COMPASS
TECHNOLOGY MANAGEMENT

IT Security
A Disciplined Approach
ICCM June 2002

ICCM 2002 Tech 3
Saturday: 3:30 …
Don Murdoch / Sr. Consultant
Compass Technology Management
505 Independence Pkwy Suite 101
Chesapeake VA 757.233.7300
www.compass.net &
www.intellisafevault.com

Topics / Agenda

- The Ten Information Security Knowledge Domains
- The Ten Immutable Laws
- Events and Statistics
- Overall Design
- Policies

- In-depth discussions on:
  - Intruder Detection
  - Firewalls
  - Remote access
  - Email
  - Auditing

The Ten Information Security Knowledge Domains

- Access Control
- Application and System Development
- Cryptography
- DRP and BCP
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Management Practices
- Security Models
- Telecommunications and Network Security

Source: Information Security Managers Handbook, 4TH Edition
Professional Certifications – CISSP, CISA, SCNP, etc.

The Ten Immutable Laws

from Scott Culp, Microsoft Corp.(1/2)

- Nobody believes anything bad can happen to them, until it does.
- Security only works if the secure way also happens to be the easy way.
- If you don't keep up with security fixes, your network won't be yours for long.
- It doesn't do much good to install security fixes on a computer that was never secured to begin with.
- Eternal vigilance is the price of security.

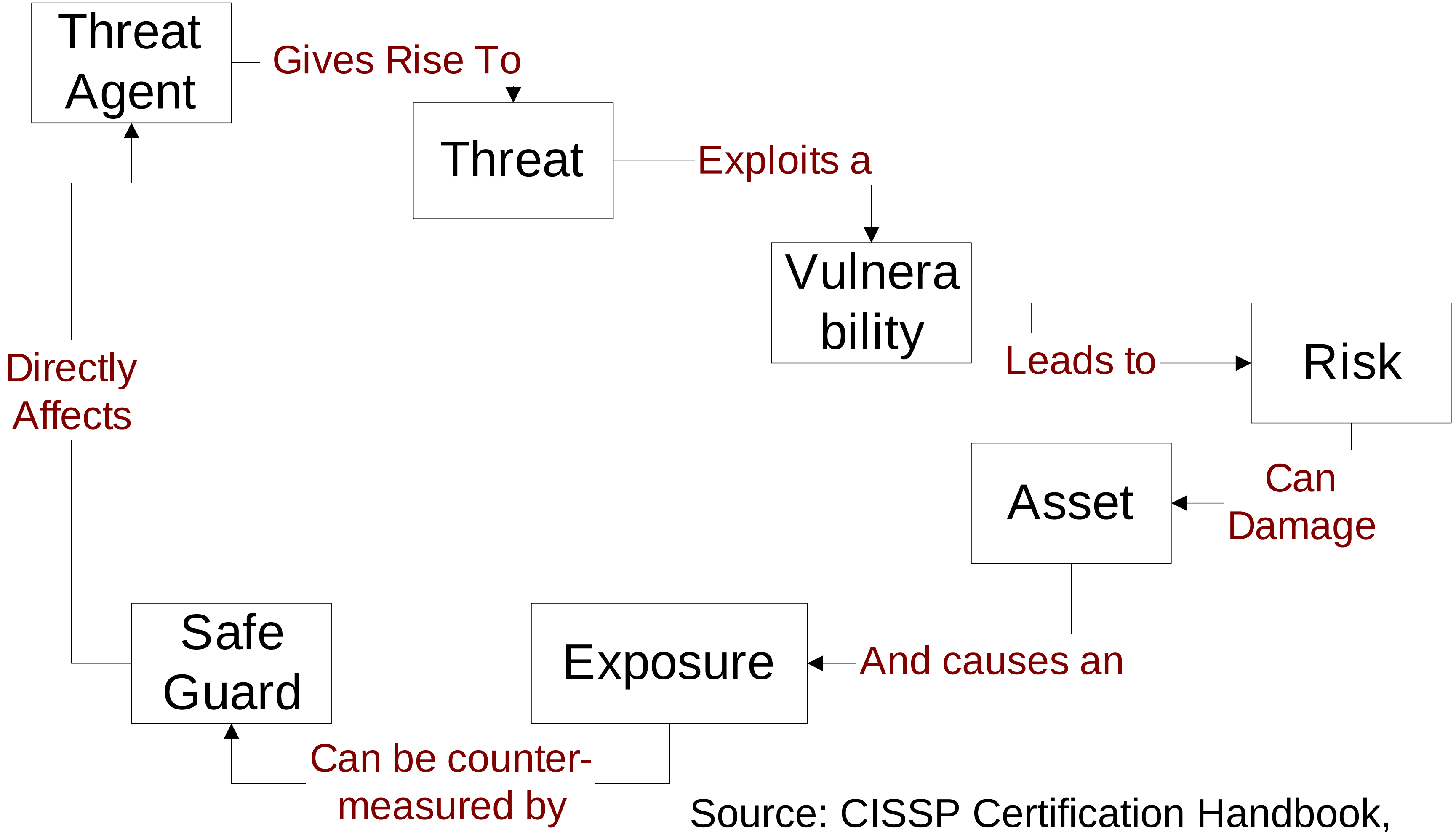
The Ten Immutable Laws

from Scott Culp from Microsoft Corp, (2/2)

- There really is someone out there trying to guess your passwords.
- **The most secure network is a well-administered one.**
- **The difficulty of defending a network is directly proportional to its complexity.**
- Security isn't about risk avoidance; it's about risk management.
- **Technology is not a panacea.**

Source: Microsoft Corporation; www.microsoft.com/security

Threat/Countermeasure Analysis Process



Threat Agent

Gives Rise To

Threat

Exploits a

Vulnerability

Leads to

Risk

Can Damage

Asset

And causes an

Exposure

Can be counter-measured by

Safe Guard

Directly Affects

Source: CISSP Certification Handbook, Shon Harris, © 2002 & US DoD Common Criteria

Statistics (2001/2002)

- Nearly 50% of all network attacks come from the inside. Source: CSI/FBI/Ernst and Young)
- Over a 12-month period, businesses los nearly $1.6 trillion in revenue due to unplanned downtime caused by security related incidents (Source: InformationWeek.com online, mid 2001)
- Klez-H is the worst virus ever, according to figures from managed services firm MessageLabs, which has blocked 775,000 (4/15) – 1 in 300 messages are infected (Source: the Register online, June 2002)

2001 Highlights

- SANS organization hacked in July 2001
- An IT manager of a major airline found out, only after being hacked, that his security consultants version of managed security was browsing his Web site every 15 minutes to make sure it was still operational.

Access Control

Access Control Systems & Methodology – the mechanisms that systems managers can use to influence the system's behavior.

