Firewall, WAF, IDS/IPS, NIDS/NIPS, Firewalking

Corso Di Sicurezza delle Reti e dei Sistemi Software aa 2016/17

Ing. Antonio Pirozzi


LOOK, ALL I'M SAYING IS
WE NEED TO BUILD A BIGGER FIREWALL
imgflip.com

Intrusion Detection Systems

- An IDS is used to Monitor and Protect Networks or System for malicious activities or policy violations. Any malicious activity is immediately reported to (system/network) administrator and collected centrally using a **security information and event management** (**SIEM**) system.
- Main purposes:
  - Report intrusion or anomalies to the Administrator, when the attack is still going on
  - Prevent Intrusion (IPS)
  - The software scans all packets on the network and attempts to classify the traffic as intrusive or non intrusive.
- **Analyzed activity**
  - **Network intrusion detection systems NIDS**
  - **Host intrusion detection systems HIDS**
- **Detection Method:**
  - **Signature-based**
  - **Anomaly-based**

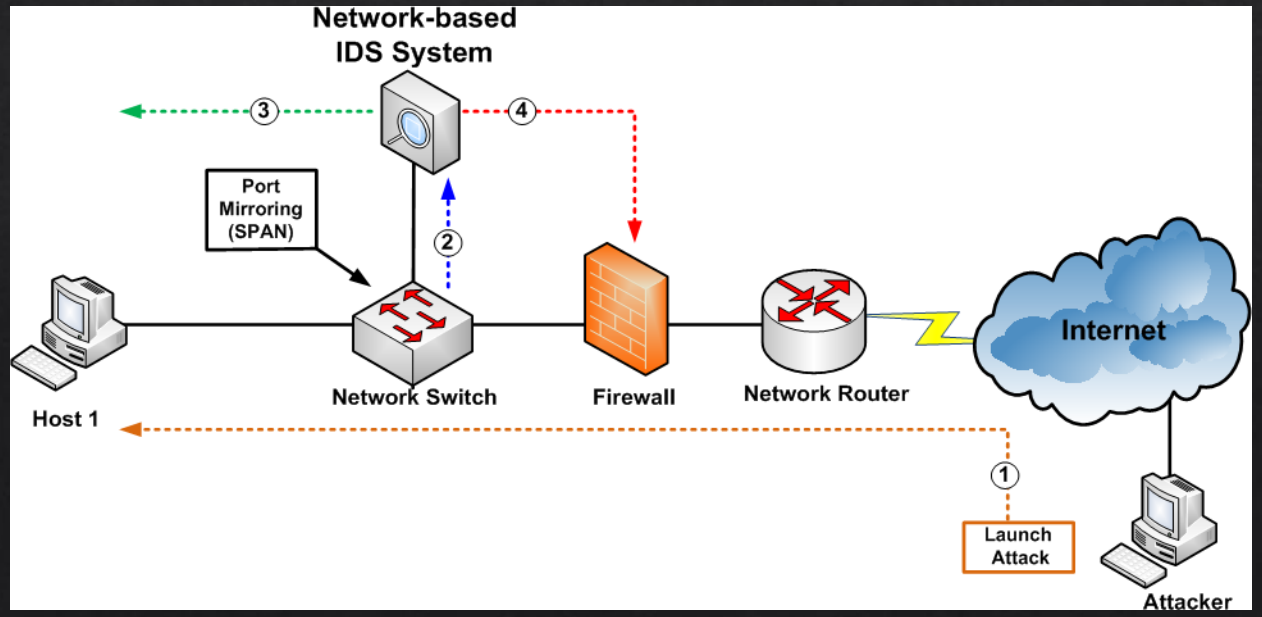
IDS is not a solution to all security concerns

Intrusion Detection Systems

- Network Intrusion Detection System (Snort, Suricata, Bro)

  Analyze the Flow of information between computers (networks), at the router and host level

  A black box that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion.



