SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks (cont.)

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

ENCRYPTION FOR NETWORKS

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Encryption for networks

- Link encryption
- End-to-end encryption,
- Tools that are commonly used for implementing network encryption

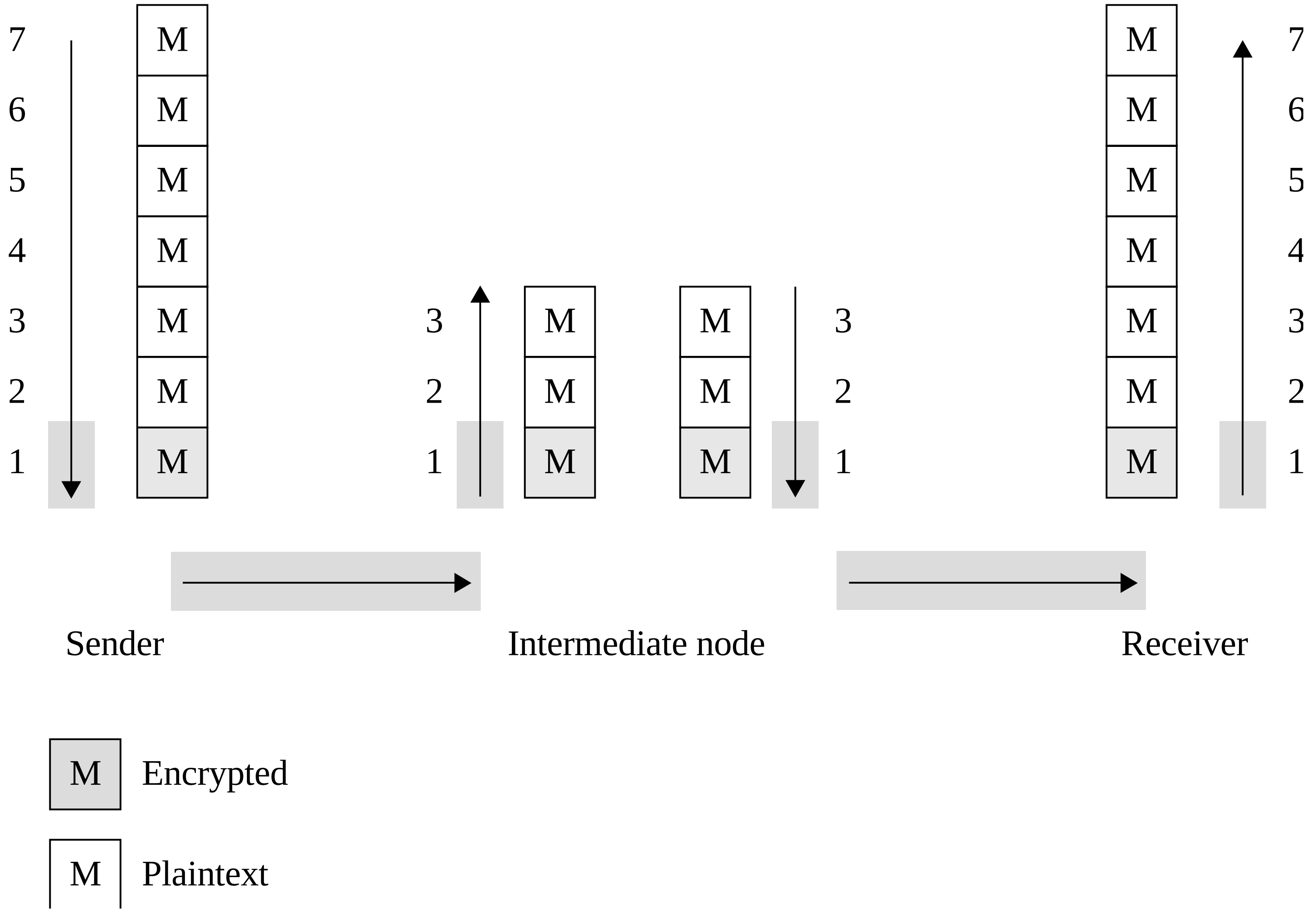
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption

- In link encryption data packets are encrypted just before system places them on the physical communications link
- Data packets are decrypted just as they arrive at the destination system.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

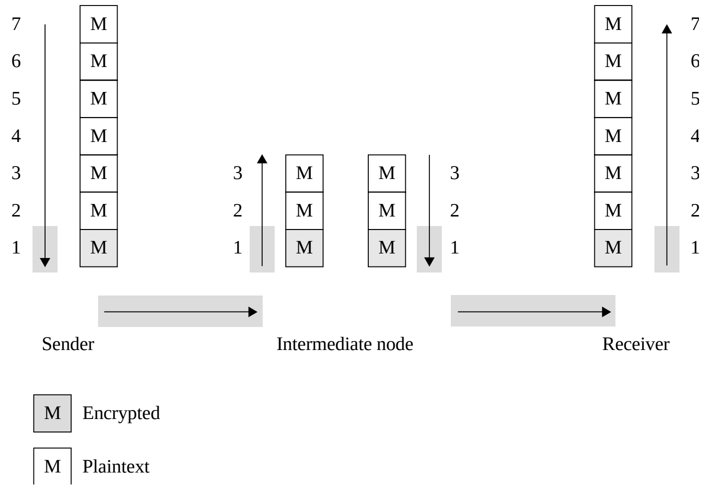
Link Encryption Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption Example

- Data is encrypted only at layer 1 OSI stack.
- If data is communicated through an intermediate node:
  - The intermediate node will decrypt the data when it arrives
  - May re-encrypt it for the next link.
- Link encryption is appropriate when the transmission line is the point of greatest vulnerability
  - such as in wireless scenarios

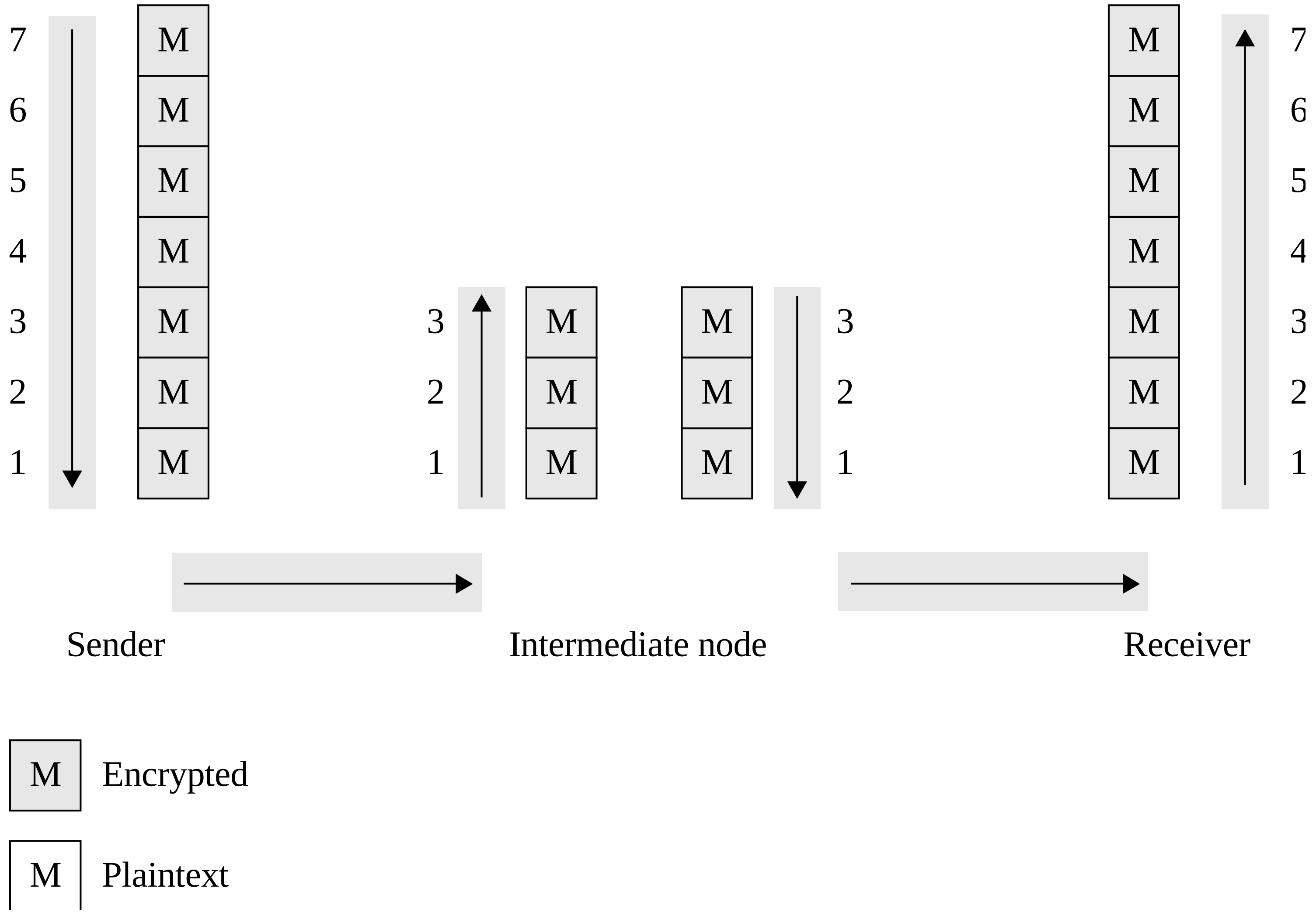


End-to-End Encryption

- Data is encrypted all the way up to OSI layer 7, the application layer
  - In contrast with link encryption
  - In real-world end-to-end encryption, the data often isn't encrypted all the way to layer 7
    - such as encryption that use SSL,
- Important: intermediate nodes cannot decrypt the data.
- End-to-end encryption is appropriate whenever sending sensitive data through untrustworthy intermediate nodes
  - such as over the Internet

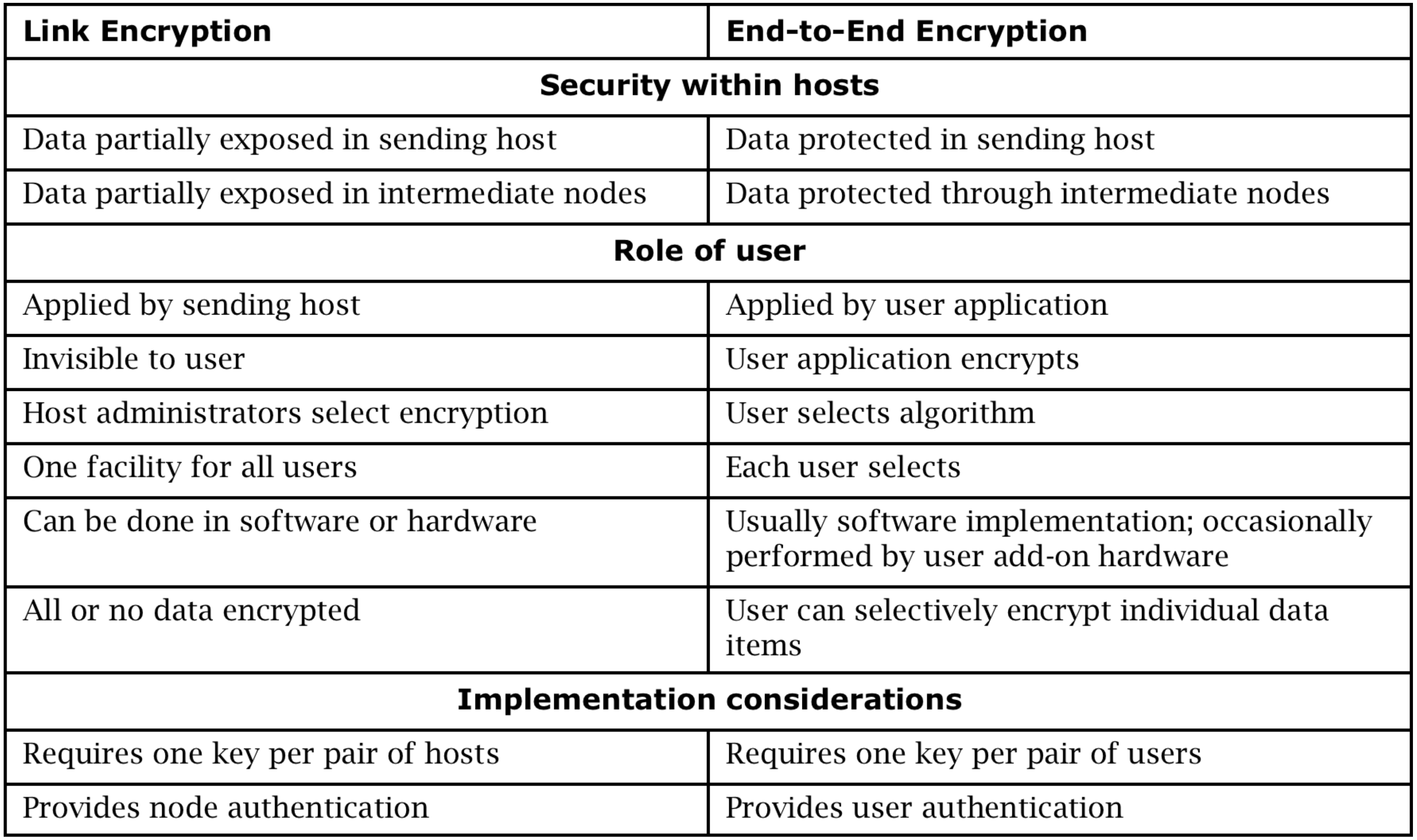
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

End-to-End Encryption



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link vs. End-to-End



Link Encryption	**End-to-End Encryption**
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Secure Shell (SSH)

- Originally developed for UNIX but now available on most OSs
- Provides an authenticated, encrypted path to the OS command line over the network
- Replacement for insecure utilities such as Telnet, rlogin, and rsh
- Protects against spoofing attacks and modification of data in communication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Secure Shell (SSH)

- A secure interactive command session:

1. The client connects to the server via a TCP session.
2. The client and server exchange information on administrative details, such as supported encryption methods and their protocol version, each choosing a set of protocols that the other supports.
3. The client and server initiate a secret-key exchange to establish a shared secret session key, which is used to encrypt their communication (but not for authentication). This session key is used in conjunction with a chosen block cipher (typically AES, 3DES) to encrypt all further communications.

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

Secure Shell (SSH)

- A secure interactive command session (cont.):

4. The server sends the client a list of acceptable forms of authentication, which the client will try in sequence. The most common mechanism is to use a password or the following public-key authentication method:
   a) If public-key authentication is the selected mechanism, the client sends the server its public key.
   b) The server then checks if this key is stored in its list of authorized keys. If so, the server encrypts a challenge using the client's public key and sends it to the client.
   c) The client decrypts the challenge with its private key and responds to the server, proving its identity.
5. Once authentication has been successfully completed, the server lets the client access appropriate resources, such as a command prompt.

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

SSL and TLS

- Secure Sockets Layer (SSL) was designed in the 1990s to protect communication between a web browser and server
- In a 1999 upgrade to SSL, it was renamed Transport Layer Security (TLS)
- While the protocol is still commonly called SSL, TLS is the modern, and much more secure, protocol
- SSL is implemented at OSI layer 4 (transport) and provides
  - Server authentication
  - Client authentication (optional)
  - Encrypted communication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites

- At the start of an SSL session, the client and server negotiate encryption algorithms, known as the “cipher suite”
- The server sends a list of cipher suite options, and the client chooses an option from that list
- The cipher suite consists of
    - A digital signature algorithm for authentication
    - An encryption algorithm for confidentiality
    - A hash algorithm for integrity

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites

- Cipher suite negotiation is at the center of a very common SSL configuration vulnerability
- It is very common for servers to be configured to offer as many cipher suites as possible to provide broad compatibility
- Cipher suite options may have significant known vulnerabilities (many actually do)
    - presents the opportunity for a man-in-the-middle to negotiate on the client's behalf for a weak cipher suite that the attacker can break

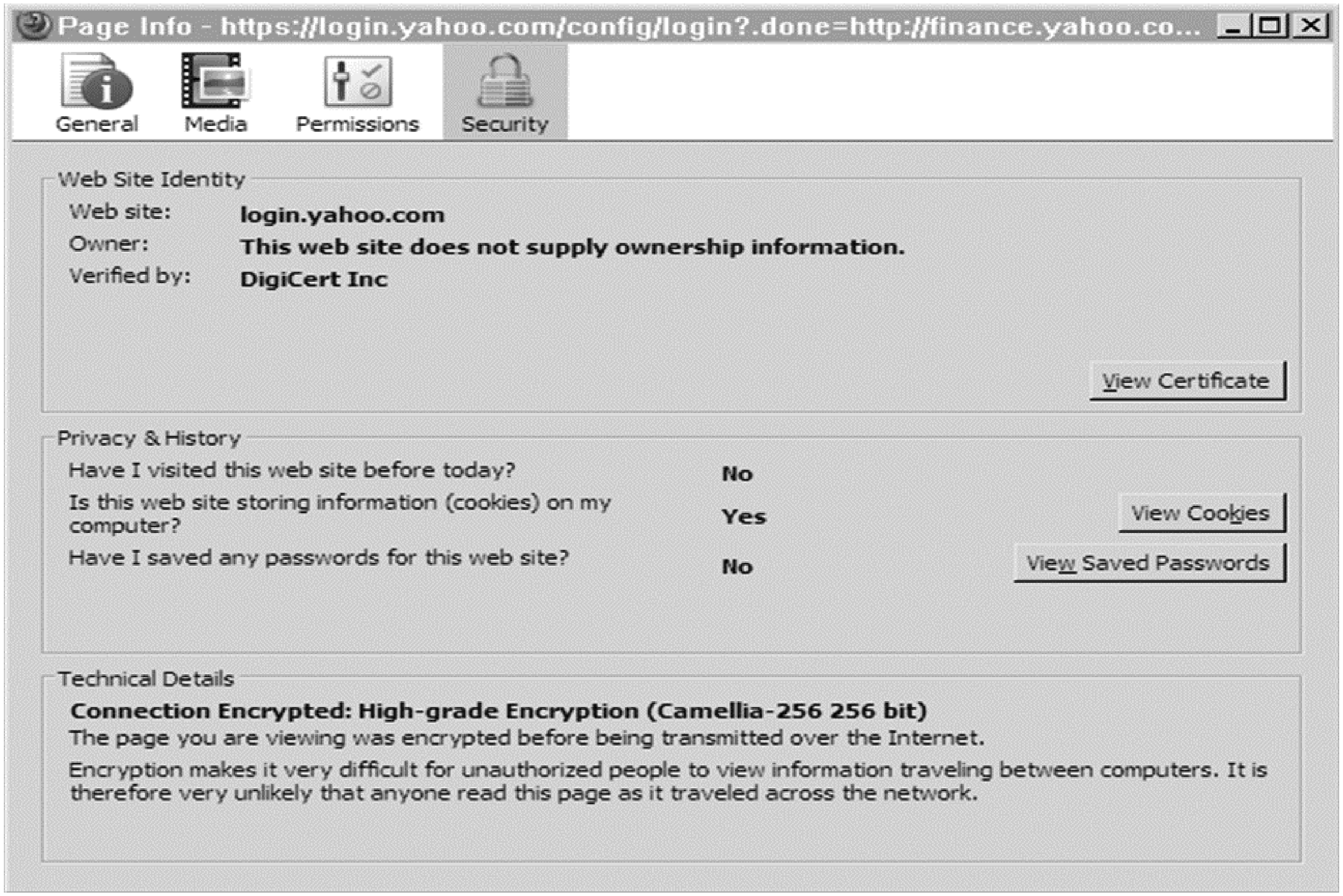
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites (Partial List)

Cipher Suite Identifier	**Algorithms Used**
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 hash function
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA	RSA authentication, AES with a 128-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_256_CBC_SHA	RSA authentication, AES with a 256-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA authentication, AES with a 128-bit key encryption, SHA-256 hash function
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA authentication, AES with a 256-bit key encryption, SHA-256 hash function
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie–Hellman digital signature standard, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA http://www.iana.org/go/rfc5932	RSA digital signature, Camellia encryption with a 256-bit key, SHA-1 hash function
TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	Elliptic curve cryptosystem digital signature algorithm, Aria encryption with a 256-bit key, SHA-384 hash function

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Session Established


Page Info - https://login.yahoo.com/config/login?.done=http://finance.yahoo.co...
General
Media
Permissions
Security
View Certificate
View Cookies
View Saved Passwords

Web Site Identity

Web site:	**login.yahoo.com**
Owner:	**This web site does not supply ownership information.**
Verified by:	**DigiCert Inc**

Privacy & History

Have I visited this web site before today?	**No**
Is this web site storing information (cookies) on my computer?	**Yes**
Have I saved any passwords for this web site?	**No**

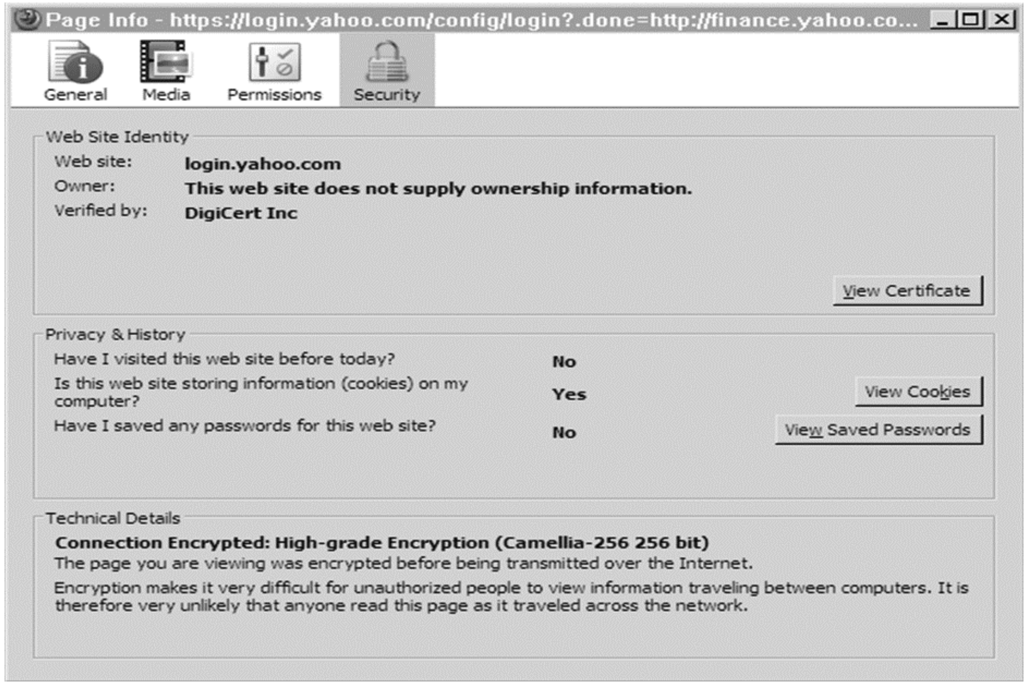
Technical Details

Connection Encrypted: High-grade Encryption (Camellia-256 256 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Session Established

- SSL session dialog includes the following:
  - Site that is verified
  - The certificate authority
  - The choice of encryption algorithm



Page Info - https://login.yahoo.com/config/login?.done=http://finance.yahoo.co...

