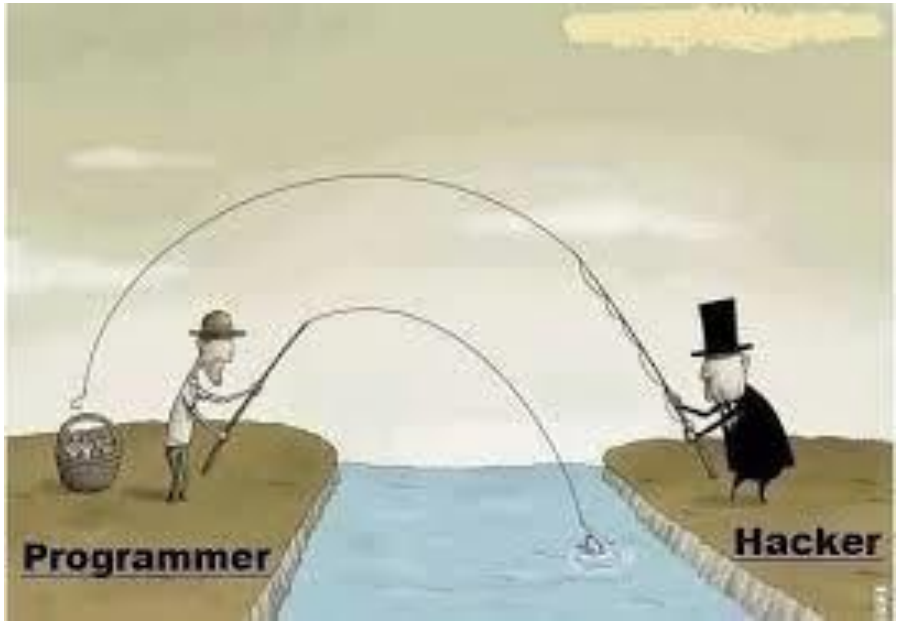
SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks



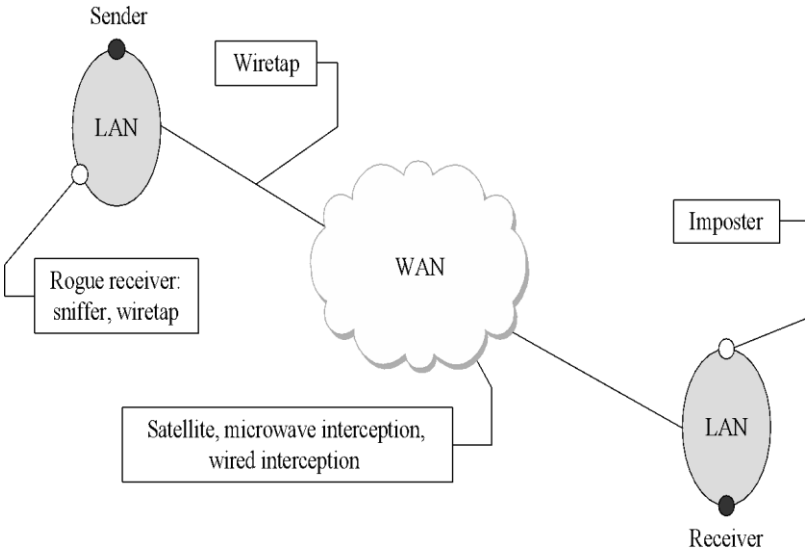
Network Transmission Media

There are vulnerabilities in each of these media.

The purpose of introducing them here is to understand that they all have different physical properties, and those properties will influence their susceptibility to different kinds of attack.

- Cable
- Optical fiber
- Microwave
- WiFi
- Satellite communication

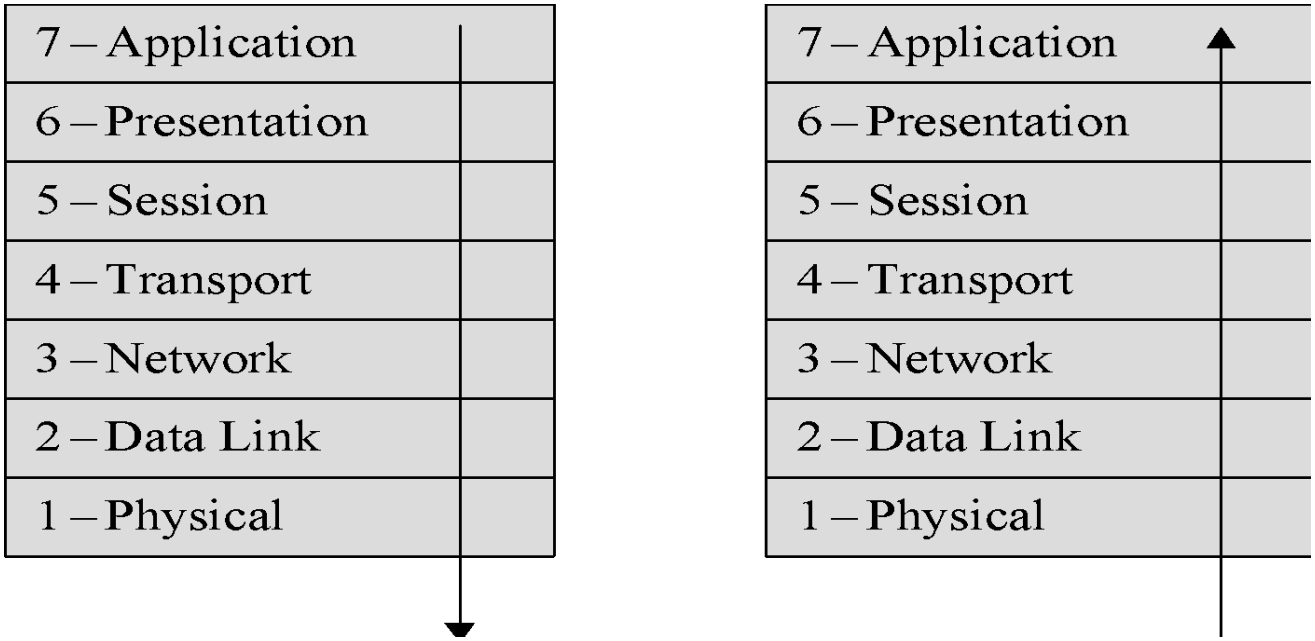
Communication Media Vulnerability



Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

Different touch points where attackers can take advantage of communication media: wiretaps, sniffers and rogue receivers, interception, and impersonation.

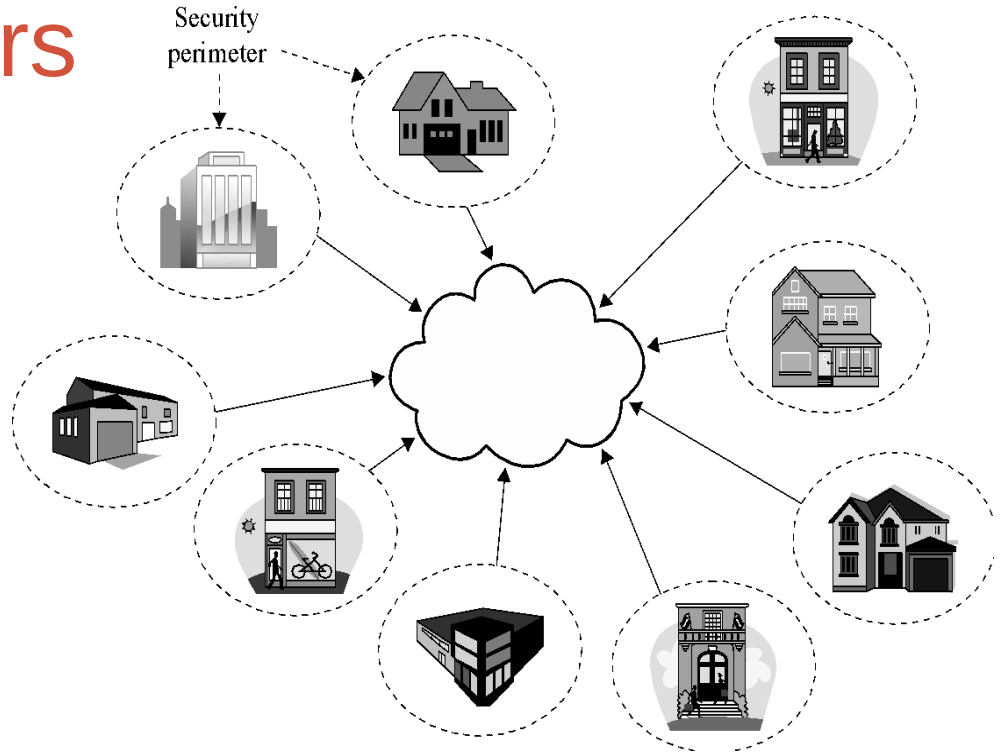
The OSI Model



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Security Perimeters



- Each of these places is a security perimeter in and of itself. Within each perimeter, you largely have control of your cables, devices, and computers because of physical controls, so you do not need to worry as much about protection.
- However, to do anything useful, you have to make connections between security perimeters, which exposes you to all sort of cables, devices, and computers you can't control.
- Encryption is the most common and useful control for addressing this threat.

What Makes a Network Vulnerable to Interception?

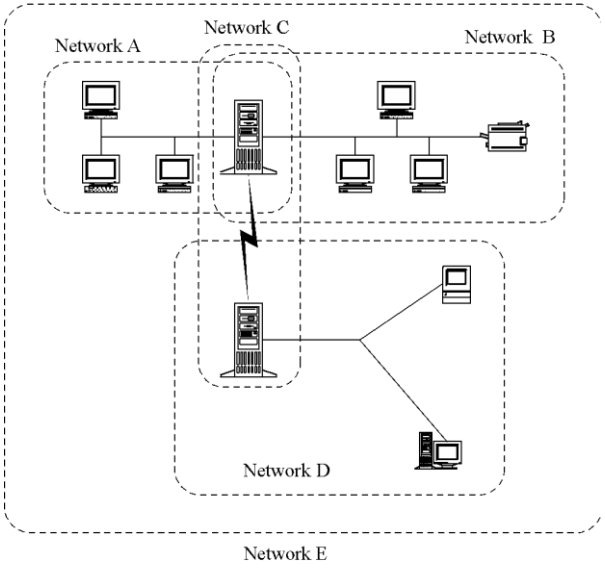
- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers
- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter (next slide)
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path (next slide)
  - There may be many paths, including untrustworthy ones, from one host to another

Network Perimeter

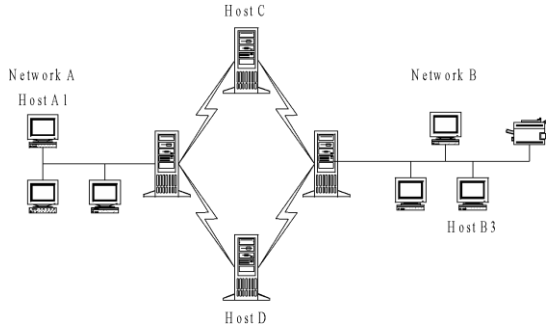
A network perimeter is the secured boundary between the private & locally managed side of a network. A network perimeter includes:

- **Border Routers:** Routers serve as the traffic signs of networks. They direct traffic into, out of, and throughout networks. The border router is the final router under the control of an organization before traffic appears on an untrusted network, such as the Internet.
- **Firewalls**: A firewall is a device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic.
- **Intrusion Detection System (IDS):** This functions as an alarm system for your network that is used to detect and alert on suspicious activity. This system can be built from a single device or a collection of sensors placed at strategic points in a network.
- **Intrusion Prevention System (IPS):** Compared to a traditional IDS which simply notifies administrators of possible threats, an IPS can attempt to automatically defend the target without the administrator's direct intervention.
- **De-Militarized Zones / Screened Subnets:** DMZ and screened subnet refer to small networks containing public services connected directly to and offered protection by firewall or other filtering device.

