Intrusion Detection

Class of Intruders

Classes of intruders: criminals

- Individuals or members of an organized crime group with a goal of financial reward
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Typically young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- Meet in underground forums to trade tips and data and coordinate attacks

Classes of intruders: activitists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
    - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
    - Website defacement
    - Denial of service attacks
    - Theft and distribution of data that results in negative publicity or compromise of their targets

Intruders: state-sponsored

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

Intruders: others

- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Skill Levels

Skill level: Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits

- They likely comprise the largest number of attackers, including many criminal and activist attackers

- Given their use of existing known tools, these attackers are the easiest to defend against

- Also known as “script-kiddies” due to their use of existing scripts (tools)

Skill level: Journeyman

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

Skill level: Mast

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty

Intruders: Another classification

- Masquerader: unauthorized individuals who penetrates a system

- Misfeasor: legit user who accesses unauthorized data

- Clandestine: seizes supervisory control

User and software trespass

- User trespass: unauthorized logon, privilege abuse
- Software trespass: virus, worm, or Trojan horse

Example of intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intruder behavior

- Target acquisition and information gathering
- Initial access
- Privilege escalation
- Information gathering or system exploit
- Maintaining access
- Covering tracks

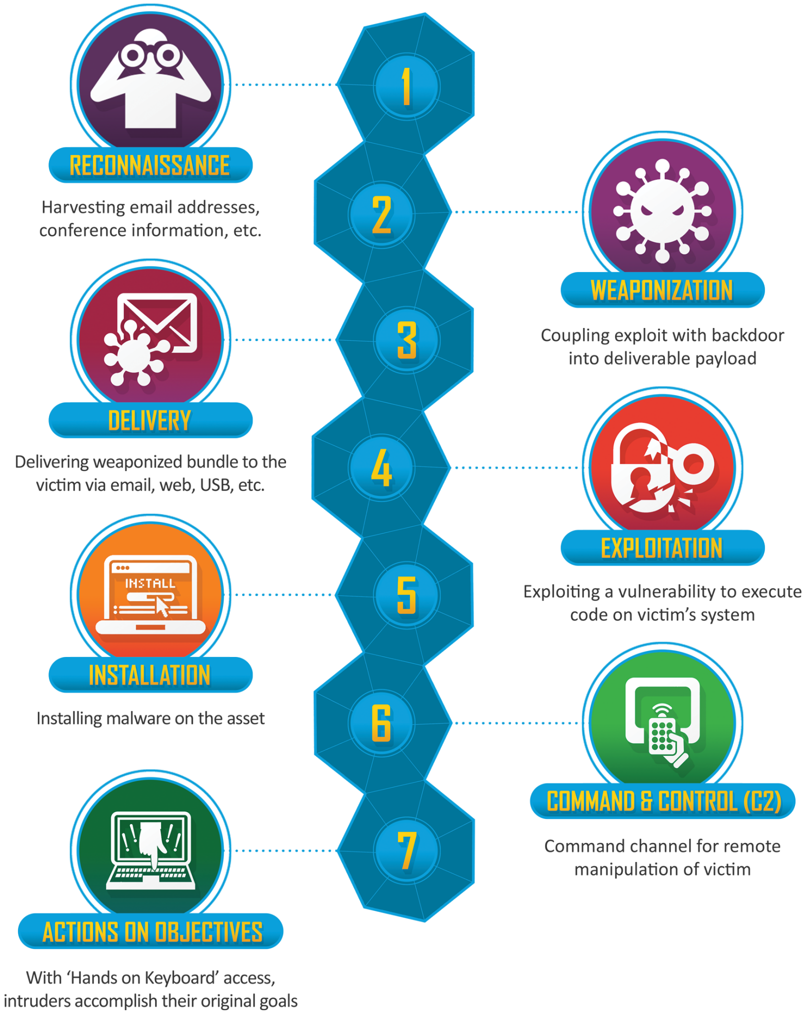
Cyber Kill Chain®

- Developed by Lockheed Martin

- Describes the identification and prevention of cyber intrusions activity

- The cyber kill chain identifies what adversaries must complete in order to achieve their objective.

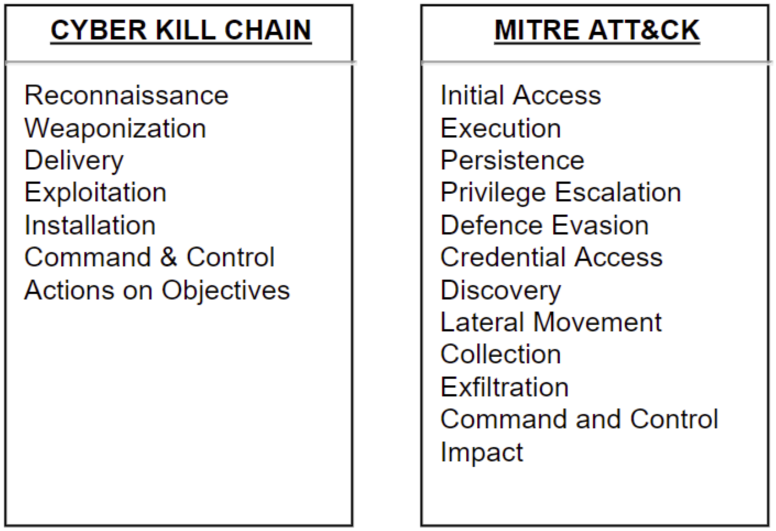
-



1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
INSTALL
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

MITRE ATT&CK

- Developed by MITRE in 2013
- The framework consists of 14 tactics categories
- Very large database of attack vectors



CYBER KILL CHAIN	MITRE ATT&CK
Reconnaissance	Initial Access
Weaponization	Execution
Delivery	Persistence
Exploitation	Privilege Escalation
Installation	Defence Evasion
Command & Control	Credential Access
Actions on Objectives	Discovery
	Lateral Movement
	Collection
	Exfiltration
	Command and Control
	Impact

Hacker behavior example

1. Select target using IP lookup tools

2. Map network for accessible services
   - study physical connectivity (via NMAP)

3. Identify potentially vulnerable services

4. Brute force (guess) passwords

5. Install remote administration tool

6. Wait for admin to log on and capture password

7. Use password to access remainder of network

Criminal intruder behavior

1. Act quickly and precisely to make their activities harder to detect
2. Exploit perimeter via vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors for re-entry
4. Use sniffers to capture passwords
5. Do not stick around until noticed
6. Make few or no mistakes

Insider intruder behavior

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn't normally use for their daily jobs
3. E-mail former and prospective employers
4. Conduct furtive (covert) instant-messaging chats
5. Visit web sites that cater to disgruntled employees, such as f*dcompany.com
6. Perform large downloads and file copying
7. Access the network during off hours

Insider attacks

- Among most difficult to detect and prevent
- Employees have access & systems knowledge
- May be motivated by revenge/entitlement
  - When employment terminated
  - Taking customer data when move to competitor
- IDS/IPS may help but also need
  - Least privilege, monitor logs, strong authentication, termination process to block access & take mirror image of employee's HD (for future purposes)

Security Intrusion & Detection (RFC 2828)

- Security intrusion: a security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.
- Intrusion detection: a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Intrusion techniques

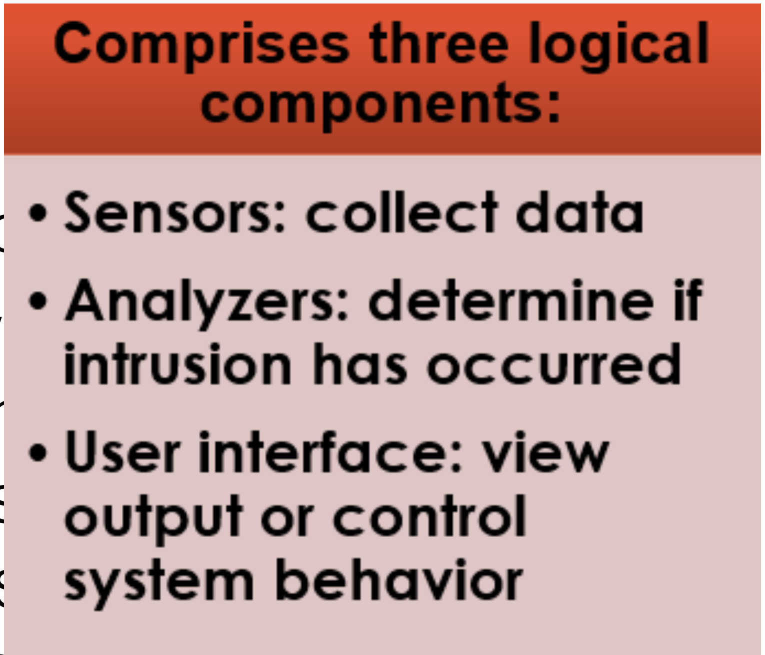
- Objective to gain access or increase privileges

- Initial attacks often exploit system or software vulnerabilities to execute code to get backdoor
    - e.g. buffer overflow

- Or to gain protected information
    - Password guessing or acquisition (or via social engineering)

Intrusion Detection Systems

- Host-based IDS: monitor single ho
- Network-based IDS: monitor netw
- Distributed or hybrid: Combines ir number of sensors, often both hos based, in a central analyzer that is identify and respond to intrusion activity



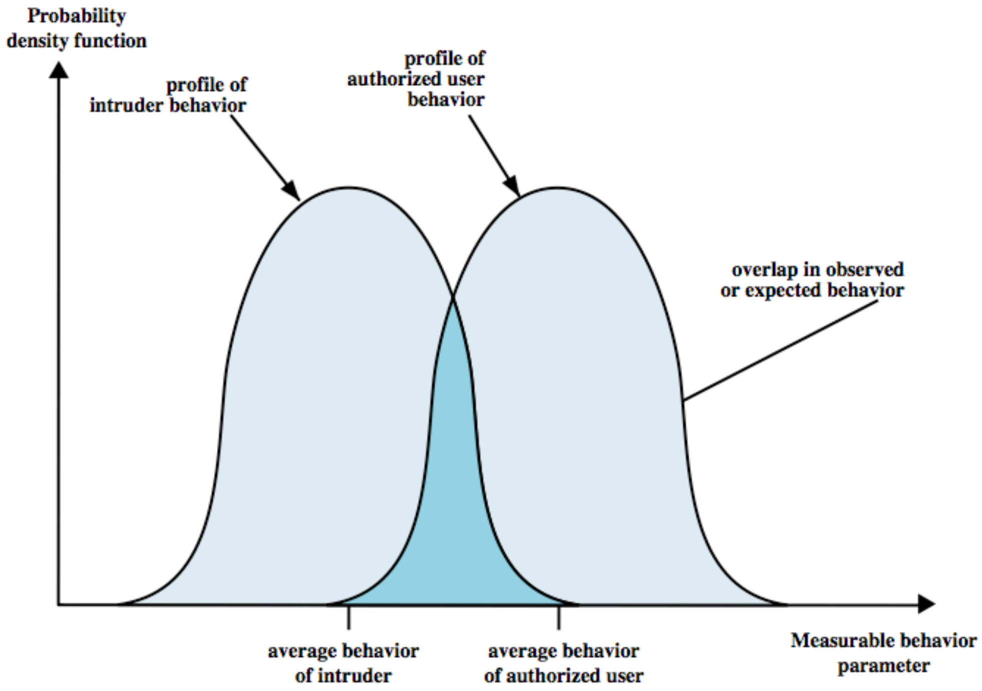
Comprises three logical components:

- **Sensors: collect data**
- **Analyzers: determine if intrusion has occurred**
- **User interface: view output or control system behavior**

IDS principles

loose vs tight interpretation:
catch more (false +) or catch less (false -)

