

Network security

- What is network security?
- Principles of cryptography
- Message integrity, authentication
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec
- Security in wireless and mobile networks
- Operational security: firewalls and IDS



What is network security?

confidentiality: only sender, intended receiver should “understand” message contents

- sender encrypts message
- receiver decrypts message

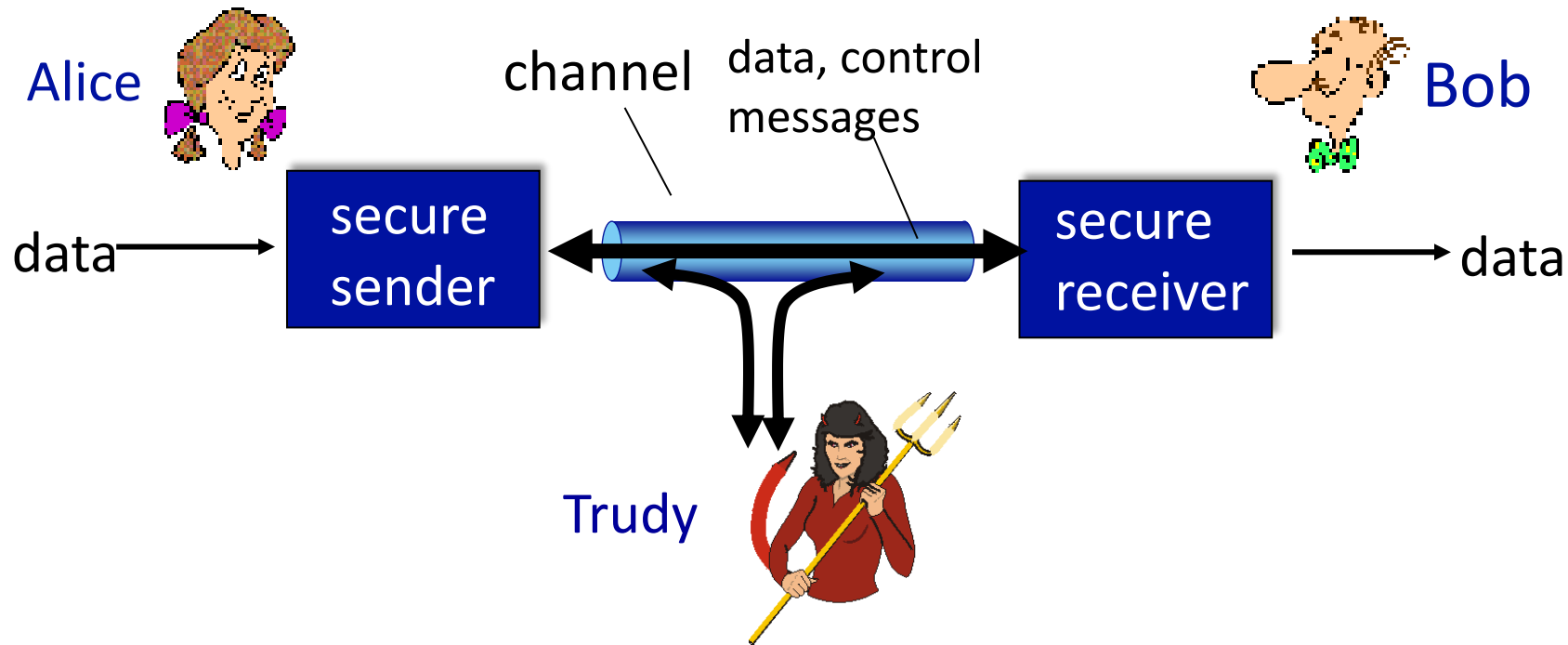
authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Friends and enemies: Alice, Bob, Trudy

Who might Bob and Alice be?

- ... well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- BGP routers exchanging routing table updates
- other examples?

There are bad guys (and girls) out there!

Q: What can a “bad guy” do?

A: A lot! (recall section 1.6)

- **eavesdrop**: intercept messages
- actively **insert** messages into connection
- **impersonation**: can fake (spoof) source address in packet (or any field in packet)
- **hijacking**: “take over” ongoing connection by removing sender or receiver, inserting himself in place
- **denial of service**: prevent service from being used by others (e.g., by overloading resources)

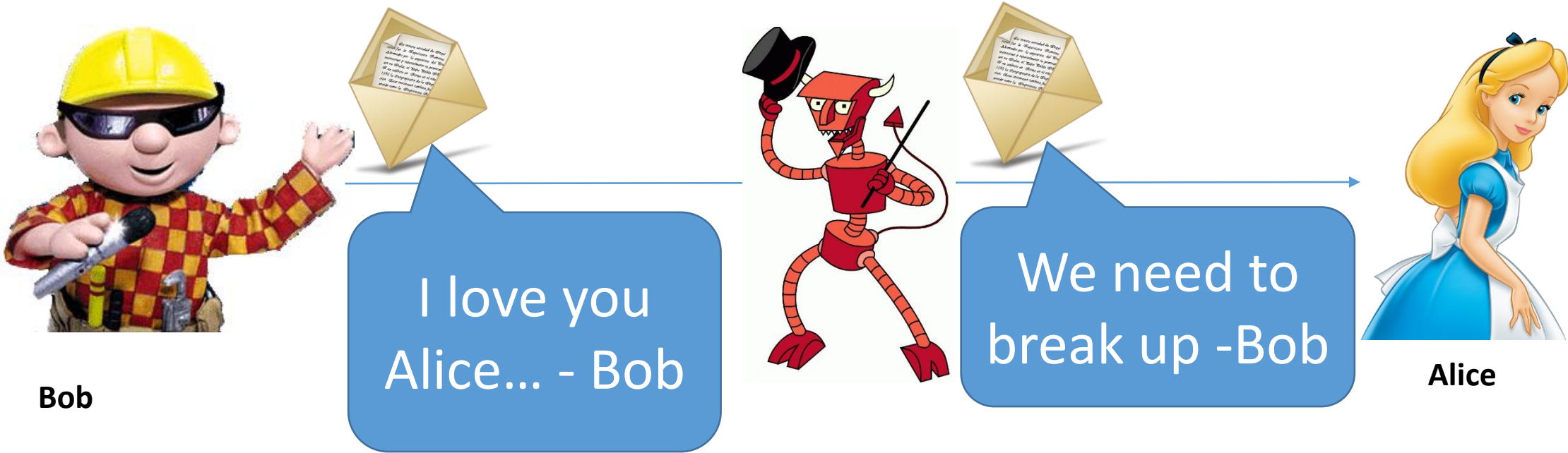
What Does It Mean to “Secure Information”

- Confidentiality (Security/Privacy)
 - Only intended recipient can see the communication

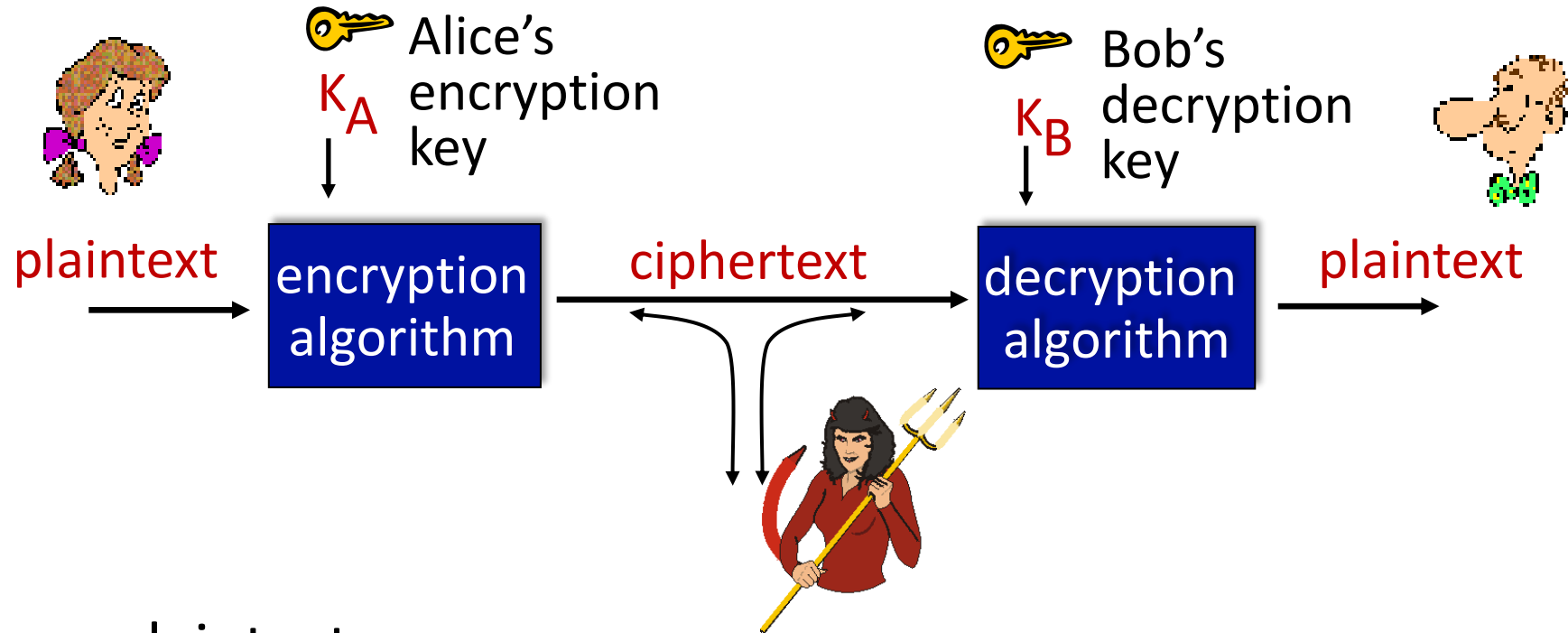


What Does It Mean to “Secure Information”

- Confidentiality (Security/Privacy)
 - Only intended recipient can see the communication
- Integrity (Authenticity)
 - The message was actually sent by the alleged sender



The language of cryptography



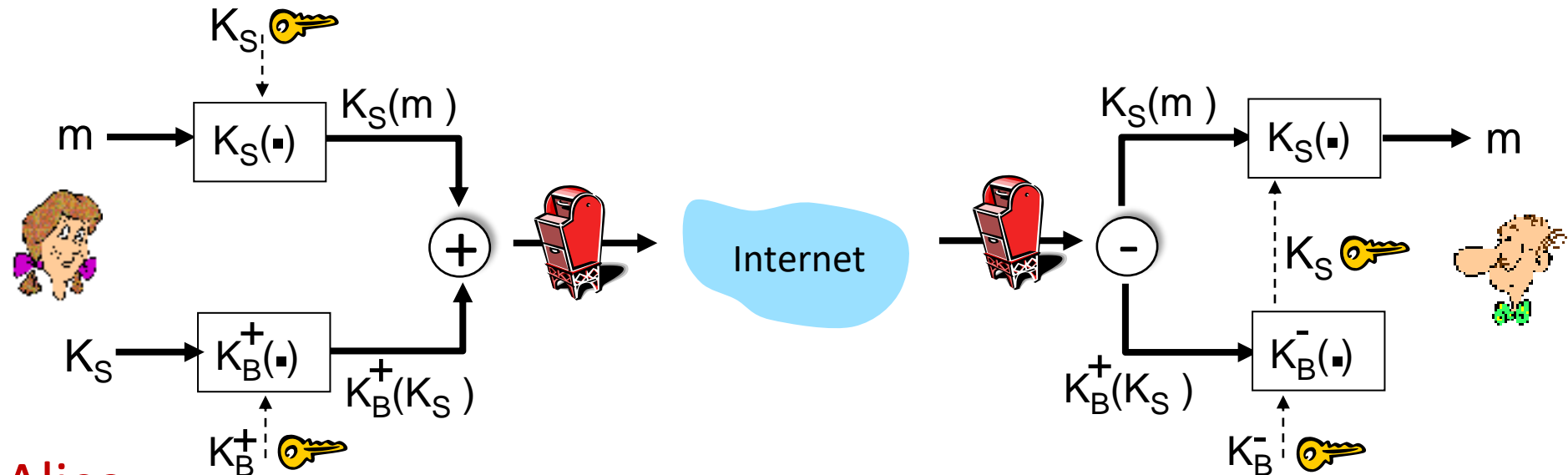
m : plaintext message

$K_A(m)$: ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Secure e-mail: confidentiality

Alice wants to send *confidential* e-mail, m , to Bob.

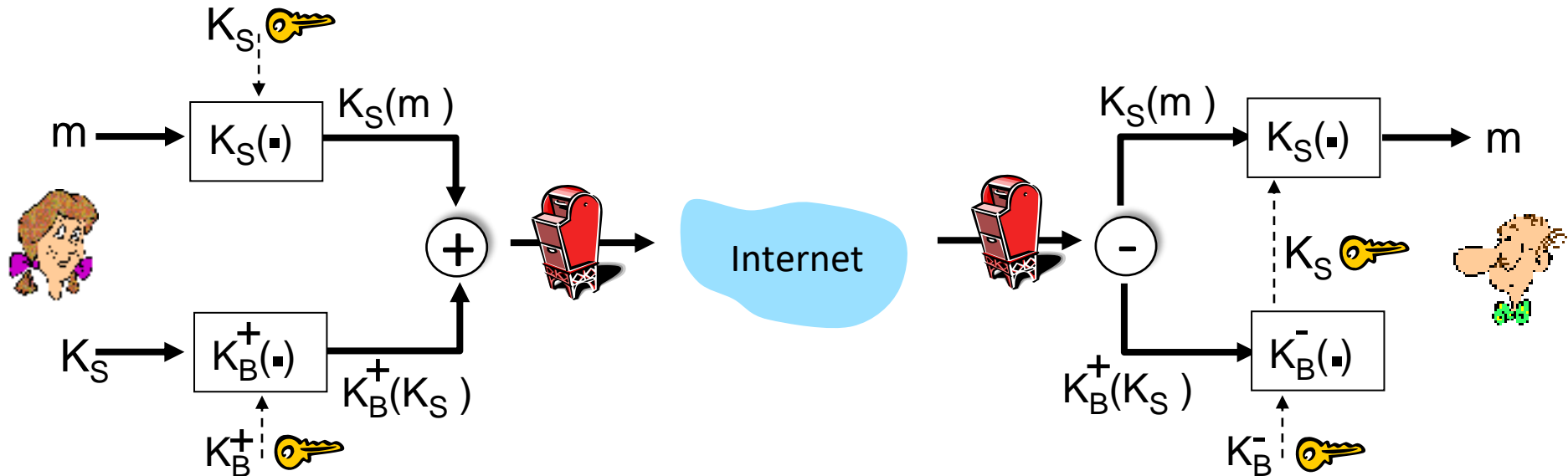


Alice:

- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B^+(K_S)$ to Bob

Secure e-mail: confidentiality (more)

Alice wants to send *confidential* e-mail, m , to Bob.

