EE 5084
Cyber Security

Tools, Firewalls and VPNs

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

BRUCE SCHNEIER, AMERICAN CRYPTOGRAPHER, COMPUTER SECURITY SPECIALIST, AND WRITER

Learning Objectives

- Familiar with security tools
- Important role of access control in computer-based information systems
- Identify and discuss widely used authentication factors
- Firewall technology and the various approaches to firewall implementation
- Approaches to control remote and dial-up access by authenticating and authorizing users
  - Discuss content filtering technology
  - Describe virtual private networks and discuss the technology that enables them

Introduction

- Tools and technology are essential in enforcing policy for many IT functions not under direct human control.
- When properly implemented, technical solutions improve an organization’s ability to balance the objectives of making information readily available and preserving information’s confidentiality and integrity.

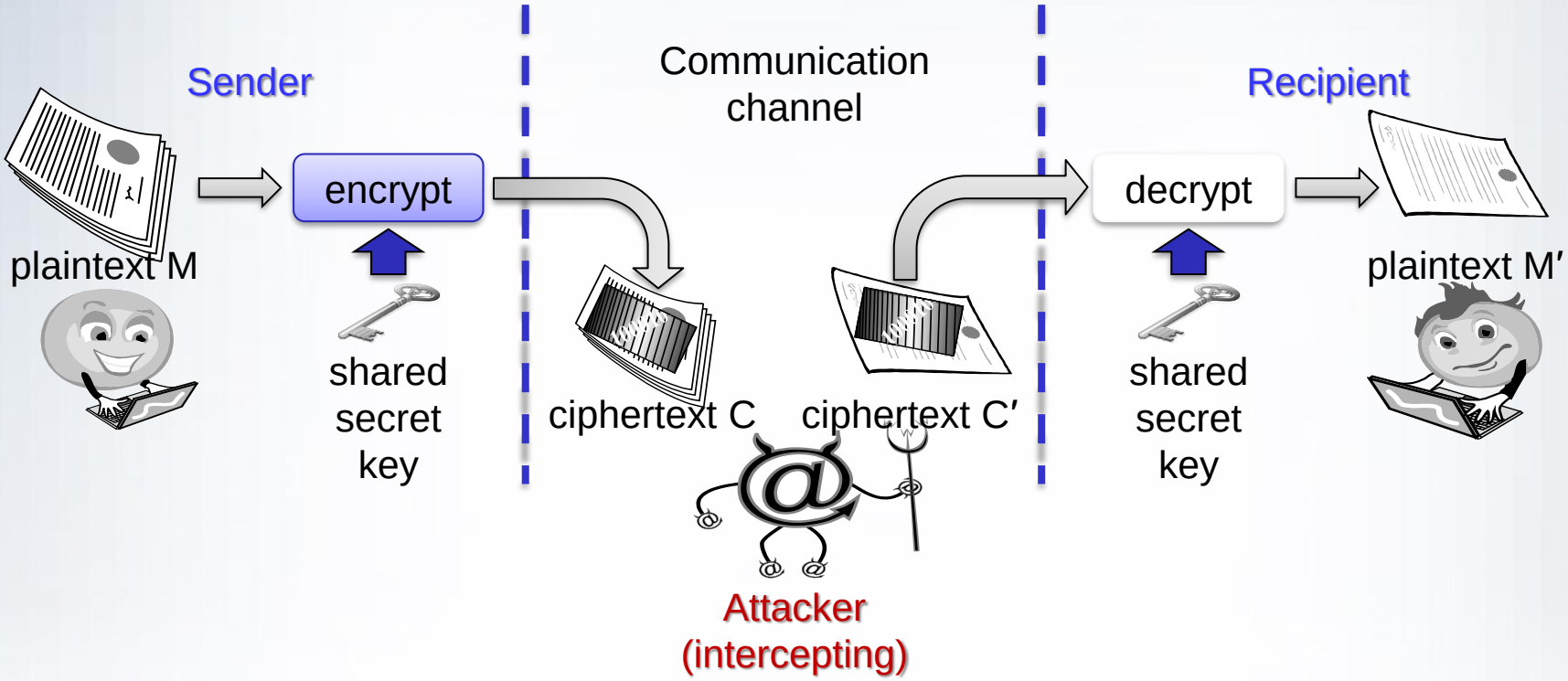
CYBER SECURITY SERVICES

- Authentication
  - Assurance that communicating entity is the one claimed.
- Access Control
  - Prevention of the unauthorized use of online resource.
- Data Confidentiality
  - Protection of data from unauthorized disclosure.
- Data Integrity
  - Assurance that data received is as sent by an authorized entity.
- Non-Repudiation
  - Protection against denial by one of the parties in a communication.
- Availability
  - Resource accessible/usable.
- Security Mechanism
  - Feature designed to detect, prevent, or recover from a security attack.

TOOLS FOR CONFIDENTIALITY (1)

ENCRYPTION

The transformation of information using a secret (encryption) key, so that the transformed information can only be read using another secret (decryption key) which may, in some cases, be the same as the encryption key.



TOOLS FOR CONFIDENTIALITY (2)

ACCESS CONTROL

Rules and policies that limit access to confidential information to those people and/or systems with a "need to know."

This need to know may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist.

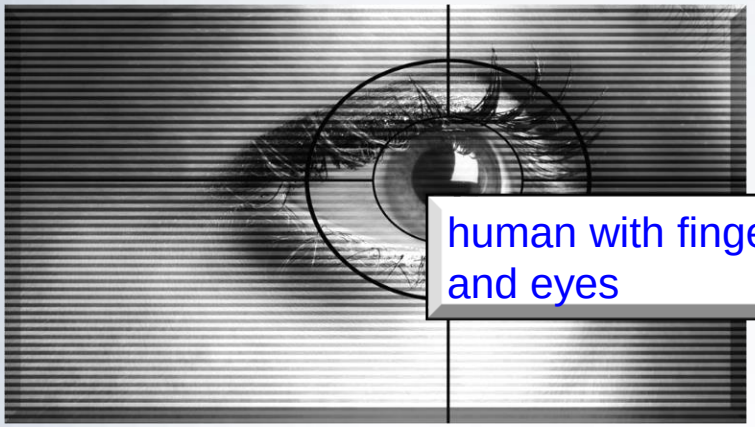
AUTHENTICATION

The determination of the identity or role that someone has.

This determination can be done in a number of different ways, but it is usually based on a combination of

- ✓ something the person has (like a smart card)
- ✓ Something the person knows (like a password)
- ✓ something the person is (like a human with a fingerprint).

TOOLS FOR CONFIDENTIALITY (3)



human with fingers and eyes

Something you are

password=uclb()w1V
mother=Jones
pet=Caesar

Something you know

radio token with secret keys

Something you have

TOOLS FOR CONFIDENTIALITY (4)

AUTHORIZATION

The determination if a person or system is allowed access to resources, based on an access control policy.

Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.

PHYSICAL SECURITY

The establishment of physical barriers to limit access to protected computational resources.

Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages)** so that electromagnetic signals cannot enter or exit the enclosure.

TOOLS FOR INTEGRITY

INTEGRITY

The property that information has not be altered in an unauthorized way.

TOOLS

- **Backups**

  The periodic archiving of data.

- **Checksums**

  The computation of a function that maps the contents of a file to a numerical value.

  A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.

- **Data Correcting Codes**

  Methods for storing data in such a way that small changes can be easily detected and automatically corrected.

TOOLS FOR AVAILABLITY

- AVAILABILITY

  The property that information is accessible and modifiable in a timely fashion by those authorized to do so.

- TOOLS

  Physical Protections

  Infrastructure meant to keep information available even in the event of physical challenges.

  Computational Redundancies

  Computers and storage devices that serve as fallbacks in the case of failures.

Attacks, Mechanisms and Services

- **Security Attack**

  Any action that compromises the security of information.

- **Security Mechanism**

  A mechanism that is designed to detect, prevent, or recover from a security attack.