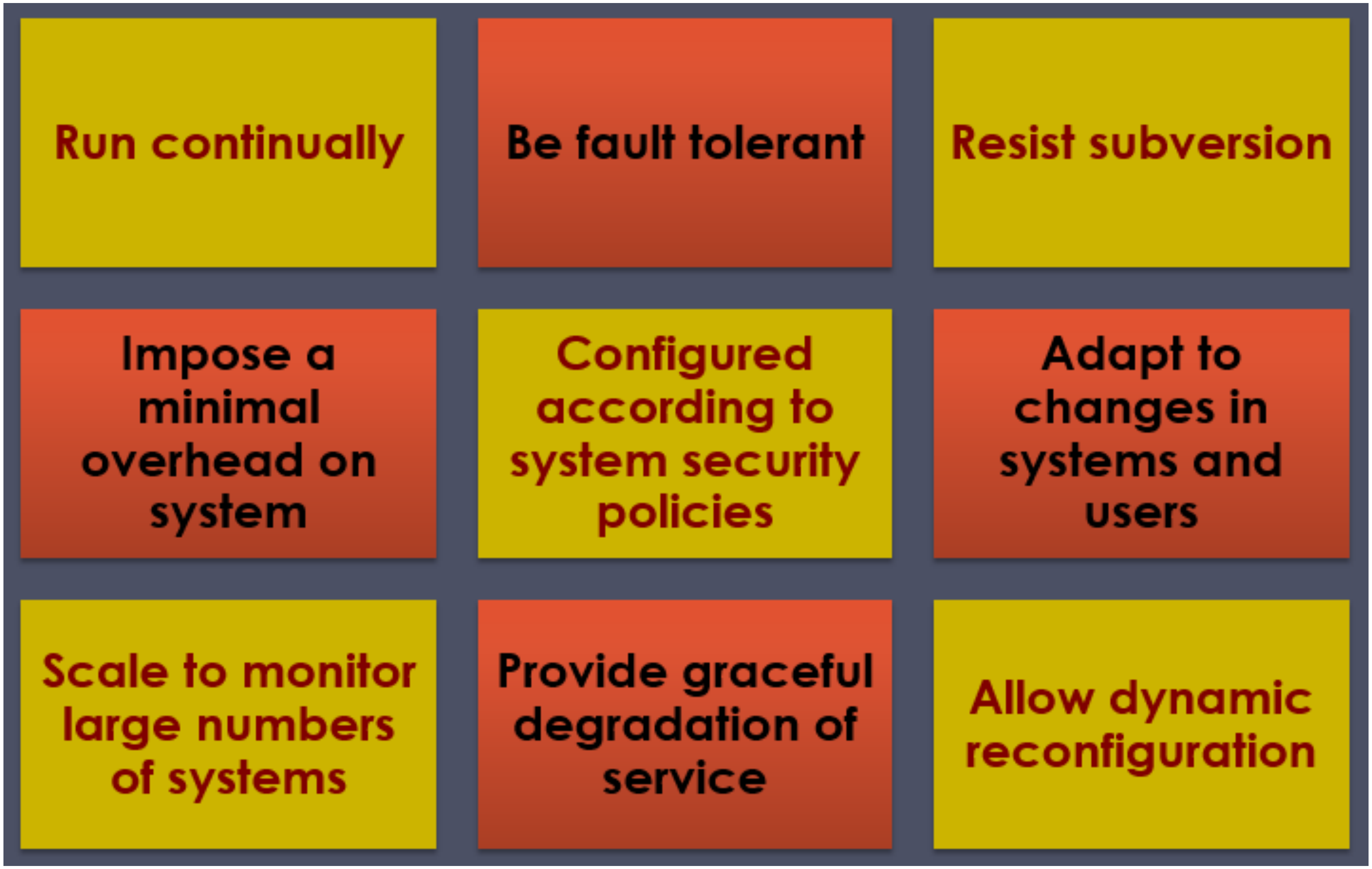
- Assumption: intruder behavior differs from legitimate users
  - Expect overlap as shown
  - for legit users:
    Observe major deviations from past history
  - Problems of:
    - false positives
    - false negatives
    - must compromise


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

valid user identified as intruder

intruder not identified

IDS requirements



- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

IDS requirements

- Run continually with minimal human supervision
- Be fault tolerant: recover from crashes
- Resist subversion: monitor itself from change by intruder
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service: if one component fails, others should continue to work
- Allow dynamic reconfiguration

Detection techniques

- Anomaly (behavior) detection
- Signature/heuristic detection

IDS: Anomaly (Behavior) Detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time

- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Anomaly detection

- Threshold detection
  - checks excessive event occurrences over time
  - alone a crude and ineffective intruder detector
  - must determine both thresholds and time intervals
  - lots of false positive/false negative may be possible
- Profile based
  - characterize past behavior of ***users/groups***
  - then detect significant deviations
  - based on analysis of audit records: ***gather metrics***

Example of metrics

- Counters: e.g., number of logins during an hour, number of times a cmd executed
- Gauge: e.g., the number of outgoing messages [pkts]
- Interval time: the length of time between two events, e.g., two successive logins
- Resource utilization: quantity of resources used (e.g., number of pages printed)
- Mean and standard deviations

Signature/heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior

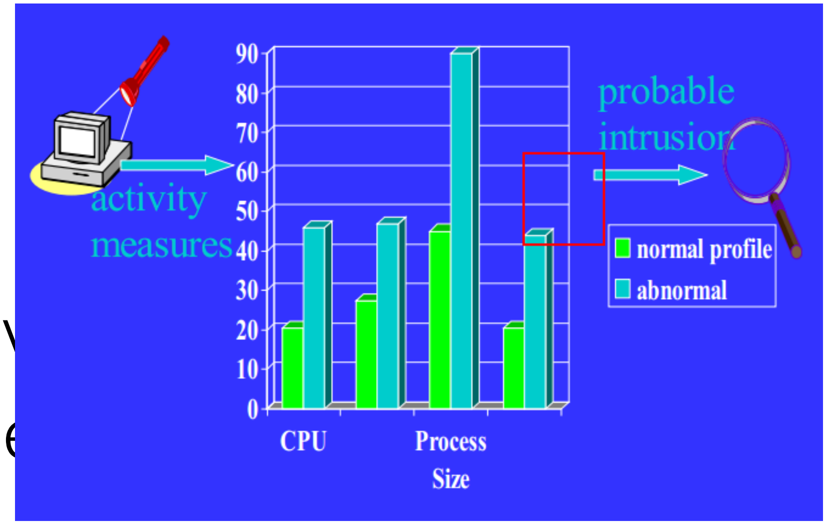
- Also known as misuse detection

- Can only identify known attacks for which it has patterns or rules (signature)
  - Very similar to anti-virus (requires frequent updates)
  - Rule-based penetration identification
    - rules identify ***known*** penetrations/weaknesses
    - often by analyzing attack scripts from Internet (CERTs)

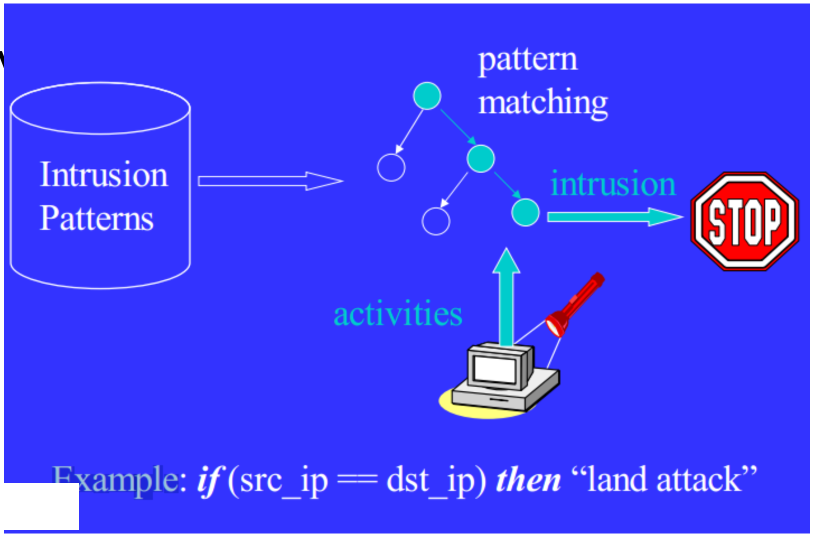
Example of rules in a signature detection IDS

- Users should not be logged in more than one session
- Users do not make copies of system, password files
- Users should not read in other users’ directories
- Users must not write other users’ files
- Users who log after hours often access the same files they used earlier
- Users do not generally open disk devices but rely on high-level OS utils

Host-based IDS: signature vs anomaly detection



- Connection attempt from a reser
- Attempt to copy the password fil
- Email containing a particular virus
- File access attack on an FTP ser directory commands to it without



Example: *if* (src_ip == dst_ip) *then* “land attack”

```
drop tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"Block Baidu Spider
```

Host-based IDS

- Specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- Two approaches, often used in combination:
  - Anomaly detection: consider normal/expected behavior over a period of time; apply statistical tests to detect intruder
    - threshold detection: for various events (#/volume of copying)
    - profile based (time/duration of login)
  - Signature detection: defines proper (or bad) behavior (rules)

Audit records

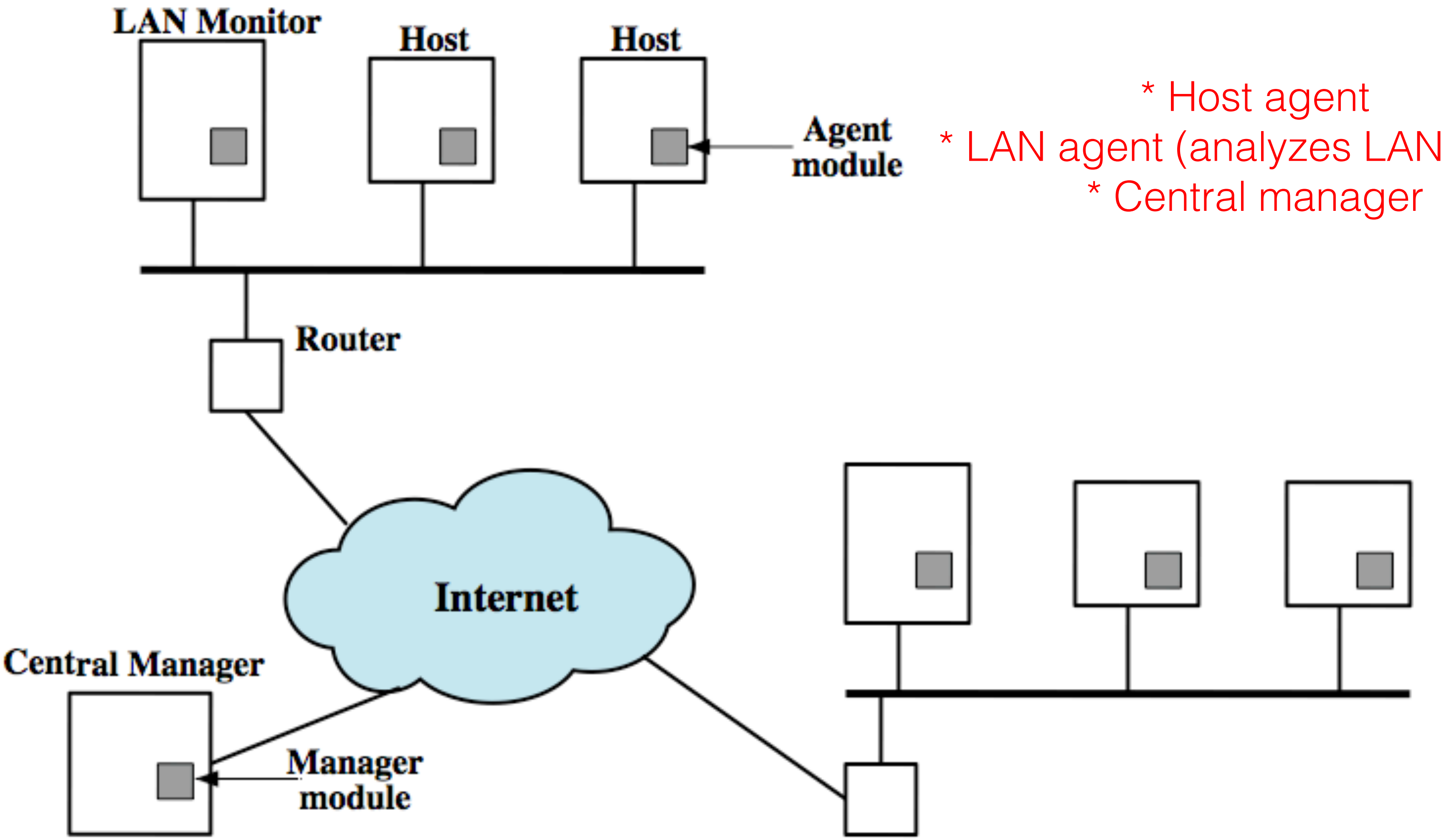
- A fundamental tool for intrusion detection

