United States Army Signal Center and Fort Gordon
Leader College for Information Technology
School of Information Technology

Information Assurance Division

Network Manager Security Course

7 July, 2005

Table of Contents

Introduction and Orientation

Module 1

September 20, 2004 1-1

Lesson Objectives

- Course Information
- Meet the Instructor
- Course Objectives
- Course Ground Rules
- Student Introductions
- Course Outline

September 20, 2004 1-1

Course Information

- Title
  - System Administrator / Network Manager Security Course, course number 7E-F66/531-F21 (CT)
- Location
  - Office: Information Assurance, Room 205, Cobb Hall, Building 25801, Fort Gordon, GA 30905
  - Phone: (706) 791-5137/5179, DSN 780, Fax 791-6161
  - Email Address: ia@gordon.army.mil
  - Web site: http://ia.gordon.army.mil
- Telephone
  - Military phones: To dial out from the military phones, dial "9" for local and 800 numbers. To dial DSN, dial "8". No phones can dial long distance.
  - Other numbers: TSACS 791-4291, 1-800-632-0196

September 20, 2004 1-1

Your Staff

Mr. Randy McNeil – Chief, IA Training

Instructors

Mr. Larry McLean (NMS) Mr. Jeff Hobday (SAS)
Mr. Kelly Larsen (SAS) Ms. Sue Clark (NMS)
Ms. Cynthia Jones (SAS) SFC LaBranche (NMS)
SFC Jedrusiejko (SAS) Mr.Tony Braddix (SAS)

Webmaster

Mr. Rodney Driggers

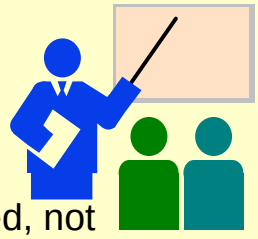
February 17, 2005 1-1

Course Objective

- Week 1
  - To train DOD personnel to recognize vulnerabilities and defeat potential threats within the computer system; identify and repair common Windows 2K and UNIX operating system weaknesses and identify approved free security-based software
- Week 2
  - To train DOD personnel to recognize vulnerabilities and defeat potential threats within the network; operate and maintain firewalls using routers and bastion hosts and a simple web server Microsoft Internet Information Server (IIS)

September 20, 2004 1-1

Ground Rules



- Course materials are yours
- Ask questions any time
- Respect opinions of others
- Products mentioned or demonstrated, not endorsed
- Logistics and break schedule (smoking area, class hours, restrooms, phones & messages)
- Do not hack your fellow students!!!
- Cell phones are prohibited in class

September 20, 2004 1-1

Student Introductions

- Name
- Where you work; unit & location
- What you do; not just the job title
- What you expect to learn
- What is your computer background

September 20, 2004 1-1

Course Outline

- Day 1
  - Introduction
  - STAT Scanner and IAVA discussion
  - Begin W2K Security Check List

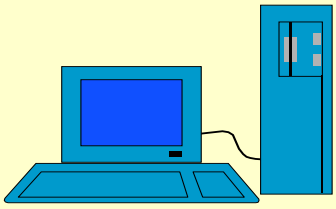
September 20, 2004 1-1

Course Outline

- Day 2
  - Continue with W2K Security Check List and Lab Work
- Day 3
  - Continue with W2K Security Check List and Lab Work
  - Begin Unix Security Check List and Lab Work
- Day 4
  - Continue with Unix Security Check List and Lab Work

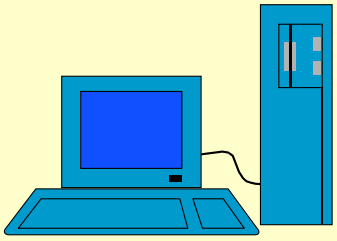
Course Outline

- Day 5
  - Finish Unix Security Check List and Lab Work
  - Exam (50 multiple choice questions, 1 hour, closed book/notes, 80% to certify)



Course Outline

- Day 6
  - Network Vulnerabilities / Reporting
  - Hackers
- Day 7
  - Encryption / Cryptography
  - Web Server Vulnerabilities



February 17, 2005 1-1

Course Outline

- Day 8
  - Router Security
- Day 9
  - Firewall Security
- Day 10
  - Intrusion Detection Systems
  - Exam (50 multiple choice questions, 1 hour, closed book/notes, 80% to certify)

September 20, 2004 1-1

Incident and Vulnerability Reporting

Module 04

Lesson Objectives

- Identify information system related incidents and vulnerabilities
- Describe how to detect and report incidents and vulnerabilities

Incidents and Violations

- Incident - Unexpected behavior by an information system that yields abnormal results or indicates unauthorized use or access, unexplained outages, denial of service, loss of accountability, or the presence of a virus

Incidents and Violations

- Technical Vulnerability - A hardware, firmware, communication, or software weakness which leaves a computer processing system open for potential exploitation or damage, either externally or internally.

TOP 20 Security Vulnerabilities Windows #1

- Internet Information Service:
  1. Failure to handle unexpected requests.
  2. Buffer Overflows
  3. Sample Applications

September 20, 2004 4-1

TOP 20 Security Vulnerabilities Windows #2

- Workstation Service:
  1. Users access to files and printers.
  2. DCE/RPC calls directly over a UDP/TCP port >1024.
  3. Buffer overflow.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #3

- Windows Remote Access Services:
  1. Anonymous Logons.
  2. RPC/ Remote registry.
  3. Netbios thru file sharing

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #4

- Microsoft SQL Server (MSSQL):
  1. Exposed by MSSQL & Spida Worms.
  2. Remote leaking of information.
  3. Ports 1433/1434 scanned.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #5

- Windows Authentication:
  1. Weak or non existent passwords.
  2. User's fail to protect them.
  3. Hashing algorithm known or easily accessible.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #6

- Web Browsers:
  1. Numerous IE vulnerabilities.
  2. Active X & active scripting vulnerability
  3. IE integrated into Operating System

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #7

- File sharing Applications
  1. Technical vulnerability.
  2. Social vulnerability
  3. Legal vulnerability.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #8

- LSAS Exposures:
  1. Buffer overflow
  2. Remote exploit
  3. W.32 Sasser & W.32 Korgo Worms

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #9

- Mail Client:
  1. Email virus & attachments.
  2. Spam
  3. Web beaconing.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Windows #10

- Instant Messaging:
  1. File sharing vulnerability
  2. Remote exploits
  3. Active X controls vulnerabilities.

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Unix #1

- The Berkeley Internet Name Domain (BIND) Domain Name System (DNS):
  1. Most widely used DNS system on the internet.
  2. Vendor is quick to supply security fixes.
  3. Outdated and misconfigured servers still exist everywhere.

September 20, 2004 4-1

TOP 20 Security Vulnerabilities Unix #2

- Web Server:
  1. Default or unpatched configurations.
  2. Apache chunk handling exploit
  3. No web server can be considered secure until considered in the context of it's interaction with web applications

February 17, 2005 4-1

TOP 20 Security Vulnerabilities Unix #3

- Authentication:
  1. Same issues as General Windows Authentication.

February 18, 2005 4-1

TOP 20 Security Vulnerabilities Unix #4

- Version Control Systems:
  1. Buffer overflow.
  2. Unpatched or outdated versions
  3. Executing of arbitrary code

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #5

- Mail Transport Service:
  1. Abuse of mail relay options.
  2. Unpatched mail systems
  3. Sendmail and mail clients.

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #6

- Simple Network Management Protocol (SNMP):
  1. Default community strings
  2. Earlier versions using unencrypted strings
  3. Handling of trap and message requests

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #7

- Open Secure Sockets Layer (SSL):
  1. Integration into applications.
  2. Multiple vulnerabilites found in it's Library.
  3. Exploitation yielding root priviledges

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #8

- Misconfiguration of Enterprise Services NIS/NFS:
  1. Allow access to the NIS and NFS servers only from authorized clients .
  2. buffer overflows, DoS and weak authentication .
  3. Poor host-authentication services.

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #9

- Databases
  1. Modern databases are port addressable .
  2. Complexity makes them difficult to configure and secure .
  3. Linking with web applications.

February 22, 2005 4-1

TOP 20 Security Vulnerabilities Unix #10

- Kernel:
  1. Remote exploits.
  2. Denial of service attacks.
  3. Improper configurations.

February 22, 2005 4-1

Incidents and Violations

- Violation - Failure to comply with the policies and procedures established which could reasonably result in the loss or compromise of classified information

Examples of Security Violations

- Removal of classified information
- Wrongful disclosure of classified information
- Introduction of high risk software
- Introduction of malicious code
- Sharing passwords

Indicators of a Reportable Incident

- Suspected intrusions
- Unauthorized access attempts
  - System or system resources
- Unexplained file modifications
- Unexplained output

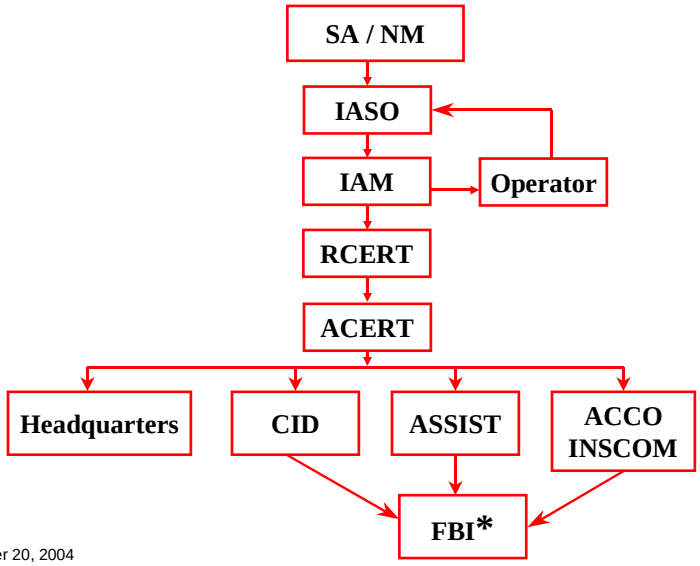
September 20, 2004 4-1

Indicators of a Reportable Incident

- Security system failures
- Abnormal system responses
- Malicious software
- Network intrusion alerts
- Anything “alarming”

September 20, 2004 4-1

Army Reporting Structure



The Security Incident Report

- Report incident to IASO
  - Information system name and/or number
  - Location
  - Date and time
  - Description
  - Impact
  - Any pertinent information
- IASO investigates and advises IAM

The Security Incident Report

- IAM advises community
- ACERT advises IAM and IASO
  - Further guidance
  - Further reporting requirements
- Vulnerability assistance

Summary

- The Army has a clear incident reporting chain of command
- Roles and responsibilities are established for your support
  - IASOs, IAMs, LIWA
- Incidents are to be reported
  - Contact Your IASO Immediately

Network Security Threats and the Hacker

Threats

- Threat Definition
  - A circumstance or event that could exploit or cause harm by violating security
- Threat Assessment
  - Consider the likelihood and possible impact of the threat
- Threat Objectives
  - Information Leakage – Viruses
  - Integrity Violation – Illegitimate Use
  - Denial of Service

5-1

Threat Methods

- Masquerading, forging, or spoofing
- Playback or replay
- Bypassing security controls
- Authorization violations or misuse of authority
- Network Attacks:
  - Smurf
  - Teardrop
  - Zombie
  - Land
  - Phishing
- Traffic analysis network scanning
- War dialing
- War driving
- Malicious code
- Back doors
- Media scavenging
- Dumpster diving
- Social engineering

5-1

Internal vs. External Threats

- Internal (Insider) Threats
  - Systems administrator, network manager, system operator, programmer, or user
  - Potential reasons
    - Fired or disgruntled
    - Coerced, greedy or financially strapped
    - Lazy or untrained
    - For the thrill or challenge
- External (Outsider) Threats
  - Foreign intelligence agent, terrorist, criminal, intruder……HACKER!!!

5-1

Pre-Hacking

- Footprinting
- Scanning
- Enumeration

5-1

Footprinting

The act of creating a profile of your target.

This profile includes the technologies used by your target.

5-1

Technologies sought out in Footprinting

- Internet
- Intranet
- Remote Access
- Extranet

(A Hacker Needs A Way In)

5-1

Internet

- Domain Names
- Static IP's
- TCP & UDP Services Running
- System Architecture (SPARC/X86)
- Firewall and Router ACLs
- Intrusion Detection Systems
- User and Group Names

5-1

Intranet

- Networking Protocols in Use
- Internal Domain Names
- Internal Static IP's
- TCP & UDP Services Running
- System Architecture (SPARC/X86)
- Firewall and Router ACLs
- Intrusion Detection Systems (IDS)
- User and Group Names

5-1

Remote Access

- Analog/Digital Telephone Numbers
- Type of Remote System
- Authentication Mechanisms

5-1

Extranet

- Connection Origination and Destination
- Type of Connection
- Access control Mechanism

5-1

Footprint Summary

The ultimate goal when a hacker footprints is to gain the following type of information:

1. Employee Names & Phone Numbers
2. IP Address Ranges
3. DNS Servers
4. Mail Servers
5. Outline of the Software and Hardware used by the company

5-1

Scanning

After Footprinting it's time to take a look at the systems we gathered information about and see what is alive on them.

Tools Used

- Ping Sweeps (ICMP Queries)
- Port Scans
- Automated Discovery Tools

5-1

ICMP ECHO Scan Prevention

- There are 13 types of ICMP traffic
- At Minimal the Following Can Be Let In

1. ICMP ECHO-REPLY
2. HOST UNREACHABLE
3. TIME EXCEEDED

5-1

Why is ICMP a vulnerability?

- If you compromise a system you can back-door the operating system and tunnel data within an ICMP ECHO packet. A program most commonly used to do this is Loki.

5-1

ICMP Query Countermeasure

- Block ICMP type 17 = ADDRESS MASK
  Block ICMP type 13 = TIMESTAMP

- This will keep an intruder from gaining knowledge of the subnets being used.

  Example:
  Access-list 101 deny ICMP any any 13
  Access-list 101 deny ICMP any any 17

5-1

Port Scanning

- The process of connecting to TCP and UDP ports on a target system to determine which services are running.
- A running service may be a potential access point on the target.

5-1

Port Scanning Objectives

- Identifying both the TCP and UDP services running on the target system
- Identifying the type of operating system of the target system
- Identifying specific applications or versions of a particular service.

5-1

Port Scan Types

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- UDP scan

5-1

Port Scan Types

- TCP connect scan - Completes a full three-way handshake (SYN, SYN/ACK, and ACK) Easily detected.
- TCP SYN scan - Also called “half-open scanning” because a full TCP connection is not made. (SYN, SYN/ACK, RST/ACK)

5-1

Port Scan Types

- TCP FIN scan - Sends a FIN packet, this will get the target to send back a RST for all ports that are closed. Usually only works on UNIX machines.
- TCP Xmas Tree scan - This sends a FIN, URG, and PUSH packet to the target. This usually gets an NT system to speak. The system will send an RST for all closed ports

5-1

Port Scan Types

- TCP Null scan - This is supposed to turn off all flags, and get the system to send back an RST for all closed ports.
- UDP scan - These are usually unreliable. It sends a UDP packet to the target, if the target responds with an “ICMP port unreachable” this lets us know that the port is closed.

5-1

Port Scan Results

- A successful port scan will yield the following results:

1. Port# 21, 23, 80 etc...
2. State open/closed
3. Protocol TCP/UDP
4. Service Ftp, SMTP, Http, Finger etc...

5-1

Port Scan Countermeasures

- Intrusion Detection Systems
- Shut down all services that are not necessary.

5-1

Automated Discovery Tools

- Due to the many differences in IP stack implementations between different Vendors operating systems. It is virtually impossible to prevent detection of the operating system running in a Intranet environment. In a Internet environment the best protection is a good bodyguard (Firewall/Proxy).

5-1

Enumeration

- Enumeration involves active connections to systems.
- Is very risky from a Hacker Standpoint
- Enumerated information can be grouped into the following areas:

1. Network resources and shares
2. Users and groups
3. Applications and banners

5-1

Enumerating NT Domains

- Standard Net View Commands (Domains and Computer List)
- NT Resource (Hacking) Kit
  - Nltest (List PDC/BDC)
  - Rmtshare (Like Net View)
  - Srvcheck (Shares & Authorized Users)
  - Srvinfo (Lists Shares)

5-1

NT Domain Countermeasure

- Tough to countermeasure
- Service packs, security rollups, and hotfixes
- Apply your System Security Checklist.
- Audit your systems regularly
- Host Intrusion Detection. (Tripwire, Tiger, SARA, etc.)

5-1

Miscellaneous NT Enumeration

- Edump, Getmac, Netdom, Netviewx
  (Shows services bound to IP #s and Ports)
  (Shows MAC #'s)
  (Probe for RAS Service)

5-1

Countermeasure

- Filter TCP and UDP ports 135-139 at perimeter network access devices.

5-1

Username Enumeration

- Almost half of the puzzle!!!
- NBTSTAT
- sid2user - Good for getting Admin acct.
- user2sid
- Once SID is gained, can determine which is administrator account.
- These will work even if RestrictAnonymous is enabled

5-1

Username Countermeasures

- Block port 139 from all perimeter networks.
- Difficult to block internally.

5-1

Reading assignment 1

Subject: **Encryption, Signatures, Hashes, and Certificate Authorities**

Pages: 89-95, 115-161, 177-201 (Cryptography Decrypted)

(Complete before day 2)

1.  at services do digital signatures provide?

2.  ine Non-Repudiation:

3.  ne some of the differences between RSA and DSA.

4.  at other names are used for a hash?

5.  at is the purpose of using a hash?

6.  at assurances are provided by message digests?

7. Define them:

8.  ne 3 non-keyed digests and their sizes:

9.  at are the 2 major PKI frameworks?

10.  efly describe them:

11.  at is a Certificate Authority?

Cryptography/Encryption

Lesson Objectives

The objectives of this lesson is to:

- Introduce definitions and basic concepts of cryptography/encryption
- Understand how Conventional Encryption (Secret Key) works
- Understand Public Key Encryption
- Understand Hashing and Digital Signatures
- Understand Public Key Infrastructure (PKI)

After halftime, we will talk about what how encryption can secure your networks. We will discuss the following:

- Types of attacks on your network traffic
- Basic strategies for encrypting network traffic
- Key distribution
- Encryption standards and tools
- Email security in encryption

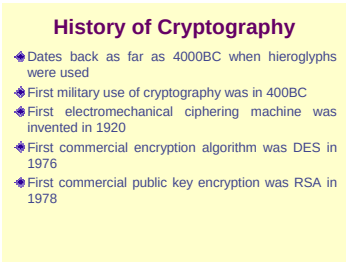
All these functions work together in the standard public key algorithms that are out there today. For example PGP uses all three functions to transfer a message. Since public key encryption uses secret keys for data transfer (normally) people need to understand that they are only as secure as their weakest key.

Governing and Investigative Authorities

U. S. Department of Commerce: Governing approval authority for all encryption methods, tools, and applications that can be used, sold, and downloaded in the U. S.

National Security Agency (NSA): Responsible for investigating, monitoring and decrypting traffic that could be of terrorist nature

History of Cryptography



Cryptography dates back as far as 4000BC when the Egyptians used hieroglyphs. They were not cryptography be themselves. They scrambled and transformed them into text, which were incorporated to hide their meaning.

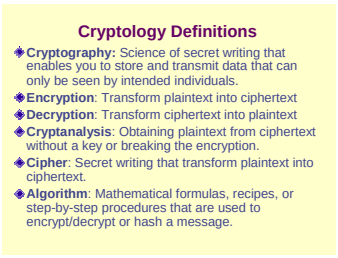
The first military use of cryptography was by the Spartans in 400BC. They invented what is called a scytale. To encrypt a message using a scytale, it was necessary to wrap a long length of parchment or papyrus around a cylindrical rod. The words of the secret message were written on the paper lengthwise along the rod, with one letter on each revolution of the strip. The strip was unrolled and removed, revealing a succession of meaningless letters. To decrypt this on the receiving end, they would need a cylinder exactly the same diameter that was used to encrypt.

In 1920, the first electromechanical ciphering machine was invented by Boris Hagelin. He called it the C-36, but in the United States, it's called a M-209. This led the way for the Germans during World War II to invent the Enigma machine and the Japanese to invent the purple code.

The first commercial symmetric encryption algorithm was invented in 1976 by IBM called Data Encryption Standard or DES. It was based on a cipher called Lucifer.

The first commercial public key or asymmetric encryption was invented in 1977 by Ronald Rivest, Adi Shmair, and Leonard Adlemen called RSA.

Cryptology Definitions



Some of the definitions that we will discuss in this lecture:

Cryptography – The science of secret writing that enables you to store and transmit data that can only be seen by intended individuals. The most popular techniques used today are Conventional (Secret Key), Public Key, and Digital Signatures/Certificates.

Encryption or Encipherment – The process of transforming plaintext into ciphertext.

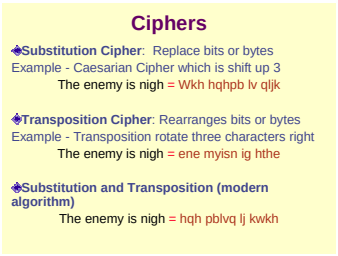
Decryption or Decipherment – The process of transforming ciphertext into plaintext.

Cryptanalysis – Obtaining plaintext into ciphertext without a key or breaking the encryption.

Cipher – Secret writing that transform plaintext into ciphertext.

Algorithm - They are mathematical formulas, recipes, or step-by-step procedures that are used to encrypt/decrypt or hash a message. Good examples of algorithms are DES (secret key), PGP (public key), SHA-1/MD-5 (hash).

Ciphers



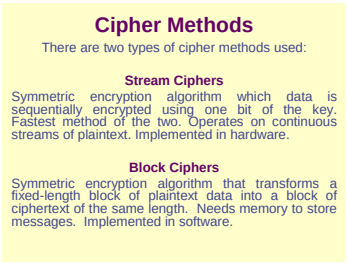
There are two fundamental types of ciphers:

Substitution ciphers replace one bit for one bit. Julius Caesar created the shift 3 to transfer messages out of Gaul back to Rome (remember we use the Roman Alphabet). He could use this simple formula because most people could not read nor could they read Latin. However this is a very easy formula to break.

Transposition ciphers shift characters around. Most modern algorithms like DES or Skipjack use rounds to shift the characters all over the place. The main advantage of transposition is that if you are one off from the real key you will not know it, because the words are scrambled. For example if in the substitution cipher you solved for t and h and e then you might be able to guess the second word is enemy, however with transposition this would not be true.

Ciphers can also combine both transposition and substitution processes, which is the more modern algorithm used today. The general process used to encrypt and decrypt data is inherent to the type of cipher used. One or more cryptographic keys are used to control the specific encryption or decryption process.

Cipher Methods

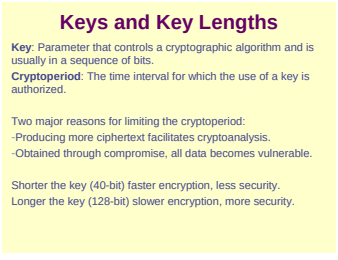


There are two types of ciphers:

Stream Ciphers: This is a type of symmetric encryption algorithm which data is sequentially encrypted using one bit of the key. This is the fastest method of encryption. Stream ciphers do not need any memory at all to operate. They operate on continuous streams of plaintext. Stream ciphers are usually implemented in hardware.

Block Ciphers: This type of symmetric encryption algorithm transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length. Block ciphers need memory to store messages. This makes is more suitably implemented in software to execute on general-purpose computers.

Keys and Key Lengths



Key: Parameter that controls a cryptographic algorithm. It is usually a sequence of bits.

Cryptoperiod: The time interval for which the use of a key is authorized.

There are two major reasons for limiting the cryptoperiod:

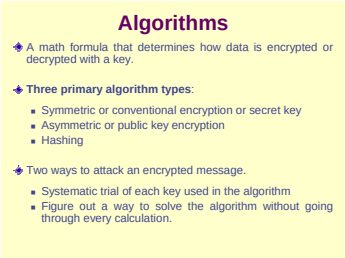
Producing more ciphertext facilitates cryptanalysis.

If a key is obtained through any means (compromised or through cryptanalysis), then all data encrypted with that key becomes vulnerable. The longer the key has been used, the greater the damage.

Shorter the key, for example a 40-bit key, will encrypt/decrypt your data faster, but will not give you satisfactory security of your data. A longer key, for example a 128-bit key, will encrypt/decrypt your data

slower, but will give your data the optimum of security it needs so that it cannot be broken by an unauthorized entity.

Algorithms



Basically, algorithms are formulas that determine how data is encrypted with a key.

The three primary types of categories of algorithms are:

- **Conventional Encryption**: DES, Triple DES, Skipjack and IDEA are very common.
- **Public Key Encryption**: RSA, PGP and Diffie-Hellman are common.
- **Hashing**: SHA-1 (Secure Hashing Algorithm 1) and MD5 are common (MD = Message Digest).

A goal of cryptography is to force someone into have to try each and every possible combination of the key to be able to solve for the message. If it is not feasible to try every combination then your message should be secure.

However some encryption algorithms like RSA use a theoretical method of doing the encryption process. If someone could find a mathematical shortcut to RSA that person might be able to break RSA and thus not have to try every combination.

Security Services Supported by Cryptography

The three main purposes of using cryptography are:

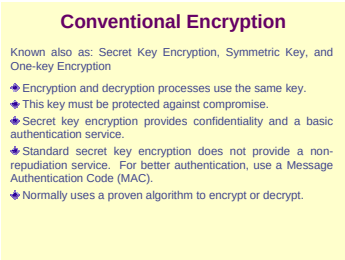
Confidentiality – Protects information against unauthorized disclosure. It helps to support the rights of individuals and organizations to control who has access to information relating to them. This right is referred to as privacy.

Integrity – Protects information against unauthorized modification. The service can sometimes protect against the insertion, reordering, deletion, and playback of information as well.

Authentication – Provided assurance for the identity of an individual or system. It can also provide assurance that information originated from a particular individual or system.

Non-repudiation – Provides protection against an individual that falsely denies that they participated in a communications exchange (that a message was transmitted and/or received).

Conventional Encryption



In Conventional Encryption (also known as symmetric, secret, or one-key encryption), the encryption and decryption processes uses the same key. It is critical that this key not be compromised at any location while it's being distributed or used. (Example: Your Credit Card)

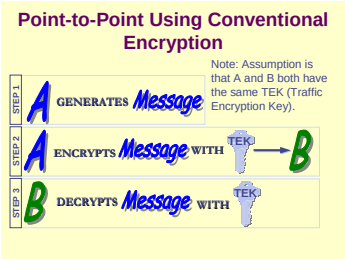
The fundamental purpose of Conventional Encryption is to provide a confidentially service. It also provides a rudimentary authentication service. If only two parties have copies of the key and the destination can decrypt a message in meaningful plaintext, this implies that the only other party that holds the same key transmitted the message. This does not however ensure that the message was just transmitted by the originator. The message could be recorded and played back by an outsider.

Conventional Encryption between two parties does not support a non-repudiation service. Suppose you have a message encrypted in a key shared between yourself and another party. Can you bring it to a judge and decrypt it under this key and then claim the other party originated the message? You cannot because it is possible that you encrypted the message yourself.

Uses mathematical formulas that are not theoretical but are mathematically proven so that no one could find a way to short cut the math. In other words to break the encryption they must use bulk decryption techniques or find a way to capture a key. The most common techniques in Conventional Encryption are:

- Block Ciphers
- Stream Ciphers
- Message Authentication Code (MAC)

Point-to-Point Using Conventional Encryption

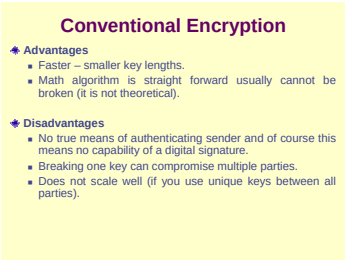


This slide shows how Conventional Encryption works. Note that the assumption is that A and B both have the same TEK (Traffic Encryption Key) which was distributed earlier.

The first party uses a TEK that he shares with person B to encrypt the message. Note we have not covered key distribution yet. This encryption assumes that B has a copy of the TEK already. The same key that encrypts the message is the same key that decrypts the message.

Remember: Both parties have the same TEK that can be used for both encrypt and decrypt messages. Example is your credit card.

Conventional Encryption



Advantages:

A primary advantage of conventional encryption is that it is 100 to 1000 times faster to use than public key encryption. This is strictly due to the fact that conventional encryption uses much smaller key lengths to provide for the same amount of security.

A second advantage is it is mathematically infeasible to short circuit the bulk decryption process.

Disadvantages:

The primary disadvantages led to the development of public key algorithms. First you cannot prove that the person who sent the message actually is the person who sent the message. This leads to an inability to truly be able to authenticate the sender.

Another disadvantage is that a lot of times conventional encryption keys are shared between multiple parties and breaking one key can lead to the compromise of everyone.

Also if you use a unique key pair (secret key) between every sender and destination then you have a factorial amount of keys. This led to the development of certificate authorities for distribution of keys. There were just to many people who had keys for everyone to have their own copies.

Public Key Cryptography

Public Key Encryption

Known as: Asymmetric Key and Two-key Encryption

This process involves the following two keys:

Public Key: Used to encrypt messages.
Does not have to protected against compromise
Available to the General Public through a trusted third party or a Key Distribution Center (KDC)

Private Key: Used to decrypt messages
Must be protected against compromise at all times
Distributed and installed on the system through a trusted third party or a KDC.

Public Key Encryption is also known as asymmetric or two-key encryption. The process of this type of encryption involved two keys:

Encryption process uses the Public Key of the receiver. Either a trusted third party will store your public key (Verisign, Entrust) or you can do it yourself with the use of a Key Distribution Center (KDC) by using products such as Exchange Server, versions 5.5, 2000, and 2003. This Key does not have to be protected against compromise due to the fact that you cannot decrypt any message with this key and it's also available to the general public.

Decryption process uses the private key of the receiver. This key is distributed and installed on their system either from trusted third party (Verisign or Entrust) or you can once again do it yourself through a KDC using products like Exchange Server, version 5.5, 2000, and 2003. This key must be protected against compromise at all times. If this key is compromised, then all keys, including the Public Key, must be replaced.

Public Key Cryptography

Public Key Encryption

The sender and receiver do not use the same key to encrypt and/or decrypt messages. The math algorithm ensures this by the use of prime numbers.

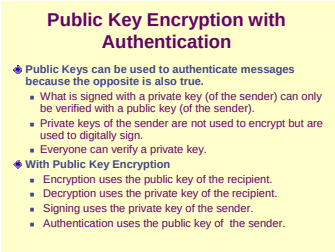
If something is encrypted with a public key it cannot be decrypted with the same public key. Public keys can be shared because of this.

Public key encryption is asymmetric because it uses two different keys for the encryption and decryption process. In other words that same key cannot decrypt the math algorithm that allows you to encrypt a message with one key. If Sam uses his public key to encrypt a message he could not decrypt that message with his public key, the math is not reversible.

Therefore the only person that holds a copy of the person's private key is himself and he is the only one that can decrypt a message that is encrypted with his public key.

Most public key algorithms work on prime numbers. The first prime number has an opposite. So that if you divide the big number that was encrypted with the opposite prime number it gets the same message. This is based on a rule of prime numbers and modular arithmetic. Note that it is exponentially impossible to calculate one key given the other key. So you cannot find the private key if you know the public key.

Public Key Encryption with Authentication



The math works in the opposite manner. What is signed with a private key can only be verified with the public key of the sender. Therefore anything that can be verified with a sender's public key could only have come from the sender because he is the only one who has that private key.

This is authentication, not encryption, since the public key is well known and anyone could verify a private key as long as you have their public key. An important point here is the verification will only come out right if the signing was done with the private key and that the keys have not either expired or placed on a revocation list.

So a person's private key is used to decrypt messages sent to him or sign messages that he is sending to someone else. A person's public key is used to encrypt messages being send to that same person and to verify messages that the person sent.

So with Public Key Encryption;

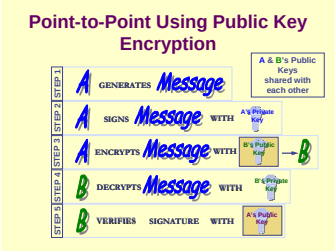
Encryption uses the Public Key of the recipient (the one who you are sending the message to).

Decryption uses the Private Key of the recipient (the one who you sent the message to. Since you used their Public Key to encrypt, only their Private Key can be used to decrypt the message).

Signing uses the Private Key of the sender (which is the person that is sending the message).

Authentication uses the Public Key of the sender (the person that is receiving the message, will need to have the Public Key of the sender to verify the digital signature so they know that the message only came from that person and no one else).

Point-to-Point Using Public Key Encryption



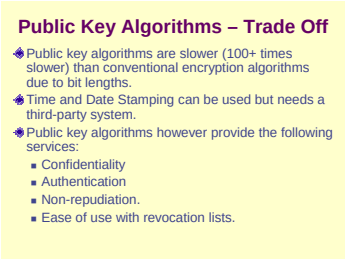
The most basic form of public key algorithm works in the following way.

A wants to encrypt a message to be sent to B. A signs the message with his own private key and then encrypts the message with B's public key. A probably will get B's public key from a certificate authority.

When B gets the message he decrypts the message with his private key. After he decrypts the message with his private key he verifies A by using A's public key (which he also probably gets from a CA).

If everything checks out B knows the message came from A and A knows that only B could read his message. Thus both confidentiality and authentication are accomplished.

Public Key Algorithms – Trade Off



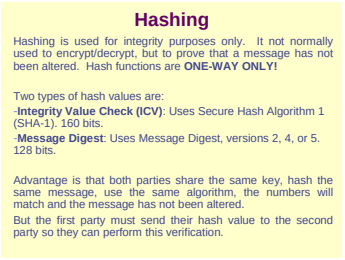
Public Key algorithms are much slower that Conventional Encryption methods (100 to 1000 times slower) due to the bit lengths.

Time and date stamping can be used only if you have a third-party system that can perform such a function for messages and data that uses Public Key algorithms.

Public Key algorithms however provide the following services:

- Authentication and non-repudiation
- Can use Revocation Lists to revoke keys or Digital Signatures/Certificates from being used if expired or compromised
- With an attached hash value (ICV or Message Digest), it provides a method of checking the integrity of the message or signature/certificate

Hashing



Hashing is used for integrity purposes only. It's not normally used to encrypt/decrypt, but to prove that a message has not been altered. Two types of hash values are Integrity Check Value (ICV) or a Message Digest (MD).

