Network Security

Chapter 3

Cornelius Diekmann

Lehrstuhl für Netzarchitekturen und Netzdienste
Institut für Informatik
Technische Universität München

Version: October 21, 2015

Security Policies and Firewalls

Introduction: What does *secure* mean?

- Definition: Security Policy

  "*A security policy, a specific statement of what is and is not allowed, defines the system's security.*" [Bishop03]

- Definition: Security Mechanisms

  "*Security Mechanisms enforce the policies; their goal is to ensure that the system never enters a disallowed state.*" [Bishop03]

- Examples of Security Mechanisms:
  - IPsec gateways, firewalls, SSL, ...

- A system is *secure* if, started in an allowed state, always stays in states that are allowed.

- The policy *defines* security, the security mechanisms *enforce* it.

The 3 Security Components

- Requirements
  - Define security goals
  - , , , , ,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals
  - , , , , ,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

What were those again?

The 3 Security Components

- Requirements
  - Define security goals
  - Data Integrity, , , , ,
  - "*What do we want?*"

  What were those again?
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals What were those again?
  - Data Integrity, Confidentiality, , , ,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals What were those again?
  - Data Integrity, Confidentiality, Availability, , ,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals What were those again?
  - Data Integrity, Confidentiality, Availability, Authenticity, ,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals What were those again?
  - Data Integrity, Confidentiality, Availability, Authenticity, Accountability,
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- Requirements
  - Define security goals
  - Data Integrity, Confidentiality, Availability, Authenticity, Accountability, Controlled Access
  - "*What do we want?*"
- Policy
  - Rules to implement the requirements
  - "*How to get there?*"
- Mechanisms
  - Enforce the policy

The 3 Security Components

- A network admin reports:

  "*Our management wants to ensure that, because of a recent incident, the originators of all internal eMails must now be clearly identifiable. I generated X.509 certificates for all employees and set up their mail clients to always sign their outgoing mails. Unsigned eMails are now dropped by default*"

- Security Requirements:
- Security Policy:
- Security Mechanisms:

The 3 Security Components

- A network admin reports:

  "*Our management wants to ensure that, because of a recent incident, the originators of all internal eMails must now be clearly identifiable. I generated X.509 certificates for all employees and set up their mail clients to always sign their outgoing mails. Unsigned eMails are now dropped by default*"

- Security Requirements:
  Sender accountability of all internal eMails

- Security Policy:

- Security Mechanisms:

The 3 Security Components

- A network admin reports:

  "*Our management wants to ensure that, because of a recent incident, the originators of all internal eMails must now be clearly identifiable. I generated X.509 certificates for all employees and set up their mail clients to always sign their outgoing mails. Unsigned eMails are now dropped by default*"

- Security Requirements:
  Sender accountability of all internal eMails

- Security Policy:
  All eMails must be cryptographically signed

- Security Mechanisms:

The 3 Security Components

- A network admin reports:

  "*Our management wants to ensure that, because of a recent incident, the originators of all internal eMails must now be clearly identifiable. I generated X.509 certificates for all employees and set up their mail clients to always sign their outgoing mails. Unsigned eMails are now dropped by default*"

- Security Requirements:
  Sender accountability of all internal eMails

- Security Policy:
  All eMails must be cryptographically signed

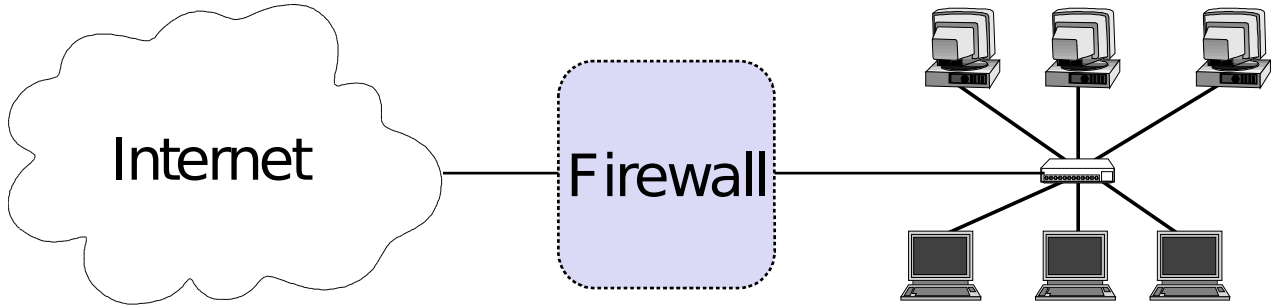
- Security Mechanisms:
  X.509 certificates + signatures, dropping of unsigned eMails by mailserver

A closer look at policy-heavy security mechanisms

Network Firewalls

Network Firewalls

- Network Firewalls



- Do not confuse with host-based firewalls!

The Story of Firewalls

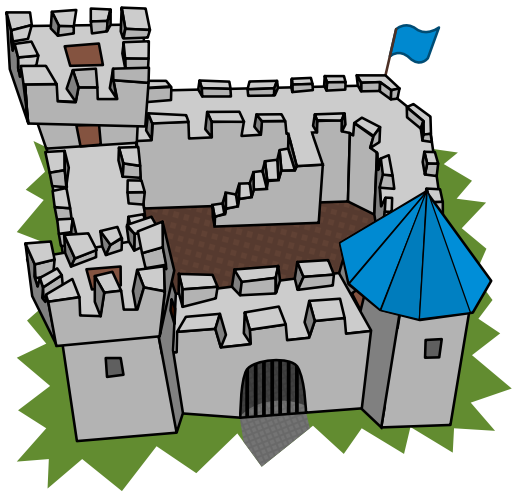
- Building construction
  - Keep a fire from spreading from one part of the building to another

The Story of Firewalls

- Building construction
  - Keep a fire from spreading from one part of the building to another
- Network:

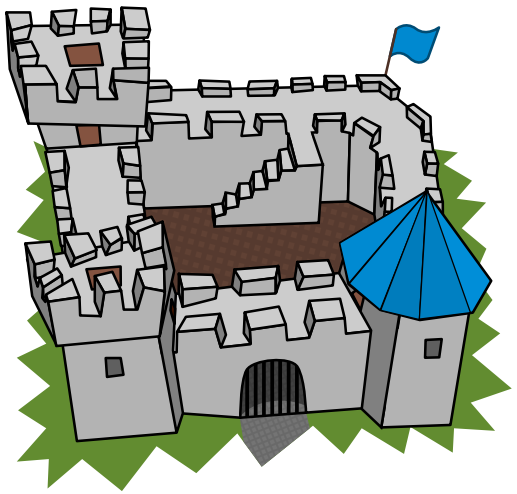
The Story of Firewalls

- Building construction
  - Keep a fire from spreading from one part of the building to another
- Network: Better compared to a moat of a medieval castle



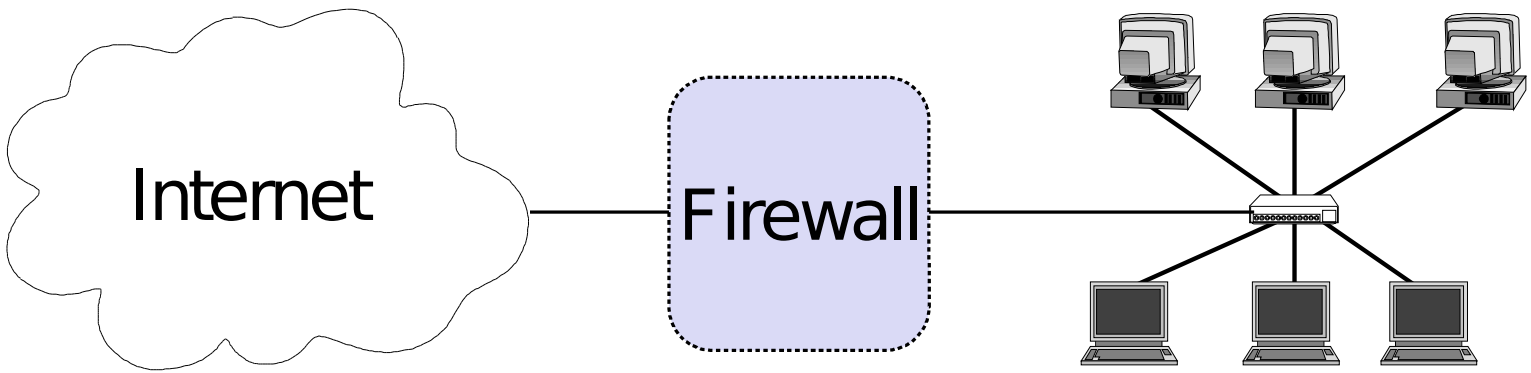
The Story of Firewalls

- Building construction
  - Keep a fire from spreading from one part of the building to another
- Network: Better compared to a moat of a medieval castle
  - Restricts people to enter at one carefully controlled point
  - Prevents attackers from getting close to other defenses
  - Restricts people to leave at one carefully controlled point

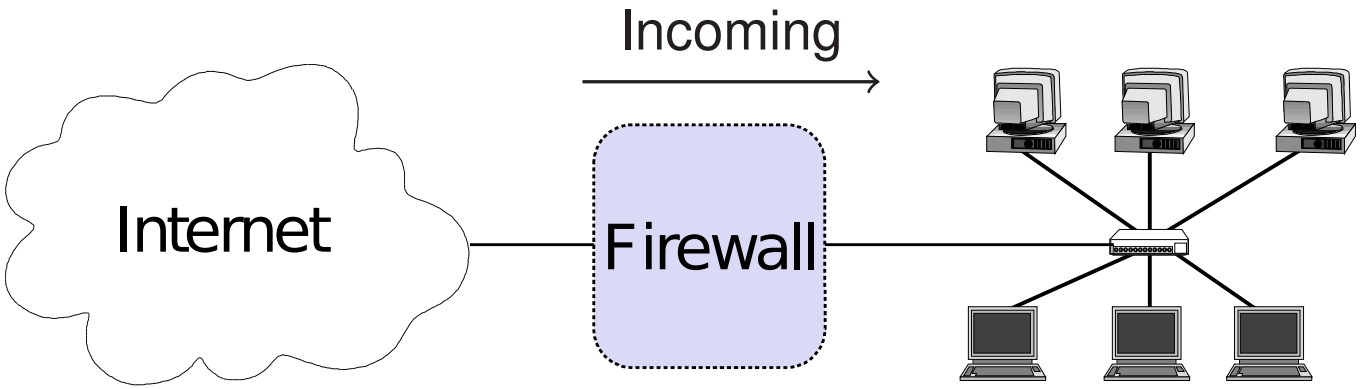


Placing Firewalls

- Controlled Access at the network level
- Install where a protected subnetwork is connected to a less trusted network
- If not specified otherwise, we assume
  - Firewall is placed between Internet and local network

