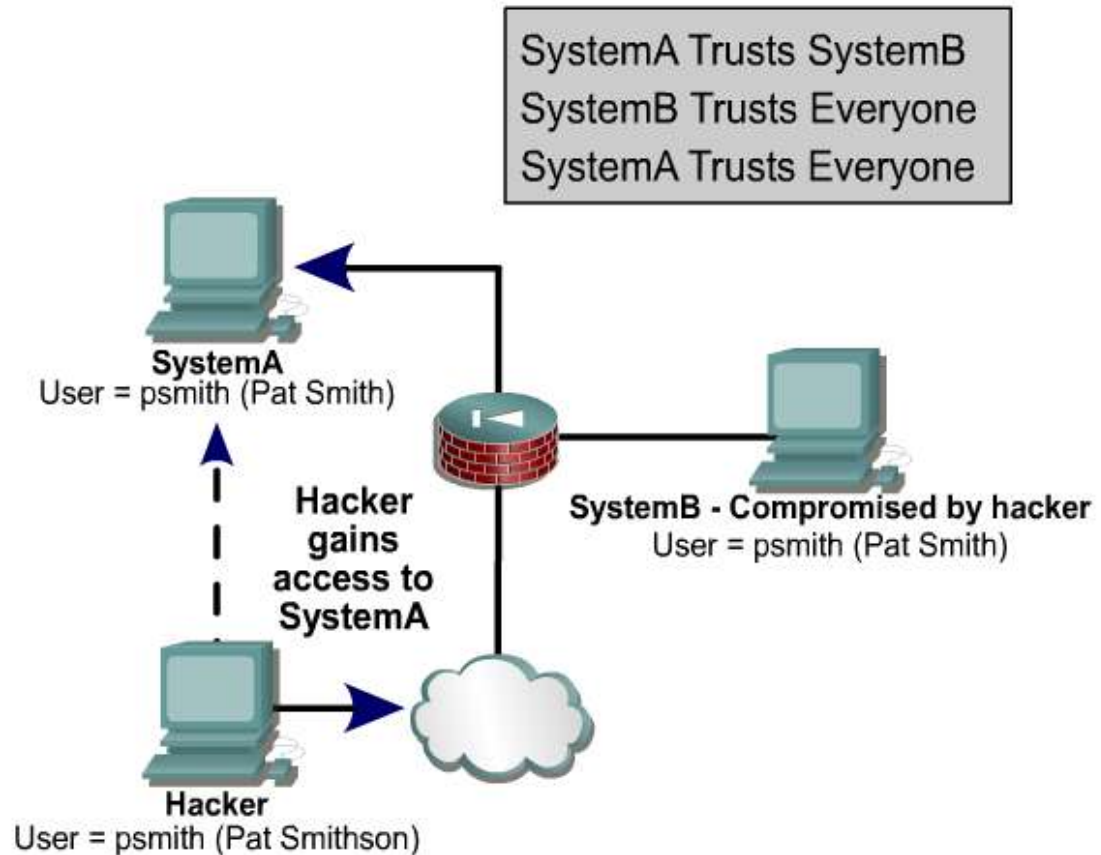
- Several trust models exist

- Windows

- Domains
- Active directory

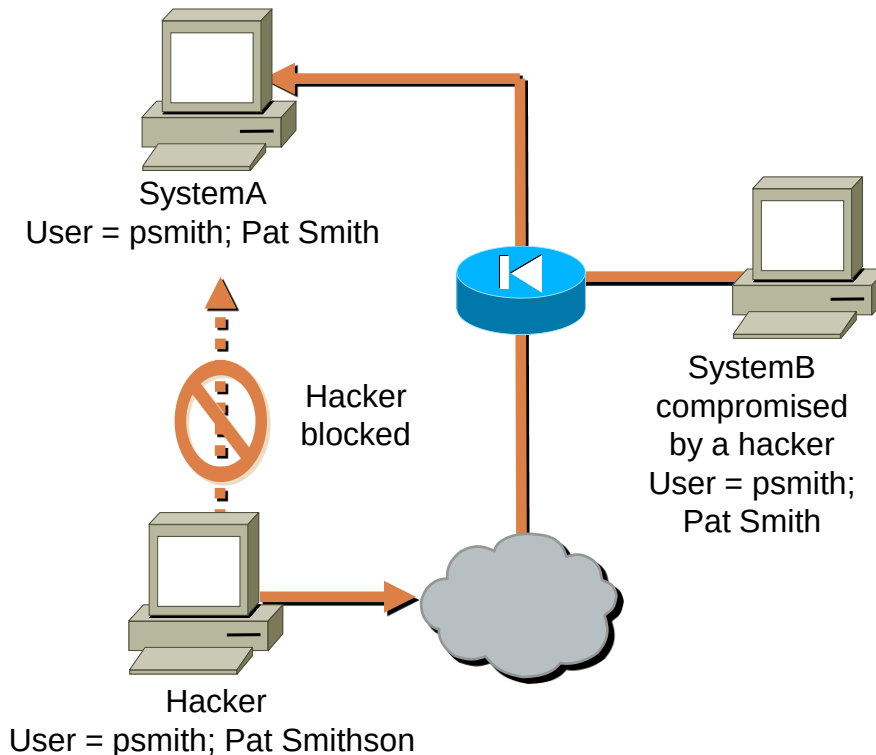
- Linux and UNIX

- NFS
- NIS+



Trust Exploitation Mitigation

33



- Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall.
- Such trust should be limited to specific protocols and should be validated by something other than an IP address where possible.

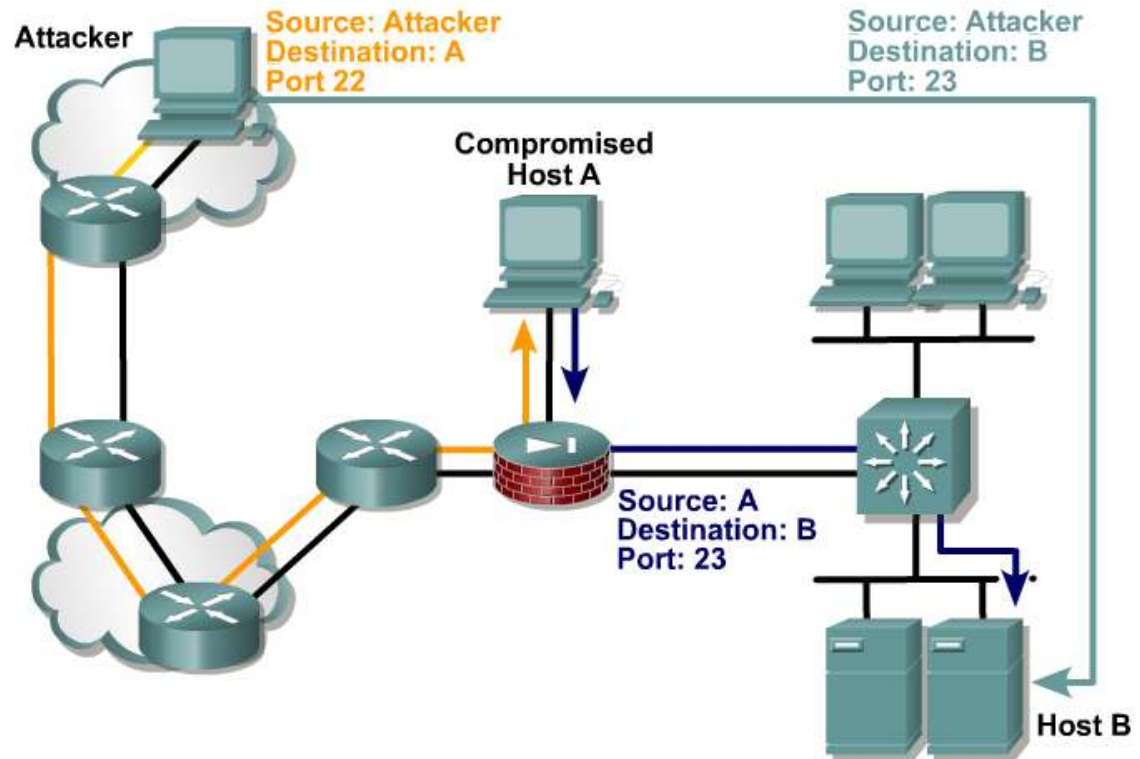
Port Redirection

34

Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.