- Sniffing

  Collect and inspect incoming traffic

- Protocol Awerness

  Protocol reassembly and normalization

- Alerting

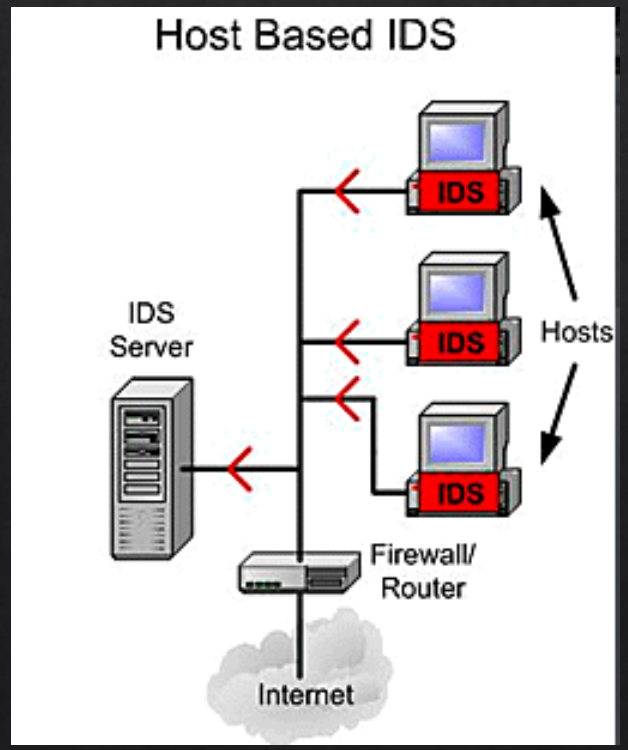
  Send mail, log event, SNMP

https://www.hackthis.co.uk/articles/basics-of-intrusion-detection-systems

Intrusion Detection Systems

- Host-based Intrusion Detection (OSSEC, Tripwire)

  The HIDS can be installed on any system ranging from a desktop PC to a server



- HIDS scans the operating system log files, application log files, or DBMS log files for activity traces
- detecting unauthorized insider activity, host-based systems
- detecting unauthorized file modification.
- focused on changing aspects of the local systems

https://www.hackthis.co.uk/articles/basics-of-intrusion-detection-systems

Intrusion Detection Systems

- **HIDS vs NIDS**

- **additional layer of protection:** in a multi-tiered security architecture, HIDS can provide another layer of security by detecting attacks missed by other security tools in the architecture
- **Direct control over System Entities :** Since HIDS work at the host level, they are more control and command over the system entities like memory, registry, system files etc
- Network based IDS sensors can detect many attacks by checking the packet headers for any malicious attack like TCP SYN attack, fragmented packet attack etc
- you can also use it to find violations of network policy. IDS will tell you an employee was using Gtalk, uploading to Box, or spending all their time watching Hulu instead of working

Intrusion Detection Systems

Modes of Detection

- **Signature-based**
- Compare Data-Packets against known malicious sequence
  - Binary signatures: such as TCP flags
  - Signature recognition can detect known attacks
  - Signatures are easy to develop and understand if you know what network behavior you're trying to identify
  - pattern matching can be performed very quickly on modern systems
  - they only detect known attacks
  - a signature must be created for every attack, and novel attacks cannot be detected
  - Signature engines are are commonly based on regular expressions and string matching. PRONE TO FP!
  - delta is the speed at which new signatures can be written and applied to the IDS engine

Intrusion Detection Systems

Modes of Detection NIDS

- **Anomaly-based**
  - Based on the concept of a **Baseline** for network behaviour
  - For every protocol that is being monitored, the engine must possess the ability to decode and process the protocol in order to understand its goal and the payload
  - protocol "dissection" is initially computationally expensive
  - A disadvantage of anomaly-detection engines is the difficultly of defining rules
  - On the other hand, once a protocol has been built and a behavior defined, the engine can scale more quickly and easily than the signature-based model
  - Another pitfall of anomaly detection is that malicious activity that falls within normal usage patterns is not detected
  - directory traversal on a targeted vulnerable server, which complies with network protocol, easily goes unnoticed since it does not trigger any out-of-protocol, payload or bandwidth limitation flags.
  - With anomaly-based IDS, the payload of the traffic is far less important than the activity that generated it.

IDS/IPS

IDS	IPS
Detection mode only	Active Traffic Control
Traffic replication required	Original traffic
Detection only	Detection and reaction support

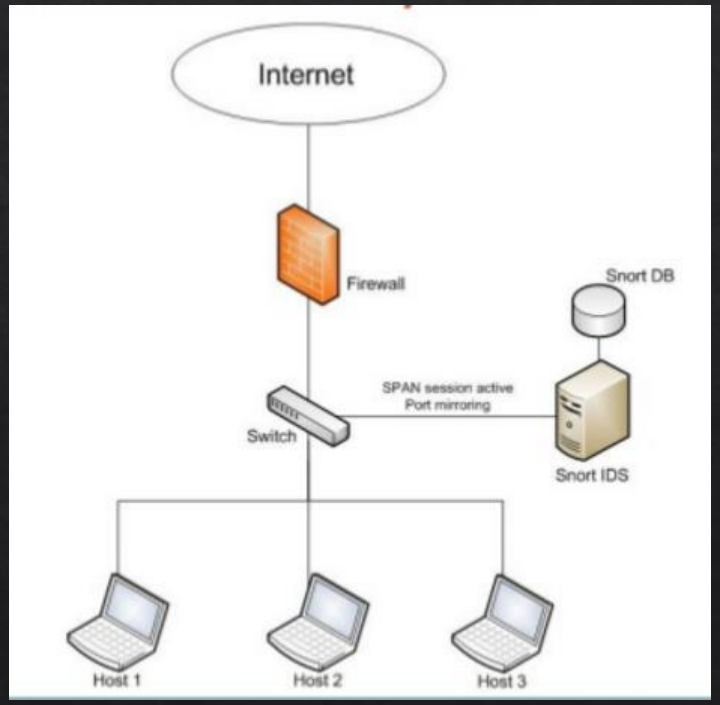
Snort

- Snort is the hands-down leader in open source NIDS solutions
- Snort uses both signature-based intrusion detection as well as anomaly-based methods, and can rely on user-created rules or signatures sourced from databases like Emerging Threats
- Detection and Prevention modes
- Traffic replication for “Detection Only”

