SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks (cont.)

ENCRYPTION FOR NETWORKS

Encryption for networks

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

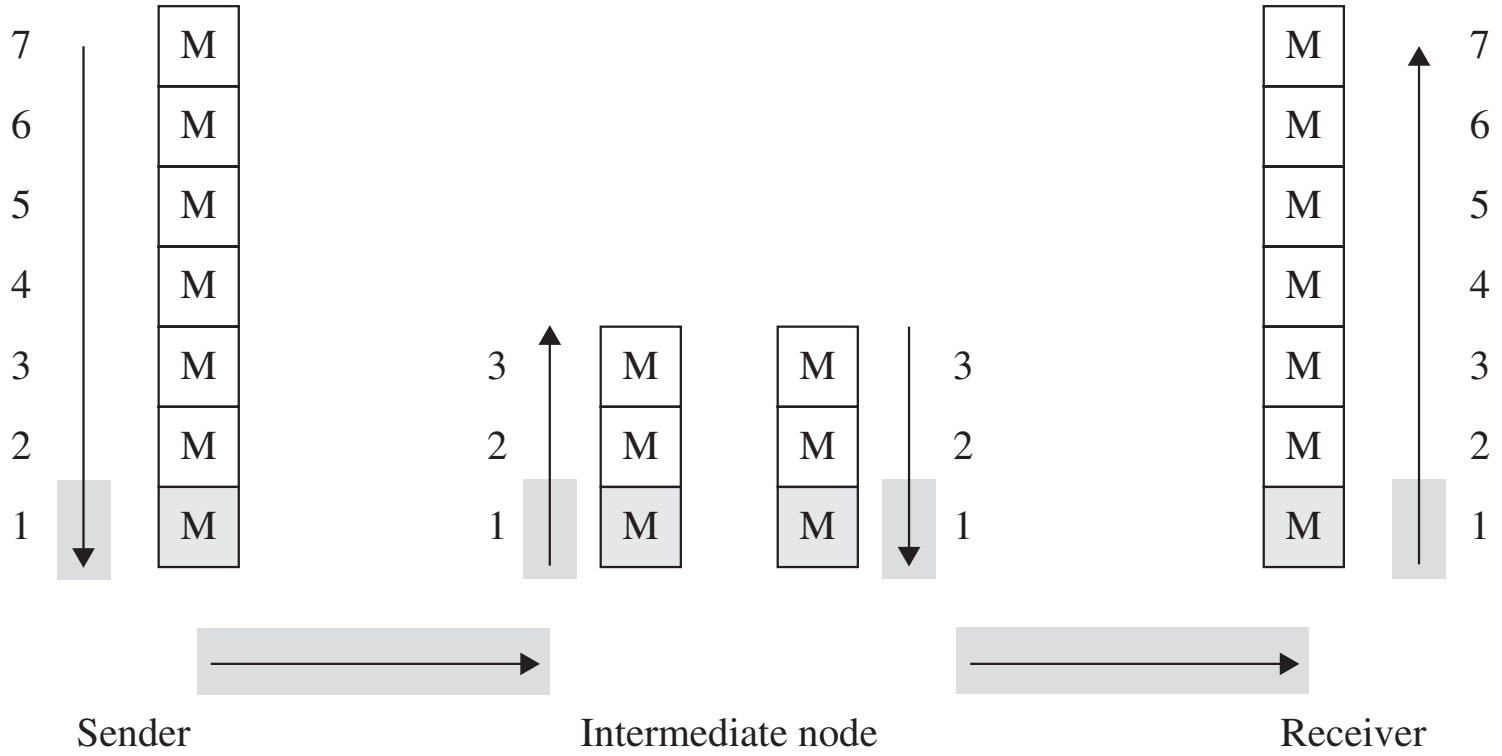
Link Encryption

- 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.

Link Encryption

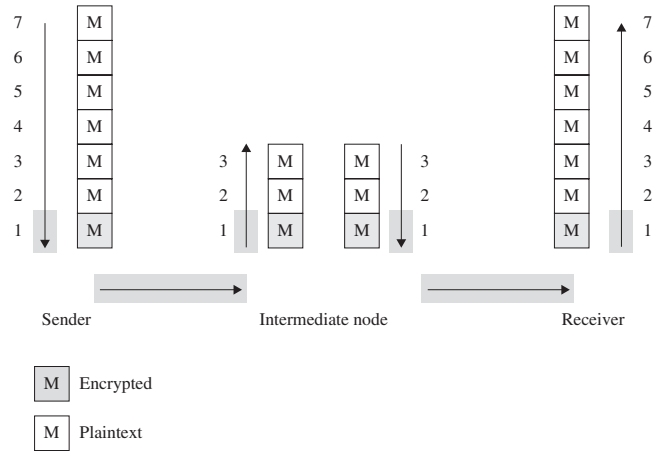
- Typically a host has only one link to the network
  - All traffic sent from this host will be encrypted by it
- However, receiving hosts need to decrypt data
  - All hosts must share keys
- If message is encrypted along some links and not others, the encryption advantages may be lost
  - Intermediate hosts may see message
  - => link encryption is usually performed on all links of a network

Link Encryption Example



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



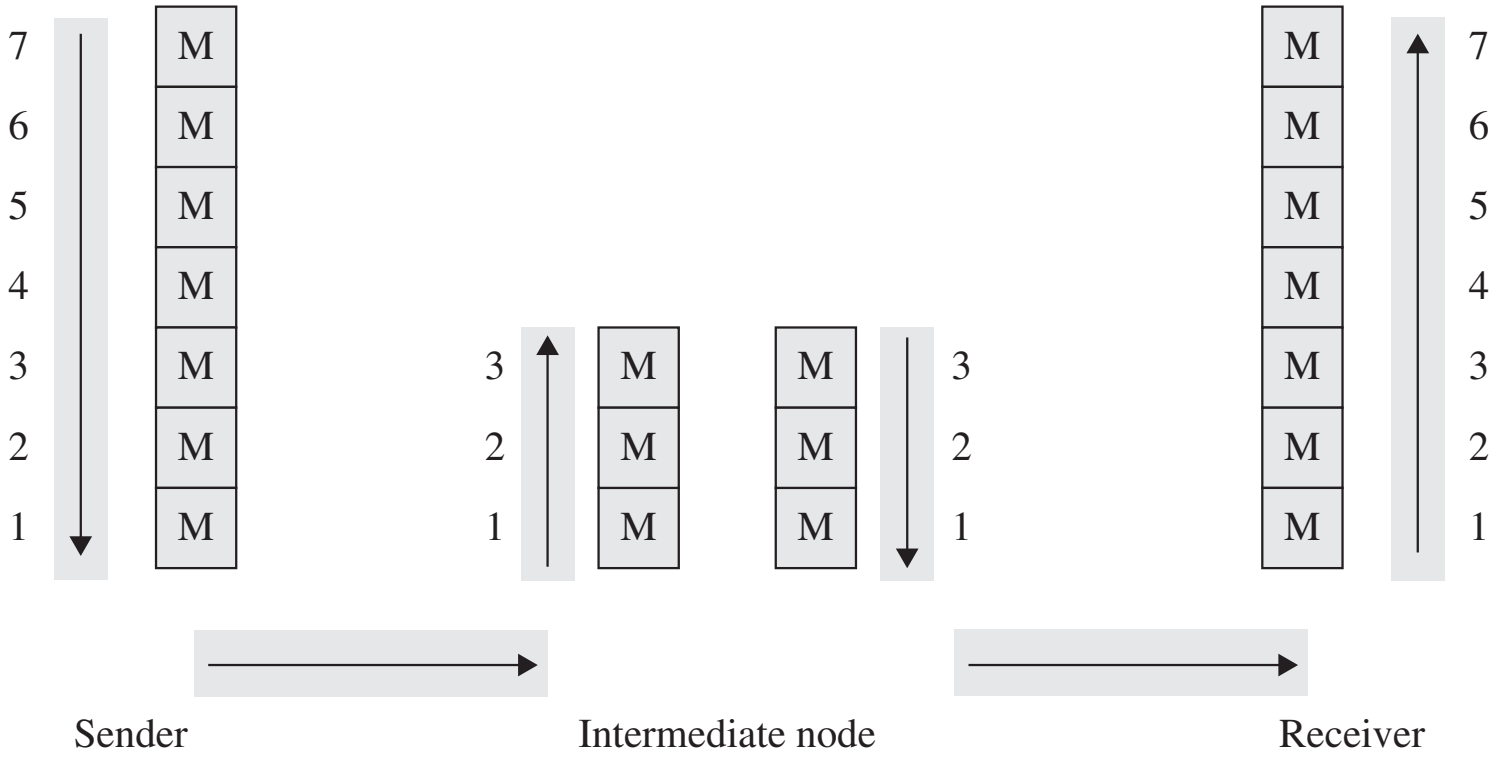
Link Encryption

- Useful when transmission line is vulnerable
  - i.e., if network hosts are secure but communication medium shared with other users
- Desirable when all communications on a single line needs to be protected
  - i.e., protecting internal communication between two offices of same company
- Can be used to implement a private network by using public resources

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

End-to-End Encryption



M Encrypted

M Plaintext

End-to-End Encryption

- Advantage: Provides a virtual cryptographic channel between each pair of users
- Disadvantage: Each pair of users should share a unique cryptographic key
  - Number of keys required = $\frac{n*(n-1)}{2}$
    - Increases rapidly as network grows
- => link encryption is faster and uses fewer keys

End-to-End Encryption

- Advantages:
  - More flexible then link encryption
  - Can be used selectively
  - Done on user level
  - Can be integrated into application
- Both encryptions can be applied simultaneously
  - End-to-end can be applied on top of link encryption

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

End-to-End Encryption

- Whatsapp incorporated end-to-end encryption
  - Whatsapp End-to-End Encryption

BROWSER ENCRYPTION

BROWSER ENCRYPTION

- Browsers can encrypt data for protection during transmission
- The browser and the server negotiate a common encryption key
  - => if an attacker does hijack a session at the TCP or IP protocol level, the attacker cannot join the application data exchange

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

SSH Secure Interactive Command Session

- The client connects to the server via a TCP session.
- 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.

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

SSH Secure Interactive Command Session (cont.)

- The client and server initiate a secret-key exchange to establish a shared secret session key
  - Used to encrypt their communication (but not for authentication).
  - Session key is used in conjunction with a chosen block cipher (typically AES, 3DES) to encrypt all further communications.
- The server sends the client a list of acceptable forms of authentication
  - which the client will try in sequence

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

SSH Secure Interactive Command Session

- The most common mechanism is to use a password or the following public-key authentication method:
  - If public-key authentication is the selected mechanism, the client sends the server its public key.
  - The server 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.
  - The client decrypts the challenge with its private key and responds to the server, proving its identity.

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

A secure interactive command session (cont.):

- 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

SSH

- How SSH Works
- SSH - Secure Shell

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)
- TLS is the modern, and much more secure, protocol
  - Although protocol is still commonly called SSL
- SSL is implemented at OSI layer 4 (transport) and provides:
  - Server authentication
  - Client authentication (optional)
  - Encrypted communication

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

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

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

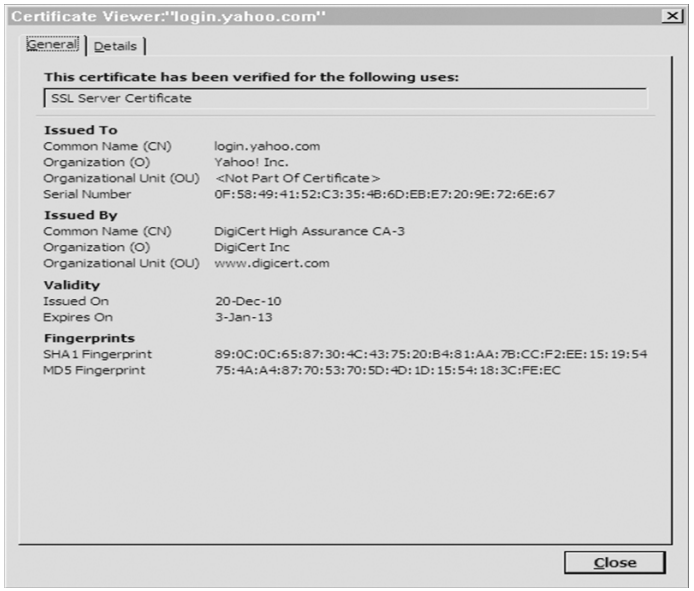
SSL Session Established

SSL Session Established

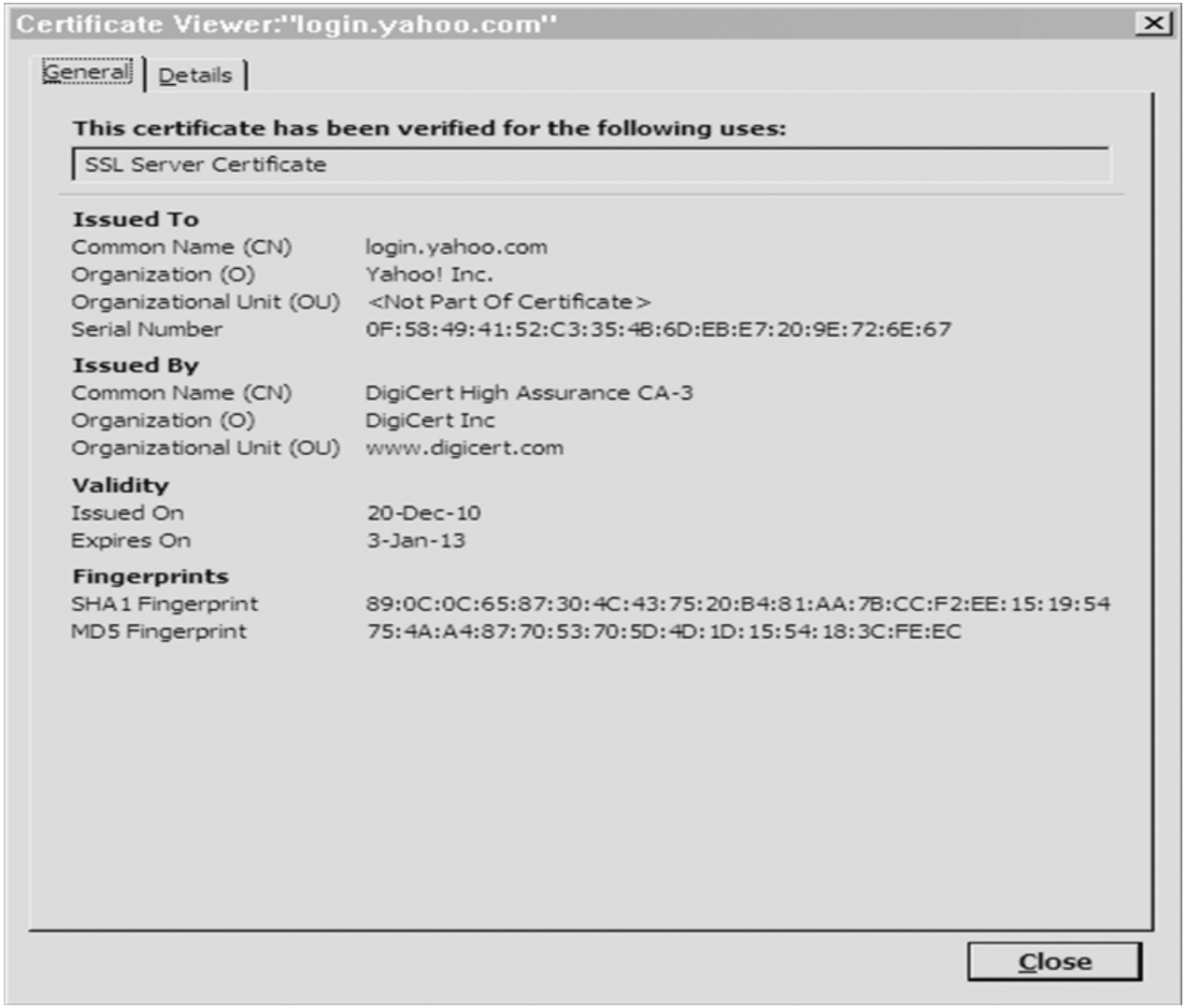
- SSL session dialog includes the following:
  - Site that is verified
  - The certificate authority
  - The choice of encryption algorithm