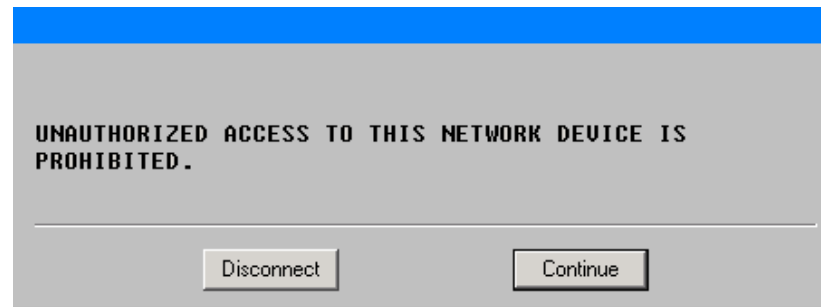
It is mitigated primarily through the use of proper trust models.

Antivirus software and host-based IDS can help detect and prevent a hacker installing port redirecting utilities on the host.



Unauthorized Access

35



- ❑ Unauthorized access includes any unauthorized attempt to access a private resource:
 - ❑ Not a specific type of attack
 - ❑ Refers to most attacks executed in networks today
 - ❑ Initiated on both the outside and inside of a network
- ❑ The following are mitigation techniques for unauthorized access attacks:
 - ❑ Eliminate the ability of a hacker to gain access to a system
 - ❑ Prevent simple unauthorized access attacks, which is the primary function of a firewall

Virus and Trojan Horses

36

□ Viruses

- ▣ malicious software that are attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.

□ Trojan horse

- ▣ the entire application was written to look like something else, when in fact it is an attack tool. A Trojan horse is mitigated by antivirus software at the user level and possibly the network level.

Vulnerabilities Exist at all OSI Layers

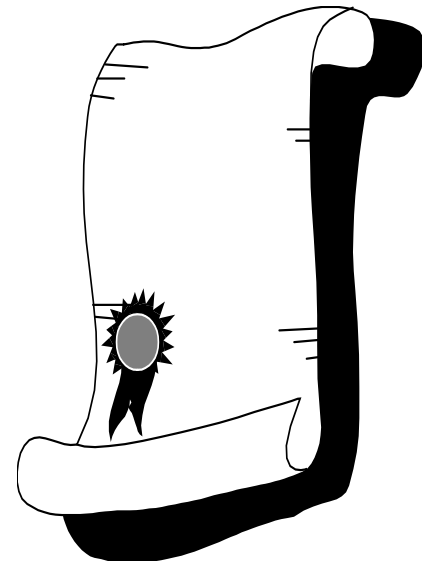
37



What Is a Security Policy?

38

- (RFC 2196, Site Security Handbook)
 - ▣ “A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.”



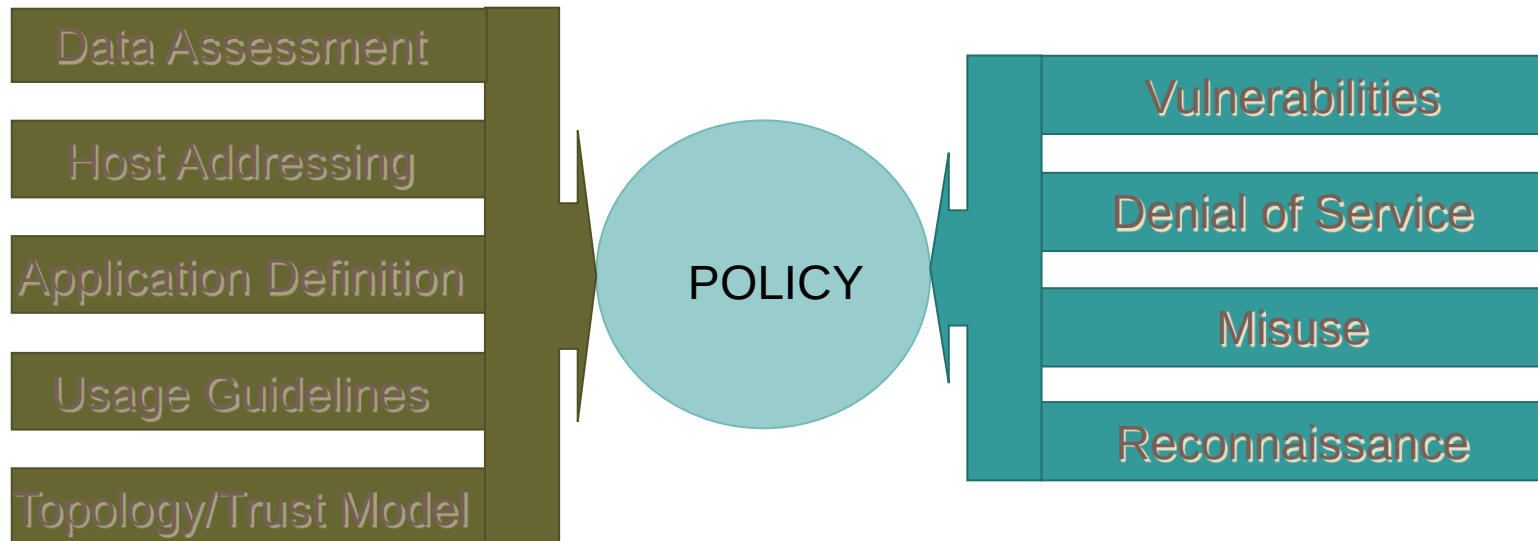
Why Create a Security Policy?

39

- ❑ To create a baseline of your current security posture
- ❑ To set the framework for security implementation
- ❑ To define allowed and not allowed behaviors
- ❑ To help determine necessary tools and procedures
- ❑ To communicate consensus and define roles
- ❑ To define how to handle security incidents

Security Policy Elements

40



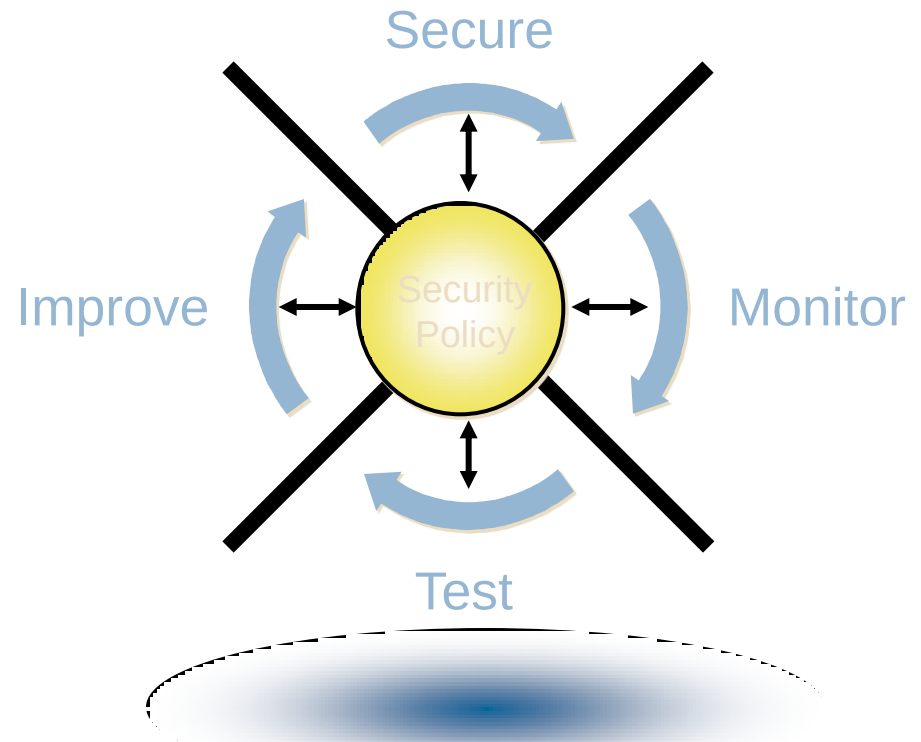
- On the left are the network design factors upon which security policy is based
- On the right are basic Internet threat vectors toward which security policies are written to mitigate

Network Security as a Continuous Process

41

- Network security is a continuous process built around a security policy.

