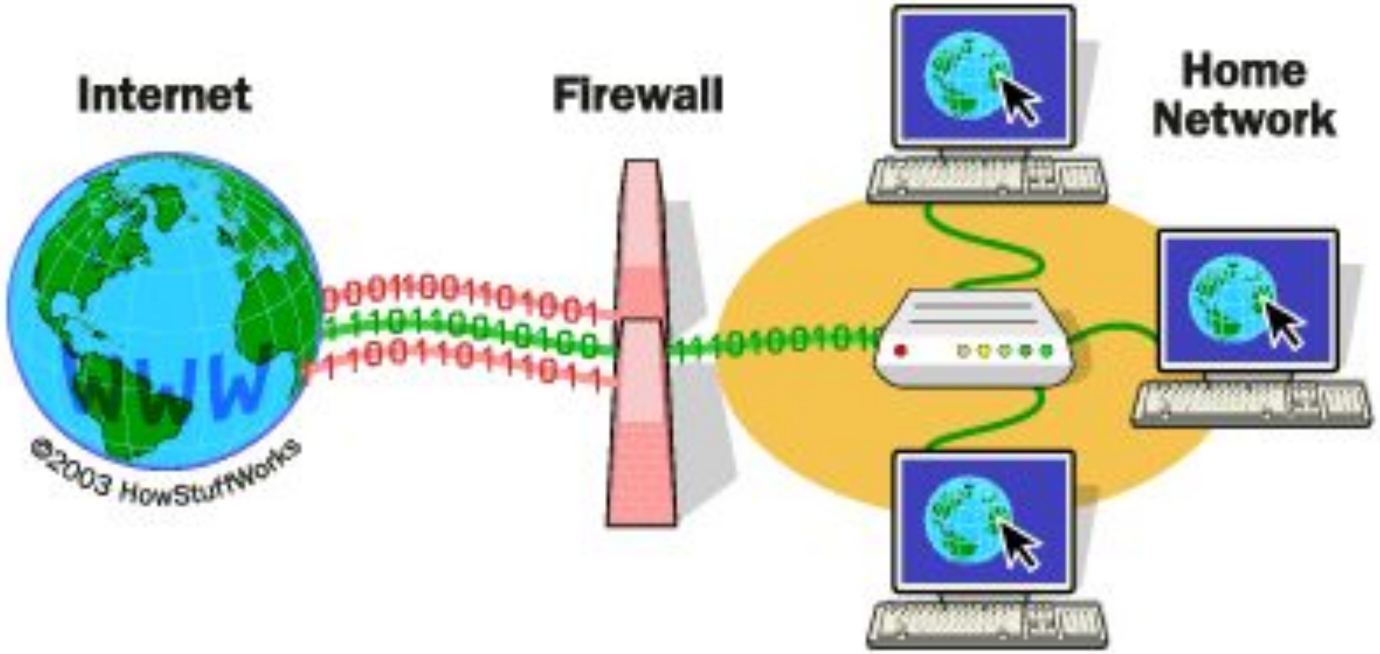
A4a: firewall, IDS

outline

- Firewall
    - What is it?
    - Categories
    - operations
- IDS/IPS
    - What is it?
    - internal mechanisms
- BYOD

firewall

- a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.



Source:
HowStuffWorks

Firewall: the first line of defense

- Analogy: an attacker at the gate
- A gate in a gated community.
  - The gate may stop 98% of unwanted visitors
  - The locks on your doors stop the remaining 2%
- The firewall is not enough!
  - Harden your machines by turning off services you don't need.

Source: charlottesvillesolutions

What should be protected?

- Anything that should not be publicized
  - Personal stuffs, digitized assets (e.g., patents, source code, transaction records,…)
  - In IoT, sensors and actuators
- Any way into your network
- Any way out of your network
- Information about your network

Why do we need a firewall?

- Block the attack traffic from outside
- Block the leakage of internal data to outside

- Fortifying individual hosts is too costly
- One firewall is simpler to administer than many hosts

What does a firewall do?

- be the sole connection between inside and outside.
  - A special router
- test all traffic against consistent rules.
- pass traffic that meets those rules.
- contain the effects of a compromised system

Firewall policies

- Who can send or receive what via the Internet?
- What Internet usage is not allowed?
- Who makes sure the policy works and is being complied with?
- When can changes be made to policy/rules?
- What will be done with the logs?
- Will we cooperate with law enforcement?

Firewall classification

- network/transport level
  - (stateless) packet filter
  - stateful packet filter (SPF)
- Application level
  - called proxy or gateway
- hybrid

3 firewall types

Packet filter (PF)

- Uses transport & internet layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Read the header and filter by rules
  - whether header fields match specific rules.

PF operations

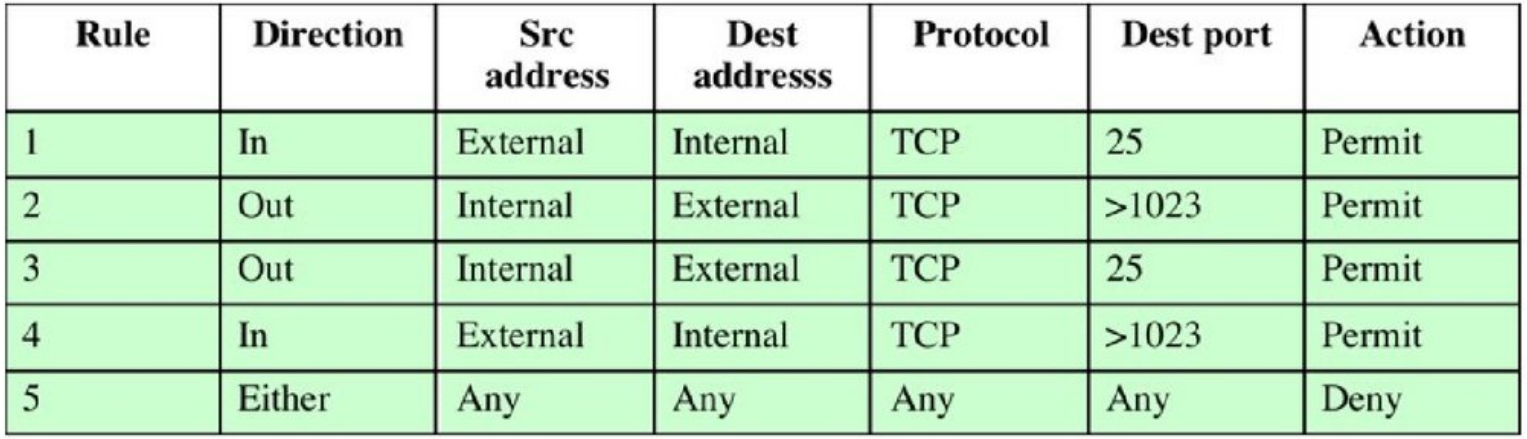
- Filtering with incoming or outgoing interfaces
  - Ingress filtering, Egress filtering
    - E.g. block spoofed address
- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port usage on a number of operating systems

PF operations: illustration

- Blocks packets based on:
  - Source IP Address or range of addresses.
  - Source IP Port
  - Destination IP Address or range of addresses.
  - Destination IP Port
  - Some allow higher layers up the OSI model.
  - Other protocols