Web Site Identity

Web site:	**login.yahoo.com**
Owner:	**This web site does not supply ownership information.**
Verified by:	**DigiCert Inc**

Privacy & History

Have I visited this web site before today?	**No**
Is this web site storing information (cookies) on my computer?	**Yes**
Have I saved any passwords for this web site?	**No**

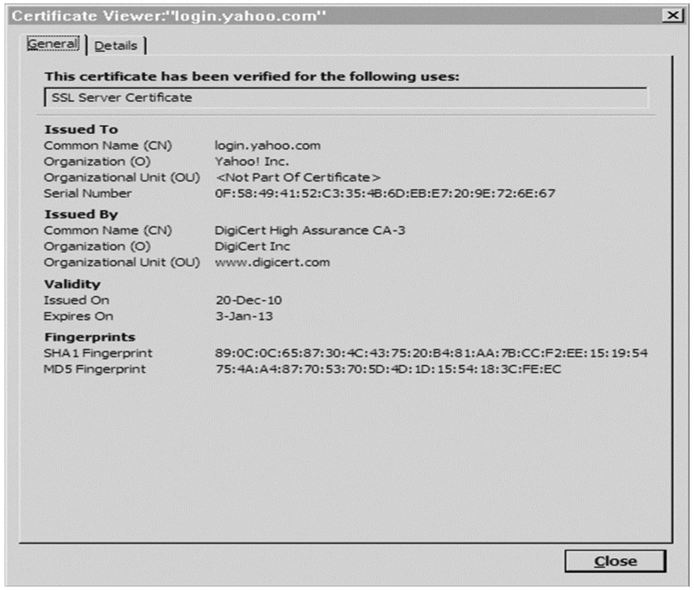
Technical Details

Connection Encrypted: High-grade Encryption (Camellia-256 256 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Certificate

- Certificate details:
  - The domain name being certified
  - The company that owns the site
  - The CA that issued the certificate
  - The relevant dates



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	login.yahoo.com
Organization (O)	Yahoo! Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0F:58:49:41:52:C3:35:4B:6D:EB:E7:20:9E:72:6E:67

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Validity

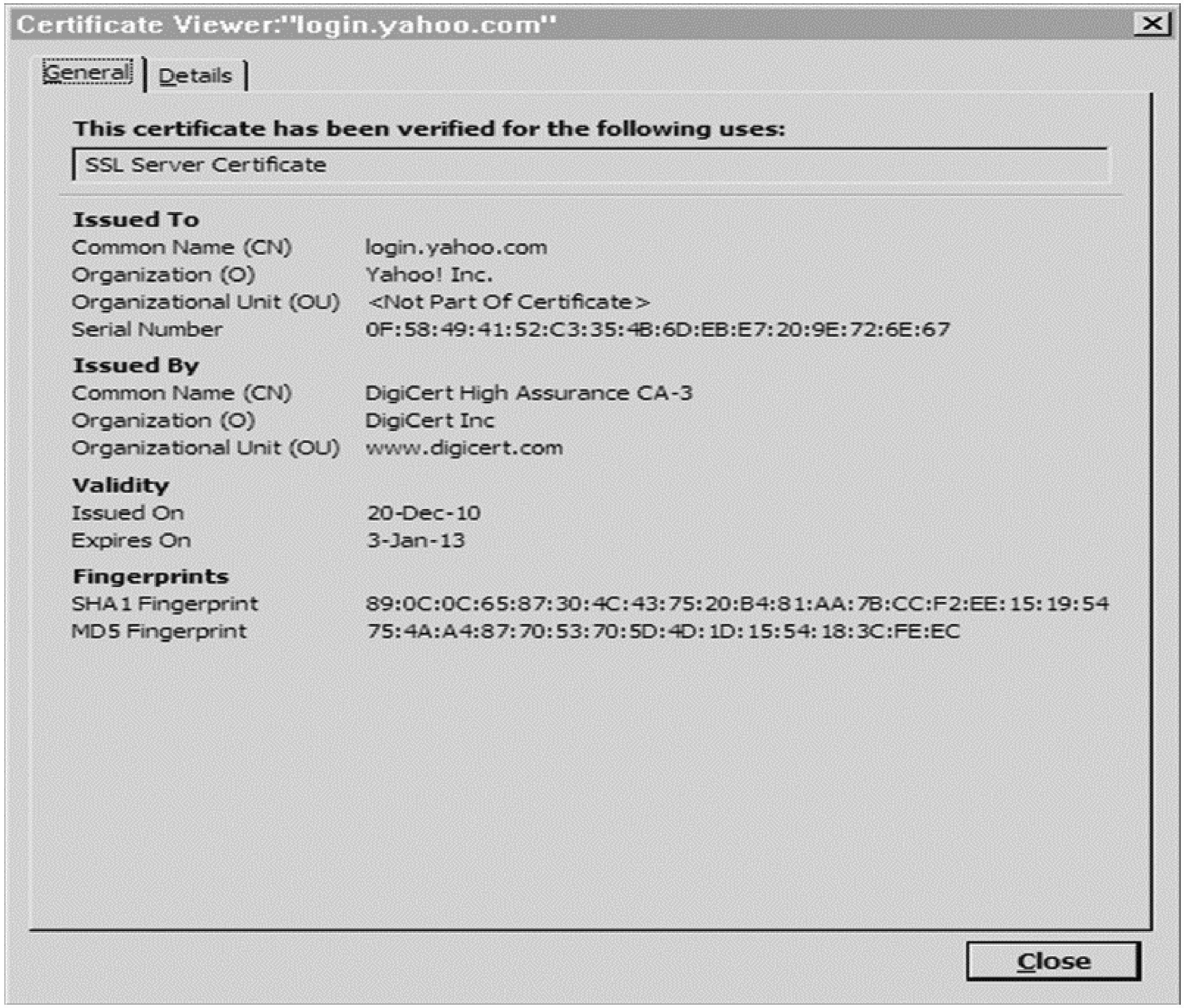
Issued On	20-Dec-10
Expires On	3-Jan-13

Fingerprints

SHA1 Fingerprint	89:0C:0C:65:87:30:4C:43:75:20:B4:81:AA:7B:CC:F2:EE:15:19:54
MD5 Fingerprint	75:4A:A4:87:70:53:70:5D:4D:1D:15:54:18:3C:FE:EC

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Certificate



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	login.yahoo.com
Organization (O)	Yahoo! Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0F:58:49:41:52:C3:35:4B:6D:EB:E7:20:9E:72:6E:67

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Validity

Issued On	20-Dec-10
Expires On	3-Jan-13

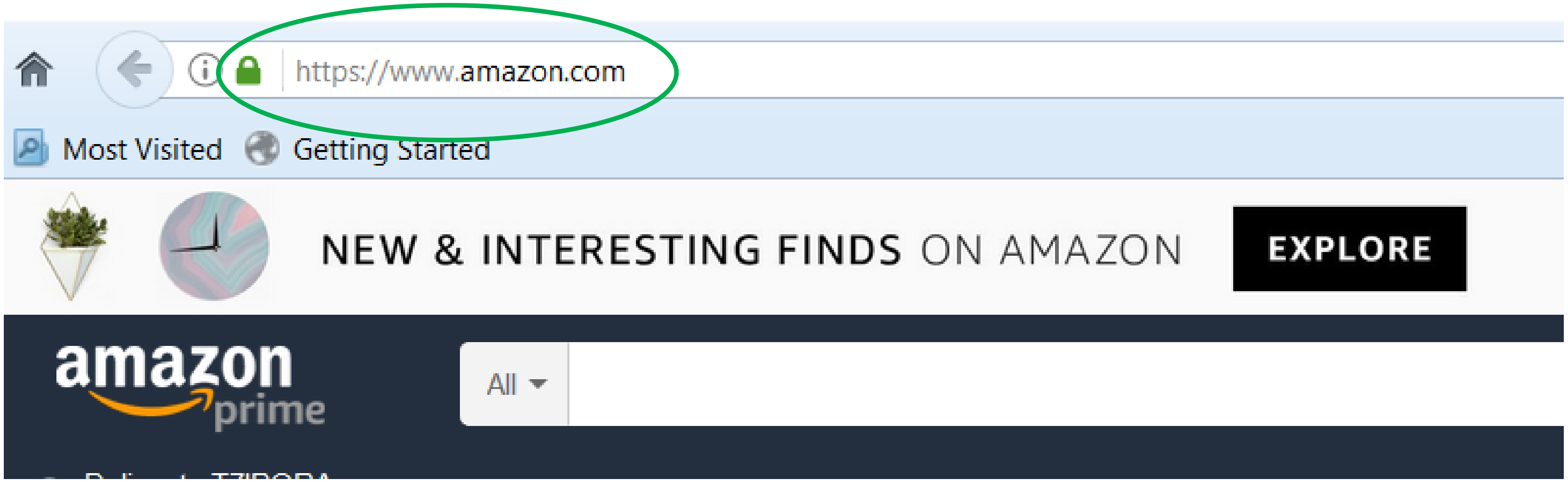
Fingerprints

SHA1 Fingerprint	89:0C:0C:65:87:30:4C:43:75:20:B4:81:AA:7B:CC:F2:EE:15:19:54
MD5 Fingerprint	75:4A:A4:87:70:53:70:5D:4D:1D:15:54:18:3C:FE:EC

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

TLS/SSL

- HTTPS (HTTP Secure) is an adaptation of HTTP for secure communication
  - In HTTPS, the communication protocol is encrypted by TLS



Onion Routing

- A technique for anonymous communication over a computer network
- Messages are encapsulated in layers of encryption, analogous to layers of an onion

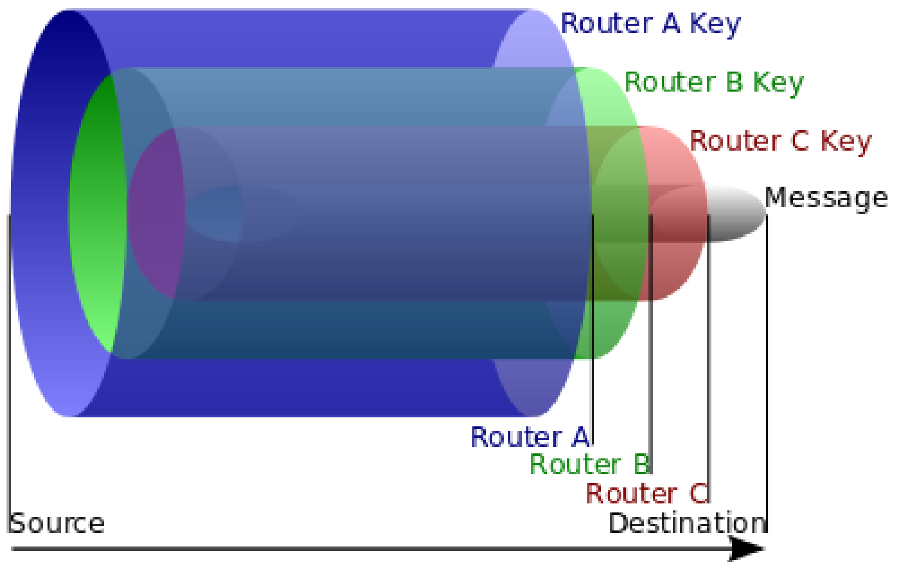
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing

- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network
- This is particularly helpful for evading authorities, such as when users in oppressive countries want to communicate freely with the outside world
- Uses asymmetric cryptography, as well as layers of intermediate hosts, so that
    - The intermediate host that sends the message to the ultimate destination cannot determine the original sender, and
    - The host that received the message from the original sender cannot determine the ultimate destination

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

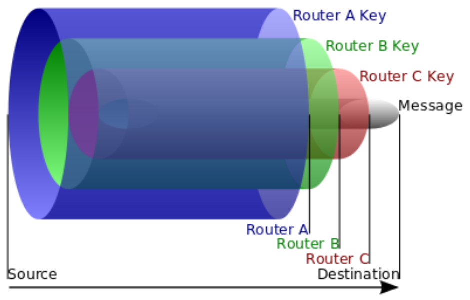
Onion Routing Example



https://en.wikipedia.org/wiki/Onion_routing

Onion Routing Example

- The source of the data sends the onion to Router A
- Router A removes a layer of encryption to learn only where to send it next and where it came from
  - Router A does not know if sender is the origin or just another node
- Router A sends it to Router B, which decrypts another layer to learn its next destination.
- Router B sends it to Router C, which removes the final layer of encryption
- Router C transmits the original message to its destination.



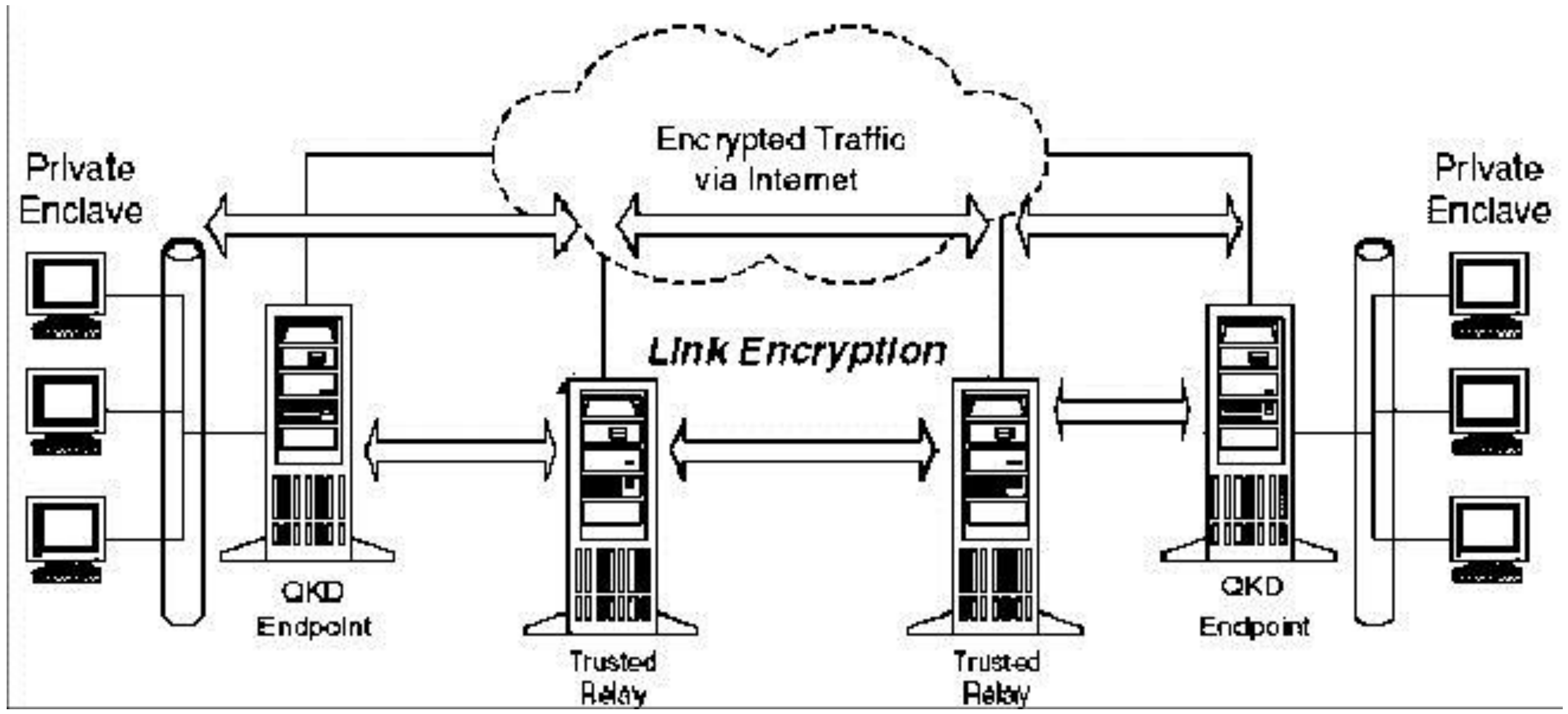
https://en.wikipedia.org/wiki/Onion_routing

Link Encryption

- In link encryption data packets are encrypted just before system places them on the physical communications link
- Data packets are decrypted just as they arrive at the destination system.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption



https://www.researchgate.net/figure/QKD-network-with-trusted-relays-and-link-encryption_fig2_51893133

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Virtual Private Networking (VPN)

- Link encryption can give a network's users the sense that they are on a private network, even when it is part of a public network.
- When applied at the link level, the encrypting and decrypting are invisible to users
- This approach is called a **virtual private network** (or **VPN**)

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

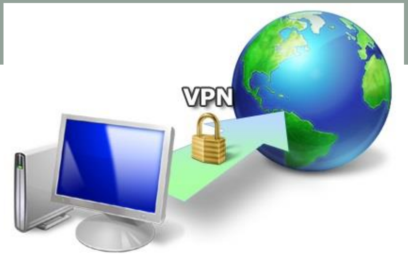
Virtual Private Networking (VPN)

- **Virtual private networking (VPN)** is a technology that allows private networks to be safely extended over long physical distances by making use of a public network, such as the Internet, as a means of transport.
- VPN provides guarantees of data confidentiality, integrity, and authentication, despite the use of an untrusted network for transmission.
- There are two primary types of VPNs, **remote access VPN** and **site-to-site VPN.**

https://www.techsupportalert.com/content/best-vpn-services.htm

Types of VPNs

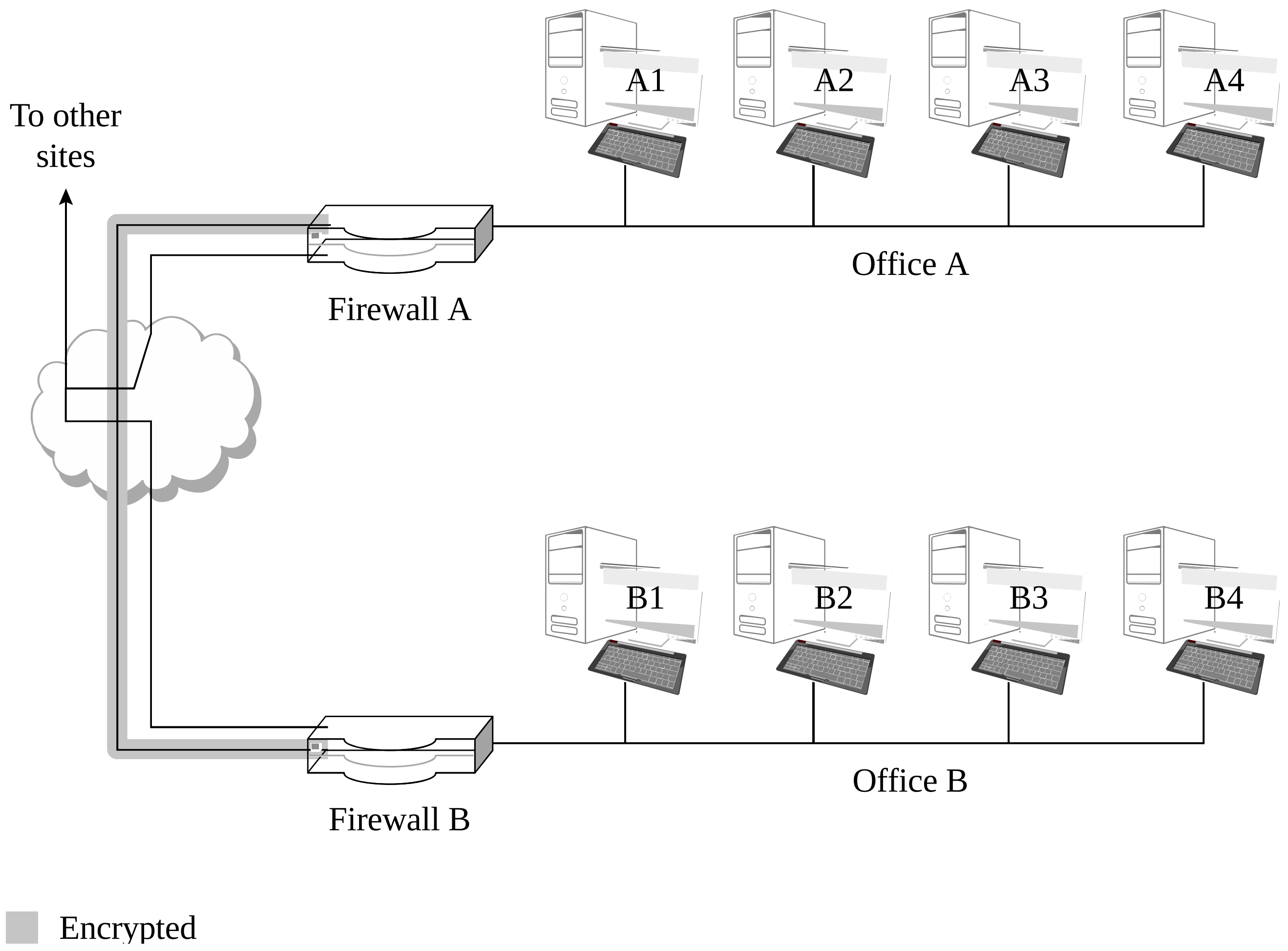
- **Remote access** VPNs allow authorized clients to access a private network that is referred to as an **intranet.**
  - For example, an organization may wish to allow employees access to the company network remotely but make it appear as though they are local to their system and even the Internet itself.
  - To accomplish this, the organization sets up a VPN endpoint, known as a **network access server, or NAS.** Clients typically install VPN client software on their machines, which handle negotiating a connection to the NAS and facilitating communication.



Types of VPNs

- **Site-to-site** VPN solutions are designed to provide a secure bridge between two or more physically distant networks.
  - Before VPN, organizations wishing to safely bridge their private networks purchased expensive leased lines to directly connect their intranets with cabling.