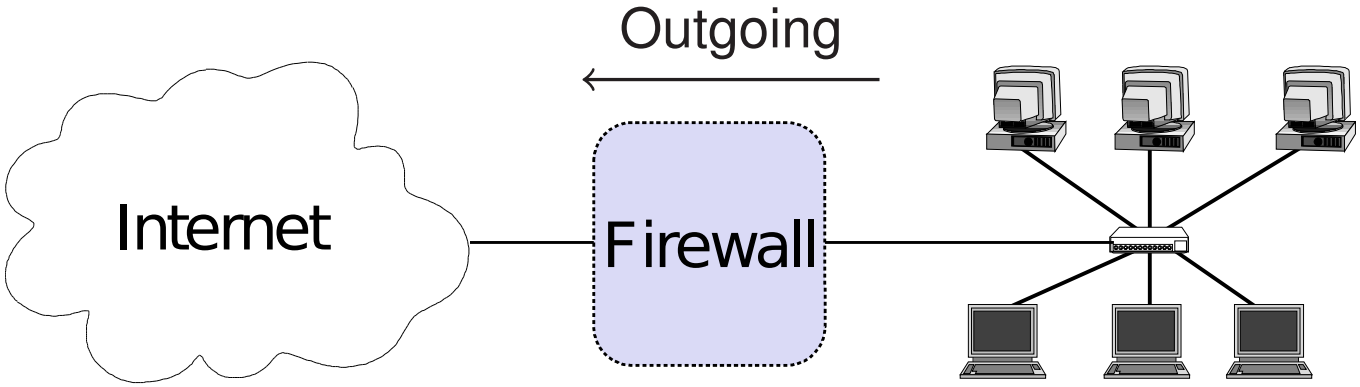


Incoming and Outgoing Packets



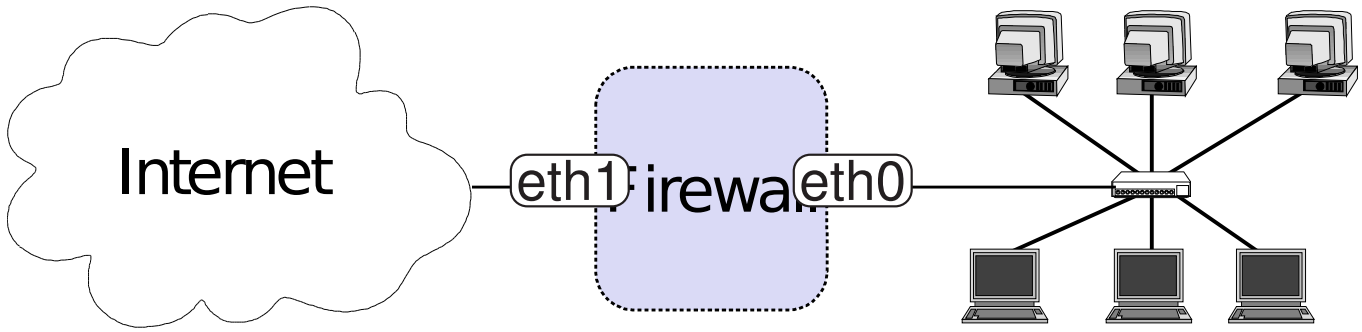
- Different views
- View 1 (e.g. by admin of the LAN)
  - Incoming: from the Internet to the local network
  - Outgoing: from the local network to the Internet

Incoming and Outgoing Packets



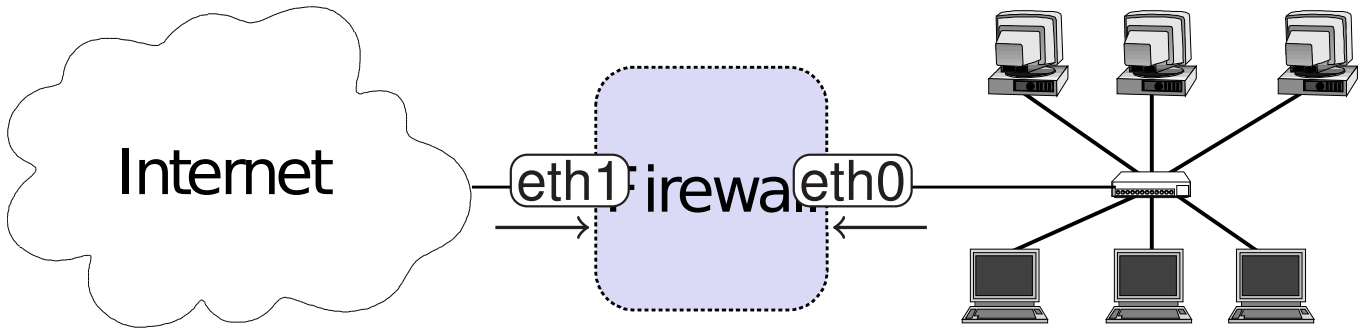
- Different views
- View 1 (e.g. by admin of the LAN)
  - Incoming: from the Internet to the local network
  - Outgoing: from the local network to the Internet

Incoming and Outgoing Packets



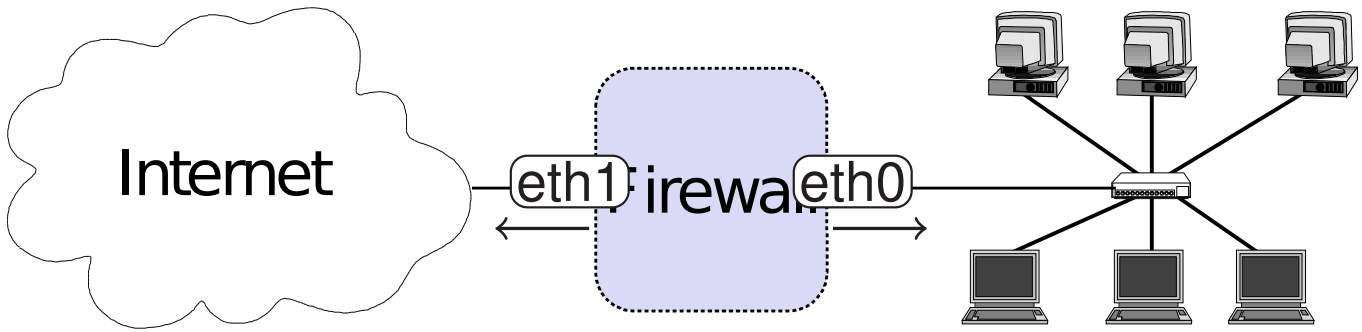
- Different views
- View 1 (e.g. by admin of the LAN)
  - Incoming: from the Internet to the local network
  - Outgoing: from the local network to the Internet
- View 2 (e.g. by firewall man page)
  - On each interface, there are incoming and outgoing packets

Incoming and Outgoing Packets



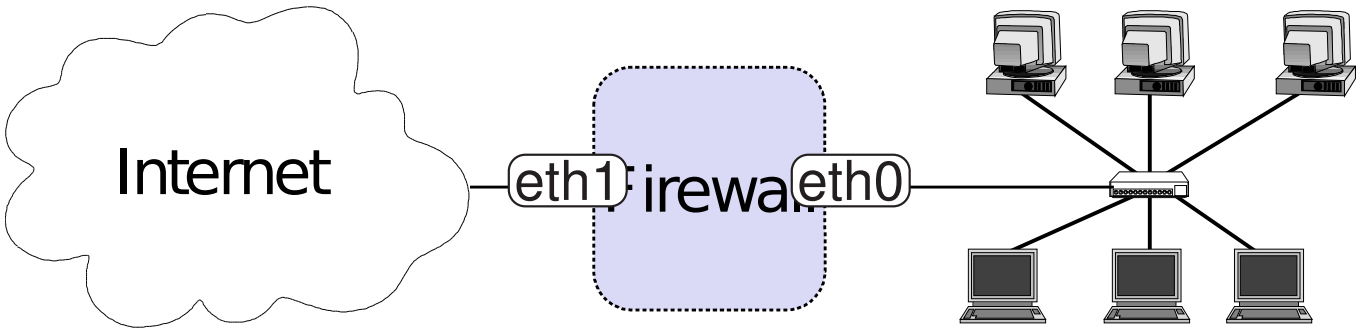
- Different views
- View 1 (e.g. by admin of the LAN)
  - Incoming: from the Internet to the local network
  - Outgoing: from the local network to the Internet
- View 2 (e.g. by firewall man page)
  - On each interface, there are incoming and outgoing packets

Incoming and Outgoing Packets



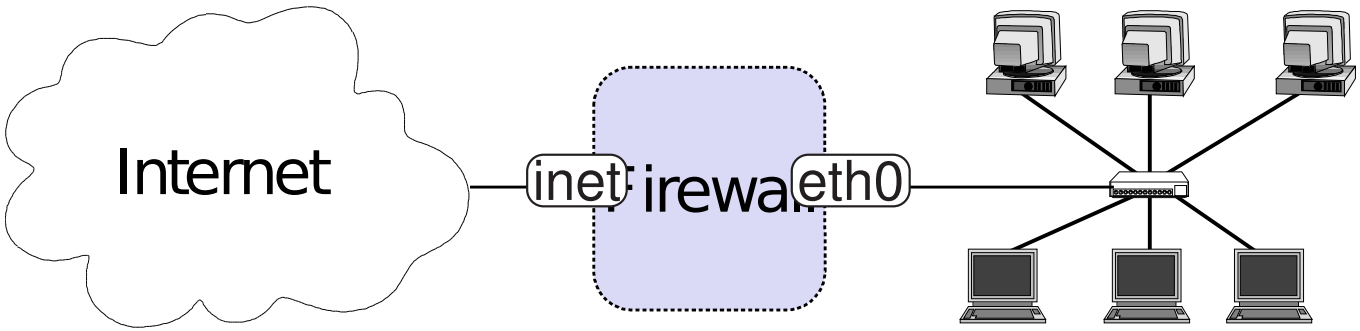
- Different views
- View 1 (e.g. by admin of the LAN)
  - Incoming: from the Internet to the local network
  - Outgoing: from the local network to the Internet
- View 2 (e.g. by firewall man page)
  - On each interface, there are incoming and outgoing packets