Snort

Snort Deployments:

Intrusion Detection (Port Mirroring) passive



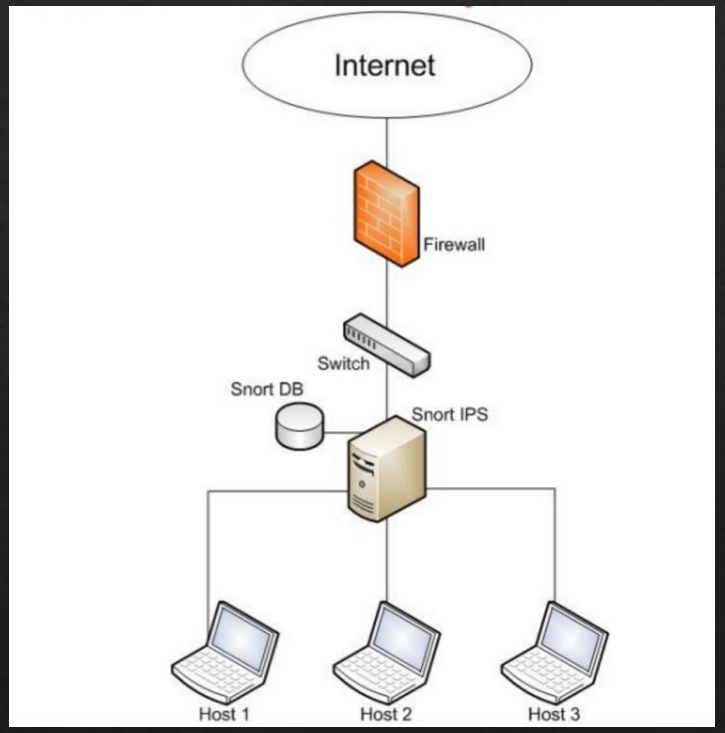
You must mirror the traffic of a switch port or VLAN.
For this, we will use the "port mirroring" mechanism which means the switch duplicates the traffic on your chosen interface or VLAN and send it to Snort.
On Cisco Catalyst, this is a “SPAN” port
You can SPAN one port to another, a group of ports to one port, or an entire VLAN to a port

http://www.slideshare.net/SimoneTino/snort-ips

Snort

Snort Deployments:

In-line mode IPS



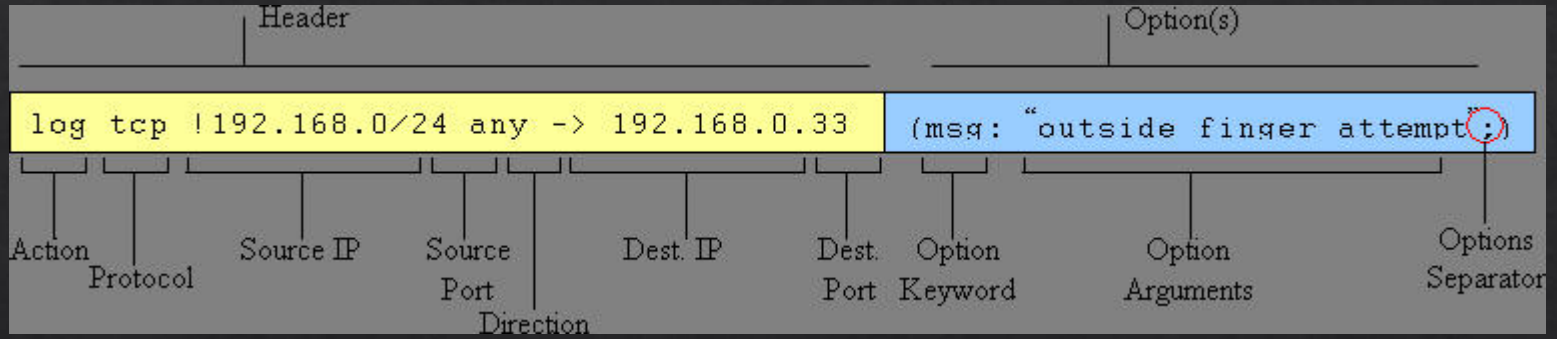
Snort in inline mode creates a transparent bridge between two network segments
Snort has two network interfaces: each on a different network segment. You will configure these interfaces without an IP address and in promiscuous mode

http://www.slideshare.net/SimoneTino/snort-ips

Snort Rules

Snort Rules

ls –l /etc/snort/rules



Rule Header

- **alert** - This the action. It can be alert, log, or pass (drop).
- **tcp** It can be tcp, udp, and icmp.
- **$EXTERNAL_NET** - This the source IP or network of the malicious packets. It can be set as a variable in the snort.conf.
- **any** - This the source port of the malicious traffic. This can set as a single port, multiple ports, or a range of ports.
- **->** - This is the direction of the traffic. In this case, we are looking for traffic moving from the EXTERNAL_NET to the internal or HOME_NET.
- **$HOME_NET** - This the destination IP address that the traffic is moving to. As with the EXTERNAL_NET, it can be set as a variable in the snort.conf.
- **any** - This the destination port. It can also contain specific ports, like 80, or a variable containing a list of ports.

