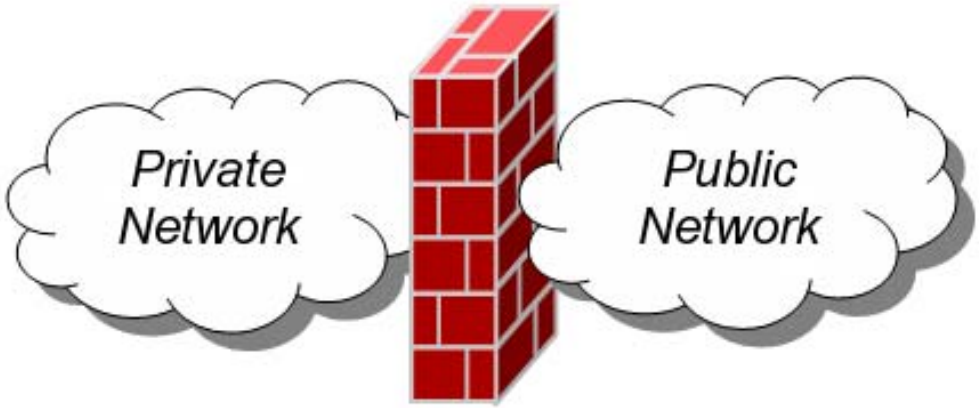
Firewalls

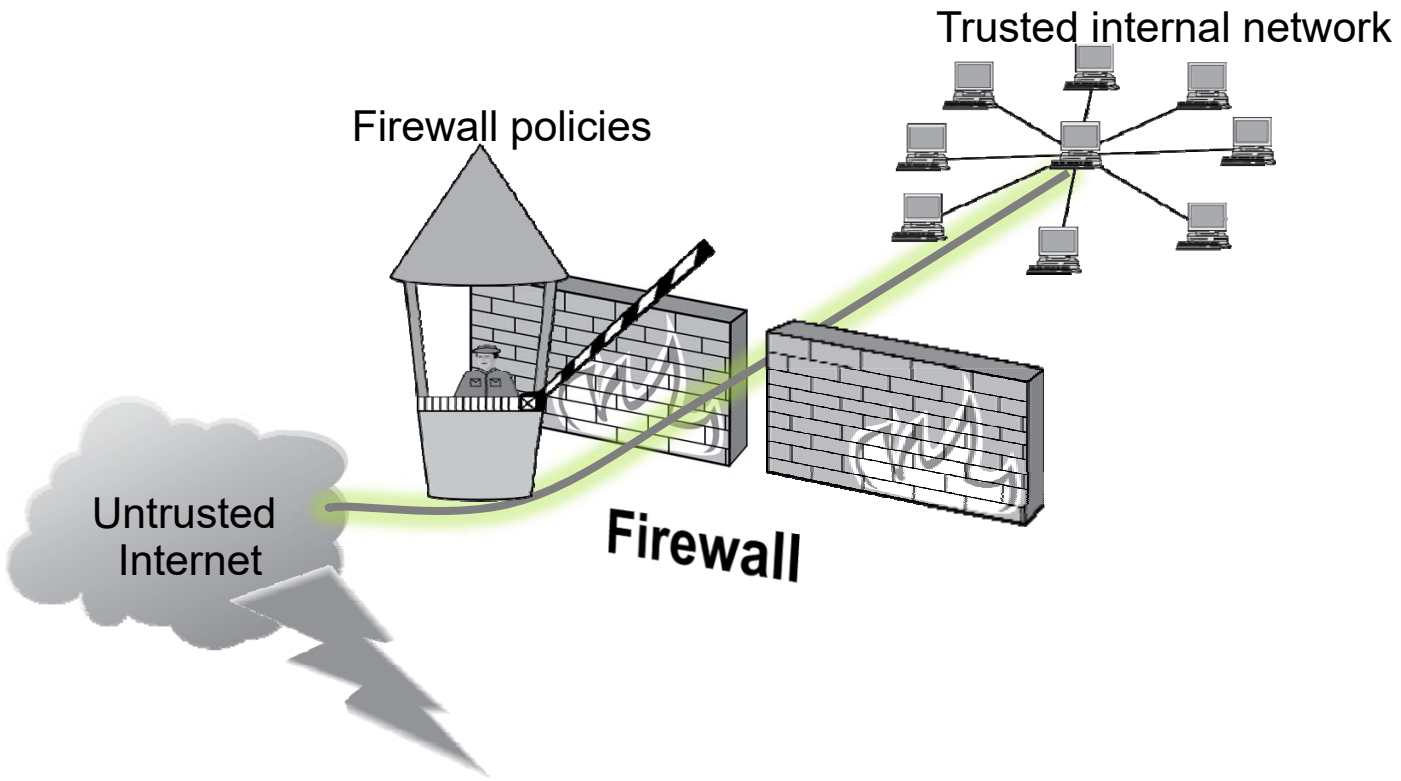
Firewalls

- A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Policies

- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
  - **Accepted:** permitted through the firewall
  - **Dropped:** not allowed through with no indication of failure
  - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
  - TCP or UDP
  - the source and destination IP addresses
  - the source and destination ports
  - the application-level payload of the packet (e.g., whether it contains a virus).

Blacklists and White Lists

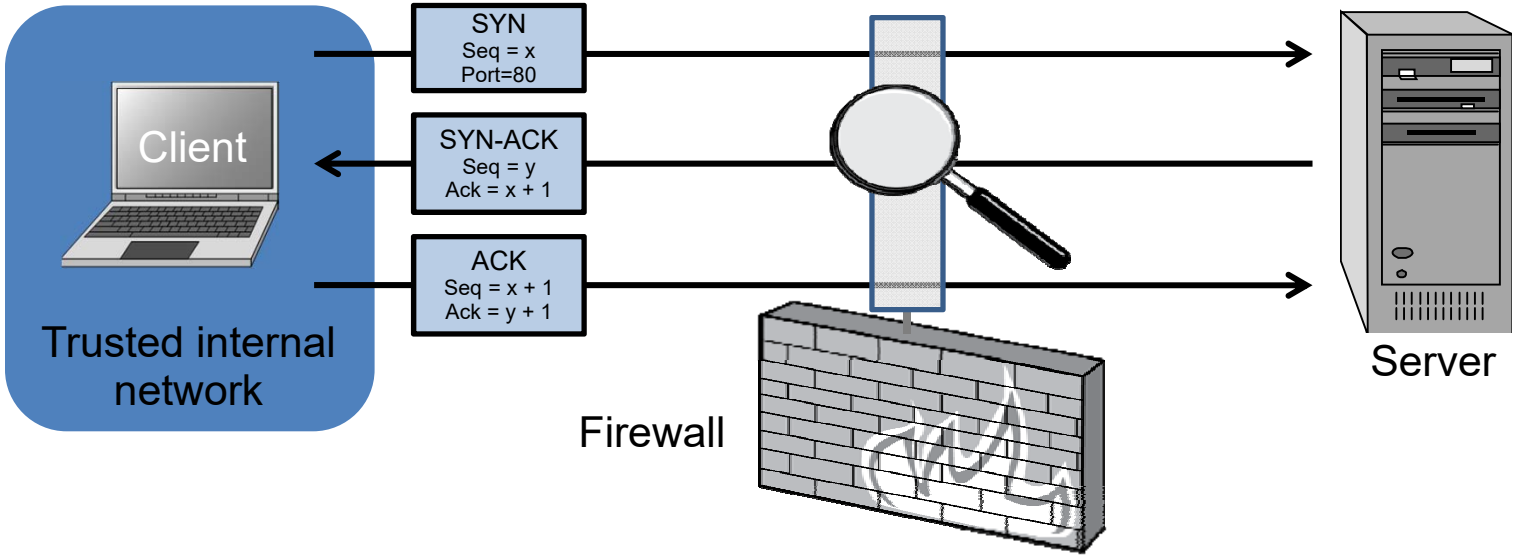
- There are two fundamental approaches to creating firewall policies (or rulesets) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network (or individual computer).
- **Blacklist** approach
  - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
  - This type of configuration is more flexible in ensuring that service to the internal network is not disrupted by the firewall, but is naïve from a security perspective in that it assumes the network administrator can enumerate all of the properties of malicious traffic.
- **Whitelist** approach
  - A safer approach to defining a firewall ruleset is the default-deny policy, in which packets are dropped or rejected unless they are specifically allowed by the firewall.