Incoming and Outgoing Packets



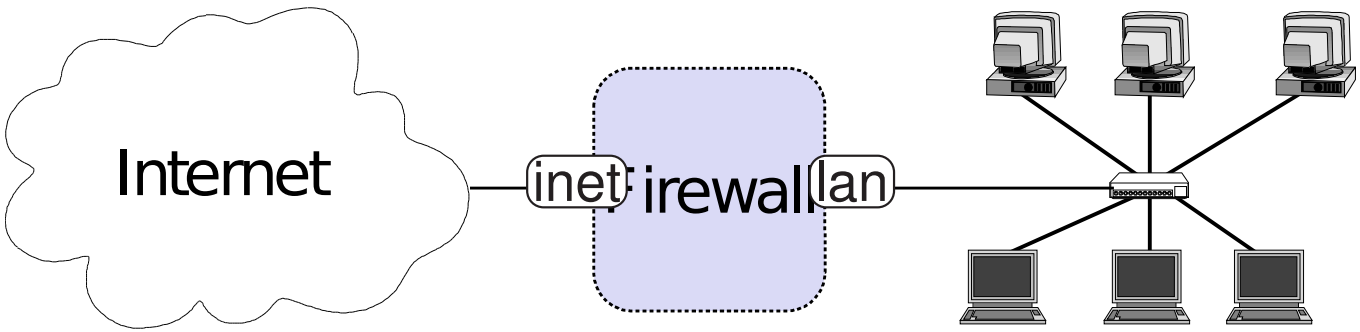
- For convenience:

Incoming and Outgoing Packets



- For convenience:
- `# ip link set eth1 name inet`

Incoming and Outgoing Packets



- For convenience:
- `# ip link set eth1 name inet`
- `# ip link set eth0 name lan`

What does a firewall do?

- By default: nothing!

What does a firewall do?

- By default: nothing!
- Needs to be configured.

Strategies

- Whitelisting
  - Default deny strategy: Everything not explicitly permitted is denied
- Blacklisting
  - Default permit strategy: Everything not explicitly forbidden is permitted

Strategies

- Whitelisting
  - Default deny strategy: Everything not explicitly permitted is denied
  - Increased security
- Blacklisting
  - Default permit strategy: Everything not explicitly forbidden is permitted
  - Less hassle with users

Strategies

- Whitelisting
  - Default deny strategy: Everything not explicitly permitted is denied
  - Increased security
- Blacklisting
  - Default permit strategy: Everything not explicitly forbidden is permitted
  - Less hassle with users
- Best Practice: Whitelisting

Example: Strict Whitelisting

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- Policy: Allow outgoing HTTP (TCP port 80), deny the rest
- LAN can initiate outgoing HTTP connections
  - Example: SYN
- The Internet may respond to established connections
  - Example: SYN,ACK
- LAN may use established connections
  - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
  - Example: DNS

Example: Strict Whitelisting

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
⇒A	lan	192.168.0.0/16	0.0.0.0/0	TCP	$>$ 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	$>$ 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- Policy: Allow outgoing HTTP (TCP port 80), deny the rest
- LAN can initiate outgoing HTTP connections
  - Example: SYN
- The Internet may respond to established connections
  - Example: SYN,ACK
- LAN may use established connections
  - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
  - Example: DNS

Example: Strict Whitelisting

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	$>$ 1023	80	New,Est.	Accept
$\Rightarrow$B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	$>$ 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- Policy: Allow outgoing HTTP (TCP port 80), deny the rest
- LAN can initiate outgoing HTTP connections
  - Example: SYN
- The Internet may respond to established connections
  - Example: SYN,ACK
- LAN may use established connections
  - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
  - Example: DNS

Example: Strict Whitelisting

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
⇒A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- Policy: Allow outgoing HTTP (TCP port 80), deny the rest
- LAN can initiate outgoing HTTP connections
  - Example: SYN
- The Internet may respond to established connections
  - Example: SYN,ACK
- LAN may use established connections
  - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
  - Example: DNS

Example: Strict Whitelisting

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	$>$ 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	$>$ 1023	Est.	Accept
$\Rightarrow$C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- Policy: Allow outgoing HTTP (TCP port 80), deny the rest
- LAN can initiate outgoing HTTP connections
  - Example: SYN
- The Internet may respond to established connections
  - Example: SYN,ACK
- LAN may use established connections
  - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
  - Example: DNS

Configuring Firewalls

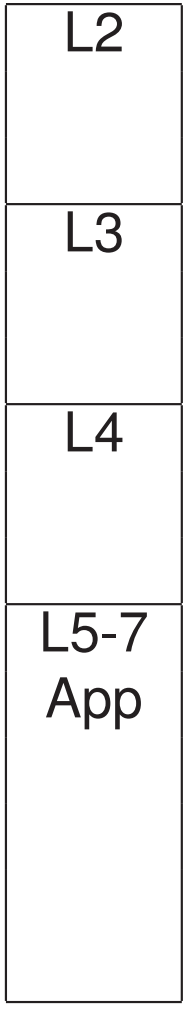
- A firewall is configured by a ruleset
  - Actually: rulelist
- For every packet, the ruleset is processed sequentially until a matching rule is found
- A rule consists of
  - Match condition
  - Action

Rules

- Actions
  - Accept
  - Drop, Reject
  - Log
  - ...
- Match Conditions
  - Incoming interface
  - All l2-l4 packet fields
    - MAC addresses, IP addresses, protocol, ports, flags, ...
  - Stateful matches
    - The firewall tracks connections for you
    - e.g. with the IP-5-tuple
  - Further advanced conditions
    - rate limiting, locally tagged packets, ...

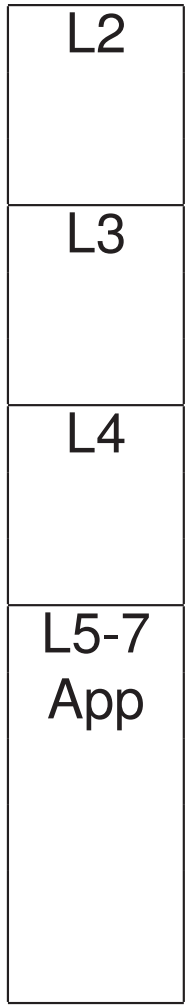
Details on Packet Fields

- Link Layer (l2) – Ethernet
  - EtherType
    - Usually: `0x0800` (IPv4)
    - Handle other EtherTypes: e.g. Drop `0x86DD` (IPv6)
  - Ethernet MAC Address
    - Easily spoofable!
    - `# ifconfig eth0 hw ether de:ad:be:ef:de:ad`
- Network Layer (l3) – IPv4
  - IP addresses
  - Transport protocol
    - TCP, UDP, ICMP, ...
  - Flags: IP fragment
  - Options: E.g. source routing
    - Please drop source routing!



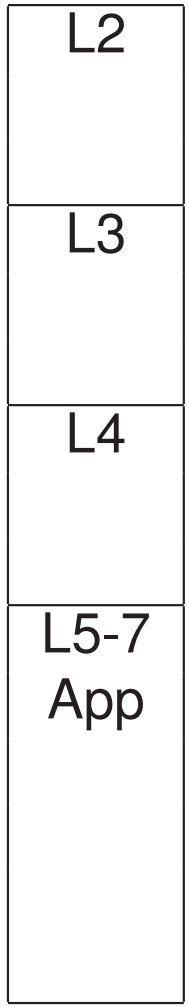
Details on Packet Fields

- Transport Layer (l4) – TCP/UDP
  - Ports
    - Determine the sending / receiving application.
    - Limited degree of confidence
    - Well-Known Ports (0-1023):
      E.g. HTTP (80), DNS (53), HTTPS (443).
    - Registered Ports (1024-49151)
      E.g. IRC (6667), BitTorrent tracker (6969), ...
    - Ephemeral Ports (49151-65535):
      ports meant to be used temporarily by clients.
  - Flags
    - ACK: set in every segment of a connection but the very first
    - SYN: only set in the first two segments
    - RST: ungraceful close of a connection



Details on Packet Fields

- Application Protocol (l5-7)
  - Deep Packet Inspection
  - usually not done by firewalls
  - easier to realize in proxy systems



Stateful Matches

- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
  - (Src IP, Dst IP, Proto, Src Port, Dst Port)

Stateful Matches

- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
  - (Src IP, Dst IP, Proto, Src Port, Dst Port)
- States of a connection
  - NEW: First packet of a connection
  - ESTABLISHED: All following packets

Stateful Matches

- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
  - (Src IP, Dst IP, Proto, Src Port, Dst Port)
- States of a connection
  - NEW: First packet of a connection
  - ESTABLISHED: All following packets
- Optional State tracking (depending on your firewall)
  - TCP sequence and ack numbers, and flags
  - ICMP sequence numbers and request/response tracking

Stateful Matches

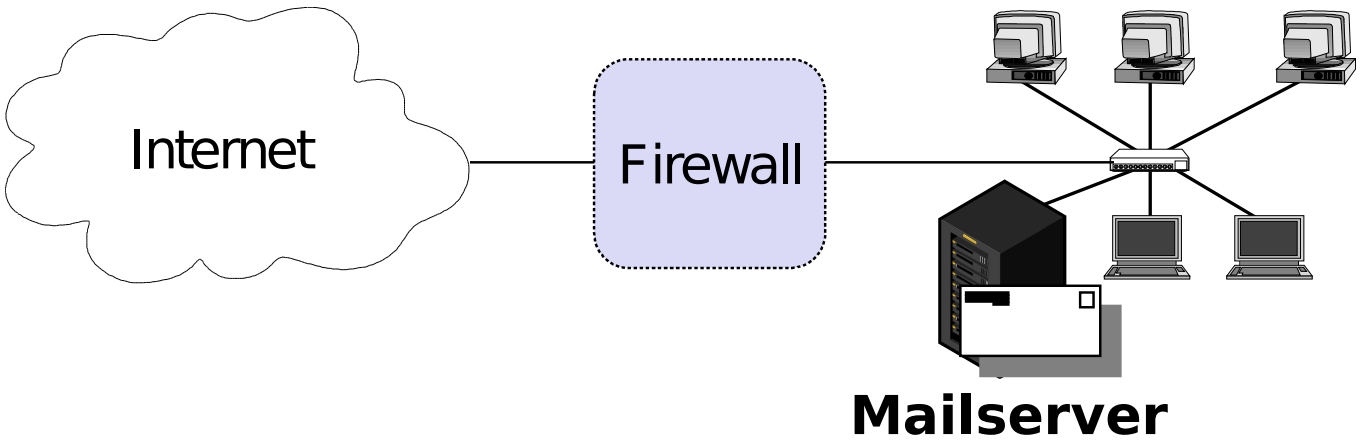
- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
  - (Src IP, Dst IP, Proto, Src Port, Dst Port)
- States of a connection
  - NEW: First packet of a connection
  - ESTABLISHED: All following packets
- Optional State tracking (depending on your firewall)
  - TCP sequence and ack numbers, and flags
  - ICMP sequence numbers and request/response tracking
- Note: UDP connection tracking as always an approximation!

