Network Security

- “Each port and underlying service has its risks. The risk comes from the version of the service, whether someone has configured it correctly, and, if there are passwords for the service, whether these are strong? There are many more factors that determine whether a port or service is safe,”

Protocols: *TCP and UDP*

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.

Protocols: *TCP and UDP*

- Each of these logical ports are technically identified as either a Transmission Control Protocol (TCP) port or a User Datagram Protocol (UDP) port depending on which transport protocol they use.
- If the protocol requires the benefits of TCP such as guaranteed delivery, it will use the TCP port. For example, web traffic using Hypertext Transfer Protocol (HTTP) uses TCP because web pages will not display properly if some of the packets aren't received. TCP tracks all the packets and if one is lost, it sends a request to have it resent. This takes a little longer but provides the assurance that all packets are received.
- Some protocols use only the UDP port. For example, Trivial File Transport Protocol (TFTP) uses UDP port 69 but not TCP port 69.

- Other protocols will use both TCP and UDP, depending on the purpose. For example, Domain Name System (DNS) will normally use UDP port 53 when responding to typical name resolution requests from clients. However, when one DNS server is transferring data to another DNS server, it will typically use TCP port 53.
- The tables on this page specify whether a protocol uses TCP, UDP, or both. If you want to know specifically which transport protocol is used for other protocols, check out Wikipedia's list of TCP and UDP port numbers.
- Interestingly, Internet Assigned Numbers Authority (IANA) previously identified which transport protocol was used for each port in their Service Name and Transport Protocol Port Number Registry . However, they seem to have defaulted to just listing both TCP and UDP for each port. For example, Telnet (defined in RFC 854) only uses TCP port 23, not UDP. However, IANAs port number registry lists both TCP and UDP for Telnet.

Ports

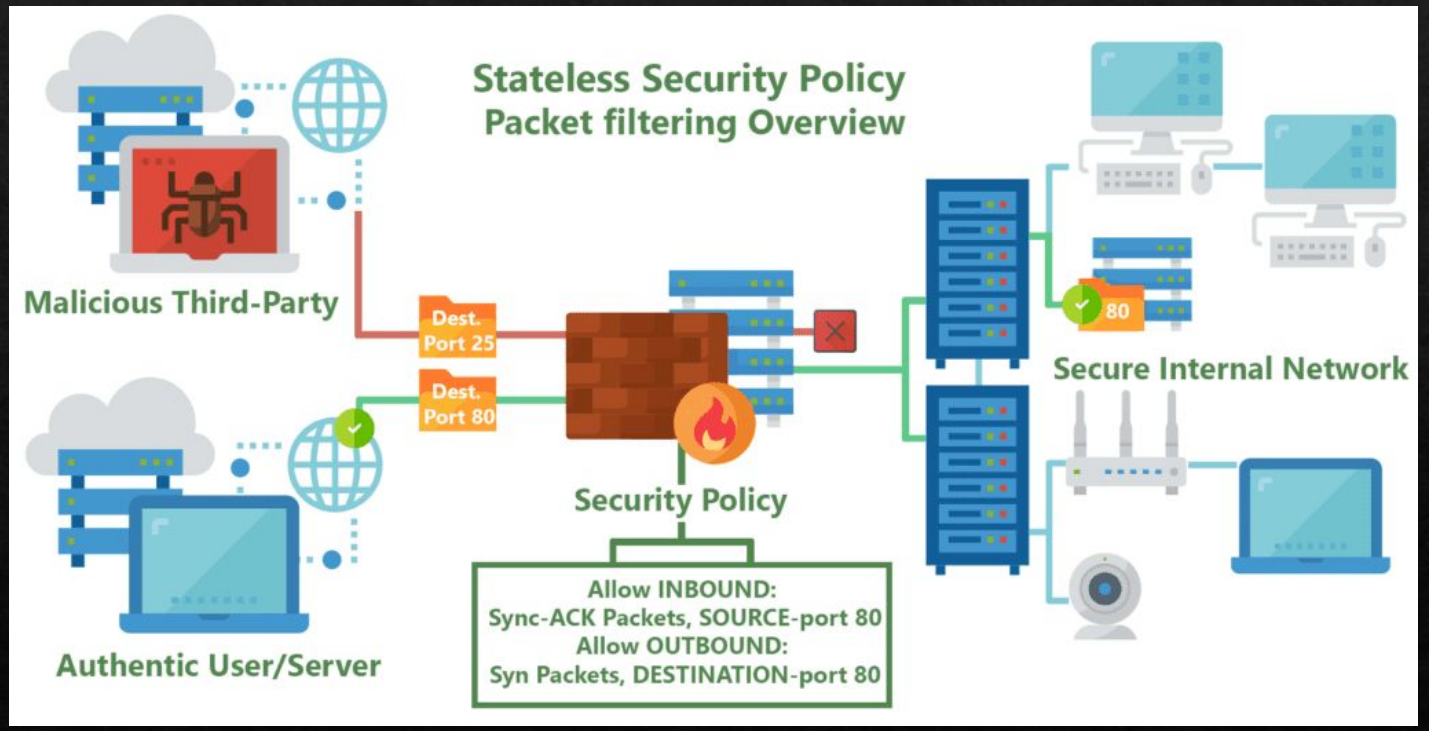
- Network ports are provided by the TCP or UDP protocols at the Transport layer. They are used by protocols in the upper layers of the OSI model.
- Port numbers are used to determine what protocol incoming traffic should be directed to. Ports allow a single host with a single IP address to run network services. Each port number identifies a distinct service, and each host can have 65535 ports per IP address. Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN). By ICANN there are three categories for ports:
  - From 0 to 1023 – well known ports assigned to common protocols and services
  - From 1024 to 49151 – registered ports assigned by ICANN to a specific service
  - From 49152 to 65 535 – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by any service on an ad hoc basis. Ports are assigned when a session is established, and released when the session ends.

Common ports

Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name System (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP
123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP
989, 990	FTP over SSL/TLS (implicit mode)	TCP
3389	Remote Desktop Protocol	TCP and UDP

What is a Firewall?

- A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits, or blocks data **packets** based on a set of security rules.
- Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



How does a firewall work?

- Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices. For example, “Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."
- Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it’s further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

What is Distributed Firewall?

- Distributed firewalls help solve this problem by using processing power across the network, not just on a single cluster or machine where a firewall is installed.
- A distributed firewall is a host-resident security software application, which protects the network as a whole against unwanted intrusion. Deployed alongside more traditional firewalls, distributed firewalls can add another layer of protection to a network while still maintaining high throughput for legitimate network traffic.
- In addition, centralized firewalls are based on a model that assumes attacks are coming from outside a network. They apply a “perimeter defense” model where a firewall guards only against malicious traffic coming from outside the network.
- This model fails, however, if an attack comes from inside the network – an all-too-common occurrence given the huge variety of ways that users can connect to an internal network, including wireless access and VPN tunnels. Traditional firewalls typically can’t effectively guard against attacks coming from sources like these, but a distributed firewall can add another layer of defense against this type of attack.