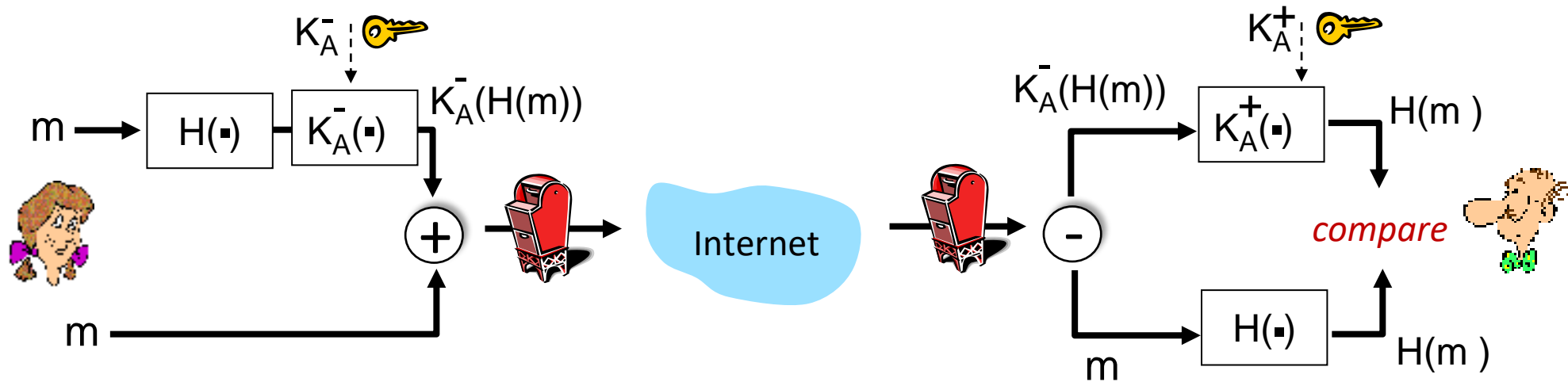


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail: integrity, authentication

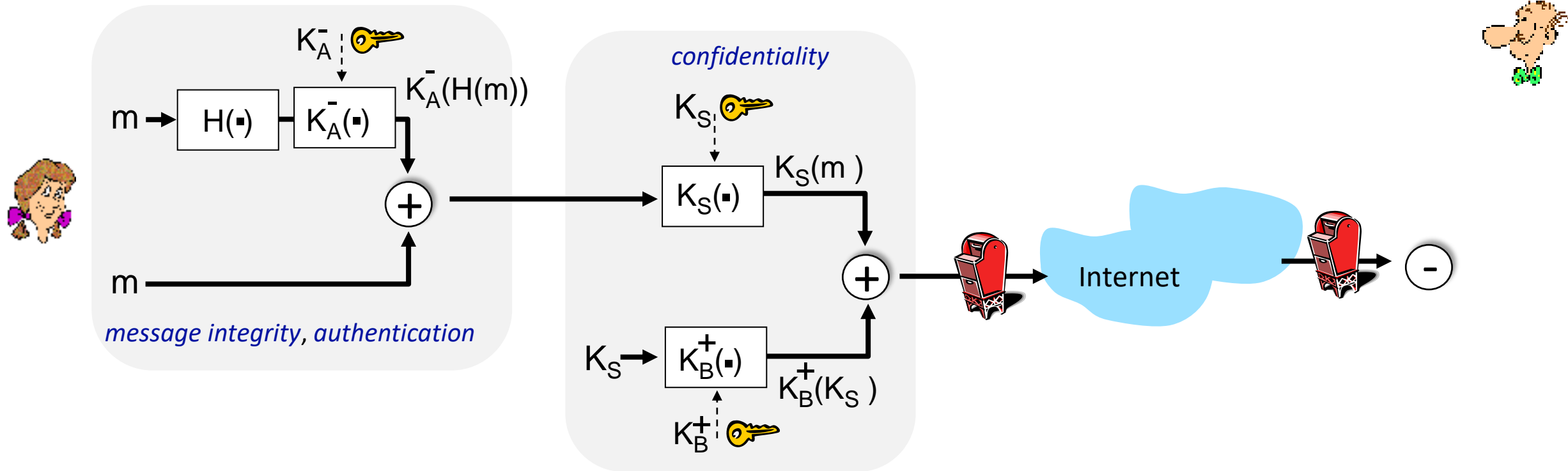
Alice wants to send m to Bob, with *message integrity, authentication*



- Alice digitally signs hash of her message with her private key, providing integrity and authentication
- sends both message (in the clear) and digital signature

Secure e-mail: integrity, authentication

Alice sends m to Bob, with *confidentiality, message integrity, authentication*



Alice uses three keys: her private key, Bob's public key, new symmetric key

What are Bob's complementary actions?

Transport-layer security (TLS)

- widely deployed security protocol above the transport layer
 - supported by almost all browsers, web servers: https (port 443)
- provides:
 - **confidentiality**: via *symmetric encryption*
 - **integrity**: via *cryptographic hashing*
 - **authentication**: via *public key cryptography*

} *all techniques we have studied!*
- history:
 - early research, implementation: secure network programming, secure sockets
 - secure socket layer (SSL) deprecated [2015]
 - TLS 1.3: RFC 8846 [2018]

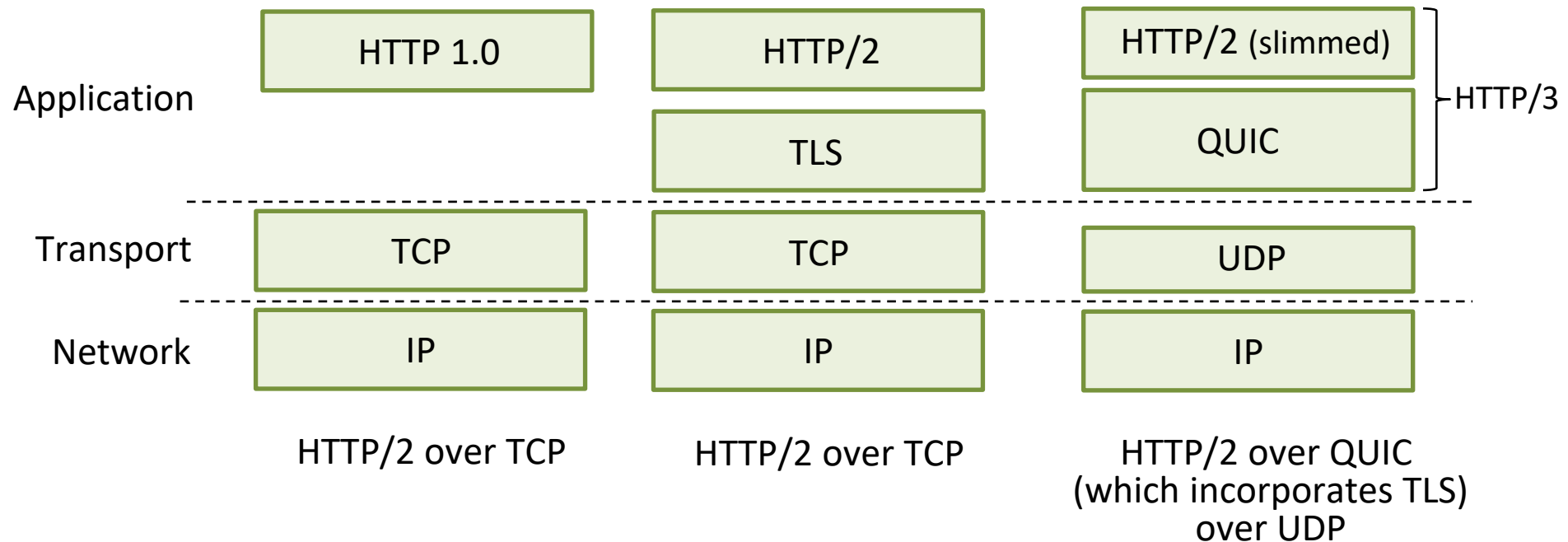
Transport-layer security (TLS)

- widely deployed security protocol above the transport layer
 - supported by almost all browsers, web servers: https (port 443)
- provides:
 - **confidentiality**: via *symmetric encryption*
 - **integrity**: via *cryptographic hashing*
 - **authentication**: via *public key cryptography*

} *all techniques we have studied!*
- history:
 - early research, implementation: secure network programming, secure sockets
 - secure socket layer (SSL) deprecated [2015]
 - TLS 1.3: RFC 8846 [2018]

Transport-layer security (TLS)

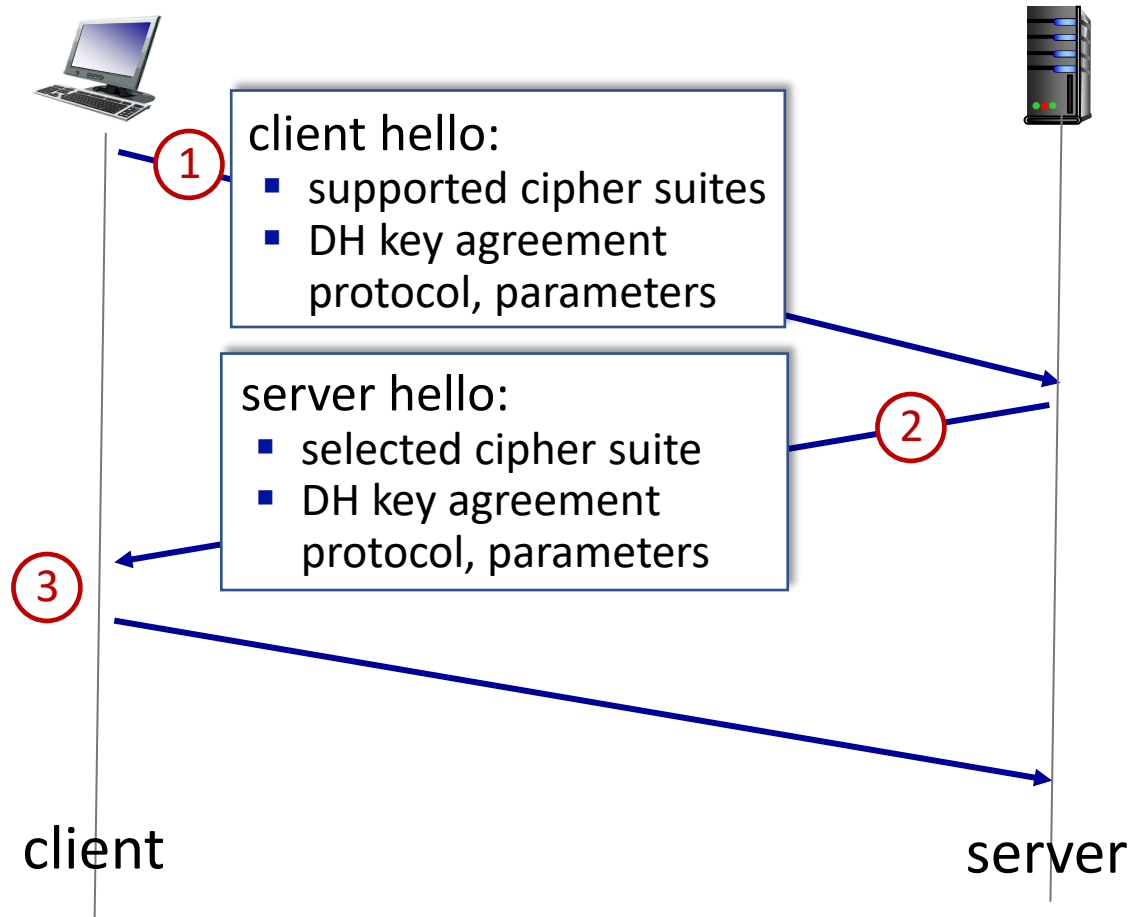
- TLS provides an API that *any* application can use
- an HTTP view of TLS:



TLS: 1.3 cipher suite

- “cipher suite”: algorithms that can be used for key generation, encryption, MAC, digital signature
- TLS: 1.3 (2018): more limited cipher suite choice than TLS 1.2 (2008)
 - only 5 choices, rather than 37 choices
 - *requires* Diffie-Hellman (DH) for key exchange, rather than DH or RSA
 - combined encryption and authentication algorithm (“authenticated encryption”) for data rather than serial encryption, authentication
 - 4 based on AES
 - HMAC uses SHA (256 or 284) cryptographic hash function

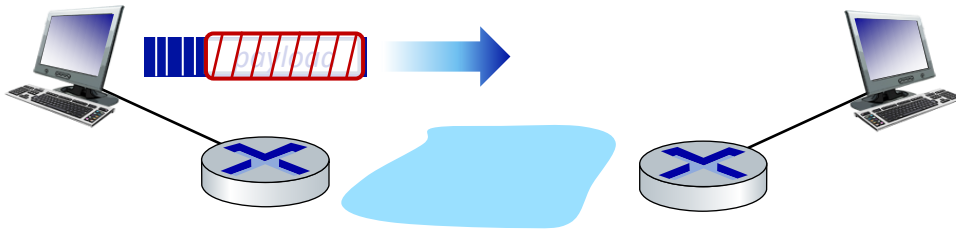
TLS 1.3 handshake: 1 RTT



- ① client TLS hello msg:
 - *guesses* key agreement protocol, parameters
 - indicates cipher suites it supports
- ② server TLS hello msg chooses
 - key agreement protocol, parameters
 - cipher suite
 - server-signed certificate
- ③ client:
 - checks server certificate
 - generates key
 - can now make application request (e.g., HTTPS GET)

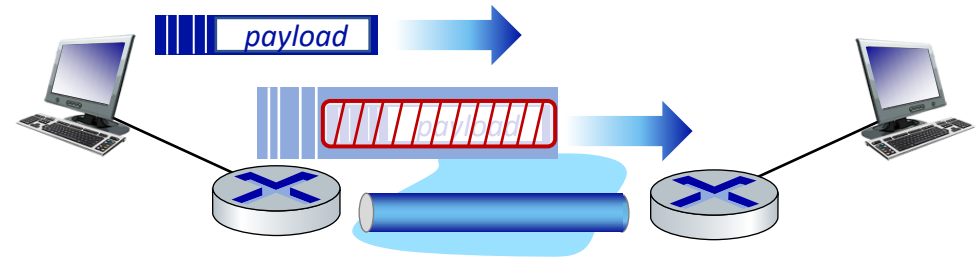
IP Sec

- provides datagram-level encryption, authentication, integrity
 - for both user traffic and control traffic (e.g., BGP, DNS messages)
- two “modes”:



transport mode:

- *only* datagram *payload* is encrypted, authenticated



tunnel mode:

- entire datagram is encrypted, authenticated
- encrypted datagram encapsulated in new datagram with new IP header, tunneled to destination