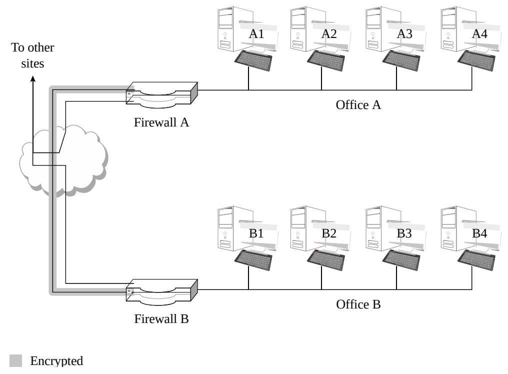
Virtual Private Networks (VPN) Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

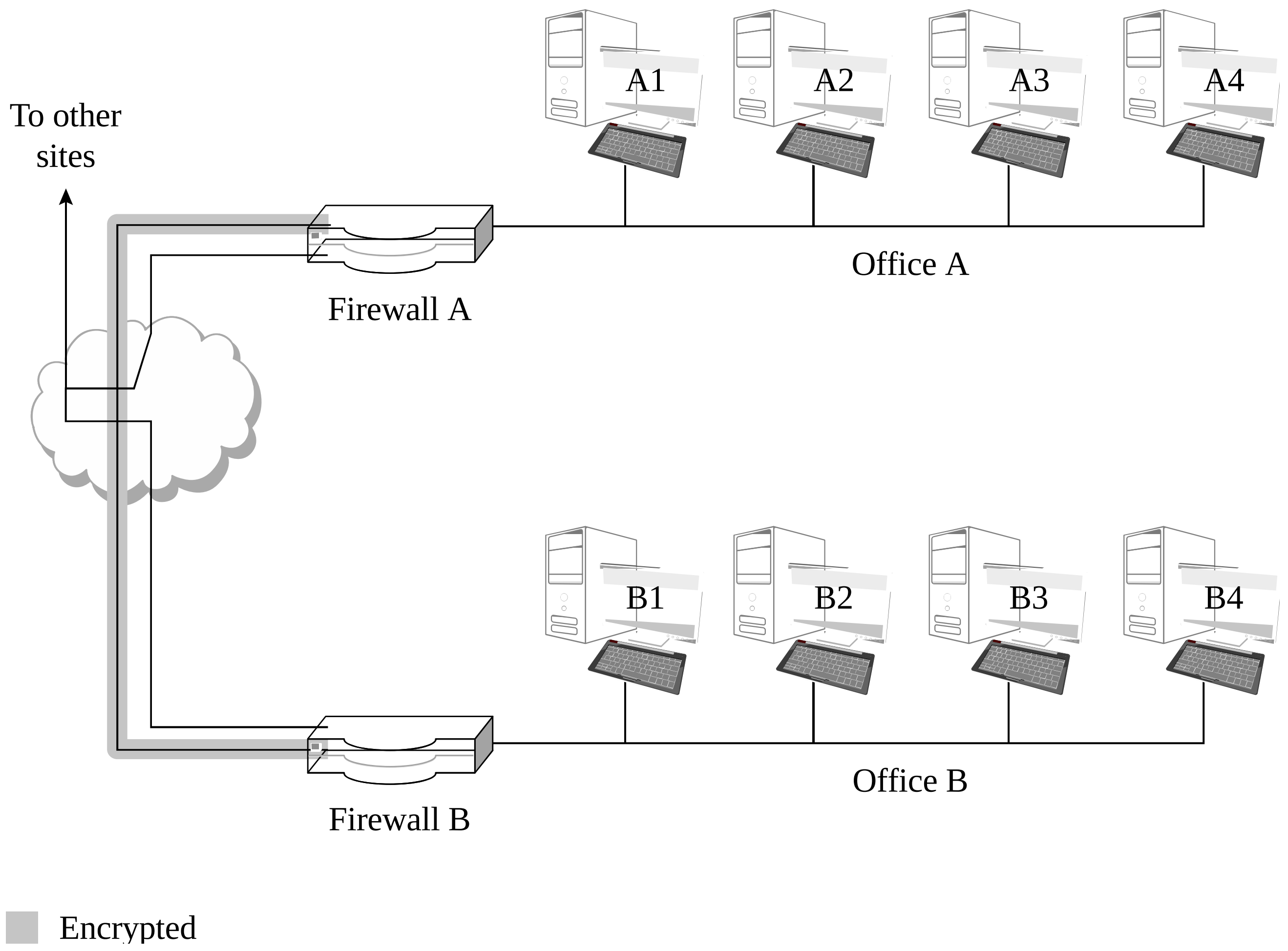
Virtual Private Networks (VPN) Example

- An encrypted tunnel provides confidentiality and integrity for communication between two sites
  - over public networks
- Connects Office A to Office B over the Internet so they appear to their users as one seamless, private network.
- The VPN is terminated by firewalls at both ends, which is often the case in the real world



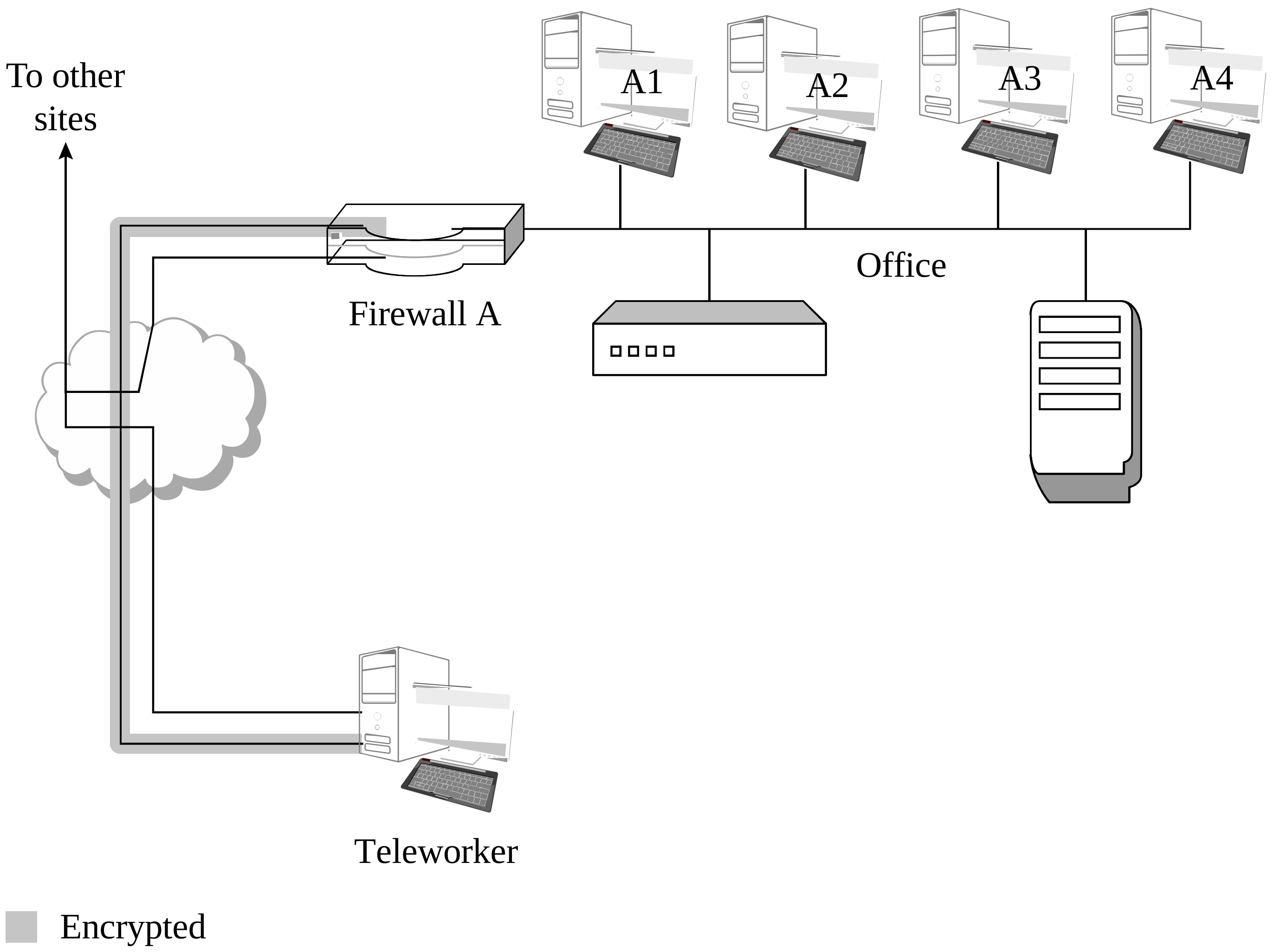
From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Virtual Private Networks (VPN) Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

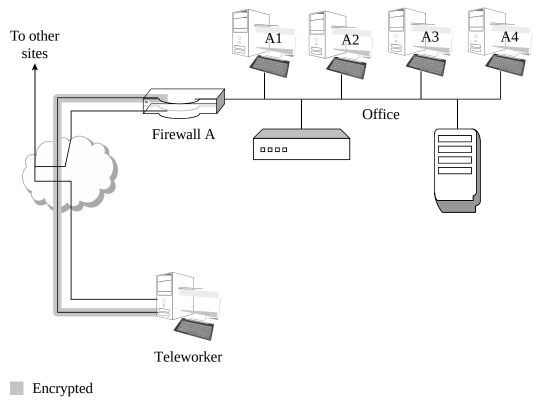
VPN (cont.) – Example 2



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

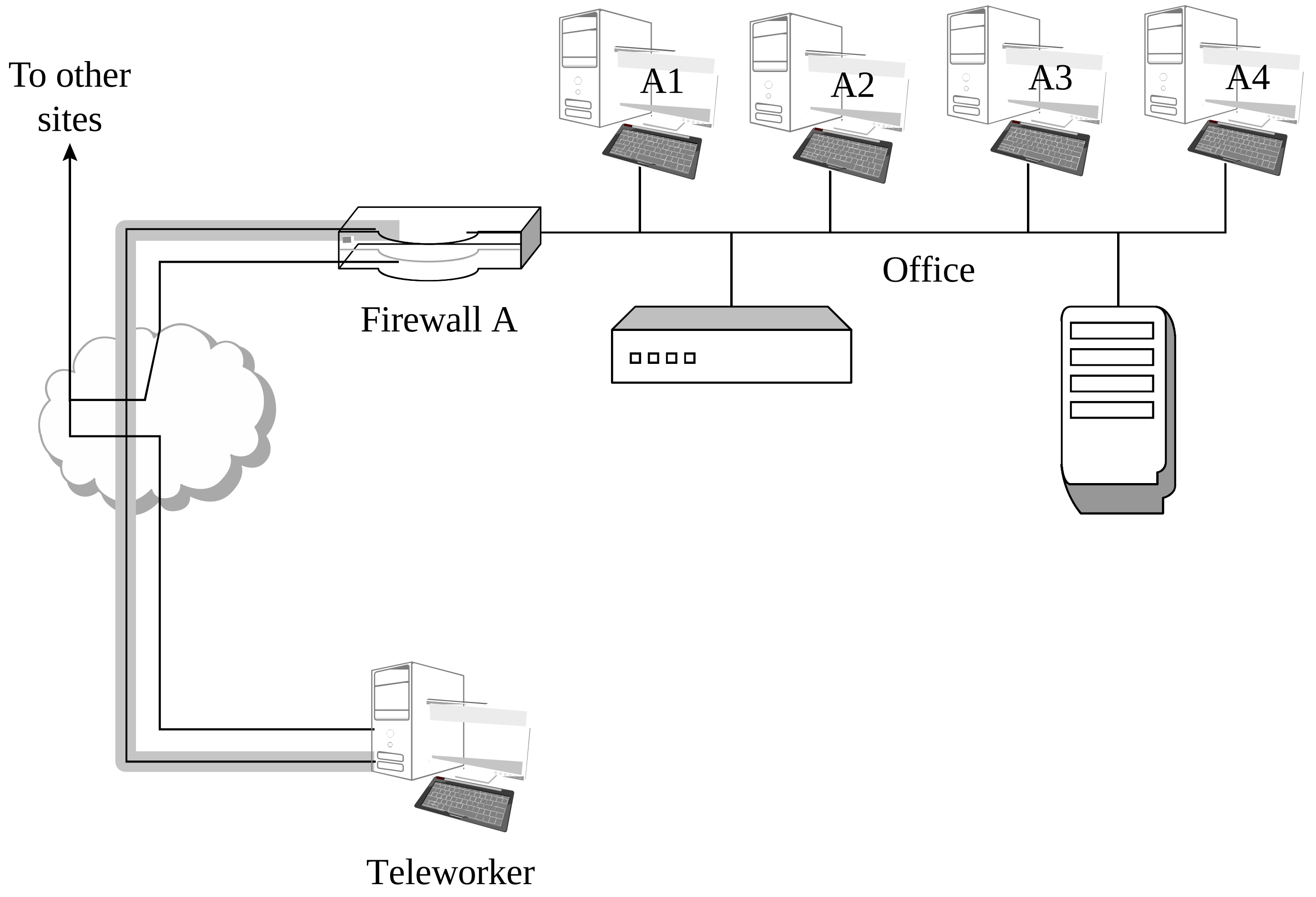
VPN (cont.) – Example 2

- A teleworker uses a VPN to connect to a remote office.
- The teleworker authenticates to the firewall
  - The firewall is acting as a VPN server
- The firewall passes that authentication information to the servers in the office
  - so teleworker can be appropriately access controlled data



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

VPN (cont.) – Example 2



▨ Encrypted

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

FIREWALLS

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

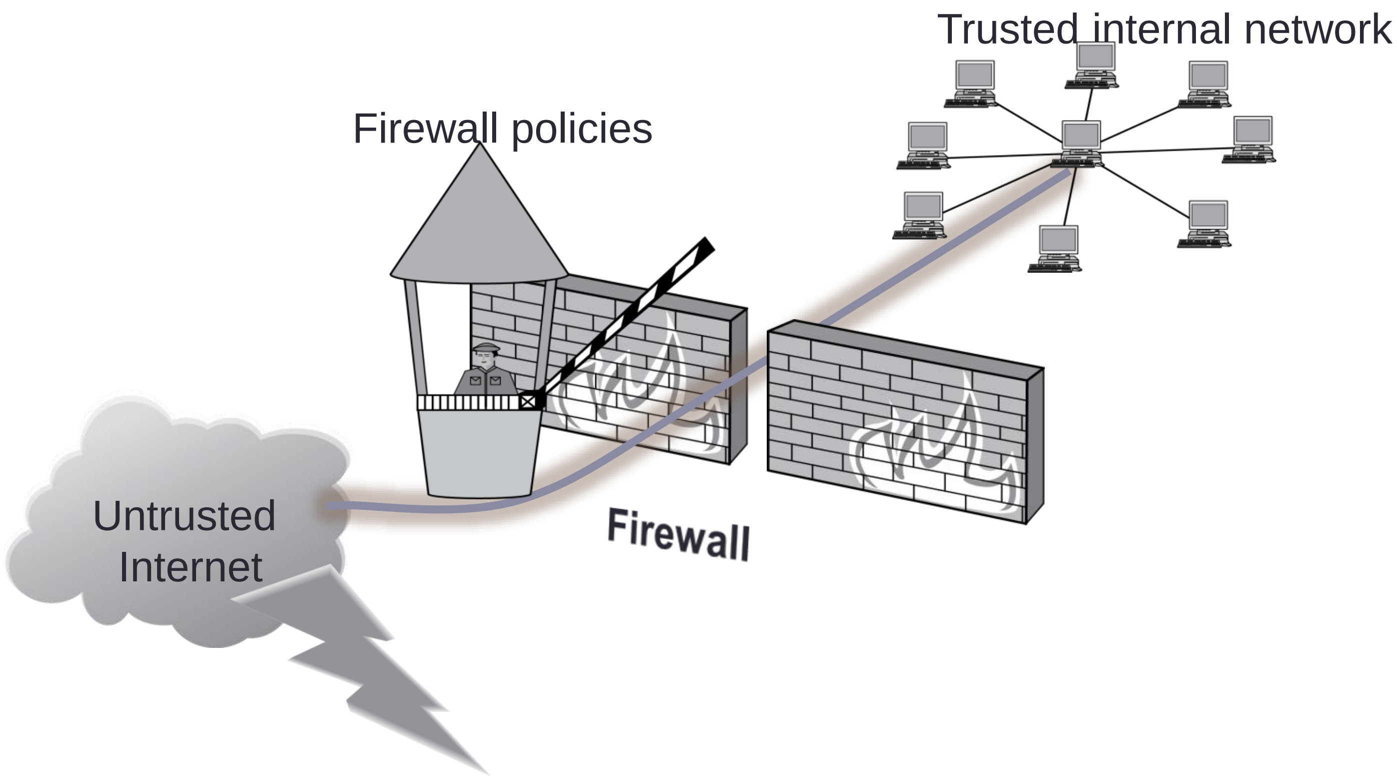
Firewalls

- A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.

Private Network
Public Network

Firewall Policies

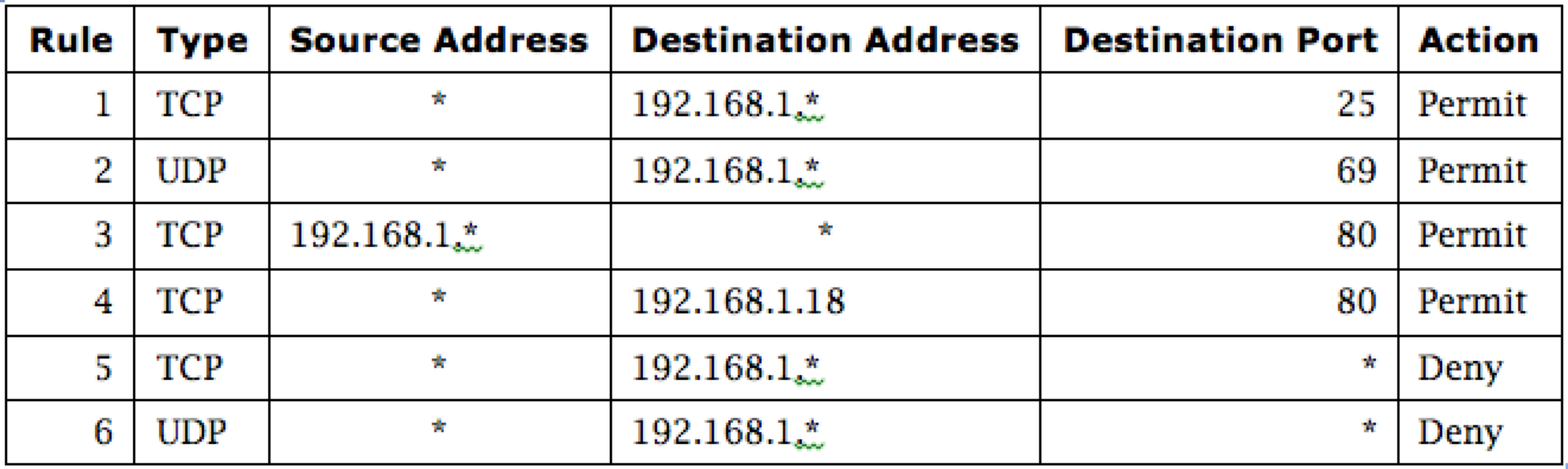
- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
  - **Accepted:** permitted through the firewall
  - **Dropped:** not allowed through with no indication of failure
  - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
  - TCP or UDP
  - the source and destination IP addresses
  - the source and destination ports
  - the application-level payload of the packet (e.g., whether it contains a virus).

Firewall Security Policy Example



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

- External traffic can reach the entire internal network on TCP/25 and UDP/69.
- Internal traffic can go out to port 80 on the external network.
- External traffic can reach TCP/80 on one internal server.
- All other traffic from external to internal is disallowed

From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Blacklists and White Lists

- There are two fundamental approaches to creating firewall policies (or rulesets) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network (or individual computer): **Blacklisting** and **Whitelisting**

https://it.sheridancollege.ca/news/what-the-tech-spring14/blacklisting.html
http://www.free-icons-download.net/whitelist-file-icon-70105/

Blacklists and White Lists

- **Blacklist** approach
  - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
  - This type of configuration is more flexible in ensuring that service to the internal network is not disrupted by the firewall, but is naïve from a security perspective in that it assumes the network administrator can enumerate all of the properties of malicious traffic.
- **Whitelist** approach
  - A safer approach to defining a firewall ruleset is the default-deny policy, in which packets are dropped or rejected unless thev are specifically allowed by the firewall.

Types of Firewalls

- Packet filtering (stateless) gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

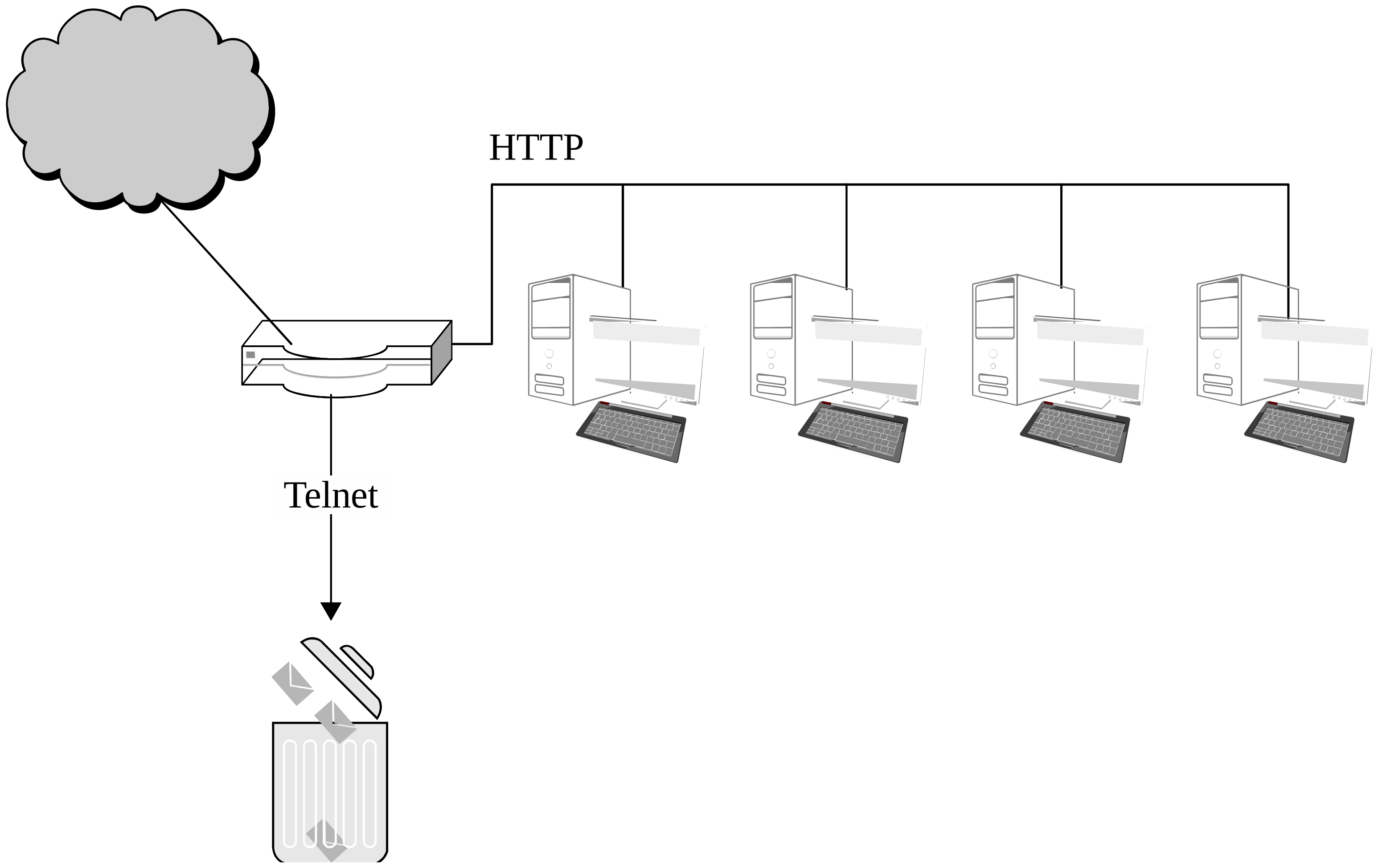
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet-Filtering Gateways

