Basic Types of Attacks

1. Packet Sniffing
2. Denial of Service/(SYN and SMURF attack)
    - flooding a network with request in order to overwhelm it
3. Malicious Code
    - Trojan horses, worms, viruses
4. Exploitation of Trust/Session hijacking
5. Spoofing
6. Brute force attack

Sniffing

- Passive security attack.
- Machine different from intended destination reads data on a NW.

Spoofing

- A m/c masquerades as a different m/c.
- Disrupts normal flow of data.
- May also inject malicious data into the NW.

SYN Attack

By filling up the queue with bogus connection requests, the attacking system can prevent the system from accepting legitimate connection requests. Thus, a SYN attack is considered a denial of service.

smurf

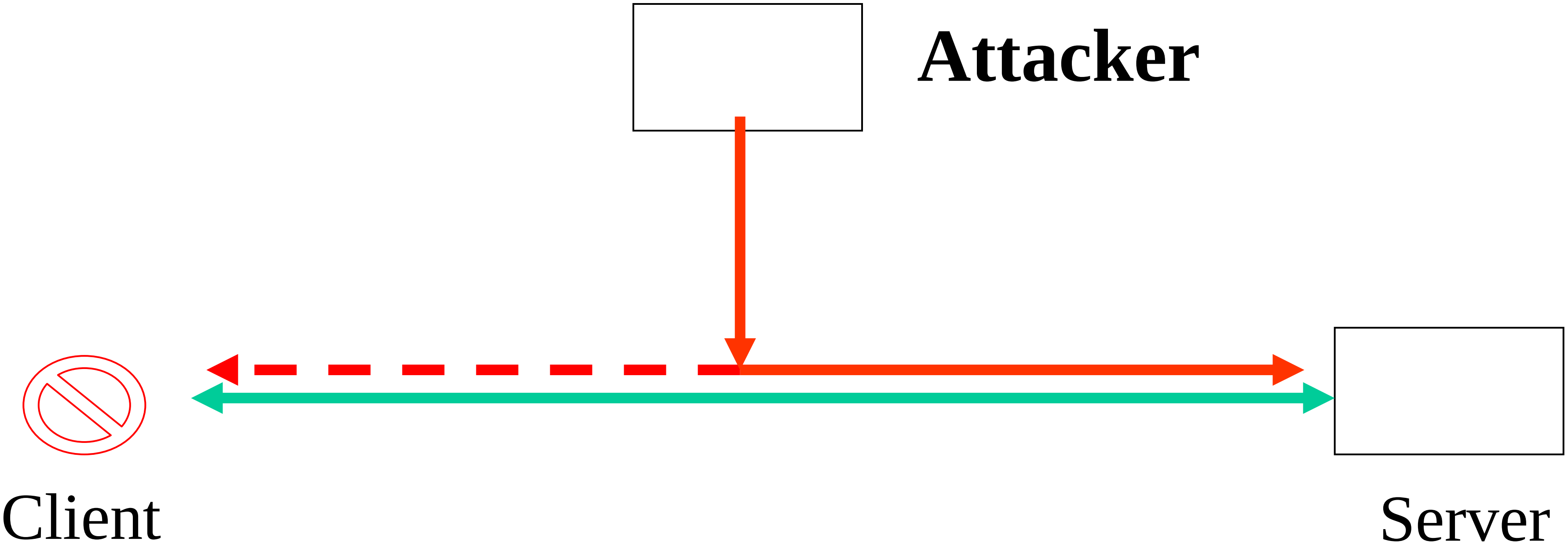
- Saturates a host with traffic thus causing a denial of service

Brute Force Attacks

- Attempts to try all possible values while authenticating
- May focus on breaking the crypto key

Session Hijacking

The source has been replaced by an attacking host in the course of communication session.



The Cost of Lax Security

- **Money**

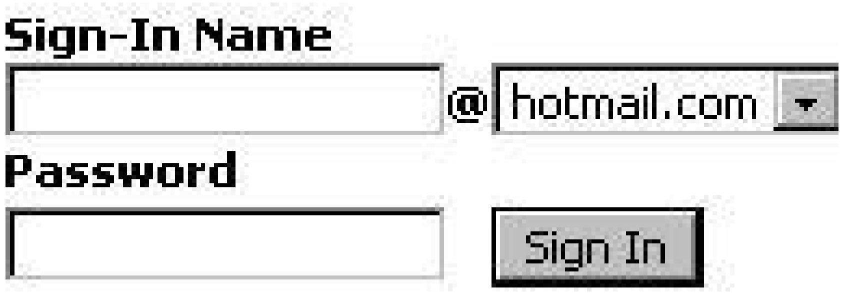
  costs associated with hiring temporary staff to repair damage and recover data

- **Time**
  - staff time needed to repair damage, recover data, supervise temps
- **Compromise in Security**
  - Confidential document can land up in the wrong hands.

Primary Goals of a Good Security System

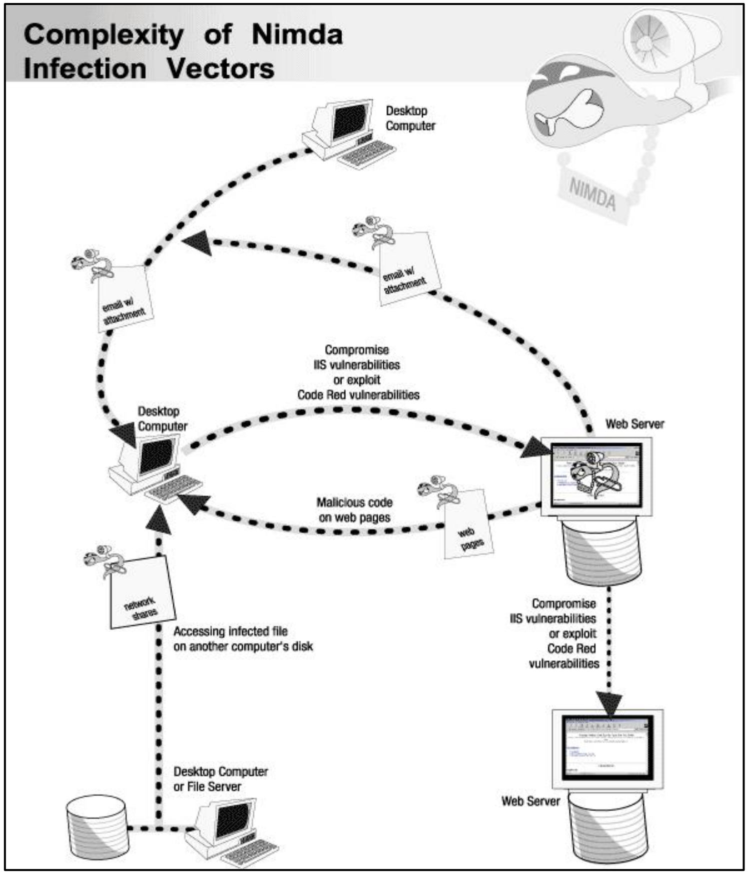
1. Protect Confidentiality
2. Ensure Data Integrity
3. Ensure Data Availability

Protect Confidentiality



- Keep passwords out of the wrong hands
- Prevent access to
  - financial information
  - circulation records
  - Confidential letters/information
  - network information

Ensure Data Integrity


Complexity of Nimda Infection Vectors
Desktop Computer
NIMDA
email w/ attachment
email w/ attachment
Compromise IIS vulnerabilities or exploit Code Red vulnerabilities
Desktop Computer
Web Server
Malicious code on web pages
web pages
network shares
Accessing infected file on another computer's disk
Compromise IIS vulnerabilities or exploit Code Red vulnerabilities
Desktop Computer or File Server
Web Server

- Ensure that you can recognize and recover from breaches of integrity
- Protect systems from viruses, worms, Trojan Horses
- Allow only appropriate physical access to computers

Ensure Data Availability

- Recognize and defend against denial-of-service attacks, viruses, worms
- Use good backup and recovery procedures
- Ensure service is not interrupted during routine hardware and software maintenance

Steps of Security Lifecycle

1. Identify Assets
2. Identify Threats and Vulnerabilities
3. Create Security Policies
4. Devise Protection Strategies
5. Constantly Monitor and Update

Identify Assets

An asset is something of value to your organization

1. **Information**
   1. Passwords
   2. Databases
   3. Confidential and Restricted document
   4. Staff Documents
   5. Circulation Data
   6. Staff Addresses
   7. Financial Records
2. **Systems**
   1. Army Network System
      1. Army E-Mail System
      2. Army web server
      3. Army data server
3. **Hardware-** Staff computers, Public access computers, Printers, Servers, Backup devices, Telecommunications equipment, Cables
4. **Software**
5. **People**

Identify Threats

1. ***People***
    1. who can deliberately or accidentally cause harm
    2. using network access (either internal or external)
    3. using direct physical access
2. ***Systems***
    1. software defects
    2. hardware defects
    3. malicious code
    4. flaws in implementation
3. ***The Force***
    1. natural disasters

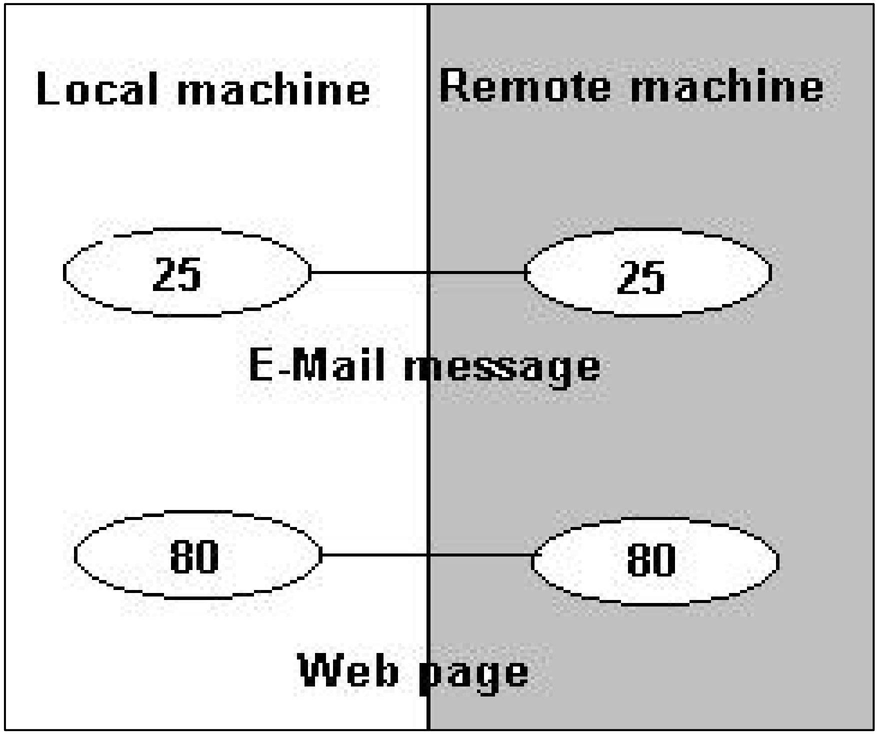
Loopholes and Vulnerabilities

1. Patches for known security problems not applied
2. Software Installation Defaults Not changed
3. Network access to internal hosts not monitored
4. Insufficient authentication systems
5. No intrusion detection tools used.
6. Ineffective Use of Passwords
7. Unreliable Backups
8. Too Many Open Ports and Services Running

Ineffective Use of Passwords

- Default passwords used
- No passwords used
- Easily guessable passwords – given names, dates, words out of the dictionary
- Passwords are less than eight characters long
- Passwords not changed often (or ever)
- Passwords written on post-its stuck to monitors
- Passwords shared with co-workers

Too Many Open Ports and Services Running



- A port is the identifying number of a service
- The more ports your servers have open, the easier it is to connect to that server
- The types of ports your server has open can give away a lot of information about it

Not Analyzing Incoming Packets

- Analyzing incoming packets allows you to weed out packets that don’t match rules that have been built into a network device’s table of acceptable traffic
  - spoofed packets
  - packets utilizing the wrong port for a service
- Watch for bursts of activity indicating a denial of service attack
- Does the traffic on a port match the activity

Unreliable Backups

- If backups are not made daily, or at an interval acceptable to your organization, you won’t be able to quickly recover from a security breach
- Establish off-site storage location for backup media and hardware needed for restoring system
- Test the integrity of your backups
- Test your backup procedure against different scenarios

Yet More Threats and Vulnerabilities

- Email Attachments
  - Viruses and worms arriving via e-mail are a constant threat to computers and networks
- Workstation alteration
  - Any computer is vulnerable to accidental or intentional alteration of operating system files
- Log files not monitored
  - Log files contain important clues about attacks
- Web browsers
  - Java, Active X and other scripting languages open large holes into a computer

Security Toolkit

- Firewalls
- Traffic Analyzers / Network Monitors
- Log Monitors and Alerts
- Intrusion Detection System
- Password Testers/Crackers
- Anti-Virus Software
- Trained Staff

Security “Best Practices”

- **Never assume a default software installation is secure**
  - – Apply appropriate patches and service packs to new installations
  - – Only install what you use
  - – Eliminate default user accounts
  - – How to know what to do: check the product support website
- **Always require strong authentication**
  - – A “strong” password is 8 or more characters and has a combination of alphanumeric characters and symbols
  - – Passwords should never be based on personal attributes
  - – Test passwords by attempting to break them with password cracking tools
  - – Use alternative forms of user authentication such as smart cards or biometrics
  - – Change default account passwords or remove them entirely

- **Always perform and verify backups**
  - Backups should always be performed, and at regular intervals
  - Rotate backup media offsite
  - Document backup procedures
  - Maintain copies of operating systems, application installation media and any necessary hardware offsite
  - Verify every backup
  - Test restore procedures
  - Establish different restore procedures for different scenarios