- **Security Service**

  A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Access Control

- Method by which systems determine whether and how to admit a user into a trusted area of the organization
- Discretionary access controls (DACs): allow users to control and possibly provide access to information or resources at their disposal
- Nondiscretionary controls: strictly enforced version of MACs that are managed by a central authority
- Mandatory access controls (MACs): use data classification schemes

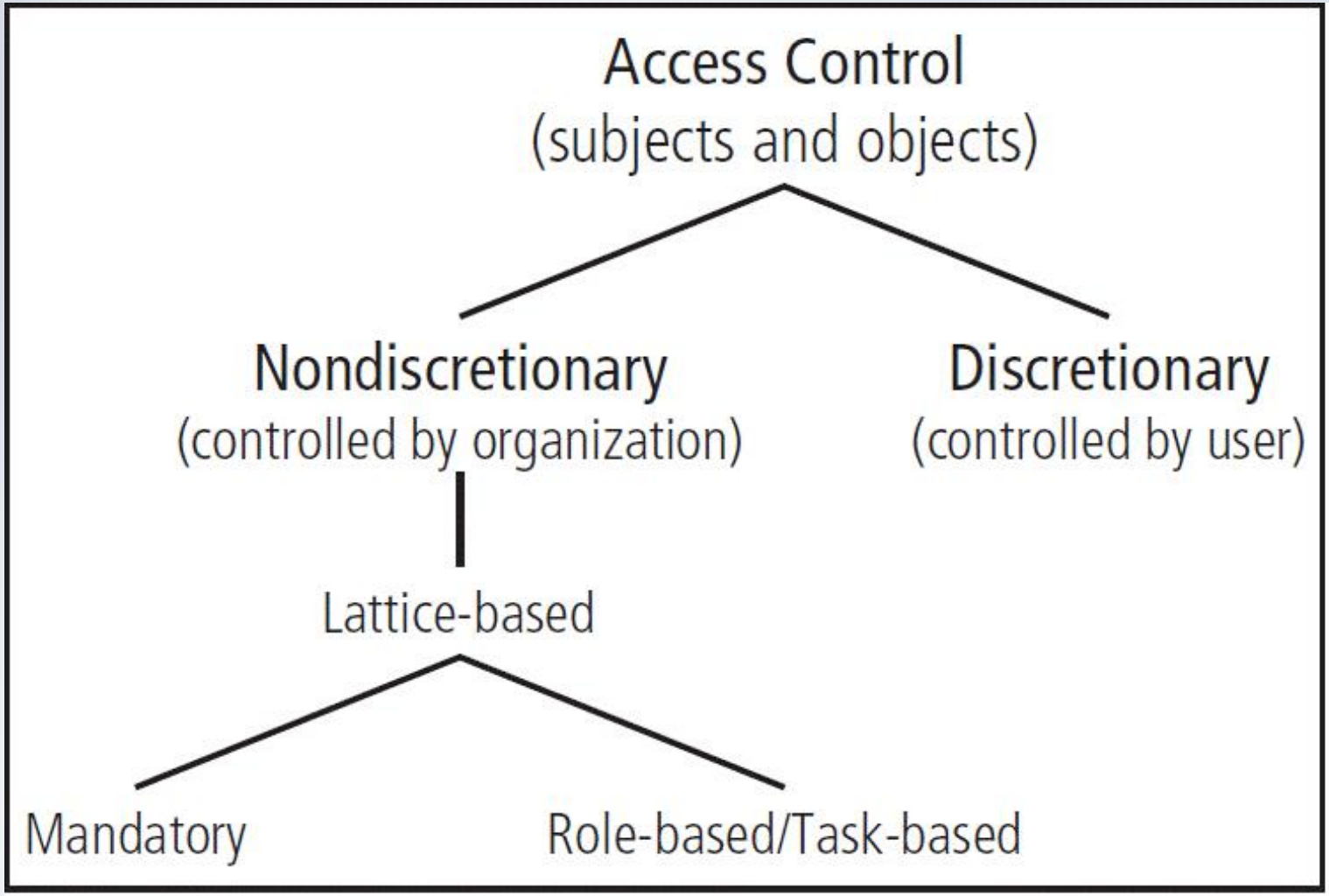


Figure 6-1 Access control approaches

Identification

- Mechanism whereby unverified entities seeking access to a resource (supplicants) provide a label by which they are known to the system
- Identifiers can be composite identifiers, concatenating elements—department codes, random numbers, or special characters—to make them unique.
- Some organizations generate random numbers.

Authentication (1)

- The process of validating a user purported identity
- Authentication factors

  Something a user knows

  – Password: a private word or a combination of characters that only the user should know

  – Passphrase: a series of characters, typically longer than a password, from which a virtual password is derived

Password security

Rules to harden password protection

- **Never install any application or service with default passwords from the vendor**
- **Make passwords at least 10 characters long**
- **Use numbers, letters, and symbols, such as $, ***
- **Do not use words. Avoid any word in the English and Klingon (from Star Trek) dictionary**
- **Avoid names of sports teams, social security #s, first names, pet or other info that might be in personnel files or displayed on the wall**
- **Change passwords at least once every 4 months**
- **Memorize passwords and keep them secret**

UNSAFE PASSWORD

123456

Despite Internet security breaches, this is world's most popular password

NEW YORK

BACK at the dawn of the Web, the most popular account password was "12345". Today, it's one digit longer but hardly safer: 123456.

Despite all the reports of Internet security breaches over the years, including the recent attacks on Google's e-mail service, many people have reacted to electronic break-ins with a shrug.

According to a new analysis, one out of five Web users is still leaving the digital equivalent of a key under the doormat. They choose simple, easily-guessed passwords like "abc123", "iloveyou" or even "password" to protect their data.

"I guess it's just a genetic flaw in humans," said Mr Amichai Shulman, the chief technology officer at Imperva, which

Facebook and MySpace.

The list was briefly posted on the Web, and hackers and security researchers downloaded it.

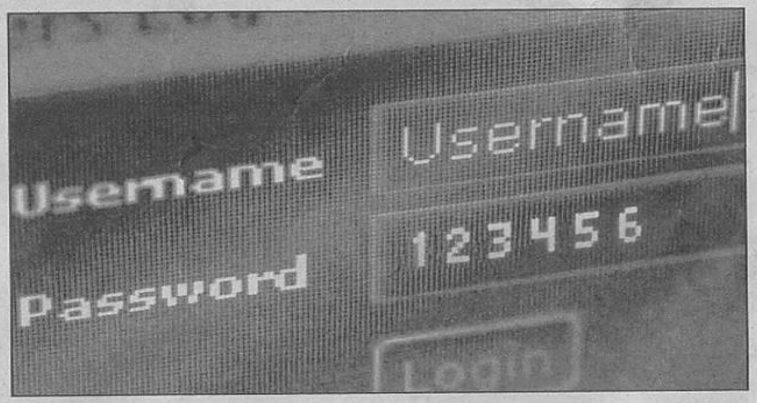
RockYou, which had already been widely criticised for lax privacy practices, has advised its customers to change their passwords, as the hacker gained information about customers' e-mail accounts as well.

The trove provided an unusually detailed window into computer users' password habits. Typically, only government agencies, like the Federal Bureau of Investigation or the National Security Agency, have had access to such a large password list.

Said Mr Matt Weir, a doctoral candidate in the e-crimes and investigation technology lab at Florida State University, where researchers are also examining the data: "This was the mother lode."

Imperva found that nearly

'ILOVEYOU' IS HOT TOO



One million RockYou users chose these passwords:

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123
11. nicole
12. daniel
13. babygirl
14. monkey
15. jessica
16. lovely
17. michael
18. ashley
19. 654321
20. qwerty
21. iloveu
22. michelle
23. 111111
24. 0
25. tigger
26. password1
27. sunshine
28. chocolate
29. anthony
30. angel
31. FRIENDS
32. soccer

SOURCE: IMPERVA PHOTO: ISTOCKPHOTO

Authentication (2)

- Authentication factors

  Something a user has

  – Dumb card: ID or ATM card with magnetic stripe

  – Smart card: contains a computer chip that can verify and validate information

  – Synchronous tokens

  – Asynchronous tokens

  Something a user is

  – Relies upon individual characteristics

  – Strong authentication

Dear all,

This announcement is made strictly for international students who are not able to come to Singapore in time for Quiz 1.

