



Aalto University

Network Security: Firewalls

Tuomas Aura

CS-E4300 Network security

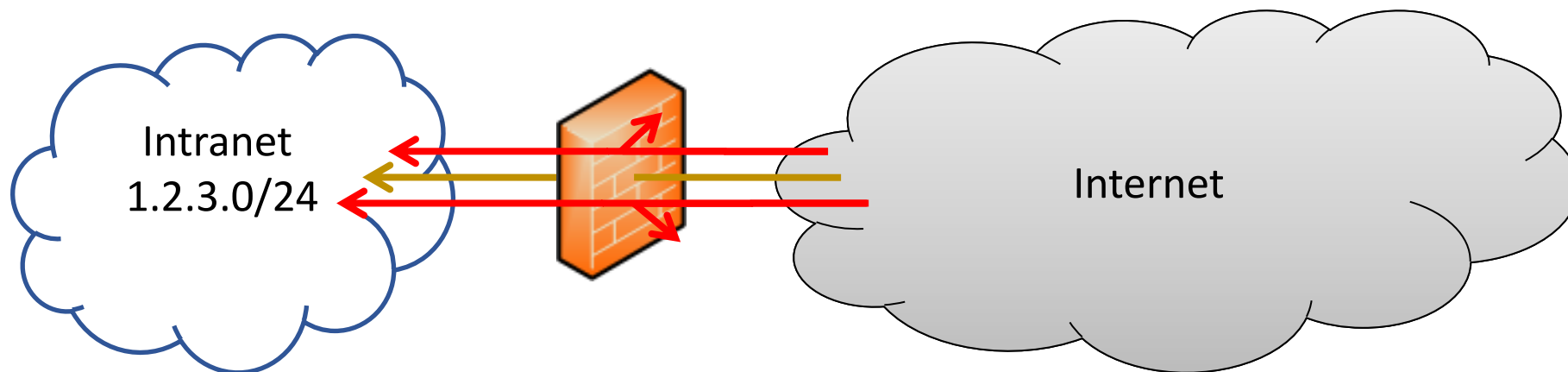
Aalto University



Perimeter defense

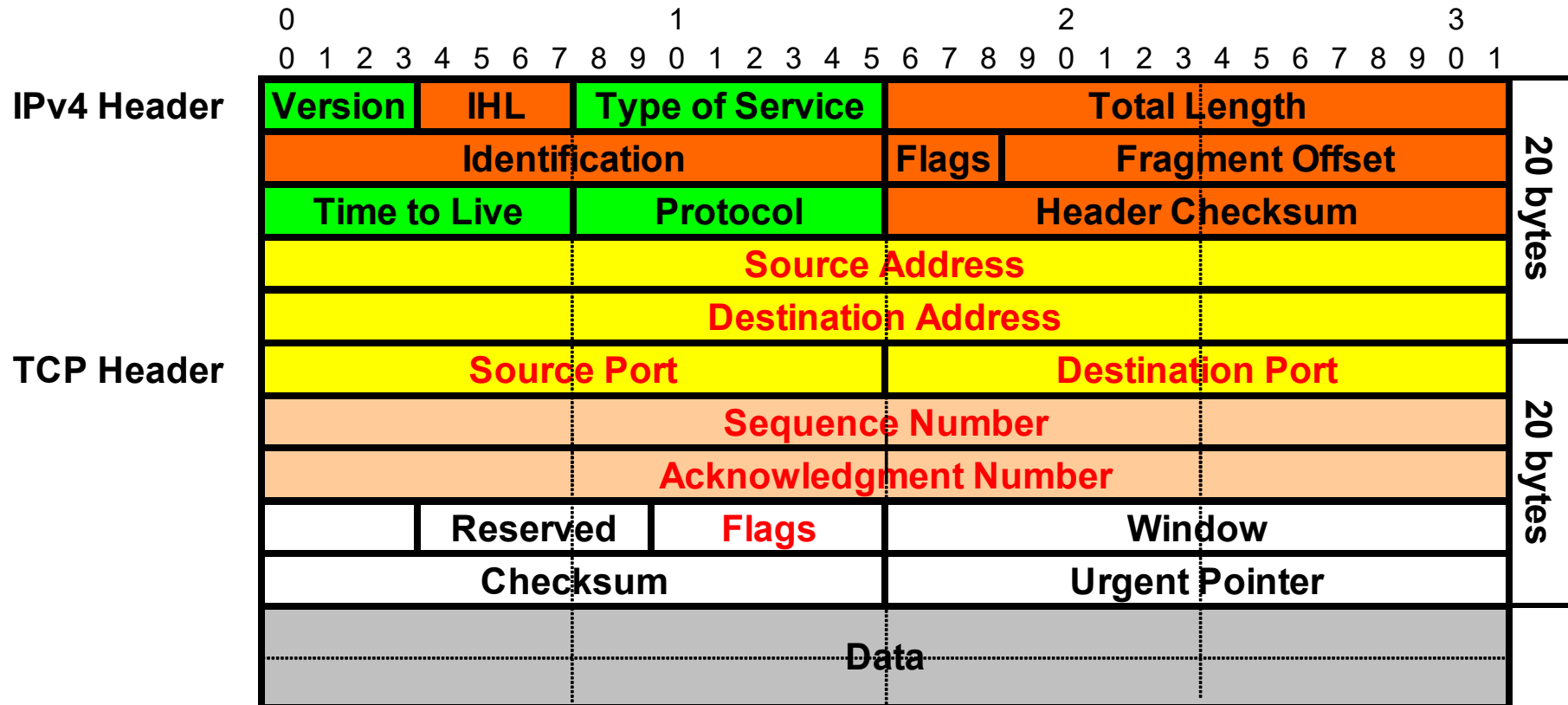
Firewall

- Perimeter defence:
 - Good/safe inside (**intranet**) and bad/dangerous outside (**Internet**)
 - Prevent anything bad from entering the inside
- Drop communication that is dangerous, high risk, or not very unnecessary



- Communication: Ethernet frames, **IP packets**, TCP connections, HTTP request, ...

IPv4 and TCP headers



(TCP flags: CWR ECE URG ACK PSH RST SYN)

- Which field should a firewall use for filtering?

Stateless packet filter

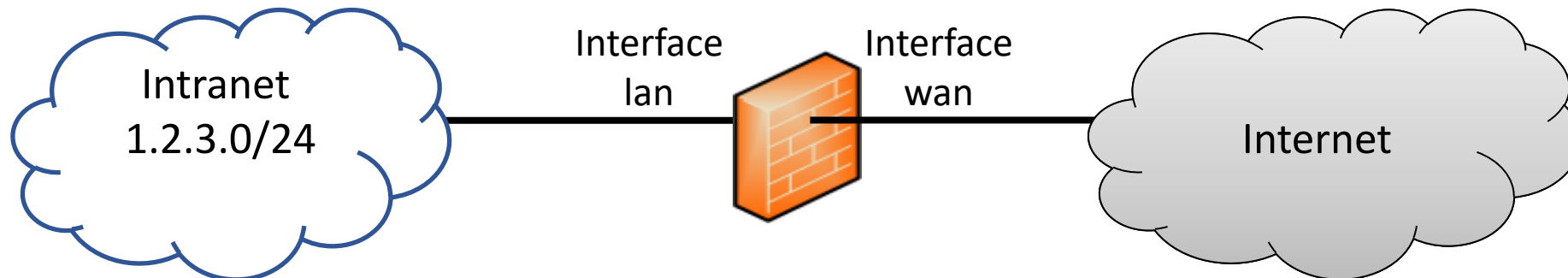
- Pass or Drop IP packets based on their **IP header fields and TCP/UDP port numbers**
 - Protocol (TCP/UDP/ICMP), source and destination IP address, source and destination port, TCP flags, ICMP type and code
- Packet filter is defined as a **rule table**
 - **Rule** consists of **conditions** and an **action**
 - In the rule table, find the **first matching rule** and select its action
- Actions: **pass = allow, accept, permit, bypass** or **drop = block, deny, discard**
 - **Reject** drops the packet and sends an ICMP error message
 - Packet can be logged, e.g., **pass and log** or **drop and log**

Packet filter example (1)

Unrealistic example rule table: inbound email to our SMTP server 1.2.3.10

Input interface	Protocol	Src IP	Src port	Dst IP	Dst port	Flags	Action	Comment
wan	TCP	4.5.6.7	*	1.2.3.10	25		Drop	Stop this spammer
wan	TCP	*	*	1.2.3.10	25		Pass	Inbound SMTP
lan	TCP	1.2.3.10	25	*	*		Pass	SMTP responses
*	*	*	*	*	*		Drop	Default rule

Note: The examples in this lecture are an abstraction and don't directly correspond to any firewall implementation



Packet filter example (2)

