Firewall và IDS

NGUYEN HONG SON
PTITHCM

Khái niệm firewall

1. Defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
2. provides a location for monitoring security-related events
3. is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs
4. A firewall can serve as the platform for IPSec to implement virtual private networks.

Four general techniques that firewalls use

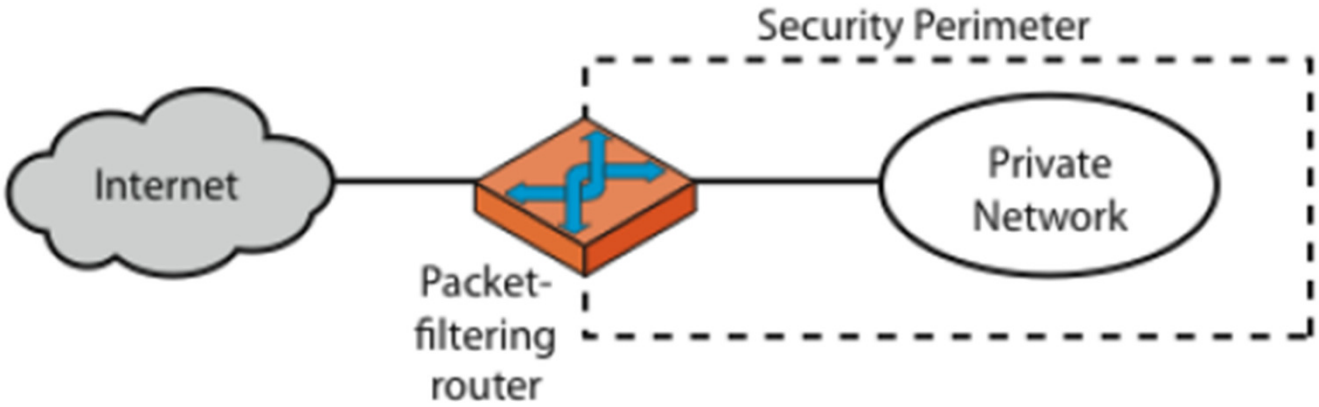
1. Service control: Determines the types of Internet services that can be accessed, inbound or outbound
2. Direction control: Determines the direction in which particular service requests are allowed to flow
3. User control: Controls access to a service according to which user is attempting to access it
4. Behavior control: Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

- Packet filters,
- Application-level gateways,
- Circuit-level gateways

Stateless Packet-filtering

Applies a set of rules to each incoming and outgoing IP packet



To forward or discard the packet

Filtering rules are based on information contained in a network packet such as src & dest IP addresses, ports, transport protocol & interface

A

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

B

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

C

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

D

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

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

A. Inbound mail is allowed to a gateway host only (port 25 is for SMTP incoming)

B. explicit statement of the default policy

C. tries to specify that any inside host can send mail to the outside, but has problem that an outside machine could be configured to have some other application linked to port 25

D. properly implements mail sending rule, by checking ACK flag of a TCP segment is set

E. this rule set is one approach to handling FTP connections

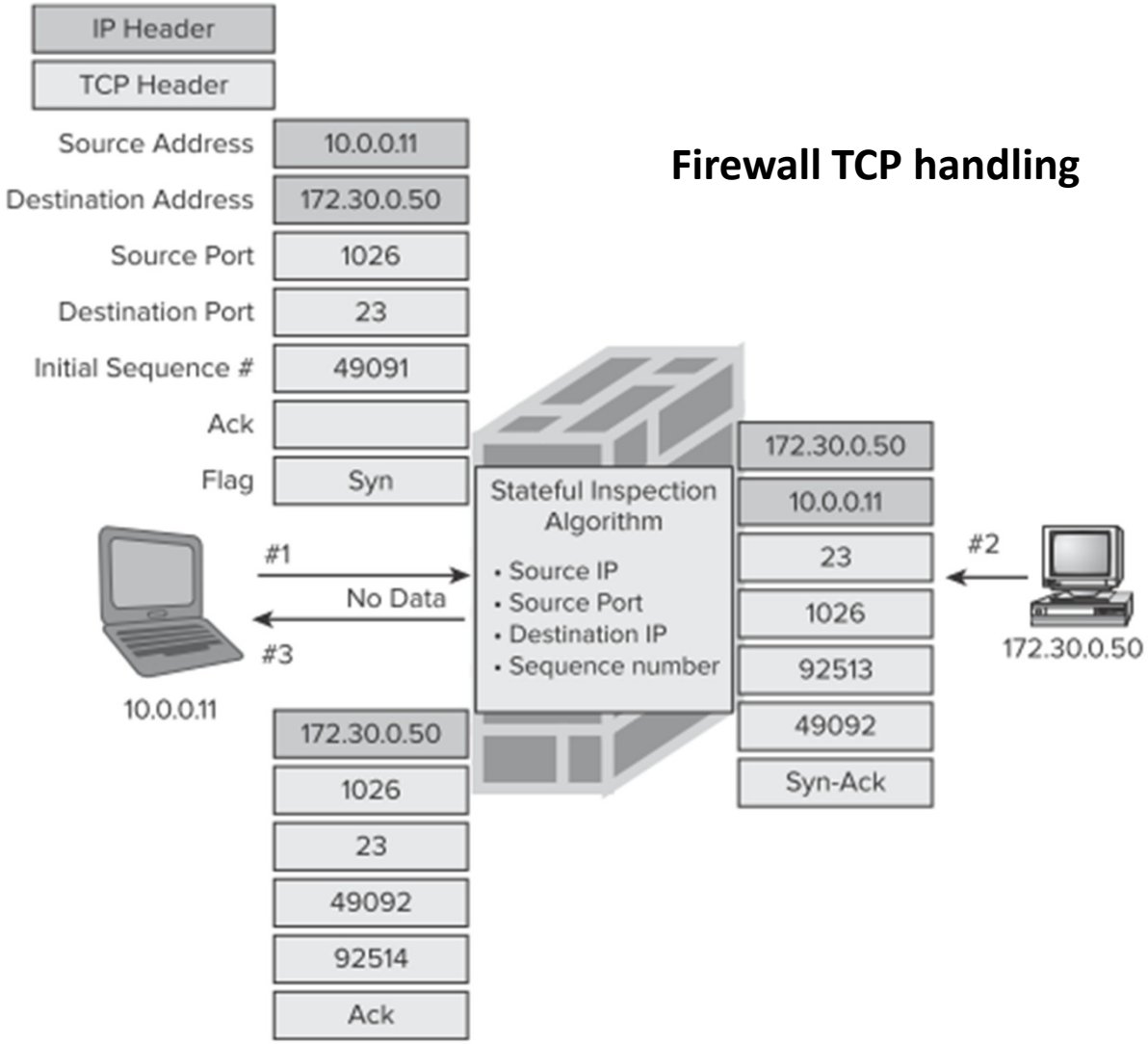
Some of the attacks

- **IP address spoofing**: where intruder transmits packets from the outside with internal host source IP addresses, need to filter & discard such packets
- **Source routing attacks**: where source specifies the route that a packet should take to bypass security measures, using IP header options SSRR (strict source and record route) and LSRR (loose source and record route). should discard all source routed packets.
- **Tiny fragment attacks**: intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into separate fragments to circumvent filtering rules needing full header info, can enforce minimum fragment size to include full header