4−tuple

well known ports	
80	http
443	https
20 & 21	ftp
23	telnet
22	ssh
25	smtp



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

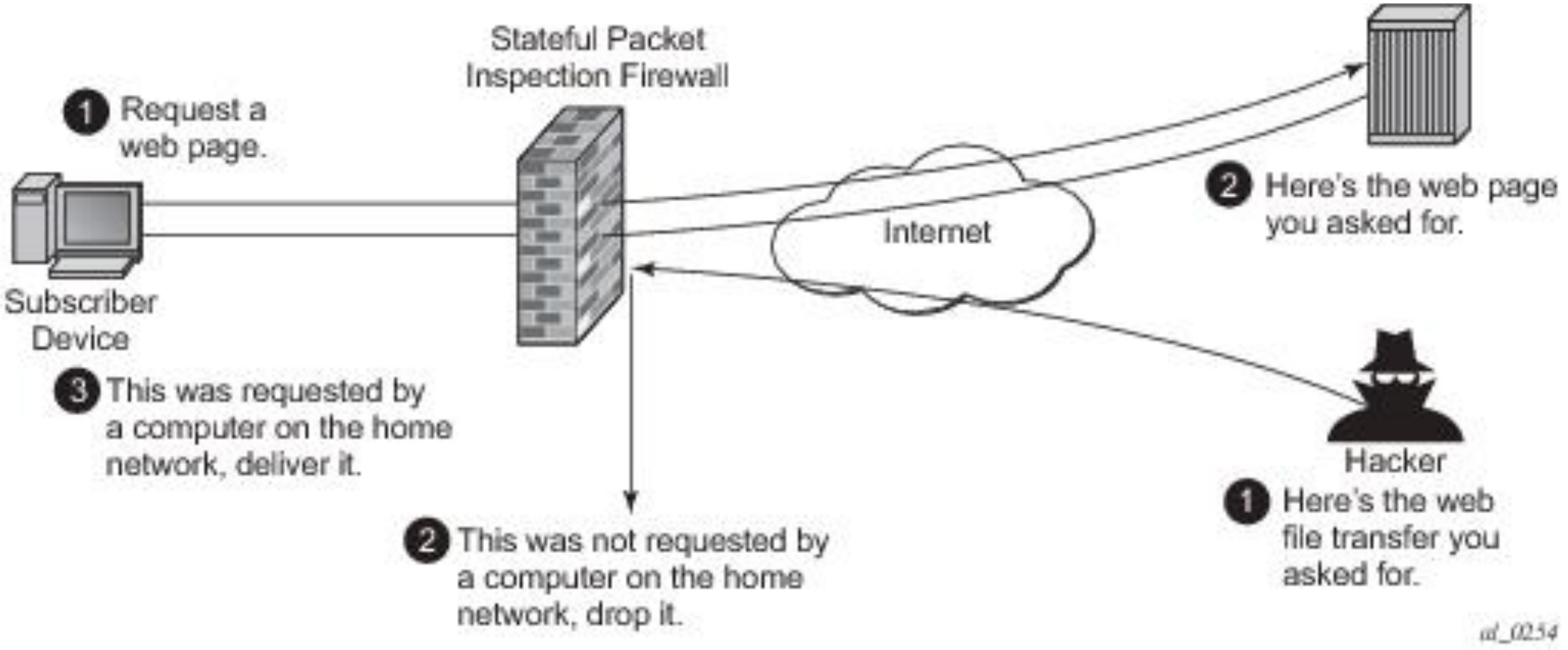
source: W Stallings and L. Brown, “Computer Security: Principles and Practice”

Packet filter weaknesses

- It's easy to botch the rules
- Good logging is hard
- Some stealth scanning is possible
  - E.g. fragmented packets (TCP header is split)
- Routers usually can't do authentication of end points
  - E.g. Spoofed address
- do not inspect the payload of the packet
  - E.g. An e-mail attachment that contains a virus could pass through the firewall if SMTP is allowed

Stateful packet filter (SPF)

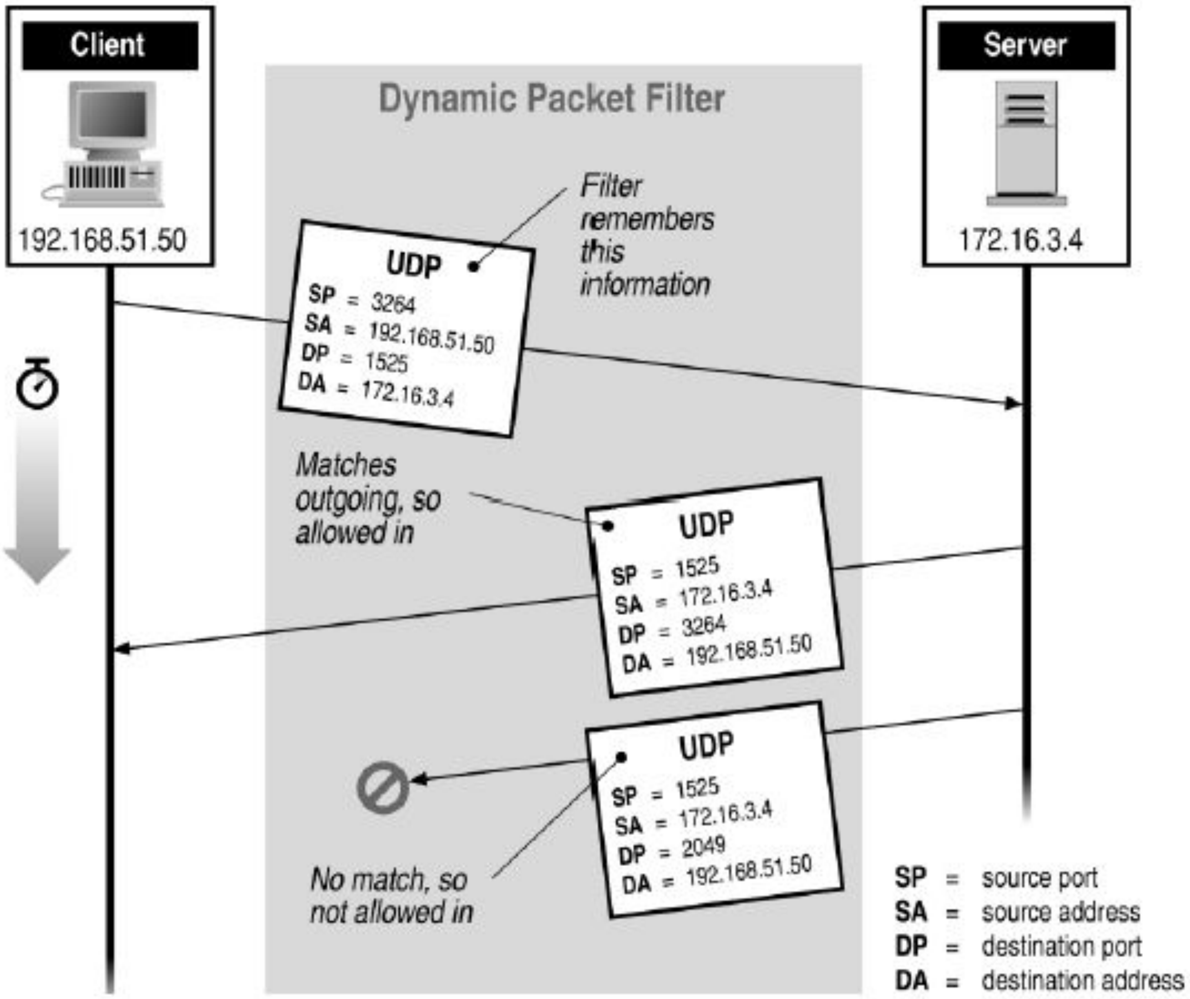
- aka connection tracking
- SPFs track the latest interval of network activity. If a packet doesn't fit in, they drop it
- SPFs have to collect and assemble packets in order to have enough data