Access Control

- IAAA
  - Identification: who are you?
  - Authorization: what can you do?
  - Authentication: O.K., prove who you are.
  - Accountability: I know what you did … maybe?
  - Techniques, technologies
- Monitoring and Auditing
- Methods
  - Administrative
  - Physical
  - Technical
  - Layers

Common Authentication Methods in use Today

- Anonymous access – any ole' Joe
- Authenticated access – various levels
  - Basic (cleartext password)
  - Digest authentication
  - Integrated Windows authentication (NTLM)
  - Kerberos – mutual auth
  - Certificate – PKI based
  - RAS – PAP, CHAP, MSCHAP, ...
  - Hardware Based (SecureID)

Security And Auditing Practical Examples

- Web Server log files
  - IIS log files in IIS, W3C format or ODBC
- Windows event logging
  - Application, Security, System, ADS, DNS
  - Most features must be enabled
- Logging does not affect performance

  (under normal conditions)
- Benefits of logging and auditing
  - Intruder Detection; Permissions abuse
  - Problem Resolution
  - Detect Misconfiiguration

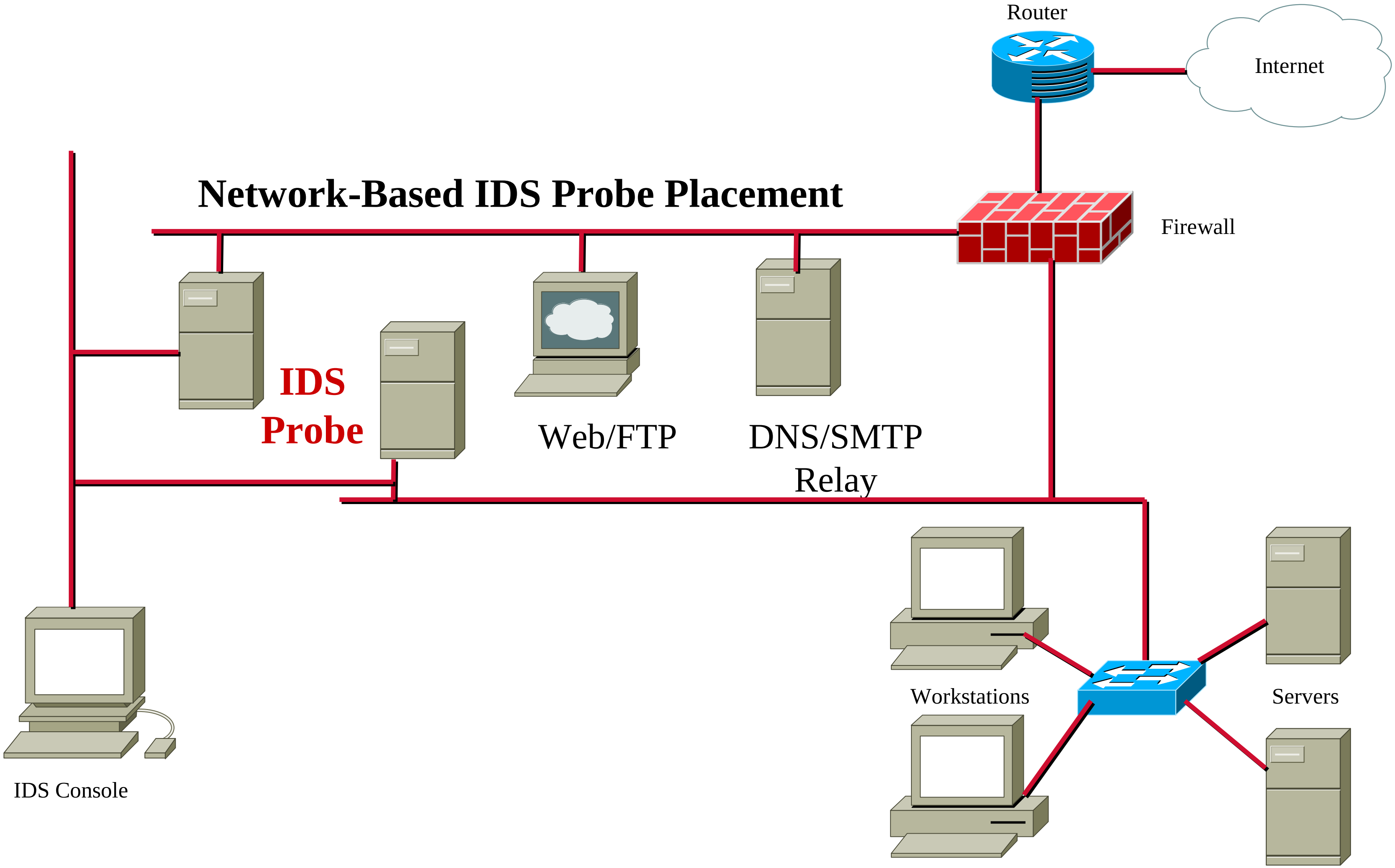
What is an IDS?

- An intrusion detection system monitors computer systems and networks, looking for signs of intrusion (unauthorized access) or misuse (authorized users).

Types of IDS

- **Host-based** - detection agents collect information reflecting the activity that occurs on a particular system
  - Example: BlackICE Defender or Microsoft ISA Server 2000's specialized filters
- **Network-based** - collects information from the network itself through sniffing on the LAN / WAN

Example IDS Diagram



Host-Based IDS

- Advantages
  - Can map problem activities to a specific user
  - Can operate in encrypted network environments
  - Can track behavioral changes
  - Can operate in switched network environments
  - Verifies the success or failure of an attack

Host-Based IDS

- Disadvantages
  - Cannot monitor network activity
  - May cause performance degradation of monitored system
  - Agents are more platform-specific, which adds to the deployment costs