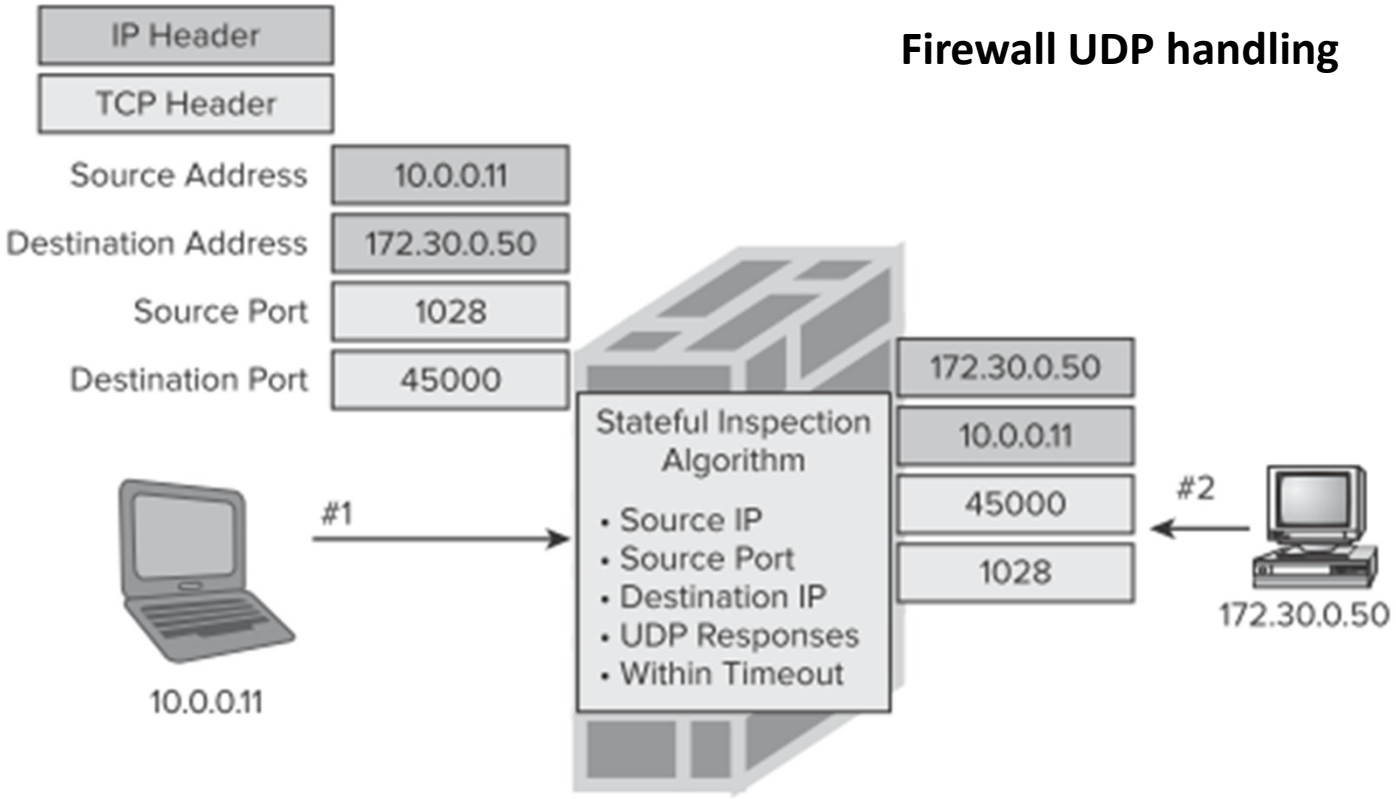
Stateful Firewalls

- **To build current connection profiles**: A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections
- **To create a directory of outbound TCP connections**
- A stateful inspection packet firewall tightens up the rules for TCP traffic by allowing incoming traffic to high-numbered ports only for those **packets** that **fit the profile** of one of the entries in directory of outbound TCP connections

Firewall TCP handling



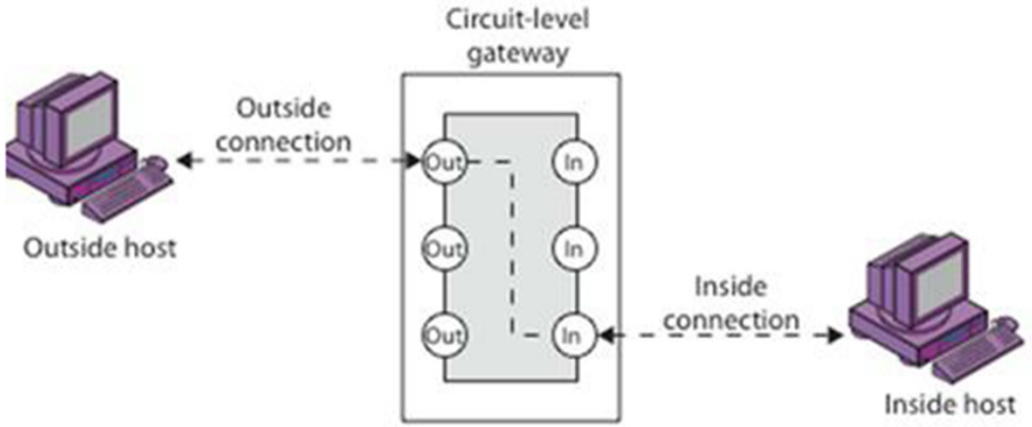
Firewall UDP handling



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	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
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	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

Circuit Level Gateway

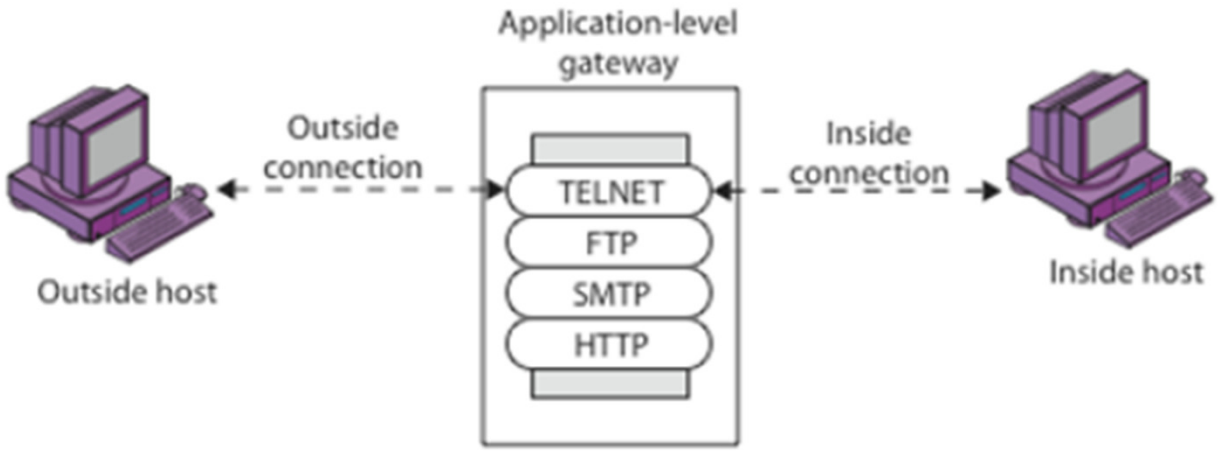
- Relays two TCP connections
- Without examining its contents
- The security function consists of determining which connections will be allowed



The most common circuit-level gateways is SOCKS, defined in RFC 1928

Application-Layer Firewalls

- Application-Layer gateway
- Proxy server
- Acts as a relay of application-level traffic
- The gateway must implement the proxy code for each of specific applications