Snort Rules

- Snort Rule Options
- **keyword:arguments**

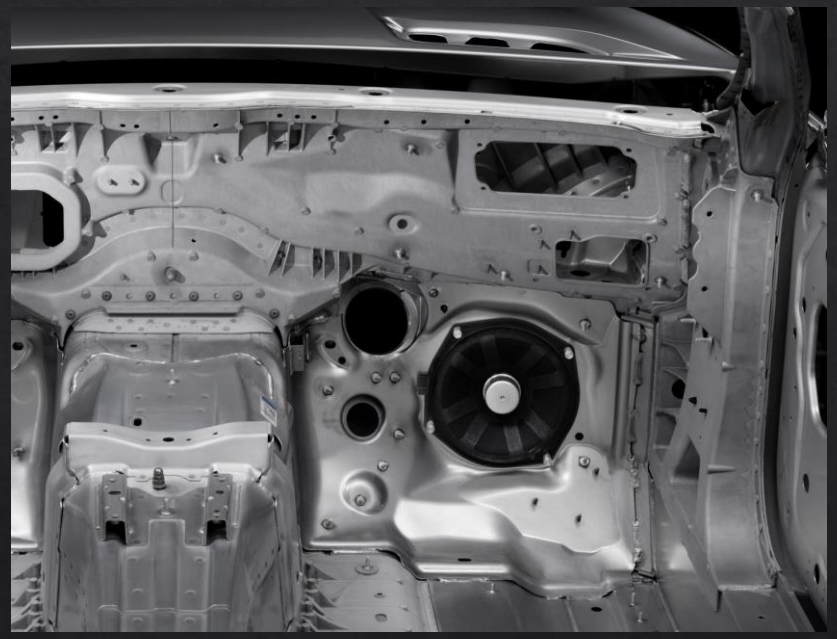
•**msg** - This is the message that's sent to the sysadmin if the rule is triggered. In this case, Snort reports to the sysadmin "SCAN SYN FIN".
•**flow** - This option allows the rule to check the flow of the traffic. It can have a number of values including established (TCP established), not established (no TCP connection established), stateless (either established or not established), etc. In our example, the rule is triggered on traffic with or without an established TCP connection.
•**flags** - This couplet checks for TCP flags. As you know, TCP flags can be SYN, FIN, PSH, URG, RST, or ACK. This rule is looking for traffic that has both the SYN and FIN flags set (SF) and in addition, has the two reserved bits in the flags byte set (12).
•**reference** - This section is for referencing a security database for more information on the attack. In our example, we can find more info on this attack in the arachnids database, attack 198.
•**classtype** - All the rules are classified into numerous categories to help the admin understand what type of attack has been attempted. In our example, we can see that it is classified as an "attempted-recon".

Snort evasion

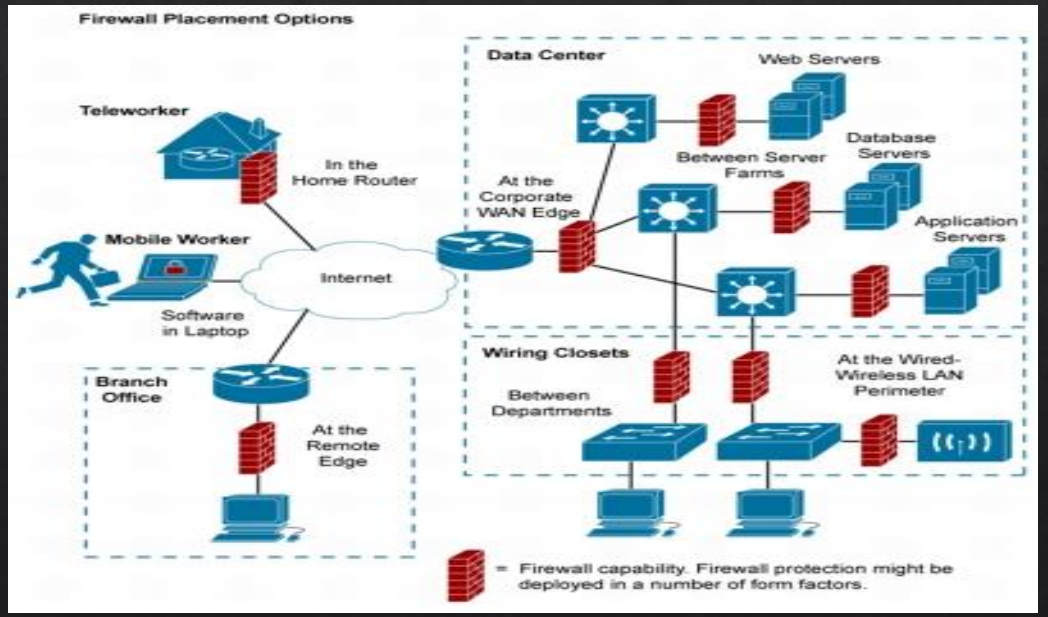
- Most of the methods of evading signature-based IDS systems rely on disguising the attack in a way that doesn't match the standard signature
- Snort has several preprocessors that will help normalize the traffic
- **stream4 preprocessor**: If the attacker is using multiple small packets to disguise the attack
- **frag2 preprocessor:** If the attacker is attempting to disguise the attack by breaking a packet up into small fragments.
- **arpspoof preprocessor**: If the attacker is attempting to use arpspoofing to gain access
- **http_inspect preprocessor:** If the attacker is attempting to use an alternative method of writing a path (*/etc/passwd* or */home/simon/../../etc/passwd*, for example), use the
- Snot, Sneeze, fragroute