SSL Certificate

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

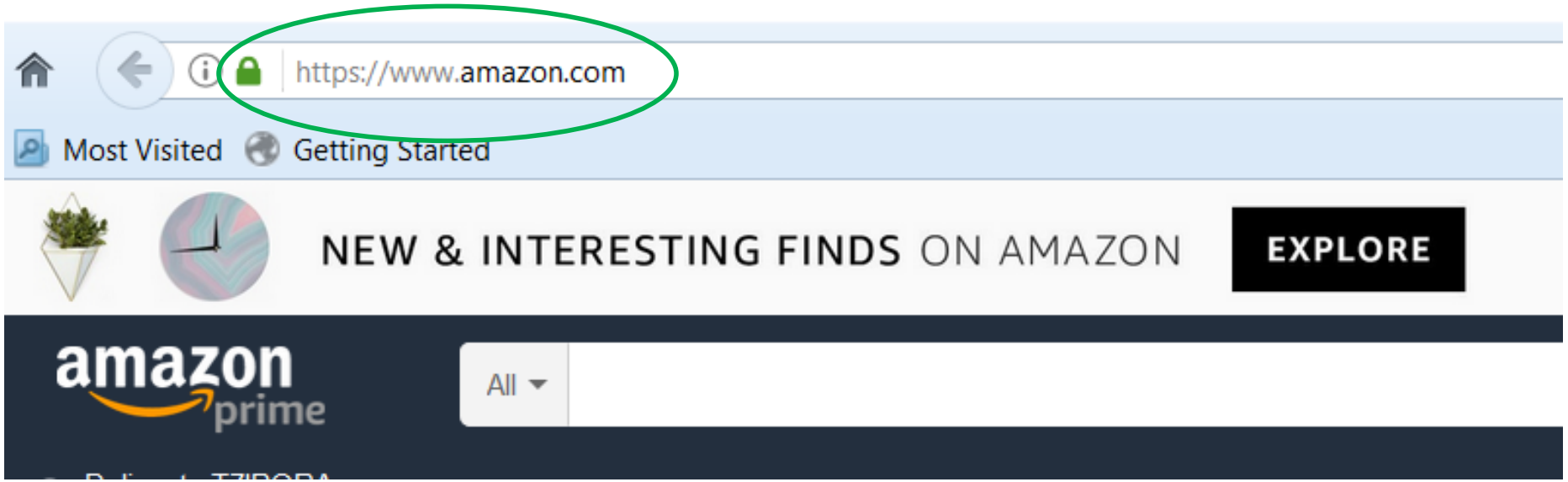


SSL Certificate



TLS/SSL

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



HTTPS/SSL

- https://www.youtube.com/watch?v=hExRDVZHhig

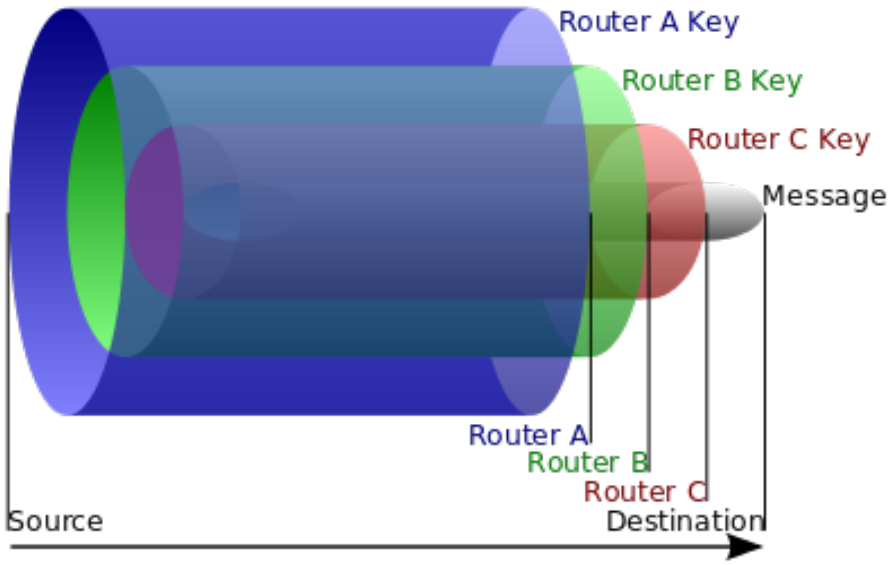
Onion Routing

- Both in link and end-to-end encryption, data is secured by addressing data is not
  - Volume may be visible to eavesdropping
- A technique for anonymous communication over a computer network
  - Enables untraceable data transmission
- Messages are encapsulated in layers of encryption, analogous to layers of an onion

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
  - The host that received the message from the original sender cannot determine the ultimate destination

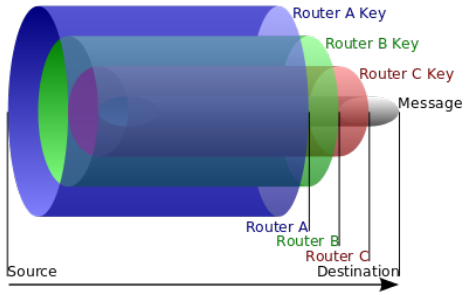
Onion Routing Example



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

Tor (The Onion Router) Project

- Uses onion routing to protect again network analysis
- Transfers communications around a distributed network
  - Run by volunteers around world
- Prevents outsiders from learning what sites users visit
- Prevents sites from learning user's physical location
- https://www.youtube.com/user/TheTorProject/

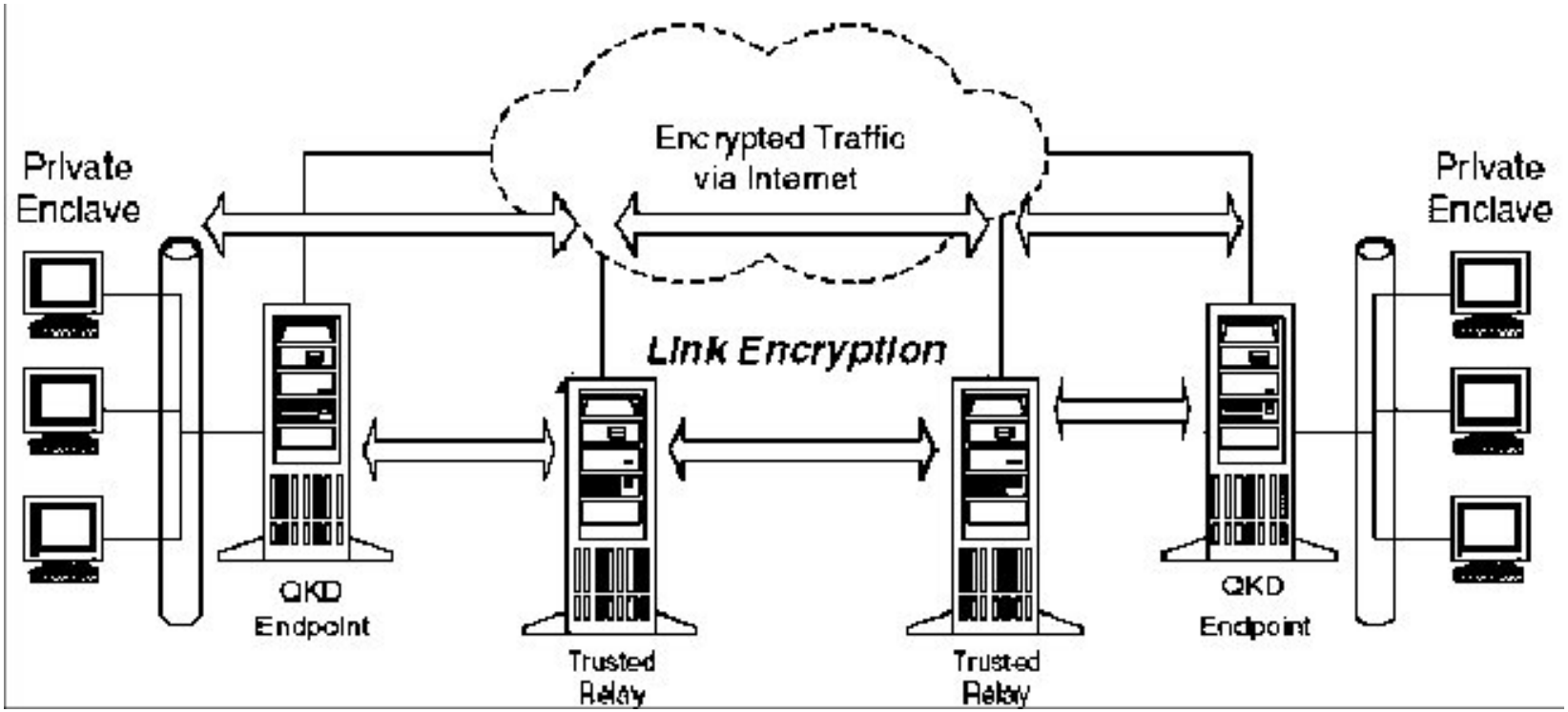
Virtual Private Networking (VPN)

- 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**)

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.

Link Encryption



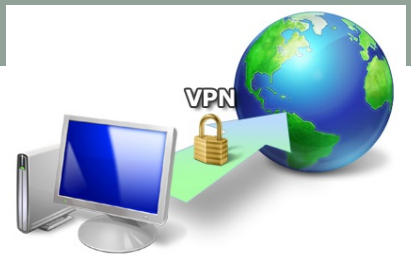
https://www.researchgate.net/figure/QKD-network-with-trusted-relays-and-link-encryption_fig2_51893133

Virtual Private Networking (VPN)

- A technology that allows private networks to be safely extended over long physical distances
  - 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.**

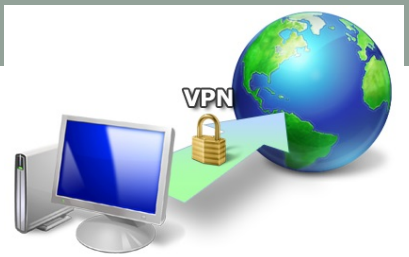
https://www.techsupportalert.com/content/best-vpn-services.htm

Types of VPNs



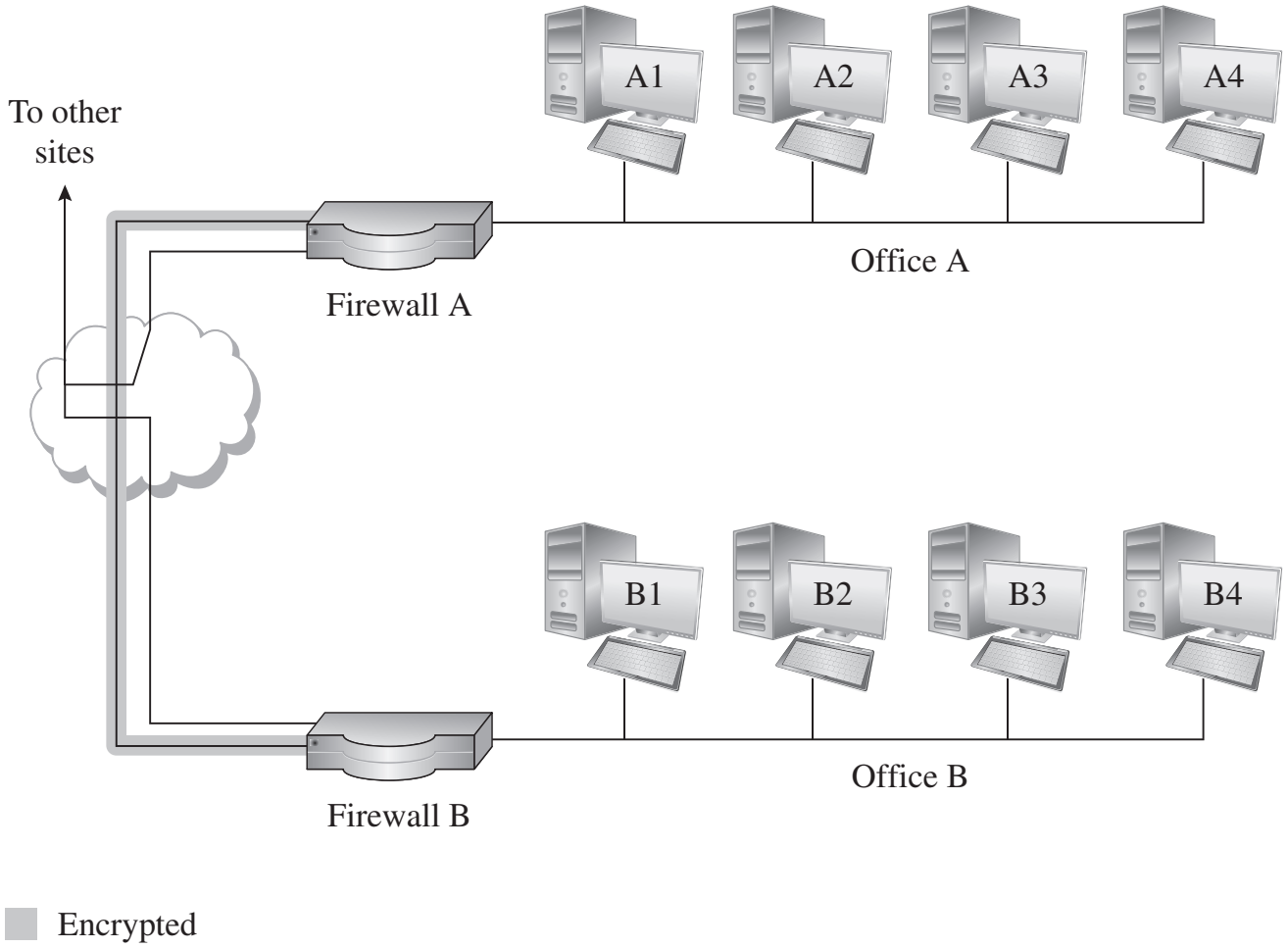
- **Remote access** VPNs allow authorized clients to access a private network that is referred to as an **intranet.**
  - For example, an organization may wish to allow employees access to the company network remotely
    - but make it appear as though they are local to their system and even the Internet 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
    - Software handles negotiating a connection to the NAS and facilitating communication.