Firewall Types

- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Stateless Firewalls

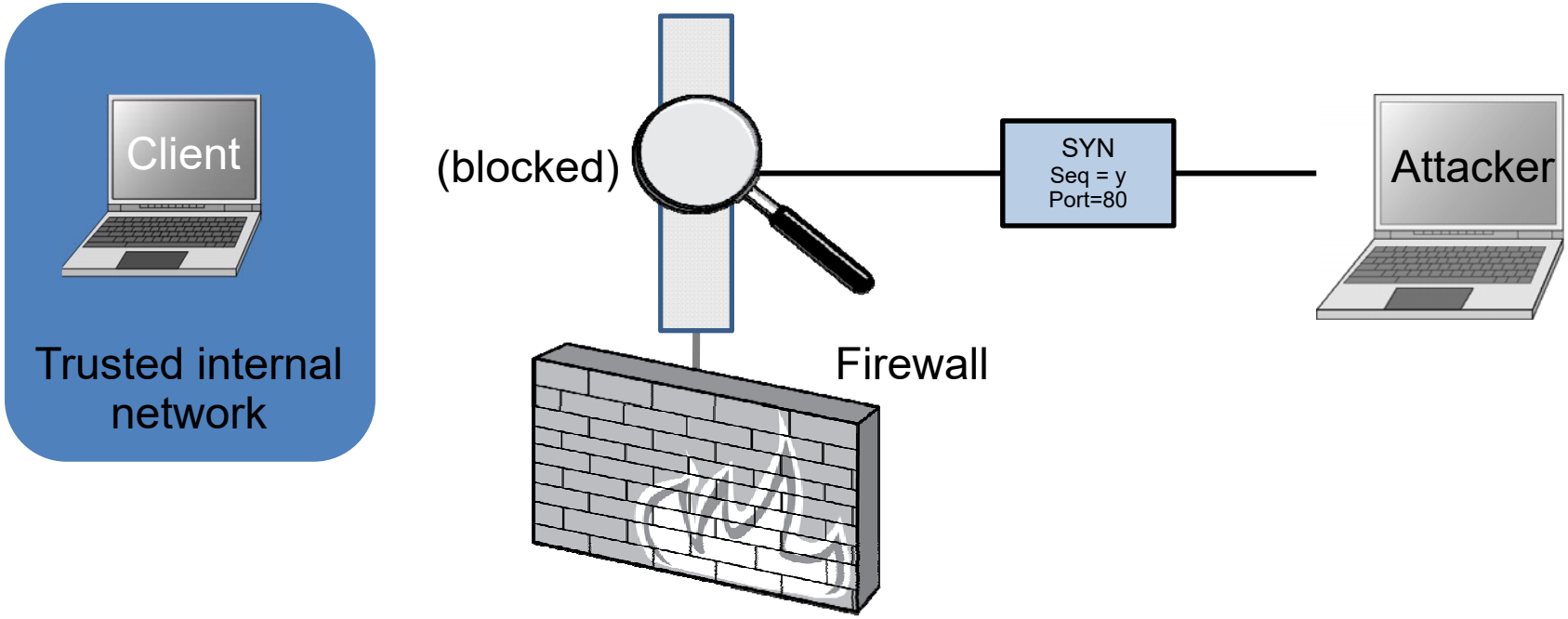
- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