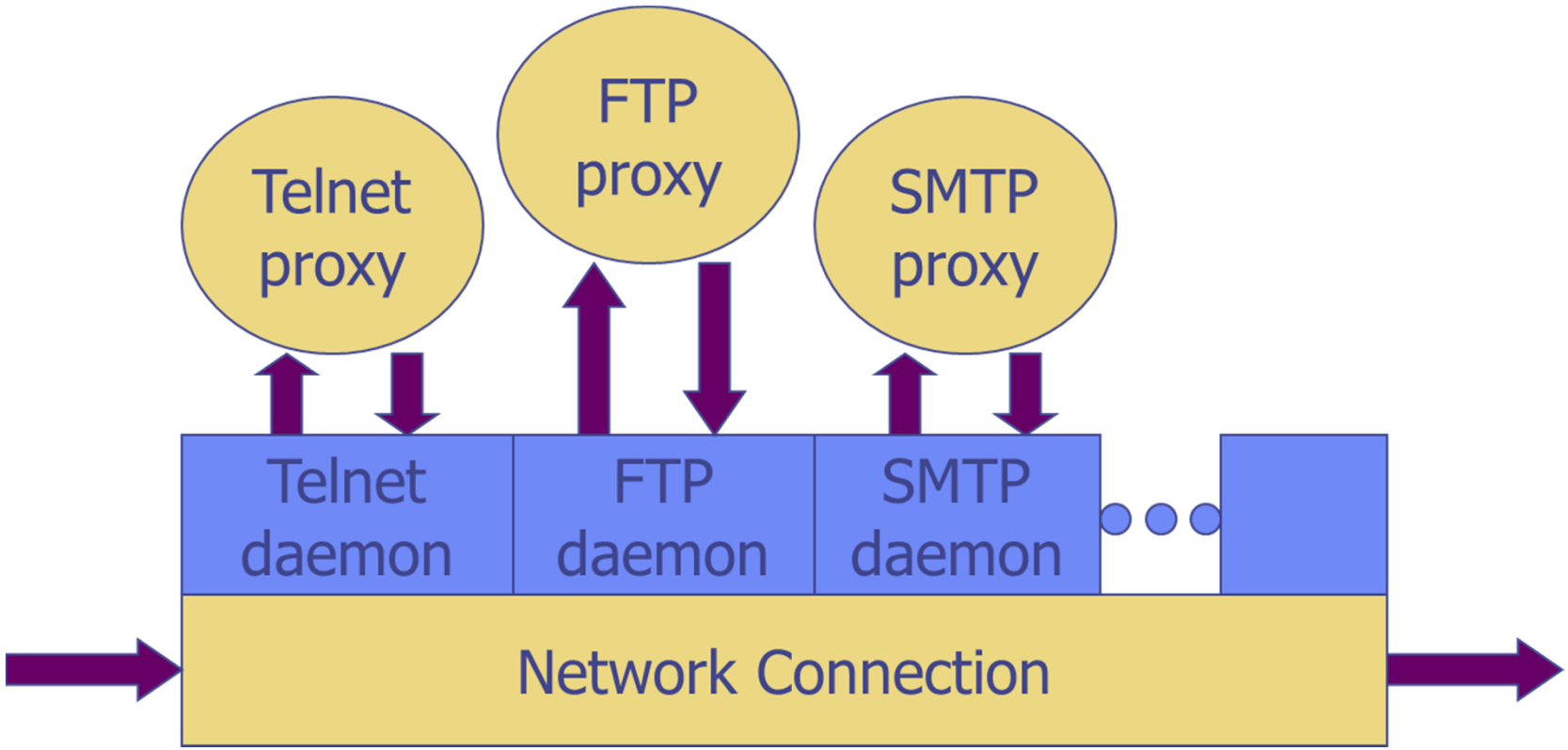


Telnet proxy

FTP proxy

HTTP proxy

.....


FTP
proxy
Telnet
proxy
SMTP
proxy
Telnet
daemon
FTP
daemon
SMTP
daemon
Network Connection

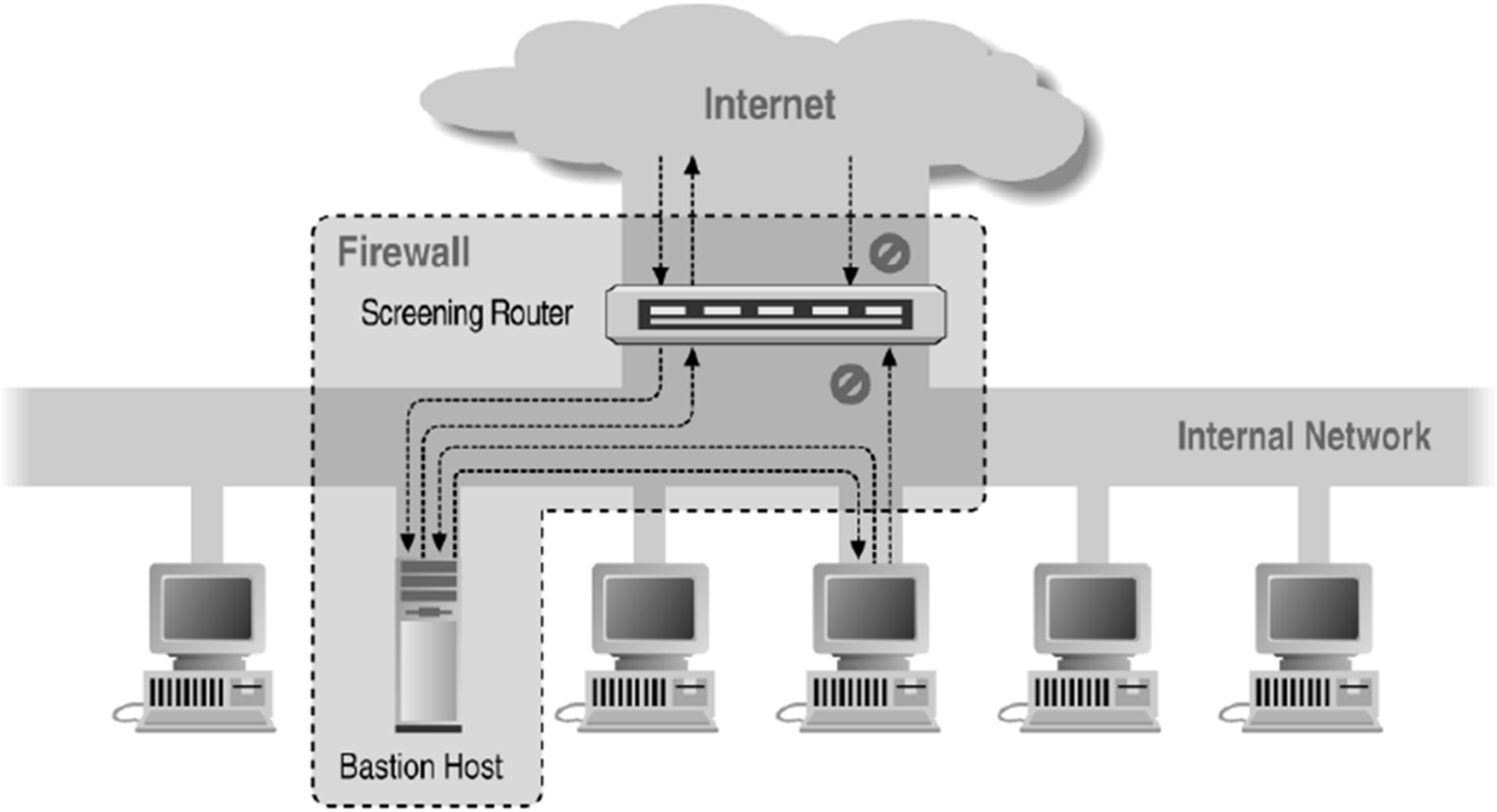
Khái niệm Bastion Host

- A critical strong point in the network's security serving as a platform for an application-level or circuit-level gateway, or for external services
- A bastion host may have two or more network interfaces (or ports)