Types of VPNs



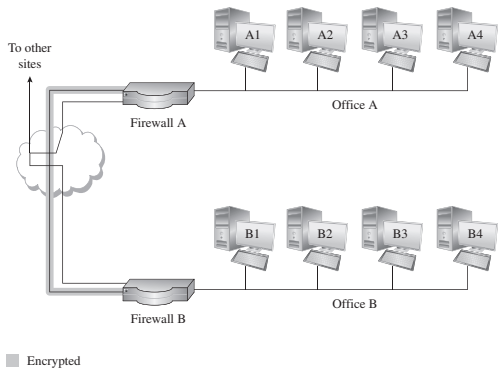
- **Site-to-site** VPN solutions are designed to provide a secure bridge between two or more physically distant networks.
  - Before VPN, organizations wishing to safely bridge their private networks purchased expensive leased lines
    - to directly connect their intranets with cabling.

Virtual Private Networks (VPN) Example

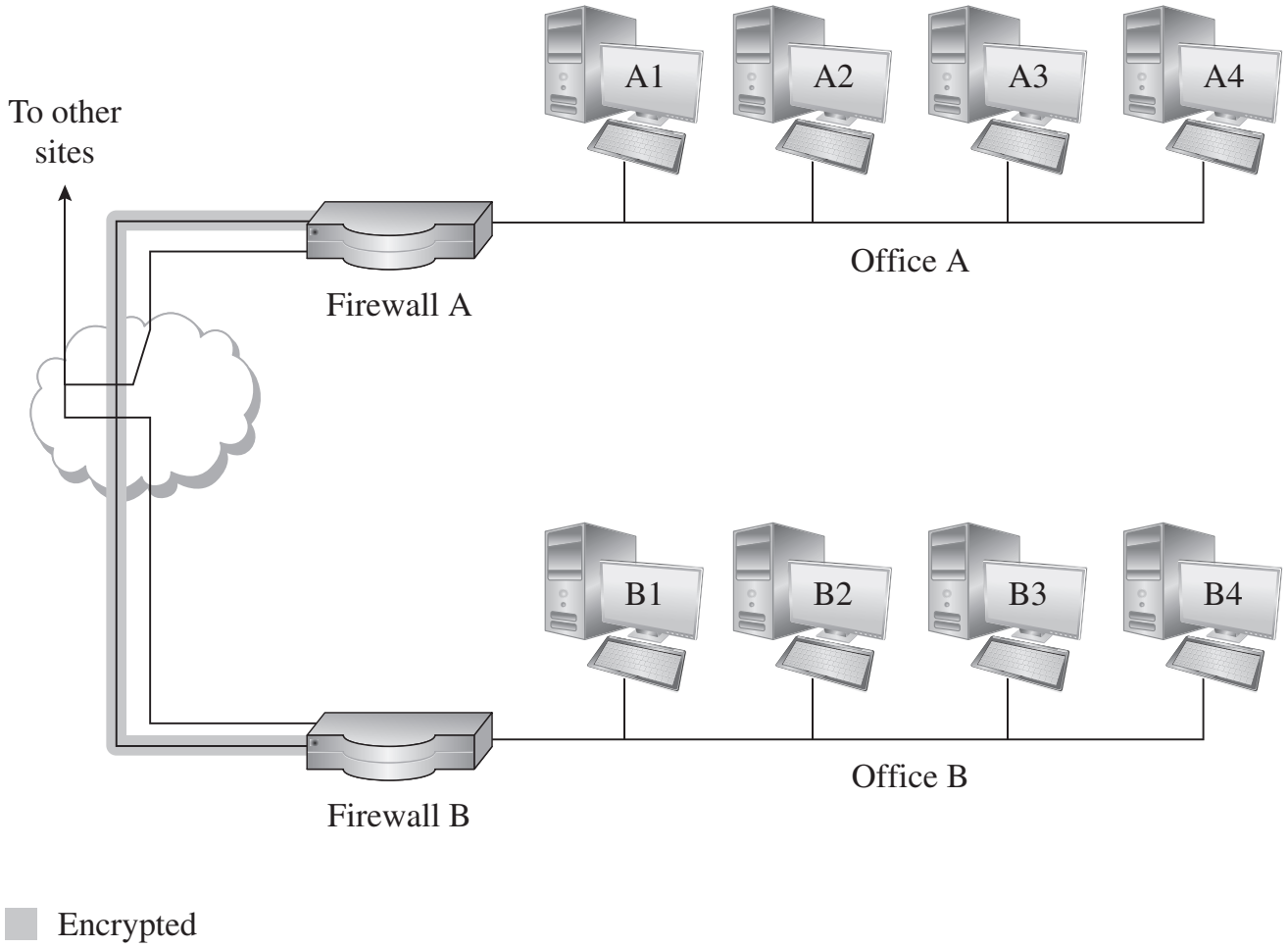


Virtual Private Networks (VPN) Example

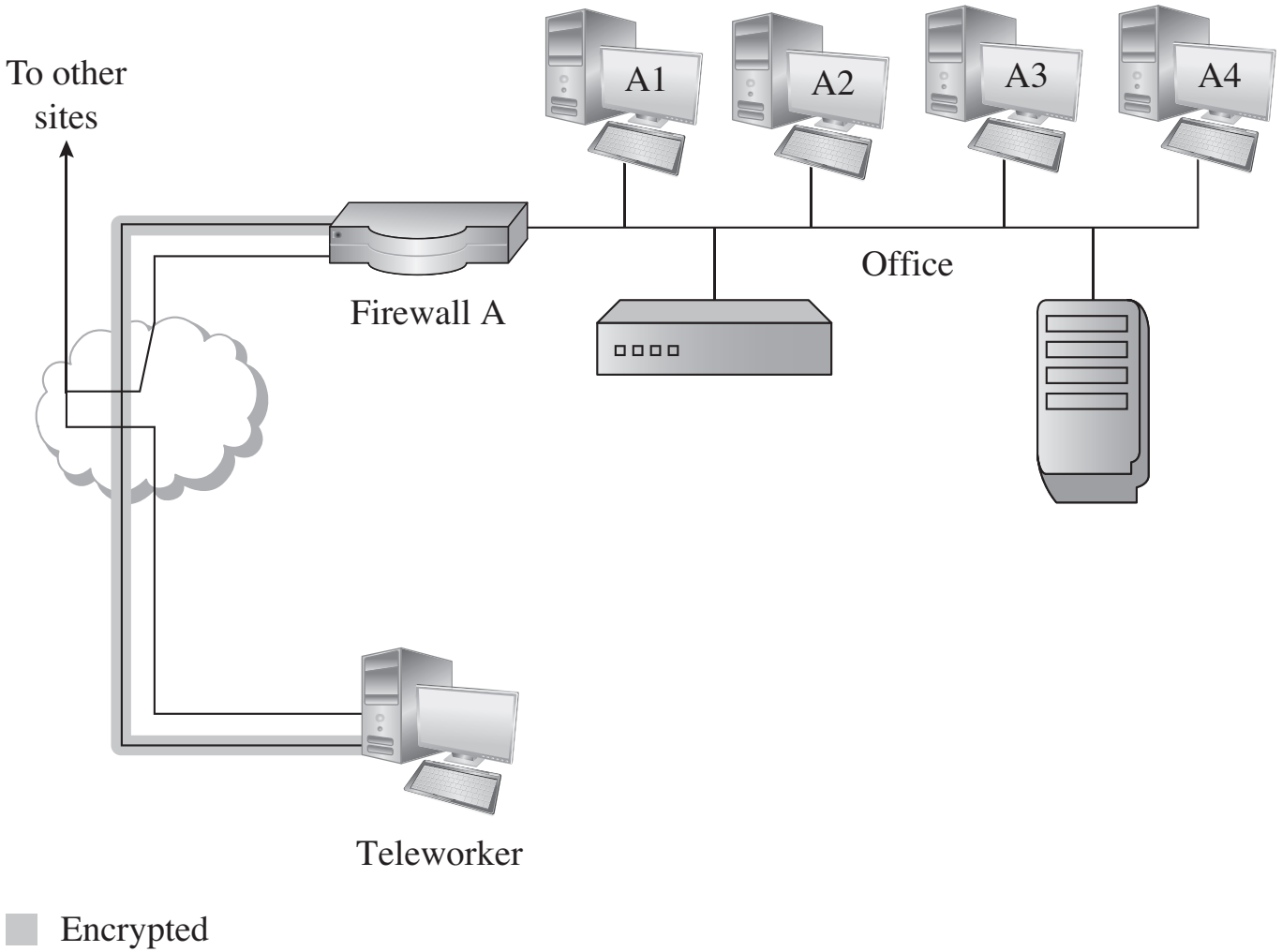
- An encrypted tunnel provides confidentiality and integrity for communication between two sites
  - over public networks
- Connects Office A to Office B over the Internet so they appear to their users as one seamless, private network.
- The VPN is terminated by firewalls at both ends, which is often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