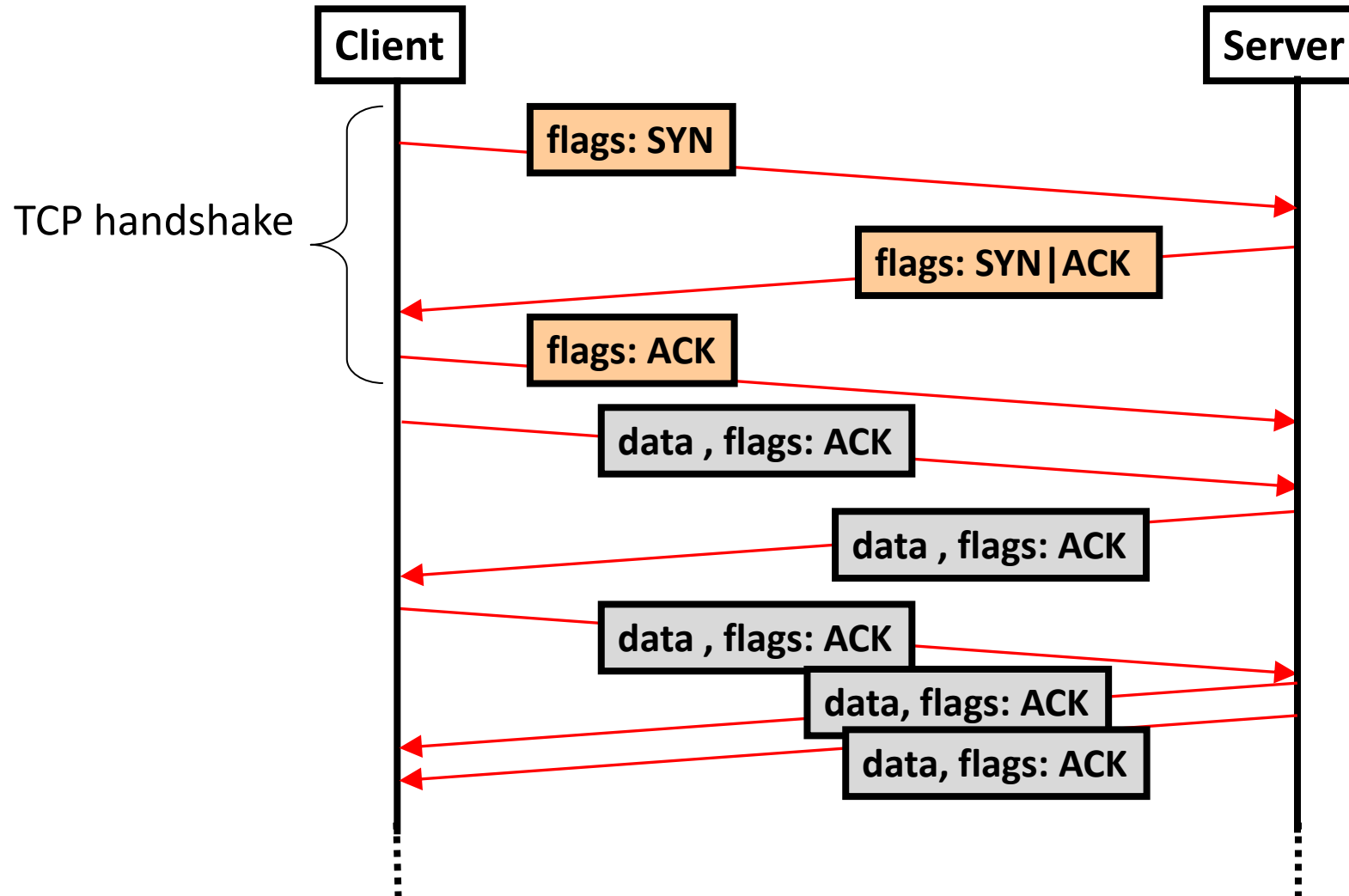
Pass web access from our subnet... not quite right (why?)

Input interface	Protocol	Src IP	Src port	Dst IP	Dst port	Flags	Action	Comment
lan	TCP	1.2.3.0/24	*	*	80		Pass	Outbound HTTP requests
wan	TCP	*	80	1.2.3.0/24	*		Pass	HTTP responses
*	*	*	*	*	*		Drop	Default rule

Slightly more restrictive rules, but still not good:

Input interface	Protocol	Src IP	Src port	Dst IP	Dst port	Flags	Action	Comment
lan	TCP	1.2.3.0/24	≥ 1024	*	80		Pass	Outbound HTTP requests
wan	TCP	*	80	1.2.3.0/24	≥ 1024		Pass	HTTP responses
*	*	*	*	*	*		Drop	Default rule

TCP handshake



Packet filter example (3)

Stateless filter that passes only outbound connections:

