UiO : Department of Informatics
University of Oslo

IN3210 – Network Security

Firewalls – Packet Filtering

Recapitulation: IPv4

- Task of IP (Network layer in general):
  - Packet forwarding incl. routing
- Properties:
  - Connection-less
  - Adressing: source + destination IP address
  - No QoS
  - No acklowledgement
  - No protection of packet order
  - No protection from packet loss / duplication
- Every single IP packet is transported **independently** through the network

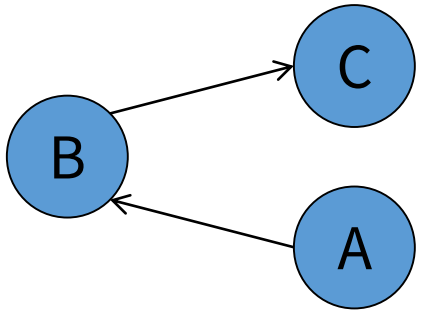
Security Properties of IP

- No mechanisms for:
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Anonymity

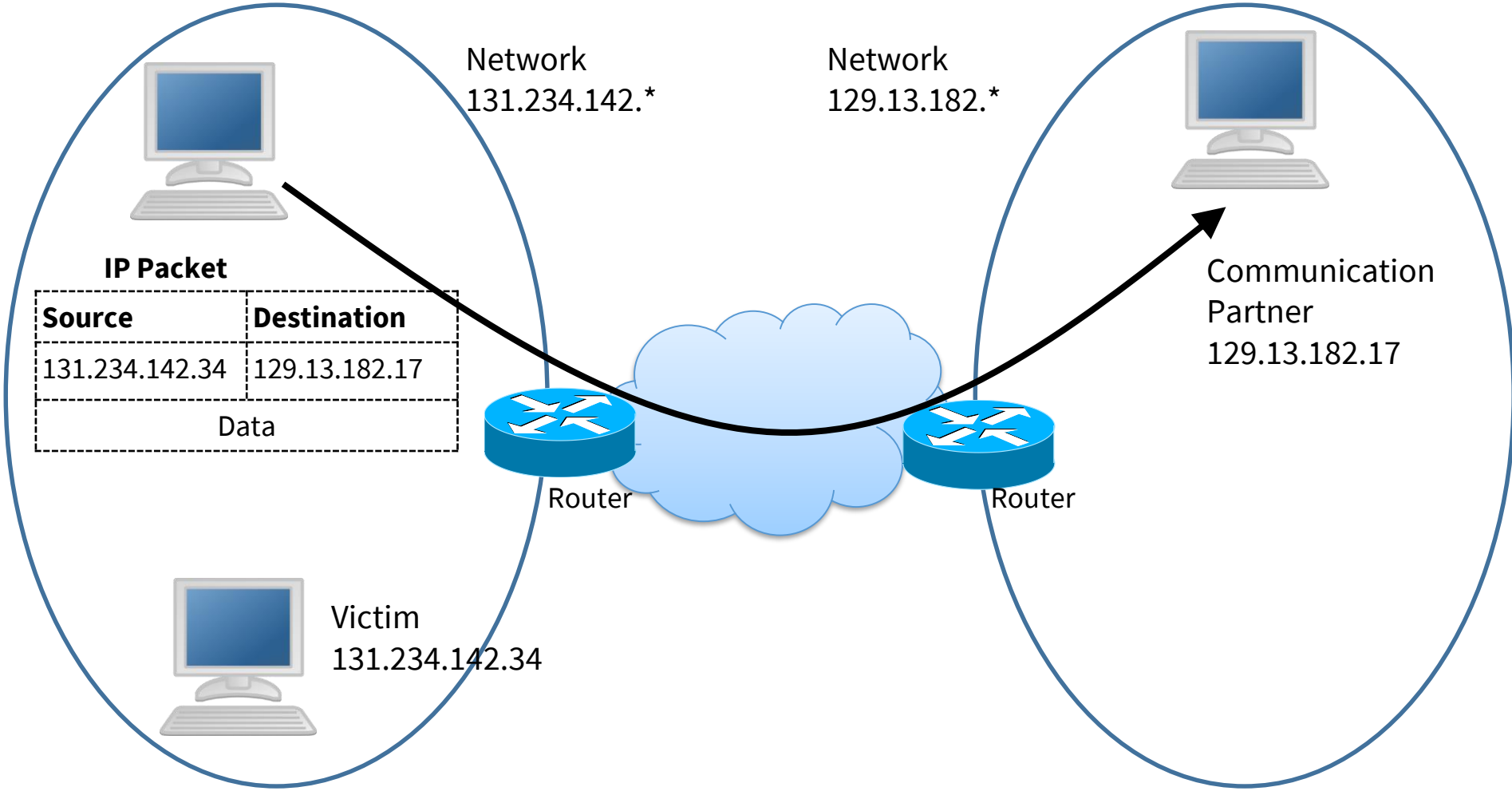
- Authenticity?

IP and Authenticity

- Problem: IP Address Spoofing
- Principle:
  - Attacker (A) sends packet to B using source IP address of C
- Variants:
  - Denial of Service on C
  - Tricking B (or C):
    - Response not required (e.g. DNS spoofing)
    - Response can be anticipated
    - Response can still be read by A



IP Spoofing – Diagram (simplified)