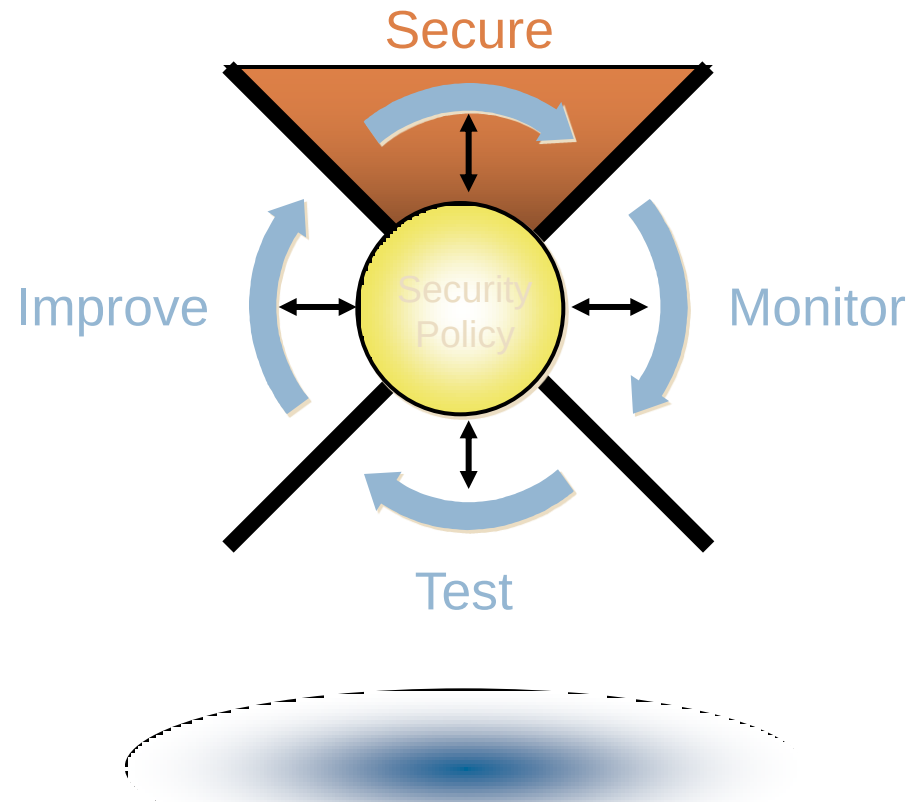
- ▣ Step 1: Secure
- ▣ Step 2: Monitor
- ▣ Step 3: Test
- ▣ Step 4: Improve



Secure the Network

42

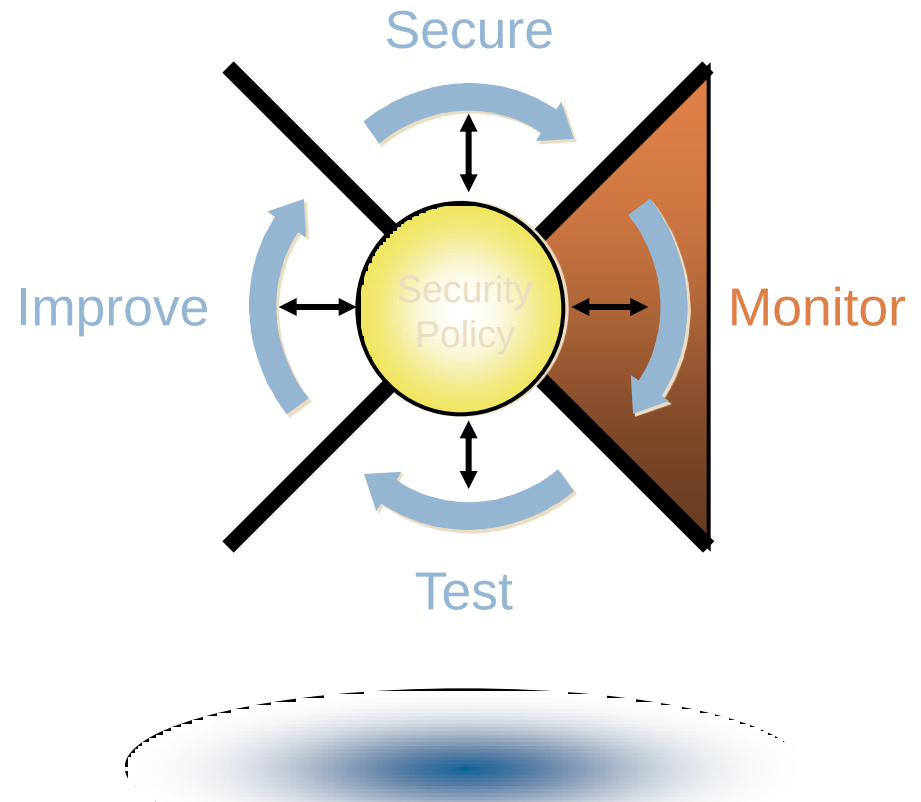
- Implement security solutions to stop or prevent unauthorized access or activities, and to protect information:
 - ▣ Authentication
 - ▣ Encryption
 - ▣ Firewalls
 - ▣ Vulnerability patching



Monitor Security

43

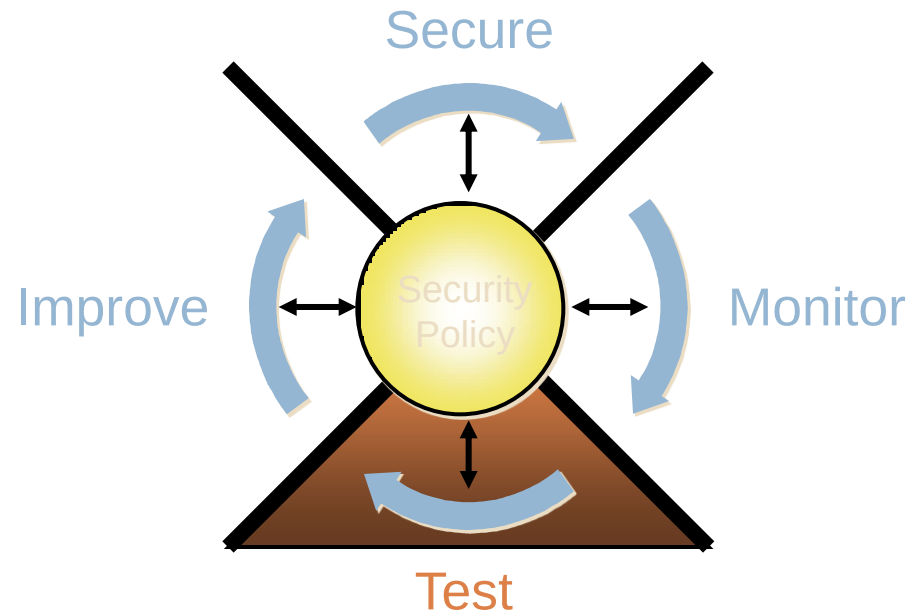
- ❑ Detects violations to the security policy
- ❑ Involves system auditing and real-time intrusion detection
- ❑ Validates the security implementation in Step 1