Virtual Private Networks (VPN) Example

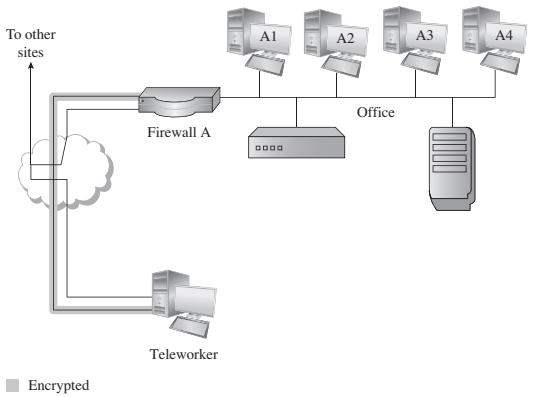


VPN (cont.) – Example 2

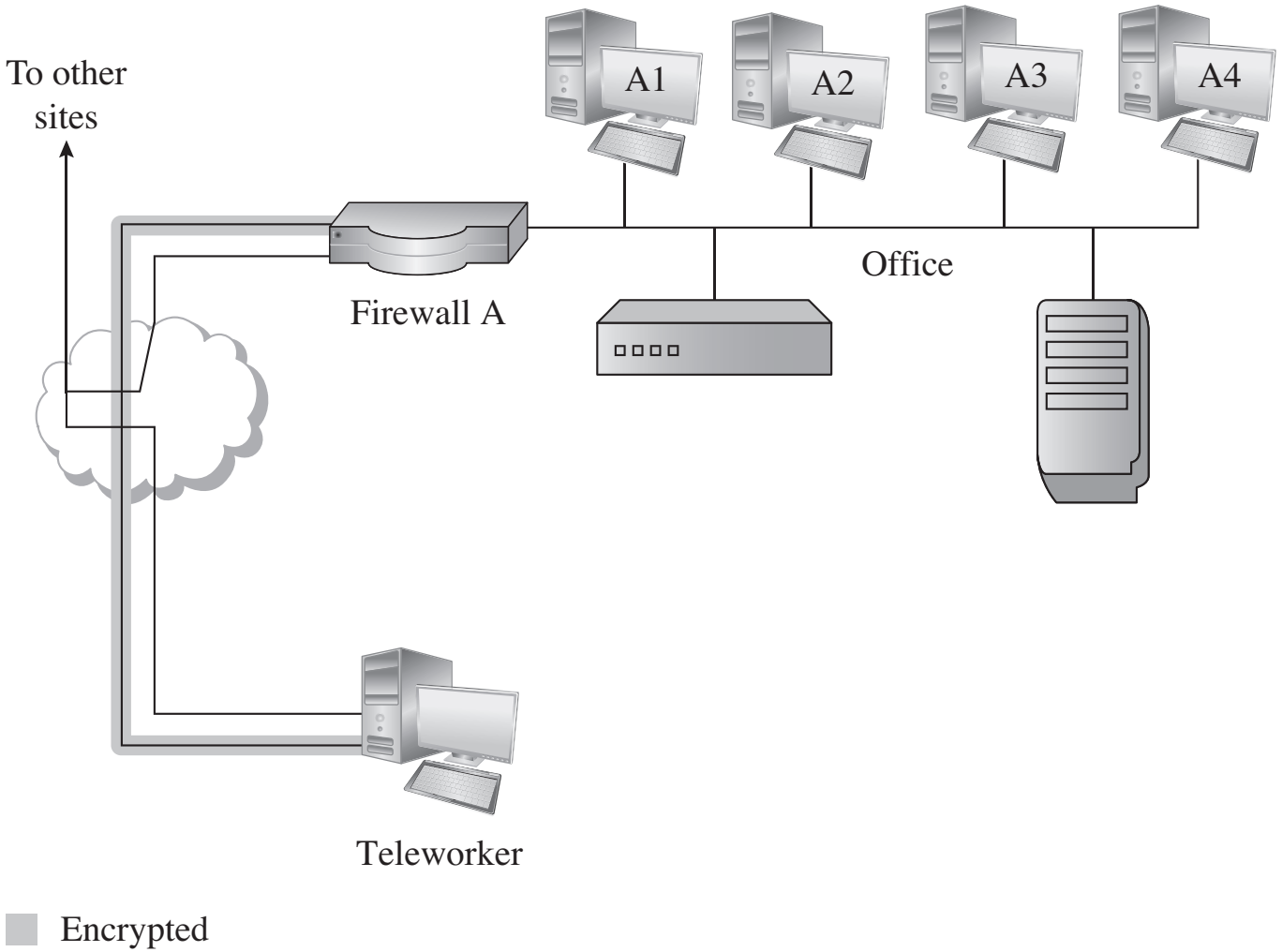


VPN (cont.) – Example 2

- 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



VPN (cont.) – Example 2



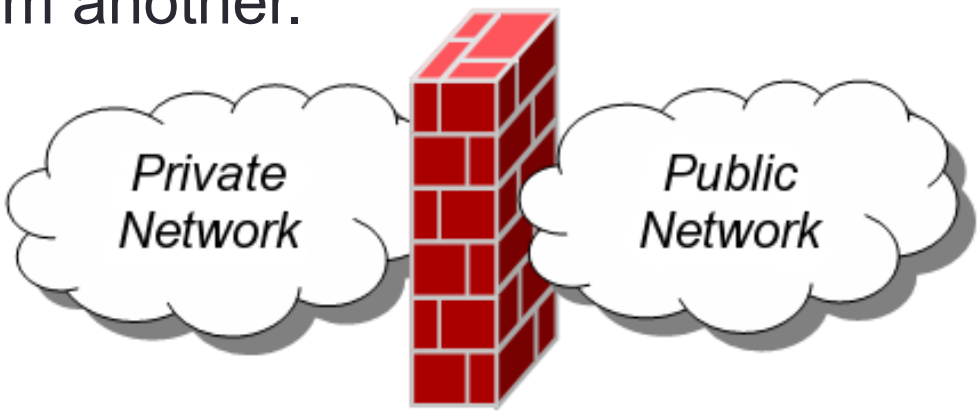
FIREWALLS

Firewalls

- What is a Firewall?

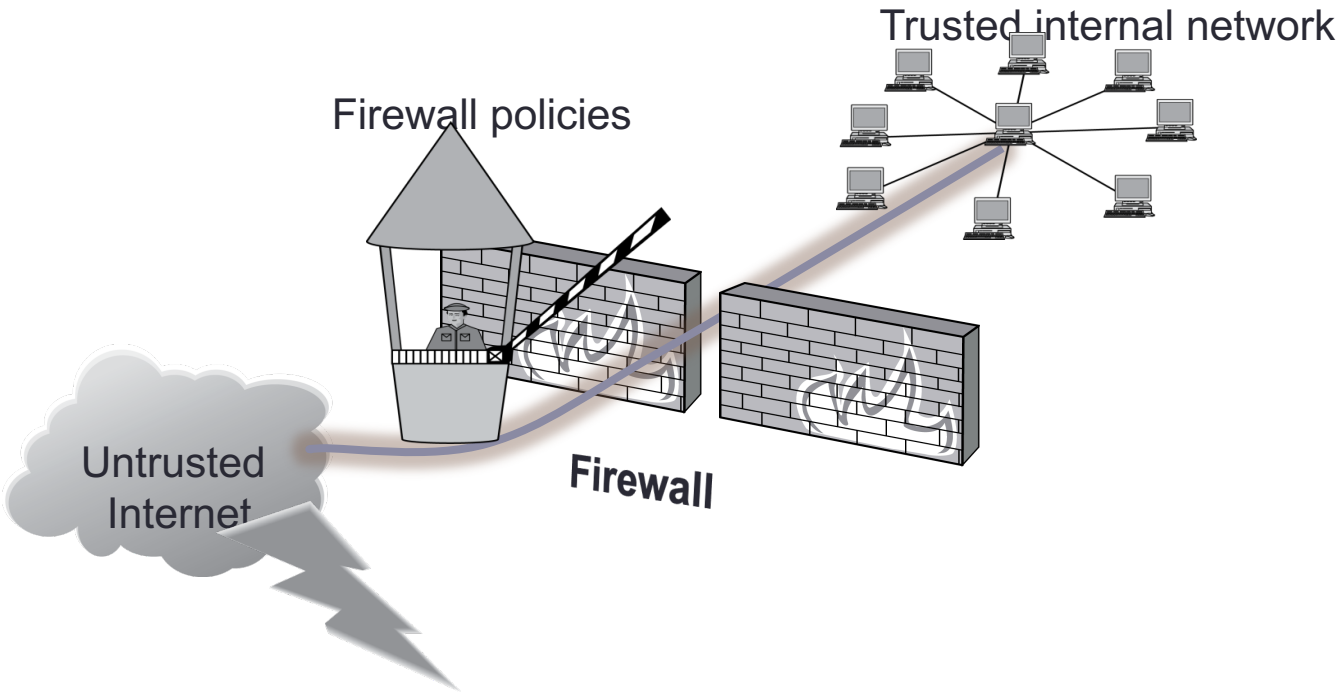
Firewalls

- 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
  - in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Policies

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



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

Policy Actions

- 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

Blacklisting and Whitelisting

- 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):

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
  - naïve from a security perspective - assumes the network administrator can enumerate all properties of malicious traffic.

Blacklists and White Lists

- **Whitelist** approach
  - A safer approach to defining a firewall ruleset is the default-deny policy
  - packets are dropped or rejected unless they are specifically allowed by the firewall.