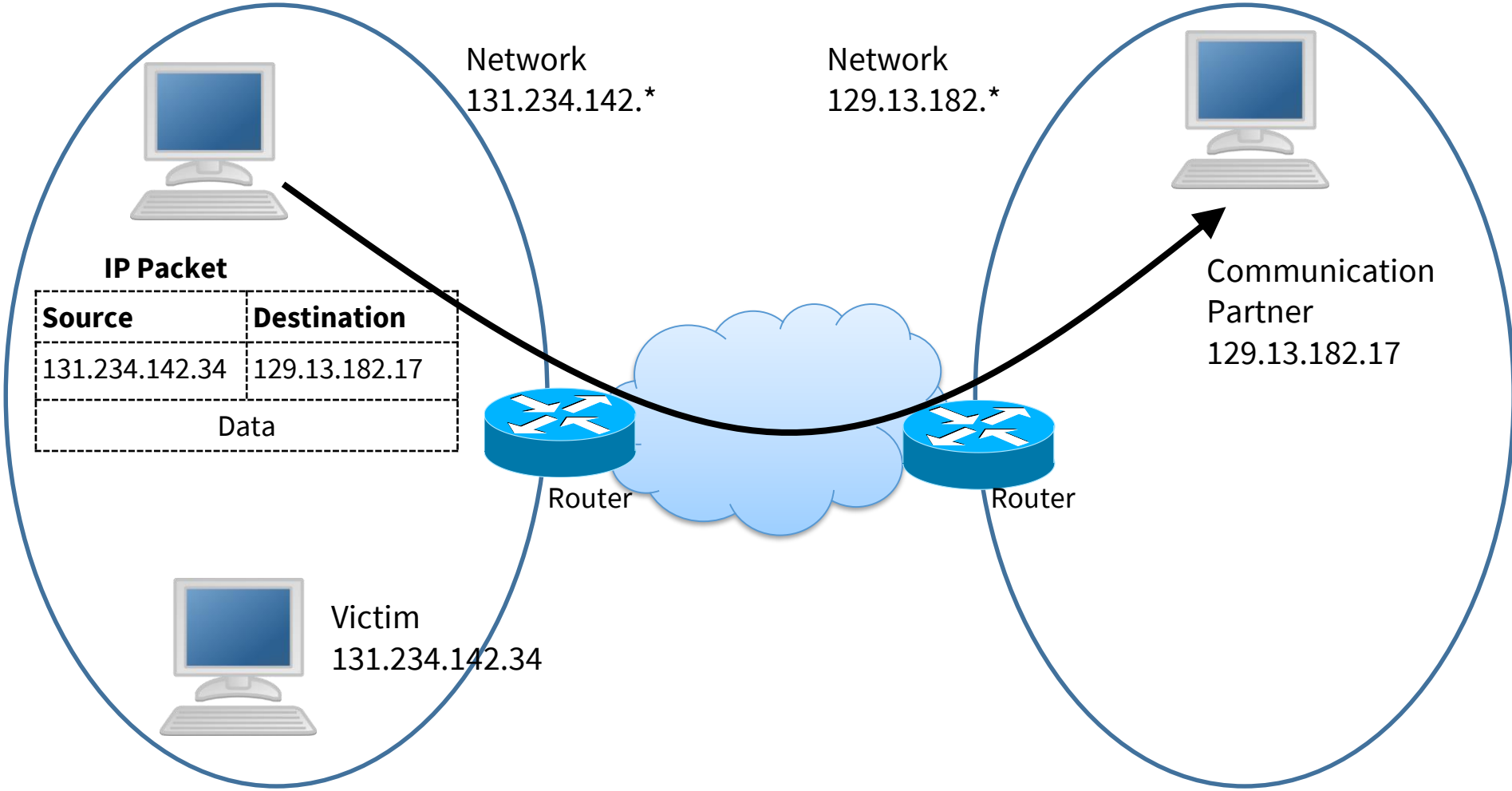


IP Spoofing

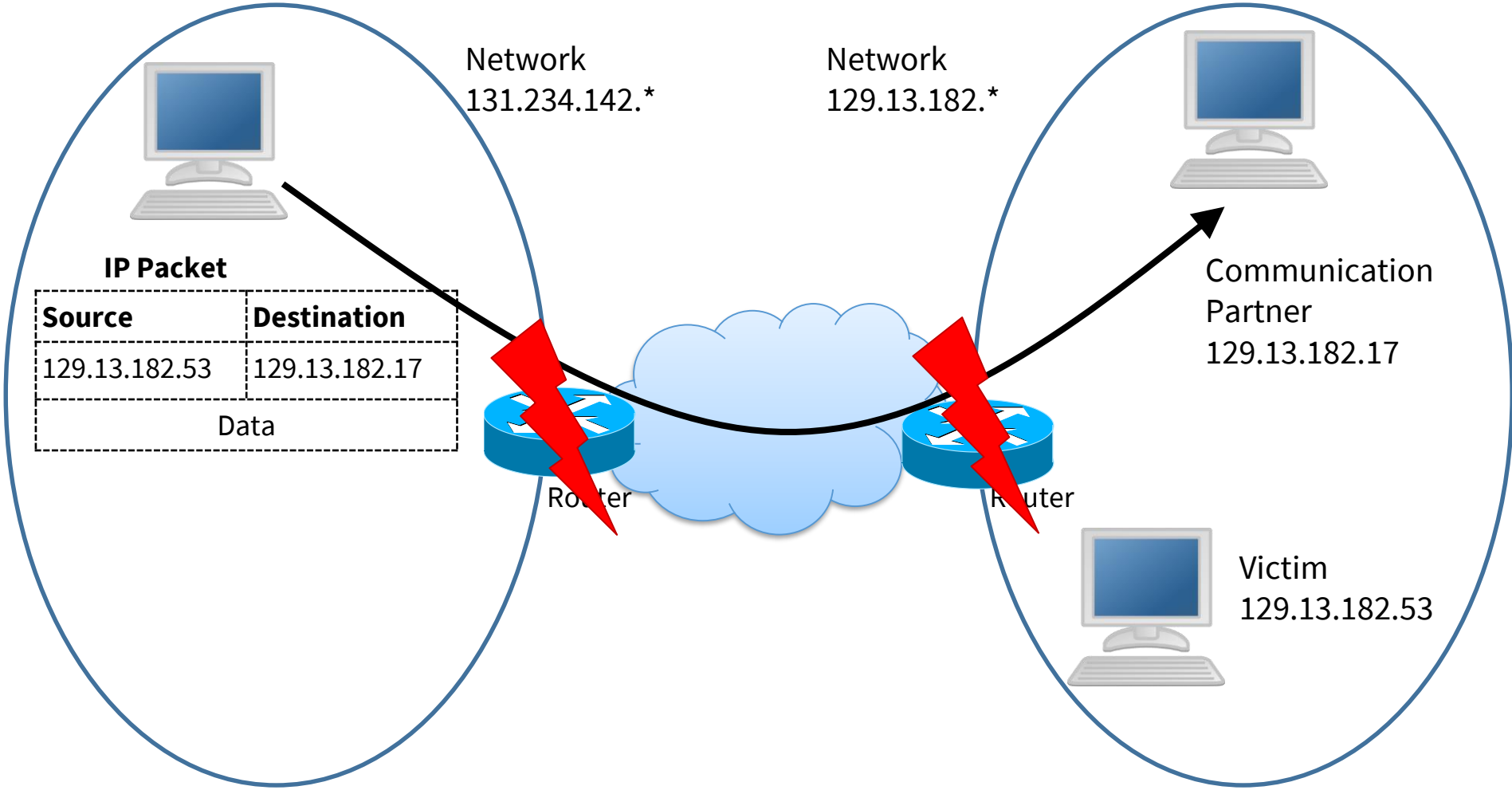
- „IP Authentication“
  - Law enforcement authorities use IP Address to identify source of criminal network actions
  - IP address is used for authentication, e.g. if you access a digital library with a university IP address
  - IP address is used for geolocation, e.g. hiding certain videos on YouTube

- How can the attack be fended …
  - if attacker and victim are in the same network?
  - if attacker and victim are **not** in the same network?