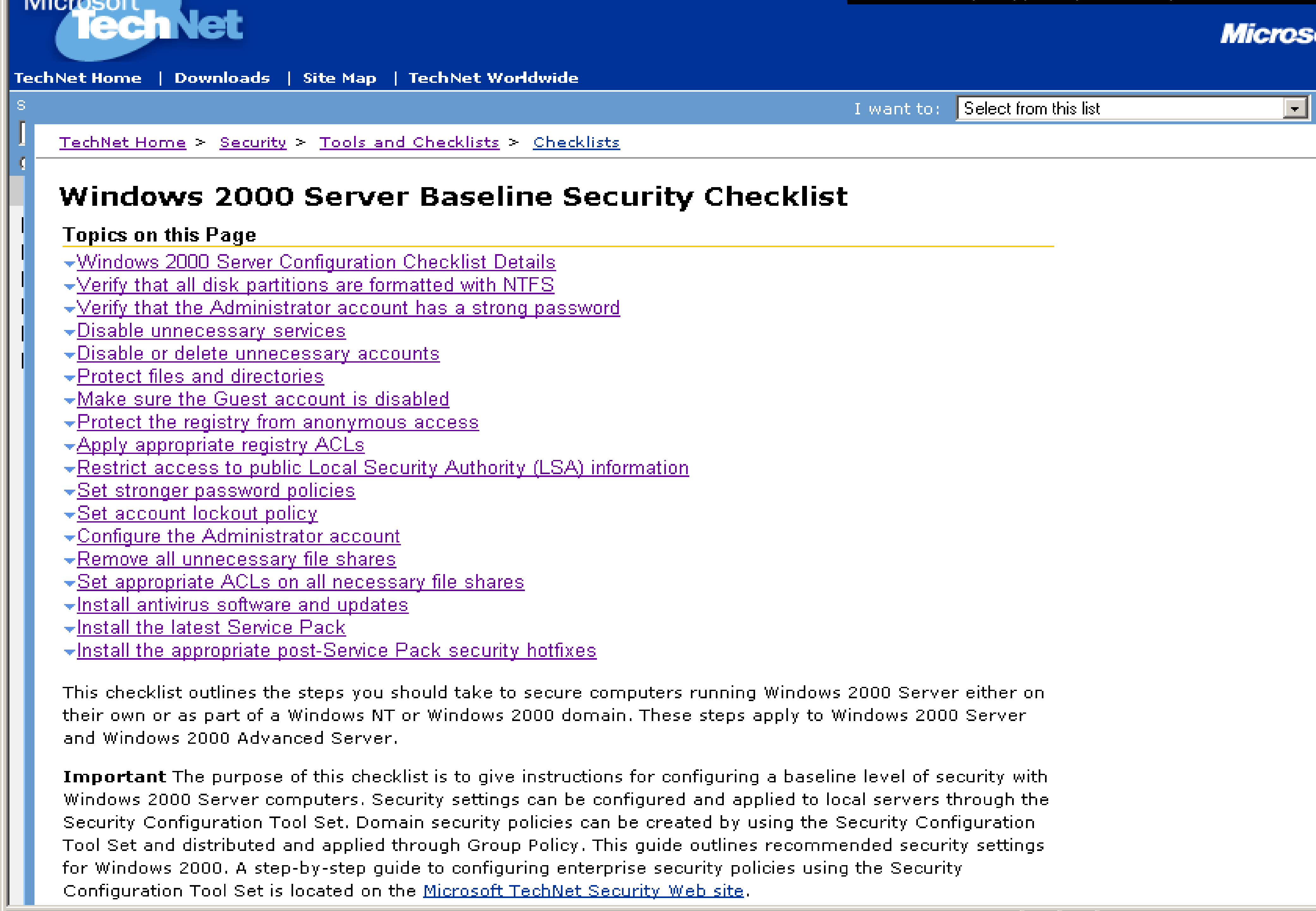
Security “Best Practices”

- **Close all unused ports**
  - Use scanning tools to check for open ports
  - Always uninstall unused services
  - Learn what services run on what ports
- **Protect Your Network Boundary**
  - Purchase and install a firewall
  - Check Point FireWall –1
  - Cisco PIX Firewall 515
  - Symantec Enterprise Firewall
  - Firewall Toolkit (FWTK)

- **Use anti-virus software**
  - Anti-virus software is a necessity
  - Virus definition files must be constantly updated
  - Prevent the acquisition of boot sector viruses by changing the boot sequence of all computers
  - Prevent worms by removing network shares
  - Run anti-virus software on servers and workstations regularly

Security “Best Practices”

- **Always monitor logs**
  - System logs should be maintained
  - Logs should be reviewed at regular intervals
  - If possible, configure logs to alert IT staff if an intrusion is detected
  - Backup and archive logs
  - Log Monitoring Tools - SWATCH
- **Keep software patched**
  - Software Release
  - Vulnerabilities discovered
  - Vulnerabilities published
  - Patches released
  - Patches can sometimes create more problems than they solve


Microsoft TechNet
Microsoft
TechNet Home | Downloads | Site Map | TechNet Worldwide
I want to: Select from this list
TechNet Home > Security > Tools and Checklists > Checklists

Windows 2000 Server Baseline Security Checklist

Topics on this Page

This checklist outlines the steps you should take to secure computers running Windows 2000 Server either on their own or as part of a Windows NT or Windows 2000 domain. These steps apply to Windows 2000 Server and Windows 2000 Advanced Server.

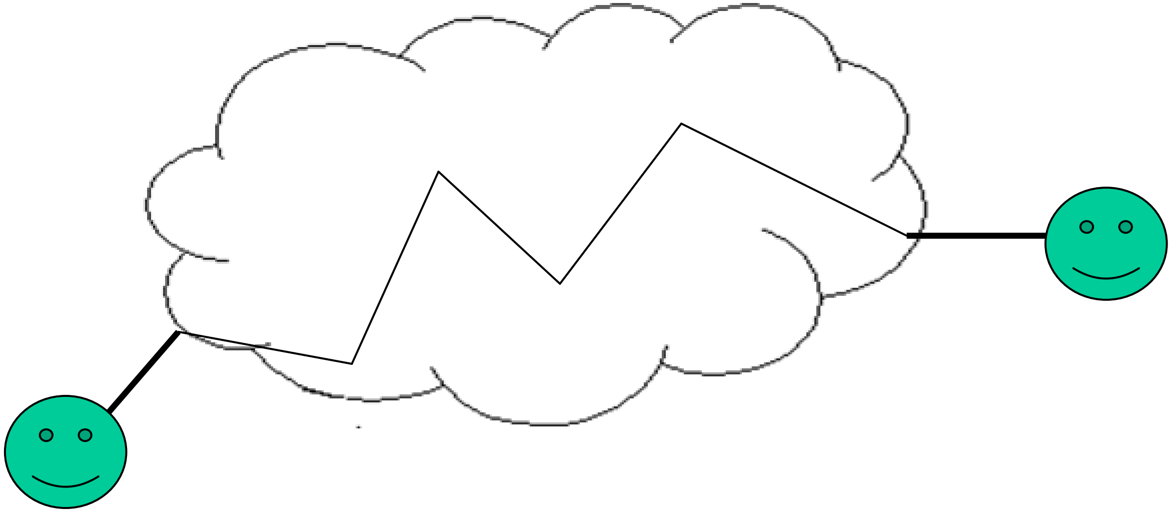
Important The purpose of this checklist is to give instructions for configuring a baseline level of security with Windows 2000 Server computers. Security settings can be configured and applied to local servers through the Security Configuration Tool Set. Domain security policies can be created by using the Security Configuration Tool Set and distributed and applied through Group Policy. This guide outlines recommended security settings for Windows 2000. A step-by-step guide to configuring enterprise security policies using the Security Configuration Tool Set is located on the Microsoft TechNet Security Web site.

Recommended Steps to Take After A Breach

- Notify security team immediately
- Isolate systems
- Capture information
- Notify appropriate parties
- Obtain fix/patch
- Change relevant passwords, encryption keys or anything that was breached
- Restore system
- Reconnect

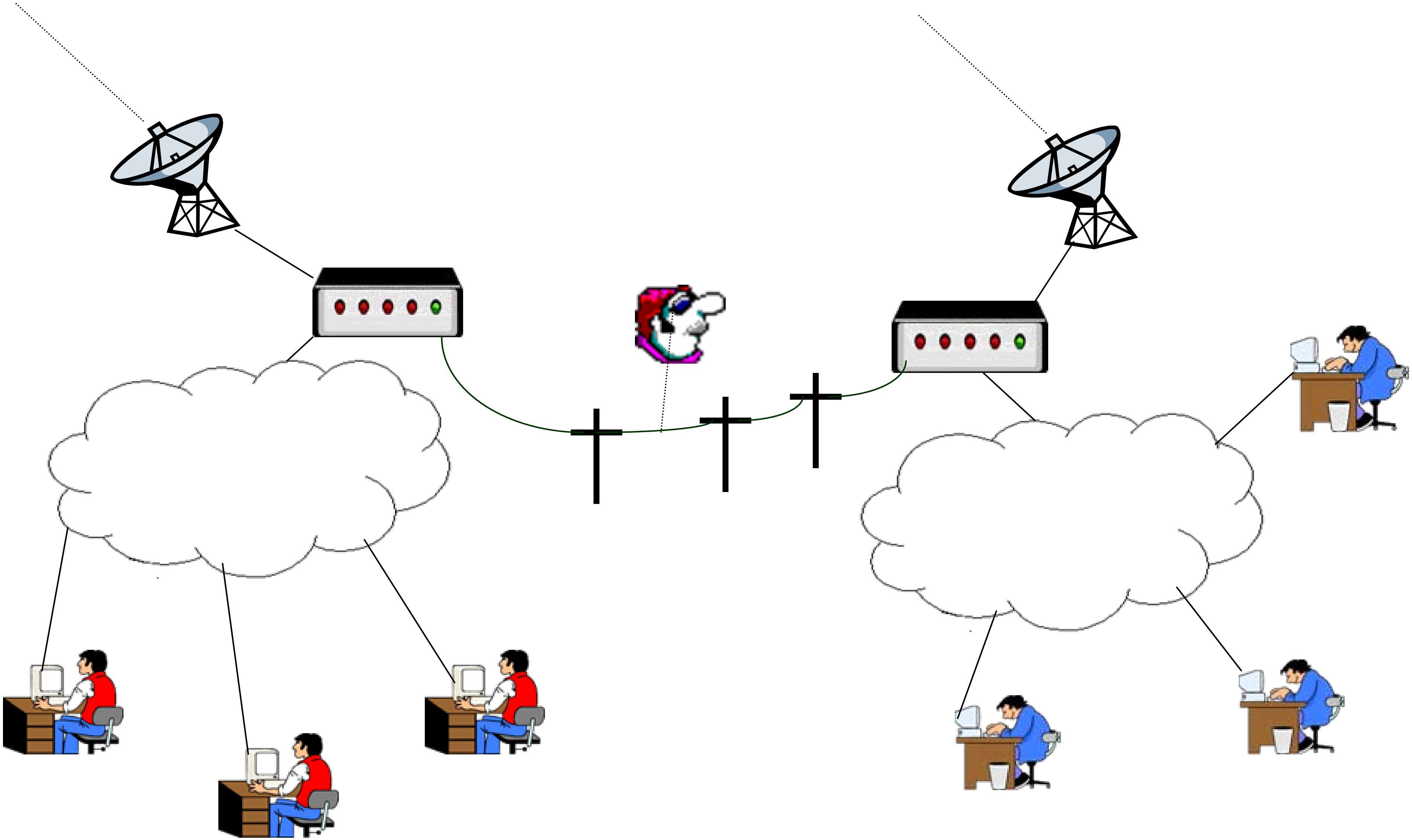
Cryptography

Traditional Telecommunications

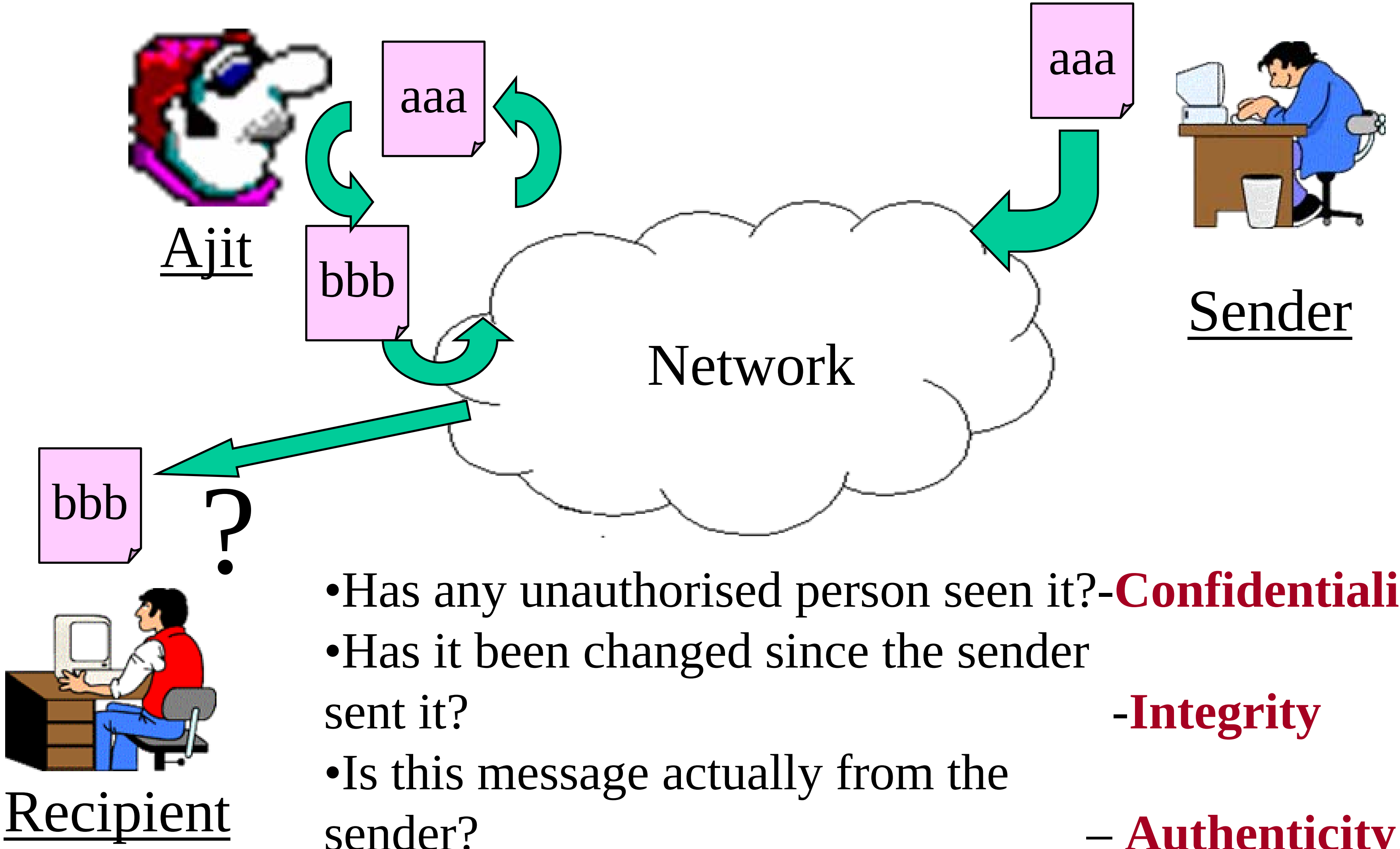


- A physical circuit exists for the duration of the communication.
- Users or applications are directly connected to the end points of the cct.

