Network Security 2 - Firewall and IDS/IPS

Kehuan Zhang

IERG4130 2022

Outlines

- The Adversary Model in Network Security
- Defense with Firewall
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Adversary Model in Network Security

Recall the Concept of Adversary Model

- Who is the attacker?
- What are they going after?
- What kind of capabilities do they have?
- What are the attacking surfaces
- And any other assumptions in considering the attack and defenses

Who Will Become the Attacker in Network Security?

- Cyber Criminals (Black-Hat Hackers)
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Activists
  - Website defacement
  - Denial of service attacks
  - Theft and distribution of data that results in negative publicity or compromise of their targets
- State-Sponsored Organizations
  - Focus on strategic targets, like infrastructure, national defense ...
  - Priority is given to be stealthy and long-term threat
  - Also known as **Advanced Persistent Threats (APTs)**
- Others
  - E.g., hobby or curious hackers

What Do They Want to Get?

- A lot, including: Money, terrorism, unsatisfactory, etc.
- But all are supposed to break the **CIA**
- Confidentiality
  - E.g., Secret information
    - ★ Like Patent, bisuness plan, customer's private information
    - ★ Or Data, model, etc.
- Integrity
  - E.g., Private Keys for digital signatures
- Availability
  - E.g, Availability of certain online services (e.g., DDoS)

Attacking Surfaces

- Network Itself
  - Bandwidth, Network Equipment (e.g., Routers, Switch, Access Points), etc.
  - Include from both inside and outside of a given network
- Critical Network Services (both software and hardware)
  - E-Mail Server, Web Server, Database Server, etc.
  - DNS Server, DHCP Server, etc.
  - Firewall and IDS can also be the target
- Hosts connected to the network
  - May contain valuable information and data

Defense with Firewall

Concept of Firewall

- Firewall is trying to hardening the surface against attacks
- Why do we need firewall?
  - Internet connectivity is necessary for most organizations
  - Internet connection is two-way
    - ★ You can access the outside world
    - ★ But outside world can also access your resources
  - Firewall is a to establish a perimeter and provide a choke point between internal and external network
- Design Goals
  - All traffic, inblude both incoming and outgoing traffics, should pass the firewall
  - Only authorized traffic (defined by the security policies) is allow to flow
  - Firewall itself should be secure enough and immune to penetration

Limitations of Firewall

- Firewall can be bypassed in some cases (the firewall-bypass attack)
- Does not protect against internal threats
  - Either insiders, or using compromised hosts as stepping-stones
- Cannot protect against the transfer of virus-infected programs
  - The cost of detecting infected programs is too high
- Increasing popularity of "firewall-friendly" protocols
  - e.g. http traffic is almost impossible to be banned, meanwhile perform deep-packet-inspection (DPI) is very expensive

Firewall Types

- Packet Filtering Firewall –> Working at Network Layer
- Stateful Packet Inspection Firewall –> Working at Transport Layer
- Application-Level Proxy/Gateway –> Working at Application Layer
- Circuit-Level Proxy/Gateway –> Working at Transport Layer

Packet Filtering Firewall

- Search in a list of rules to decide whether to forwards or discards the packet
  - Inspect every packet
  - And every packet is processed independently (**do not keep state info**)
  - And in both directions
- Rules normally are based on layer-3 and -4 information from IP packets
  - 5-tuple: (srcIP, destIP, srcPort, destPort, protocol)
  - May also use (TOS, Inf), i.e., Type of Service, Interface
- Two type of default strategy (similar to white- and black-list)
  - Discard a packet unless it is allowed to pass explicitly by a rule
  - Forward a packet unless it is prohibited explicitly by a rule

Example of Packet Filtering Policy

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Comments on Packet Filtering Firewall