Firewalls

- In automotive engineering:



In the Real Word:



Firewalls

- A firewall is a set of related programs located at the network gateway server that protects the resources of a private network from users on other networks. Firewalls are a set of tools that monitor the flow of traffic between networks CEHv8
- A firewall is an intrusion detection mechanism.
- The firewall verifies the incoming and outgoing traffic against firewall rules
- All the attempts to log in to the network are identified for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to login
- Firewalls can filter packets based on address and types of traffic.

Firewall policies

- What Internet usage is not allowed?
- What will be done with the logs?
- Will we cooperate with law enforcement?
- Internal security policy

:D

Poorly Configured fw

Firewalls architectures

- Bastion Host
  - Bastion host is a computer system designed and configured to protect network resources from attack
  - Traffic entering or leaving the network passes through the firewall, it has two interfaces:
    - **public interface** directly connected to the Internet
    - **private interface** connected to the Intranet
  - The bastion host is designed for the purpose of defending against attacks. It acts as a mediator between inside and outside networks

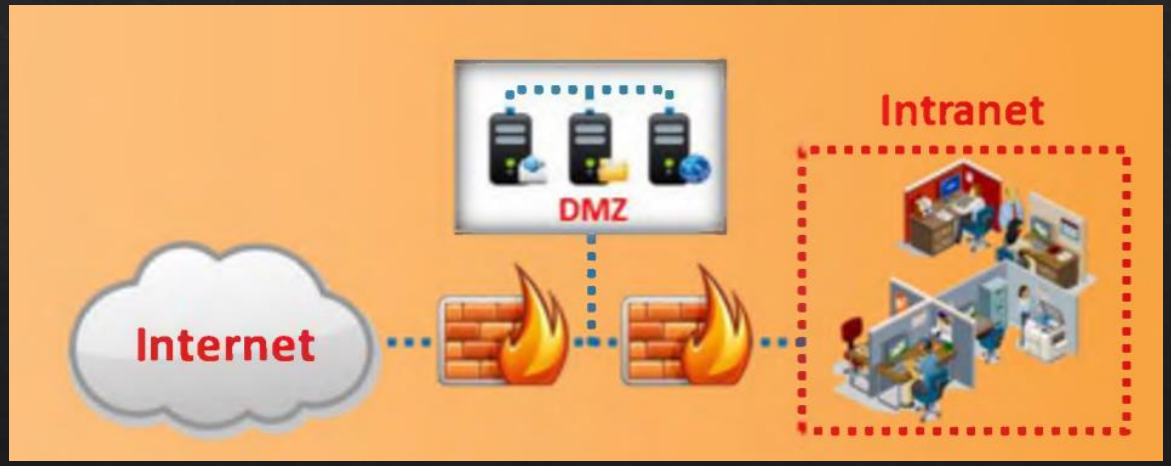
Firewalls architectures

- Screened subnet
  - Network architecture that use a single firewall with three interfaces:
    1. One to connect to internet
    2. Used to connect to DMZ
    3. Used to connect to intranet

The main advantage with the screened subnet is it separates the DMZ and Internet from the intranet so that when the firewall is compromised access to the intranet won't be possible.