Computer Networking Scenario



Secure Document Delivery



- Has any unauthorised person seen it?-**Confidentiality**
- Has it been changed since the sender sent it? -**Integrity**
- Is this message actually from the sender? – **Authenticity**

What is the solution?

- Prevent any unauthorised person from accessing the network
  - This may not be possible because the entire network may not be under your control
  - Even dedicated channels cannot guarantee 100 foolproof security.
- Make the message itself secure so that even if someone reads it it will not be understood

Cryptography

A major concern has been that just how secure the Internet is, especially when you're sending sensitive information through it. There's a whole lot of information that we don't want other people to see, such as:

- Credit-card information
- Social Security numbers
- Private correspondence
- Personal details
- Sensitive information like pertaining to defence
- Bank-account information

Cryptography

The most popular forms of security rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it.

Cryptography

Computer encryption is based on the science of **cryptography**, which has been used throughout history. The existence of coded messages has been verified as far back as the Roman Empire.

Most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer to crack.

Statistics on key search

Key Size (bits)	***Number of Alternative Keys***	***Time required at 1 encryption/ms***	***Time required at 10^6 encryptions/ms***
32	2^{32} = 4.3 x 10^{9}	2^{31} ms = 35.8 minutes	2.15 milliseconds
56	2^{56} = 7.2 x 10^{16}	2^{55} ms = 1142 years	10.01 hours
128	2^{128} = 3.4 x 10^{38}	2^{127} ms = 5.4 x 10^{24} years	5.4 x 10^{18} years
26 char permutation	26! = 4 x 10^{26}	2 x 10^{26} ms = 6.4 x 10^{12} years	6.4 x 10^{6} years

Note: key size of DES algorithm - 56/128-bit

Cryptography

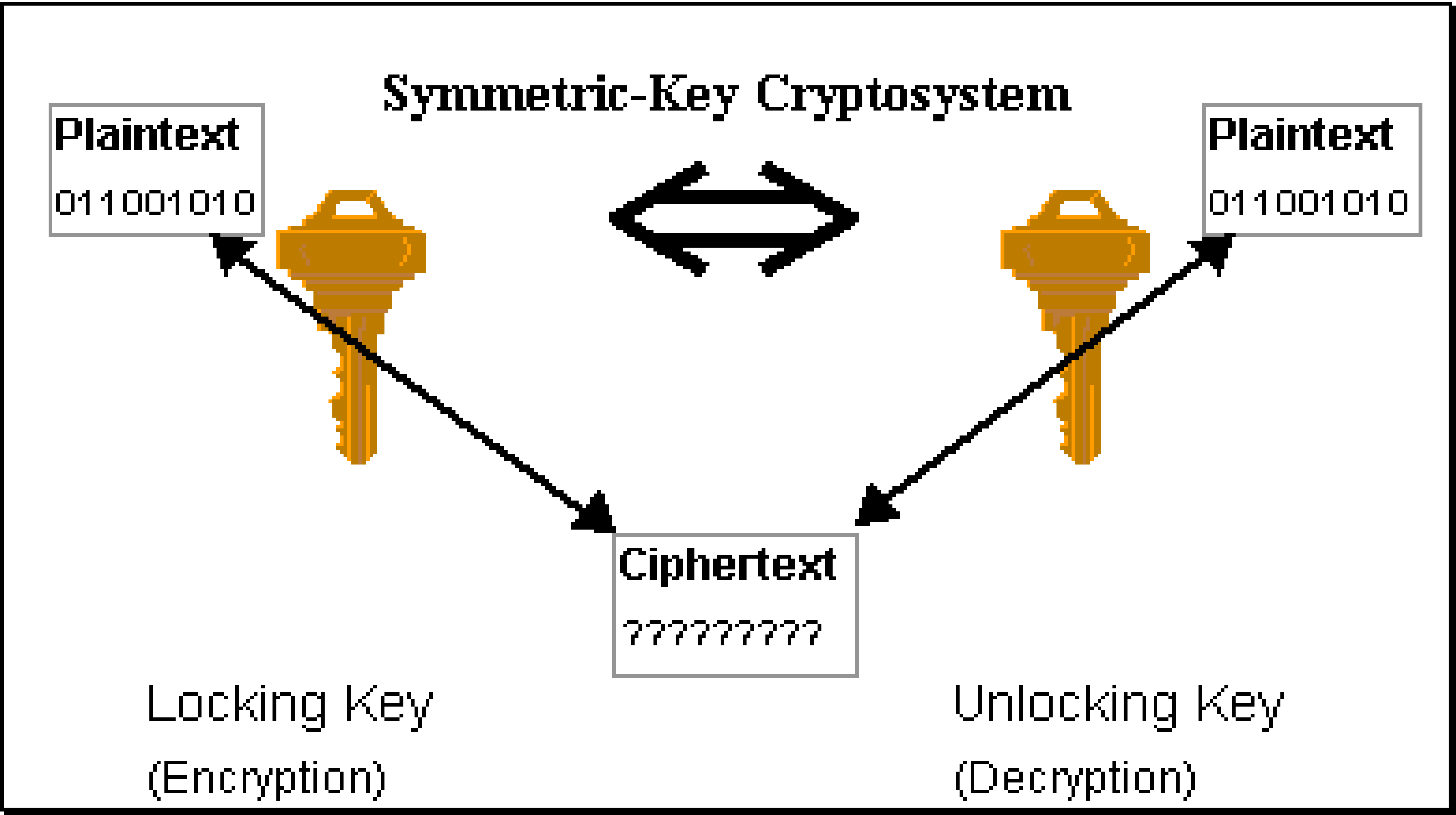
Most computer encryption systems belong in one of following categories:

- **Secret or Symmetric Key**
- **Public or Asymmetric Key**
- **Hash Function.**

Secret or Symmetric Key

In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plain text and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that both the sender and the receiver must know the key; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

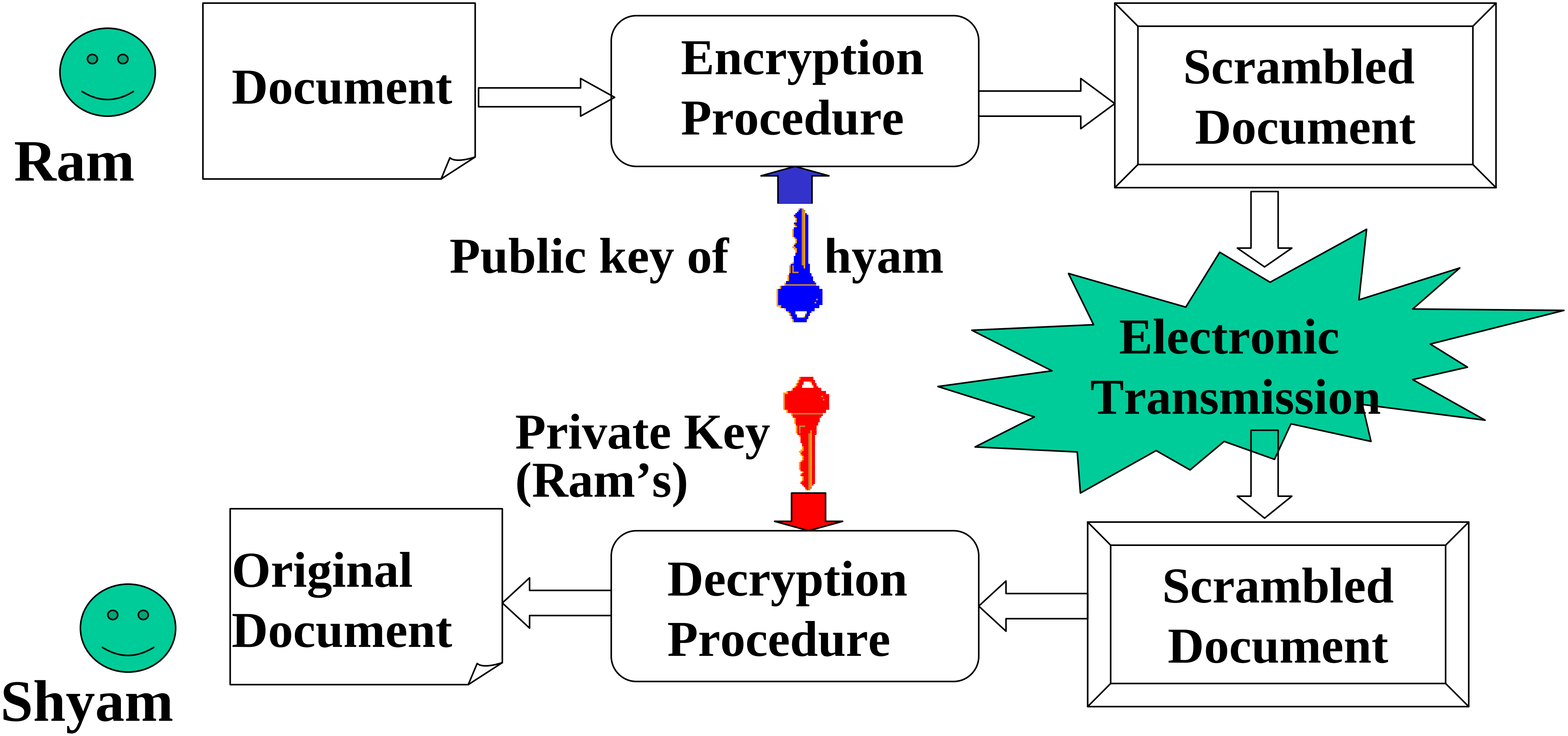
Secret or Symmetric Key



Features of Asymmetric key Cryptography

- Two keys are required viz. private and public.
- Both the keys are mathematically related but one cannot be derived from the other.
- This property lets a user, Alice, publish her encryption key. Anyone can use that public key to encrypt a message that only Alice can decipher with her private key.
- We say that Alice “owns” the “key- pair.”
- Problem of key exchange solved.
- Slower as compared to symmetric key cryptography.

Public or Asymmetric Key Cryptography



Ram

Document

Encryption Procedure

Scrambled Document

Public key of hyam

Electronic Transmission

Private Key (Ram's)

Shyam

Original Document

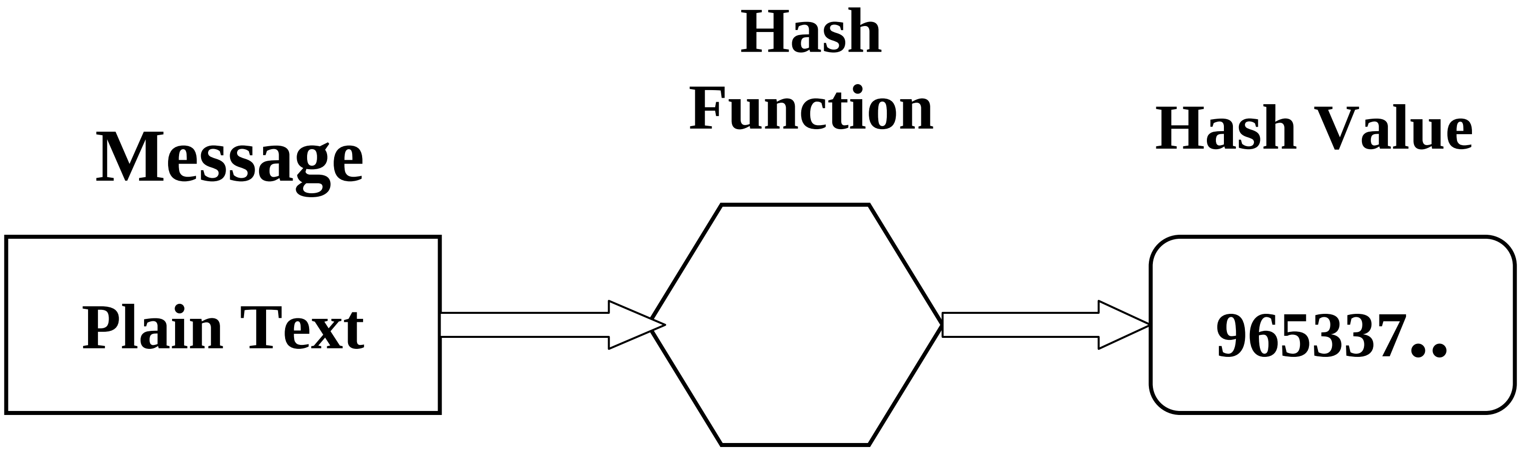
Decryption Procedure

Scrambled Document

Hash Function

- Hash functions are algorithms which transform the plaintext mathematically so that the contents and length of the plaintext are not recoverable from the cipher text.
- Furthermore, there is a very low probability that two different plaintext messages will yield the same hash value.
- Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that an intruder or virus has not altered the file.
- Usually fixed lengths: 48-128 bits