IP Spoofing – Diagram (simplified)



IP Spoofing – Diagram (simplified)



Recapitulation: ICMP

- ICMP: Internet Control Protocol
- Communication of status and error message, e.g.
  - „Fragmentation required“
  - „Destination host unreachable”
- Well-known example:
  - Ping command:
    - Creates ICMP „Echo Request“
    - Destination host responses with ICMP „Echo Reply“

ICMP: Security Issues (partly historical)

- Sending „Destination unreachable“
  → connection interrupted
- Sending „fragmentation required“
  → Increasing network load
- Sending „ping-of-death“
  - Sending large ICMP ping packet
  - Packet is fragmented during transport
  - Reassembling results in message with illegal message size (> 65.535 bytes)

  → Crash of target system
- Sending „Redirect message“
  → Router forward packets to other location

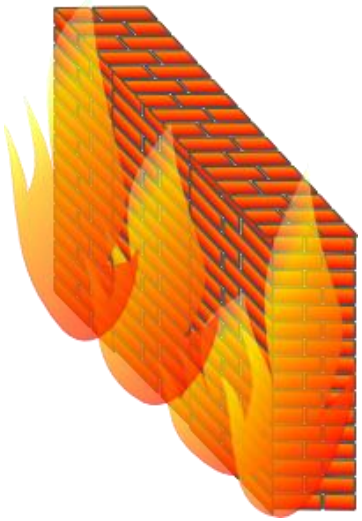
Network Services

- Example: network services on a desktop computer (Windows)

Proto.	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTEN
TCP	0.0.0.0:135	0.0.0.0:0	LISTEN
TCP	0.0.0.0:445	0.0.0.0:0	LISTEN
TCP	0.0.0.0:554	0.0.0.0:0	LISTEN
TCP	0.0.0.0:623	0.0.0.0:0	LISTEN
TCP	0.0.0.0:2869	0.0.0.0:0	LISTEN
TCP	0.0.0.0:5357	0.0.0.0:0	LISTEN
TCP	0.0.0.0:10243	0.0.0.0:0	LISTEN
TCP	0.0.0.0:16992	0.0.0.0:0	LISTEN
TCP	0.0.0.0:49152	0.0.0.0:0	LISTEN
TCP	0.0.0.0:49153	0.0.0.0:0	LISTEN
TCP	0.0.0.0:49154	0.0.0.0:0	LISTEN
TCP	0.0.0.0:49155	0.0.0.0:0	LISTEN
TCP	0.0.0.0:49157	0.0.0.0:0	LISTEN
TCP	0.0.0.0:56238	0.0.0.0:0	LISTEN

Firewalls: Introduction

- Original:
  - Protection for a building / building part from fire and smoke
- Network security:
  - No complete sealing
  - Controlling network traffic
- Firewall:
  - Located between two networks
  - Investigates all network traffic between networks
  - Checks conformance to „access control policy“
    - Forwarding allowed packets
    - Droping / Rejecting denied packets



Firewalls: Introduction

- Common usage:
  Separating local (Intranet) and Internet
- Required steps for buiding firewall:
  - Modelling security requirements
  - Knowledge on weaknesses and threats
  - Designing security strategy
- No or limited protection from:
  - New attack patterns
  - Insider attacks

Basic Security Policy Principles

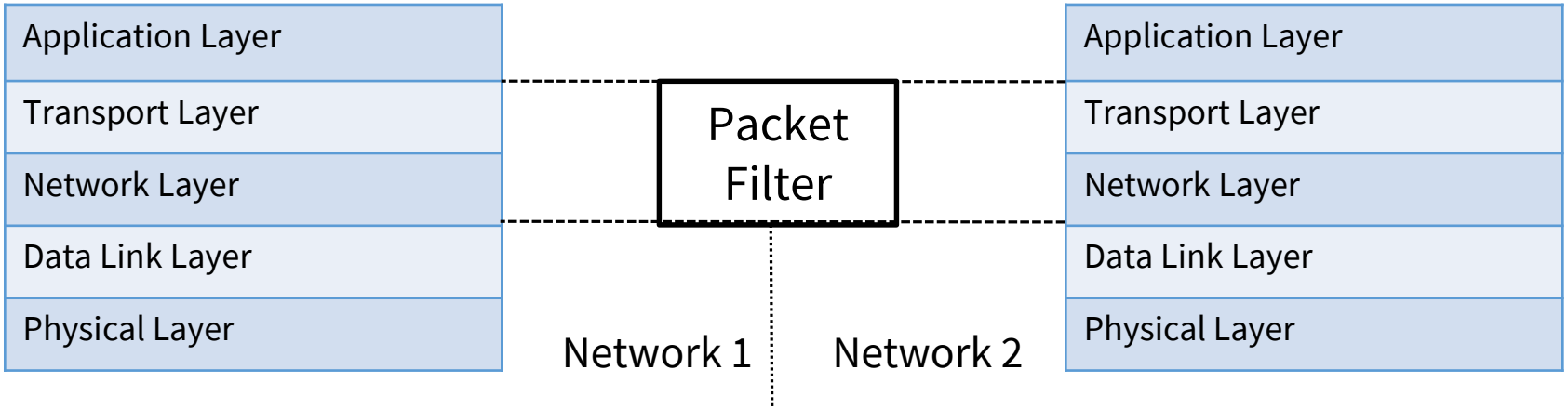
- „Default Permit“
  - Default policy rule allows all incoming and outgoing traffic
  - Selectively block known attack communication patterns
  - Flexible regarding new services
  - No protection from new or disregarded attacks
- „Default Deny“
  - Default policy rule denies all traffic
  - Selectively allow required addresses/ports/applications
  - Provides better security
  - New service result in (expensive) policy changes

Firewall inside the ISO/OSI Layer Model

- Checking protocol headers of different layers:
  - Layer 3 + 4 (Packet Filter)
  - Layer 7 (Application Level Gateway)
- Checking protocol content
  (typically not called firewall anymore)
  - Anti Virus Scanner
  - Checking content with regard to company export policy

Packet Filter

- Remarks
  - Typically implemented inside routers (but not required) – Network Packet Filters
  - Layer 2 information mostly not regarded (you can have though MAC Address Filtering when needed, mainly for end-points in an organization)
  - Does not inspect application layer protocol



Packet Filter

- Possible Actions
  - Forwarding Packet
  - Dropping Packet
  - Rejecting Packet (and sending ICMP error message)
  - Logging (partly or completely) Packet
- Information used in packet filter rules
  - Source and Destination IP Address
  - Transport protocol
  - Source and Destination port (from transport layer)
  - Specific flags (e.g. ACK bit from TCP)
  - Network interface
  - *Action*