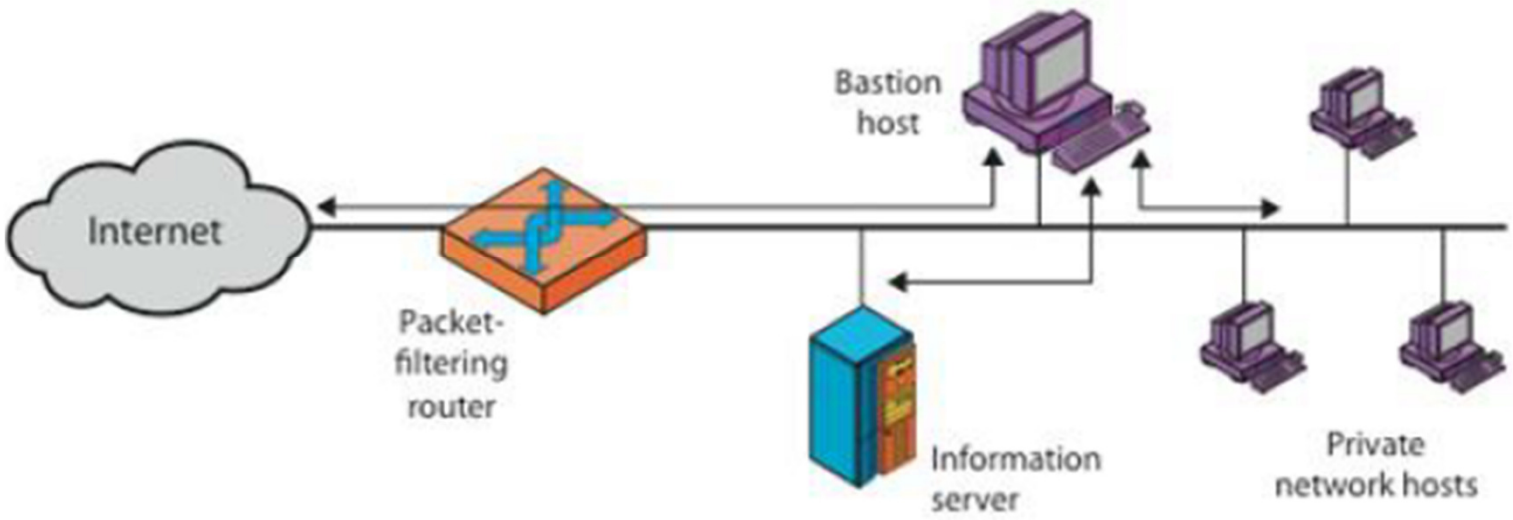
Firewall Configurations

- Screened host firewall, single-homed bastion configuration
- Screened host firewall, dual-homed bastion configuration
- Screened subnet firewall configuration

Screened Host Architecture

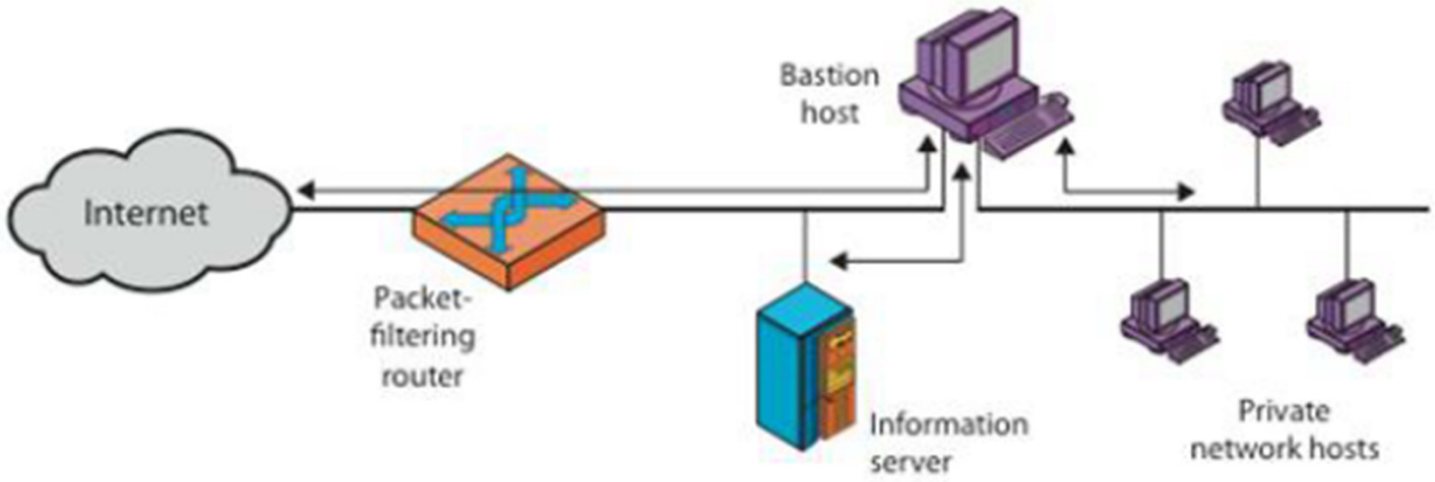


Screened host firewall, single-homed bastion configuration



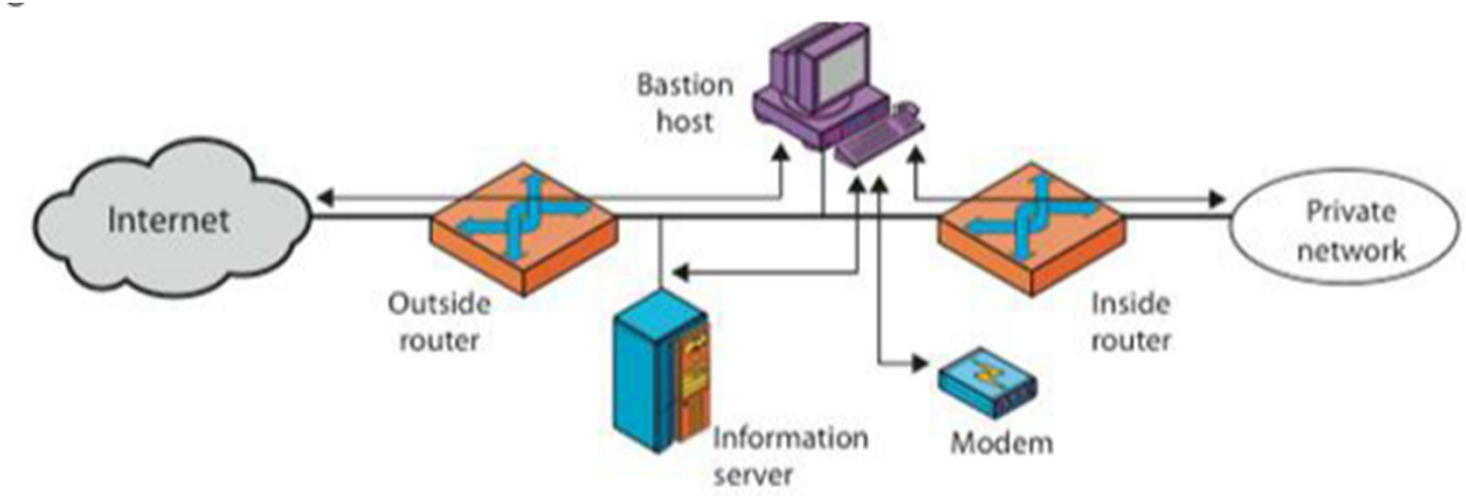
- packet-filtering router - allows Internet packets to/from bastion only
- bastion host - performs authentication and proxy functions

