INFORMATION SECURITY

Lecture 6 – Authorisation (Firewalls and VPN)

UNIVERSITY
OF
JOHANNESBURG

Agenda

- Authorisation
- Firewalls
- Firewall architectures
- Content filters
- Remote connections

Firewalls

- In information security, a combination of hardware and software that filters or prevents specific information from moving between the outside (untrusted) network and the inside (trusted) network.
- May be:
  - Separate computer system
  - Software service running on existing router or server
  - Separate network containing supporting devices

Firewalls Processing Modes

- Processing modes by which firewalls can be categorized:
  - Packet filtering
  - Application layer proxy
  - MAC layer firewalls
  - Hybrids

Packet-Filtering Firewalls

- 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 the device.

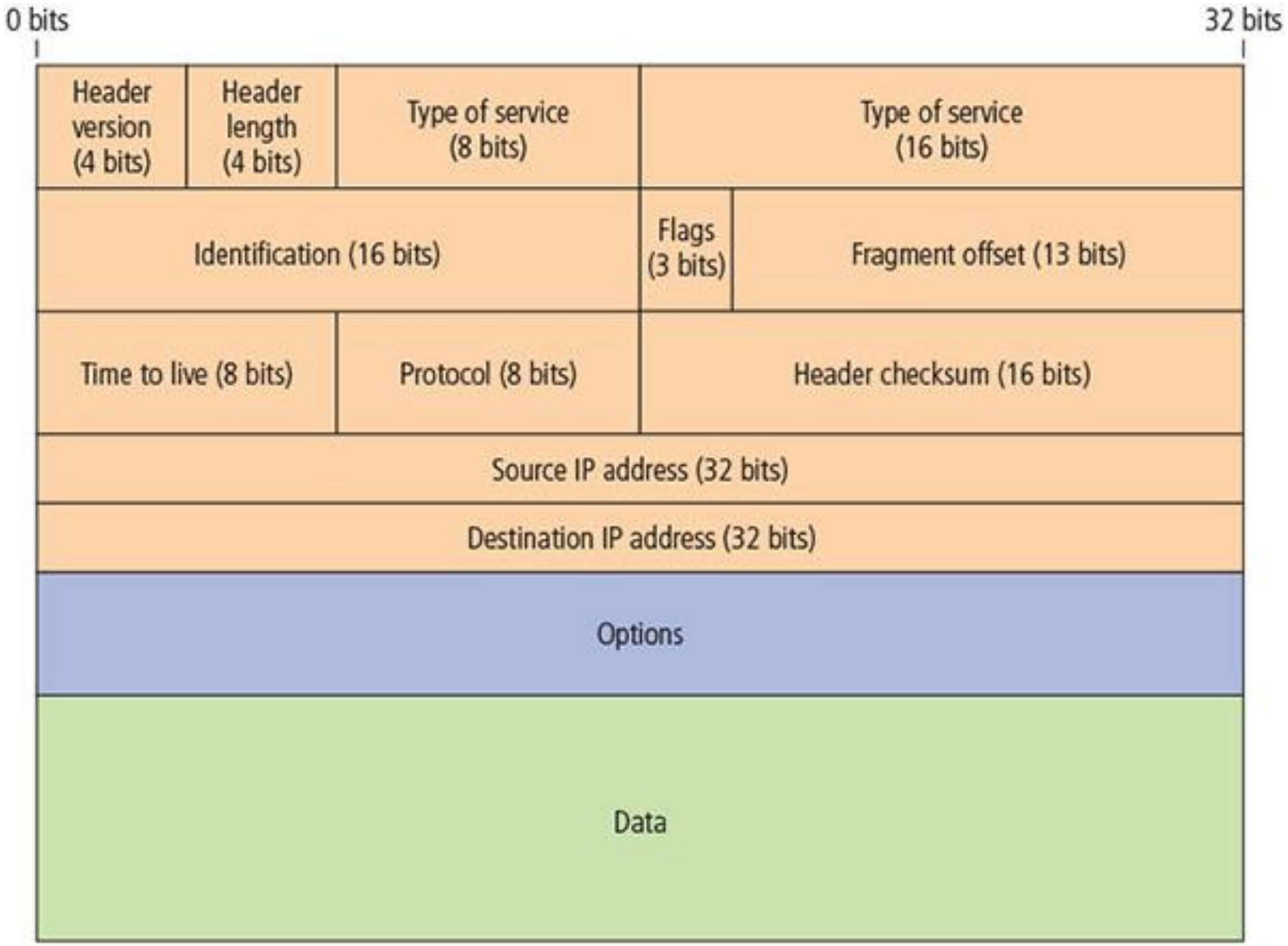
Packet-Filtering Firewalls

- 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 an emergent event and update or create rules to deal with that event
  - Dynamic filtering ensures traffic goes through an authorisation process. Once authorised it opens the holes are required for that specific session and then closes the holes when completed.
  - Stateful packet inspection (SPI) firewalls keep track of each network connection between internal and external systems using a state table

SPI Firewalls

- Some sources categorise SPI firewalls as a dynamic filtering firewall
- SPI firewalls uses a state table to keep track of the state of each connection
- SPI firewalls deny connections that has not been expressly requested from an inside source
- SPI firewalls require more processing power and more memory
- SPI firewalls are vulnerable to DOS or DDOS attacks

IP packet structure



0 bits

32 bits

Header version (4 bits)

Header length (4 bits)

Type of service (8 bits)

Type of service (16 bits)

Identification (16 bits)

Flags (3 bits)

Fragment offset (13 bits)

Time to live (8 bits)

Protocol (8 bits)

Header checksum (16 bits)