Hash Function



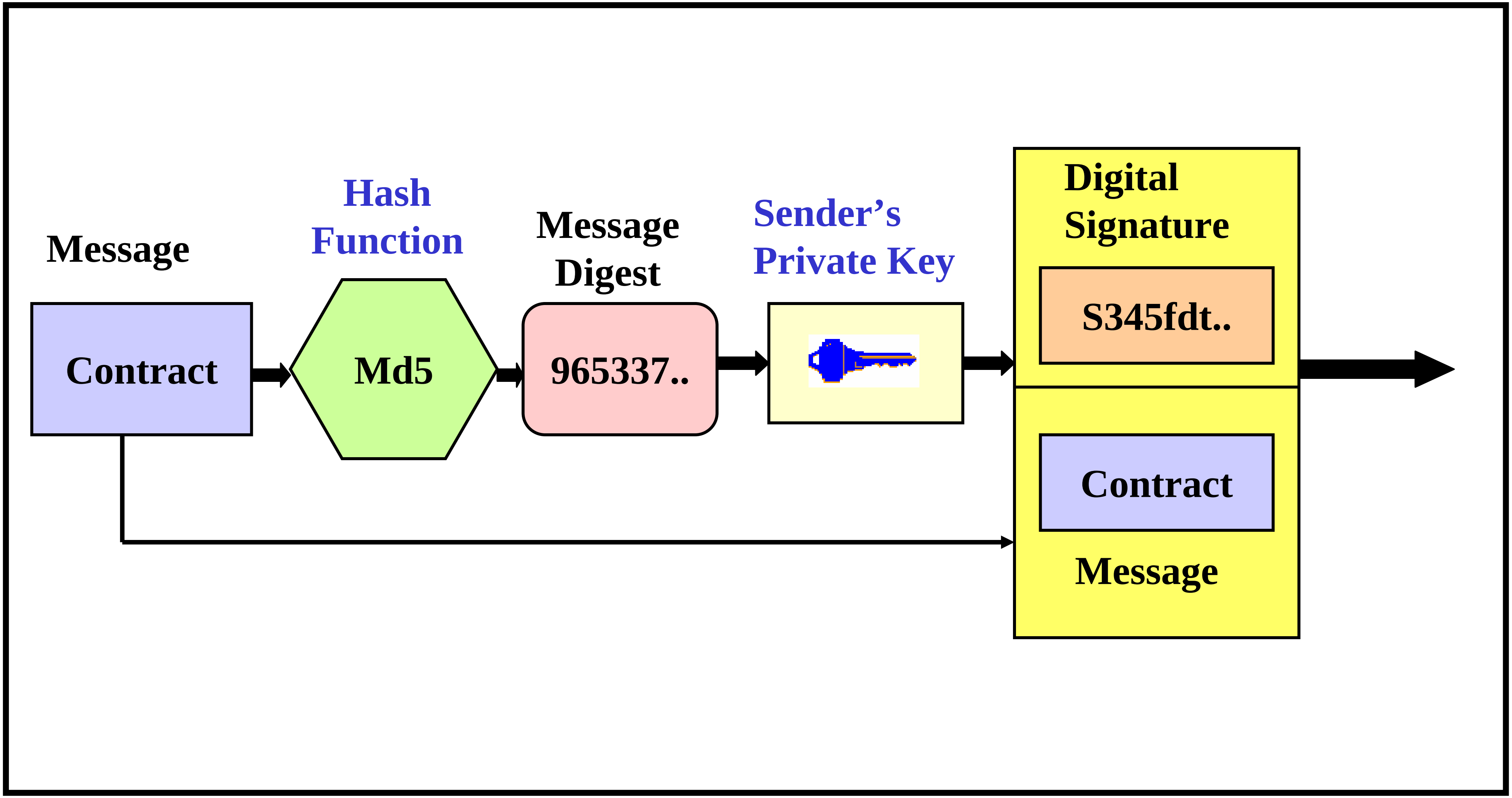
- Used in digital signatures.

Digital Signatures

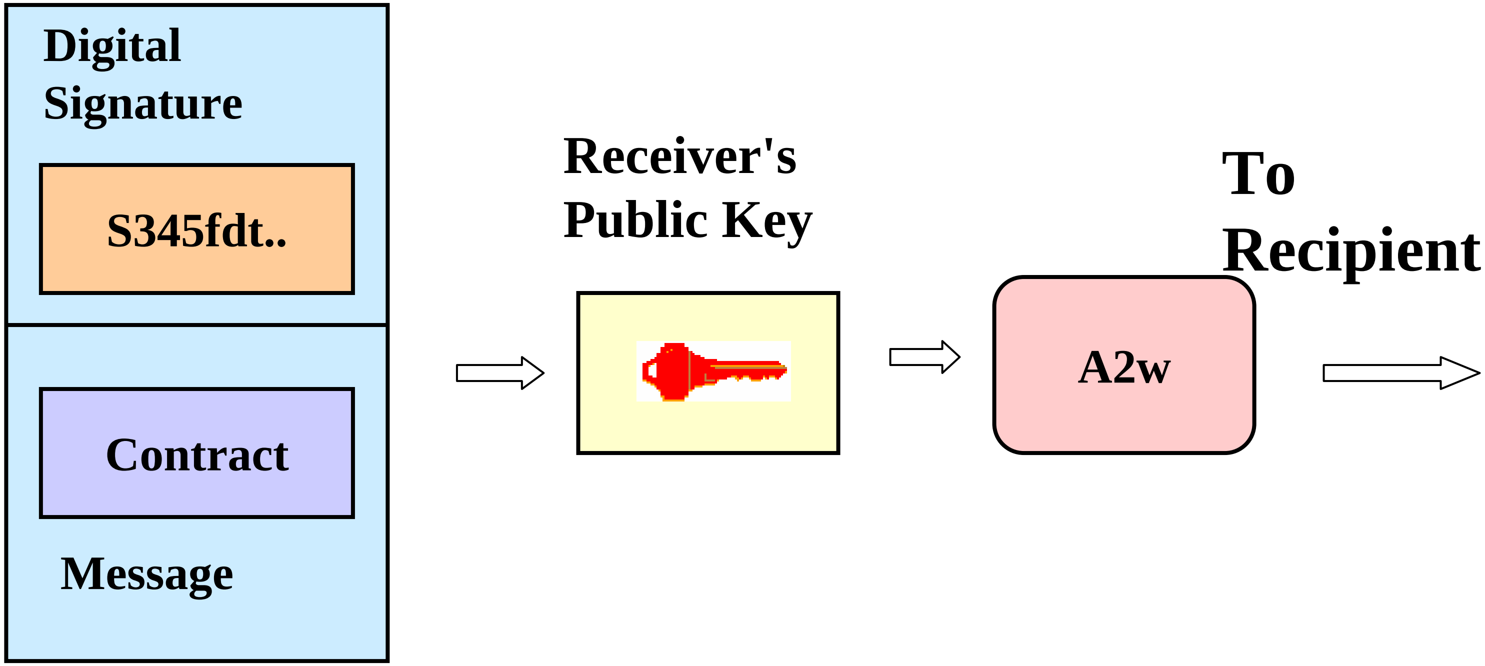
- **Digital signature is actual transformation of electronic message using cryptographic techniques.**
- **Not a digitized image of a signature.**
- **Bound to the signer and document both.**
- **Extremely secure and cannot be reproduced.**
- **Mostly used for signing electronic documents and in Internet applications.**

- Creation
  - Sign
  - Seal
  - Deliver
- Verification
  - Accept
  - Open
  - Verify

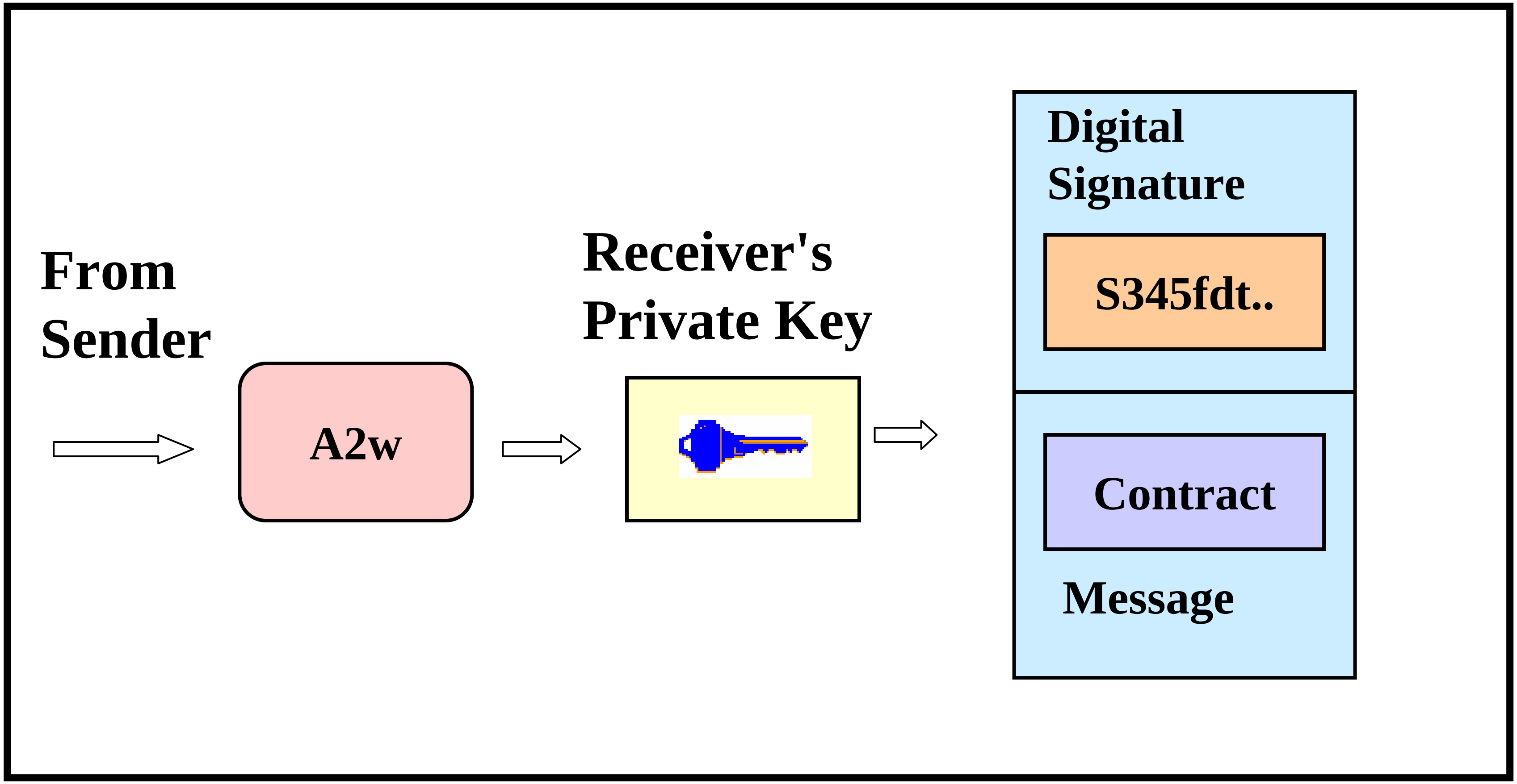
Digital Signature Signing



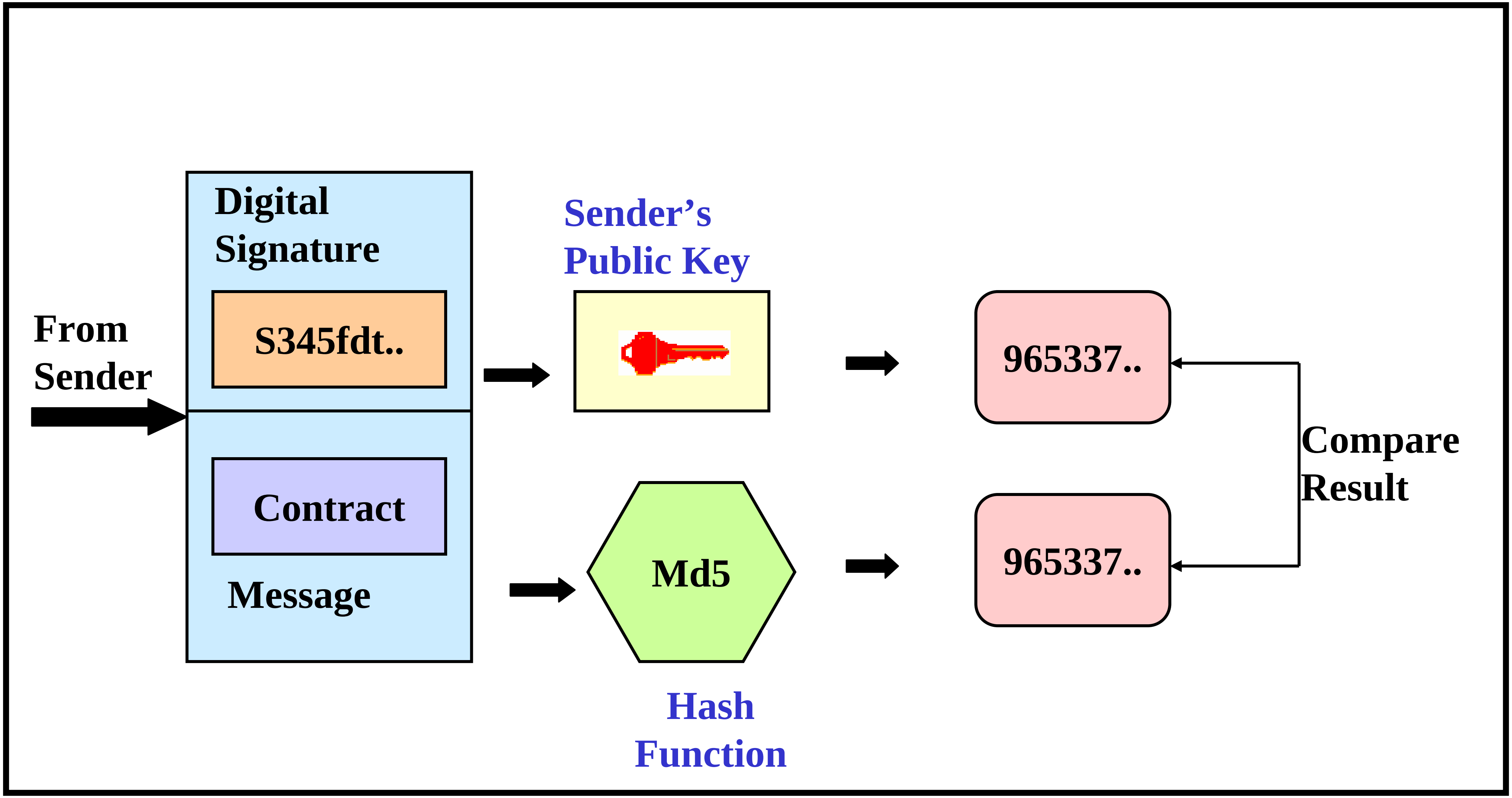
Digital Signature Sealing



Digital Signature Opening



Digital Signature Verification



Encryption Vulnerabilities

- **Mishandling or human error.**

  Mishandling of secure key can result into compromise of the encryption

- **Deficiency in cipher.**
- **Brute force attack.**

Securing the Network from Attacks launched using the Media

- **Firewalls.**
- **Intrusion Detection system(IDS).**
- **Antivirus measures.**
- **Comprehensive security policy.**

Securing the Network from Attacks launched using the Media

Firewalls.