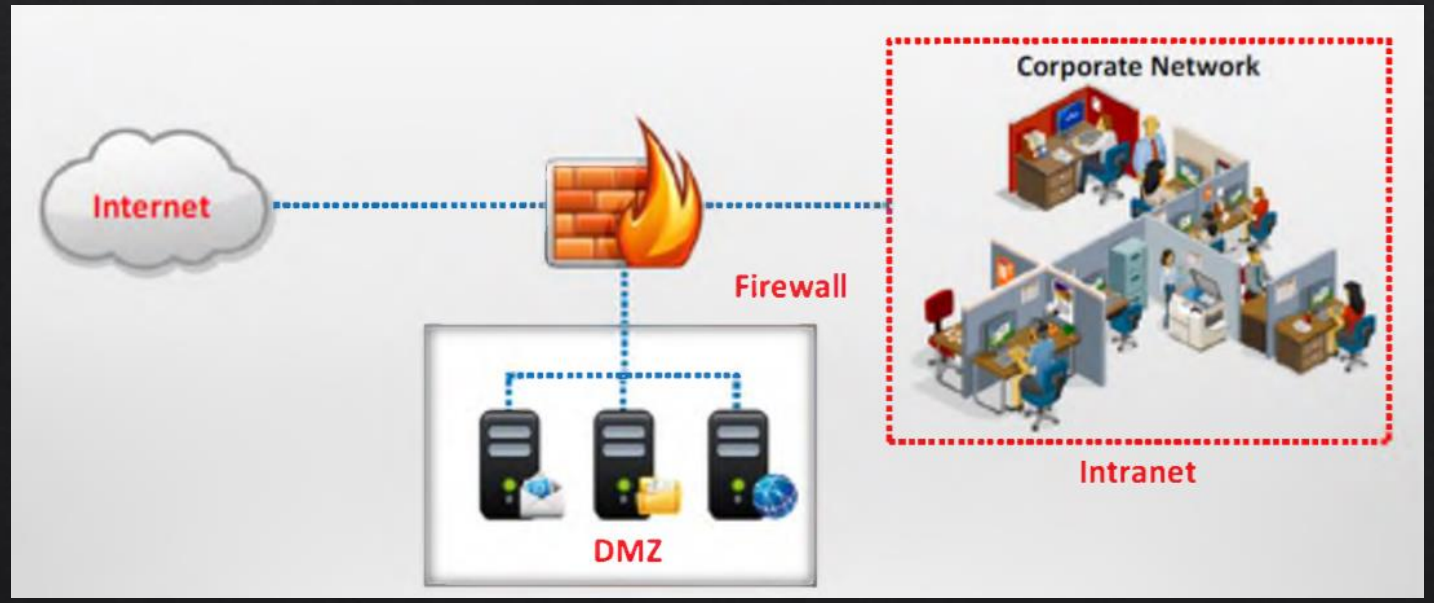
Firewalls architectures

- Multi-homed firewall
  - Refers to 2 are more network, ieach iface is connected to a separate network segment
  - A multi-homed firewall is used to increase efficiency and reliability of an IP network



De-Militarized Zone: DMZ

- Is a Network that serve as a buffer between internal intranet and (untrusted) external internet
- It is created using a firewall with 3 or more network iface
- n external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.



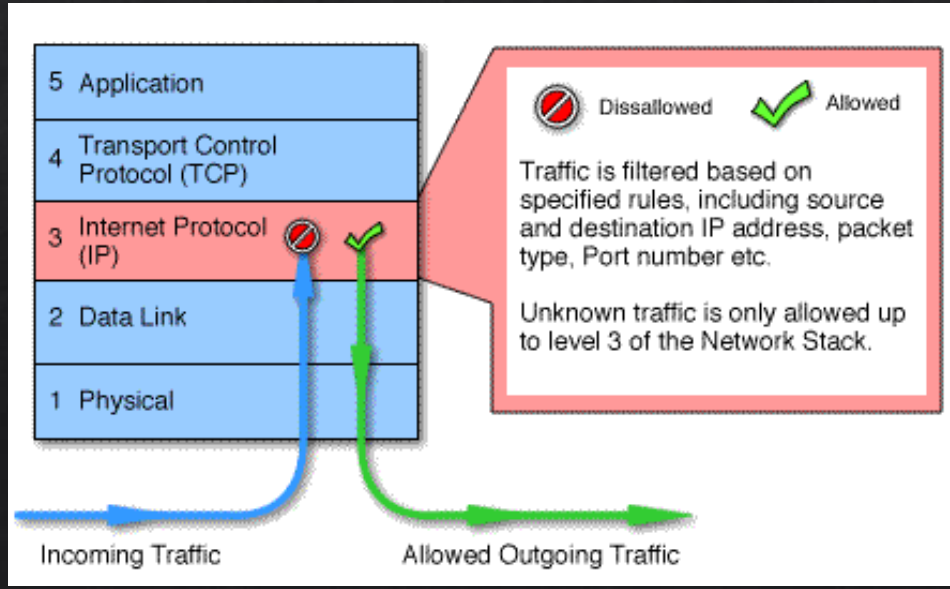
The most common of these services are:
• web server
• ftp server
•Mail server

Types of Firewalls

- Packet Filters
- Circuit-level gateways
- Application-level gateways
- Stateful multilayer inspection firewall