Stateful Matches

- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
  - (Src IP, Dst IP, Proto, Src Port, Dst Port)
- States of a connection
  - NEW: First packet of a connection
  - ESTABLISHED: All following packets
- Optional State tracking (depending on your firewall)
  - TCP sequence and ack numbers, and flags
  - ICMP sequence numbers and request/response tracking
- Note: UDP connection tracking as always an approximation!
  - Example: Attacker sends spoofed DNS replies in the hope that victim might accept one as an answer to a previous DNS query.

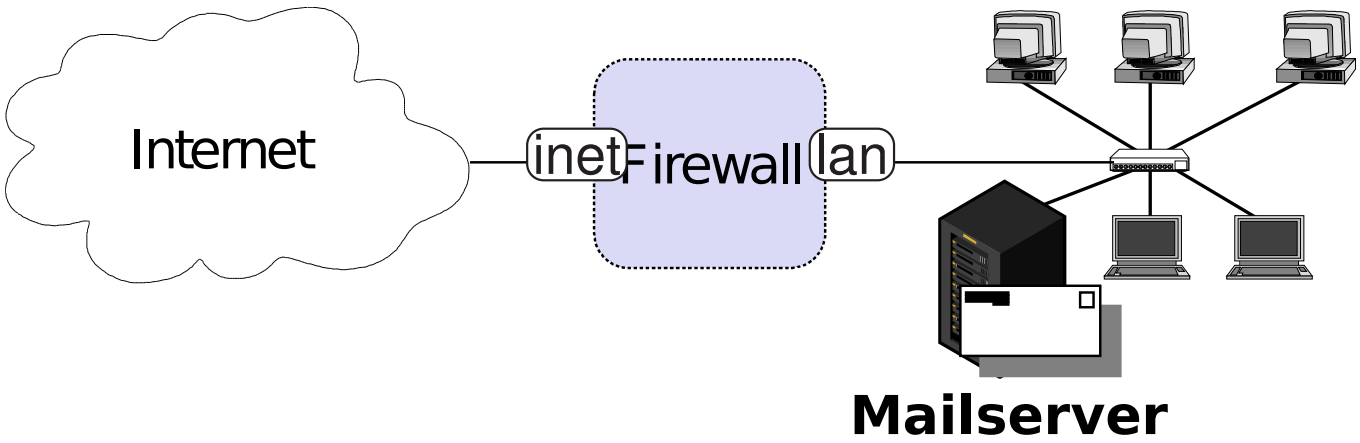
Example: LAN with Mail Server

Example: LAN with Mail Server



- Security policy
  - Incoming and outgoing email should be the only allowed traffic into and out of a protected network
  - Email is SMTP, TCP port 25
  - Anyone in the internal network can send out emails to arbitrary mailservers in the Internet
  - Incoming emails must only arrive at the Mailserver

Example: LAN with Mail Server



- Security policy
  - Incoming and outgoing email should be the only allowed traffic into and out of a protected network
  - Email is SMTP, TCP port 25
  - Anyone in the internal network can send out emails to arbitrary mailservers in the Internet
  - Incoming emails must only arrive at the Mailserver

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
⇒A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
⇒B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
⇒C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
⇒D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	*	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)
- Any difference?

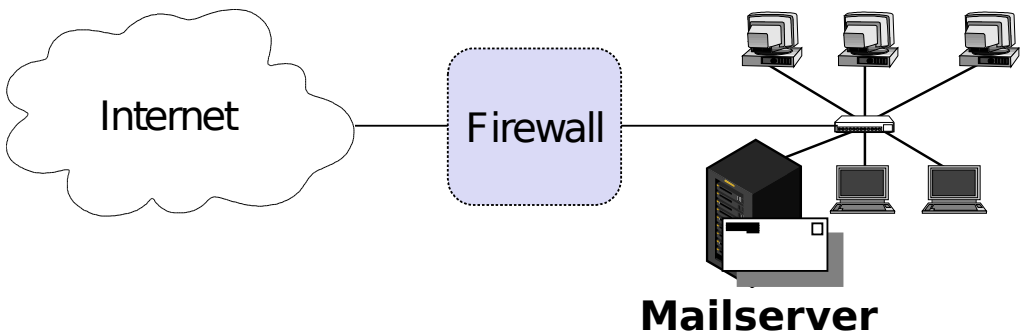
Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	*	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mailserver
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)
- Any difference? No, only TCP can get get into Est. state!

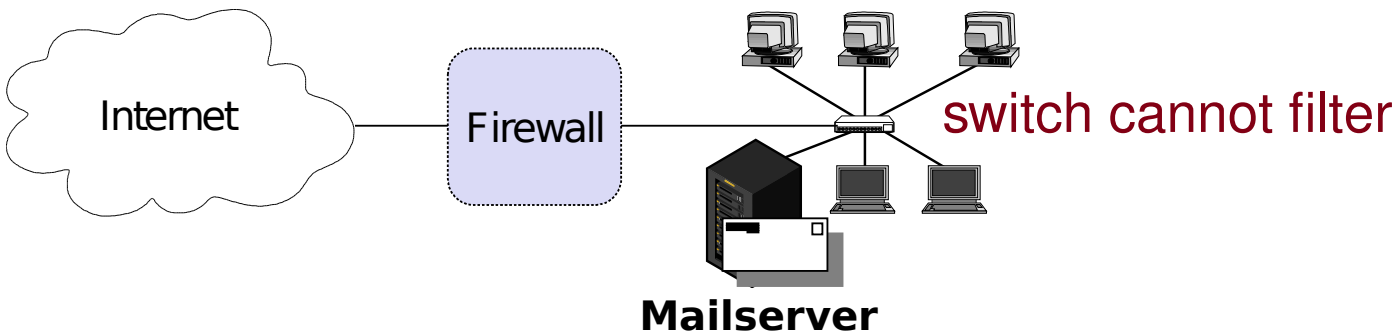
Example: LAN with Mail Server – Discussion

- Can we do better?
  - Internal hosts can establish connections to the Mailserver
- Can we prevent his?



Example: LAN with Mail Server – Discussion

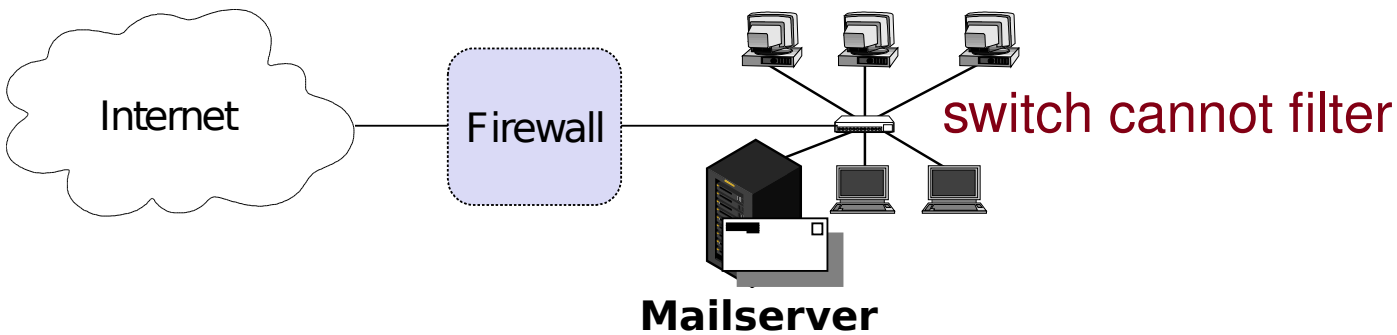
- Can we do better?
  - Internal hosts can establish connections to the Mailserver
- Can we prevent his?
  - No! The firewall cannot intercept these connections, attributable to the network topology.



- This subverts the security policy

Example: LAN with Mail Server – Discussion

- Can we do better?
  - Internal hosts can establish connections to the Mailserver
- Can we prevent his?
  - No! The firewall cannot intercept these connections, attributable to the network topology.



- This subverts the security policy
- Simple fix 1: Check the security requirements, update the policy
- Simple fix 2: Replace the internal switch by a second firewall

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.
  - No!

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.
  - No!
  - Assume an internal host sends out a TCP packet with source and destination port 25 to `shadymail.example`

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.
  - No!
  - Assume an internal host sends out a TCP packet with source and destination port 25 to `shadymail.example`
  - Rule B establishes a new state in the firewall.

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.
  - No!
  - Assume an internal host sends out a TCP packet with source and destination port 25 to `shadymail.example`
  - Rule B establishes a new state in the firewall.
  - Now, for `shadymail.example`, using source port 25, the internal host is reachable on the well-known port 25!