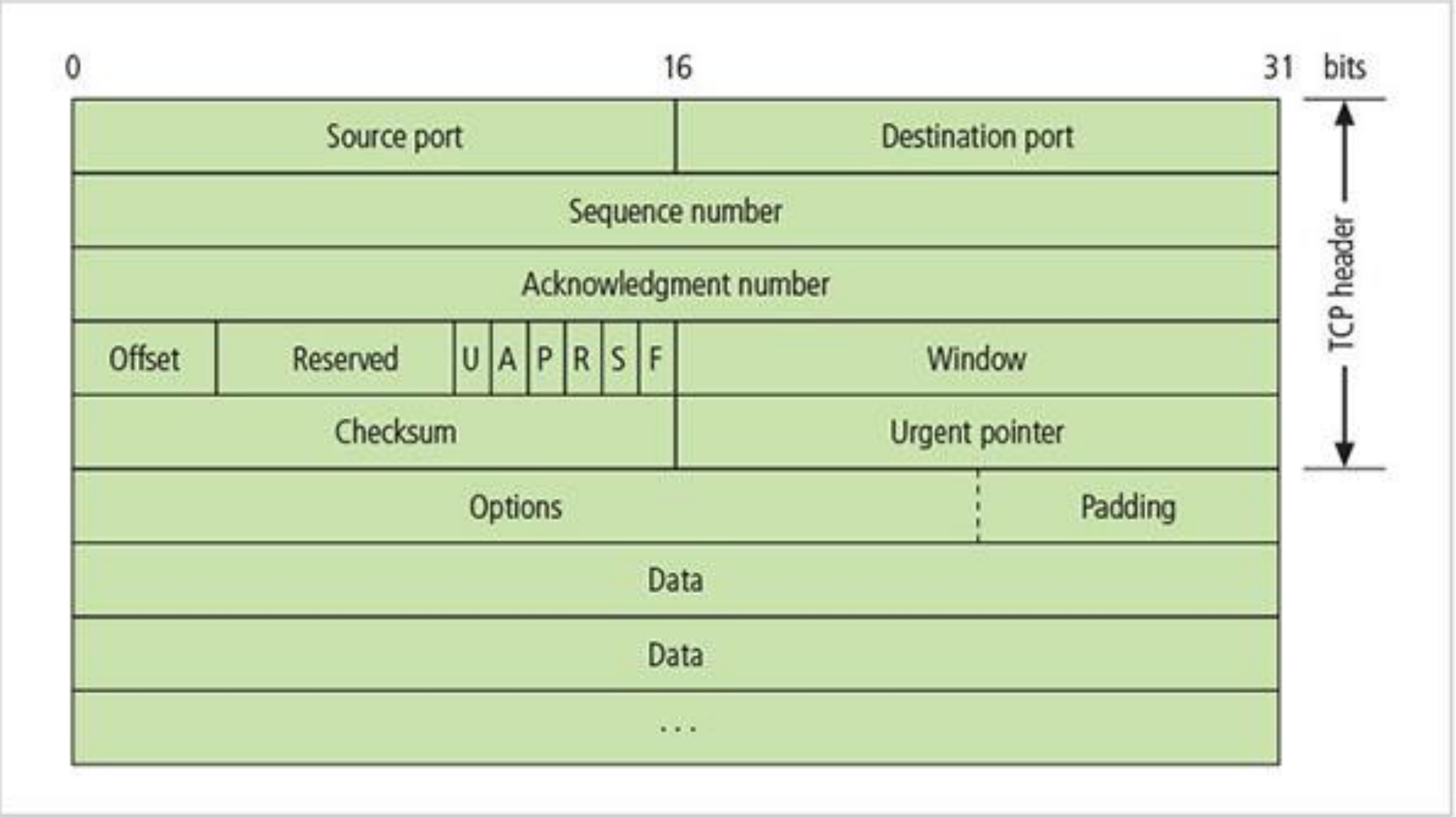
Source IP address (32 bits)

Destination IP address (32 bits)

Options

Data

TCP Packet Structure



0 16 31 bits

Source port | Destination port

Sequence number

Acknowledgment number

Offset | Reserved | U | A | P | R | S | F | Window

Checksum | Urgent pointer

Options | Padding

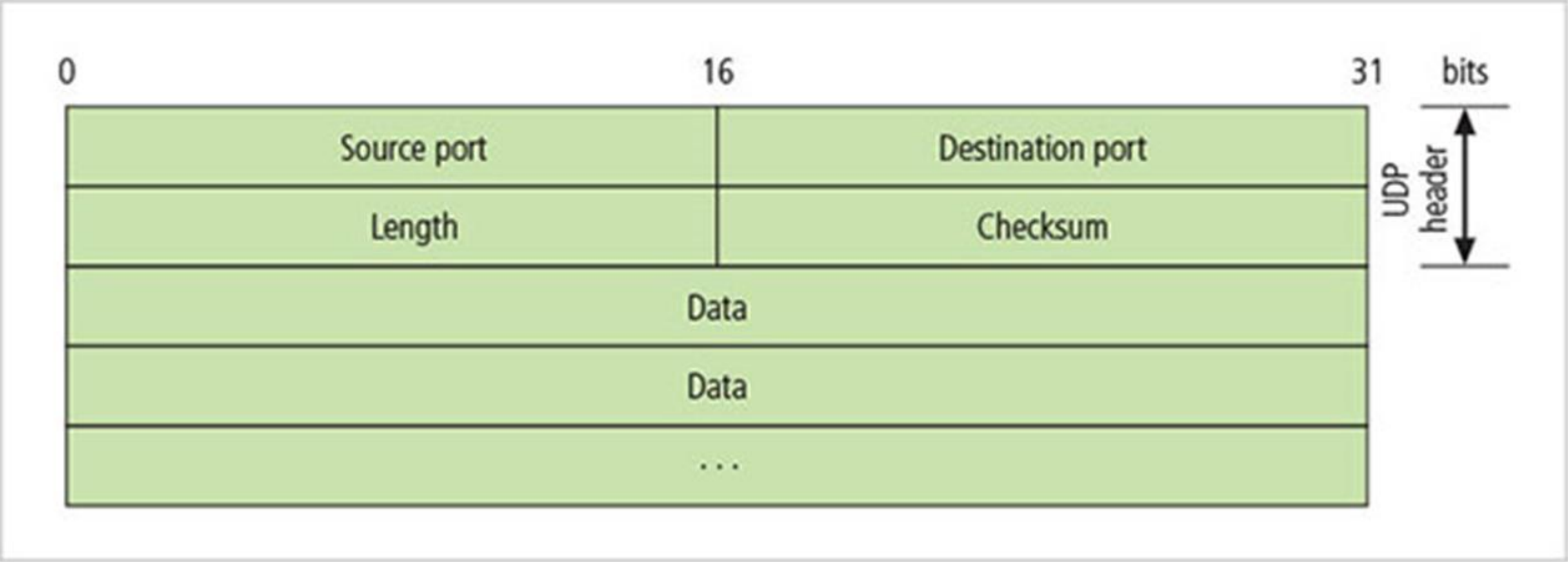
Data

Data

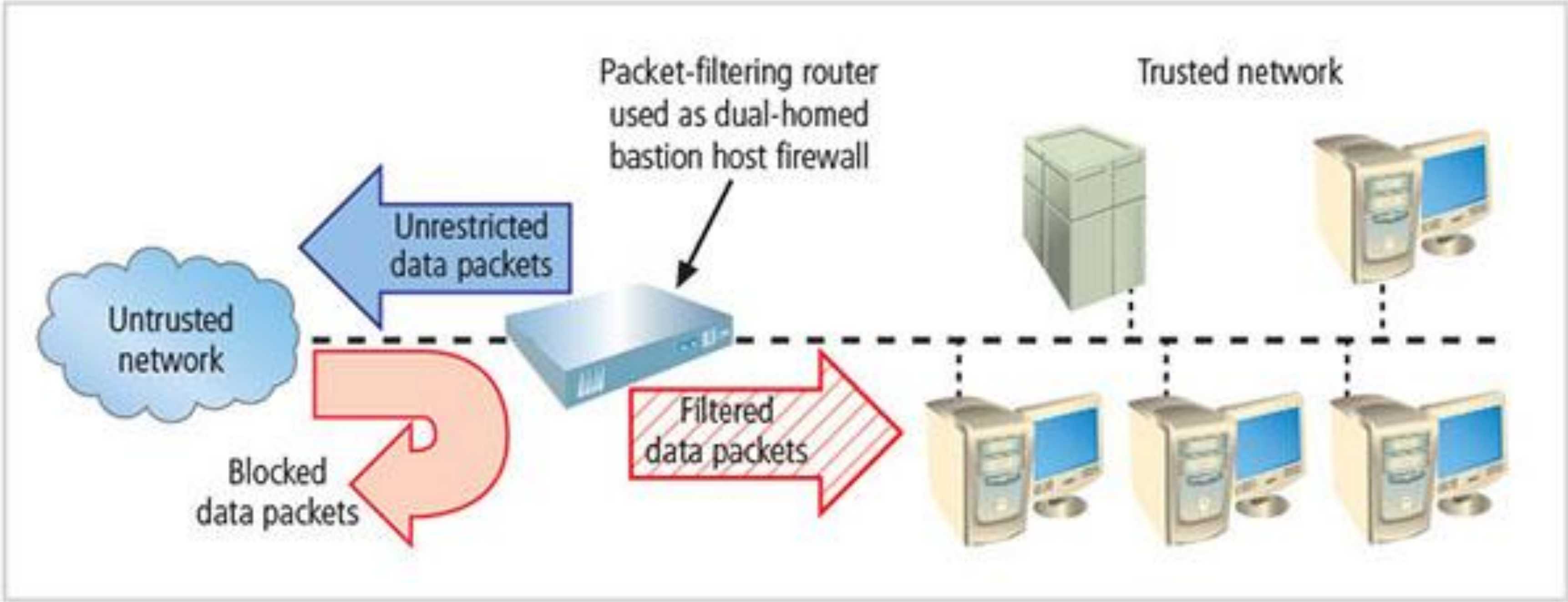
. . .

