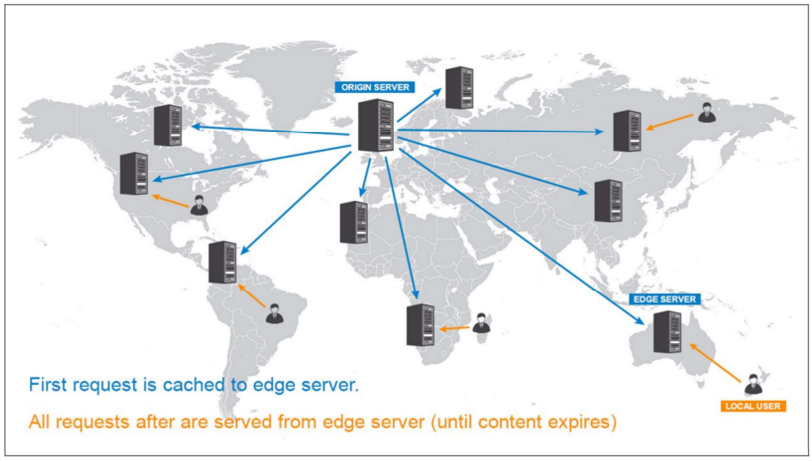
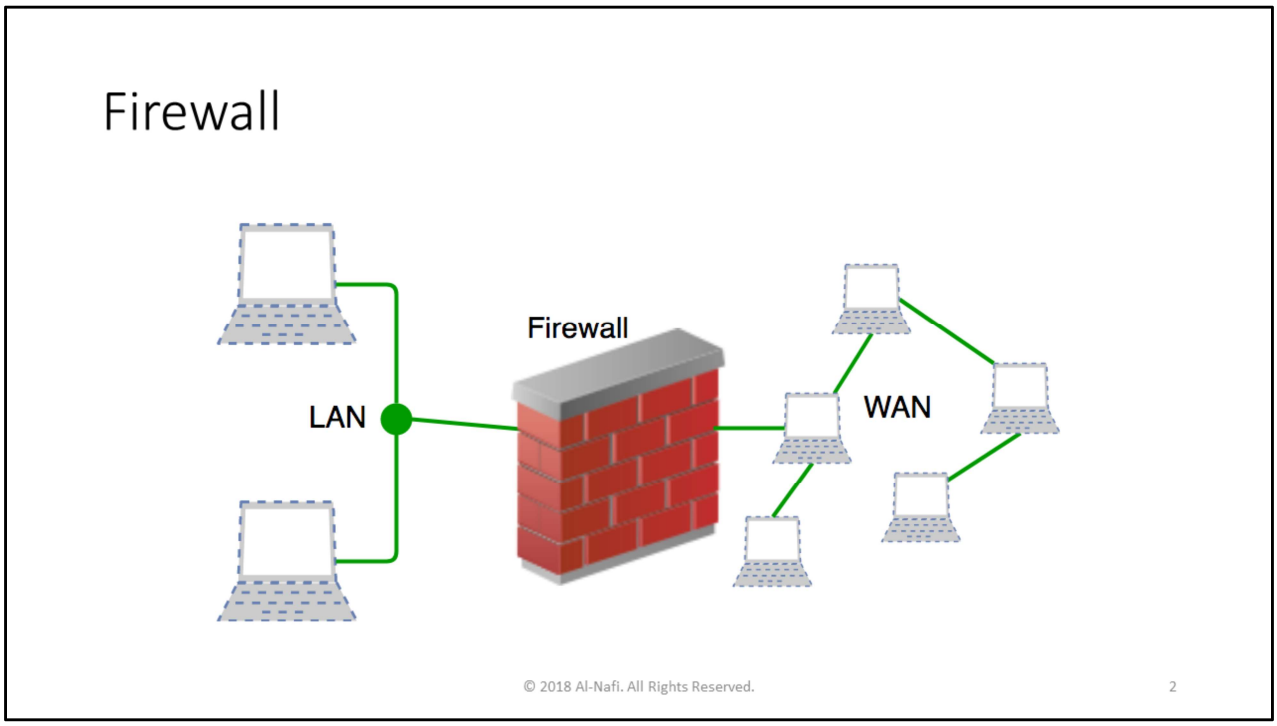
Content Distribution Networks (CDNs)



A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the internet. The goal of a CDN is to serve content to end users with high availability and high performance. A key capability of CDN is to provide for capacity management in that original content will not be easily exhausted by request from a wide geographic field.