Please read the list of students and inform me if I have left out or mistype your name.

IMPORTANT:

- ✓ Please read and follow all the instructions uploaded in the content folder.
- ✓ Please sign the consent form for the online quiz. This is the link for the consent form: https://forms.office.com/r/kVydwCHm2N

Regards,

Dr Chan

Authorization

- Authorization: the matching of an authenticated entity to a list of information assets and corresponding access levels
- Authorization can be handled in one of three ways:
  - Authorization for each authenticated user
  - Authorization for members of a group
  - Authorization across multiple systems
- Authorization tickets

Accountability

- Accountability (auditability): ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity
- Most often accomplished by means of system logs and database journals, and the auditing of these records
- Systems logs record specific information.
- Logs have many uses.

Biometrics

- Approach based on the use of measurable human characteristics/traits to authenticate identity
- Only fingerprints, retina of eye, and iris of eye are considered truly unique.
- Evaluated on false reject rate, false accept rate, and crossover error rate
- Highly reliable/effective biometric systems are often considered intrusive by users.

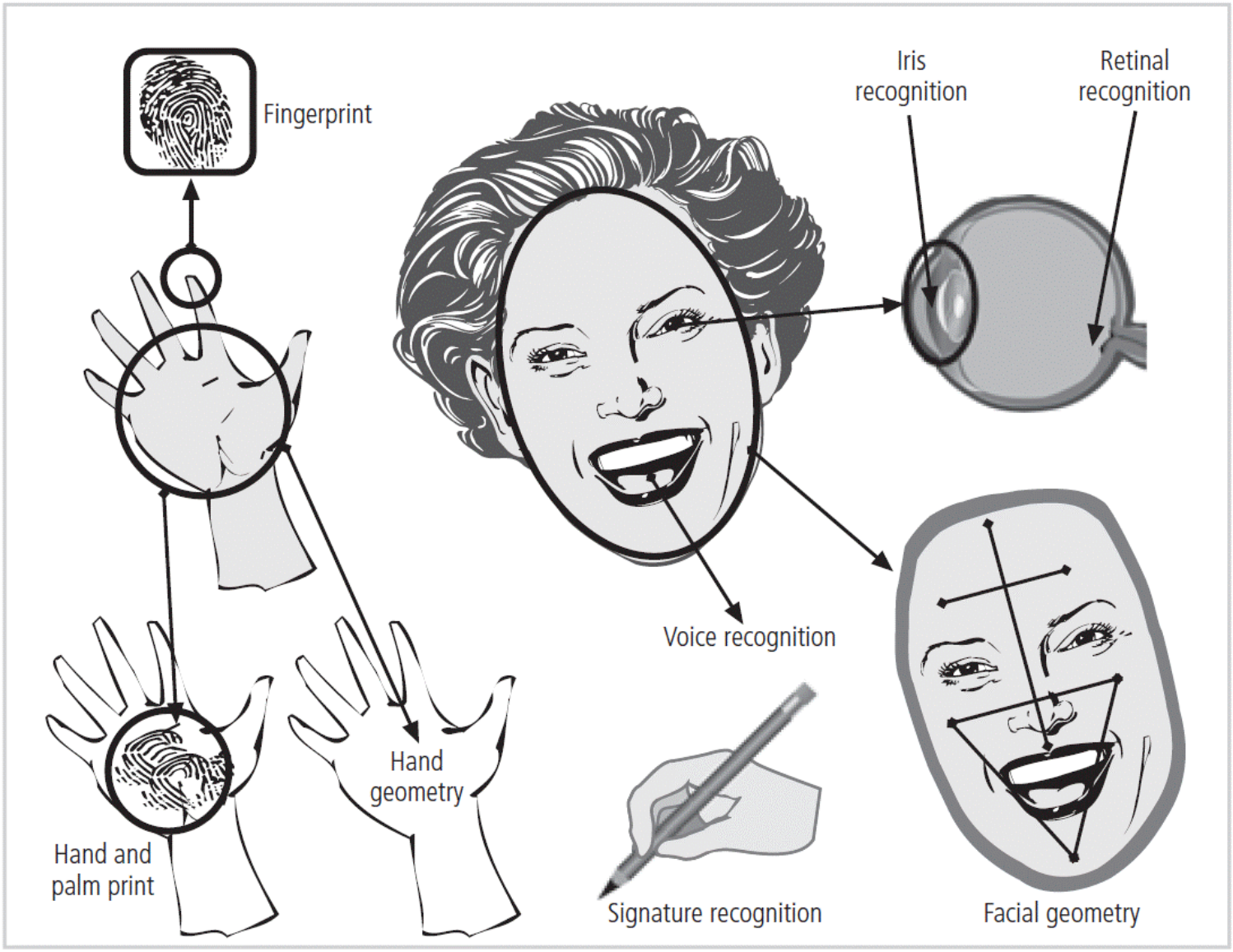


Figure 6-5 Biometric recognition characteristics

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Eye: Iris	H	H	H	M	H	L	H
Eye: Retina	H	H	M	L	H	L	H
DNA	H	H	H	L	H	L	L
Odor & Scent	H	H	H	L	L	M	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M

Table 6-1 Ranking of Biometric Effectiveness and Acceptance

In the table, H = High, M = Medium, and L = Low.

From multiple sources.[3]

Firewalls

- Prevent specific types of information from moving between an untrusted network (the Internet) and a trusted network (organization's internal network)
- May be
  - Separate computer system
  - Software service running on existing router or server
  - Separate network containing supporting devices

Firewalls Processing Modes

- Five processing modes by which firewalls can be categorized:
  - Packet filtering
  - Application gateways
  - Circuit gateways
  - MAC layer firewalls
  - Hybrids

Packet-Filtering Firewalls (1)

- Packet-filtering firewalls examine the header information of data packets.
- Most often based on the combination of:
  - IP source and destination address
  - Direction (inbound or outbound)
  - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests
- Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