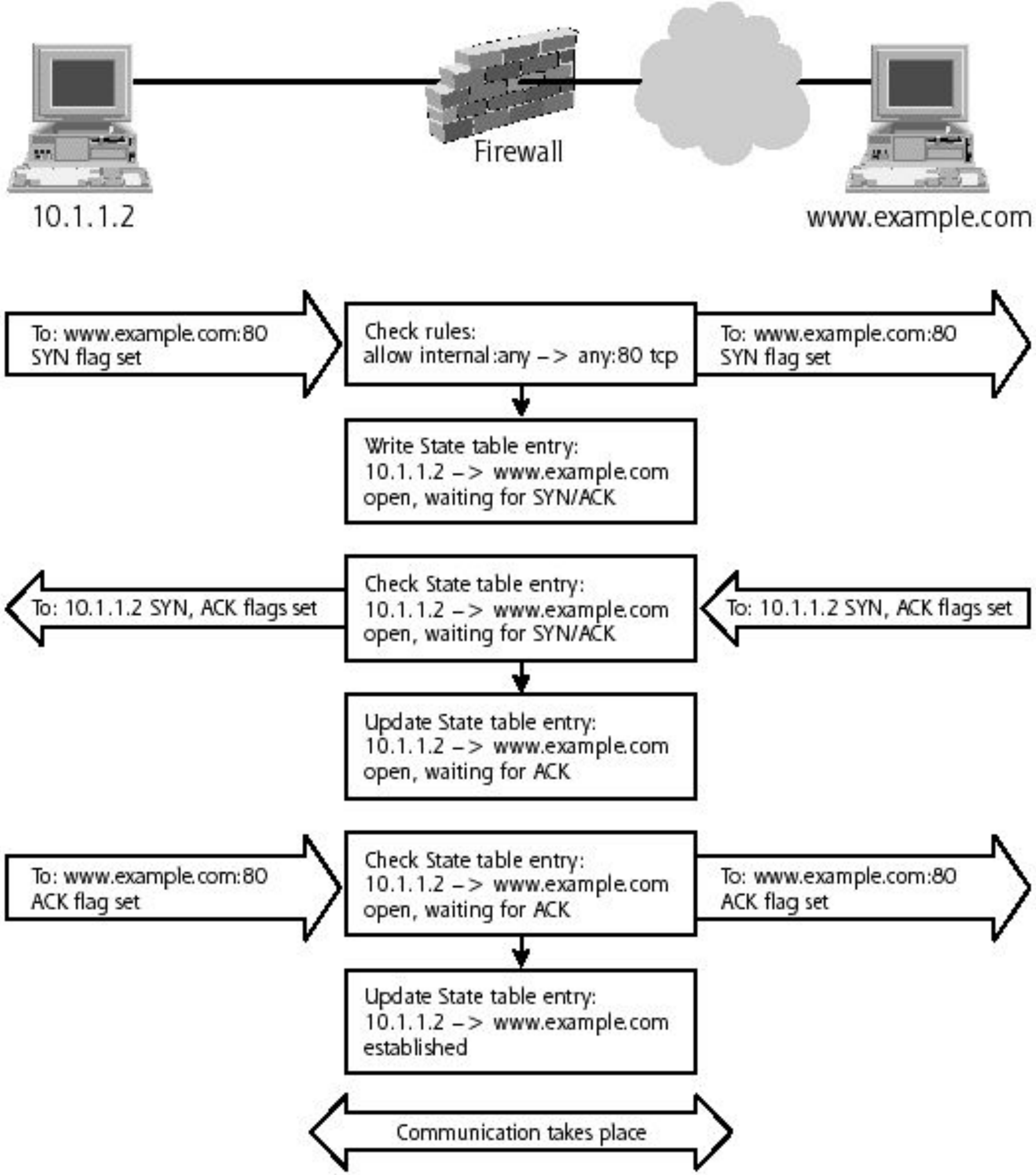


Stateful Packet Inspection Firewall
1 Request a web page.
Subscriber Device
Internet
2 Here's the web page you asked for.
3 This was requested by a computer on the home network, deliver it.
2 This was not requested by a computer on the home network, drop it.
Hacker
1 Here's the web file transfer you asked for.
al_0254

Source: alcatel-lucent

Stateful firewall




10.1.1.2
Firewall
www.example.com
To: www.example.com:80 SYN flag set
Check rules: allow internal:any –> any:80 tcp
To: www.example.com:80 SYN flag set
Write State table entry: 10.1.1.2 –> www.example.com open, waiting for SYN/ACK
To: 10.1.1.2 SYN, ACK flags set
Check State table entry: 10.1.1.2 –> www.example.com open, waiting for SYN/ACK
To: 10.1.1.2 SYN, ACK flags set
Update State table entry: 10.1.1.2 –> www.example.com open, waiting for ACK
To: www.example.com:80 ACK flag set
Check State table entry: 10.1.1.2 –> www.example.com open, waiting for ACK
To: www.example.com:80 ACK flag set
Update State table entry: 10.1.1.2 –> www.example.com established
Communication takes place

source: https://www.informit.com/articles/article.aspx?p=31945&seqNum=3

SPF weaknesses

- Most of the flaws of standard filtering still apply.
- if the cache entry is removed while the flow is still active – all remaining traffic will be dropped, and the connection will break.
  - Cache table overflow
  - Time-out too short
- Data inside an allowed connection can be destructive
  - e.g., email attachment, javascript in web page