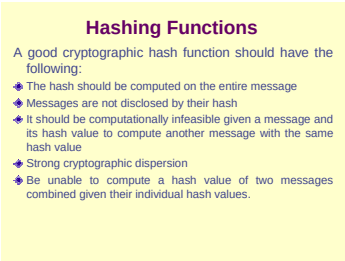
Hash functions are **ONE-WAY ONLY**. This will confirm that the message has not altered and are not disclosed by their hashes.

Hashing requires that only the sender and the recipient know the key that is used to conduct the hash using a commonly known formula like SHA-1 (160 bits), MD 4 or 5 (both 128 bits).

After conducting a hash on a message a unique number will be the result that unique number will be 160 bits long for SHA-1 or 128 bits long for MD 4 or 5. If one bit in the message was hashed changes then it completely changes the hash value (the 128 or 160 bit number).

The advantage of this is that if both parties share the same key hash the same message with the same algorithm they will get the same number or hash value. If the hash value is the same both parties know the message has not been altered (one-wayness). However the first party must send his hash value to the second party so he can perform this verification (so normally he must encrypt this in some manner).

Hashing Functions



A good cryptographic hash functions should have the following properties:

The hash should be computed on the entire message. Remember, hashes are one-way functions. They can be used to decrypt the ciphertext and produce the original data.

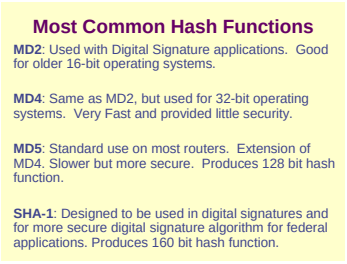
Messages are not disclosed by their hash. When the hash is broken, it allows a cryptanalyst to generate another message with the same hash, which the attacker could substitute for the original.

It should be computationally infeasible given a message and its hash value to compute another message with the same hash value. This is called a Birthday attack, which the attacker finds a second message that produces the same hash.

Strong cryptographic dispersion. This means that if even a single character in a large message is changed, the two hashes will look completely different.

Be unable to compute a hash value of two messages combined given their individual hash values.

Most Common Hash Functions



Types of Message Digests:

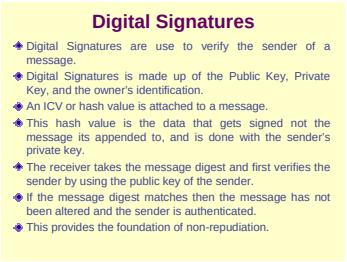
MD2: Used with Digital Signature applications. Used when a large file must be compressed in a secure manner before signed with a Private Key. Good for older 16-bit operating systems (Windows 3, 3.1, 3.11).

MD4: This was designed to be used on 32-bit operating systems and was quite fast. Does not require large substitution tables and can be coded quite compactly. Still had speed but some security.

MD5: Used as today's standard on most routers. Extension of MD4. Slightly slower, but more conservative. Less speed, more security.

SHA-1: Designed to be used in digital signatures and for more secure digital signature algorithm for federal applications. Produces 160 bit hash function.

Digital Signatures



A digital signature supports authentication, integrity and the foundation of a non-repudiation service.

Authentication is supported because if a person can verify the signature of a message with the sender's public key then he knows that only he could of signed the message.

Normally a message has an attached hash value. So normally the sender hashes the message with a key known to both the sender and destination and signs the hash value of the message with his (the sender's) private key.

Therefore when the receiver gets the message he decrypts the message with his private key and verifies (decrypts) the hash value attached at the end of the message with the sender's public key.

When the receiver hashes the message the resultant value of his hash should be equivalent to the sender's hash value that was attached to the end of the message.

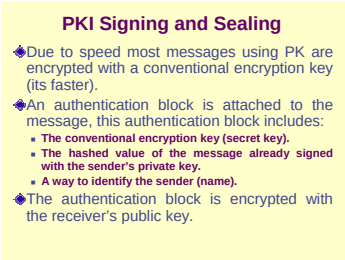
If both of these values are equivalent then the recipient knows that the sender sent the message and it has not been altered. **THIS IS A POWERFUL CONCEPT.**

Note: When you sign your message using a Digital Signature and you want to add more information to your message (attachments), you can add the information, but you must re-sign the message again or the ICV or Message Digest will not match and the message will bounce back.

Digital Signatures need the following:

- Public Key for authentication of the sender.
- Private Key for signing the message.
- Owner's Identification which is the hash or fingerprint.

PKI Signing and Sealing



To solve the need for speed problem, most public key algorithms use the public key to encrypt a conventional encryption key that it generates for the recipient. By sending an encrypted secret or conventional encryption key to the recipient the public key algorithm can use conventional encryption to encrypt and decrypt a message.

To perform this function the usual process is as follows:

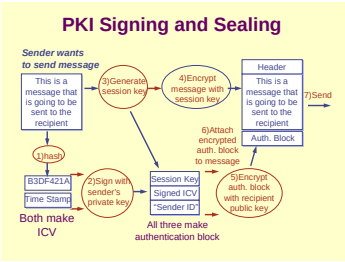
The sender creates an authentication block that is attached to the sent message.

In this authentication block is the hashed value of the message (message digest), the conventional encryption key that the sender wants to use with the destination to encrypt and decrypt all the messages and usually a way to identify the sender.

The sender will then encrypt the authentication block with the recipient's public key.

After the authentication block is encrypted the sender encrypts the message portion with the generated secret key that he put in the authentication block.

PKI Signing and Sealing



So the process is:

Take the original message and run a hashing algorithm to come up with a hash value.

Hash the message to get a message digest or hash value.

Generate a secret key using a secret key algorithm for example PGP uses the 128-bit IDEA key.

Encrypt the message with the generated secret key.

Take the hash value (which may have a time stamp with it) and sign it with the sender's private key (his digital signature).

Attach all three together, which makes an authentication block and encrypt this message with the destination's public key.

Then attach the authentication block to the message that is encrypted with the secret key (also sometimes called a session key).

PKI Unsealing and Verifying

PKI Unsealing

- The authentication block is detached and decrypted with recipient's private key. The recipient now has:
  - **A signed hash value.**
  - **The name of the sender.**
  - **The conventional (session) key used to encrypt the message.**
- The conventional key is then used to decrypt main message.
- The recipient then uses public key of sender to authenticate sender and verify integrity of message.
- Two examples - PGP uses IDEA for conventional encryption and RSA normally uses DES.

The authentication block at the recipient has to be taken off of the message. You can do this because the length of the authentication block is known.

The recipient now has to decrypt the block with his private key. He will get a signed hash value (which he will need the public key of the sender to verify). The recipient now also has the secret key that was used to encrypt the main message.

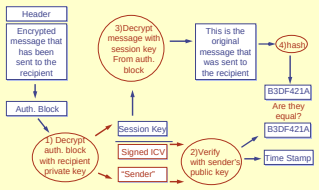
The recipient then decrypts the main message with that conventional key. He then can read the message, but will in addition hash the message to verify the integrity of the message (comparison with the sent hash value) and of course this verifies the sender (remember the hash value was signed with the sender's private key).

Two examples of this type of encryption are:

- PGP, which uses IDEA (International Data Encryption Algorithm) for Conventional Encryption.
- RSA, which normally uses DES (Data Encryption Standard). Will be using AES (Advanced Encryption Standard)

PKI Unsealing and Verifying

PKI Unsealing and Verifying



The recipient decrypts the authentication block with his private key.

The recipient gets the secret key and decrypts the main message.

The recipient then decrypts the signed hash value with the sender's public key.

After hashing the main message the recipient compares this with the sent hash value or ICV if they are equivalent this proves the sender sent the message and it has integrity.

As a side note the encryption and decryption of additional data can be conducted using the same conventional encryption key and the time stamp is normally used for a TTL or time to live for that conventional encryption key.

Security Services Supported by Cryptography

Security Services Supported by Cryptography

- **Confidentiality** – Encryption whether with a public or conventional algorithm.
- **Integrity** – Hash or message digest or ICV.
- **Authentication** – Verifying the sender by an assumption or by a signature.
- **Non-repudiation** – Validating a digital signature where no one can disclaim it.

Therefore the above 4 services are provided using most public key algorithms.

This is why the Army is switching to public key algorithms. Combined they provide the advantages of all three cryptographic techniques and enforces authentication, something that was previously missing.

Encryption Weaknesses

Encryption Weaknesses

Encryption Weaknesses could come from any of the following:

- Brute Force Attacks
- Mishandling or Human Error
- Deficiencies in the cipher itself

Encryption weakness could occur from the following:

- Brute Force Attacks
- Mishandling or Human Error
- Deficiencies in the cipher itself

Halftime

HALFTIME

In the second half, we will discuss:

- Types of Attacks on your Network Traffic
- Basic Strategies for Encrypting Network Traffic
- Key Distribution
- Encryption Standards and Tools
- Email Security in Encryption

In the second half, we will discuss:

- Types of attacks on network traffic
- Basic strategies for encrypting network traffic
- Key distribution
- Encryption standard and tools
- Email security

Attacks on Network Traffic

Attacks on Network Traffic

Passive Methods (Packet Sniffing)

Content Analysis: Reconstruct entire session. Most common attack against current networks.

Traffic Analysis: Using traffic flow to map a network's potential weak points. More difficult and low payoff.

Countermeasure: Both can be countered by using encryption tools.

Networks may consist of point-to-point or broadcast channels. Intruders have several approaches for attacking the network traffic that is transmitted over these channels, depending on the type of access available and the desired results of the attack.

There are two types of attacks on network traffic:

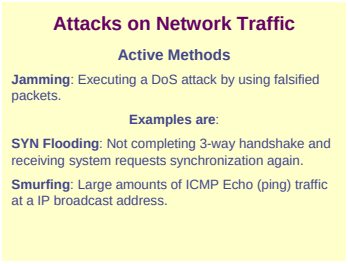
Passive Methods

Content Analysis: If the content can be read, the attacker can reconstruct entire sessions, including usernames and passwords since most of them are passed in clear text (in the clear). This is the most common attack against current networks.

Traffic Analysis: If the content cannot be read, the attacker may still be able to reconstruct some information, and use traffic flow to map a network's potential weak points. A large change in the amount of traffic may also be an indicator. Traffic Analysis is significantly more difficult and usually has a lower payoff in useful information than Content Analysis, but may still produce worthwhile results.

Both Content and Traffic Analysis can be countered by using encryption tools.

Attacks on Network Traffic

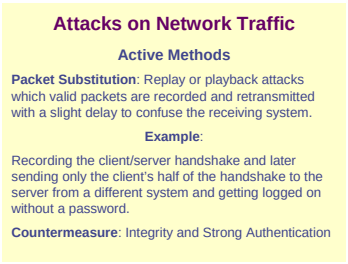


Active Methods

Jamming: Whether or not the attacker is able to directly read the content of network traffic, an attacker may be able to execute a DoS (Denial of Service) attack by "jamming" the network with falsified packets. Example of this would be SYN Flooding and Smurfing.

Note: Smurfing is one of the most recent in the category of network-level or denial-of-service attacks against hosts. A perpetrator sends large amounts of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim.

Attacks on Network Traffic

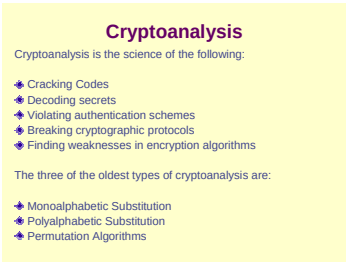


Packet Substitution: These are replay or playback attacks in which valid packets are recorded and retransmitted with a slight delay, to confuse the receiving computer. A sophisticated attacker, who is able to read the contents of the traffic, may be able to inject traffic onto the network, which is accepted and acted upon by other computers.

An example of this would be recording the client/server handshake and later sending only the client's half of the handshake to the server from a different machine and getting logged on without a password.

Checking integrity of the traffic flow and using some form of strong authentication can counter both Jamming and Packet Substitution.
Spoofing: Recording a communication session and using the data received to plan and attack the network. This can be countered by using some form of authentication.

Cryptoanalysis



Cryptoanalysis is another type of attack on networks. Cryptoanalysis is the science of:

- Cracking codes
- Decoding secrets
- Violating authentication schemes
- Breaking cryptographic protocols
- Finding weaknesses in encryption algorithms

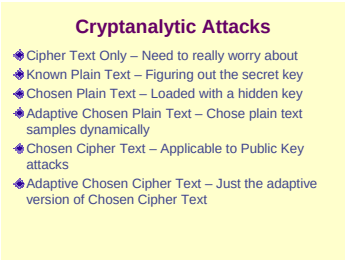
It is only a myth that modern cryptoalgorithms are broken by mathematicians working with pen, paper, and supercomputers. Now computers are faster and can do the cracking with brute force programs. Known cryptoanalytic methods were developed long ago and are of historical interest.

Monoalphabetic Substitution: This uses one list of characters and letters are substituted according to it. They are not safe and can be easily cracked.
Polyalphabetic Substitution: This uses several substitution lists.

Permutation Algorithms: They change the order of letters and are simple to crack as well.

Basically, in order to crack these kinds of algorithms, you will need to guess a word or 3 to 4 letters, after which guessing gets easier.

Cryptoanalytic Attacks



There are several cryptanalysis attack methods that we need to be fully aware of. These attacks can be used against text and/or the key that is used to either encrypt, decrypt, or for verification of one's identity.

Cipher Text Only Attack: This attack uses a sample of cipher text that is available, without the plain text associated with it. It is the most difficult because you do not know anything about the algorithm, key lengths being used, or the clear text.

Known Plain Text Attack: With this attack, the cipher text and the corresponding plain text is also available.

Chosen Plain Text Attack: A crypto device is loaded with a hidden key that is provided and the input of any plain text is allowed to see the output.

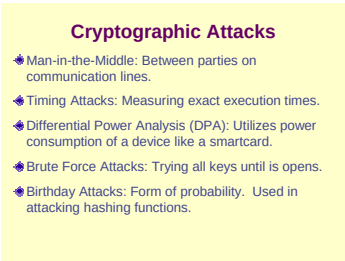
Adaptive Chosen Plain Text Attack: Just like the Chosen Plain Text Attack except you are able to chose plain text samples dynamically and alter your choices based on results of previous encryptions. This is the easiest form of attack than the previous mentioned.

Now, the ones just discussed above are mostly for plain text traffic. We will now look at attacks on just cipher text.

Chosen Cipher Text Attack: The attacker may choose a piece of cipher text and attempt to obtain the corresponding decrypted plain text. This is generally applicable to attacks against public key algorithms.

Adaptive Chosen Cipher Text Attacks: This is the adaptive version of the Chosen Cipher Text Attack. The attacker can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

Cryptographic Attacks



Other are other cryptographic attacks that we need to be aware of while trying to achieve network security using encryption.

Man-in-the-middle Attack: The attacker puts himself between parties on a communication line. Relevant for cryptographic communications and key exchange protocols.

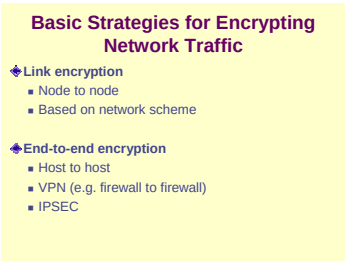
Timing Attacks: Repeatedly measuring exact execution times of modular exponentiation operations. Relevant to at least RSA, Diffie-Hellman, DSS, and Elliptic Curve methods.

Differential Power Analysis (DPA): The attacker does not have to know anything about the algorithm that is being used, only the power consumption of a particular cryptographic device, such as a smartcard. Unfortunately, this attack involved hundreds to thousands of samples, but once finished with the processing and statistical analysis, then the process can reconstruct the full secret or private key within several minutes. Cost of equipment ranges from a few hundred to a few thousand dollars and the attacks are non-invasive and very difficult to detect. Requires little or no information about the target device, can be fully automated, and has been very successful in the past.

Brute Force Attacks: The most common attacks on encrypted traffic. Trying all the keys until the correct key is identified. With advances in technology and computing performance makes brute force attacks an increasingly practical attack on keys of a fixed length.

Birthday Attacks: They are a form of brute force attacks and works on using probability and statistics. As an example, the birthday paradox of the probability that two or more people in a group of say 23, have the same birthday is > 50%. This type of attack can be applied to hash functions and Message Authentication Code.

Basic Strategies for Encrypting Network Traffic

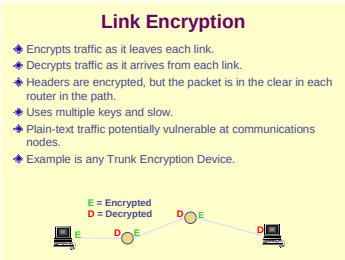


There are two fundamental strategies, which can be used to protect network traffic using encryption.

Link encryption is node-to-node (router to router normally) based encryption. It will encrypt all the transmission control headers and routing headers (normally).

End to end encryption is normally an encryption technique done from the destination to the recipient. An exception would be Virtual Private Network (VPN), which is done from a network to a network. VPN's use a preexisting network backbone to encrypted traffic however the IP headers (or whatever header is used to route the traffic) are in the clear. The rest of the encapsulated message is encrypted.

Link Encryption



All traffic is encrypted as it is about to be transferred over any communications link and then immediately decrypted upon arriving at the other end of the link. Traffic traversing the links is encrypted but is in the clear within the nodes, which is the primary weakness of this type of encryption.

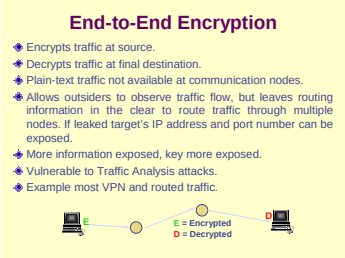
Headers are encrypted, but the packet is in the clear in each router in the path.

Encryption points at each end of a given link must share the same key, which can be selected independently from the other links that comprise the network. Due to the decryption and encryption process that happens at each node the packet goes through this does slow down traffic.

Full Period Encryption: This implies that the security environment at the communication nodes should provide adequate protection to handle this traffic, since it could be potentially accessed. If Link Encryption is implemented at the physical layer, everything transferred over the channel can be encrypted. It also provides a traffic flow confidentiality service.

An example of Link Encryption is any Trunk Encryption Device such as a TACLANE, KIEV-7, or a KG-175.

End-to-End Encryption



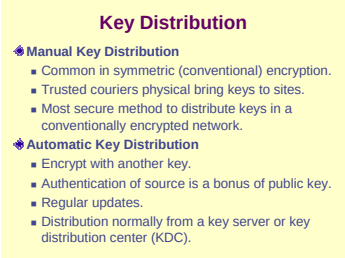
Traffic is encrypted at the source host or workstation and decryption is postponed until the traffic arrives at the destination.

End-to-end encryption protects the traffic that enters the communications nodes, so plain text traffic is not available. This does allow outsiders to observe the flow of traffic across the individual communications links because the routing information has to be left in the clear to route the traffic through multiple nodes.

Each pair of hosts that are to communicate must use the same algorithm. Since the encrypted message is exposed at all points. A cryptanalyst could use a larger sampling of the encrypted message text which aids in the breaking of the message.

Very vulnerable to Traffic Analysis attacks. If leaked, the target's IP address and port numbers can be exposed. More information exposed, the key is more exposed. Examples of End-to-End Encryption are most VPNs and routed traffic.

Key Distribution



Key Management deals with the generation, storage, distribution, deletion, archiving, and application of keys in accordance with some security policy.

Manual Key Distribution: Trusted couriers physically bring keys to the sites where they will be used. These keys can be conveyed on paper, cards, paper tapes, etc. These keys are called **Traffic Encryption Keys (TEKs)**, as they are intended for network data encryption.

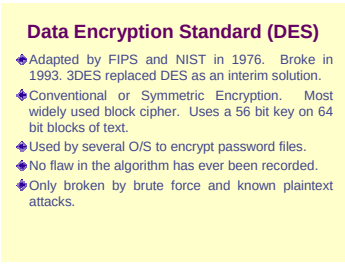
Manual key distribution was very common in conventional encryption and is the most secure method to distribute keys in order to establish a conventionally encrypted network. However the move today is to automate the key distribution in a trusted manner.

Automatic Key Distribution: TEKs are distributed to remote sites over communications channels. Distribution is accomplished without compromising the TEKs by using other keys called **Key Encrypting Keys (KEKs)**. KEKs can be used to encrypt other KEKs as well as TEKs.

TEKs are normally conventional encryption keys. Encrypting them with the public key of the recipient using a public key algorithm can also send session keys.

Normally key distribution in a network is done from a key server (KS) or a key distribution center (KDC). When getting a public key for an intended recipient this is normally received from a certificate authority (CA).

Data Encryption Standard



DES is a very old encryption algorithm. Most widely used symmetric or conventional block cipher. Adopted as the NIST and FIPS as the standard encryption algorithm for unclassified data in 1976.

Because it was broken in 1993, We use Triple DES (3DES) and was the interim solution until a suitable replacement can be developed. NIST maintained acceptance of DES in the form of 3DES for commercial use because so many financial institutions have hardware encryptors that still use DES.

DES uses a 56 bit key (the key length is 64 bits but every 8th bit is ignored and used for parity checking only) on 64 bit blocks. Normally a method called CBC-64 or cipher block chaining 64 is used to conduct the encryption. The CB and 64 stand for the block size and chaining refers to the fact that the outcome of the first block of encryption affects every following block (they are chained). This prevents someone from reordering the blocks.

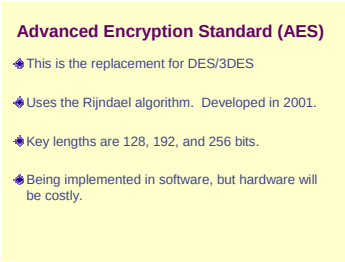
When you encrypt blocks of data you can use transposition to reorder the bits. DES uses 16 rounds of transposition ciphers.

The main problem with DES is that 56 bit keys are breakable now and that several operating systems still use DES to encrypt their shadow files (like some UNIX O/S). There has been no known flaw in the algorithm that has ever been recorded, but has been broken by brute force and known plaintext attacks.

As a side note the length of the key does not determine how many bits you can encrypt with it. The length of the key determines how many different versions of that key their can be. For example Skipjack the key used with DMS uses 80 bit key lengths to encrypt 64 bit blocks.

DES was removed by NSA's list of acceptable cryptography in the early 90s. This meant it could not be used in government transactions.

Advanced Encryption Standard (AES)

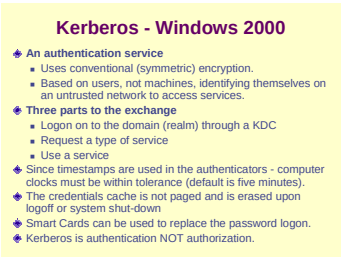


This is the replacement for DES/3DES. It uses the Rijndael algorithm for its strength and was developed in Belgium in 2001.

The key lengths are much stronger than DES. They start out at 128 and move to 192 and tops out at 256 bits.

Although AES is now an accepted standard, there are not many implementations of it because DES has been the standard for so long now. AES has been implemented mostly in software. DES has been often implemented in hardware, which means that in order to switch to AES, the hardware must be upgraded and can become very costly.

Kerberos – Windows 2000



Kerberos has been through several versions. Currently Windows 2000 use Kerberos version 5. Kerberos does not use Public Key Encryption it bases its encryption entirely on conventional encryption.

The KDC (Key Distribution Center) stores a "long-term" key for a security principal, the long-term key is normally a derivation of the user's password. So every member of a domain has their password stored at the KDC.

There are 3 steps in the Kerberos sequence:

- Note that Step 1 is used when the user logs onto the network. The finished login process gives User A a TGT which he cannot read, because the TGT is actually encrypted with the KDC (key distribution center's) long term key.
- The second step gives the client the ability to access different services based upon his TGT which was issued to him upon login. The TGS is done normally once a day or once for every logon session for the user. The user uses the TGS to access different services based upon the user's authorization data.
- The third step is the actual access to a specific service.

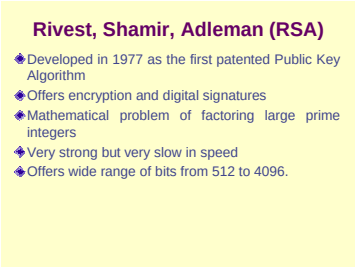
Since timestamps are used in the authenticators, computer clocks must be within tolerance. (Default is 5 minutes).

The credentials cache is not paged and is erased upon logoff or system shutdown.

Smart Cards can be used to replace the password logon.

Kerberos is authentication NOT authorization

Rivest, Shamir, Adleman (RSA)



Developed by three of the top mathematicians in the United States, Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. This was the first patented Public Key algorithm in this country.

This asymmetric encryption standard offers the ability to encrypt and decrypt messages along with a digital signature so that you can sign your message and be able to authenticate or verify the signature, which is our foundation for non-reputation.

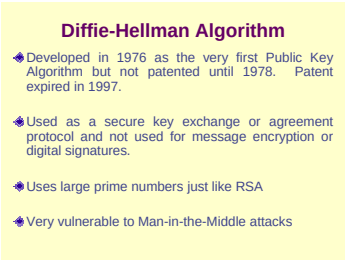
What makes RSA so strong is the mathematics of this algorithm is factoring multiple large prime integers. Crackers have tried for many years to find those prime numbers to break it, but have not succeeded. Along with it's strength, it is very slow in the encryption portion. How slow?

- 100 times slower than conventional encryption in software
- 1,000 – 10,000 times slower that conventional encryption in hardware

Why so slow is once again going back to key lengths. Remember, the larger the key, the slower it will be to encrypt and decrypt, but you get outstanding security.

RSA offers a wide range of bits to choose from, depending on the type of security you desire. 512, 768, 1024, 2048, 3072, and 4096. The government users mostly 4096 in some of its transactions, which requires mini super computers to run.

Diffie-Hellman Algorithm



Developed by two foremost mathematicians in the United States, Whitfield Diffie and Martin Hellman in 1976. This was the very first Public Key Algorithm, but not patent until 1978. The patent expired in 1997.

This type of asymmetric encryption does not encrypt/decrypt messages or has an digital signature that is available. This is used as a secure key exchange or agreement, so that in our modern PKI, we can securely send the symmetric key to the recipient so that the body of the message can be encrypted and/or decrypted.

Like RSA, it also uses large prime numbers to generate its public key, usually 1024 bits in length.

Since the symmetric key is sent over the wire in PKI and this algorithm is used to secure that key while it's being sent, this makes it very vulnerable to Man-in-the-Middle attacks.

Certificate Authority (CA)

Certificate Authority (CA) is an organization that maintains and issues public key certificates either from a third-party entity or you can setup a server and issue your own.

When a person requests a certificate, the CA verifies that the individual's identity, constructs the certificate, signs it, delivers it to the requestor, and maintains the certificate over it's lifetime.

The CA manages Public Keys.

Certificate authorities use public keys to provide authentication and integrity services. First by using a public key for itself it can prove that any public key that it sends to a party that requests that public key is valid (it signs this with its private key). Integrity is provided using the same hashing mechanism as talked about earlier in this lecture.

In addition the CA gives a person the ability to revoke certificates. In other words a Certificate Authority can revoke a person's certificate – which has the person's public key (maybe the person moved, quit or turned out to be a bad guy). If a certificate is revoked then any person that comes to the CA to get a public key will be told that the other person is an invalid user and will stop the process.

The critical part of certificate distribution is that the private key is always protected against compromise.

Certificate Revocation List: This is a list of certificates that have been revoked before their scheduled expiration date due to the key was compromise or the individual who created the certificate has left the company. Normally the CRL is on the CA.

In Windows 2000, Certificate Authority takes on a whole new look. In NT, we could only produce a stand-alone CA and had to do this on all systems. In Windows 2000, we still have stand-alone CA, but now we have Enterprise Root and Enterprise Subordinate CA and we can have our files/directories protected by a CA.

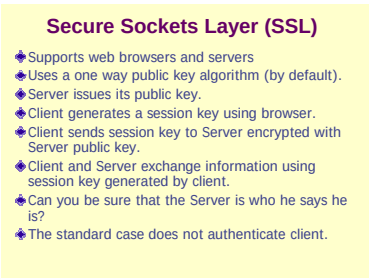
Root Enterprise CA: This can only be setup on W2K Domain Controllers (Active Directory). This is setup first before you can setup and use Enterprise Subordinate CA's. The person that will be responsible for this type of CA must be a member of the Enterprise Admins group or they cannot create, administer, and modify the certificates. This will only issue certificates to enterprise subordinates CA's only.

Enterprise Subordinate CA: This is also setup on a W2K Domain Controller (Active Directory). They perform the following:

- Issue certificates to computer accounts automatically.
- Can be setup by modifying the Domain Security Policy.
- Allow for several key choices depending on your needs.

The Private Keys are stored in an encrypted folder on each system and cannot be moved.

Secure Socket Layer (SSL)



SSL provides the following features:

Supports web browsers and servers: This feature have been built into most major browsers and web servers (IIS, Apache). It lies between TCP and IP and uses HTTP as its protocol.

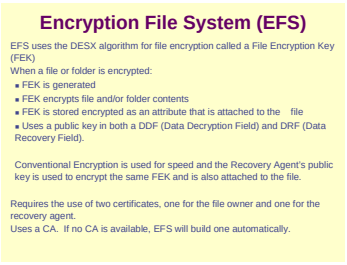
Security Services: Includes Authentication of the server to the client, mutual authentication between client and server, data confidentiality, and data integrity.

Storage Requirements: Server store their own Public and Private key, the certificate for their Public Key, and the Public Key of the CA who signed the certificate. Browsers that support client authentication store the same types of parameters. That is why you need a 128-bit browser if you are going to visit CA sites.

Authentication from client to server and server to client.

Encryption and Integrity: When authentication is successful, the client will generate a Master Key and transfers it to the server. This key is only good for the life of the session. Once terminated, a new Master Key must be generated.

Encrypted File System (EFS)



We talked about the functions of EFS in the Windows 2000 lecture last week. Now, we'll talk about the encryption end of EFS.

EFS uses a version of DES called DES extended or DESX, the key length according to Microsoft is 120 bits long.

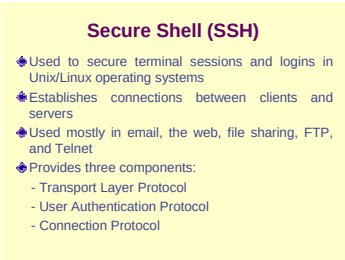
When a file or folder is encrypted:

- File Encryption Key (FEK) is generated
- FEK encrypts the file and/or folder contents
- FEK is stored encrypted as an attribute that is attached to the file or folder
- Uses a public key in both the Data Decryption Field (DDF) and the Data Recovery Field (DRF)

Conventional encryption is used due to speed. In addition a recovery agent's public key is used to encrypt the same FEK and is attached to the file.

It requires the use of two certificates, one for the file owner and one for the recovery agent, due to the public keys are for both the DRF and the DDF and because the FEK is encrypted and stored with the public key (so that they can recover the FEK with the private key).

Secure Shell (SSH)



SSH or Secure Shell, is a protocol which permits secure remote access over a network from one computer to another. Mostly used in Unix/Linux operating systems.

SSH will negotiate and establish an encrypted connection between an SSH client and an SSH server, and can authenticate the client and server in any of a variety of ways (examples: RSA, SecurID, and passwords).

That connection can then be used for a variety of purposes, such as creating a secure remote connection on the server replacing Telnet, rlogin, or rsh, or setting up a Virtual Private Network (VPN).

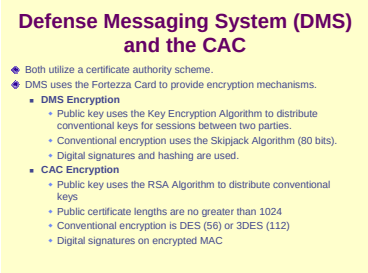
Users have a secure, encrypted tunnel to gain access to other TCP/IP connections like

- Secure access to email
- The web
- File Sharing
- File Transfer Protocol (FTP)
- Telnet

SSH provides three components:

- Transport Layer Protocol: Server authentication, confidentially, and integrity.
- User Authentication Protocol: Authenticates the client to the server.
- Connection Protocol: Multiplexes encrypted tunnel into several logical channels.

Defense Message System (DMS) and the Fortezza Card (CAC)



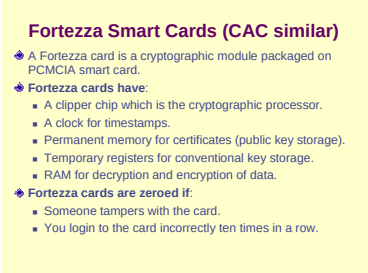
DMS uses a Certificate Authority (CA) scheme. DMS uses the Fortezza card to provide all the encryption functionality. The Public Key uses the Key Encryption Algorithm to distributed conventional keys for sessions between two parties, also called a session key.

The CAC or Common Access Card is similar to the Fortezza card in functionality although slimmer. The primary point here is that both cards are smart cards with cryptographic engines on them. The SA needs to have an understanding of what crypto is supported on each card and how the certificates are generated and distributed. This will have an impact on the placement of the CA and how it integrates the encryption into the network and system applications.

The Fortezza card which has a computer processor called Clipper on it (Clipper is also considered a cryptographic engine) is used to conduct both public and conventional encryption schemes. Much like in the diagram in the cryptography slides Fortezza uses a common public key algorithm to exchange conventional keys for encryption between two parties. The conventional encryption keys use the Skipjack algorithm (which uses 80 bit key lengths). Digital signatures and hashing are used (normally SHA-1).

The CAC card uses the RSA algorithm. The conventional encryption key supported is DES or 3DES. Digital signatures are used much like a signed hashed (it is different, but it is close enough). Ensure that you point out the weakness of DES vs. 3DES. 3DES is 2 to the power of 56 times stronger than regular DES (that is a large number over a trillion times harder to crack).

Fortezza Smart Cards



FORTEZZA smart cards are cryptographic modules that incorporate a variety of cryptographic algorithms (conventional and public key). FORTEZZA smart cards follow the PCMCIA industry standard.