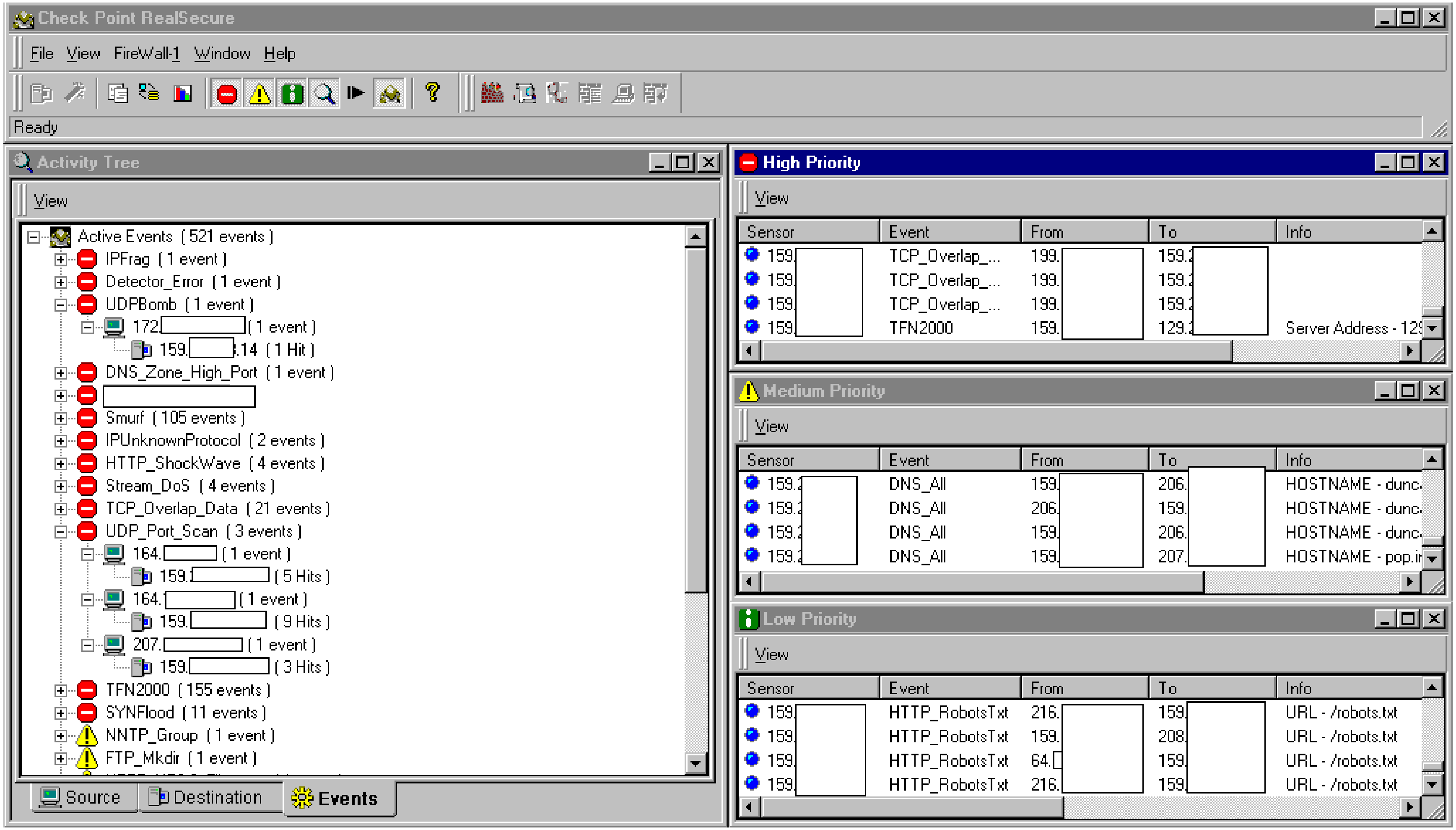
Network-Based IDS

- Advantages
  - Can detect and monitor network attacks (i.e. packet storm attacks and SYN floods)
  - Does not require logging or auditing to be enabled
  - Are not Operating System specific by their very nature

Network-Based IDS

- Disadvantages
  - Can show what is happening on a network, but cannot tell the outcome of commands executed on a host
  - Cannot be used on encrypted networks
  - Can be difficult to implement in modern switched networks
  - Cannot keep up with today's high speed networks

Network-Based IDS



```
Active Events ( 521 events )
  IPFrag ( 1 event )
  Detector_Error ( 1 event )
  UDPBomb ( 1 event )
    172.[redacted] ( 1 event )
      159.[redacted].14 ( 1 Hit )
  DNS_Zone_High_Port ( 1 event )
  [redacted]
  Smurf ( 105 events )
  IPUnknownProtocol ( 2 events )
  HTTP_ShockWave ( 4 events )
  Stream_DoS ( 4 events )
  TCP_Overlap_Data ( 21 events )
  UDP_Port_Scan ( 3 events )
    164.[redacted] ( 1 event )
      159.[redacted] ( 5 Hits )
    164.[redacted] ( 1 event )
      159.[redacted] ( 9 Hits )
    207.[redacted] ( 1 event )
      159.[redacted] ( 3 Hits )
  TFN2000 ( 155 events )
  SYNFlood ( 11 events )
  NNTP_Group ( 1 event )
  FTP_Mkdir ( 1 event )
```

Source | Destination | Events

High Priority

Sensor	Event	From	To	Info
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TFN2000	159.[redacted]	129.2[redacted]	Server Address - 12

Medium Priority

Sensor	Event	From	To	Info
159.2[redacted]	DNS_All	159.[redacted]	206.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	206.[redacted]	159.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	159.[redacted]	206.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	159.[redacted]	207.[redacted]	HOSTNAME - pop.i

Low Priority

Sensor	Event	From	To	Info
159.[redacted]	HTTP_RobotsTxt	216.[redacted]	159.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	159.[redacted]	208.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	64.[redacted]	159.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	216.[redacted]	159.[redacted]	URL - /robots.txt

Source: This image is an example of a production network using RealSecure.

Remote Control / Access Practical Thoughts

- Prevent remote control to critical resources where possible
- User a different password for remote control when possible
- Enable security audit logging for success and failures
- Dial in authentication code independent of userid

Application and System Development

Applications & Systems Development – controls within software itself to ensure the application is used properly.

Application and System Development

- How many software developers start with Security in mind?
  ICCM 2002 – 2 people in 60 raised hands.
- Device or Software security?
- RDBMS issues – Views, Stored procedures
- Application risks and mitigation
  - COM/DCOM
  - Java and Applets

Secure Applications

- ◆Building secure Web apps is very difficult
  - Complex technologies
  - Difficult to implement
  - Difficult to hide complexity from users
  - Often “pasted” on after the fact
  - Lack of skills in the market
- ◆Building secure Web apps means
  - Analyzing your threats
  - Designing a system to cope with the threats
  - Choosing the technologies
  - Finally, building the system

Examples of Common Exploits

- Web server attacks
- CGI scripts
- Web browser attacks
- SMTP attacks
- IP Spoofing
- Buffer Overflows
- Default passwords

Network Backdoors

- Modems – The most overlooked and used network entry point
- Telecommuters - (DSL, cable modems)
  - Split Tunneling is a specific concern.
  - Example: CheckPoint VPN1 only encrypts traffic to protected network hosts

Cryptography

Cryptography – data encryption and digital signatures which are required to support nonrepudiation.

Cryptography

- Secure messaging with digital certificates
  - Example: Verisign™, Thawte™ Web of Trust™
- Secure file system – Win2K EFS
  - Dangerous on a Win2K Pro PC unless you take steps to protect the recovery agent
- SSL on web servers – Server Cert’s
- Hardware based encryption devices
  - GemPlus™, Schlumberger™, Aladdin™ USB
  - Certificate's Private key is stored in H.W. and protected with a PIN
  - Microsoft – CryptoAPI and PCSC
  - Linux/Unix – Serial PCSC only devices

Disaster Recovery and Business Continuity

Business Continuity Planning (Disaster Recovery Planning) – how the business will respond from interruption of service.

DRP and BCP

- What is your DRP/BCP/HA play? Backup tape? Warm site? Prayer?
- DRP – everything from a failed disk to the data center burning down – oh, and the servers melted after the lightning storm.
- BCP – keeping things afloat while you restore.

Law, Investigation, and Ethics

Having a response that will
stand up in court
(criminal or civil).

Law, Investigation and Ethics

Your speaker is NOT a lawyer and this slide is not meant to replace proper legal advice.

- Its all about the evidence….
  - Criminal – Method, Opportunity, Means must by shown by prosecution
  - Civil – 51% needs to show "guilt"
- Investigation Process/Issues
  - Based on established company policies
  - Produce and catalog evidence as if you were sworn law enforcement – document, bag, serialize, etc.
  - Computer records must be part of "everyday business" to be admissible

Operations Security

Operations Security – controls over the environment of the system, or what to do after everything is installed.

Operations Security

- What are you doing on a day to day basis?
- Accountability – checks and balances
- Hacking and Attacking – can you detect attempts to breach your systems?
- Anti Virus
- Policies – technical and administrative

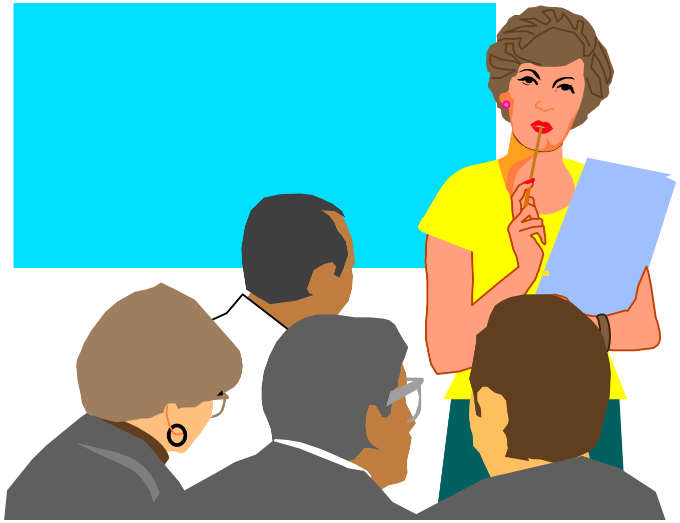
Virus Issues

- They will keep coming.
- Numerous delivery methods
  - Media, email, files, macros, browser controls, ...
- Higher degree of "being connected" increases the threat plane

- Costs:
  - Initial software
  - Deployment
  - Maintenance
  - False alarms
- Cost of nonconformance:
  - Productivity loss
  - System downtime
  - Damage (many forms)
  - Public image
  - Others may not communicate if you keep infecting them

Spreading The Word

- How do you get security information to your employees?
  - Awareness programs
  - Distribute translated excerpts from main security policy
  - New employee orientation.
  - Webcast / Streaming



Security based Testing

- When to test
  - Changes in policy
  - Changes in staffing
  - Network architectural changes
  - System updates (software, firmware, hardware)
- How often?
  - DAILY – test or review something

Physical Security

Physical Security – threats, threat agents, vulnerabilities, and their countermeasures to a system.