A special case: ftp

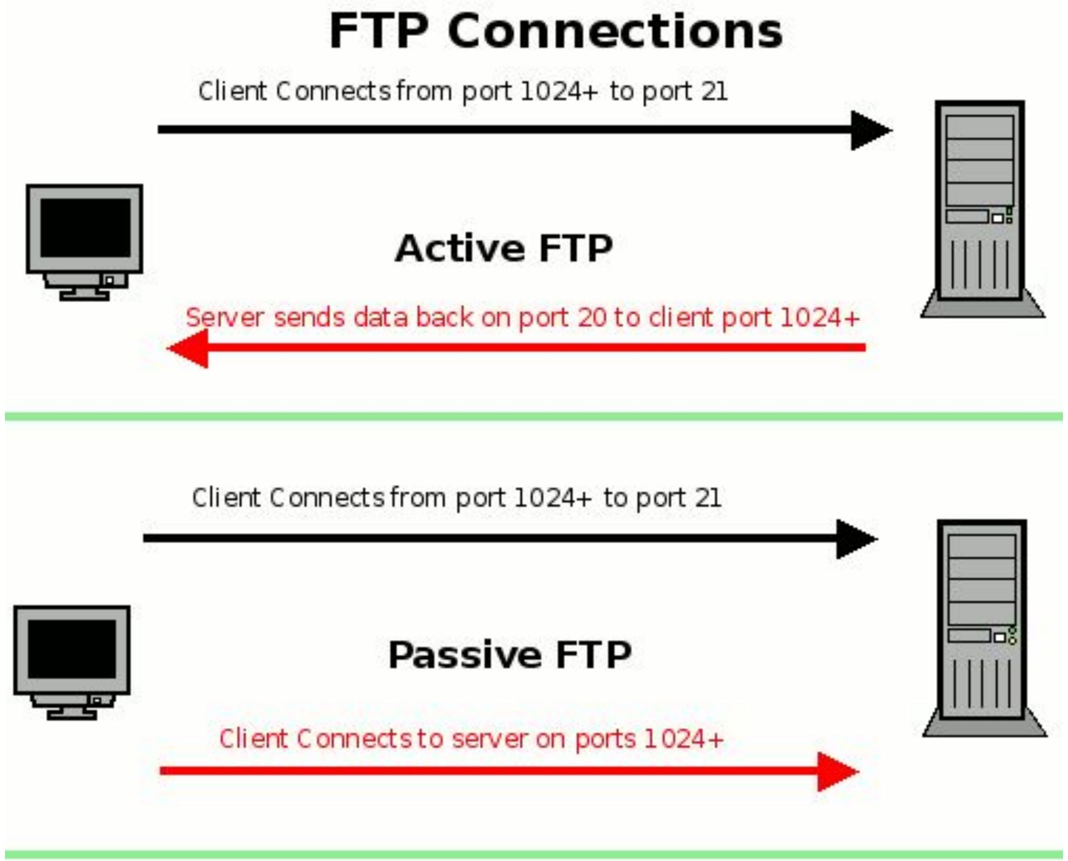
- original (or active) ftp

1. A client connect to a server using port 21
2. The server connects to the client using port 20

why two connections?

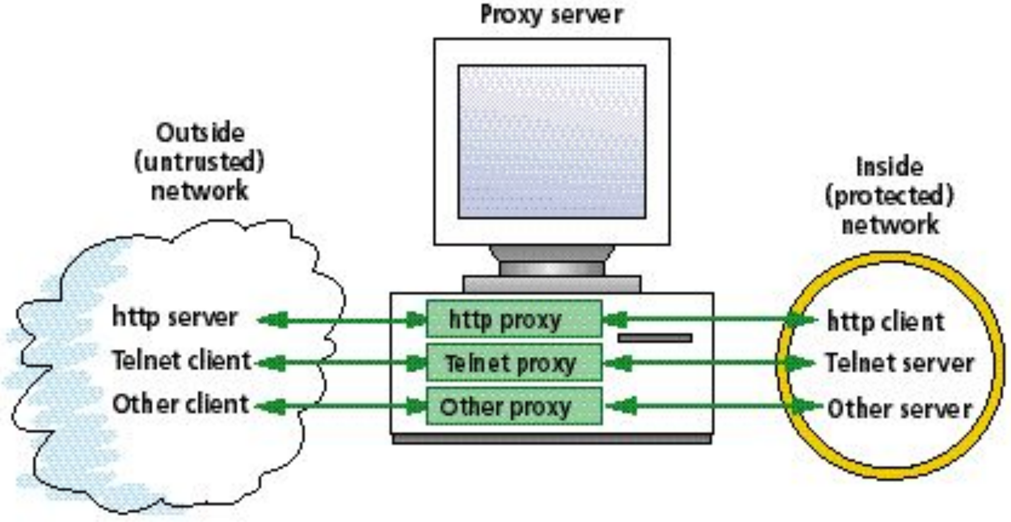
- passive ftp

1. A client connect to a server using port 21
2. The client then connects to the server using port 20


FTP Connections
Client Connects from port 1024+ to port 21
Active FTP
Server sends data back on port 20 to client port 1024+
Client Connects from port 1024+ to port 21
Passive FTP
Client Connects to server on ports 1024+

Application level firewall

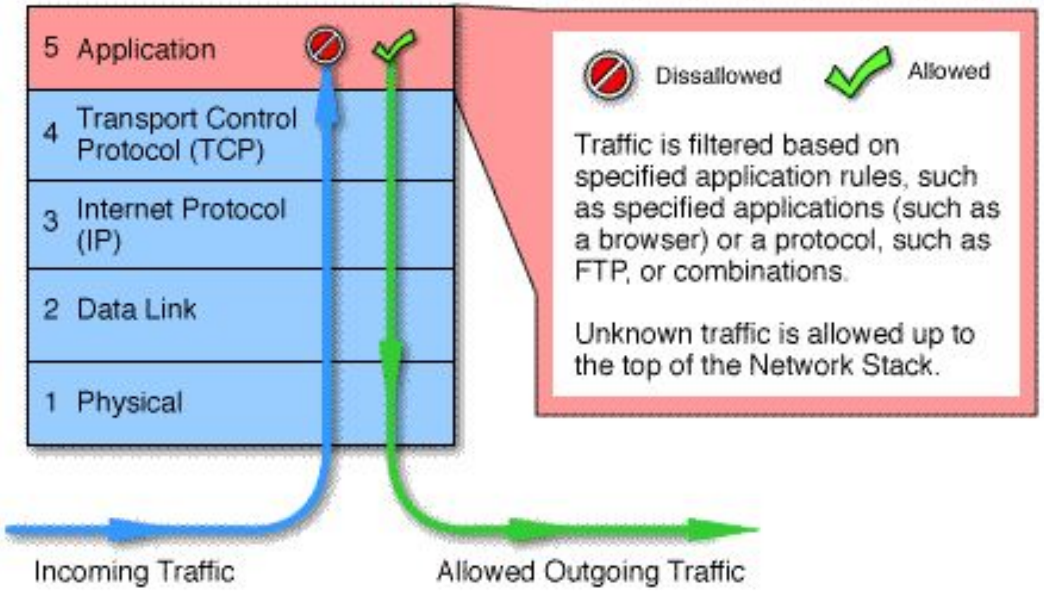
- aka proxy firewall
- Proxy firewalls pass data between two separate connections, one on each side of the firewall.
  - Proxies should not route packets between interfaces by looking at TCP/IP headers only
- Firewall transfers only acceptable content between the two connections.
- The proxy can understand the application protocol and filter the content.
  - URL filtering, data modification, and HTTP object caching



source: http://www.schuba.com/christoph/pub/courses/icns-0203/lectures/lecture.10.html