These are the two primary components of a CDN:

- Origin servers: Housing original content in the form of web and rich media composed of audio and video files
- Edge servers: Holds cached copies of the original content that distributes media to regionally close clients to speed delivery



Firewalls

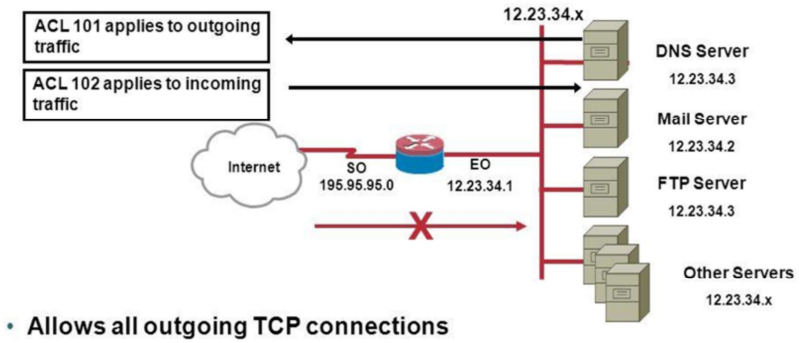
Firewalls will not be effective right out of the box. Firewall rules must be defined correctly not to inadvertently grant unauthorized access. Like all hosts on a network, administrators must install patches to the firewall and disable all unnecessary services. Also, firewalls offer limited protection against vulnerabilities caused by applications flaws in server software on other hosts. For example, a firewall will not prevent an attacker from manipulating a database to disclose confidential information.

Firewalls filter traffic based on a rule set. Each rule instructs the firewall to block or forward a packet based on one or more conditions. For each incoming packet, the firewall will look through its rule set for a rule whose conditions apply to that packet and block or forward the packet as specified in that rule. Below are two important conditions used to determine if a packet should be filtered.

By address: Firewalls will often use the packet's source or destination address, or both, to determine if the packet should
be filtered.

By service: Packets can also be filtered by service. The firewall inspects the service the packet is using (if the packet is part of the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), the service is the destination port number) to determine if the packet should be filtered. For example, firewalls will often have a rule to filter the Finger service to prevent an attacker from using it to gather information about a host. Filtering by address and by service are often combined in rules. If the engineering department wanted to grant anyone on the LAN access to its web server, a rule could be defined to forward packets whose destination address is the web server's and the
service is HTTP (TCP port 80). Firewalls can change the source address of each outgoing (from trusted to untrusted network) packet to a different address. This has several applications, most notably to allow hosts with RFC 1918 addresses access to the internet by changing their private address to one that is routable on the internet. A private address is one that will not be forwarded by an internet router and, therefore, remote attacks using private internal addresses cannot be launched over the open internet. Anonymity is another reason to use network address translation (NAT). Many organizations do not want to advertise their IP addresses to an untrusted host and, thus, unnecessarily give information about the network. They would rather hide the entire network behind translated addresses. NAT also greatly extends the capabilities of organizations to continue using IPv4 address spaces.