Screened host firewall, dual-homed bastion configuration



physically separates the external and internal networks

Screened subnet firewall configuration



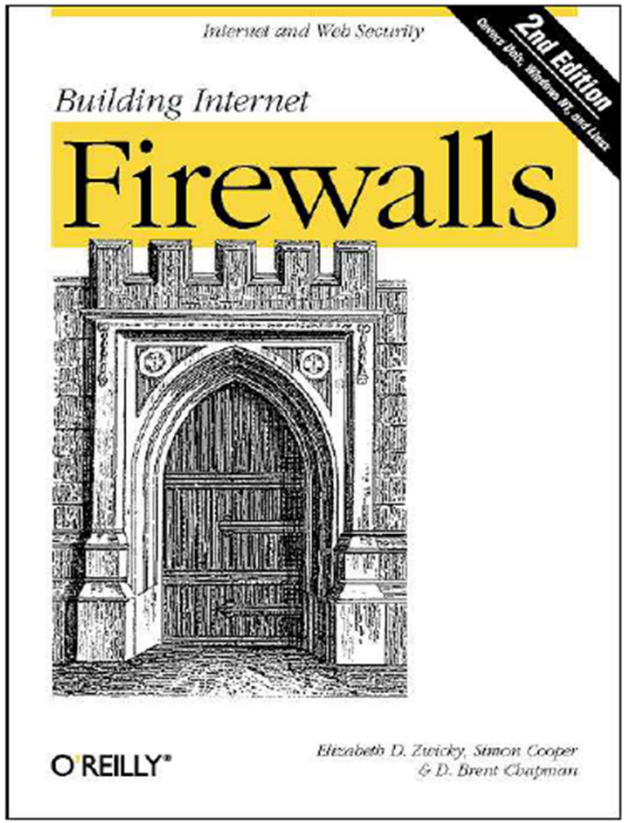
Three levels of defense

The internal network is invisible to the Internet

Systems on the inside network cannot construct direct routes to the Internet

Disadvantages ????

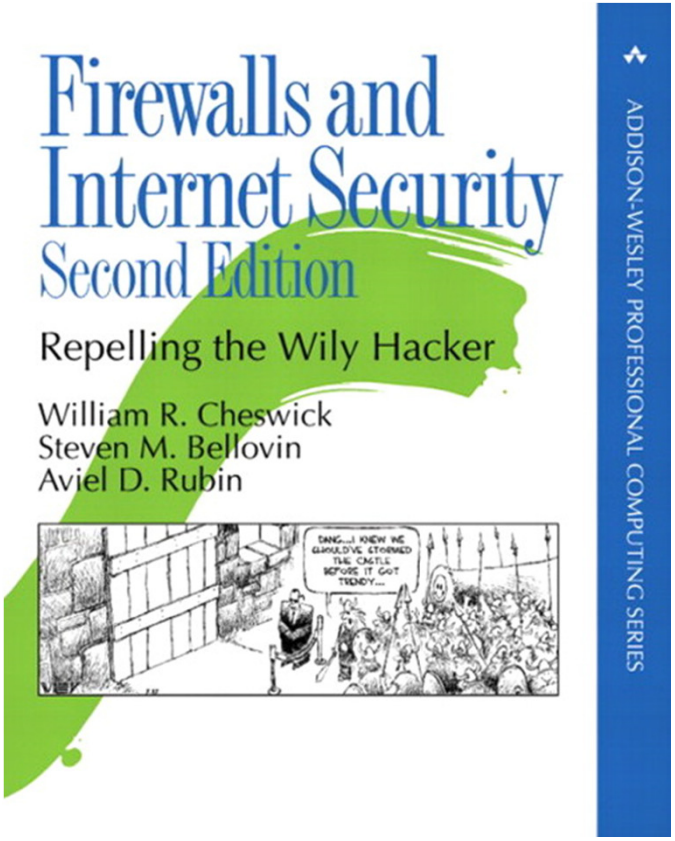
References



Elizabeth D. Zwicky

Simon Cooper

D. Brent Chapman



William R Cheswick

Steven M Bellovin

Aviel D Rubin

IDS

- Intrusion detection systems (IDSs) can be used to inspect network/host activity.
- IDSs are considered first-generation products because by design they are detective systems
- Second-generation IDSs are known as intrusion prevention systems (IPSs)
- Some vendors and other entities have actually begun using the term ‘‘intrusion detection and prevention’’ (IDP)

IDS Types: NIDS

- Network-based intrusion detection systems (NIDSs) and host-based intrusion detection systems (HIDSs)
- A NIDS makes use of a computer that has its NIC placed in promiscuous mode
- The disadvantage of a NIDS is that it will not detect attacks against a host made by an intruder who is logged in at the host's terminal

Some examples of a NIDS

- Snort (www.snort.org),
- Cisco Intrusion Detection System (http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/index/html)
- Symantec NetProwler (http://securityresponse.symantec.com/avcenter/security/Content/ Product/Product NP.html).

IDS Types: HIDS

- HIDSs only monitor traffic on one specific system
- HIDSs looks for unusual events or patterns that may indicate problems
- HIDSs can also look at the state of a system and verify that all contents appear as expected

Some examples of HIDSs

- Tripwire

  (http://sourceforge.net/projects/tripwire),
- Samhain (http://la-samhna.de/samhain),
- Swatch (http://swatch.sourceforge.net),
- RealSecure (http://www.iss.net)

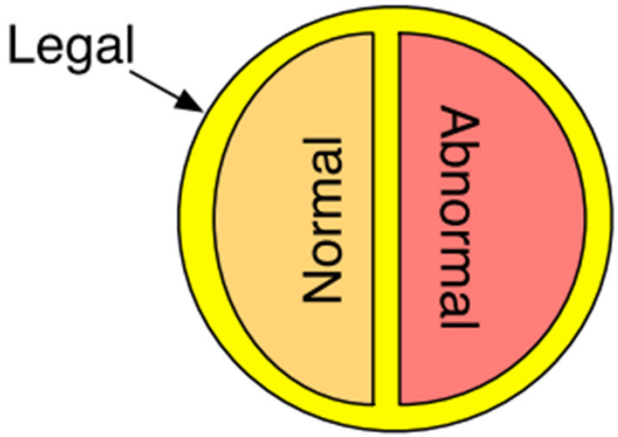
Components of IDS

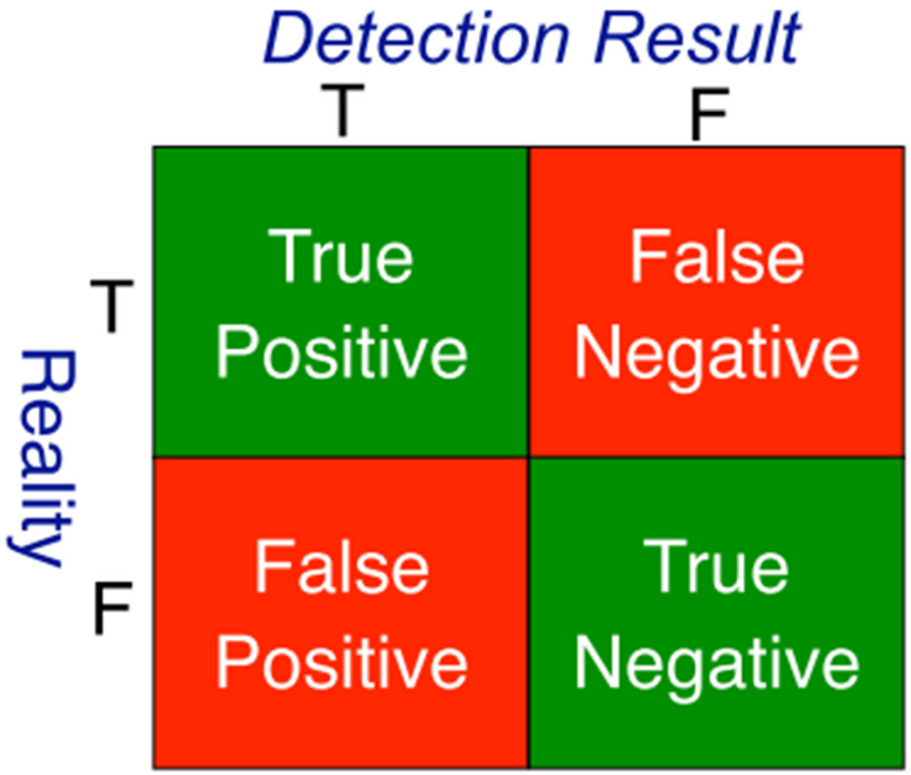
- Most IDSs consist of more than one application or hardware device. IDSs are composed of the following parts:
  - **Network sensors** : Detect and send data to the system
  - **Central monitoring system** : Processes and analyzes data sent from sensors
  - **Report analysis** : Offers information about how to counteract a specific event
  - **Database and storage components** : Perform trend analysis and store the IP address and information about the attacker
  - **Response box** : Inputs information from the previously listed components and forms an appropriate response