- A packet-filtering gateway controls access on the basis of packet address and specific transport protocol type
  - e.g., HTTP traffic.
- If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- Packet-filtering gateways maintain no state from one packet to the next
  - They simply look at each packet’s IP addresses and ports and compare them to the configured policies

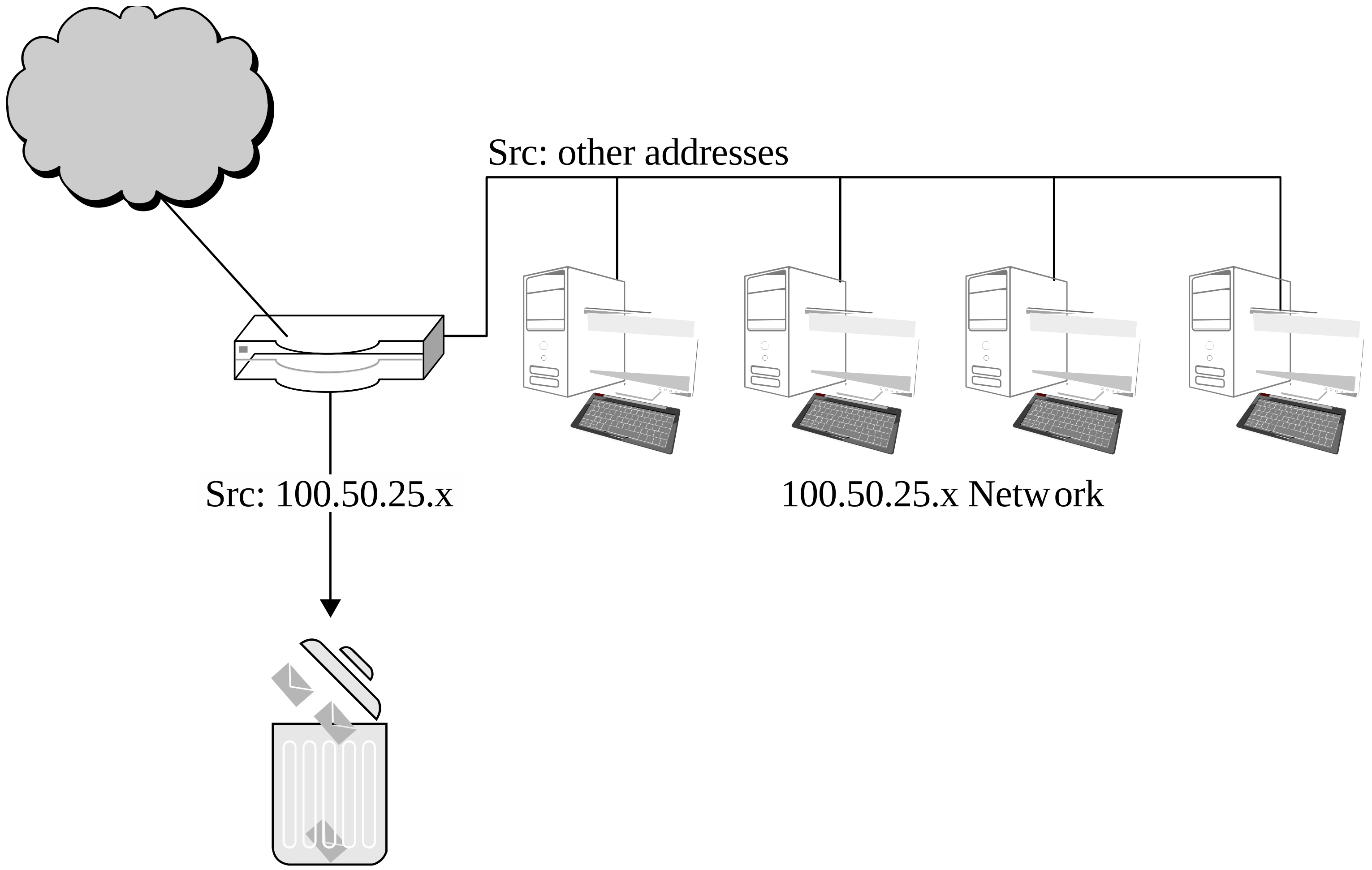
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet-Filtering Gateways



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

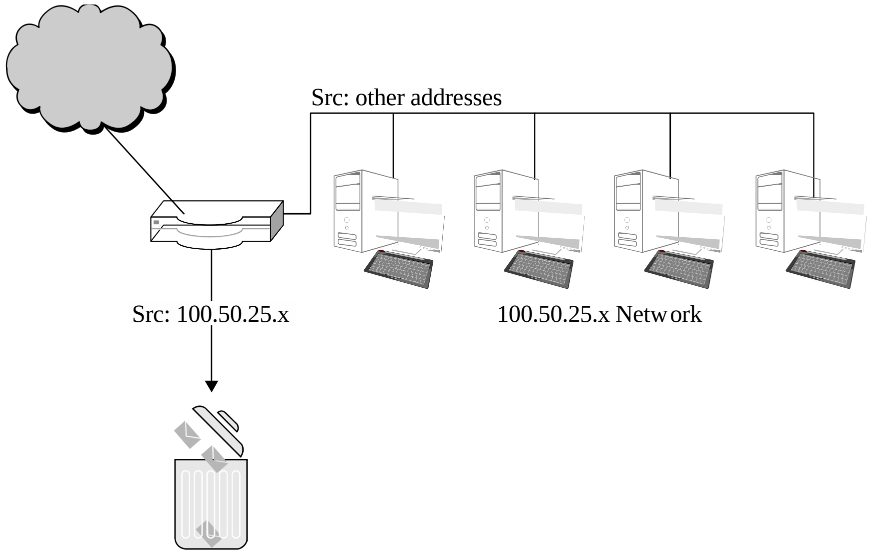
Packet-Filtering Gateways Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet-Filtering Gateways - Example

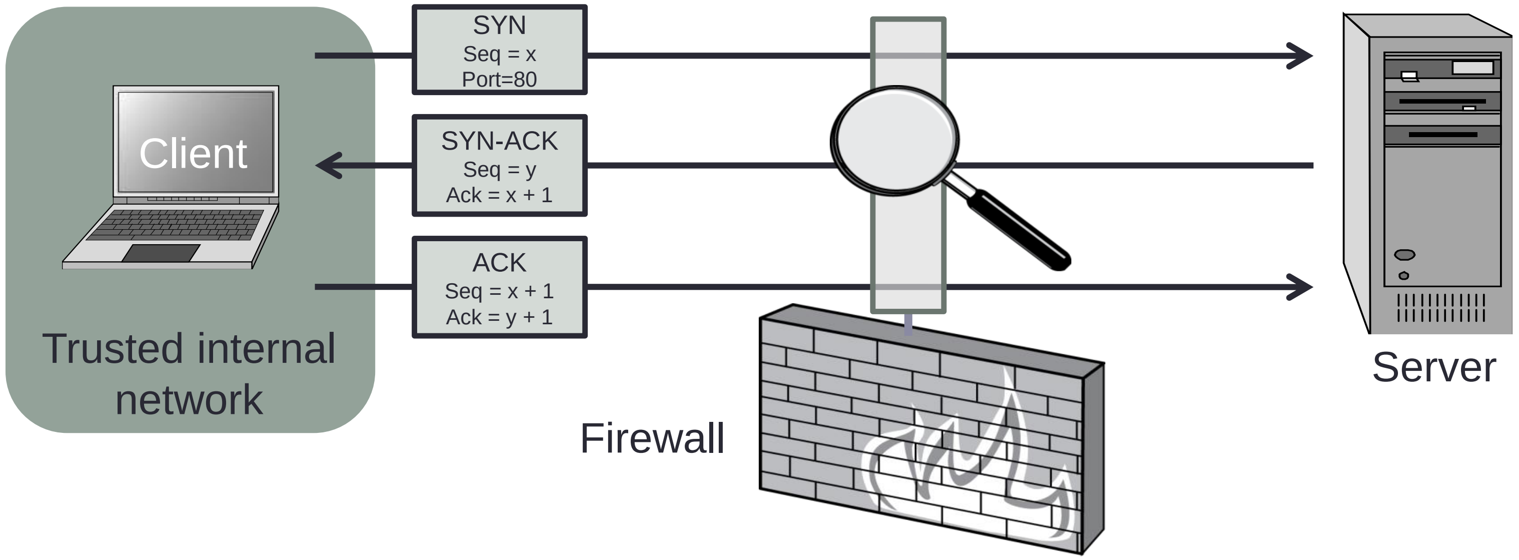
- Here, firewall is filtering traffic on the basis of source IP
  - rather than port.
- Filtering rules can also be based on combinations of addresses and ports/protocols



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet-Filtering (Stateless) Gateways

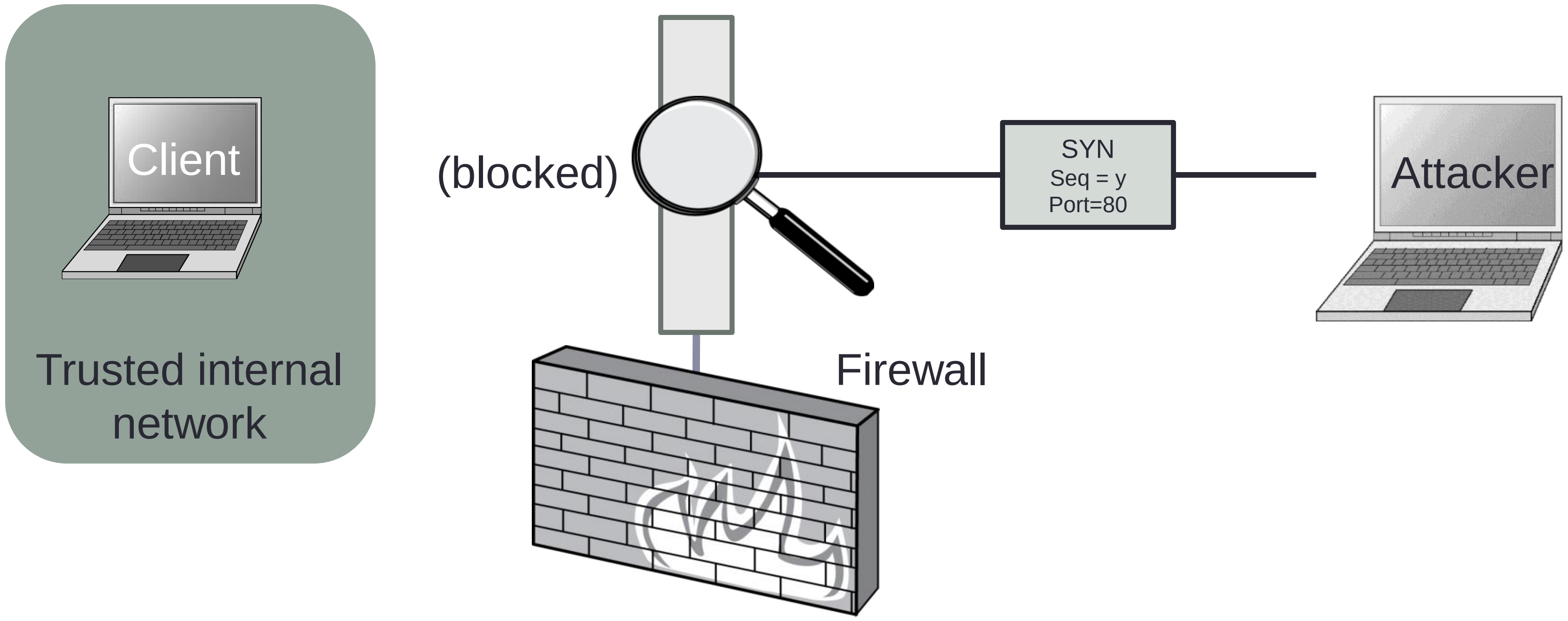
- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Stateful Inspection Firewall

- Stateful inspection firewalls maintain state information from one packet to the next
  - In contrast to packet-filtering gateways
- It maintains records of all connections passing through it
- Can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.

From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

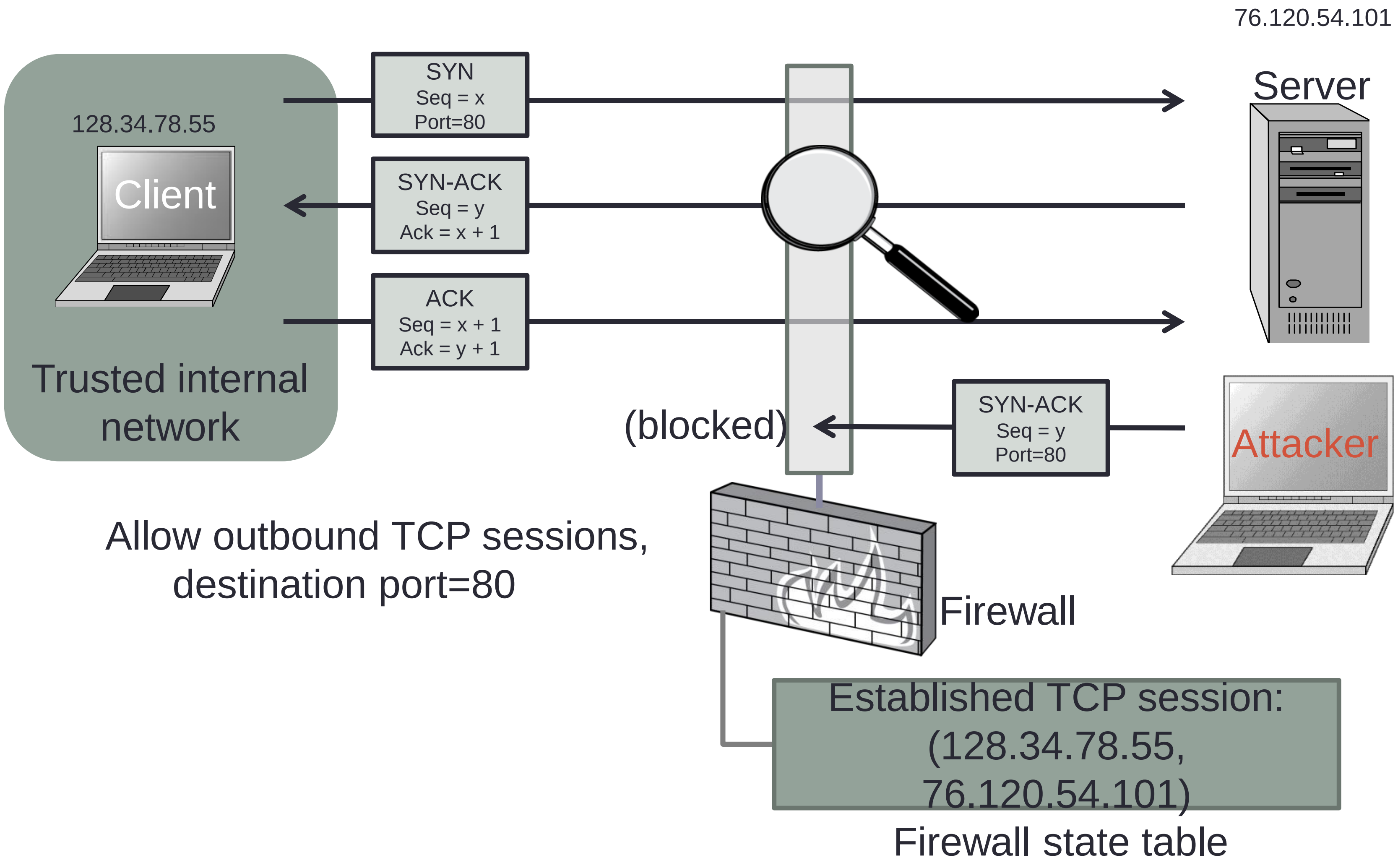
Statefull Firewalls

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

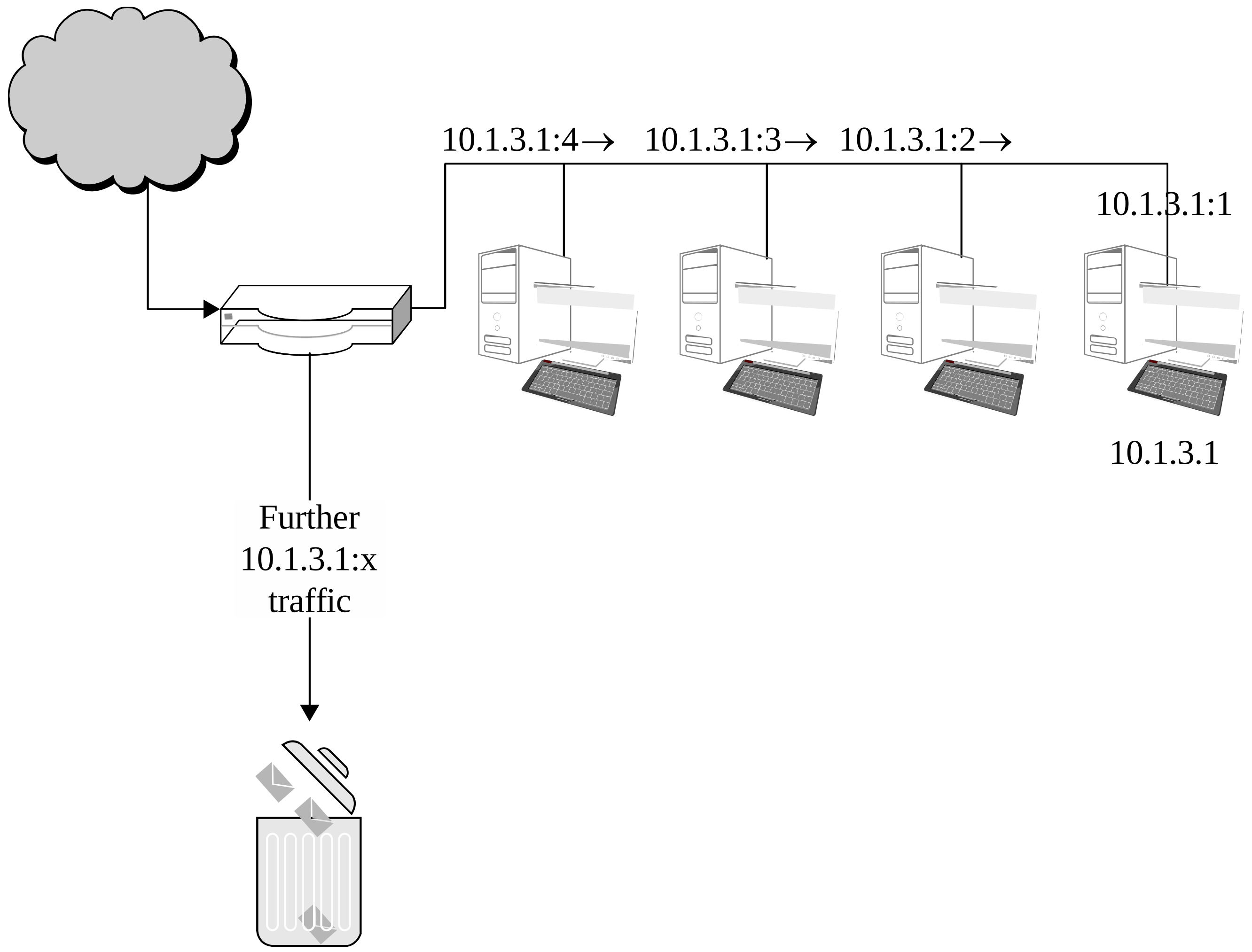
https://www.deciso.com/opnsense-tour/stateful-inspection-firewall/

Statefull Firewall Example

- Allow only requested TCP connections:



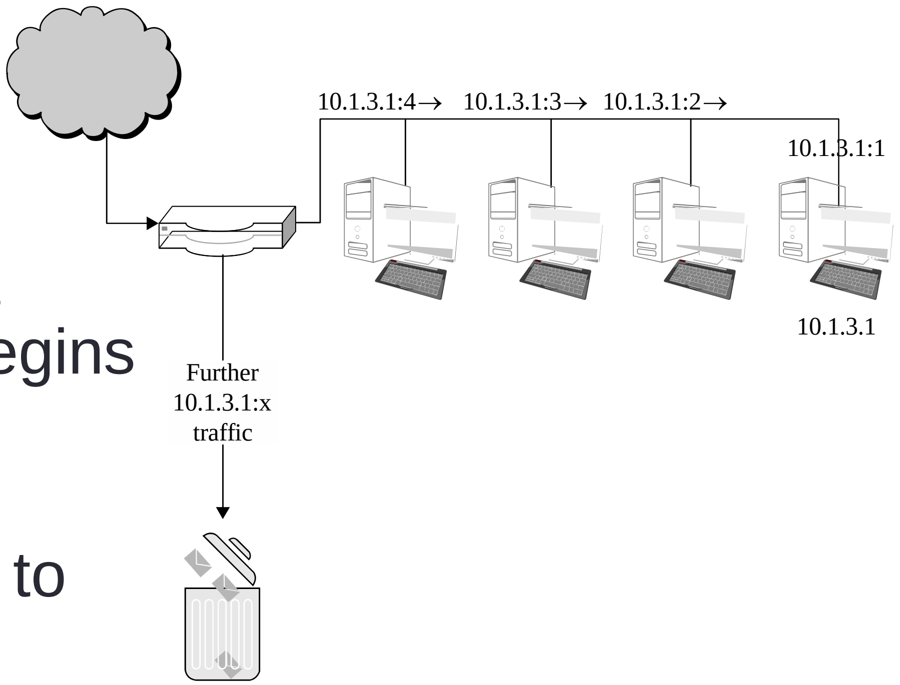
Stateful Inspection Firewall Example



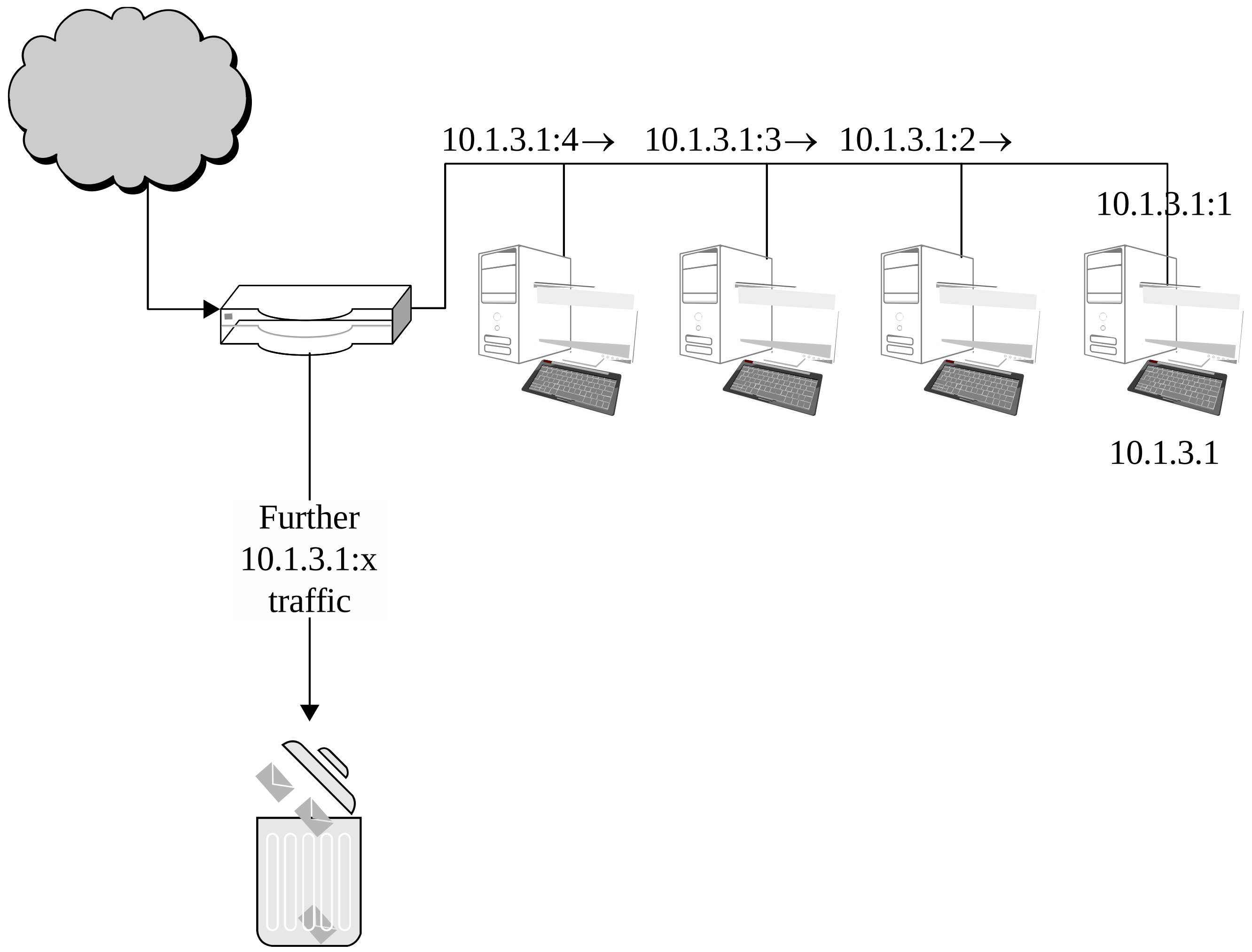
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Stateful Inspection Firewall Example