- A firewall is a system (either software or hardware or both) that imposes an access control policy between two networks. Once you have determined the level of connecting you wish to provide, it is the firewalls job to ensure that no additional access beyond this scope is allowed

Means of Establishing a Security Framework

- **Firewalls**
- **Authentication**
- **Intrusion Detection System**
- **Antivirus**
- **Encryption**

WHAT IS A FIREWALL
Firewall Aim

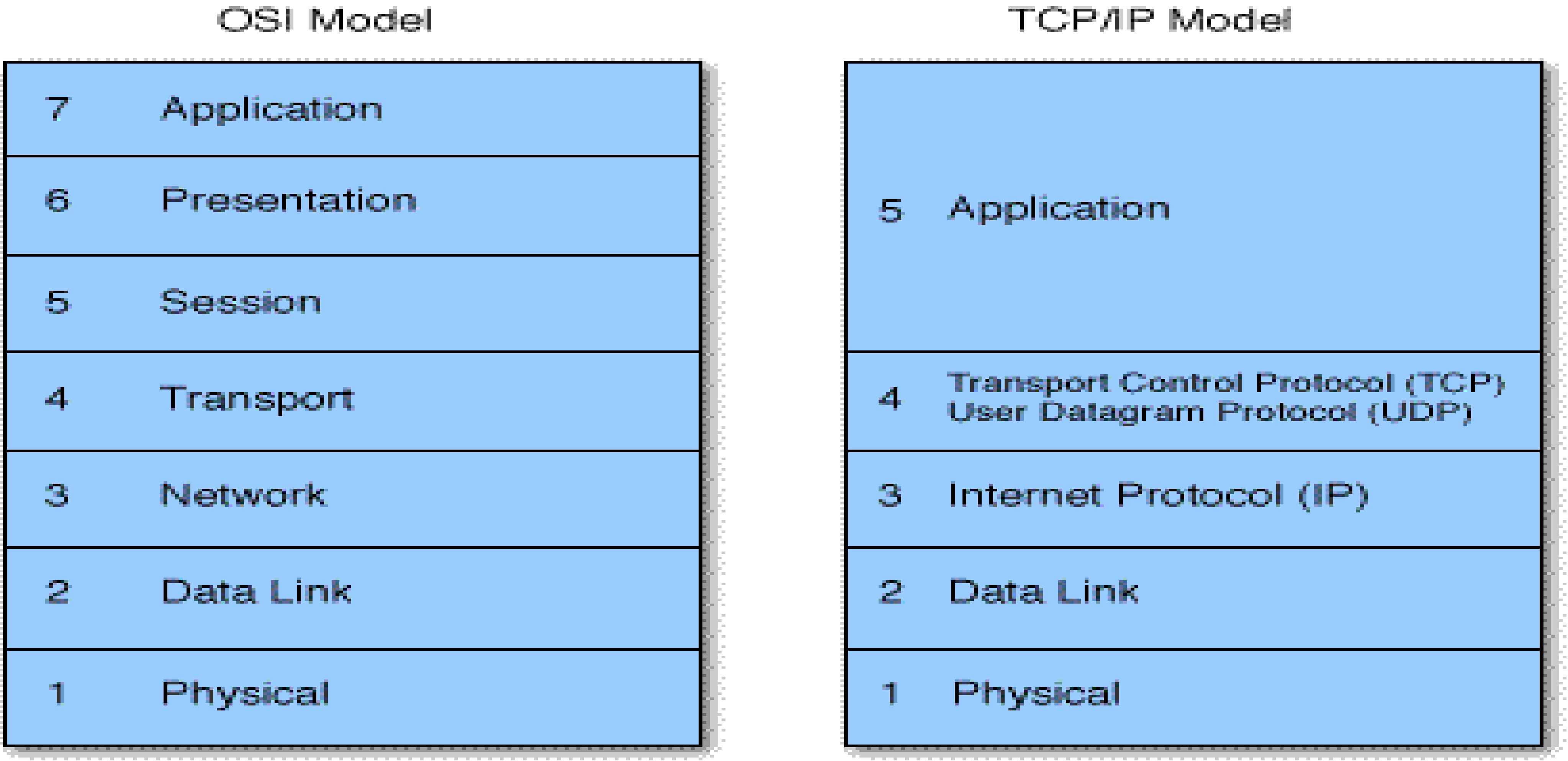
- Main aim is to control access , both from Internet to the Private Network and from Private Network to Internet

- Defending the Private Network from Hackers/Attackers

Types of Firewalls

- **Static packet filtering**
- **Dynamic packet filtering**
- **Proxy**

OSI verses TCP/IP Model



OSI Model

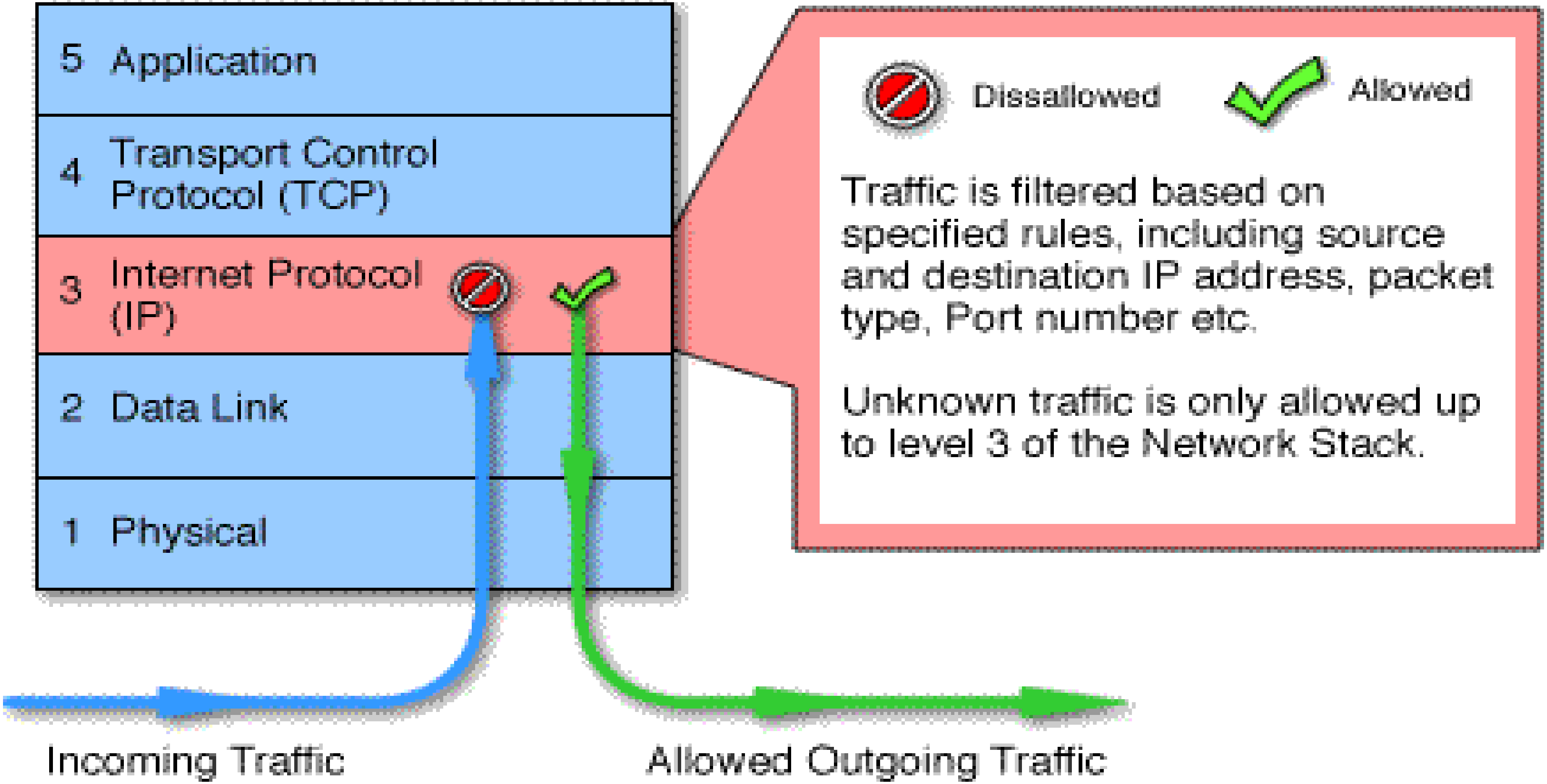
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

TCP/IP Model

5 Application
4 Transport Control Protocol (TCP)
User Datagram Protocol (UDP)
3 Internet Protocol (IP)
2 Data Link
1 Physical

Static Packet Filtering

(IP/Network Layer)



5 Application

4 Transport Control Protocol (TCP)

3 Internet Protocol (IP) ⊘ ✓

2 Data Link

1 Physical

Incoming Traffic

Allowed Outgoing Traffic

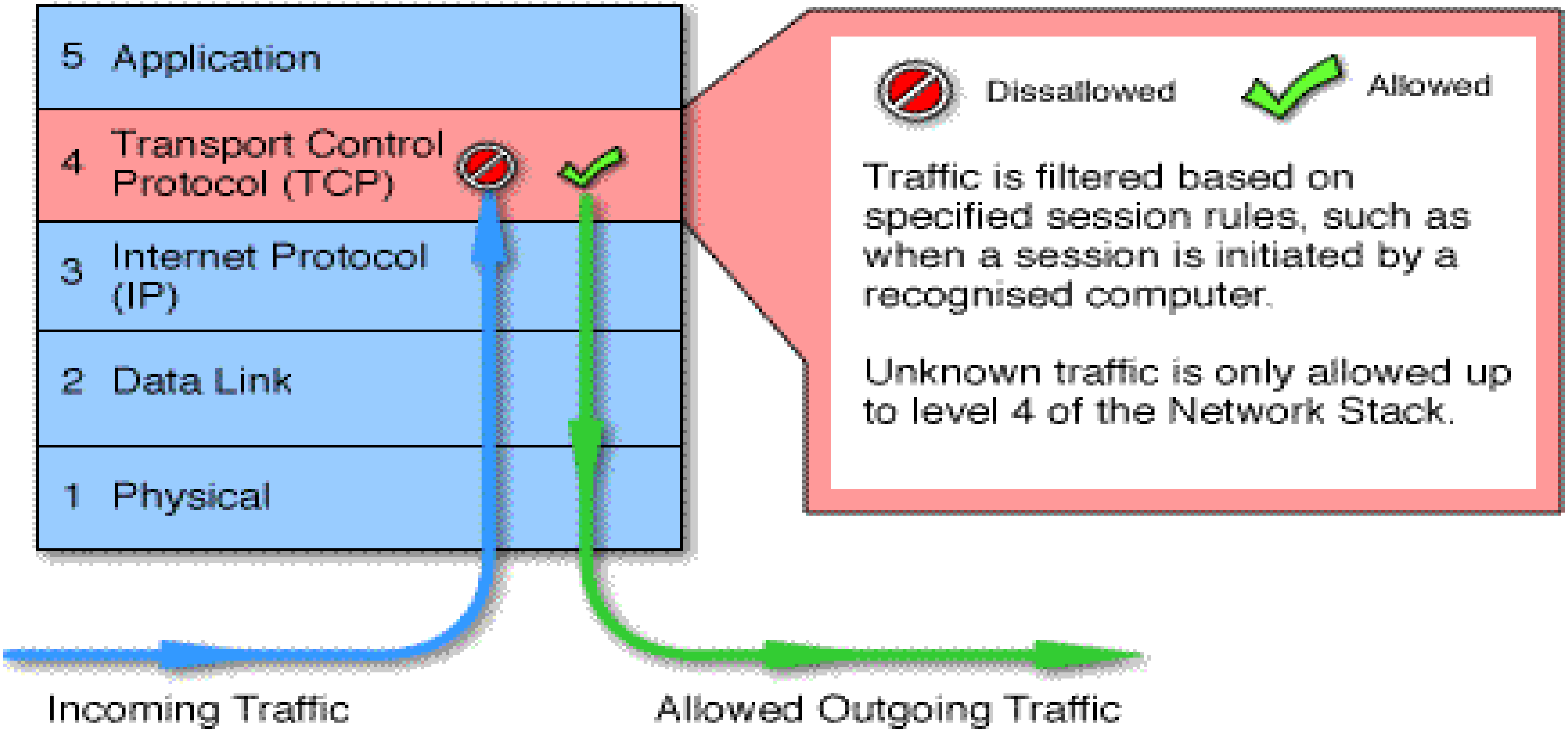
⊘ Dissallowed ✓ Allowed

Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.