TCP header

UDP Packet Structure



Packet-filtering router


Packet-filtering router used as dual-homed bastion host firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

Sample Firewall Rule and Format

Source Address	Destination Address	Service (e.g. HTTP, SMTP, FTP)	Action (Allow or Deny)
172.16x.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

State Table Entries

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	2,275	3,600	TCP

Application Layer Proxy Firewall

- A device capable of functioning both as a firewall and an application layer proxy server.
- Since proxy servers are often placed in unsecured area of the network (e.g., DMZ), they are exposed to higher levels of risk from less trusted networks.
- Additional filtering routers can be implemented behind the proxy firewall, further protecting internal systems.

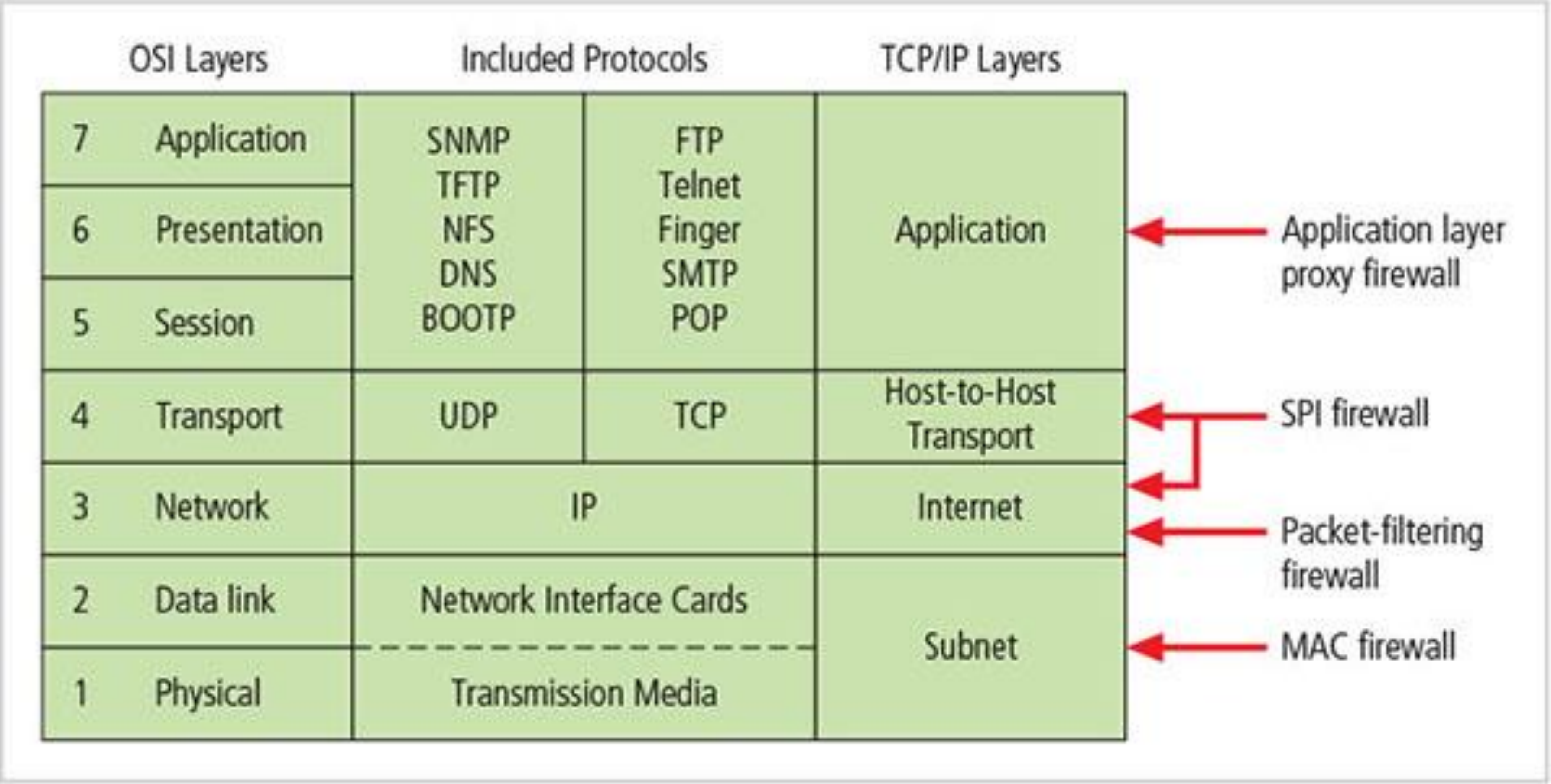
MAC Layer Firewalls

- 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

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
- Include the Next Generation Firewall (NGFW) and Unified Threat Management (UTM) devices

Firewall Types and Protocol Models



OSI Layers		Included Protocols		TCP/IP Layers
7	Application	SNMP TFTP NFS DNS BOOTP	FTP Telnet Finger SMTP POP	Application
6	Presentation			
5	Session			
4	Transport	UDP	TCP	Host-to-Host Transport
3	Network	IP		Internet
2	Data link	Network Interface Cards		Subnet
1	Physical	Transmission Media		