- Fortezza cards uses a Clipper Chip, a cryptographic processor, to conduct the hashing, encryption and decryption processes.
- A clock for use with timestamps.
- Permanent memory to store the owner's private key and public keys of the owner and destinations. Temporary registers to store conventional Skipjack encryption keys (up to 10 although the 10th register is not used).
- RAM is used for data storage (the data that is to be decrypted or encrypted with the clipper processor).

You must login to use a Fortezza card. If you login incorrectly 10 times in a row the card is zeroed (if you log in on the 10th time then the log-in count is reset back to 0). Also tampering will zero the card.

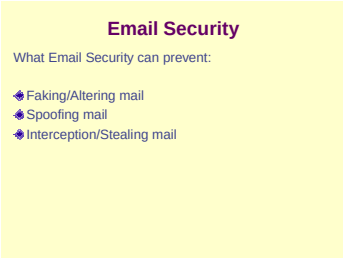
Email Security – Functions

A section that we really need to discuss and has become a high priority in our networks today, and that is Email Security. More and More threats are now coming though our email system at an alarming rate.

To achieve good email security, we need to have the following functions in place:

- **Message Origin Authentication**: Verifying that the sender is who they say that they are.
- **Content Integrity**: Verifying that he message was not changed after the sender sent it.
- **Content Confidentiality**: Making certain that only the intended recipient(s) reads the message.
- **Proof of Delivery**: Making certain that the message was delivered and to the intended individual(s).
- **Message Sequence Integrity**: Making certain that all messages were delivered in proper order.
- **Non-Repudiation of Origin**: Being able to prove that the sender sent the message.
- **Non-Repudiation of Delivery**: Being able to prove that the recipient got a message.
- **Message Security Labeling**: Labeling a message with handling instructions.
- **Secure Access Management**: Making certain no one uses your email address without being authorized (Domain Hijacking).

Email Security



Email security can prevent:

- Faking/Altering mail
- Spoofing mail
- Interception/Stealing mail

It also refers to techniques to ensure that the sender is the actual sender **(Authenticity)**, no one except the intended recipient can read the message **(Confidentiality)**, an intercepted message cannot be altered without detection **(Integrity)**.

Email Security – Standards

Now, let's take a look at some of the most popular email security standards on the market today.

Privacy Enhanced Mail (PEM): This is the standard proposed by the Internet Engineering Task Force (IETF). It defines procedures for message encryption and authentication services for email on the Internet (portal email like AKO, Hotmail, Yahoo) and is fully compliant with Public Key Cryptography Standards (PKCS). It is not utilized as a standard in any current email systems and is not designed to support MIME. Uses MD5 for hashing, DES for text encryption, and RSA for Public Key encryption.

Pretty Good Privacy (PGP): PGP is a very common public key algorithm that has wide acceptance. PGP uses a Peer Trust instead of a Certificate Authority. This means that there is no way to centrally revoke certificates and each member must store the public key certificates for people that they are going to send messages to. It uses a very secure Public Key algorithm called RSA. The keys can be 512, 768, 1024, 2048, 3072, and 4096 in length. Remember, longer the keys, takes longer to use but offers more security. PGP uses IDEA (International Data Encryption Algorithm) as its conventional encryption. IDEA uses strong encryption (128-bit). PGP can use digital signatures and normally uses MD5 (128-bit hash) for integrity checks. The bottom line is PGP is a great security algorithm but it lacks centralized control and the use of a certificate authority.

MIME Object Security Services (MOSS): Offers the same functionally as PEM, but supports attachments. Does not force a single trust model and allows identification of users by names that do not have any relationship to X.500, such as email addresses. Users MD5 for hashing, DES for text encryption, and RSA for Public Key encryption.

Secure Multipurpose Internet Mail Extensions (S/MINE): This is the de facto secure email standard in the industry. Most enterprise email solutions use this standard. Built into most email clients (Outlook Express, Outlook) and all you need is a certificate unlike PGP where you have to establish Peer Trust. Developed to fix interception and forgery of email messages. Easily integrated into email and messaging products. Provides confidentiality, data integrity, and authentication.

Message Security Protocol (MSP): This is the military's answer to PEM. It was developed by NSA at the end of the 1980s. It is an X.400 compatible application protocol used to protect email. This component of the NATO-approved military message format is an integral part of the Defense Messaging System (DMS).

Questions

PKI Practical Exercise

Lesson 1

This practical exercise is intended as a supplement to material learned during the Cyrptography and Encryption lectures. Students will become familiar with concepts and implementation necessary to configure and send encrypted emails.

You will need a partner for this exercise.

1.Open My Computer and double-click on the C: drive and go to the Temp folder.
   a. Open the PGP folder.
   b. Double-click on Setup.exe
   c. Click Next at the Welcome.
   d. Read the Agreement and click Yes.
   e. Read Product Information, and click Next.
   f. Accept the name and company information by clicking Next.
   g. Click Next at Choose Destination.
   h. At Select Components, ensure that PGP Microsoft Exchange/Outlook Plugin, PGP Outlook Express Plugin, and PGP Command-line are checked.
   i. Click Next.
   j. Click Next to copy files.
   k. When asked if you have an existing keyring, click No.
   l. Ensure "Launch PGPkeys" is checked, and click Finish.

2.The Key Generation Wizard will open. Click Next.
   a. Enter your fullname.
   b. Enter your **classroom email address** for your email address.
      (ask the instructor if you don't know what it is)
   c. Accept the pre-selected Diffie-Hellman/DSS and click Next.
   d. Accept the pre-selected 2048 bit key strength, and click Next.
   e. Accept the pre-selected "Key pair never expires" and click Next.
   f. Type in a passphrase that **YOU CAN REMEMBER** and confirm it by entering it again in the confirmation box. Click Next.
      (**IF** you are warned that your passphrase is a potential security hazard, click Next.
      IF asked to move the mouse to create some random data, do so, then click Next.)
      Once your key is generated, click Next.
   h. Your Digital Certificate will be generated. What 3 pieces of information does your digital certificate consist (Hint, it was in the lecture and the slides earlier.)
      _____
      _____
      _____
   i. **DO NOT** check “send my key to the root server now.” Click Next, and Finish.
   j. Now, manually start PGPtray. (Start -> Programs -> PGP -> PGPtray) (Nothing will open. You will see a small lock icon in your taskbar tray afterwards.)

k. Close the “My Computer” window that is currently displaying the PGP folder.

3.PGPkeys should still be open. PGPkeys is a user interface to allow you to manage your “keyring”, and access a certificate server for the purpose of sending, finding, and retrieving public keys.

a. Select all keys that are not yours, and delete them. (You can right click them, or you can use the trash-can icon on the toolbar.)
b. Click Edit, and then Options.
c. Select the Servers tab.
d. Click New. Leave the protocol at LDAP, set the server name to the classroom's server IP (The instructor will tell you it's IP), and set the port to 3890. Click OK.
e. Select the server you just added, and click the "Set as root" button.
f. Delete the other servers in the list by selecting them and clicking Remove.
g. Check every box in the “Synchronize with server upon” section of this window.
g. Click OK.
h. Select your key pair in PGPkeys.
i. Right-click it, and select "Send to". Select the server you just added to your list to have your key sent to it.
j. You will get a message "Key(s) successfully uploaded to server." At this point, the classroom server will now make your keys available to anyone who asks for them. Click OK.

4.Once your partner has reached this step, add their key to your keyring:

a. Click the magnifying glass on the toolbar. A search window will open. Do not type in anything, just click on search. This will return a list of all the keys that have been uploaded to the classroom server. Find your partner's key in the list, and add it to your keyring by right-clicking on it, and selecting "Import to local keyring".
b. Close the search window.

5.Open Outlook Express.

a. Click "Create Mail", and enter your partner's **FULL** email address in the "To:" field.
b. For the subject, enter ENCRYPTION TEST MESSAGE 1.
c. Write out a test message in the body of the email.
d. Click on the ">>" symbol on the toolbar if there is one, or stretch the message window out, you will see "Encrypt (PGP)" and "Sign (PGP)". Notice that there are **two** sets of buttons or menu entries labeled "Encrypt Message" and "Sign Message". The first set is for use with Microsoft and Commercial Certificates such as Verisign. The second set is there because you ran PGPtray earlier. (Step “j” at the top of this page. You *DID* take that step, didn’t you?) Make sure you use the PGP buttons for this exercise. The others **will not work.**
   Click each of them once.
e. Click Send.

6. If the Recipient Selection dialogue box opens, ensure the right key for your partner is in the Recipients area of the window. If it is not, you can click-and-drag it down. Click OK. Are you prompted for your passphrase? If so, why?

_____

_____

_____

7. When your partner reaches this point in the PE, check your email. (Click "Send/Recv" in Outlook Express.)

8. Go to your Inbox, and select the email with the subject: ENCRYPTION TEST MESSAGE 1. Are you able to read it from the preview pane? _____

9. Double-click the message in the message list, this will open the message in it's own window. Click the >> button if there is one, and then click the button labeled "Decrypt PGP message". Are you prompted for your passphrase? If so, why?

_____

_____

10. Once the passphrase was entered, what was done with the encrypted/signed message? Which keys were used for which parts?

_____

_____

_____

11. What is the signature's status? _____

12. What does it say next to the signer's name and address? _____

13. The (Invalid) indicates that the key used to verify the signature is not yet a trusted key. Let's assign this key some trust.

14. Open PGPkeys, select your partner's key, right-click on it, and select "Sign..."

15. Look at the statement at the top of the Sign Key window. What is the term for the kind of trust those two sentences are talking about?

_____

16. Click "Allow signature to be exported", and click OK.

17. Enter your passphrase if asked. Right-click on your partner's key again, and select Properties. Slide the Trust Model slide bar over to Trusted and click Close. You have just assigned trust to your partner's key.

18. Go back to Outlook Express. Open your Inbox, and double-click on your partner's message. Decrypt it as you did before. Is the (Invalid) still by the signer's name and address

_____

19. Now, send your partner an email that is signed, but not encrypted. Which key did you just use

_____

20. When your partner reaches this point in the Practical Exercise, click on Send/Recv and open the new message. You can read it, but there is a signature attached. In order to verify that signature, you can use the decrypt button again. Did the signature authenticate Were you asked for a passphrase Which key did you use to authenticate this message

_____

21. Now, send your partner an email that is encrypted, but not signed. Which key did you use to encrypt the message Were you asked for a passphrase this time Why

_____

_____

_____

22. When your partner reaches this point in the Practical Exercise, click on Send/Recv and open the new message. Decrypt it as before. Is there a signature status What key did you just use

_____

_____

_____

23. Try some more encryption tests between yourself and your partner, or with other people in the classroom. Don't forget which keys you need, and how to get them.

System Availability, Fault Tolerance, and System Recovery

Module 8

February 15, 2005 8-1

Lesson Objectives

- Review IS technologies available for high system availability
- Describe and implement various techniques for disaster prevention and system recovery
- Review Contingency Planning basics

System Availability

- **Backup**
- **RAID**
- **UPS**

Backup Strategies

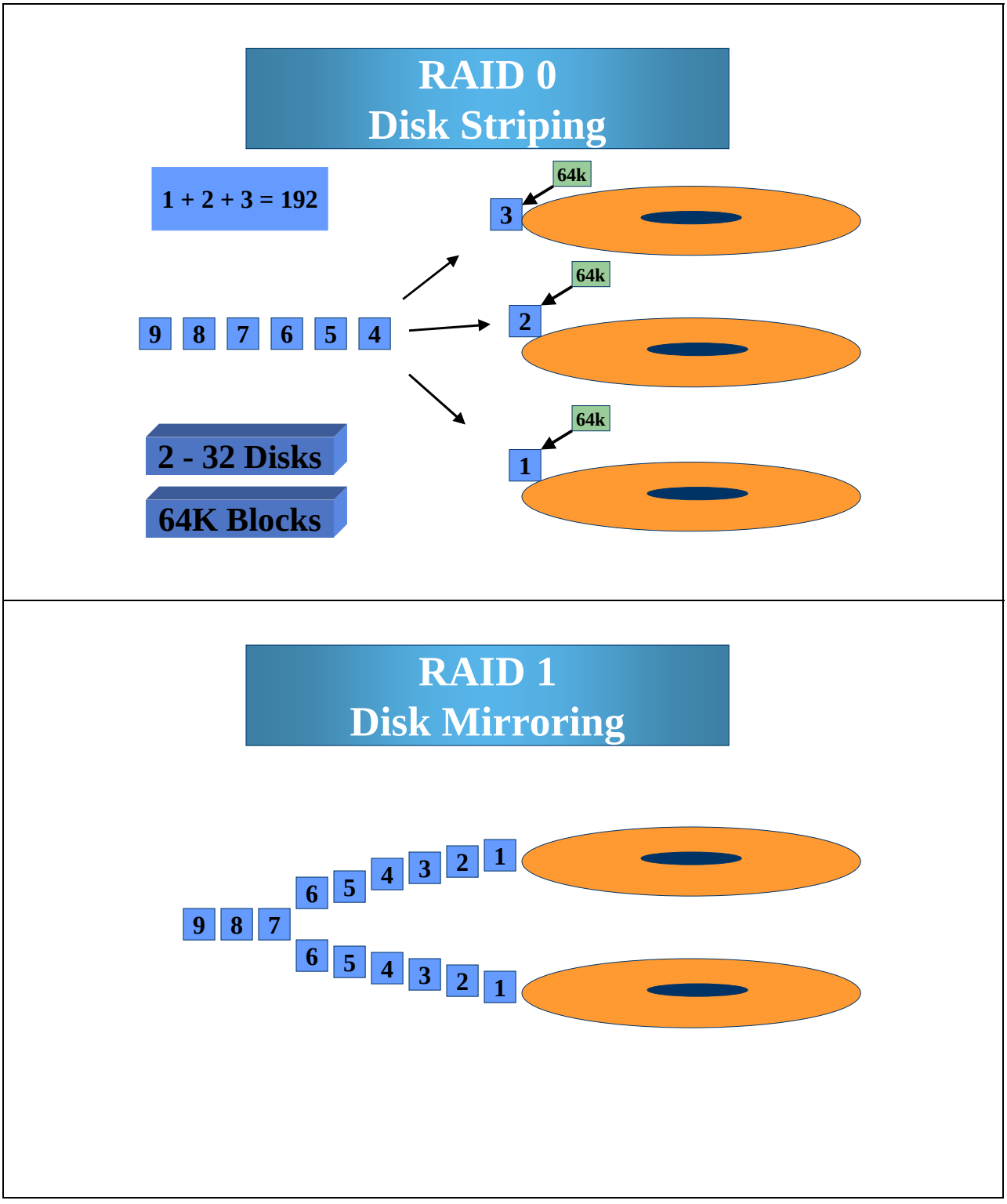
- **Why Backup ?**
- **What are some good software choices?**
- **What is your backup policy?**
- **Remember… Its Your Last Line of Data Protection**

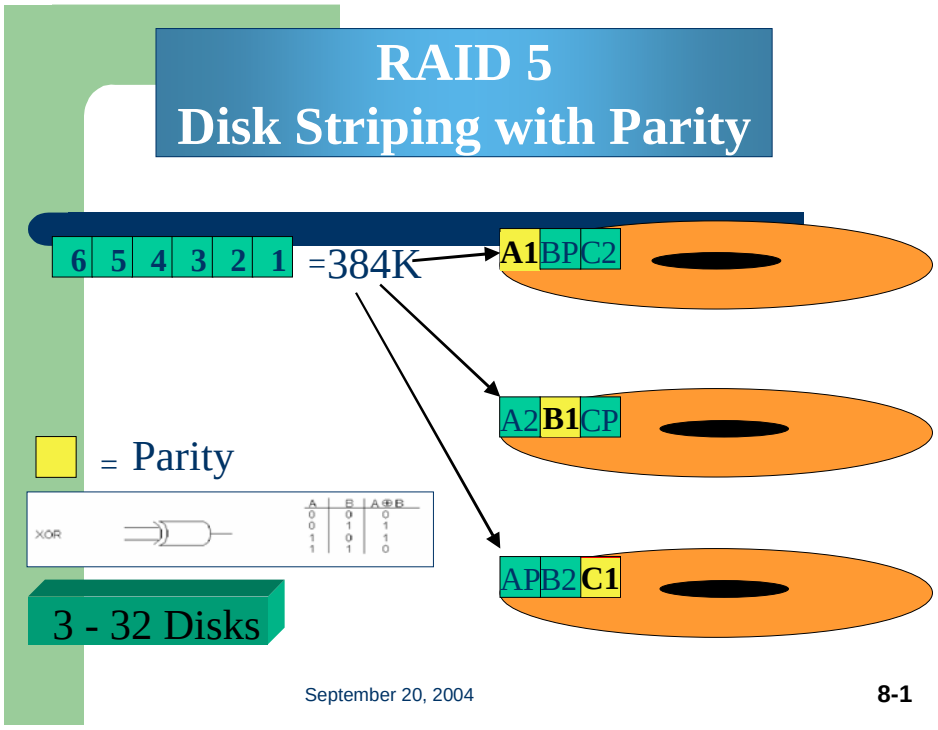
Backup Policy

Backup regime:

- **Media rotation / retention schedule**
- **Encryption, compression, and error-checking and correcting**
- **Automate backup**
- **Train operators**
- **Off-site storage**
- **Document policy and procedures**
- **Distribute policy to interested parties**
- **Full, Incremental, Differential**

RAID


RAID 0
Disk Striping
1 + 2 + 3 = 192
9 8 7 6 5 4
2 - 32 Disks
64K Blocks
64k
3
64k
2
64k
1
RAID 1
Disk Mirroring
9 8 7
6 5 4 3 2 1
6 5 4 3 2 1



Power Protection

- Power conditioning
  - Surges, Spikes, Brownouts, Sags
- Capacity planning
  - VA , Uptime

System Recovery Basics

- **Develop recovery plans and procedures**
- **Test initial system recovery measures**
- **Maintain system configuration information**

The Bigger Picture…

Purpose of Contingency Planning

- **Road map to recovery**
- **Minimize recovery period**
- **Minimize errors in decision making**
- **Minimize errors in implementation**
- **Identifies critical assets / processes**
- **Establish responsibilities**
- **Establish priorities and resources**

Contingency Planning Update

- **Obtain Commitment from Management**
- **Establish Planning Committee**
- **Conduct Capability Assessment**
- **Conduct Risk Analysis**
- **Establish Priorities**
- **Define Requirements for Plan**
- **Develop Plan**
- **Train for Plan**
- **Test Plan**
- **Update Plan**

Wireless Network Security

System Administrator/Network
Manager Security Course

Institute of Electrical & Electronic Engineers (IEEE) 802.11x

- Relevant protocols
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11i
  - 802.11n

IEEE 802.11a

- **(Wi-Fi)** Up to 54Mbps in the 5GHz band
- WEP & WPA
- Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.

IEEE 802.11b

- **(Wi-Fi)** Up to 11Mbps in the 2.4GHz band
- WEP & WPA
- Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.

IEEE 802.11g

- **(Wi-Fi)** Up to 54Mbps in the 2.4GHz band
- WEP & WPA
- Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.

IEEE 802.11i

- Security fix not a new bandwidth specification
- Supports 802.1x authentication, TKIP, & AES
- Referred to as WPA2
- Improved security enhancements over 802.11x.
- Compatible with 802.11x.

IEEE 802.11n

- boost 802.11a and 802.11b speeds to 108 Mbps and higher
- Backward compatible with 802.11x products
- Standard not finalized

Common Wireless LAN Vulnerabilities

- No configured security or poor security
- No set physical boundaries
- Physically insecure locations
- Untrained users setting up unauthorized workstations and access points
- Rogue access points
- Lack of network monitoring
- Insufficient network performance

Common Wireless LAN Vulnerabilities (cont.)

- MAC address filtering
- Inadequate encryption standards
- Off hours traffic/war driving
- Unauthorized data rates
- Easy to eavesdrop
- Man in the middle attacks
- Unsecured holes in the network
- Denial of Service (DOS) attacks

DoD Policy

- Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks and must comply with DoD 8500.1 and 8500.2 and be accredited in accordance with DoDI 5200.40

DoD Policy (cont.)

- For data, strong authentication, nonrepudiation, and personal identification is required for access to a DoD IS. Encryption of unclassified data for transmission to and from wireless devices is required. Encryption must be implemented “end to end”. Encryption must also meet FIPS 140-2 requirements.

Army Best Business Practice (BBP)

- Wireless LANs and PEDs with LAN connectivity must meet the same certification and accreditation security requirements as the wired LAN
- Wireless solutions will be engineered to preclude backdoors and trapdoors into the Army LANs
- All bridges must comply with FIPS 140-2 compliance
- Strong authentication required.
- ESSID/SSID broadcast option turned off

Army BBP (cont.)

- Wireless solutions must meet IA requirements
- Wireless as well as wired infrastructure must be accredited
- Encryption strength will be 128 bit 3DES or AES as a minimum
- Wireless devices used to extend the LAN environment shall support IA related security software, have a host based firewall, an approved anti-virus product installed, management application, and require user-unique authentication as absolute minimums

Standard for implementing a wireless LAN

- Must be certified FIPS 140-2 level 1 end to end encryption. 3DES or AES only
- Must protect OSI layer 2 (Data Link) with an approved FIPS 140-2 encryption module
- Must be able to detect and suppress rogue access points
- Must incorporate a location aware protection scheme

FIPS 140-2

- Standard that describes requirements IT products should meet for Sensitive, but Unclassified (SBU) use.
- Has 4 levels of security
- Covers areas related to the secure design and implementation of a cryptographic module.
- Establishes encryption requirements for 128bit 3DES, AES or better.

Wi-Fi Protected Access Version 2 (WPA2)

- Uses strong AES encryption based on Rijndael algorithm
- Has 128, 192, 256 bit key sizes
- 802.1x for user authentication and key distribution
- Has two strong authentication features
  - Wireless robust authentication protocol (WRAP)
  - Counter with cipher block chaining message authentication code protocol (CCMP)

Not approved for Army use

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access Version 1 (WPA)
- Temporal Key Integrity Protocol (TKIP)
- Encryption based on the RC4 encryption algorithm

- Encryption must be FIPS 140-2 compliant

DoD References

- DISA Wireless Security Technical Implementation Guide April 2004
- DISA Wireless LAN Security Framework Jan 2004
- DISA Wireless Security Checklist Nov 2004
- FIPS PUB 140-2 May 2001
- NIST Wireless Guidance SP 800-48 Dec 2002
- DoDD 8100.2 April 2004 **"Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)"**
- DoD 8500.1 "Information Assurance"
- DoD 8500.2 "Information Assurance Implementation"
- DoDI 5200.40 "DITSCAP"
- DoDD 8510.1-m "DITSCAP Application Manual"

Army References

- AR 25-2 "Information Assurance"
- AR 380-53 "Information Systems Security Monitoring"
- Army BBP Wireless Security Standards June 2004

QUESTIONS?

AIRCRACK PE

This practical exercise (PE) is designed to show you the advantage that increased encryption key size affords you. Most home users utilize what is known as Wired Equivalency Protocol (WEP). This protocol has an important function: It outlines a way to encrypt the data packets that travel over IEEE 802.11 networks. Unfortunately, WEP encryption is based on a symmetric stream cipher (RC4). As is true for all stream ciphers, it's important that each packet have a different WEP secret key. The WEP standard specified the use of different keys for different data packets, which is a very good idea. This approach relied on the use of so-called initialization vectors (IVs). Originally, these IVs were intended to be unique for each packet. But the space of possible vectors was too small to avoid duplications. As a result, the IVs had to be reused. When an IV is reused, an attacker will yield the plain text. We are going to use this IV problem to decipher the encrypted key of wireless communications.

We will examine data capture that utilized a 40 bit WEP key and then a 104 bit key. See if you can spot the difference in effectiveness.

This PE will be using Linux and Linux tools to crack the key. First we will start by copying some data capture files onto our hard drive using XP Pro.

1. Using XP Pro, insert the disk labeled “air captures” into your CDROM drive.
2. Copy the two files to your XP Pro drive
    a. outfile-07min-40bit-key.cap
    b. outfile-15min-104bit-key.cap
3. Once you’ve copied the files, remove the “air captures” CDROM and replace it with the provided Linux boot disk.
4. Left-click on the start button and restart your computer
5. Your computer should start booting up in Linux.
6. Once the system boots up you’ll be asked to log in. Type: **root** (hit enter).
7. You’ll be presented with a # prompt. Welcome to the command line.
8. First we have to be able to access the files you copied over to the XP Pro drive.
9. Create a directory to mount the drive to. Type: **mkdir /mnt/hda?** (where ? is the number of the partition that XP Pro resides on. For example the c: drive would be hda1)
10. Now mount the drive to the new directory.
    a. Type: **mount –t ntfs /dev/hda? /mnt/hda?**

11. If it worked, your prompt should come back and you should not get any message. If you get a message to the contrary, try changing the number you used instead of ? to identify the proper partition number.

12. Type: **cd /mnt/hda?**

13. Type: **ls**

14. Did you see the files you copied over? _____

15. The two files represent two separate captures of wireless traffic. One is a 40bit capture of 7 minutes of data and one is a 15 minute capture of 104 bit traffic

16. We will use aircrack to crack the encryption of the initialization vectors used in sending the wireless packets.

17. Type: **aircrack –n 64 ./outfile-07min-40bit-key.cap**

18. Was the key successfully cracked? _____

19. Did it take a long time? _____

20. Lets try a tougher key this time.

    a. Type: **aircrack –n 64 ./outfile-15min-104bit-key.cap**

21. What was the result this time? _____

22. Can you make any conclusions at this point?_____

23. The 104bit sampling provided twice as much data but still proved to be beyond the capabilities of aircrack. FIPS 140-2 compliancy requires a 128bit AES encryption strategy.

24. Lets take a peek at the capture and locate the initialization vector that is being decrypted.

25. At the # prompt type: **startx**

26. The Xwindows program will startup and you will be in what is known as the KDE window manager. In the lower left corner you'll see a K in a gear sprocket. This is the equivalent of the windows start button. **Left-click** on the K

27. A menu will pop up, **left-click** on the security toolbox

28. **Left-click** on the network traffic analyzer (Ethereal)

29. **Left-click** in the upper left corner on file

30. **Left-click** on open

31. **Double left-click** on filesystem to open up the file system

32. in the right window pain, **double left-click** on mnt

33. **Double left-click** on hda? (the directory you created and mounted the drive to). This should open up the XP Pro home directory for viewing

34. **highlight** the outfile-07min-40bit-key.cap file

35. **click open**

36. The capture should be displayed. You may get a message stating the capture stopped in the middle of a packet, if so **click ok** as this is normal.

37. look in the packet captures and **highlight** one from an intel source (NIC card)

38. In the middle window, **left-click** on the directional arrow next to IEEE 802.11. This will open up the data for viewing

39. **Left-click** on the directional arrow next to WEP parameters.

40. When this opens up you should see the initialization vector. This hexadecimal value is what is being decrypted to find the key.

41. Go ahead and close the program by **left-clicking** the x in the upper right corner of the window.

42. **Left-click** on the K button in the lower left corner of the screen and **select** logout.

43. **Left-click** on end session to go back to your shell prompt

44. At the # prompt type: **reboot**

45. Take out the Linux CDROM during reboot and reboot into XP Pro

46. End of PE

ading assignment 2

Subject: **Defense in Depth, and Router Intro**

Pages: 3-21, 26-37, 42-43

(Complete before day 3)

1. Briefly define the following in your own words:

   der Router:

   wall:

   :

   N:

   Z:

   eened Subnet:

   xy:

   figuration Management:

2. the range of numbers used to define a standard vs. extended access list, and explain the primary differences of each.

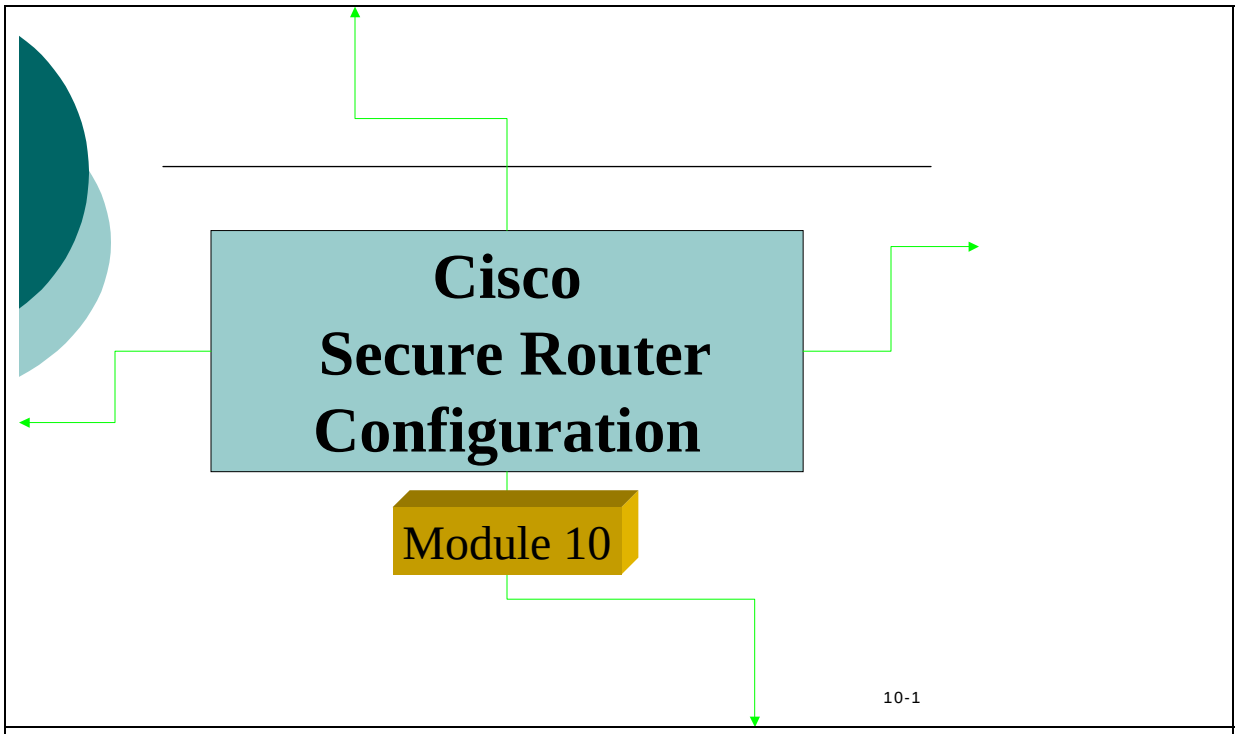
3. ine "Implicit Deny." And describe where it occurs in an access list.

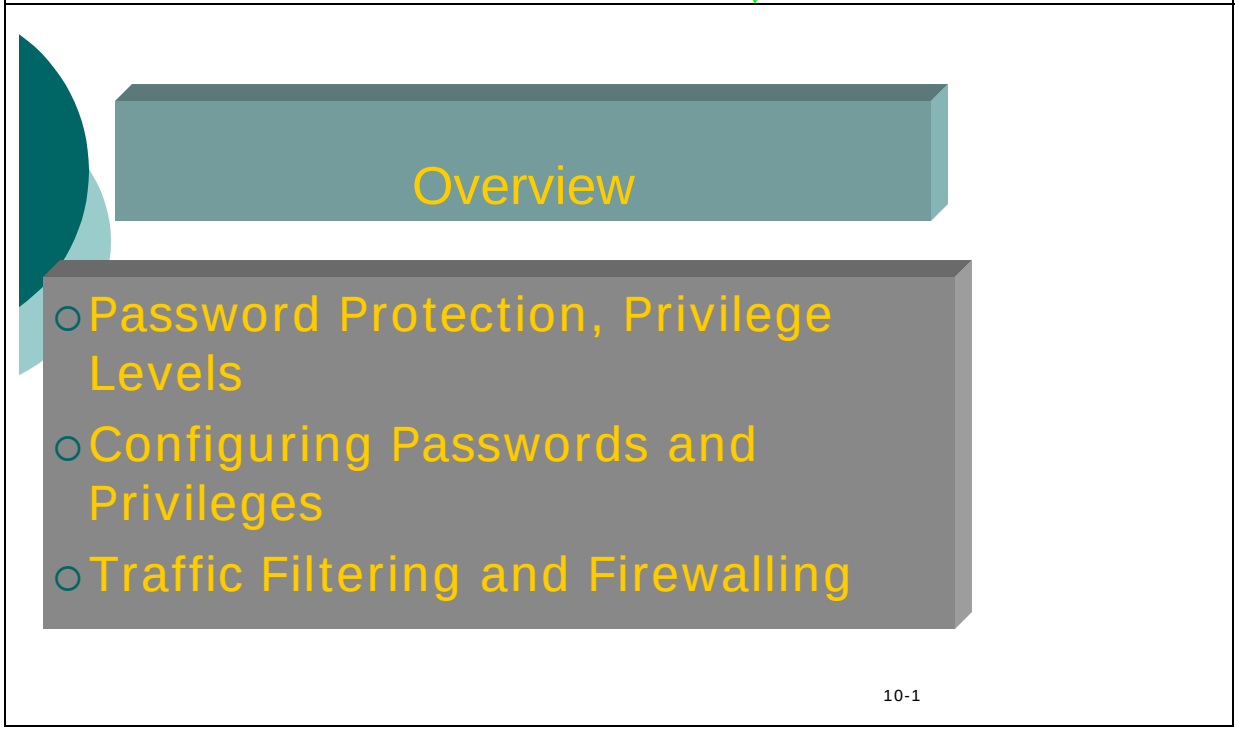
4. y use an ACL on a router when you have a high-tech firewall right behind it?

5. 
en you create a group of IP addresses to always be denied by your ACLs, what is this group sometimes called?

6. 
at does an ingress filter protect, and what does it protect it from?

7. 
at does an egress filter protect, and what does it protect it from?