- Firewall is counting the number of systems coming from external IP 10.1.3.1
- After the external system reaches out to a fourth computer, the firewall hits a configured threshold and begins filtering packets from that address.
- In real life, it can be difficult to define rules that require state/context and that attackers cannot circumvent



Stateful Inspection Firewall Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Application Layer Firewall

- Application layer firewall works like a **proxy**
  - can “understand” certain applications and protocols.
- It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

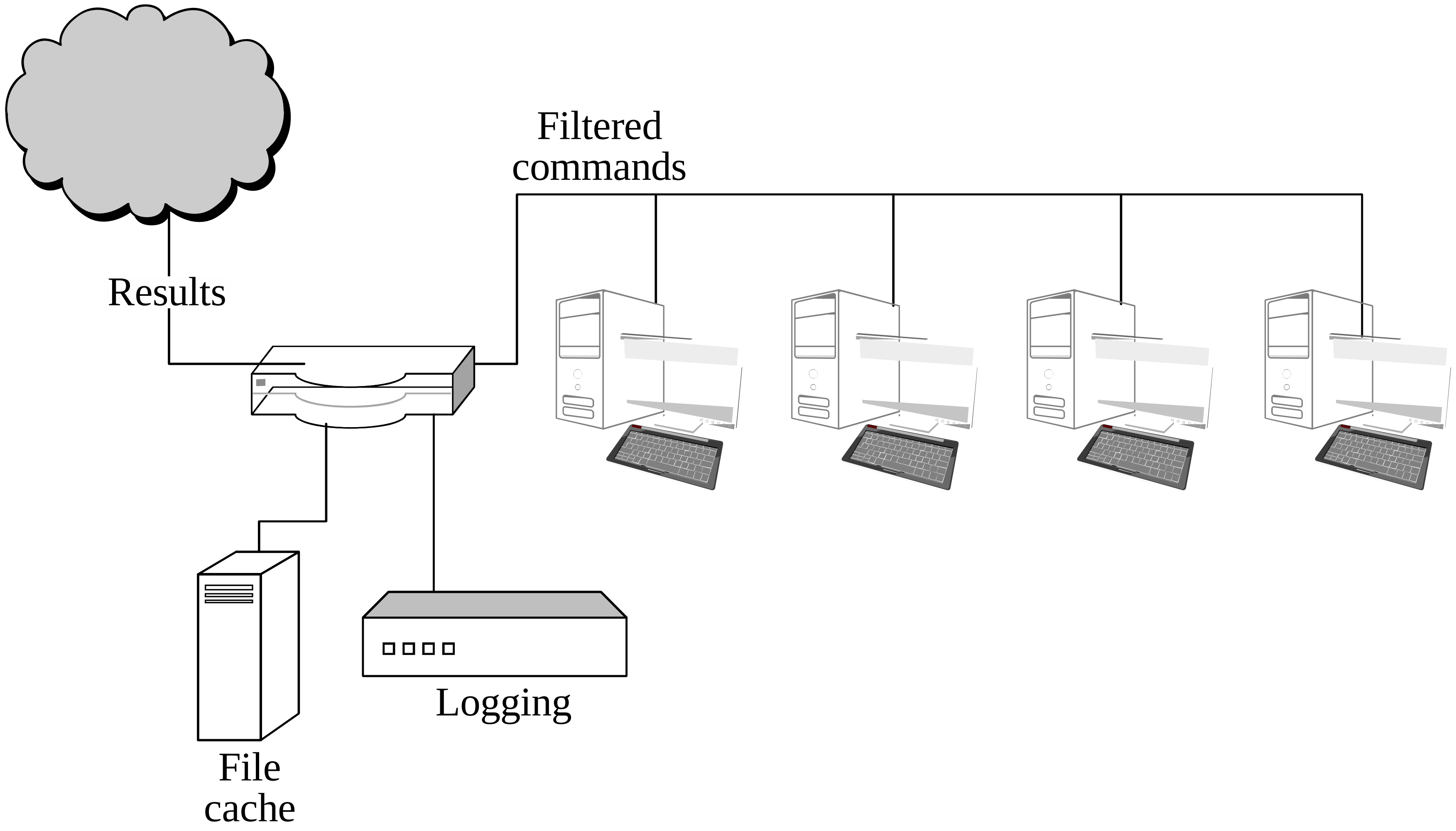
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Application Proxy Firewall

- An application proxy simulates the behavior of an application at OSI layer 7 so that the real application receives only requests to act properly
- Application proxies can serve a number of purposes:
  - Filtering potentially dangerous application-layer requests
  - Log requests/accesses
  - Cache results to save bandwidth
- For example, web proxy is used by companies often to monitor and filter employee internet use

From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Application Proxy



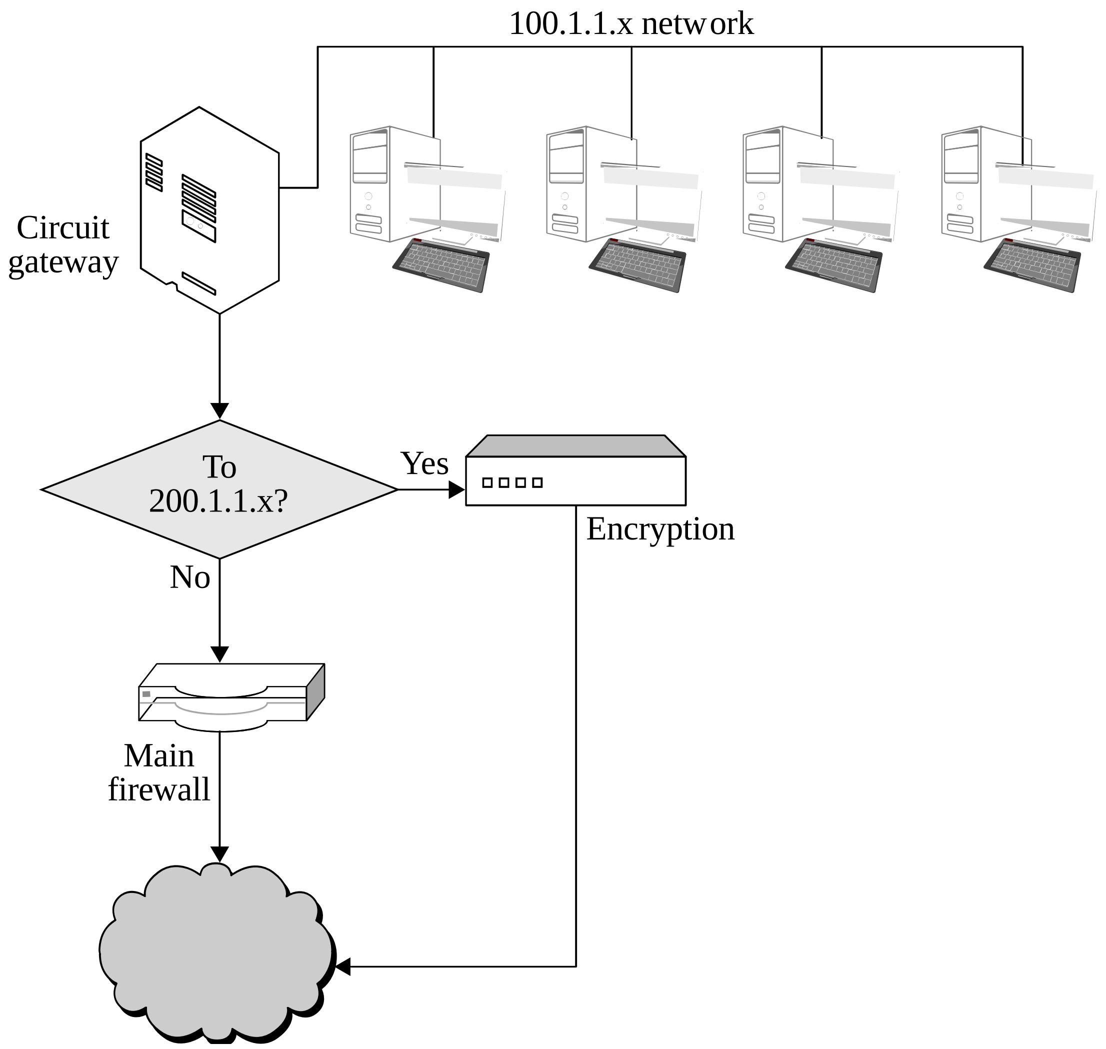
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Circuit-Level Gateway

- A firewall that essentially allows one network to be an extension of another.
- Operates at OSI layer 5, the session layer
- Functions as a virtual gateway between two networks
- One use of a circuit-level gateway is to implement a VPN

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Circuit-Level Gateway



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Guard

- A sophisticated firewall that, like an application proxy, can interpret data at the protocol level and respond
- The distinction between a guard and an application proxy can be fuzzy; the more protection features an application proxy implements, the more it becomes like a guard
- Guards may implement any programmable set of rules; for example:
  - Limit the number of email messages a user can receive
  - Limit users' web bandwidth
  - Filter documents containing the word "Secret"
  - Pass downloaded files through a virus scanner

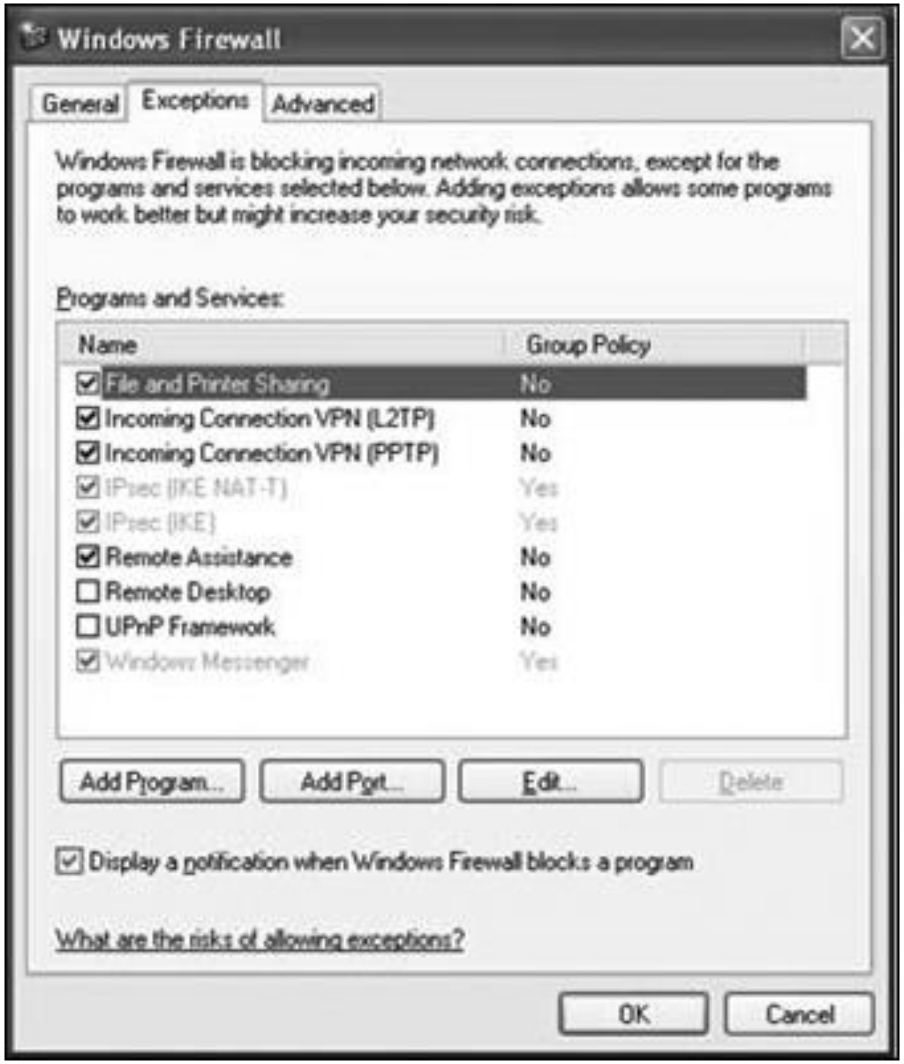
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Personal Firewalls

- A personal firewall runs on a workstation or server and can enforce security policy like other firewalls.
- Restricts traffic by source IP and destination por
- Can also restrict which applications are allowed to use the network.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Personal Firewalls



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name	Group Policy
☑ File and Printer Sharing	No
☑ Incoming Connection VPN (L2TP)	No
☑ Incoming Connection VPN (PPTP)	No
☑ IPsec (IKE NAT-T)	Yes
☑ IPsec (IKE)	Yes
☑ Remote Assistance	No
☐ Remote Desktop	No
☐ UPnP Framework	No
☑ Windows Messenger	Yes

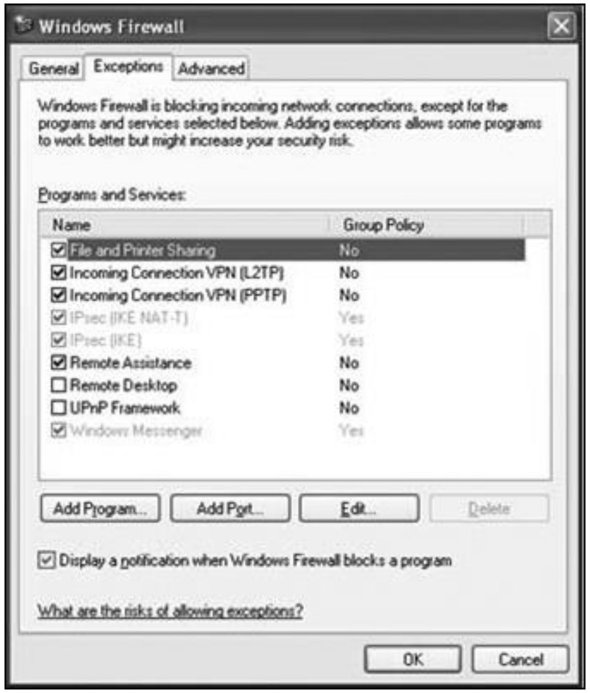
☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Personal Firewalls

- In this example Windows firewall configuration dialog, an administrator can select which protocols and applications should be allowed to communicate to and from the host



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name	Group Policy
☑ File and Printer Sharing	No
☑ Incoming Connection VPN (L2TP)	No
☑ Incoming Connection VPN (PPTP)	No
☑ IPsec (IKE NAT-T)	Yes
☑ IPsec (IKE)	Yes
☑ Remote Assistance	No
☐ Remote Desktop	No
☐ UPnP Framework	No
☑ Windows Messenger	Yes

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

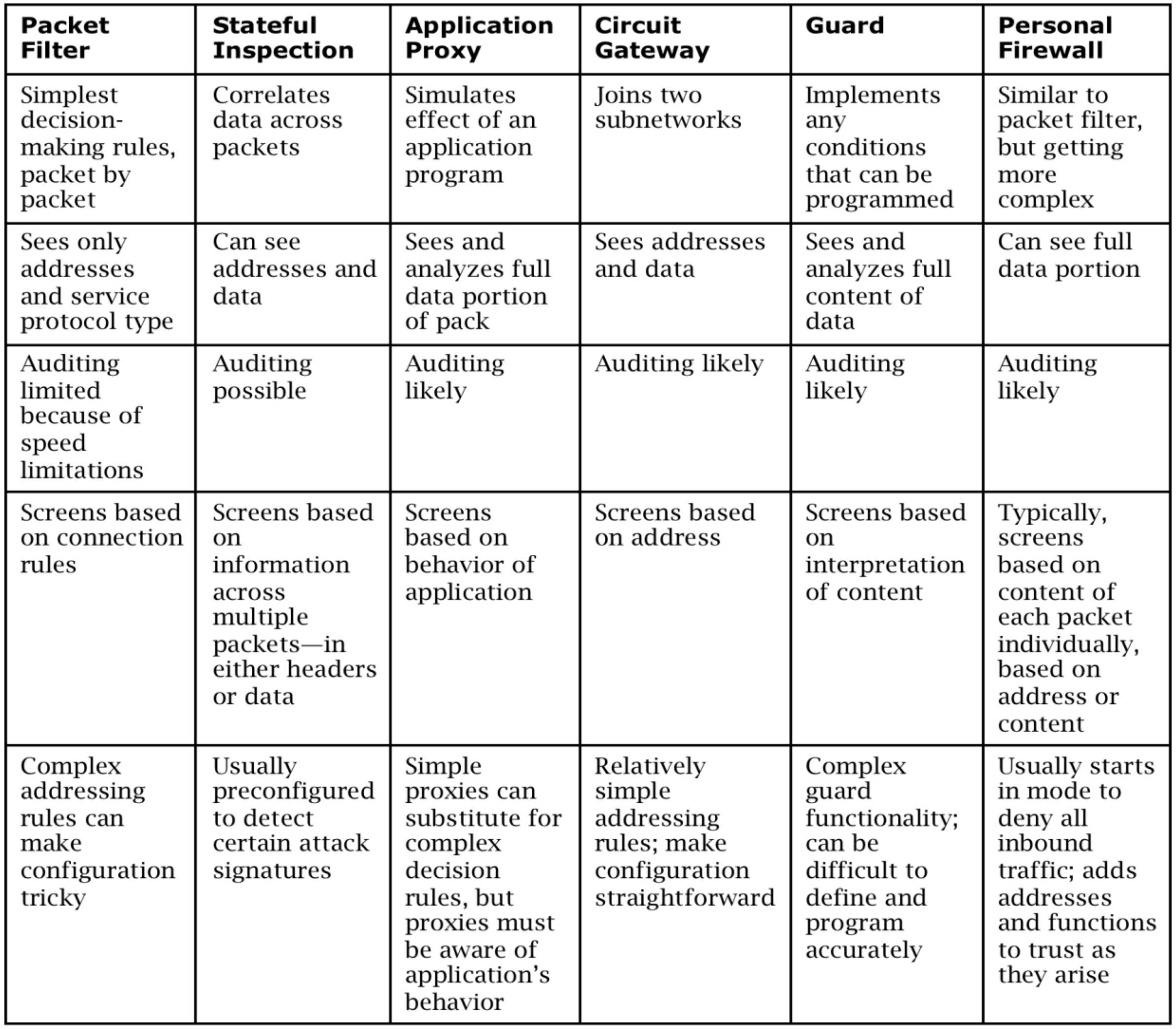
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Firewalls - summary

- A device that filters all traffic between a protected or "inside" network and less trustworthy or "outside" network
- Most firewalls run as dedicated devices
  - Easier to design correctly and inspect for bugs
  - Easier to optimize for performance
- Firewalls implement security policies, or set of rules that determine what traffic can or cannot pass through
- A firewall is an example of a reference monitor, which means it should have three characteristics:
  - Always invoked (cannot be circumvented)
  - Tamperproof
  - Small and simple enough for rigorous analysis

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

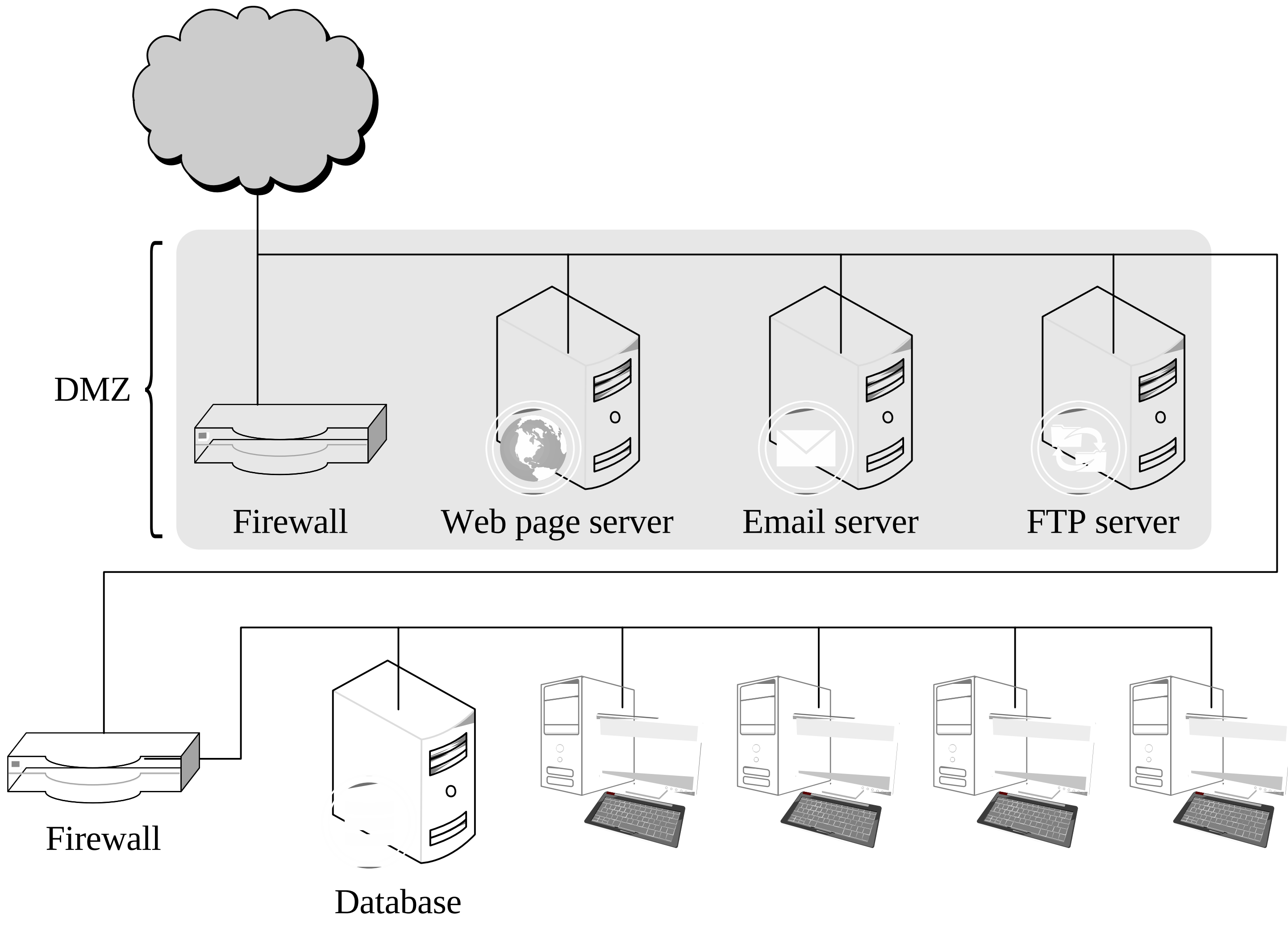
Comparison of Firewall Types



Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Demilitarized Zone (DMZ)