Example: LAN with Mail Server – Possible Weaknesses

- In the range of the well-known ports, is Mailserver on TCP dest. port 25 (incoming) the only entity which can exchange traffic with the Internet?
- Assume we are `tcpdump`ing on the firewall.
  - No!
  - Assume an internal host sends out a TCP packet with source and destination port 25 to `shadymail.example`
  - Rule B establishes a new state in the firewall.
  - Now, for `shadymail.example`, using source port 25, the internal host is reachable on the well-known port 25!
  - Fix: make sure that only source ports $>$ 1023 are allowed to establish a connection

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	*	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

Example: LAN with Mail Server

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	> 1023	25	New	Accept
B	lan	internal	external	TCP	> 1023	25	New	Accept
C	*	*	*	*	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

Example: LAN with Mail Server – Tuning

- Firewall rules are matched sequentially
- Few packets will establish a new connection
- Many packets will use an established connection
- Move rule C to the front
- A connection can only be in ESTABLISHED state by rule A and B, the transformation preserves the semantics

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
C	*	*	*	*	*	*	Est.	Accept
A	inet	external	mailserver	TCP	> 1023	25	New	Accept
B	lan	internal	external	TCP	> 1023	25	New	Accept
D	*	*	*	*	*	*	*	Drop

Best Practice: Put the ESTABLISHED rule first

- Performance
  - Our firewall (September 2014)
  - $>$ 15 billion packets, 19+ Terabyte data since the last reboot
  - $>$ 95% of all packets match the ESTABLISHED rule
- Management
  - First rule: “enable stateful matching”
  - All following rules: Access control list

Stateless Filtering

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.
- Only few rules: stateless filtering may be faster
  - $\mathcal{O}$(# rules)

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.
- Only few rules: stateless filtering may be faster
  - $\mathcal{O}$(# rules)
- Many rules: statefull filtering may be faster
  - Majority matches first rule, $\mathcal{O}(1)$ lookup

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.
- Only few rules: stateless filtering may be faster
  - $\mathcal{O}$(# rules)
- Many rules: statefull filtering may be faster
  - Majority matches first rule, $\mathcal{O}(1)$ lookup
  - Possible DOS attacks
    - sending packets which need $\mathcal{O}$(# rules) processing
    - Filling the state table

Stateless Firewalls

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.
- Only few rules: stateless filtering may be faster
  - $\mathcal{O}$(# rules)
- Many rules: statefull filtering may be faster
  - Majority matches first rule, $\mathcal{O}(1)$ lookup
  - Possible DOS attacks
    - sending packets which need $\mathcal{O}$(# rules) processing
    - Filling the state table
- Many network boxes have stateless firewall features embedded
  - Router access lists
  - Some switches
  - ...

Statefull vs. Stateless Firewalls

- Rule of thumb

Statefull vs. Stateless Firewalls

- Rule of thumb
- Stateless firewalls are more complex to configure

Statefull vs. Stateless Firewalls

- Rule of thumb
- Stateless firewalls are more complex to configure
- Which makes configuration errors more likely

Statefull vs. Stateless Firewalls

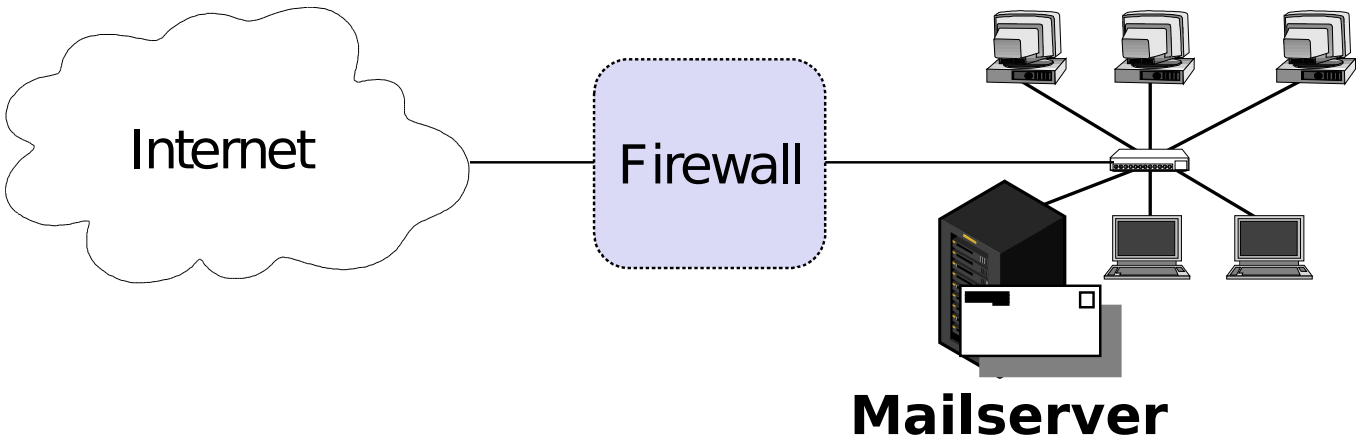
- Rule of thumb
- Stateless firewalls are more complex to configure
- Which makes configuration errors more likely
- Whenever possible, go for the statefull firewall!

Statefull vs. Stateless Firewalls

- Rule of thumb
- Stateless firewalls are more complex to configure
- Which makes configuration errors more likely
- Whenever possible, go for the statefull firewall!
- Hardware is cheap

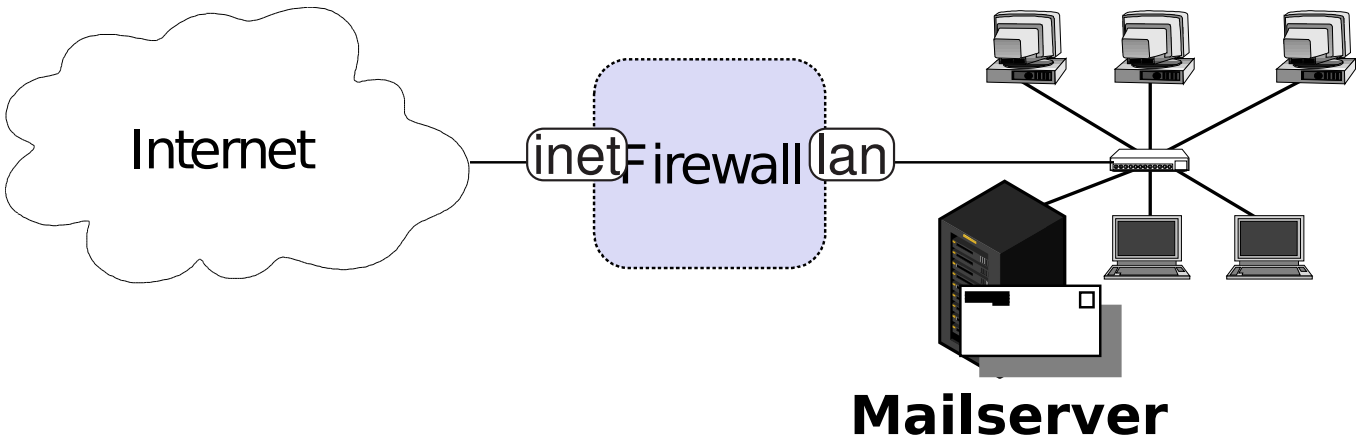
Example: LAN with Mail Server Stateless

Example: LAN with Mail Server – Stateless



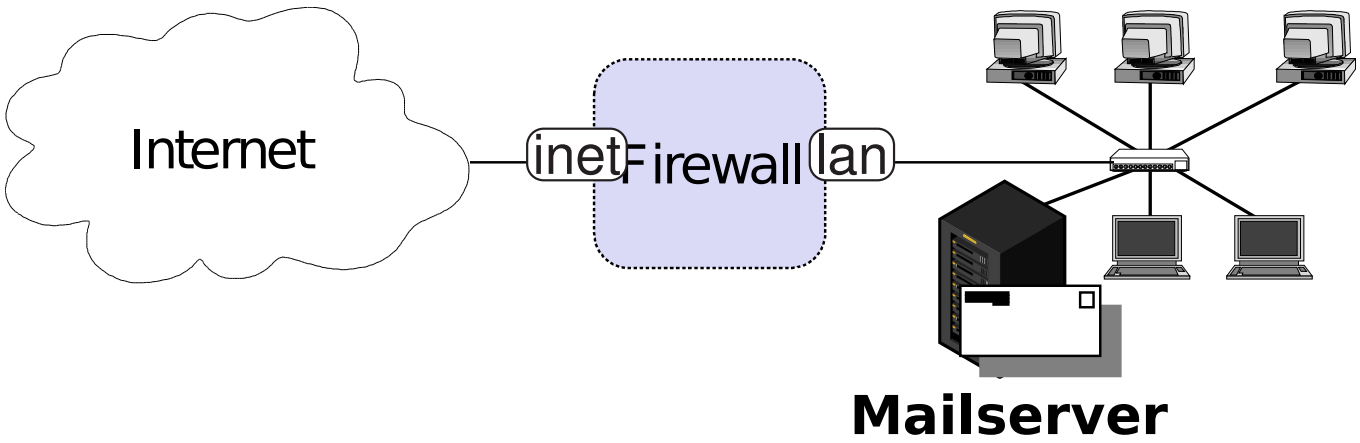
- Security policy
  - Incoming and outgoing email should be the only allowed traffic into and out of a protected network
  - Email is SMTP, TCP port 25
  - Anyone in the internal network can send out emails to arbitrary mailservers in the Internet
  - Incoming emails must only arrive at the Mailserver

Example: LAN with Mail Server – Stateless



- Security policy
  - Incoming and outgoing email should be the only allowed traffic into and out of a protected network
  - Email is SMTP, TCP port 25
  - Anyone in the internal network can send out emails to arbitrary mailservers in the Internet
  - Incoming emails must only arrive at the Mailserver

Example: LAN with Mail Server – Stateless



- Security policy
  - Incoming and outgoing email should be the only allowed traffic into and out of a protected network
  - Email is SMTP, TCP port 25
  - Anyone in the internal network can send out emails to arbitrary mailservers in the Internet
  - Incoming emails must only arrive at the Mailserver

Example: LAN with Mail Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	*	25		Accept
A_2	lan	mailserver	external	TCP	*	$>$ 1023		Accept
B_1	lan	internal	external	TCP	*	25		Accept
B_2	inet	external	internal	TCP	*	$>$ 1023		Accept
C	*	*	*	*	*	*		Drop