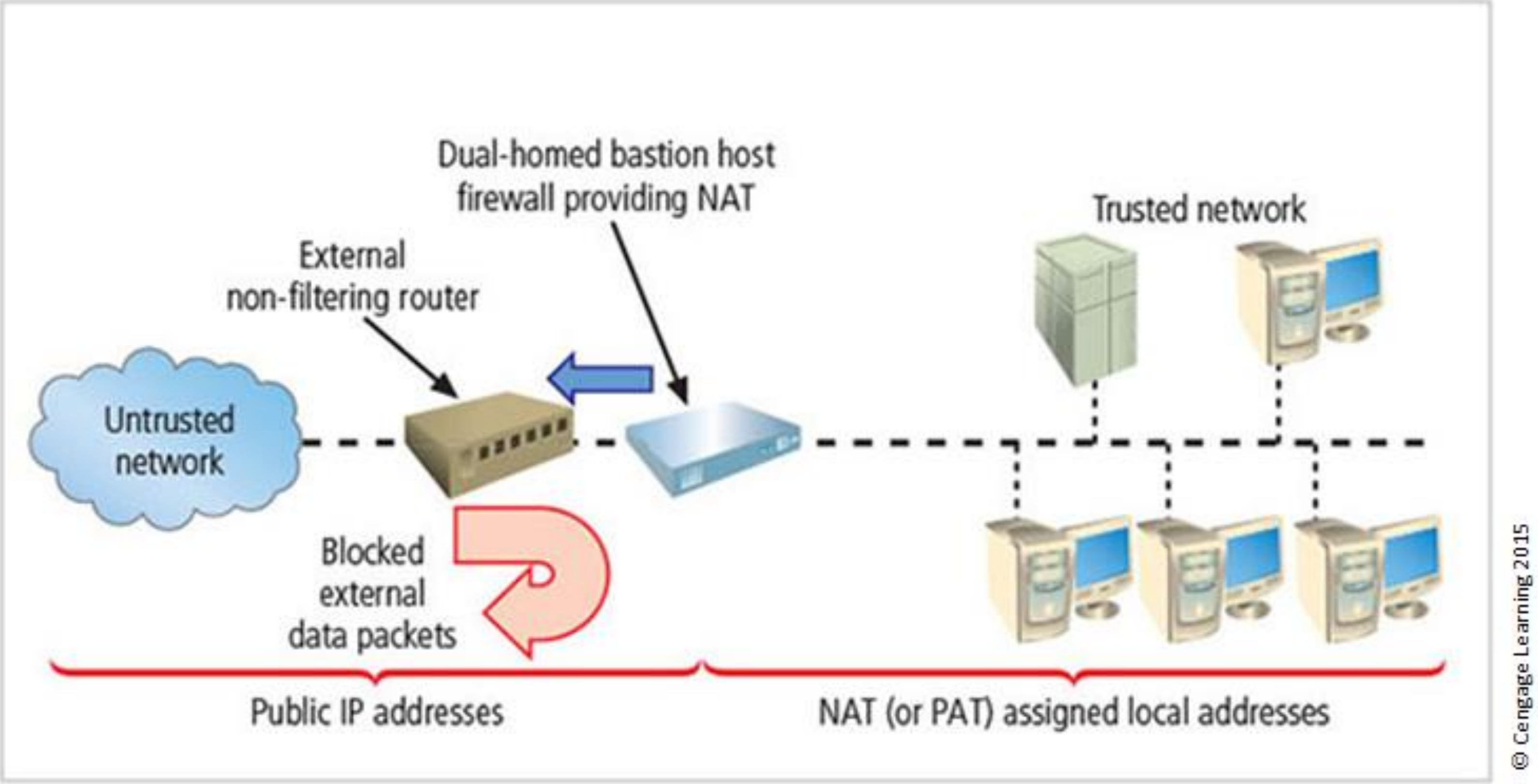
Firewall Architectures

- 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
- Three common architectural implementations of firewalls: single bastion hosts, screened host, and screened subnet (with DMZ).

Firewall Architectures

- Single bastion hosts
  - Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
  - Usually implemented as a dual-homed host, which contains two network interface cards (NICs): one that is connected to external network and one that is connected to internal network
  - Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers

Dual-homed bastion host

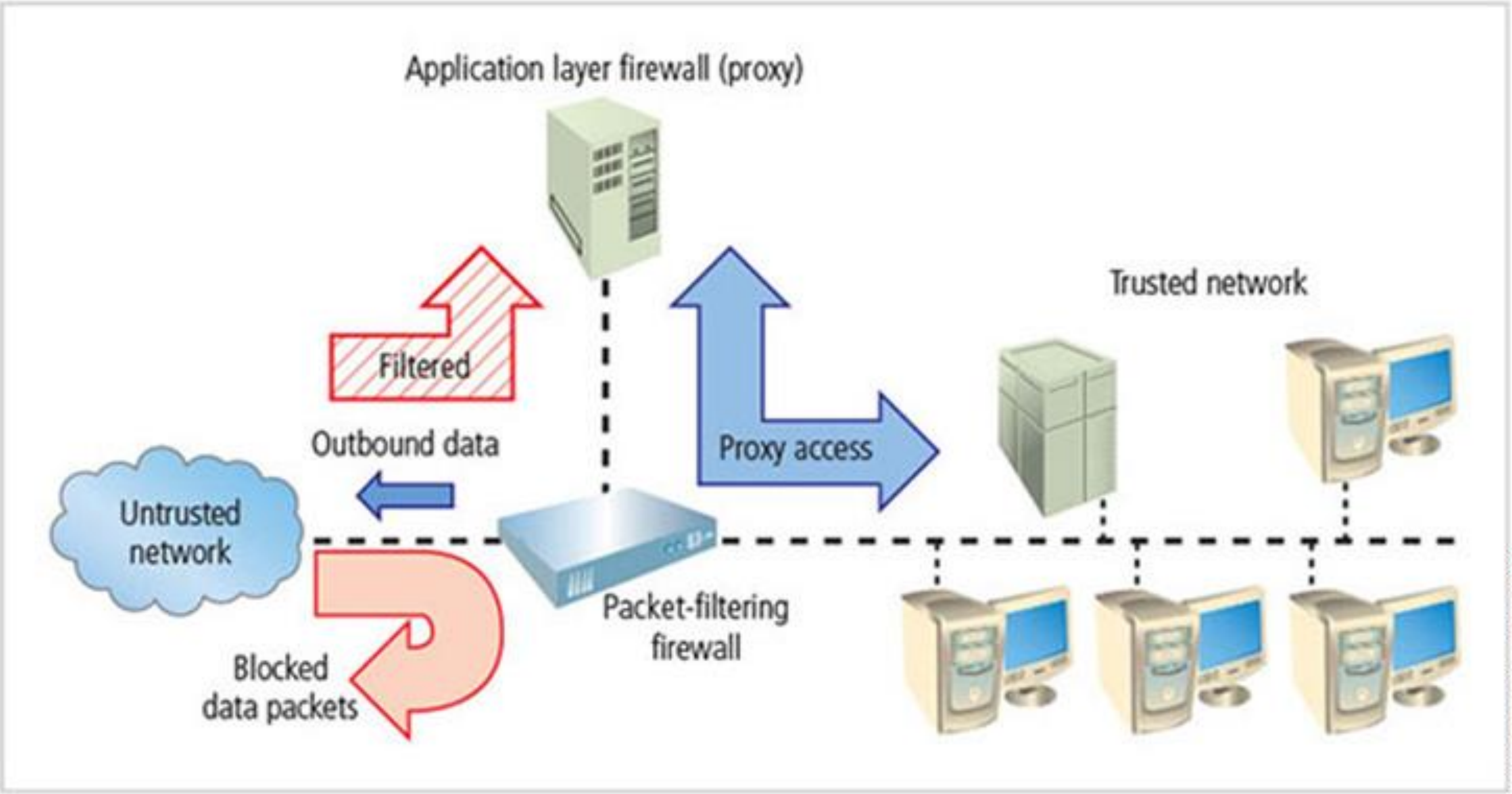


© Cengage Learning 2015

Firewall Architectures

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

Screened host architecture



© Cengage Learning 2015

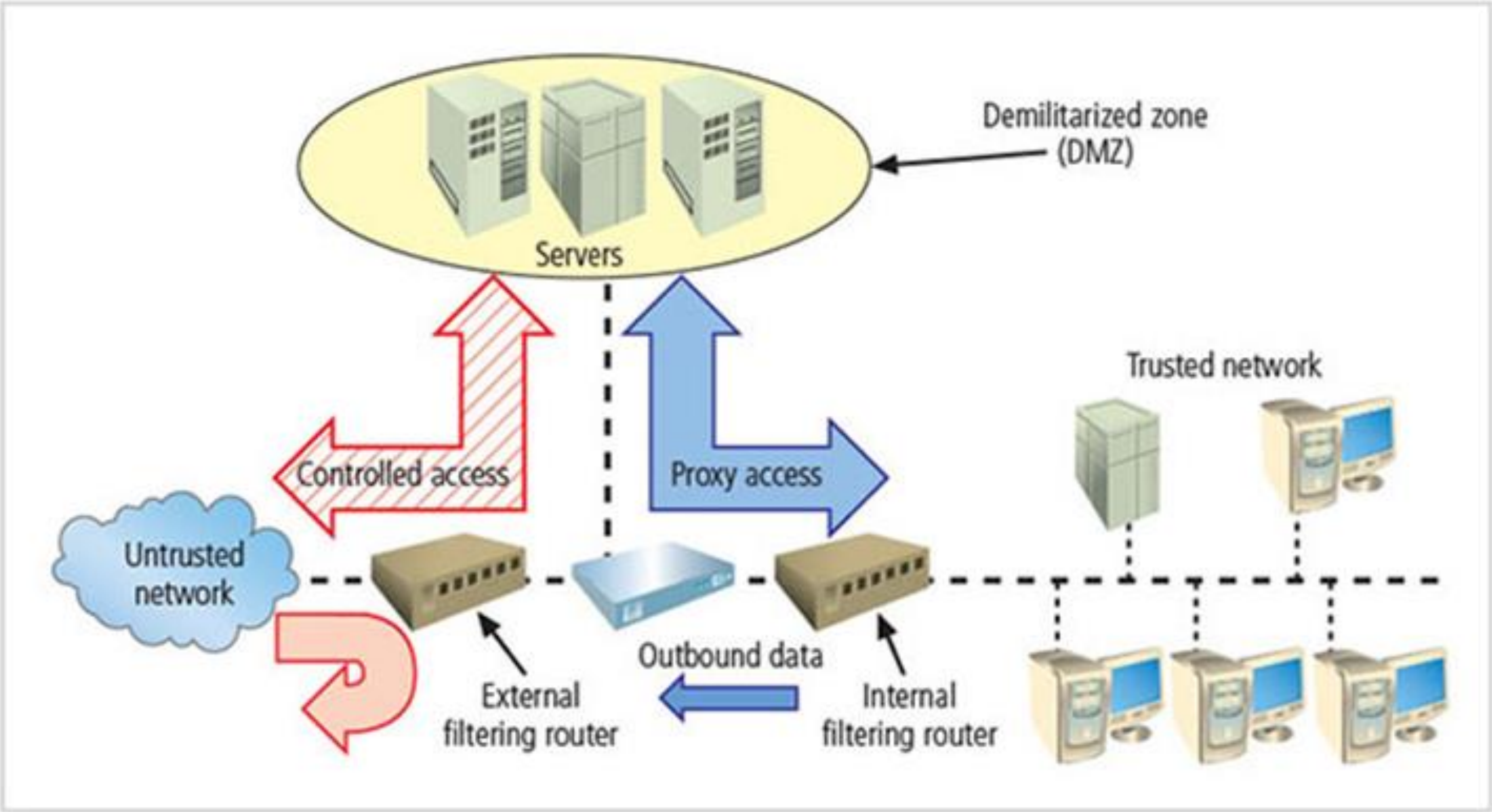
Firewall Architecture

- Screened subnet architecture (with DMZ)
  - Is the dominant architecture used today
  - Commonly consists of two or more internal firewalls behind packet-filtering router, with each 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.

Firewall Architectures

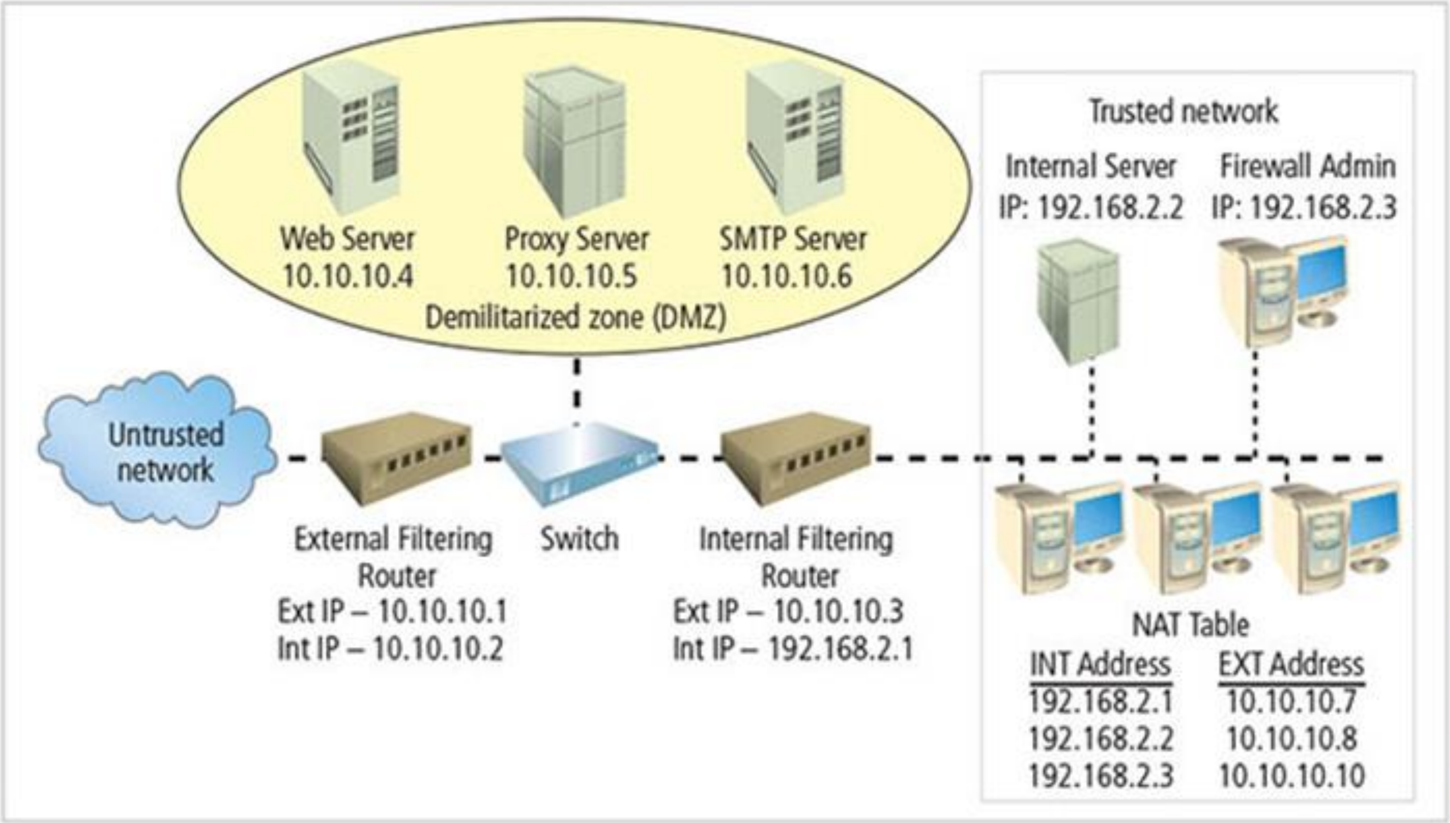
- Screened subnet performs two functions:
  - Protects DMZ systems and information from outside threats
  - Protects the internal networks by limiting how external connections can gain access to internal systems
- Another facet of DMZs: creation of extranets