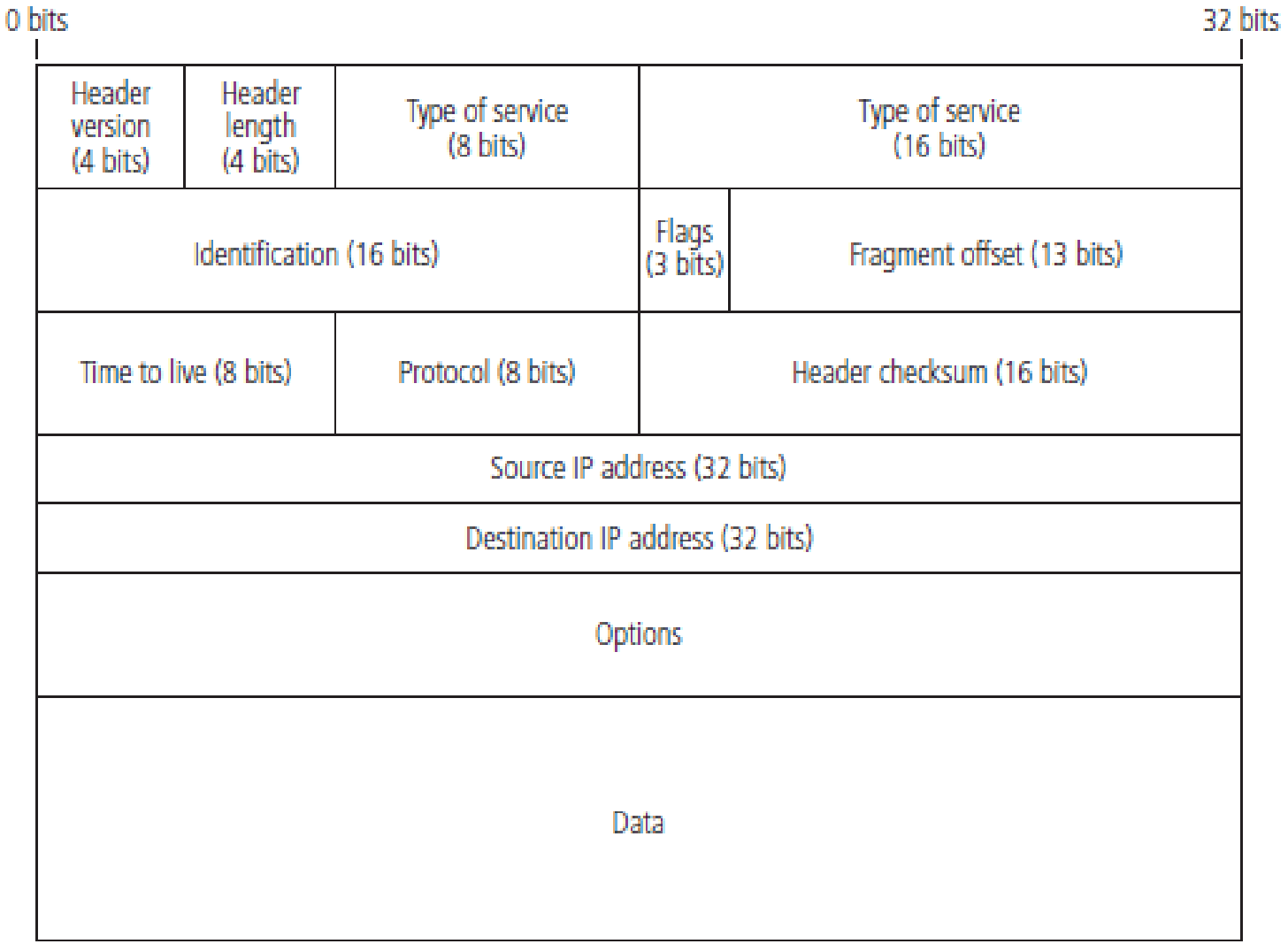


Figure 6-7 IP packet structure

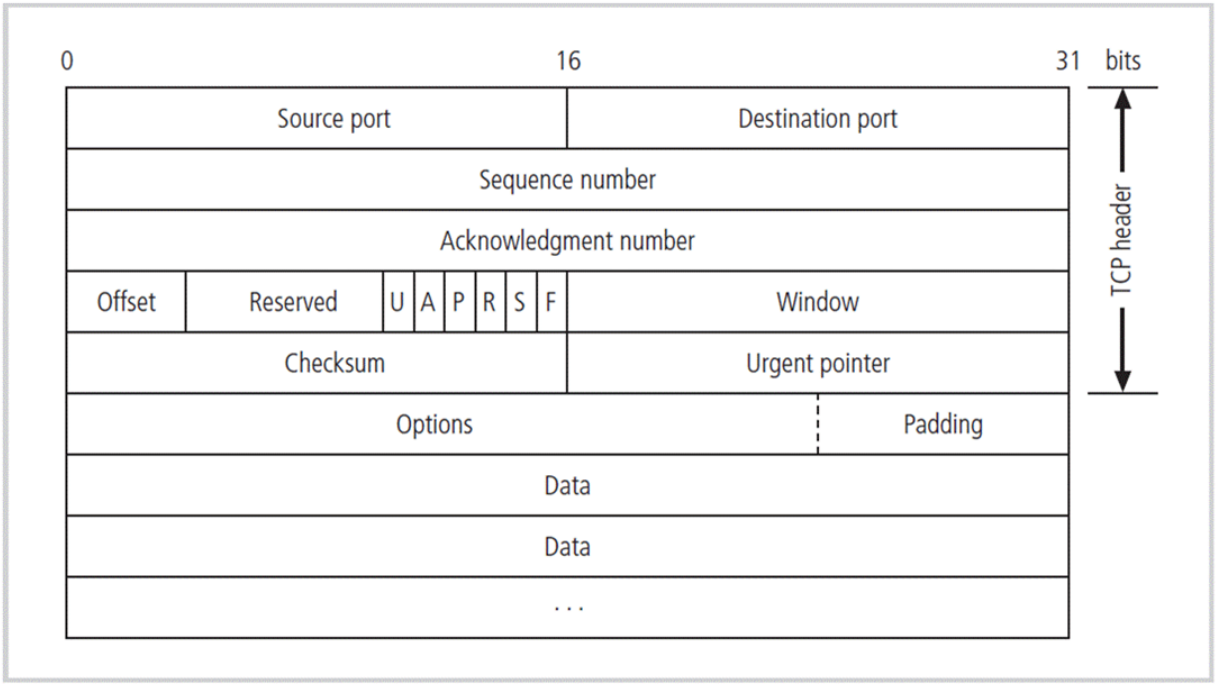


Figure 6-8 TCP packet structure

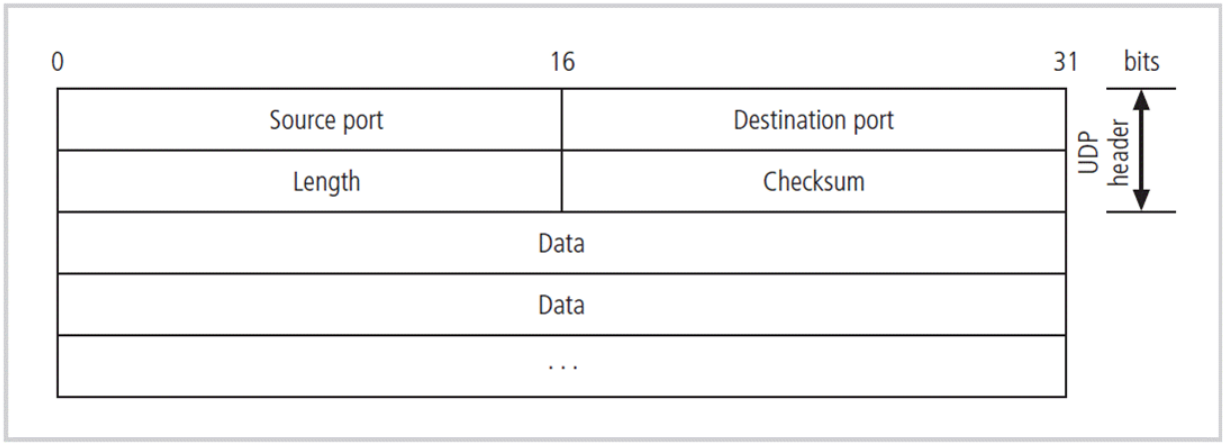


Figure 6-9 UDP datagram structure

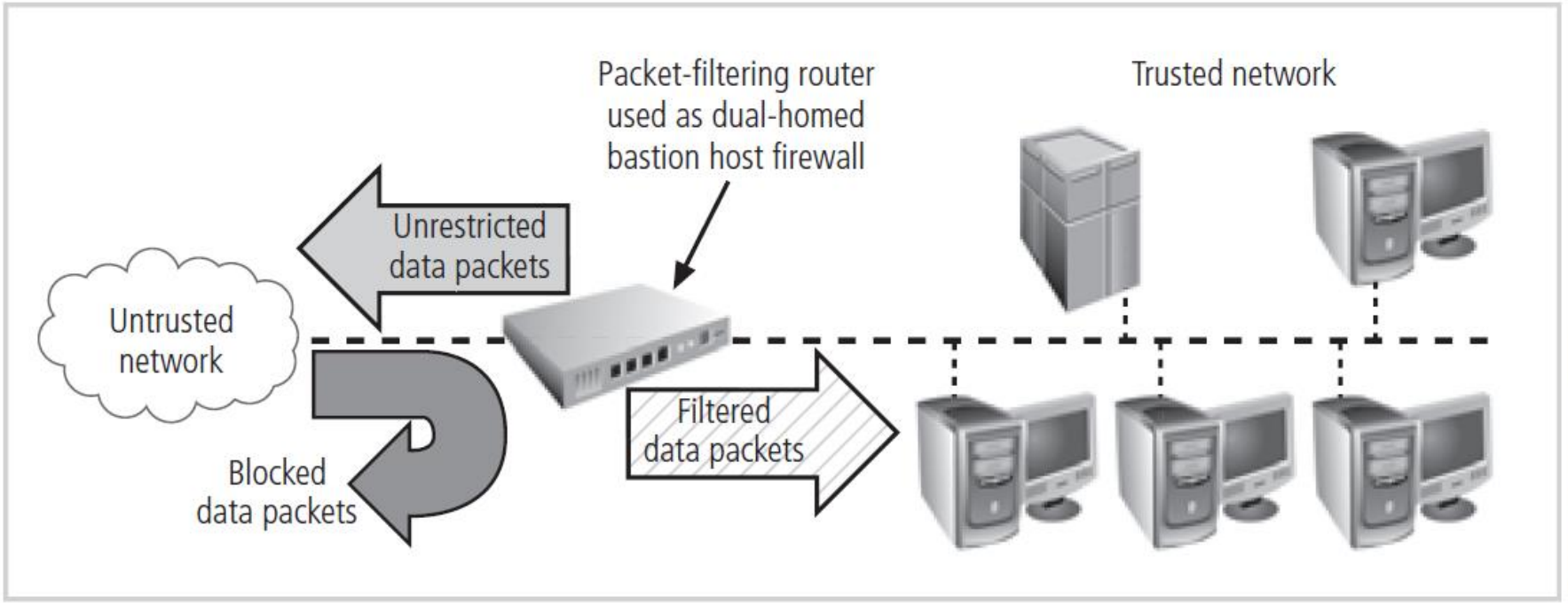


Figure 6-10 Packet-filtering router

Source address	Destination address	Service (e.g., HTTP, SMTP, FTP)	Action (allow or deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Table 6-2 Sample Firewall Rule and Format

Packet-Filtering Firewalls (2)

- Three subsets of packet-filtering firewalls:
  - Static filtering

    requires that filtering rules be developed and installed within the firewall
  - Dynamic filtering

    allows firewall to react to emergent event and update or create rules to deal with event
  - Stateful packet inspection (SPI)

    firewalls that keep track of each network connection between internal and external systems using a state table

Source address	Source port	Destination address	Destination port	Time remaining (in seconds)	Total time (in seconds)	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Table 6-3 State Table Entries

Application Layer Firewall

- Frequently installed on a dedicated computer; also known as a proxy server
- Since proxy server is often placed in unsecured area of the network (e.g., DMZ), it is exposed to higher levels of risk from less trusted networks.
- Additional filtering routers can be implemented behind the proxy server, further protecting internal systems.

MAC layer firewalls

- Designed to operate at media access control sublayer of network's data link layer
- Make filtering decisions based on specific host computer's identity