Firewalls and VPNs

Firewalls

- Prevent specific types of information from moving between the outside world (untrusted network) and the inside world (trusted network)
- May be separate computer system; a software service running on existing router or server; or a separate network containing supporting devices
- A Roadmap
 - Firewall categorization
 - Firewall configuration and management

Firewall Categorization

- ① Processing mode
- ② Development era
- ③ Intended deployment structure
- ④ Architectural implementation

Firewall Categorization (1): Processing Modes

- Packet filtering
- Application gateways
- Circuit gateways
- MAC layer firewalls
- Hybrids

Firewall Proc. Modes: Network Layers

Processing Mode	Network Layer (OSI)	Network Layer (TCP/IP)
Application gateways	7: Application	5: Application
	6: Presentation	
	5: Session	
Circuit gateways	4: Transport	4: Transport
Packet filtering	3: Network	3: Network
MAC address filtering	2: Data Link	2: Data Link
—	1: Physical	1: Physical

Source: Adapted from Fig. 6-5 in the textbook

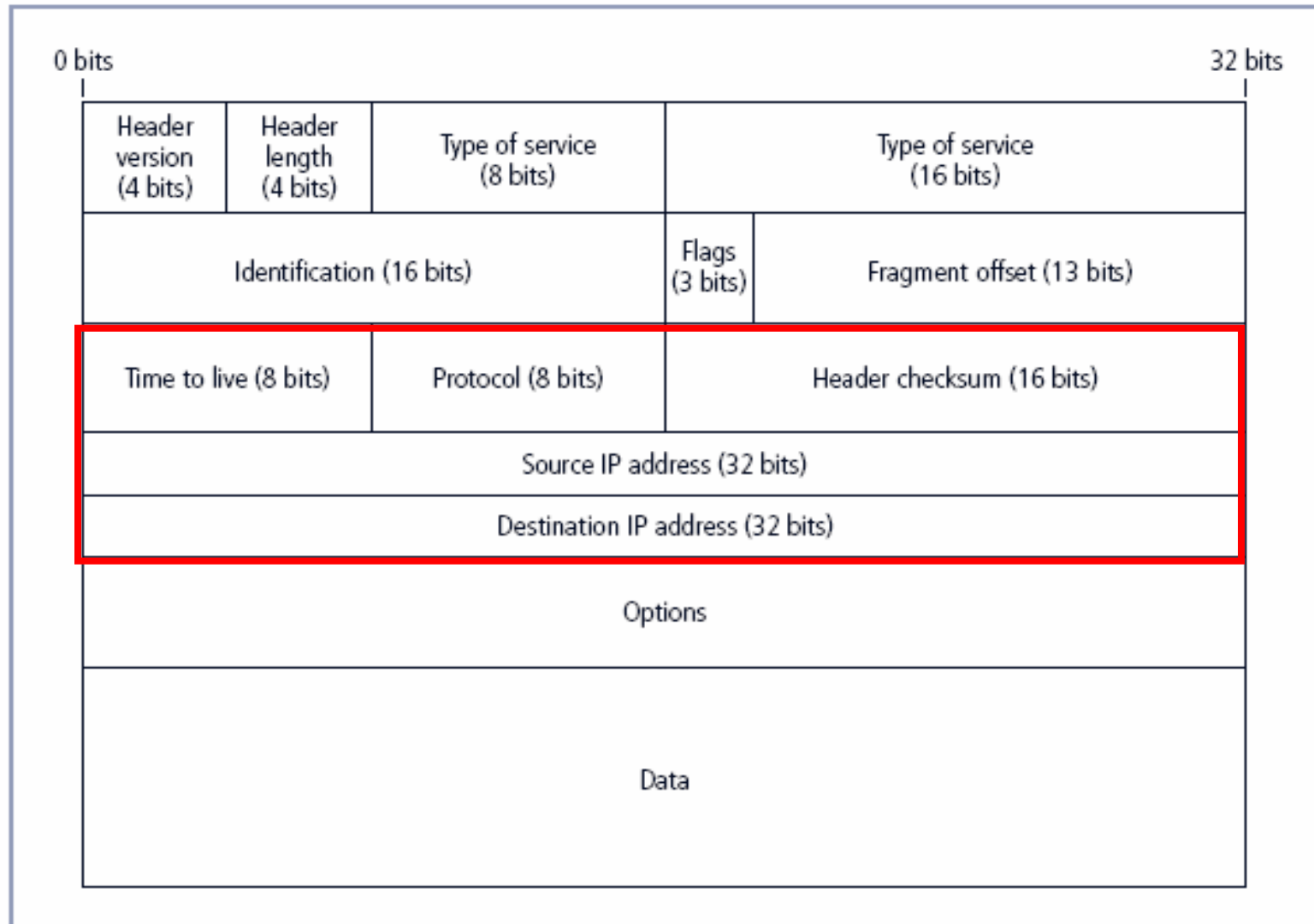
Packet Filtering (1)

- Packet filtering firewalls examine header info. for data pkts
- Most often based on combination of:
 - Internet Protocol (IP) source and destination address
 - Direction (inbound or outbound)
 - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), destination port requests
- Simple firewall models enforce rules that prohibit packets with certain IP address ranges

Packet Filtering (2)

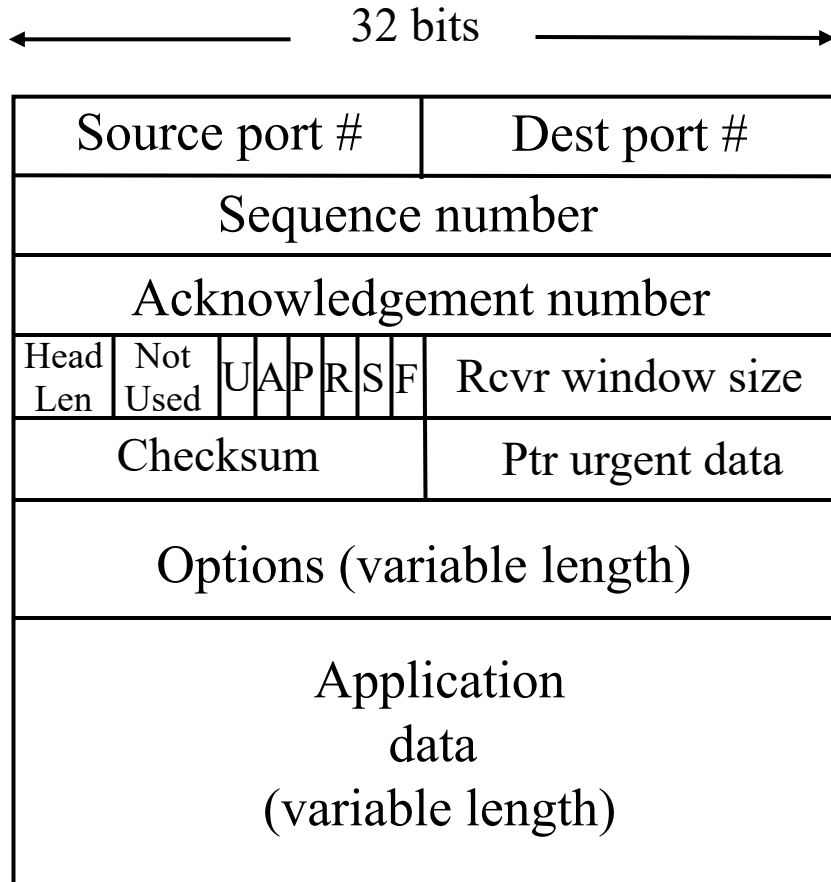
- Three subsets of packet filtering firewalls:
 - *Static filtering*: requires manual configuration of firewall rules that determine which packets are allowed, denied
 - *Dynamic filtering*: firewall can react to emergent event, update/create rules to deal with it
 - *Stateful inspection*: firewalls track each network connection between internal and external systems using a state table

IPv4 Packet Structure (Fig. 6-1)

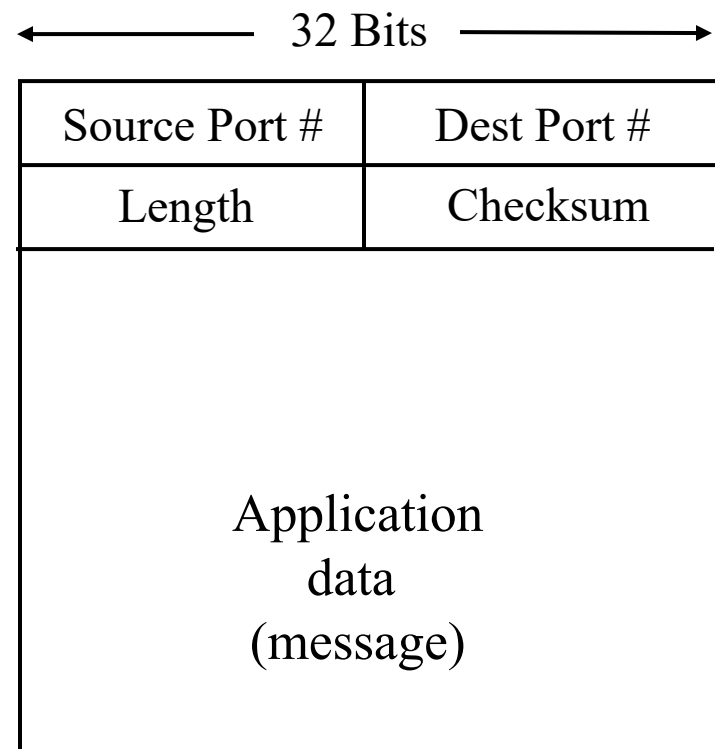


TCP, UDP Segment Structures

TCP Segment



UDP Segment



Source: J.F. Kurose and K.W. Ross,
Computer Networking: A Top-Down Approach,
7th ed., Addison-Wesley, 2013.

Packet Filtering Router (Fig. 6-4)

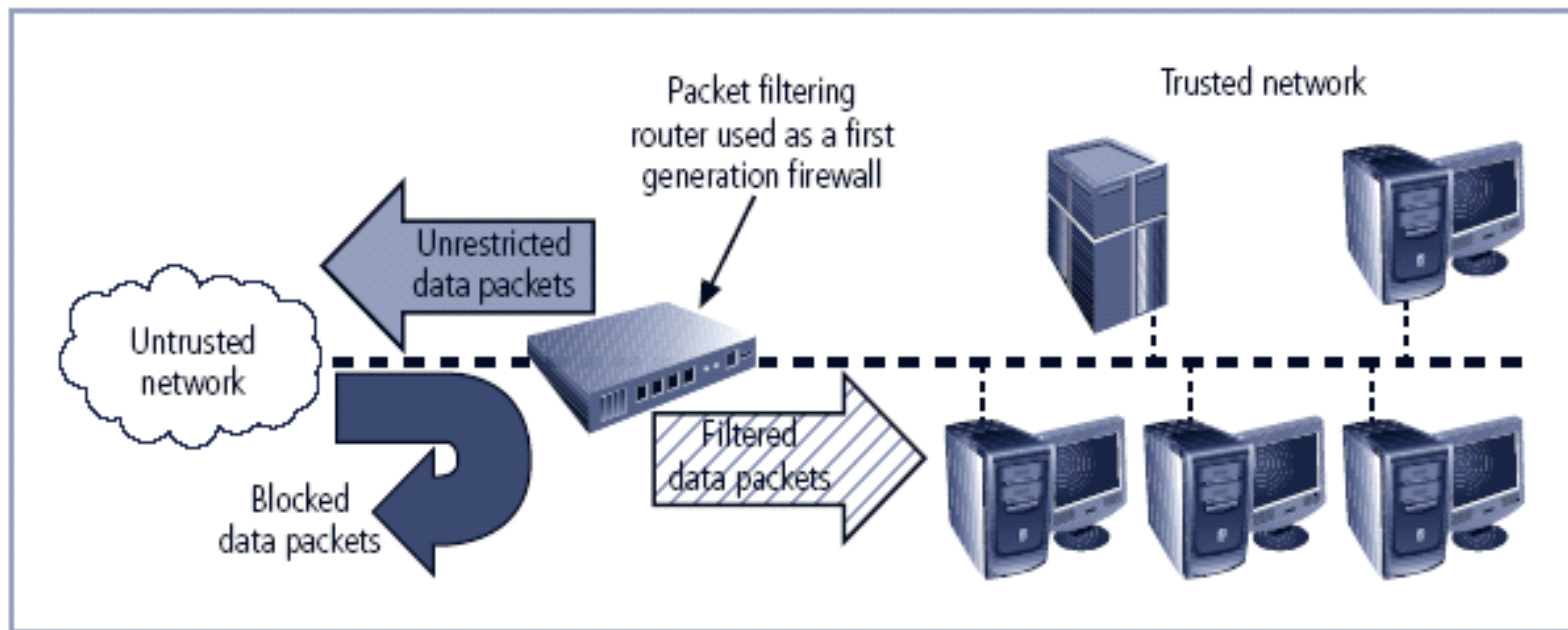


FIGURE 6-4 Packet Filtering Router

Sample Firewall Rules (Table 6-1)

TABLE 6-1 Sample Firewall Rule and Format

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Application Gateways

- Frequently installed on a dedicated computer; also called *proxy server*
- Proxy server is often placed in unsecured area of network (e.g., DMZ) \Rightarrow it faces higher levels of risk from attackers
- We can place extra filtering routers behind the proxy server to protect internal systems

Circuit Gateways

- Circuit gateway firewall: transport layer
- Does not usually look at data traffic flowing between two networks; prevents direct connections between one network and another
- Mechanism: create tunnels connecting specific processes/systems on each side of firewall; only allow authorized traffic in tunnels

MAC Layer Firewalls

- Operates at data-link layer
- Considers specific host computer's identity in filtering decision
- Only outbound traffic originating from MAC addresses of specific computers allowed
 - Mechanism: link (MAC address, Ethernet port #), administered via switches

Hybrid Firewalls

- Combine elements of multiple types of firewalls (e.g., packet filtering and proxy servers; packet filtering and circuit gateways)
- Alternately, may consist of two separate firewall devices; separate firewall systems connected to work together

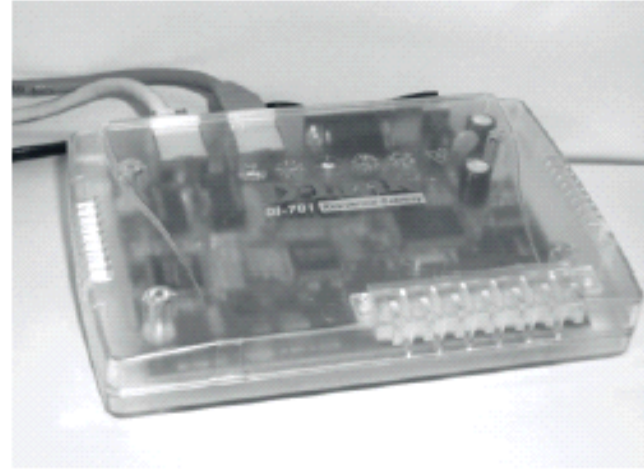
Firewall Categorization (2): Development Era