- Rule A_1 allows incoming email to enter the network.
  Rule A_2 allows the mailserver's answers to exit the network.
- Rules B_2 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Example: LAN with Mail Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
$\Rightarrow A_1$	inet	external	mailserver	TCP	*	25		Accept
$\Rightarrow A_2$	lan	mailserver	external	TCP	*	$>$ 1023		Accept
B_1	lan	internal	external	TCP	*	25		Accept
B_2	inet	external	internal	TCP	*	$>$ 1023		Accept
C	*	*	*	*	*	*		Drop

- Rule A_1 allows incoming email to enter the network.
  Rule A_2 allows the mailserver's answers to exit the network.
- Rules B_2 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Example: LAN with Mail Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	*	25		Accept
A_2	lan	mailserver	external	TCP	*	$>$ 1023		Accept
$\Rightarrow B_1$	lan	internal	external	TCP	*	25		Accept
$\Rightarrow B_2$	inet	external	internal	TCP	*	$>$ 1023		Accept
C	*	*	*	*	*	*		Drop

- Rule A_1 allows incoming email to enter the network.
  Rule A_2 allows the mailserver's answers to exit the network.
- Rules B_2 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Example: LAN with Mail Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	*	25		Accept
A_2	lan	mailserver	external	TCP	*	$>$ 1023		Accept
B_1	lan	internal	external	TCP	*	25		Accept
B_2	inet	external	internal	TCP	*	$>$ 1023		Accept
$\Rightarrow$C	*	*	*	*	*	*		Drop

- Rule A_1 allows incoming email to enter the network.
  Rule A_2 allows the mailserver's answers to exit the network.
- Rules B_2 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Example: LAN with Mail Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	*	25		Accept
A_2	lan	mailserver	external	TCP	*	$>$ 1023		Accept
B_1	lan	internal	external	TCP	*	25		Accept
B_2	inet	external	internal	TCP	*	$>$ 1023		Accept
C	*	*	*	*	*	*		Drop

- Rule A_1 allows incoming email to enter the network.
  Rule A_2 allows the mailserver's answers to exit the network.
- Rules B_2 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Discussion

- Packets with spoofed IP addresses
  - Inbound packets must have an external source address
    Rules A_1 and B_2
    $\longrightarrow$ successfully blocked
  - Same for outbound packets; Rules A_2 and B_1
- Telnet traffic
  - telnet server: TCP port 23
  - Allowed inbound traffic must be to port 25 or port $>$ 1023
    $\longrightarrow$ incoming packets to initiate telnet connection blocked
  - Same for outgoing telnet connections

Discussion – A possible attack

- Ruleset does not block the X11-protocol for the Mailserver
  - X11-server listens at port 6000, clients use port numbers > 1023
  - X11-protocol allows reading/manipulating the display and keystrokes
  - Incoming X11-request is not blocked (Rule B_2)
  - neither is any answer (Rule A_2)

Example: LAN with Mail Server – Fix # 1

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	> 1023	25		Accept
A_2	lan	mailserver	external	TCP	25	> 1023		Accept
B_1	lan	internal	external	TCP	> 1023	25		Accept
B_2	inet	external	internal	TCP	25	> 1023		Accept
C	*	*	*	*	*	*		Drop

- Fixing the flaw: include source ports
  - Outbound traffic to ports > 1023 only allowed if the source port is 25 (Rule A_2)
    $\longrightarrow$ traffic from internal X-clients or -servers blocked
  - Same for inbound traffic to ports > 1023 (Rule B_2)
- Fix the attack: use non-standard port 25 for attacking X-client
  - Firewall will let this traffic pass

Example: LAN with Mail Server – Fix # 2

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	> 1023	25	*	Accept
A_2	lan	mailserver	external	TCP	25	> 1023	Yes	Accept
B_1	lan	internal	external	TCP	> 1023	25	*	Accept
B_2	inet	external	internal	TCP	25	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- Checking whether the TCP ACK flag is set
- ACK flag not set is required for establishing new connection
  - C.f. TCP 3-way handshake
- Rule of thumb: ACK $\approx$ not NEW

Stateless filtering – The ACK flag

- ACK flag: approximate the state of TCP connections
- Assumes that information in packets can be trusted
  - Attacker could send SYN/ACK as initial packet
  - Passes the firewall.
  - Hosts will ignore it .

Stateless filtering – The ACK flag

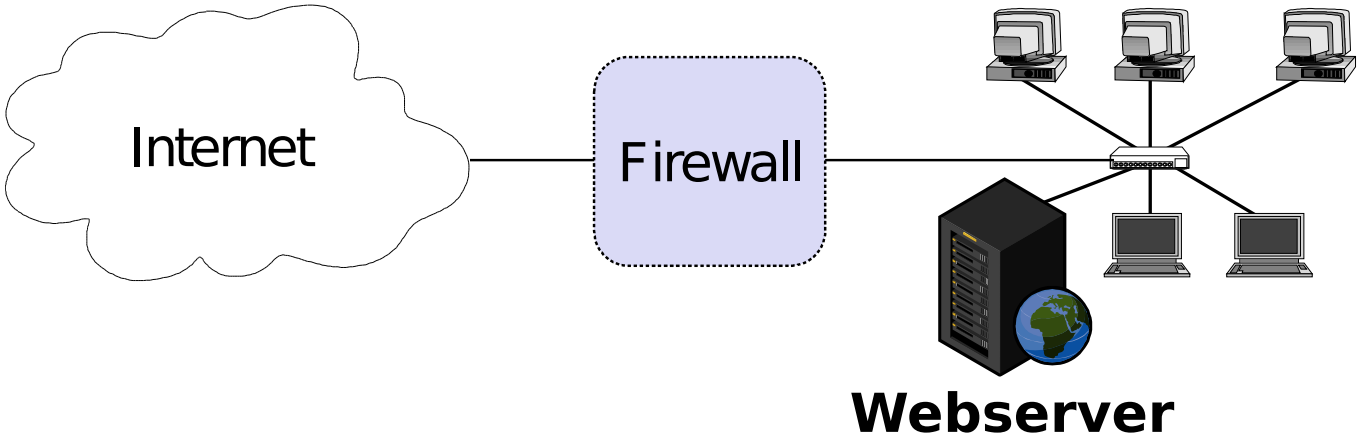
- ACK flag: approximate the state of TCP connections
- Assumes that information in packets can be trusted
  - Attacker could send SYN/ACK as initial packet
  - Passes the firewall.
  - Hosts will ignore it if they don’t have a flaw int their network stack.

Stateless filtering – The ACK flag

- ACK flag: approximate the state of TCP connections
- Assumes that information in packets can be trusted
  - Attacker could send SYN/ACK as initial packet
  - Passes the firewall.
  - Hosts will ignore it if they don’t have a flaw int their network stack.
- Protocols such as UDP don’t have state information
  - Not possible to differentiate between initiator and responder.
  - UDP has no ACK field: Always set ACK to *

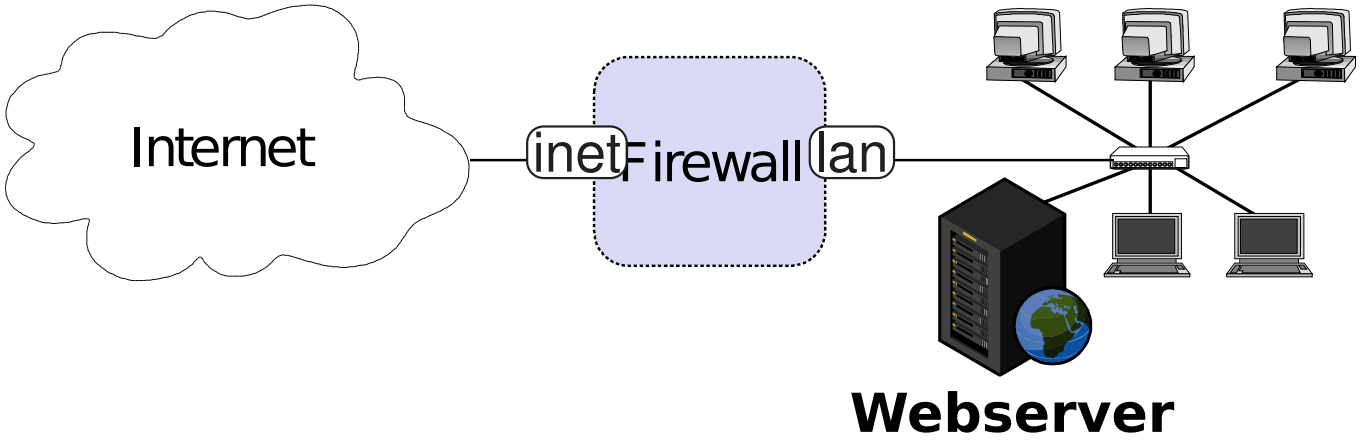
Example: LAN with Web Server

Example: LAN with Web Server



- Security policy
  - Allow HTTP traffic initiated by external hosts to webserver
  - Allow internal hosts to initiate HTTP and DNS
    - HTTP: TCP port 80
    - DNS: UDP port 53
  - Do not allow other communication, in particular no communication initiated by external hosts to the local hosts other than the webserver.

Example: LAN with Web Server



- Security policy
  - Allow HTTP traffic initiated by external hosts to webserver
  - Allow internal hosts to initiate HTTP and DNS
    - HTTP: TCP port 80
    - DNS: UDP port 53
  - Do not allow other communication, in particular no communication initiated by external hosts to the local hosts other than the webserver.

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action

- First rule?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept

- First rule?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	$>$ 1023	80	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	$>$ 1023	80	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	> 1023	80	New	Accept
C	lan	internal	external	TCP	> 1023	80	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	> 1023	80	New	Accept
C	lan	internal	external	TCP	> 1023	80	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	>1023	80	New	Accept
C	lan	internal	external	TCP	>1023	80	New	Accept
D	lan	internal	external	UDP	>1023	53	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	$>$ 1023	80	New	Accept
C	lan	internal	external	TCP	$>$ 1023	80	New	Accept
D	lan	internal	external	UDP	$>$ 1023	53	New	Accept

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?
- Do not allow other communication ... ?