Cisco
Secure Router
Configuration
Module 10
10-1

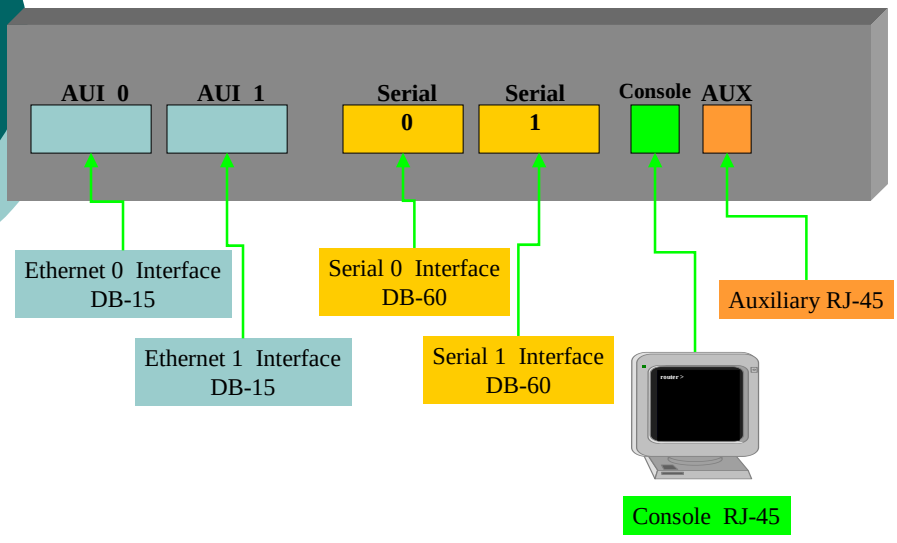

Overview
Password Protection, Privilege Levels
Configuring Passwords and Privileges
Traffic Filtering and Firewalling
10-1

Cisco 2500 Series Router

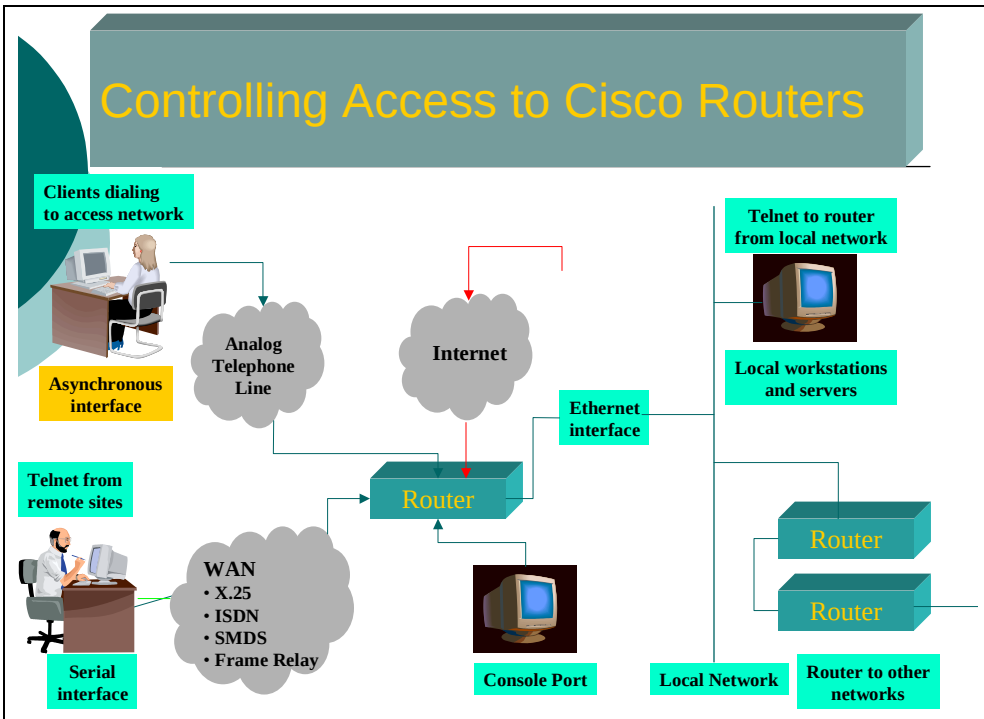
- Primary function is to route network traffic
- Secondary function is to provide packet filtering capabilities for network traffic control and security
- Best suited for small network environments

10-1

Back of Model 2514 Router



10-1



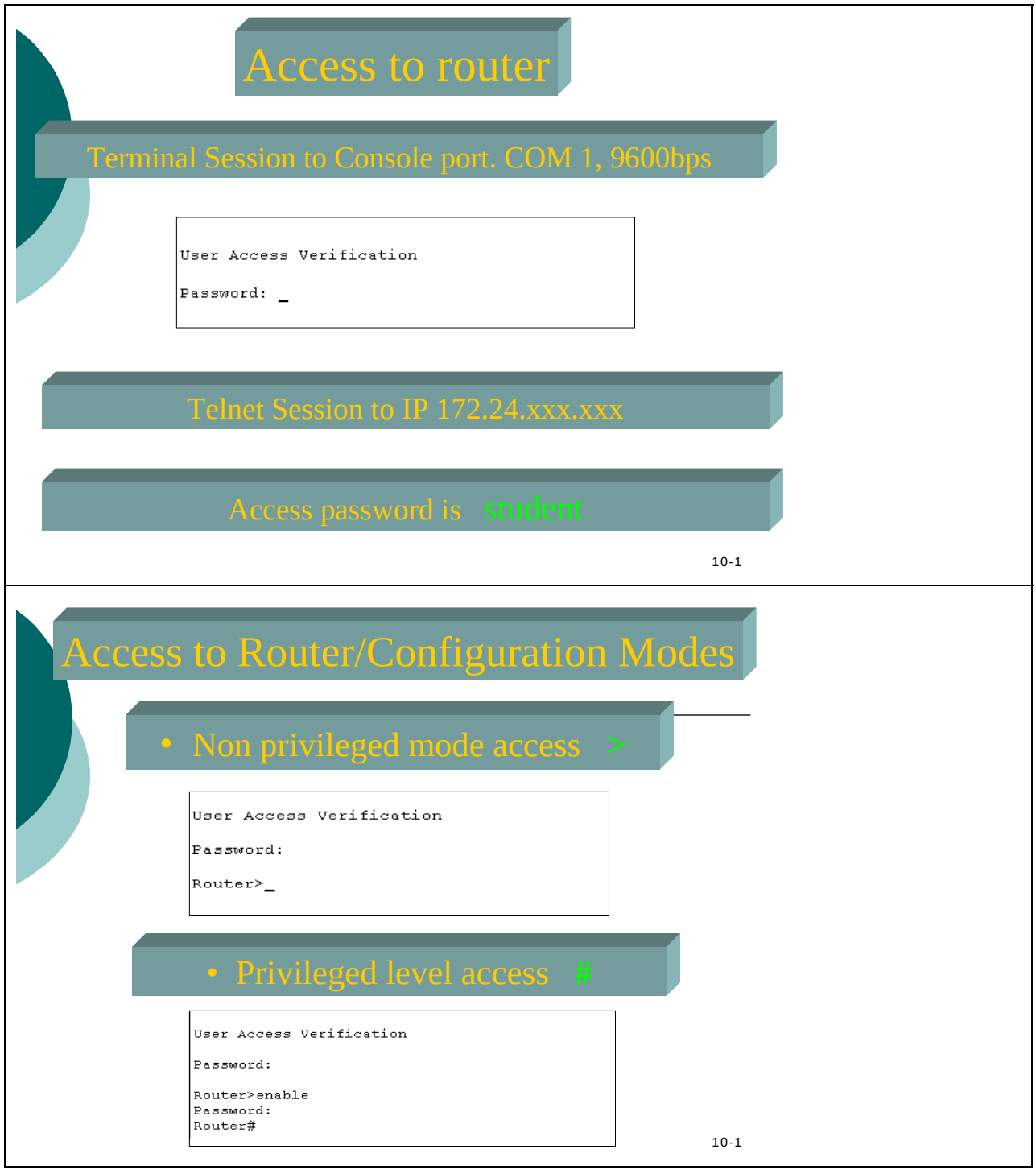
Two Types of Password Access Control Password & Secret

Sniffers can examine packets (and read passwords), you can increase access security by configuring the Cisco IOS software to encrypt passwords. Encryption prevents the password from being readable in the configuration file

- Enable password is **NOT** encrypted
- Secret password is encrypted (MD5)

When enable password and enable secret are both set, users must enter the enable secret password

10-1


Access to router
Terminal Session to Console port. COM 1, 9600bps
User Access Verification
Password: _
Telnet Session to IP 172.24.xxx.xxx
Access password is student
10-1
Access to Router/Configuration Modes
• Non privileged mode access >
User Access Verification
Password:
Router>_
• Privileged level access #
User Access Verification
Password:
Router>enable
Password:
Router#
10-1

Access to Router/Configuration Modes

- Global configuration mode access

```
Router # config t
Router (config) #
```

- Interface configuration mode access

```
Router (config) # int f 0/0
Router (config-if) #
```

10-1

Note: If you need help

```
Router # ?

Exec commands:
  atmsig           Execute Atm Signalling Commands
  cd               change current device
  connect          Open a terminal connection
  dir              List files on given device
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  name-connection  Name an existing network connection
```

10-1

Access to Router

- Privileged level access #
- 16 different privilege levels 0-15
- 15 is the default fully privileged level

Establishing default fully privileged level password

Router (Config) # enable password *student*

OR

Router (Config) # enable secret *instructor*

10-1

Access to Router

Establishing intermediate privilege level passwords

Router (Config) # enable password level 5 *private*

OR

Router (Config) # enable secret level 5 *new_user*

10-1

Defining Level Command Access

- New levels will have normal user exec mode access by default
- To define access privileges to the ping and trace command for level 5, use the following command:

```
Router (Config) # privilege exec level 5 ping
Router (Config) # privilege exec level 5 trace
```

10-1

After defining level command access and setting passwords, the next step is to control console, auxiliary and vty (telnet) access.

To verify that the changes we have made are active, type the following command:

```
Router # show running-config
```

To view the original settings when the router booted up, type the following command:

```
Router # show startup-config
```

10-1

Controlling Console, Aux & Vty Access

- Restrict access to console port

```
Router (Config) # line console 0
Router (Config-line) # login
Router (Config-line) # password student
```

- Restrict access to auxiliary port

```
Router (Config) # line aux 0
Router (Config-line) # login
Router (Config-line) # password dialup
```

10-1

Controlling Console, Aux & Vty Access

- Restrict telnet access to vty terminals
- Each ethernet access port on a Cisco router is called a virtual terminal (vty)
  - Cisco routers can have a maximum of 5 virtual terminal ports numbered 0 - 4

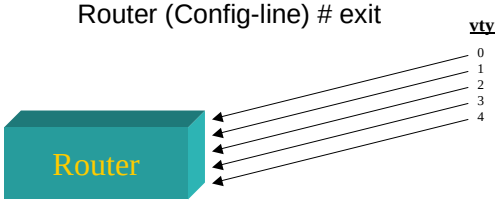
```
Router (Config) # line vty 0 4
Router (Config-line) # login
Router (Config-line) # password student
```

10-1

Controlling Console, Aux & Vty Access

Tip: You may wish to limit the amount of available vty ports (default of 5 may be too many). Use the "transport input none" command to accomplish this.

```
Router (Config) # line vty 0 1
Router (Config-line) # transport input none
Router (Config-line) # exit
```



10-1

Controlling Console, Aux & Vty Access

Tip: As administrator you may wish to protect one of the remaining vty ports for your private use only. Do the following to reserve your own vty port.

```
Router (Config)# line vty 2 3
Router (Config-line)# login
Router (Config-line)# Password telnet_users
Router (Config-line)# exit
Router (Config)# line vty 4
Router (Config-line)# login
Router (Config-line)# password MyBackDoor
```

10-1

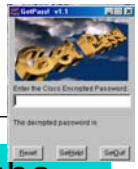
Protecting Console, Aux & Vty Access

Now that we've set passwords on all the access ports we have to protect the password passwords from being discovered. The following command will encrypt the enable password password. Note: The enable secret password is already encrypted.

```
Router (Config) # service password-encryption
```

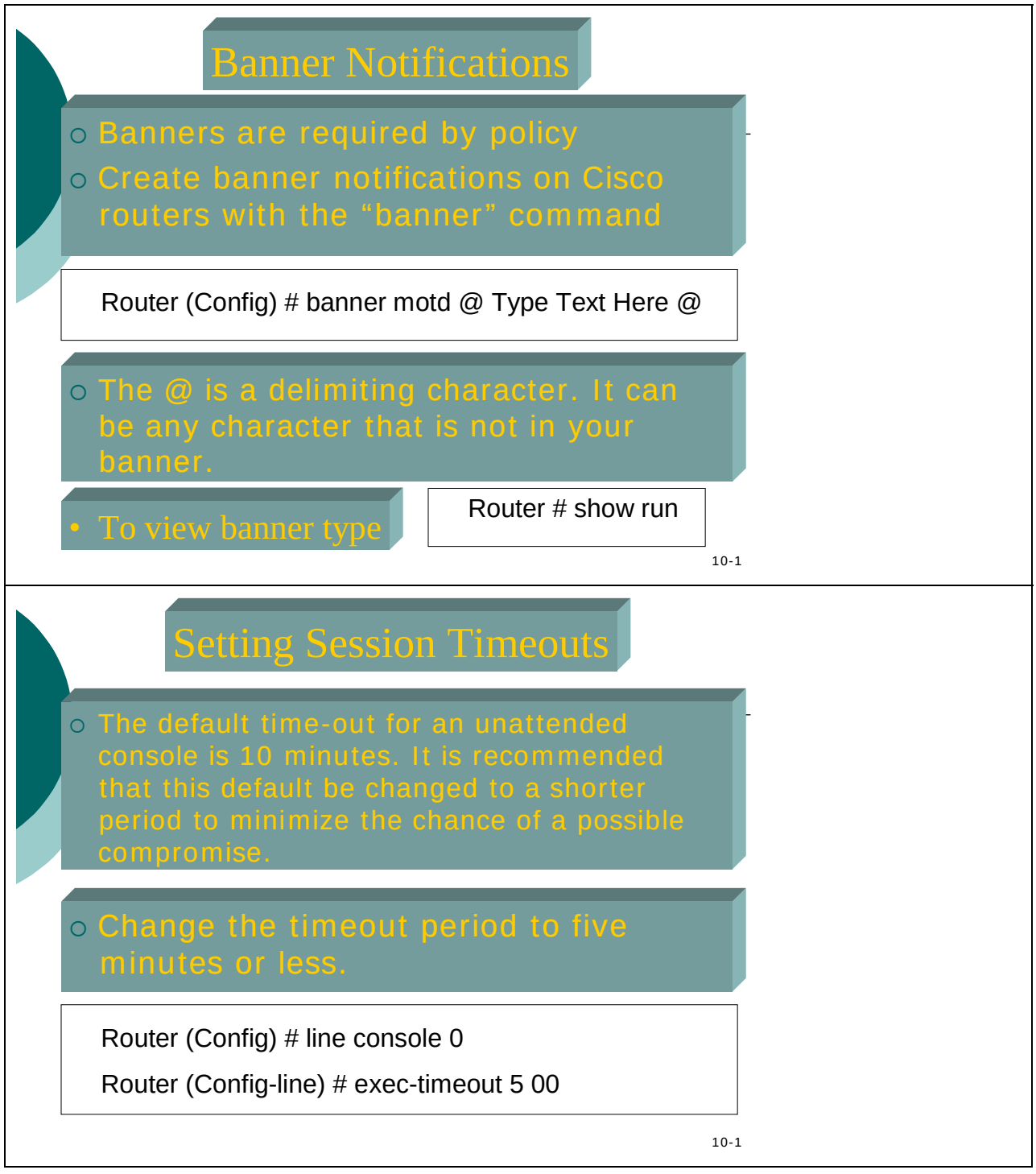
10-1

Cisco Password Hacks



- Programs are readily available on the Internet which are capable of decrypting user passwords on Cisco routers
  - Not capable of decrypting enable secret ????
  - Can decrypt passwords using the standard Cisco encryption scheme
- It is very important to maintain strict control of configuration files

10-1


Banner Notifications
Banners are required by policy
Create banner notifications on Cisco routers with the "banner" command
Router (Config) # banner motd @ Type Text Here @
The @ is a delimiting character. It can be any character that is not in your banner.
To view banner type
Router # show run
10-1
Setting Session Timeouts
The default time-out for an unattended console is 10 minutes. It is recommended that this default be changed to a shorter period to minimize the chance of a possible compromise.
Change the timeout period to five minutes or less.
Router (Config) # line console 0
Router (Config-line) # exec-timeout 5 00
10-1

Mid-Break Summary

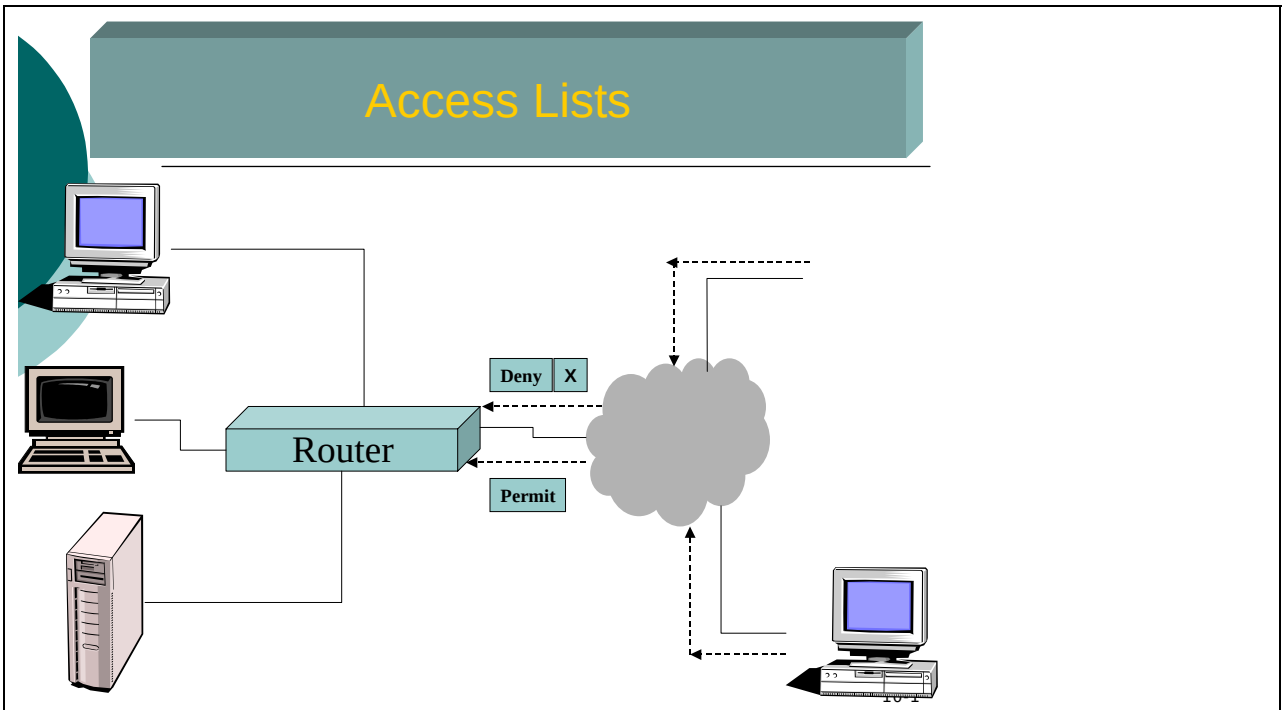
We talked about the following security controls:

1. Password password & Secret Password
2. Password restrictions for privilege level access.
3. Setting command access for privilege levels.
4. Access control to Console, Aux and Vty ports.
5. Creating a warning banner for implied notification.
6. Setting a session timeout for inattentive administrators

10-1

Access Lists

10-1

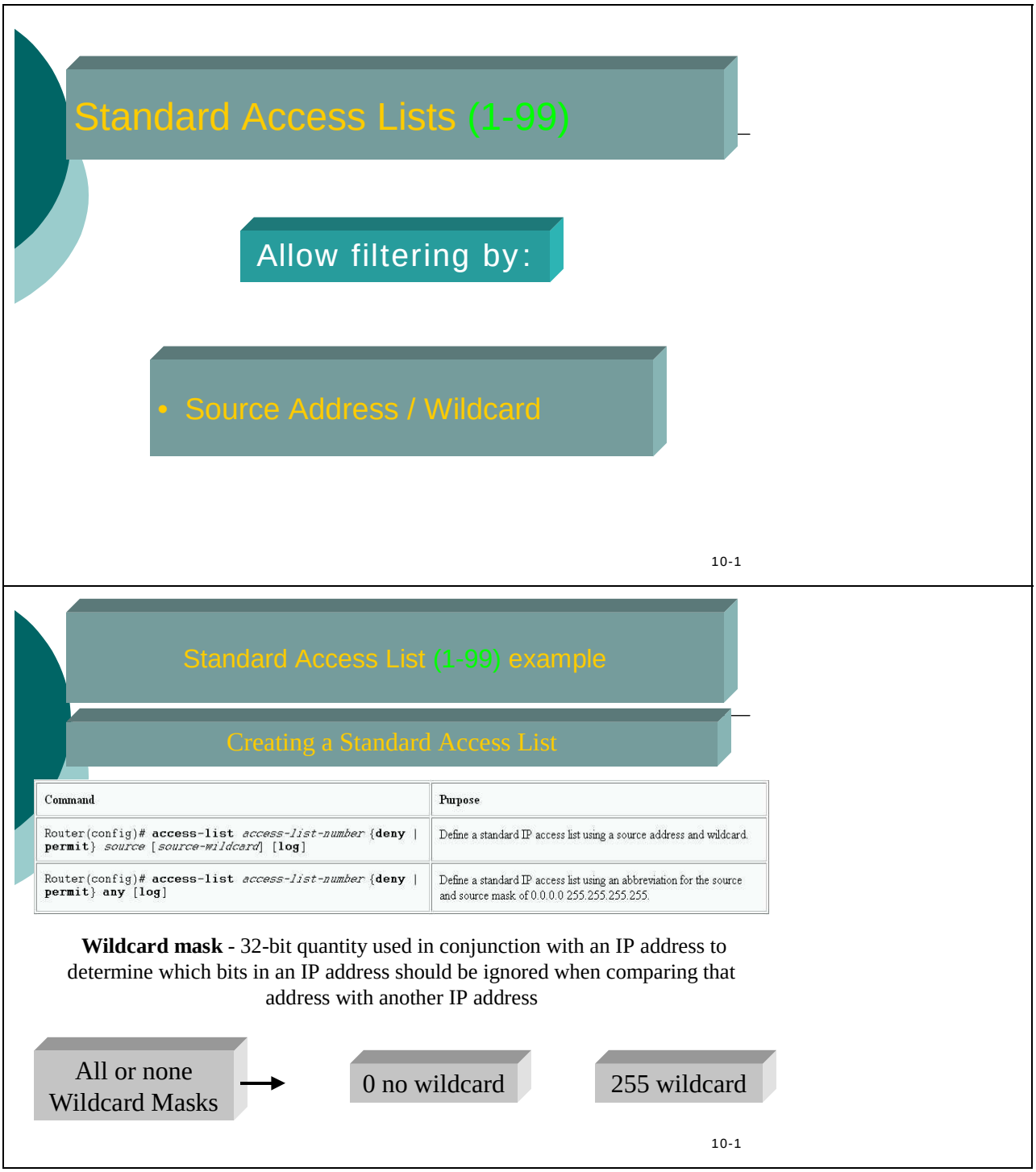


Why Use Access Lists?

By default, if there are no access lists… all packets will be allowed to any part of your network. You can enhance security and improve network performance by providing control over the traffic forwarded through or blocked from your network

Cisco access lists default to an implicit deny statement for everything that has not been permitted. This supports a deny all and allow
only as needed security policy.

10-1


Standard Access Lists (1-99)
Allow filtering by:
• Source Address / Wildcard
10-1
Standard Access List (1-99) example
Creating a Standard Access List
Command
Purpose
Router(config)# access-list access-list-number {deny | permit} source [source-wildcard] [log]
Define a standard IP access list using a source address and wildcard.
Router(config)# access-list access-list-number {deny | permit} any [log]
Define a standard IP access list using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255.
Wildcard mask - 32-bit quantity used in conjunction with an IP address to determine which bits in an IP address should be ignored when comparing that address with another IP address
All or none Wildcard Masks
0 no wildcard
255 wildcard
10-1

Standard Access List (1-99) example

Applying a Standard Access List to a virtual terminal line

access-class

Command	Purpose
Router(config-line)# **access-class** *access-list-number* {**in** | **out**}	Restrict incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list.

Applying a Standard Access List to an interface

access-group

Command	Purpose
Router(config-if)# **ip access-group** {*access-list-number* | *name*} {**in** | **out**}	Control access to an interface.

10-1

Standard Access List (1-99) example

Case 1

Create an access list that will only allow IP source addresses 192.168.12.42 and 192.168.12.55 to enter an interface.

Case 2

Create an access list that will deny only the IP source networks 192.168.12.0 and 192.168.13.0 from entering an interface.

Case 1 Solution

```
Router (config) # access-list 1 permit 192.168.12.42 0.0.0.0
Router (config) # access-list 1 permit 192.168.12.55 0.0.0.0
```

Case 2 Solution

```
Router (config) # access-list 2 deny 192.168.12.0 0.0.0.255
Router (config) # access-list 2 deny 192.168.13.0 0.0.0.255
Router (config) # access-list 2 permit any
```

Access Lists

Access lists are processed in sequential order

Access lists cannot be edited on the router. For long access lists, create offline on a text editor, then copy and paste on the router

10-1

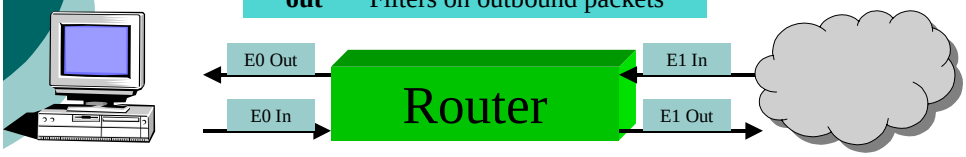
Standard Access List (1-99) example

Subnet

in Filters on inbound packets.

out Filters on outbound packets

Internet

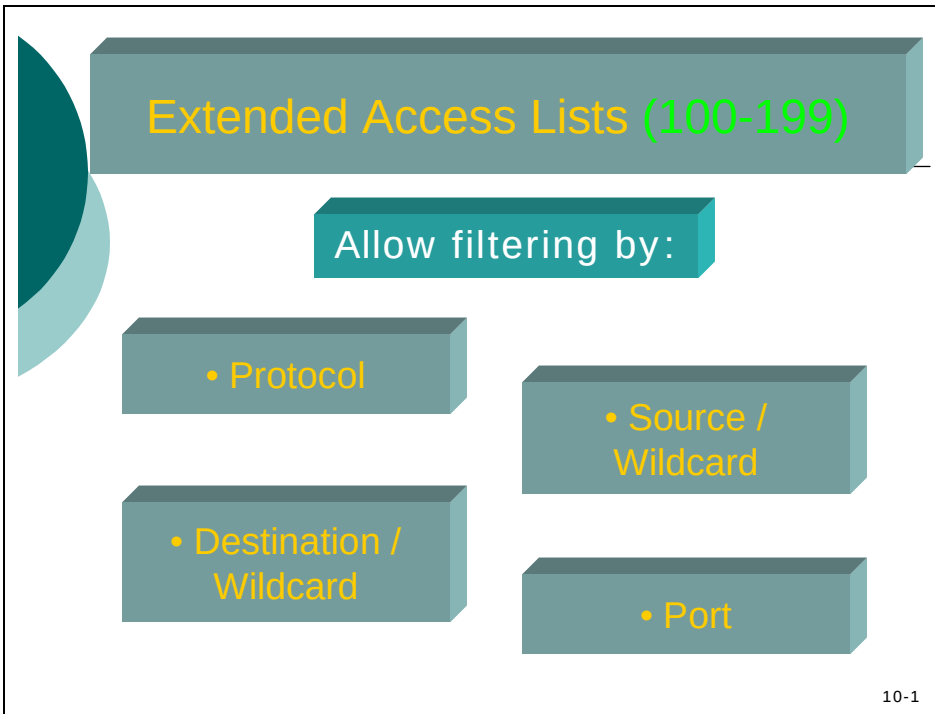


Note: You can only apply one of each type of access list per group and/or class, per interface. Remember, traffic flows both ways on an interface.

Applying Case 2 access-list

```
Router (config) # interface f 0/1
Router (config-if) # ip access-group 2 in
```

10-1



Extended Access Lists (100-199)

Router (config) # access-list [*access-list-number*] {permit | deny} [*protocol*] [*source*] [*source-wildcard-mask*] [*destination*] [*destination-wildcard-mask*] [*operator*] [*port*]

- Access-list-number = 100-199
- Protocol = IP, TCP, UDP, ICMP
- Source = Source IP Address
- Source-Wildcard-Mask = Assign Wildcard Bits
- Destination = Destination IP Address
- Destination-Wildcard-Mask = Assign Wildcard Bits
- Operand = lt (Less than) gt (Greater than) eq (equal to) neq (Not equal to)
- Port = Port numbers and/or range of port numbers you wish to specify
- **Established = For the TCP protocol only: to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set**

Extended Access Lists (100-199)

Case 1 — Create an access list that will allow access to TCP port 80 on an interface and deny all UDP traffic.

Case 2 — Create an access list that will deny the TCP protocol on ports 135 and 139 from entering an interface and allow all other protocols and ports.

Case 1 Solution

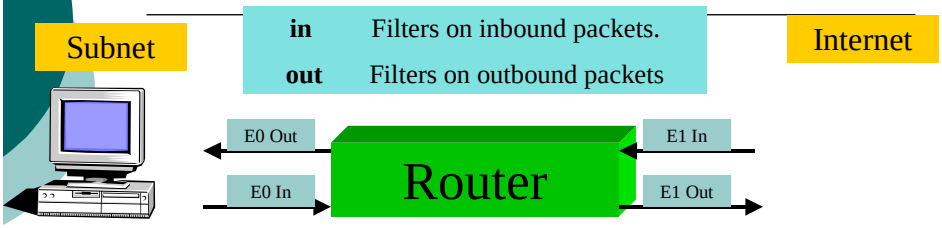
```
Router (config) # access-list 101 deny udp any any
Router (config) # access-list 101 permit tcp any any eq 80
```

Case 2 Solution

```
Router (config) # access-list 102 deny tcp any any eq 135
Router (config) # access-list 102 deny tcp any any eq 139
Router (config) # access-list 102 permit ip any any
```

10-1

Extended Access Lists (100-199)



Note: you can only apply one of each type of access list per group and/or class, per interface. Remember, traffic flows both ways on an interface.

Applying Case 2 access-list

```
Router (config) # interface f 0/1
Router (config-if) # ip access-group 102 in
```

10-1

To view access lists

Router# **show access-lists**

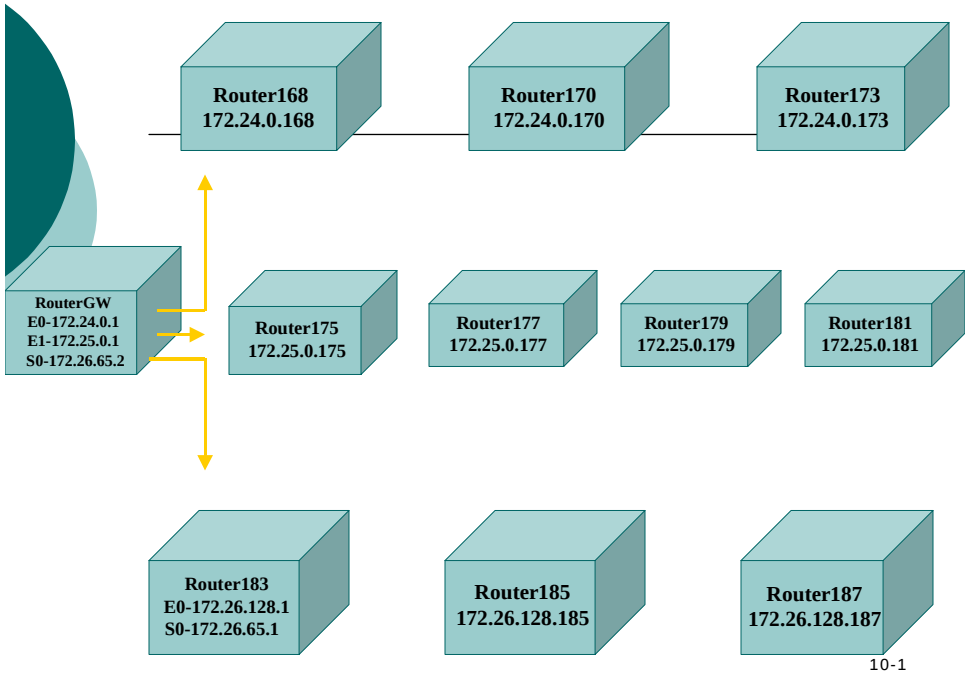
10-1

Removing access groups and access lists

Router # config t
Router (config) # int f0/1
Router (config-if) #no ip access-group 2 in
Router (config-if) #exit
Router (config) #no access-list 2
Router (config) #<Ctrl> <Z>

It is important to remove the list from the interface before removing the access-list itself. If the access-list were to be deleted before it is removed from the interface, corruption of data could occur

10-1



10-1

Questions

10-1

Router Security

Lesson 3

This practical exercise is intended as a supplement to material learned during the Router lecture. Students will become familiar with concepts and commands necessary to operate and secure a Router. Students will become familiar with creating and applying Standard and Extended Access-lists.

Objectives

1. Inspect and change router configurations.
2. Setup and maintain Standard Access-lists.
3. Setup and maintain Extended Access-lists.
4. Recover lost passwords.

Practical Exercise 1

Privilege Levels

The purpose of this PE is to guide you through configuration of privilege level passwords on a router and to familiarize you with the user mode.

1. From the user mode (>) Enter the command: **?**
   Notice the limited amount of commands. This is privilege level-1. All privilege levels from 1-14 will only have privilege level 1 commands unless other commands are added. Privilege level (0) can also be edited.

2. Open Notepad, then copy and paste all of the commands in the list to it. Save this list as **priv-lvl-1.txt**.

3. Enter the command: **enable**
   (Password is student)
   What mode have you just entered?
   What privilege level are you now at?

4. Enter the command: **?**
   Do the same as in step 2 above and save to **priv-lvl-15.txt**. Now compare the lists. Which list gives you the most commands?

5. Enter the command: **show running-config**

6. Enter the command: **configure Terminal**
   What mode are you now in?

7. Enter the command: **?**
   Compare this list to the commands in priv-lvl-15.txt. As you can see, the command list is different for each mode.