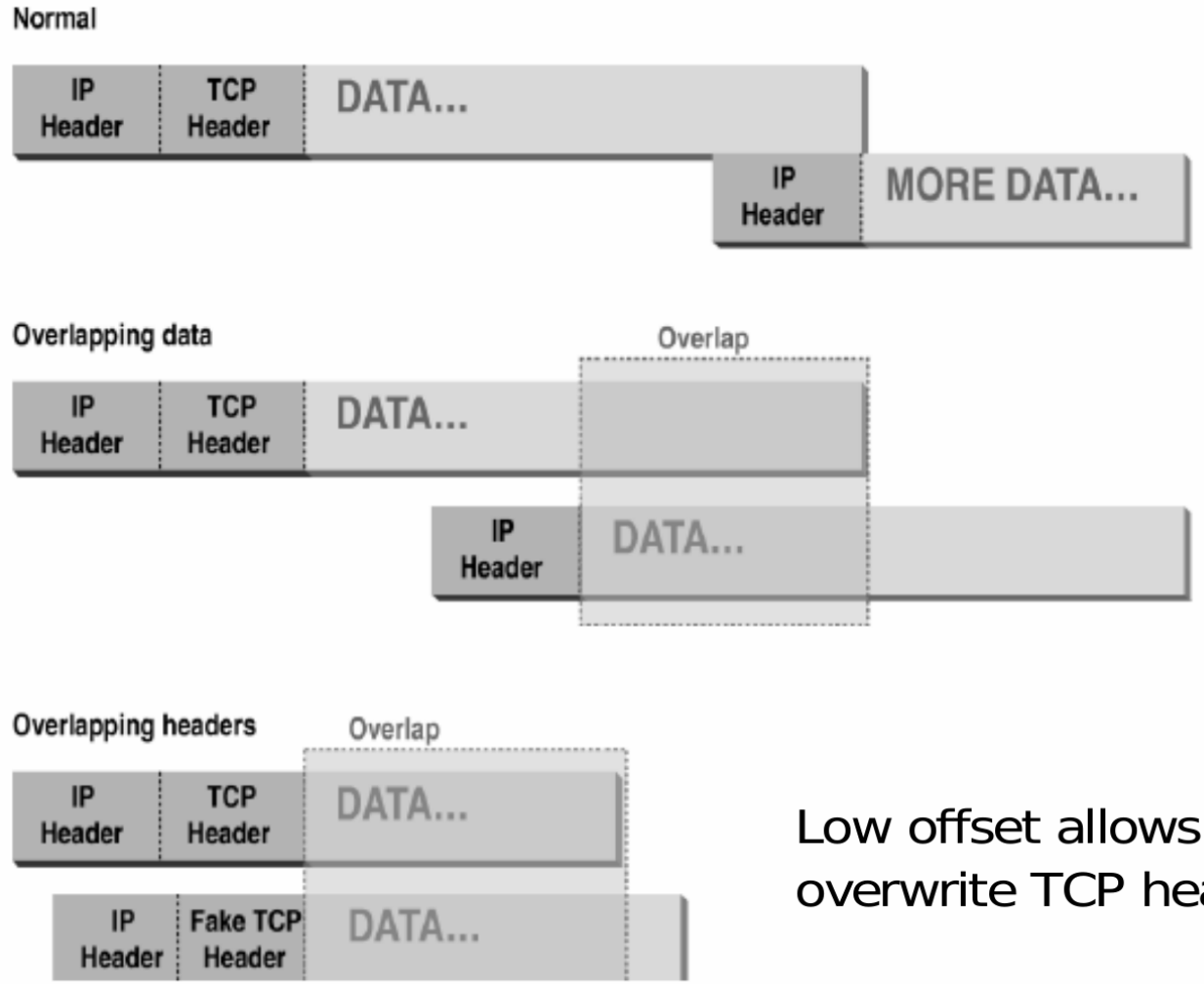
- Advantages
  - Simple, transparent, and very fast
- Disadvantages
  - Difficult to set up rules correctly
    - ★ Conflicts, rule-overriding, etc.
  - Relatively easy to be attacked and bypassed
    - ★ IP address spoofing attack
    - ★ Packet Fragmentation Attack
  - Limitation on openning high-end port numbers
    - ★ Typically, incoming traffic with destPorts > 1023 is permitted to allow returning TCP traffic for the clients behind the firewall
    - ★ In order to support some dynamic protocols, like Netmeeting, Real-audio etc, are in use, entire ranges of ports must be allowed for the protocol to work.

Packet Fragmentation Attack - 1

- How IP Fragmentation works

Packet Fragmentation Attack - 2

- Normal and Abnormal IP Fragmentation



Low offset allows second packet to overwrite TCP header at receiving host

Packet Fragmentation Attack - 3

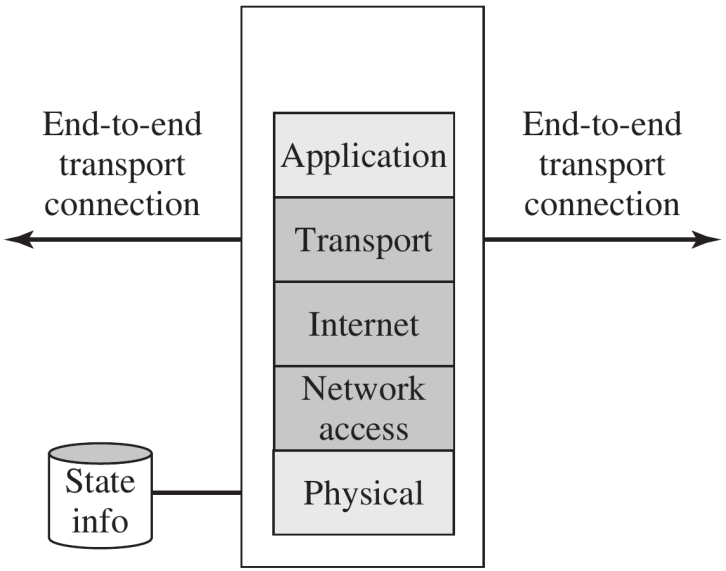
- Assume: TCP port 23 is blocked but SMTP port 25 is allowed
- Steps to launch fragmentation attack