Input interface	Protocol	Src IP	Src port	Dst IP	Dst port	Flags	Action	Comment
lan	TCP	1.2.3.0/24	*	*	80		Pass	Outbound HTTP requests
wan	TCP	*	80	1.2.3.0/24	*	ACK	Pass	HTTP responses
*	*	*	*	*	*		Drop	Default rule

All TCP packets, except the first SYN packet, have ACK flag set
→ stateless way to prevent inbound TCP connections

Packet filter example (3)

First even remotely realistic example

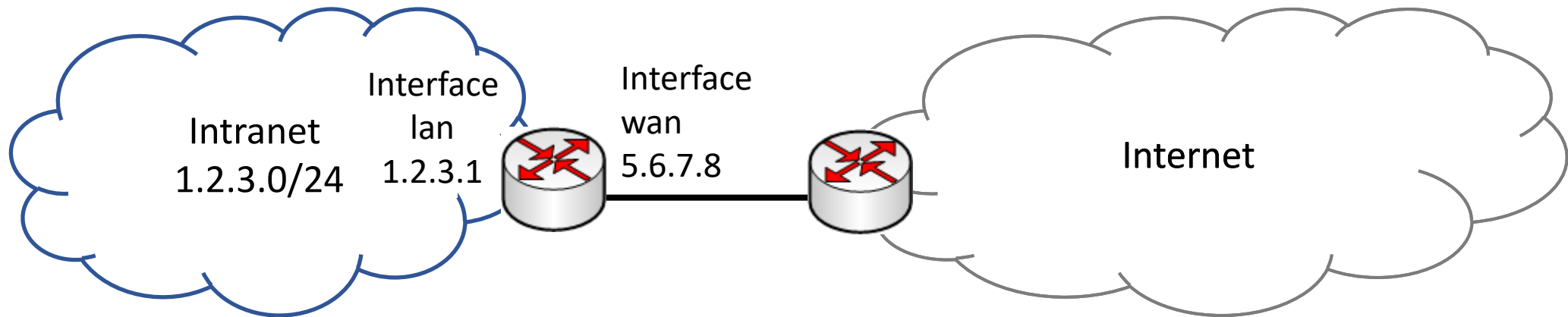
University lab network 1.2.3.0/24
HTTP/Mail/DNS server 1.2.3.10

Input interface	Protocol	Src IP	Src port	Dst IP	Dst port	Flags	Action	Comment
*	UDP	*	*	*	53		Pass	DNS queries in/out
*	UDP	*	53	*	*		Pass	DNS responses
wan	TCP	*	*	1.2.3.10	25		Pass	Inbound SMTP
wan	TCP	*	*	1.2.3.10	80		Pass	Inbound HTTP
lan	TCP	1.2.3.121	*	*	*		Drop	Bob's test machine
wan	TCP	*	*	1.2.3.121	*		Drop	Bob's test machine
wan	TCP	*	*	1.2.3.0/24	22		Pass	Inbound SSH
lan	TCP	1.2.3.0/24	*	*	*		Pass	All outbound TCP
wan	TCP	*	*	1.2.3.0/24	*	ACK	Pass	All TCP responses
*	*	*	*	*	*		Drop	Default rule

Is this correct? How could we drop inbound DNS queries to hosts other than the server?

Router as packet filter

- Firewall rule table is similar to a **routing table**, with some differences:
 - Can match many header fields, not only the destination IP address
 - Can drop some packet, not only forward them
- Most routers can be used as a packet filter
 - Enabling **firewall features may case significantly lower the router throughput**



Ingress and egress (anti-spoofing) filter

- Filter packets with **topologically incorrect source IP addresses** because they are probably spoofed
- **Ingress filtering by local network gateway:**
 - At the gateway router of a local network, drop inbound packets with source addresses that belong to the local network
- **Egress filtering by local network gateway:**
 - At the gateway router of a local network, drop outbound packets with non-local source addresses
- **Ingress filtering by ISP (recommended):**
 - At the gateway router towards a customer, drop packets from the customer if the source address does not belong to the customer
- Egress filtering by ISP (less common)

Anti-spoofing filter example

At our local network's gateway router:

Input interface	Protocol	Src IP	Port	Dst IP	Port	Flags	Action	Comment
lan,wan	*	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	*	*	*		Drop	Unrouteable private addresses
wan	*	1.2.3.0/24	*	*	*		Drop	Ingress filter
wan	*	5.6.7.8	*	*	*		Drop	Router address
wan	*	*	*	*	*		Pass (1)	Ingress filter
lan	*	1.2.3.1	*	*	*		Drop	Router address
lan	*	1.2.3.0/24	*	*	*		Pass (2)	Egress filter
lan	*	*	*	*	*		Drop	Egress filter