8. Enter the command: **enable password level 6 cisco**
   Explain what this command sets for the router:

9. Enter the command: **privilege exec level 6 debug**
   privilege exec level 6 reload
   What have these commands done?

10. Enter the command: **CTRL-Z** (This means hold down the control key, and press Z)
    Enter the command: **show running-config**
    Verify your changes by looking for the privilege commands in the configuration.

11. Enter the command: **Exit**
    Press **ENTER** to get back to the > prompt.
    What privilege level are you in now?

12. Enter the command: **Enable 6**
    Are you prompted for a password ?
    Which password works with this command?
    What type of prompt do you have now?

13. Enter the command: **?**
    Are there any extra commands added? (Compare to priv-lvl-1.txt)

14. Enter the command: **Exit**

Practical Exercise 2

ssword Management

You can control access to your router and to the use of privileged commands through the use of passwords. We will be setting passwords for console, VTY, and the enable secret. We will also encrypt all the passwords on the router.

Setting the console terminal password.

1. Set the console password to **con_user** by entering the following commands:

   Router>**enable**
   Password: **student**
   Router#**config t**
   Router (config) #**line console 0**
   Router (config-line) #**login**
   Router (config-line) #**password con_user**
   Router (config-line) #<**CTRL-Z**>

2. Type **exit** and ensure that the password has been changed by logging back into the router.

Setting the password for telnet connections.

3. Set the vty 0-4 passwords to **telnet_user** by entering the following commands:

   Router#**config t**
   Router (config) #**line vty 0 4**
   Router (config-line) #**login**
   Router (config-line) #**password telnet_user**
   Router (config-line) #<**CTRL-Z**>

4. Now **exit** and verify the password was successfully changed by telneting to the Router. (Remember, if you decide to telnet from the console, you will have to enter the console password first)

Take a look at the running configuration file:

Router# *show running-config*

Are the passwords you just set viewable in clear-text?  **S/NO**

Encrypting all passwords.

5. Encrypt the passwords by entering the following command:

   Router#**config t**
   Router (config) #**service password-encryption**
   Router (config) #**<CTRL-Z>**

Let's take another look at the running configuration file:

Router# ***show running-config***

Are the passwords you just set viewable in clear-text? **YES/** 

Changing the Secret password.

6. Set the Secret password to **Roscoe** by entering the following commands: (The Enable Secret password will override the Enable password for privileged level access)

   Router#**config t**
   Router (config) #**enable secret Roscoe**
   Router (config) #**<CTRL-Z>**

7. Now **exit** and verify the password was successfully changed. (Remember the console password from earlier, you will still need it before you can check your new Enable Secret.)

Take a third look at the running configuration file:

Router# show running-config

Is there a difference between the encrypted **Password** password and the **Secret** password?
 **S/NO** Explain:

_____

_____

Practical Exercise 3

Banner Creation Configuration

The purpose of this lab is to show you how to use the banner commands to create specific login banners.

Create a login banner that is viewable while gaining terminal access to your router.

You must be in global configuration mode to configure a banner.

Router (config) # **banner motd @** <Hit Enter>

"THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."
@ *< Hit En**ter**>*

Router (config) #

Now exit and log back in to verify the functionality of your banner. Have another person telnet into your router to verify the functionality of it.

After verifying the functionality of the banner, continue to PE 4.

Practical Exercise 4

Standard Access List (SAL) Configuration

Objective: Configure a SAL to block a network and activate the access-group for inbound traffic.

1. Choose one network in your classroom to be a trusted network. Once you have the IP and wildcard mask figured out for that network, use them in the following commands to ensure that they are the only network allowed to send data into yours. You also need to decide which interface(s) to apply the access-list to. Fill in the blanks below, enter the Global Configuration, and type the following: (note that steps **d** and **e** may not be necessary if you only need to apply this to one interface)

   a. Router (config) # **access-list 1 permit _____ _____**
   b. Router (config) # **interface _____ ____**
   c. Router (config-if) # **ip access-group 1 in**
   d. Router (config-if) # **interface _____ ____**
   e. Router (config-if) # **ip access-group 1 in**
   f. Router (config-if) # **Ctrl Z**

2. Once you have applied your access list, try to "**PING**" one of the IPs in a blocked network. Were you successful? **Yes /** 

3. Now "**PING**" one of the IPs you allowed. Were you successful?  **/ No**

4. Use the "**show access-list**" command from the Privileged Mode prompt to look at your access-list.

5. Once the **instructor** has verified that the access list is working you need to remove the access list. Fill in the blanks below, and use these commands. Remember: If you only applied to one interface, then some of these steps aren't needed.
   Router (config) # int ____
   Router (config-if) # no ip access-group 1 in (This removes the list from the interface)
   Router (config-if) # int ____
   Router (config-if) # no ip access-group 1 in (This removes the list from the interface)
   Router (config-if) # exit
   Router (config) # no access-list 1 (This deletes the entire list)
   Router (config) # <Ctrl-Z> (This means press the "control" and "z" keys together)

It is important to remove the list from the interface before removing the access-list itself. If the access-list were to be removed before it is removed from the interface, corruption of data could occur.

6. After removing the access-lists, try to "**PING**" one of the routers in the other networks. Were you successful?  **/ No**

Practical Exercise 5

Standard Access List (SAL) Configuration #2

Objective: Configure a SAL to block two specific IP address **within** trusted networks, and activate the access-group on your router.

Choose 2 networks in the classroom to be the **only trusted networks**.
Choose 1 computer IP address **from each** of those networks to be **untrusted systems**.

We need to develop an access list with the following definitions being true:

A. Permit access from any trusted networks.
B. Deny access from all untrusted addresses.

You now have the required information to create the SAL. Keep the untrusted addresses from entering your router and allow the trusted networks access to your router. All other networks that have not been defined as trusted are to be considered untrusted. Fill in the blanks with the appropriate commands.

Fill in the blanks, and then enter the commands into your router from Global Configuration Mode. (All lines and blanks may or may not be necessary)

Router (config) # **access-list** ____ _____ _____ _____
Router (config) # **access-list** ____ _____ _____ _____
Router (config) # **access-list** ____ _____ _____ _____
Router (config) # **access-list** ____ _____ _____ _____
Router (config) # **access-list** ____ _____ _____ _____
Router (config) # **interface** _____ ____
Router (config-if) # **ip access-group** ____ ____
Router (config) # **interface** _____ ____
Router (config-if) # **ip access-group** ____ ____
Router (config-if) # **Cntrl Z**

After applying your access list, have the untrusted addresses try to access your router. (Telnet and/or Ping) Were they successful? **Yes /** 

The **instructor** will verify that your access list is working.

Now, pick the first network you allowed and deny the other host on that network. (Hint: A text editor might prove useful)

The following instructions will walk you through the basics on it:

Router#**sh run**

(From this prompt you may copy/paste the ACL to notepad, and edit the ACL to add the new host that you want to deny.)

Now, remove the old ACL, and put the new one back in its place. (note that all of these commands may not be necessary if you only placed an ACL on one interface.)
This removes it: (Fill in the blanks first, then perform the steps on your router)

Router#**config t**
Router (config) # **int ____**
Router (config-if) #**___ip access-group _____ in** (Remove the list from the first interface)
Router (config-if) # **int ____**
Router (config-if) # **___ip access-group 1 in** (Remove the list from the second interface)
Router (config-if) # **exit**
Router (config) # **___access-list ____** (Delete the entire list)

Time to add it back:

Router (config) #
(From this point, recall how you placed the access list the first time, and do it again.)

Configure an ACL for your VTY connections. Use the second trusted network and only allow VTY connection from that network.

Fill in the blanks, and then enter the commands into your router from Global Configuration Mode. (All lines and blanks may or may not be necessary)

Router (config) # **access-list ____ _____ _____ _____**
Router (config) # **access-list ____ _____ _____ _____**
Router (config) #**line vty** _____
Router (config-line) #**access-**_____ _____ _____
Router (config-if) # **Cntrl Z**

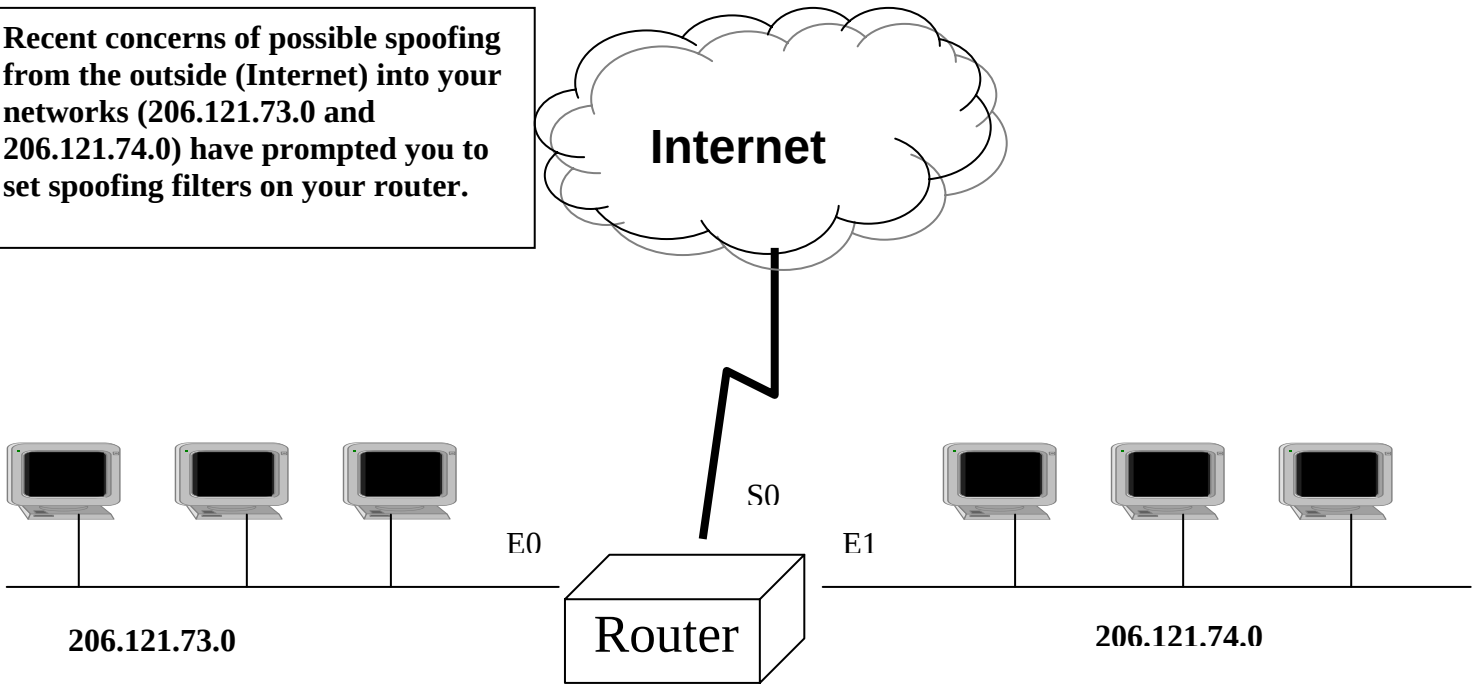
Practical Exercise 6

Spoofing Filter

Note: This will be covered in discussion. DO NOT APPLY THIS TO YOUR ROUTER!

Objective 1: Configure a SAL to prevent untrusted networks from spoofing inside addresses.
Objective 2: Configure a SAL to prevent your inside trusted networks from spoofing other outside networks.

Recent concerns of possible spoofing from the outside (Internet) into your networks (206.121.73.0 and 206.121.74.0) have prompted you to set spoofing filters on your router.



What statements must be included in your access list to prevent your internal networks from being spoofed? (Only write out the entries that apply to the problem above, don't worry about the whole list.)

Router(config)#_____

Router(config)#_____

What port(s) will you apply the access-list to?_____ Will it be applied inbound or outbound?_____

Can you prevent inside users from spoofing out? _____ If so, show how?
(Remember, maximum security.)

Router(config)#_____

Router(config)#_____

What port(s) will you apply the access-list to?_____ Inbound or outbound?_____
NOTE: Answers may vary!

Practical Exercise 7

Extended Access List (EAL) Configuration

Objective: Configure an EAL to block certain TCP/IP services from specified networks, and apply the EAL on the interface(s) of the router.

1. Configure an EAL on your router for traffic coming in from connected networks.

A. Allow certain addresses to Telnet (port #23) to your network (pick a few IPs in the room).
B. Block all Telnet (port #23) traffic from all other networks.
C. Allow Pings (ICMP Echo Packets) from only certain addresses (pick a few IPs in the room).
D. Deny all other ICMP traffic to enter your router.
E. Once you have decided on the IPs, fill in the blanks below, and apply to your router.

Router # **config t**
(repeat the next step for all IP addresses you want to allow to telnet to your router)
Router (config)# **access-list 101 permit tcp _____ _____ any eq 23**
(this will deny everybody else)
Router (config)# **access-list 101 deny tcp any any eq 23**
(specify the IPs you want to allow to ping to you)
Router (config)# **access-list 101 permit icmp _____ _____ any**
(allow ICMP replies to work)
Router (config)# **access-list 101 permit icmp any any echo-reply**
(block all other ICMP)
Router (config)# **access-list 101 deny icmp any any**
(allow anything else not specified above to work)
Router (config)# **access-list 101 permit ip any any**
(repeat the next two lines for any interfaces this should be applied to)
Router (config)# **interface _____ ____**
Router (config-if)# **ip access-group 101 in** (applies the access list 101 to the interface)
Router # **<Ctrl> Z**

2. Once you have completed loading your Extended Access List do the following:

Have someone you allowed telnet to your router.
Were they successful? **Yes / No**
Have someone that was not allowed telnet to your router.
Were they successful? **Yes /**
Have someone you allowed ping your router.
Were they successful? **Yes / No**
Have someone you did not allow ping your router.
Were they successful? **Yes / No**

Practical Exercise 8

Password Recovery Procedures

Objective: Recovery in case the Enable Secret password is lost or forgotten. This procedure works for all 2500 series routers running Cisco Release 10.0 and above.

1 Power cycle (turn off and then on) the router and within 10 seconds after the router starts to load, hold down the "**ctrl**" key and hit the "**break**" key several times. The system will stop the Boot Process and you will not get a router prompt.

2 Type **o/r 0x2142** at the > prompt to boot from Flash without loading the configuration.
Example: >**o/r 0x2142**

3 Reboot the router.
Example: >**i** (the router reboots but ignores its saved configuration)

4 Answer **NO** for "Would you like to enter the initial configuration dialog?"

5 Enter privileged mode.
Example: Router>**enable**

6 Load NVRAM to active memory.
Example: Router#**configure memory** (you might have to hit enter twice).

7 Type **show run** to show the configuration of the router. In this configuration you will see that all the interfaces are currently shutdown. You will also see the passwords in either encrypted or unencrypted format.
Example: Router#**show run**

8 Type **config t** to access the global configuration. Then change the enable-secret password and bring up the interfaces.

Example: Router#**config t**
Router(config)#**enable secret student** (change the password back to student)
Router(config)#**interface f0/0** (specifies the fastetherne t0/ 0 interface)
Router(config-if)#**no shut** (turns on the interface)
NOTE: IF YOU ARE USING MORE THAN ONE INTERFACE, YOU WILL HAVE TO REPEAT THE COMMANDS ABOVE TO TURN ON THOSE PORTS AS WELL!

9 Enter the command to specify the original configuration setting.
Example: Router(config)# **config-register 0x2102**

10 Press <**Ctrl-z>** to return to privileged mode. Then save changes to NVRAM.
Example: Router(config)# **<Ctrl-z> <Enter>**
Router# **write mem** or **copy run start**

Reading assignment 3

Subject: **Firewalls, Proxies, and VPNs**

Pages: 55-69, 85-96, 138-142, 297-321

(Complete before day 4)

1. ere are some typical locations for firewall placement?

2. at are 2 strategies of multiple firewall deployment?
   1.
   2.

3. at are their purposes?

4. ne 3 types of proxies:
   1.
   2.
   3.

5. efly explain each type:

6. at are 2 types of NAT assignment?
   1.
   2.

7. at are some other names used for PAT?

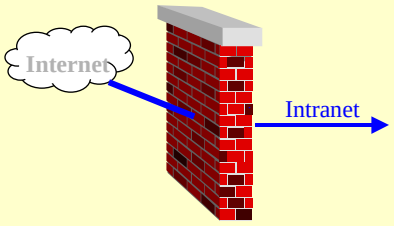
8. at does NAPT allow you to do with hosts in your network?

Firewalls

Module 11

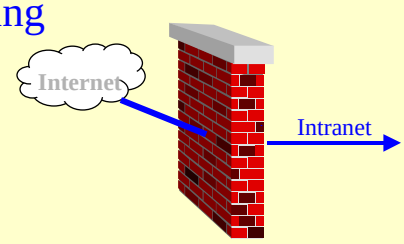
What is a Firewall?

A firewall is any computer, router, or combination of both, that controls access between two networks, whether it is a commercial product or home-made box.



Firewall Types

- Static packet filtering
- Dynamic packet filtering
- Stateful packet filtering
- Proxy

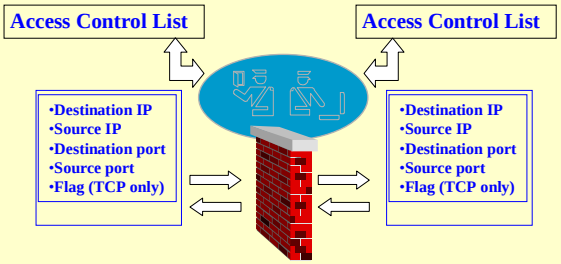


September 20, 2004

11-1

Static Packet Filtering

Controls traffic by using information stored within the packet headers. Packets received are compared against the access control policy in effect. Packets will be either be forwarded or dropped depending on the active policy.

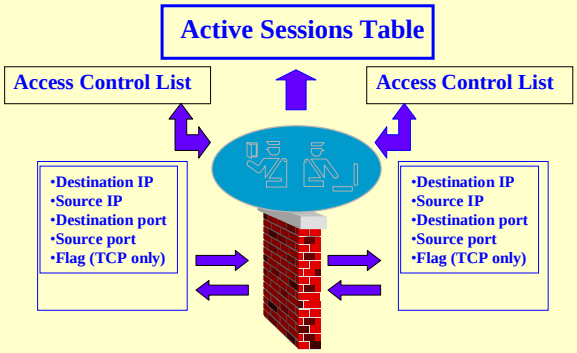


September 20, 2004

11-1

Dynamic Packet Filtering

Similar to static packet filtering except that it also maintains an active connections table that monitors the state of a communication session.

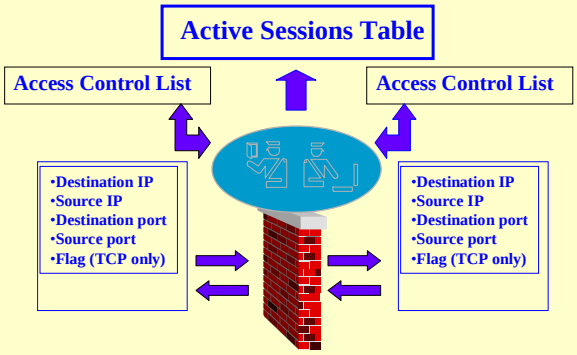


September 20, 2004

11-1

Stateful Packet Filtering

Similar to dynamic packet filtering except that it also maintains an active connections table that monitors the sequence of events for a communication session.

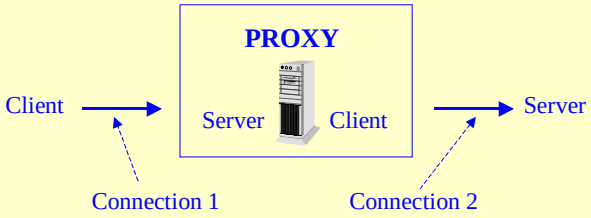


September 20, 2004

11-1

Proxy or Application Gateway

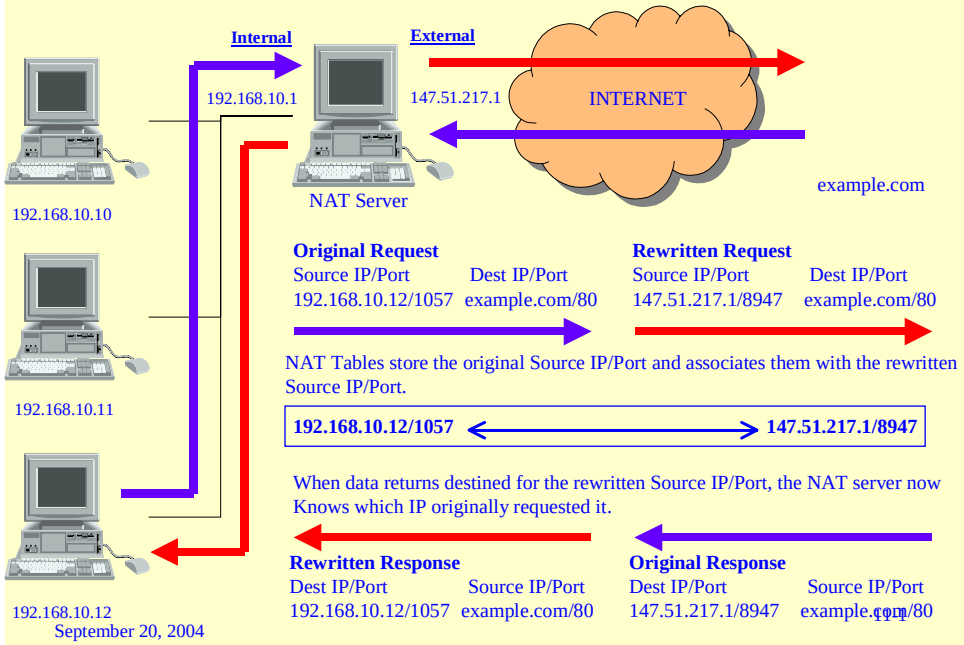
- Plays middleman between two network segments
- Source and destination never actually connect
- Stands in and speaks for each system on each side of the firewall



September 20, 2004

11-1

Network Address Translation



Original Request

Source IP/Port	Dest IP/Port
192.168.10.12/1057	example.com/80

Rewritten Request

Source IP/Port	Dest IP/Port
147.51.217.1/8947	example.com/80

NAT Tables store the original Source IP/Port and associates them with the rewritten Source IP/Port.

192.168.10.12/1057 ⟷ **147.51.217.1/8947**

When data returns destined for the rewritten Source IP/Port, the NAT server now Knows which IP originally requested it.

Rewritten Response

Dest IP/Port	Source IP/Port
192.168.10.12/1057	example.com/80

Original Response

Dest IP/Port	Source IP/Port
147.51.217.1/8947	example.com/80

September 20, 2004

11-1

Firewall Capabilities

- Logging and Notification
  Documents all traffic that passes through it and can provide alerts
- Virtual Private Networking (VPN)
  As a "flowpoint" for external traffic, firewalls are a perfect place to implement VPNs for remote access
- Filter Java, ActiveX, and HTML Scripts
  Remove Java/ActiveX applets from incoming HTTP datastream

Firewall Capabilities

- Address Processing
  Provides the ability to control how systems are identified through the firewall
- Weak and Strong Authentication methods
  ACE/Server
  Cryptocard
  S/Key
  Gateway passwords
  NT Domain authentication

Potential Firewall Weaknesses

- Have you compromised your own firewall?
- Tunneled Protocols and Firewalls
- Other ways to neutralize a firewall

Compromised Your Own Firewall?

- Where's your perimeter?
  It's hard to prove you're protecting your assets when you can't even identify all of them
- Dial-in modem access commonly bypasses the firewall
- "Flavor of the day" protocols often allowed
  Proxy-based firewall bypassed by opening ports for applications which don't yet have proxies available

Tunneled Protocols and Firewalls

•Anything can be tunneled over other protocols
e.g, Pointcast over HTTP, Telnet/NFS over e-mail

•Tunneling/Encapsulating traffic is routine

•Even if you only allow e-mail in and out, almost anything can "piggyback" over that channel

Other ways to neutralize a firewall

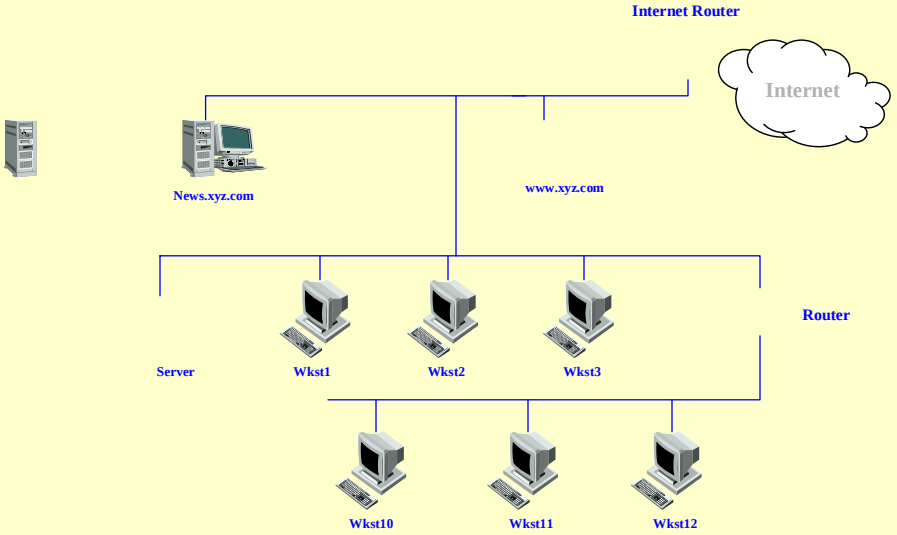
•Excessive Alarms

•Bypassing the firewall
If users get into the network in any way besides through the firewall, it does nothing to protect your systems

•Compromise an insider
Not every user, programmer, or system administrator is perfectly ethical. Firewalls do not protect from insider attacks!

•Trojan horses

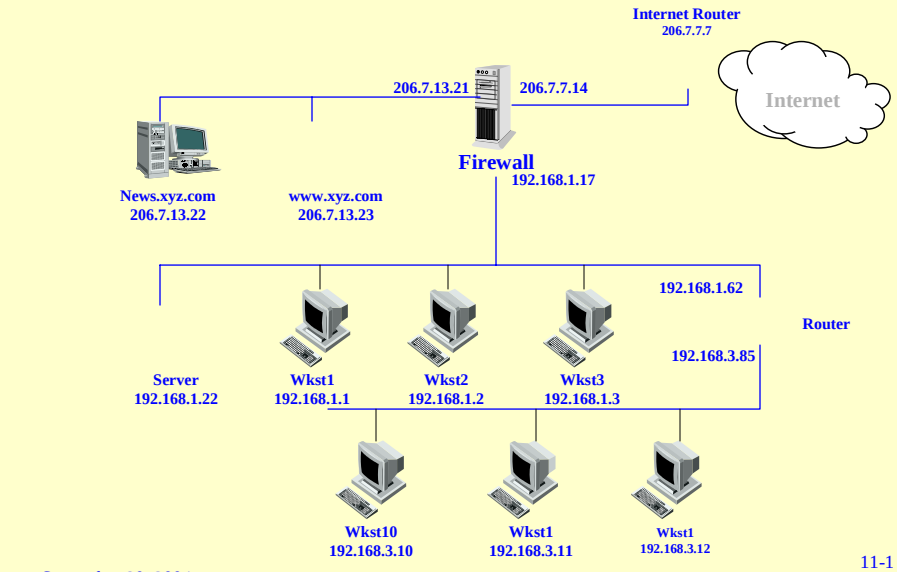
Network without a Firewall



September 20, 2004

11-1

Network with a Firewall



September 20, 2004

11-1

Summary

- Intelligent employment and configuration of Firewalls can significantly improve organizational security
- The goal is to allow inside and outside users access to as many services as possible without compromising the security of the network
- There are certain things which Firewalls cannot defend against

Symantec Enterprise Firewall (SEF)

Module 12

Student Handout page 81

SEF

- Software and hardware solutions that employ a multi-layered security approach
- Industry-tested firewall, virtual private networking, content filtering, and high availability and load balancing
- Easily configurable through a platform independent management interface
- Symantec security gateways are designed for small and medium size companies that may not have a dedicated security staff and equipment.

SEF

Industry-tested firewall

- The mature Symantec Enterprise Firewall-based component protects at the network layer and at the application layer with full application inspection proxies that provide protection against a variety of application-based attacks.
- The core of the firewall component is the Symantec driver. The driver incorporates several security features including fragment reassembly, header and datagram validation, and SYN flood protection.
  - A security guard that checks the credentials and integrity of both incoming packets, outgoing packets and determines whether or not those packets go on to more sophisticated checks.
- Symantec's application proxies reduce overhead, create access to services that may not exist on the security gateway, and provide security by creating a virtual air gap between the client and the server.

SEF

Virtual private networking

- The security gateway incorporates a robust VPN component, letting organizations securely extend their network. The VPN component is a standards-based solution, that establishes encrypted connections from remote locations. The security gateway uses IPsec tunnels to send encrypted and encapsulated traffic across public networks to other IPsec-compliant endpoints.
- A central piece of any VPN implementation is the algorithms used to provide encryption and integrity checks.
  - Advanced Encryption Standard (AES), Triple DES and DES are also supported, as well as MD5 and SHA1 for packet integrity.

Content filtering

- Symantec security gateways include a strong content filtering component that lets administrators simply and efficiently deny access to Web sites and Web site content.
  - You can make manual entries to the Web site database.

SEF

High availability/load balancing

- The security gateway includes support for high availability and load balancing (HA/LB).
- The integrated HA/LB technology is based on a share nothing model.
  - Symantec's implementation is network-based, where the network provides the means of communication between all nodes in a cluster. Every node in the cluster shares responsibility in maintaining the state of the cluster over a controlled network.

Anti-spam support

- Many email clients try to address the issue by filtering email messages, but filters are usually only effective when the sending source or information in the header remains constant.
- SMTP proxy to prevent the security gateway from functioning as an SMTP relay. You can impose hard and soft limits on the number of recipients in an email. Additionally, you can check email sources can, and if they don't resolve, block them. Optionally, you can elect to use one of the public real-time blackhole lists (RBL) when deciding to accept or reject an email.

SEF

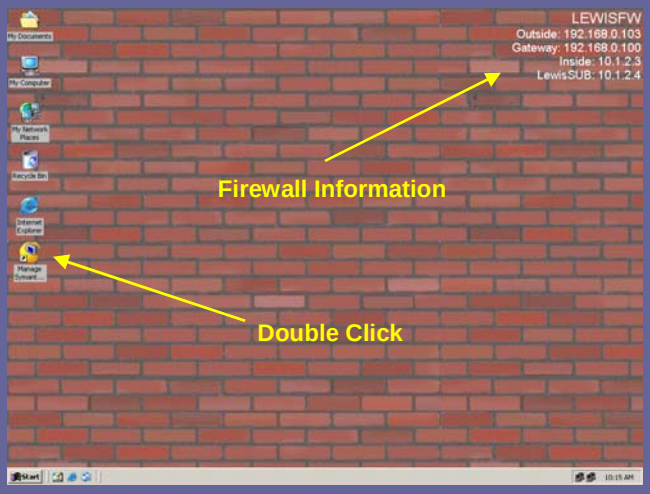
Antivirus

- As new threats emerge, Symantec's LiveUpdate technology updates both virus definitions and the engine without service interruption, keeping you fully protected now and in the future.
- The antivirus component incorporates bloodhound technology for heuristic detection of known and unknown viruses.
- The antivirus component detects malicious viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats.

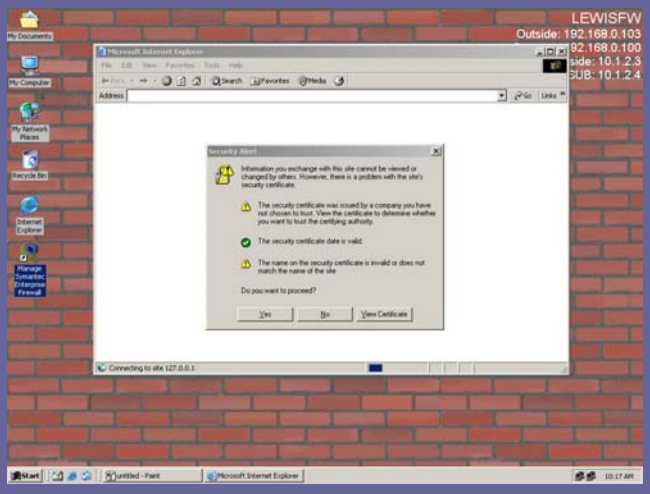
Intrusion detection and prevention

- Symantec security gateways monitor network traffic for suspicious behavior and respond to detected intrusion in real-time.
- Symantec's intrusion detection and prevention component provides a common, highly coordinated approach to detect attacks at very high speeds within the network environment.
- the intrusion detection and prevention component collects evidence of malicious activity with a combination of protocol anomaly detection (PAD), traffic rate monitoring, protocol state tracking, and IP packet reassembly.