1. The first packet
   - Fragmentation Offset = 0.
   - DF bit = 0 : "May Fragment"
   - MF bit = 1 : "More Fragments"
   - destPort = 25, so firewall allows it to pass-through
2. Second packet
   - Fragmentation Offset = 1: second packet overwrites all but first 8 bits of the first packet
   - DF bit = 0 : "May Fragment"
   - MF bit = 0 : No More Fragment $\rightarrow$ "Last Fragment"
   - destPort = 23. Normally be blocked, but sneaks by!

- What happens
  - The "TCP header" in the 2nd packet is ignored since it's a fragment
  - At destination, packet reassembled and eventually received at port 23

Stateful Packet Inspection Firewall

- Packet decision made in the context of a TCP connection
  - Context based on State Table - used to validate any inbound traffic.
  - If packet is a new connection, check against security policy
  - If packet is part of an existing connection, match it up in the state table & update table

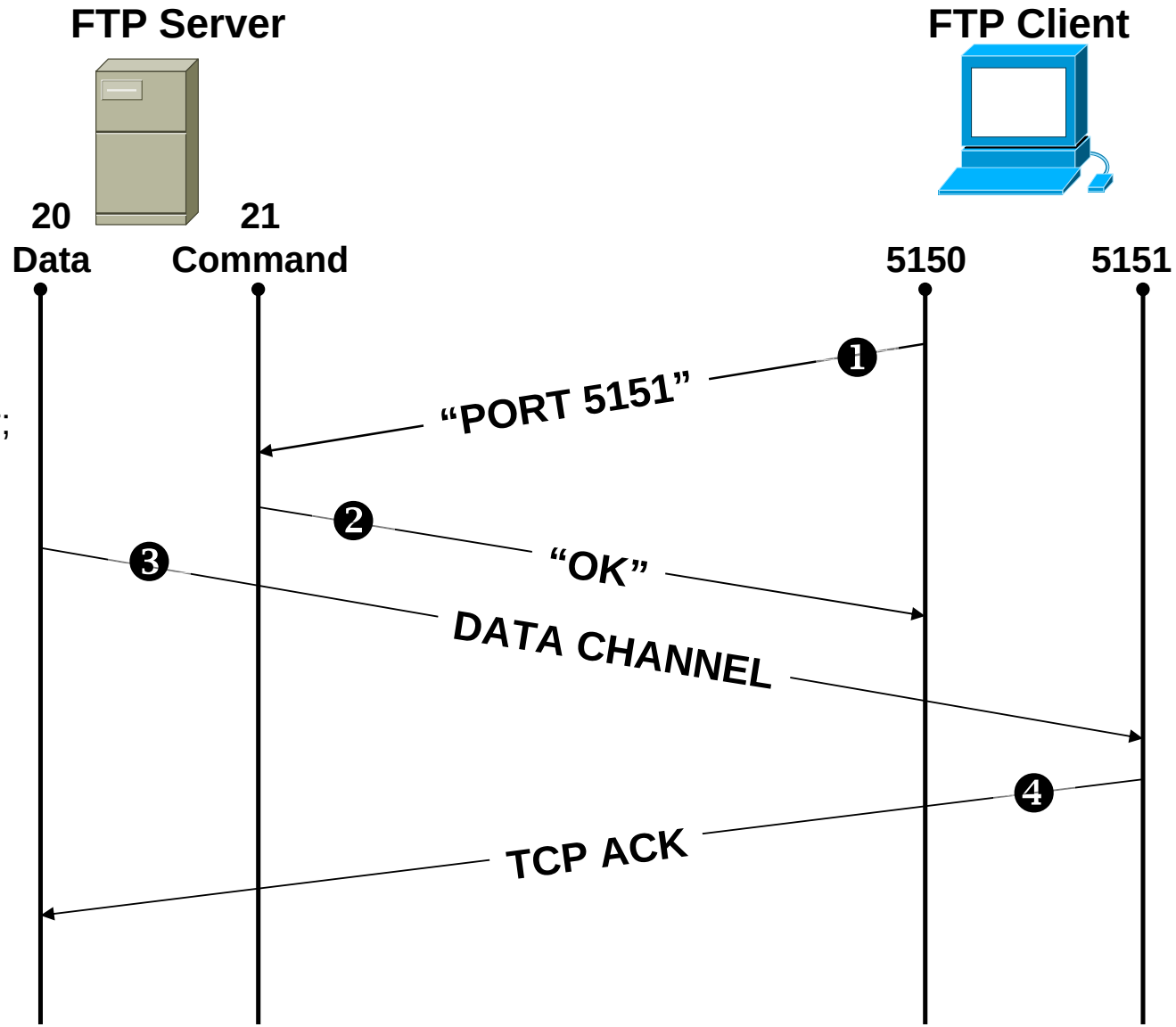


Stateful Packet Inspection Firewall (Cont.)