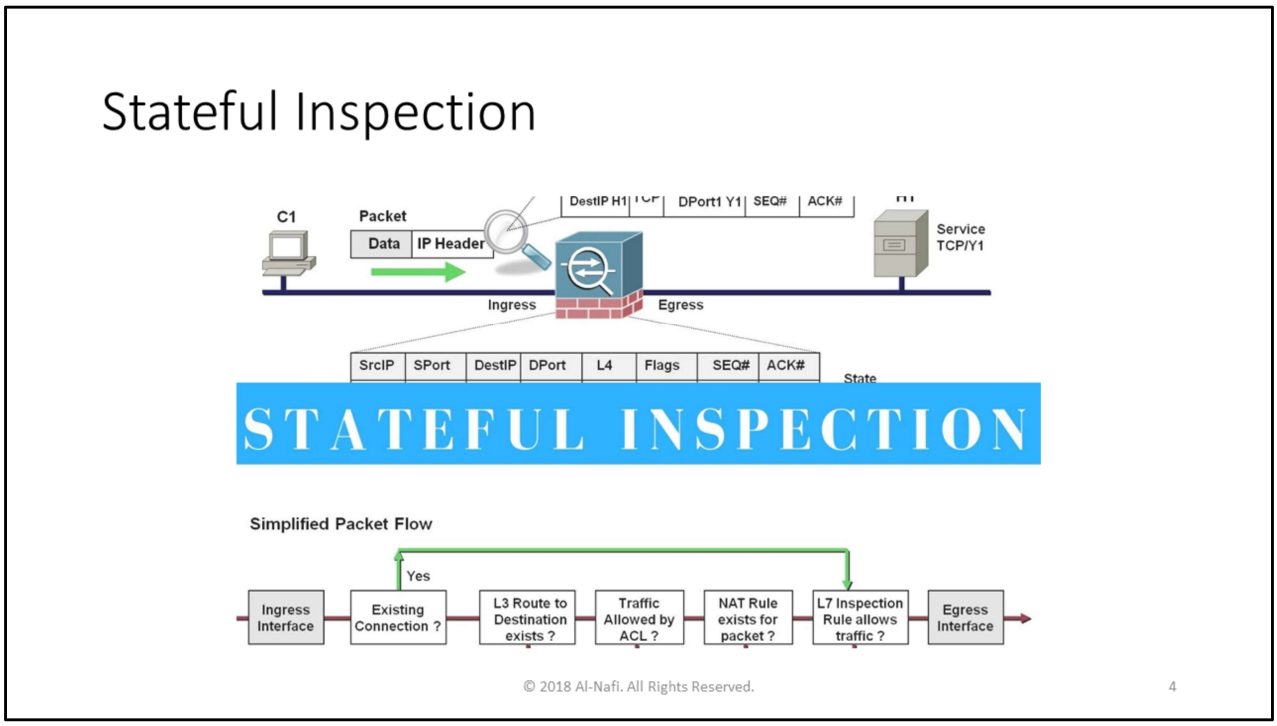
Static Packet Filtering Firewall



- Allows all outgoing TCP connections
- Allows incoming DNS, SMTP, and FTP connections and return traffic
- Denies all other services

Static Packet Filtering

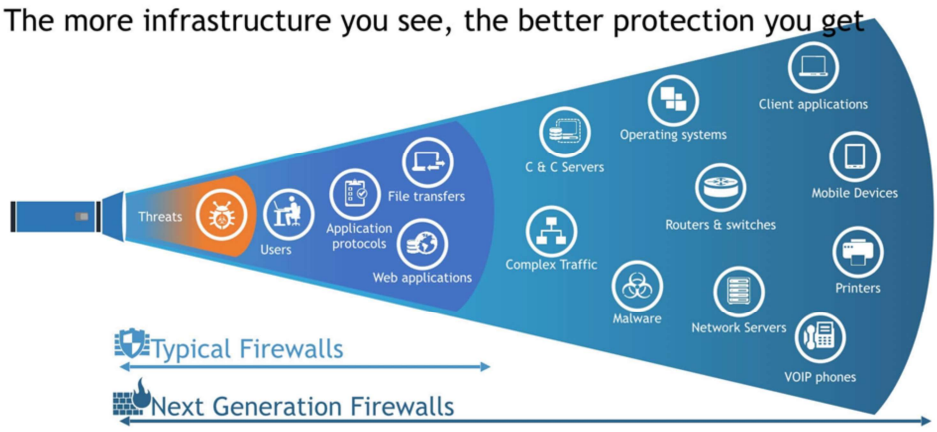
When a firewall uses static packet filtering, it examines each packet without regard to the packet's context in a session. Packets are examined against static criteria, for example, blocking all packets with a port number of 79 (finger). Because of its simplicity, static packet filtering requires very little overhead, but it has a significant disadvantage. Static rules cannot be temporarily changed by the firewall to accommodate legitimate traffic. If a protocol requires a port to be temporarily opened, administrators must choose between permanently opening the port and disallowing the protocol.