Test Security

44

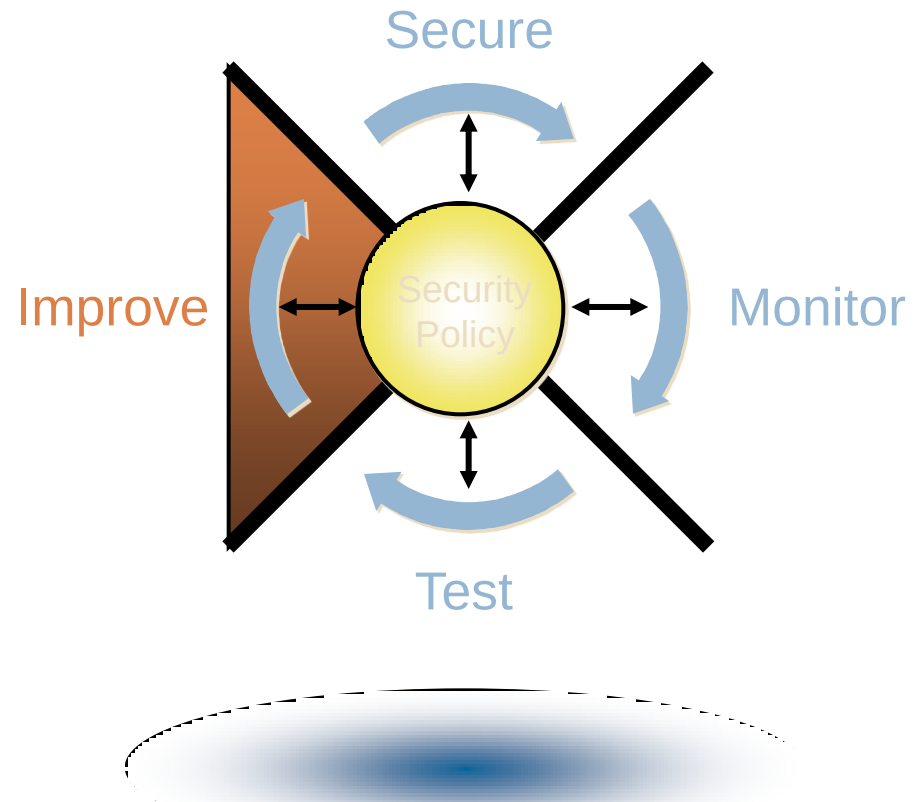
- Validates effectiveness of the security policy through system auditing and vulnerability scanning



Improve Security

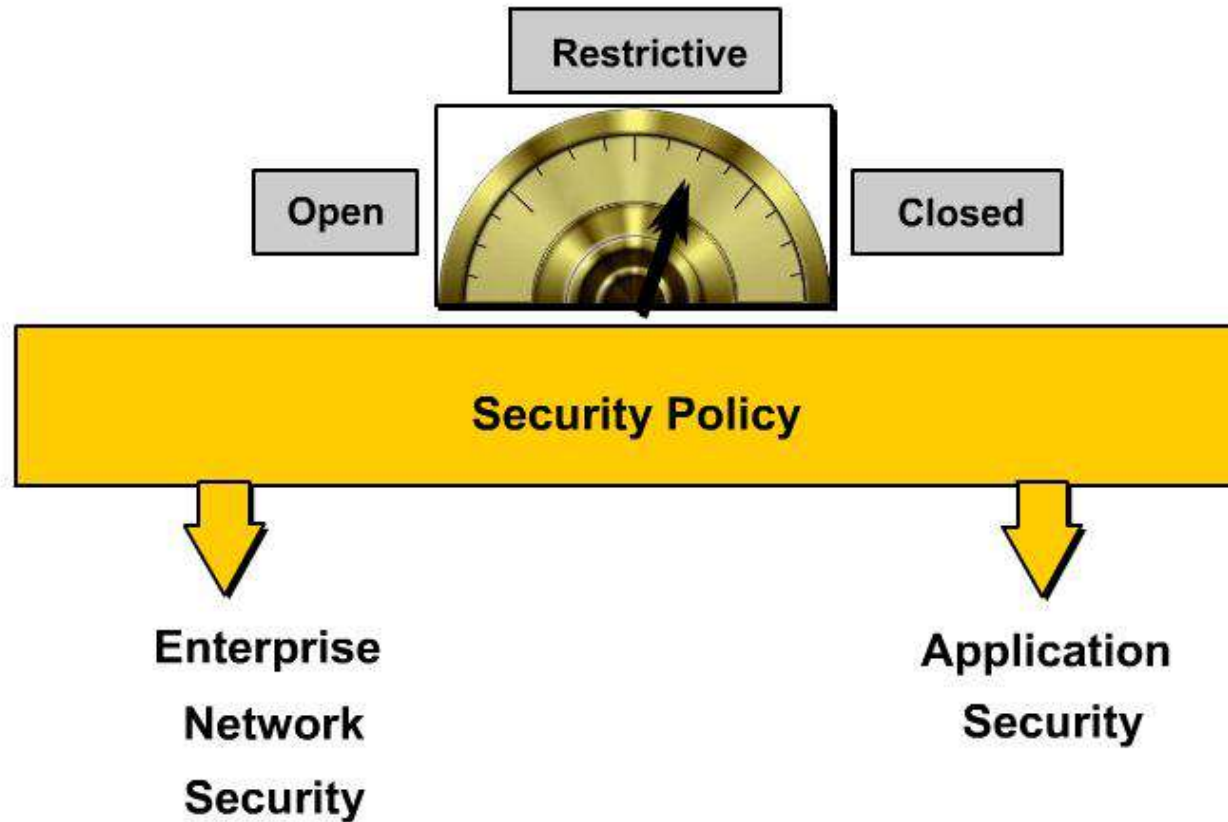
45

- Use information from the monitor and test phases to make improvements to the security implementation.
- Adjust the security policy as security vulnerabilities and risks are identified.