Physical Security

- Lock it up!
- Secure tapes!
- Environmental issues
  - HVAC, Power
  - Fire detection/prevention
  - Facility access
- The perimeter may be larger than you think

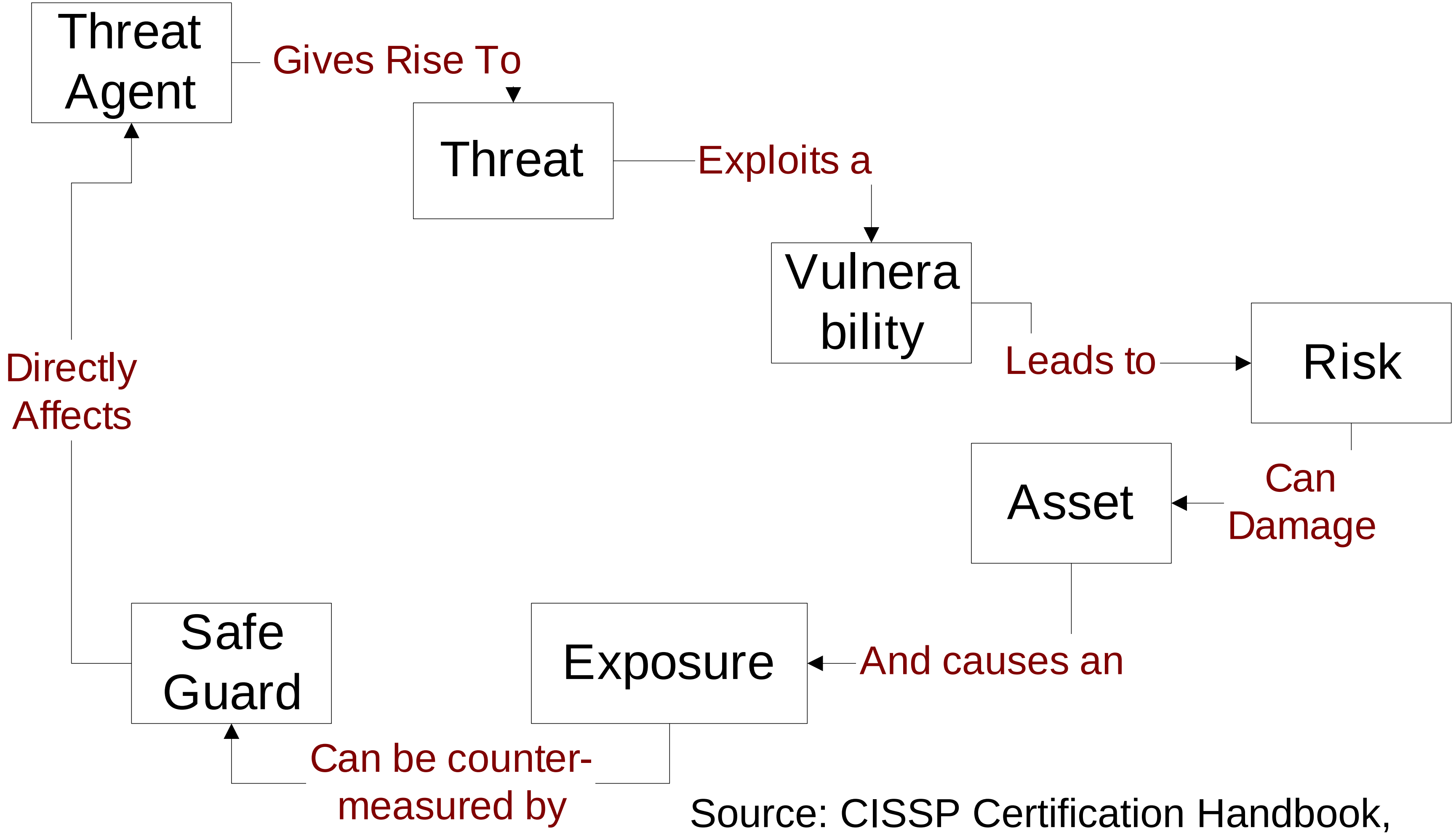
Security Management Practices

Security Management Practices – asset identification and policy implementation along with risk management and mitigation.

Security Management Practices

- CIA Triad
  - Confidential, Accessible, Integrity
- Risk Analysis
  - Asset Identification
  - Threat analysis and threat agent/contagion
  - End Goal: Does the cost of the mitigation outweigh the cost of the asset?
- Security Policies
- Layers of Responsibility

Have we seen this before? You bet!



Threat Agent

Gives Rise To

Threat

Exploits a

Vulnerability

Leads to

Risk

Can Damage

Asset

And causes an

Exposure

Can be counter-measured by

Safe Guard

Directly Affects

Source: CISSP Certification Handbook, Shon Harris, © 2002 & US DoD Common Criteria

Why Use A Policy?

- The function of a security policy is to preserve the availability, integrity, and confidentiality of information resources.
- Company's current and past activities become the *de facto* policy in the absence of an established policy.
- Policies guide how an investigation can be conducted.

Policy Content

Should establish the following:

- What – is protected?
- Who – is responsible?
- Where - within the company is the policy in effect?
- How – will compliance be monitored?
- When – does the policy take effect?

Successful Policies

- Clear up confusion, not generate new problems
- Have management support
- Written for a general audience (not “techies”)
- Available to everyone
- Your written policy will drive how you can investigate and respond to possible intrusion.

Internet Security Policy

- Authentication – what is required by your own servers
- Virus Detection – required on remote/local clients?
- Remote Access
- Intrusion Detection
- Appropriate Use of file transfer, web (HTTP, HTTPS) and Email

A Solid Security Policy Design

- Starts with good planning
- Most network security plans focus on Perimeter defense only or the firewall itself
- Better design includes perimeter, internal, and information conduits along with acceptable use semantics and language
- Are not overly long
- Communicate why as well as what

Security Models

- This topic is beyond the scope of today's talk.
- Suffice it to say that the most modern security model you can consult and use as a reference is the US DoD Common Criteria at www.commoncriteria.org.

Telecommunications and Network Security

Telecommunications, Network & Internet Security – the measures taken to safely transmit data “over the wire”.

Telecommunications and Network Security

- Common threats and countermeasures
- TCP/IP Protocols and their usage
- Firewall Configuration and management
- Security Tools

Common Threats and Countermeasure (CM)

Denial of Service (DoS/DDoS) Attacks –

CM: CIR, Stateful firewall system

IP Spoofing

CM: RFC 2827 and RFC 1918 filtering and egress routing configured.

Unauthorized Access

CM: ACL for protocol and users

Trust Exploitation – CM: Private VLANs.

Application Layer Attacks –

CM: OS, devices and applications kept up to date with latest security fixes & Host Intrusion Detection System (HIDS).