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

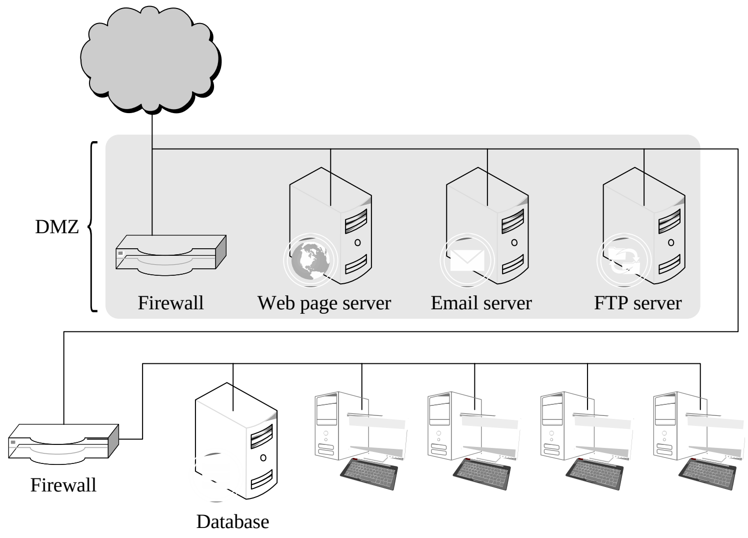
Demilitarized Zone (DMZ)

- A form of network architecture in which a network enclave is dedicated to services that should be somewhat accessible from the outside.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

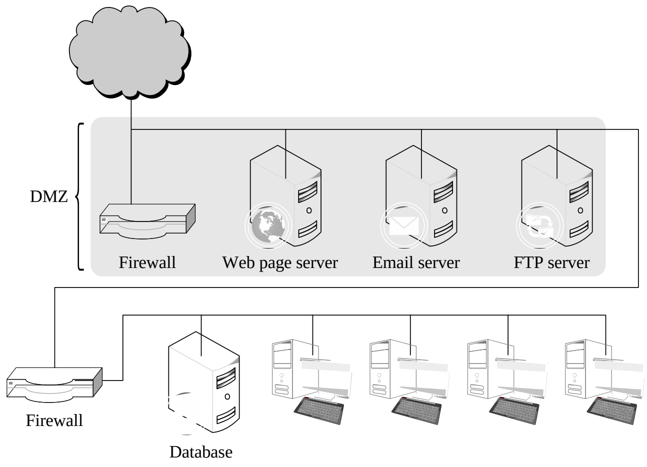
Demilitarized Zone (DMZ) Example

- A firewall protects a DMZ that contains web, email, and FTP servers
- A second firewall protects an internal network—that should not be reachable from the Internet—from the DMZ
  - in case a DMZ host becomes compromised.



Demilitarized Zone (DMZ) Example

- The hosts that need to be accessible from the Internet—and are therefore most at risk from outside attack—can only do limited damage
  - to internal hosts that do not need to be reachable from the Internet.
- An even more careful option would separate the web, email, and FTP servers from one another
  - with further firewalls



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

What Firewalls Can and Cannot Do

- Firewalls can protect an environment only if they control the entire perimeter
- Firewalls do not protect data outside the perimeter
- Firewalls are the most visible part of an installation to the outside, so they are an attractive target for attack
- Firewalls must be correctly configured, that configuration must be updated as the environment changes, and firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion
- Firewalls exercise only minor control over the content admitted to the inside, meaning that inaccurate or malicious code must be controlled by means inside the perimeter

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Network Address Translation (NAT)

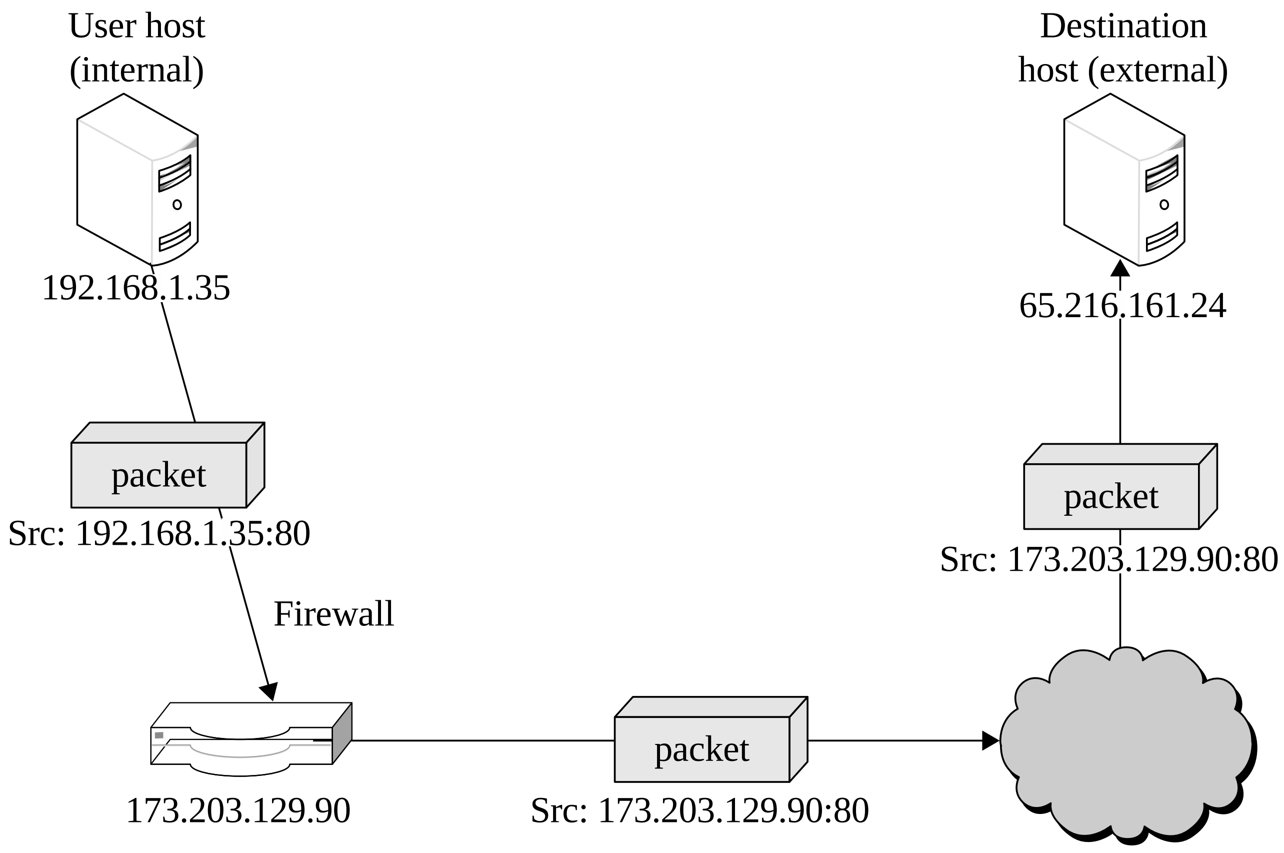


Table of translations performed	
Source	Dest
192.168.1.35:80	65.216.161.24:80

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Network Address Translation (NAT)

- With NAT, the source firewall converts the source address in the packet into the firewall's own address.
- The firewall also makes an entry in a translation table showing the destination address, the source port, and the original source address
  - to be able to forward any replies to the original source address.
- The firewall then converts the address back on any return packets
  - This has the effect of concealing the true address of the internal host and prevents the internal host from being reached directly

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Data Loss Prevention (DLP)

- DLP is a set of technologies that can detect and possibly prevent attempts to send sensitive data where it is not allowed to go
- Can be implemented as
  - Agent installed as an OS rootkit
  - Guard
- Indicators DLP looks for:
  - Keywords
  - Traffic patterns
  - Encoding/encryption
- DLP is best for preventing accidental incidents, as malicious users will often find ways to circumvent it

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved
https://blogs.quickheal.com/guide-data-leakage-data-loss-prevention-dlp-tools-help/.

Intrusion Detection Systems

- Intrusion
  - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing/networking resources)

https://gbhackers.com/intrusion-detection-system-ids-2/

Intrusion Detection System

- Security controls we covered so far:
  - Perimeter controls, firewall, and authentication and access controls
  - Block certain actions
  - Most of these controls are preventive
    - They block known bad things from happening
- After using those controls, some users are admitted to use a computing system
- Studies show that most computer security incidents are caused by insiders or people impersonating them
  - people who would not be blocked by a firewall

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Intrusion Detection System

- Insiders require access with significant privileges to do their daily jobs
- Harm from insiders may not be malicious
  - it is honest people making honest mistakes
- However, potential malicious outsiders who have somehow passed the screens of firewalls and access controls exist
- Prevention, although necessary, is not a complete computer security control
  - Detection during an incident copes with harm that cannot be prevented in advance

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

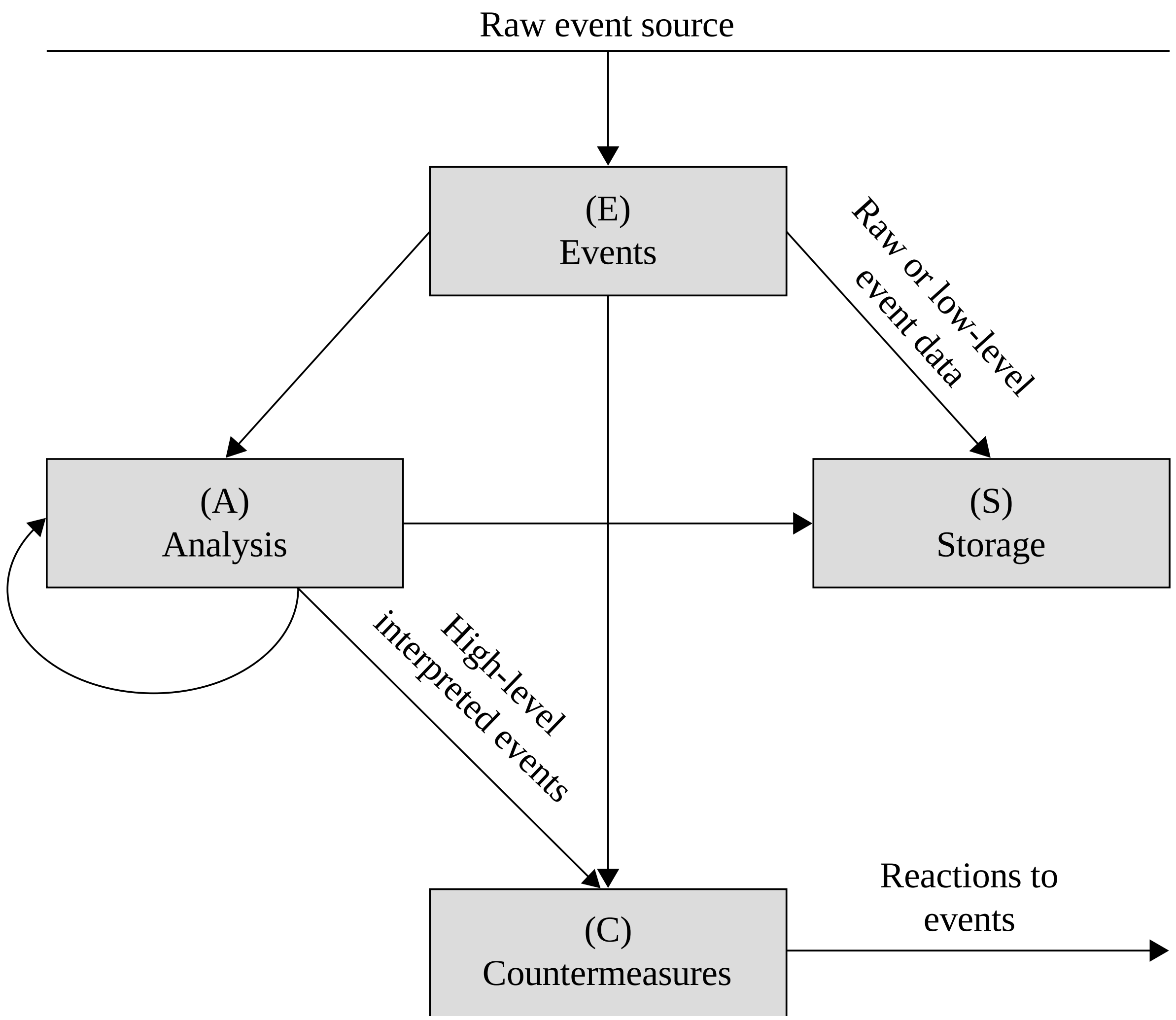
Intrusion Detection Systems

- Intrusion detection
  - The identification through intrusion signatures and report of intrusion activities
- Intrusion prevention
  - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

IPS
INTRUSION PREVENTION SYSTEM
Detect irregular traffic and prevent intrusions before costly damage occurs

http://www.stonesoft-security.co.uk/product/stonesoft-intrusion-prevention-system/

Intrusion Detection Systems (IDS)



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Intrusion Detection Systems (IDS)

- IDSs complement preventative controls as a next line of defense. IDSs monitor activity to identify malicious or suspicious events.
- IDSs may:
  - Monitor user and system activity
  - Audit system configurations for vulnerabilities and misconfigurations
  - Assess integrity of critical system and data files
  - Recognize known attack patterns in system activity
  - Identify abnormal activity through statistical analysis
  - Manage audit trails and highlight policy violations
  - Install and operate traps to record information about intruders

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Types of IDS

- Detection method
  - Signature-based
    - can only detect known patterns
  - Heuristic
    - for patterns of behavior that are out of the ordinary
- Location
  - Front end
    - looks at traffic as it enters the network
  - Internal
    - monitors traffic within the network

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

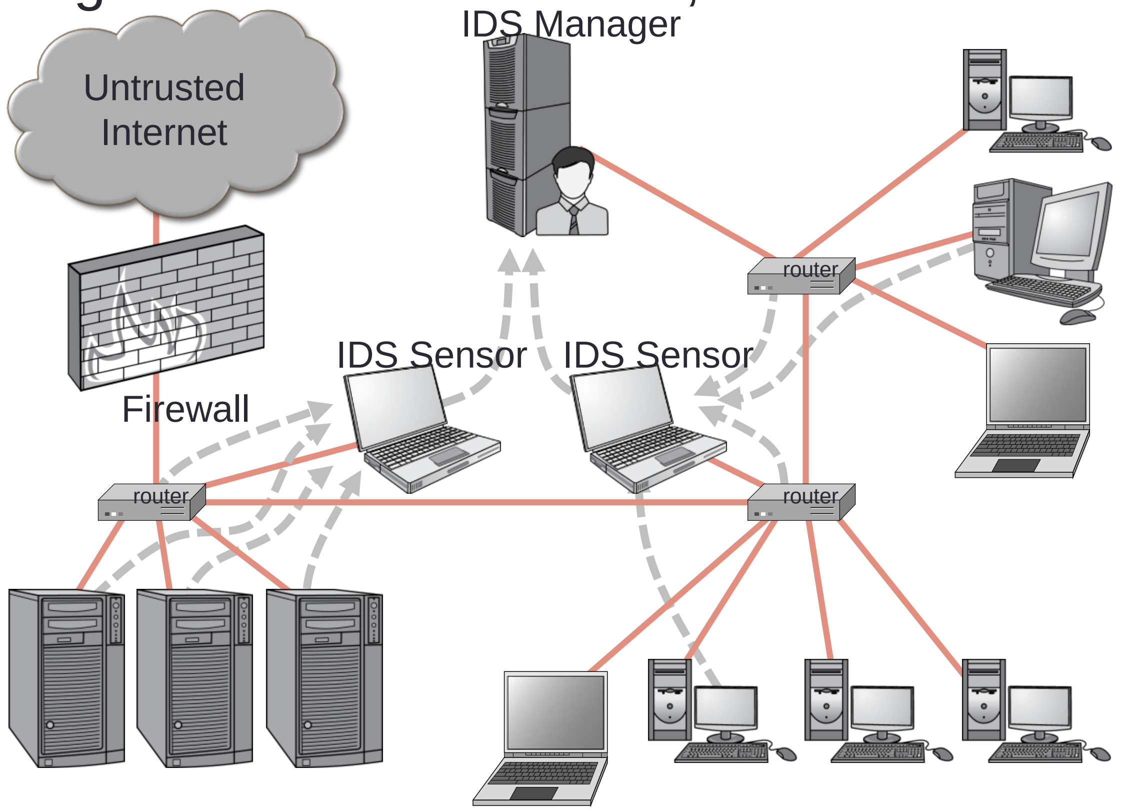
Types of IDS

- Scope
  - Host-based IDS (HIDS)
    - protects a single host by monitoring traffic from the OS
  - Network-based IDS (NIDS)
    - a server or appliance that monitors network traffic
- Capability
  - Passive
  - Active, also known as intrusion prevention systems (IPS)
    - tries to block or otherwise prevent suspicious or malicious behavior once it is detected

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

IDS Components

- The **IDS manager** compiles data from the IDS sensors to determine if an intrusion has occurred.
- This determination is based on a set of **site policies,** which are rules and conditions that define probable intrusions.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.



IDS Data

- In an influential 1987 paper, Dorothy Denning identified several fields that should be included in IDS event records:
  - Subject: the initiator of an action on the target
  - Object: the resource being targeted, such as a file, command, device, or network protocol
  - Action: the operation being performed by the subject towards the object
  - Exception-condition: any error message or exception condition that was raised by this action
  - Resource-usage: quantitative items that were expended by the system performing or responding to this action
  - Time-stamp: a unique identifier for the moment in time when this action was initiated

Intrusions

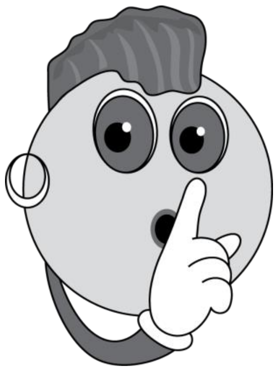
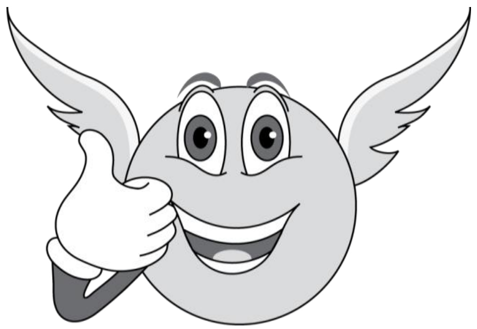
- An IDS is designed to detect a number of threats, including the following:
  - **masquerader:** an attacker who is falsely using the identity and/or credentials of a legitimate user to gain access to a computer system or network
  - **Misfeasor:** a legitimate user who performs actions he is not authorized to do
  - **Clandestine user:** a user who tries to block or cover up his actions by deleting audit files and/or system logs

Intrusions

- In addition, an IDS is designed to detect automated attacks and threats, including the following:
  - **port scans:** information gathering intended to determine which ports on a host are open for TCP connections
  - **Denial-of-service attacks:** network attacks meant to overwhelm a host and shut out legitimate accesses
  - **Malware attacks:** replicating malicious software attacks, such as Trojan horses, computer worms, viruses, etc.
  - **ARP spoofing:** an attempt to redirect IP traffic in a local-area network
  - **DNS cache poisoning:** a pharming attack directed at changing a host’s DNS cache to create a falsified domain-name/IP-address association

Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative)

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	True Positive	False Positive
No Alarm Sounded	 False Negative	 True Negative

The Base-Rate Fallacy

- It is difficult to create an intrusion detection system with the desirable properties of having both a high true-positive rate and a low false-negative rate.
- If the number of actual intrusions is relatively small compared to the amount of data being analyzed, then the effectiveness of an intrusion detection system can be reduced.
- In particular, the effectiveness of some IDSs can be misinterpreted due to a statistical error known as the **base-rate fallacy.**
- This type of error occurs when the probability of some conditional event is assessed without considering the "base rate" of that event.