Appl. level firewall

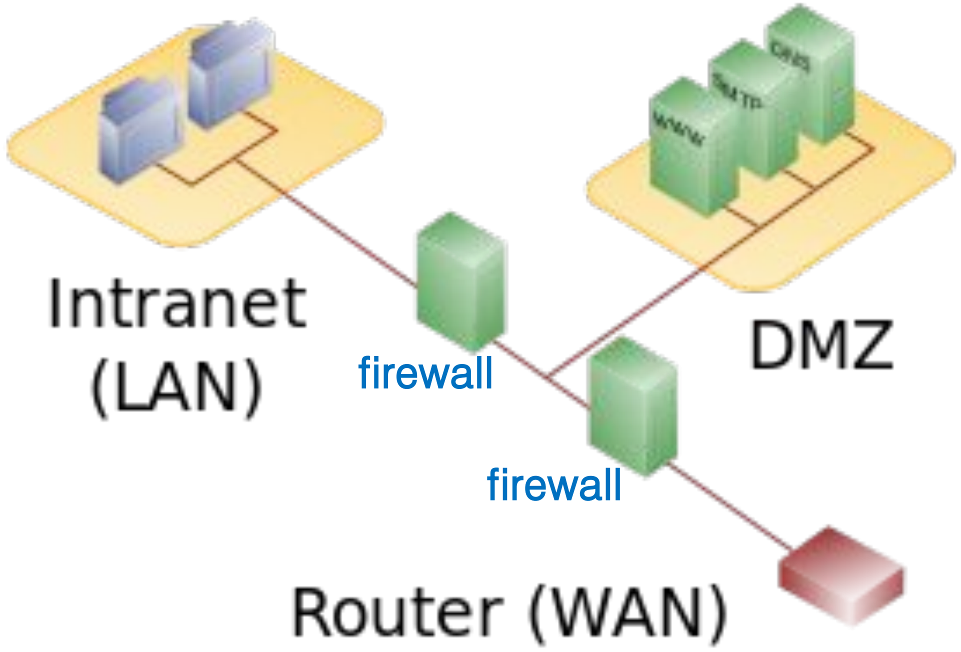
- user program is now involved, and accessible to attack.
  - program must be hardened
- Higher latency & lower throughput
- A new proxy program usually must be installed for each protocol
- Proxy services are vulnerable to operating system and application level bugs


5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
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.
Incoming Traffic
Allowed Outgoing Traffic

source: http://www.vicomsoft.com/knowledge/reference/firewalls1.html

DeMilitary Zone (DMZ)

- a subnet that contains and exposes an organization's external-facing services to an untrusted Internet.
- DMZ functions as a small, isolated network positioned between the Internet and the private network, usually intervened by firewalls

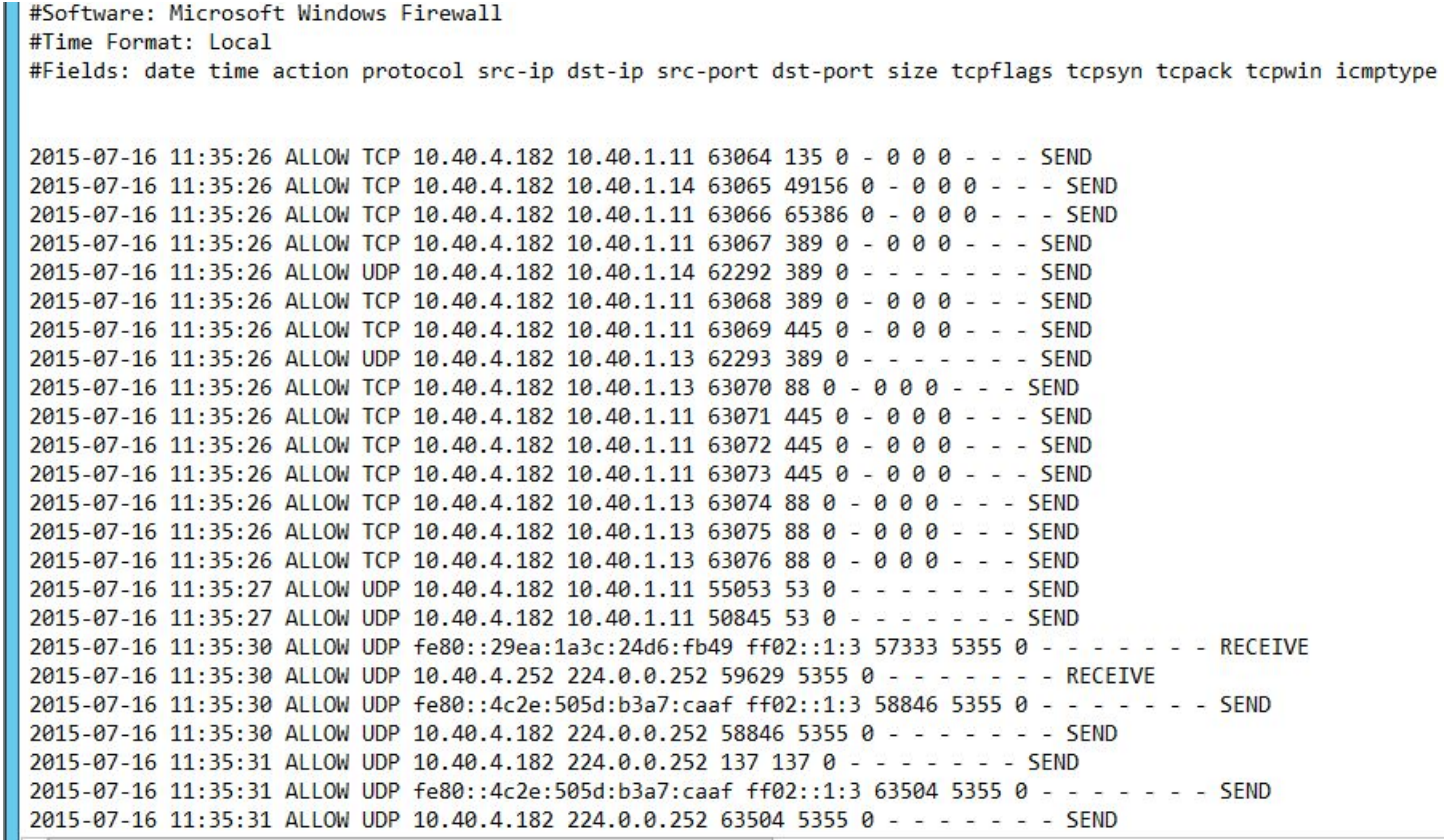


source: https://en.wikipedia.org/wiki/DMZ_(computing)

Firewall logging

- Logging is very important
  - Provides history of access
  - Provides attack information
  - Provides for Policy audit checking
  - Provides trending analysis for capacity planning
  - Provides evidence for events
- issues
  - Many firewalls do not log effectively
  - Extremely large files
  - Difficult to manage and review
  - Products have logs written to different files
  - Access to many logs requires root access to firewalls
  - Log analysis products are add-on and expensive
  - Few organizations log effectively

Firewall log sample



```
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype


2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND
```

IDS/IPS

Intrusion detection/prevention system

intrusion?

- Intrusions
  - Actions that attempt to bypass security mechanisms
  - E.g., unauthorized access, inflicting harm, etc.
- Example intrusions
  - DoS/DDoS attacks
  - Scans
  - Worms and viruses
  - Host compromises
- Intrusion detection
  - Monitoring and analyzing traffic
  - Identifying abnormal activities
  - Assessing severity and raising alarms

Where to Detect Intrusions?