Network Security Models

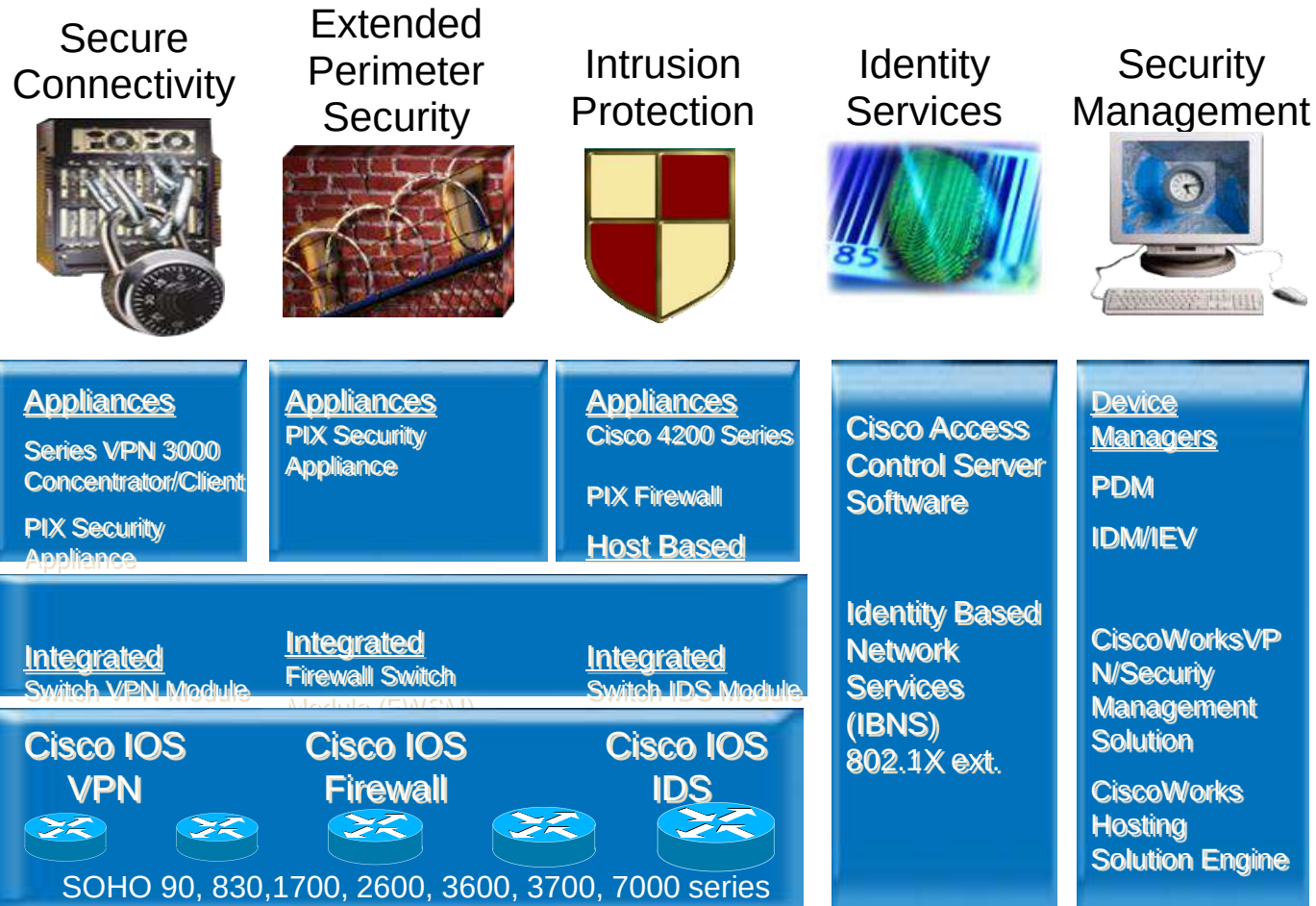
46



Overview of network Security

Security Products and Solutions

47



Overview of network Security

User Identity

48

- Mechanisms for proving who you are
 - ▣ Both people and devices can be authenticated
- Three authentication attributes:
 - ▣ Something you know
 - ▣ Something you have
 - ▣ Something you are
- Common approaches to Identity:
 - ▣ Passwords
 - ▣ Tokens
 - ▣ PKI (Digital Certificates)
 - ▣ Biometrics



Cisco ACS 3.1 and Appliance

49

- ❑ Windows 2000 & NT
- ❑ RADIUS and TACACS+
- ❑ High performance (400+ authentications per second)
- ❑ Wireless security enhancements
- ❑ Supports any access: wireless, Firewall, VPN, voice, content or switched
- ❑ 802.1x provides IBNS for wireless and switch port authentication
- ❑ Support for directory services and LDAP



Types of Firewalls

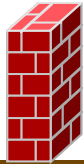
50



- Server Based
 - Microsoft ISA
 - CheckPoint
 - BorderManager
- Appliance
 - PIX Security Appliance
 - Netscreen
 - SonicWall
- Personal
 - Norton
 - McAfee
 - ZoneAlarms
- Integrated
 - IOS Firewall
 - Switch Firewall

Firewall Solutions

51

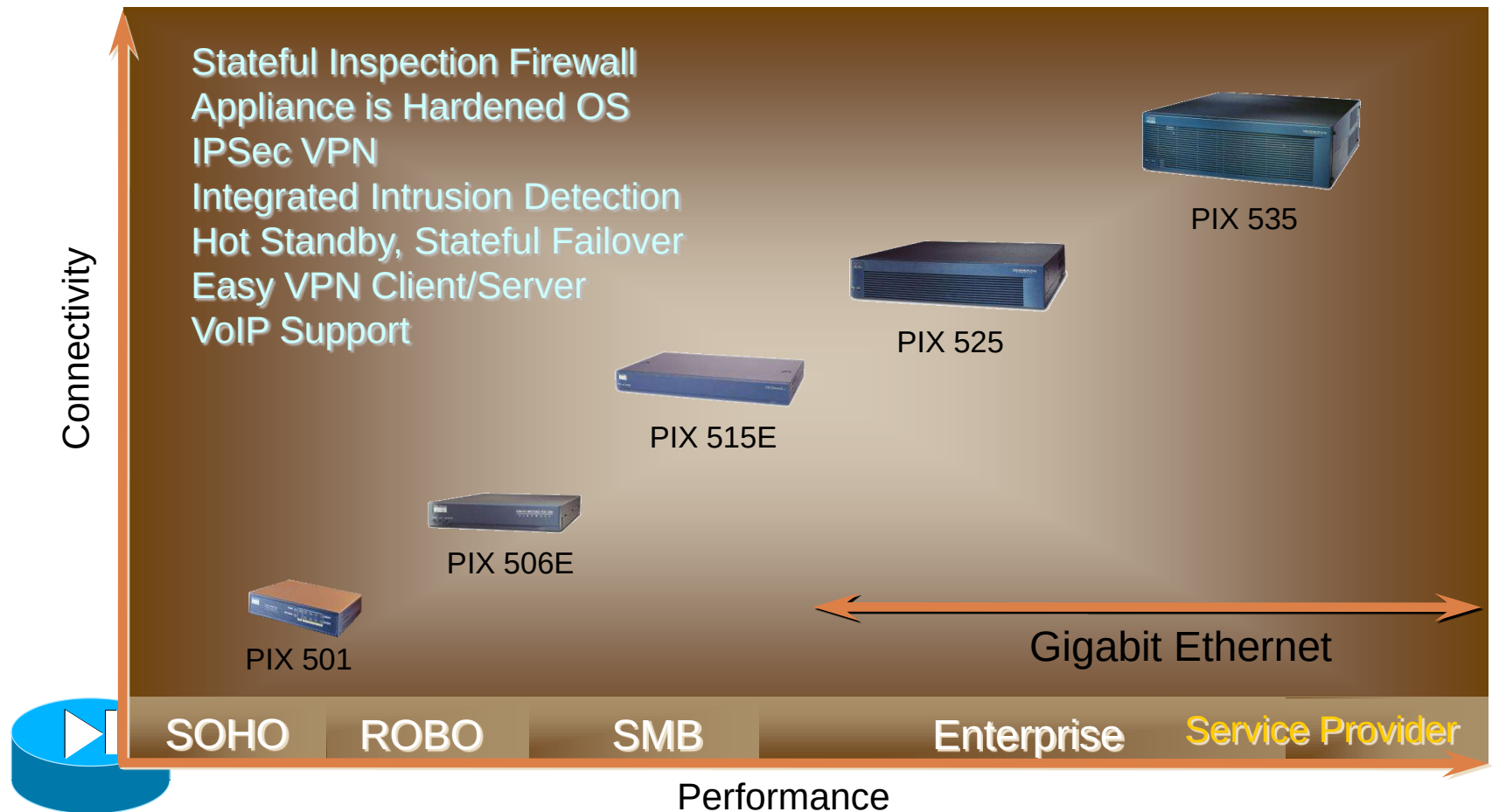


		Solution Breadth				
PIX Appliance		PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Switch Module		Firewall Service Module (FWSM)				
IOS FW Router		800	1700	2600	3xxx	7xxx
VPN Client		VPN Client Software — Built in Personal FW				
Mgmt		Secure CLI		Web UI Embedded Mgr		Enterprise Mgmt VMS