- Two variants:
  - Native audit records: provided by O/S
    - always available but may not be optimum
  - Detection-specific audit records: IDS specific
    - additional overhead but specific to IDS task
    - often log individual elementary actions
    - e.g. may contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp
    - possible overhead (two such utilities)

Common data sources

- Common data sources include:
  - System call traces
  - Audit (log file) records
  - File integrity checksums
  - Registry access

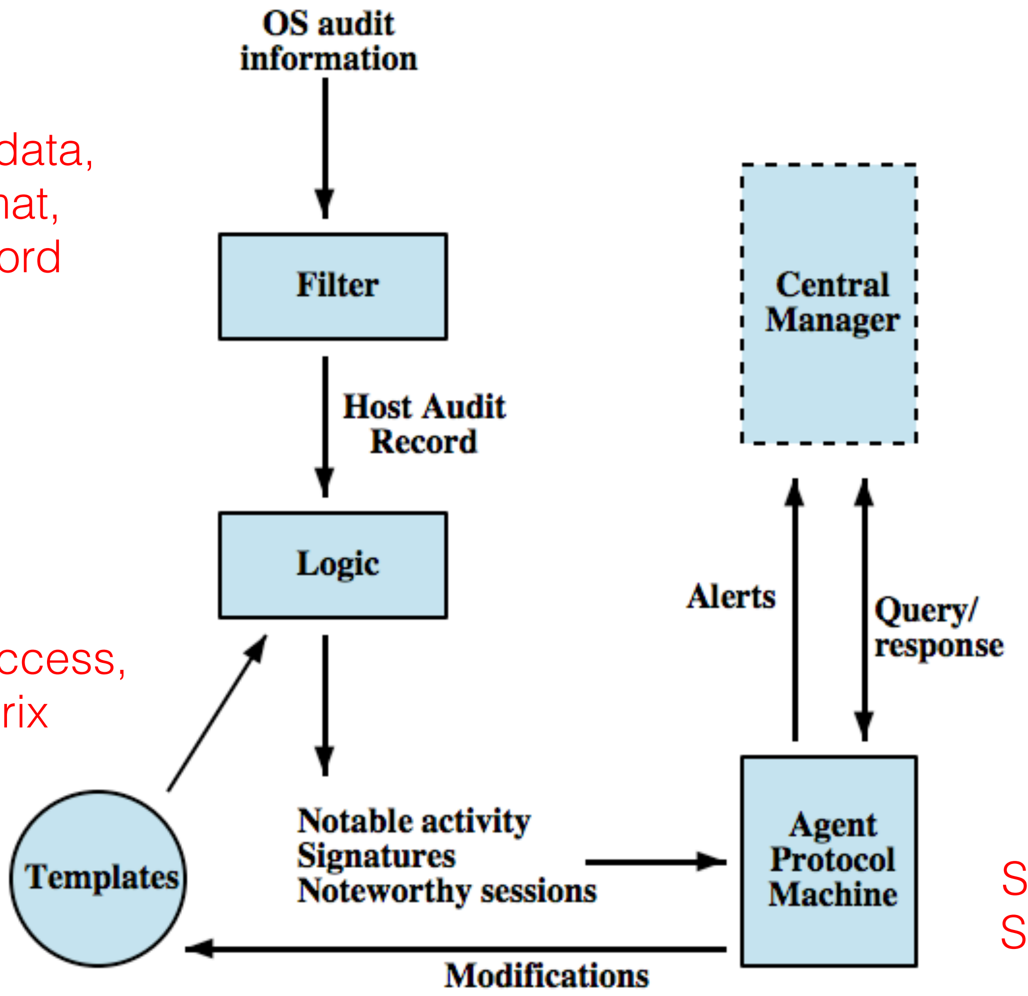
Distributed host-based IDS



* Host agent
* LAN agent (analyzes LAN traffic)
* Central manager

Distributed host-based IDS: agent architecture

retain only sec data,
use a std format,
host audit record



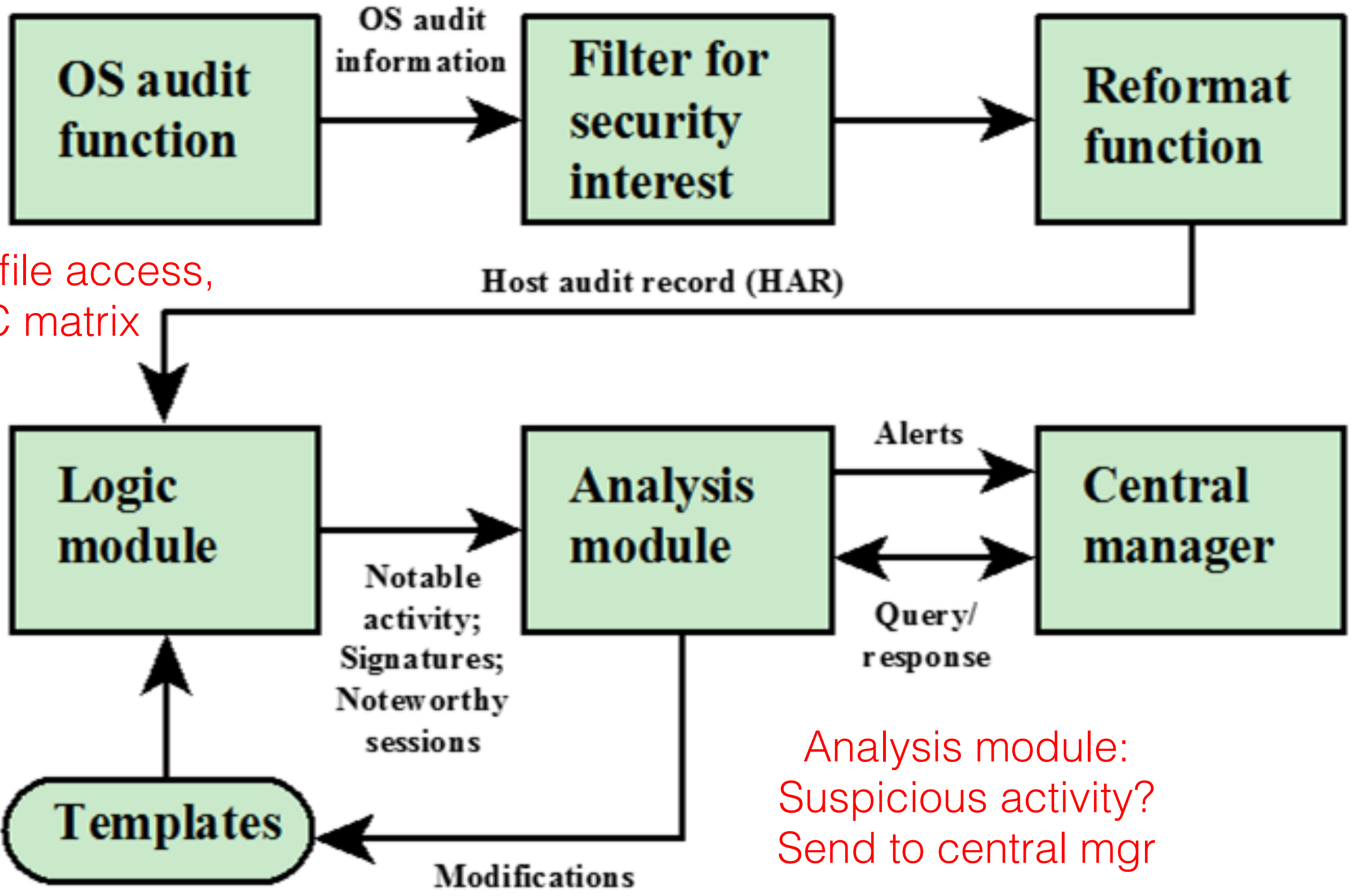
analyze for failed file access,
change to AC matrix

Analysis module:
Suspicious activity?
Send to central mgr

Distributed host-based IDS: agent architecture

retain only sec data,
use a std format,
host audit record

analyze for failed file access,
change to AC matrix



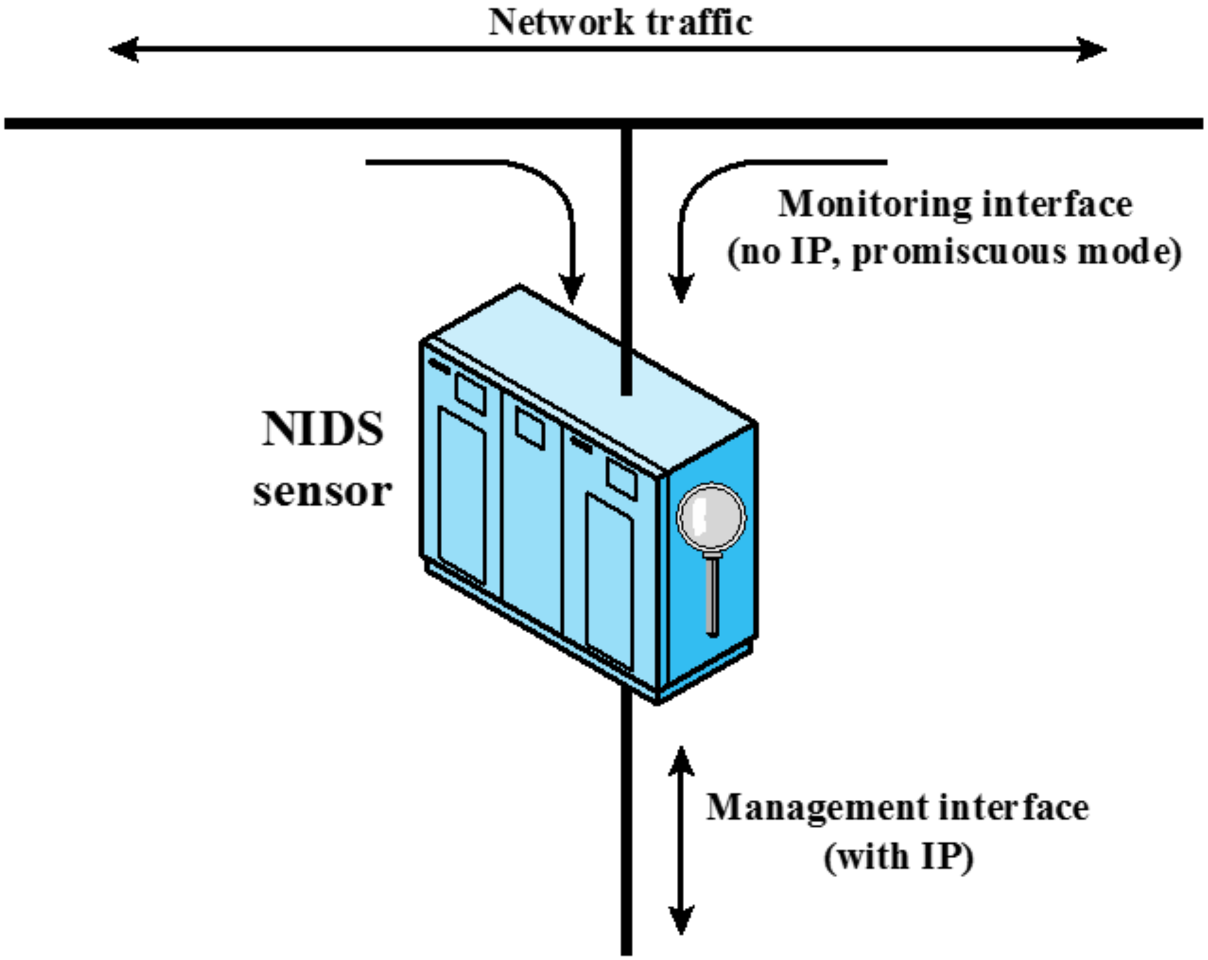
Analysis module:
Suspicious activity?
Send to central mgr