- Mainly to handle Inbound connections above port 1023
- Solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding high- numbered client port
- Some commercial stateful firewalls do keep even more sophisticated state-info tracking
  - E.g., track the port number negotiations for applications like video streaming or FTP, in order to open and close necessary ports dynamically

An Example of Dynamic Ports for FTP Protocol

- FTP will use separate channels for commands and data

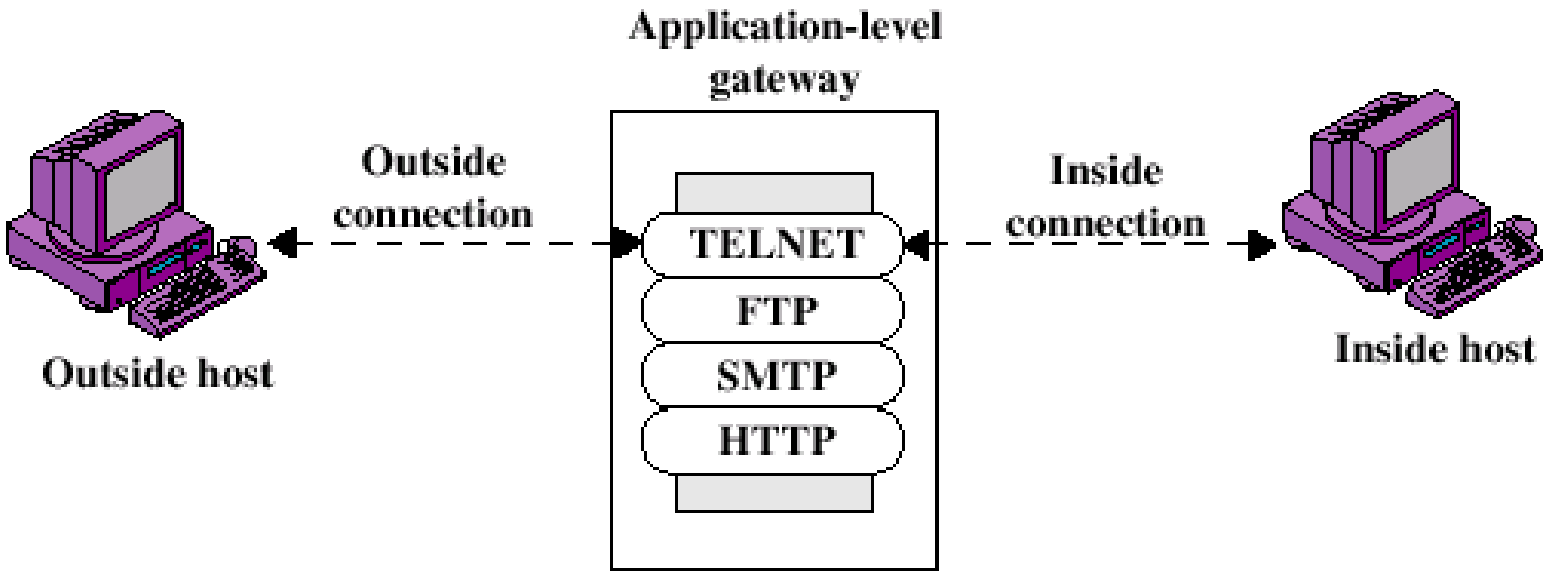


Characteristics of Stateful Packet Inspection Firewall

- More secure because the firewall tracks client ports individually rather than opening all high -numbered ports for external access.
- Adds Layer 4 or Higher awareness to the standard packet filter architecture.
- Useful or applicable only within TCP/IP network infrastructures
- Superset of packet filter firewall functionality
- The more state-info is tracked, the bigger the challenge for support high speed communications link