Overview of network Security

PIX Security Appliance Lineup

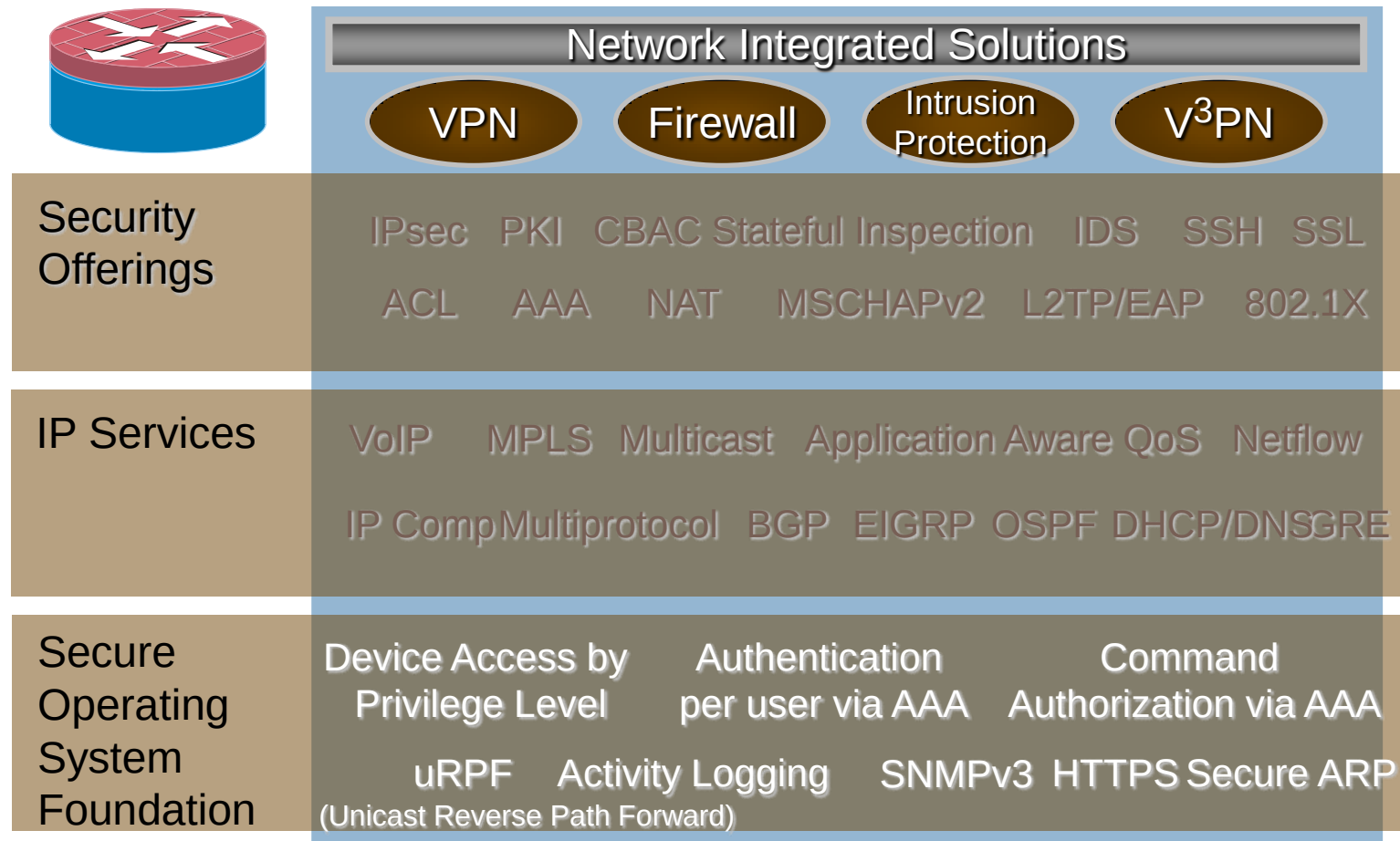
52



Overview of network Security

IOS Firewall

53



Overview of network Security

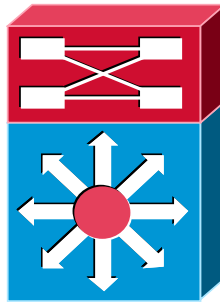
Catalyst Switch Integration

54

Appliance Capabilities



Cisco Infrastructure



Security Services Modules



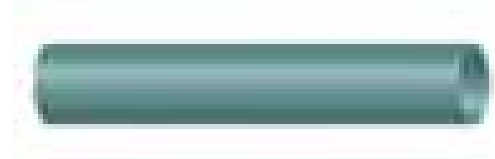
© 2002, Cisco Systems, Inc. All rights reserved.

Overview of network Security

Secure Connectivity

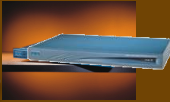
55

- Defines “peers”
 - ▣ Two devices in a network that need to connect
 - ▣ Tunnel makes peers seem virtually next to each other
 - ▣ Ignores network complexity in between
- Technologies
 - ▣ Point-to-Point Tunneling Protocol (PPTP)
 - ▣ Layer 2 Tunneling Protocol (L2TP)
 - ▣ IP Security (IPSec)
 - ▣ Secure Shell (SSH)
 - ▣ Secure Sockets Layer (SSL)
 - ▣ Transport Layer Security (TLS)



VPN Solutions

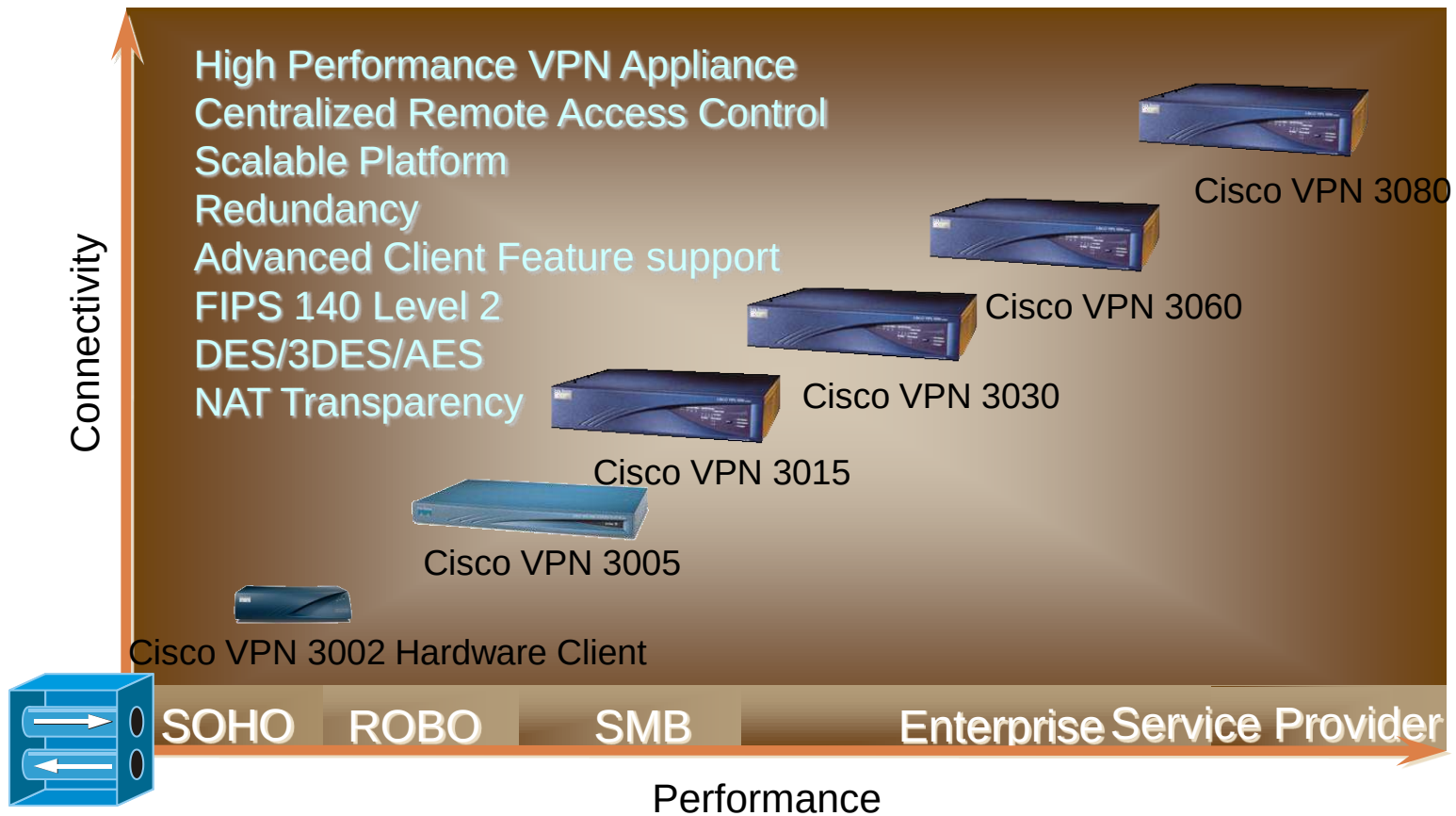
56

Solution Breadth						
3000 Concentrator		3005	3015	3030	3060	3080
Switch Module		VPN Service Module (VPNSM)				
VPN Client		VPN Client Software		3002		
Router		800	1700	2600	3xxx	7xxx
PIX		PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Mgmt		Secure Menu, CLI		Web UI Embedded Mgr		Enterprise Mgmt VMS