More Attacks

- SMURF – collusion based ICMP ECHO‘s send to multiple systems via amplifying network
  - CM: Control ICMP traffic at the border/edge
- Fraggle – like a SMURF, using UDP
  - CM: Control inbound UDP traffic
- SYN – attacker sends spoofed SYNch packets – attacker won’t get the SYN/ACK
  - CM: modify connection timeout, increase TCP port size

Firewall! Good Enough?

- Firewalls cannot protect against inside attacks

  (Most loss due to computer security incidents is caused by insider abuse)
- Various firewalls are subject to a variety of well-known port attacks with frequent updates
- Firewalls do not protect against attacks that bypass it (i.e. tunneling or application based attacks)

Types of Firewalls?

- Personal Firewall products (sub $100)
  - ZoneAlarm
  - Ontrack SystemSuite
  - BlackICE Defender
  - Norton Internet Security / Personal Firewall
- Firewall Appliances
  - Cisco Secure PIX Firewall, Nokia Firewall, SonicWall, Linksys cable/DSL
- OS server based
  - Microsoft ISA Server
  - Check Point FireWall-1
  - Linux based systems

Firewall Certification

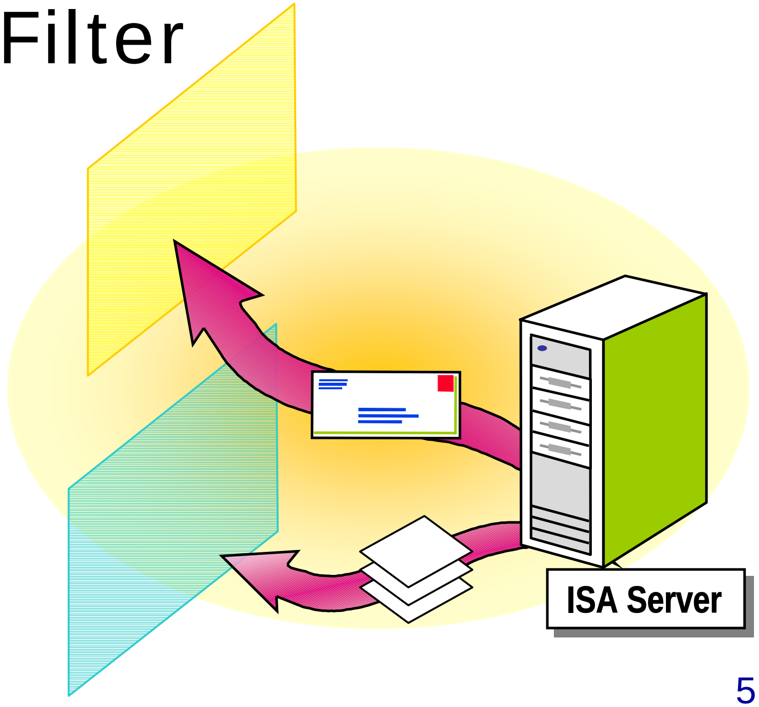
- “At ICSA Labs, we direct a certification program aimed at testing the security of commercially available firewall products.”
  - ICSA Certification means that the product is installed AND configured correctly
- Check out those products that have the distinction of being ICSA Certified Firewall Products at:*www.icsalabs.com/html/communities/firewalls/certification/vendors/index.shtml*

Microsoft Internet Security and Acceleration (ISA) Server

- Builds on Windows 2000 security & Active Directory
- Combines firewall and Web cache functions
- Integrated Virtual Private Networking (VPN)
- Integrated Intrusion Detection and filters

ISA Drill Down
Application Filter Overview

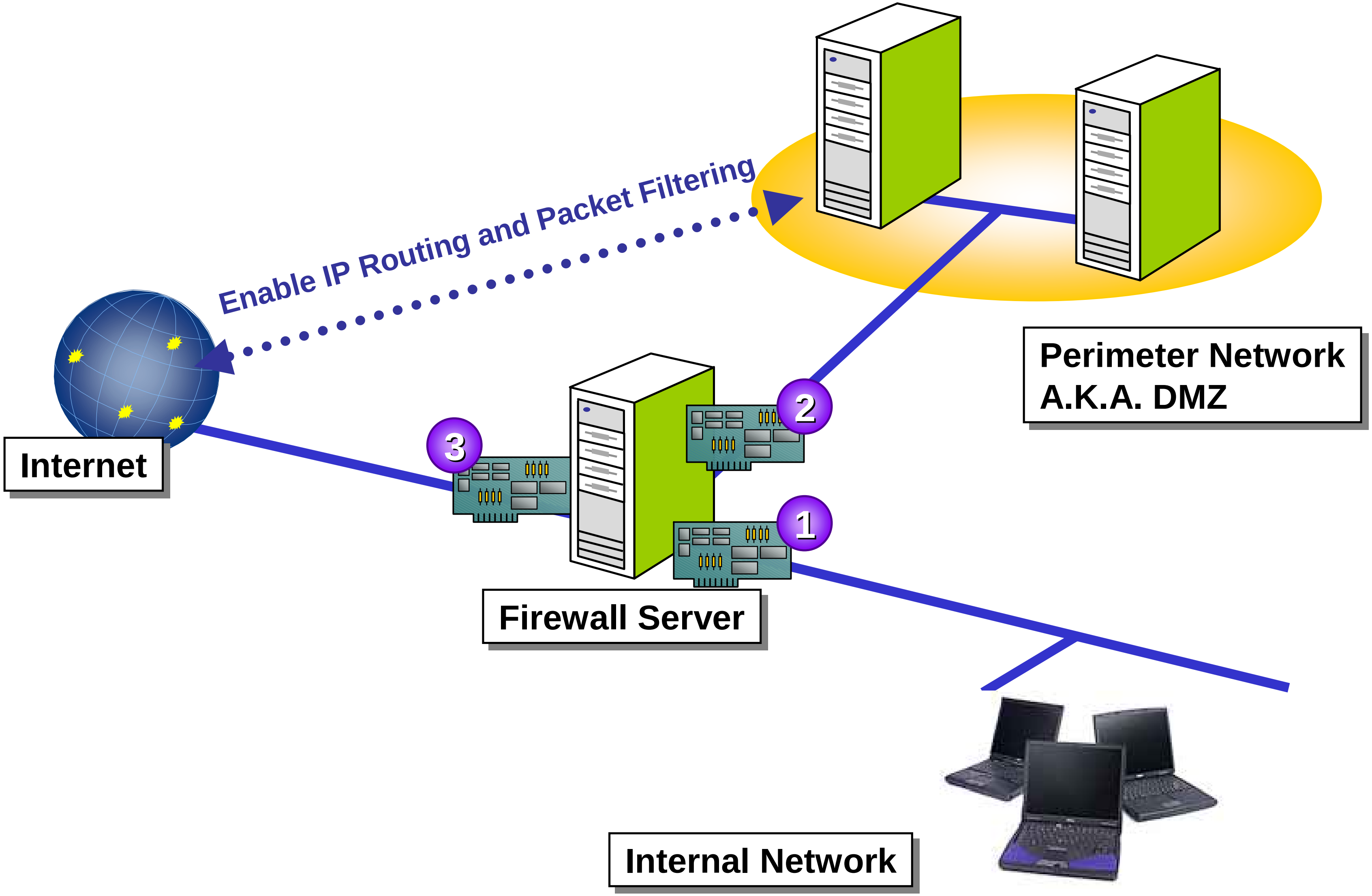
- DNS Intrusion Detection Filter
- FTP Access Filter
- H.323 Filter
- HTTP Redirector Filter
- POP Intrusion Detection Filter
- RPC Filter
- SMTP Filter
- SOCKS V4 Filter
- Streaming Media Filter