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked.

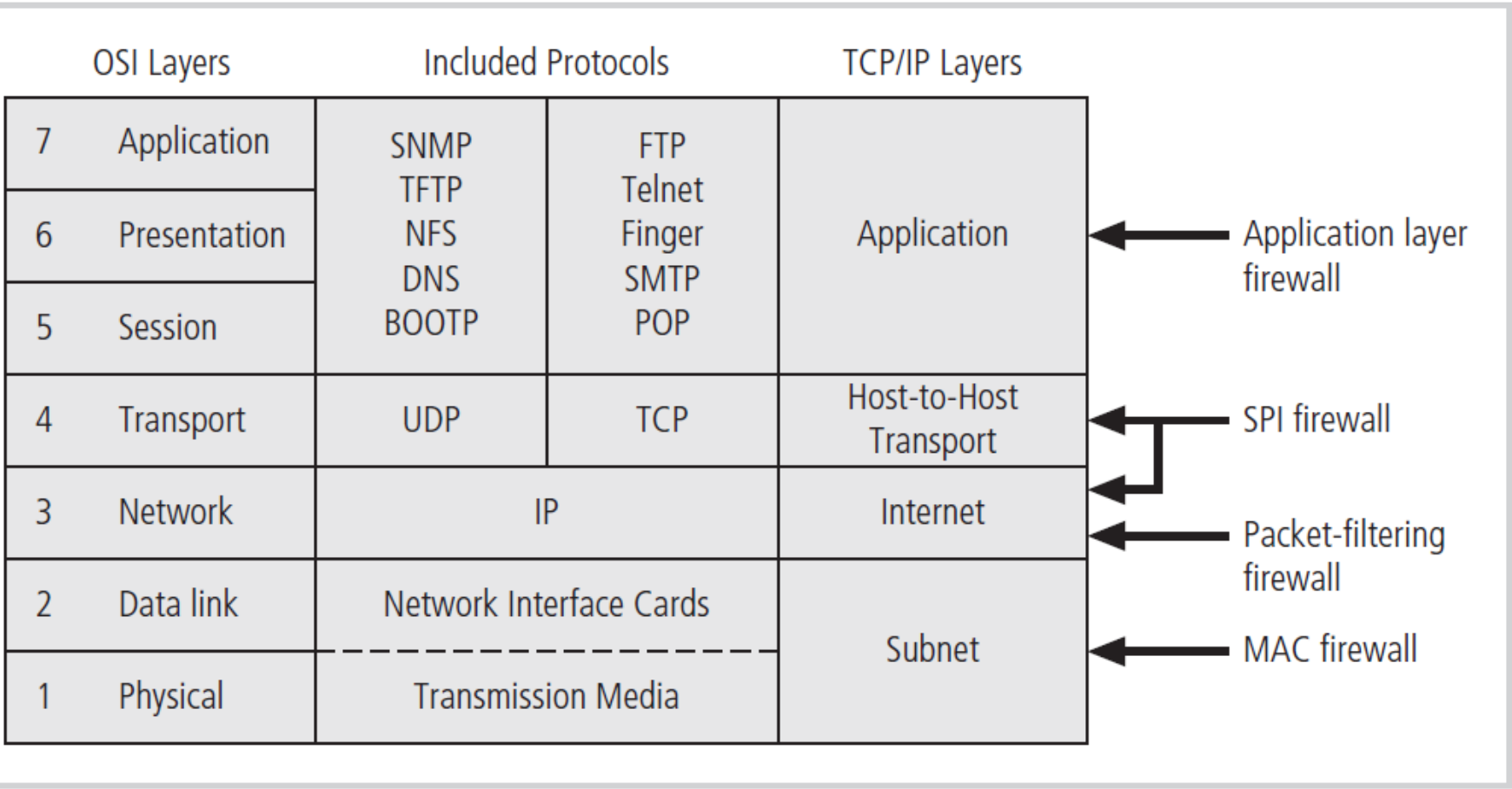


Figure 6-11 Firewall types and protocol models

Hybrid firewalls

- Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways
- Alternately, may consist of two separate firewall devices; each a separate firewall system, but connected to work in tandem
- Enables an organization to make security improvement without completely replacing existing firewalls

Reminder: Quiz 1

On Site:

Thursday 16 Sept, session 1 or 2 in the lab (check the uploaded file)

Be familiar with the lab location

Online (only for IS students who are not in Singapore):

Thursday 16 Sept, login by 4:30pm

Please read and follow instructions carefully

Please prepare 2 devices

Please download and install Lockdown Browser

Please sign consent form before quiz

Please bring along matric card, or passport if you don't have matric card

Firewall Architectures

- Firewall devices can be configured in several network connection architectures.
- Best configuration depends on three factors:
  - Objectives of the network
  - Organization's ability to develop and implement architectures
  - Budget available for function
- Four common architectural implementations of firewalls: packet-filtering routers, dual-homed firewalls (bastion hosts), screened host firewalls, screened subnet firewalls

Packet-filtering routers

- Most organizations with Internet connection have a router at the boundary between internal networks and external service provider.
- Many of these routers can be configured to reject packets that the organization does not allow into its network.
- Drawbacks include a lack of auditing and strong authentication.