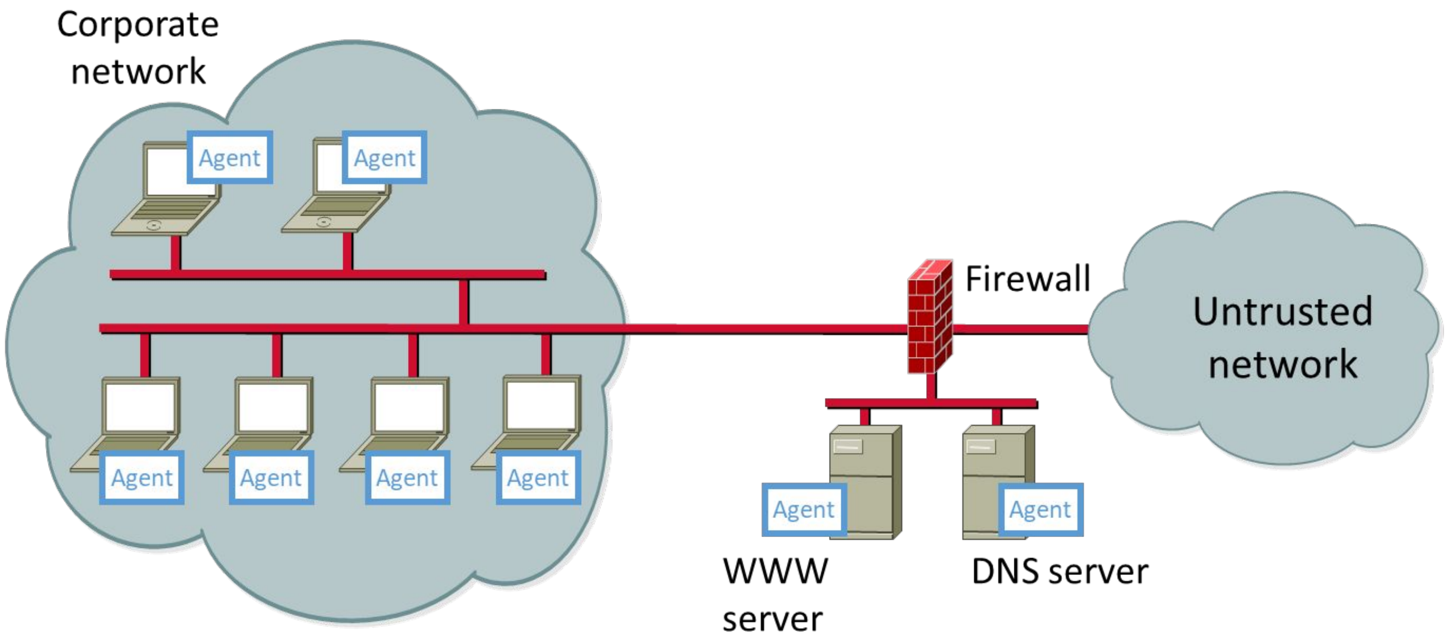
- **End host:** OS or application
  - Includes logins, file I/O, program executions, etc.
  - Can work with encrypted traffic and at lower speeds
  - Avoid extra packet reassembly and ambiguity
- **Network:** at enterprise edge
  - Single location for detecting and blocking attacks
  - Avoid reliance on the end host, OS, user, ..
  - Reduce overhead on the end host and network
- **Network**: in the backbone
  - Very limited

Intrusion detection/prevention system

- **Intrusion detection system** (**IDS**) is software or hardware designed to monitor, analyze and respond to events occurring in a computer system or network for signs of possible incidents of violation in security policies.
  - Host-based vs. Network-based
- **Intrusion prevention system** (**IPS**) adds more functionalities to stop/mitigate attacks

Host based intrusion detection Systems

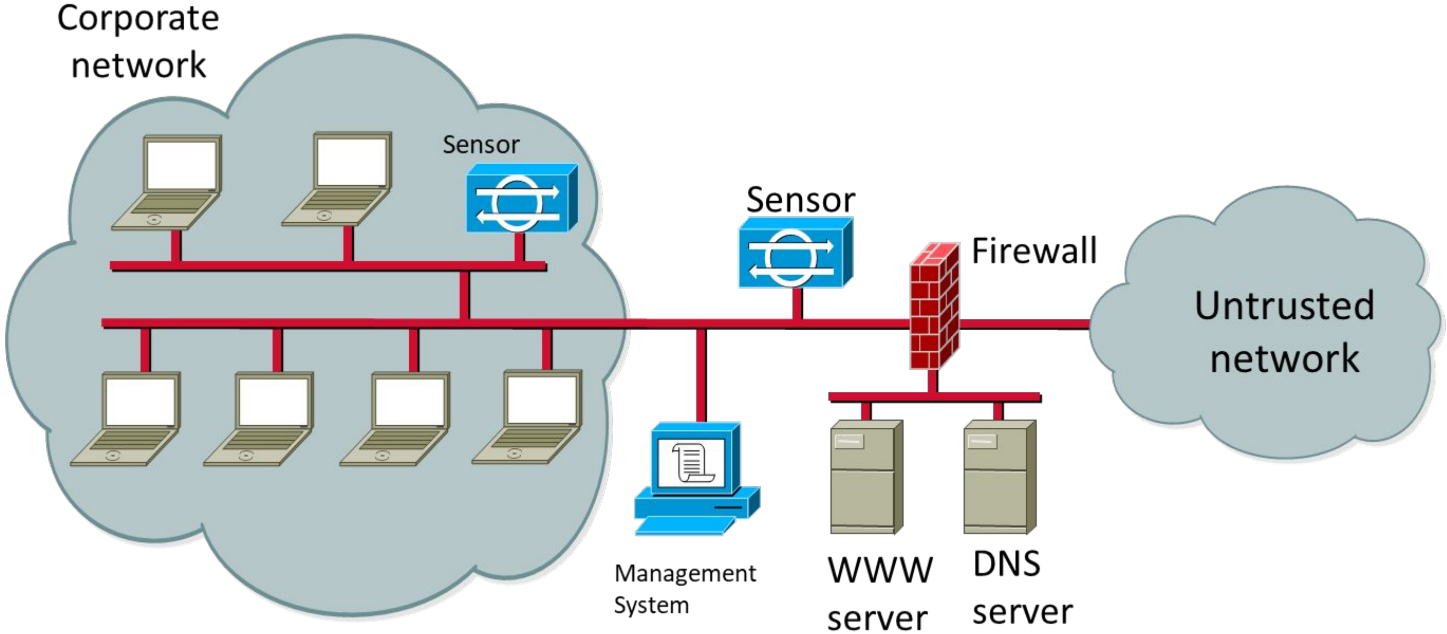
- Software (Agents) installed on computers to monitor input and output packets from device
- It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.



source: https://gbhackers.com/intrusion-detection-system-ids-2/

Network-Based Intrusion Detection Systems (NIDS)

- Connected to network segments to monitor, analyze and respond to network traffic.
- A single IDS sensor can monitor many hosts
- NIDS sensors are available in two formats
  - **Appliance:** It consists of specialized hardware sensor and its dedicated software. The hardware consists of specialized NIC's, processors and hard disks to efficiently capture traffic and perform analysis.
  - **Software:** Sensor software installed on server and placed in network to monitor network traffic.



source: https://cyberhoot.com/cybrary/network-based-intrusion-detection-system-nids/

How to Detect Intrusions?