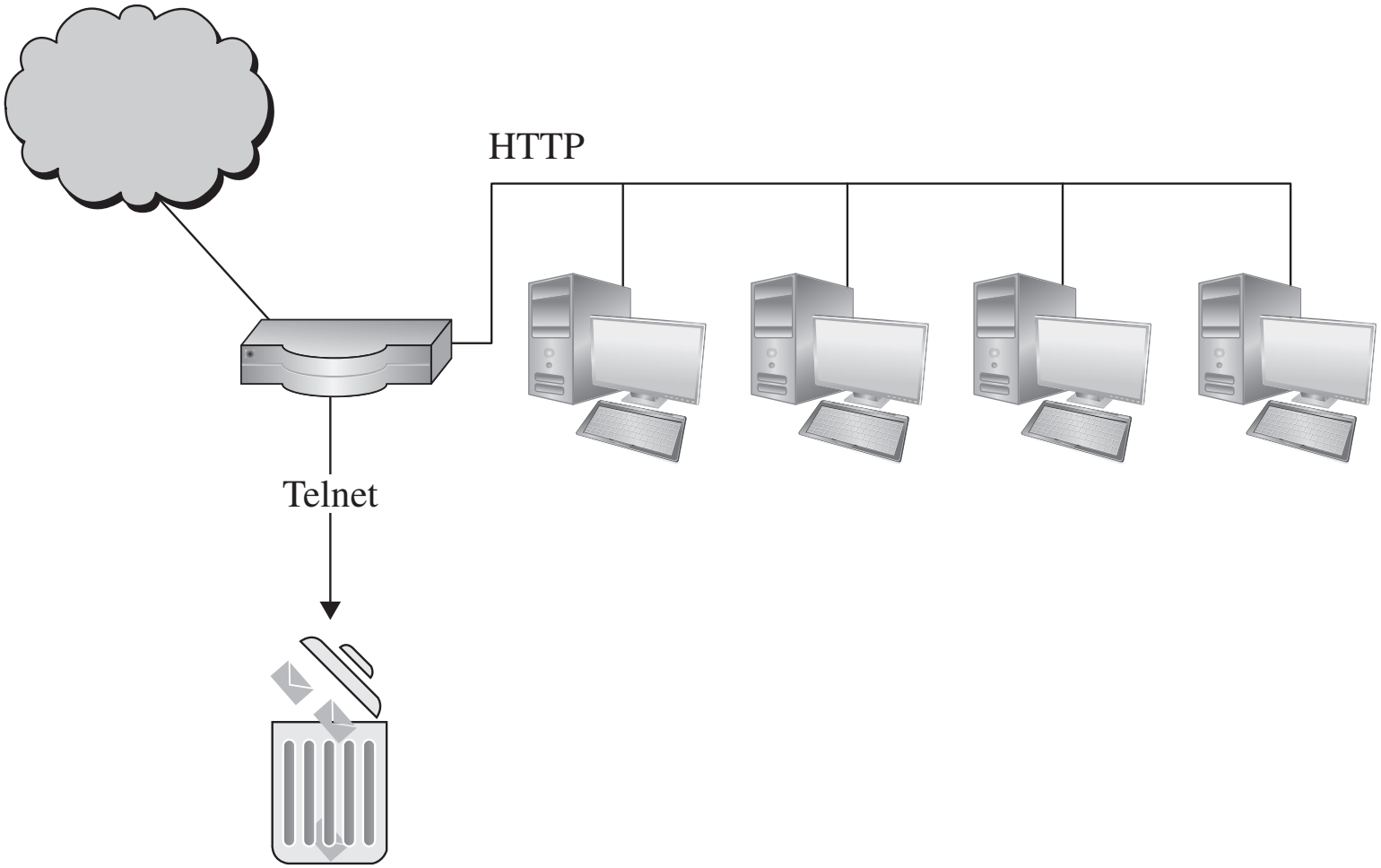
Types of Firewalls

- 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

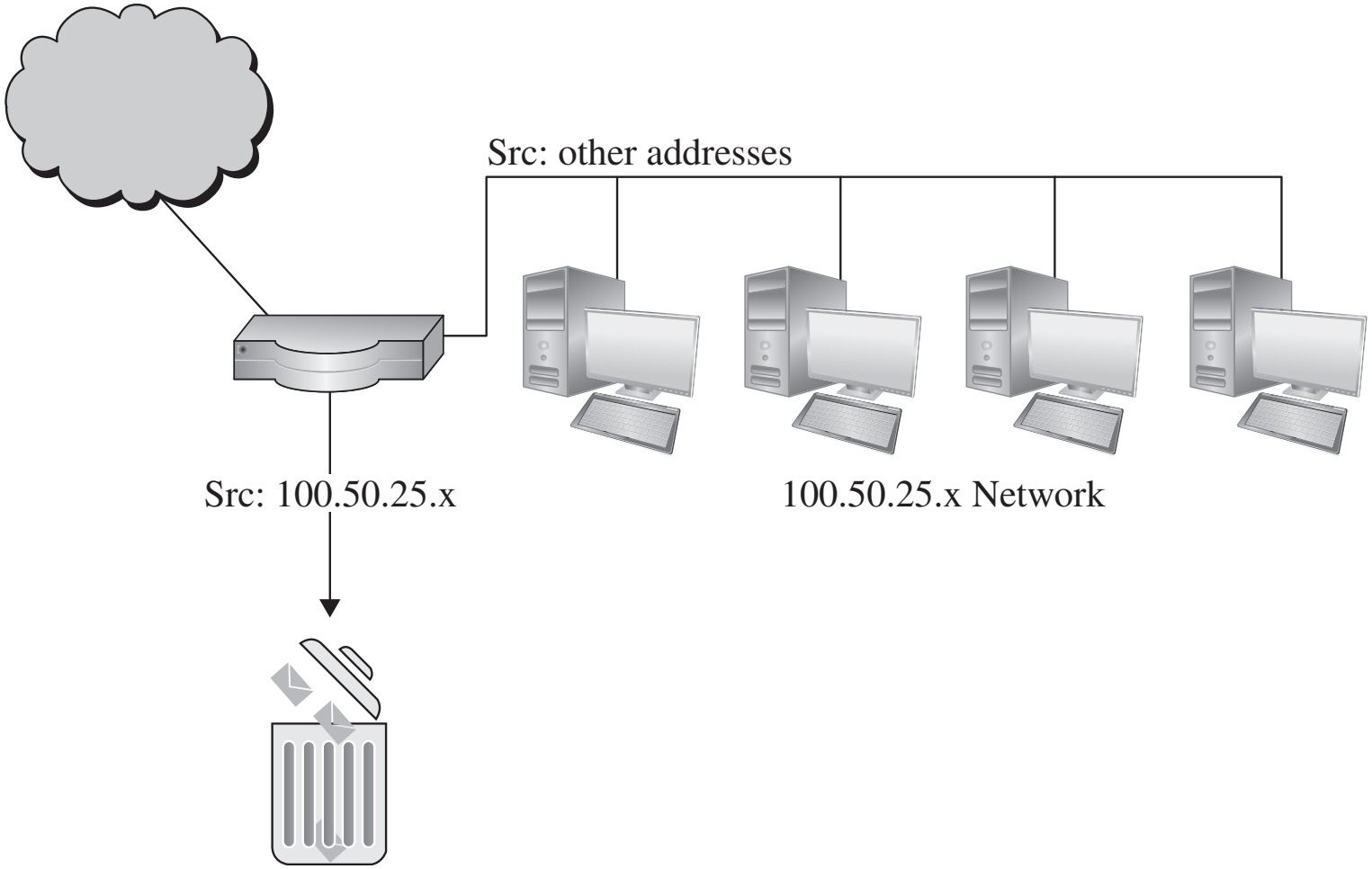
Packet-Filtering Gateways

- 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

Packet-Filtering Gateways

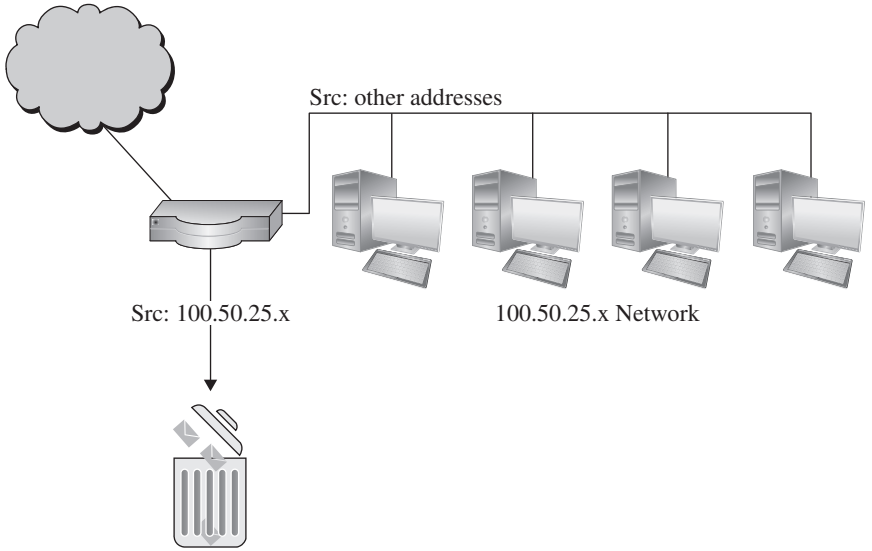


Packet-Filtering Gateways Example



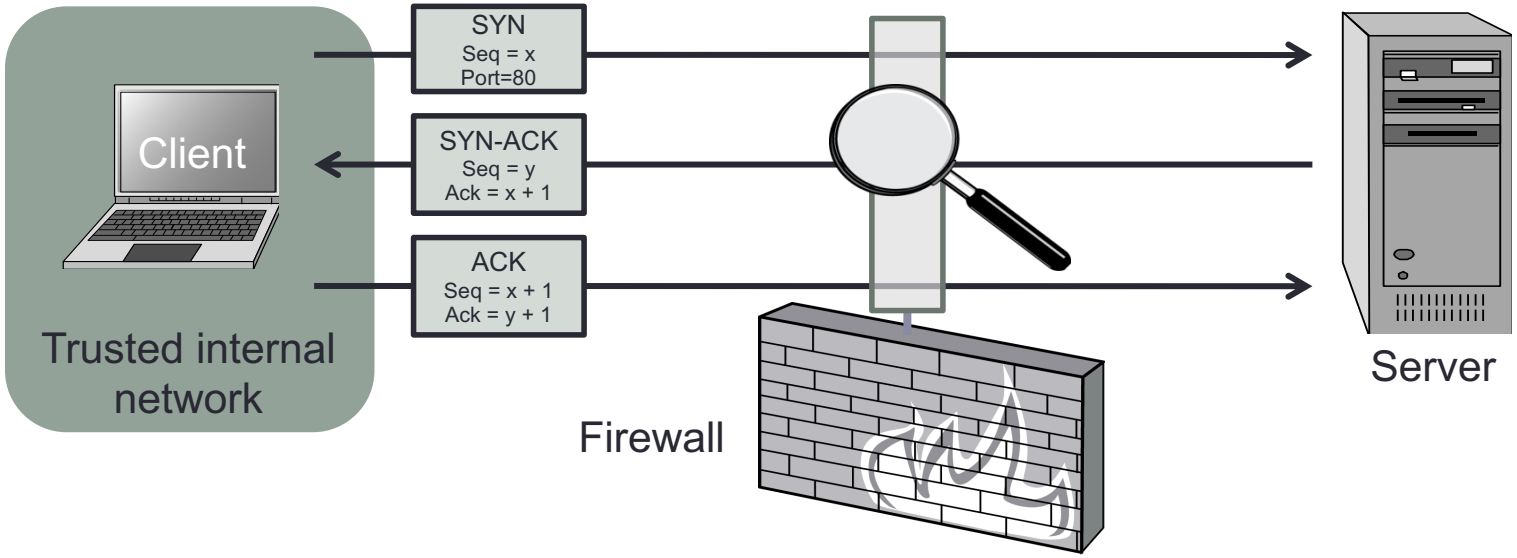
Packet-Filtering Gateways - Example

- 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



Packet-Filtering (Stateless) Gateways

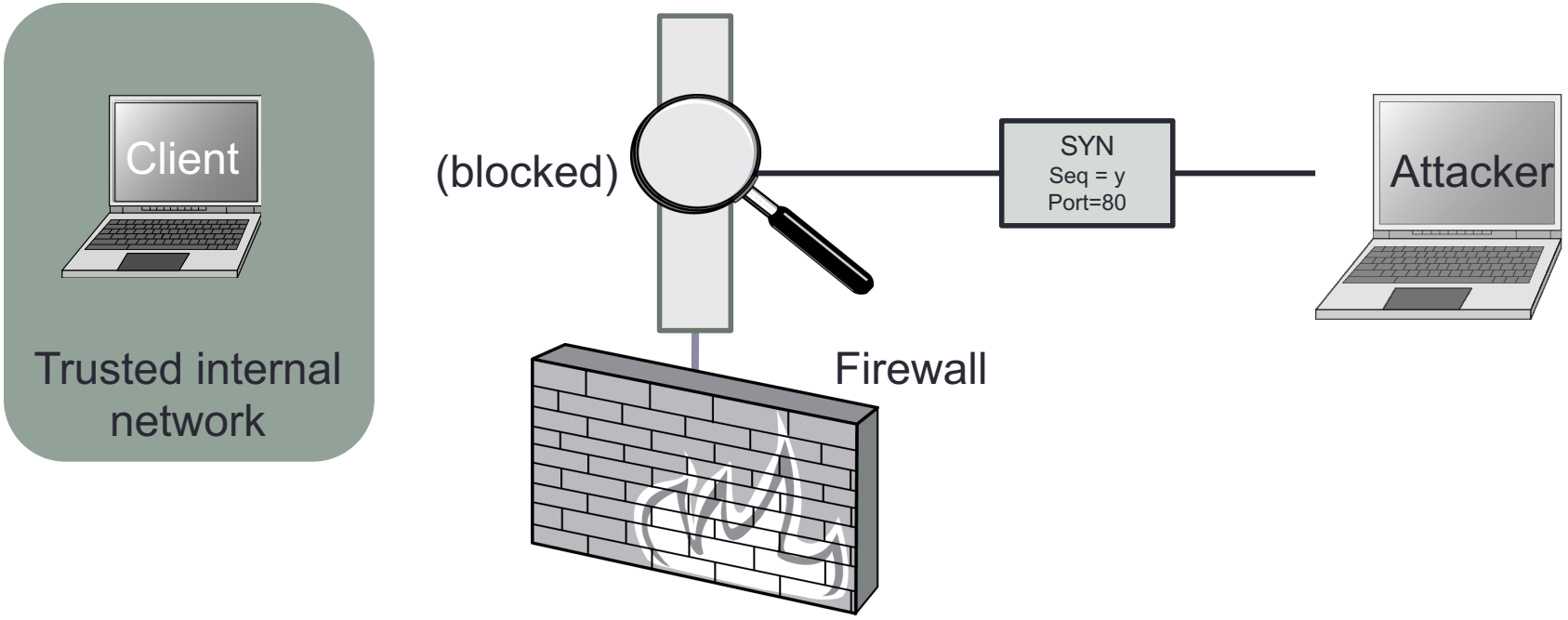
- A stateless firewall doesn't maintain any remembered context ("state") with respect to the packets it is processing
  - Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previousl.



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.

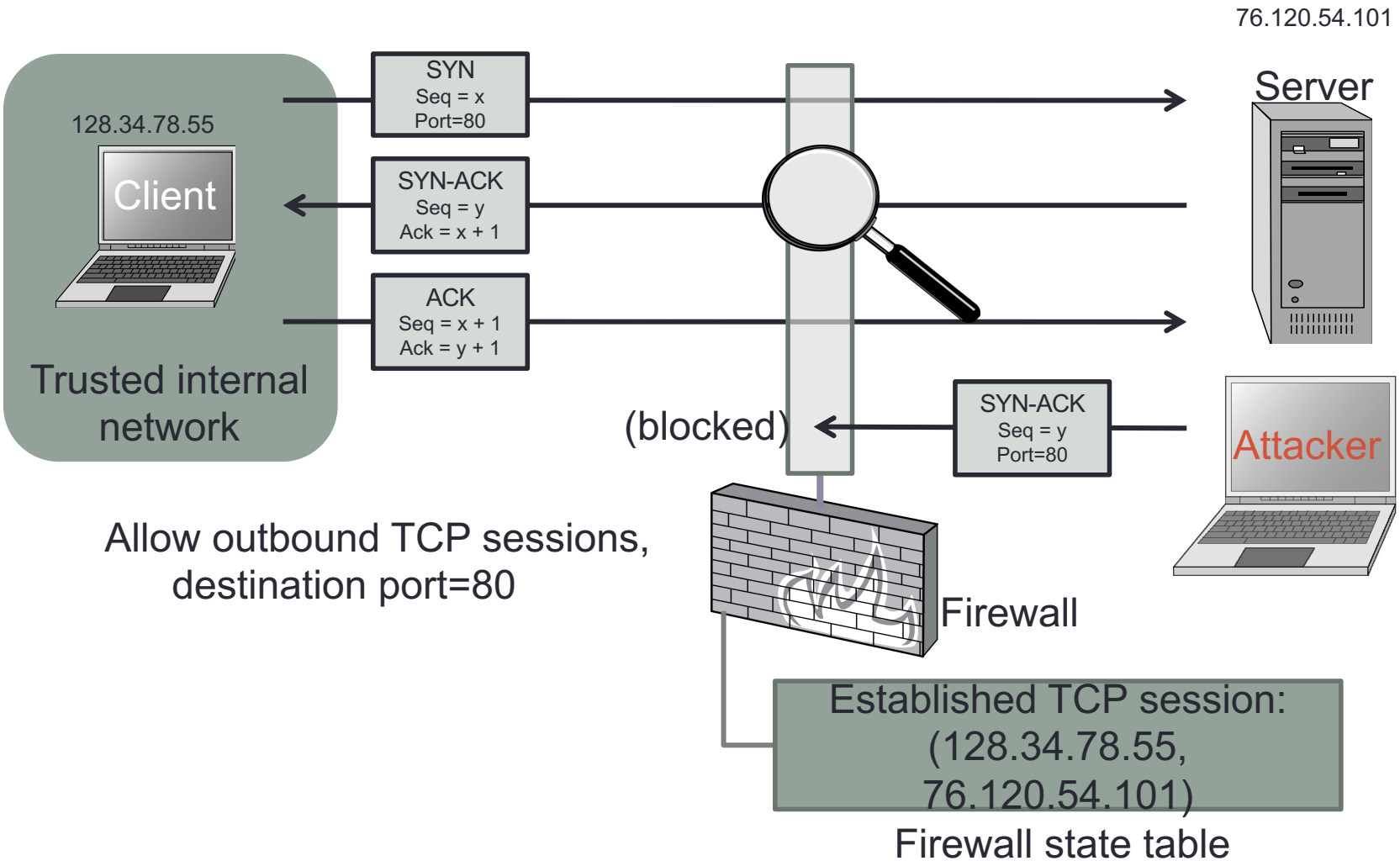
Statefull Firewalls

- **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.

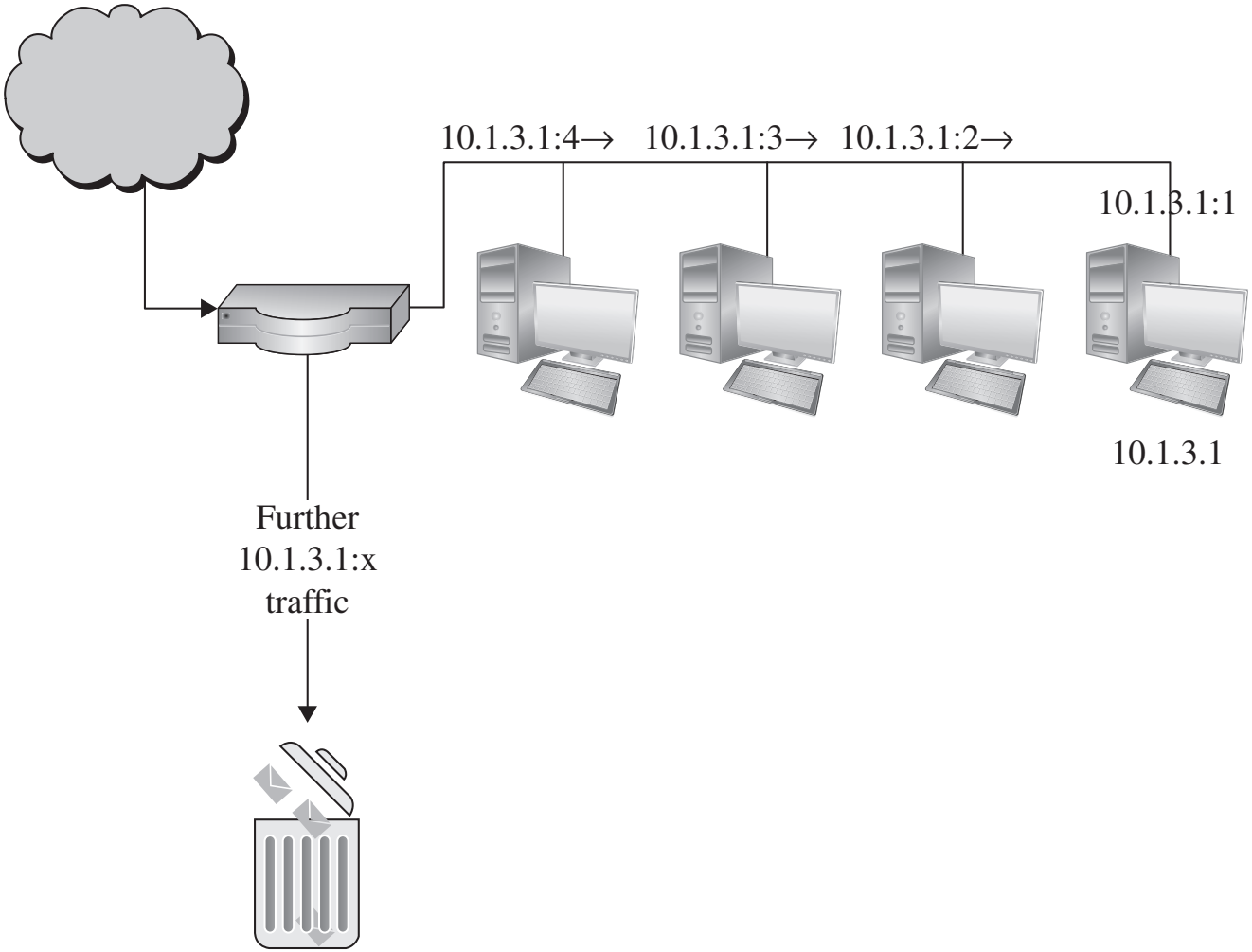
https://www.deciso.com/opnsense-tour/stateful-inspection-firewall/