Dual-homed firewalls (bastion hosts)

- Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
- Contains two network interface cards (NICs): one connected to external network, one connected to internal network
- Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers.

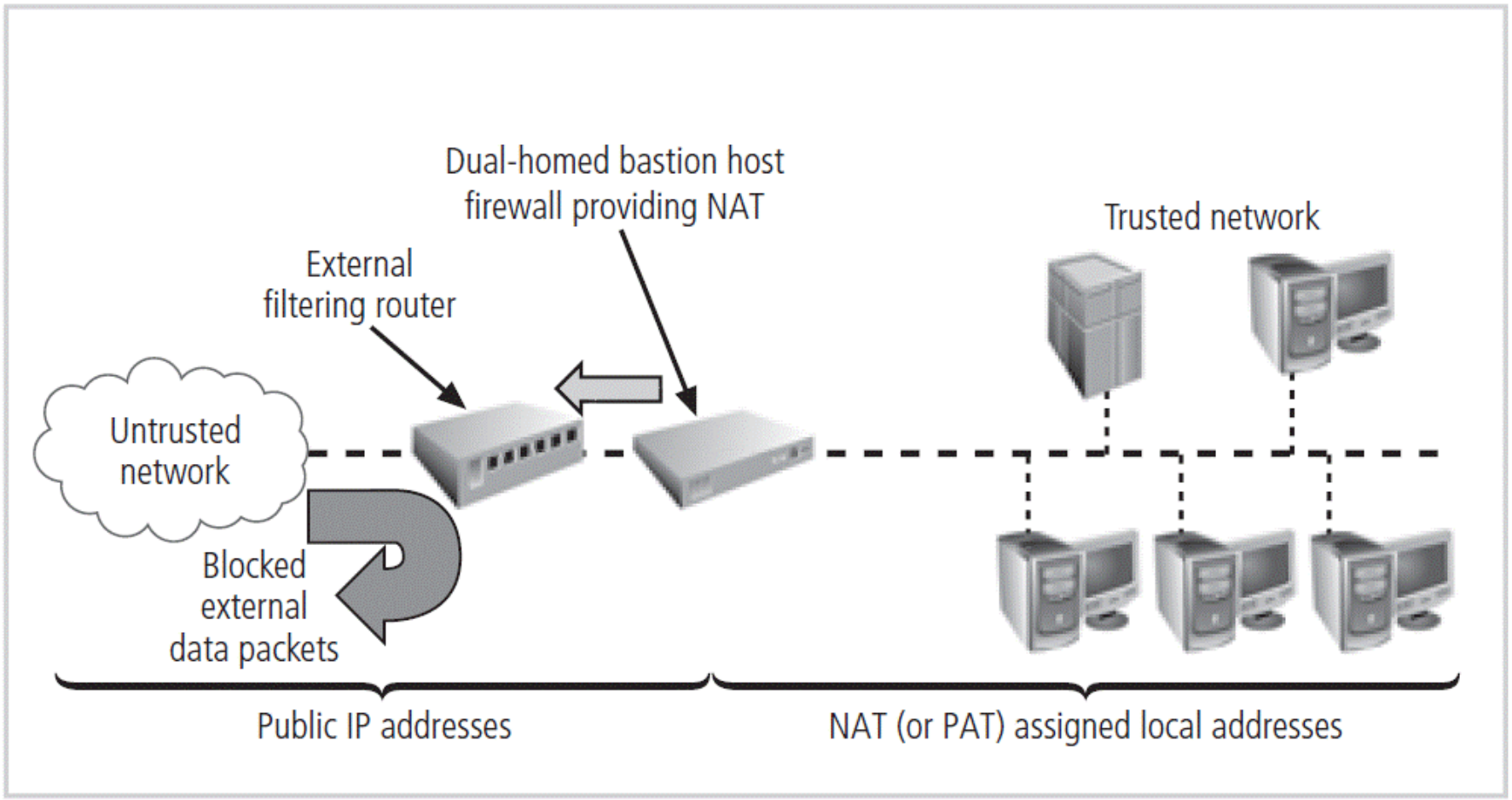


Figure 6-16 Dual-homed bastion host firewall

Screened host firewalls

- Combines packet-filtering router with separate, dedicated firewall such as an application proxy server
- Allows router to prescreen packets to minimize traffic/load on internal proxy
- Requires external attack to compromise two separate systems before attack can access internal data

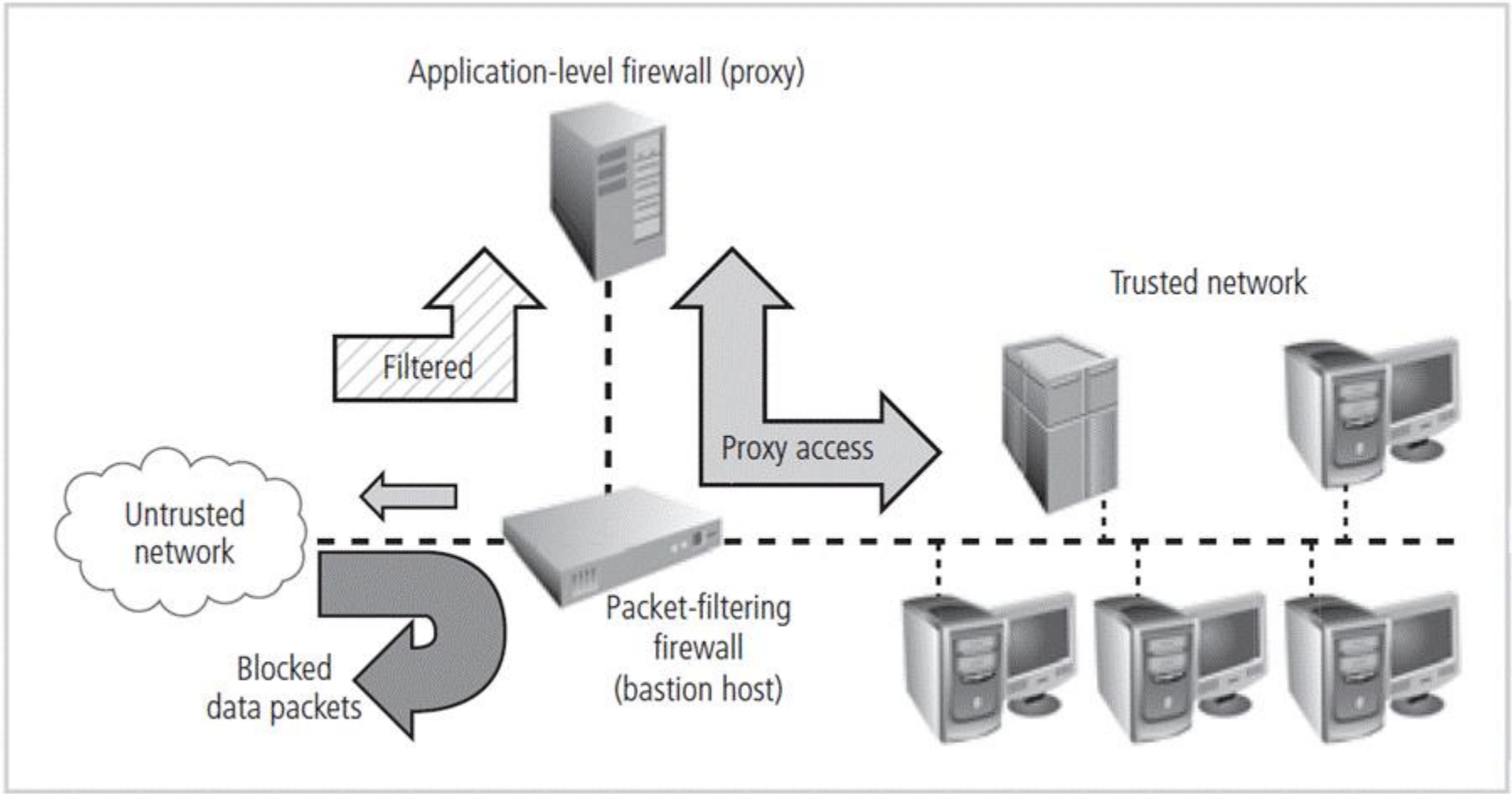


Figure 6-17 Screened host firewall

Screened subnet firewall with DMZ (1)

- Is the dominant architecture used today
- Commonly consists of two or more internal bastion hosts behind packet-filtering router, with each host protecting a trusted network:
  - Connections from outside or untrusted network are routed through external filtering router.
  - Connections from outside or untrusted network are routed into and out of routing firewall to separate the network segment known as DMZ.
  - Connections into trusted internal network are allowed only from DMZ bastion host servers.