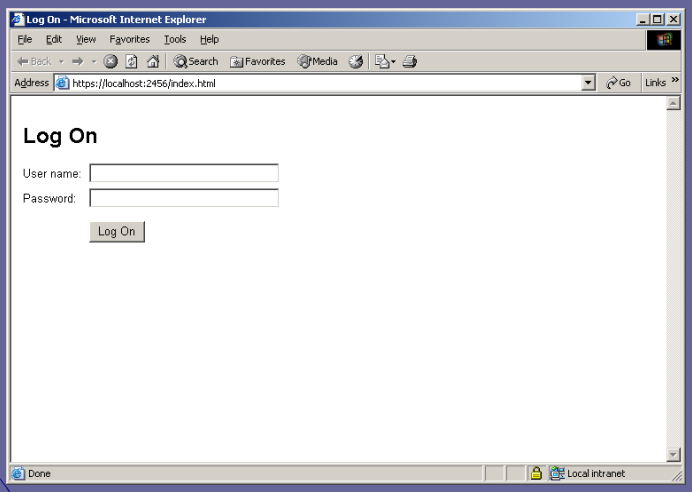
Desktop View



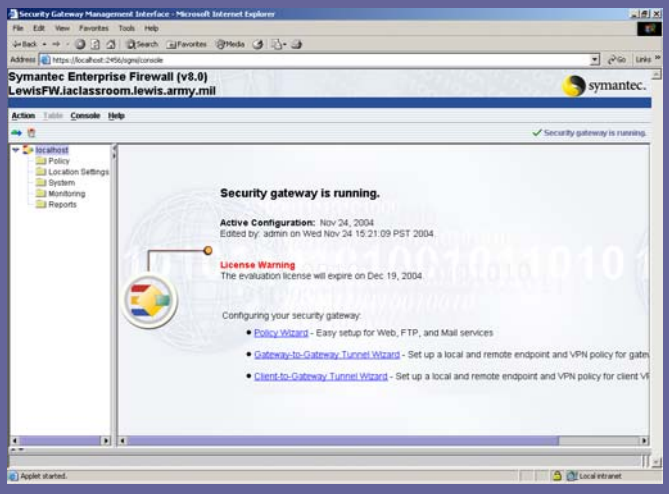
Security Alert



Log On



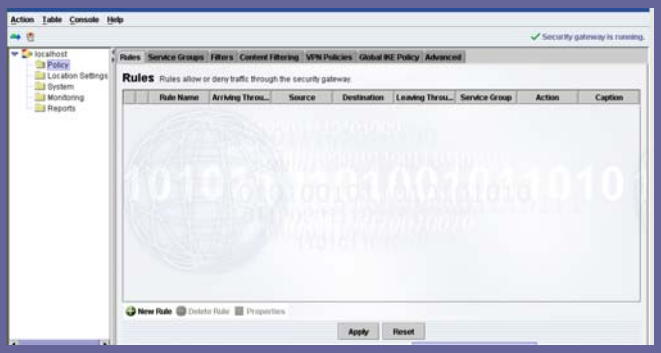
Home Page



Policy Folder

- Rules
- Service Groups
- Filters
- Content Filtering
- VPN Policies
- Global IKE Policy
- Advanced

Policy - Rules



- When the security gateway receives a connection request, it searches for rules that match the time window and definition of the connection request.
- From this list of possible matches, the security gateway then selects the rule that most closely matches the source address, destination address, protocol, and interface or VPN tunnel. The rule that best fits is then applied; the connection is either allowed or denied.

Policy - Rules

Similar to rules themselves, the rule parameters also have a priority as to which takes precedence. For similarly configured rules, the following order is checked:

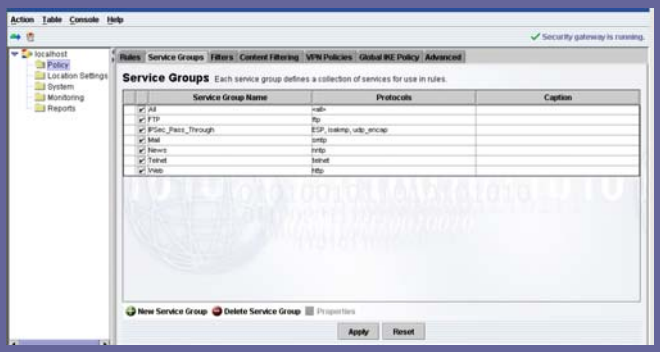
- Rules that define a time period take precedence over those with no defined time period (<ANYTIME>) when the connection request arrives during that time period. If the connection request arrives outside of the defined time period (trying to access the network on the weekend when WorkingHours is defined, for example), then the rule with <ANYTIME> takes precedence.
- Rules with more source network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are chosen before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with source interface restrictions (eth0, eth1, and so forth) have a higher priority than those with no interface restrictions.

Policy - Rules

- Rules with more destination network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are selected before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with destination interface restrictions are higher in priority than those with no interface restrictions.
- Rules that explicitly deny traffic supersede matching rules.
- Rules with user restrictions overrule those with no restrictions.
- Rules with authentication override those with no authentication.

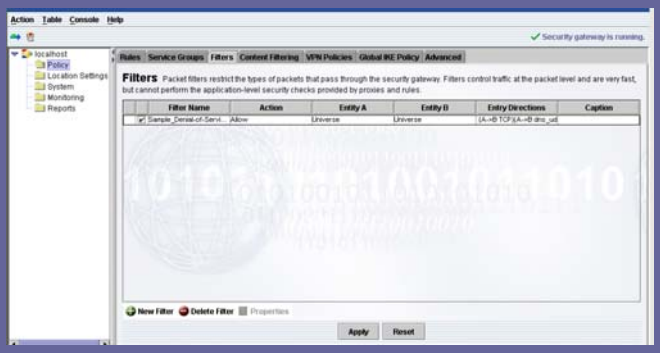
This order also defines top-down priority. That is, a rule with a time period takes precedence over a similar rule with authentication.

Policy – Service Groups



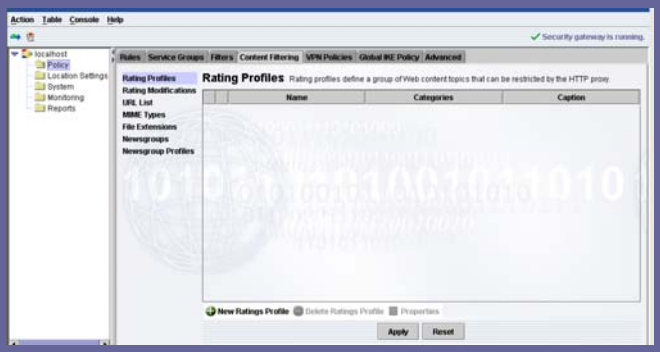
- A definition of network traffic that includes one or more protocols
- Used in rules to define the type of traffic to allow or deny, and offer a simple way to group multiple protocols into a single entity.
- Consists of the service group name, an assigned ratings profile (if appropriate), both a short and long description, assigned protocols, and any additional parameters.

Policy - Filters



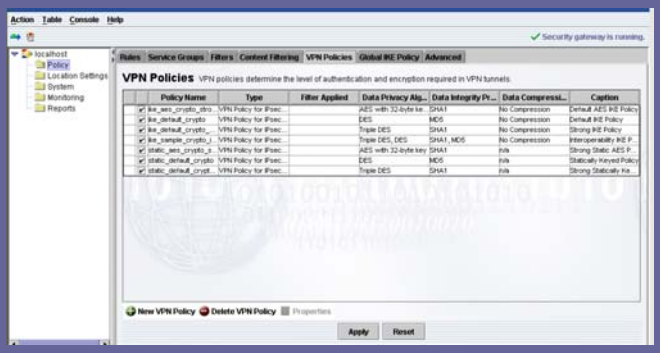
- Filters let the administrator discard packets that should not be forwarded or serviced locally. A well constructed filter can reduce a significant portion of undesired traffic, freeing up valuable resources to address legitimate connections. Packet filtering is a versatile security gateway feature that is sometimes considered complicated because packet filters are order-dependent and use different logic from authorization rules, which are based on best fit. Make sure you understand how packet filters work and how to use them before creating any filters.

Policy – Content Filtering



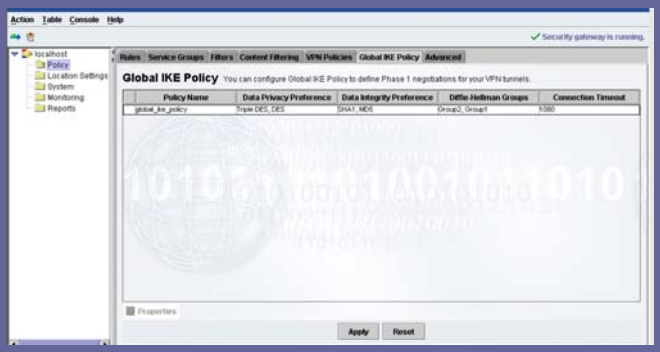
- Content filtering lets an administrator prevent access to objectionable material, or allow access to specific sites. The security gateway can allow or deny access to content through the following types of content filtering:
  - > Rating profiles
  - > URL list
  - > URL pattern matching
  - > MIME types
  - > File Extensions
  - > Newsgroup profiles

Policy – VPN Policies



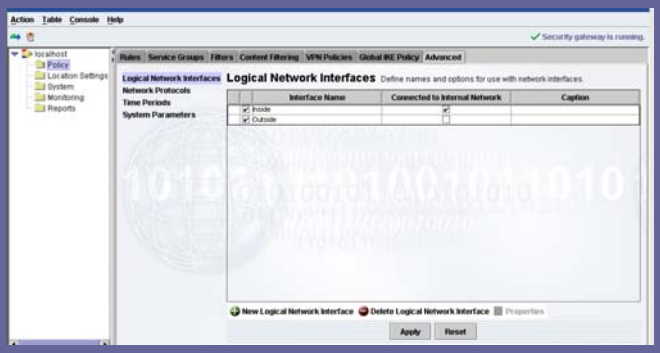
- Rather than configuring data privacy, data integrity, and data compression algorithms for every tunnel you create, the security gateway lets you configure standard, reusable VPN policies and then later apply them to multiple secure tunnels. VPN policies group together common characteristics for tunnels, and allow for rapid setup of additional tunnels with the same characteristics. The security gateway also includes a handful of commonly used VPN policies, for both static and dynamic tunnels.

Policy – Global IKE Policy



- The security gateway comes with a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations. This global IKE policy works in conjunction with the IPsec/IKE VPN policy you configure, providing the parameters for Phase 1 negotiations for your IKE tunnel, while the VPN policy you configure and select provides the parameters for Phase 2 negotiations.

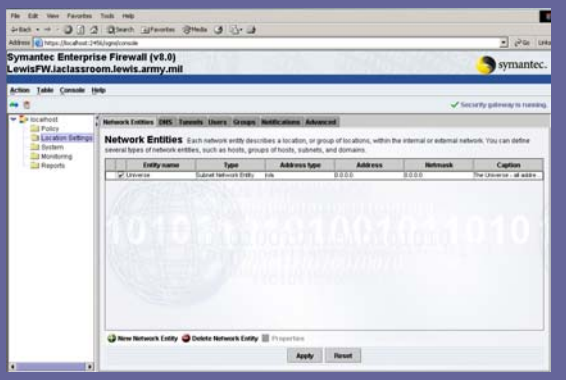
Policy - Advanced



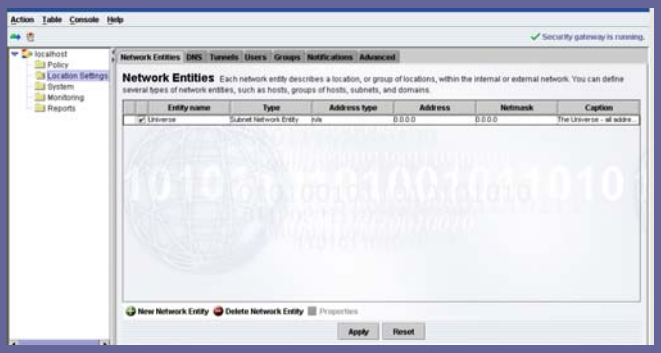
- Logical Network Interfaces – Define names and options for use with network interfaces
- Network Protocols – Most frequently used protocols are shipped with the product
  - New protocols may be added
- Time Periods – Control network access by time of day, day of week and periods of time
- System Parameters – Reverse lookup, hostnames included in logs, etc

Location Settings Folder

- Network Entities
- DNS
- Tunnels
- Users
- Groups
- Notifications
- Advanced

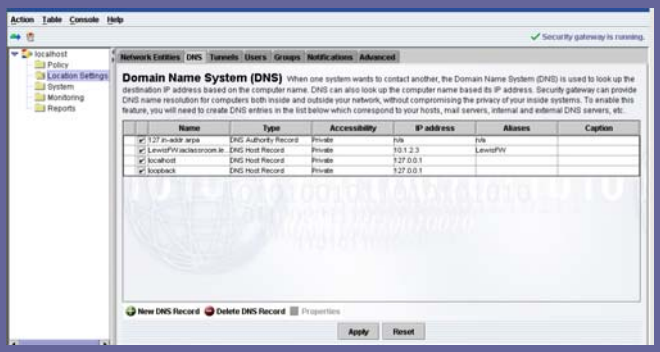


Location Settings – Network Entities



- A network entity is a host or group of hosts that reside locally on the protected network, or on the public network external to the security gateway. A network entity is defined by an IP address, a group of IP addresses, or a domain name. You must define network entities to describe the hosts that pass data through the security gateway. Once the appropriate network entities are defined, you can construct rules and VPN tunnels.

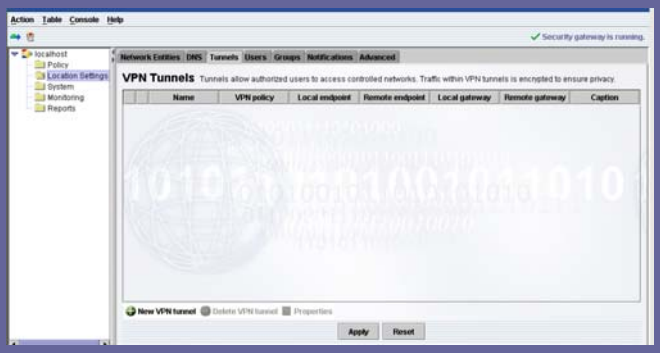
Location Settings - DNS



- The security gateway includes support for the domain name service (DNS). The security gateway's DNS implementation supports many of the features of standard
- DNS implementations, including full name resolution and reverse name resolution. DNS configuration on the security gateway may seem a bit more challenging than a standard DNS implementations because the security gateway supports security-conscious DNS configurations only.

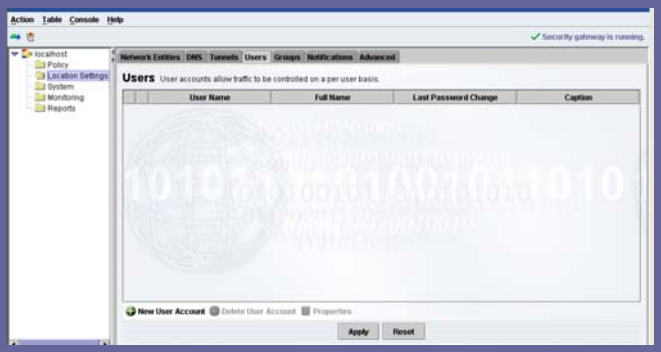
  > Name resolution > Reverse name resolution > Mail exchange information

Location Settings – Tunnels



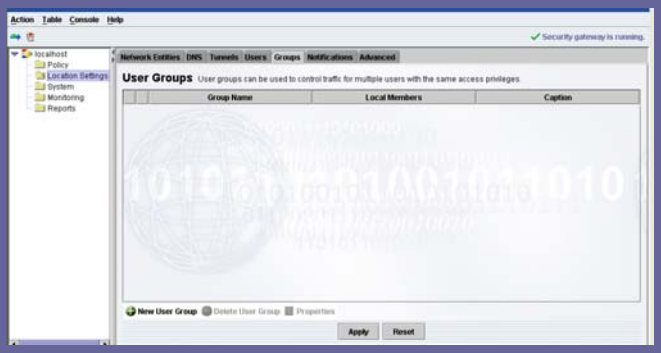
- Early networking pioneers originally created tunneling to pass data of one protocol type (IPX, for example) over a network using a different protocol
- (IP, for example). These virtual tunnels let packets travel over foreign networks without modifying their contents. Virtual private networks evolved by adding encryption and authentication checks to the tunnels, which let encrypted packets propagate securely over the network.

Location Settings - Users



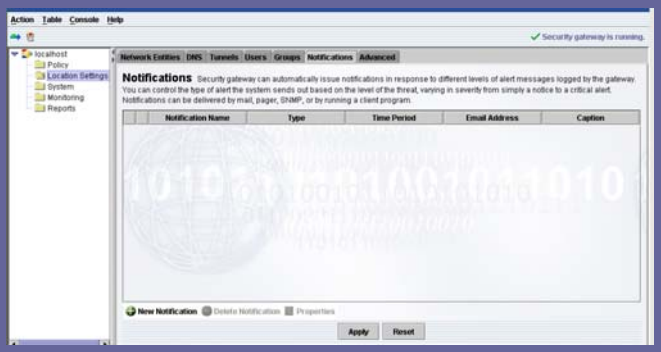
- A user represents an individual with rights to access your protected network resources, and must be defined for rules and tunnels to limit access to authorized connections only. Users are also required for most types of authentication. Users are defined by creating a user account consisting of a unique user name and authentication method.
  - General > Trusted > Gateway or Static
  - Dynamic > Default IKE user

Location Settings - Groups



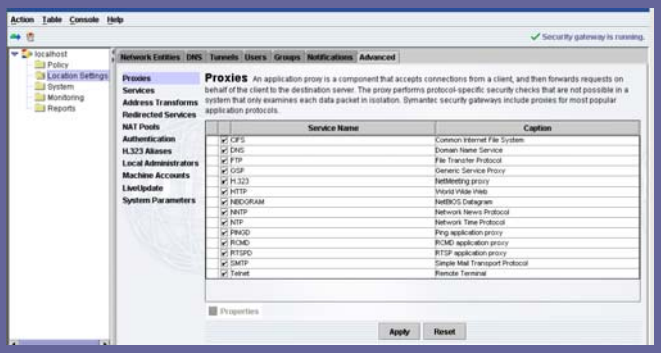
- Used to control traffic for multiple users with the same access privileges.

Location Settings - Notifications



- Security Gateway can automatically issue notifications in response to different levels

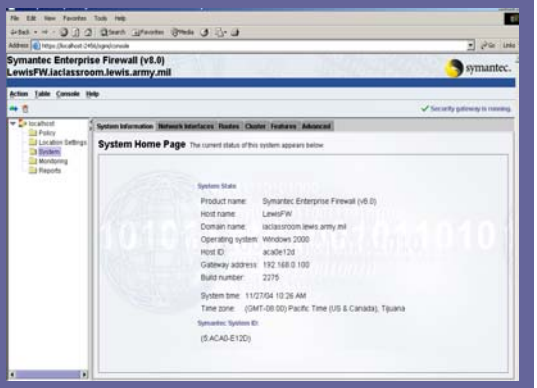
Location Settings – Advanced



- Proxies
- Services
- Address Transformations
- Redirected Services
- Nat Pools
- Authentication
- H.323 Aliases
- Local Administrators
- Machine Accounts
- Live Update
- System Parameters

System Folder

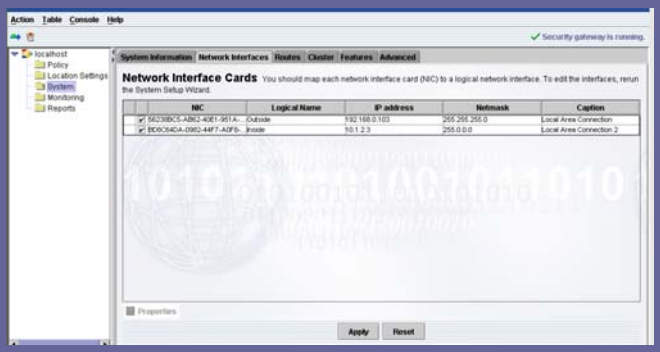
- System Information
- Network Interfaces
- Routes
- Cluster
- Features
- Advanced



System – System Information

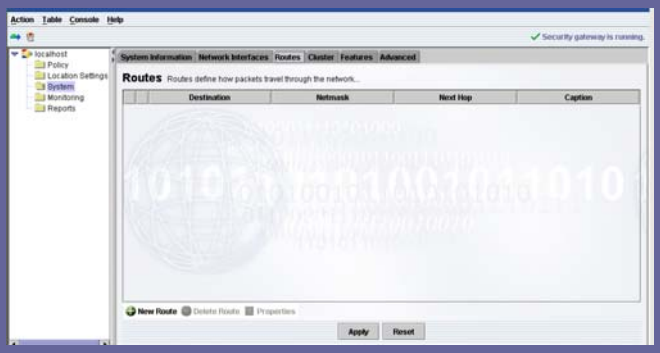
- Current status of the system

System – Network Interfaces



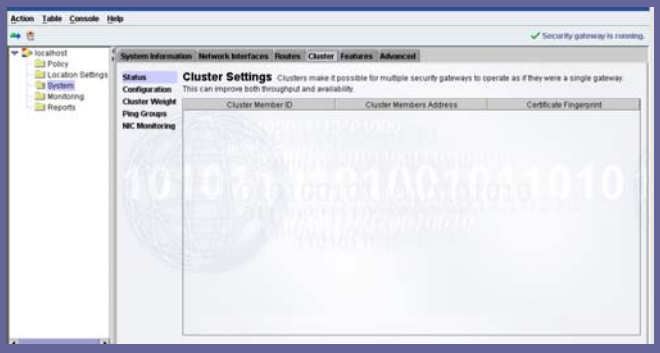
- Logical network interfaces are an abstraction of the system's network interfaces. Logical network interfaces let an administrator apply the same general configuration to multiple security gateways, even if those security gateways have different physical hardware adapters installed. The benefit of logical network interfaces becomes clear when you understand that you can create rules that apply to a logical network interface instead of a specific interface with a static IP address.

System - Routes



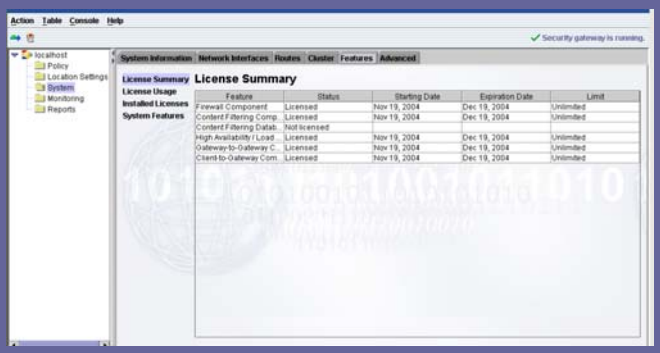
- Routing is the process of choosing a path over which to send packets of information. For the security gateway to function properly, you must define specific routes. Administrators set default routes according to instructions specific to their platforms. Almost all discussions on routing and data communications require an understanding of the publicly accepted terms and technology involved.

System – Cluster Settings



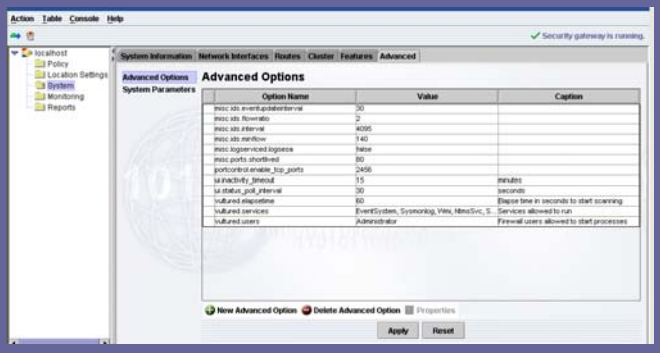
- Group of machines, called nodes, that ensure continued connectivity (high availability) and leverage their processing power (load balancing), even if one or more nodes fail. In a cluster, multiple machines are grouped together and instructed to work as a single entity. All nodes in the cluster share the state information of all other nodes, and any node can immediately assume and support a connection for a failed node. Additionally, you can distribute work evenly among all node members, letting the cluster handle significantly more load than a single machine can.

System – Features



- License Summary – Licensed components
- License Usage – Current license usage for security gateway and client VPN
- Installed Licenses – Current installed licenses
- System Features – Features that can be enabled or disabled
  - > Gateway-to-Gateway VPN
  - > HA/LB
  - > Client VPN Support
  - > Content Filtering

System - Advanced



- Advanced Options – Settings for processes that are running
- System Parameters – Enable antivirus in all rules

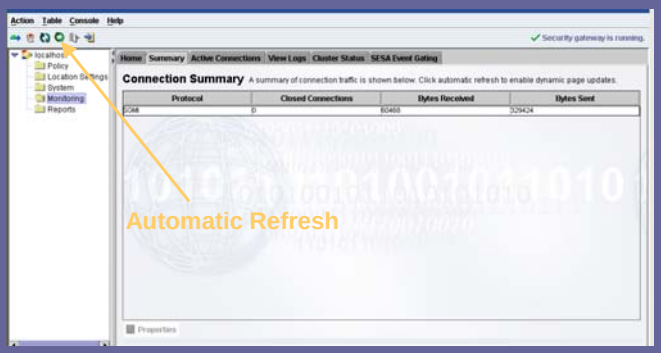
Monitoring Folder

- Home
- Summary
- Active Connections
- View Logs
- Cluster Status
- SESA Event Gating

Monitoring - Home

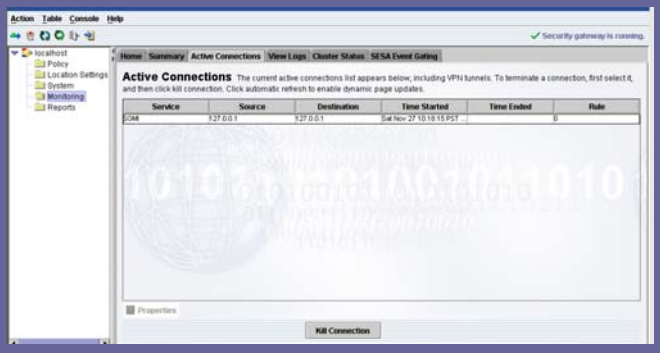
- See following tabs.

Monitoring - Summary



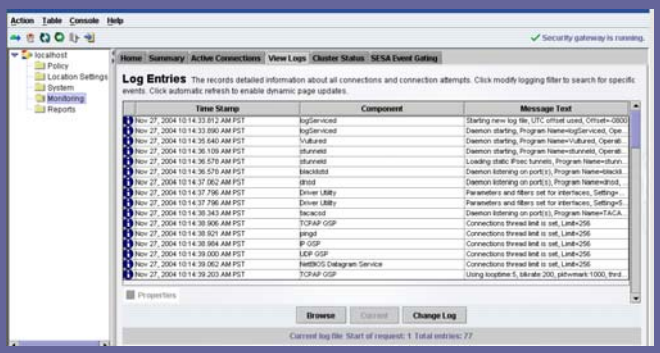
- Summary of connection traffic
  - Should select Automatic Refresh

Monitoring – Active Connections



- Current and recently finished connections are monitored through the Active Connections window.
  - Type of connection, source and destination IP address, time the connection started and time connection finished, and rule that allowed the connection.
  - Viewing the properties of a connection shows the source and destination ports, and the source and destination interfaces.
- Killing a normal session immediately terminates that connection.

Monitoring – View Logs

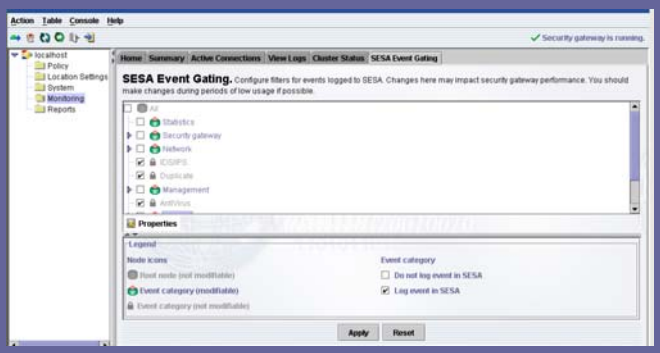


- Log files maintain a record of all activity to or through the security gateway. You can search and filter log files to display only pertinent information, or leave unfiltered to display all activity. The View Logs window provides detailed information on all connections and connection attempts made.

Monitoring – Cluster Status

- Monitor the cluster of two or more (up to eight) to support high availability and load balancing.

Monitoring – SESA Event Gating



- One of the strengths of the Symantec security gateways is that they are capable of reporting events to Symantec's SESA architecture. By doing so, you can correlate events from many security gateways into a single report. The SESA event gating option appears in the local SGMI because you configure the messages to report to SESA prior to joining the security gateway to the SESA environment.

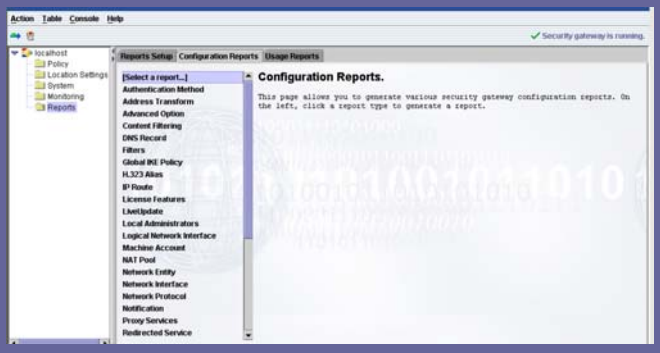
Reports Folder

- Reports Setup
- Configuration Reports
- Usage Reports

Reports – Reports Setup

- The reports setup section defines how configuration reports should be saved and displayed to the administrator. Reports saved in HTML are displayed in the window to the right of the report selection list. To view PDF reports, the management host must have Adobe Acrobat Reader installed. The security gateway displays reports generated in PDF in a separate window. From this window, you can save the report.

Reports – Configuration Reports



- All The Configuration Reports feature lets you view the status of all security gateway configurations from one central location (the Configuration Reports tab in the Reports window). You can view individual component configuration reports or you can view all configuration reports by selecting the Master Configuration report in the Configuration Reports tab.
- Each report contains system-level information at the top.

Report type contents

- Authentication Method report: Configuration of authentication methods
- Address Transform report: Configured address transforms
- Advanced Option report: Configured advanced option information
- Content Filtering report: Configured content filtering information
- DNS Record report: Configured DNS records
- Filters report: Configured filters and filter groups
- Global IKE Policy report: Configured Global IKE policy information
- H.323 Alias report: Configured H.323 information
- IP Route report: Configured routing information
- License Features report: Configured licensing information
- LiveUpdate report: Configured LiveUpdate information
- Local Administrator report: Configured local administrator information
- Logical Network Interface report: Configured logical nic information
- Machine Account report: Configured machine account information
- NAT Pool report: Configured NAT pools
- Network Entity report: Configured network entities

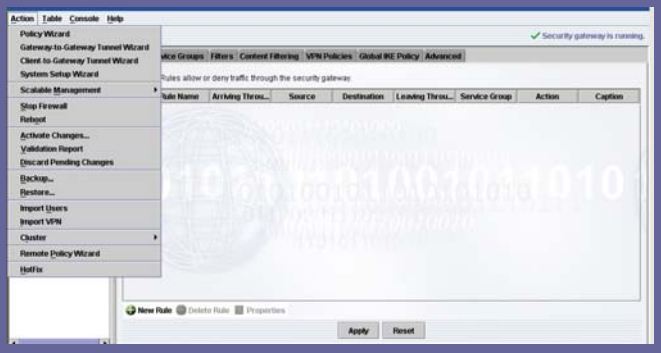
Report type contents

- Network Interface report: Configured network interface information
- Network Protocol report: Configured protocol information
- Notification report: Configured security gateway notification information
- Proxy Services report: Configured proxy information
- Redirected Service report: Configured service redirects
- Rule report: Configured security gateway rules
- VPN Tunnel report: Configured VPN tunnel information
- VPN Tunnel Policy report: Configured VPN policy information
- Service Group report: Configured service group information System Parameters for Location
- Settings report: Configured location setting information
- System Parameters for Policy Report: Configured policy information
- System Information report: Machine-specific status information
- Time Period report: Configured time period and group information
- User Account report: Configured user information
- User Group report: Configured user group information
- Services report: Configured service information

Report – Usage Reports

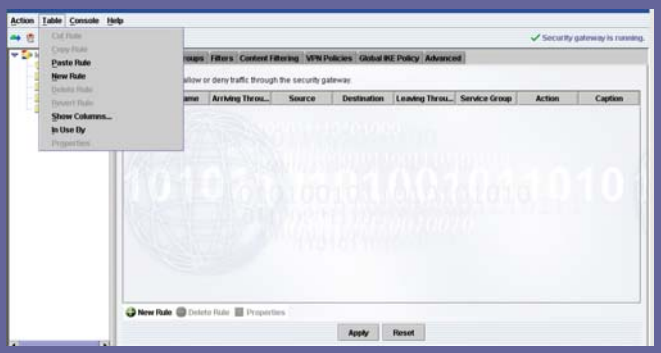
- Diagnostic report
  - Useful in troubleshooting system problems

Action Drop Down



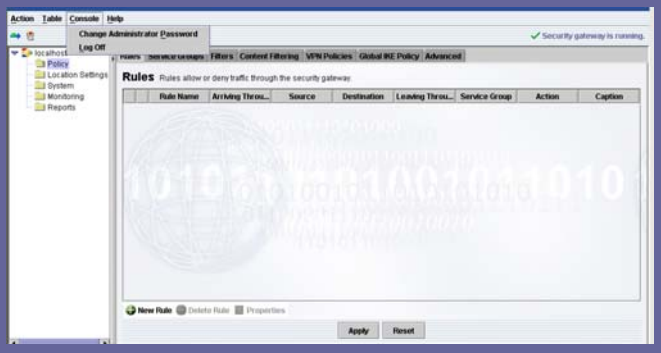
- Wizards
- SESA Management
- Stop Firewall
- Reboot
- Acitvation and discarding of changes
- Backup / restore

Table Drop Down



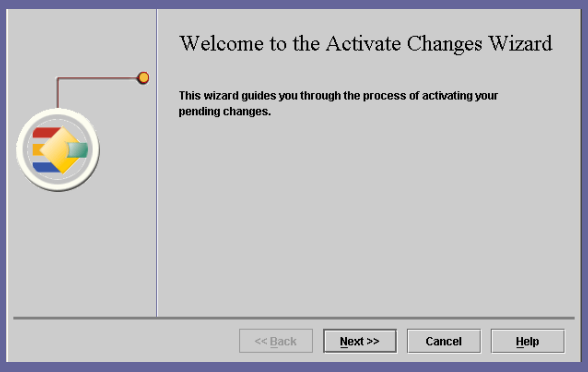
- Selections vary per folder and tab you are in

Console Drop Down

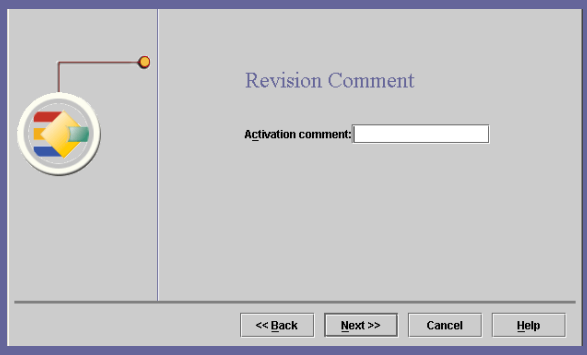


- Change Administrator Password
- Log Off
  - Time out for inactivity

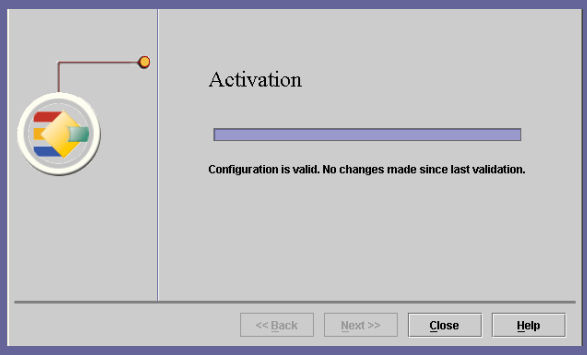
Activate Changes Wizard

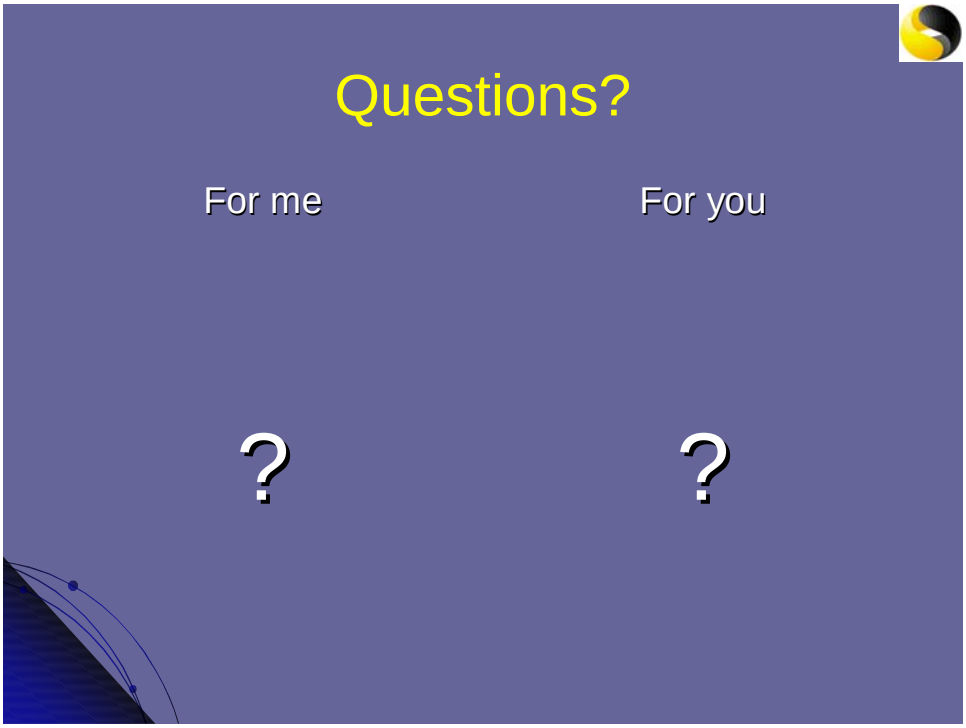


Revision Comment



Activation Complete




Questions?
For me
For you
?
?