Statefull Firewall Example

- Allow only requested TCP connections:

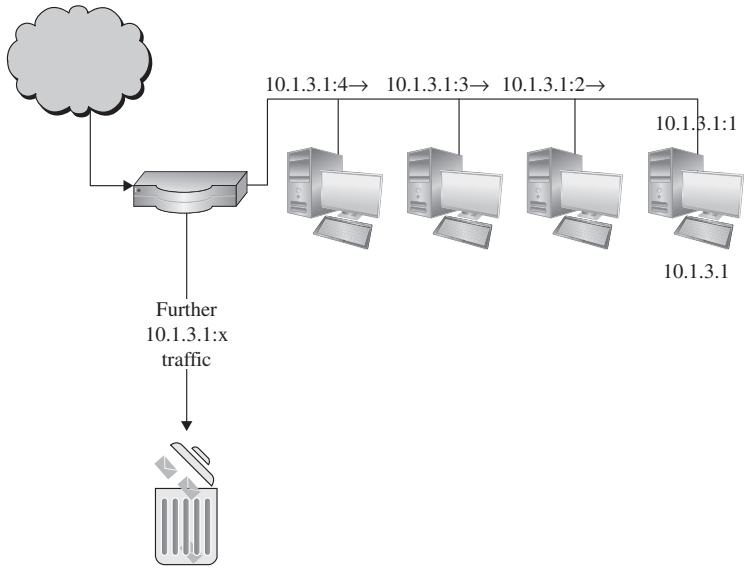


Stateful Inspection Firewall Example



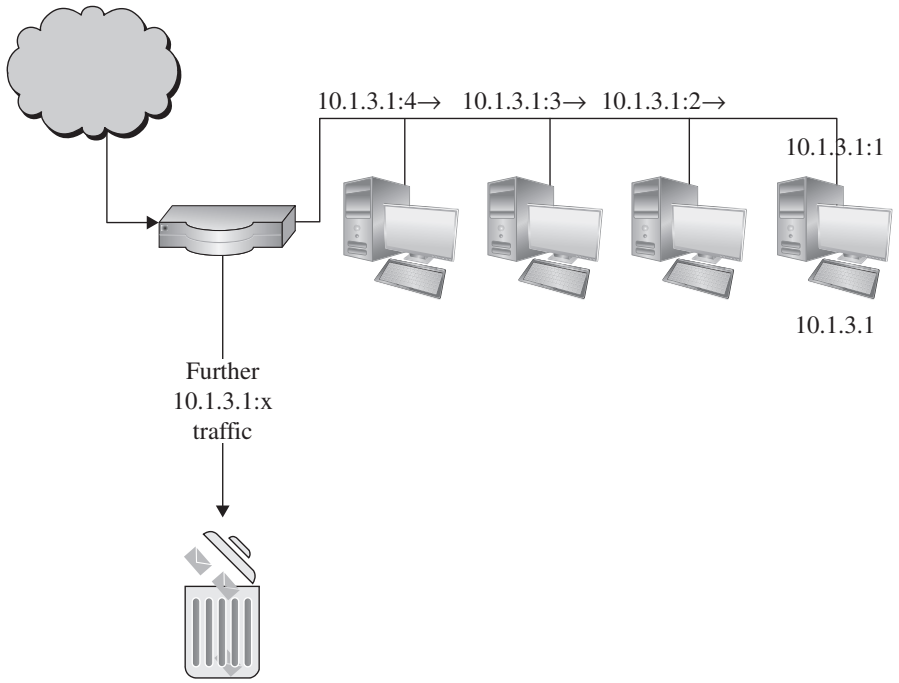
Stateful Inspection Firewall Example

- 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
  - begins filtering packets from that address.

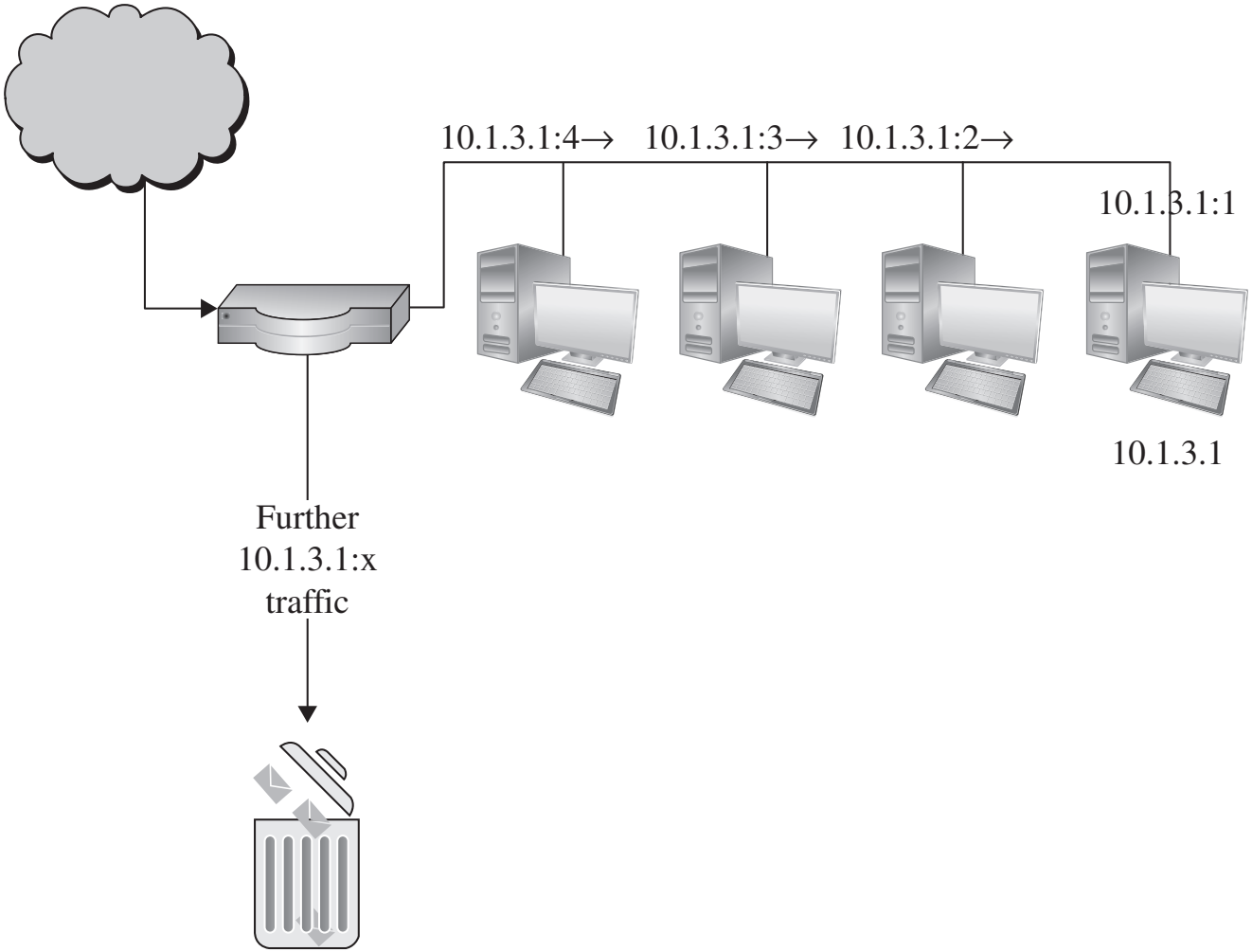


Stateful Inspection Firewall Example

- In real life, it can be difficult to define rules that require state/context and that attackers cannot circumvent



Stateful Inspection Firewall Example



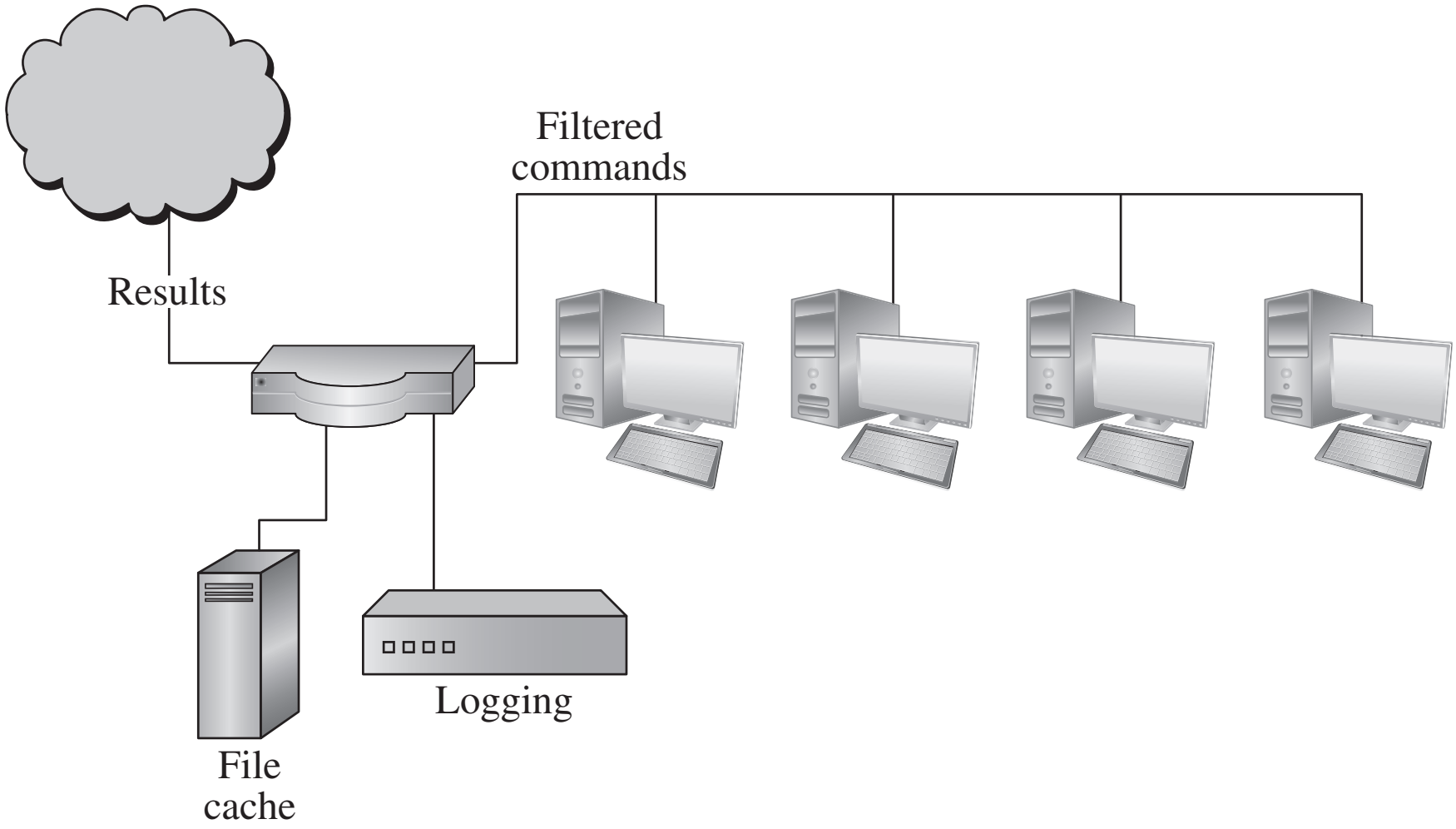
Application Layer Firewall

- 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, ...)

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

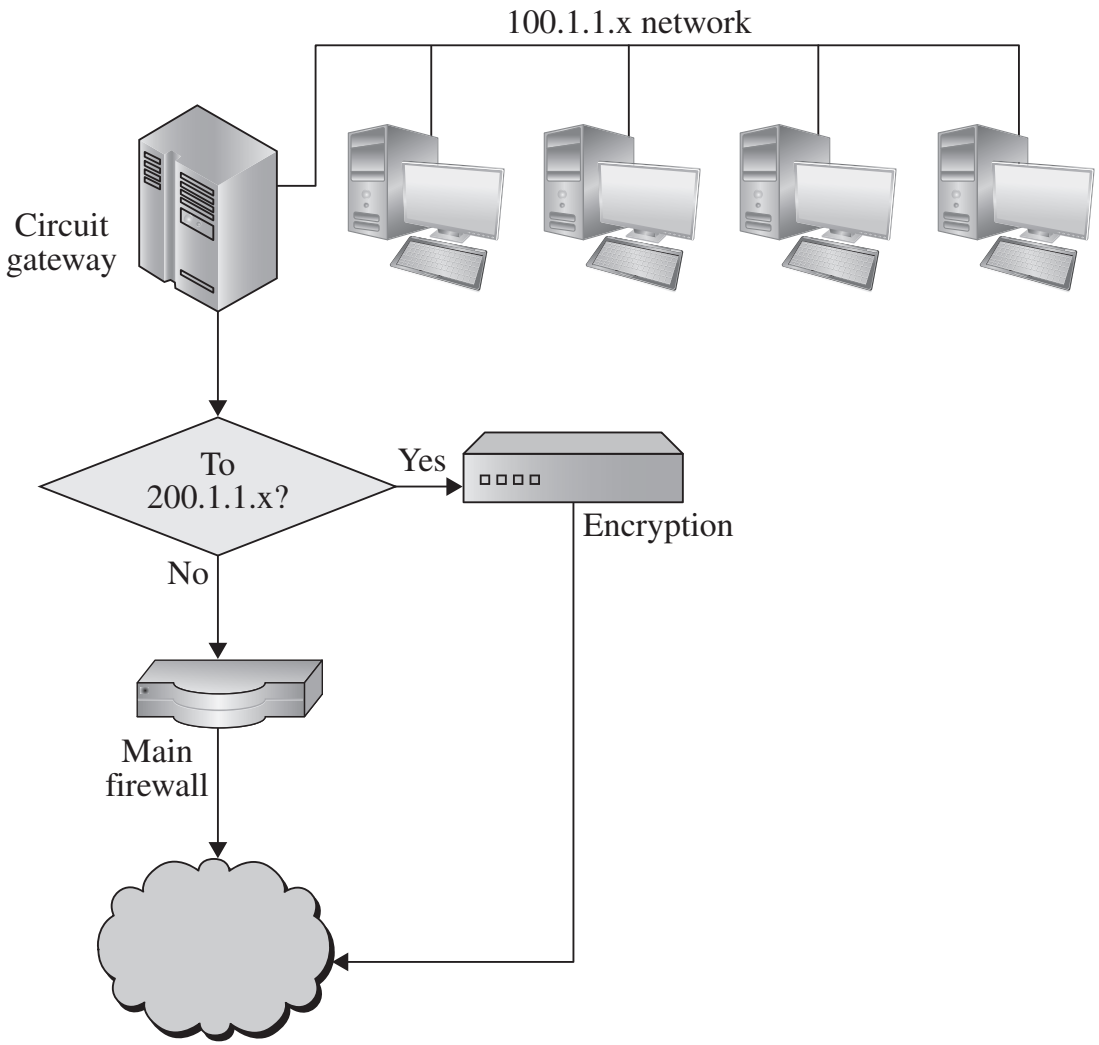
Application Proxy



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

Circuit-Level Gateway



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

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

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 port
- Can also restrict which applications are allowed to use the network.