- First generation: static packet filtering firewalls
- Second generation: application-level firewalls or proxy servers
- Third generation: stateful inspection firewalls
- Fourth generation: dynamic packet filtering firewalls; allow only packets with particular source, destination and port addresses to enter
- Fifth generation: kernel proxies; specialized form working under operating system kernel

Firewall Categorization (3): Deployment Structure

- Most firewalls are appliances: stand-alone, self-contained systems
- Commercial firewall systems: consists of firewall software running on general-purpose computer
- Small office/home office (SOHO) or residential firewalls connect users' LANs or specific computers to network devices
 - Often, firewall software placed on user system

Sample Firewall Devices (Fig. 6-6)



Firewalls Categorization (4): Architectural Implementation

- Firewall devices can be configured in a number of network connection architectures
- Four common architectural implementations of firewalls:
 - Packet filtering routers
 - Screened host firewalls
 - Dual-homed firewalls
 - Screened subnet firewalls

Packet Filtering Routers

- Most organizations with Internet connection have a router connecting to Internet
- Routers can be configured to reject packets that org. forbids entering its network
- Drawbacks: limited auditing, weak authentication

Packet Filtering Router (Fig. 6-4)

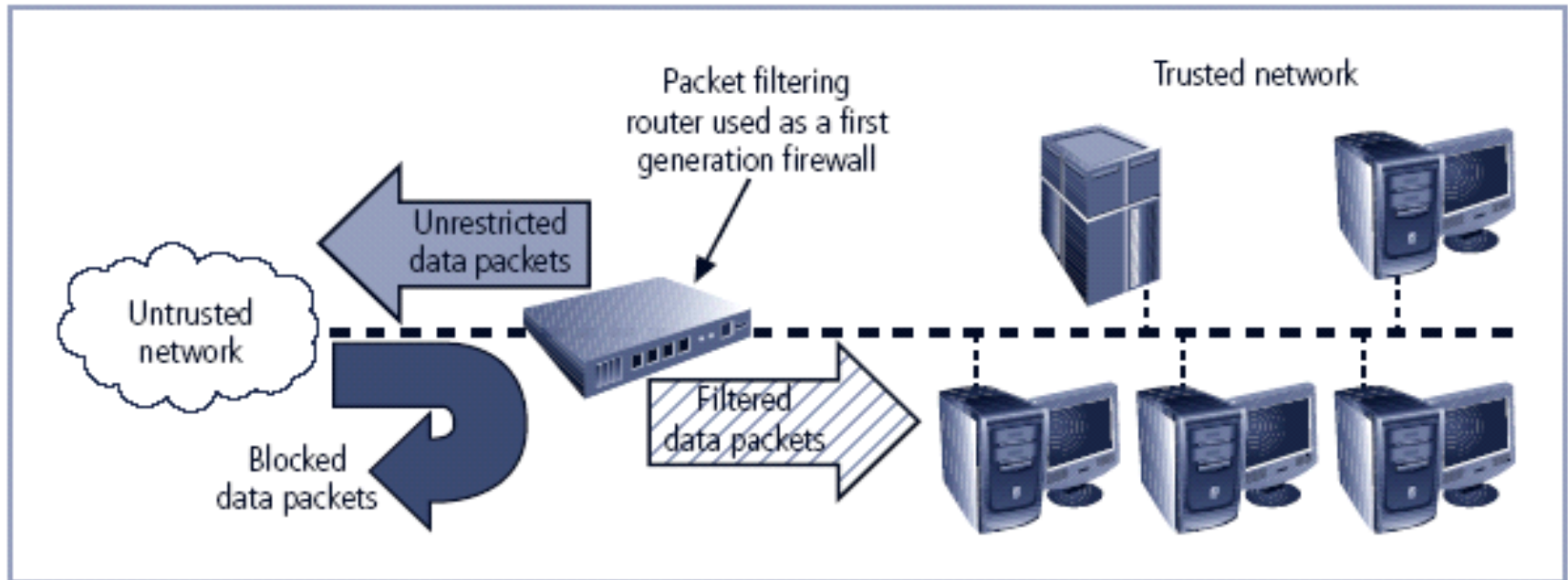


FIGURE 6-4 Packet Filtering Router

Screened Host Firewalls

- Combines packet filtering router with stand-alone firewall (e.g., application proxy server)
- Allows router to pre-screen packets to minimize load on internal proxy
- Separate host is often referred to as *bastion host*; can be rich target for external attacks, needs to be secured carefully

Screened Host Firewall (Fig. 6-11)

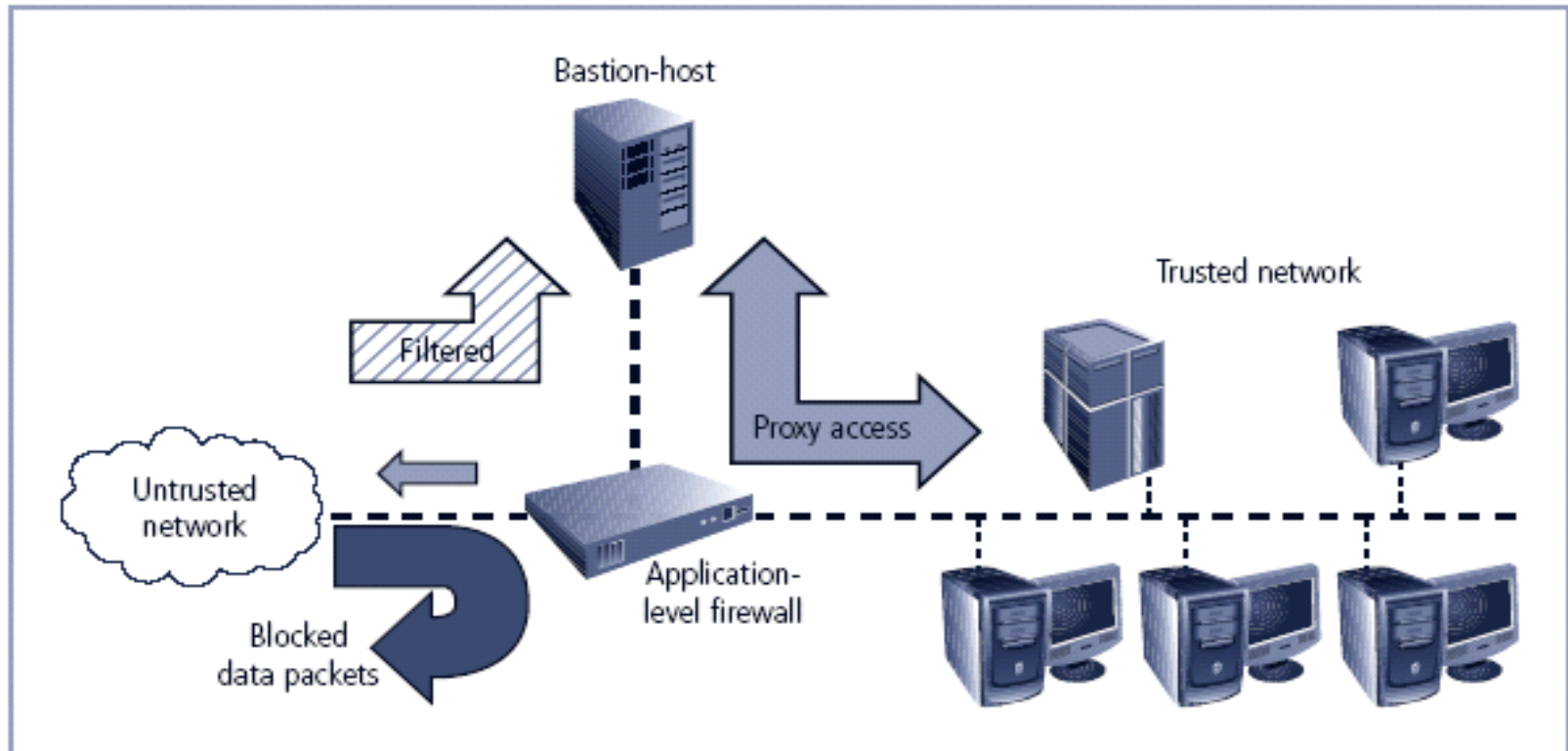


FIGURE 6-11 Screened Host Firewall

Dual-Homed Host Firewalls

- Bastion host contains two network interface cards (NICs): one connected to external network, other connected to internal network
- Architecture typically uses network address translation (NAT)
 - Another barrier to intrusion from attackers

Non-Routable IP Address Ranges

Type	IP Address Range	CIDR Mask	IP Subnet Mask	# Addresses
Class A	10.0.0.0 – 10.255.255.255	/8	255.0.0.0	2^{24} (> 16 M)
Class B	172.16.0.0 – 172.31.255.255	/12 or /16	255.240.0.0 or 255.255.0.0	2^{12} (4,096) or 2^{16} (> 65K)
Class C	192.168.0.0 – 192.168.255.255	/16 or /24	255.255.0.0 or 255.255.255.0	2^{16} (> 65K) or 2^8 (256)

Source: Adapted from Table 6-4 in textbook, RFC 1918

Dual-Homed Firewall (Fig. 6.12)

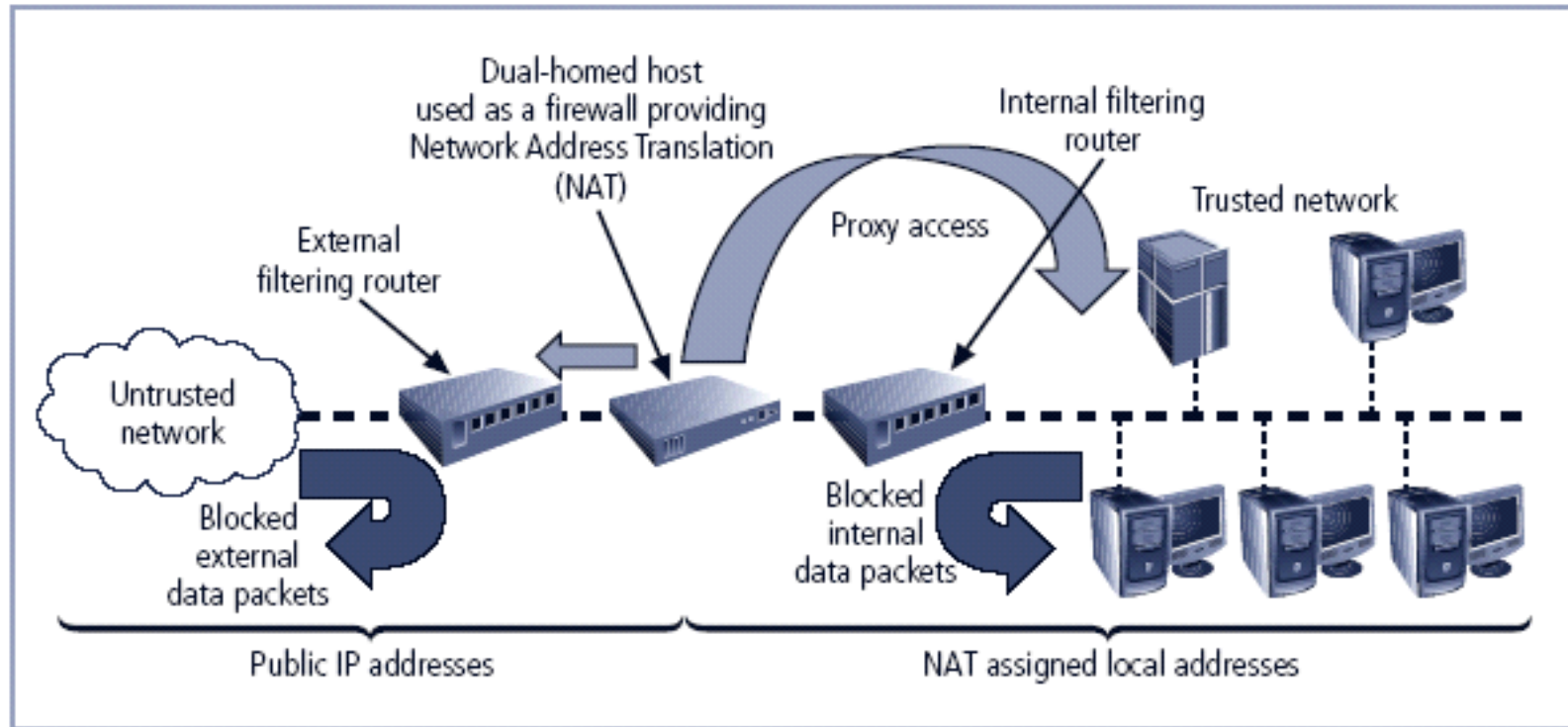


FIGURE 6-12 Dual-Homed Host Firewall

Screened Subnet Firewalls (DMZ) (1)

- Dominant architecture used today
- Typically has ≥ 2 internal bastion hosts behind packet filtering router, each host protects trusted network:
 - Connections from outside (untrusted network) routed through external filtering router
 - Connections from outside (untrusted network) are routed into, out of routing firewall to separate network segment: *demilitarized zone* (DMZ)
 - Connections into trusted internal network allowed only from DMZ bastion host servers

Screened Subnet Firewalls (DMZ) (2)

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

Screened Subnet Firewall (Fig. 6-13)