Example: LAN with Web Server – Stafefull

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	$>$ 1023	80	New	Accept
C	lan	internal	external	TCP	$>$ 1023	80	New	Accept
D	lan	internal	external	UDP	$>$ 1023	53	New	Accept
E	*	*	*	*	*	*	*	Drop

- First rule?
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?
- Do not allow other communication ... ?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action

- A first rule comparable to the stateful case?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action

- A first rule comparable to the stateful case? No.

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	> 1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	> 1023	Yes	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	> 1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	> 1023	Yes	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	> 1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	> 1023	Yes	Accept
C_1	lan	internal	external	TCP	> 1023	80	*	Accept
C_2	inet	external	internal	TCP	80	> 1023	Yes	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	> 1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	> 1023	Yes	Accept
C_1	lan	internal	external	TCP	> 1023	80	*	Accept
C_2	inet	external	internal	TCP	80	> 1023	Yes	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	>1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	>1023	Yes	Accept
C_1	lan	internal	external	TCP	>1023	80	*	Accept
C_2	inet	external	internal	TCP	80	>1023	Yes	Accept
D_1	lan	internal	external	UDP	>1023	53	-	Accept
D_2	inet	external	internal	UDP	53	>1023	-	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	> 1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	> 1023	Yes	Accept
C_1	lan	internal	external	TCP	> 1023	80	*	Accept
C_2	inet	external	internal	TCP	80	> 1023	Yes	Accept
D_1	lan	internal	external	UDP	> 1023	53	-	Accept
D_2	inet	external	internal	UDP	53	> 1023	-	Accept

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?
- Do not allow other communication ... ?

Example: LAN with Web Server – Stateless

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B_1	inet	external	webserver	TCP	>1023	80	*	Accept
B_2	lan	webserver	external	TCP	80	>1023	Yes	Accept
C_1	lan	internal	external	TCP	>1023	80	*	Accept
C_2	inet	external	internal	TCP	80	>1023	Yes	Accept
D_1	lan	internal	external	UDP	>1023	53	-	Accept
D_2	inet	external	internal	UDP	53	>1023	-	Accept
E	*	*	*	*	*	*	*	Drop

- A first rule comparable to the stateful case? No.
- Allow HTTP traffic initiated by external hosts to webserver?
- Allow internal hosts to initiate HTTP? and DNS?
- Do not allow other communication ... ?

Spoofing Protection

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don’t be an operator who facilitates spoofed DOS attacks to the Internet!

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don’t be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow ‘valid’ source IPs

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don’t be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow ‘valid’ source IPs
  - For a varying definition of ‘valid’

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don’t be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow ‘valid’ source IPs
  - For a varying definition of ‘valid’
  - IPs which belong to you are not valid

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don’t be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow ‘valid’ source IPs
  - For a varying definition of ‘valid’
  - IPs which belong to you are not valid
  - Local and special purpose IPs are not valid

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don't be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow 'valid' source IPs
  - For a varying definition of 'valid'
  - IPs which belong to you are not valid
  - Local and special purpose IPs are not valid
  - Rule of thumb: $\mathrm{UNIV} \setminus (\mathrm{Your\ IPs} \cup \mathrm{Special\ Purpose\ IPs})$

Spoofing Protection

- Outgoing (to the Internet)
  - Only allow source IPs which belong to you
  - Don't be an operator who facilitates spoofed DOS attacks to the Internet!
- Incoming (from the Internet)
  - Only allow 'valid' source IPs
  - For a varying definition of 'valid'
  - IPs which belong to you are not valid
  - Local and special purpose IPs are not valid
  - Rule of thumb: $\mathrm{UNIV} \setminus (\mathrm{Your\ IPs} \cup \mathrm{Special\ Purpose\ IPs})$
- Spoofing must always be filtered close to the source. Why?

Example: Spoofing Protection

- Assume your institutions owns 131.159.20.0/24

Rule	Iface	Src IP	Dst IP	Action
A	lan	! 131.159.20.0/24	*	Drop
B	inet	131.159.20.0/24	*	Drop
B	inet	192.168.0.0/16	*	Drop
B	inet	10.0.0.0/8	*	Drop
B	inet	172.16.0.0/12	*	Drop
B	*	*	*	Accept

- There are more addresses you might want to drop [RFC6890]

Automatic Spoofing Protection

- The Linux kernel offers some spoofing protection for free
- `/proc/sys/net/ipv4/conf/all/rp_filter`
- If a packet arrives at interface *i*, the kernel checks
  - Is the source IP of the packet reachable through *i*
  - If not, drop the packet
- Only considers local routing and interface configuration

Common Errors

Common Errors

- How is your firewall management interface reachable?
  - From the Internet? From the complete internal network?
  - Via telenet? Via UPnP?
- What is allowed over the Internet?
  - NetBIOS? NFS? RPC? Telnet?
  - Other ICMP than Unreachable, Fragmentation Needed, TTL Exceeded, Ping?
  - IP header options?
- IPv4 and IPv6?
  - Are the rule sets compliant?
- Outbound rule ANY? (c.f. spoofing)
  - Even private IP ranges or IP ranges that don't belong to you?
- Policy's vs. Firewalls understanding of Inbound and Outbound?
  - If `eth0` is your internal interface and the firewall says inbound on eth0, policy might say outbound.

Shadowing

"refers to the case where all the packets one rule intends to deny (accept) have been accepted (denied) by preceding rules"
[fireman06]

Rule	Iface	Src IP	Dst IP	Action
A	*	*	192.168.0.0/16	Accept
B	*	*	192.168.42.0/24	Drop

- Rule B will never match!

Another Example

- No spoofing for the following networks:
  - eth0 $\longleftrightarrow$ 10.0.0.0/16
  - eth1 $\longleftrightarrow$ 10.1.0.0/16
  - eth2 $\longleftrightarrow$ 10.2.0.0/16
- Accessible by all three networks: 10.1.1.1

Rule	Iface	Src IP	Dst IP	Action
A	eth0	! 10.0.0.0/16	*	Drop
B	eth1	! 10.1.0.0/16	*	Drop
C	*	*	10.1.1.1	Accept
D	eth2	! 10.2.0.0/16	*	Drop
E	*	*	*	Drop

- Correct?

Another Example

- No spoofing for the following networks:
  - eth0 $\longleftrightarrow$ 10.0.0.0/16
  - eth1 $\longleftrightarrow$ 10.1.0.0/16
  - eth2 $\longleftrightarrow$ 10.2.0.0/16
- Accessible by all three networks: 10.1.1.1

Rule	Iface	Src IP	Dst IP	Action
A	eth0	! 10.0.0.0/16	*	Drop
B	eth1	! 10.1.0.0/16	*	Drop
C	*	*	10.1.1.1	Accept
D	eth2	! 10.2.0.0/16	*	Drop
E	*	*	*	Drop

- Correct?
- Anyone at eth2 can send spoofed packets to 10.1.1.1

Another Example

- No spoofing for the following networks:
  - eth0 $\longleftrightarrow$ 10.0.0.0/16
  - eth1 $\longleftrightarrow$ 10.1.0.0/16
  - eth2 $\longleftrightarrow$ 10.2.0.0/16
- Accessible by all three networks: 10.1.1.1

Rule	Iface	Src IP	Dst IP	Action
A	eth0	! 10.0.0.0/16	*	Drop
B	eth1	! 10.1.0.0/16	*	Drop
C	*	*	10.1.1.1	Accept
D	eth2	! 10.2.0.0/16	*	Drop
E	*	*	*	Drop

- Correct?
- Anyone at eth2 can send spoofed packets to 10.1.1.1
- Rule D is partly shadowed

What Firewalls can not do

A firewall

- can’t protect against malicious insiders

What Firewalls can not do

A firewall

- can’t protect against malicious insiders
- can’t protect against connections that don’t go through it

What Firewalls can not do

A firewall

- can’t protect against malicious insiders
- can’t protect against connections that don’t go through it
- can’t protect against completely new threats

What Firewalls can not do

A firewall

- can’t protect against malicious insiders
- can’t protect against connections that don’t go through it
- can’t protect against completely new threats
- can’t fully protect against viruses

What Firewalls can not do

A firewall

- can’t protect against malicious insiders
- can’t protect against connections that don’t go through it
- can’t protect against completely new threats
- can’t fully protect against viruses
- does not perform cryptographic operations, e.g. message authentication

What Firewalls can not do

A firewall

- can't protect against malicious insiders
- can't protect against connections that don't go through it
- can't protect against completely new threats
- can't fully protect against viruses
- does not perform cryptographic operations, e.g. message authentication
- can't set itself up correctly

Bastion Hosts

Bastion Hosts

- Definition:

  "*A bastion host is a host that is more exposed to the hosts of an external network than the other hosts of the network it protects.*"

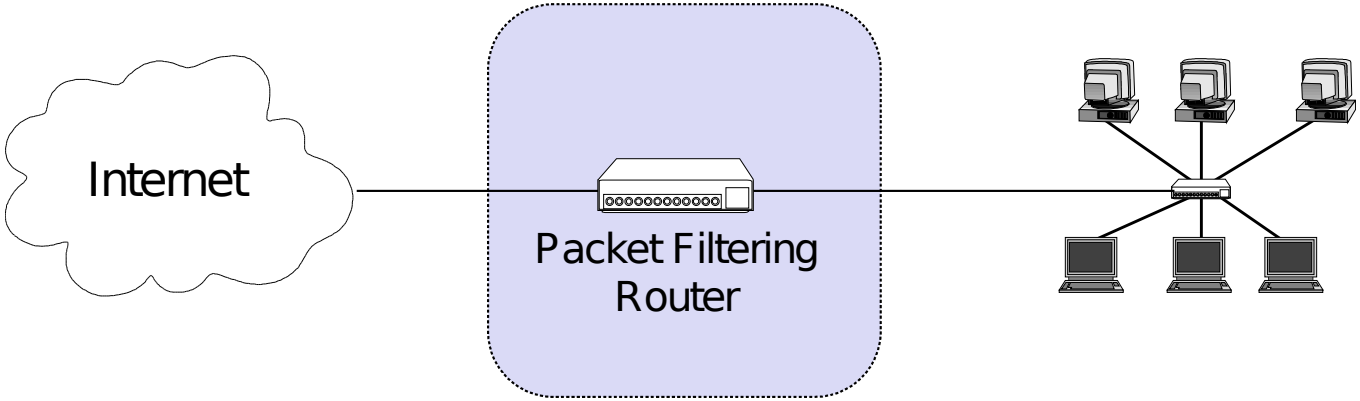
- A bastion host may serve for different purposes:
  - Packet filtering
  - Providing proxy services
  - A combination of both