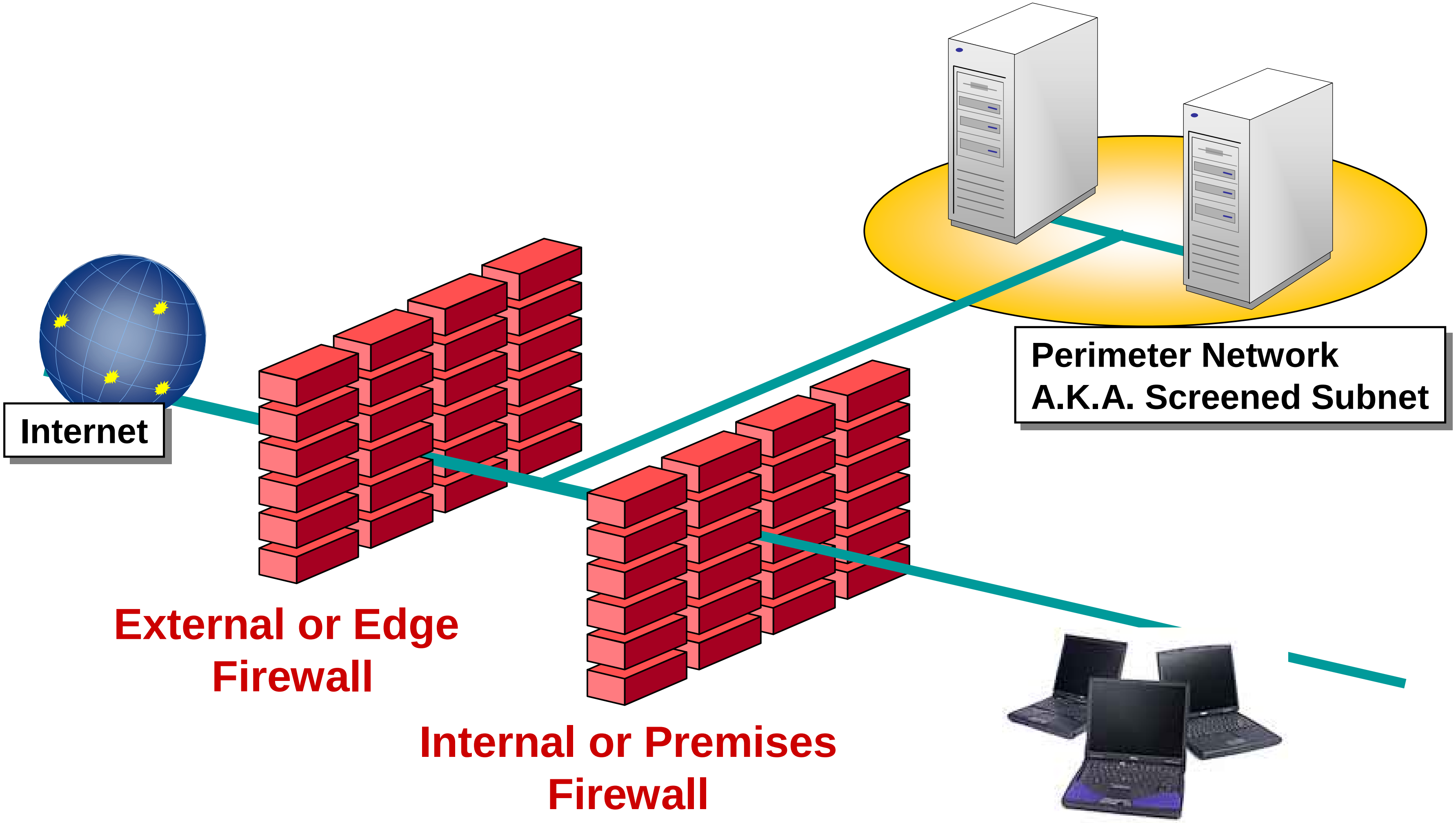
General Firewall Features you should look for or build into your systems

- Network Configuration
  - Inside, Outside, Perimeter, Traffic flow is controlled
- Security Policy Rule Base
  - Zones
  - Time of day
  - Content management, allowed content
- Network Address Translation (NAT)
- Virtual private networks (VPNs)
  - PPTP
  - L2TP/IPSec

Three-Homed Perimeter Network



Perimeter Network with Back-to-Back Firewalls



Internet

Perimeter Network
A.K.A. Screened Subnet

External or Edge
Firewall

Internal or Premises
Firewall

Common Best Practices

- Stay Informed About Security Issues
- Install the Latest Service Pack and Security Updates
- Do Not Run Unnecessary Services or Accept Unnecessary Packets
- Audit Security-Related Events and Review the Associated Log Files
- Document All Aspects of Your Network Configuration and discuss it with few
- Understand the Network Protocols that You Use inside and outside your network – what is acceptable based on service, capability, protocol
- Maintain Physical Security

Security Tools

- Security scanners
  - Windows: Security configuration toolkit or MMC snap in
- "Honey Pots" – as described in Cheswick
- Port Scanners
  - NMap for Linux, nessus (nessus.org)
- Intrusion Detection Systems
- Firewalls
- Scan sites HackerWhacker.com