Symantec Firewall Security

Lesson 4

This practical exercise is intended as a supplement to material learned during the Firewall and Symantec Enterprise Firewall lecture. Students will setup and configure the firewall to provide security and prevent unauthorized access to their internal network.

Objectives

1. Configure rules on the firewall
2. Check firewall for configuration management
3. Inspecting Logfile and Active Connections

Exercises

1. Getting Started with Symantec Enterprise Firewall 8.0
2. Checking Connectivity
3. Allowing and Controlling Outbound Access
4. Monitoring Logs
5. Monitoring Active Connections
6. HTTP and FTP Control
7. Rules

Firewall Practical Exercise #1

Getting Started with Symantec Enterprise Firewall 8.0

→ *Your Symantec Firewall has been installed already.*
→ *The interface does not have to be activated for the firewall to run.*
→ *Symantec Gateway Management Interface (SGMI) is used for configuration and management of the firewall*
→ *Follow these instructions below and answer the questions—use the firewall computers, and the "subnet" computers as instructed*

Remember: Anytime you make any changes, additions, and/or subtractions to the firewall, press the Apply button and Activate Changes from the Action drop down.

1. Start the firewall application:
   - **Double-click the Symantec Gateway Management Interface icon on the desktop**

2. A web browser will open. The url will be *https://localhost:2456/index.html*. Notice the Security Alert, click Yes after reading the contents of the Security Alert. After clicking yes, you will be presented with a Log On screen. Type in **admin** for User name and **student** in the Password and then click on the Log On button.

3. Verify the Security gateway is running. *This information is available on the main SGMI screen as well as in the upper right hand portion of the screen.*
   [If you see the message "CHANGES PENDING" in red letters contact the instructor]

4. Notice also the Active Configuration. *This information is available on the main SGMI screen.*
   What is the current Active Configuration? _____

5. In the SGMI, select the system folder in the left column. Select the Features tab: Notice the License Information.
   What does it say about the license we are using? _____

6. In the SGMI, select the **System folder.** Click on **Network Interfaces**. You will see two network adapters. The IP address **172.16.xx.xx** is the **Inside NIC** and the IP address **10.0.x.x.** is the **Outside NIC**.
   Make note of your outside and inside addresses
   Outside: _____
   Inside: _____

(If you do not see both interfaces contact the instructor)

Firewall Practical Exercise #2

Checking Connectivity

→ *Follow these instructions below and answer the questions—use both the firewall computers AS WELL AS the Subnet computers (**the Subnet computer is the computer behind the firewall**)*
→ *Write down abbreviated responses in your answers only*
→ Use Command Prompt for ping.

1. **Firewall Computer:** check out the firewall's interface status by doing the following steps:

   Write the response after you type in **ping localhost (127.0.0.1): _____ (HINT: you should get a reply)**

   Write the response after you **ping the Instructor's computer (10.0.0.1): _____(HINT: you should get a reply)**

   Write the response after you **ping the Subnet computers interface card (172.16.xx.xx): _____ (HINT: you should get a reply)**

2. ***Subnet computer*:** type the following commands:

   Write the response after you **ping the internal interface of the firewall computer (172.16.xx.xx): _____(HINT: you should get a reply)**

   Write the response after you **ping the external interface of the firewall computer (10.0.xx.xx): _____**
   (HINT: you should see "request timed out")

   Write the response after you **ping the Instructor's computer (10.0.0.1): _____**
   (HINT: you should see "request timed out")

3. Why did we receive the above responses?

   _____

Firewall Practical Exercise #3

Allowing and Controlling Outbound Access

→ *Write down abbreviated responses in your answers only.*
→ *REMEMBER: Any and all changes must be saved, using apply button and Activate Changes, before they can take place.*

1. Select the **Policy** folder, choose the **Service Groups** tab.

2. Click on **New Service Group**. Once the **new_service_group** is created, select it and then click on **Properties**. Make the following changes:
   - General Tab
     - Service Group Name: Ping
     - Ratings Profile: None (default)
     - Caption: Exercise 3
   - Protocols Tab
     - Locate **ping** in the Available Protocols pane, select it, click on the >> button. You should now see **ping** in Included Protocols pane.

3. Repeat Step 2 (to create another Service Group). Make the following changes:
   - General Tab
     - Service Group Name: Outbound
     - Ratings Profile: None (default)
     - Caption: Exercise 4-8
   - Protocols Tab
     - Locate **ping, ftp, http, telnet and dns_udp** in the Available Protocols pane, select each, click on the >> button. You should now see **ping, ftp, http, telnet and dns_udp** in Included Protocols pane.

4. Click Apply (Notice up at the top of your screen that ***Changes Pending** is displayed. That will be displayed until Activate Changes has concluded.

5. **Select** Rules tab. Select **New Rule**. Once the **new_rule** is created, select it and then click on **Properties**. Make the following changes:
   - Rule Name: Exercising
   - Arriving through: Inside
   - Source: Universe
   - Destination: Universe
   - Leaving through: Outside
   - Service Group: Ping
   - Action: Allow (default)
   - Caption: (leave blank)

Firewall Practical Exercise #3 Con't

6. Click **Apply**. Go to the **Action** Drop Down, Scroll down to **Activate Changes**.

7. On the Activate Changes window click **Next** twice. Wait for the Close option to appear. Select **Close**. Changes you have made above now have gone into effect.

8. ***Subnet computer*:** Ping the **Instructor's computer** (10.0.0.1). Were you able to receive a reply back from the host pinged? Why? or why not?
   _____

9. ***Subnet computer*:** Telnet to the **Gateway Router** (155.8.216.1). Do not attempt to login, you are just verifying that telnet works. Do you get a login prompt? _____ Why did you get that response?
   _____
   _____

10. ***Subnet computer***: Telnet to the Outside NIC of the firewall (10.0.xx.xx). Do you get a hostname prompt? _____ Why did you get that response?
    _____
    _

11. Select the **Location Settings** folder, choose the **Network Entities** tab.

12. Click on **New Network Entity**, choose New **Host Network Entity**. Once the **new_host_network_entity** is created, click **Properties**. Make the following changes:
    - Entity Name:Woxxx (use your subnet computers name)
    - IP Address: 172.16.xx.xx (use subnet computers IP)

13. Click **Ok**, click **Apply**.

14. Go back to step 5 and change the rule named **Exercising.** Click on **Properties**. Change the following items only:
    - Source: Woxxx (use your subnet computers name)
    - Service Group: *Outbound*

15. Repeat steps 6 and 7. To apply and activate changes.

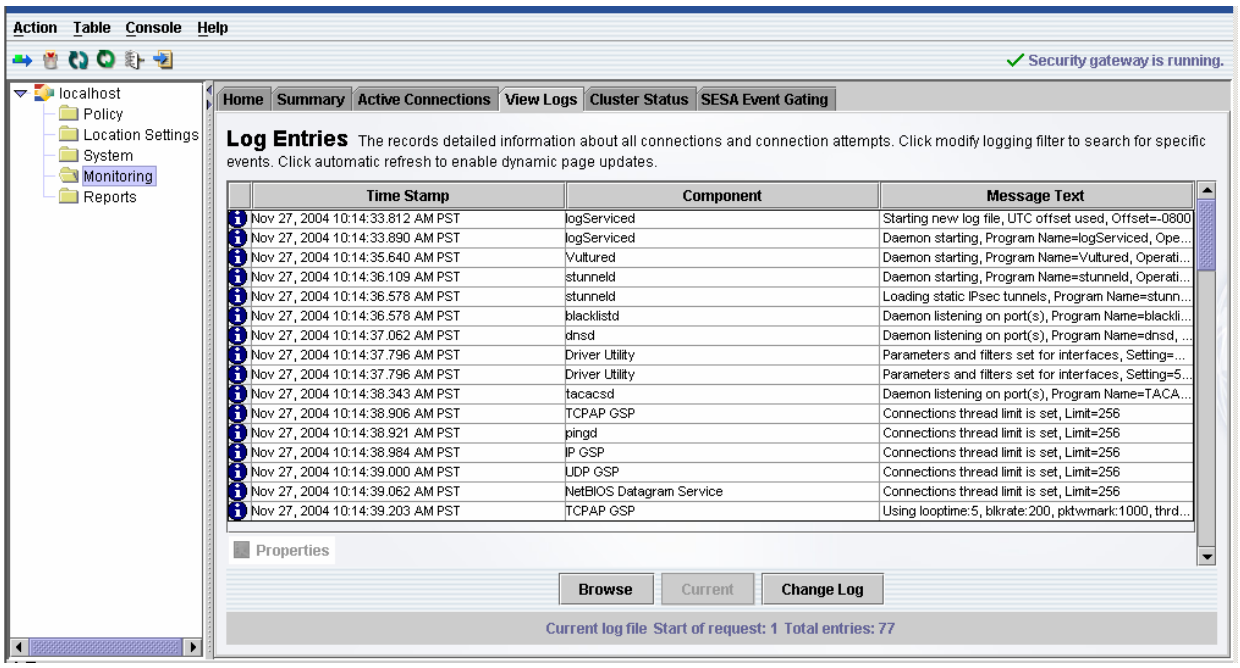
16. Repeat steps 8, 9 and 10 from Subnet PC. Record your results now.
    - Ping Instructor's computer? _____
    - Telnet to Gateway Router? _____
    - Telnet to Outside NIC of firewall? _____

    Why did you get the responses this time around?_____
    _____

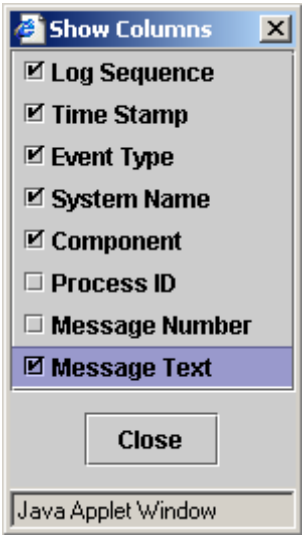
Firewall Practical Exercise #4

Monitoring Logs

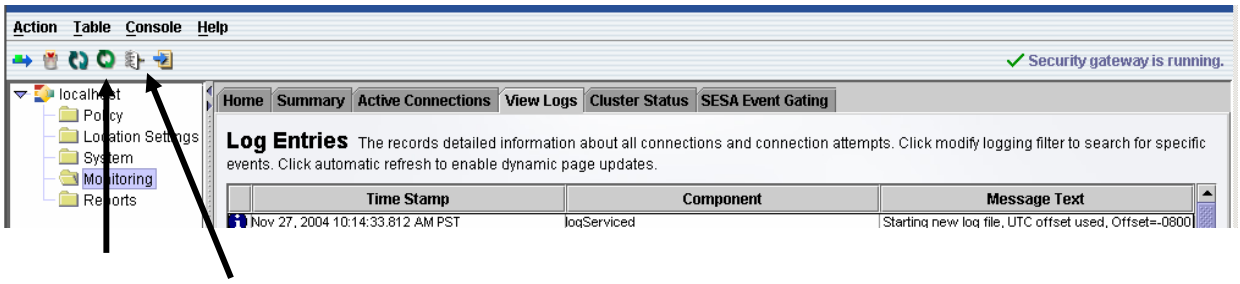
1. Select the **Monitoring** folder and choose **View Logs** tab. You will see data already picked up by the firewall.



2. Go to the **Table** Drop Down and select **Show Columns**. Select the options so that your table matches the screen shot below. **Close** the window **Show Columns**.



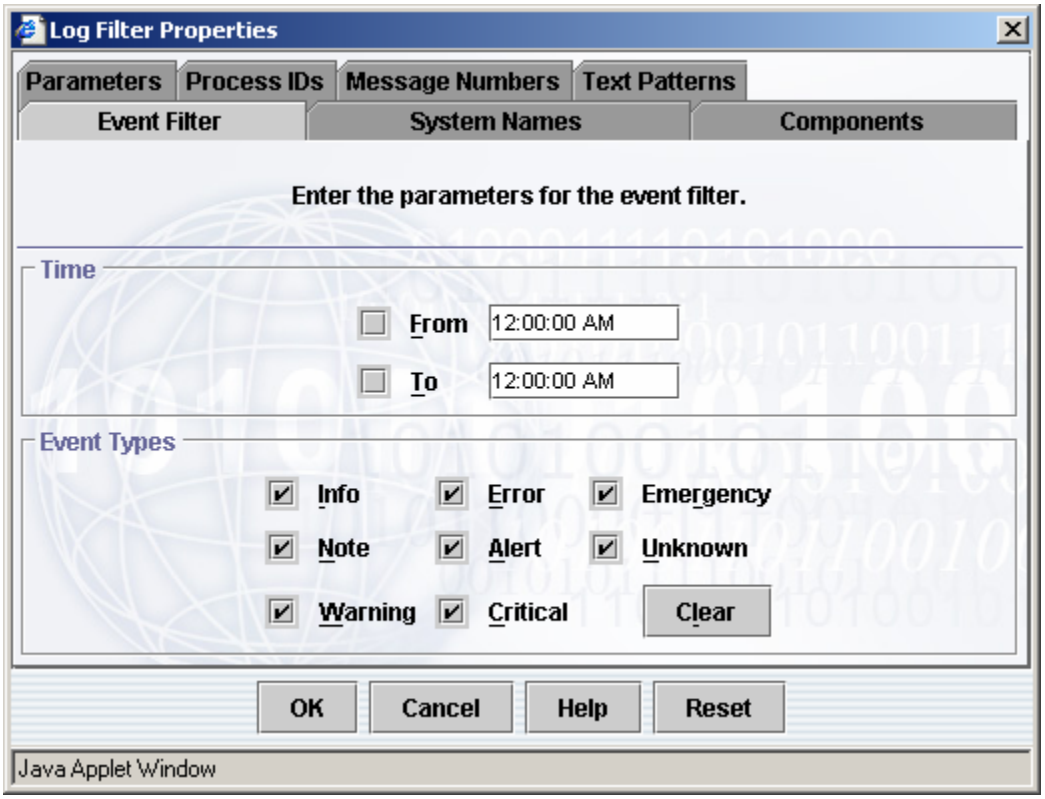
3. Click on the Icon in the task bar labeled Modify Logging Filter.



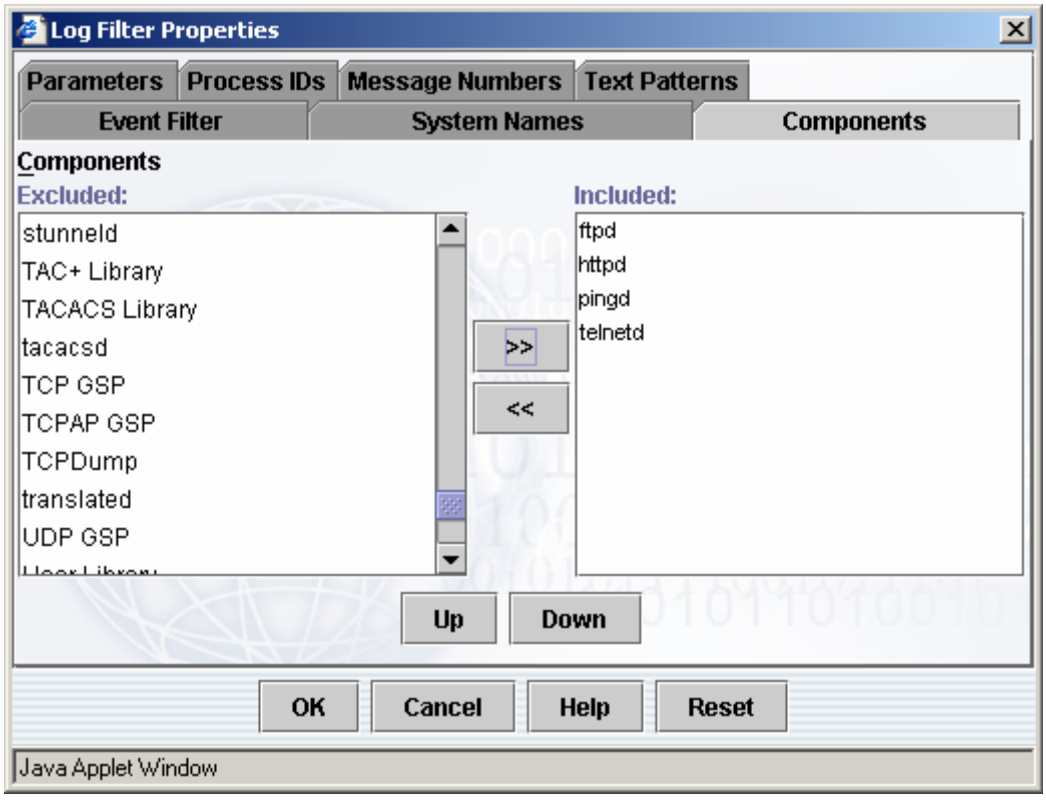
Automatic Refresh

Modify Logging

4. Once the **Log Filter Properties** display is open, select the **Event Filter** tab. Match your settings to reflect the same as the screen shot below in the **Event Types**.



5. Select the **Components** tab. Select from the **Excluded** components window: **ftpd**, and then click the **>>** button. Notice now ftpd is in the **Included** window. Continue on and add **httpd, telnetd**, and **pingd**. When finished, click OK, and only those components will show up in the logs throughout the rest of the Firewall Practical Exercises.



6. You should now be back at the **View Logs** tab.

7. Identify the log entries for Telnet and Ping connections that were conducted earlier. Can you identify the IP addresses used for the connections? Can you determine the session duration of the telnet session? _____
   _____

8. ***Subnet computer*:** type in **ftp 10.0.0.1 at the Command Prompt**: (Login as anonymous. Use any e-mail address for password). Run the **ls** command.

1. Watch the log entries on the firewall. What messages do you get on the logs because of this FTP action? _____

10. ***Subnet computer*:** download a file from the FTP server by doing the following command:

get present.rtf [enter]

11. Can you identify the downloaded file in the firewall's log file? _____

12. What port does the FTP connection use going through the firewall and what port does it use to connect to the FTP server? Are these the same ports used on every connection?
_____
_____

13. ***Subnet computer***: Connect to a few websites. See if the firewall administrator can track through the logs to find out your misuse of government resources.

Firewall Practical Exercise #5

Monitoring Active Connections

→ *Continue to answer the following questions*

1. **Firewall Computer:** Select the **Active Connections** tab and monitor the Subnet computers behavior.

2. ***Subnet computer*: ftp** to **10.0.0.1**, log on as **anonymous**; password is any email address.

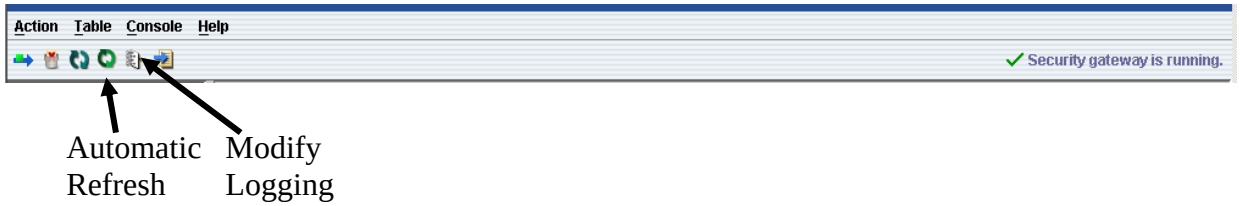
3. **Firewall Computer:** Select the **FTP** session in Active Connections. Press the **KILL CONNECTION** button.

4. ***Subnet computer*:** run the **ls** command. Is the FTP session still active? What message did you receive? _____

5. **Firewall Computer:** Wait for ftp connection to time out of Active Connections. Look at the Log file. What message does the log file contain because of the termination of the FTP session from the firewall? _____

6. ***Subnet computer*:** open an **ftp** connection to **10.0.0.1** again.

7. **Firewall Computer:** Look at the **ACTIVE CONNECTIONS** window. Did the firewall prevent the user from re-connecting? Why or why not? (Notice the rule associated with this connection.)



8. **Firewall Computer:** Be prepared to kill the Subnet computers connection to foxnews.com. (You may want to click on the automatic refresh icon in the task bar.)

9. ***Subnet computer*:** Connect to www.foxnews.com

10. **Firewall Computer:** As soon as the http traffic pops up in the Active Connections tab, click Kill Connection.
11. ***Subnet computer*:** Did the page fail to load? _____

Firewall Practical Exercise #6

HTTP and FTP Control

***1. Subnet computer*:** Go to **http://10.0.0.1**, what site have you visited, look carefully?

2. **Firewall Computer:** Go to the **Monitoring** Folder and select the **View Logs** tab. What does the log file tell you? _____

3. ***Subnet computer*:** Via the web browser, type in the following in the URL box: **ftp://10.0.0.1**

4. ***Subnet computer*:** What system response did you get? Were you successful in reaching the FTP server via the web browser? (if you successfully reach it, do NOT download anything).
_____

5. ***Subnet computer*:** Return to the URL **http://10.0.0.1**

6. **Firewall Computer:** Select the **Policy** Folder, choose the **Service Groups** tab. Click on the **Outbound** Service Group. Click **Properties**. Select the **Protocols** tab. Remove the **HTTP** protocol from the included protocols window. (This should stop all HTTP traffic)

7. **Firewall Computer:** What should be your next step? _____. Do that step.

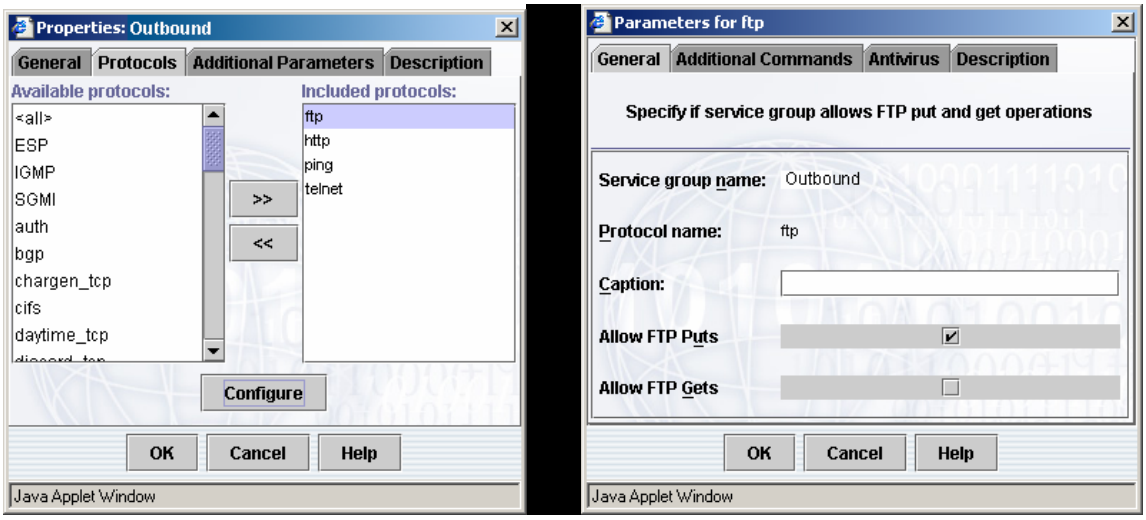
8. ***Subnet computer*:** Refresh your browser session to **http://10.0.0.1**
What occurs? Did you get an error message as expected?_____
_____

Firewall Practical Exercise #6 Con't

HTTP and FTP Control (con't)

2. **Firewall Computer: Add** the **HTTP** protocol back into your **Outbound** Service Group.

3. Click on **FTP** and click the **Configure** button. Remove the checkmark for **Allow FTP Gets**. (See screen shots below) Click OK twice. Make sure you **Apply** and **Activate Changes**.



11. ***Subnet computer*:** Via the command prompt, type in **ftp 10.0.0.1** Log in as anonymous and provide the password. At the ftp> prompt, type the following command: **get fw.ppt**

12. What is the result of this command? _____

13. **Firewall Computer**: What do the Log Entries tell you about this activity? _____
_____

Firewall Practical Exercise #7

RULES!

1. **Firewall Computer:** Select the **Location Settings** folder, choose the **Network Entities** tab.

2. **Firewall Computer:** Create a new host network entity to block access to Yahoo Mail.

   - Click New Network Entity
   - Click Host Network Entity
   - Click Properties
   - Entity Name: Yahoo.Mail.Blocker
   - IP Address: mail.yahoo.com
   - Click OK

3. **Firewall Computer:** Create a new host network entity to block access to cnn.com.
   - Click New Network Entity
   - Click Properties
   - Entity Name: CNN.Blocker
   - IP Address: www.cnn.com
   - Click OK

4. **Firewall Computer:** Create new **Rules** that will deny your ***Subnet computer*** (source) access to **Yahoo Mail** and **CNN** (destined for) while permitting access to all other web sites. Create the rules similar to the way you did in Exercise #3, but this time click on the "**Deny"** rather than "allow". Make sure to **Apply** and **Activate Changes**.

5. ***Subnet computer*****:** Go to the **mail.yahoo.com** and **www.cnn.com**. Did the rules work properly? _____

6. ***Subnet computer*****:** Now try **www.yahoo.com** and **www.cnn.com/TECH**. How did the rules work this time? _____

Before continuing to the next practical exercise, remove ALL rules that were created by you and apply and activate your changes.

Reading assignment 4

Subject: **Network Intrusion Detection Systems**

Pages: 161-184

(Complete before day 5)

1. w does an IDS capture information off of the network it is monitoring?

2. at are 2 methods used by IDS' to generate alerts?
   1.
   2.

3. efly describe each of them:

4. ne 4 actions an IDS can take upon detection of an event:
   1.
   2.
   3.
   4.

5. ere are IDS' typically placed in a network?

6. w do switches affect your IDS placement?

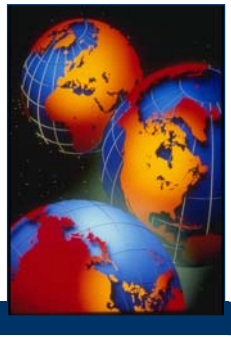
7. ine a "False Positive":

8. ine a "False Negative":

9. ne two methods hackers sometimes employ to avoid detection by an IDS:
   1.
   2.

RealSecure

Module 13



13-1

RealSecure Overview

- Real-time intrusion detection and response system
- Packet “greper” looks for signatures in the data stream.
- Active response, notification, and storage options
- Monitors the network traffic for “attacks” and “misuse”

13-1

Attack Detection

- 400+ different network danger signs:
  - Denial of service attacks
  - Network probes (port scans, SATAN scans)
  - Brute force attacks, password cracking attempts
  - Windows attacks, including WinNuke, remote registry accesses, and anonymous logins

13-1

Distributed Architecture

- RealSecure uses a distributed architecture and has two major components:
  - the Sensor
  - the Workgroup Manager

Note: Although not recommended due to performance issues, you can install both components on the same computer.

13-1

RealSecure Sensors

- The Sensor is a software component that is installed on a UNIX or Win2K/NT host.
- Sensors are installed on key network segments where you have critical data to protect.

13-1

RealSecure Sensors

- Sensors then examines all of the network traffic on their local segment.
- Sensors monitor network packets and look for signatures that could indicate an attack against your network

13-1

Sensor Specs

- OS
  - Windows 2000 or Windows NT
  - Solaris 2.6 and later
  - Linux
- System
  - 400MHz PII +
  - 256+ MB RAM
- Disk Space
  - 2 GB + (for logfiles and database entries)

Note: The Network card must support promiscuous mode.

13-1

Workgroup Manager

- The Workgroup Manager represents the central management points
- Receive alarms from Sensors
- Control the Sensors and configurations
- Aggregate data and generate reports about network activity.