Securing Bastion Hosts

- Keep it simple
- Prepare for the bastion host to be compromised
- Connect in such a way that it cannot sniff internal traffic
- Extensive and tamper-resistant logging
- Reliable hardware configuration and physically secure location
- Disable ssh password login (only public key login)
- Disable user accounts
- Monitor the machine closely (reboots, usage / load patterns, etc.)
- Regular backups

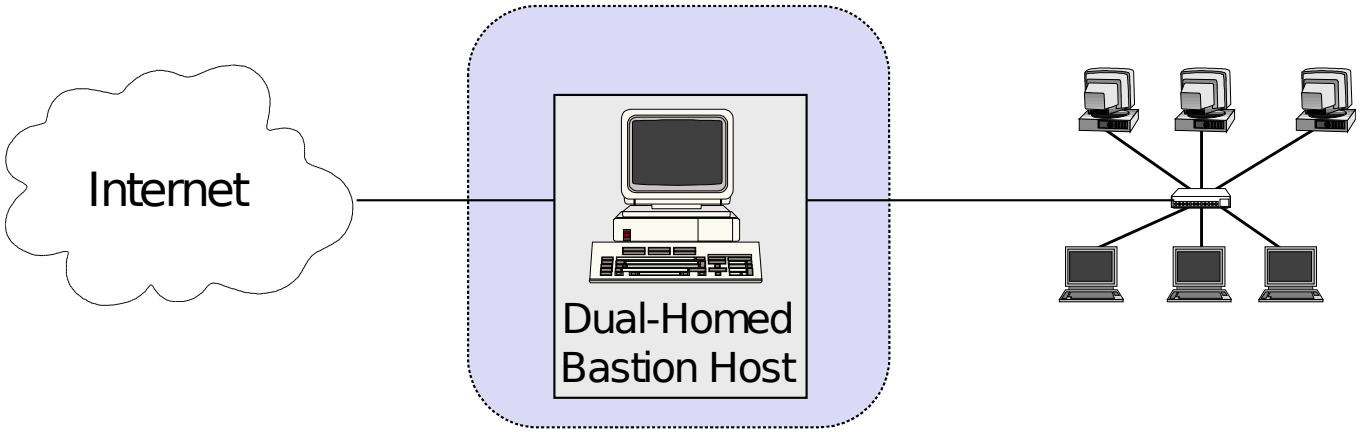
Firewall Architectures

Simple Packet Filter Architecture



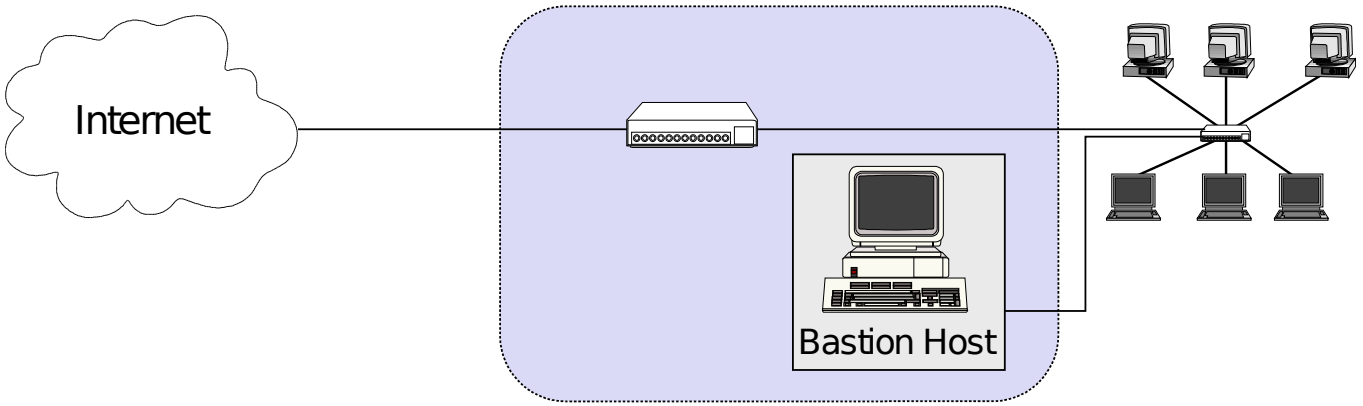
- A packet filtering router or firewall with two interfaces

Dual-Homed Host Architecture



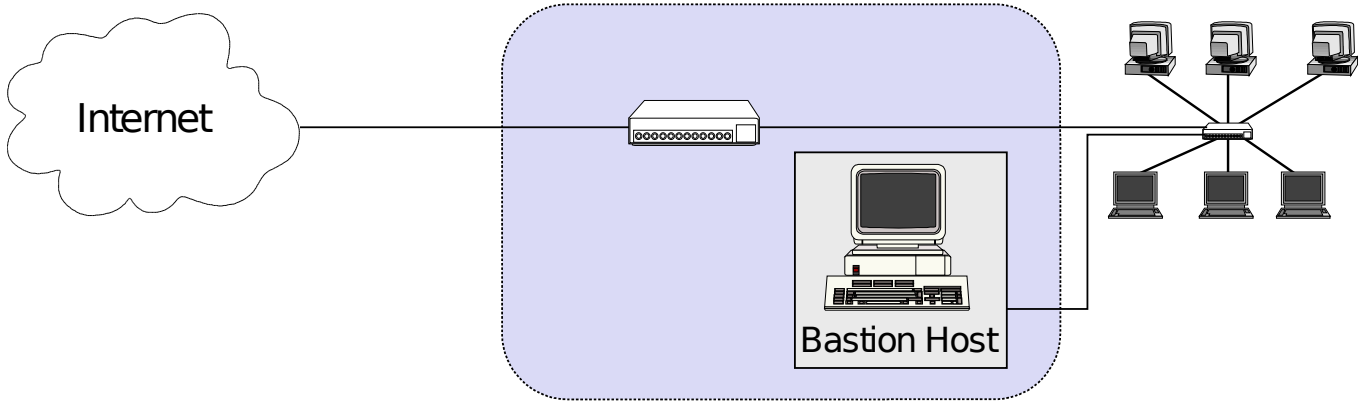
- Dual-Homed: Host is part of two networks (has two NICs)
- Bastion Host is Firewall + Application Proxy
- Drawbacks
  - Bastion Host is bottleneck
  - Compromised Bastion Host is worst-case scenario

Screened Host Architecture



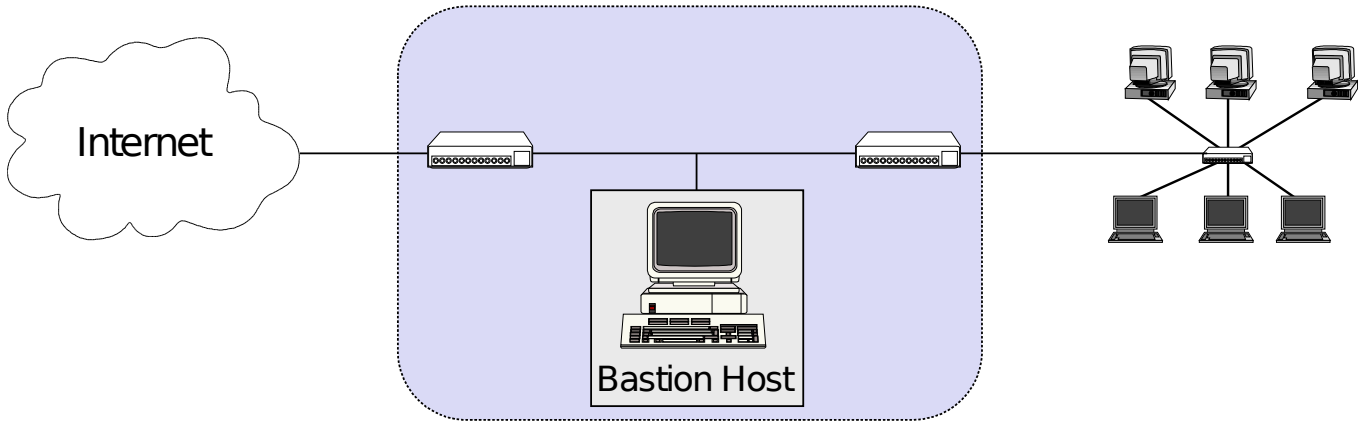
- Packet filter protects network an Bastion Host
- Bastion Host is Proxy (may be accessible from the Internet)
  - Compromised Bastion Host compromises the internal network

Screened Host Architecture



- Packet filter protects network an Bastion Host
- Bastion Host is Proxy (may be accessible from the Internet)
  - Compromised Bastion Host compromises the internal network
- If you have a home server and configured port-forwarding on your router, this is probably your architecture

Screened Subnet Architecture – DMZ



- Demilitarized Zone (DMZ): perimeter network
- Hosts Bastion Host (Proxy) and publicly accessible servers
- Second packet filter in case they are compromised
  $\longrightarrow$ Protection for the internal network
- Requires two firewalls or one firewall with at least 3 NICs

Literature

- M. Bishop. *What is computer security?* Security and Privacy, 2003
- L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra. *FIREMAN: a toolkit for firewall modeling and analysis.* Security and Privacy, 2006
- A. Wool. *A quantitative study of firewall configuration errors.* Computer, IEEE 37(6), 2004, pp. 62 – 67
- `man iptables`
- `man iptables-extensions`
- J. Engelhardt, *Towards the perfect ruleset.* May 2011. `http://inai.de/documents/Perfect_Ruleset.pdf`
- M. Cotton, L. Vegoda, R. Bonica, and B. Haberman, *SpecialPurpose IP Address Registries.* RFC 6890
- *BCP38*, `http://www.bcp38.info/`