Example Scenario

- Router uses Linux Netfilter/IPtables

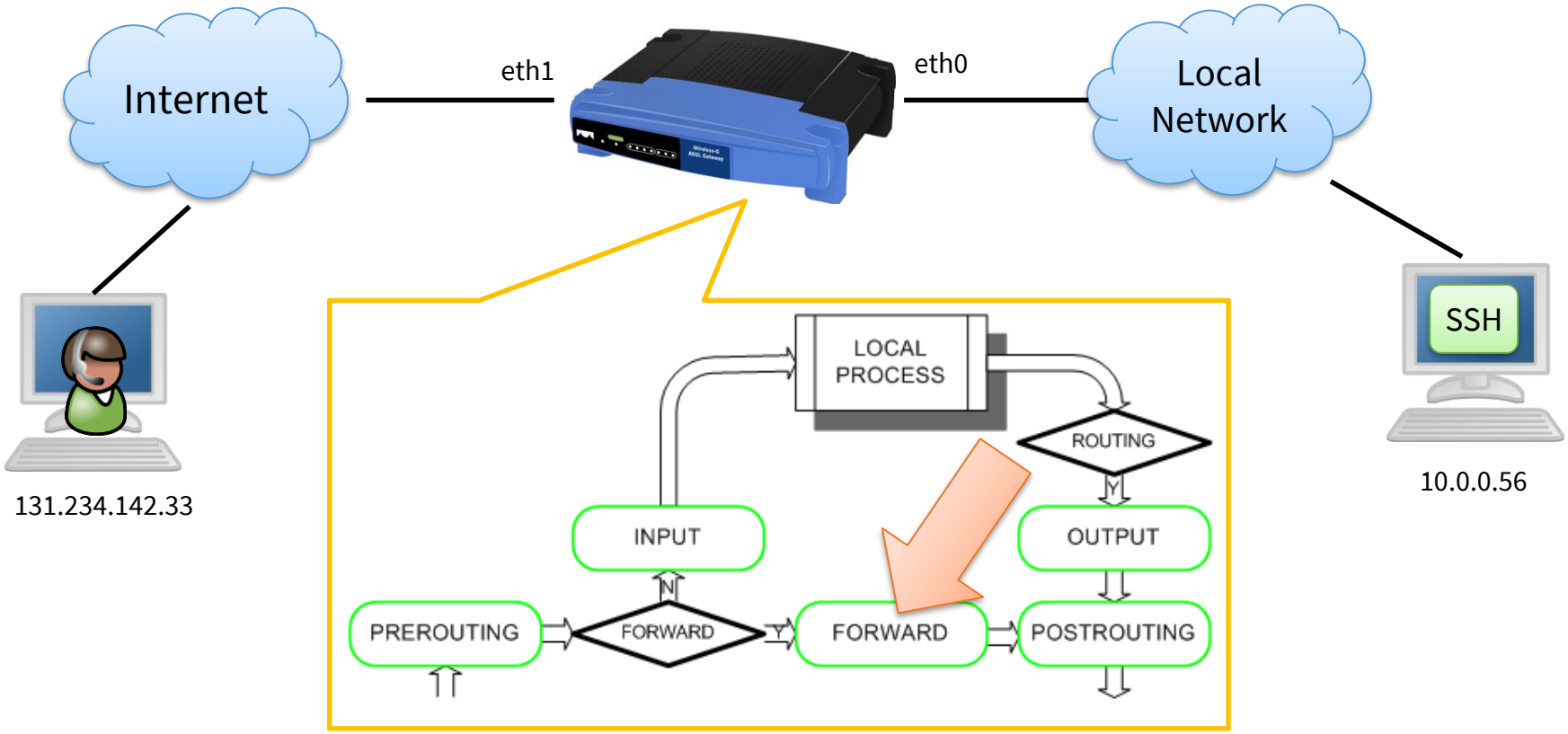


Image Source: http://ebtables.netfilter.org/br_fw_ia/br_fw_ia.html

Security Requirements

- Requirements for the sample scenario:
  - Clients from the local network can use all services on the Internet
  - The administrator can access the local network from his home office (131.234.142.33)
  - The SSH service on a server inside the local network (10.0.0.56) can be accessed from the Internet
  - All other connections shall be blocked!

Stateful / Stateless Firewall

- Stateless packet inspection:
  - Decision is solely based on current packet
- Stateful packet inspection (SPI):
  - Current state is stored (e.g. „TCP connection established“)
  - Decision based on current packet and current state (Checks a table indicating the connections that have been established – faster)
  - More powerful than stateless inspection
  - However:
    - Storing states consumes resources
    - Denial-of-Service attacks possible
    - Image the amount of packet per seconds transmitted in a contemporary Gigabit network!

Filter Rules: iptables

- Sample filter rules:

```
iptables -P FORWARD -j DROP
iptables -A FORWARD -m state --state NEW
  -i eth0 -j ACCEPT
iptables -A FORWARD -m state
  --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -s 131.234.142.33 -j ACCEPT
iptables -A FORWARD -p tcp -d 10.0.0.56 --dport 22 -
  j ACCEPT
```

Explanation of iptables rules

```
iptables -P FORWARD -j DROP
```

- Definition of Default policy for FORWARD chain
  - `DROP`
    - All packets are dropped (without informing the sender)
  - Alternatives:
  - `REJECT`
    - All packets are rejected and the sender is informed (ICMP „Port Unreachable“)
  - `ACCEPT`
    - All packets are accepted (=forwarded)

Explanation of iptables rules

```
iptables -A FORWARD -m state --state NEW
  -i eth0 -j ACCEPT
```

- Loading extension for stateful inspection:
  - `-m state`
- Rule …
  - `--state NEW`
- … matches on packets that start a connection (e.g. TCP SYN)
  - `-i eth0`
- … matches on packets coming from interface `eth0` (assuming this is the LAN interface)
- Packets that match the condition are accepted
  - `-j ACCEPT`

Explanation of iptables rules

```
iptables -A FORWARD -m state
   --state ESTABLISHED,RELATED -j ACCEPT
```

- Loading extension for stateful inspection:
  - `-m state`
- Rule …
  - `--state ESTABLISHED,RELATED`
- … matches on packets:
  - that are part of an established connection
  - that are related to a connection (e.g. ICMP messsages)
- Packets that match the condition are accepted
  - `-j ACCEPT`

Explanation of iptables rules

```
iptables -A FORWARD -s 131.234.142.33 -j ACCEPT
iptables -A FORWARD -p tcp –d 10.0.0.56 --dport 22 -
  j ACCEPT
```

- All packets from source IP Address 131.234.142.33 are accepted
- All packets using transport protocol and destination address 10.0.0.56 and destination port 22 are accepted

Filtering Multimedia Data

- (Example) problems with multimedia protocols :
  - T.120 (ITU conference protocol): Chat, white board, application sharing, data transfer:
    - Different service with different criticality
    - However: same TCP port
  - H.323, SIP (used for VoiP telefony, video conferencing):
    - Session initiation protocol defines ports for communication protocol → unknown to the packet filter
  - Skype:
    - Designed to circumvent firewalls

Packet Filter: Advantages

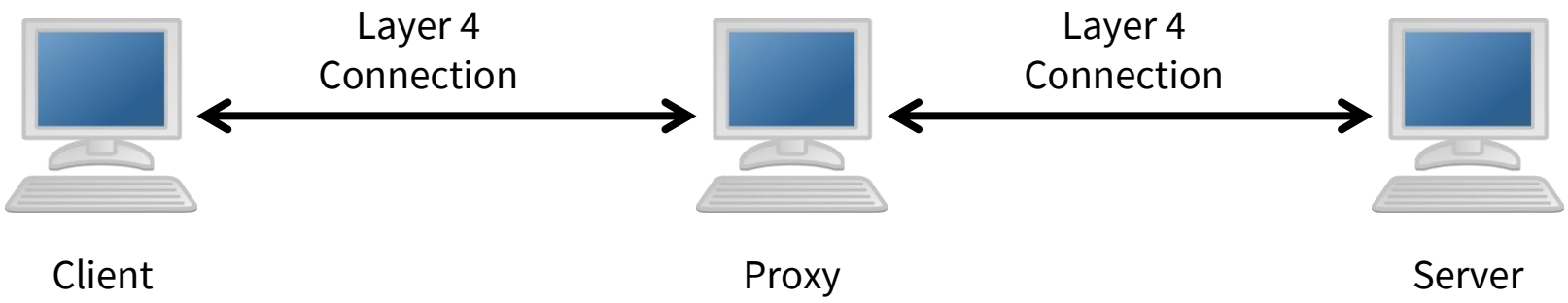
- Simple and transparent to the end systems
  (no changes to applications required)
- Cheap: uses standard technologies
- Simple protection of whole subnet using single router
- Efficient: part of the standard routing system