Overview of network Security

VPN 3000 Concentrator Lineup

57

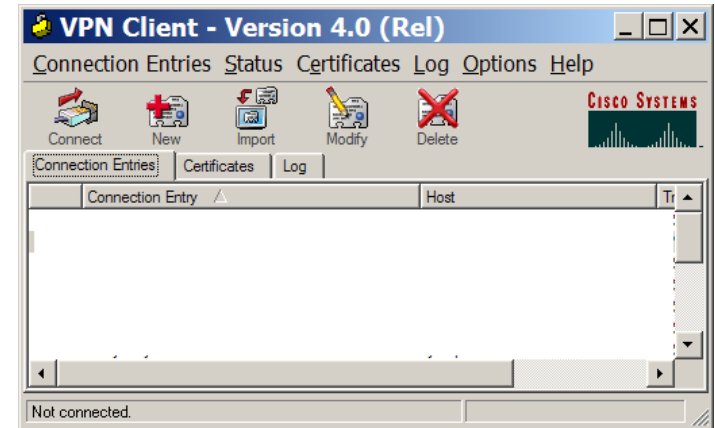


Overview of network Security

Cisco VPN Software Client

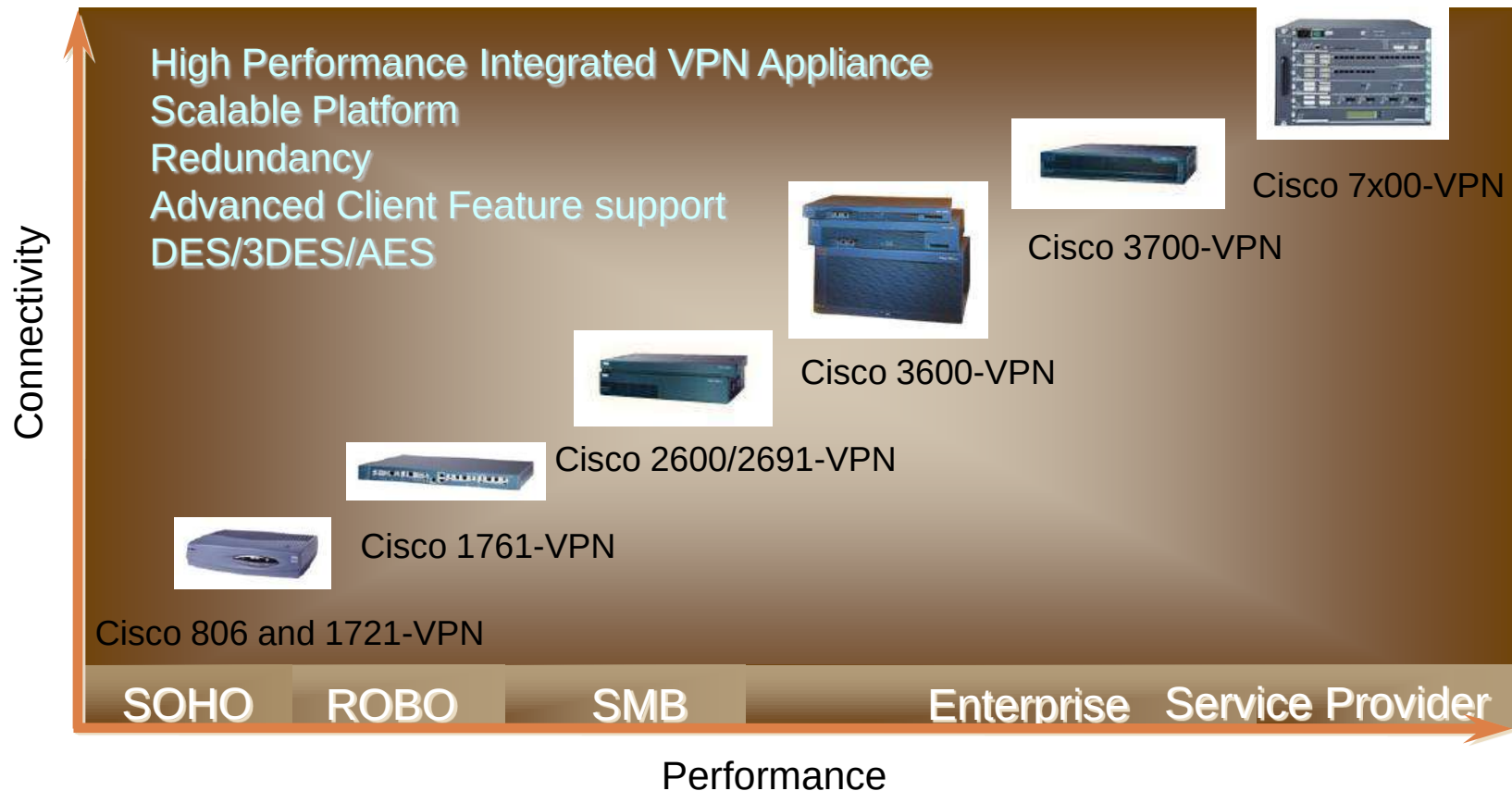
58

- ❑ Supported Operating Systems
- ❑ Windows 95, 98, NT, 2K ME XP
- ❑ Solaris, Linux
- ❑ Mac OS X
- ❑ Virtual Adapter (Win2K / XP)
- ❑ Common Graphical Interface for Windows and Mac VPN Clients (New GUI)
- ❑ Alerts (Delete With Reason)
- ❑ Personal Firewall Enhancements (including AYT for Cisco Security Agent & Sygate)
- ❑ Coexistence with Third-Party VPN Vendors
- ❑ Encryption using DES, 3DES, or AES
- ❑ Terminate on Cisco IOS routers, PIX firewalls, VPN 3000
- ❑ Centralized Configuration & Policy Management
- ❑ v3.6 is FIPS 140-1 Level 1 Certified