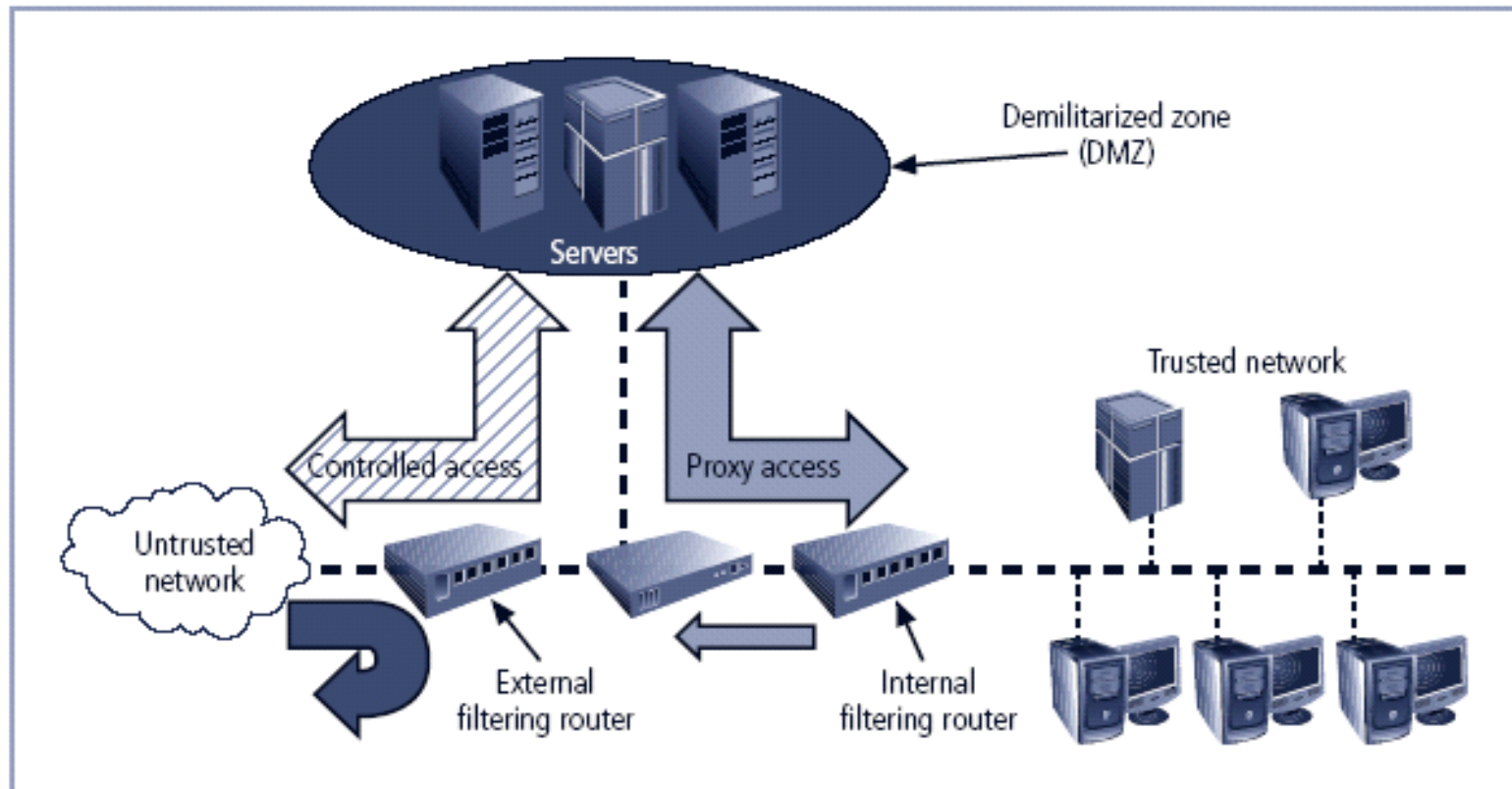


FIGURE 6-13 Screened Subnet (DMZ)

Selecting the Right Firewall

- When selecting firewall, consider a number of factors:
 - Which is the best trade-off between protection, cost for needs of organization?
 - What's included (and what's *not*) in base price?
 - How easy is configuration? Are staff technicians available for this purpose?
 - How well firewall adapt to org.'s growing network?
- Second most important issue: cost

Configuring and Managing Firewalls

- Each firewall device must have own set of configuration rules regulating its actions
- Firewall policy configuration is usually complex and difficult (“black art”)
- When security rules conflict with business performance, security often loses!
- Linux firewall

Best Practices for Firewalls

- All traffic from trusted network is allowed out
- Use MAC address filtering for Ethernet ports, authentication for wireless LANs
- Firewall device never directly accessed from public network
- Allow Simple Mail Transport Protocol (SMTP)
- Deny Internet Control Message Protocol (ICMP)
- Telnet access to internal servers should be blocked
- If Web services offered outside firewall, block HTTP traffic from reaching internal networks

Firewall Rules

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

Example Network Config. (Fig. 6-14)

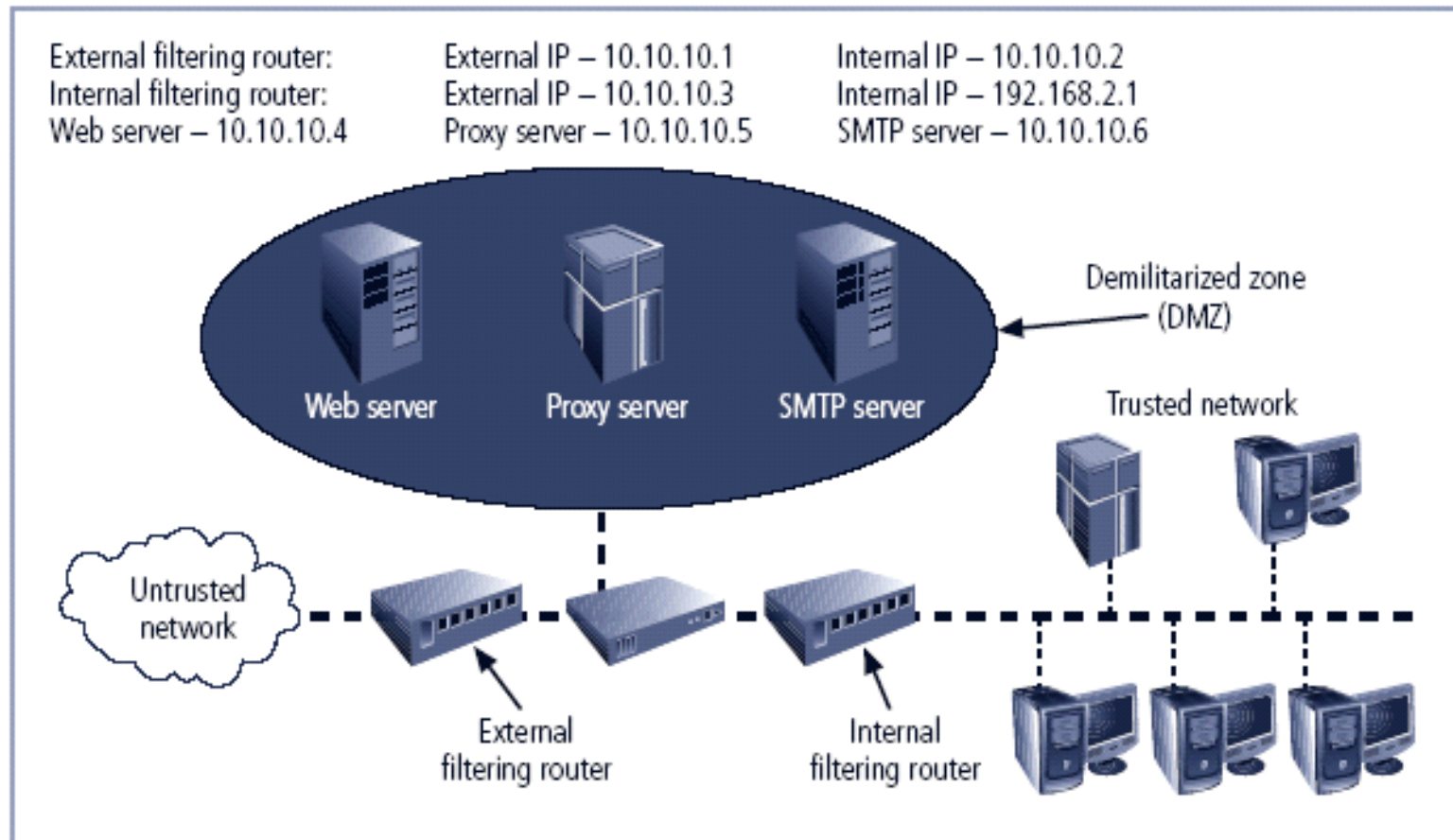


FIGURE 6-14 Example Network Configuration

Firewall Rules (1) (Table 6-16)

TABLE 6-16 External Filtering Firewall Rule Set

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

Firewall Rules (2) (Table 6-17)

TABLE 6-17 Internal Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.3	Any	Deny
3	Any	Any	192.168.2.1	Any	Deny
4	10.10.10.3	Any	Any	Any	Deny
5	192.168.2.1	Any	Any	Any	Deny
6	192.168.2.0	Any	Any	Any	Allow
7	10.10.10.5	Any	192.168.2.0	Any	Allow
8	Any	Any	Any	Any	Deny

Virtual Private Networks (VPNs) (1)

- Private, secure network connection between systems over insecure, public Internet
- Securely extends org.'s internal network connections to remote locations beyond its perimeter

Virtual Private Networks (VPNs) (2)

- VPN must achieve three goals:
 - Encapsulate incoming, outgoing data
 - Encrypt incoming, outgoing data
 - Authenticate remote computer, user (?)

Transport Mode

- IP packet data is encrypted, header info. is not
- Lets user establish secure link directly with remote host easily
- Two popular uses:
 - End-to-end transport of encrypted data
 - Remote worker connects to office network over Internet by connecting to VPN server at perimeter

Transport Mode VPN (Fig. 6-18)

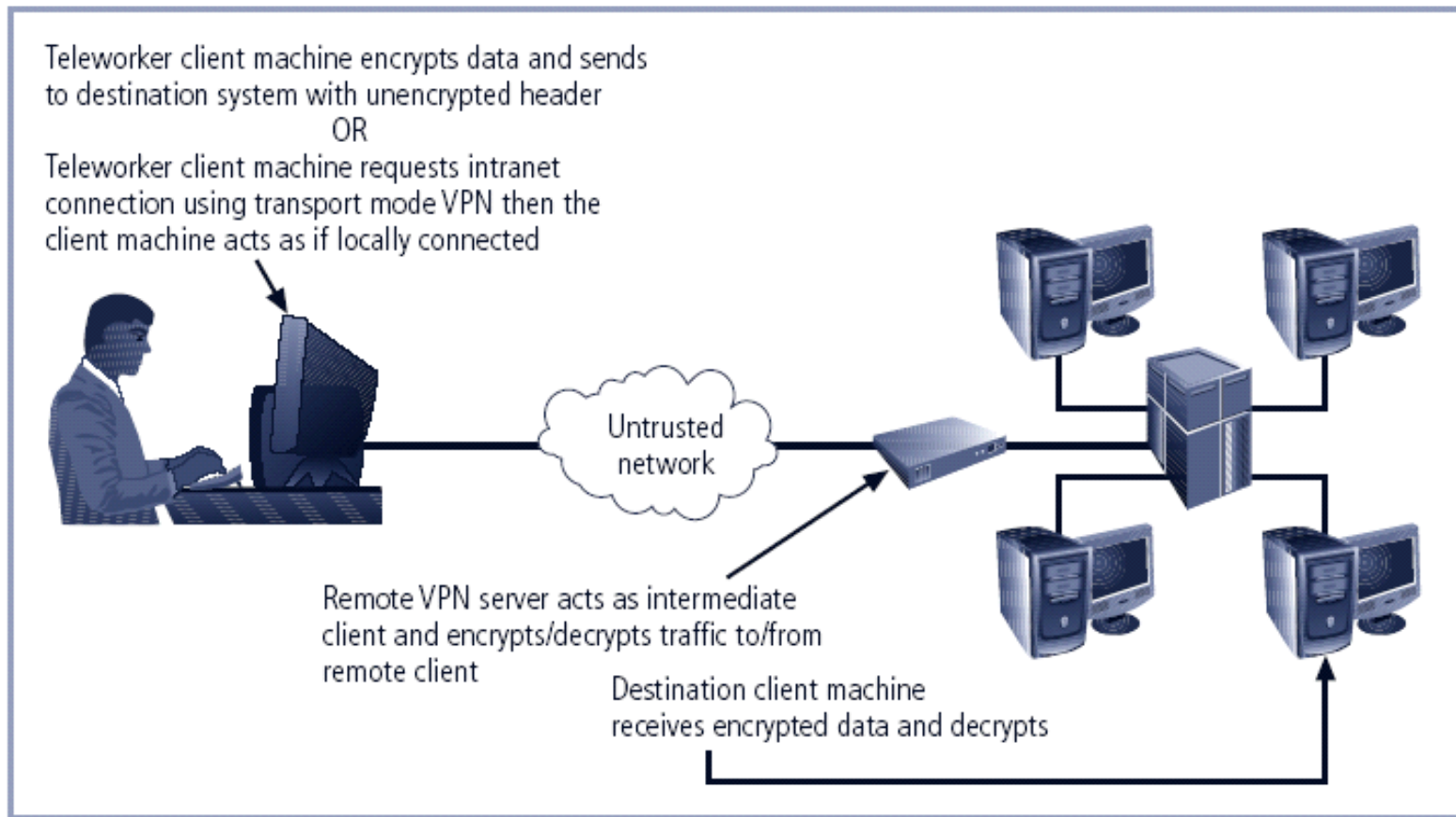


FIGURE 6-18 Transport Mode VPN

Tunnel Mode

- Org. sets up two perimeter tunnel servers as *encryption points*: all net traffic encrypted in transit
- Main benefit to tunnel mode: intercepted packets reveal nothing about true destination
- Examples of tunnel mode VPNs:
 - Pulse Secure appliance
 - Microsoft Internet Application Gateway

Tunnel Mode VPN (Fig. 6-19)