Requirements of IDS implement

- **The key** : where the network sensors are placed. This requires: work well at detecting problems there but will prove useless for attackers
- An IDS must be trained to look for suspicious activity
- Process of tuning: To detect true incidents, it is necessary to know how to identify them and how to distinguish them from normal activity
- Base-Rate Fallacy: the **false alarm rate** at an acceptable level

Analyzing IDS Effectiveness

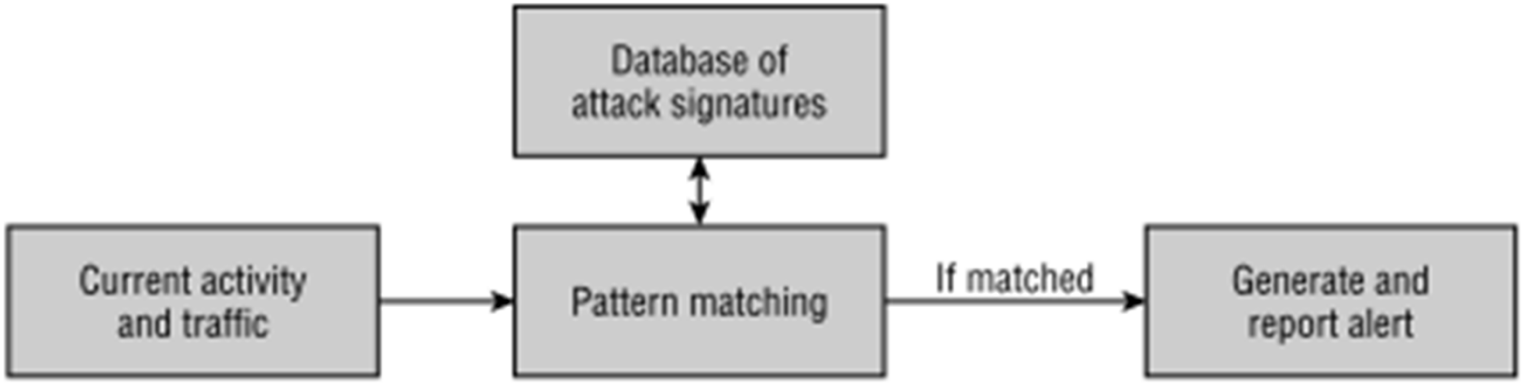




Fundamental problem: too many false alarms

IDS Engines (1/6)

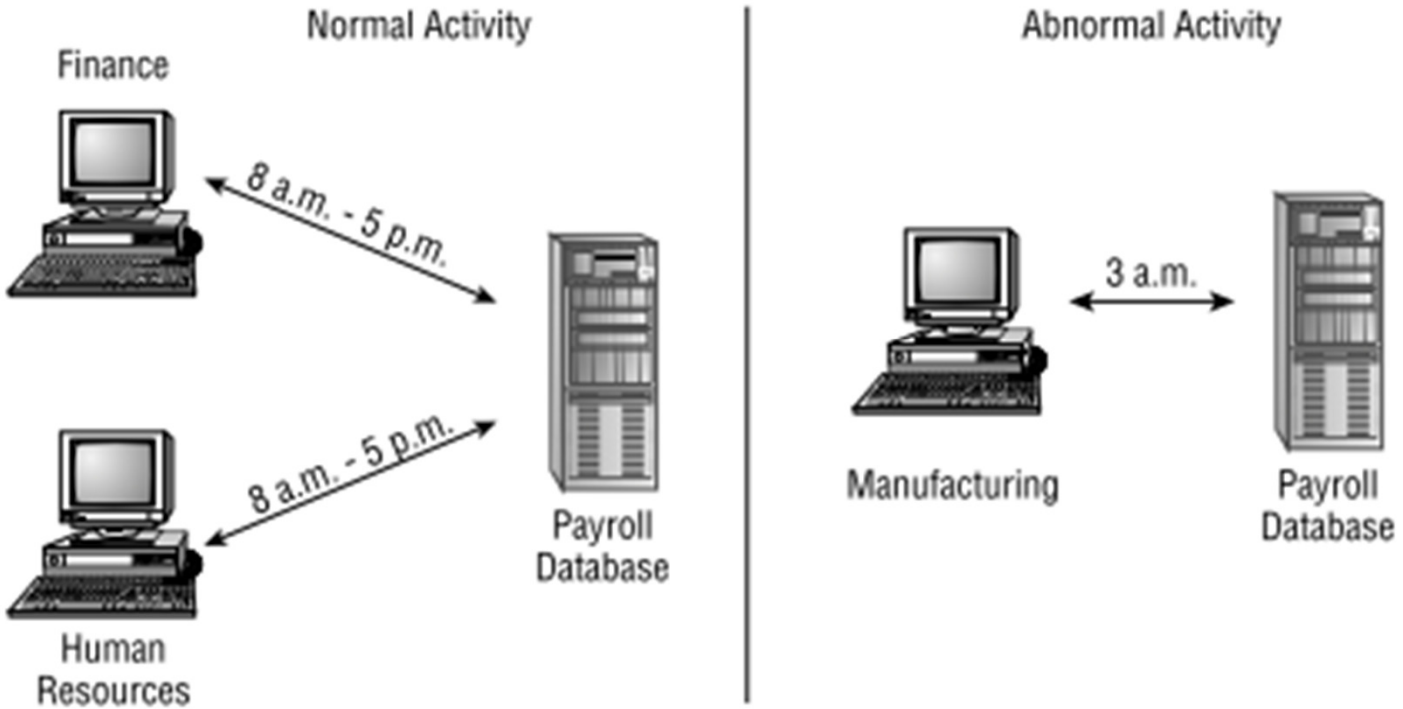
- Intrusion detection engines or techniques can be divided into two distinct types or methods:
  - Signature –based (Rule-based techniques, pattern-matching)
  - Anomaly-based (Statistical anomaly detection techniques)
  - Policy-based
- **Signature-based:** IDS relies on a database of known attacks
- Known attacks are loaded into the system as signatures