Screened subnet architecture



© Cengage Learning 2015

Example network configuration



INT Address	EXT Address
192.168.2.1	10.10.10.7
192.168.2.2	10.10.10.8
192.168.2.3	10.10.10.10

© Cengage Learning 2015

Selecting the Right Firewall

- When selecting the firewall, consider the following factors:
  - Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?
  - What features are included in the base price? What features are available at extra cost? Are all cost factors known?
  - How easy is it to set up and configure the firewall? Does the organization have staff on hand that are trained to configure the firewall, or would the hiring of additional employees be required?
  - Can the firewall adapt to the growing network in the target organization?
- Most important factor is provision of required protection
- Second most important issue is cost

Configuring and Managing Firewall

- 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

- 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 that are not verifiably authentic should be denied.

Configuring and Managing Firewalls

- 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 a specific packet should be allowed or denied.

Content Filters

- A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves 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 (1 of 5)

- 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 a modem picks up.
- Some technologies (Kerberos; RADIUS systems; TACACS; CHAP password systems) have improved the authentication process.

Remote Access (2 of 5)

- RADIUS, Diameter, and TACACS
  - Systems that authenticate user credentials for those trying to access an organization’s network via dial-up
  - Remote Authentication Dial-In User Service (RADIUS) centralizes responsibility for user authentication in a central RADIUS server
  - Diameter: emerging alternative derived from RADIUS
  - Terminal Access Controller Access Control System (TACACS) validates user’s credentials at centralized server (like RADIUS); based on client/server configuration

Remote Access (3 of 5)

- Kerberos
  - Provides secure third-party authentication
  - Uses symmetric key encryption to validate individual user to various network resources
  - Keeps database containing private keys of clients/servers
  - Consists of three interacting services:
    - Authentication server (AS)
    - Key Distribution Center (KDC)
    - Kerberos ticket granting service (TGS)

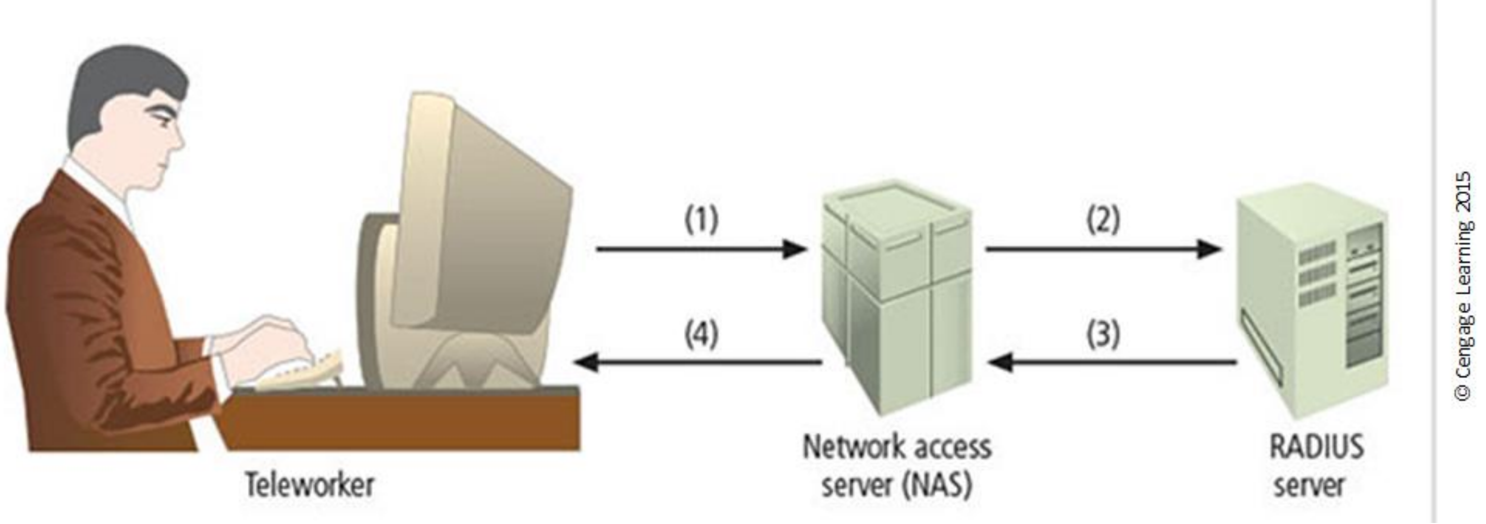
Remote Access (4 of 5)

- Kerberos
  - Provides secure third-party authentication
  - Uses symmetric key encryption to validate individual user to various network resources
  - Keeps database containing private keys of clients/servers
  - Consists of three interacting services:
    - Authentication server (AS)
    - Key Distribtion Center (KDC)
    - Kerberos ticket granting service (TGS)

Remote Access (5 of 5)

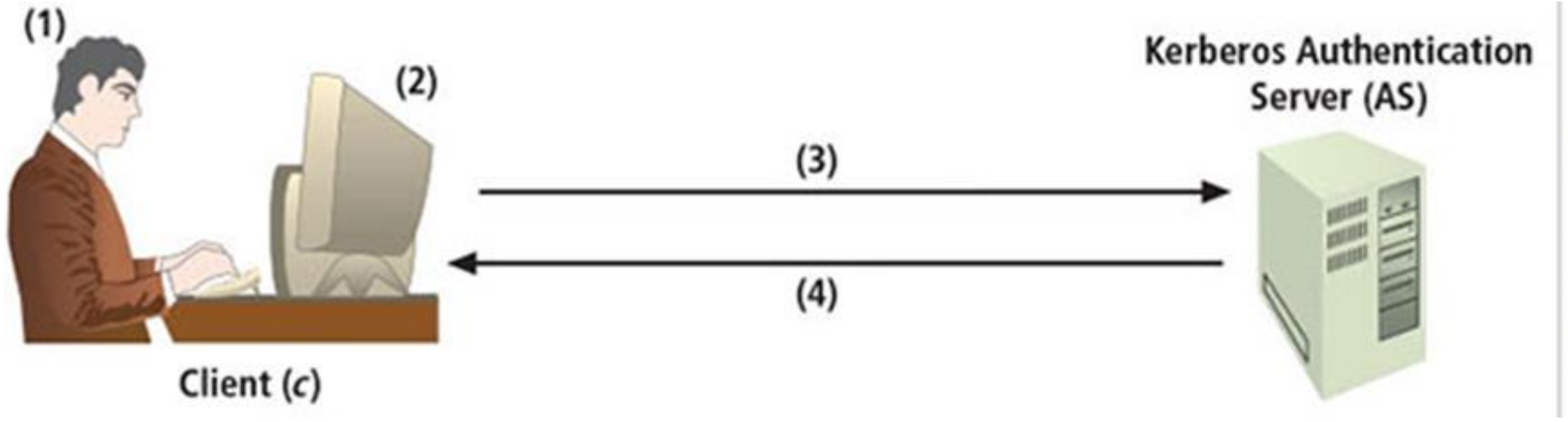
- SESAME
  - Secure European System for Applications in a Multivendor Environment (SESAME) is similar to Kerberos
    - User is first authenticated to authentication server and receives token
    - Token is then presented to a privilege attribute server as proof of identity to gain a privilege attribute certificate
    - Uses public key encryption, adds sophisticated access control features, more scalable encryption systems, improved manageability, auditing features, and options for delegation of responsibility for allowing access