Packet Filter: Limitations

- Filter decision based on spoofable information (no integrity or authenticity guarantees)
- Coarse grained control: based on services or end-systems, not on users
- Stateless filters are not able to handle dynamic communication patterns (e.g. multimedia protocol, callbacks)
- Stateful filter:
  - lower performance
  - vulnerable to DoS attacks
  - filter has only limited view on the actual protocol state
- Expensive building and management of filter rules

Proxy Firewall

- Client communicates with the proxy as a delegate of the server
- Server communicates with the proxy as a delegate of the client



- Proxy is Server to the client and client to the server
- Alternative term: circuit-level gateway

Properties of Proxy Firewall

- Can authenticate user (not only end system)
- Checks authorization
- Creates proxy connection to server
- Performs further operation based on authentication (e.g. logging)

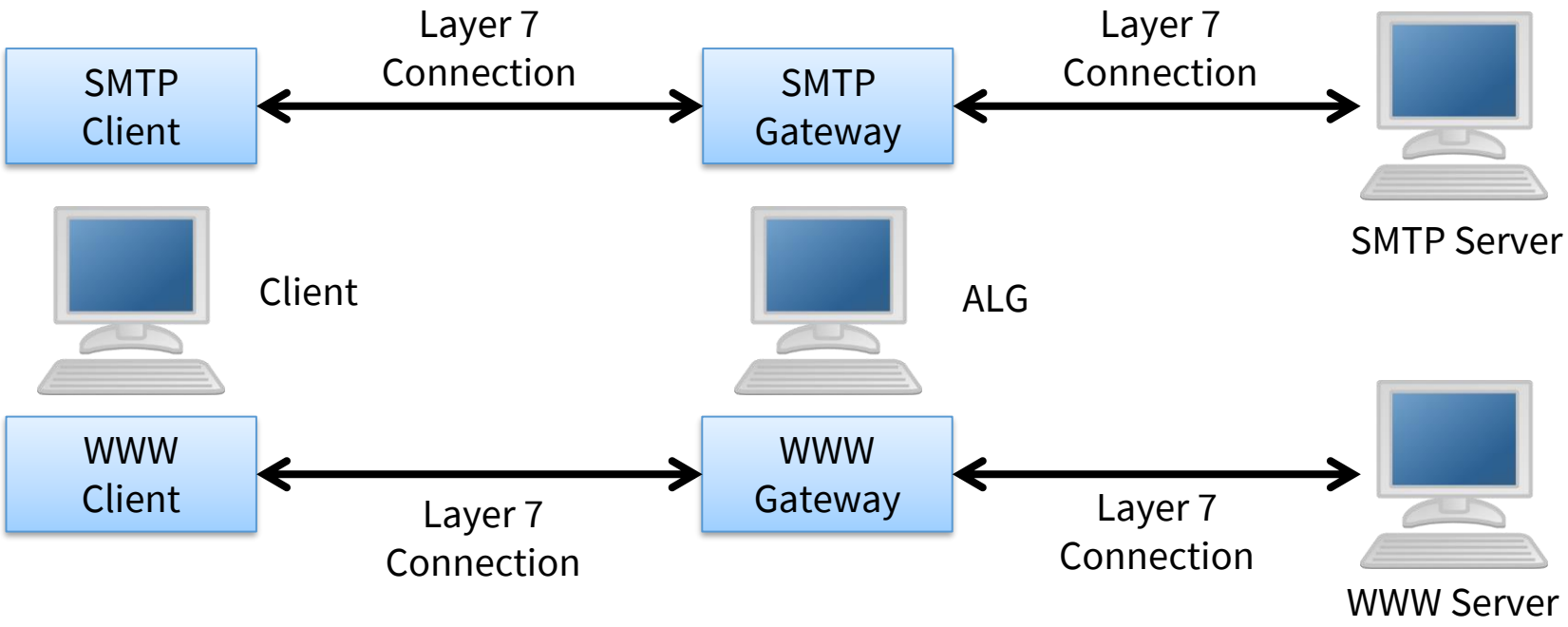
Properties of Proxy Firewall

- Advantages
  - No changes to application protocol
  - Better control compared to packet filter (including authentication)
- Disadvantages
  - No analysis of application protocol
    - Services are either allowed or denied
    - No application data dependent policies possible
  - Typically modification of client software required

Application Level Gateway (ALG)

- Operates on application level
- Comparable to proxy (but on layer 7)
- Supports and analyses application protocols
- Application specific filtering possible, e.g.
  - Detecting malicious HTTP header
  - Analyses active content on Web pages
- ALG handles only supported applications
  - Individual proxies for each application
  - Combination with packet filter recommended

Application Level Gateway



Application Level Gateway: Security

- Security Issues:
  - Application layer protocols:
    - are more complex
    - more vulnerable to attacks
  - Application Level Gateway:
    - has to implement large portions of the application protocol
    - significantly more complex than layer 4 proxy firewall
    - Is typically implemented on standard platform (e.g. Linux system)
- Required security means:
  - Reduce services on ALG to minimum
  - Keep OS and gateway up-to-date

Application Level Gateway: Advantages

- User level authentication
  → Fine grained access control
  → User specific accounting
- Detecting attack patterns on application level
  → Intrusion Detection
- Service level filtering and controlling