Types of Firewalls

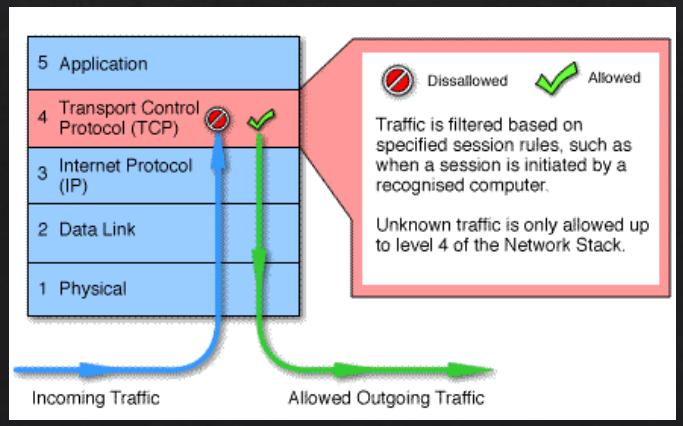
- Packet Filters
  - Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP
  - Inspect each packet passing through it and make a decision based on header information.
  - Packet filter firewall make a decision based on the following:
    - Source IP addr
    - Destination IP addr
    - Source TCP/UDP port
    - Destination TPC/UDP port
    - TCP code bits
    - Protocol in use
    - Direction
    - interface



http://randy94112.tripod.com/types.htm

Types of Firewalls

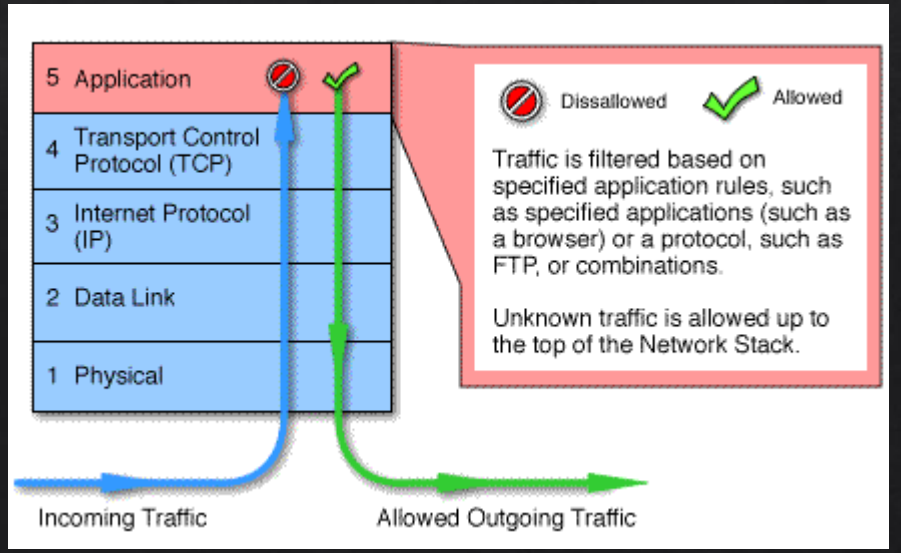
- Circuit-level gateway
  - Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
    - Circuit-level gateways do not filter individual packets.
    - Circuit-level gateways are relatively inexpensive and hide the information about the private network that they protect
    - They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
    - Information passed to remote computer through a circuit level gateway appears to have originated from the gateway



http://randy94112.tripod.com/types.htm

Types of Firewalls

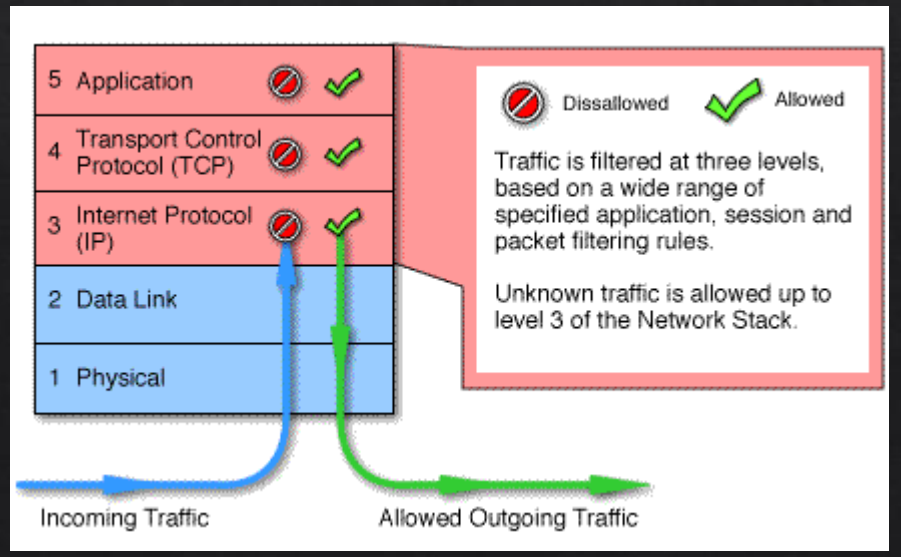
- Application-level gateway (Proxy)
  - Application-specific
  - They can filter packets at the application layer of the OSI model
  - Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc. This cannot be accomplished with either packet filtering firewalls or circuit level



http://randy94112.tripod.com/types.htm

Types of Firewalls

- Stateful multilayer inspection firewall
  - Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls.
  - They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer
  - Stateful multilayer inspection firewalls offer a high level of security, good performance and transparency to end users