Base-Rate Fallacy Example

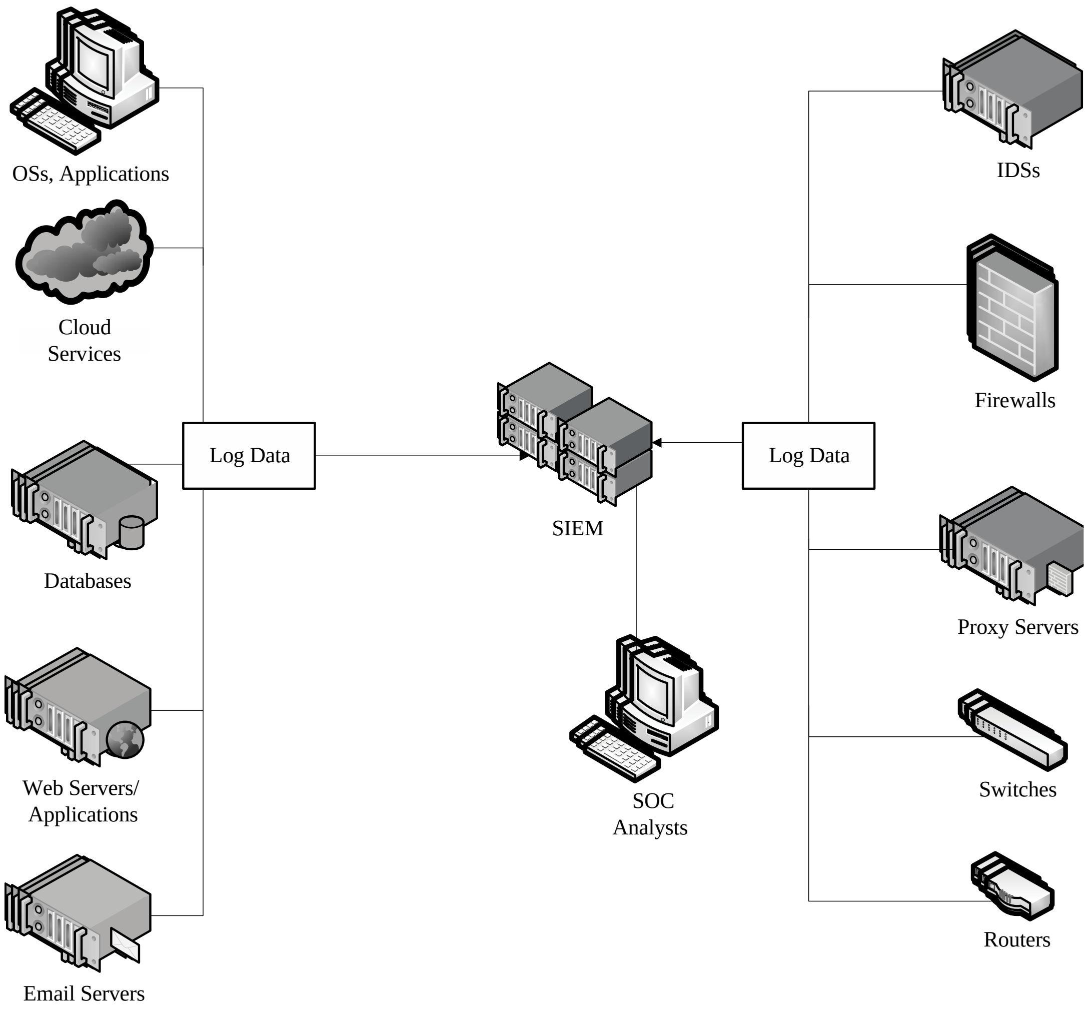
- Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives. Suppose further…
- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative.**
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That is, roughly 99% of our alarms are false alarms.

Security Information and Event Management (SIEM)

- SIEMs are software systems that collect security-relevant data—usually audit logs—from a variety of hardware and software products
- Create a unified security dashboard for security operations center personnel.
- SIEMs range in functionality
  - Simple ones allow for basic search and alerting
  - Complex platforms allow for completely custom dashboards, reports, alerts, and correlation

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Security Information and Event Management (SIEM)



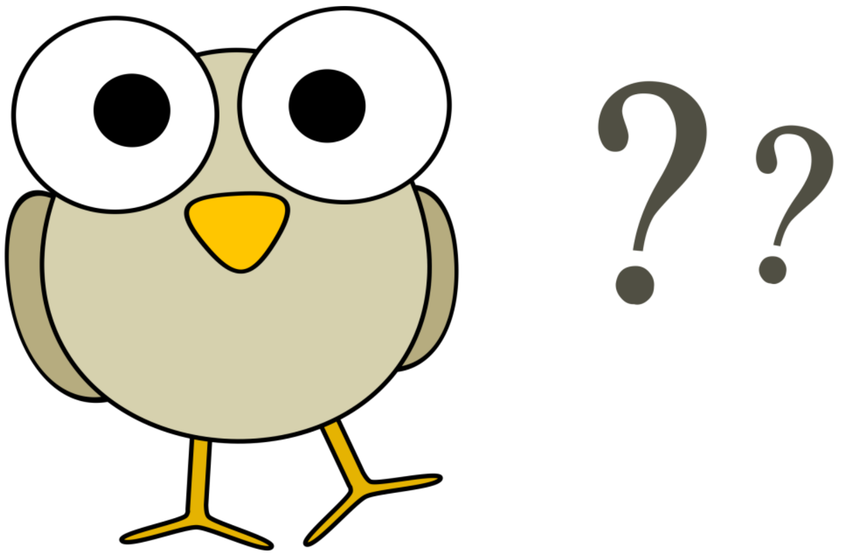
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Summary

- Networks are threatened by attacks aimed at interception, modification, fabrication, and interruption
- WPA2 has many critical security advantages over WEP
- DoS attacks come in many flavors, but malicious ones are usually either volumetric in nature or exploit a bug
- Network encryption can be achieved using specialized tools—some for link encryption and some for end-to-end—such as VPNs, SSH, and the SSL/TLS protocols
- A wide variety of firewall types exist, ranging from very basic IP-based functionality to complex application-layer logic, and both on networks and hosts
- There are many flavors of IDS, each of which detects different kinds of attacks in very different parts of the network

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

- Questions?



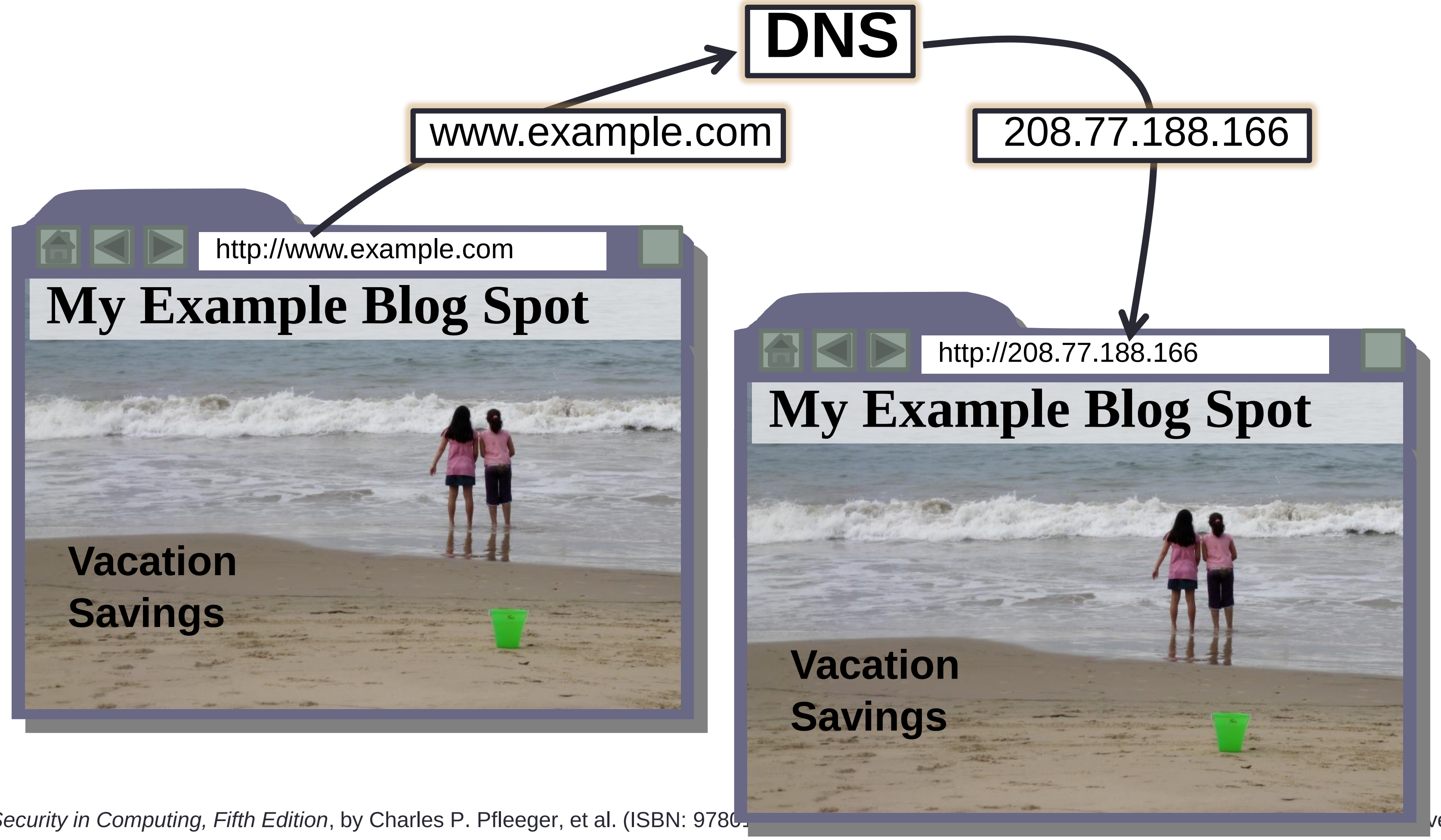
EXTRA SLIDES

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Computer Networks: Domain Name System

Domain Name System

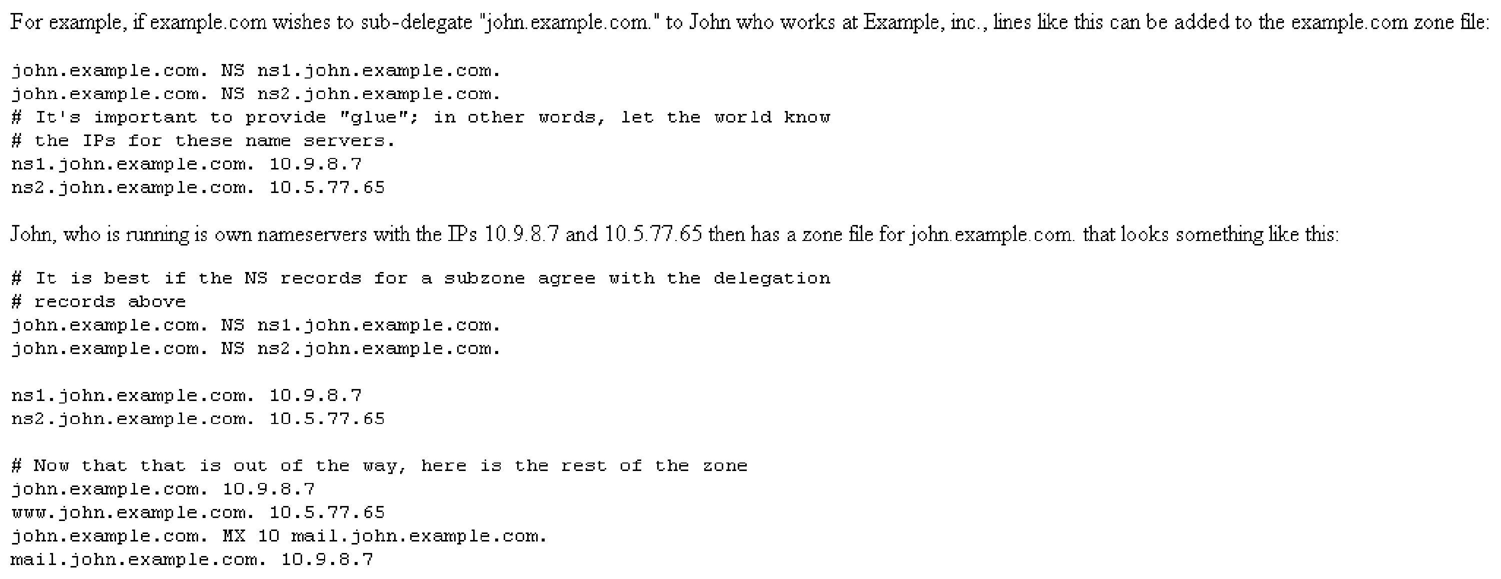
The domain name system (DNS) is an application-layer protocol for mapping domain names to IP addresses



Domain Name System

DNS provides a distributed database over the internet that stores various resource records, including:

- Address (A) record: IP address associated with a host name
- Mail exchange(MX) record: mail server of a domain
- Name server (NS) record: authoritative server for a domain



For example, if example.com wishes to sub-delegate "john.example.com." to John who works at Example, inc., lines like this can be added to the example.com zone file:

```
john.example.com. NS ns1.john.example.com.
john.example.com. NS ns2.john.example.com.
# It's important to provide "glue"; in other words, let the world know
# the IPs for these name servers.
ns1.john.example.com. 10.9.8.7
ns2.john.example.com. 10.5.77.65
```

John, who is running is own nameservers with the IPs 10.9.8.7 and 10.5.77.65 then has a zone file for john.example.com. that looks something like this:

```
# It is best if the NS records for a subzone agree with the delegation
# records above
john.example.com. NS ns1.john.example.com.
john.example.com. NS ns2.john.example.com.

ns1.john.example.com. 10.9.8.7
ns2.john.example.com. 10.5.77.65

# Now that that is out of the way, here is the rest of the zone
john.example.com. 10.9.8.7
www.john.example.com. 10.5.77.65
john.example.com. MX 10 mail.john.example.com.
mail.john.example.com. 10.9.8.7
```

Example DNS entries from http://www.maradns.org/tutorial/recordtypes.html

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Name Servers

.info
.com
.biz
.edu
Domain Name System (DNS)
.org
.net
.in
.gov
thehappylearning.com

Domain names:

- Two or more labels, separated by dots (e.g., cs166.net)
- Rightmost label is the top-level domain (TLD)

Hierarchy of authoritative name servers

- Information about root domain
- Information about its subdomains (A records) or references to other name servers (NS records)

The authoritative name server hierarchy matches the domain hierarchy: root servers point to DNS servers for TLDs, etc.

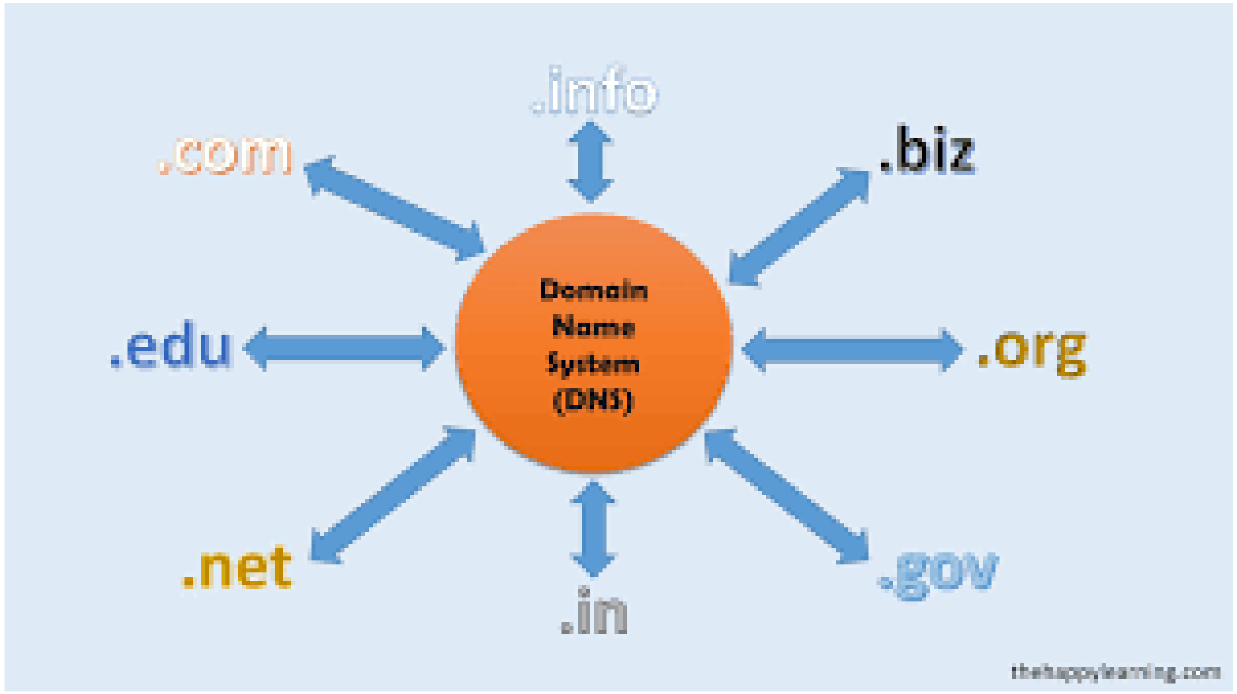
Root servers, and servers for TLDs change infrequently

DNS servers refer to other DNS servers by name, not by IP: sometimes must bootstrap by providing an IP along with a name, called a glue record

http://thehappylearning.com/what-is-domain-name-and-how-does-domain-name-system-dns-work/

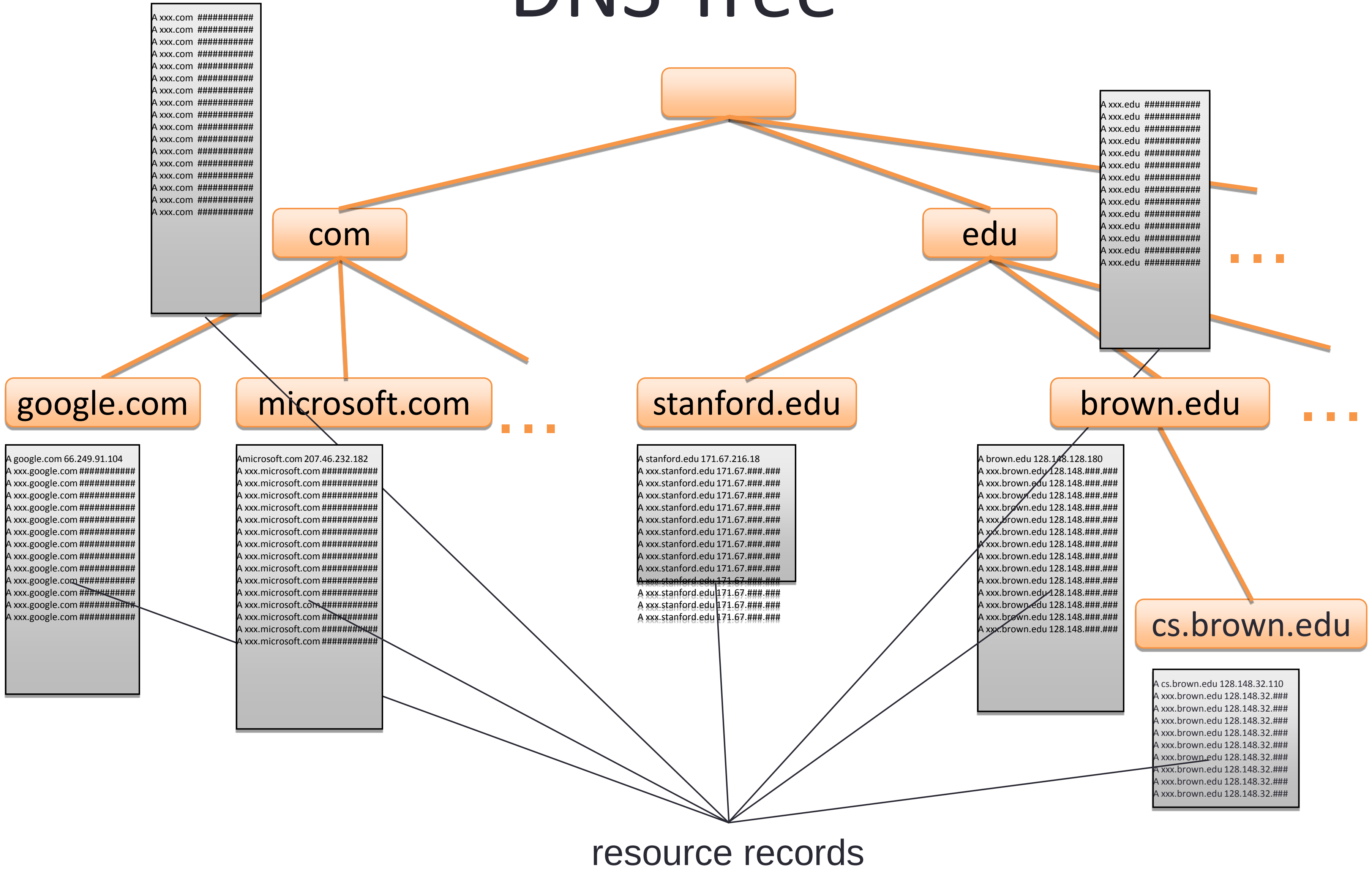
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DNS



http://thehappylearning.com/what-is-domain-name-and-how-does-domain-name-system-dns-work/

DNS Tree



com
edu
google.com
microsoft.com
stanford.edu
brown.edu
cs.brown.edu
. . .
resource records
A xxx.com ###########
A xxx.edu ###########
A google.com 66.249.91.104
A xxx.google.com ###########
Amicrosoft.com 207.46.232.182
A xxx.microsoft.com ###########
A stanford.edu 171.67.216.18
A xxx.stanford.edu 171.67.###.###
A brown.edu 128.148.128.180
A xxx.brown.edu 128.148.###.###
A cs.brown.edu 128.148.32.110
A xxx.brown.edu 128.148.32.###

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

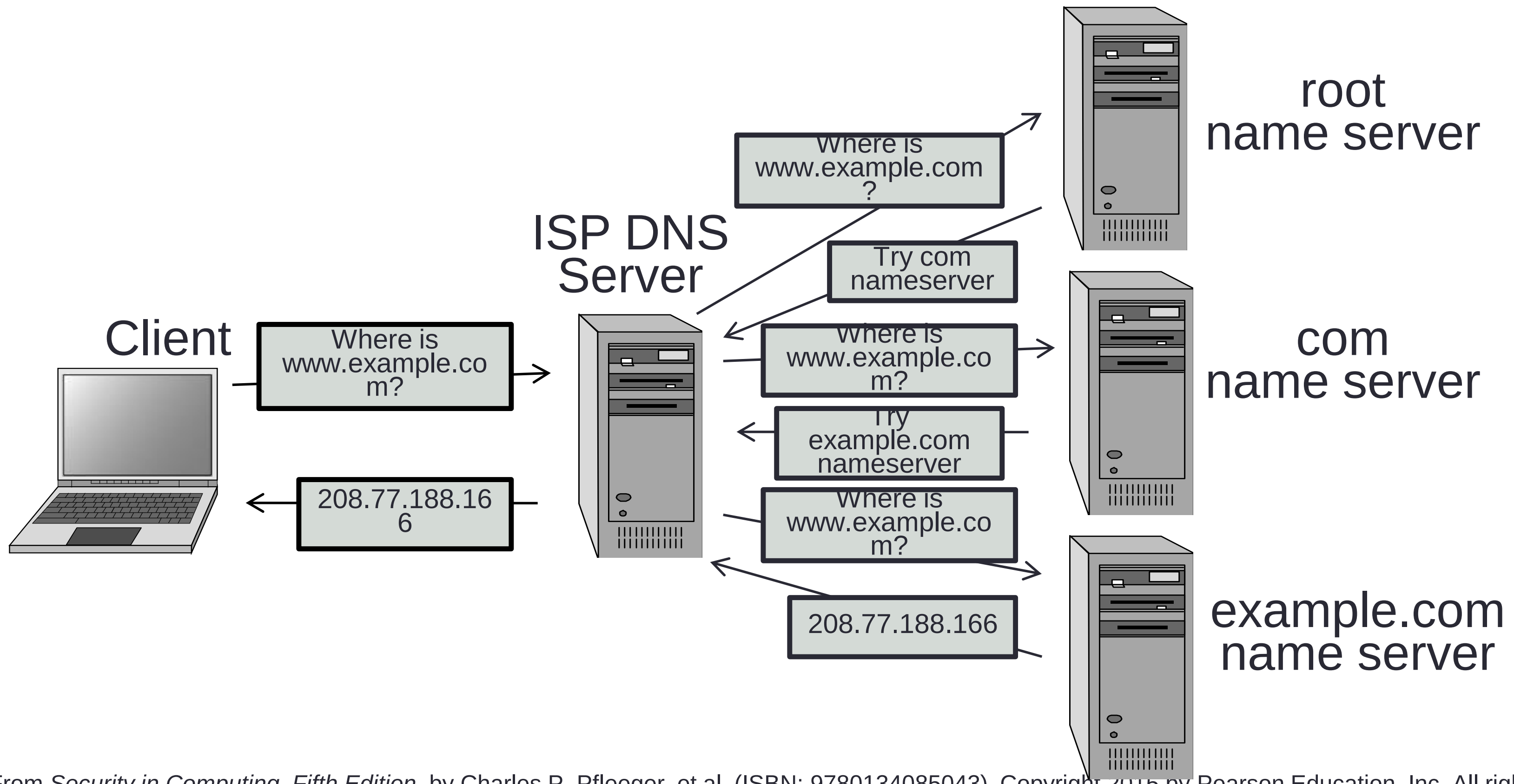
Top Level Domains

- Started in 1984
- Originally supposed to be named by function
  - .com for commercial websites, .mil for military
- Eventually agreed upon unrestricted TLDs for .com, .net, .org, .info
- In 1994 started allowing country TLDs such as .it, .us
- Tried to move back to hierarchy of purpose in 2000 with creation of .aero, .museum, etc.