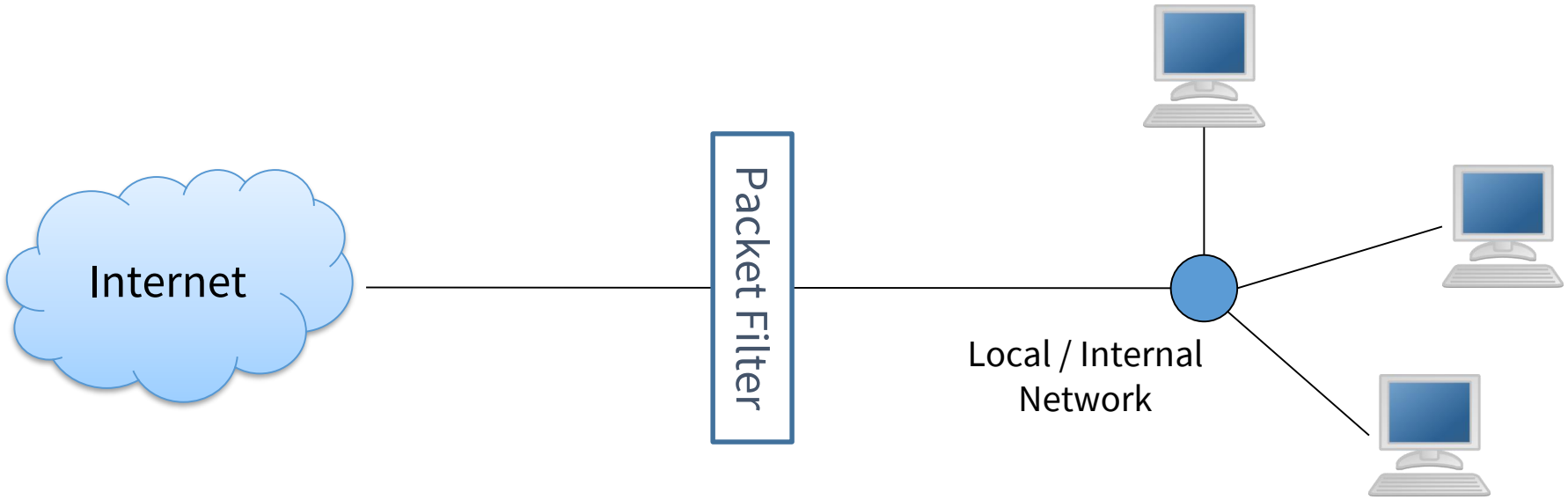
Application Level Gateway: Limitations

- High resource requirements
  → Potential for Denial-of-Service
- Hiding / obfuscating malicious content still possible
  (e.g. compression, encryption)
- Only available for limited applications
- Separating „critical“ and „non-critical“ application parts still hard to realize

Configuration of Network Perimeter Security

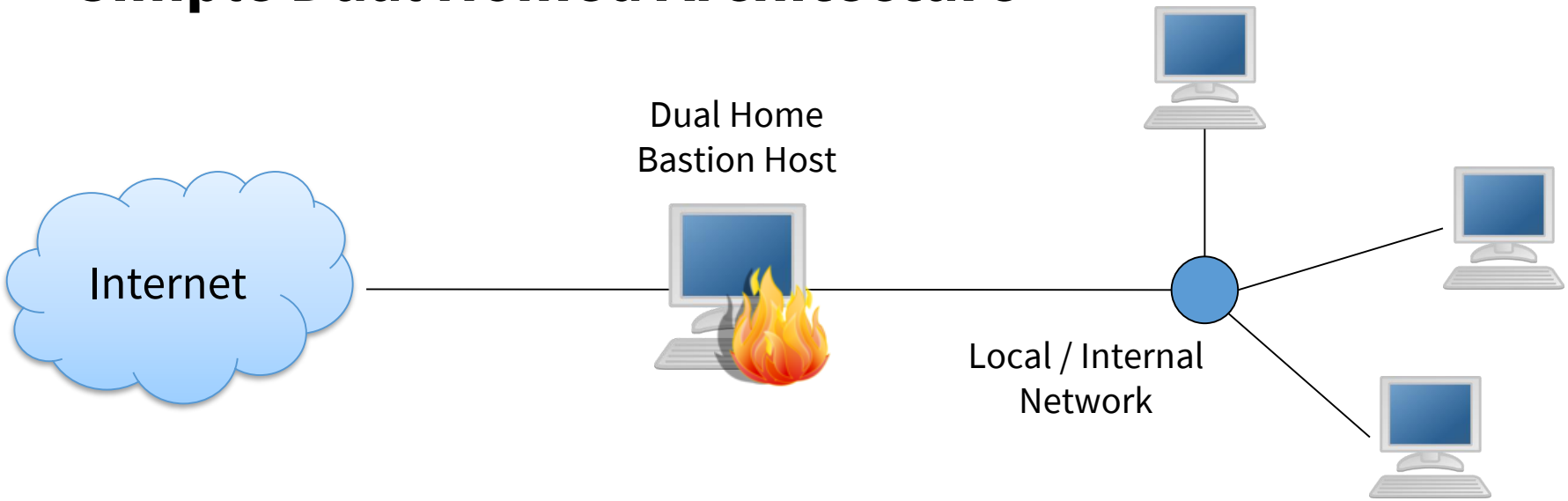
- Traditionally configured with terminal/cli access (advanced)
- Home routers and host firewalls provide simplified GUI
- Vendor Firewalls come with GUI that allows flexible configuration
- When integrating multiple technologies where firewalls need to be configured in real-time the use of APIs is important
  - APIs that connect multiple technologies (interfaces between different technologies) allow for rapid configuration of firewalls.
  - Needs expertise in software development and security enginnering

Simple Packet Filter Architecture



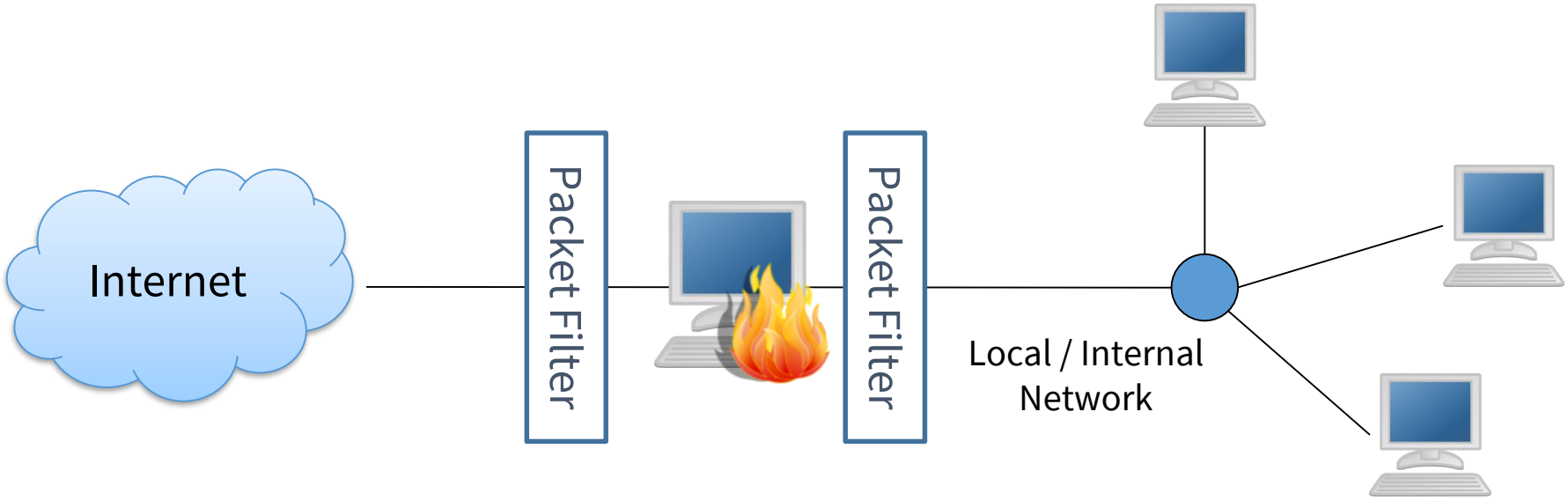
- Realisation:
  - PC with 2 network interfaces
  - Integrated into router
- Filtering of „illegal“ packets