Network-Based IDS

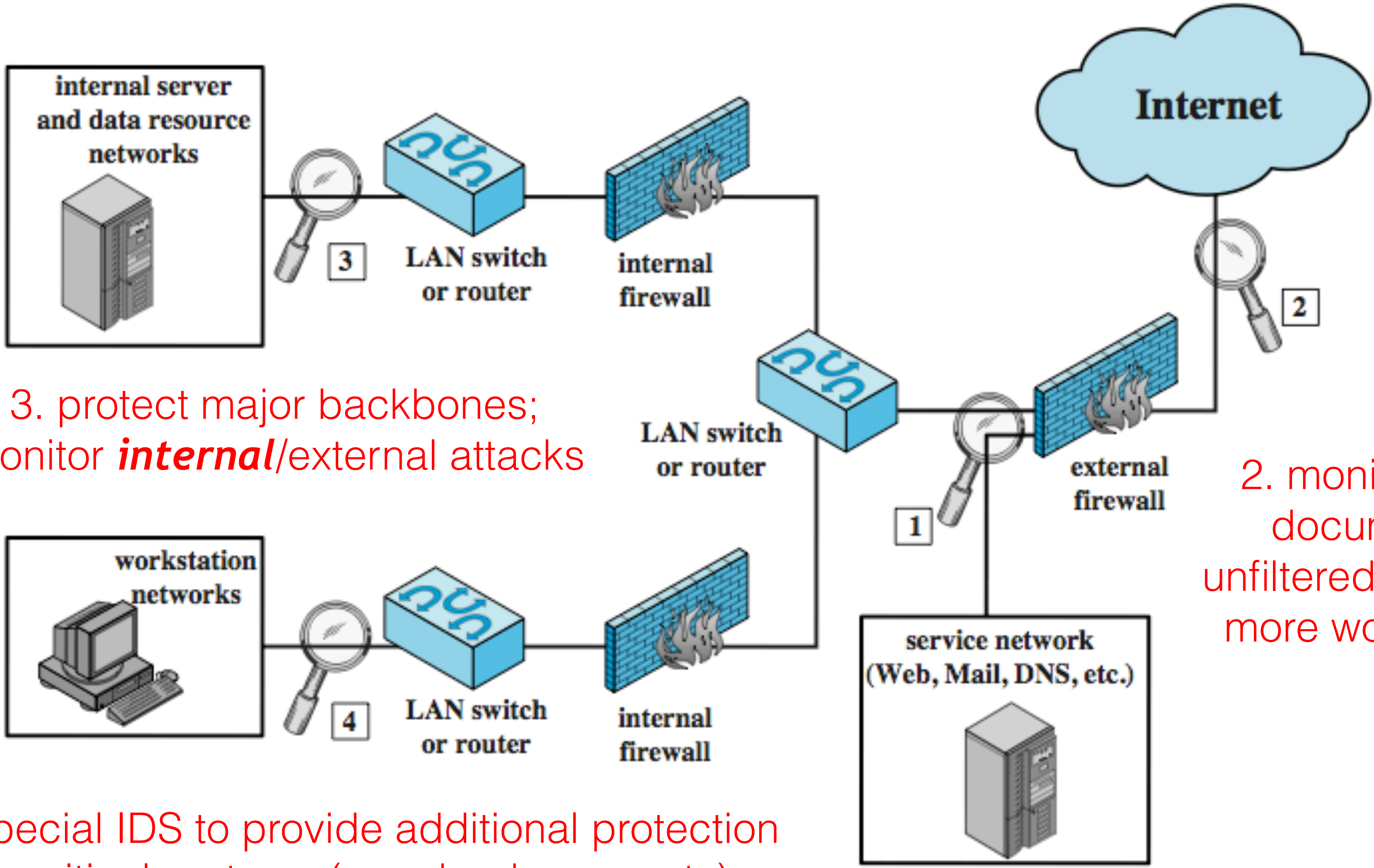
- Network-based IDS (NIDS)
  - ***Monitor traffic at selected points on a network* (e.g., rlogins to disabled accounts)**
  - In (near) real time to detect intrusion patterns
  - May examine network, transport and/or application level ***protocol*** activity directed toward systems

- Comprises a number of sensors
  - Inline (possibly as part of other net device) – traffic passes thru it
  - Passive (monitors copy of traffic)

Passive sensors



NIDS Sensor Deployment



3. protect major backbones; monitor ***internal***/external attacks

2. monitor and documents unfiltered packets; more work to do

4. Special IDS to provide additional protection for critical systems (e.g., bank accounts)

1. monitor attacks from outside (see attacks to servers)

NIDS intrusion detection techniques

- Signature detection
  - at application (*FTP*), transport (*port scans*), network layers (*ICMP*); unexpected application services (*host running unexpected app*), policy violations (*website use*)
- Anomaly detection
  - of denial of service attacks, scanning, worms (*significant traffic increase*)
- When potential violation detected, sensor sends an alert and logs information
  - Used by analysis module to refine intrusion detection parameters and algorithms
  - by security admin to improve protection

Distributed hybrid intrusion detection (host-based, NIDS, distributed host-based)

Issues:

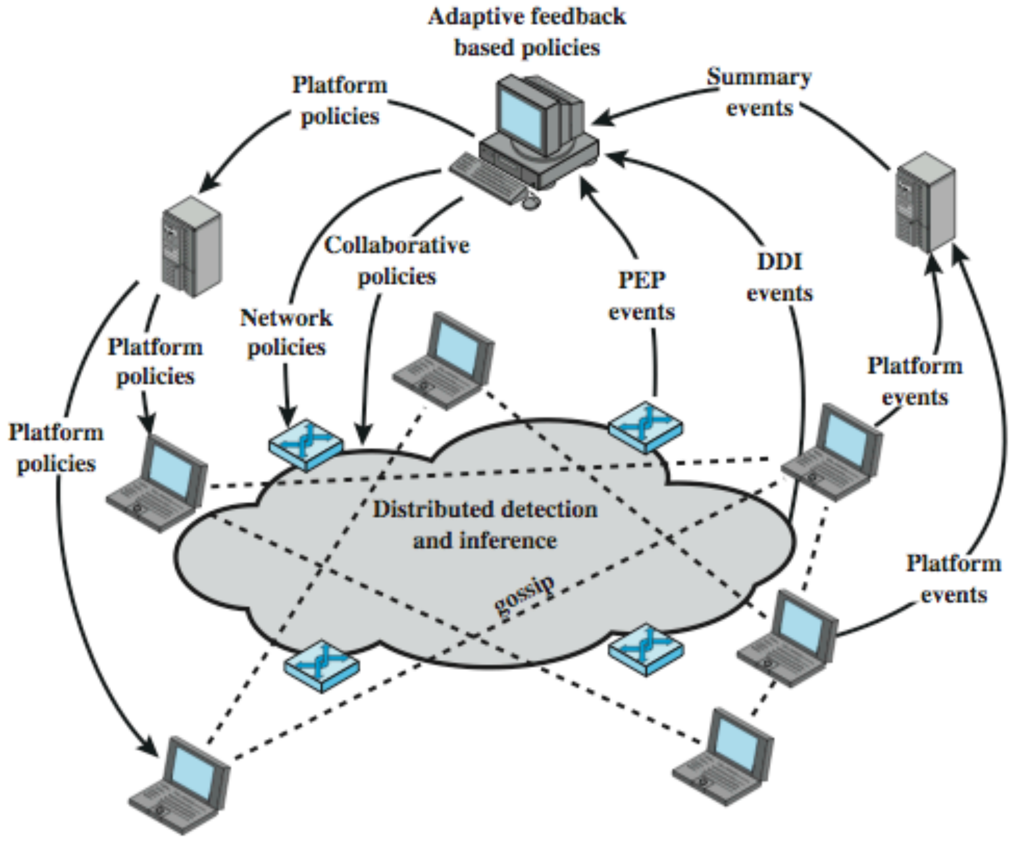
1. Tools may not recognize new threats

2. Difficult to deal with rapidly spreading attacks

Solution:

Distributed Adaptive IDS thru Peer-to-peer gossip and cooperation

One developed by Intel



PEP = policy enforcement point
DDI = distributed detection and inference

Logging of alerts (for all types)

- Typical information logged by a NIDS sensor includes:
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - Decoded payload data, such as application requests and responses
  - State-related information