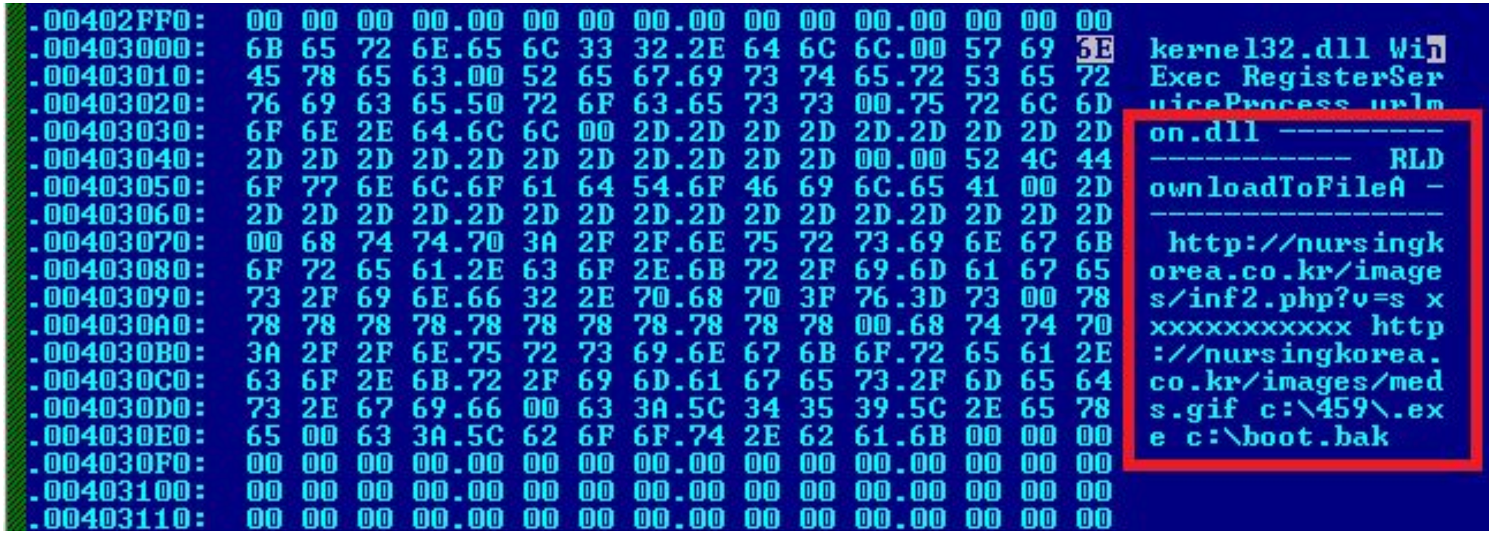
	Anomaly Detection	Signature Detection
Patterns	Train to create a baseline of normal network traffic	Codify patterns of known vulnerabilities or attacks
Detection	Detect statistically significant deviations from normal	Detect matches to the patterns in the signatures
Pros	Can detect novel (“zero day”) attacks	Builds on past experiences
Cons	May miss low-rate attacks; high rate of false alarms	Misses novel attacks; requires continuous updates to signatures

Anomaly Detection

- Traffic volume
  - Detect deviations in bytes/sec or packets/sec over time
  - Not effective for detection low-volume attacks
- Traffic features
  - Detect changes in distributions of traffic characteristics
  - E.g., traffic distribution by IP address, port number, packet size, TCP flags, etc.
  - Aids in classifying the anomaly (e.g., DoS vs. port scan)
- Detection techniques
  - Statistical techniques
  - Machine learning
  - …

Signature Detection

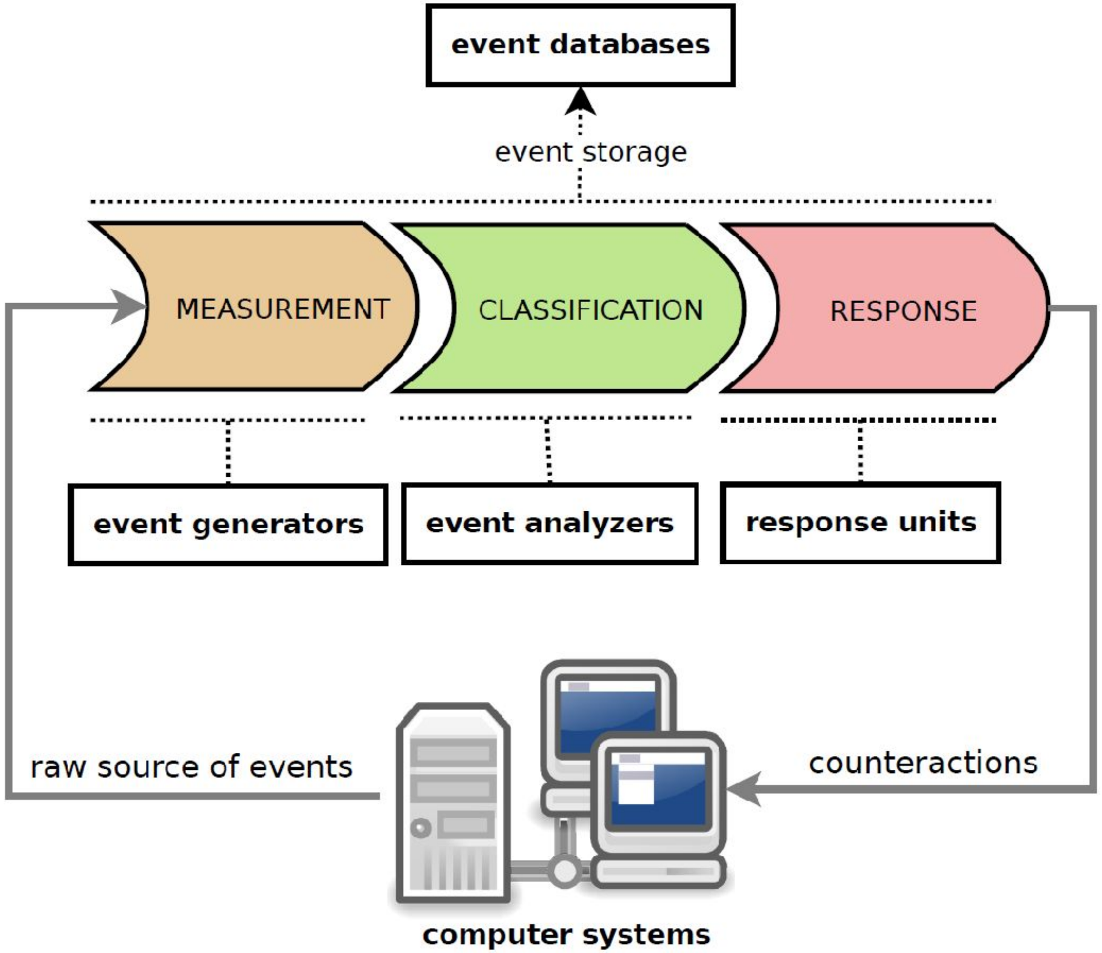
- Examples
  - Excessive login attempts
  - TCP packet with both SYN and RST set
  - A particular string of bytes
- Packet processing
  - Deep-packet inspection
  - Regular expression matching



```
.00402FF0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403000:  6B 65 72 6E.65 6C 33 32.2E 64 6C 6C.00 57 69 6E  kernel32.dll Win
.00403010:  45 78 65 63.00 52 65 67.69 73 74 65.72 53 65 72  Exec RegisterSer
.00403020:  76 69 63 65.50 72 6F 63.65 73 73 00.75 72 6C 6D  viceProcess urlm
.00403030:  6F 6E 2E 64.6C 6C 00 2D.2D 2D 2D 2D.2D 2D 2D 2D  on.dll ---------
.00403040:  2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 00.00 52 4C 44  -----------  RLD
.00403050:  6F 77 6E 6C.6F 61 64 54.6F 46 69 6C.65 41 00 2D  ownloadToFileA -
.00403060:  2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D  ----------------
.00403070:  00 68 74 74.70 3A 2F 2F.6E 75 72 73.69 6E 67 6B   http://nursingk
.00403080:  6F 72 65 61.2E 63 6F 2E.6B 72 2F 69.6D 61 67 65  orea.co.kr/image
.00403090:  73 2F 69 6E.66 32 2E 70.68 70 3F 76.3D 73 00 78  s/inf2.php?v=s x
.004030A0:  78 78 78 78.78 78 78 78.78 78 78 00.68 74 74 70  xxxxxxxxxxx http
.004030B0:  3A 2F 2F 6E.75 72 73 69.6E 67 6B 6F.72 65 61 2E  ://nursingkorea.
.004030C0:  63 6F 2E 6B.72 2F 69 6D.61 67 65 73.2F 6D 65 64  co.kr/images/med
.004030D0:  73 2E 67 69.66 00 63 3A.5C 34 35 39.5C 2E 65 78  s.gif c:\459\.ex
.004030E0:  65 00 63 3A.5C 62 6F 6F.74 2E 62 61.6B 00 00 00  e c:\boot.bak
.004030F0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403100:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403110:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
```