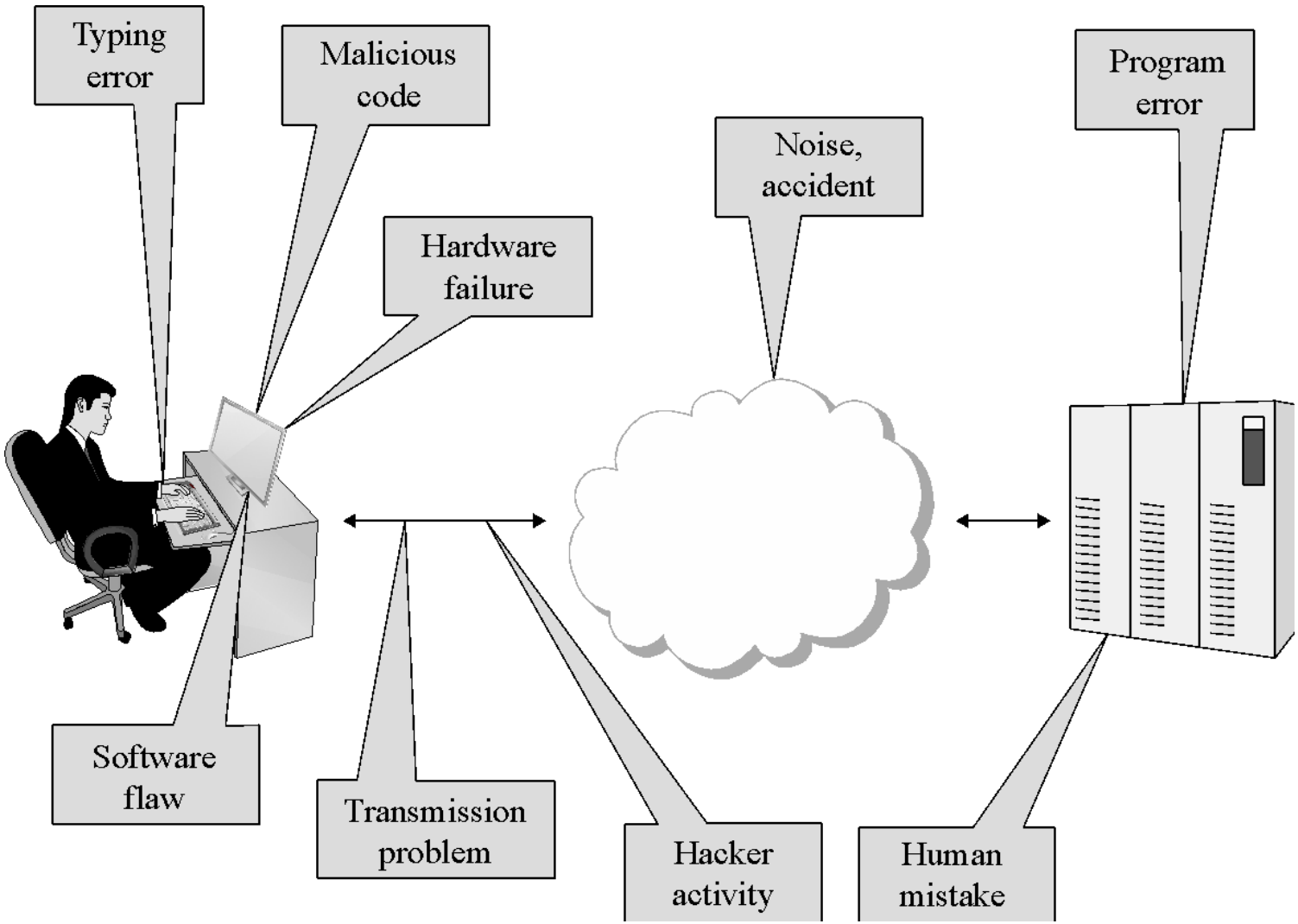
Unknown Perimeter



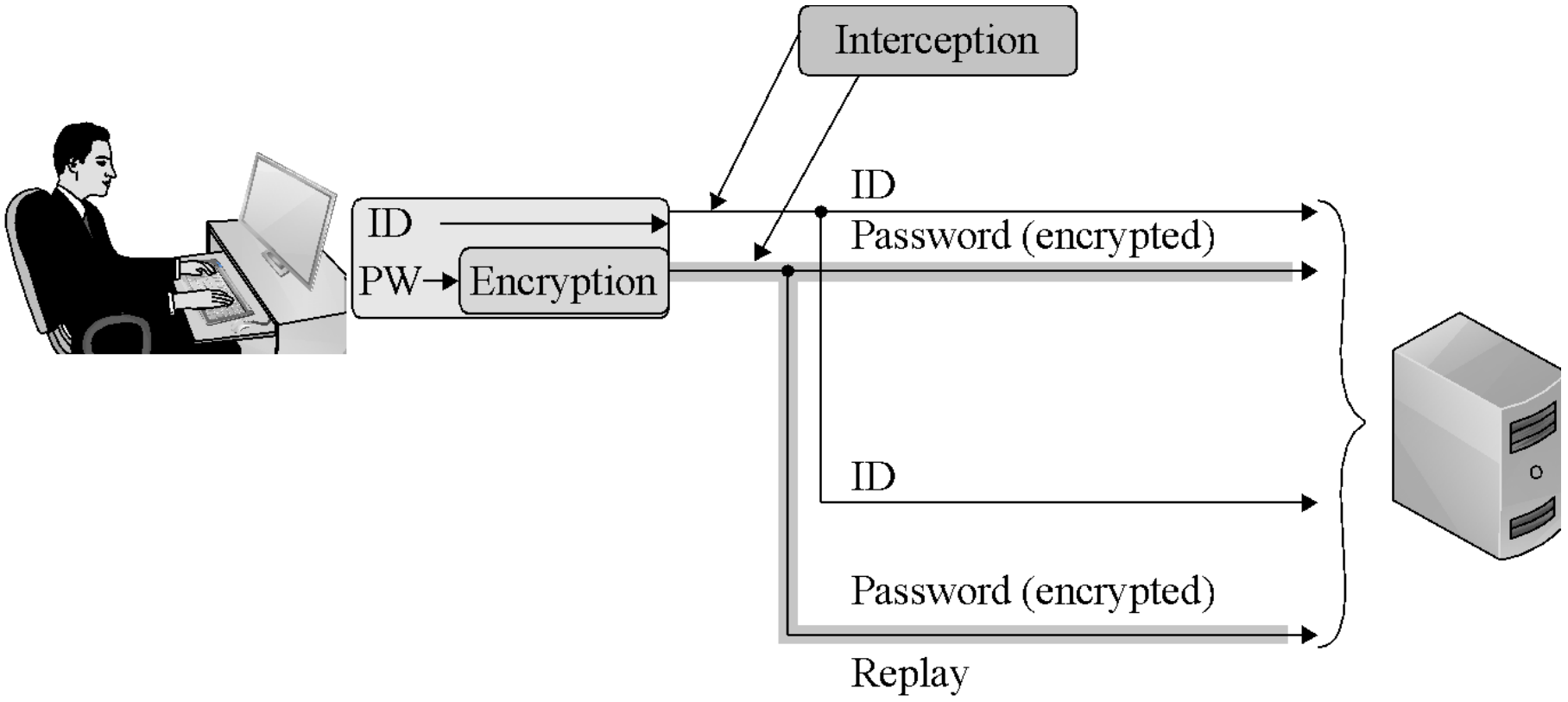
Unknown Path



Sources of Data Corruption



Simple Replay Attack



Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port       State      Service  Reason       Product  Version  Extra info
21   tcp   open       ftp      syn-ack      ProFTPD  1.3.1
22   tcp   filtered   ssh      no-response
25   tcp   filtered   smtp     no-response
80   tcp   open       http     syn-ack      Apache   2.2.3    (CentOS)
106  tcp   open       pop3pw   syn-ack      poppassd
110  tcp   open       pop3     syn-ack      Courier pop3d
111  tcp   filtered   rpcbind  no-response
113  tcp   filtered   auth     no-response
143  tcp   open        imap     syn-ack      Courier Imapd       released
2004
443  tcp   open       http     syn-ack      Apache  2.2.3       (CentOS)
465  tcp   open       unknown  syn-ack
646  tcp   filtered   ldp      no-response
993  tcp   open       imap     syn-ack      Courier Imapd       released
2004
995  tcp   open                syn-ack
2049 tcp   filtered   nfs      no-response
3306 tcp   open       mysql    syn-ack      MySQL   5.0.45
8443 tcp   open       unknown  syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Port scanning can best be described as a reconnaissance—and as such doesn't fit cleanly into the category of attack, threat, or vulnerability.

However….note the kind of data that is available: port, protocol, state, service, product, and version.

Vulnerabilities in Wireless Networks

- Confidentiality—Every message in WiFi is a broadcast, unencrypted messages can be read by anyone who's listening and within range
- Integrity—When WiFi access points receive two streams of communication claiming to be the same computer, they necessarily accept the one with greater signal strength. This allows attackers to take over and forge sessions by spoofing legitimate computers and boosting signal strength.
- Availability—In addition to the obvious availability issues, WiFi creates new availability problems, such as session hijacking, forced disassociation, and jamming.
- Unauthorized WiFi access—Some form of cryptographic control is necessary to address this
- Picking up the beacon—Hidden SSIDs can easily be discovered by monitoring client requests for SSIDs in the absence of SSID beacons from the access point
- SSID in all frames—Similar to picking up the beacon, once a client connects to an access point, the SSID is stored in all communication frames and can be sniffed that way
- Association issues—WiFi clients generally have preferred associations—networks they know and trust to connect to automatically—and these may include very common SSID names, such as AT&Twifi and Apple. Without additional security measures, attackers can spoof these trusted SSIDs and trick devices into connecting to rogue access points.

WEP

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- More weaknesses were discovered over the course of years, until any WEP-encrypted communication could be cracked in a matter of minutes

How it works:

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client, which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it’s the same number to authenticate the client
- Once the client is authenticated, the AP and client communicate using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV), thus reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in and were therefore vulnerable to dictionary attacks
- Static key
  - Since the key was just a value the user typed in at the client and AP, and since users rarely changed those keys, one key would be used for many months of communications
- Weak encryption process
  - A 40-bit key can be brute forced easily. Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well
- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign), which resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
  - There were only 16 million possible values of IV, which, in practice, is not that many to cycle through for cracking. Also, they were not as randomly selected as they should have been, with some values being much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed in 2003 as a replacement for WEP, followed in 2004 by WPA2, algorithm remains standard today

- Non-static encryption key
  - WPA uses a hierarchy of keys: New keys are generated for confidentiality and integrity of each session, and the encryption key is automatically changed on each packet
  - This way, the keys that are most important are used in very few places and indirect ways, protecting them from disclosure

- Authentication
  - WPA allows authentication by password, token, or certificate

WPA2 is adequately secure if configured well: Choose a strong encryption algorithm (AES without TKIP), and use a long, random passphrase.

- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm

- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check

- Session initiation
  - WPA sessions begin with authentication and a four-way handshake that results in separate keys for encryption and integrity on both ends

While there are some attacks against WPA, they are either of very limited effectiveness or require weak passwords

Denial of Service (DoS)

DoS attacks are attempts to defeat a system's availability:

- Volumetric attacks
- Application-based attacks
- Disabled communications
- Hardware or software failure

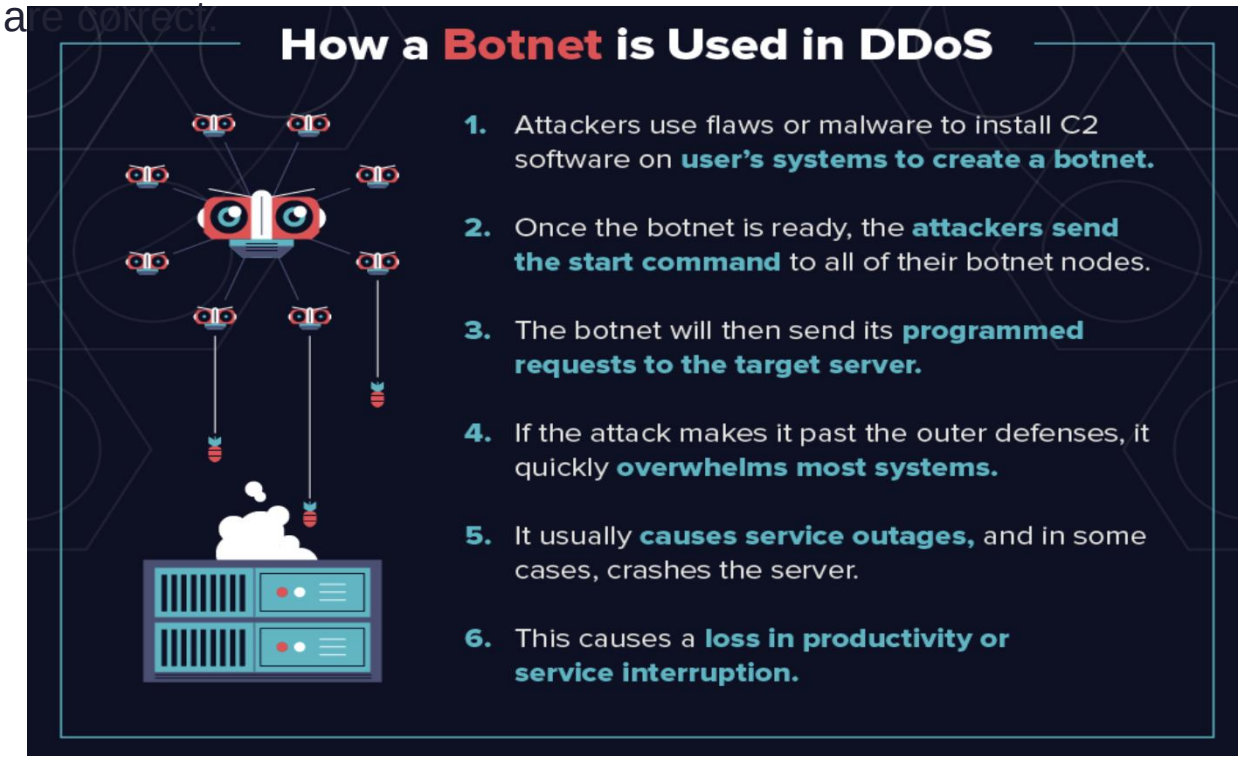
DDoS attacks most often work by botnets – a large group of distributed computers that act in concert with each other –simultaneously spamming a website or service provider with data requests.

Attackers use malware or unpatched vulnerabilities to install Command and Control (C2) software on user's systems to create a botnet. DDoS attacks rely on a high number of computers in the botnet to achieve the goal, & the cheapest way to get control of that many machines is by leveraging exploits.

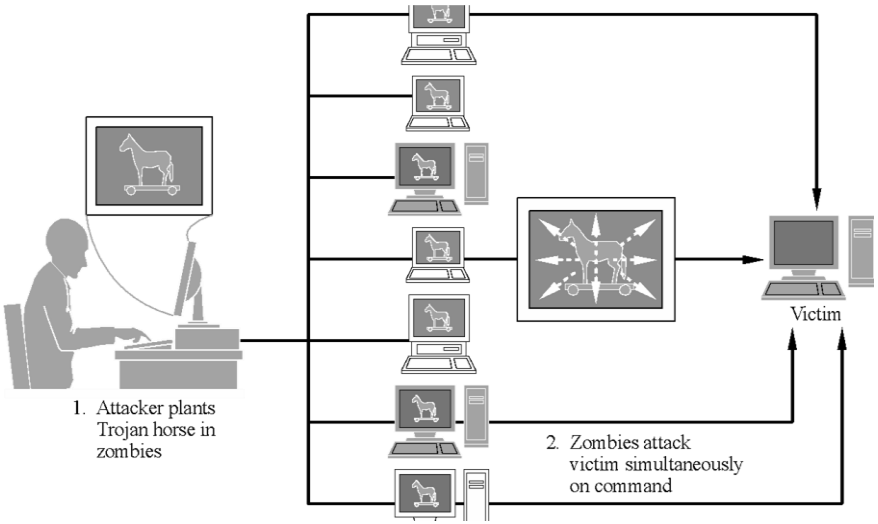
The DYNDNS attack exploited WIFI cameras with default passwords to create a huge botnet. Once they have the botnet ready, the attackers send the start command to all of their botnet nodes, and the botnets will then send their programmed requests to the target server. If the attack makes it past the outer defenses, it quickly overwhelms most systems, causes service outages, and in some cases, crashes the server.

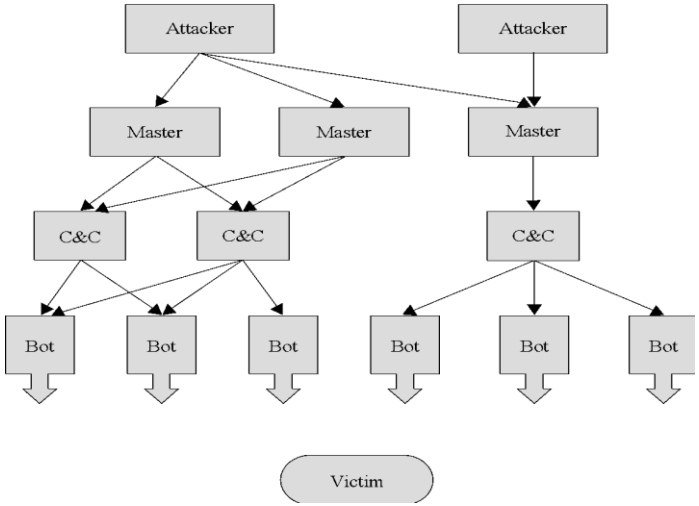
DoS vs DDoS

- A Denial of Service (DoS) attack includes many kinds of attacks all designed to disrupt services. In addition to DDoS, you can have application layer DoS, advanced persistent DoS, and DoS as a service. Companies will use DoS as a service to stress test their networks.
- In short, DDoS is one type of DoS attack – however, DoS can also mean that the attacker used a single node to initiate the attack, instead of using a botnet. Both definitions are correct.



Distributed Denial of Service (DDoS)





1) Conscript an army of compromised machines to attack a victim.
2) Choose a victim, and have the whole army unleash a DoS attack at once.

DDoS attacks are much more effective than traditional DoS attacks, employing a multiplied version of the same methods.

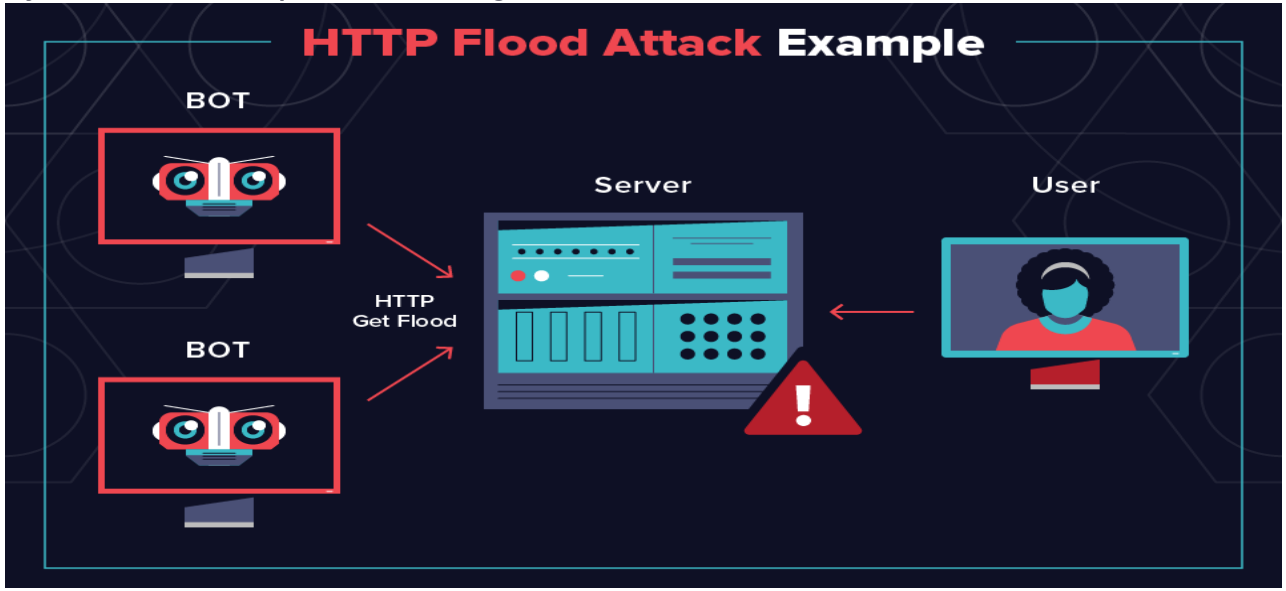
- Botnets are machines running malicious code under remote control.
- They often go undetected because they do little harm to the machines they run on.
- Attacker separated from bots by multiple layers, making attacker difficult to trace. Redundancy built in so that if one master or C&C node is down, the bots can continue….

Application Layer Attacks

- Application layer DDoS attacks aim to exhaust the resources of the target and disrupt access to the target's service.

- Attackers load the bots with a complicated request that taxes the target server as it tries to respond. The request might require database access or large downloads. If the target gets several million of those requests in a short time, it can very quickly get overwhelmed and either slowed to a crawl or locked up completely.

- An HTTP Flood attack, for example, is an application layer attack that targets a web server on the target and uses many fast HTTP requests to bring the server down.

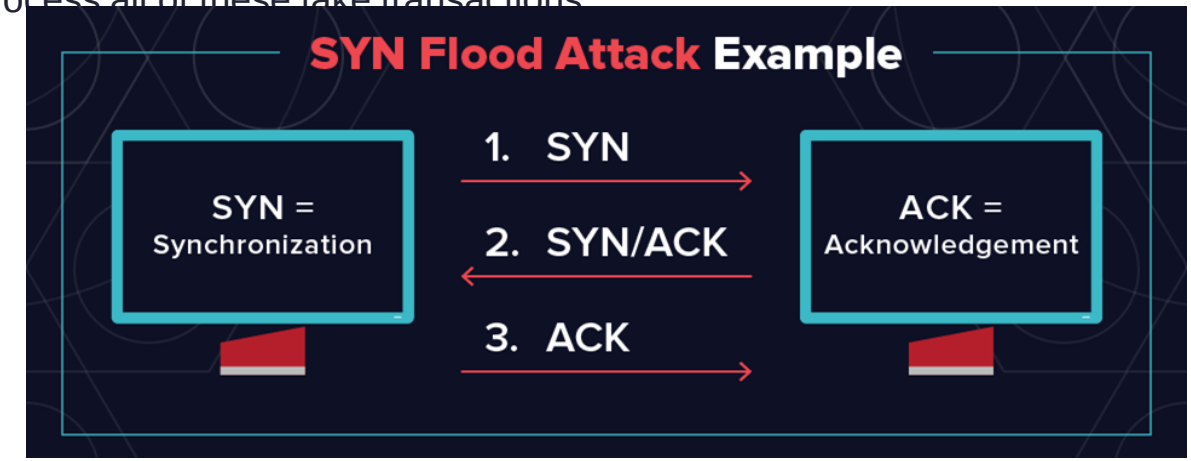


Protocol Attacks

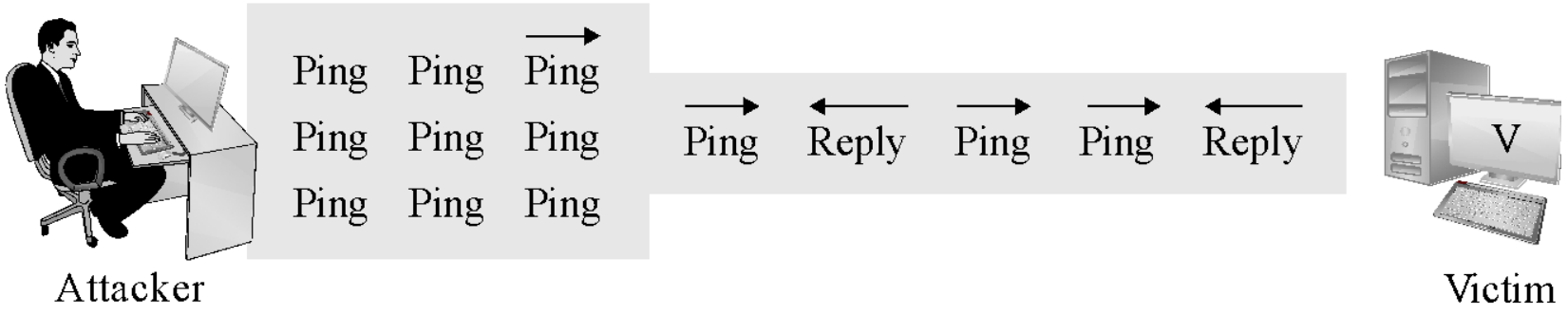
- Protocol DDoS attacks target the networking layer of the target systems. Their goal is to overwhelm the tablespaces of the core networking services, the firewall, or load balancer that forwards requests to the target.