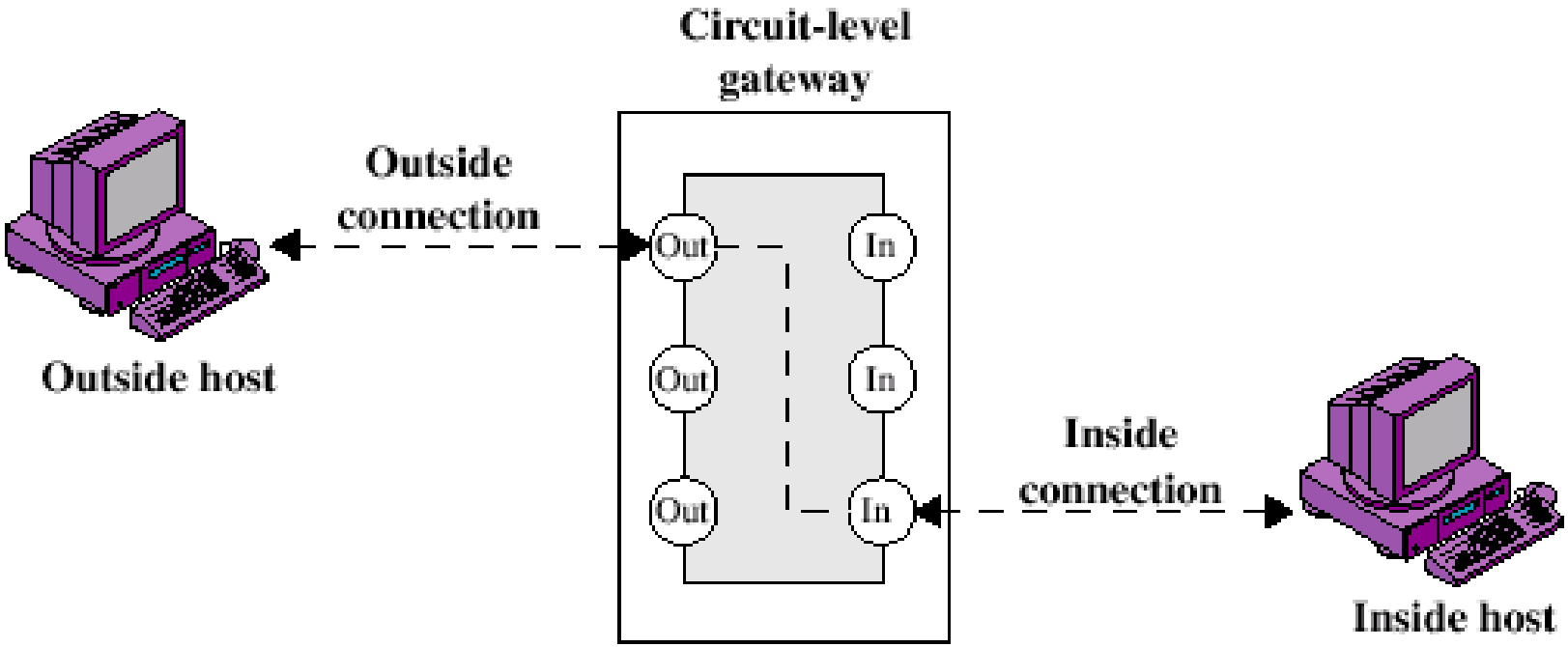
Application-Level Proxy/Gateway

- Acts as a relay of application level traffic (also called *gateway*)
- An example: user contacts gateway for TELNET to remote host, user is authenticated, then gateway contacts remote host and relays info between two end points
- It can examine the packets to ensure the security of the application
  - Full packet awareness, very easy to log since entire packet was seen
- Disadvantage: additional processing overhead for each connection - slow



Circuit-Level Proxy/Gateway

- Relay at Transport layer (and forbid direct end-to-end TCP connection)
  - Sets up two TCP connections, one between itself and inside TCP user, and the other one between itself and an outside TCP user
  - Relays TCP layer payloads from one connection to the other
- Security policy will determine what connections was allowed
- Used where internal users are trusted for all outbound services