Figure 6-20 RADIUS configuration



1. Remote worker dials NAS and submits username and password
2. NAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. NAS provides access to authorized remote worker

Figure 6-21 Kerberos login (1 of 2)

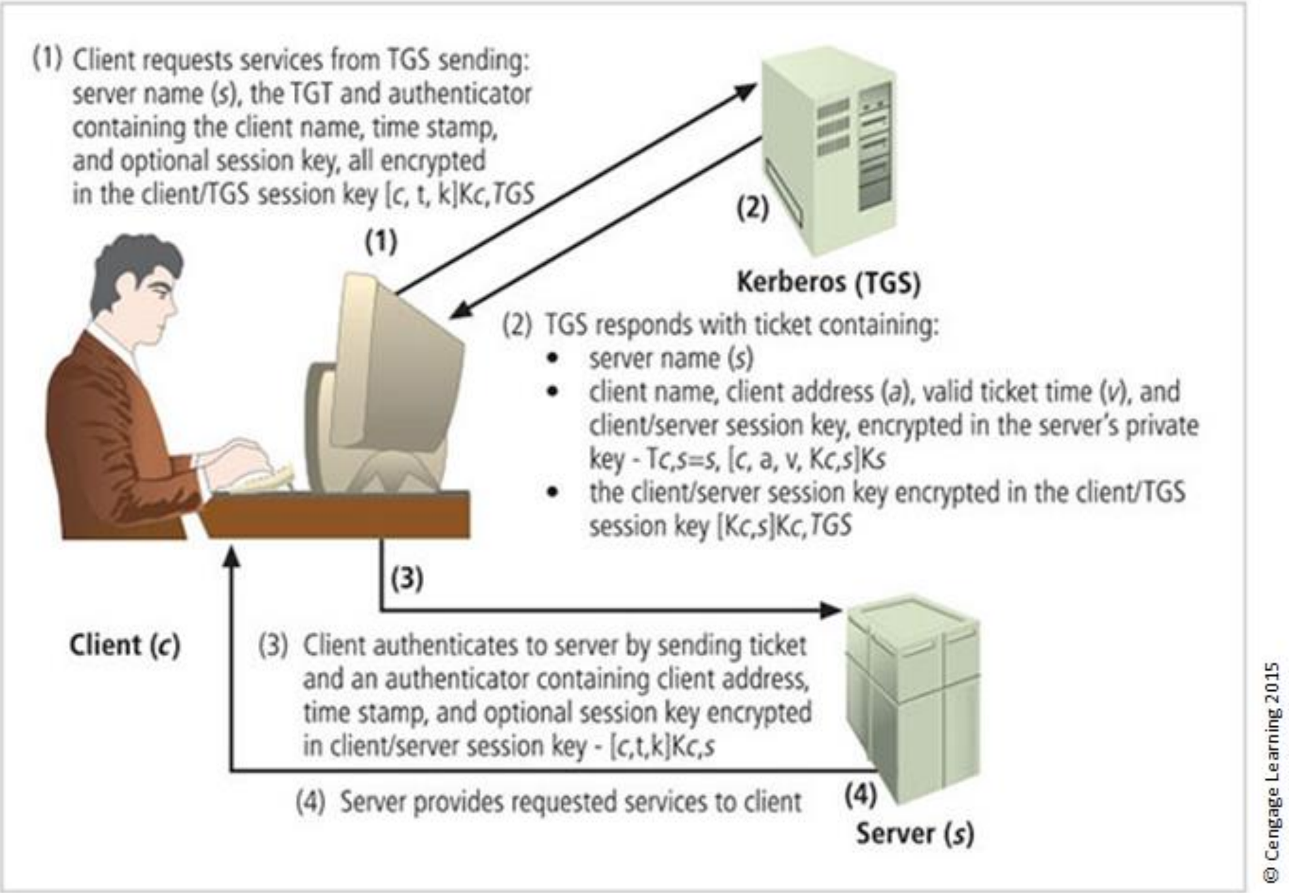


© Cengage Learning 2015

Figure 6-21 Kerberos login (2 of 2)

1. User logs into client machine (c)
2. Client machine encrypts password to create client key (Kc)
3. Client machine sends clear request to Kerberos Authentication Server (AS)
4. Kerberos AS returns ticket consisting of:
   - Client/TGS session key for future communications between client and TGS [Kc,TGS], encrypted with the client's key
   - Ticket granting ticket (TGT). The TGT contains the client name, client address, ticket valid times, and the client/TGS session key, all encrypted in the TGS' private key

Figure 6-22 Kerberos request for services



(1) Client requests services from TGS sending: server name (s), the TGT and authenticator containing the client name, time stamp, and optional session key, all encrypted in the client/TGS session key [c, t, k]Kc,TGS
(1)
(2)
Kerberos (TGS)
(2) TGS responds with ticket containing:
• server name (s)
• client name, client address (a), valid ticket time (v), and client/server session key, encrypted in the server's private key - Tc,s=s, [c, a, v, Kc,s]Ks
• the client/server session key encrypted in the client/TGS session key [Kc,s]Kc,TGS
(3)
Client (c)
(3) Client authenticates to server by sending ticket and an authenticator containing client address, time stamp, and optional session key encrypted in client/server session key - [c,t,k]Kc,s
(4) Server provides requested services to client
(4)
Server (s)

© Cengage Learning 2015

Virtual Private Networks (VPNs) (1 of 4)

- 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
  - Secure VPN
  - Hybrid VPN (combines trusted and secure)

Virtual Private Networks (VPNs) (2 of 4)