Stateful Inspection or Dynamic Packet Filtering

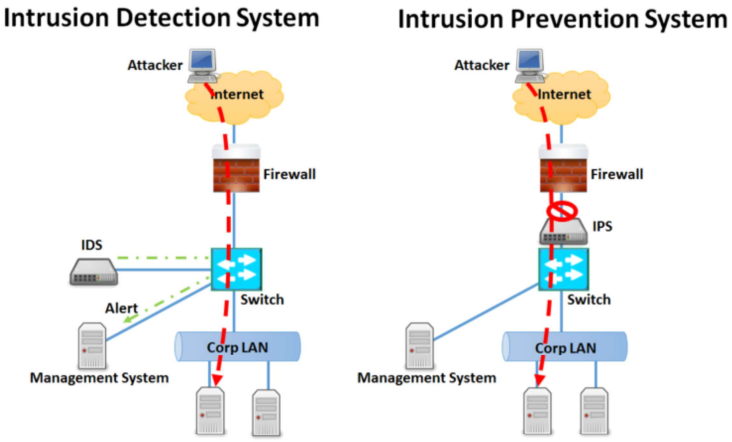
Stateful inspection examines each packet in the context of a session that allows it to make dynamic adjustments to the rules to accommodate legitimate traffic and block malicious traffic that would appear benign to a static filter. For example, if a user sends a Syn request to a server and receives a Syn Ack back from the server, the next appropriate frame to send is an Ack. If the user sends another Syn request, the stateful inspection device will see and reject this next “inappropriate” packet.

Next-generation firewalls (NGFWs)



Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, along with malware awareness and prevention. NGFWs are not the same as intrusion prevention system (IPS) stand-alone devices or even firewalls that are simply integrating IPS capabilities. Included in what is called the third generation of firewall technology is in-line deep inspection of traffic, application programming interface (API) gateways, and Database Activity Monitoring.

Intrusion Detection and Prevention Systems (IDS/IPS)



 6

Intrusion Detection and Prevention Systems (IDS/IPS)
Intrusion detection systems (IDSs) monitor activity and send alerts when they detect suspicious traffic. There are two broad classifications of IDS/IPS:

- Host-based IDS/IPS: Monitor activity on servers and workstations.
- Network-based IDS/IPS: Monitor network activity. Network IDS services are typically stand-alone devices or at least independent blades within network chassis. Network IDS logs would be accessed through a separate management console that will also generate alarms and alerts.

Currently, there are two approaches to the deployment and use of IDSs.

An appliance on the network can monitor traffic for attacks based on a set of signatures (analogous to antivirus software), or the appliance can watch the network's traffic for a while, learn what traffic patterns are normal and send an alert when it detects an anomaly. Of course, the IDS can be deployed using a hybrid of the two approaches as well.

Independent of the approach, how an organization uses an IDS determines whether the tool is effective. Despite its name, the IDS should not be used to detect intrusions because IDS solutions are not designed to be able to take preventative actions as part of their response. Instead, it should send an alert when it detects interesting, abnormal traffic that could be a prelude to an attack.

For example, someone in the engineering department trying to access payroll information over the network at 3 a.m. is probably very interesting and not normal. Or, perhaps a sudden rise in network utilization should be noted.

Intrusion systems use several techniques to determine whether an attack is underway:

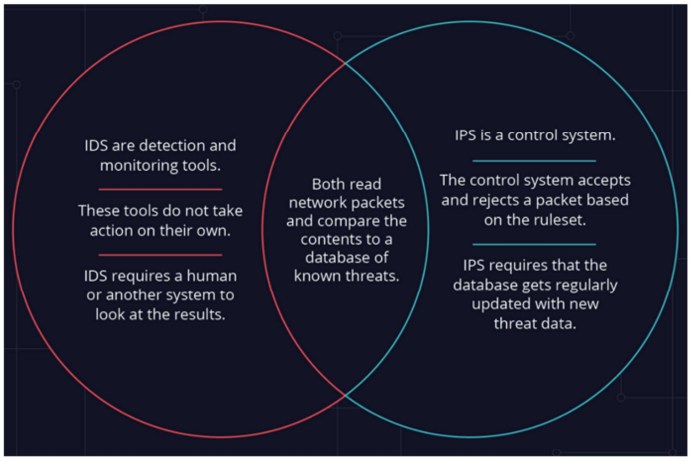
- Signature or pattern-matching systems examine the available information (logs or network traffic) to determine if it matches a known attack.
- Protocol-anomaly-based systems examine network traffic to determine if what it sees conforms to the defined standard for that protocol; for example, as it is defined in a Request for Comment (RFC).
- Statistical-anomaly-based systems establish a baseline of normal traffic patterns over time and detect any deviations from that baseline.