- Network services work off a first-in, first-out (FIFO) queue. The first request comes in, the computer processes the request, and then it goes and gets the next request in the queue so on. There are a limited number of spots on this queue, and in a DDoS attack, the queue could become so huge that there aren't resources for the computer to deal with the first request.

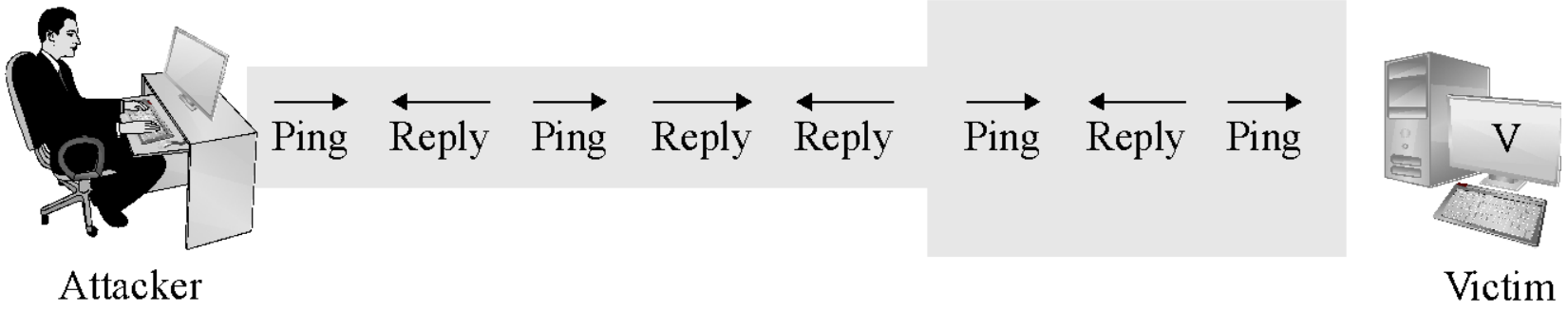
- A SYN flood attack is a specific protocol attack. In a standard TCP/IP network transaction, there is a 3-way handshake. They are the SYN, the ACK, and the SYN-ACK. The SYN is the first part, which is a request of some kind, the ACK is the response from the target, and the SYN-ACK is the original requester saying "thanks, I got the information I requested." In a SYN flood attack, the attackers create SYN packets with fake IP addresses. The target then sends an ACK to the dummy address, which never responds, and it then sits there and waits for all those responses to time out, which in turn exhausts the resources to process all of these fake transactions.



DoS Attack: Ping Flood



(a) Attacker has greater bandwidth



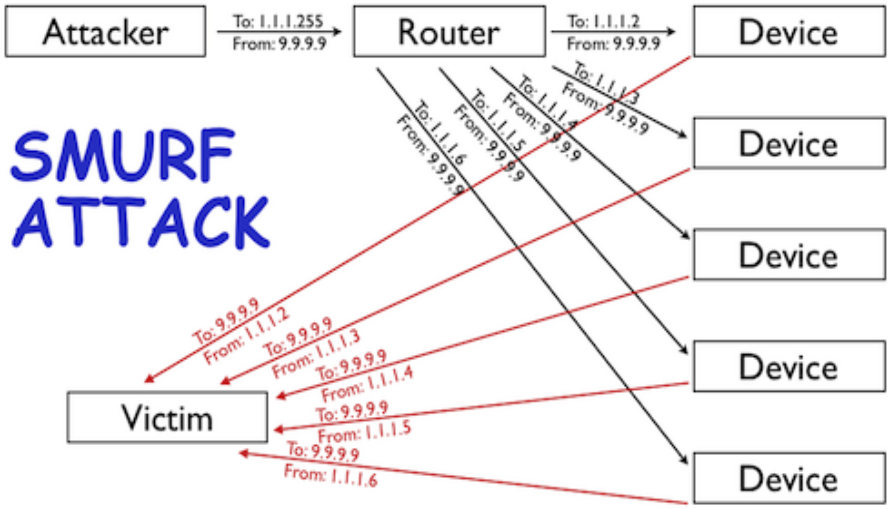
(b) Victim has greater bandwidth

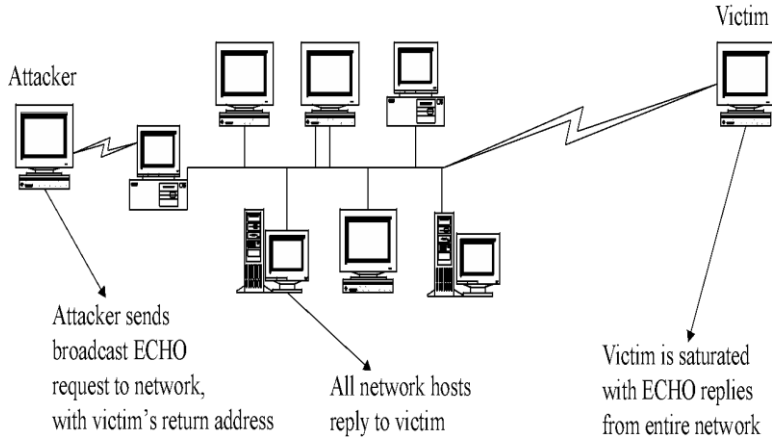
DoS Attack: Smurf Attack

The original amplification attack involves an attacker sending ICMP requests (i.e., ping requests) to the network's broadcast address (i.e., X.X.X.255) of a router configured to relay ICMP to all devices behind the router.

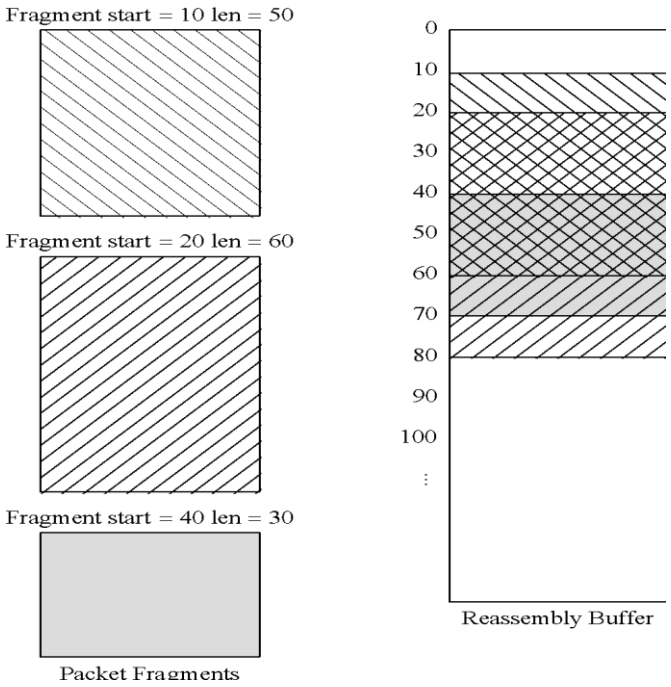
The attacker spoofs the source of the ICMP request to be the IP address of the intended victim. Since ICMP does not include a handshake, the destination has no way of verifying if the source IP is legitimate. The router receives the request and passes it on to all the devices that sit behind it.

All those devices then respond back to the ping. The attacker is able to amplify the attack by a multiple of how ever many devices are behind the router (i.e., if you have 5 devices behind the router then the attacker is able to amplify the attack 5x).





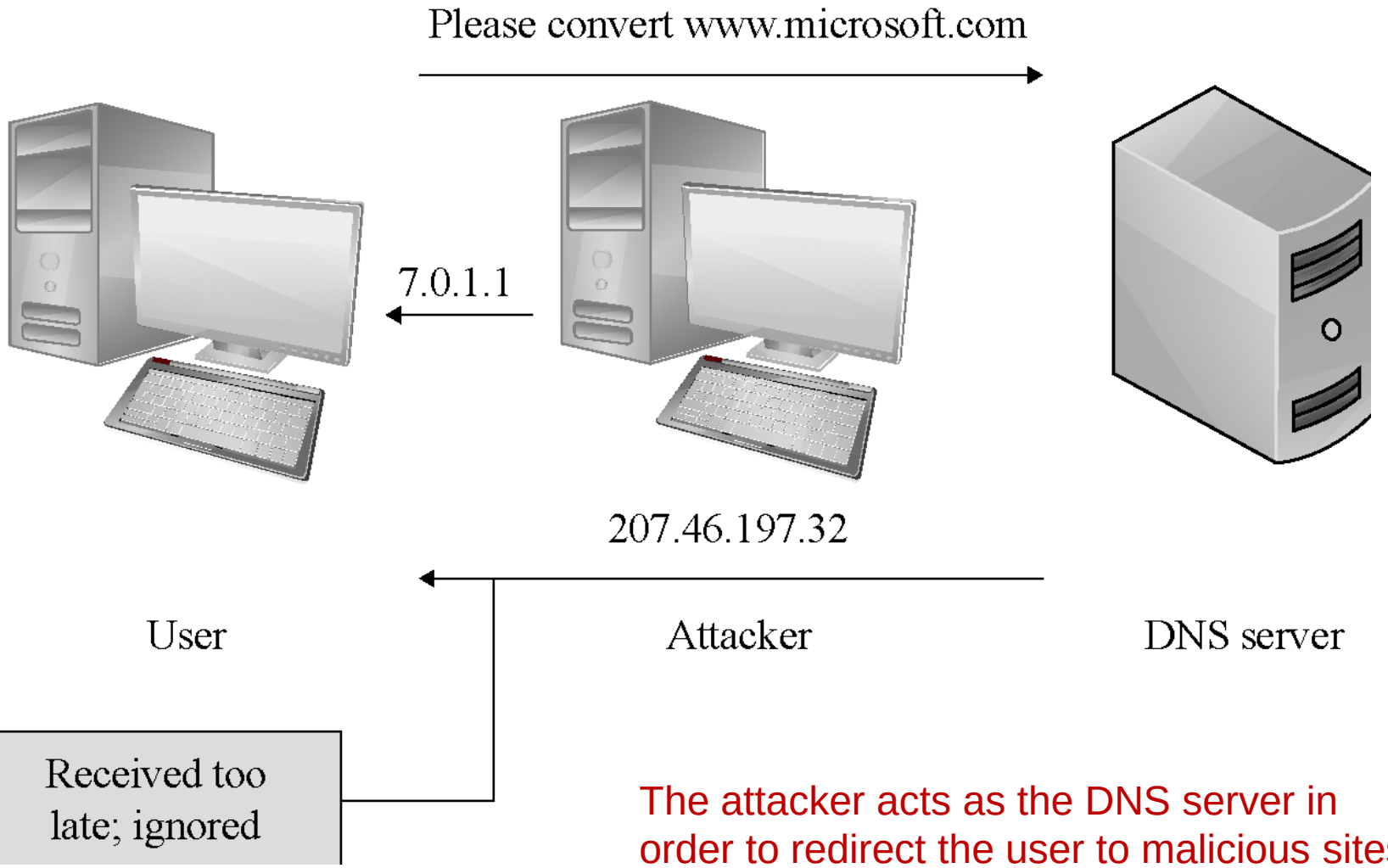
DoS Attack: Teardrop Attack



The attacker sends packets that cannot possibly be reassembled (conflicting reassembly instructions).