Screened subnet firewall with DMZ (2)

- Screened subnet performs two functions:
  - Protects DMZ systems and information from outside threats
  - Protects the internal networks by limiting how external connections can gain access to internal systems
- Another facet of DMZs: extranets

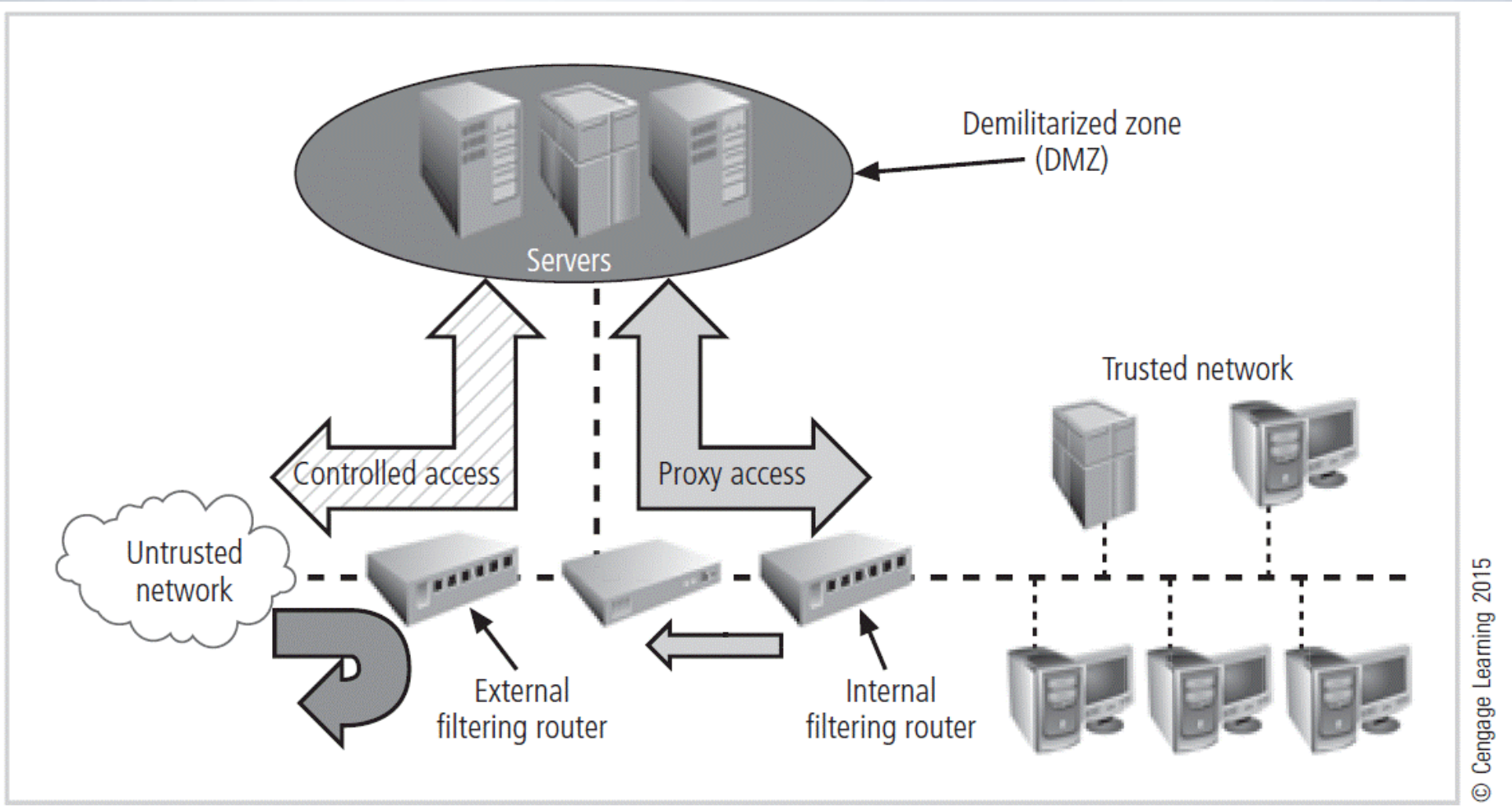


Figure 6-18 Screened subnet (DMZ)

Configuring and Managing Firewalls (1)

- The organization must provide for the initial configuration and ongoing management of firewall(s).
- Each firewall device must have its own set of configuration rules regulating its actions.
- Firewall policy configuration is usually complex and difficult.
- Configuring firewall policies is both an art and a science .
- When security rules conflict with the performance of business, security often loses.

Configuring and Managing Firewalls (2)

- Best practices for firewalls
  - All traffic from the trusted network is allowed out.
  - Firewall device is never directly accessed from public network.
  - Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall.
  - Internet Control Message Protocol (ICMP) data are denied
  - Telnet access to internal servers should be blocked.
  - When Web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks.
  - All data not verifiably authentic should be denied.

Configuring and Managing Firewalls (3)

- Firewall rules
  - Firewalls operate by examining data packets and performing comparison with predetermined logical rules.
  - The logic is based on a set of guidelines most commonly referred to as firewall rules, rule base, or firewall logic.
  - Most firewalls use packet header information to determine whether specific packet should be allowed or denied.

Port number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

Table 6-5 Well-Known Port Numbers

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.0	Any	Any	Any	Deny
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	Any	Any	10.10.10.0	>1023	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	Deny

Table 6-16 External Filtering Firewall Inbound Interface Rule Set

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.12	Any	10.10.10.0	Any	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow
7	Any	Any	Any	Any	Deny

Table 6-17 External Filtering Firewall Outbound Interface Rule Set

Content Filters (not a firewall)

- Software filter - allows administrators to restrict content access from within a network
- Essentially a set of scripts or programs restricting user access to certain networking protocols/Internet locations
- Primary purpose to restrict internal access to external material
- Most common content filters restrict users from accessing non-business Web sites or deny incoming spam.

Protecting Remote Connections

- Installing Internetwork connections requires leased lines or other data channels; these connections are usually secured under the requirements of a formal service agreement.
- When individuals seek to connect to an organization’s network, a more flexible option must be provided.
- Options such as **virtual private networks (VPNs)** have become more popular due to the spread of Internet.

Remote Access

- Unsecured, dial-up connection points represent a substantial exposure to attack.
- Attacker can use a device called a war dialer to locate the connection points.
- War dialer: automatic phone-dialing program that dials every number in a configured range and records number if modem picks up
- Some technologies (RADIUS systems; TACACS; CHAP password systems) have improved the authentication process.

Virtual Private Networks (VPNs) (1)

- Private and secure network connection between systems; uses data communication capability of unsecured and public network
- Securely extends organization's internal network connections to remote locations
- Three VPN technologies defined:
  - **Trusted VPN** - private circuits leased from a trusted communications provider
  - **Secure VPN** - send encrypted traffic over the public Internet
  - **Hybrid VPN** (combines trusted and secure) **-** using a secure VPN over a trusted VPN

Virtual Private Networks (VPNs) (2)

- VPN must accomplish:
  - Encapsulation of incoming and outgoing data
  - Encryption of incoming and outgoing data
  - Authentication of remote computer and perhaps remote user as well
- In most common implementation, it allows the user to turn Internet into a private network.