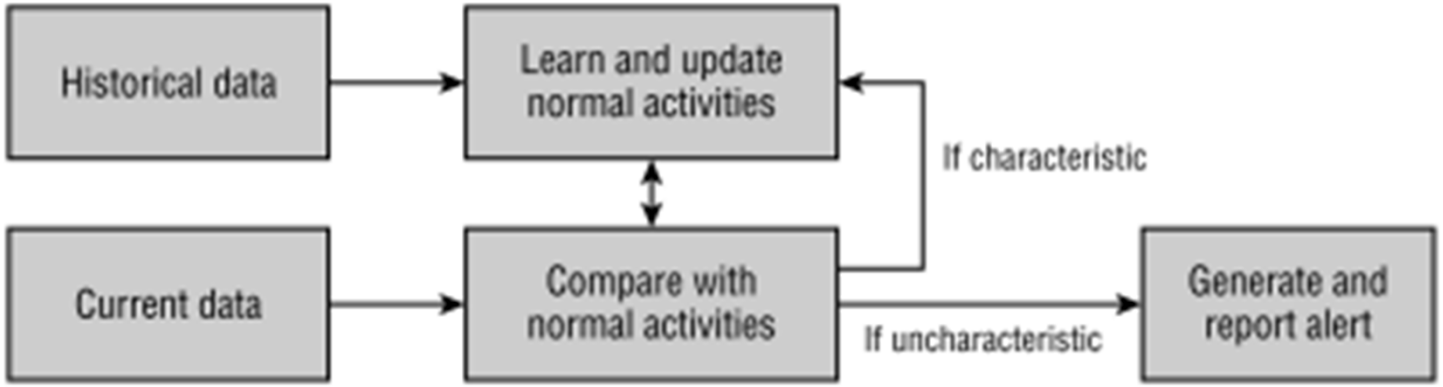
IDS Engines (2/6)

- The biggest disadvantage of signature-based systems is that they can trigger only on signatures that have been loaded. *Snort is a good example of a signature-based IDS*
- Anomaly-based IDS require the administrator to make use of **profiles** of authorized activities or place the IDS into a **learning mode** so that it can learn what constitutes normal activity

IDS Engines (3/6)



IDS Engines (4/6)



Anomaly-based IDS

- Foundation of this approach is analysis of audit records
- Metrics that are useful for profile-based intrusion detection are: counter, gauge, interval timer, resource use
- Various tests can be performed to determine whether current activity fits within acceptable limits, such as: Mean and standard deviation, Multivariate, Markov process, Time series, Operational.

IDS Engines (5/6)

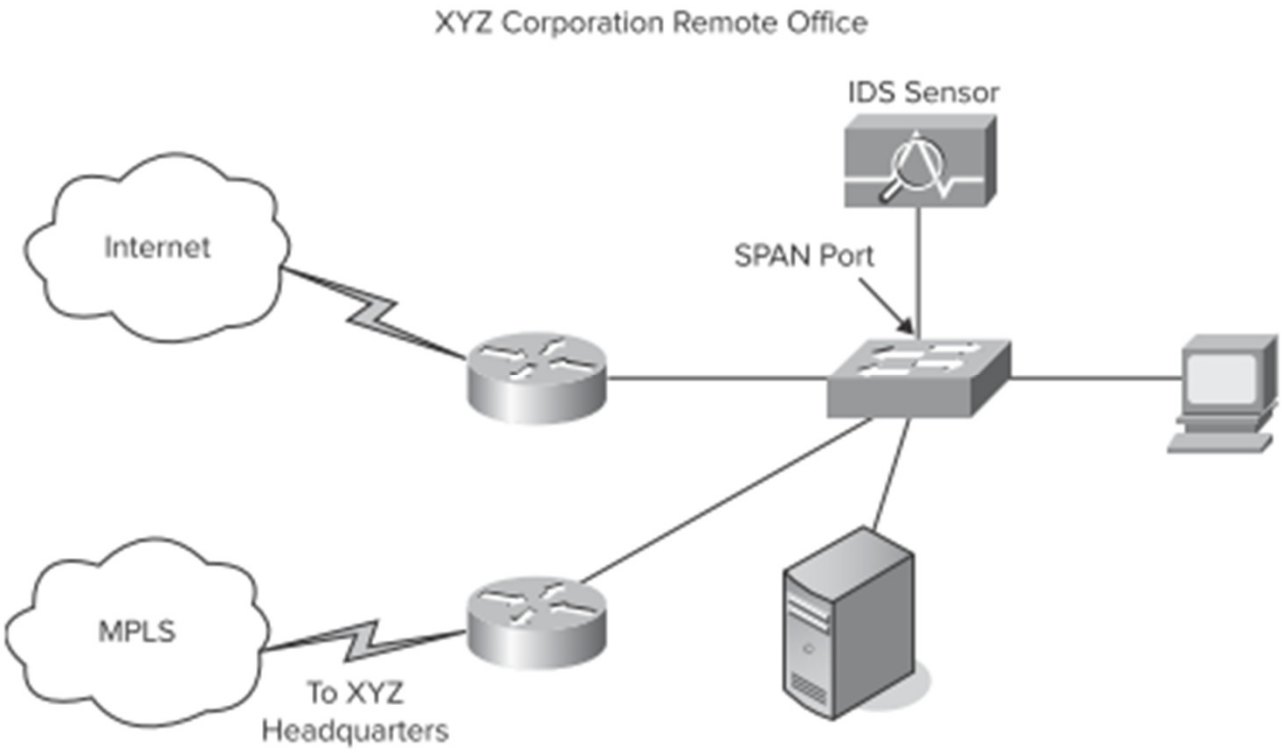
- One of the most unique features of an IDS is the capability to decode packets (‘‘deep packet inspection’)
- If the IDS knows the normal activity of the protocol, it can pick out abnormal activity.
- *Protocol-decoding* intrusion detection requires the IDS to maintain state information

IDS Engines (6/6)

- A policy-based approach to intrusion detection uses an algorithm to make decisions
- A policy-based sensor has been implemented that detects a port sweep. The policy can be set to look for the presence of a unique port or set of ports that are being scanned on a particular machine.
- When a specific threshold of ports or packets probing the ports is reached, the policy sends an alarm.
- The policy could be further restricted or filtered to look for specific types of packets that are of interest