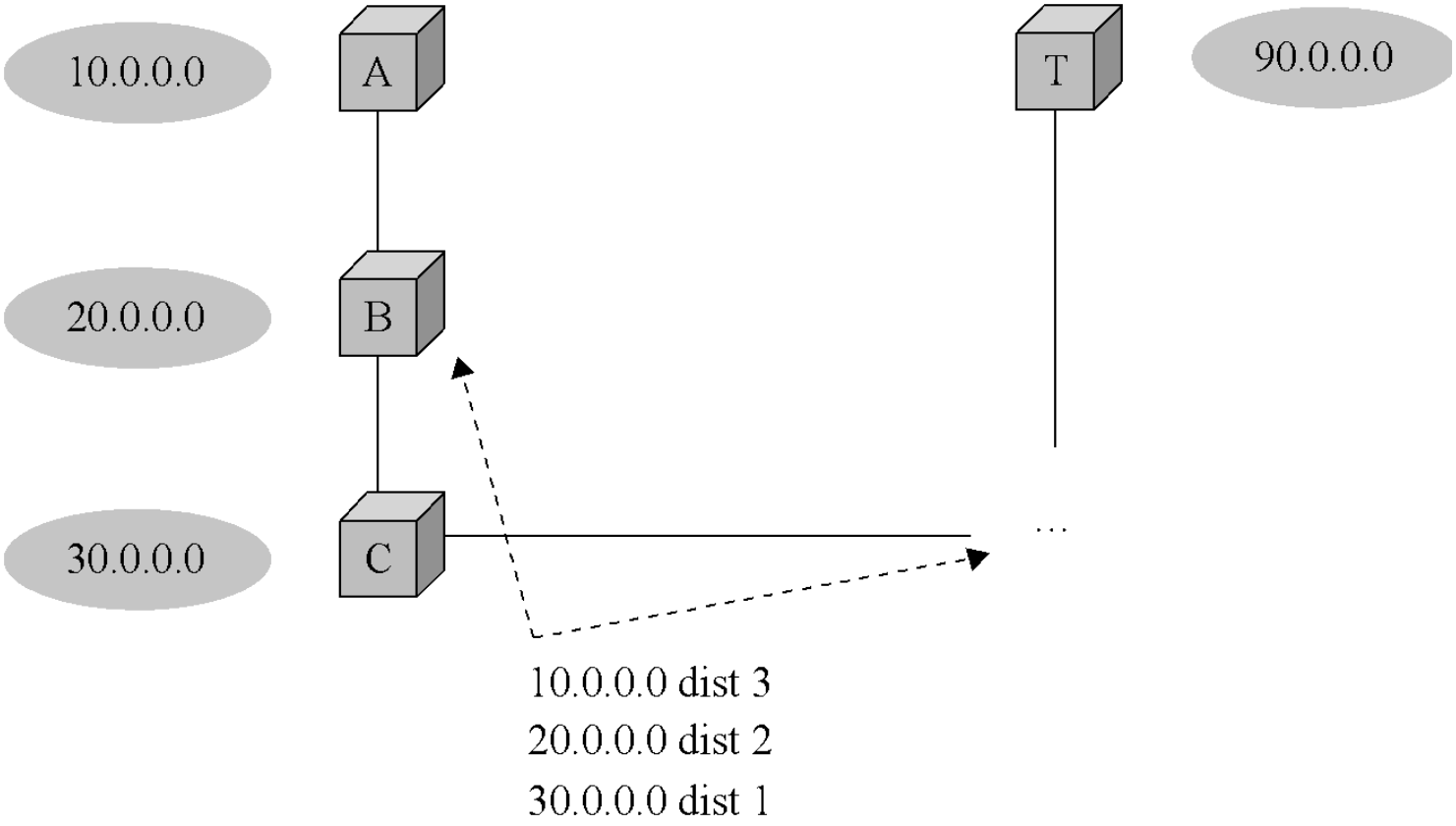
In extreme cases, this can cause the entire OS to lock up.

DoS Attack: DNS Spoofing



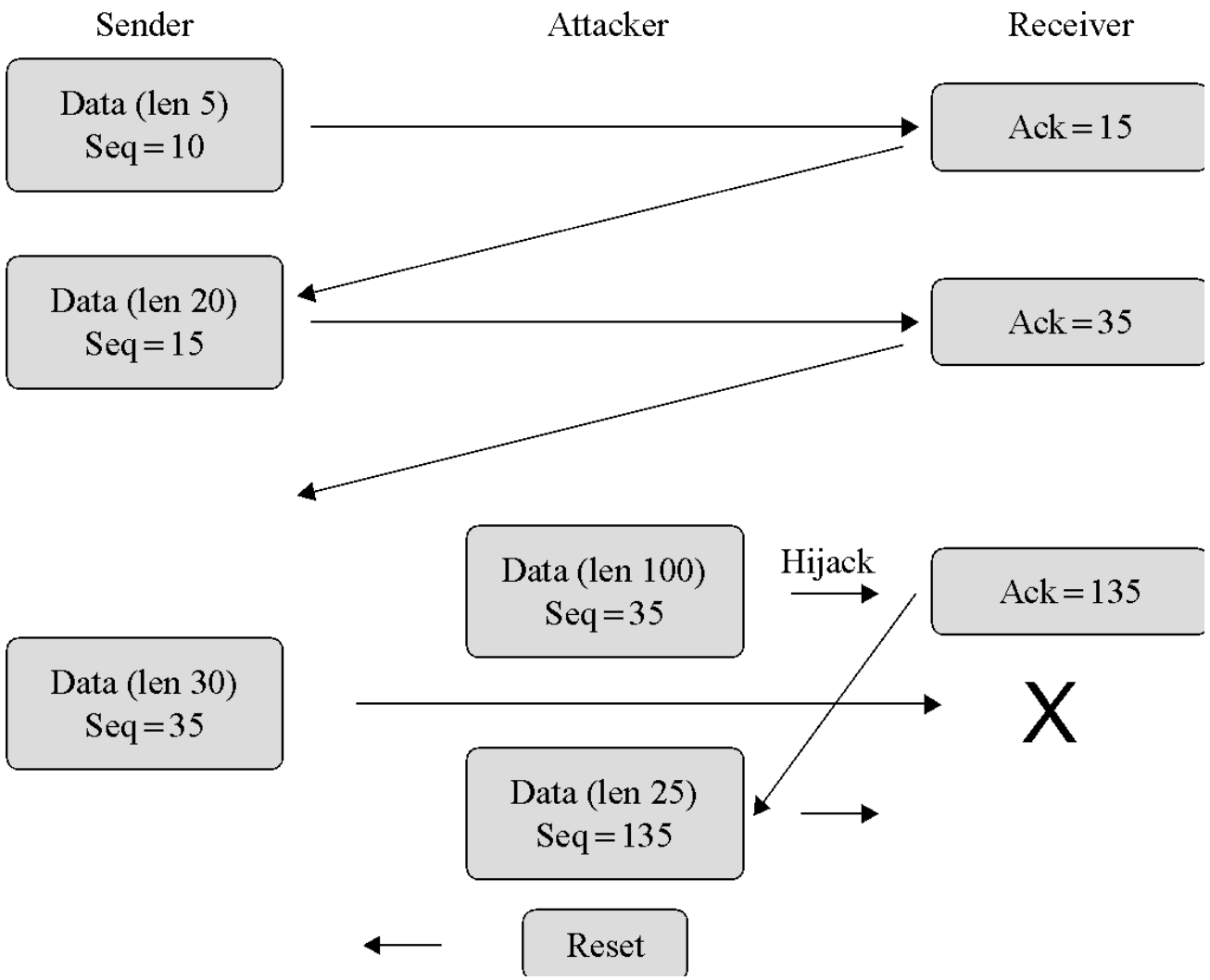
The attacker acts as the DNS server in order to redirect the user to malicious sites.

DoS Attack: Rerouting Routing

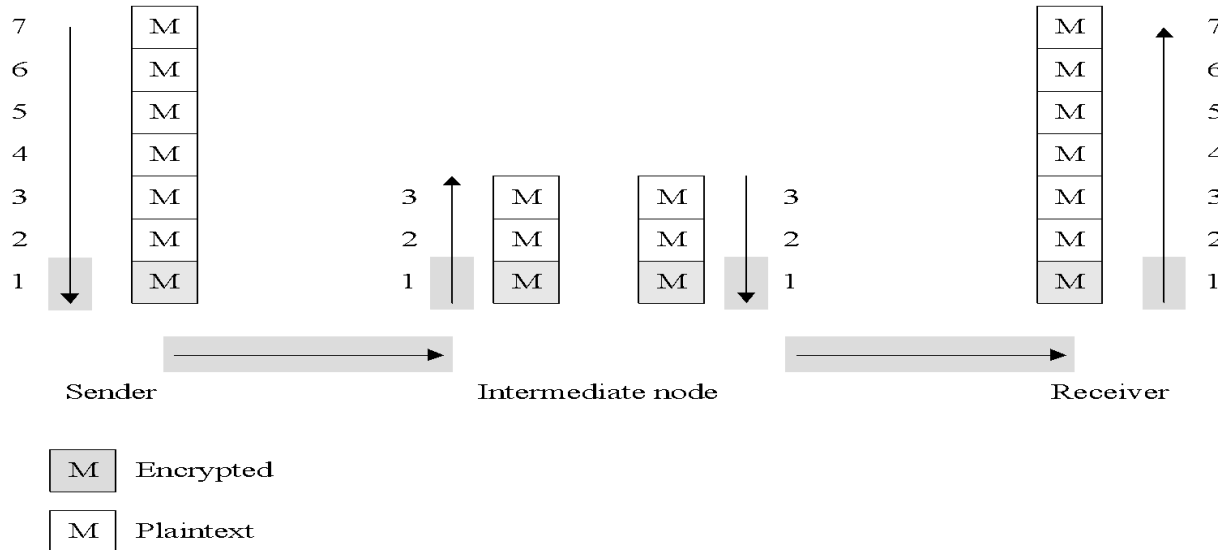


This picture doesn't show anything malicious happening. It just shows how one router, C, advertises the routes it knows about to the routers adjacent to it. Routers rely on these advertising messages to be accurate; when they aren't, DoS can ensue.

DoS Attack: Session Hijacking

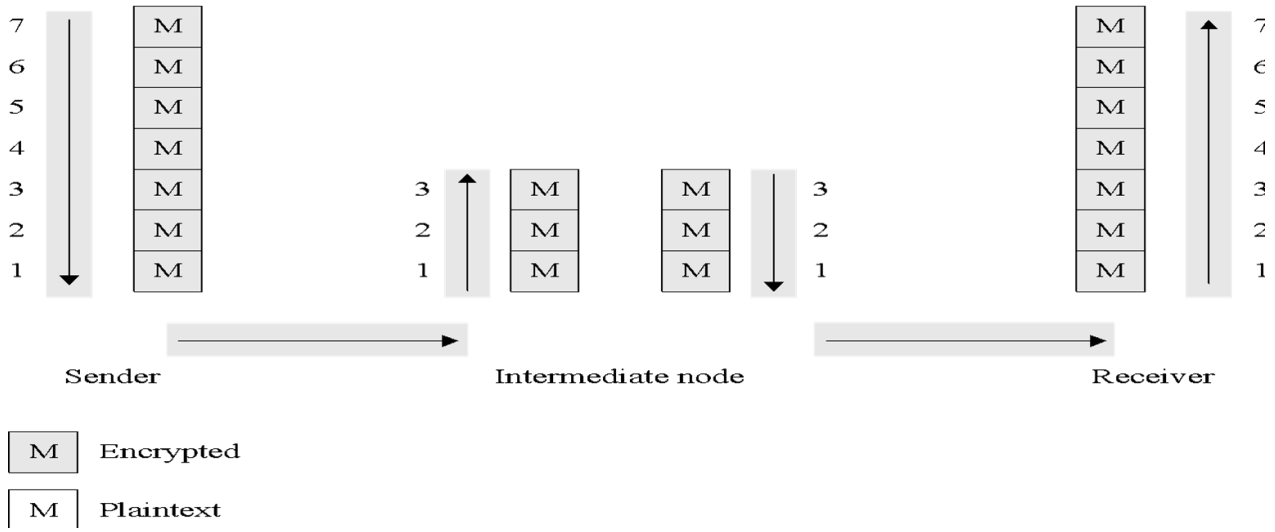


Link Encryption



- In link encryption, data are encrypted just before the system places them on the physical communications link and are decrypted just as they arrive at the destination system. In this graphic, we see that the data is encrypted only at layer 1 of the OSI stack.
- If the data is communicated through an intermediate node, that intermediate node will decrypt the data when it arrives, and then 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



In contrast with the previous slide, this end-to-end encryption diagram shows our data encrypted all the way up to OSI layer 7, the application layer.