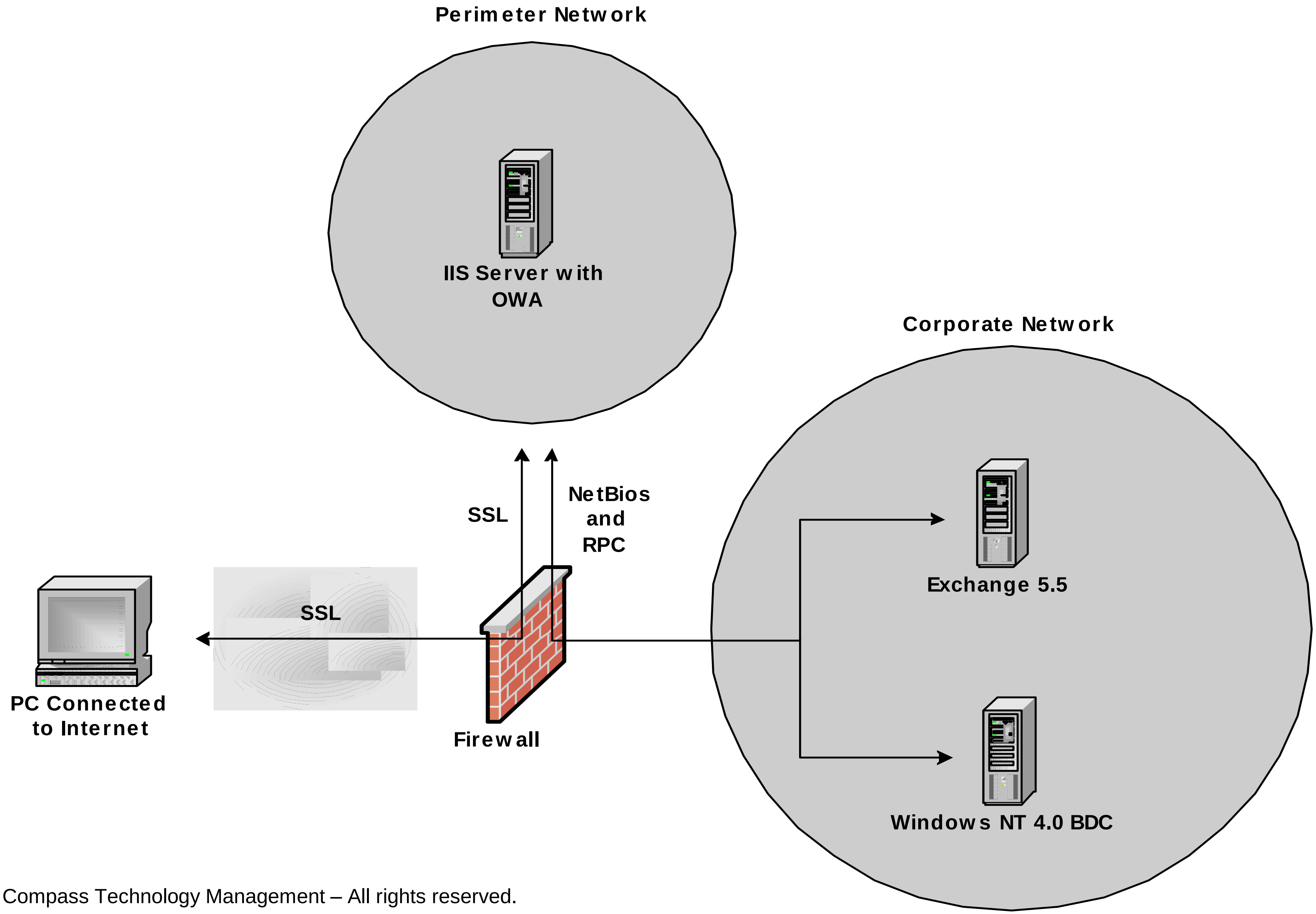
Configuring Email systems

- Messaging and message system availability behind firewall systems
- Middle perimeter / screened subnet system allows access through the firewall for an authenticated user.

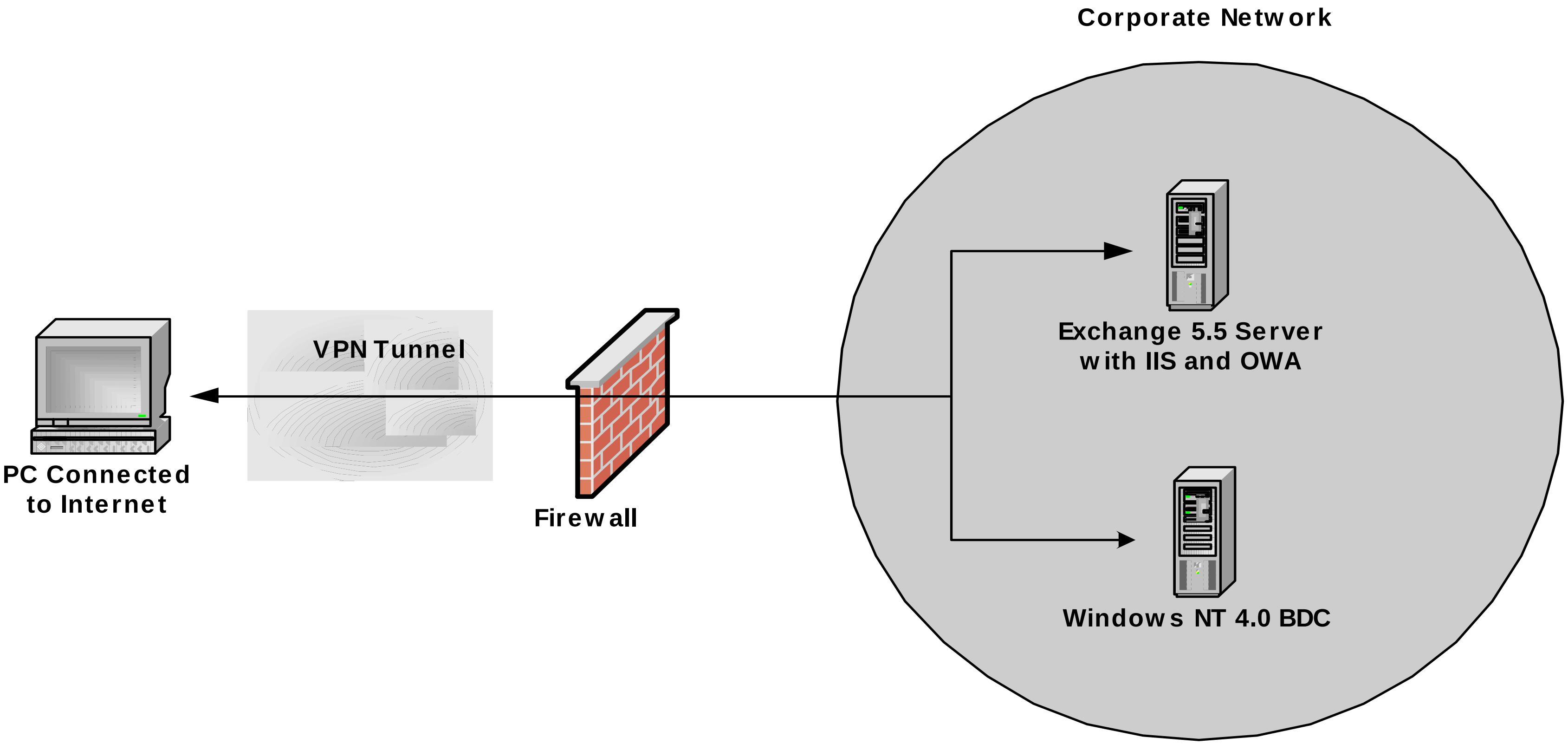
Microsoft Exchange OWA

- OWA - Microsoft Web based Collaboration solution
- Secure access through Digital Certificates and SSL
- Secure access through a VPN tunnel
- Access Microsoft Exchange Server from non-Microsoft Systems