Simple Dual Homed Architecture



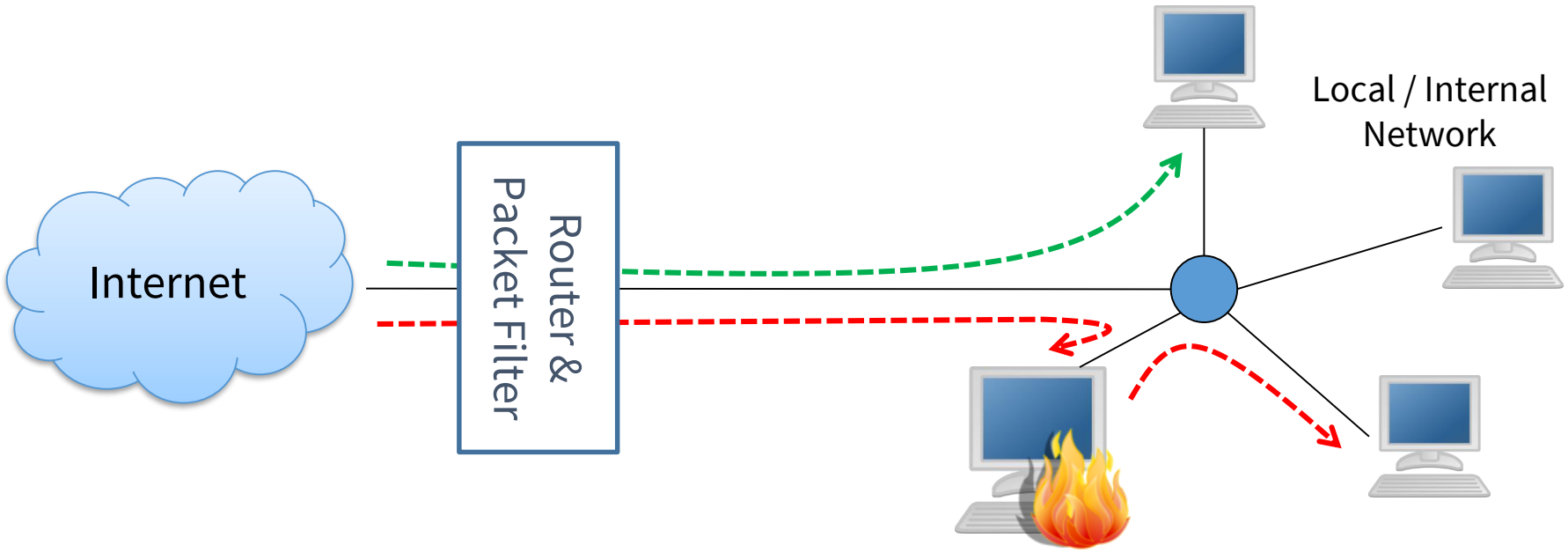
- Bastion Host, here: Proxy Firewall or ALG
- Realisation
  - PC with 2 network interfaces
- Problems:
  - Single point of failure
  - Processing bottlenet → performance problems

Extended Dual Homed Architecture



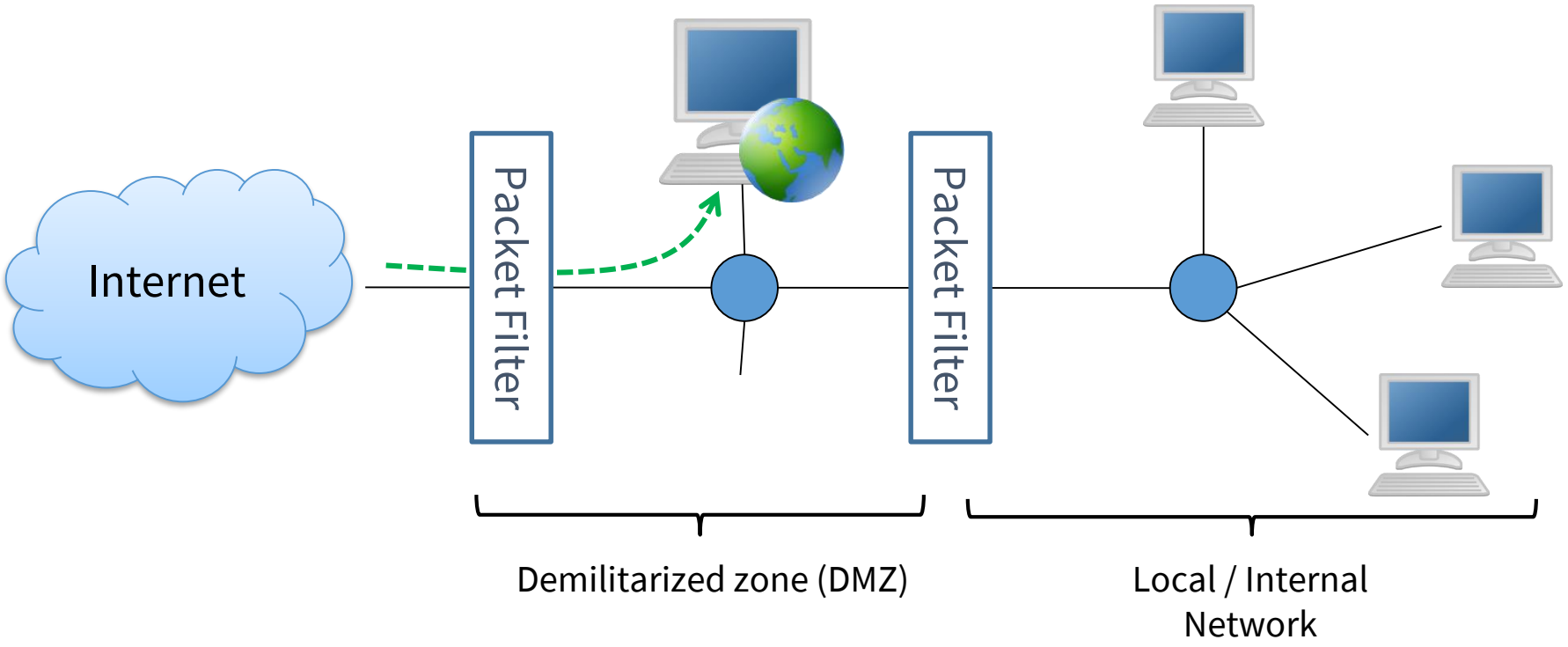
- Additional packet filters for protecting the Bastion Host and the internal network
- Same problems as before