In real-world end-to-end encryption, such as those that use SSL, the data often isn't encrypted all the way to layer 7; the important element is that 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.

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

SSL and TLS

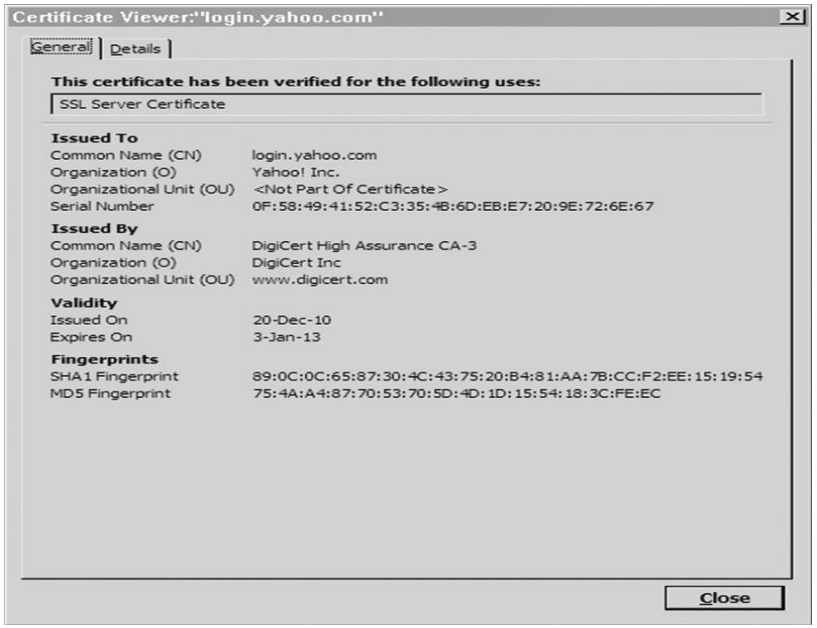
- Secure Sockets Layer (SSL) was designed in 1990s to protect communication between browser & server
- In a 1999 upgrade to SSL, it was renamed Transport Layer Security (TLS)
- While the protocol is still commonly called SSL, TLS is the modern, and much more secure, protocol
- SSL is implemented at OSI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

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.

However, if a server offers cipher suite options that have significant known vulnerabilities (many do), it 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.

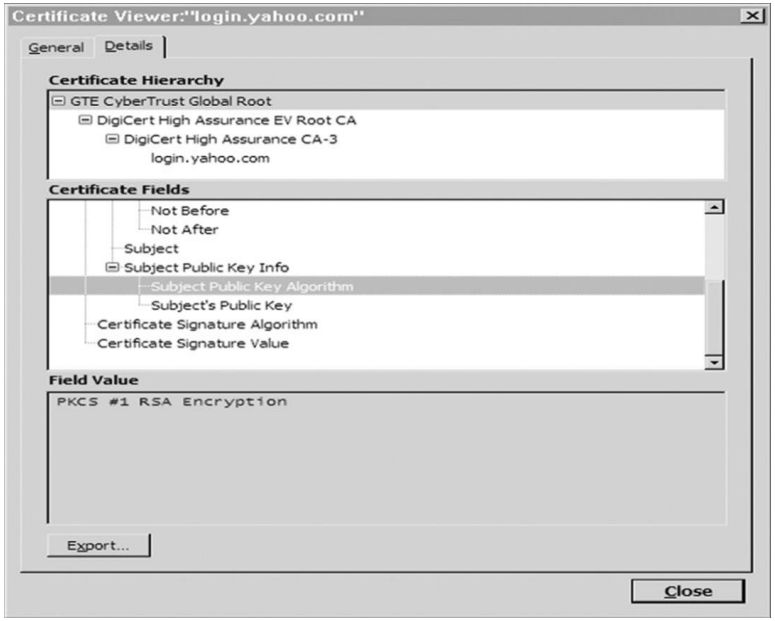
Cipher Suite Identifier	Algorithms Used
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 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 Certificate



In this dialog, we see the certificate details: the domain name being certified, the company that owns the site, the CA that issued the certificate, and the relevant dates.

Chain of Certificates



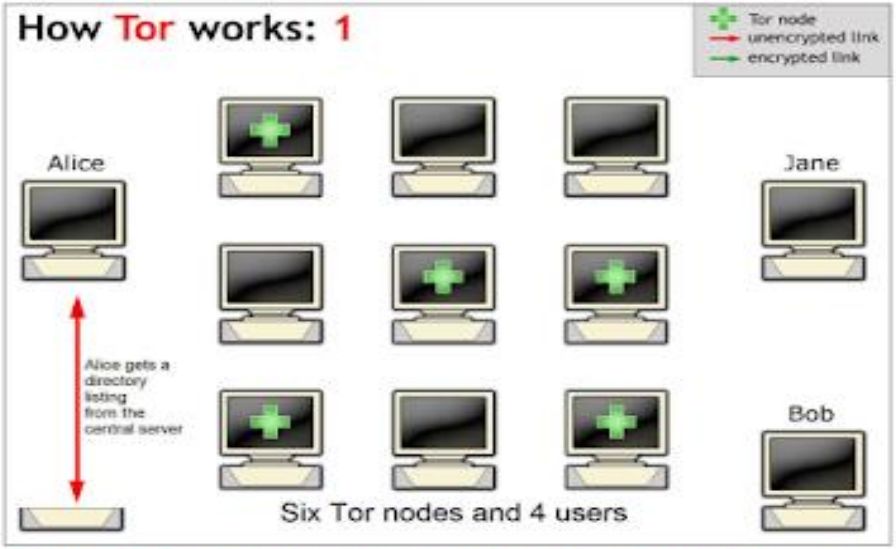
The chain of certificates, starting with GTE CyberTrust Global Root. This dialog also shows the algorithm used for signing the certificate.

If GTE CyberTrust is trusted by my browser, and it, or one of the CAs it authorizes, signs a certificate, then that certificate is valid as far as my browser is concerned.