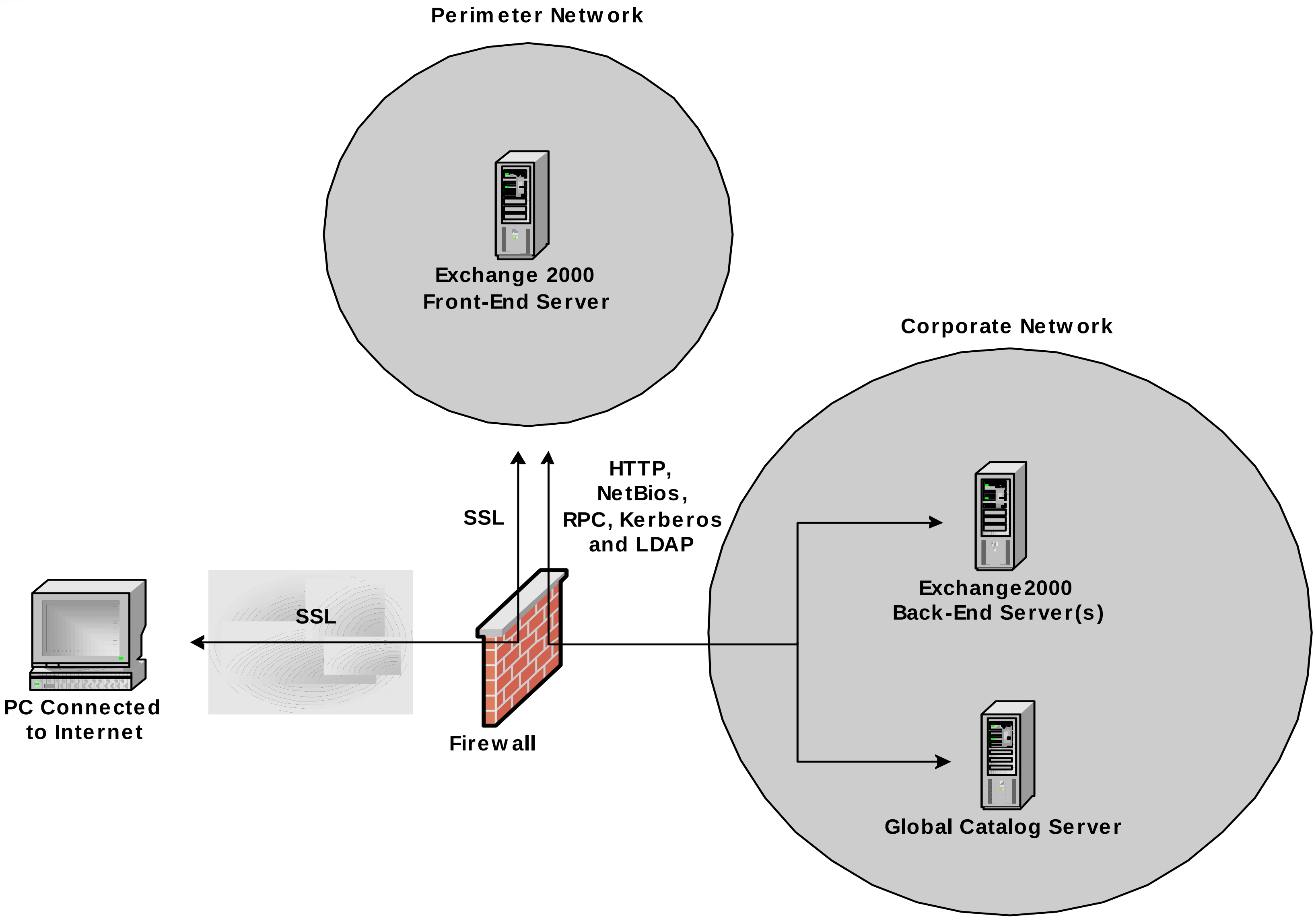
Exchange 5.5 OWA via SSL



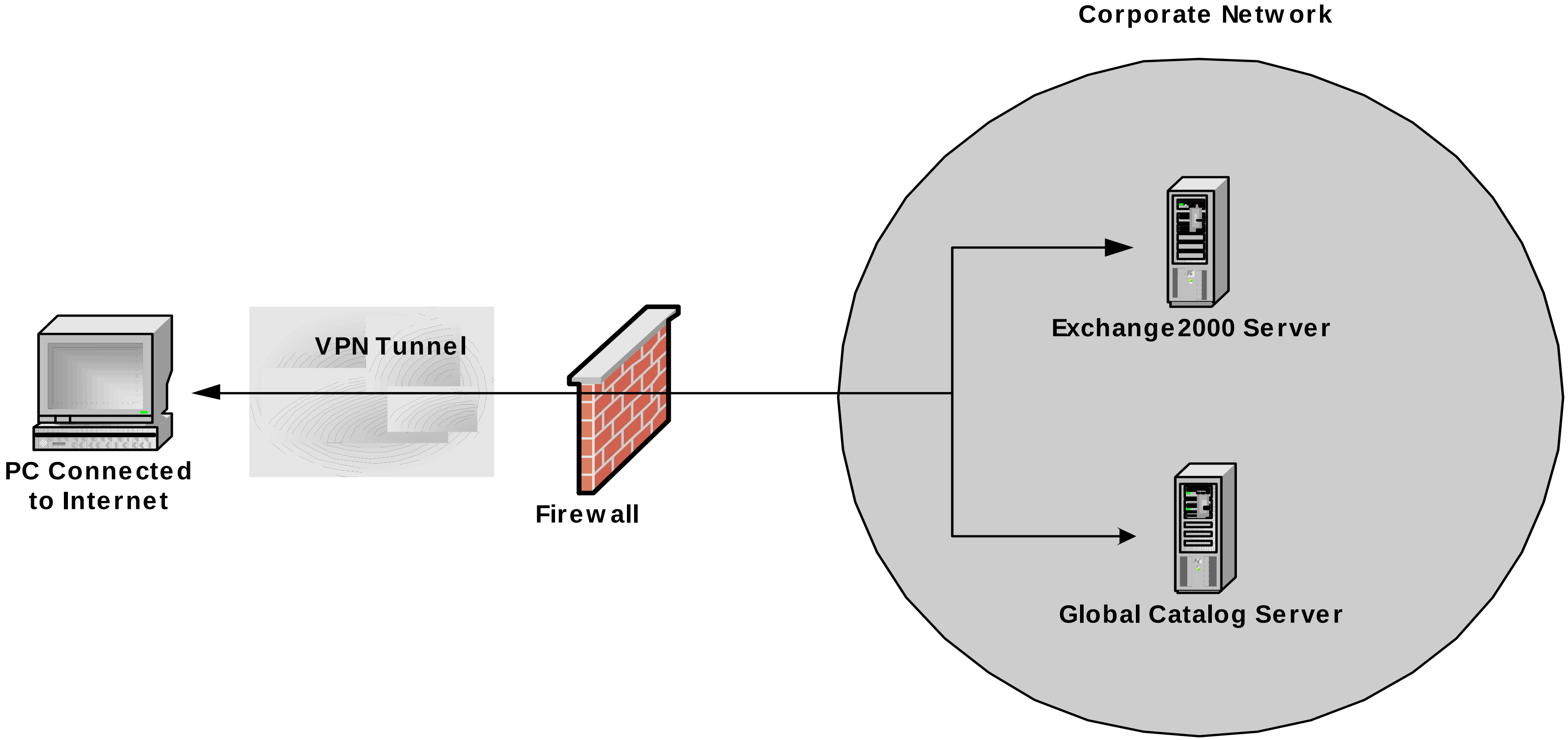
Exchange 5.5 OWA via VPN



Exchange 2000 OWA via SSL



Exchange 2000 OWA via VPN



TCP/IP Security

- Identify the protocols used
  - HTTP, FTP, NTP, SMTP, HTTPS, NetBIOS, H.323, Streaming, NNTP, POP3, ARP, RARP, SNMP, ….. To name a few.
- Verify the ports required by the protocols and the direction of travel
- TCP/IP security can applied via:
  - IP address and domain name restrictions
  - TCP/IP filtering
  - IP security policy snap in
  - Security configuration tool set

IIS 5/6 Authentication

- Anonymous Access
  - Public Web pages
- Basic Access
  - Username/Password cleartext
- Integrated NTLM authentication
- Digest
  - Strong security in a lightweight fashion
- Certificates
  - Code signing, E-commerce, user mapping

How secure are you?

- One way businesses can figure out their vulnerability is to hire a testing company to see how well their security security infrastructure is performing. Such testing uses a combination of software and "ethical hacking" to analyze a company's security.

Internet Reference Sites

- www.sans.org
- www.microsoft.com/security
- www.ntbugtraq.com
- xforce.iss.net
- project.honeynet.org

Microsoft Specific sites

- ISA: www.isaserver.org
- Refer to the TechNet Web site at www.Microsoft.Com/TechNet/
- Windows NT security (whitepapers, etc.)

  http://www.Microsoft.com/windows/server/Technical/security/default.asp

  Http://www.Microsoft.Com/windows/server/technical/security/pki.Asp

  Http://www.Microsoft.Com/windows/server/technical/security/pkiintro.Asp

Definitions

PKI	Public key infrastructure
Schannel	Secured channel
Ssl	Secure sockets layer
TLS	See SSL
Web DAV	Web digital audio video protocol
Web folders	Office 2000
NCSA	National center for supercomputing applications
W3c	World wide web consortium
LDAP	Light weight directory access protocol
Ca	Certificate authority
EFS	Encrypted file system
CN	Common name
CRL	Certificate revocation list
CSP	Cryptographic service provider
IPSEC	Internet protocol security
PPTP	Point to point tunneling protocol
L2tp	Layer 2 tunneling protocol