Personal Firewalls

Personal Firewalls

- Example: Windows firewall configuration dialog
  - an administrator can select which protocols and applications should be allowed to communicate to and from the host

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

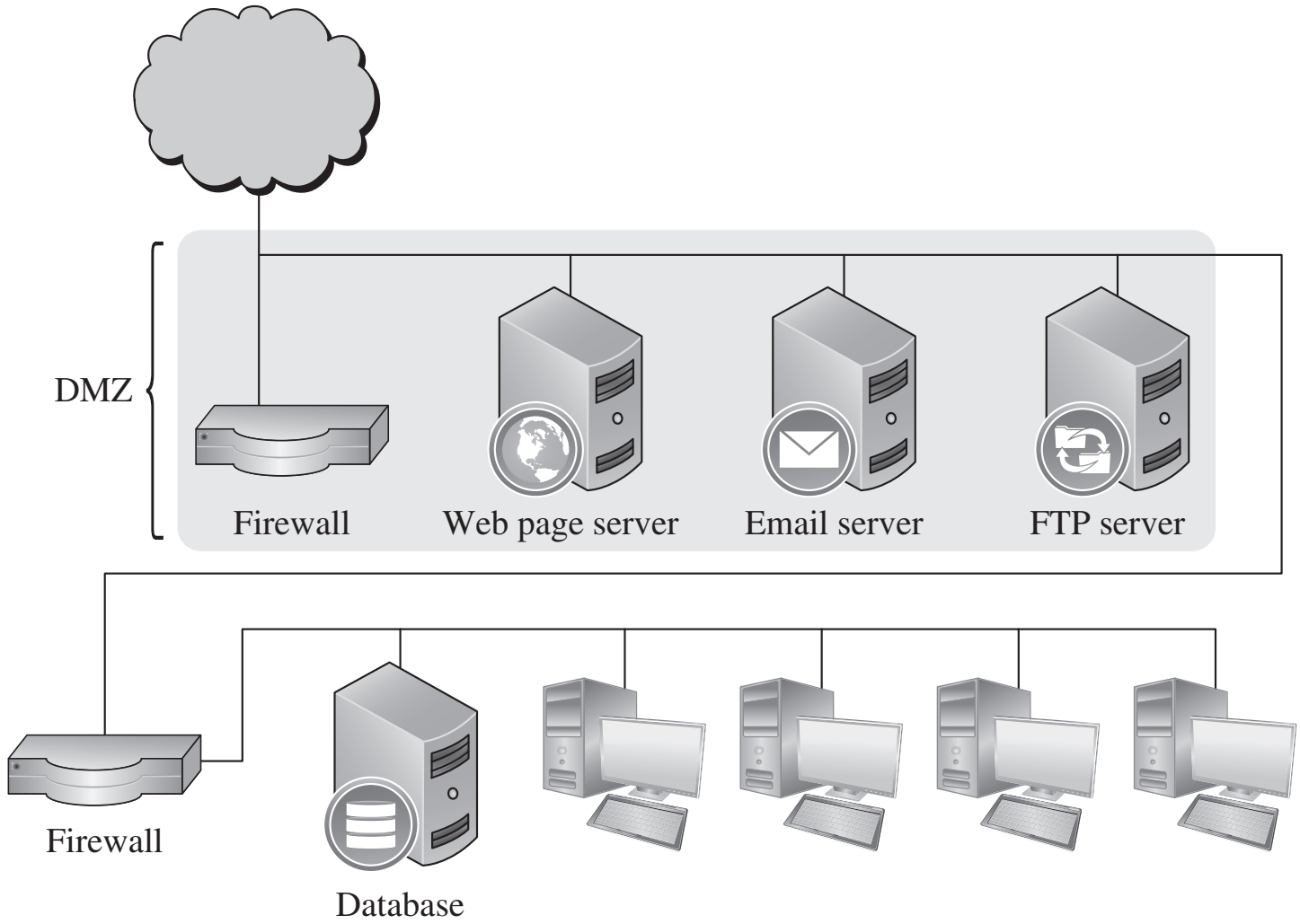
Firewalls – summary (cont.)

- 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

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

Demilitarized Zone (DMZ)

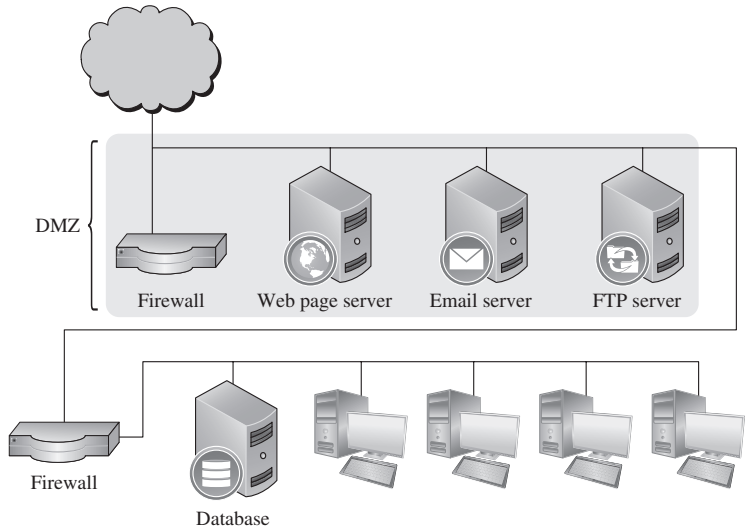


Demilitarized Zone (DMZ)

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

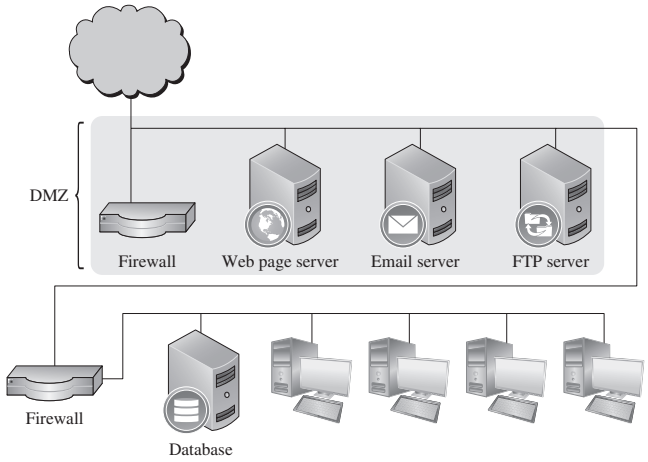
Demilitarized Zone (DMZ) Example

- 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 are typically the most at risk from outside attacks
- With DMZ, they 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



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
  - configuration must be updated as the environment changes,
  - firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion

What Firewalls Can and Cannot Do

- Firewalls exercise only minor control over the content admitted to the inside
  - inaccurate or malicious code must be controlled by means inside the perimeter

Network Address Translation (NAT)

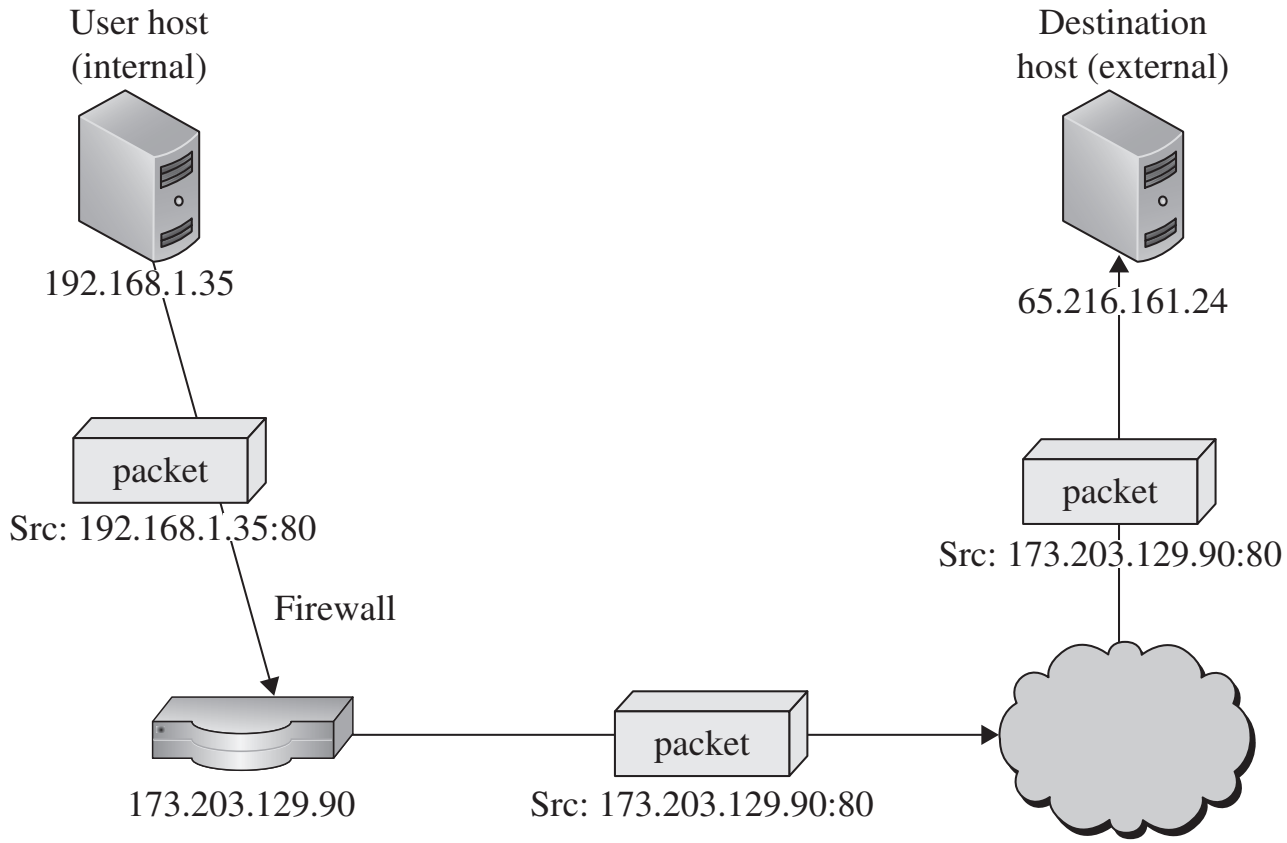


Table of translations performed	
Source	Dest
192.168.1.35:80	65.216.161.24:80

Network Address Translation (NAT)

- A process that can be used by firewalls to prevent IP addresses leakage
  - For example, if internal host sends it to external host it asks for a reply from

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

Data Loss Prevention (DLP)

- Approach similar to firewall or guard
- DLP is a set of technologies that can:
  - Detect (and possibly prevent) attempts to send sensitive data where it is not allowed to go

Data Loss Prevention (DLP)

- Can be implemented as
  - Agent installed as an OS rootkit
  - Network-based solutions
    - Monitor connections and file transfers
  - Applications specific
    - E.g., software for monitoring email
- Indicators DLP looks for:
  - Keywords
  - Traffic patterns
  - Encoding/encryption

Data Loss Prevention (DLP)

- DLP is best for preventing accidental incidents, as malicious users will often find ways to circumvent it