Dynamic Packet filtering

(Transport Layer)



5 Application

4 Transport Control Protocol (TCP)

3 Internet Protocol (IP)

2 Data Link

1 Physical

Incoming Traffic

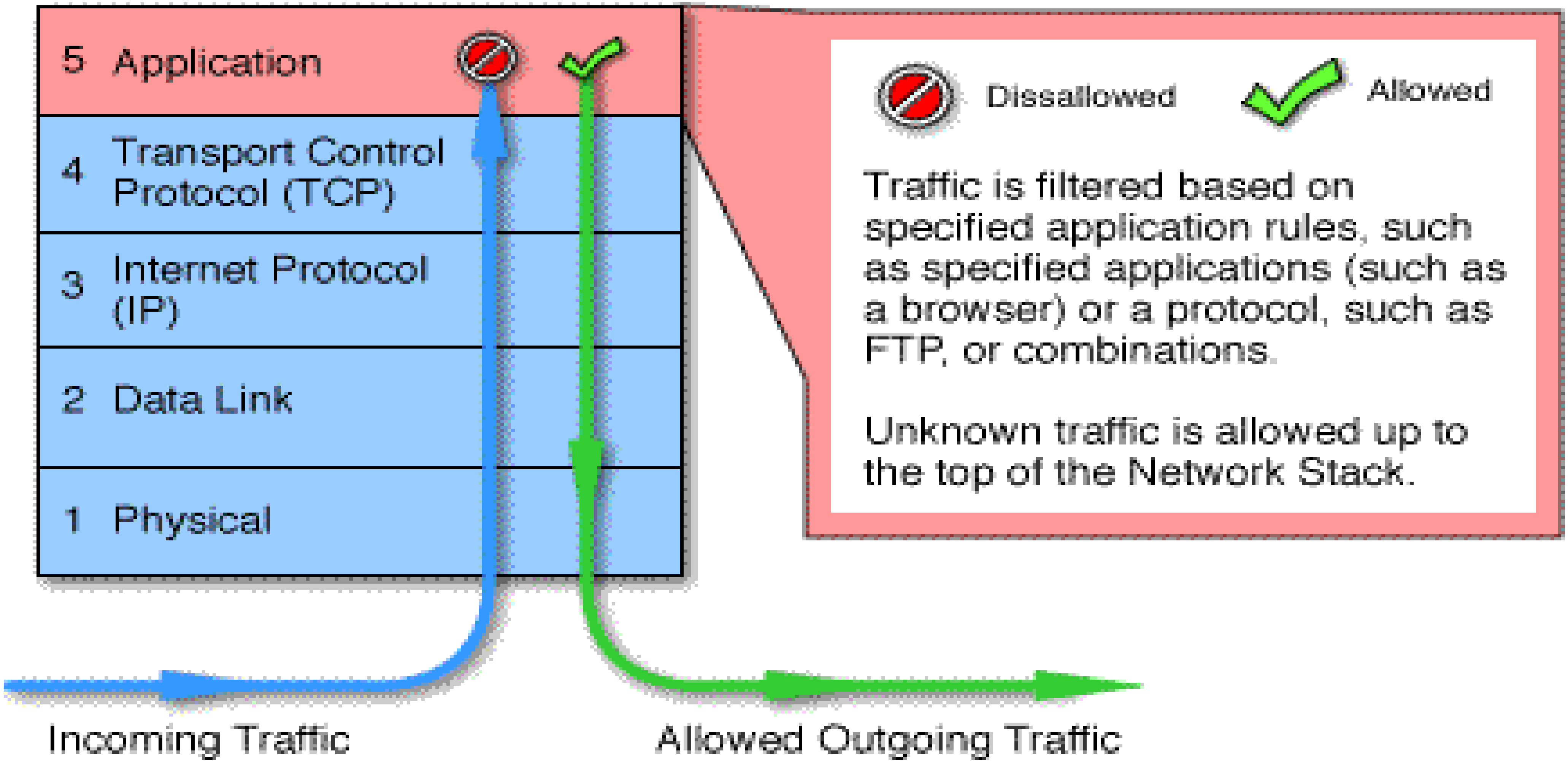
Allowed Outgoing Traffic

⊘ Dissallowed ✓ Allowed

Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.

Proxy
(Application Layer)



5 Application

4 Transport Control Protocol (TCP)

3 Internet Protocol (IP)

2 Data Link

1 Physical

Incoming Traffic

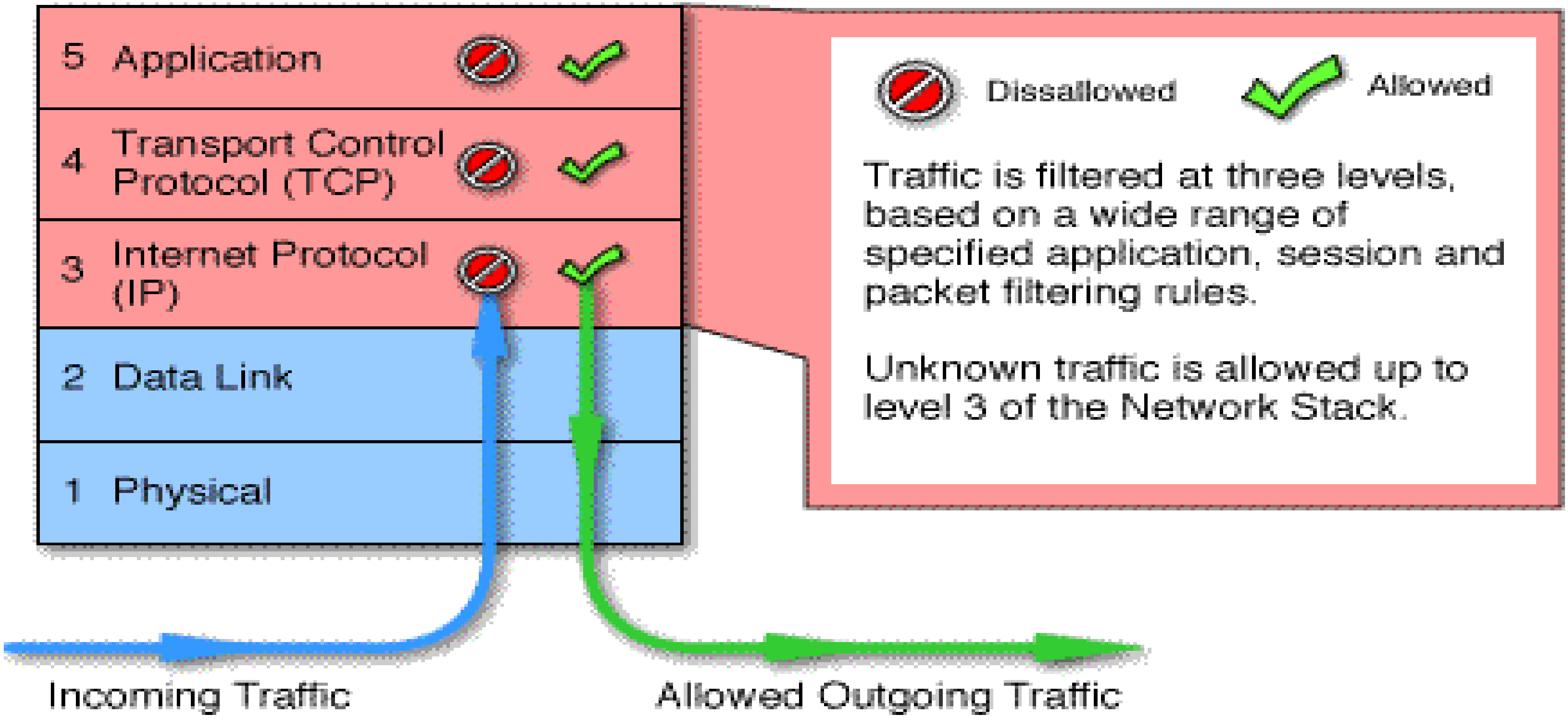
Allowed Outgoing Traffic

🛇 Dissallowed ✓ Allowed

Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Firewall(Working at All the Three layer)



Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

Unknown traffic is allowed up to level 3 of the Network Stack.

Static Packet Filtering

- Destination IP address or subnet
- Source IP address or subnet
- Destination service port
- Flag(TCP only)
- Source Service port

Dynamic Packet filtering

It creates state table. Every time when the remote server tries to respond to the protected host, the state table is referred to insure the following:

- **The protected host actually made a data request.**

- **The source port information matches the data request.**

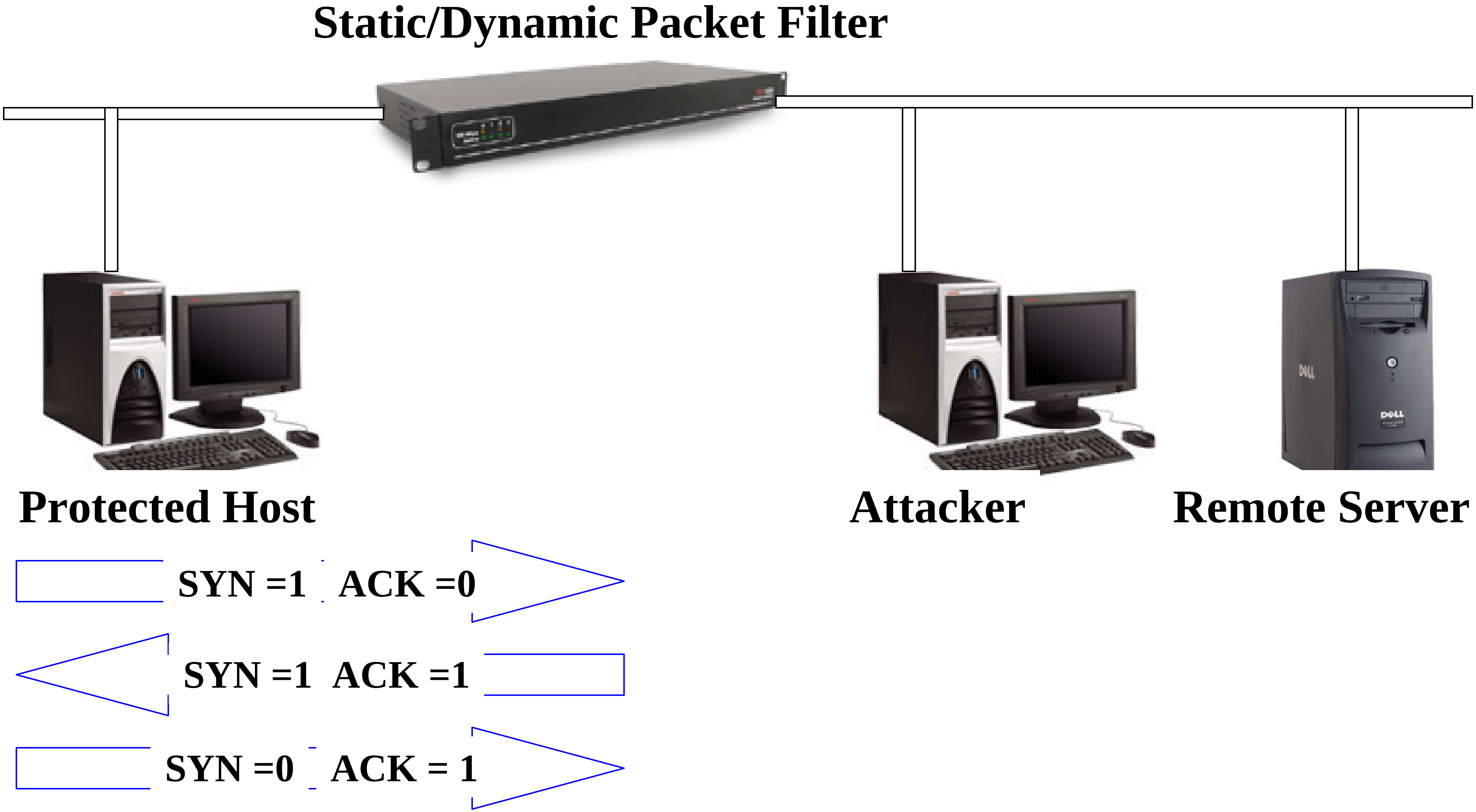
- **The destination port information matches the data request.**

TCP/IP Packet

Header	Data

- Source Port
- Destination Port
- Sequence number
- TCP flags
  - ACK
  - SYN
  - FIN
  - RST
  - PSH