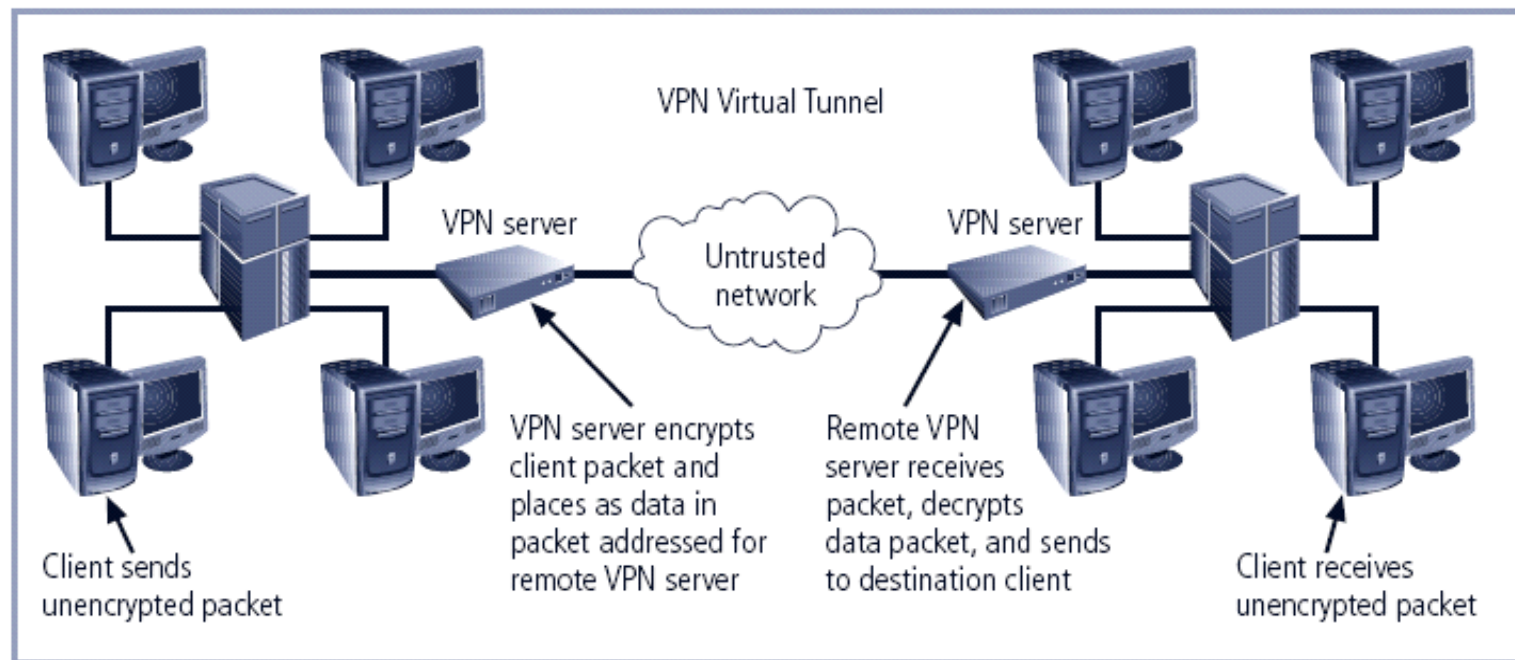
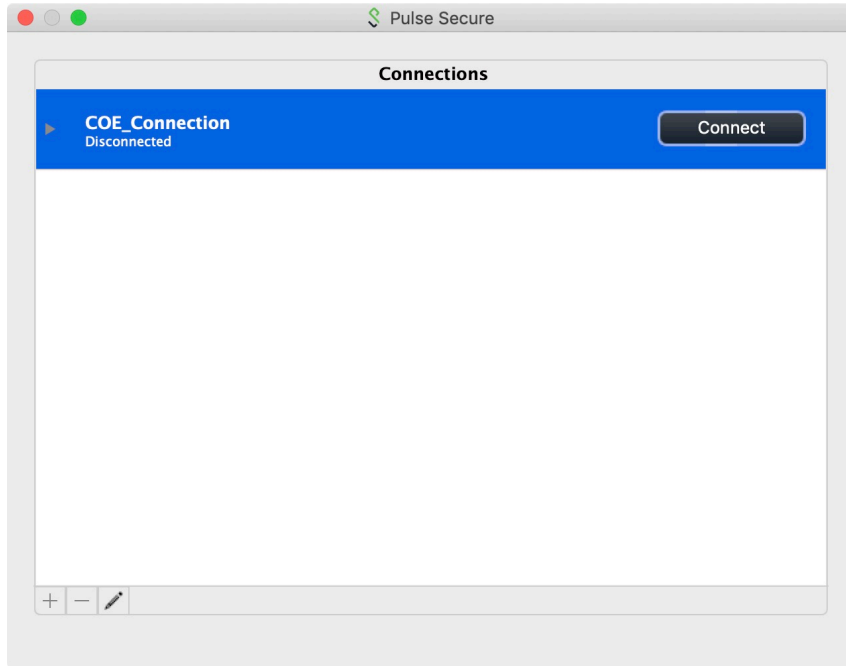


FIGURE 6-19 Tunnel Mode VPN

Example VPN: Pulse Secure



Source: Pulse Secure, LLC;

<https://www.pulsesecure.net/products/psa-series/>
(PSA 5000)

– More VPN info: A. Marshall, Tech Radar,
<https://www.techradar.com/vpn/best-vpn>,
16 May 2019.



Summary

- Firewall technology
 - Four methods for categorization
 - Firewall configuration and management
- Virtual Private Networks
 - Two modes

Intrusion Detection, Access Control and Other Security Tools

CSE 4471: Information Security

Instructor: Adam C. Champion, Ph.D.

Intrusion Terminology

- ***Intrusion:*** attack on information where malicious perpetrator tries to break into, disrupt system
- ***Intrusion detection:*** includes procedures and systems created and operated to detect system intrusions
- ***Intrusion reaction:*** covers actions organization takes upon detecting intrusion
- ***Intrusion correction activities:*** restore normal operations
- ***Intrusion prevention:*** actions that try to deter intrusions proactively

Intrusion Detection Systems (IDSs)

- Detects “configuration” violation, sounds alarm
- IDSs inform admins of trouble via e-mail, pagers
- Can configure systems to notify external security org. of “break-in”

IDS Terminology

- *Alert, alarm:* self-explanatory
- *False negative:* IDS fails to detect *actual* attack
- *False positive:* Attack alert when none occurred
- *Confidence value:* Estimate of attack probability
- *Alarm filtering:* self-explanatory

IDS Classification Methods

① IDS detection methods:

- Signature-based (sig IDS)
- Statistical anomaly-based (stat IDS)

② IDS operation:

- Network-based intrusion detection syst. (NIDS)
- Host-based IDS (HIDS)
- Application-based systems (AppIDS)

Classification (1): Sig. IDS

- Find network, host traffic patterns that match known signatures
- Advantage: Many attacks have distinct signatures
- Disadvantages:
 - IDS's signature database must be updated to keep pace with new attacks
 - Malicious code authors intentionally use tricks to fool these IDSs

Classification (1): Stat. IDS

- Statistical anomaly-based IDS sample network activity, compare to “known normal” traffic
- IDS sounds alarm when activity is outside baseline parameters
- Advantage: IDS can detect new types of attacks
- Disadvantages:
 - Requires more overhead, compute power than signature-based IDSs
 - May generate many false positives

Host IDS: Examines the data in files stored on host and alerts systems administrators of changes

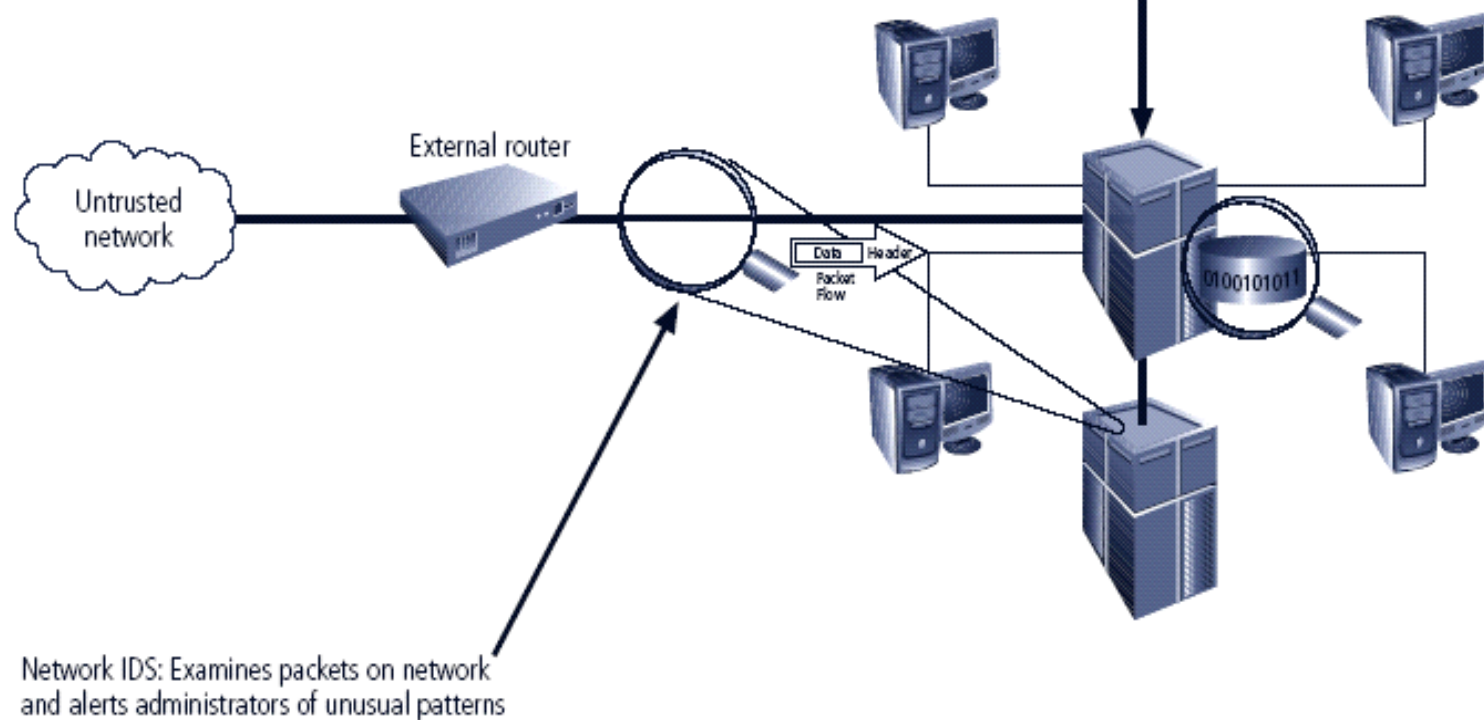


FIGURE 7-1 Intrusion Detection Systems

Classification (2): NIDS

- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- When examining packets, a NIDS looks for attack patterns
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment

NIDS Signature Matching

- NIDSs look for attack patterns for detection
- Accomplished via certain implementation of TCP/IP stack:
 - Protocol stack verification: look for invalid packets
 - App. protocol verification: look at higher-order protocols for unexpected behavior or improper use

NIDS Advantages, Disadvantages

Advantages

- Org. can monitor large network with few devices
- Passive; deployment minimally disrupts operations
- Less susceptible to attack; attackers may not detect them

Disadvantages

- Can be overwhelmed by volume of network traffic
- Need to monitor *all* traffic
- Cannot analyze encrypted network packets
- Cannot determine if attack was successful
- Cannot detect some attacks (e.g., fragmented packets)

Classification (2): HIDS

- HIDS runs on a particular computer, monitors activity only on that system
- Benchmarks, monitors key system files; detects when intruders' file I/O
- HIDSs work on principle of configuration management
- Unlike NIDSs, HIDSs can be installed to access info. that's encrypted in transit over network

HIDS Advantages, Disadvantages

Advantages

- Detect local events, attacks on host systems that NIDSs may not
- Can view encrypted traffic (as it has been decrypted on system)
- HIDSs unaffected by switched network protocols
- Can detect inconsistencies in apps, programs by examining audit logs

Disadvantages

- Harder to manage than NIDSs
- Vulnerable to attacks against host operating system, HIDS
- Cannot detect scans of multiple hosts, non-network devices
- HIDSs potential targets for denial-of-service (DoS) attack
- May use lots of disk space
- Possible large compute performance overhead on host systems

Application-Based IDS

- Application-based IDS (AppIDS) looks at apps for abnormal events
- AppIDS may be configured to intercept requests:
 - File System
 - Network
 - Configuration
 - Process's Virtual Memory Address Space

Advantages and Disadvantages of AppIDSs

- Advantages

- Aware of specific users; can observe interaction between apps and users
- Functions with encrypted incoming data

- Disadvantages

- More susceptible to attack
- Less capable of detecting software tampering
- May be fooled by forms of spoofing

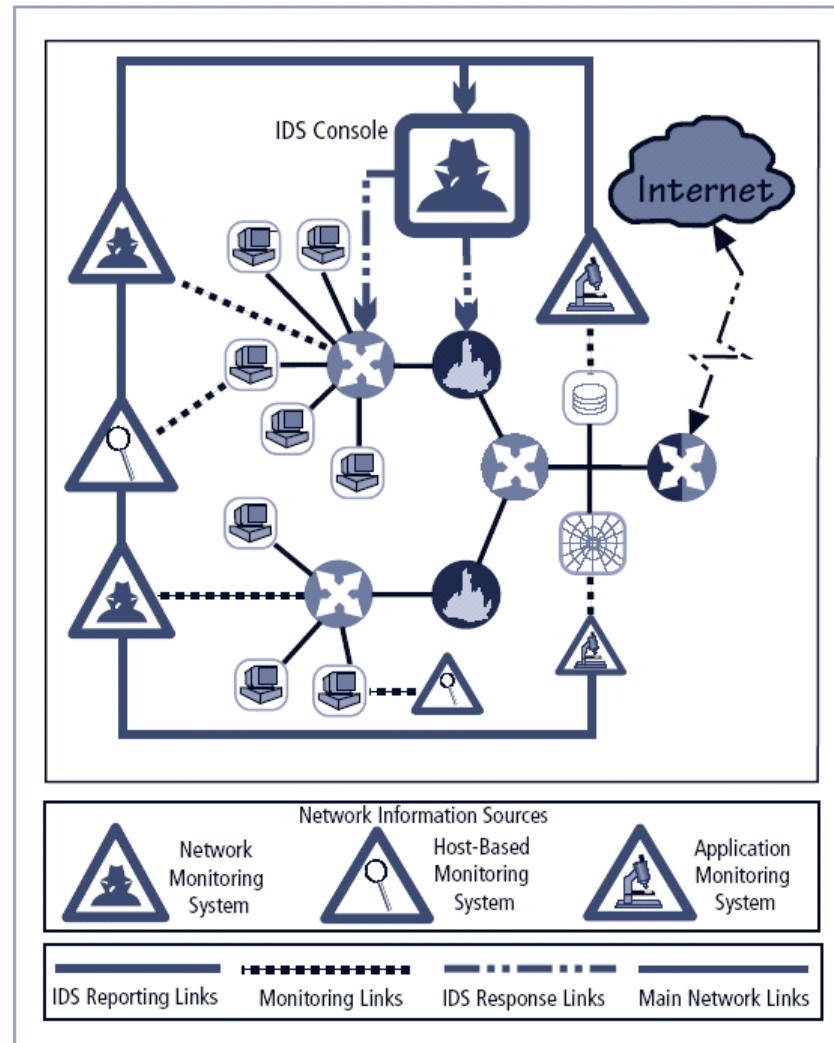
Selecting IDS Approaches and Products

- Technical and policy considerations
 - What is your systems environment?
 - What are your security goals?
 - What is your existing security policy?
- Organizational requirements and constraints
 - What requirements are given from outside the org.?
 - What are your org's resource constraints? (\$\$\$)