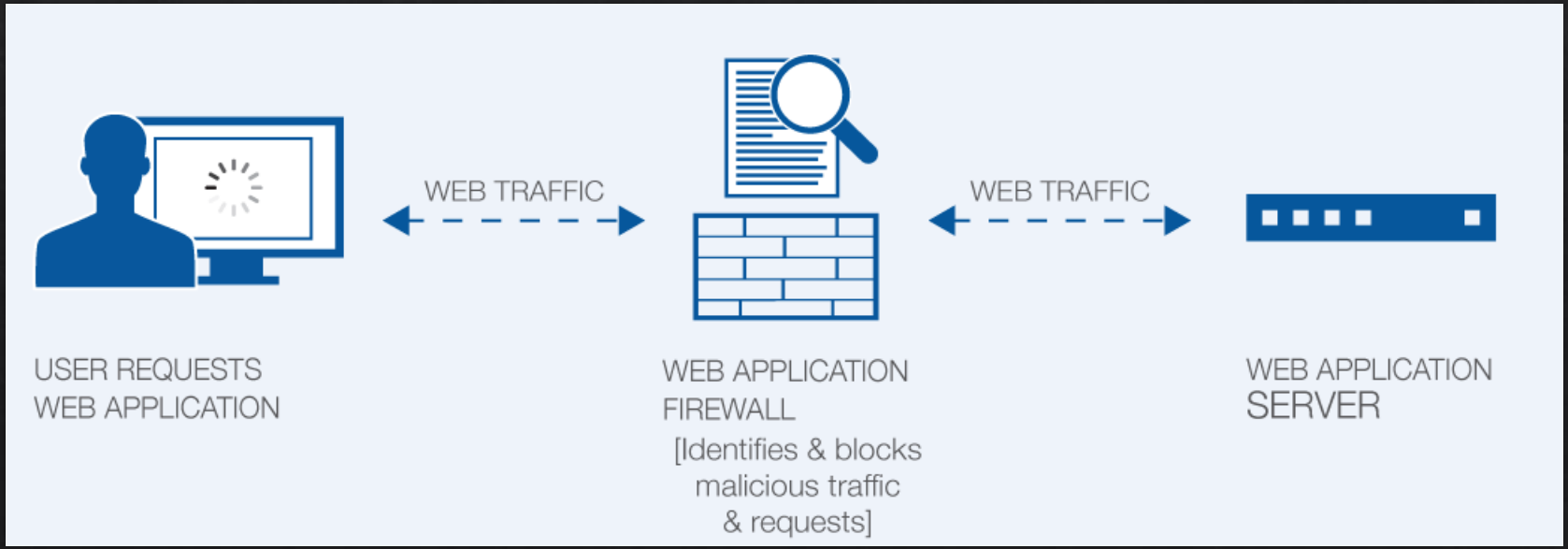


http://randy94112.tripod.com/types.htm

Web Application Firewall

A **web application firewall (WAF)** is an application firewall for HTTP applications. Filters or blocks the HTTP traffic to and from a web application

- PCI DSS requires that Web applications be fortified through either a code security review or a WAF.
- Citrix Systems Inc.'s NetScaler AppFirewall, Fortinet Inc.'s FortiWeb-400C and F5 Networks Inc.'s BIG-IP Application Security Manager, mod_security



Barracuda WAF

Firewall identification

- **Port Scanning**

- Some firewalls will uniquely identify themselves using simple port scans. For example:
  - Check Point's FireWall-1 listens on **TCP** ports **256**, **257**, **258**, and **259**
  - Microsoft's Proxy Server usually listens on **TCP** ports **1080** and **1745**.

Firewalking
Can Attackers See Through Your Firewall?

Toolchain:

- Traceroute
- Firewalk
- Nmap
- hping2

A fw Reconnaissance technique developed by Mike Schiffman and David Goldsmith. It utilizes traceroute, TTL values and TCP flags in order to identify fw and their respective ACLs.

Firewalking
Can Attackers See Through Your Firewall?

- A techniques that use TTL values to determine gateway ACL filters by analyzing IP packet response
- Attacker send a packet to the target firewall with a TTL set to one hop greater than that of the firewall
- If the packet pass through the gw, it is forwarded to the next hop where TTL equals one and elicit an “TTL exceeded in transit” to be returned, as the original packet is discarded