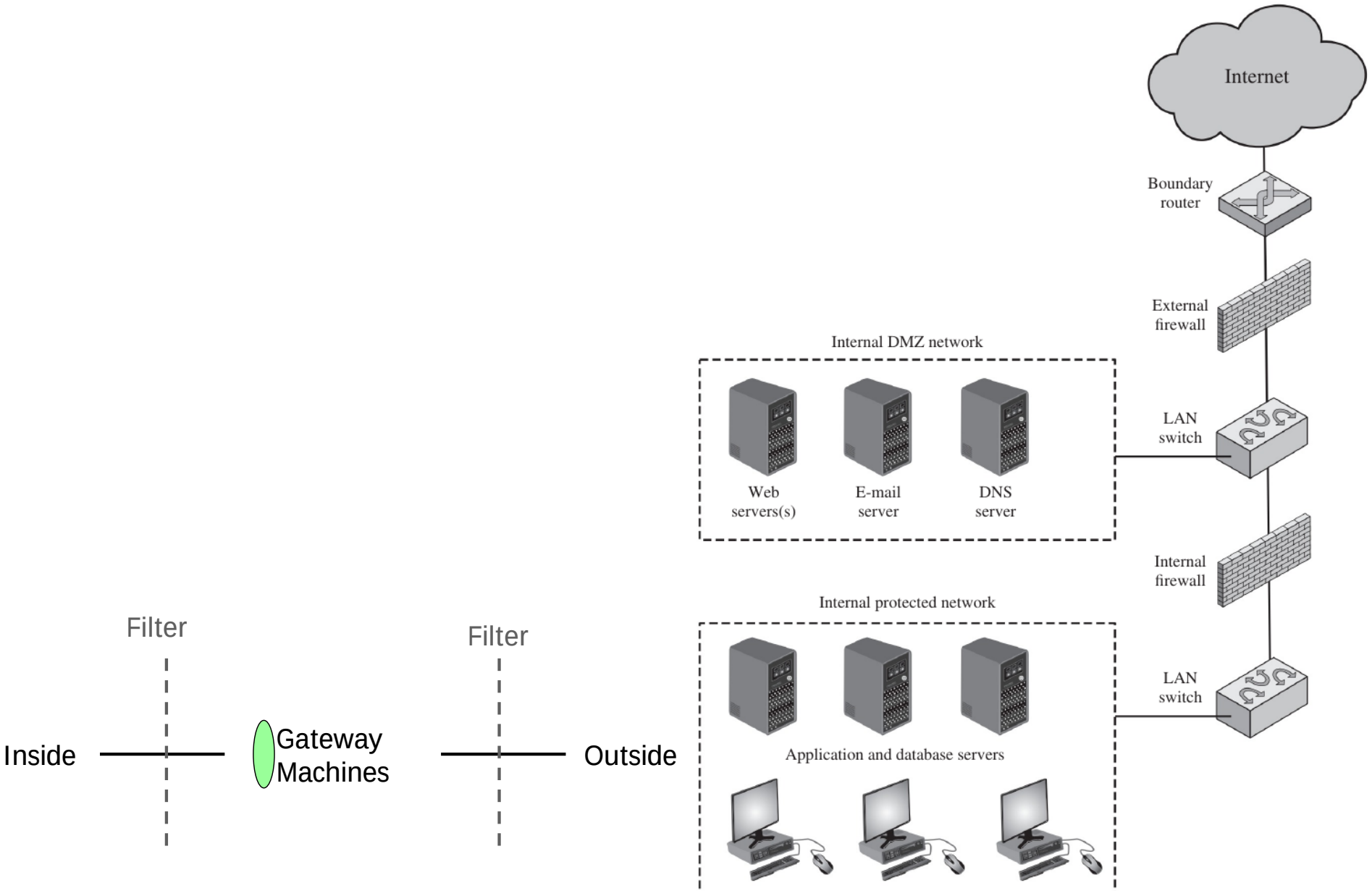


Circuit-Level Proxy/Gateway (Cont.)

- Protect against fragmentation problem
- Support more services than Application-level Gateway
- But has less control over data
- Hard to handle dynamic protocols like FTP
- Clients must be aware they are using a circuit-level proxy
  - Some implementations require a special client, e.g. requires SOCKS-ified client
- SOCKS package V5 – RFC 1928
  - Uses port 1080

Firewall Placement and Configuration

- Concept of **DMZ** and the principle of **Defense-in-Depth**



Guidelines for De-Militarized Zone

- Keep It Simple (KISS) principle
  - The more simple the firewall solution, the more secure and more manageable
- Use Devices as They Were Intended to Be Used
  - Don't make switches into firewalls
- Apply the principle of "Defense-in-Depth"
  - Defense at multipel layers: e.g., double firewalls, IDS
- Pay Attention to Internal Threats
  - "crown jewels" go behind internal firewall
  - Remember: "all rules are meant to be broken"

Other Types of Firewalls

- Host Based Firewalls
  - Comes with some operating systems (LINUX, WIN/XP)
  - For example:
    - ★ Microsoft's Defender on Windows
    - ★ Uncomplicated Firewall (UFW) on Linux (demo of UFW rule/log)
- Personal Firewalls Appliances
  - Personal firewall appliances are designed to protect small networks such as networks that might be found in home offices
  - Provide: print server, shared broadband use, firewall, DHCP server and NAT
- Avoids Crunchy Cookie Syndrome
  - Hard and crunchy on the outside, soft and chewy on the inside

Intrusion Detection Systems (IDS)
and
Intrusion Prevention System (IPS)

How to Detect Network Attacks?