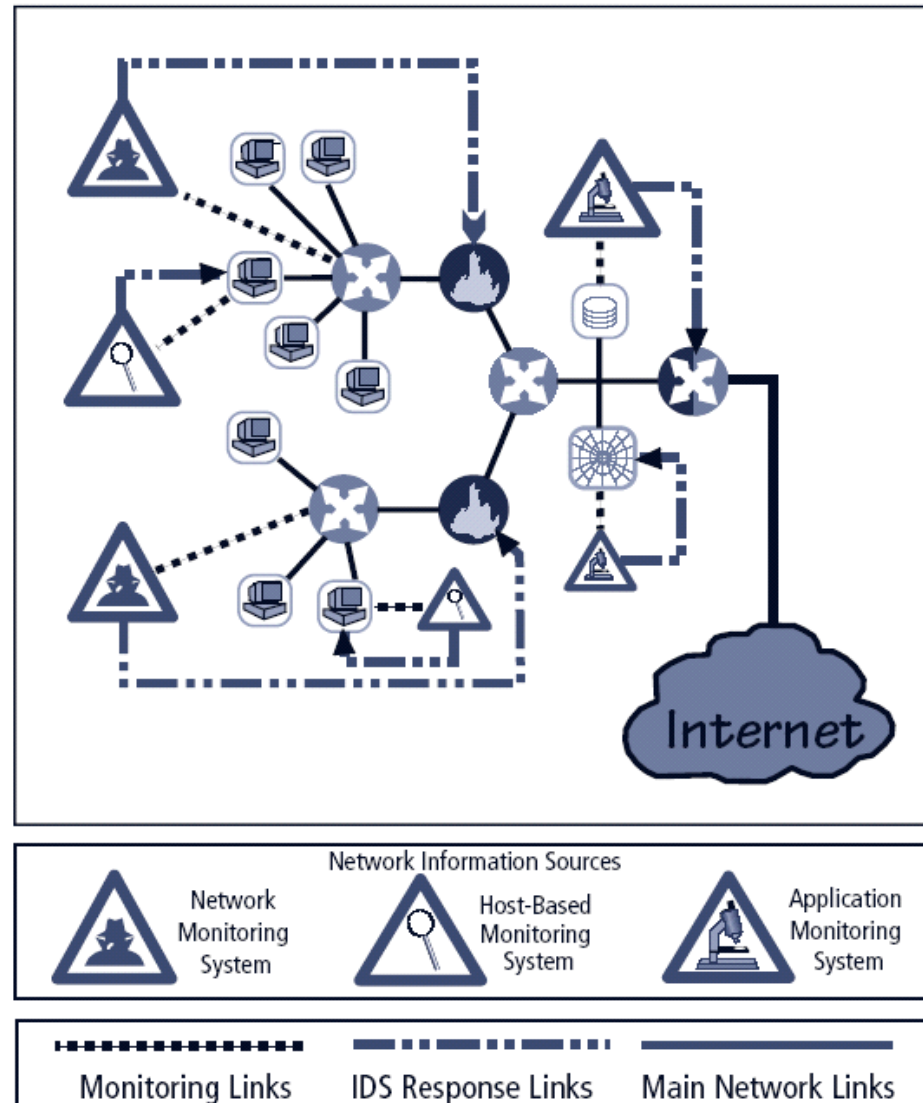
IDS Control Strategies

- An IDS can be implemented via one of three basic control strategies
 - Centralized: all IDS control functions are implemented and managed in a central location
 - Fully distributed: all control functions are applied at the physical location of each IDS component
 - Partially distributed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks

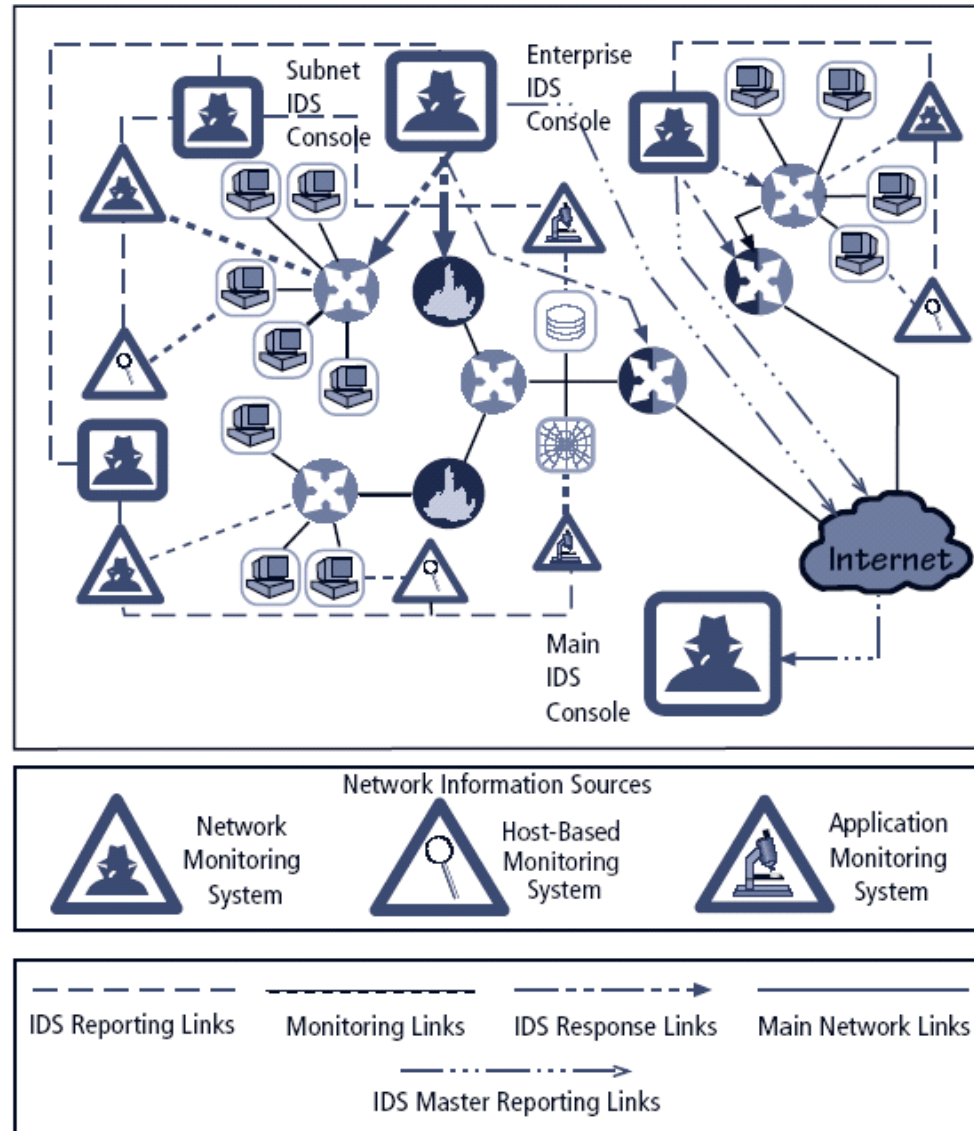
Centralized IDS Control (Fig. 7-4)



Fully Distributed IDS Control (Fig. 7-5)



Partially Distributed IDS Control (Fig. 7-6)



IDS Deployment Overview

- IDS system placement can be a “black art”
 - Similar to “what type of IDS should be use?” question
- Need to balance organization’s security needs with budget
- We can use NIDS and HIDS in tandem to cover both individual systems that connect to an org’s networks *and* the networks themselves

Deploying NIDSs (1)

- NIST recommends four locations for NIDSs:
 - Location 1: behind each external firewall, in the network DMZ
 - Location 2: outside an external firewall
 - Location 3: on major network backbones
 - Location 4: on critical subnets

Deploying NIDSs (2) (Fig. 7-7)

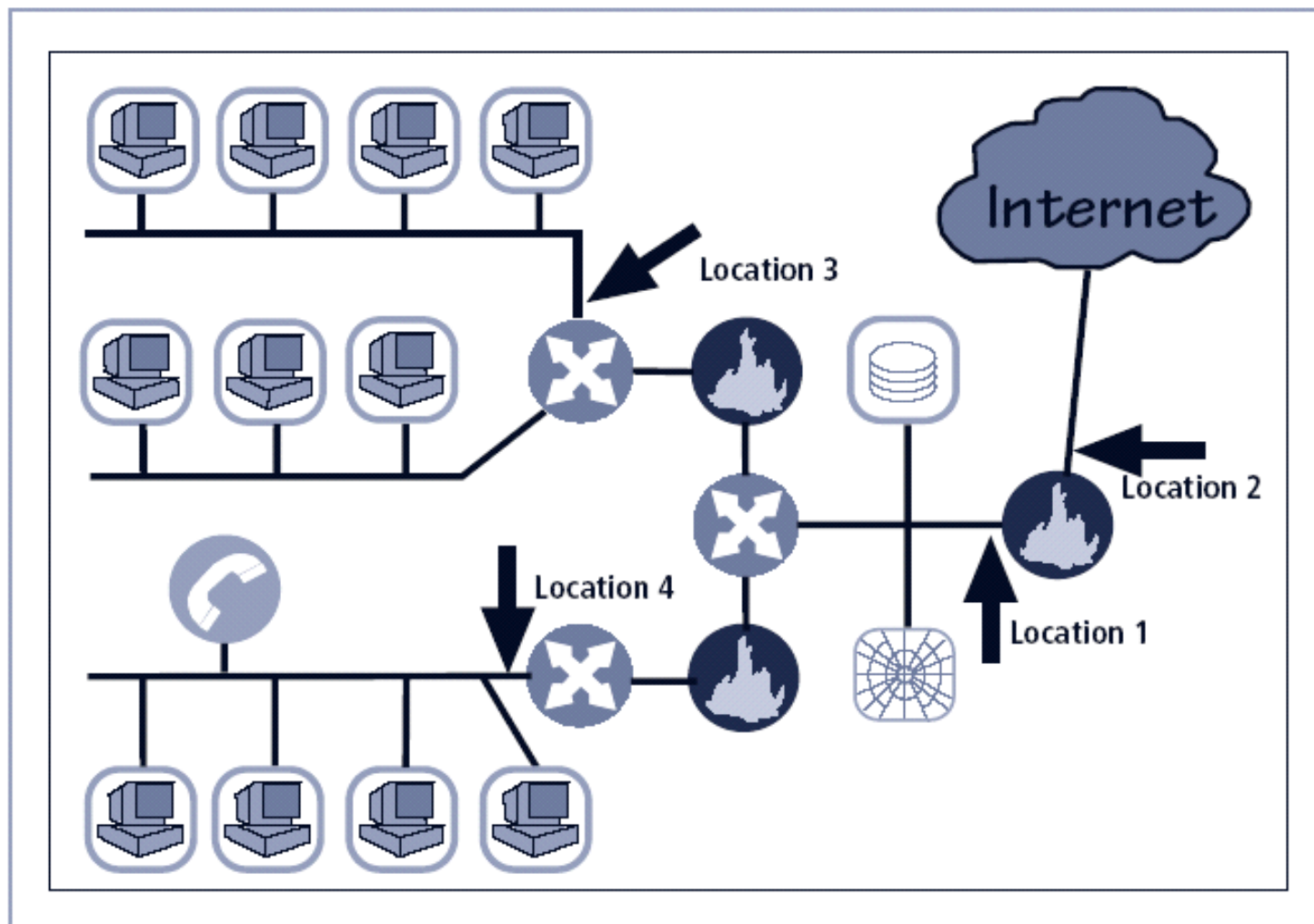


FIGURE 7-7 Network IDS Sensor Locations¹⁷

Deploying HIDS

- Setting up HIDSs: tedious, time-consuming (?)
- Steps:
 - First: install HIDSs on most critical systems
 - Next: install HIDSs on all systems or until organization reaches tolerable degree of coverage

Measuring Effectiveness of IDSs

- IDSs are evaluated using two dominant metrics:
 - # of attacks detected in a known collection of probes
 - Network bandwidth at which IDSs fail
- Example: *At 1 Gbits/sec, IDS detected 95% of directed attacks against it*
- Many vendors provide test suites for verification
- Example test suites:
 - Record, retransmit real packet trace from virus/worm
 - Perform same for malformed packets (e.g., SYN flood)
 - Launch

Honeypots, Honeynets, and Padded Cell Systems

- **Honeypots:** decoy systems designed to lure potential attackers away from critical systems
- Design goals:
 - Divert attacker from accessing critical systems
 - Gather information about attacker's activity
 - Encourage attacker to linger so admins can document event, respond
- **Honeynets:** collection of honeypots connected in a subnet
- **Padded cell:** honeypot protected in order to hinder compromise
 - Typically works in tandem with traditional IDS
 - When IDS detects attackers, it transfers them to “special environment” where they cannot cause harm (hence the name)

Honeypots: Advantages and Disadvantages

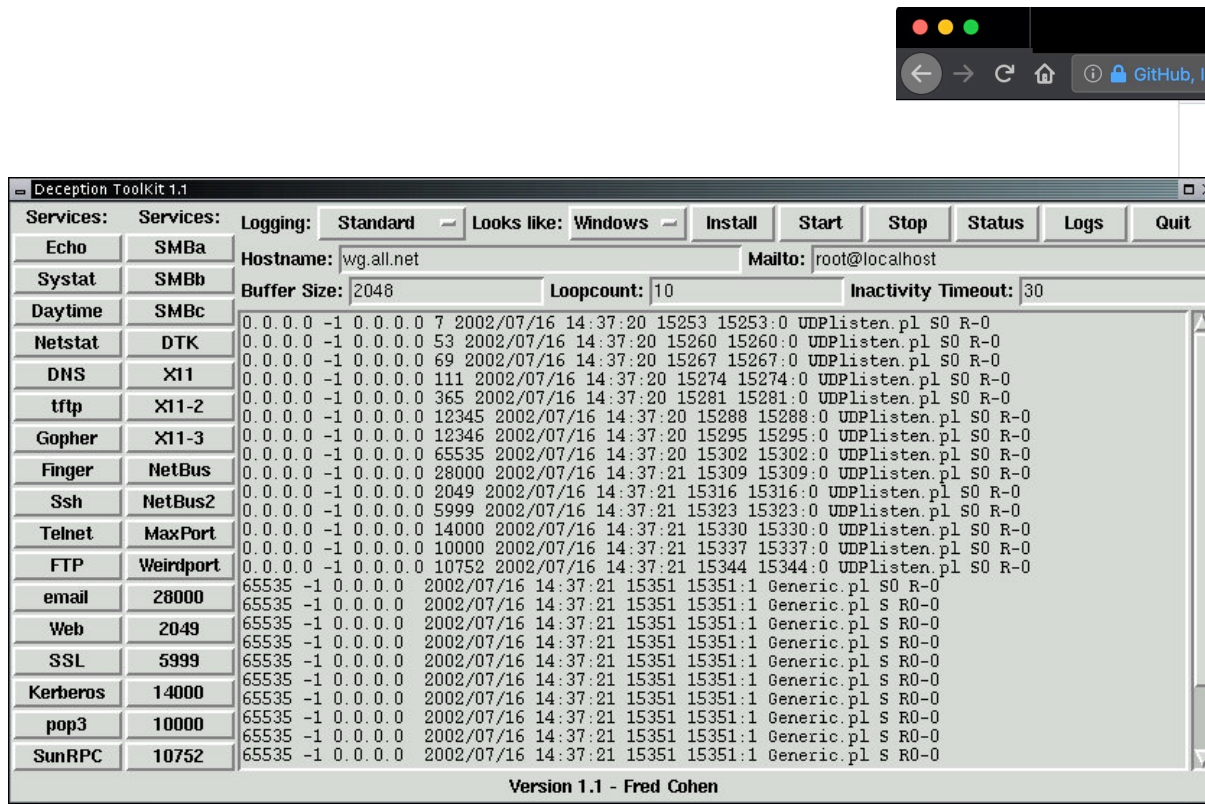
Advantages

- Diverts attackers to targets they can't damage
- Admins have time to determine response
- Honeypots can monitor attackers' actions; attack logs can help improve system security
- Honeypots may catch insiders snooping around network

Disadvantages

- Legal implications are not well defined
- Honeypots' effectiveness as security tech is unclear
- Expert attacker detecting honeypot may get angry, launch worse attack against org.
- Admins, security managers need expertise to use honeypots

Honeytrap Examples



Awesome Honeytraps awesome

A curated list of awesome honeytraps, plus related component services, and others, with a focus on free and open source projects.