VPN Router Lineup

59



IDS Solutions

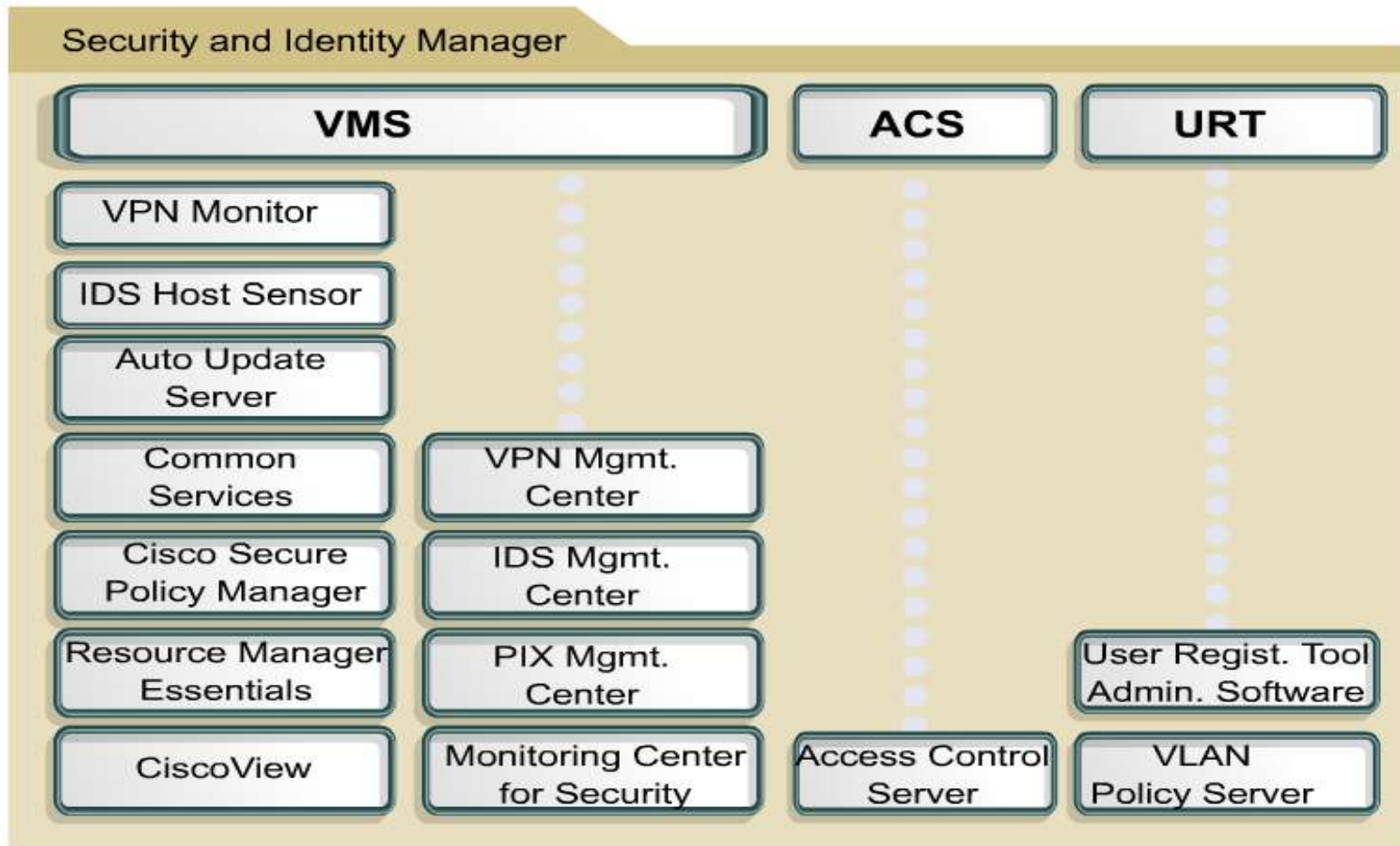
60

		Solution Breadth				
Network Sensor		4210	4235	4250	4250-XL	
Switch Sensor		IDSM-2				
Host Sensor		Server Agent		Desktop Agent		
Router Sensor		800	1700	2600	3xxx	7xxx
Firewall Sensor		PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Mgmt		Secure Command Line		Web UI Embedded Mgr	Enterprise Mgmt VMS	

Overview of network Security

Security and Identity Management Solutions Lineup

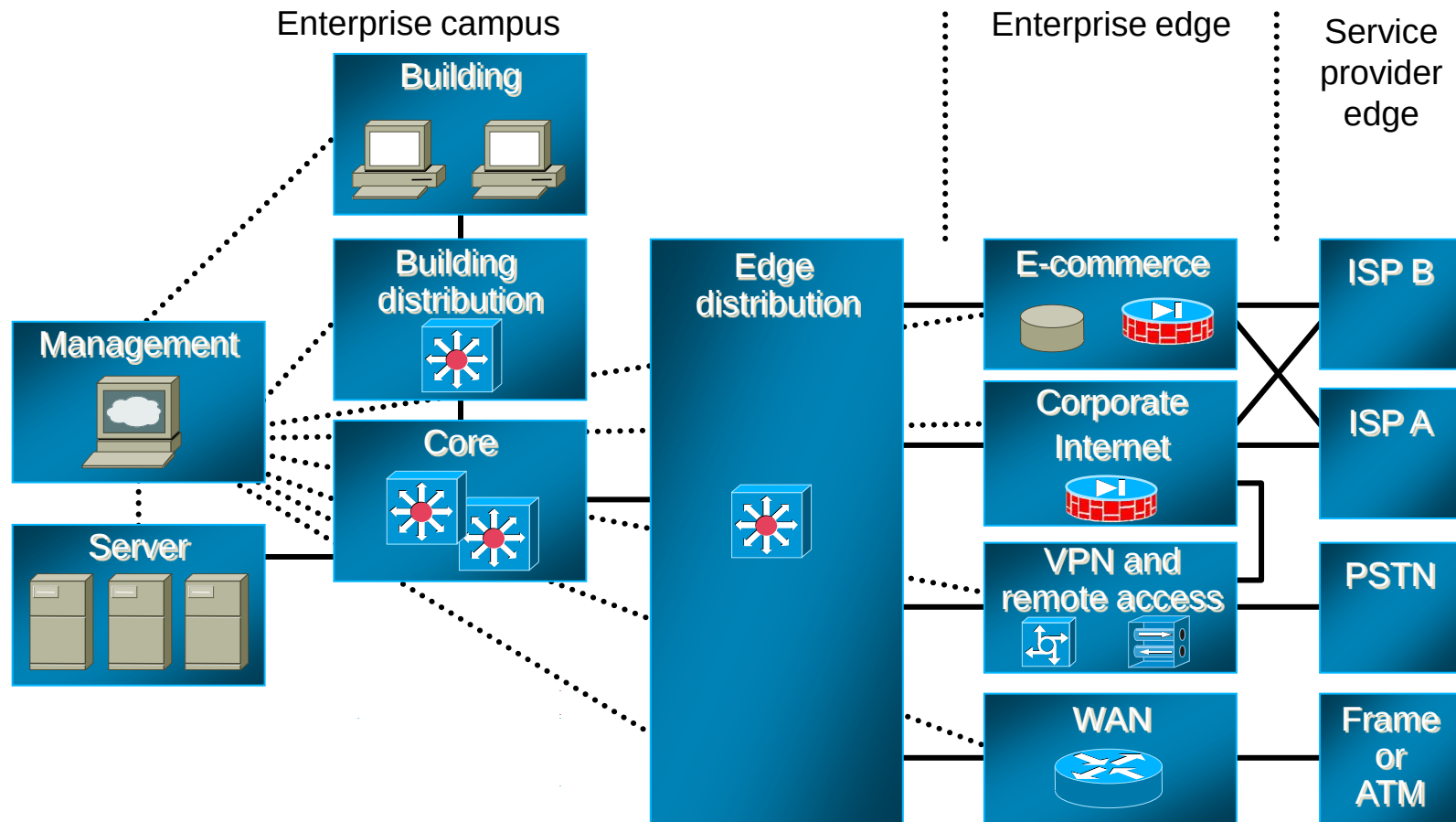
61



Overview of network Security

SAFE Modular Blueprint

62



Overview of network Security

Security Resources on the Internet

63

- ❑ Cisco Connection Online—<http://www.cisco.com>
- ❑ SecurityFocus.com—<http://www.securityfocus.com>
- ❑ SANS—<http://www.sans.org>
- ❑ CERT—<http://www.cert.org>
- ❑ CIAC—<http://www.ciac.org/ciac>
- ❑ CVE—<http://cve.mitre.org>
- ❑ Computer Security Institute—<http://www.gocsi.com>
- ❑ Center for Internet Security—<http://www.cisecurity.org>
- ❑ Cisco Connection Online—
 - ❑ <http://www.cisco.com/go/security>
- ❑ Cisco Product Specific Incident Response Team (PSIRT)—
 - ❑ <http://www.cisco.com/go/psirt>

Summary

64

- ▣ The need for network security has increased as networks have become more complex and interconnected.
- ▣ The following are the four types of security threats:
 - Structured
 - Unstructured
 - Internal
 - External
- ▣ Common attack methods and techniques used by hackers
 - Reconnaissance
 - Access
 - Denial of Service

Summary (cont.)

65

- ▣ The Security Wheel is the graphical representation of security improvement life cycle.
- ▣ There are many components of a complete security policy
- ▣ Common management protocols are integral to maintaining a secure infrastructure
- ▣ Five key areas of network security are
 - Perimeter Security
 - Secure Connectivity
 - Identity Services
 - Intrusion Detection
 - Management