Name Resolution

- Zone: collection of connected nodes with the same authoritative DNS server

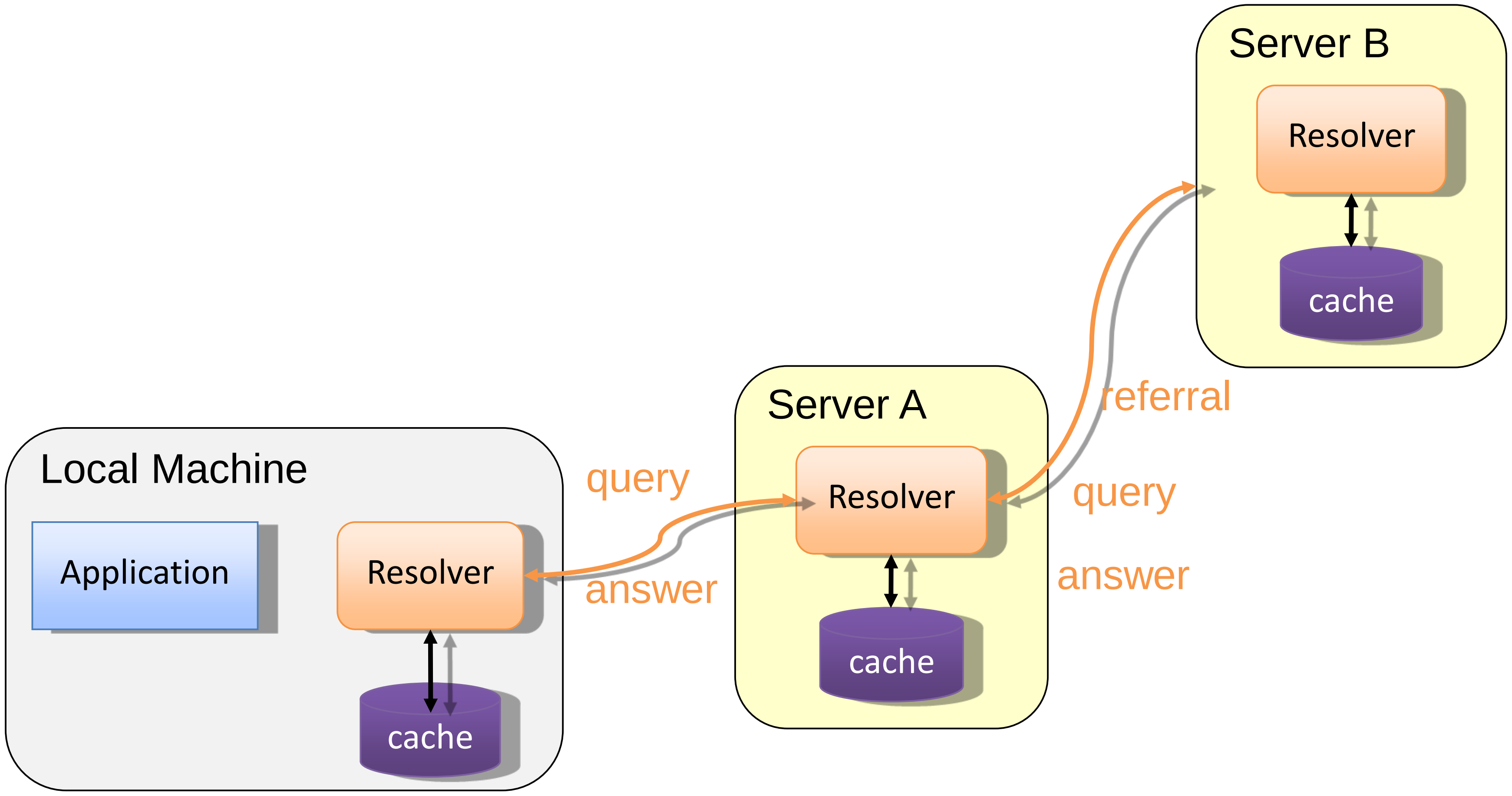
  Resolution method when answer not in cache:


root
name server
com
name server
example.com
name server
ISP DNS
Server
Client
Where is www.example.com?
Where is www.example.com?
Try com nameserver
Where is www.example.com?
Try example.com nameserver
Where is www.example.com?
208.77.188.166
208.77.188.166

Recursive Name Resolution

- The DNS Client sends a Query to a DNS Server for name resolution
  - If the DNS Server doesn't know the answer to provide accurate answer to the DNS Client, DNS Server may query other DNS Servers on behalf of the DNS Client
- The preferred name resolution
- Maybe disabled for performance reasons
- If recursion is disabled, DNS server uses a process called iteration for name resolution

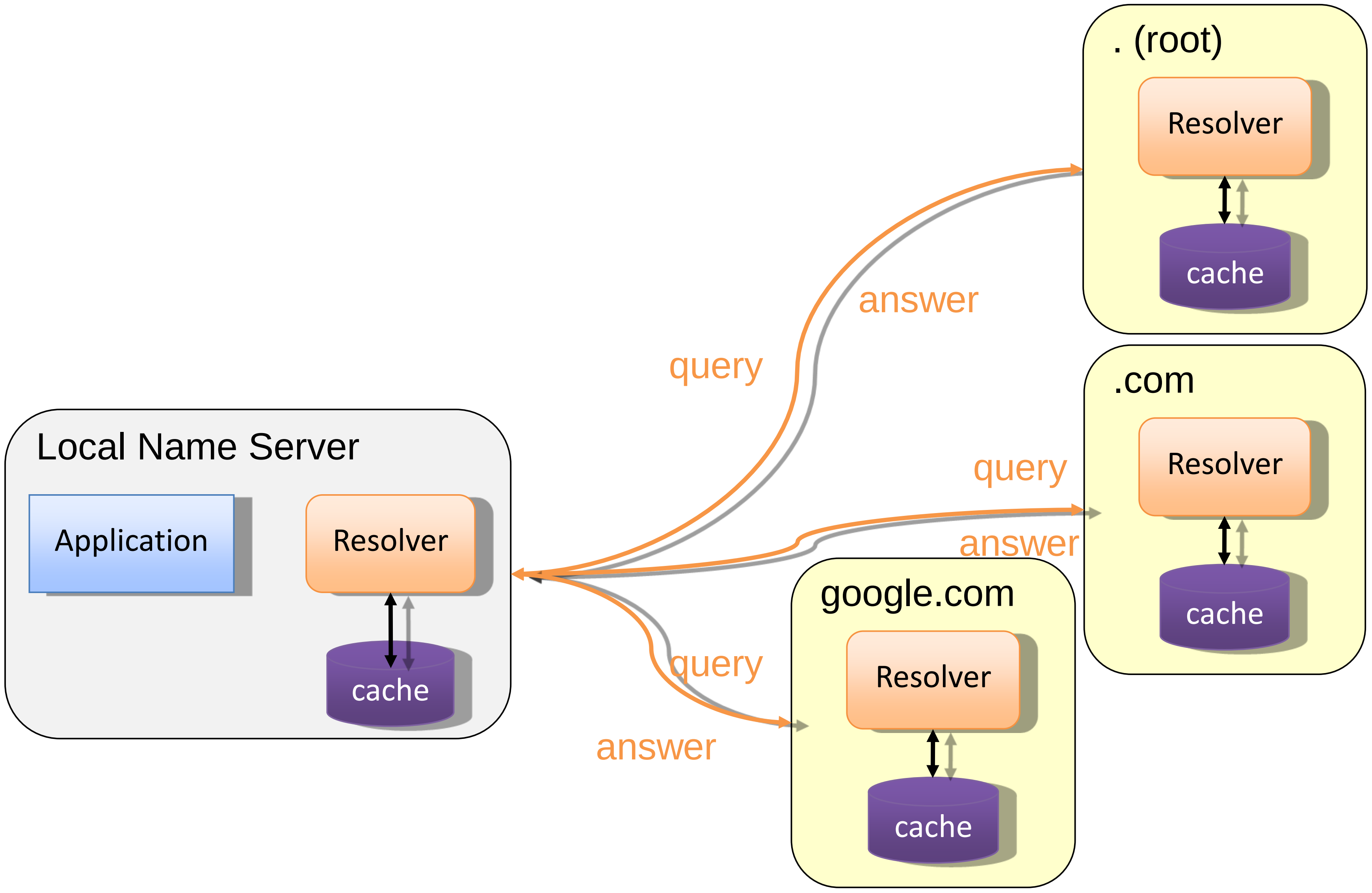
Recursive Name Resolution



Iterative Name Resolution

- DNS Client, making repeated DNS Queries to different DNS Servers for name resolution
- The DNS Server provides the best answer it has.

Iterative Name Resolution



Authoritative Name Servers

- Control distributed among authoritative name servers (ANSs)
  - Responsible for specific domains
  - Can designate other ANS for subdomains
- ANS can be master or slave
  - Master contains original zone table
  - Slaves are replicas, automatically updating
- Makes DNS fault tolerant, automatically distributes load
- ANS must be installed as a NS in parents' zone

Dynamic Resolution

- Many large providers have more than one authoritative name server for a domain
- Problem: need to locate the instance of domain geographically closest to user
- Proposed solution: include first 3 octets of requester's IP in recursive requests to allow better service
- Content distribution networks already do adaptive DNS routing

DNS Caching

There would be too much network traffic if a path in the DNS tree would be traversed for each query

- Root zone would be rapidly overloaded

DNS servers cache results for a specified amount of time

- Specified by ANS reply's time-to-live field

Operating systems and browsers also maintain resolvers and DNS caches

- View in Windows with command ipconfig /displaydns
- Associated privacy issues

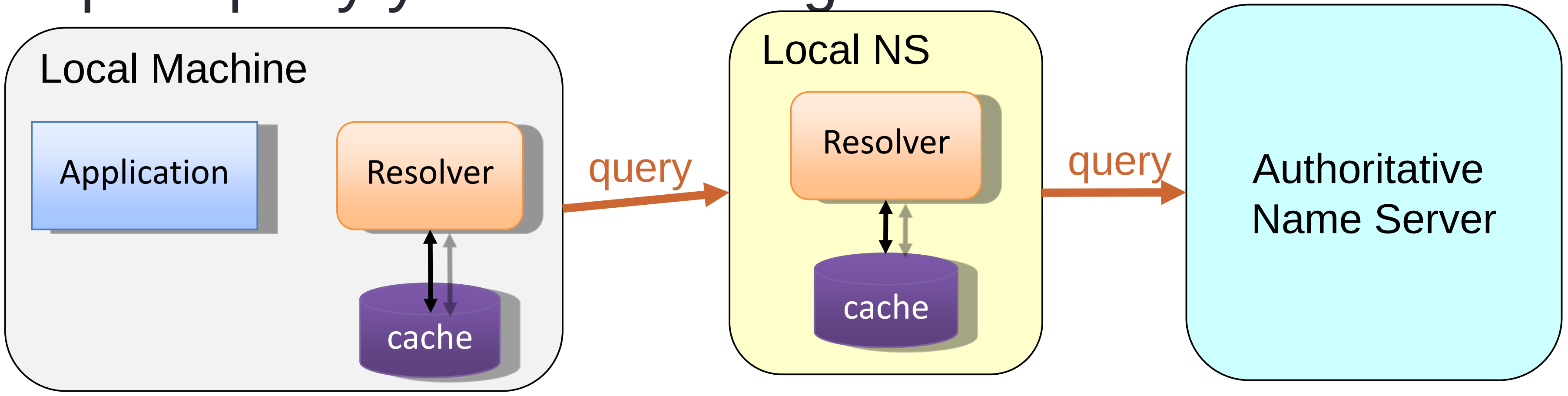
DNS queries are typically issued over UDP on port 53

- 16-bit request identifier in payload

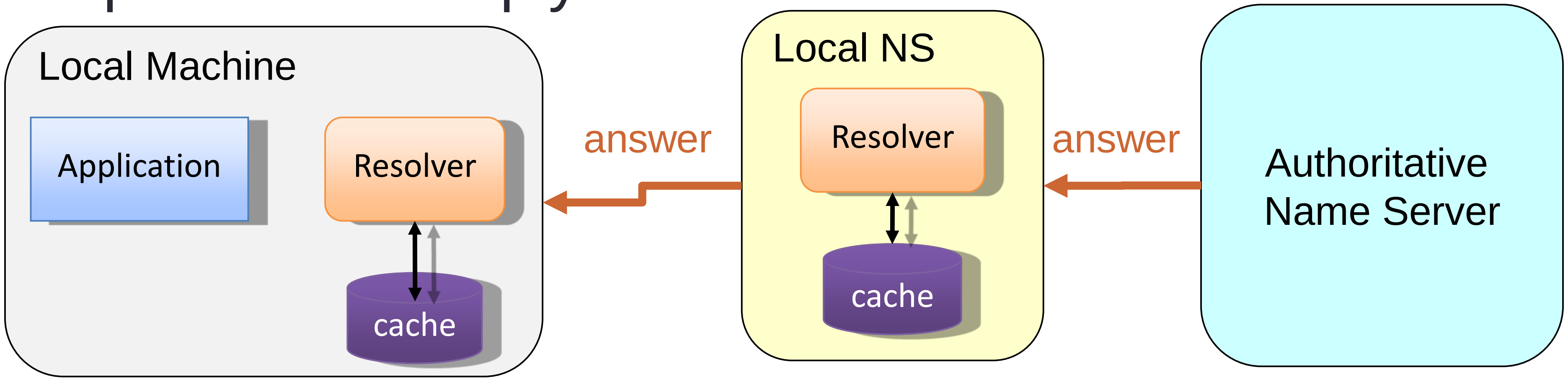
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DNS Caching

Step 1: query yourdomain.org



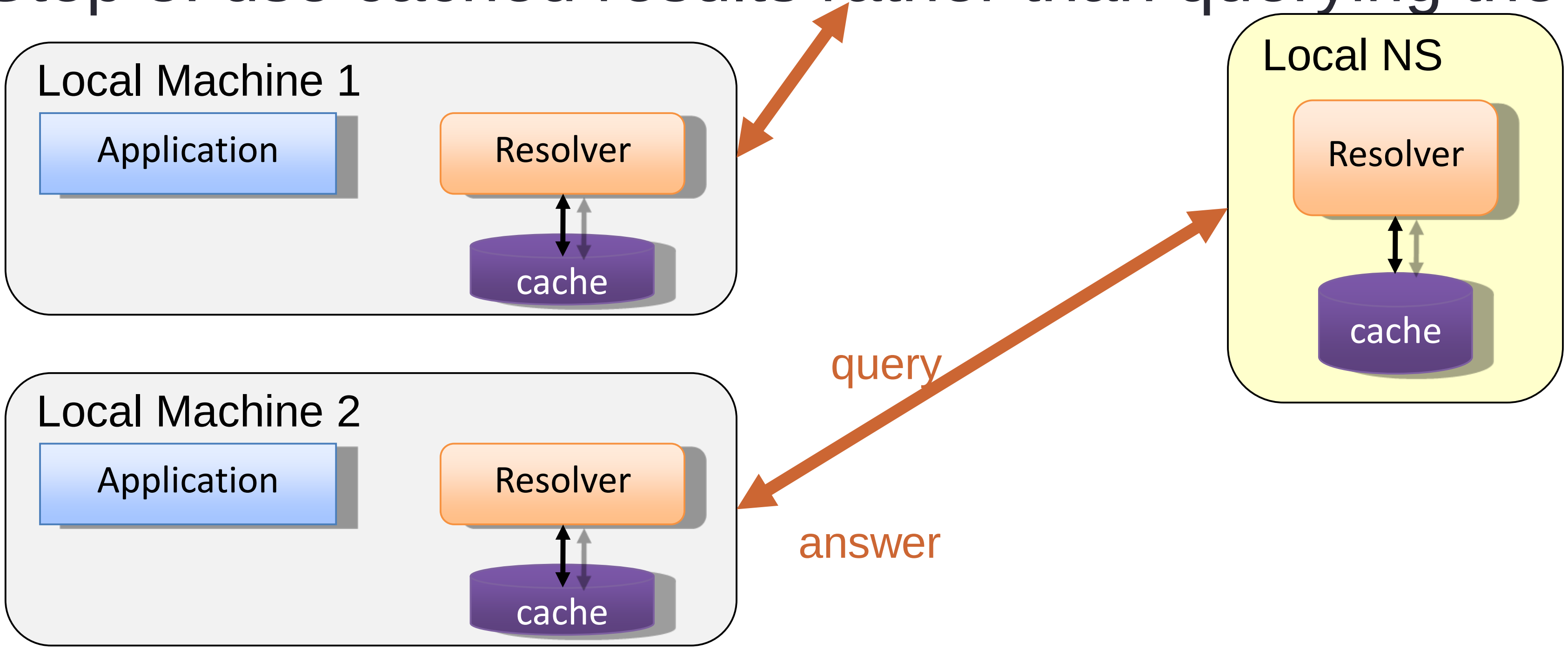
Step 2: receive reply and cache at local NS and host



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DNS Caching (con'd)

Step 3: use cached results rather than querying the ANS

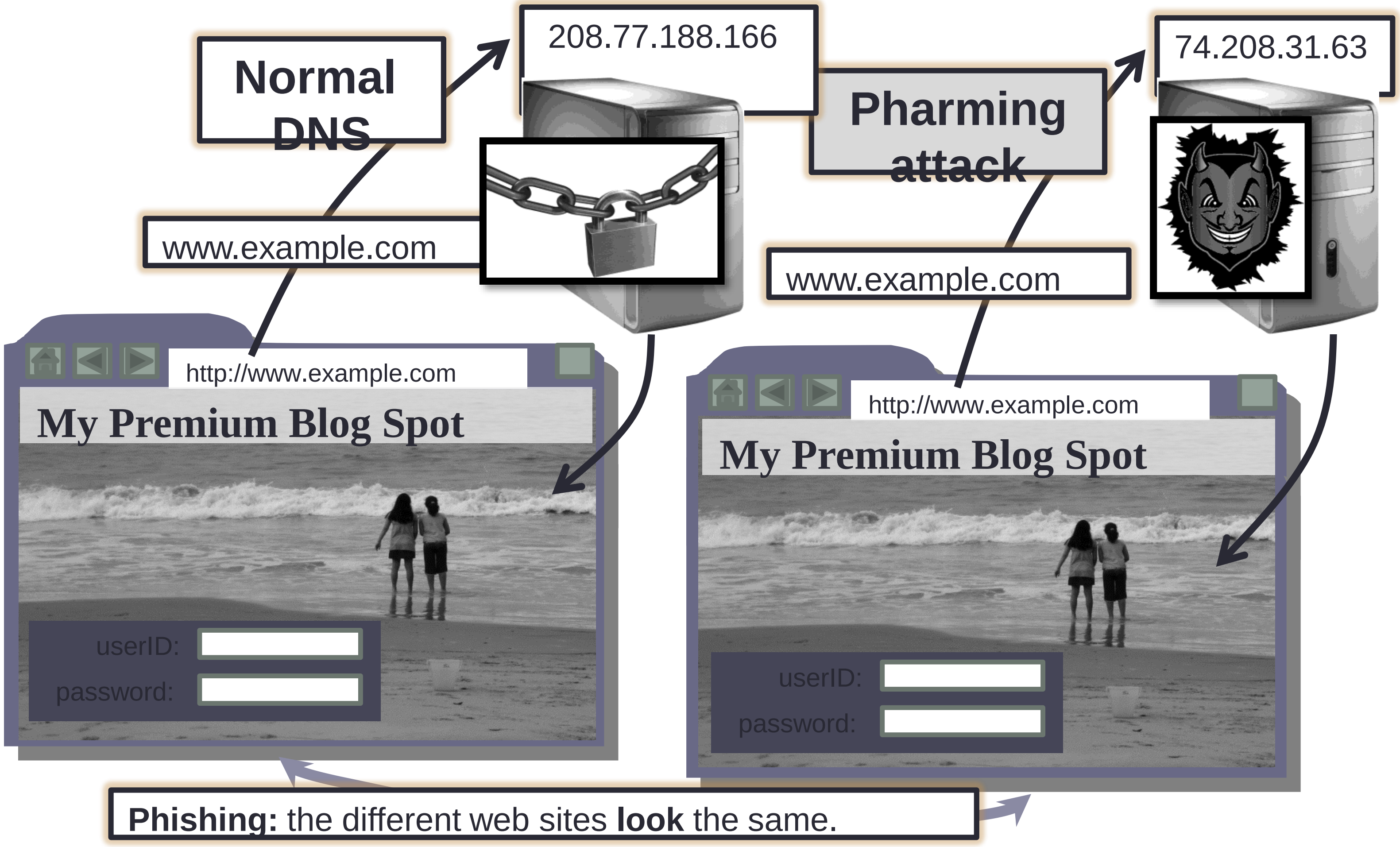


Step 4: Evict cache entries upon ttl expiration

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Pharming: DNS Hijacking

- Changing IP associated with a server maliciously:



DNS Cache Poisoning

- Basic idea: give DNS servers false records and get it cached
- DNS uses a 16-bit request identifier to pair queries with answers
- Cache may be poisoned when a name server:
  - Disregards identifiers
  - Has predictable ids
  - Accepts unsolicited DNS records

DNS Cache Poisoning Prevention

- Use random identifiers for queries
- Always check identifiers
- Port randomization for DNS requests
- Deploy DNSSEC
  - Challenging because it is still being deployed and requires reciprocity

- Questions?