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

Intrusion Detection System

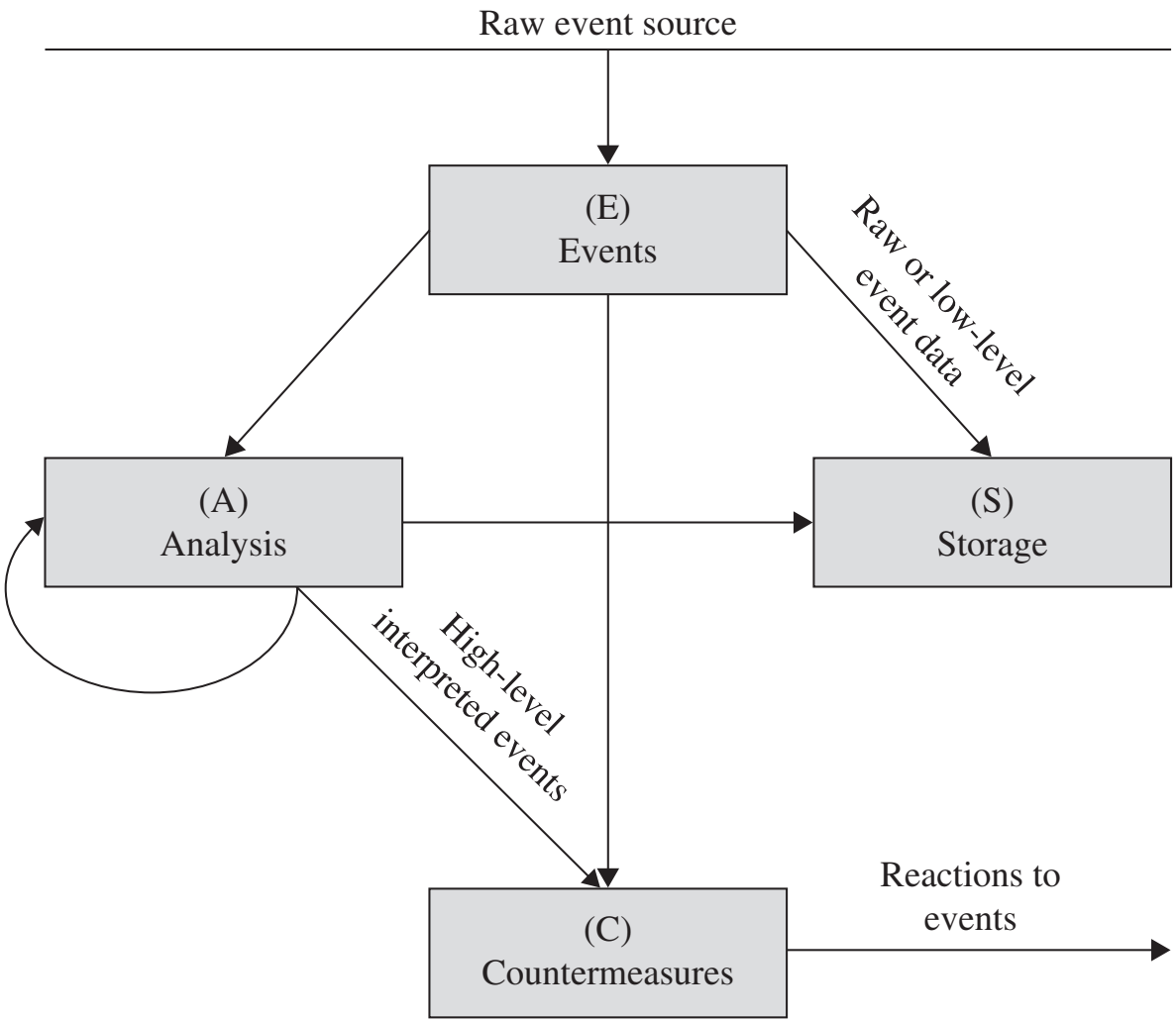
- Insiders require access with significant privileges to do their daily jobs
- Harm from insiders may not be malicious
  - it is honest people making honest mistakes
- However, potential malicious outsiders who have somehow passed the screens of firewalls and access controls exist
- Prevention, although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

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

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

Intrusion Detection Systems (IDS)



Intrusion Detection Systems (IDS)

- IDSs complement preventative controls as a next line of defense
  - 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

Types of IDS

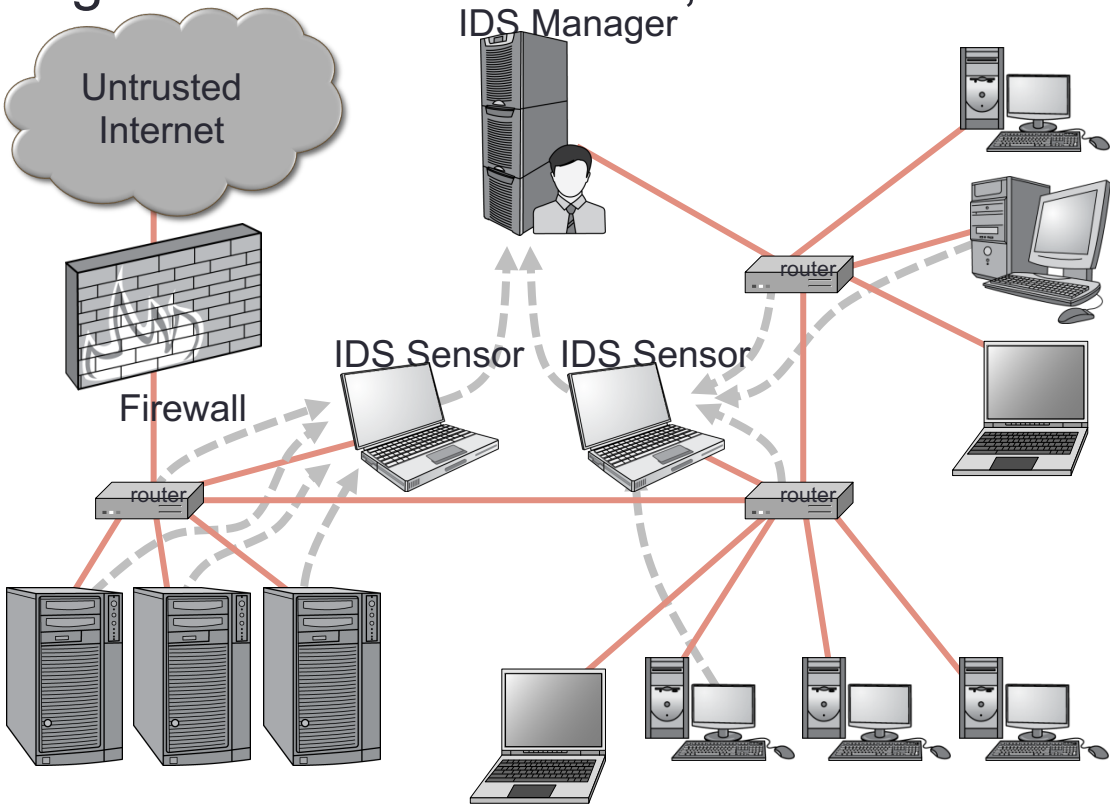
- Detection method
  - Signature-based
    - can only detect known patterns
  - Heuristic
    - for patterns of behavior that are out of the ordinary
- Location
  - Front end
    - looks at traffic as it enters the network
  - Internal
    - monitors traffic within the network

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

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

- Dorothy Denning identified several fields that should be included in IDS event records [1987]
  - 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

IDS Data

- Dorothy Denning identified several fields that should be included in IDS event records [1987] (cont.):
  - 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

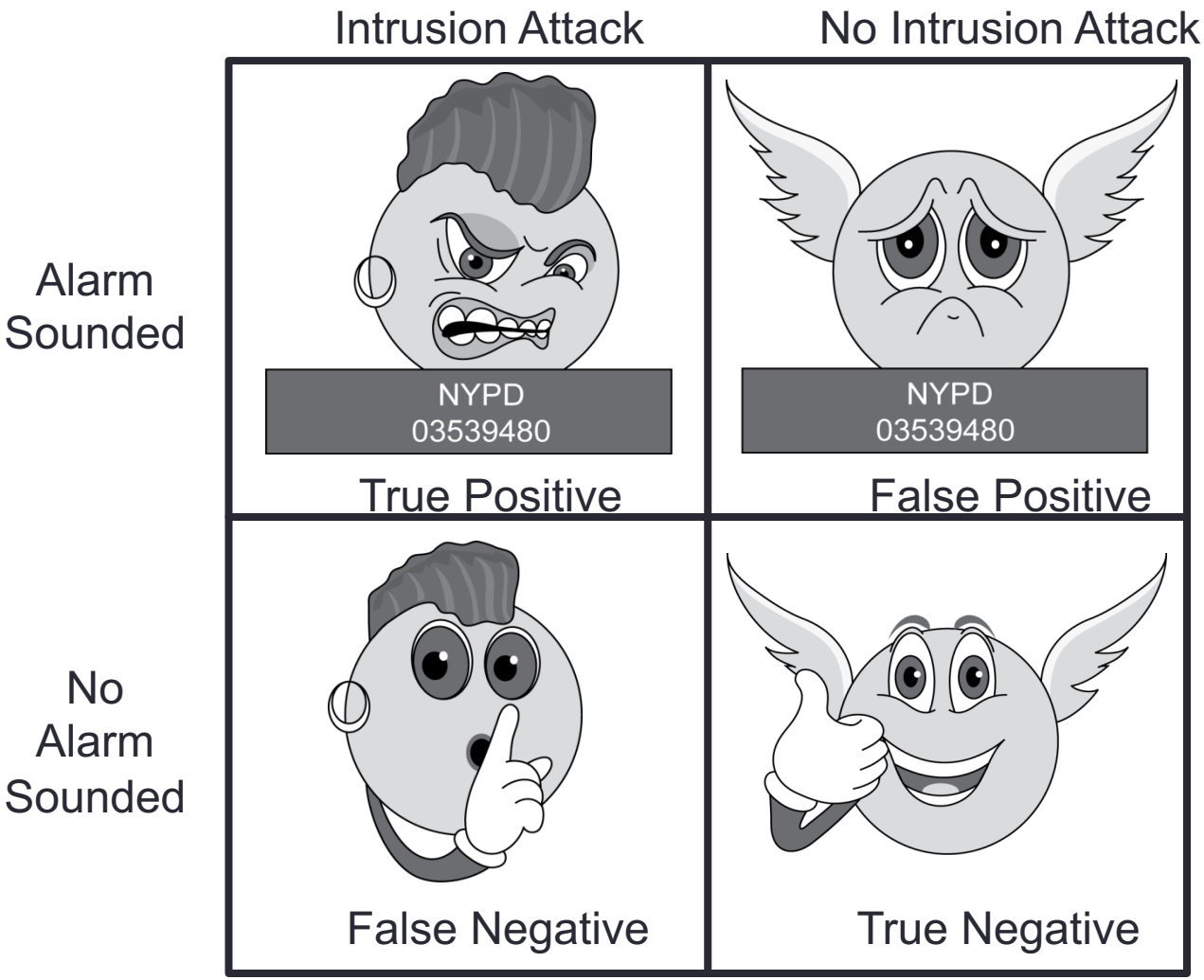
- An IDS is designed to detect a number of threats, including the following:
  - **masquerader:** an attacker who is falsely using the identity and/or credentials of a legitimate user
    - to gain access to a computer system or network
  - **Misfeasor:** a legitimate user who performs actions he is 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)



The Base-Rate Fallacy

- It is difficult to create an intrusion detection system with both a high true-positive rate and a low false-negative rate
  - Both are desirable properties
- If number of actual intrusions is relatively small compared to the amount of data being analyzed
  - => the effectiveness of an intrusion detection system can be reduced.

The Base-Rate Fallacy

- 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.

Base-Rate Fallacy Example

- Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious
  - => we have **1 false negative.**
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious
  - => 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.

IDS

- https://www.youtube.com/watch?v=EQyhoT-XgoE

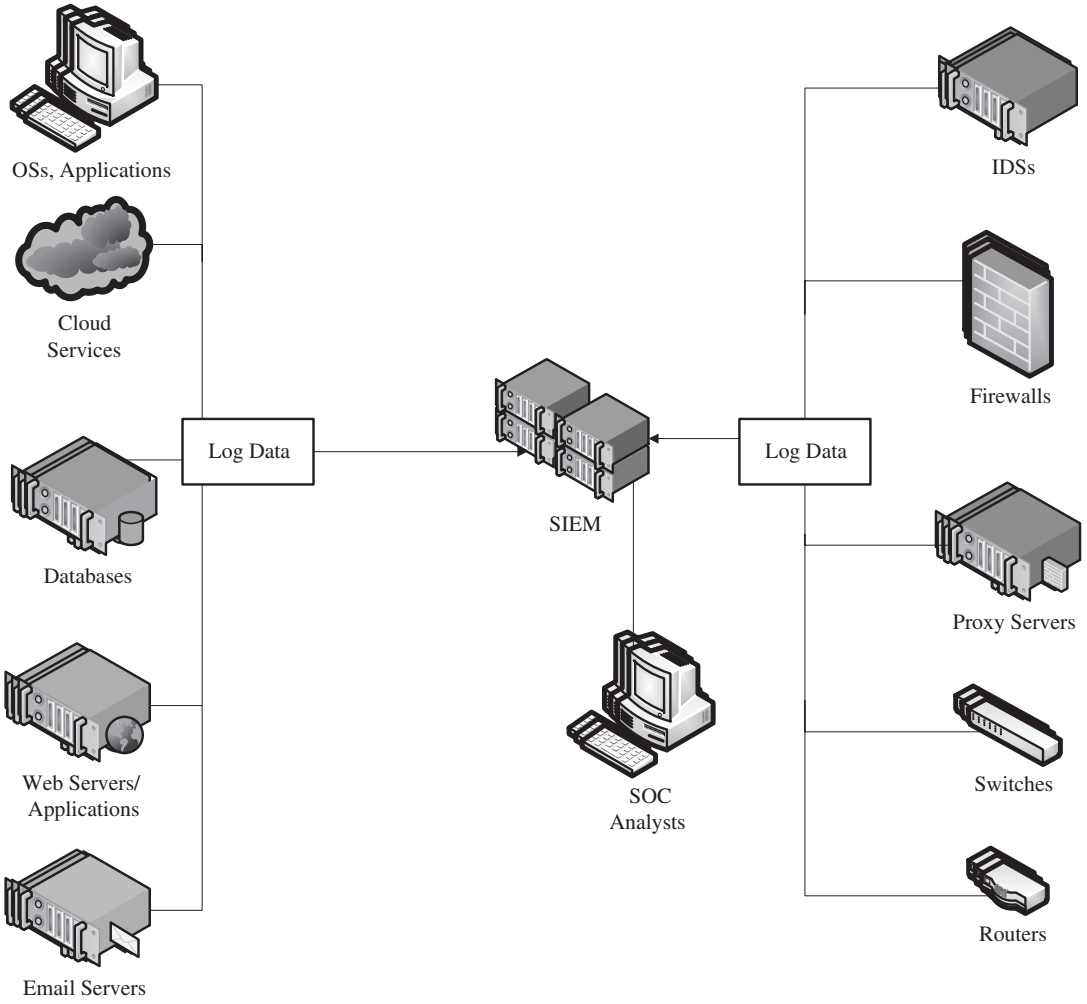
Security Information and Event Management (SIEM)

- SIEMs are software systems that collect security-relevant data from a variety of hardware and software products
  - usually audit logs
- 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

Security Information and Event Management (SIEM)

- https://www.youtube.com/watch?v=ZuLazPgFtBE

Security Information and Event Management (SIEM)



Security Information and Event Management (SIEM)

- Without an SIEM, analysts would need to:
  - log into each device individually on a constant basis
  - manually correlate events on one system against events on another
- This is impossible on any reasonably sized system.

Summary

- Networks are threatened by attacks aimed at interception, modification, fabrication, and interruption
- WPA2 has many critical security advantages over WEP
- Malicious DoS attacks 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

Summary

- 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 detects different kinds of attacks in very different parts of the network

- Questions?