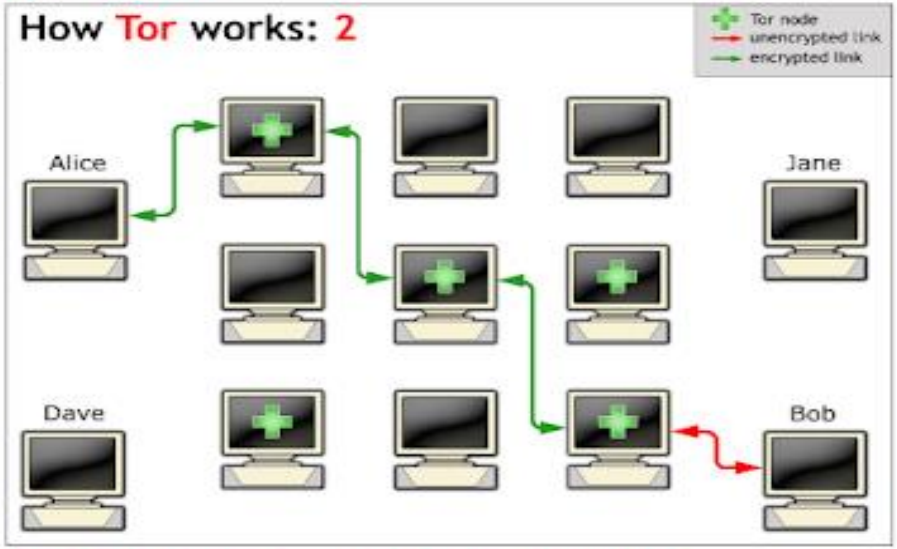
Onion Routing

- 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

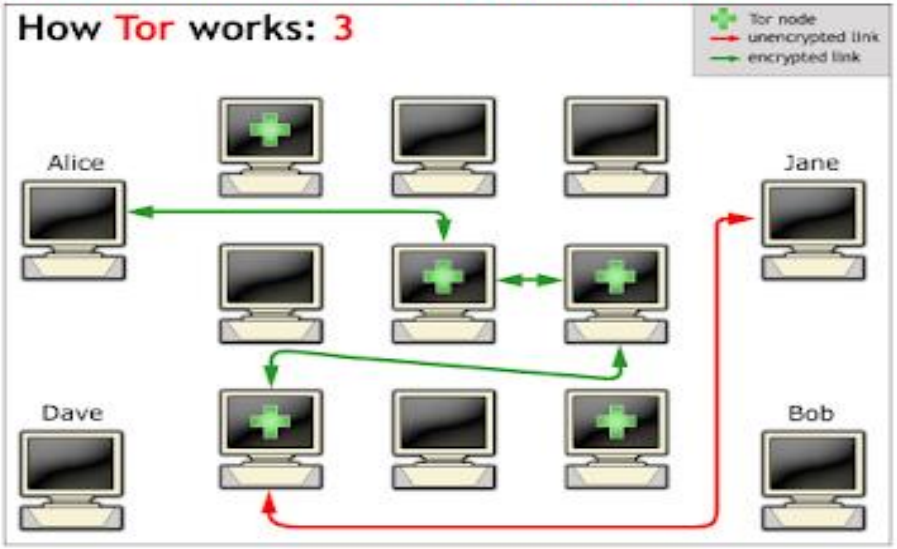
Connection set up



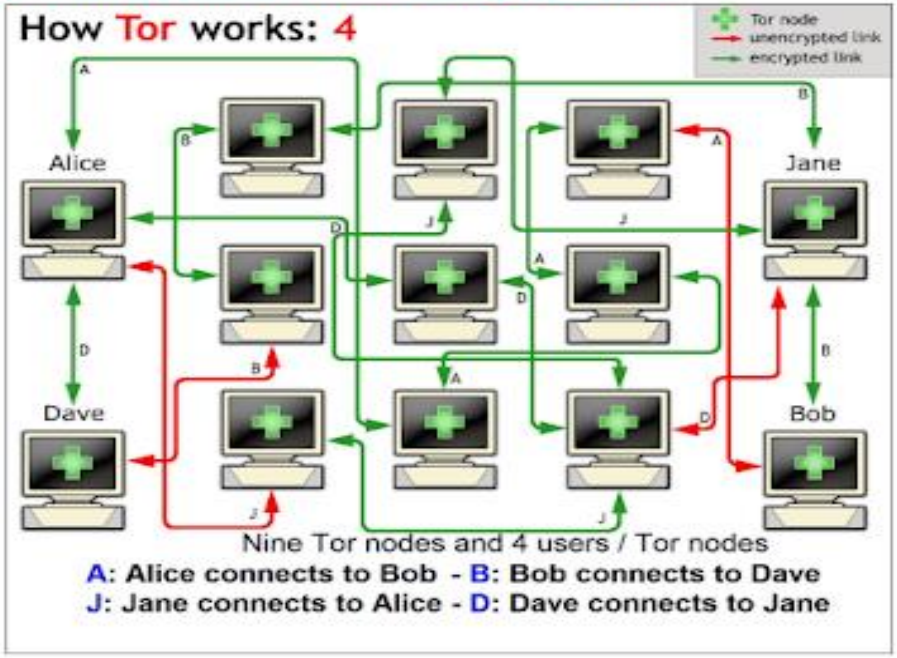
Connection



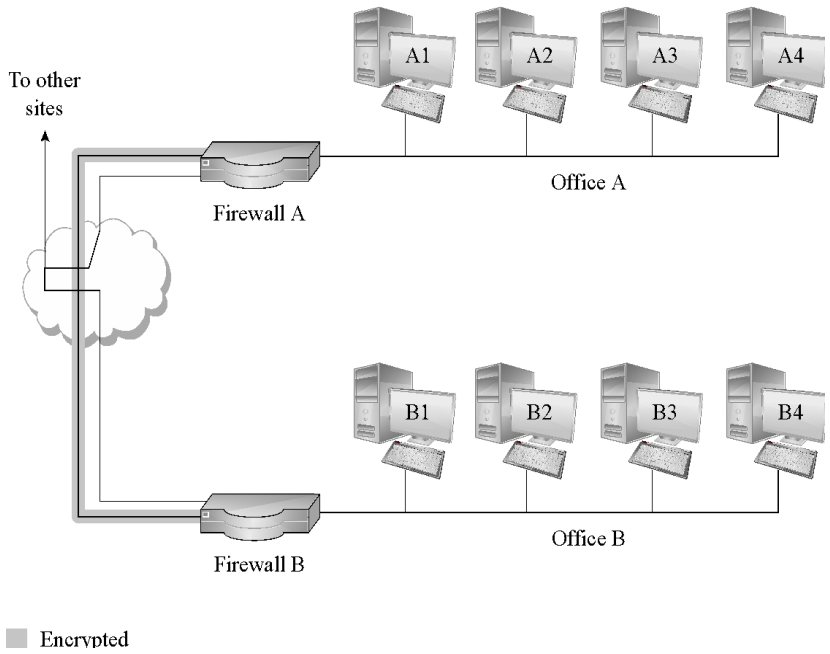
Connection Timeout - entry node change

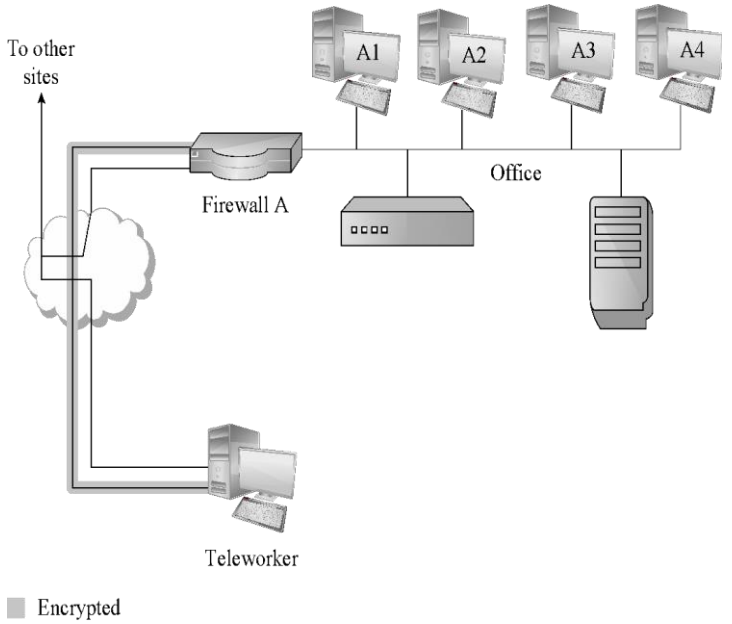


A real scenario - multi purpose node



Virtual Private Networks (VPN)





A VPN—an encrypted tunnel that 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.

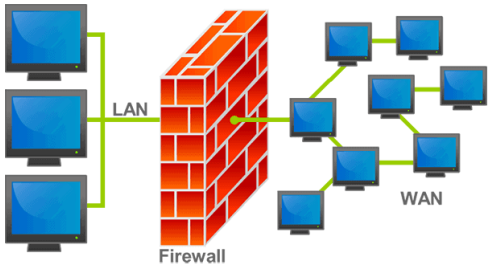
The VPN is terminated by firewalls at both ends, which is often the case in the real world.

In this VPN scenario, a teleworker uses a VPN to connect to a remote office.

She authenticates to the firewall (that's acting as a VPN server), and the firewall passes that authentication information to the servers in the office so she can be appropriately access controlled.

Firewalls

- 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



Firewall Security Policy

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

In this example firewall configuration…

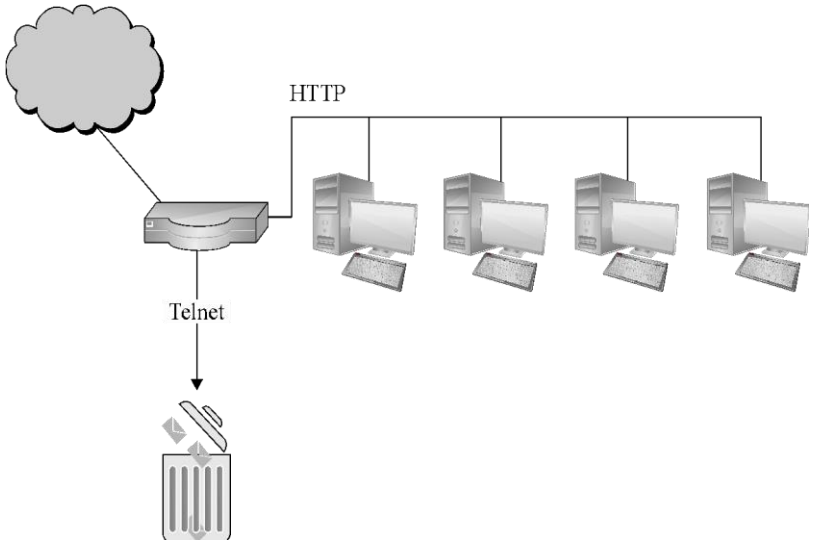
- External traffic can reach the entire internal network on TCP/25 and UDP/69.
- Internal traffic can go out to port 80 on the external network.
- External traffic can reach TCP/80 on one internal server.
- All other traffic from external to internal is disallowed.

Types of Firewalls

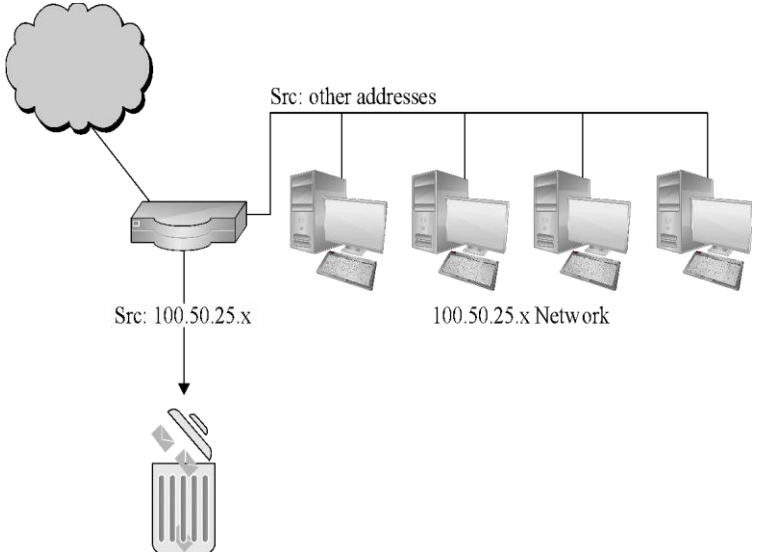
- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

Packet-Filtering Gateways

A packet-filtering gateway controls access on the basis of packet address and specific transport protocol type (e.g., HTTP traffic).



The firewall is filtering out Telnet traffic but allowing HTTP traffic in.



The 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.

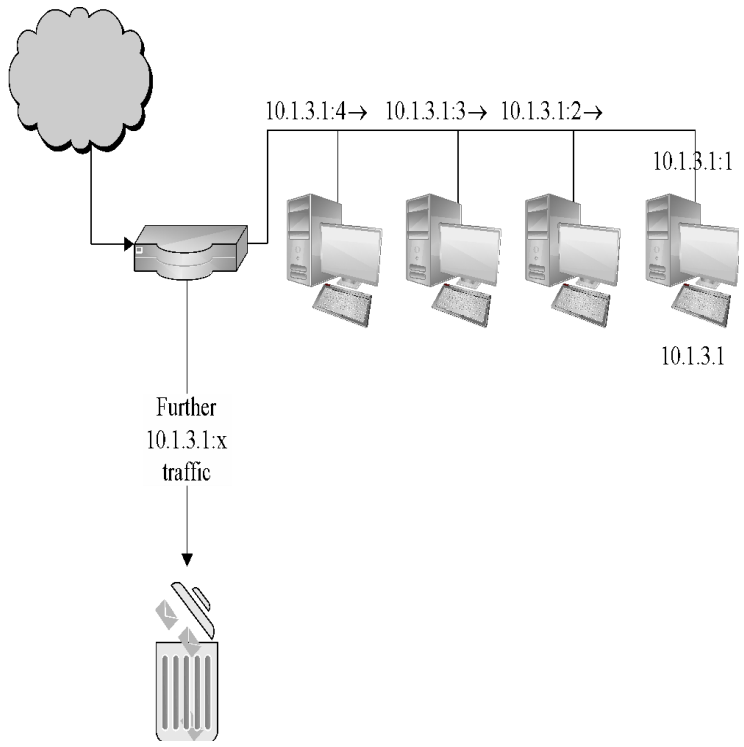
Stateful Inspection Firewall

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. Stateful inspection firewalls, on the other hand, maintain state information from one packet to the next.

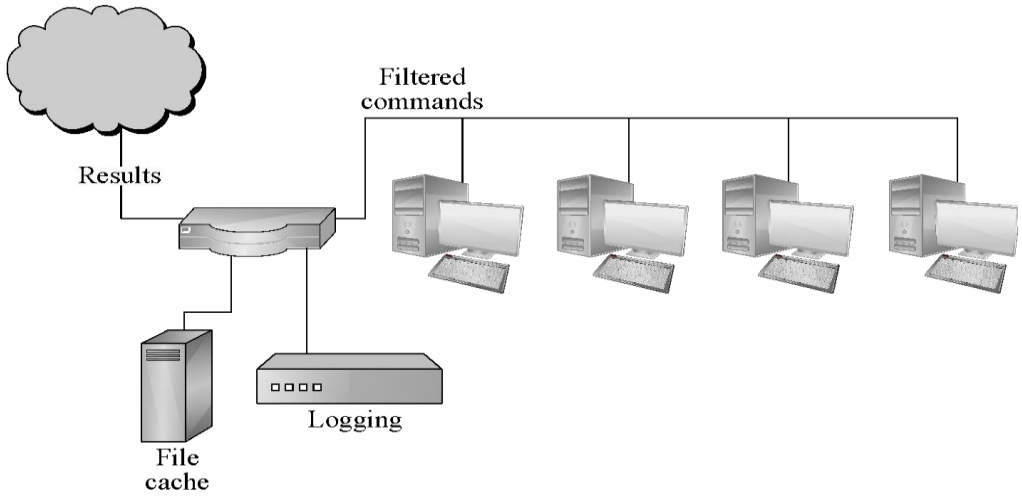
Stateful inspection firewalls, on the other hand, maintain state information from one packet to the next.

In the example in the image, the 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.