13-1

Workgroup Manager Specs

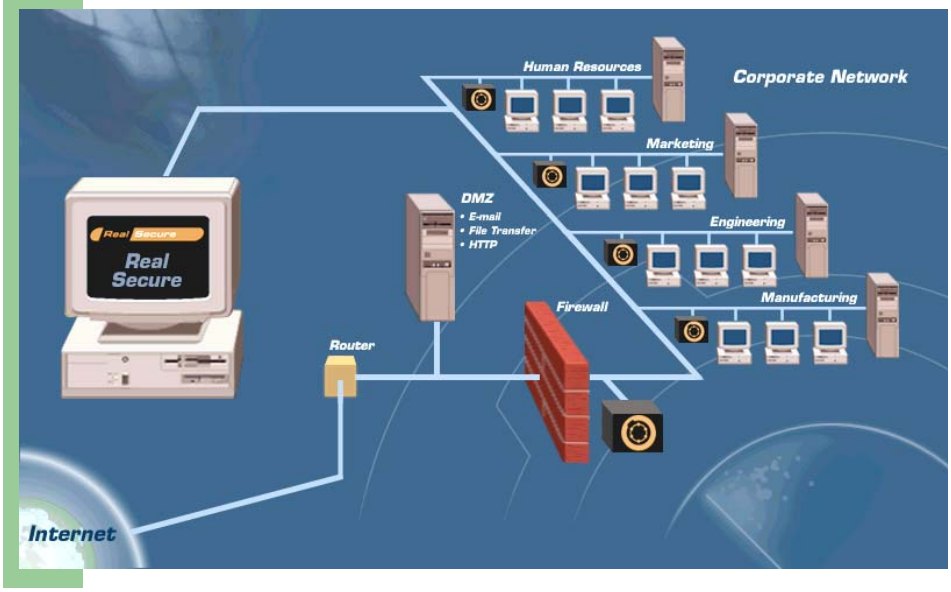
- OS
  - Windows 2000 Server or Pro w/SP1
  - Windows NT w/SP4 thru SP/6a
- System
  - 400MHz PII +
  - 256+ MB RAM
- Disk Space
  - 2 GB + (for logfiles, database entries)

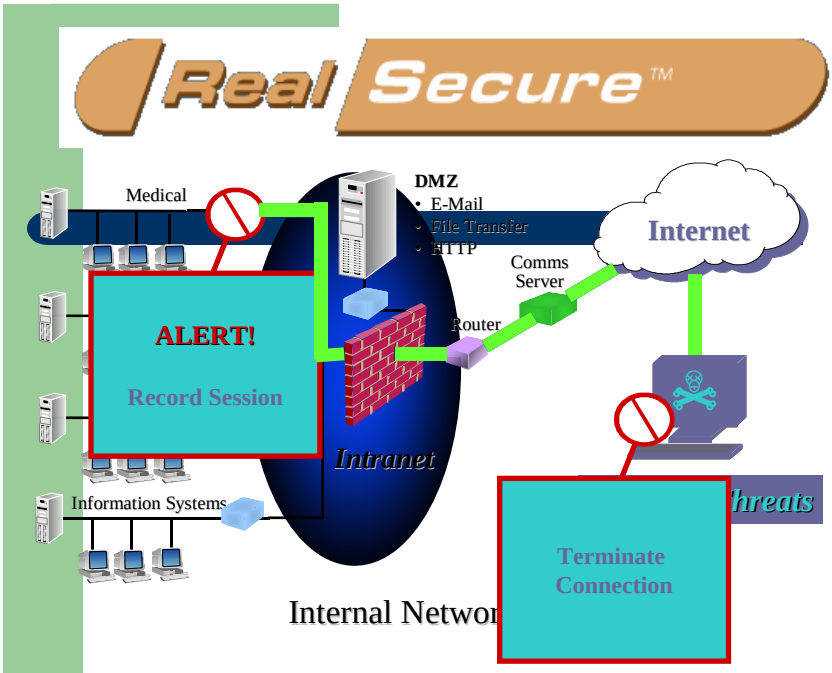
13-1

RealSecure™

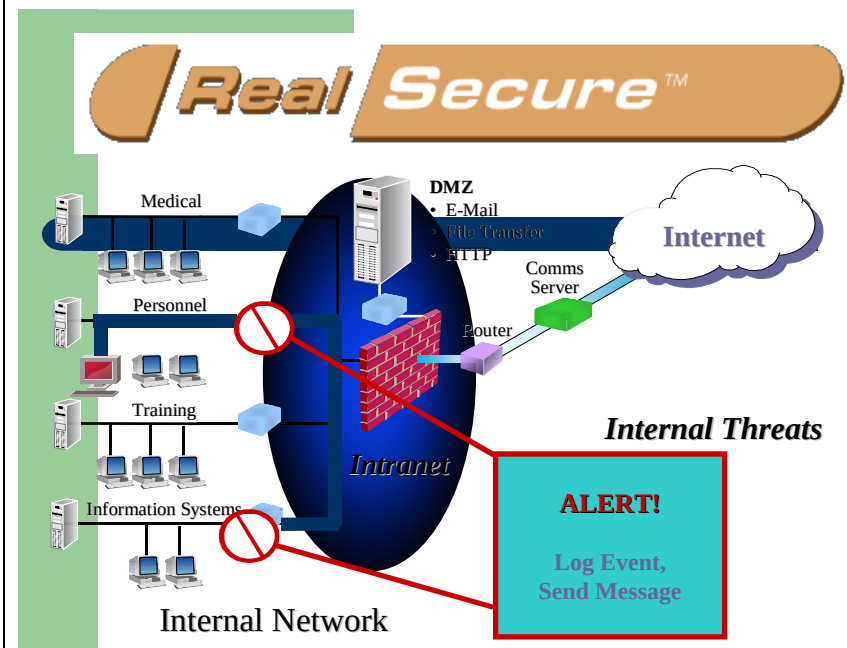
Features	Benefits
Operates 24 hours per day	Continuous network protection
Distributed client-server architecture	Centralized view of enterprise security status
Non-obtrusive solution	Avoids central point of failure
Industry's widest variety of attack signatures	Administrator not required to be a security expert
Customizable by the administrator	Can be configured to meet the needs of the organization
Six-to-eight updates per year	Always has latest attack patterns
Centralized configuration control	Allows configuration of all Detectors from one location

13-1

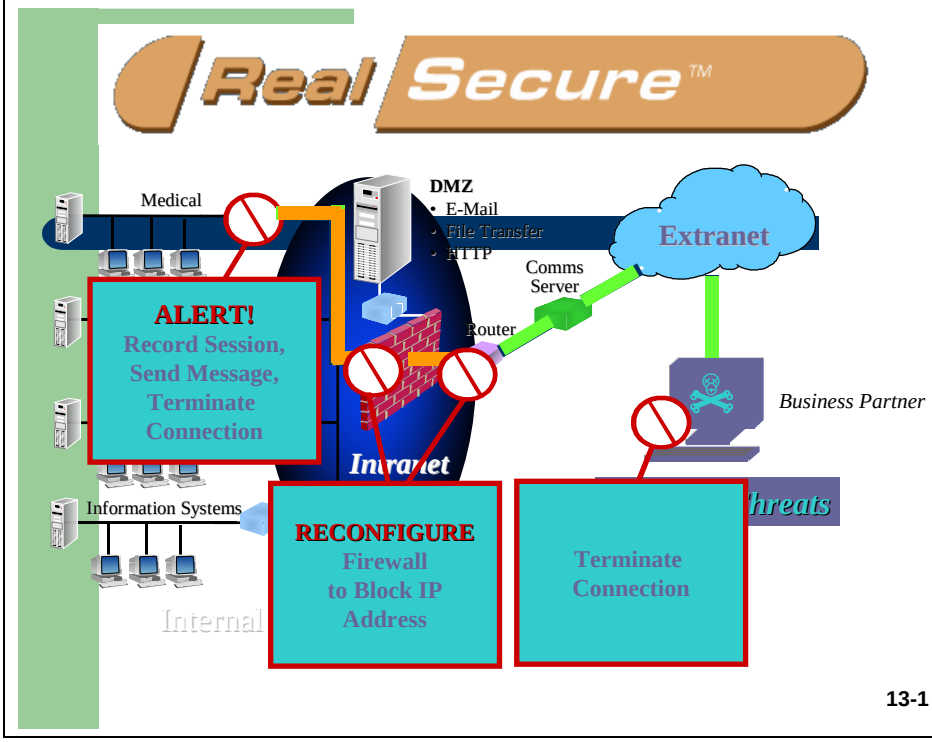

Real Secure™
Human Resources
Corporate Network
Marketing
DMZ
• E-mail
• File Transfer
• HTTP
Engineering
Manufacturing
Firewall
Router
Real Secure
Internet


Real Secure™
Medical
DMZ
• E-Mail
• File Transfer
• HTTP
Internet
Comms Server
Router
ALERT!
Record Session
Intranet
Information Systems
Threats
Terminate Connection
Internal Networ

13-1


RealSecure™
Medical
Personnel
Training
Information Systems
Internal Network
DMZ
• E-Mail
• File Transfer
• HTTP
Comms Server
Router
Internet
Intranet
Internal Threats
ALERT!
Log Event,
Send Message

13-1


RealSecure™
Medical
Information Systems
DMZ
• E-Mail
• File Transfer
• HTTP
Comms Server
Router
Extranet
Business Partner
ALERT!
Record Session,
Send Message,
Terminate
Connection
RECONFIGURE
Firewall
to Block IP
Address
Terminate
Connection

13-1

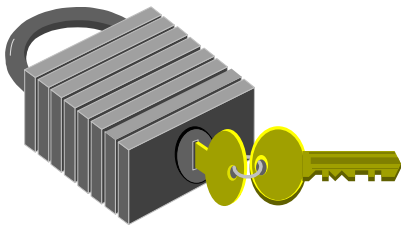
Authentication

- Each end of the communications channel will have its own private and public key pair.
  - Keys are generated at product installation.
  - For the highest level of security, public keys should be distributed among the components of the RealSecure system manually.
  - Ultimately, RS will use X.509 certificates to exchange public keys.

13-1

Encryption

- During installation, the administrator can select either weak (40 bit) or strong (128 bit) for the Sensor and the Workgroup Manager.



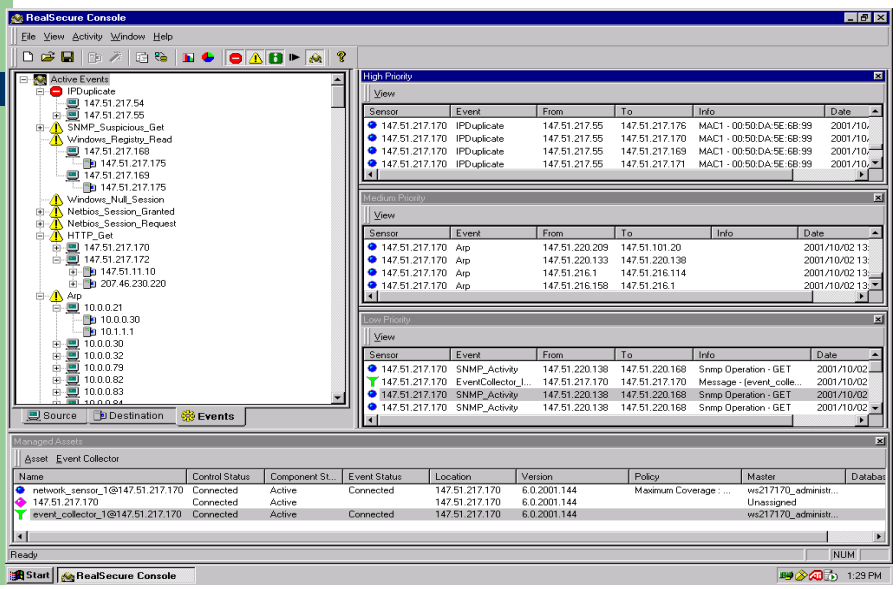
13-1

TCP Ports

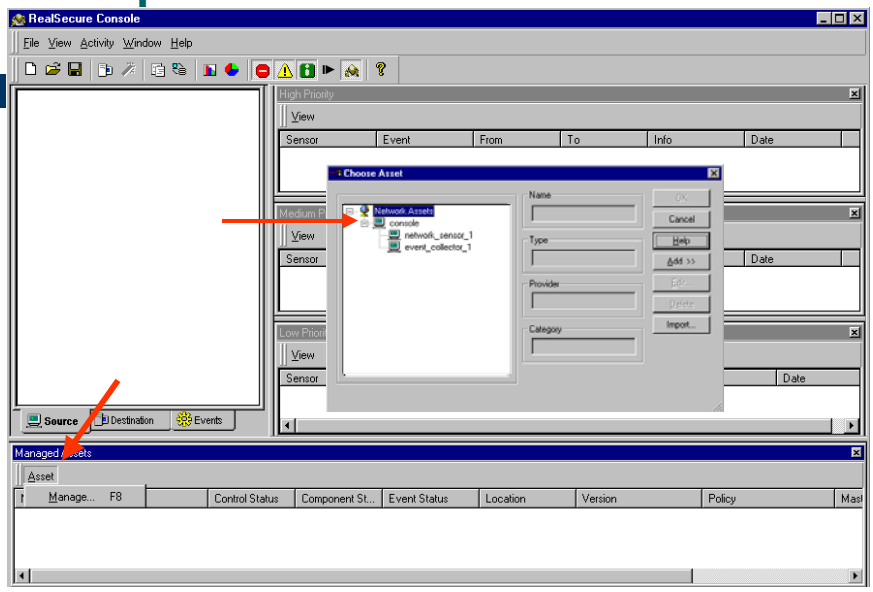
- TCP 2998 for management control data
- Dynamically assign an additional TCP port for exchange of event and log data (typically TCP 901).
- Override these defaults with your own preferences (ports already open through your firewalls, for example).

13-1

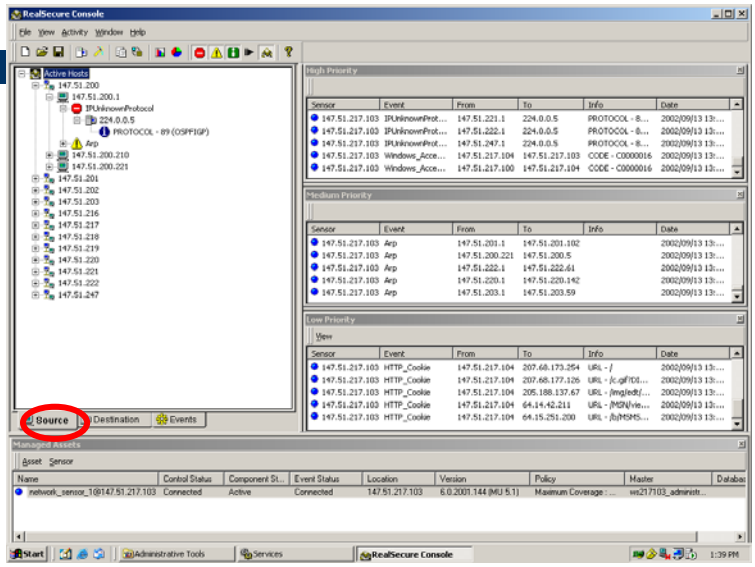
RealSecure Walk-through



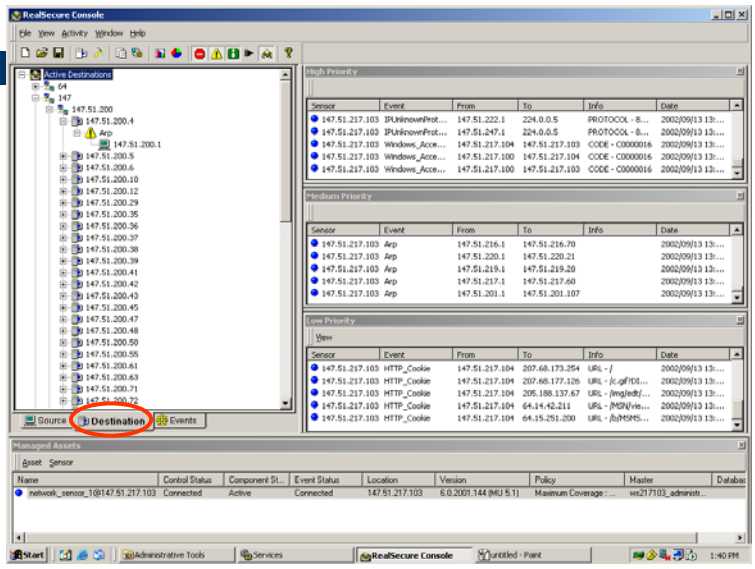
Fire up the Sensor



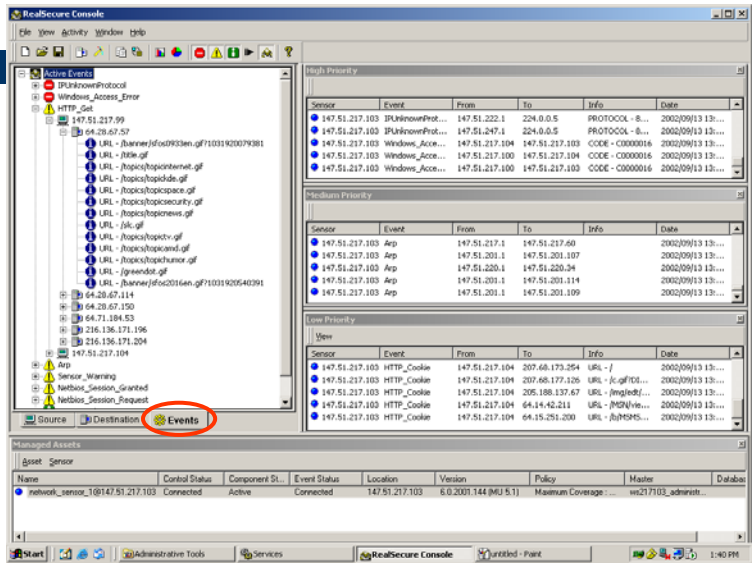
Activity Tree - Source



Activity Tree - Destination

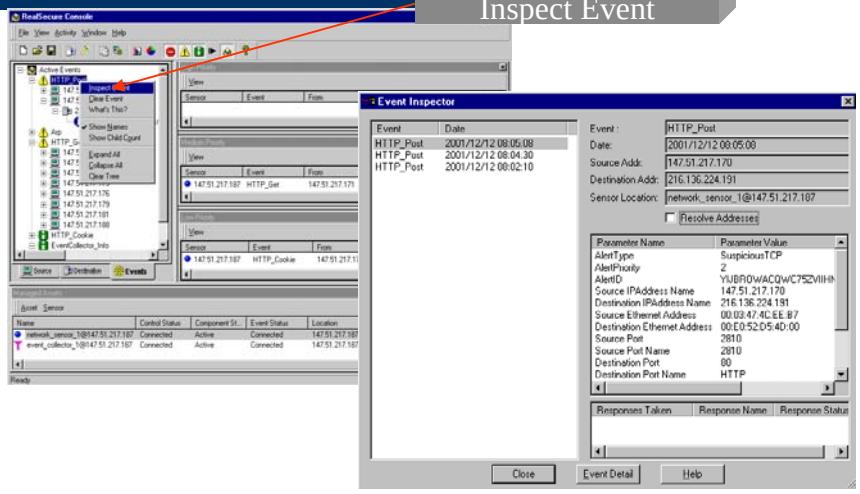


Activity Tree - Events



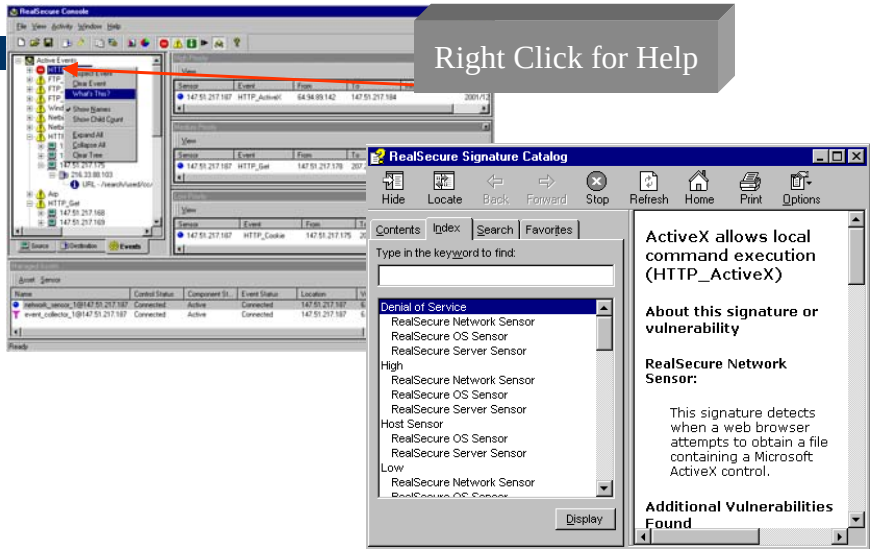
Inspecting Events

Right Click, then Inspect Event

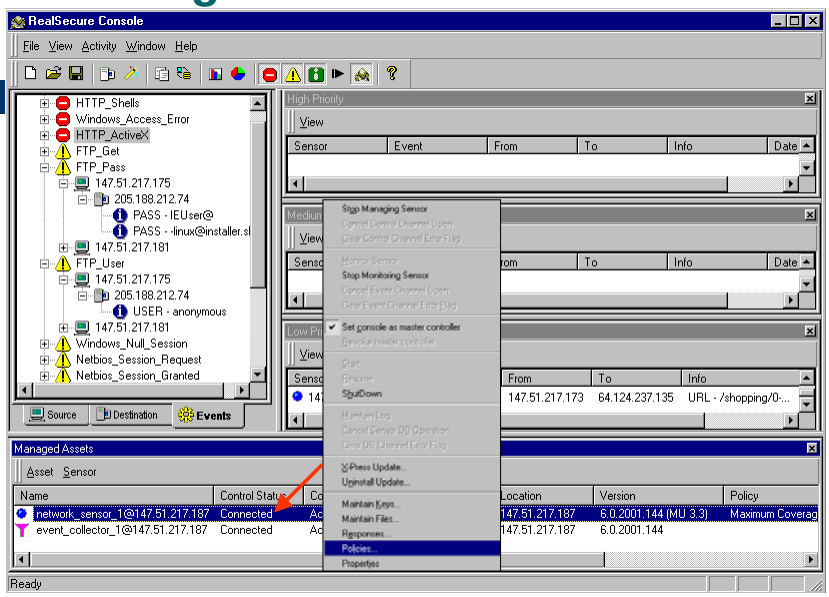


Priorities & Help

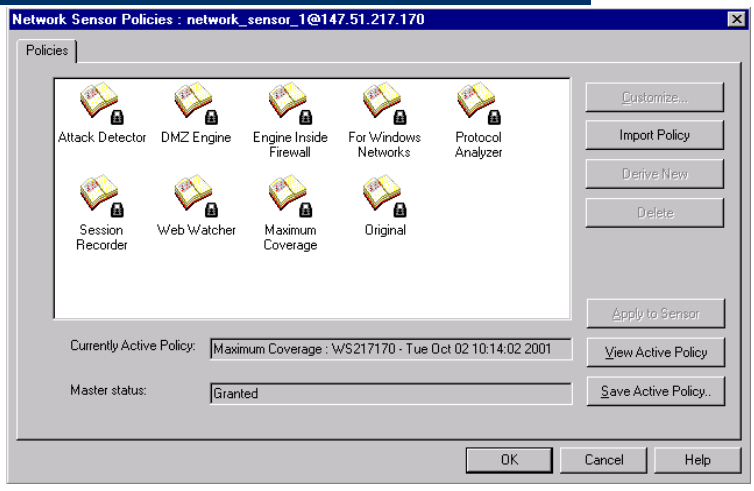
Right Click for Help

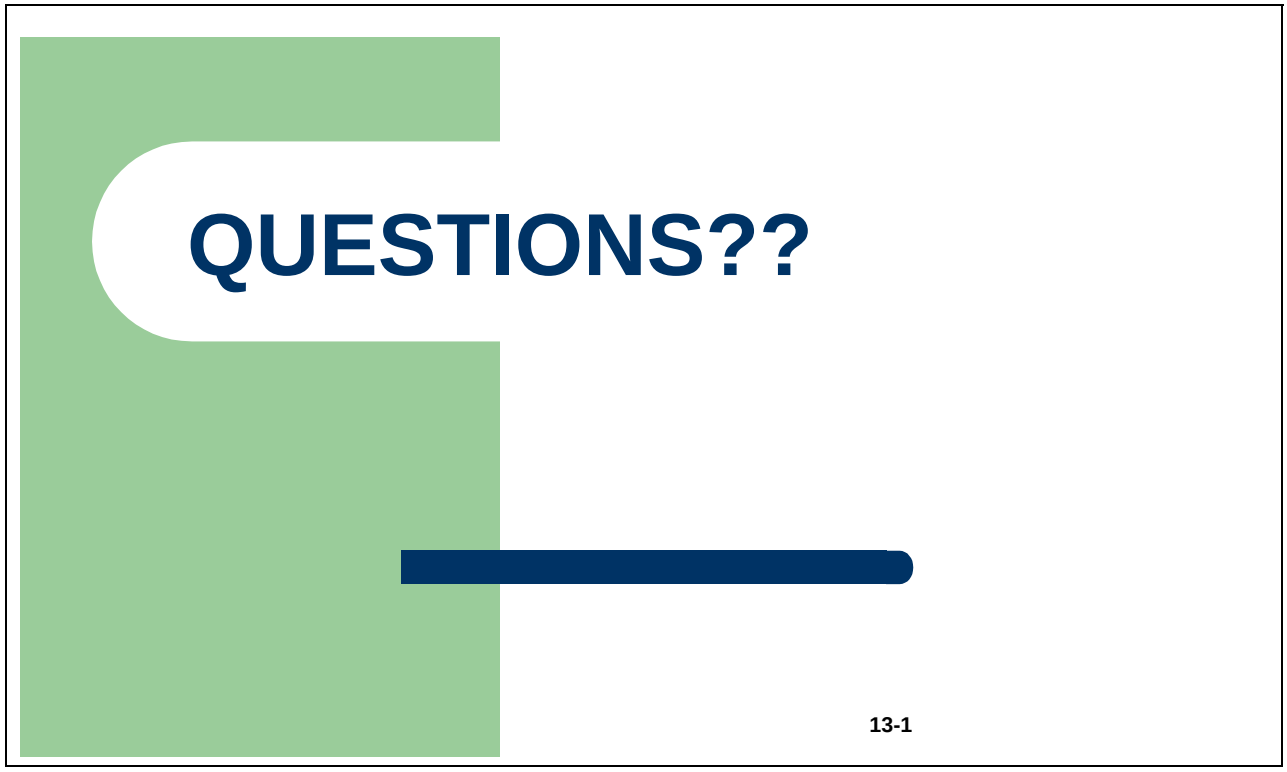


Sensor Engine Policies



Network Sensor Policies




QUESTIONS??
13-1

Intrusion Detection Systems (RealSecure)

Lesson 5

This practical exercise is intended as a supplement to material learned during the IDS and RealSecure lecture. Students will be expected to be familiar with concepts and basic operations related to the RealSecure Intrusion Detection System.

Objectives

1. Setup and operate Realsecure
2. Apply and modify policies
3. Observe real-time attacks

RealSecure Practical Exercise #1
Initialization

→ *Your ISS RealSecure IDS device has been installed already*
→ *Follow the instructions below and answer the questions*

1. Check on the status of the RealSecure application on your W2K server system:
   - **Start** > **Settings** > **Control Panel > Administrative Tools** > **Services**

   Is the RealSecure daemon (issdaemon) on? If not, START IT UP!!

   What is the STARTUP setting

   Would you want to have the STARTUP as "automatic" Why

2. Press **CTRL – ALT – DELETE**, then click **Task Manager** to bring up current processes.

   What processes are running for RealSecure? (Hint: they start with "iss")

3. Click on Start, Search, "For Files or Folders"
   - Search for a file named "iss.key" (There may be more than one, but they are identical)
   - Open up the file using Notepad
   - Scroll to the bottom of the "iss.key" file and write down the IP range and the key expiration date—save this for the next PE:

RealSecure Practical Exercise #2
Setup of the IDS Device

- *Your ISS RealSecure IDS device has been installed already*
- *The console is your configuration tool; the sensor runs in the background. Several sensors can be monitored per console*
- *Follow the instructions below and answer the questions*

1. Start the RealSecure application (console):
   - **Start** > **Programs** > **ISS** > **RealSecure 6.0**

2. RealSecure console screen will appear; then:
   - Click on **View** > **Options** (pull-down menu)

   This is the location of the key files on your hard drive.

   - Click on **View** > **Display Key** (pull-down menu)

   What is the Key expiration date? What is the key's IP range?

3. Start your detectors!
   - Go to the bottom-left window and click on the **Assets** > **Manage** option on the pull-down menu
   - Expand the tree, highlight **Network Sensor** and hit **OK** button
   - ***If the daemon is not reached, your key is invalid or your RealSecure daemon is not running Notify Instructor***

   What is the current component status

   What is the type of policy coverage

   Do you think this policy type can cause a problem monitoring the network? Why

RealSecure Practical Exercise #3
Port Scan and WinNuke

- *Your ISS RealSecure IDS device has been installed already*
- *Follow these instructions below and answer the questions*

1. Wait for the instructor to try a port scan against a target in the classroom:
   Did you detect the scan

   Were you able to determine which ports were scanned? If so, what ports did the instructor scan?

   What was the source of the scan?

2. Highlight the Event Name and **Right Click,** then **Inspect Event**
   What Alert Priority was it? Is this appropriate

3. Now, wait for the instructor to conduct a Win Nuke attack against the a target in the classroom:
   Did you pick up this attack

   What kind of event was this attack

   What priority was it (High, Medium. Low) Is this appropriate

RealSecure Practical Exercise #4
Web Watcher Template

- *Your ISS RealSecure IDS device has been installed already*
- *Follow these instructions below and answer the questions*

1. Go to the bottom-left window and highlight the **Network Sensor**, then right-click > **Policies**
2. Highlight **Web Watcher** and click on the **Apply to Sensor** button
3. Highlight Web Watcher and click on the view
4. Expand tree and highlight HTTP:
   List the following events:

PRIORITY **RESPONSE** **DESCRIPTION**

- HTTP_JAVA
- HTTP_PHF
- HTTP_PHP_READ
- HTTP_SHELL
- HTTP_WEBSITE_UP

5. Now, wait for the instructor to repeat his two attacks—Port Scan and Win Nuke—against the a target in the classroom:
   Did you pick up these attacks

   Why did (or didn't) you detect these attacks

RealSecure Practical Exercise #5
Capture Authentication Traffic

- *Your ISS RealSecure IDS device has been installed already*
- *Make sure that the **Max Coverage** policy is active*
- *Follow these instructions below and answer the questions*

1. Set your IDS policy back to "Maximum Coverage"
2. Wait for the instructor to go to his web browser – he'll try to log a web site that requires a username and password
3. Now, highlight the HTTP_COOKIE event:
   What kind of event ("What's this?") is HTTP_COOKIE

4. Highlight any URL under the HTTP_COOKIE event:
   What kind of info do you get here

   What does HTTP_GET signify

5. Look at HTTP_AUTHENTICATION
   Can you read the password sent from the instructor's browser

   What would it take to safeguard the password via the web

   What does the HTTP_AUTHENTICATION events signify

   What are the source and destination of this event?

RealSecure Practical Exercise #6
RealSecure Reports

- *Your ISS RealSecure IDS device has been installed already*
- *Follow the instructions below and answer the questions*

1. On the RealSecure Console (upper left), click on **View > Reports** on the main pull-down menu.
   Note: If asked to SYNCHRONIZE LOGS, click on **File > Synchronize All Logs.** Then try #1 again.

   What were the top 5 events?

   What were the top 5 destinations?

   What were the top 5 source locations?

   What were some of the most active source and destination IP's?

Appendix A – Public Key Example

```
-----------------------Here is a copy of my public key:-----------------------

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.7 (GNU/Linux)

mQGiBD1SuUURBAChB8cgzc8UuPC23VZ5Zta1O/DFf8vIAHU45d8stZ8PR3oWrK5U
30xg02DCeqJSwCGNd7yCOhy5KMJg26r5H/688GYCpA7Q043gZiMyRibDVWaONo/p
/4zKDFDw/4OHZ7tiGwPa1pmasc0AmdVIR2cJ3jjwbNIZk8TQ64n/YWiL/wCgwW+w
sVxXerOPKefeidlZkBKqs6sEAI6q8Y8RP22tqrJR5NsfJkOV7JGU/nfQwMP0l+Lm
o4CjBcY4/9UjXYTXmzJUJ3tc4PD+cm+1cH8T04IlobdJV1JZ4JjS/eixJCxvYtAs
U0fq1Mj9Cwee4R1k6gMI0hbunTTSXD7W55loRYZMRLdNELlYENGDQwIQeNgKyf02
wBEjA/0cdTumFOZmSVt+RY8nbkzSMOZpoW4xOkUg83vP/ZuvMlkpdonDD2yOBfh9
RzpellV5TAyR2iAUJcXwCHbvhYEi0ZptHCk0aXKLnKE4Af9YYSggJtCXGQrsMOIW
zYUiKWMHUegdVwRA31Igm7ILCgjTG77V8oRpESn63XNGJGWl07Q2Q2hhcmxlcyBK
b25lcyAoQzItUHJvdGVjdCkgPGxpbnV4Y2h1Y2tAcGhvZW5peGJveC5vcmc+iFkE
ExECABkECwcDAgMVAgMDFgIBAh4BAheABQI9UrlHAAoJEK8V6KhJF2a26HAAnR+S
bYtIY19Ayeo1EsFKJDGFHFojAJ0QLHeALOSW1rUj3SX8UXo2O+mbMLQ8Sm9uZXMs
IENoYXJsZXMgTS4gKFNBL05NLVNlY3VyaXR5KSA8am9uZXNjbUBnb3Jkb24uYXJt
eS5taWw+iF8EExECAB8CGwMECwcDAgMVAgMDFgIBAh4BAheAAhkBBQI9Usa2AAoJ
EK8V6KhJF2a2RI8AnAgPwetWLqfBabbZ/byFOlX/QYTCAKCQnx15mN9e4+1biseC
Nqm/dAl+YrkBDQQ9UrlGEAQA22hNqWGRBhAdKvopGkR8yQlsD7egdyHYSLXN/A7o
uMGAEYBEpuS0eeTBbn0p13oXsW6MM6v1kjW9LJuz3GUqBUCx0qjvZ2IJdV9a3eyz
cfLsT0pGiH0Fo+8dZCX+G4neGTLsRVie9qBT/3l4hZ6QeMLKpwtvXXtzFMSrfMmH
SYcAAwUD/jj/89QwKbcCkqJePJ2f8aKOKaHw2nZRX+JYckkmm+BTOFf10e3uycL9
/tS1xwFRLWEL2wv30GBHfm6tHOQqVY99gHMzPtMWMeoVws3wYQDY54eLtqUyuhKH
RvUAjNjqWWv93Pkm5j92kqXferi9lhMvRPnEfhWHqUdGtUHxdinziEYEGBECAAYF
Aj1SuUYACgkQrxXoqEkXZrapwQCfYvRzfKD9CdRLhin3Bic9oLazGYUAnRmXmBP/
6PNlWRI09R5nQqayPqni
=uyZt
-----END PGP PUBLIC KEY BLOCK-----

----------------------------example test message-----------------------------

This is a test message for classroom usage of the PKI example

Charles Jones

----------------------------signed test message-----------------------------

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

This is a test message for classroom usage of the PKI example

Charles Jones

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE9hY9GrxXoqEkXZrYRAls1AJ9tTx9o0ROy/Ex2Th/C4zAOgynBtACguOqr
ojHGB5rTYeE3H2xua7ONjiw=
=oVkI
-----END PGP SIGNATURE-----
```

```
-----------------------------encrypted test message--------------------------

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.7 (GNU/Linux)

hQEOAzeF/JeNCXxyEAQAtK8KNr46viwTh1E+sklvwrc/KKz0X5h5tpXSCbsvAOBi
BNpeJGdoxQVijVA7nGzroGPIF9WDsJCdbnu7Cg/K6m9Tq2/FnZTk7t9a2lxw/T0h
Z3mM+96urKZIKeH3uLK/hvhIW3CWSfunrM+IUhBT6AewGv7RQjUQtyKmgg2uKmQE
AKbwdklSFEOPdQLILwWV8Y4IgRgGghJk6HTAiHbyvFlKDPtHOSO3fwMzfAKJf3ex
ZznCj6+wcG1oLUDppxxGRbJyc1LqsLzNUozhWbJL2tbFziMgg0HzD7uw1h40hKRR
Mh49ZU4/6Pt3/ENqZiIoeK5x0cdeAm+Mc45jxt0lOO1A0sB7AYkURk1e/3Q8X8V6
dBvzWLyFt8ynUkXB+NO7AOdv97fclvrUjF6B2kRNADCfg9yhg2rQreVAuSrGrUg3
+CtWXl3boGK9NrabLz9wKG3mZfmHKHV/GhRyE7FFqBUYKqMCL7ptpKodYFcDAAtX
0HmxtEU6ycJb0tDwHv4p0/dCA8DqAGP43JKgoe/81+rQWK/tvHspk/v1VdF5ZwLO
7szgX0rMr59eyP52FoDzXXd8otjOCqCn4QyCLd7sisI8EUxVculM6/cSqVuj/RQ2
22DF8yWn4yVziTSi6qP/htXJQo2JAy9H86q4Jld7xH4XiWdJW/RuoQgeYtnXhok3
/QZ9YmGFZ3TLppcax4MksGc+qwnPRPMLU82+PZceFHt154Rtdvqyuu9Uvzt4vQvv
QUUDENa2uTCx72apaUrD
=xOMA
-----END PGP MESSAGE-----
```