Connection Establishment From The Protected Host



Static/Dynamic Packet Filter

Protected Host

Attacker

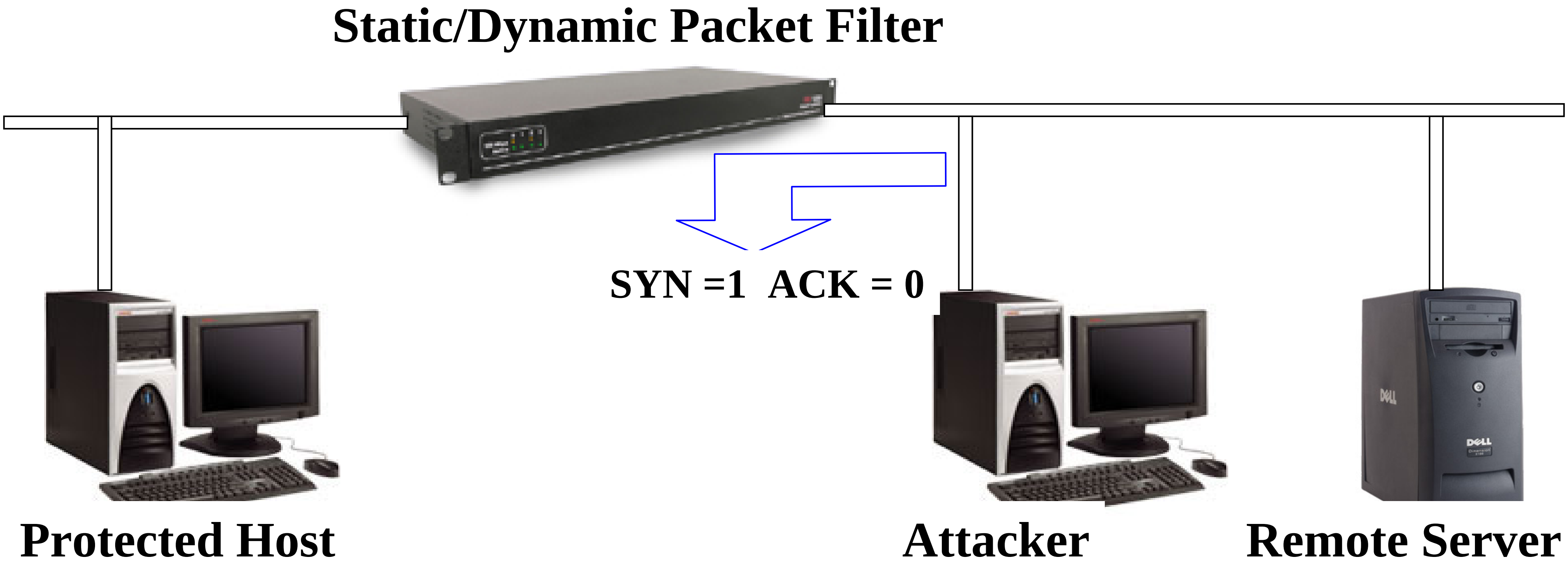
Remote Server

SYN =1 ACK =0

SYN =1 ACK =1

SYN =0 ACK = 1

Both Filtering Methods can block a Port Scan



Static/Dynamic Packet Filter

SYN =1 ACK = 0

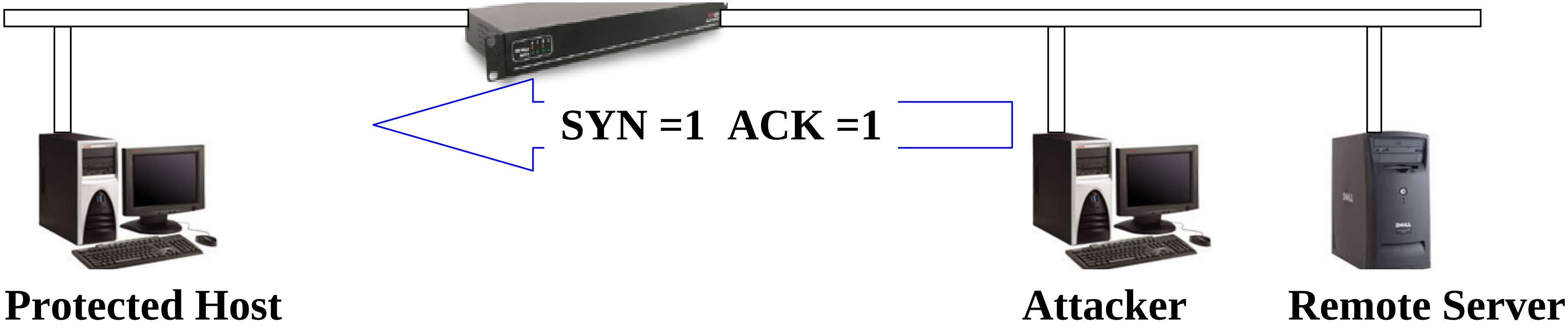
Protected Host

Attacker

Remote Server

Dynamic Filter Blocks The Wrong Packet

Static Packet Filter



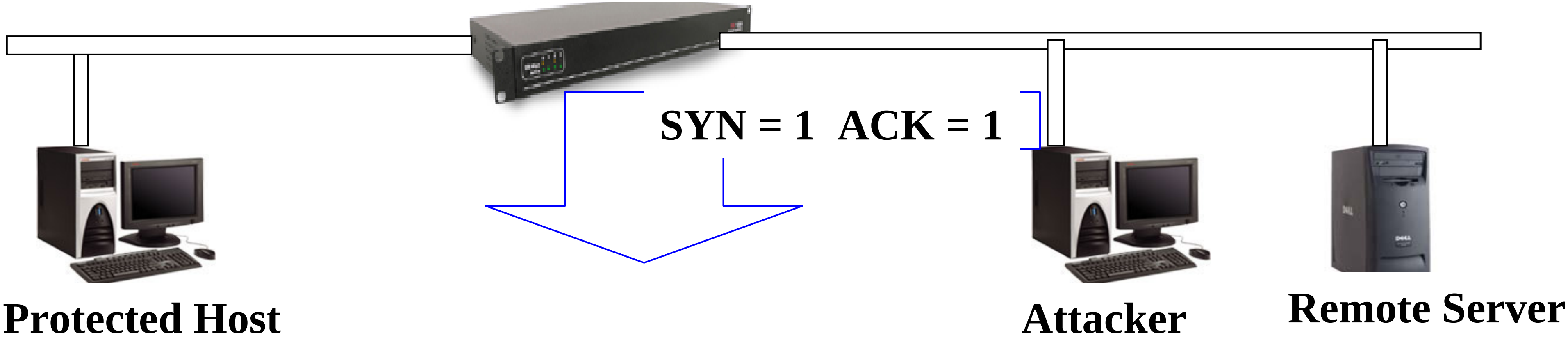
SYN =1 ACK =1

Protected Host

Attacker

Remote Server

Dynamic Packet Filter



SYN = 1 ACK = 1

Protected Host

Attacker

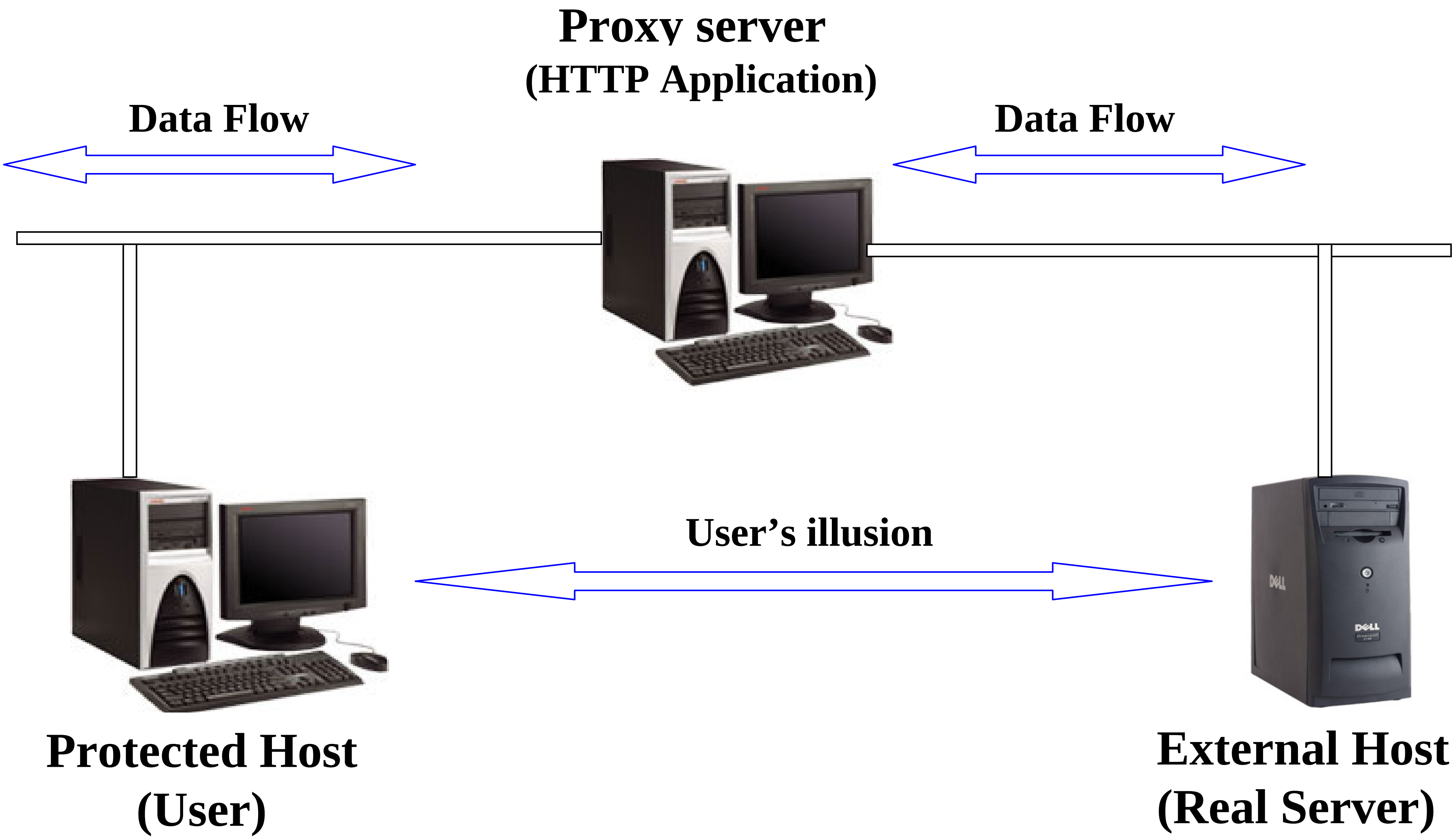
Remote Server

Proxies

- A proxy server is an application that mediates traffic between two network segment from passing directly between networks.

- The source and destination systems never actually connect with each other

Proxies



Proxy server
(HTTP Application)

Data Flow

Data Flow

User’s illusion

Protected Host
(User)

External Host
(Real Server)

Security policy/Access control policy

- Direction
- Services (HTTP, FTP)
- Individual users
- Time of the day

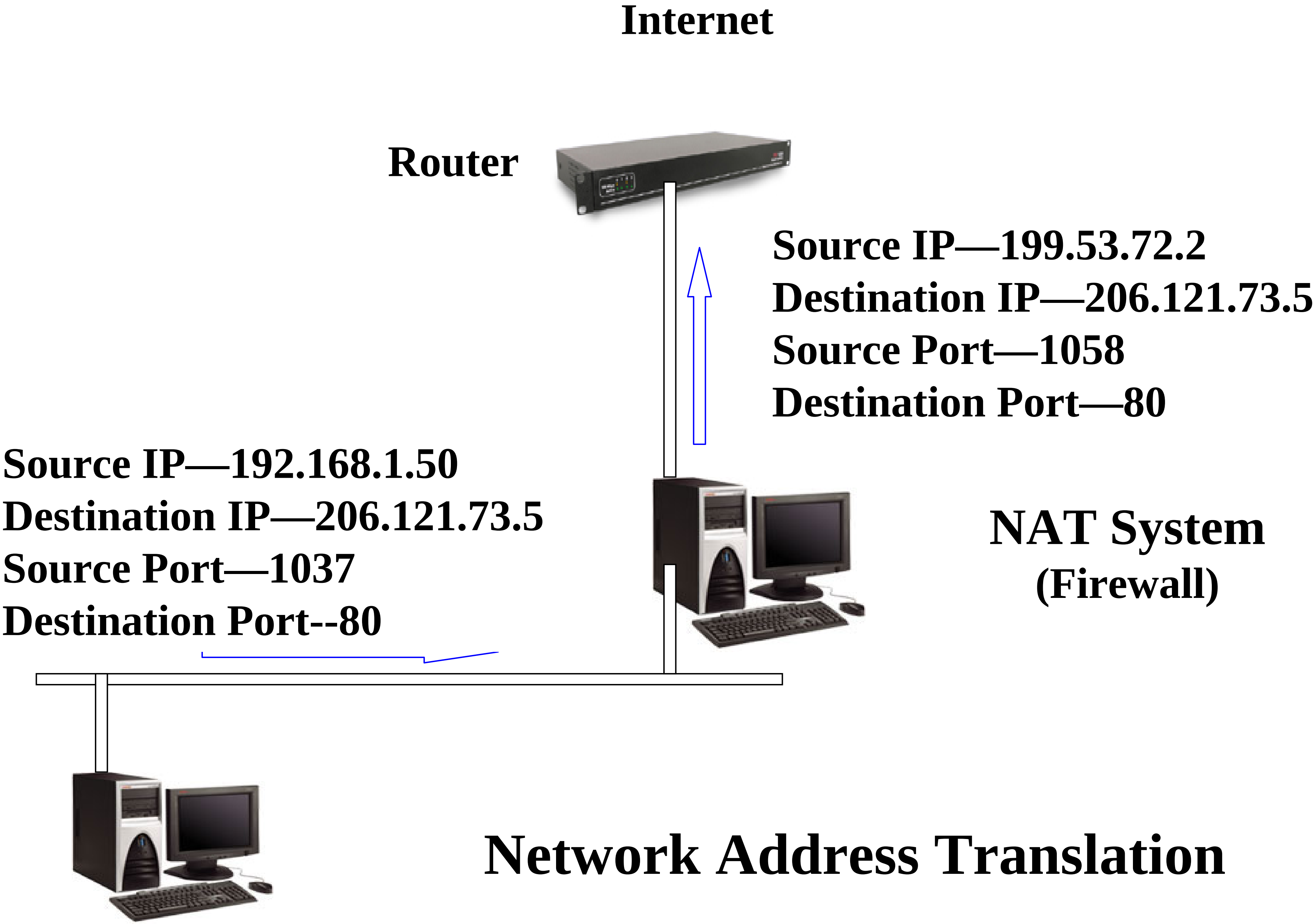
Other Additional Features of Firewall

- Authentication
- Address translation:
- Content Security
- Load balancing
- Logging
- Encryption(Virtual Private Network)

Network Address translation

Network Address Translation (NAT) allows a network to use one set of network address internally and a different set dealing with external networks. It helps to conceal the internal network layout. When an internal machine sends a packet to the outside, the network address translation system modifies the source address of the packet to make the packet look as if it is coming from a valid address. When an external machine sends a packet to the inside, the network address translation system modifies the destination address to turn the externally visible address into the correct internal address. The network address translation system can also modify the source and destination port numbers.