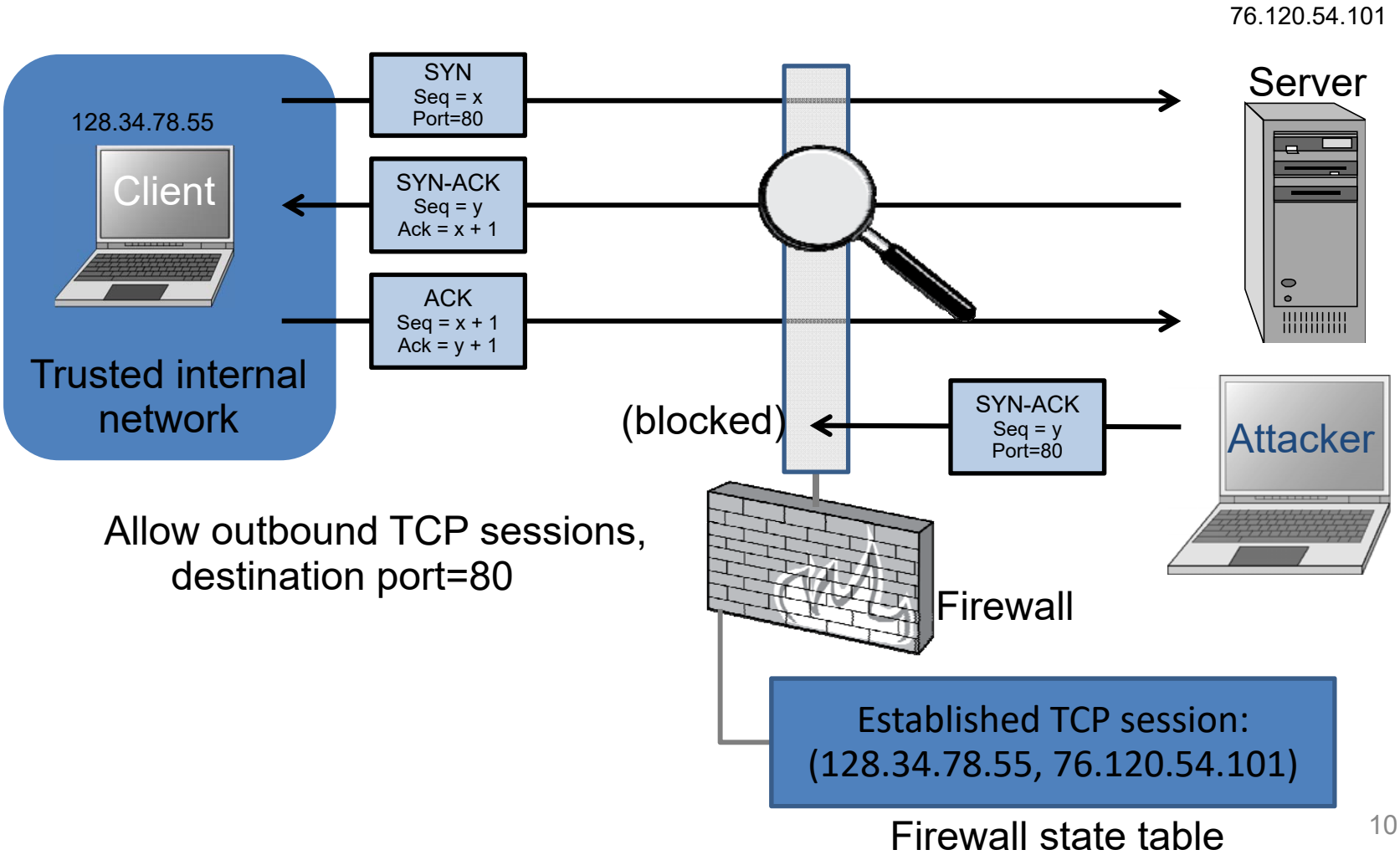
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Statefull Firewalls

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Statefull Firewall Example

- Allow only requested TCP connections:



Iptables

- A stateful firewall on Linux
- Example commands: (more on http://www.unixnewbie.org/iptables-cheat-sheet/)
  - Block an IP address:
    - iptables -I INPUT -s "201.128.33.200" -j DROP
  - block all connections to a port:
    - iptables -A INPUT -p tcp --dport 25 -j DROP
    - iptables -A INPUT -p udp --dport 25 -j DROP
- Stateful rules (http://en.gentoo-wiki.com/wiki/Iptables/Iptables_and_stateful_firewalls)
    - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Iptables (cont.)

- Stateful rules (http://en.gentoo-wiki.com/wiki/Iptables/Iptables_and_stateful_firewalls)
  - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

- States:
  - NEW: the first packet in a session (one direction)
  - ESTABLISHED: follow-up packet in an established connection (e.g., after a handshake)
  - RELATED: packets are those that are starting a new connection, but are related to another currently existing connection (e.g., ICMP packets related to a SSH connection)
  - INVALID: those that can't be classified into one of the above three categories