There is no pre-established order of items in each category, so please read the [guide](#).

Discover more awesome lists at sindresorhus/awesome.

Contents

- [Related Lists](#)
- [Honeytraps](#)
- [Honeyd Tools](#)
- [Network and Artifact Analysis](#)
- [Data Tools](#)
- [Guides](#)

Related Lists

Sources: Fred Cohen & Associates (<http://all.net/WG/index.html>);
<https://github.com/paralax/awesome-honeytraps/>

Trap and Trace Systems

- Various techniques that detect intrusion, trace it to origin
- “Trap” consists of honeypot/padded cell, alarm
- Legal drawbacks to trap and trace:
 - Enticement: attracts attacker to system by placing tantalizing info. in certain places
 - Entrapment: lures person into committing crime for conviction purpose
 - Enticement is legal/ethical; entrapment is *not*
- More info: D.J. Gottfried, “Avoiding the Entrapment Defense in a Post-9/11 World,” *FBI Law Enforcement Bulletin*, 1 Jan. 2012, <https://leb.fbi.gov/articles/legal-digest/legal-digest-avoiding-the-entrapment-defense-in-a-post-911-world>.

Scanning and Analysis Tools (1)

- Often used to collect information that attacker would need to launch successful attack
- Attack protocol: sequence of attacker's steps to attack target system/network
- Footprinting: determining what hostnames, IP addresses a target org. owns
- Fingerprinting: systematic survey of resources found in footprinting stage
 - Useful for discovering weaknesses in org.'s network or systems

Scanning and Analysis Tools (2)

- Hostname queries: nslookup, dig (Un*x)
- IP address ownership:
 - whois, <https://whois.domaintools.com/>
- Internet search queries:
“Proprietary”, “Confidential”
- Also: <https://tools.wordtothewise.com/>

```
adamcchampion ~ > Teaching > CSE4471 > AdamSlides > nslookup bigcorp.com
Server:      2606:4700:4700::1111
Address:     2606:4700:4700::1111#53

Non-authoritative answer:
Name:   bigcorp.com
Address: 198.71.233.161

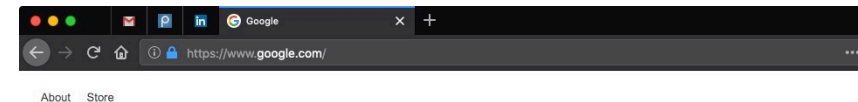
adamcchampion ~ > Teaching > CSE4471 > AdamSlides > dig bigcorp.com

; <<>> DiG 9.10.6 <<>> bigcorp.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 5328
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;bigcorp.com.                IN      A

;; ANSWER SECTION:
bigcorp.com.                529     IN      A      198.71.233.161

;; Query time: 43 msec
;; SERVER: 2606:4700:4700::1111#53(2606:4700:4700::1111)
;; WHEN: Sun Jun 02 15:25:38 EDT 2019
;; MSG SIZE rcvd: 56
```



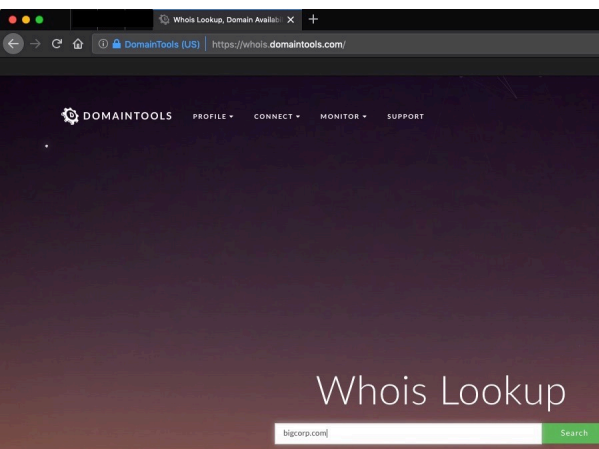
Sources: Self-taken screenshots;
<https://whois.domaintools.com>



proprietary confidential site:bigcorp.com

Google Search

I'm Feeling Lucky



Port Scanners

- Tools used by attackers, defenders to identify computers on network (plus other info.)
- Can scan for certain computers, protocols, resources (or generic scans)
- Example: nmap (<https://nmap.org/>)

```
15:39 Welcome to Termux!

Wiki: https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode

Working with packages:

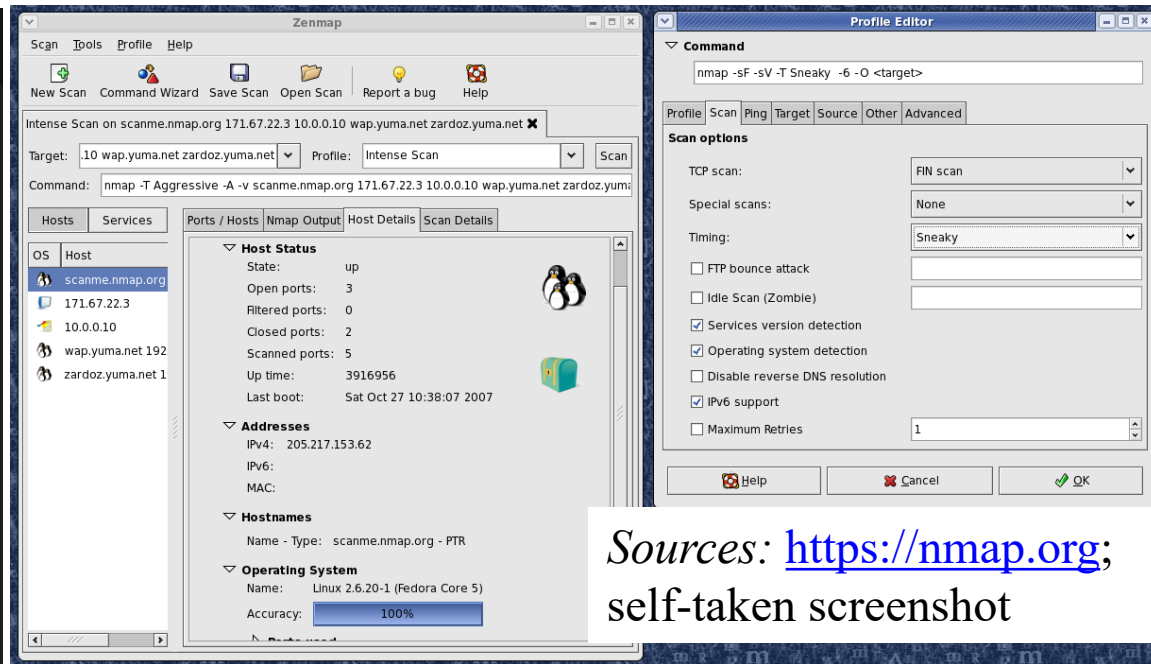
* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade

Subscribing to additional repositories:

* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo

Report issues at https://termux.com/issues

$ nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 15:38 EDT
```



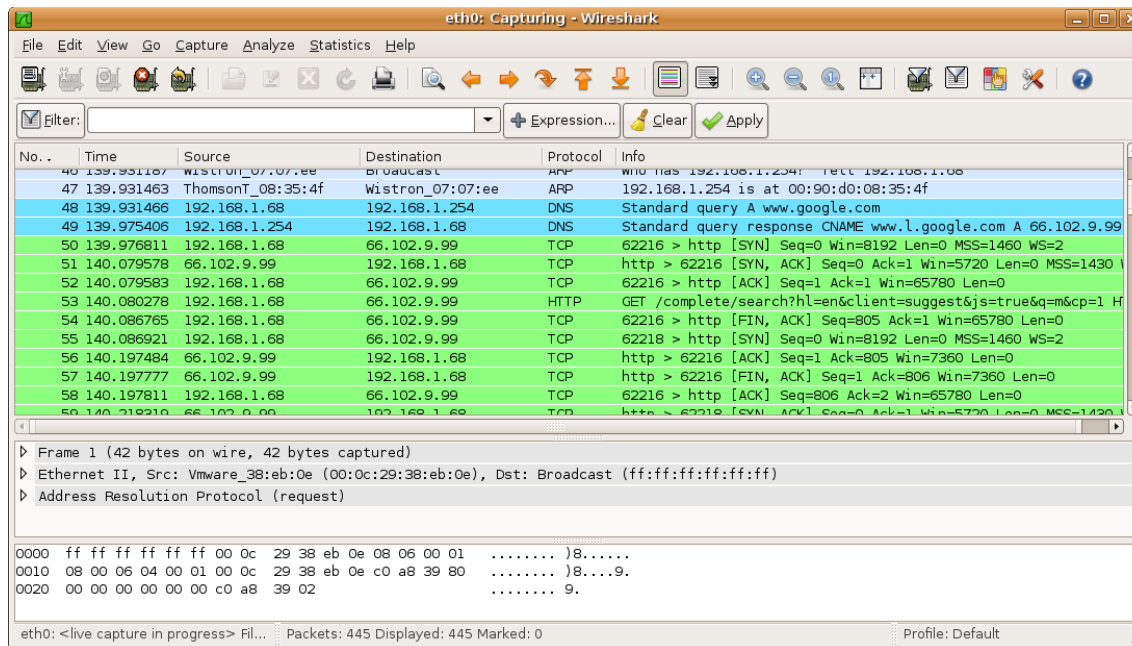
Firewall Analysis Tools

- Several tools automate discovery of firewall rules, assist admins in rule analysis
- Admins who are wary of using same tools that attackers use should remember:
 - User intent dictates how gathered info. is used
 - Need to understand ways to attack computer/network in order to defend it!
- Example: Nessus
(<https://www.tenable.com/products/nessus>)

Packet Sniffers

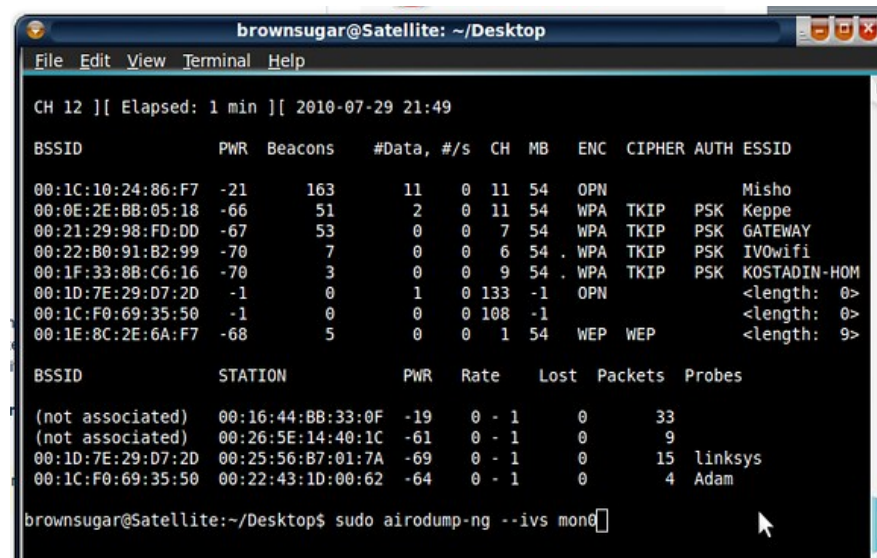
- Tool that gathers network packets, analyzes them
- Can provide network admin with info. to solve networking issues (or attacker eavesdropping)
- For legal use: admin must be on org.-owned network and have consent from net. owners
- Example tool: Wireshark

*Source: Wikipedia
(user SF007)*



Wireless Security Tools

- Organization needs to consider wireless security in tandem with its deployed wireless networks
- Toolkits can sniff wireless traffic, scan hosts, and assess network privacy
- Don't use WEP!
- Example tools:
 - Wireshark
 - aircrack-ng



The screenshot shows a terminal window titled "brownsugar@Satellite: ~/Desktop". The terminal displays the output of the command "sudo airodump-ng --ivs mon0". The output is divided into two sections. The first section shows a list of detected wireless networks with columns for BSSID, PWR, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The second section shows a list of stations with columns for BSSID, STATION, PWR, Rate, Lost, Packets, and Probes. The command prompt at the bottom is "brownsugar@Satellite:~/Desktop\$ sudo airodump-ng --ivs mon0".

```
brownsugar@Satellite: ~/Desktop
File Edit View Terminal Help

CH 12 ][ Elapsed: 1 min ][ 2010-07-29 21:49

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:1C:10:24:86:F7 -21   163      11   0  11  54  OPN             Miso
00:0E:2E:8B:05:18 -66    51       2   0  11  54  WPA  TKIP  PSK  Keppe
00:21:29:98:FD:DD -67    53       0   0   7  54  WPA  TKIP  PSK  GATEWAY
00:22:80:91:B2:99 -70     7       0   0   6  54  WPA  TKIP  PSK  IVOwif
00:1F:33:8B:C6:16 -70     3       0   0   9  54  WPA  TKIP  PSK  KOSTADIN-HOM
00:1D:7E:29:D7:2D -1      0       1   0  133 -1  OPN             <length: 0>
00:1C:F0:69:35:50 -1      0       0   0  108 -1             <length: 0>
00:1E:8C:2E:6A:F7 -68     5       0   0   1  54  WEP  WEP             <length: 9>

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
(not associated) 00:16:44:8B:33:0F -19   0 - 1    0     33
(not associated) 00:26:5E:14:40:1C -61   0 - 1    0      9
00:1D:7E:29:D7:2D 00:25:56:B7:01:7A -69   0 - 1    0    15 linksys
00:1C:F0:69:35:50 00:22:43:1D:00:62 -64   0 - 1    0      4 Adam

brownsugar@Satellite:~/Desktop$ sudo airodump-ng --ivs mon0
```

Source: Flickr (user: raynadata)

Access Control Devices

- Access control: authenticates, authorizes users
 - Authentication: validate a person's identity
 - Authorization: specify what the person can do with computers, networks
 - Recommended: use \geq two types of auth. technology
- Four main ways to authenticate person:
 - What a person knows (e.g., password);
 - What a person has (e.g., Duo Mobile app code);
 - Who a person is (e.g., fingerprint);
 - What a supplicant produces (e.g., work badge)

Summary

- *Intrusion detection system (IDS)* detects configuration violation and sounds alarm
- *Network-based IDS (NIDS) vs. host-based IDS (HIDS)*
- Complex selection of IDS products that fit an organization's needs!
- *Honeypots* are decoy systems; two variations are *honeynets* and *padded cell systems*

Summary

- Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of network
- Authentication is validation of prospective user's (supplicant's) identity