Intrusion detection exchange format

To facilitate development of a distributed IDS

Not a product, but a proposed IETF standard

Key elements

Data source: raw data from an IDS

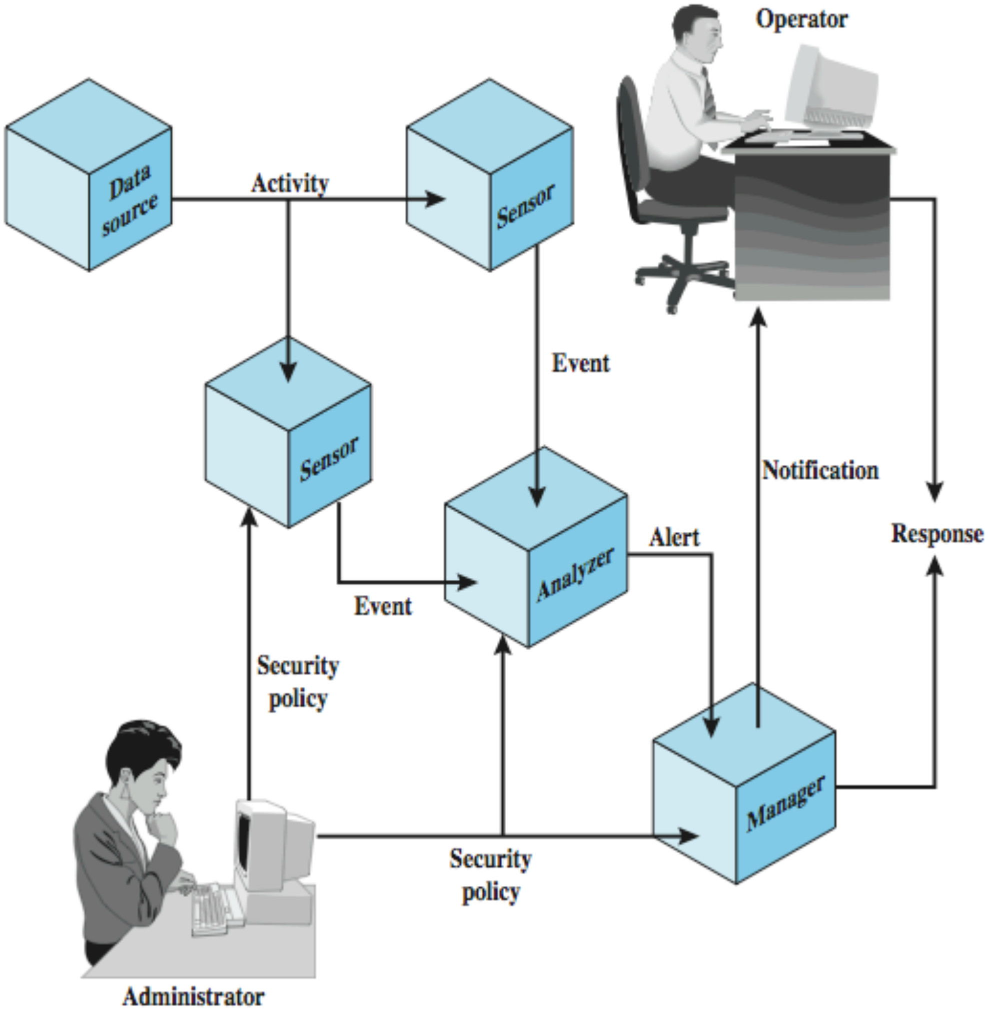
Sensor: collect and forward events

Analyzer: process data

Administrator defines sec policy

Manager: a process for operator to manage the IDS system

Operator: the user of the Manager



Example of a response: **log an activity**

Honeypots

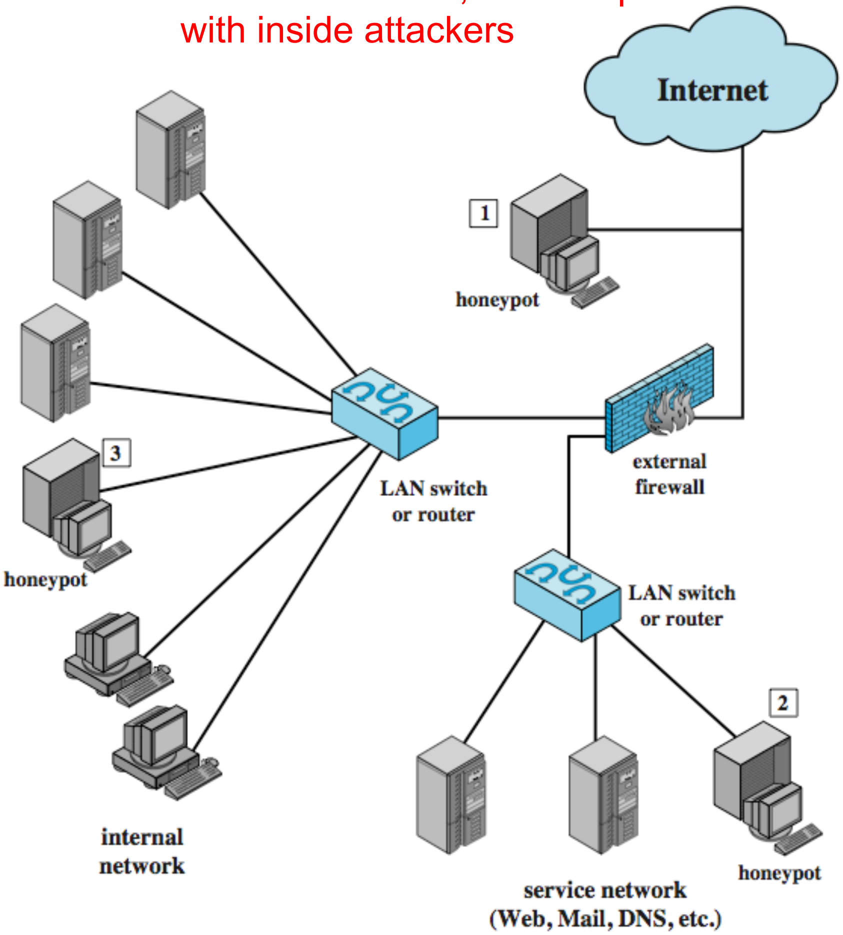
- Decoy systems
  - Filled with fabricated info and instrumented with monitors/ event loggers
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
  - Divert and hold attacker to collect activity info without exposing production systems
- Initially were single systems
- More recently are/emulate entire networks

Honeypot classification

- Low interaction honeypot
  - Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
  - Provides a less realistic target
  - Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
  - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers

Honeypot deployment

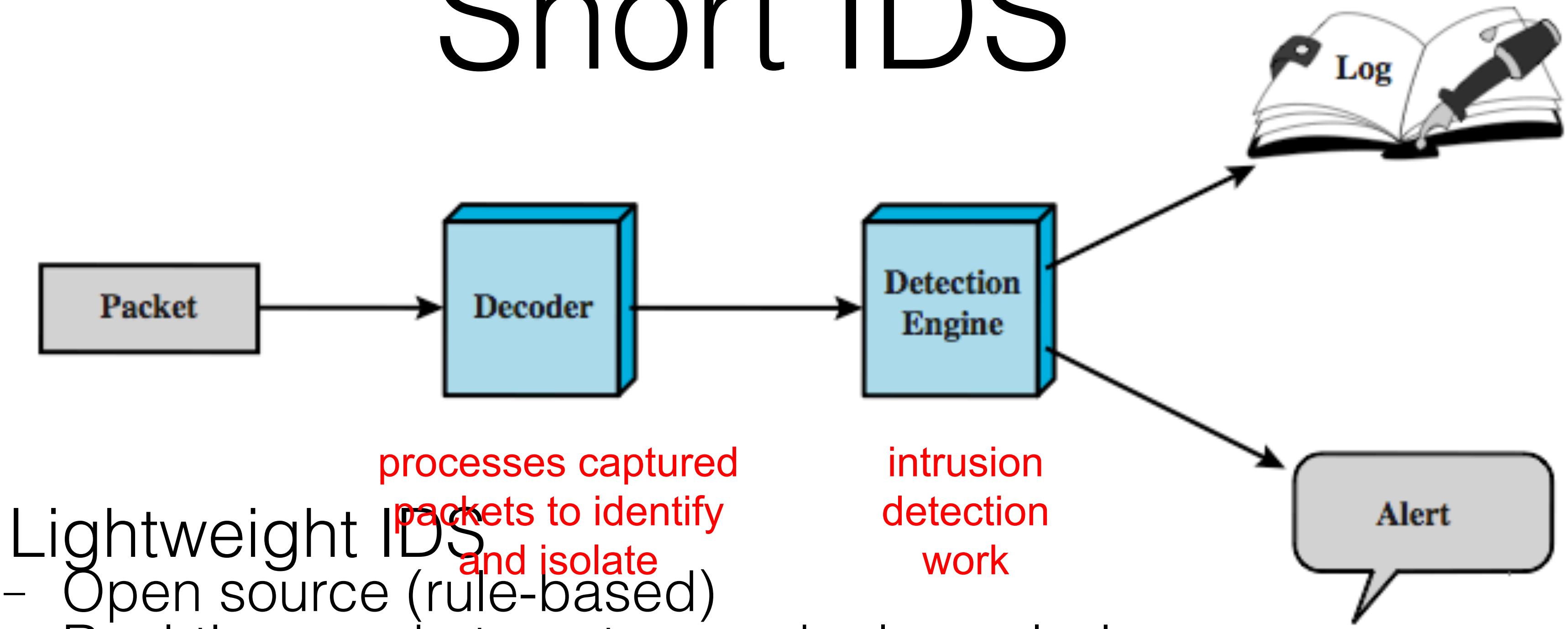
1. Tracks attempts to connect to an unused IP address; can't help with inside attackers



3. Full internal honeypot; can detect internal attacks

2. In DMZ; must make sure the other systems in the DMZ are secure; firewalls may block traffic to the honeypot

Snort IDS



processes captured packets to identify and isolate

intrusion detection work

- Lightweight IDS
  - Open source (rule-based)
  - Real-time packet capture and rule analysis
  - Passive or inline
  - Components: decoder, detector, logger, alerter

SNORT Rules

- Use a simple, flexible rule definition language
- Fixed header and zero or more options
- Deader includes: action, protocol, source IP, source port, direction, dest IP, dest port
- Many options
- Example rule to detect TCP SYN-FIN attack:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```

  - detects an attack at the TCP level; $strings are variables with defined values; any source or dest port is considered; checks to see if SYN and FIN bits are set

Firewalls

Firewalls and Intrusion Prevention Systems

- Effective means of protecting LANs

- Internet connectivity essential
  - For organization and individuals
  - But creates a threat

- Could secure workstations and servers

- Also use firewall as perimeter defence
  - Single choke point to impose security

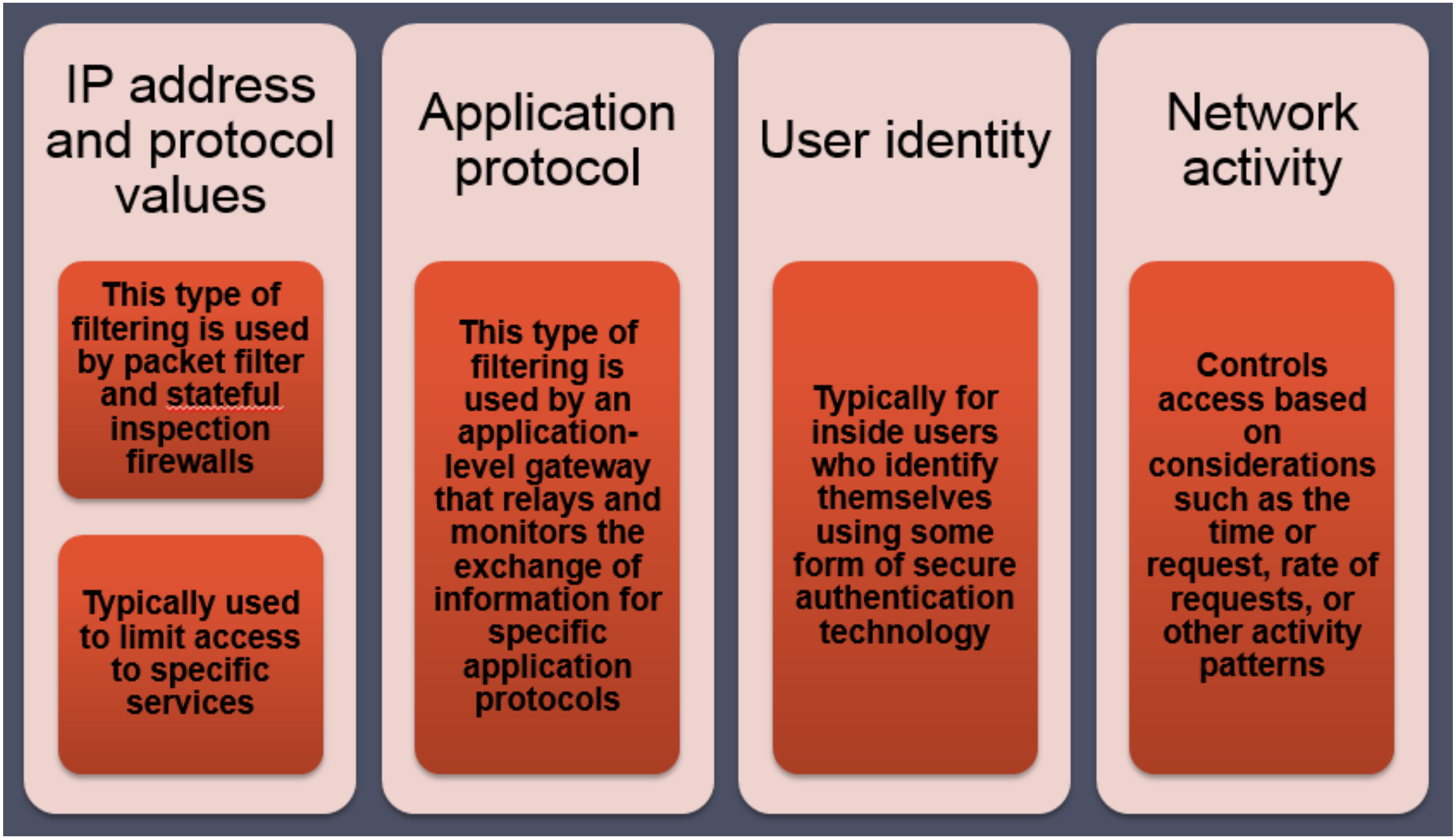
Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
  - Types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- The policy should be developed from the organization's security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Capabilities & Limits

- Capabilities
  - Defines a single choke point
  - Provides a location for monitoring security events
  - Convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC, VPNs
- Limitations
  - Cannot protect against attacks bypassing firewall
  - May not protect fully against internal threats
  - Improperly secure wireless LAN
  - Laptop, PDA, portable storage device infected outside then used inside