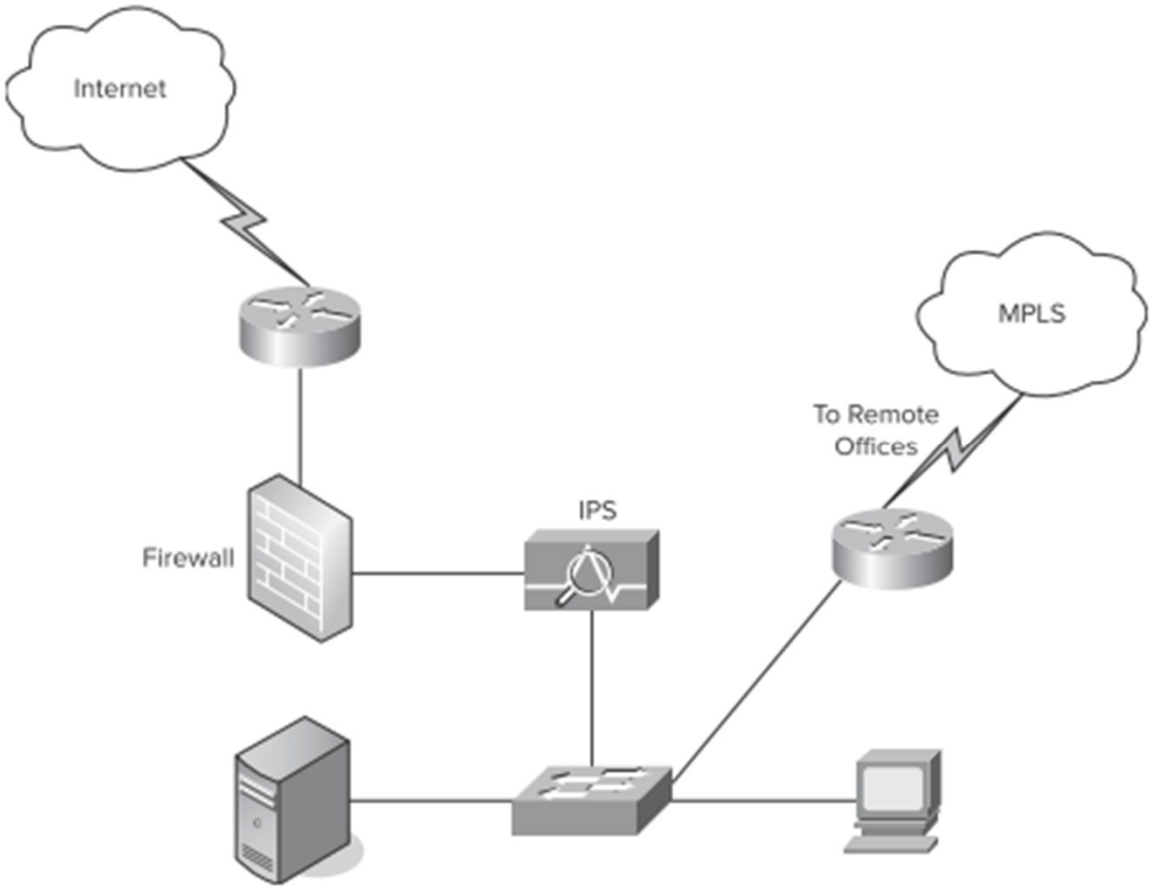
Capabilities of IDS

- Send an alert to a management station
- IDS to block malicious traffic using other network devices, but only after it has detected the traffic
- The IDS is also capable of sending a TCP reset to the end or source host and terminating any malicious TCP connections


XYZ Corporation Remote Office
IDS Sensor
Internet
SPAN Port
MPLS
To XYZ
Headquarters

IPS

- Intrusion Prevention System (IPS) is implemented as an inline sensor and can take action based on the alert type, requires the use of more than one physical interface or the use of virtual interfaces, and all network traffic must pass through the sensor. Network traffic enters through one interface and exits through another.
- When an IPS detects malicious traffic, it can send an alert to the management station, just like an IDS. But, more importantly, it can immediately block the malicious traffic.
- You can configure the IPS to perform other actions, as appropriate for a given threat.


Internet
MPLS
To Remote
Offices
IPS
Firewall

Capabilities of IPS

- **Send an alarm**: send an alarm to a syslog server or a centralized management interface. This action is typically combined with other preventive actions.
- **Drop the packet** : This action is effective for all Internet protocols and prevents malicious packets from reaching the intended target.
- **Reset the connection** : sending a TCP reset to the end or source host and terminating any malicious TCP connections.
- **Block traffic** : block traffic from the source IP address of the attacker or block traffic on a connection for which an attack signature was seen.

Signature Microengine

- The actual process within an IPS sensor that matches traffic to a signature is called a microengine or a signature microengine
- A signature microengine is a kind of preprocessor that handles specific groups of signatures.
- A sensor has multiple microengines; each of the microengines is responsible for a group of signatures.
- The signatures are grouped by protocol or other similar characteristics.

Signature Types

- **Exploit signatures:** Exploit signatures typically identify a traffic pattern unique to a specific exploit..
- **Connection signatures:** Connection signatures generate an alarm based on conformity to and validity of the network connections and protocols.
- **String signatures:** The string signature engines support regular expression pattern matching and alarm functionality.
- **DoS signatures:** DoS signatures contain behavior descriptions that are considered characteristic of a DoS attack.

How traffic is scanned by the sensor

1. Traffic passes through the sensor.

2. The sensor decides which microengine to activate, so the traffic can be scanned with the right signatures to determine whether the traffic is malicious.

3. The sensor activates one or more sensor microengines.

4. Once activated, the microengine inspects the data.

How traffic is scanned by the sensor

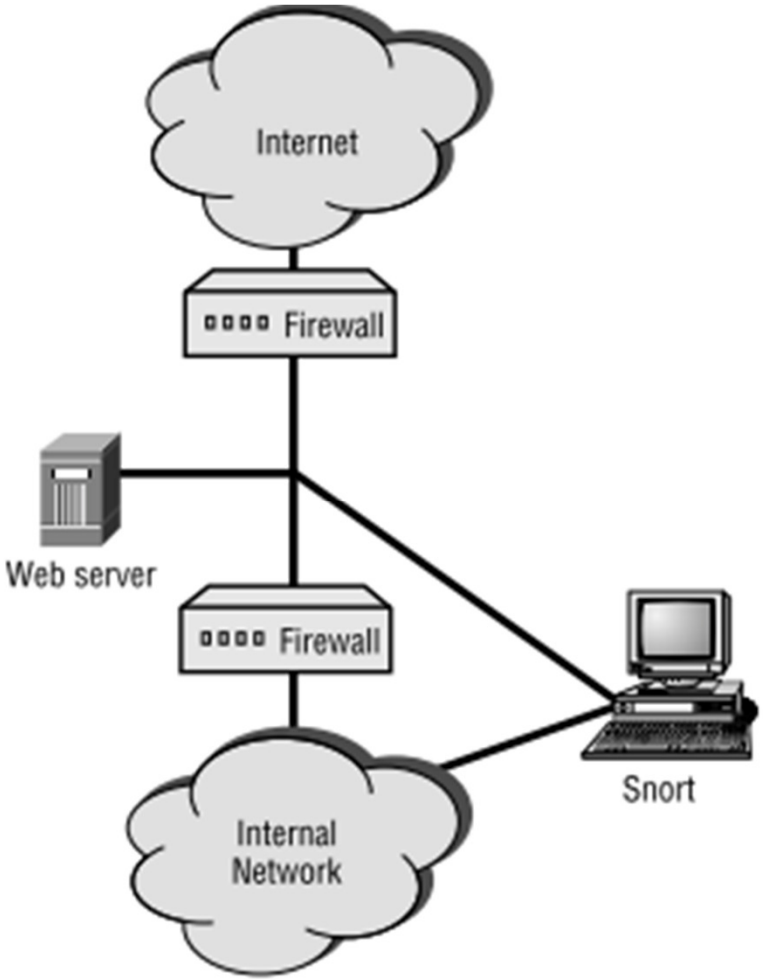
- The sensor bases its microengine selection on the following:
  - The network protocol of the traversing traffic
  - The type of operating system associated with a signature
  - The session port
  - The type of attack

Signature Files

- The signatures that an IPS sensor uses are loaded into the system with a signature definition file (SDF)
- The SDFs can be downloaded from website (example www.cisco.com)

An Overview of Snort

- Snort is a freeware IDS developed by Martin Roesch and Brian Caswell. It's considered a NIDS that can be set up on a Linux or Windows host
- Popular GUIs can be used: SnortSnarf and IDScenter
- Snort operates as a network sniffer and logs activity that matches predefined signatures. Signatures can be designed for a wide range of traffic, including IP, TCP, UDP, and ICMP
- Having at least two NICs for your Snort system. One NIC can be used for remotely managing the system, while the second NIC can be used for sniffing traffic.


Internet
Firewall
Web server
Firewall
Snort
Internal
Network

Difficulties in intrusion detection

- Lack of training data
  - Lots of “normal” network, system call data
  - Little data containing realistic attacks, anomalies
- Data drift
  - Statistical methods detect changes in behavior
  - Attacker can attack gradually and incrementally
- Main characteristics not well understood
  - By many measures, attack may be within bounds of “normal” range of activities
- False identifications are very costly
  - Sys Admin spend many hours examining evidence

The End