Some also use heuristics to evaluate the intended behavior of network traffic to determine if it intended to be malicious or not. Most modern systems combine two or more of these techniques together to provide a more accurate analysis before it decides whether it sees an attack or not.

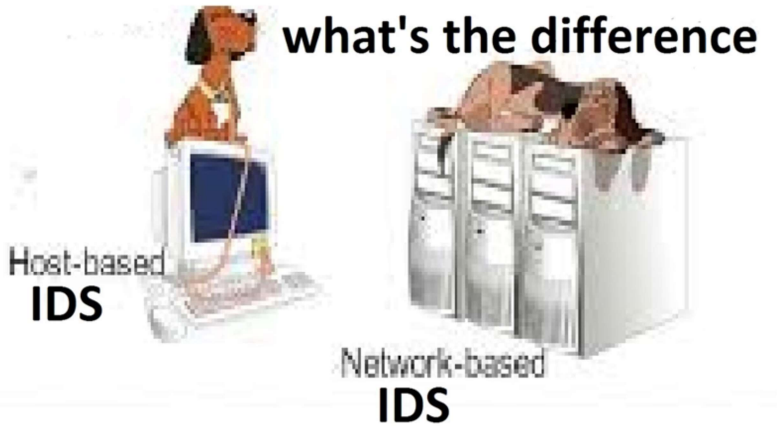
In most cases, there will continue to be problems associated with false positives as well as false-negatives. False-positives occur when the IDS or IPS identifies something as an attack, but it is in fact normal traffic. False-negatives occur when the IPS or IDS fails to interpret something as an attack when it should have. In these cases, intrusion systems must be carefully “tuned” to ensure that these are kept to a minimum.

An IDS requires frequent attention. An IDS requires the response of a human who is knowledgeable enough with the system and types of normal activity to make an educated judgment about the relevance and significance of the event. Alerts need to be investigated to Determine if they represent an actual event, or if they are simply background noise.

IDS vs IPS



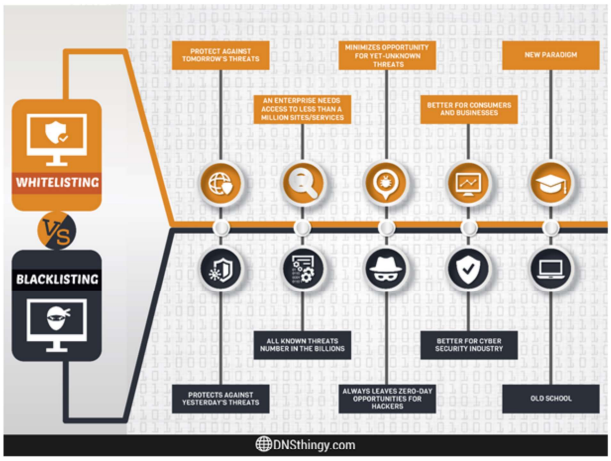
Host Based IDS/IPS



IDS/IPS uses many techniques for protection purposes like

- Signature or pattern-matching systems
- Protocol-anomaly-based systems
- Statistical-anomaly-based systems

Whitelisting/Blacklisting



Whitelisting/blacklisting: A whitelist is a list of email addresses and/or internet addresses that someone knows as “good” senders. A blacklist is a corresponding list of known “bad” senders. So, an email from an unrecognized sender is neither on the whitelist or the blacklist and, therefore, is treated differently. Grey listing works by telling the sending email server to resend the message sometime soon. Many spammers set their software to blindly transmit their spam email, and the software does not understand the “resend soon” message. Thus, the spam would never actually be delivered.