Firewall Filter Characteristics



IP address and protocol values

This type of filtering is used by packet filter and stateful inspection firewalls

Typically used to limit access to specific services

Application protocol

This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols

User identity

Typically for inside users who identify themselves using some form of secure authentication technology

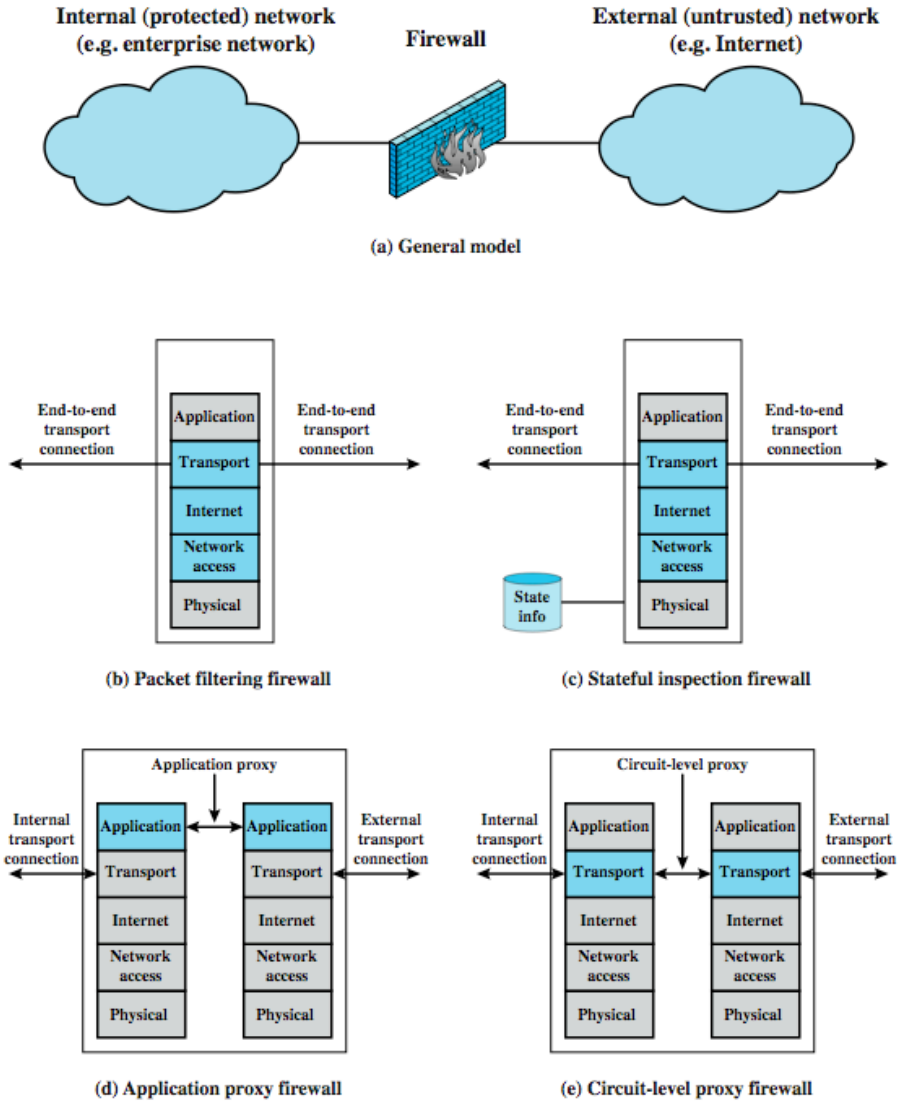
Network activity

Controls access based on considerations such as the time or request, rate of requests, or other activity patterns

Types of Firewalls

Positive (negative) filter: Allow (reject) packets that meet a criteria

Stateful inspection: Keeps track of TCP connections


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info
Application proxy
Circuit-level proxy
Internal transport connection
External transport connection

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

(d) Application proxy firewall

(e) Circuit-level proxy firewall

Packet Filtering Firewall

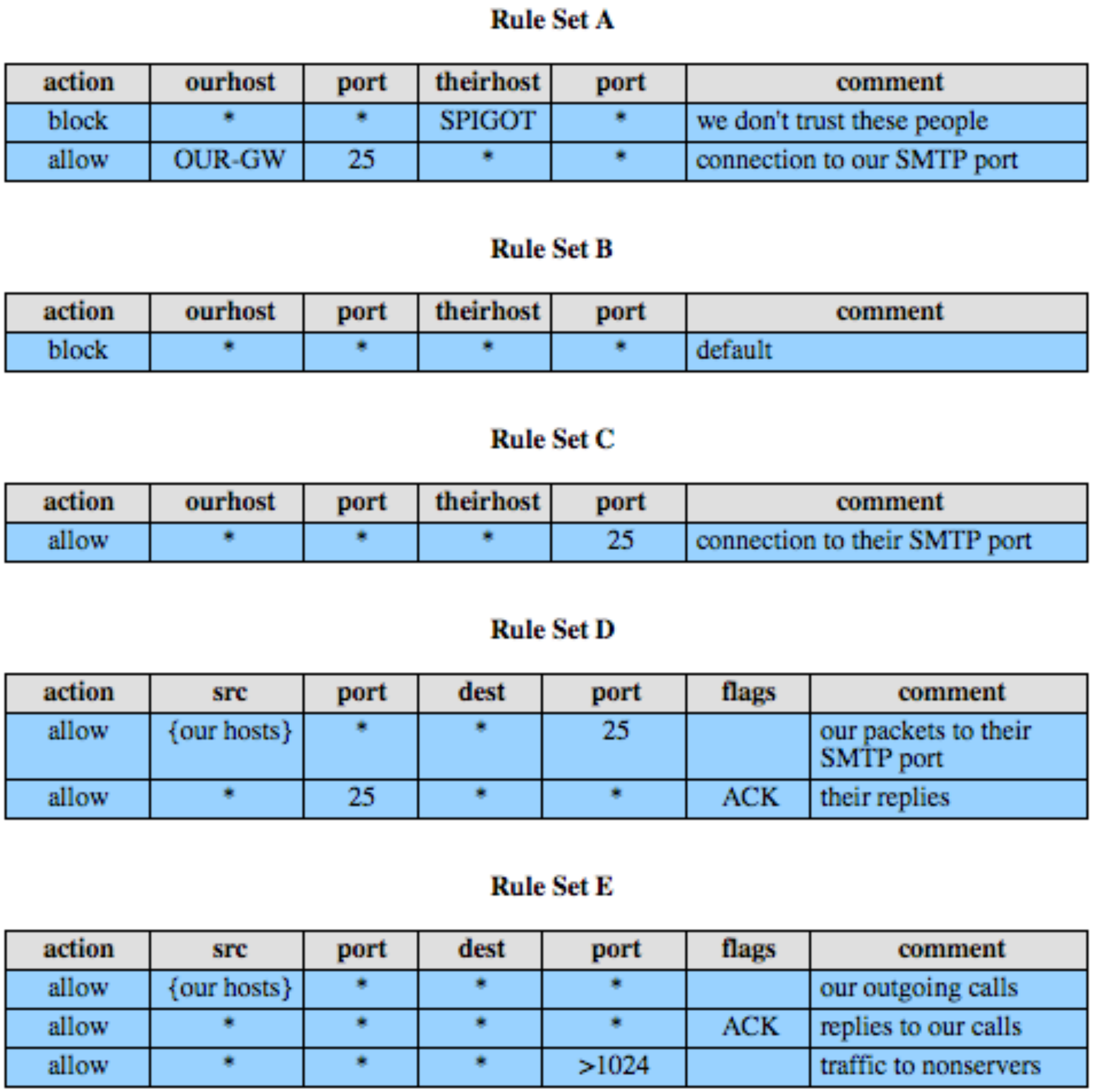
- Applies rules to packets in/out of firewall

- based on information in packet header
  - src/dest IP addr & port, IP protocol, interface

- Typically a list of rules of matches on fields
  - If match rule says if forward or discard packet

- Two default policies:
  - Discard: prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - Forward: permit unless expressly prohibited
    - easier to manage/use but less secure

Packet Filter Rules



Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

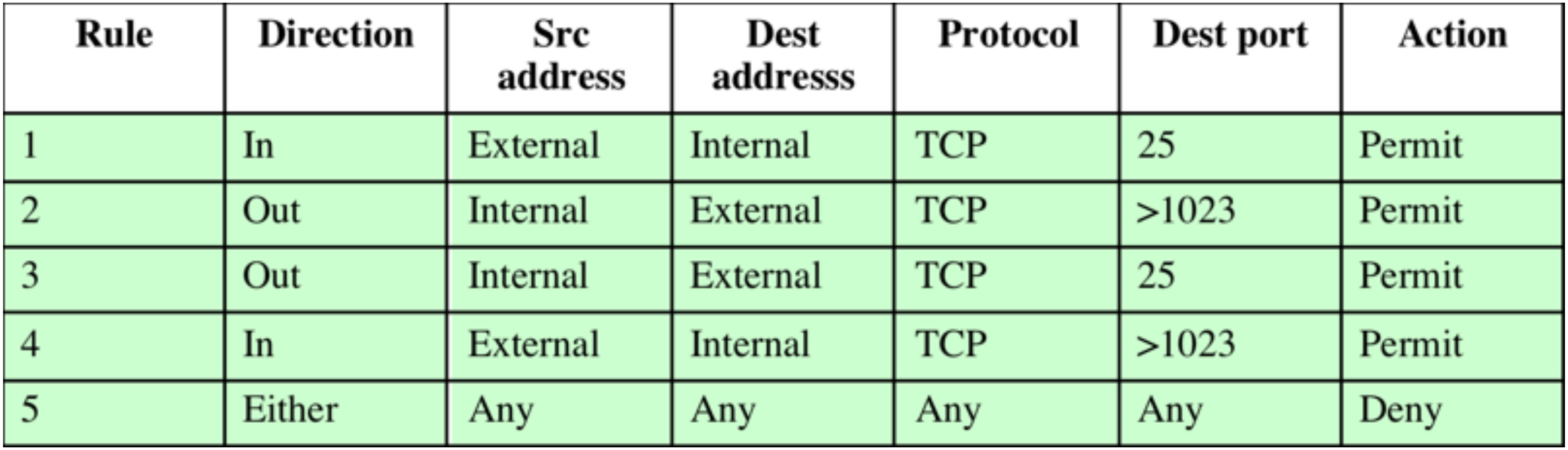
Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet Filter Rules