Network Address Translation



Internet

Router

Source IP—199.53.72.2
Destination IP—206.121.73.5
Source Port—1058
Destination Port—80

Source IP—192.168.1.50
Destination IP—206.121.73.5
Source Port—1037
Destination Port--80

NAT System
(Firewall)

System Logs

- To determine what is going on the network. E.g whether employee is accessing a wrong site like playboy-delete

- To determine what happened during break in

System Logs should be prevented from being accessed by hackers

- vital information
- username and passwords

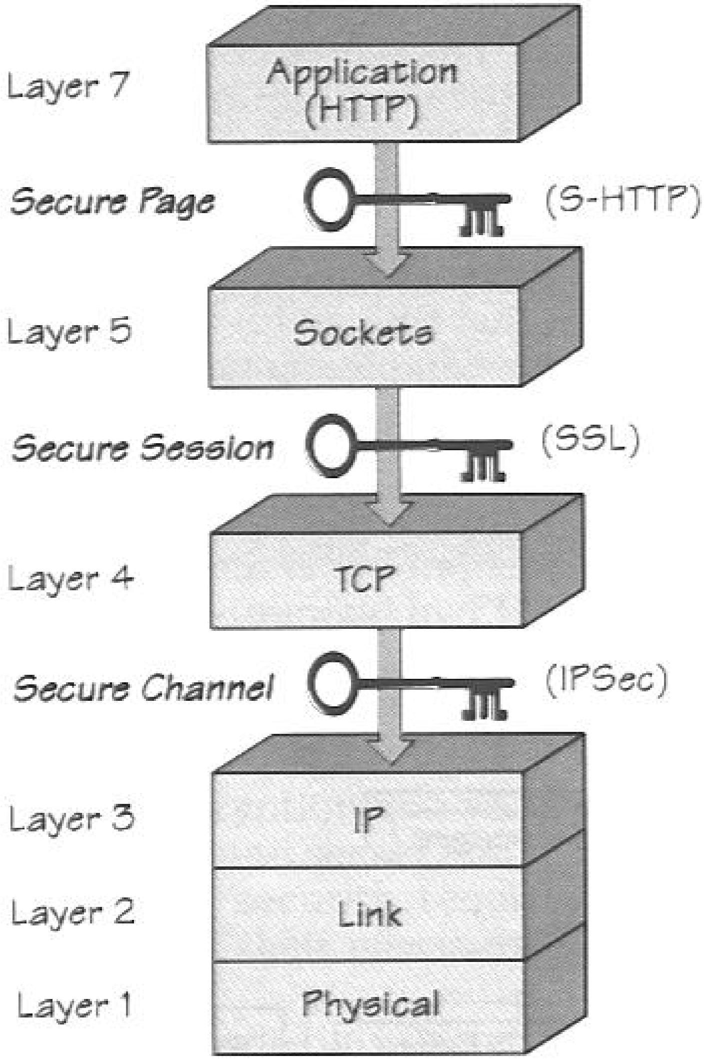
Conclusion

- Firewall will work only if properly configured Firewall Administrator must be abreast to the latest development in the field of network security

- Firewall in combination of Intrusion Detection Device and Authentication provides good security

TCP/IP Encryption at Different Layers

- S-HTTP – individual documents (web pages) encrypted / signed
- SSL – ensures the channel of communication between 2 parties is encrypted and authenticated
- IPSec – like SSL but at IP layer
- These security measures are complementary and can coexists



Secure Socket Layer (SSL)

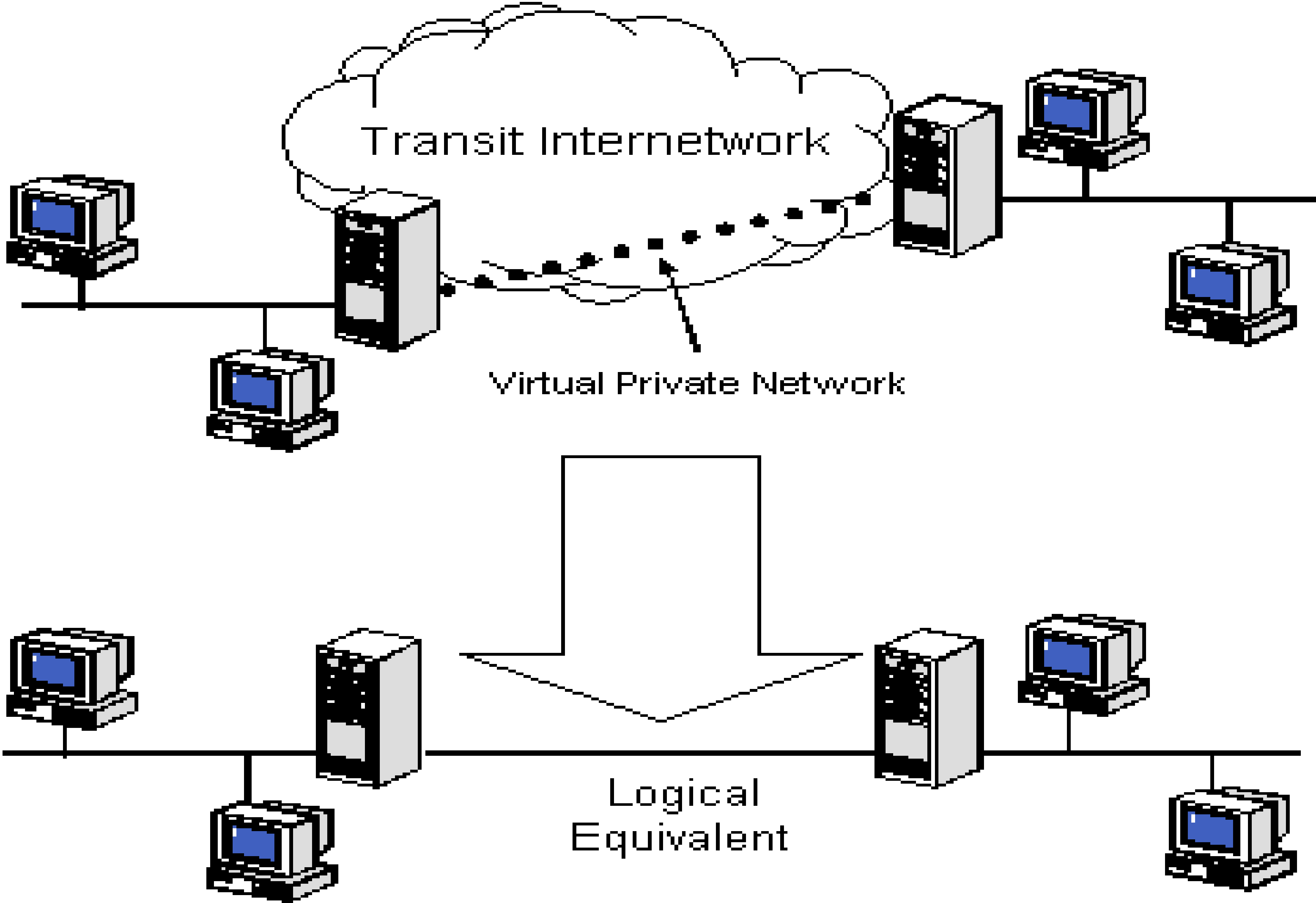
- HTTP servers that implement SSL must run on port 443 instead of 80
- Now all commercial browsers and web servers support SSL
- At the browser, you can tell whether you are using SSL by
  - URL begins with https://
- **Main Functions**
  - **SSL server authentication (certificate)**
  - **Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support**
  - **SSL client authentication (certificate)**
  - **Use public-key encryption techniques to generate shared secrets**
  - **An encrypted SSL connection**

SSL Handshake (Reference)

1. The client sends the server the client's SSL version number, cipher settings, randomly generated data, etc.
2. The server sends the client the server's SSL version number, cipher settings, etc., with its own certificate. If the client is requesting a server resource that requires client authentication, requests the client's certificate.
3. The client uses some of the information sent by the server to authenticate the server
4. Creates the *premaster secret* for the session, encrypts it with the server's public key and sends the encrypted premaster secret to the server.
5. If the server has requested client authentication, the client also signs and send another piece of data that is unique to this handshake and known by both the client and server.
6. If the server has requested client authentication, the server attempts to authenticate the client. If OK, the server uses its private key to decrypt the premaster secret, then performs a series of steps to generate the **master secret.**
7. Both the client and the server use the master secret to generate the *session keys* (symmetric keys)
8. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.
10. The SSL handshake is now complete, and the SSL session has begun.

What Is A Virtual Private Network?

A Virtual Private Network (VPN) connects the components and resources of one network over another network. It accomplishes this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks.


Transit Internetwork
Virtual Private Network
Logical
Equivalent

VPN

VPN technology also allows a corporation to connect to branch offices or to other companies (Extranets) over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a Wide Area Network link between the sites. In both of these cases, the secure connection across the internetwork appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork-hence the name Virtual Private Network.

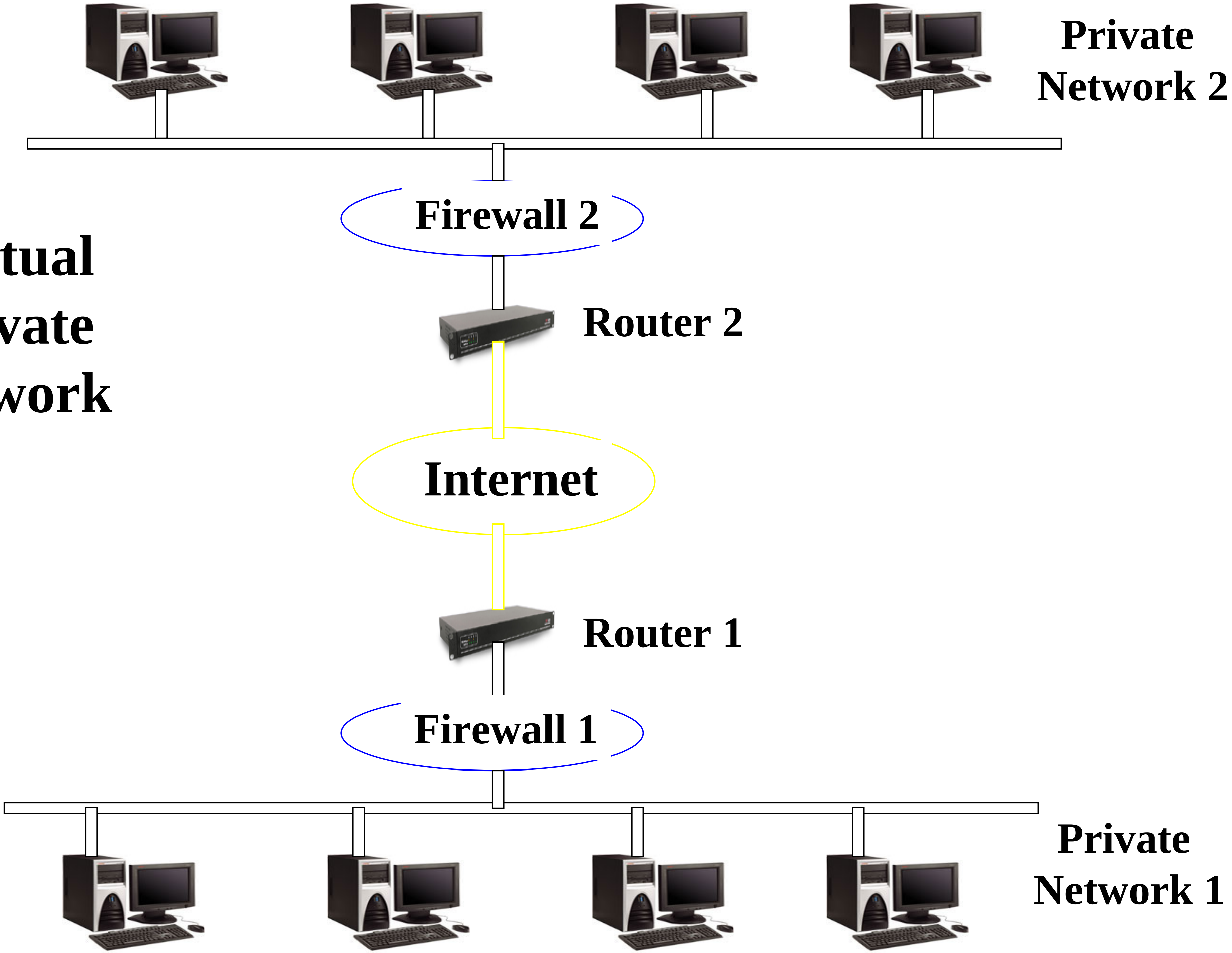
WHY VPNs?

- Increased telecommuting.
- Widely distributed operations.
- Laying dedicated lines is an expensive proposition.
- Providing info on need to know basis.
- Focus on core competencies increases productivity.

BASIC VPN REQMTS

- **Authentication-** The means whereby a user’s or an organization’s identity is protected, and VPN access is restricted to authorized users only
- **Data encryption-** Data that is being transported on public networks must be secured against the “man-in-the-middle” attacks, and be unreadable to unauthorized organizations or individuals.
- **Key management -** When Authentication and Data Encryption are being used, effective Key Management is essential to ensure that security is not compromised.
- Support for common protocols e.g. TCP/IP, IPX/SPX, NET BEUI, SNA and NET BIOS.

Virtual Private Network



Private Network 2

Firewall 2

Router 2

Internet

Router 1

Firewall 1

Private Network 1