- 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

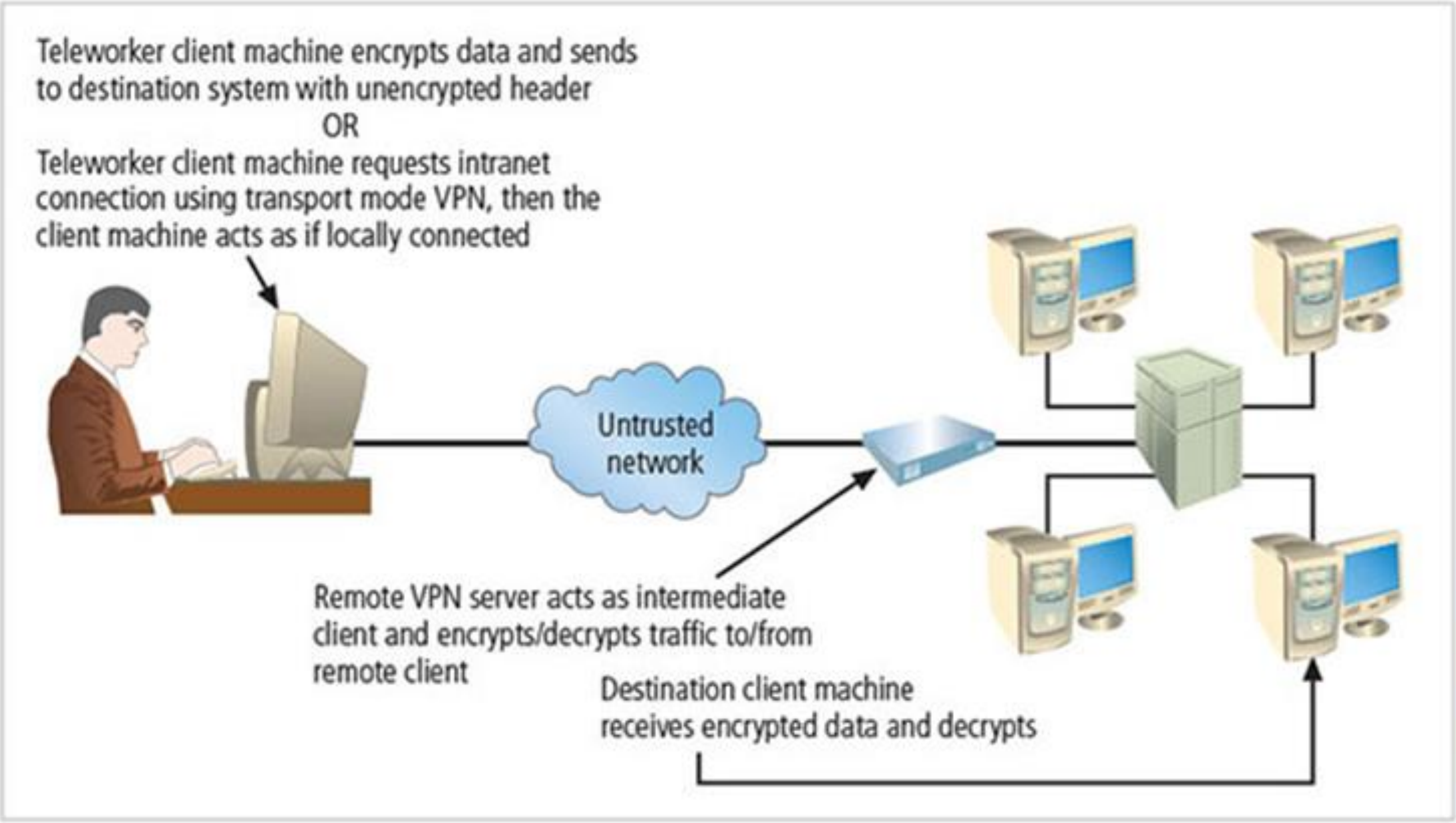
Virtual Private Networks (VPNs) (3 of 4)

- Transport mode
    - Data within IP packet are 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 an office network over Internet by connecting to a VPN server on the perimeter

Virtual Private Networks (VPNs) (4 of 4)

- Tunnel mode
  - Establishes two perimeter tunnel servers to encrypt all traffic that will traverse an 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 6-23 Transport mode VPN



Teleworker client machine encrypts data and sends to destination system with unencrypted header

OR

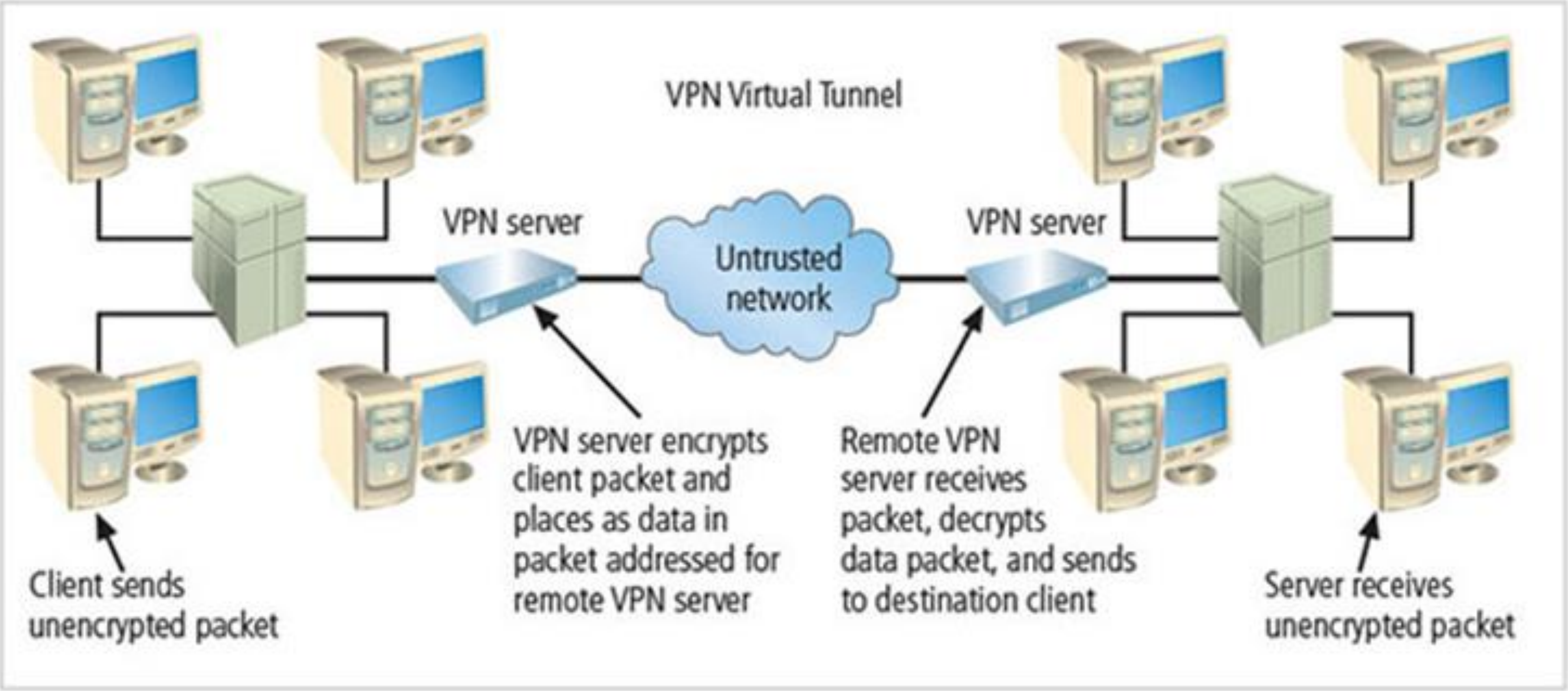
Teleworker client machine requests intranet connection using transport mode VPN, then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client

Destination client machine receives encrypted data and decrypts

© Cengage Learning 2015

Figure 6-24 Tunnel mode VPN


VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client sends unencrypted packet
Server receives unencrypted packet

© Cengage Learning 2015