Transport Mode VPN

- Data within IP packet is encrypted, but header information is not.
- Allows user to establish secure link directly with remote host, encrypting only data contents of packet
- Two popular uses:
  - End-to-end transport of encrypted data
  - Remote access worker connects to office network over Internet by connecting to a VPN server on the perimeter.

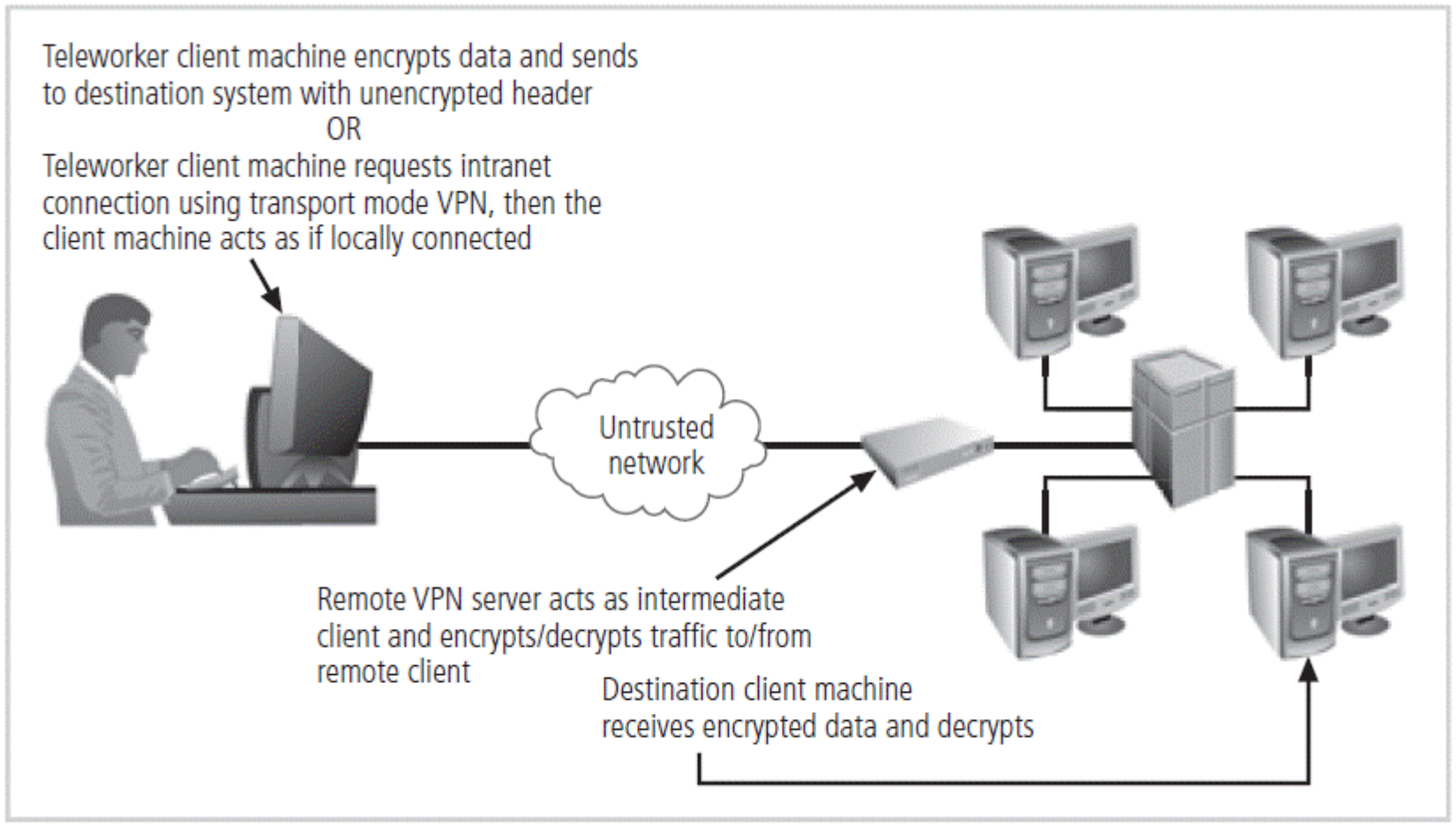


Figure 6-23 Transport mode VPN

Tunnel Mode VPN

- Establishes two perimeter tunnel servers to encrypt all traffic that will traverse unsecured network
- Entire client package encrypted and added as data portion of packet from one tunneling server to another
- Primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.
- Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server

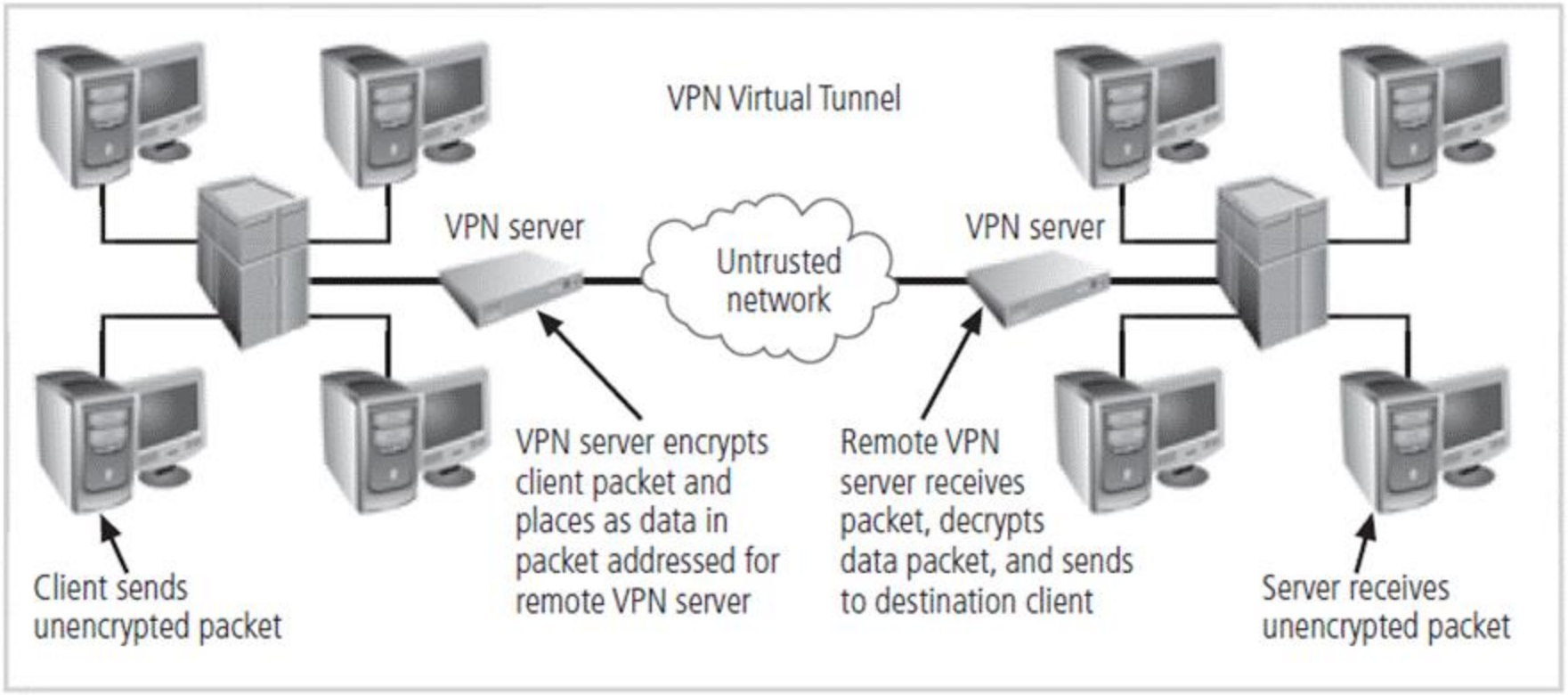


Figure 6-24 Tunnel mode VPN

Summary

- Tools
- Firewall technology
- Content filtering technology
- Various approaches to remote and dial-up access protection
- Virtual private networks