What to Do After Detection?

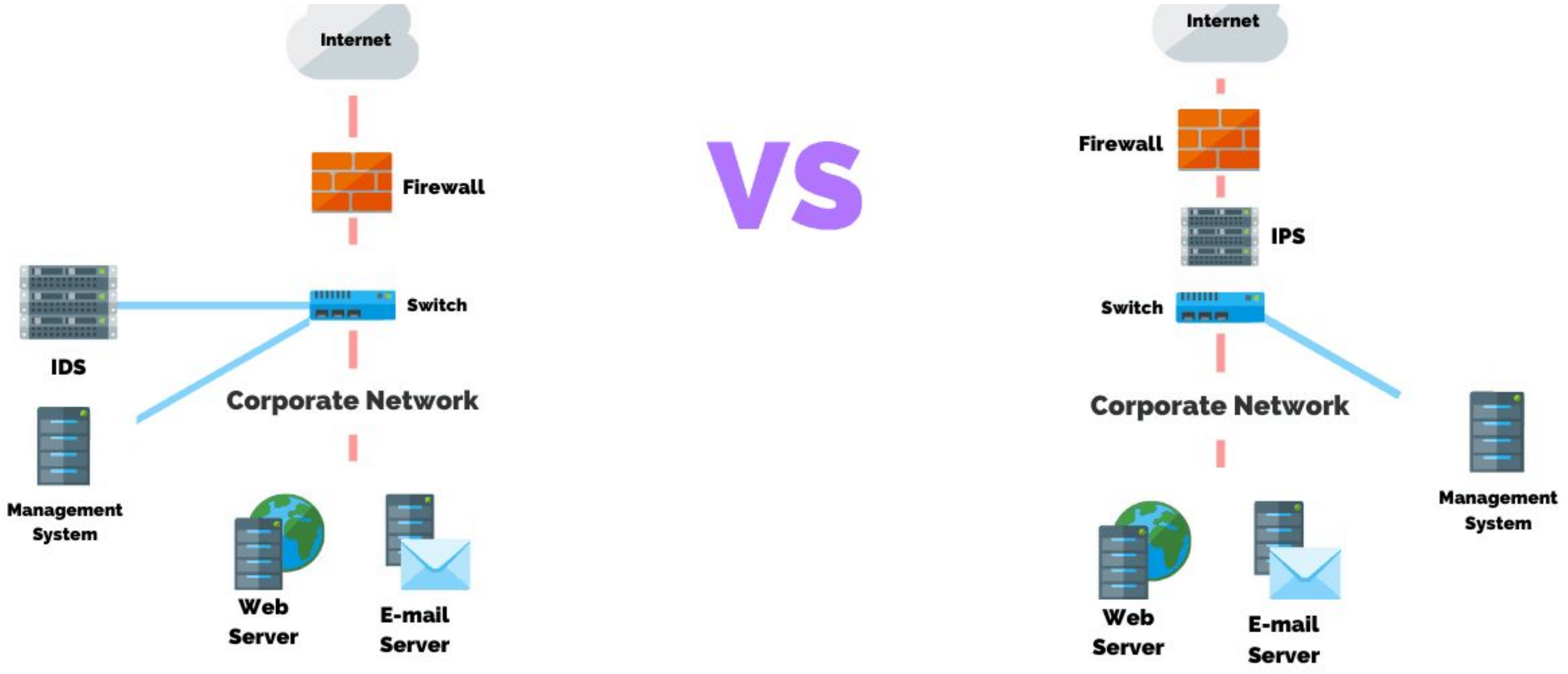
- Passively log
  - Collect, analyze, and record data
  - Report results to system/network administrator
  - Allow human to drive any response
  - Slower response, but better handling of false positives
- Actively defend
  - Detect problems in real time
  - Automatically generate a response
  - E.g., drop the traffic, engage the adversary
  - Faster response, but worse handling of false positives



Source: U. of Cagliari

IDS vs IPS

IDS	IPS
monitoring system	control system
basically doesn’t alter traffic	accept or reject traffic
requires a human/system to look at the results	requires the DB gets regularly updated
may not be located inline	located inline (on the traffic path)



source: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/#IPS

middlebox vs TLS

- there are many middleboxes in your connections
  - middleboxes want to look at your traffic
    - IDS/IPS, application level firewall,…
    - anti–virus software
    - Content delivery network (CDN)
  - mostly for your own good
- TLS allows only endpoints to look at the traffic
  - endpoints: browser, web server
- Can middleboxes and TLS co–exist happily?

byod

bring your own device (BYOD)

- BYOD advantages
    - faster technologies
    - less time to train employees
    - lower upfront costs during onboarding
    - employer saves more money
- BYOD disadvantages
    - increased complexity for security protocols
    - increased security risk
    - device as a distraction
    - limited privacy

BYOD policy

- securing your network in a BYOD environment is challenging
- how to protect your networks while using a BYOD policy?
  - conduct an IT Audit Before Enacting BYOD
  - Limit Access (role or profile-based)
  - requires two-factor authentication for mobile access
    - at least two of password, SMS, email, HW element,…
  - install mobile device management (MDM) technology
    - or Enterprise mobility management
  - enforce up-to-date software in devices
  - protect your endpoints (scan all the devices requesting access)
  - require immediate notification for lost or stolen devices
  - use device locator and remote wiping services