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

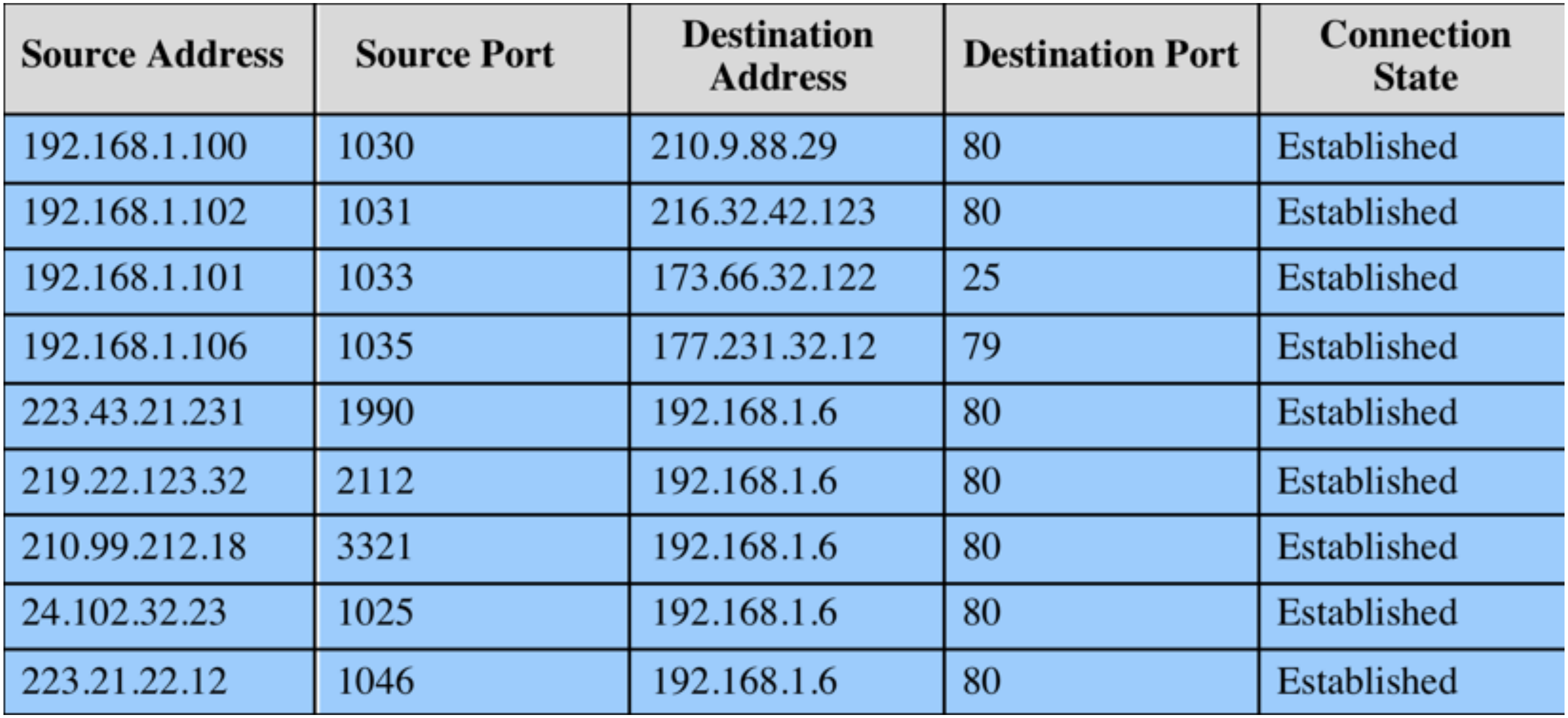
Packet Filter Weaknesses

- Weaknesses
  - Cannot prevent attack on application bugs
  - Limited logging functionality
  - Do no support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs (e.g., IP address spoofing)
  - Improper configuration can lead to breaches
- Attacks
  - IP address spoofing
  - Source route attacks (srs dictates the pkt route)
  - Tiny fragment attacks (to circumvent filtering rules that depend on TCP header info)

Stateful Inspection Firewall

- Reviews packet header information but also keeps info on TCP connections
  - Typically have low, “known” port # for server and high, dynamically assigned (ephemeral) client port #
  - Stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  - only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  - may also track TCP seq numbers as well

Connection State Table



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

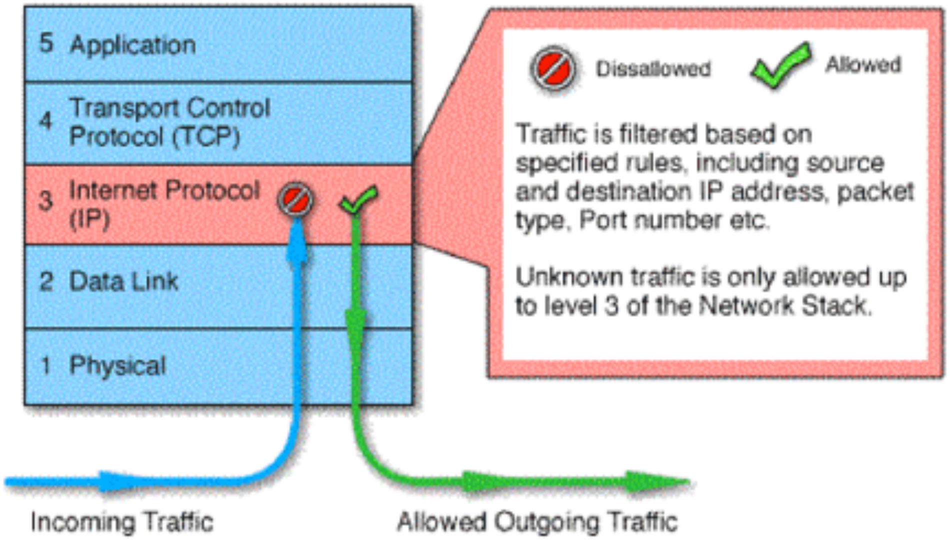
Application-Level (Proxy) Gateway

- Acts as a relay of application-level traffic
  - User contacts gateway with remote host name
  - Authenticates themselves
  - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
  - May restrict application features supported
  - Some services may not be available
- More secure than packet filters
- But have higher overheads

Circuit-Level Gateway

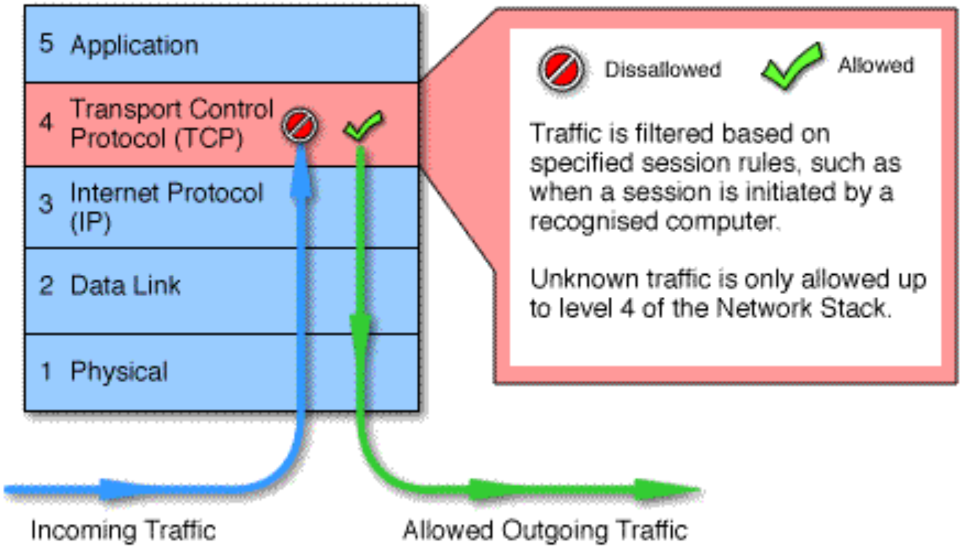
- Sets up two TCP connections, to an inside user and to an outside host
- Once connection is established, relays TCP segments from one connection to the other without examining contents
  - Hence independent of application logic
  - Just determines whether relay is permitted
- Typically used when inside users trusted
  - May use application-level gateway inbound and circuit-level gateway outbound
  - Hence lower overheads

Packet Filtering vs Gateway vs Application-Level Firewall



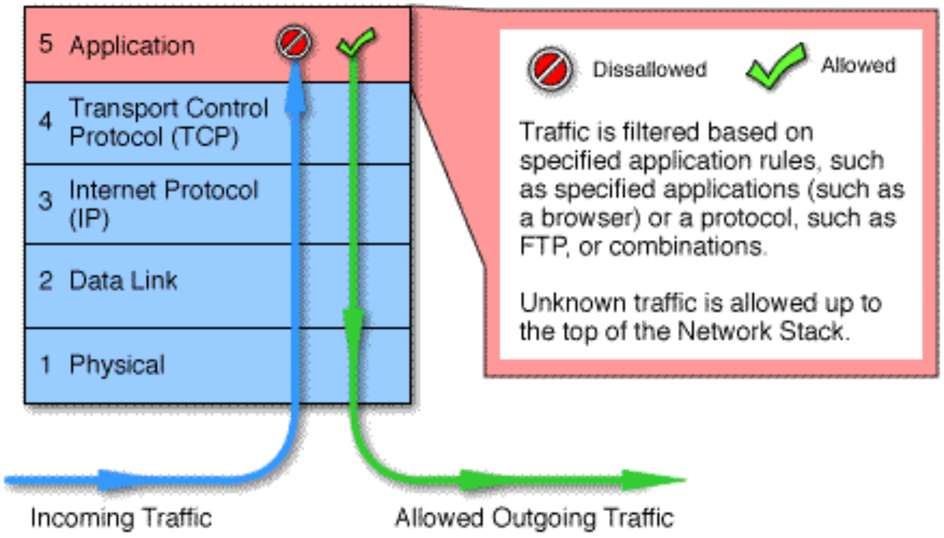
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.



Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Firewall Basing

- Several options for locating firewall:
- Bastion host
- Individual host-based firewall
- Personal firewall

Bastion Hosts

- Critical strongpoint in network
- Hosts application/circuit-level gateways
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user auth to access proxy or host
  - There may be many proxy services
  - Each proxy can restrict features, hosts accessed
  - Each proxy small, simple, checked for security
  - Each proxy is independent, can be uninstalled

Host-Based Firewalls

- Used to secure individual host
- Available in/add-on for many O/S
- Filter packet flows
- Often used on servers
- Advantages:
  - Tailored filter rules for specific host needs
  - Protection from both internal/external attacks
  - Additional layer of protection to org firewall when used with a standalone firewall

Personal Firewall

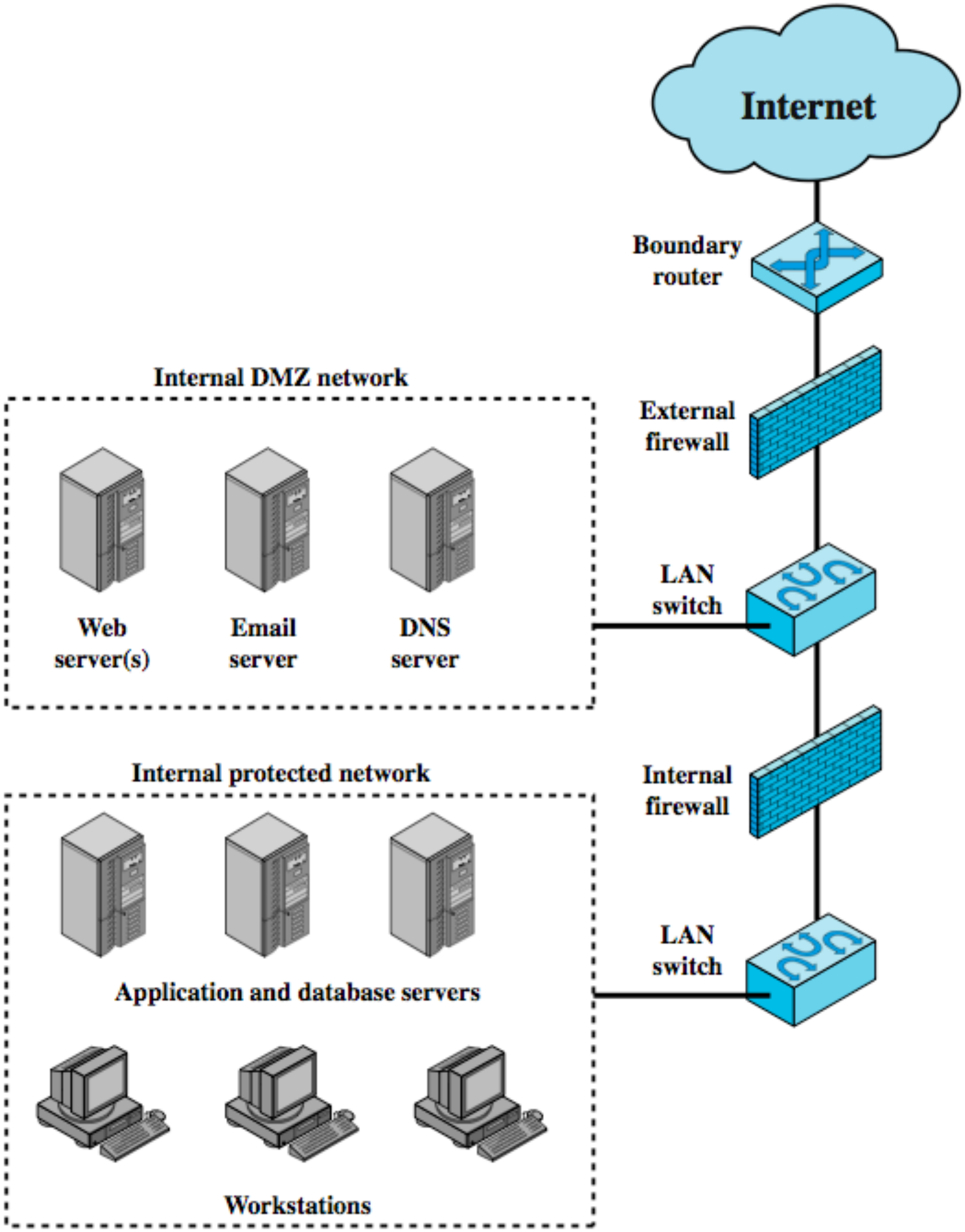
- Controls traffic flow to/from PC/workstation
- For both home or corporate use
- May be software module on PC
- Or in home cable/DSL router/gateway
- Typically much less complex
- Primary role to deny unauthorized access
- May also monitor outgoing traffic to detect/block worm/malware activity