- First we need to understand typical flows of network attacks
  - Collection Information
    - ★ E.g., port scanning, OS fingerprinting (to find vulnerable service or OS)
  - Initial Access
    - ★ May leave traces in log files (e.g., login activities in /var/log/auth.log)
  - Privilege Escalation (exploiting vulnerabilities)
    - ★ May trigger alarms in log files (like wrong password or abnormal crashes)
  - System Exploit (and Further Information Collection)
    - ★ Leverage system and/or application vulnerabilities
  - Maintaining Access
    - ★ Setup a backdoor
  - Covering Attacking Traces (to stay stealthy)
    - ★ Wipe various log data/entries
- What kind of features (or traces) are available?
  - Network traffics with specific patterns
  - Warnings, sensitive operations in log files
  - Changing of patterns in CPU usage, disk access, system call usage, etc.

Concept of IDS

- IDS is a monitor system (mostly passive by only observing network traffics) for system and network behaviours and raise warnings/alarms in case of possible intrusions were detected
- Types of IDS
  - Host-based IDS (HIDS)
    - ★ Typically a piece of software running on a monitored host to find hints of network intrusions
  - Network-based IDS (NIDS)
    - ★ A system that monitors (by sniffing at) the network traffic to find hints of network attacks
  - Distributed or Hybrid IDS
    - ★ Comprehensive analysis on information from both network-based IDS systems and a set of distributed host-based IDSes
- Difference between IDS and Firewall?
- Difference between Host-based IDS and anti-virus software?

Analysis Approaches in IDS: Anomaly vs. Signature

- Anomaly Detection
  - Anomaly-based IDSs compare the current "behavior" with a nominal profile of system/network
  - Can detect never-seen-before (zero-day threat) of intrusions
  - The challenge is to decide what is "normal" – need to balance between false positive and false negative rate
    - ★ False positive: an alarm is generated even when there is no intrusion
    - ★ False negative: fails to generate an alarm when there is an intrusion
- Signature Detection
  - Signature-based IDSs compare the observed packets/system calls/commands with a database of known attack packet/system call signatures
  - Less prone to false positive but require update of signature database all the time and not effective to new attacks before new signatures are installed

Possible Limitations of IDS

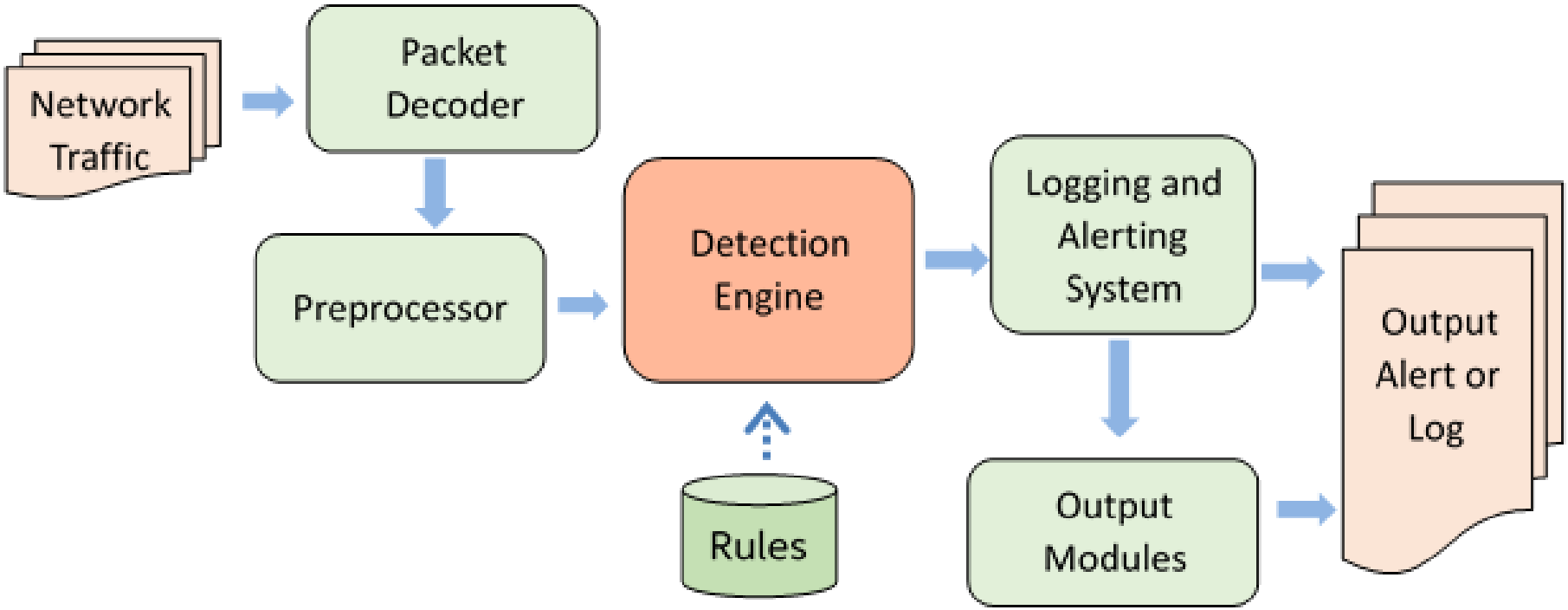
- For an IDS to be useful, the false positive rate and false negative rates must be kept to an acceptable limit
- IDS evasive techniques include:
  - Flooding (a kind of DoS attack to IDS)
  - Fragmentation (e.g. break an TCP segment into multiple IP fragments)
  - Encryption
  - Obfuscation (disguise, use unicode or hex to encode special keywords)
- The industry trend is for IDSs to evolving towards the so-called Intrusion Protection System (IPS)