Application Proxy

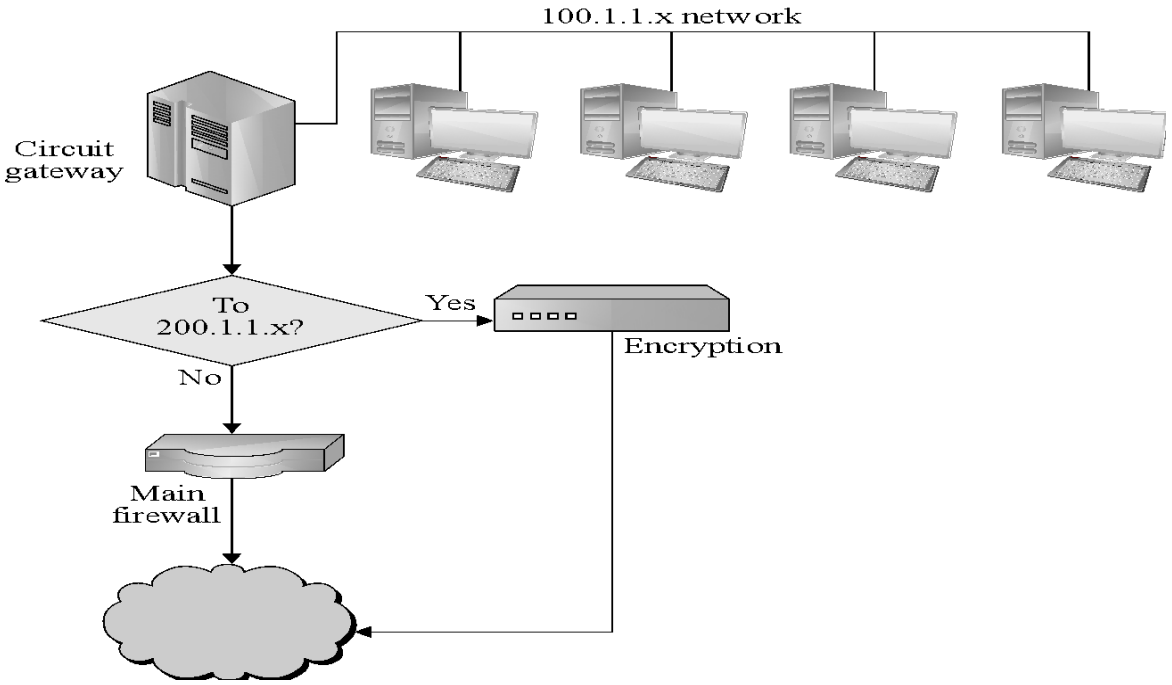


An application proxy simulates the behavior of an application at OSI layer 7 so that the real application receives only requests to act properly. Application proxies can serve several purposes:

- Filtering potentially dangerous application-layer requests
- Log requests/accesses
- Cache results to save bandwidth

Perhaps the most common form of application proxies in the real world is a web proxy, which companies often use to monitor and filter employee Internet use.

Circuit-Level Gateway



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

Personal Firewalls

A personal firewall runs on a workstation or server and can enforce security policy like other firewalls. In addition to restricting traffic by source IP and destination port, personal firewalls can restrict which applications are allowed to use the network.

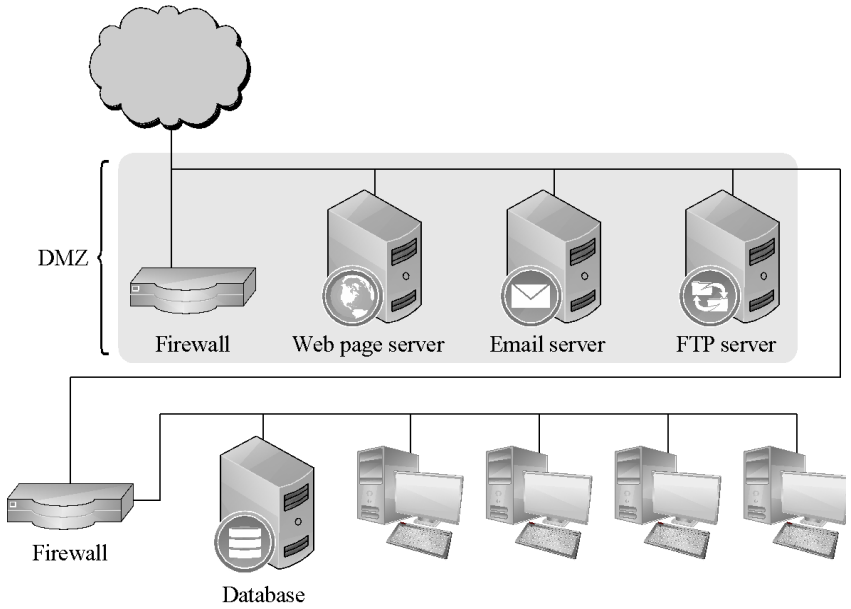
In this example Windows firewall configuration dialog, an administrator can select which protocols and applications should be allowed to communicate to and from the host.

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)

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



In this example, a firewall protects a DMZ that contains web, email, and FTP servers, and 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.

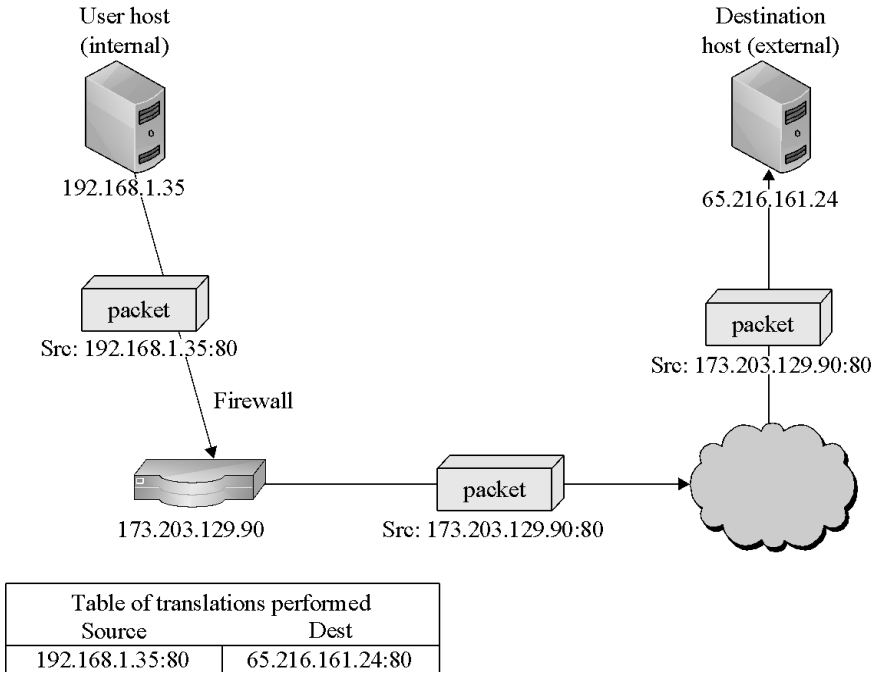
The benefit of such a configuration is that the hosts that need to be accessible from the Internet—and are therefore most at risk from outside attack—can only do limited damage to the internal hosts that do not need to be reachable from the Internet.

An even more careful option would separate web, email & FTP servers 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, 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

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 & 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.

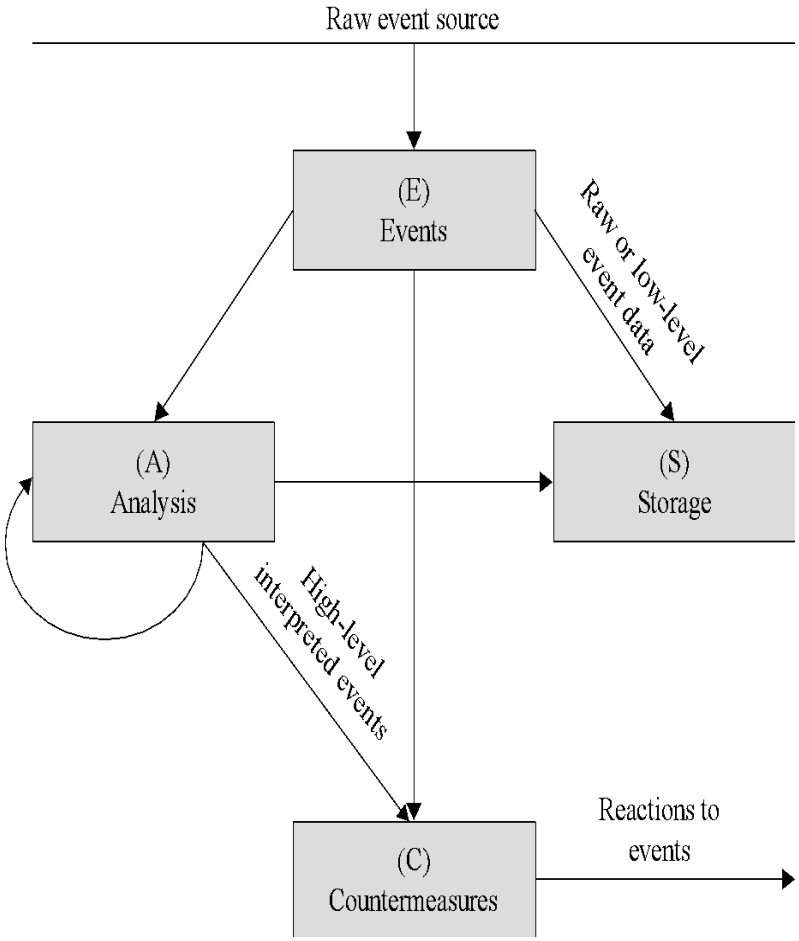
Data Loss Prevention (DLP)

- 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

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



Types of IDS

- Detection method
  - Signature-based, Heuristic
- Location
  - Front end, Internal
- Scope
  - Host-based IDS (HIDS), Network-based IDS (NIDS)
- Capability
  - Passive, Active, also known as intrusion prevention systems (IPS)

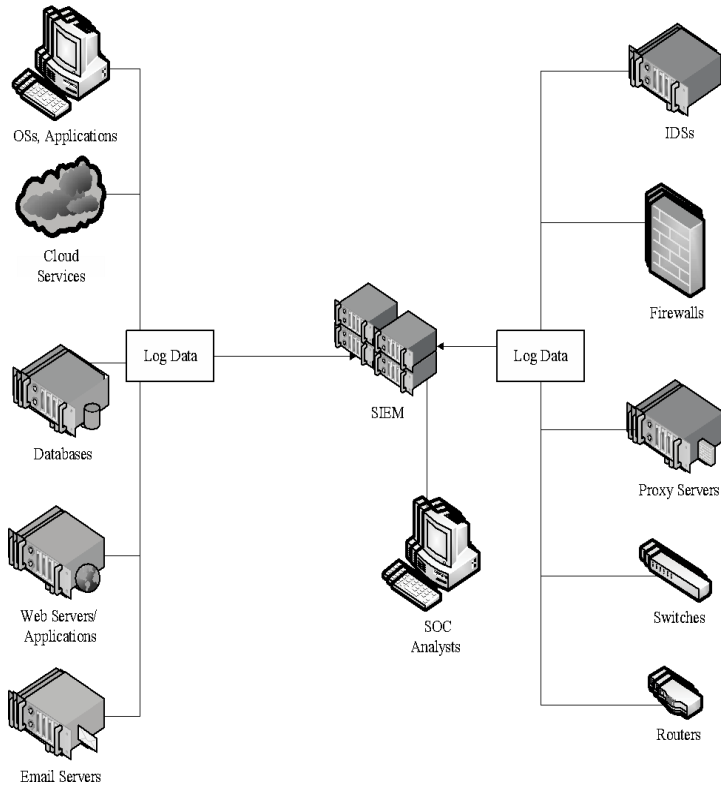
- A signature-based IDS can only detect known patterns.
- A heuristic IDS looks for patterns of behavior that are out of the ordinary.
- A front-end IDS looks at traffic as it enters the network, while an internal IDS monitors traffic within the network.
- A host-based IDS protects a single host by monitoring traffic from the OS.
- A network-based IDS is a server or appliance that monitors network traffic.
- An IPS is an IDS that tries to block or otherwise prevent suspicious or malicious behavior once it is detected.

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 to create a unified security dashboard for security operations center personnel.

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

SIEMs range in functionality from simple ones that allow for basic search and alerting to complex platforms that allow for completely custom dashboards, reports, alerts, and correlation.



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