Firewall

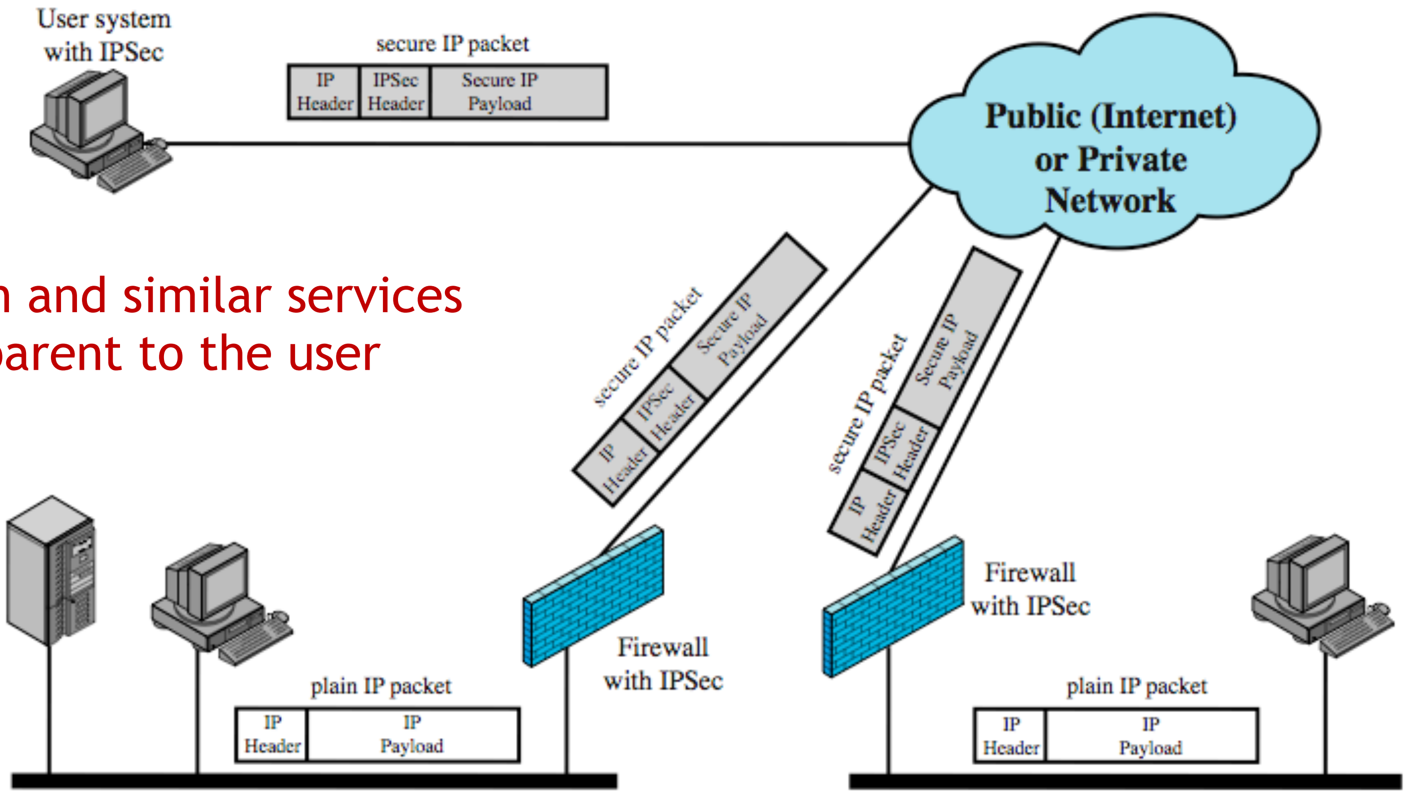
External firewall: protection for the DMZ consistent with their need for external connectivity

Internal firewall:

(a)more stringent filtering capability to provide protection from external attacks
(b) provides two way protection wrt the DMZ network



Virtual Private Networks

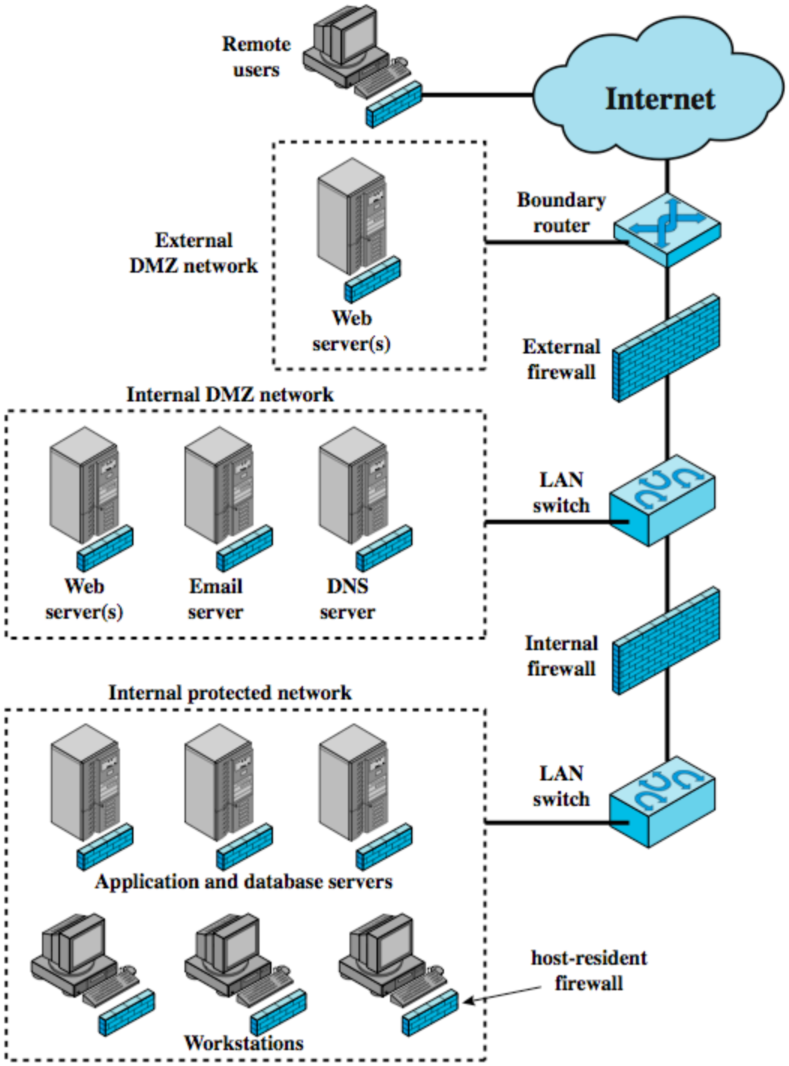


Encryption and similar services
but transparent to the user

Distributed Firewalls

A combination of earlier firewalls

Host-resident firewall on 100s of PCs plus standalone firewalls under a central administration



Firewall Topologies

- Host-resident firewall: personal firewall and firewall on servers (used alone or part of a defense in-depth)
- Screening router: a **single** router between internal and external networks, e.g., SOHO apps)
- Single bastion inline: **single** firewall **device** between an internal and external router (*stateful or app proxies*)
- Single bastion T: similar to above but has a **3rd NIC** on bastion to a DMZ (for medium to large organizations)
- Double bastion inline: DMZ is between (for large organizations)
- Distributed firewall configuration

Intrusion Prevention Systems (IPS)

- Recent addition to security products which
  - Inline network-/host-based IDS that can block traffic
  - Functional addition to firewall that adds IDS capabilities
- Using IDS algorithms but can block or reject packets like a firewall
- May be network or host based

Host-Based IPS

- Identifies attacks using both:
  - Signature techniques
    - malicious application packets
  - Anomaly detection techniques
    - behavior patterns that indicate malware
  - Example of malicious behavior: buffer overflow, access to email contacts, directory traversal

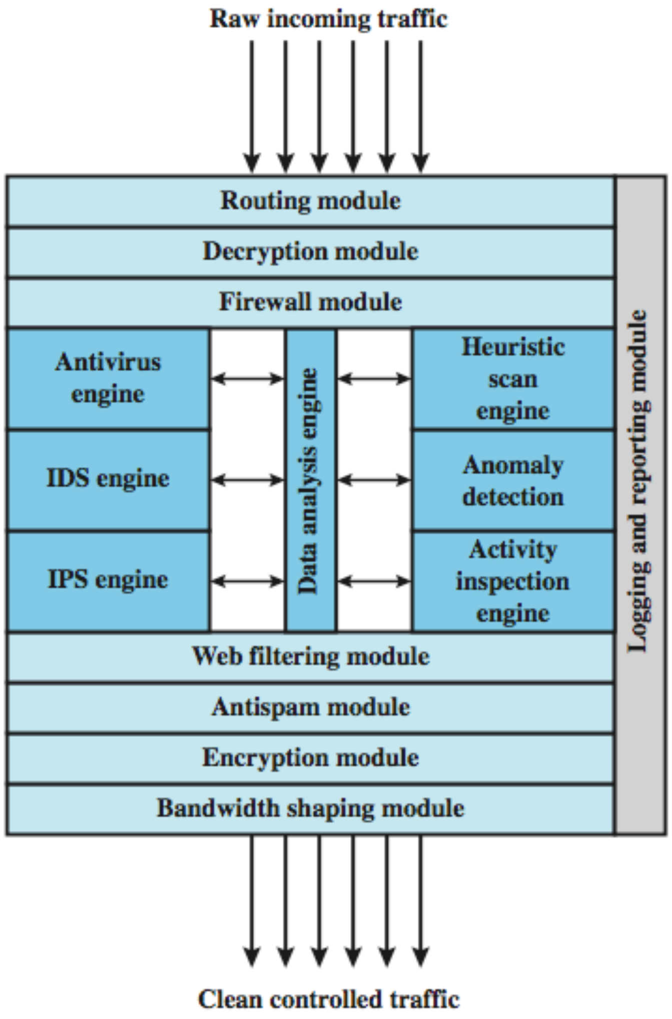
- Can be tailored to the specific platform
  - e.g. general purpose, web/database server specific

- Can also sandbox applets to monitor behavior

- May give desktop file, registry, I/O protection

Unified Threat Management Products

Reduce admin burden by replacing network products (firewall, IDS, IPS, …) With a single device


Raw incoming traffic
Routing module
Decryption module
Firewall module
Antivirus engine
IDS engine
IPS engine
Data analysis engine
Heuristic scan engine
Anomaly detection
Activity inspection engine
Logging and reporting module
Web filtering module
Antispam module
Encryption module
Bandwidth shaping module
Clean controlled traffic