Screened Host Architecture



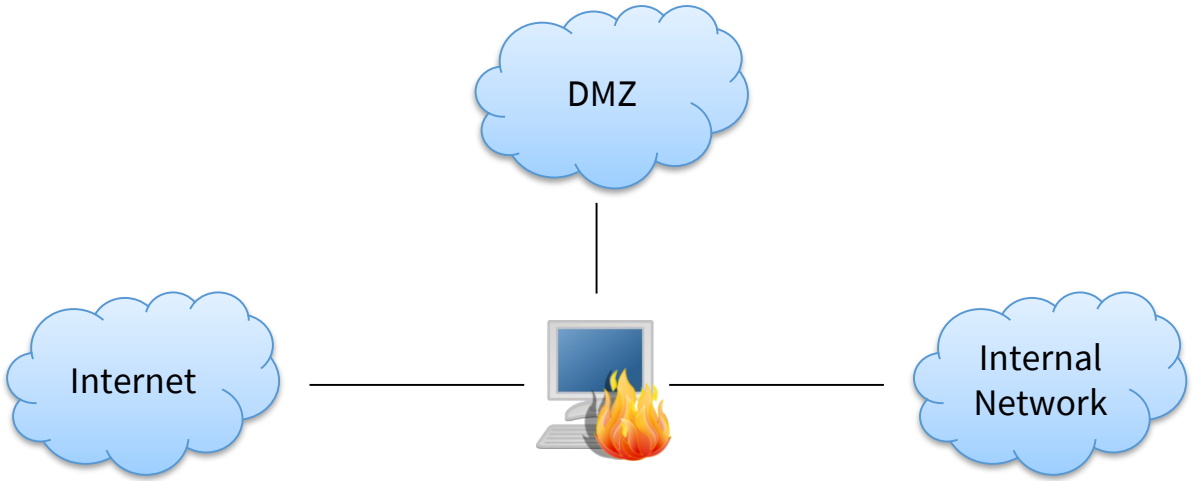
- Bastion Host located inside the internal network
- Critical data is forward by the router to the Bastion Host
- Uncritical data is forward directly to the target host

Screened Subnet Architecture

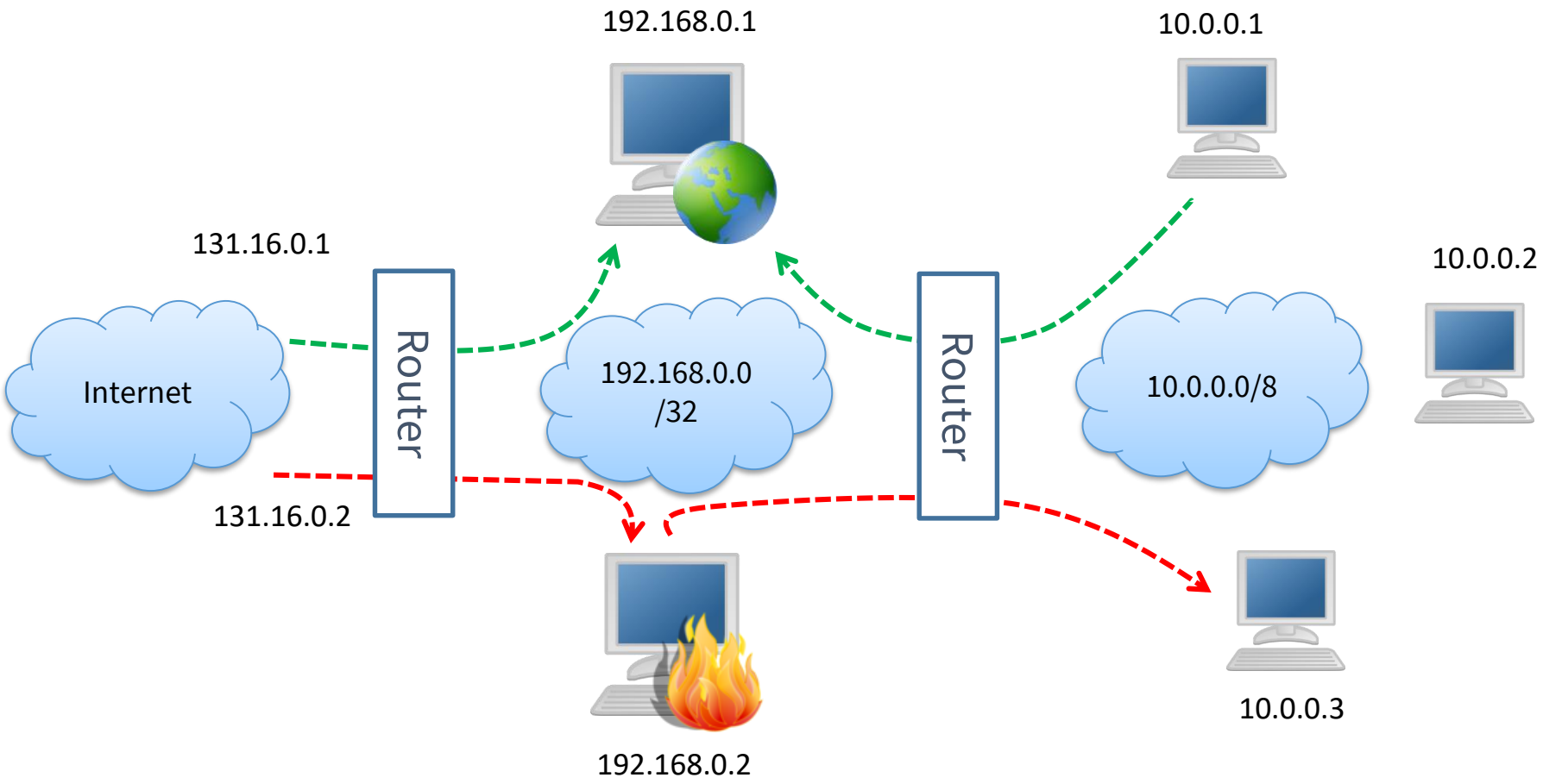


Screened Subnet Architecture

- Demilitarized Zone between internal and external network
- Bastion Host inside the DMZ
- 2 Packet Filter between the 3 network
- Public accessible servers (e.g. WWW) inside the DMZ
- Filtering functionality can be implemented on single device



DMZ: Example IP Configuration



Screened Subnet Architecture: Advantages

- Higher Security for internal network compared to screened host architecture
- High flexibility for service without ALG filtering (same as screened host architecture)
- Hiding internal network structure
- Clear seperation of internal external services
- Recommended by the German Federal Information Security Agency BSI

Firewall – Summary

- Firewall increases security of computer networks:
  - Centralizing security mechanisms / security policies
  - Fine grained control mechanisms of different layers
- Firewalls are no „magic bullet“
- Limitations / Restrictions:
  - Configuration requires expert knowledge
  - New / modified service require configuration changes
  - Application data can only partly be controlled

Firewall – Summary

- Limitations / Restrictions (continued):
  - No protection inside the individual network segments
  - No protection from „leaking network link“, e.g. laptop with 3G card
  - No control over data inside VPN tunnels (e.g. IPSec)
  - Security and configuration issues with multimedia protocols
- Summary:
  - Firewalls are essential in all networks (enterprise and home)
  - DMZ paradigm state-of-the-art, but insufficient for dynamic, mobile or open systems (now and in the future)
  - Additional security service required inside applications / on end systems