Concept of IPS

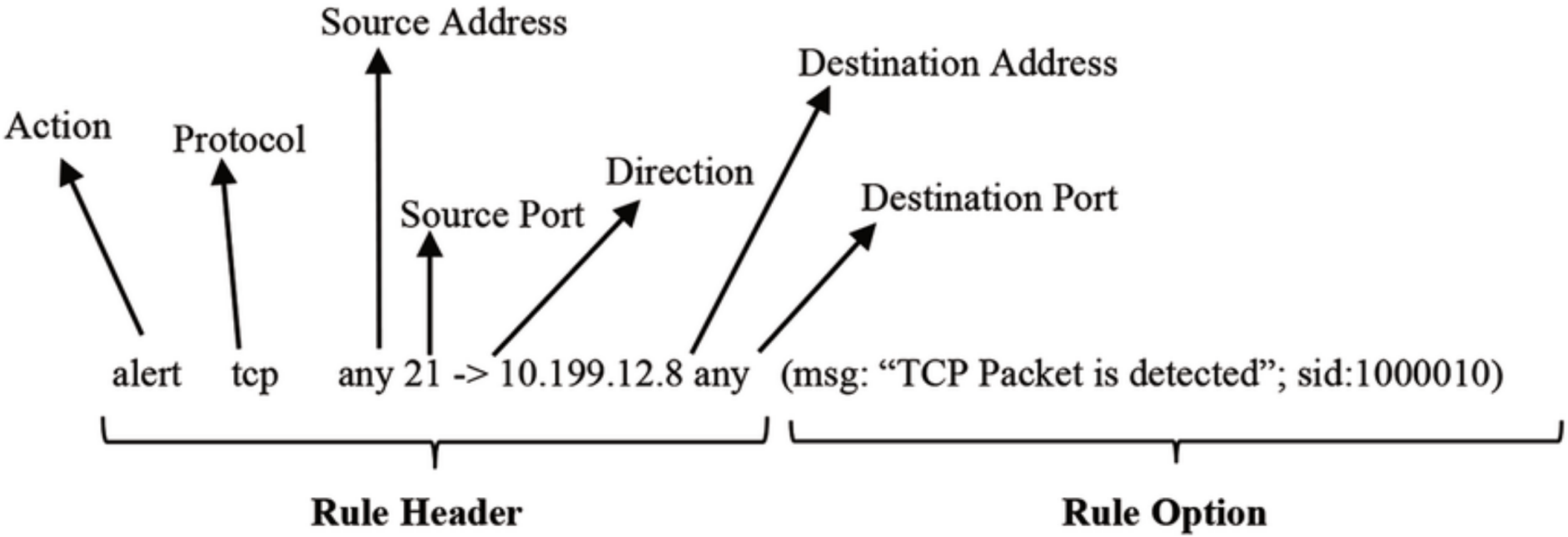
- A system that will act as a chokepoint of network traffic or intercept system-calls within a host/OS, and take active actions, e.g. discard attacking packets, when an intrusion is identified
  - IPS itself contains functionalities of IDS
  - But can take prevention measures ACTIVELY when it detected something bad was happening
    - ★ E.g., change firewall configurations to block certain incoming packets
  - Further blurring the lines between Firewalls and IDSs
- Types:
  - Host-based IPS (HIPS)
  - Network-based IPS (NIPS)

Snort: An Example of NIDS

- What is Snort?
  - Snort is a multi-mode packet analysis tool Sniffer
  - Packet Logger
  - Forensic Data Analysis tool
  - Network Intrusion Detection System



Snort Rules



- Action Field: alert, log, pass, activate, dynamic
- Protocol Field: tcp, udp, icmp, ip
- srcIP srcPort <directionIndicator> destIP destPort
- Rule Options: msg, logto, id, dsize, seq, ack, flags, content, session

Honeypots - A Special Case of IDS

- Honeypot is a decoy system designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
  - Therefore incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised
- Classified as being either low or high interaction
  - Low interaction honeypot consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but won't execute a full version of those services or systems
  - High interaction honeypot is a real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers