Security architecture:
- Firewalls and tunnels
- Other security architecture components
- Old-school vs new world
- OT/SCADA

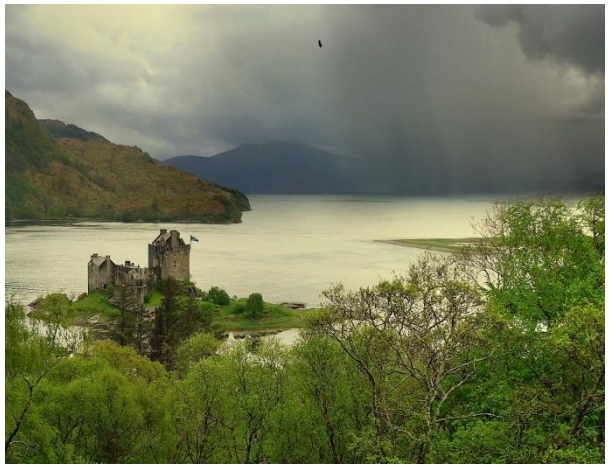
Hardware hacking

Carsten Jørgensen
Department of Computer Science, DIKU
September 29. 2025

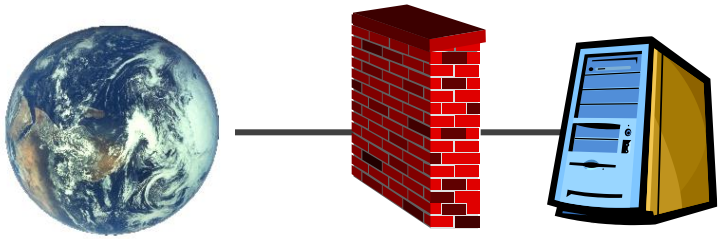
UNIVERSITY OF COPENHAGEN

Security architecture
ports, protocols and firewalls

What is a firewall ?



Perimeter protection



Firewalls

Hardware or software designed to prevent unauthorized access through perimeter (network) protection

Matches packets to **policies**, and applies different **rules** to different packets

All modern firewalls are **hybrids** and typically use multiple methods

Firewall types

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on defined filter rules (addresses and port numbers). Packet filtering is effective and transparent to users, but is difficult to configure

Stateful inspection / Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can often flow between the hosts without further checking

Application gateway: Applies security mechanisms to specific applications, such as HTTP, FTP and Telnet servers. IP packets are not passed to internal hosts rather the application acts as an interpreter. This is very effective but can impose performance degradation

WAF – Web Application Firewall

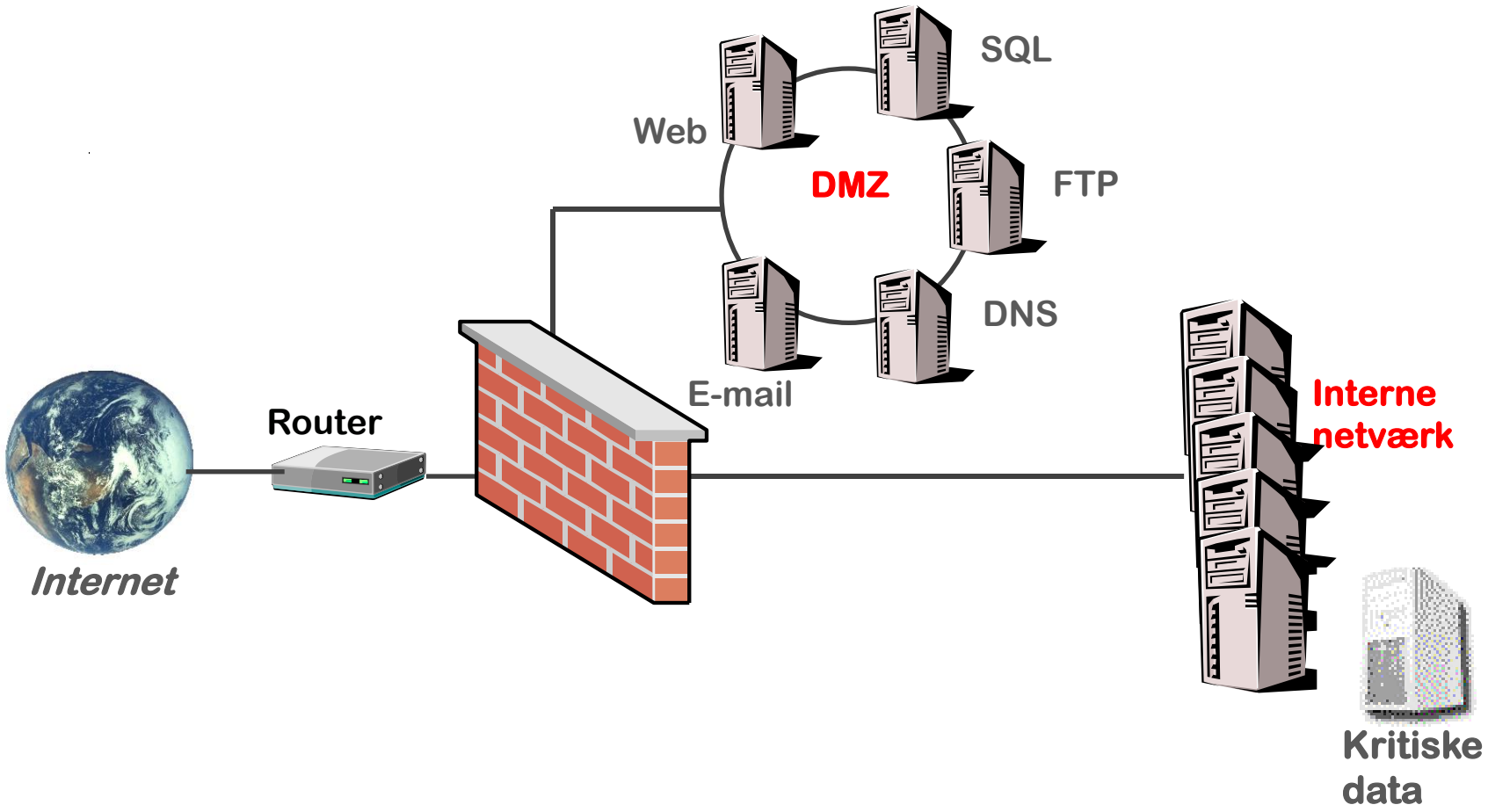
Firewall types and policies

- **Stateless:** Do I like this packet?
- **Statefull:** This packet is part of a flow. Do I like this flow?

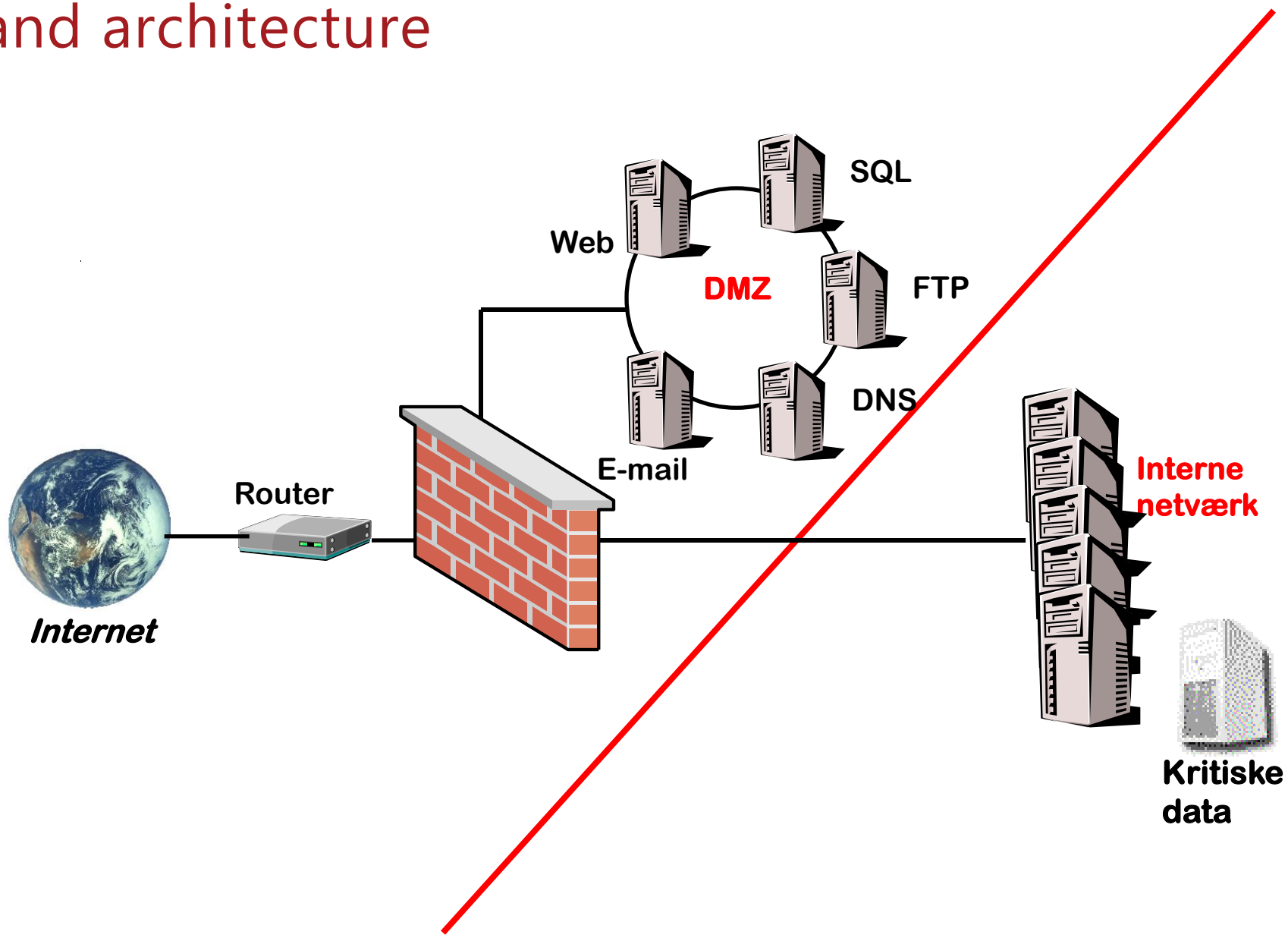
Firewall policies can be anything and can do anything

- Limit maximum bandwidth
- Increase minimum latency
- Alter content – add advertising into traffic

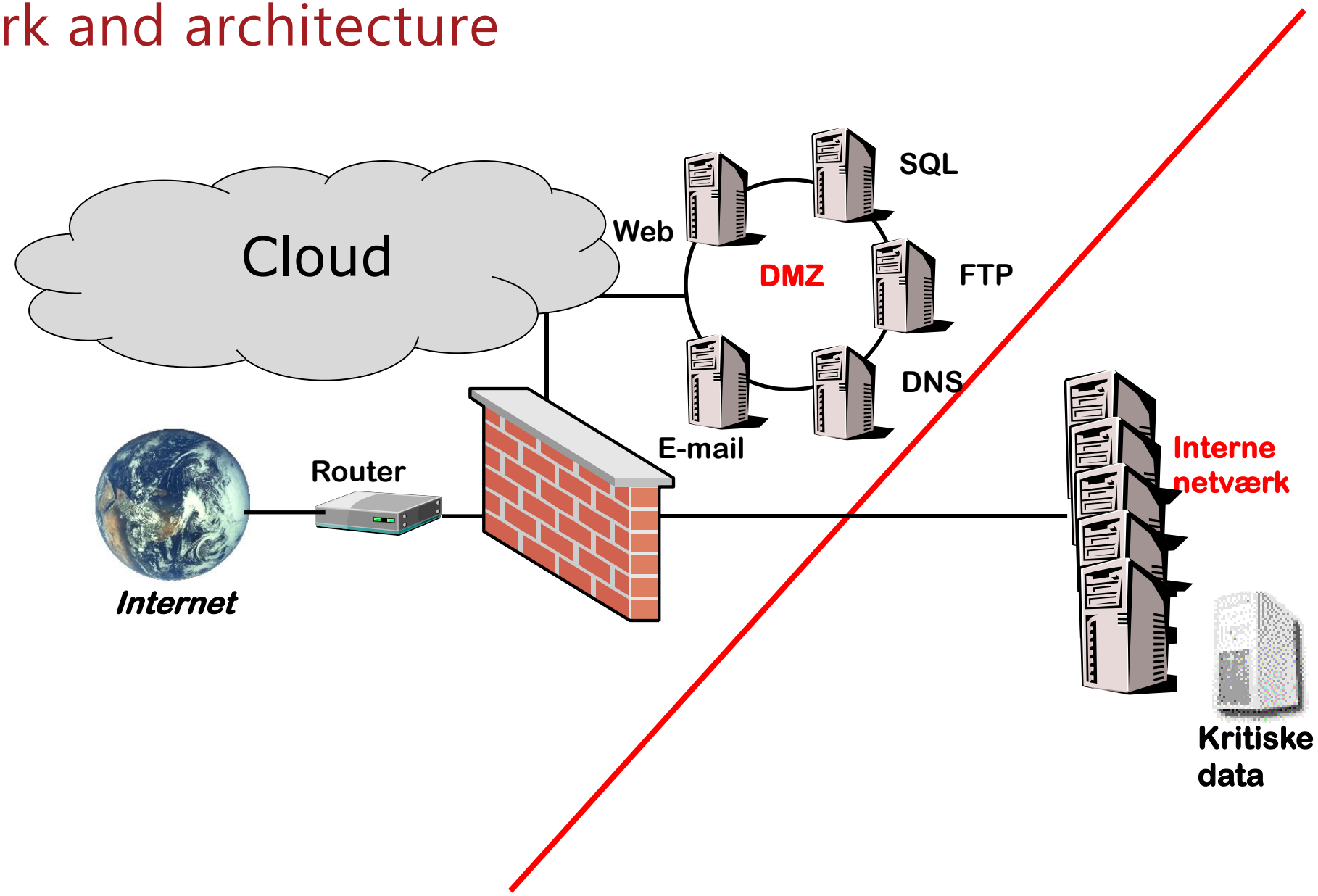
Network and architecture



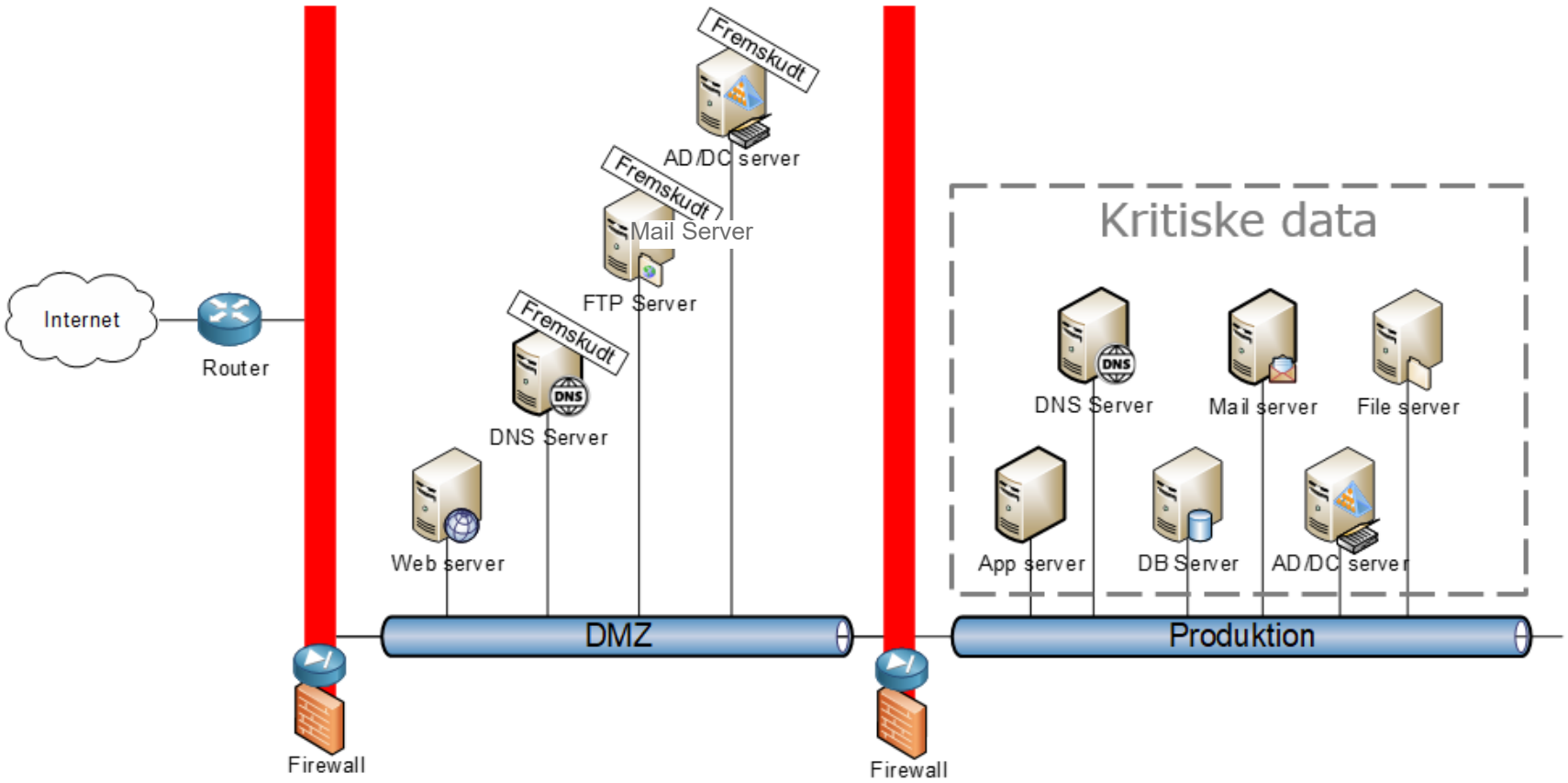
Network and architecture

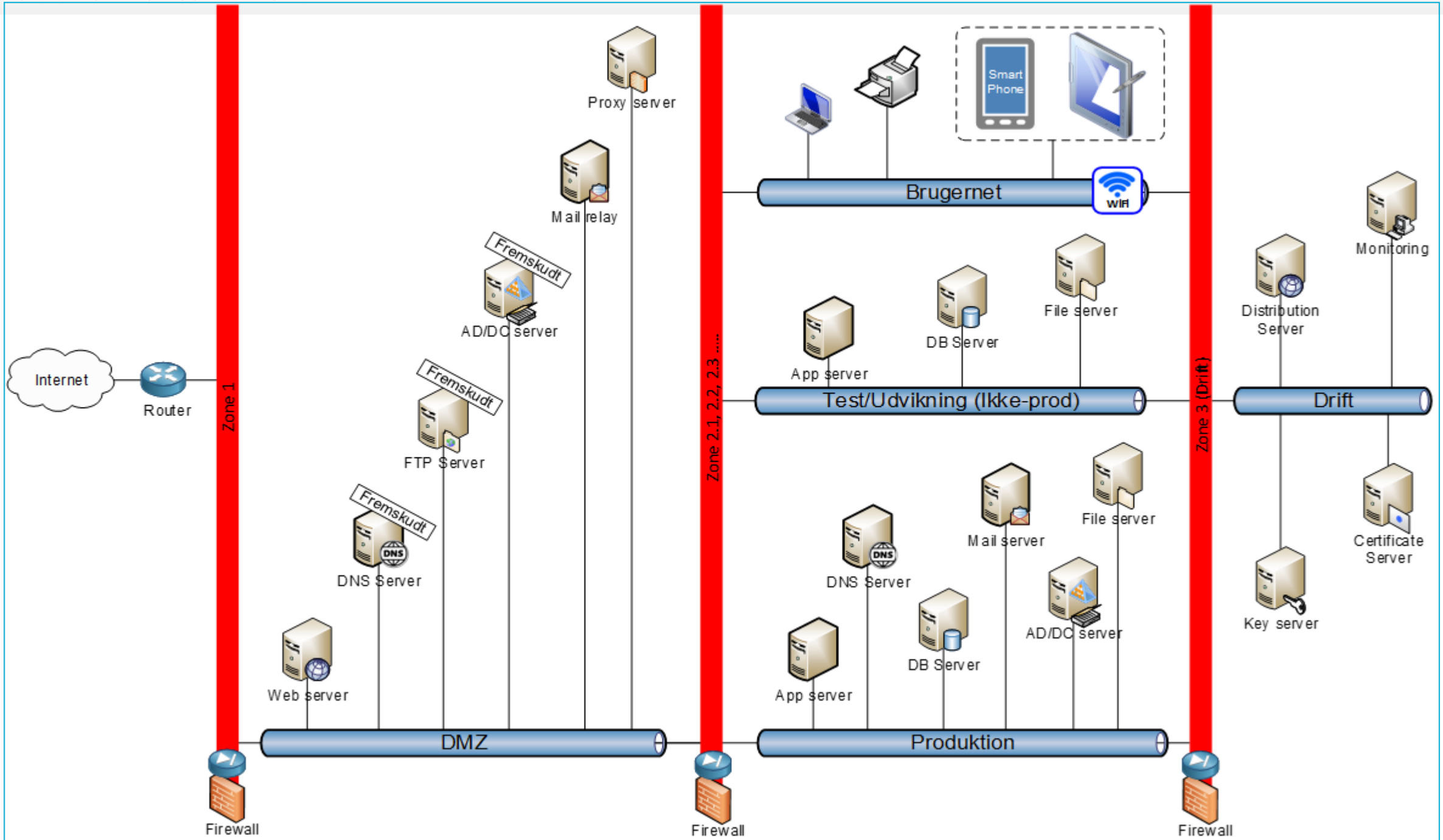


Network and architecture



Sikkerhedsarkitektur – netværk og segmentering



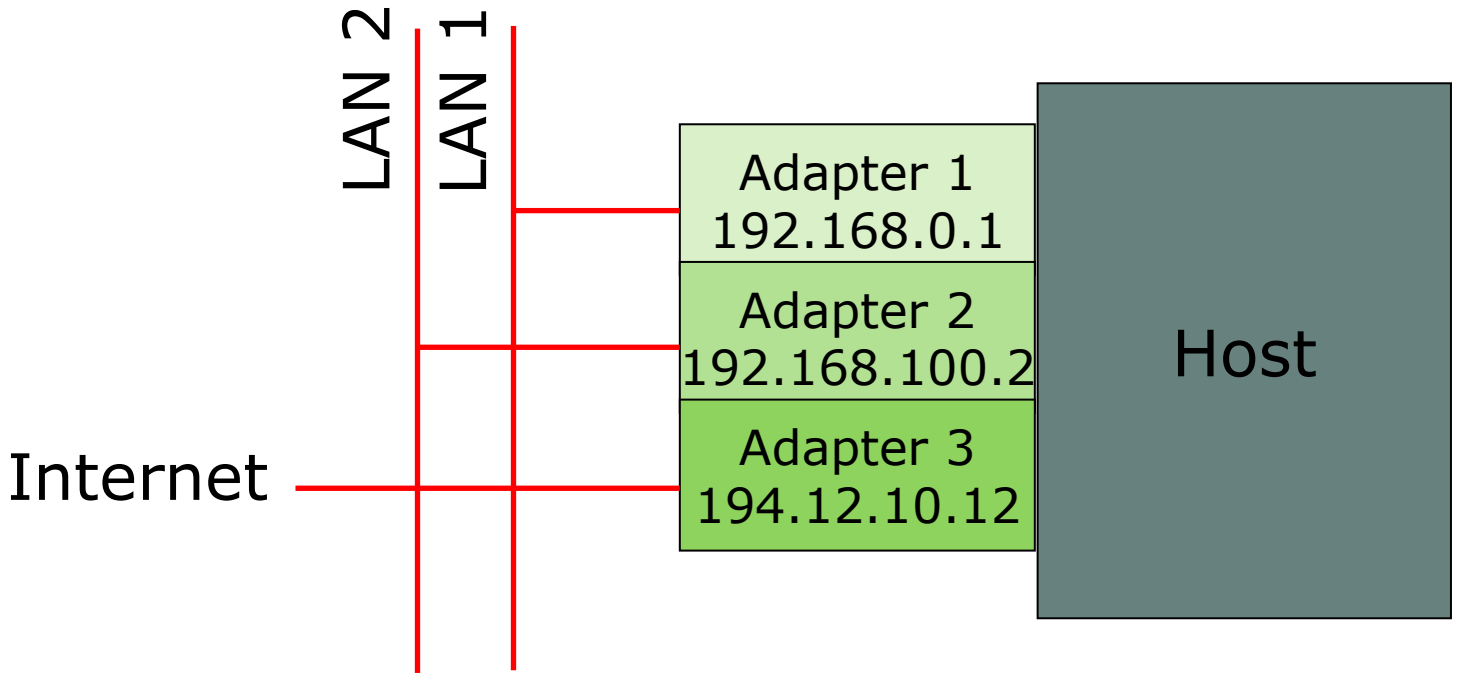

Internet
Router
Zone 1
Proxy server
Mail relay
Fremskudt
AD/DC server
Fremskudt
FTP Server
Fremskudt
DNS Server
Web server
DMZ
Firewall
Zone 2.1, 2.2, 2.3 .....
Smart Phone
Brugernet
WIFI
App server
DB Server
File server
Test/Udvikning (Ikke-prod)
DNS Server
Mail server
File server
App server
DB Server
AD/DC server
Produktion
Firewall
Zone 3 (Drift)
Distribution Server
Monitoring
Drift
Certificate Server
Key server
Firewall

Ports, IP-addresses and firewalls

Firewalls – physically (or virtually)

IP addresses are associated with adapters (netværkskort), not CPUs

A single host can have many IP addresses



Ports

To provide access to services over an IP-network applications are assigned a unique address – a port

The application binds to the port and starts when a connection-request is issued to the port

65.535 TCP and UDP ports

First 1024 ports are "*well known ports*", but services can be configured to run on all ports

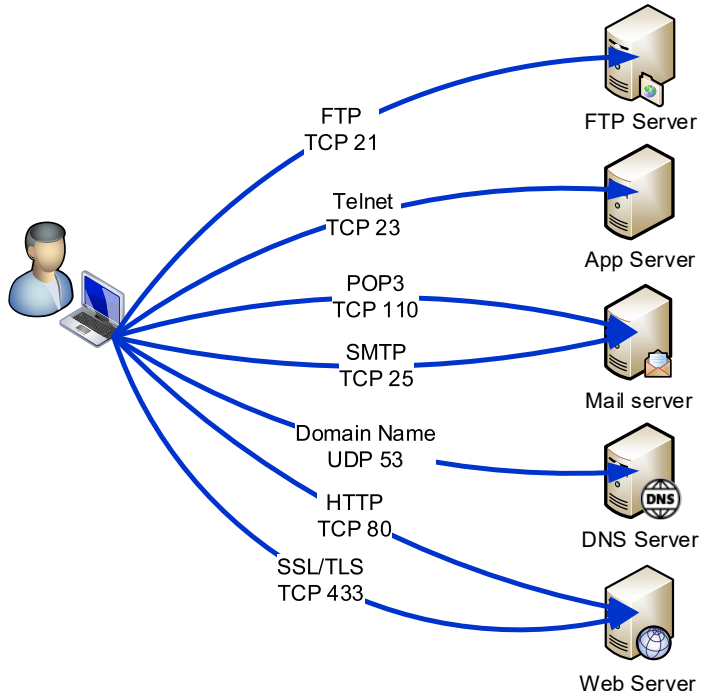
1024 – 49151: Registered ports
49152 – 65535: Dynamic and/or private ports

http://www.iana.org/assignments/port-numbers

IP + port: 192.168.10.1:80

A few well-known ports

Service	Port	Protocol
FTP	21	TCP
SSH	22	TCP
Telnet	23	TCP
Simple Mail Transfer Protocol (SMTP)	25	TCP
Domain Name	53	UDP
HTTP (web server)	80	TCP
SSL/TLS	443	TCP



TCP/IP

Protocol	Name	Description
IP	Internet Protocol	En protokol der gør det muligt at route (dirigere) datapakker fra kilde (source) til modtager (destination)
TCP	Transmission Control Protocol	Connection oriented/forbindelses orienteret: kræver svar på levering fra modtager = kan genfremsende fejlede IP data pakker
UDP	User Datagram Protocol	Som et postkort - connectionless/forbindelsesløs: svar ikke krævet = gensender ikke fejlede IP data pakker
ICMP	Internet Control Message Protocol	Anvendt i netværksenheder til at kunne håndtere netværks kommunikations hændelser

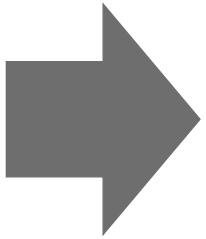
Many other protocols: IGMP, OSPF etc.

Firewall – basic terminology

Firewall policy

Firewall rules

- Default-deny policy
- Outbound rules
- Comment the rules



- Block unwanted traffic, only allow necessary
- Direct incoming traffic to internal nodes
- Hide vulnerable nodes from external threats
- Log traffic to and from the network

Firewall rules

Protocol	Source	Port	Destination	Port	Action
TCP	194.1.1.1	Any	180.2.2.2	80	Accept
TCP	Any	Any	Any	Any	Deny

Rule#	Source	Destination	Protocol	Destination port	Action
1	External	Webserver	TCP	80	Allow
2	Hacker	Internal	Any	Any	Drop
3	210.1.2.3	10.0.0.7	TCP	37337	Allow

Word variations, same meaning: deny/forbid/disallow/drop/block/refuse

Firewall Rulesets - Comments

Rule #	Action	Path	Source addr	Source port	Destination addr	Destination port	Protocol	Extra field	Comments
1	NO	in	us	*	*	*	*		ingress and egress
2	NO	out	them	*	*	*	*		filtering (Sect. 11.3)
3	NO	in	listed	*	*	*	*		block bad servers
4	OK	in	them	high	GW	25	TCP		inbound mail...
5	OK	out	GW	25	them	high	TCP	ACK	...our responses out
6	OK	out	GW	high	them	25	TCP		SMTP mail out...
7	OK	in	them	25	GW	high	TCP	ACK	...inbound response
8	OK	out	us	high	them	80	TCP		HTTP request out...

Always comment the firewall rules

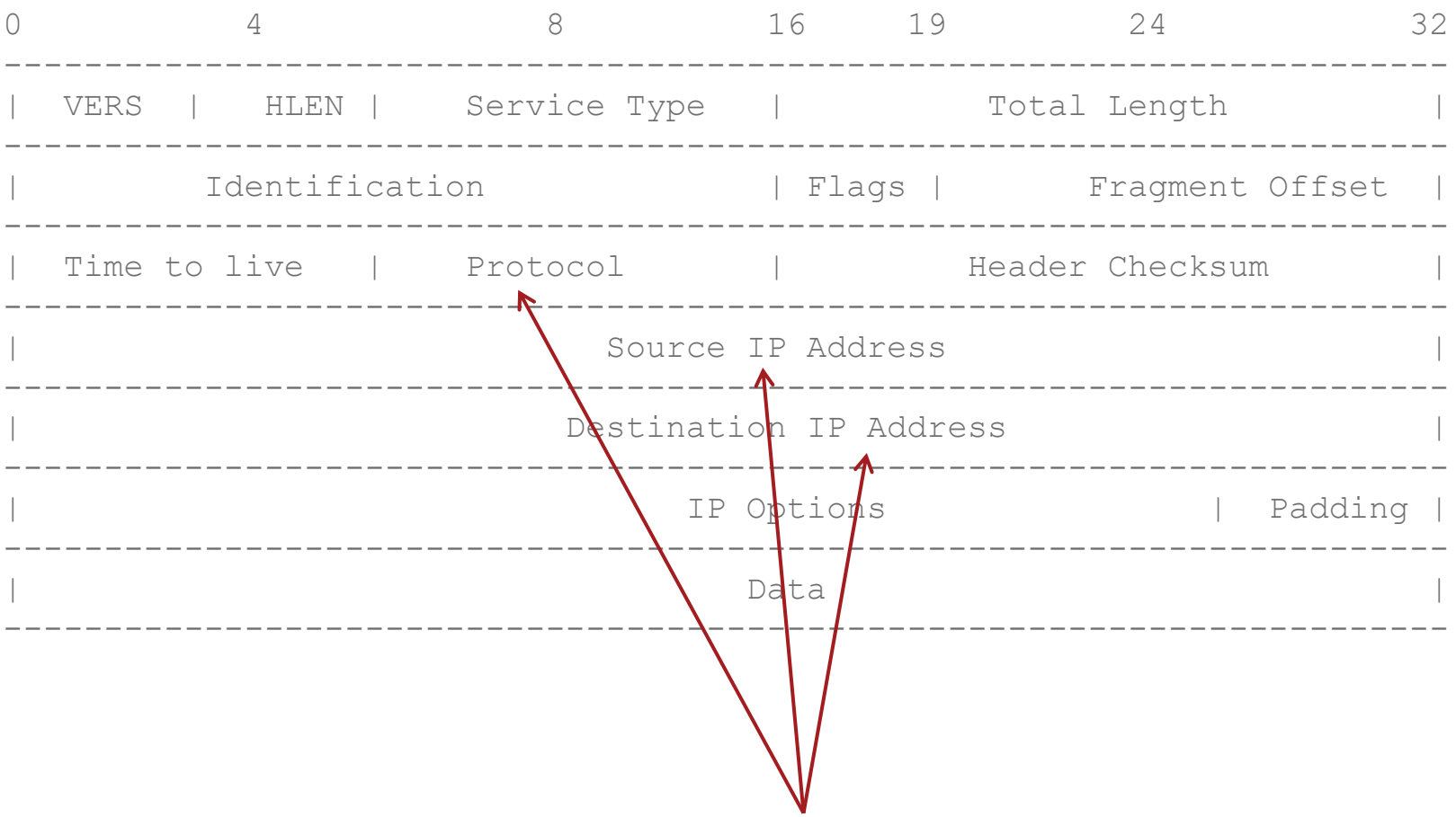
Example Stateful Firewall - Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

TCP - Transmission Control Protocol

IP Header

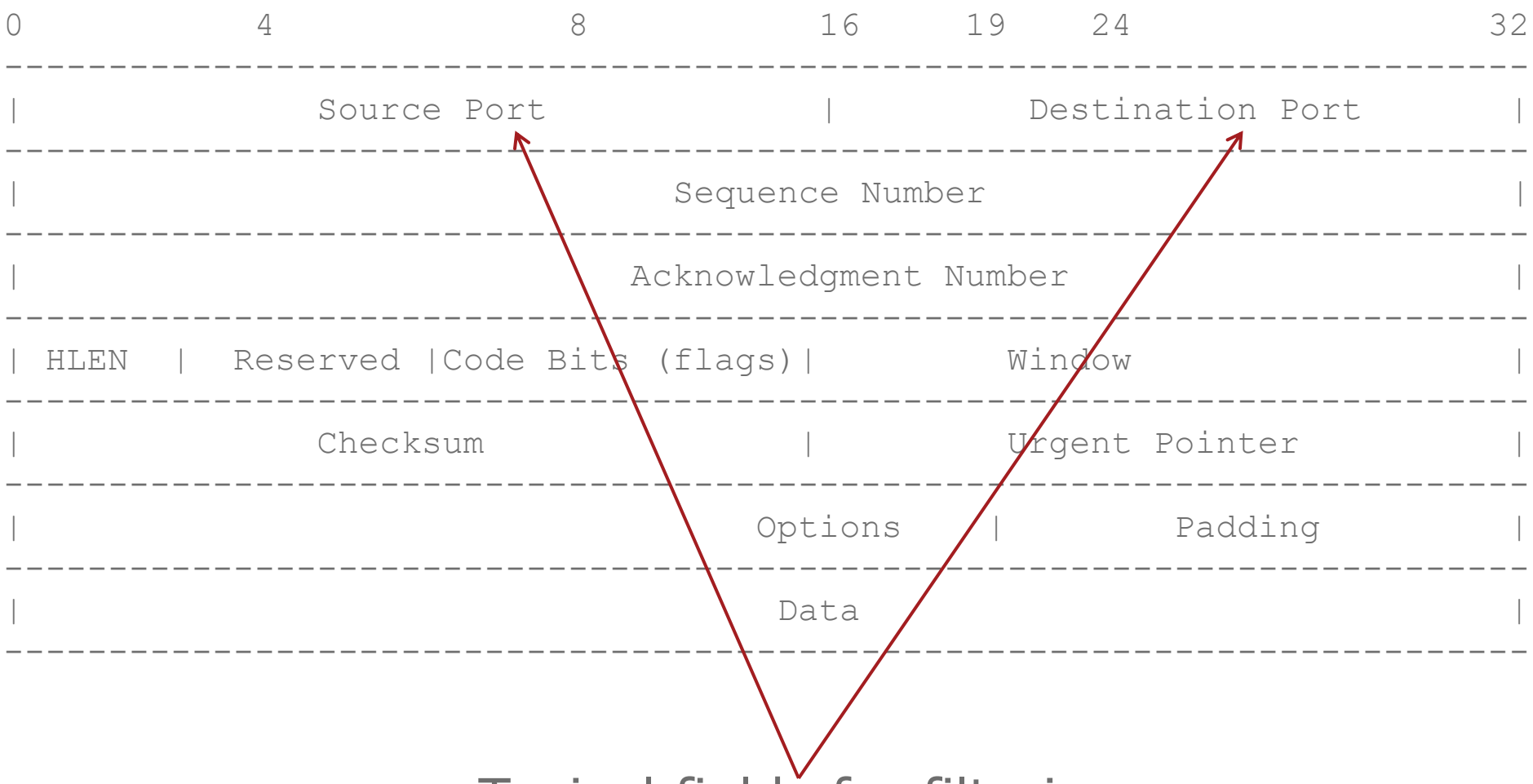
Protocol	Source	Port	Destination	Port	Action
TCP	194.1.1.1	Any	180.2.2.2	80	Accept



Typical fields for filtering

TCP Header

Protocol	Source	Port	Destination	Port	Action
TCP	194.1.1.1	Any	180.2.2.2	80	Accept



Typical fields for filtering

IPtables

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html#HOWARULEISBUILT

iptables -F INPUT *(flush)*

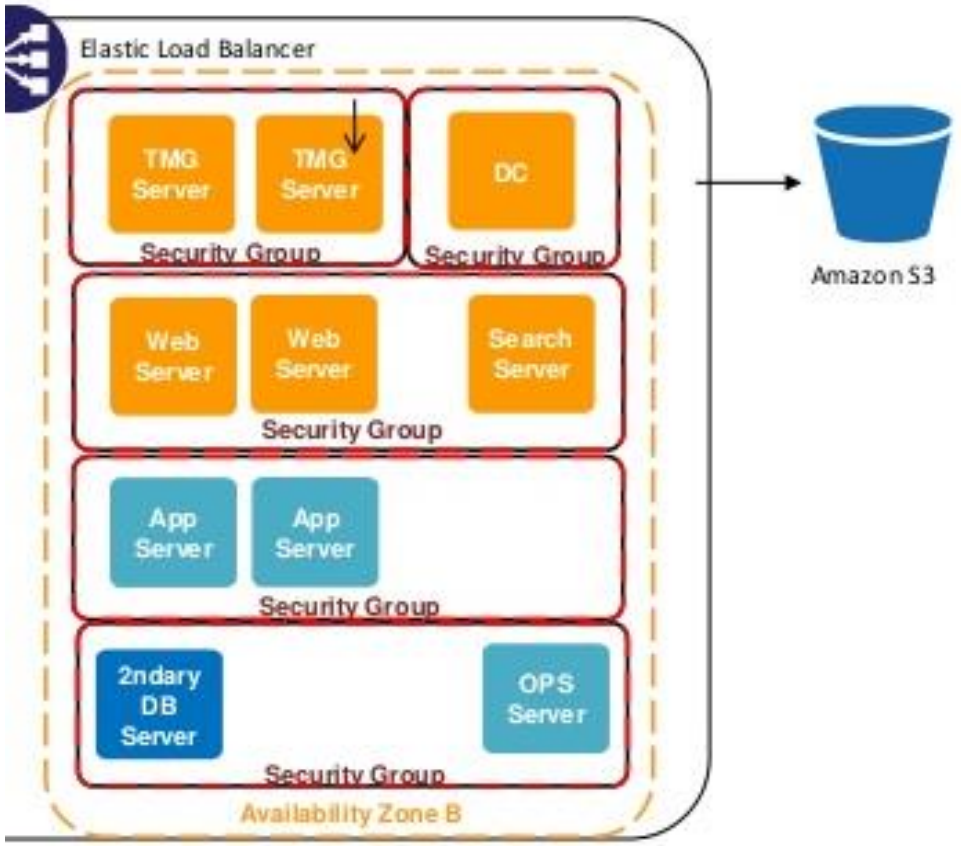
iptables -A INPUT -i eth0 -j DROP *(append)*

Firewalls and Security Groups - Software Defined Networking

Security Groups

A *Security Group* is like a 'basic stateless firewall'

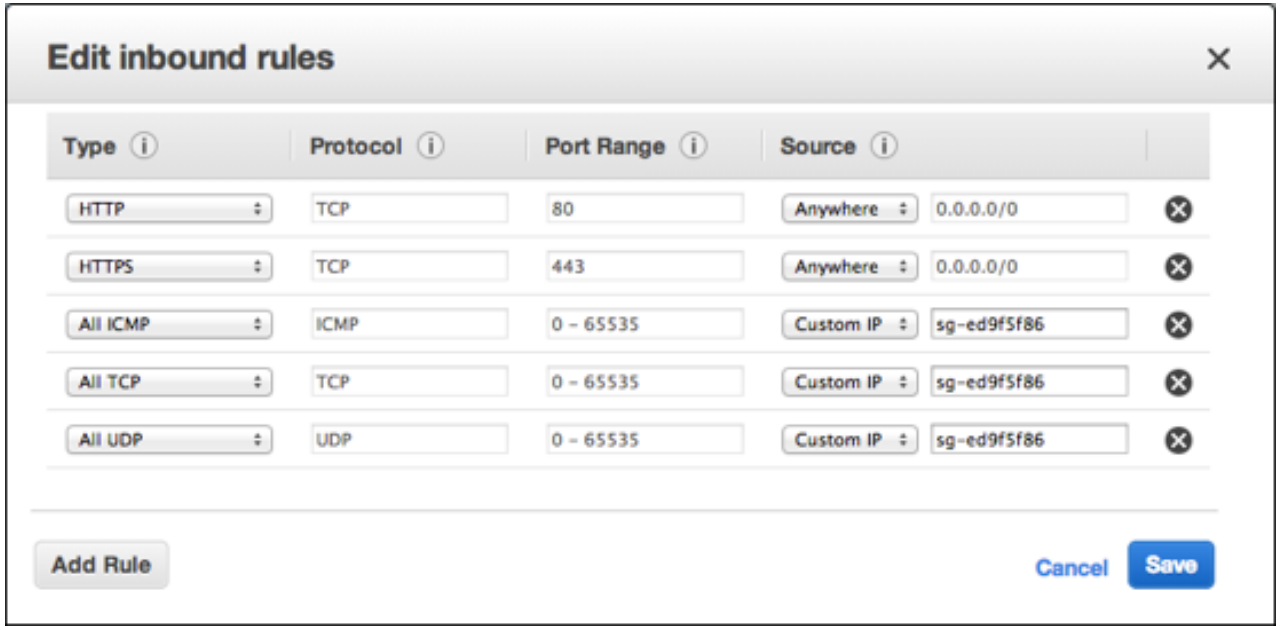
A Security Group is a container for security group rules.
Works like firewalls – isolating traffic to VMs, controlling traffic to and from ports and instances



Security Groups – Cloud computing

One or more Security Groups can be assigned to an instance

Security group rules control the inbound traffic allowed to reach the instances associated with the security group.
All other inbound traffic is discarded, and all outbound traffic is allowed by default



Security Groups

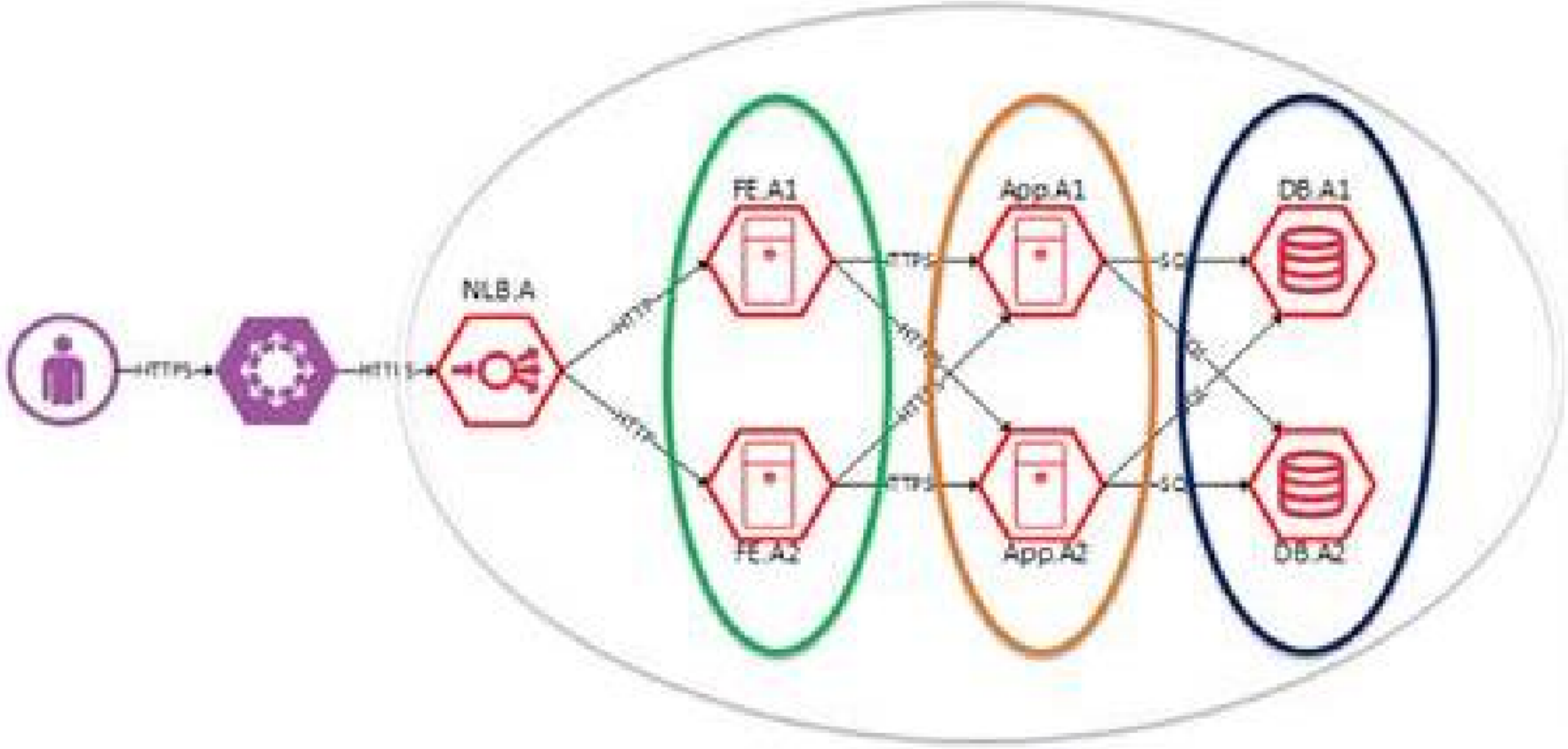
Instances in a Security Group cannot communicate with other instances unless specifically allowed.

"Small cheap firewalls" in front of every single server/system.

As default are each instance firewalled from other instances – level of segmentation that is almost impossible outside cloud.

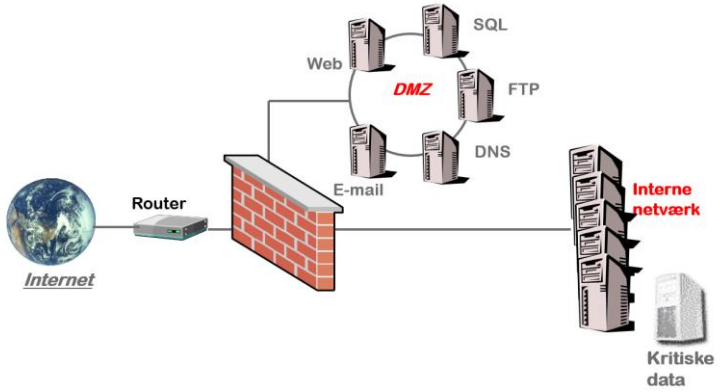
SDN – "Software Defined Networking"

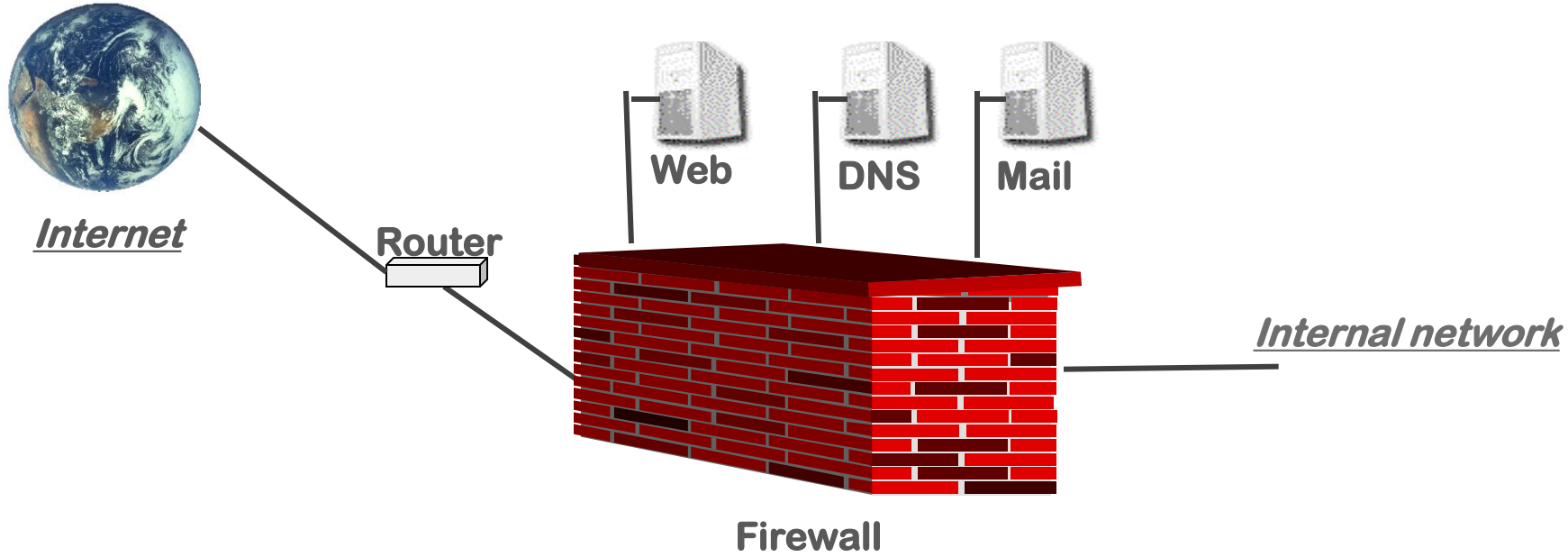
Microsegmenting – no trust (SDN)



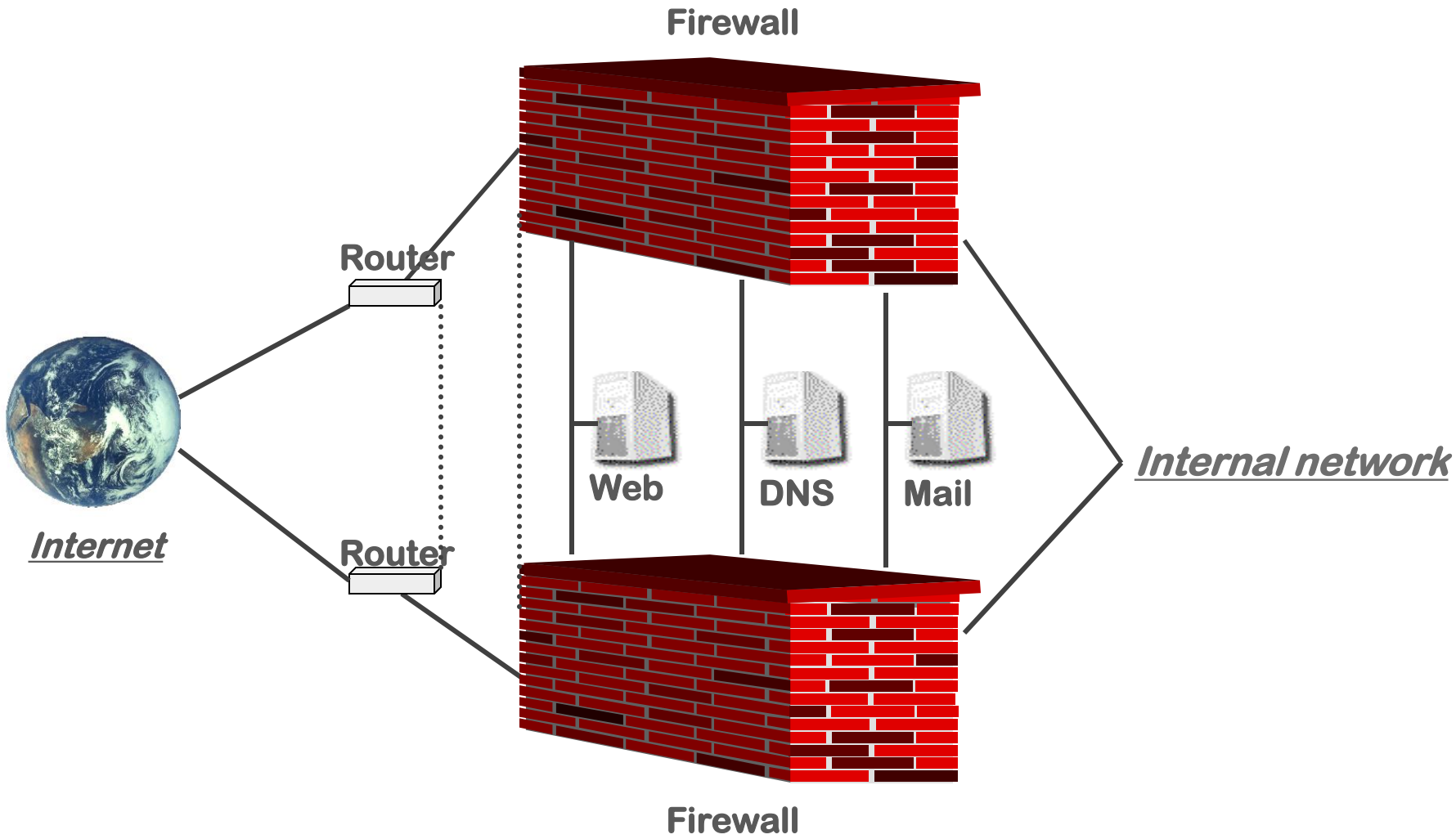
Security architecture
classic security measures

Multiple DMZs

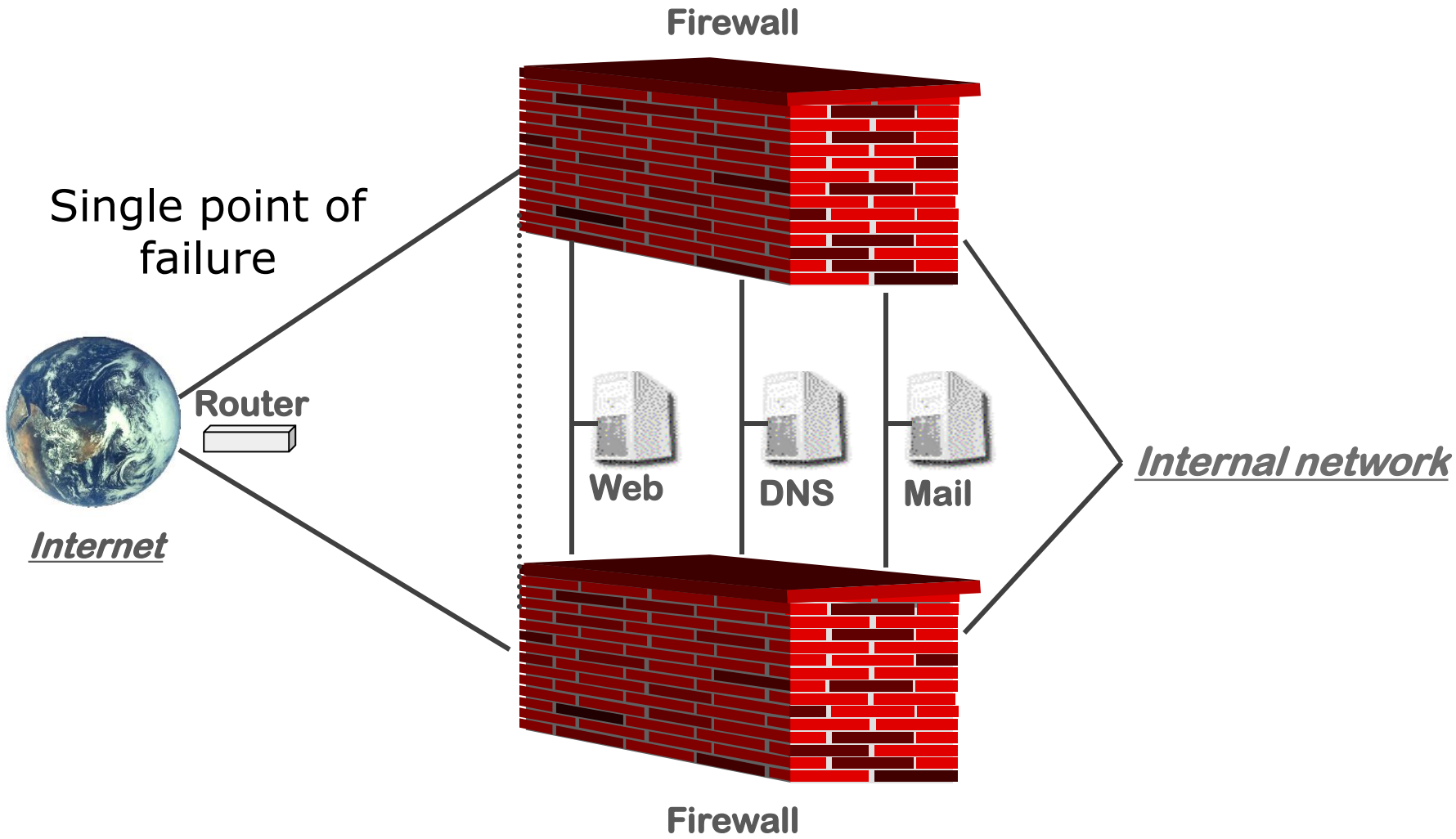




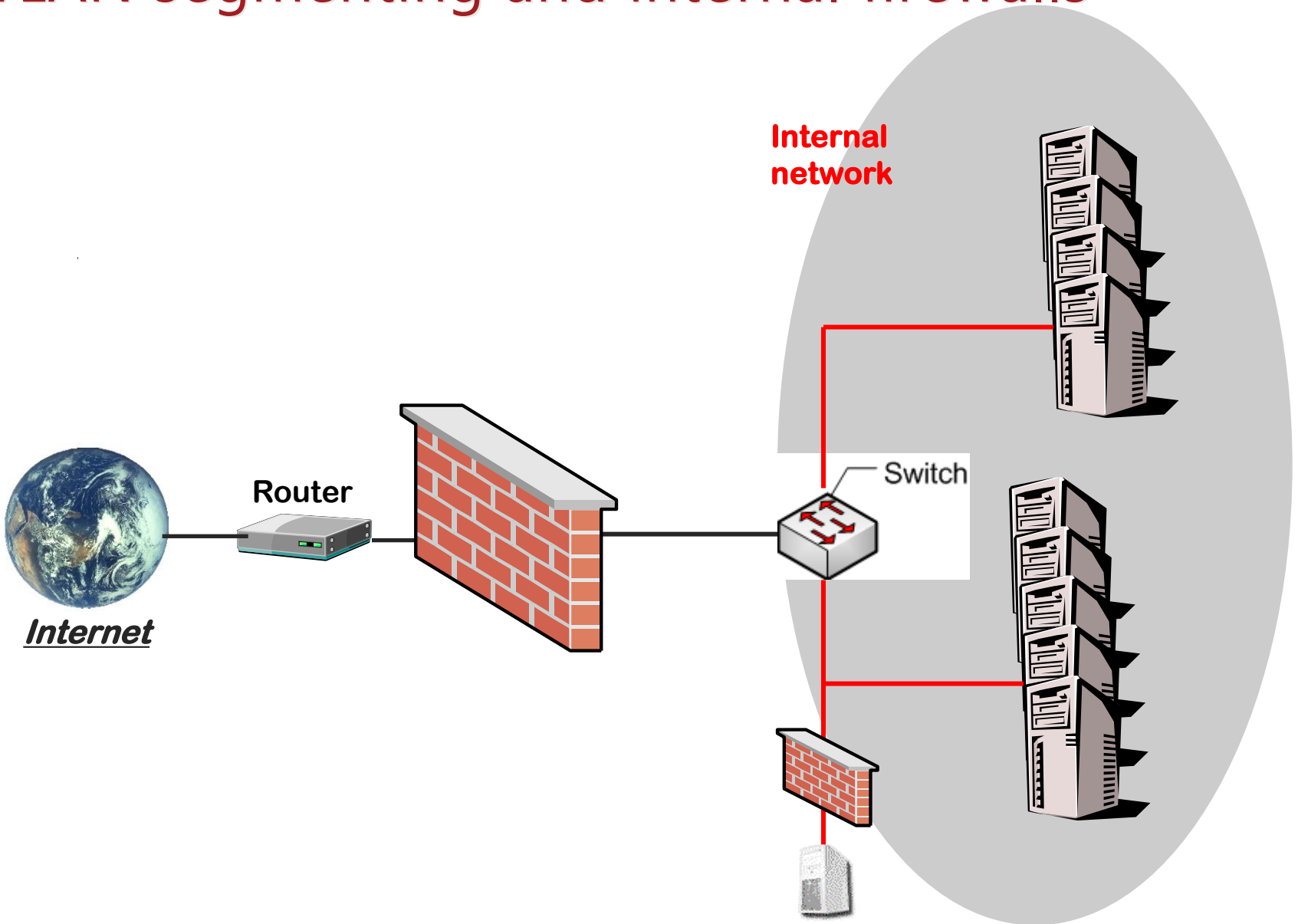
Multiple firewalls



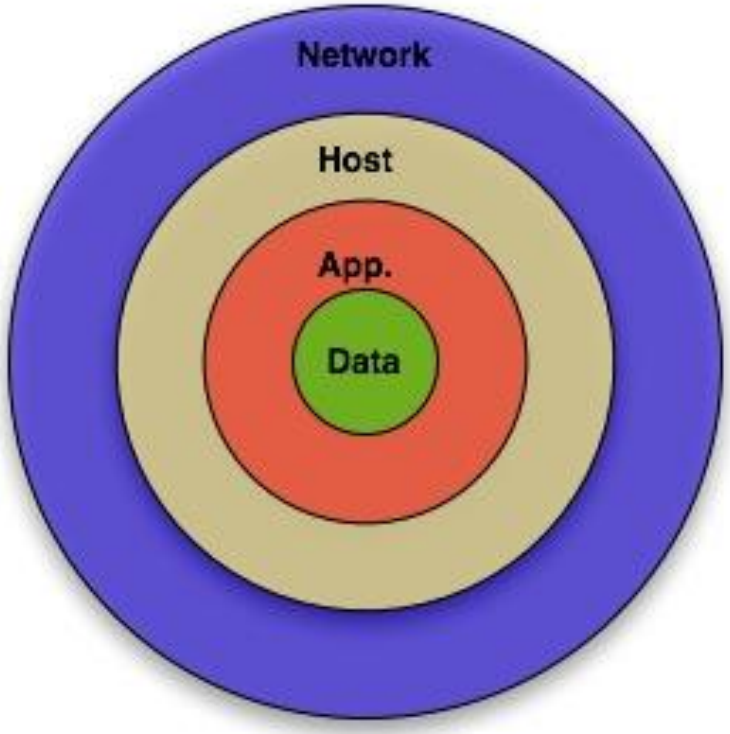
Multiple firewalls



Network – vLAN segmenting and internal firewalls

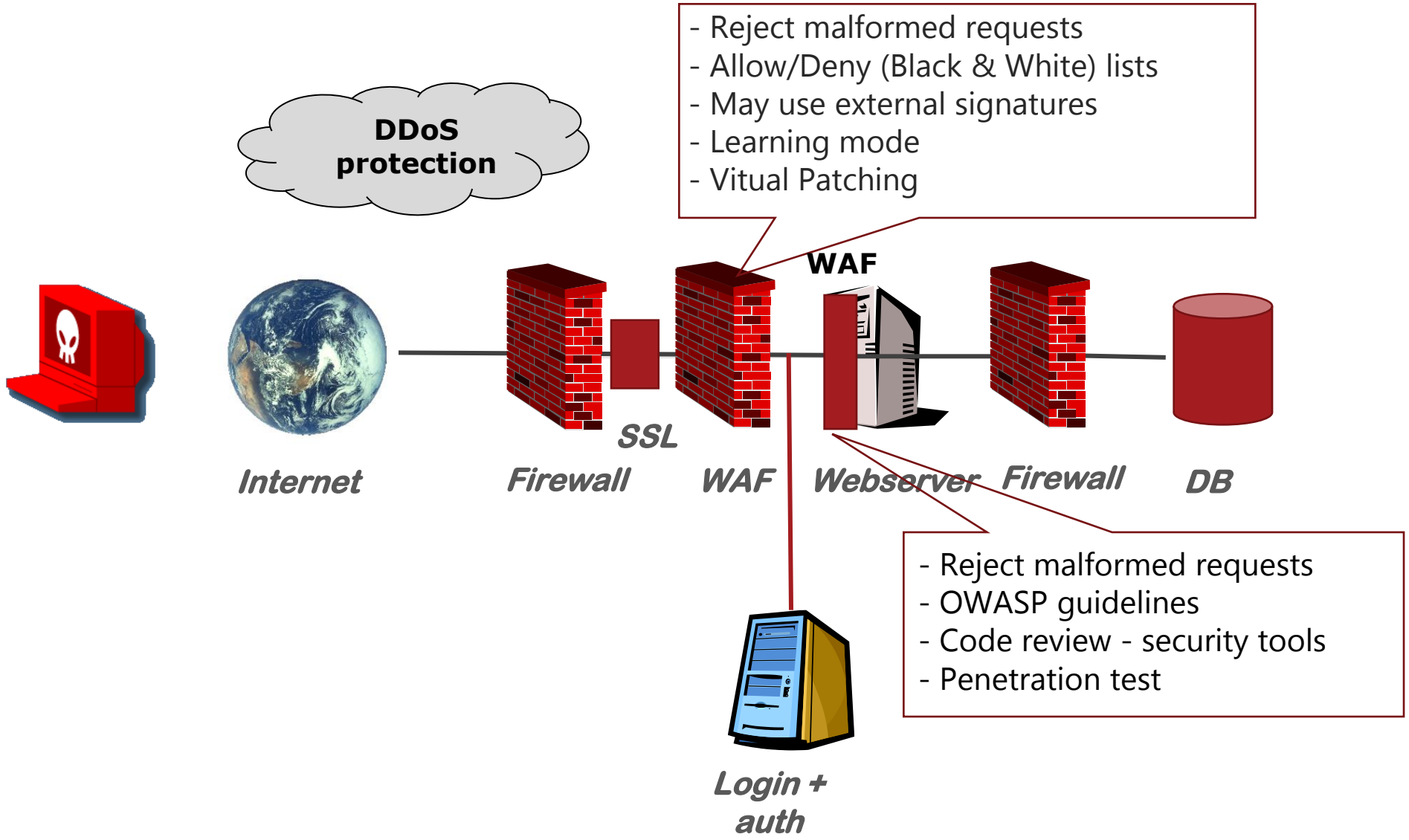


Security architecture



Defense in Depth

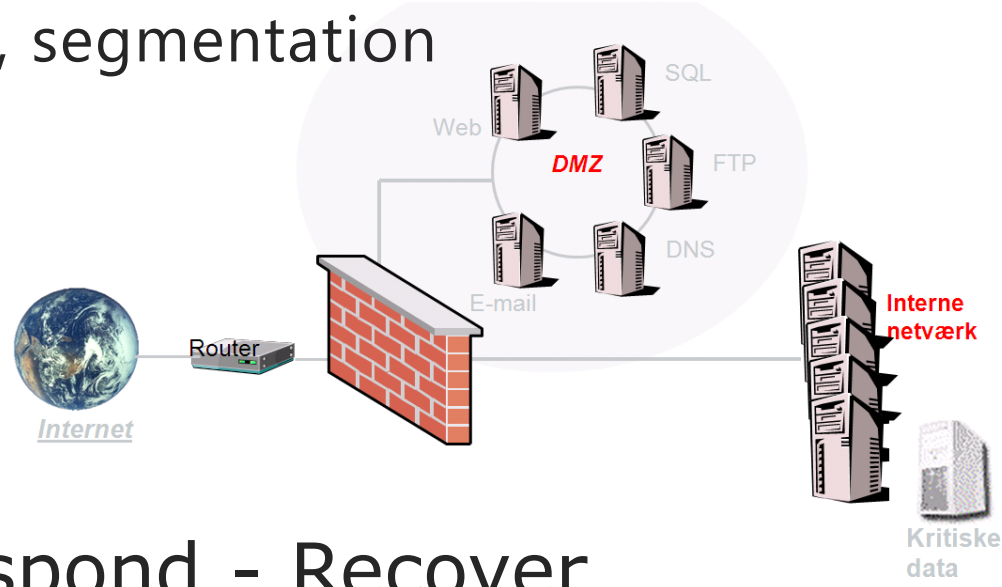
Security architecture - Layers of security and the firewall



Which is “Best”?

Security measures

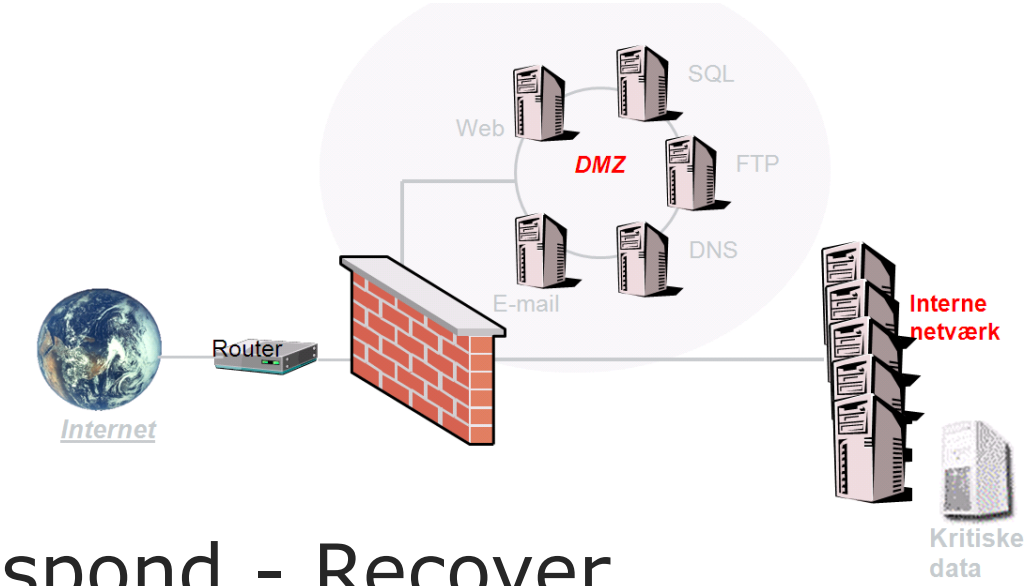
- IDS/IPS
- Scanning for virus and webtraffic
- Central loghost
- SIEM (Security Information and Event Mangement – log collection)
- Many DMZ's
- VLAN, internal firewalls, segmentation
- DDoS protection
- DNS security
- …



Prevent – Detect – Respond - Recover

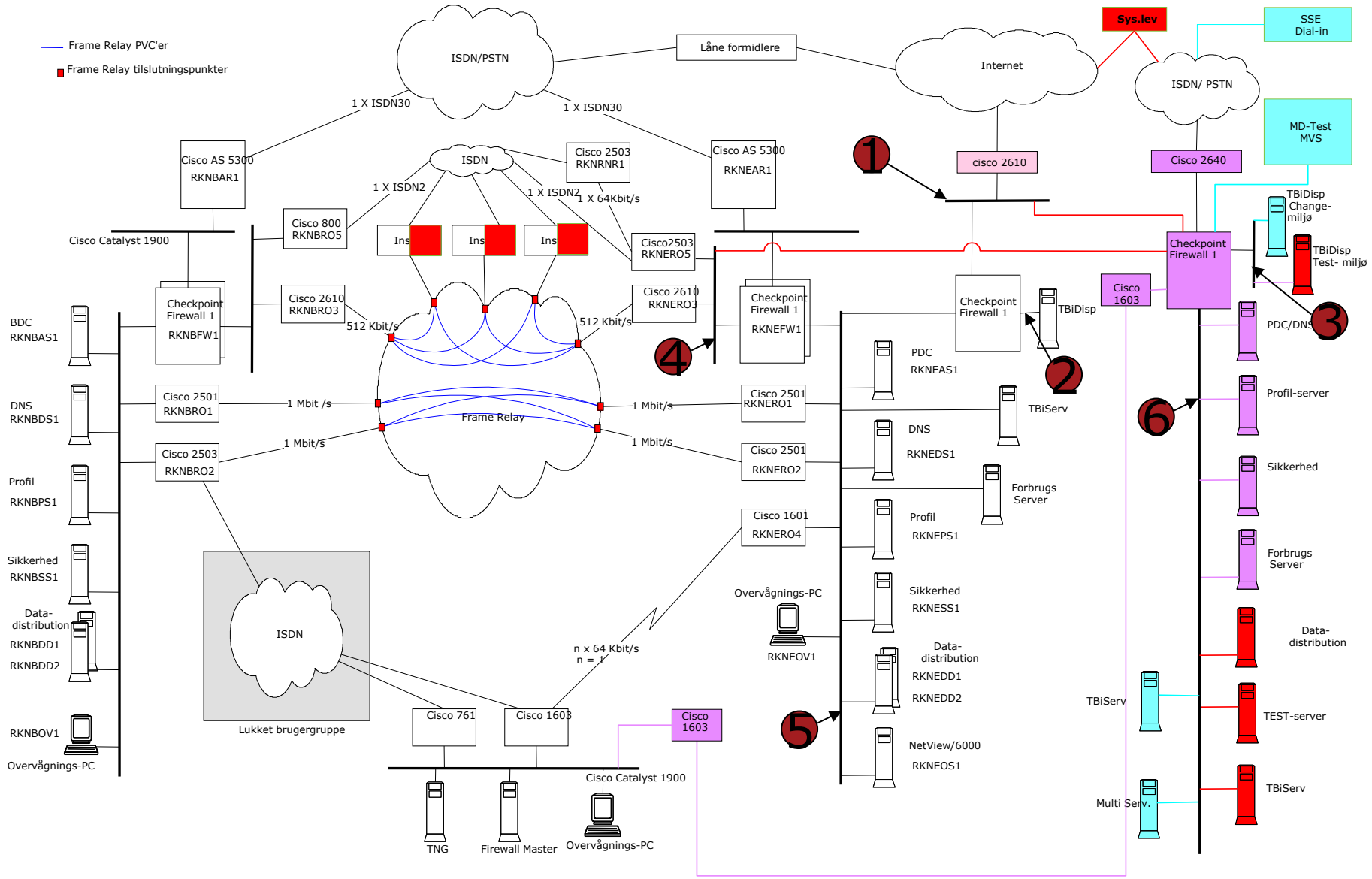
More examples of security measures

- Patching/updating
- Configuration management
- Filtering outgoing traffic
- Minimizing number of services (hardening)
- Allow/Deny list (Whitelist/Blacklist)
- …



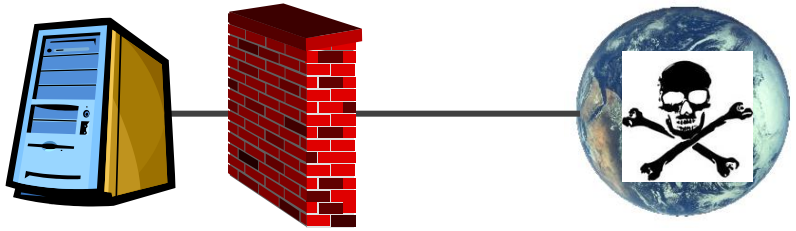
Prevent – Detect – Respond - Recover

Large network (example)

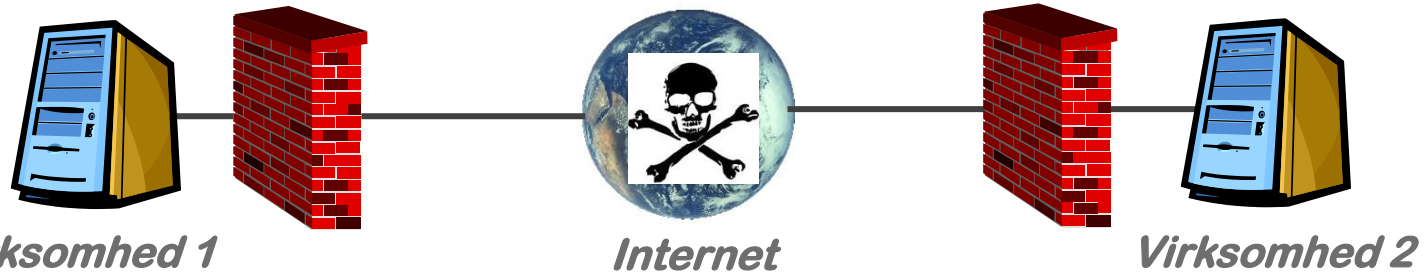


Tunnels

The need for tunnels



"I'm ok – but we can't trust the network"



"I'm ok, and you're ok – but we can't trust the network"

The need for tunnels

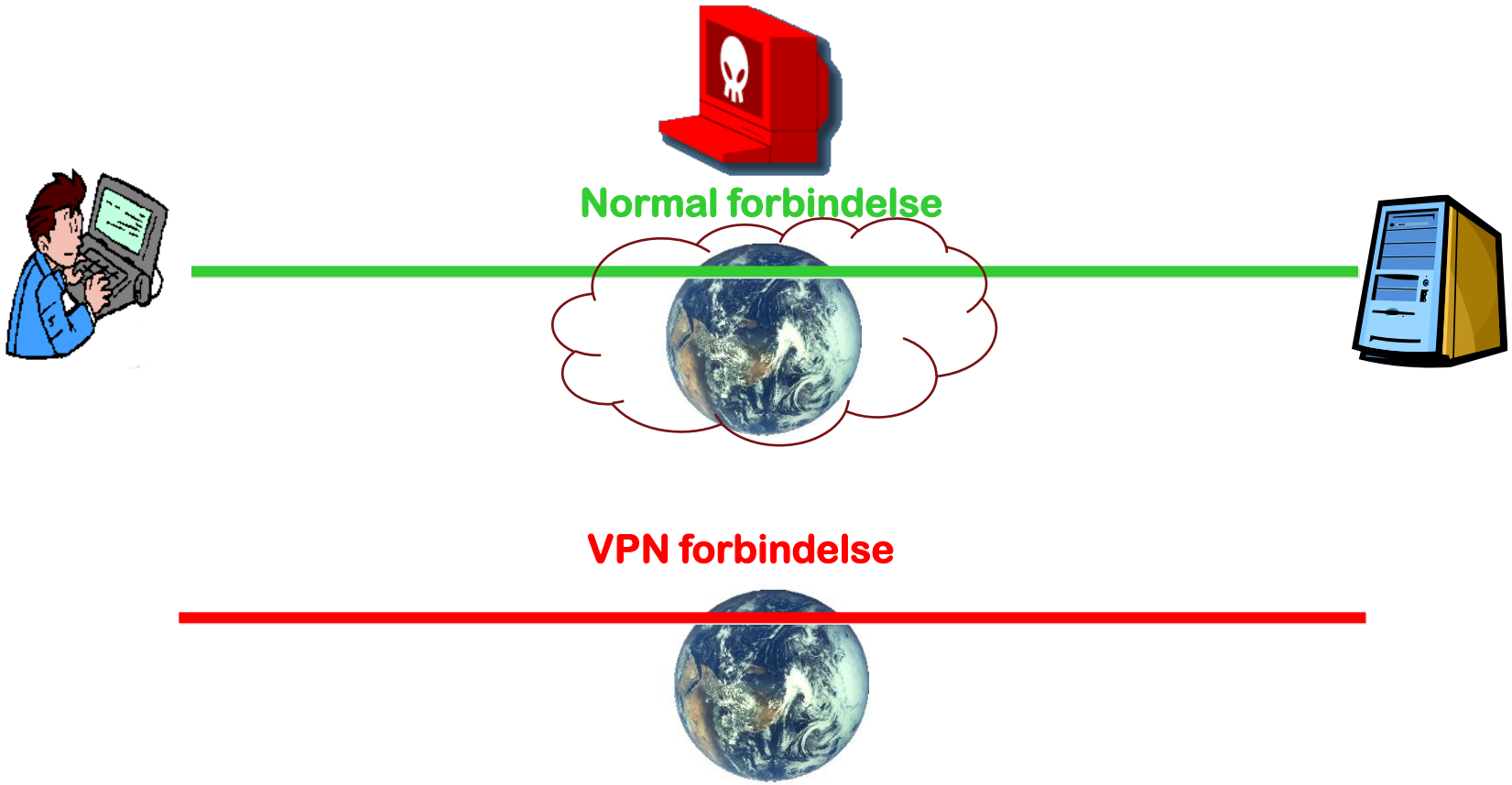
Default TCP/IP packets are plaintext

The full packet content (header plus payload) is visible to every party with access to the packet stream, and alterable by any inline party
(all intervening routers, switches, gateways, and service provider equipment)

For protection, one idea is to encrypt entire packets at origin devices before network transmission

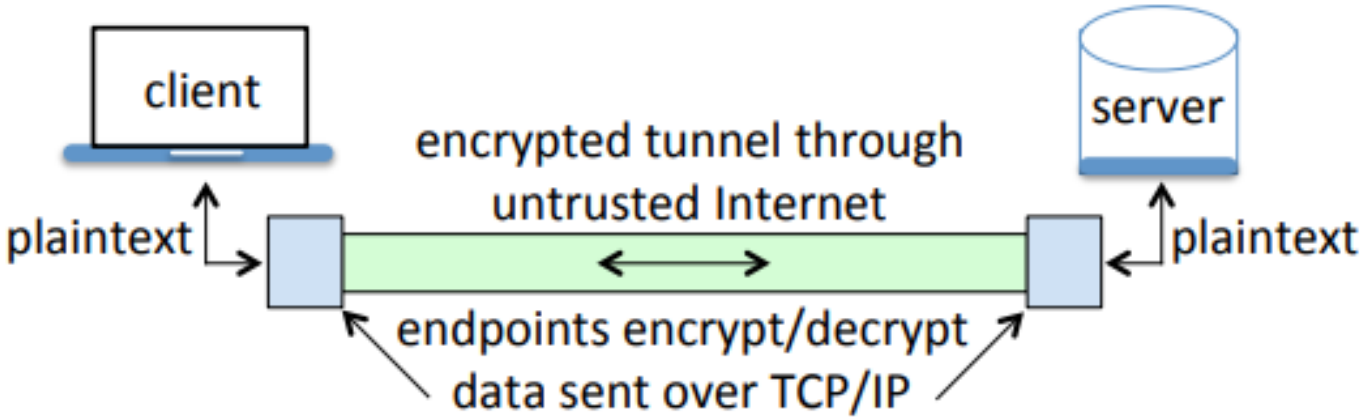
VPN

VPNs encrypt traffice between you and the VPN endpoint



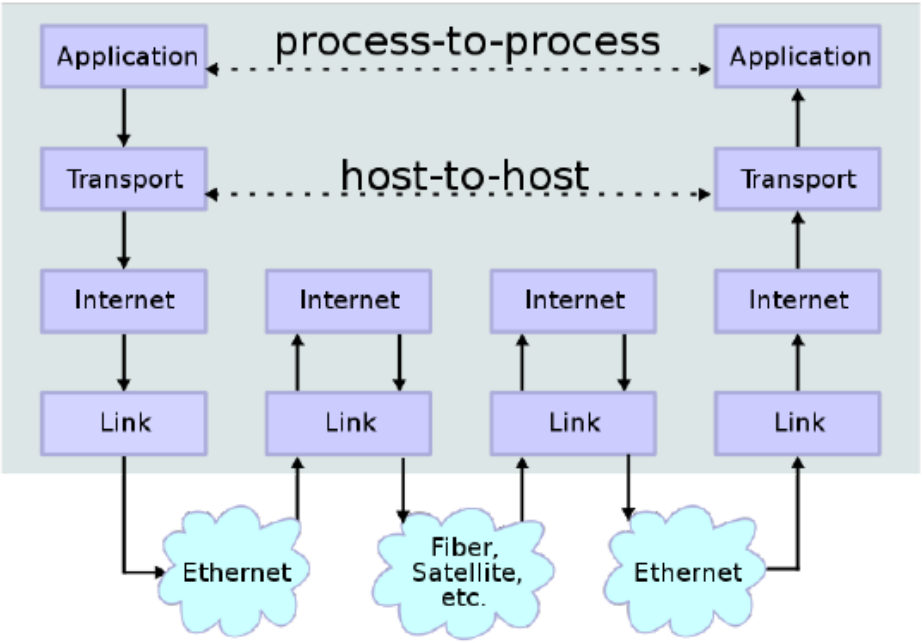
VPN

Encrypted connection between two networks

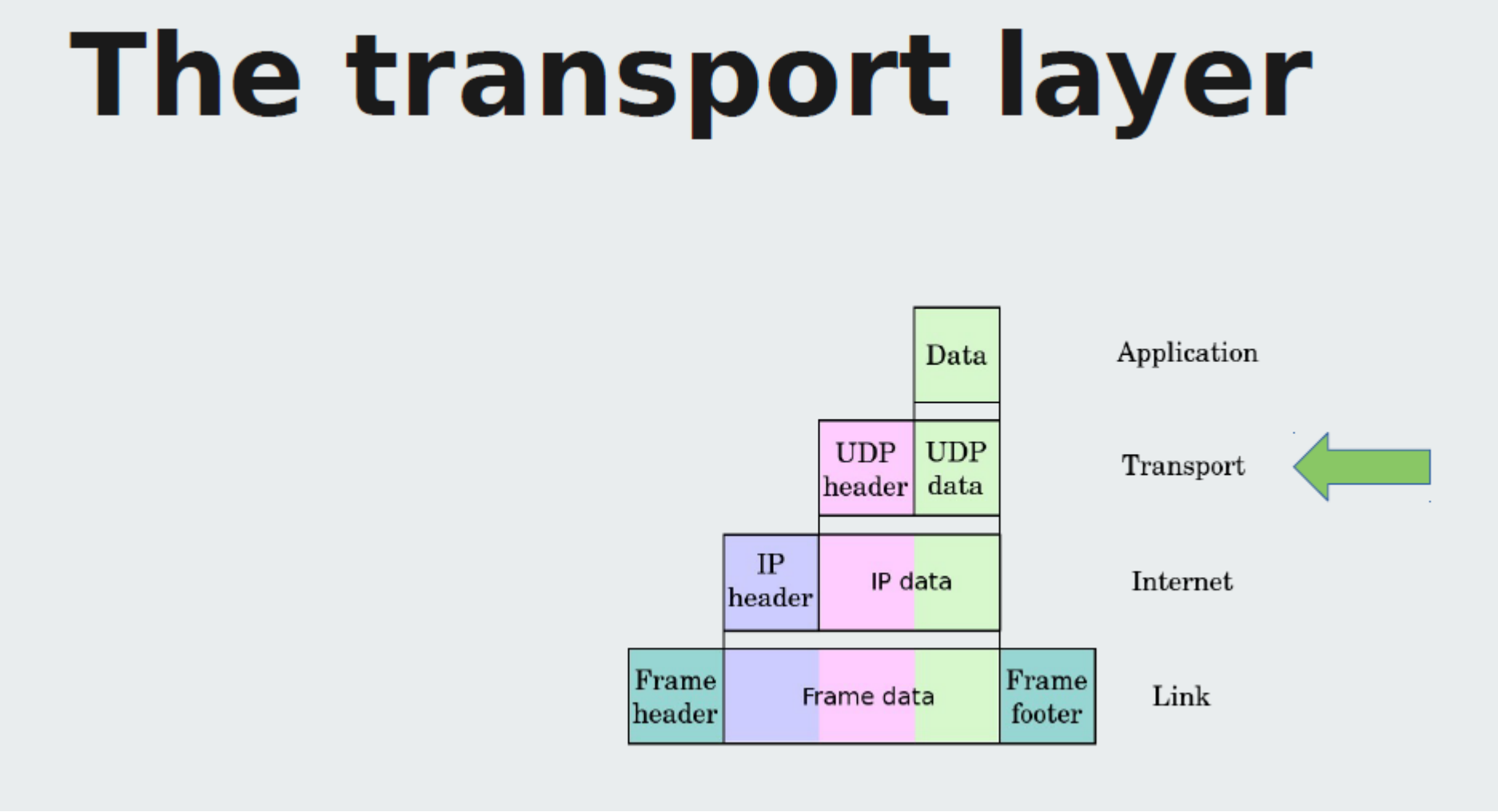


Tunnels

Where to encrypt?



Tunnels


The transport layer
Data
Application
UDP header
UDP data
Transport
IP header
IP data
Internet
Frame header
Frame data
Frame footer
Link

Tunnels

SSL/TLS

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to:

"Provide a secure channel between two communicating peers" [RFC 8446 TLS 1.3]

SSL and TLS protocols

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecation planned in 2020[11]
TLS 1.1	2006	Deprecation planned in 2020[11]
TLS 1.2	2008	
TLS 1.3	2018	

Tunnels

Security goals of TLS

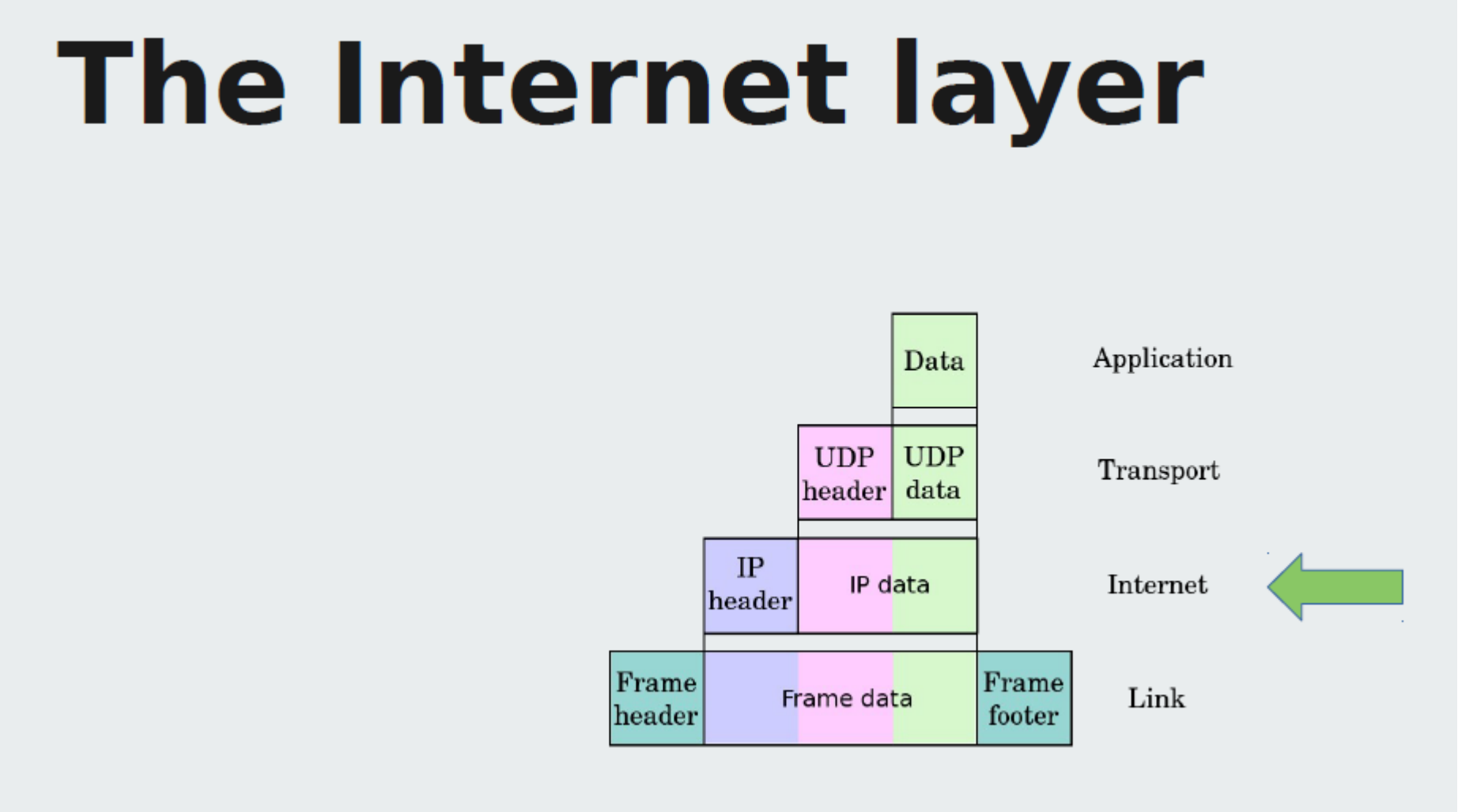
Specifically, the secure channel should provide the following properties:

Authentication: The server side of the channel is always authenticated; the client side is optionally authenticated.

Confidentiality: Data sent over the channel after establishment is only visible to the endpoints.

Integrity: Data sent over the channel after establishment cannot be modified by attackers without detection.

Tunnels – network layer security



IP-Sec VPN

Encrypted connection:
host-host
network-network, host-network

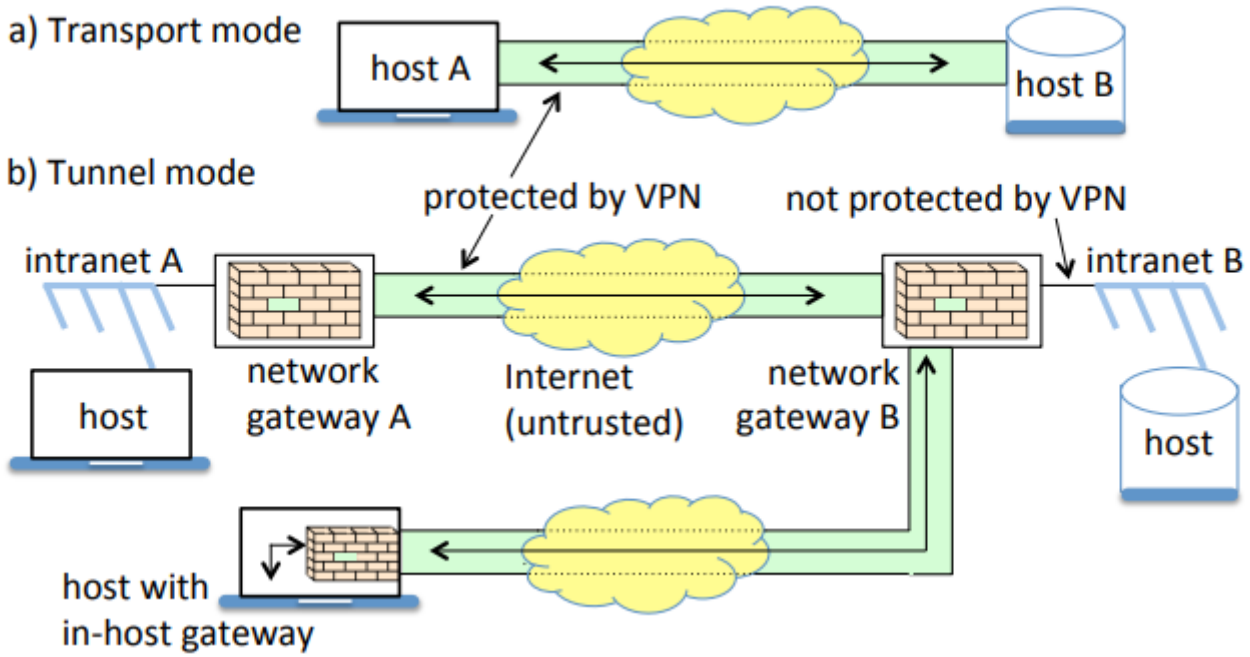
VPN design	VPN architecture	Notes and use cases
transport mode	host-to-host VPN	provides end-to-end security (VPN endpoints are final destination)
tunnel mode	network-to-network	network gateways add/remove VPN security (no VPN protection internal to gateway)
	host-to-network	for remote host access to enterprise (in-host gateway adds/removes VPN security)

Table 10.3: VPN designs and architectures. See Fig. 10.9 for illustrations.

Note that transport mode cannot be used if one endpoint is a network, as the resulting IPsec packet has only one IP header thus there would be no IP address available for a second-stage delivery

VPN

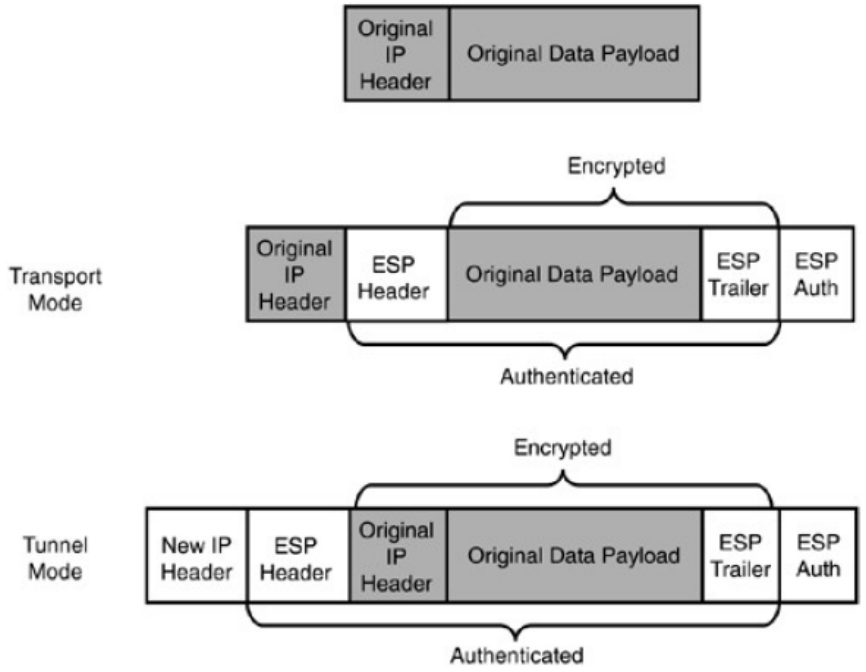
Transport mode or tunnel mode



Tunnels

IPSec – AH, ESP, SA

- Authentication Header (AH)
  - Integrity and authentication
- Encapsulating Security Payload (ESP)
  - Confidentiality
- Security Association
  - Details on ciphers, keys, lifetime, etc.
  - One directional



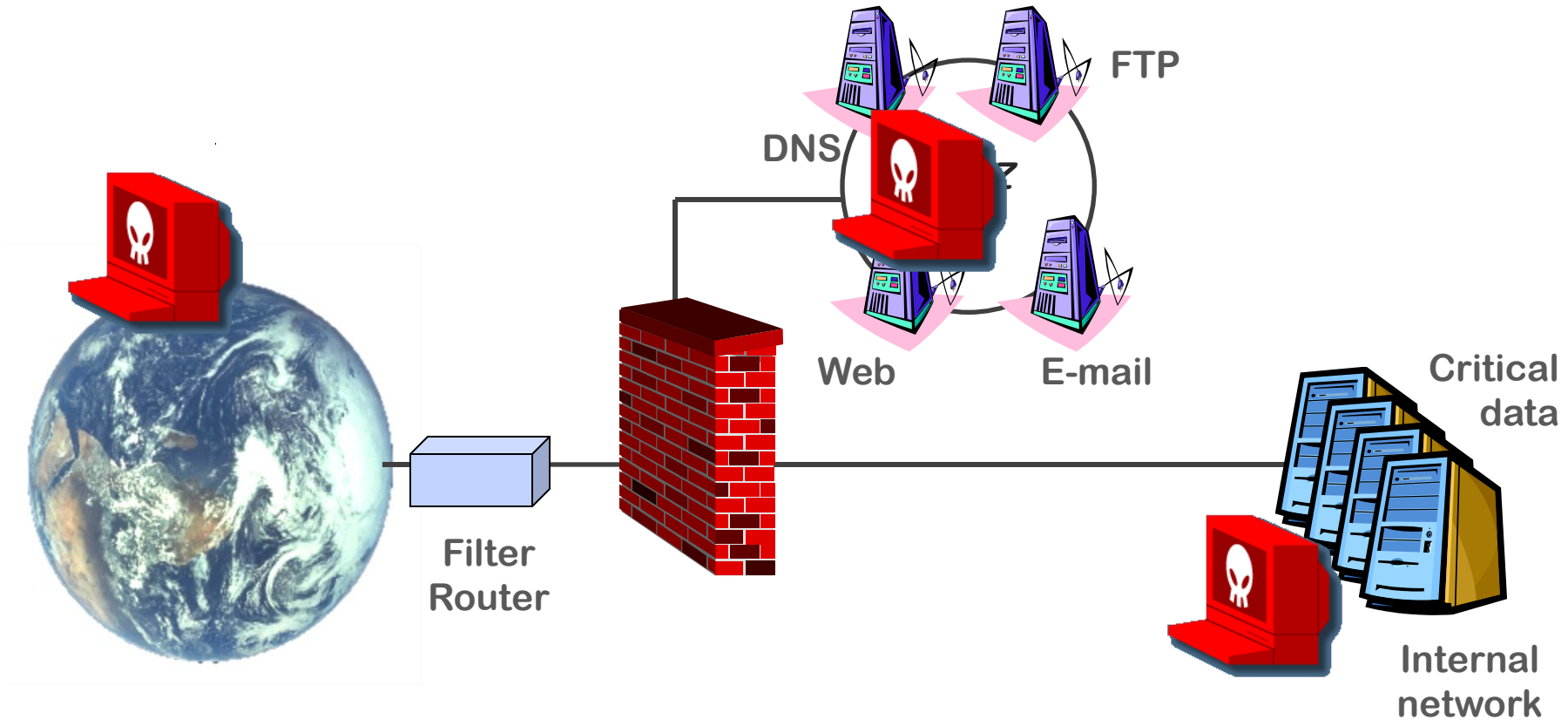
Pause


SECURITY CHECK
VISA
MasterCard
Is there your card in the hackers database?
You can easily check here, just enter your card info:
Card number:
- - -
CVC@ (CW2):
Check!

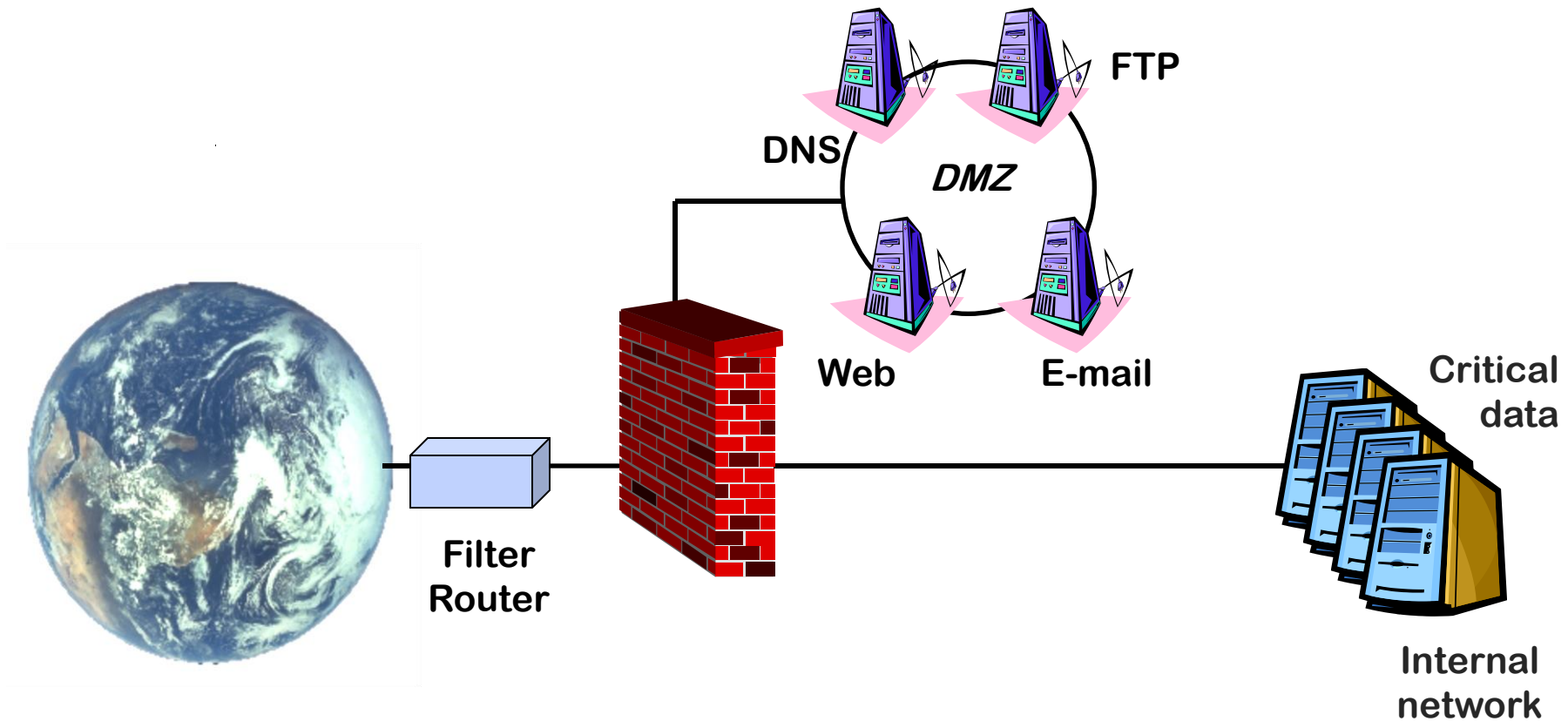
Security architecture

components and common security issues

3 major areas of attack



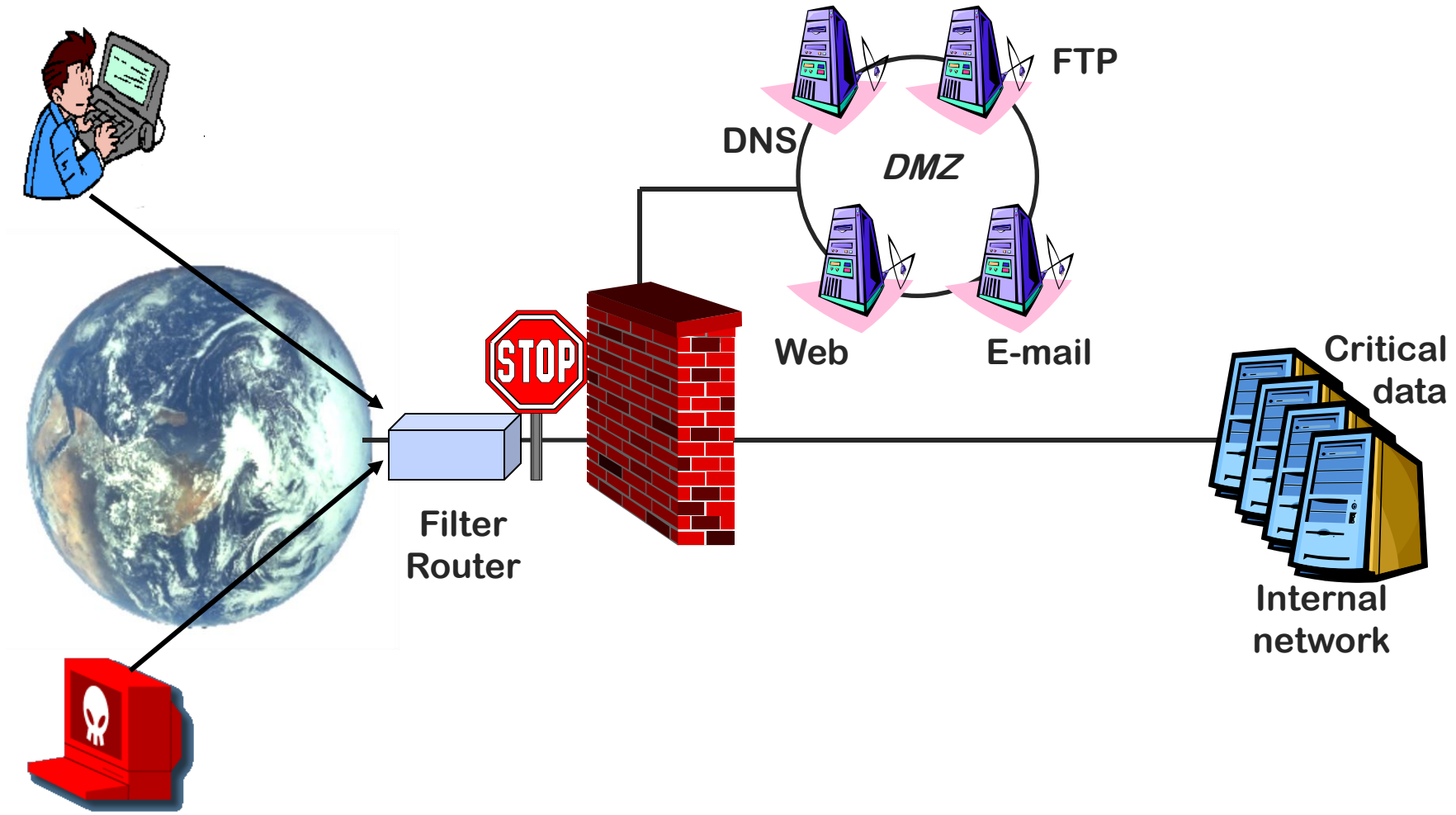
The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

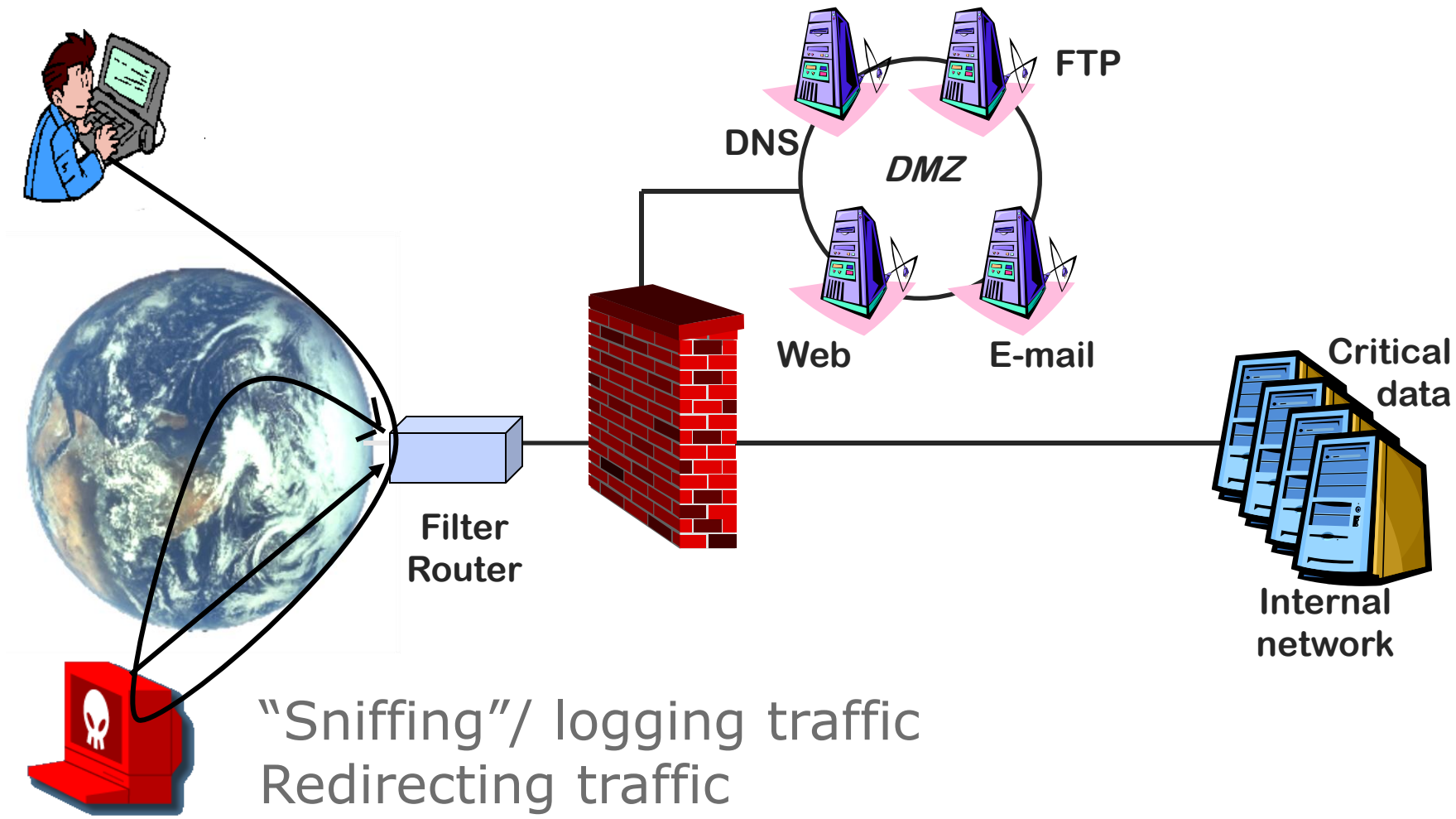
Typical router problems

Too many open ports (access or DoS)
Router default accounts and bad passwords

Router problems - consequences

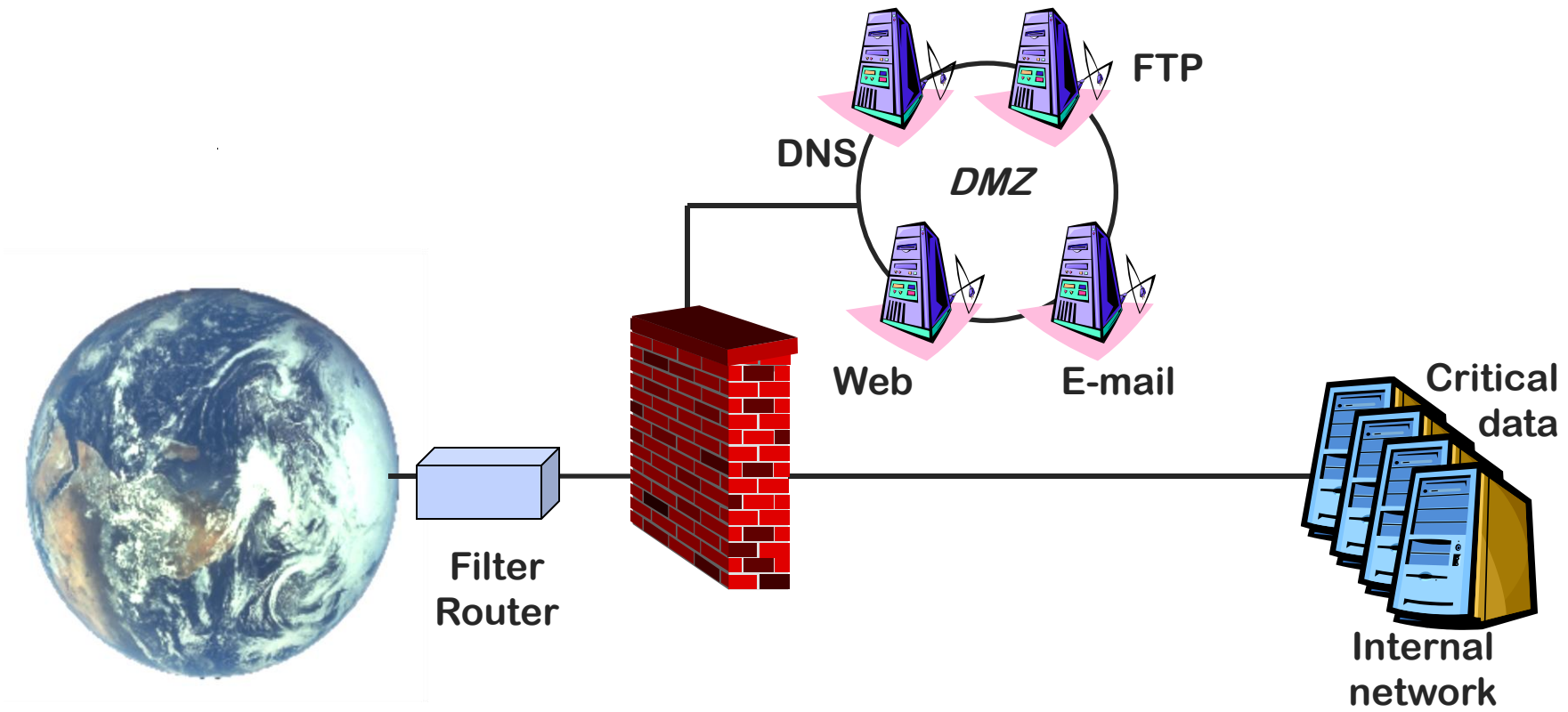


Router - consequences

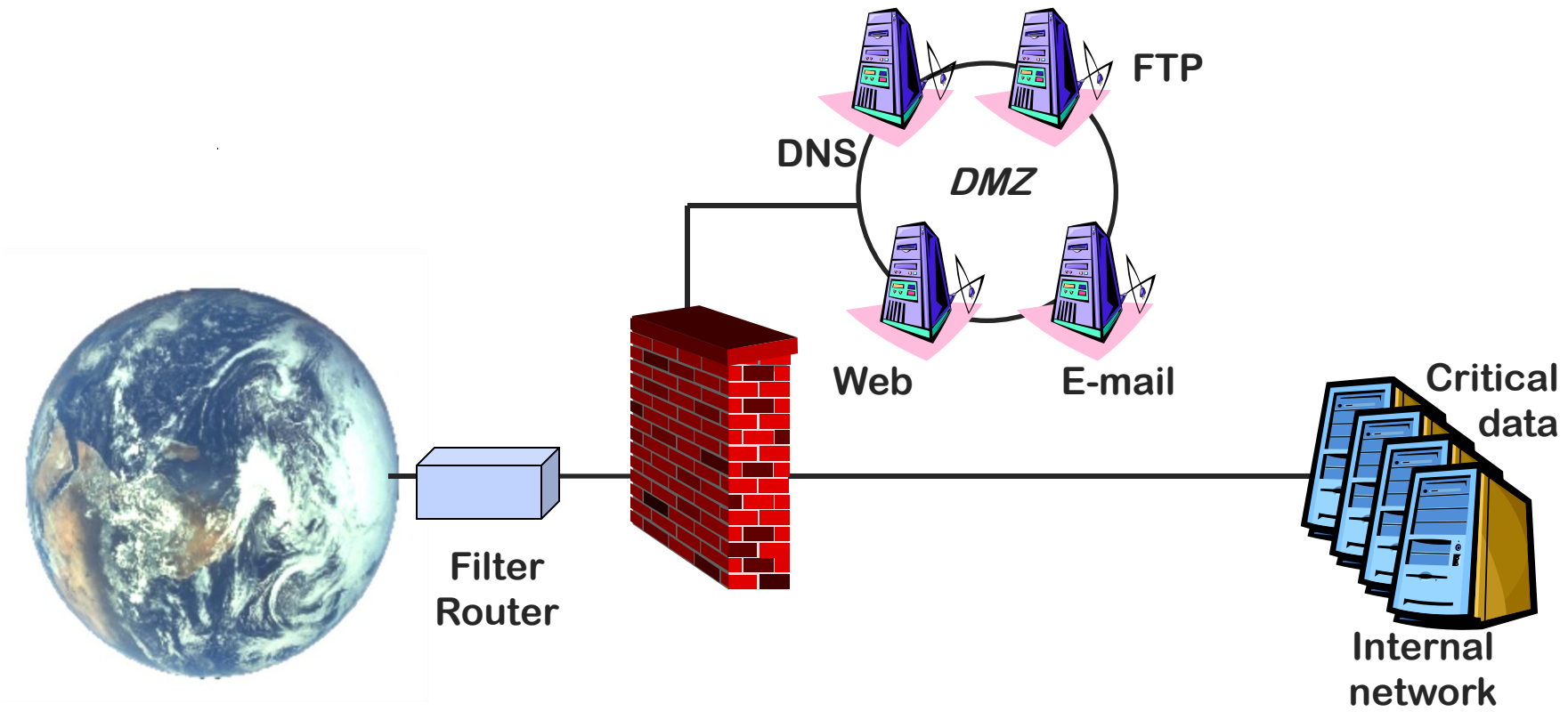


"Sniffing"/ logging traffic
Redirecting traffic

The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

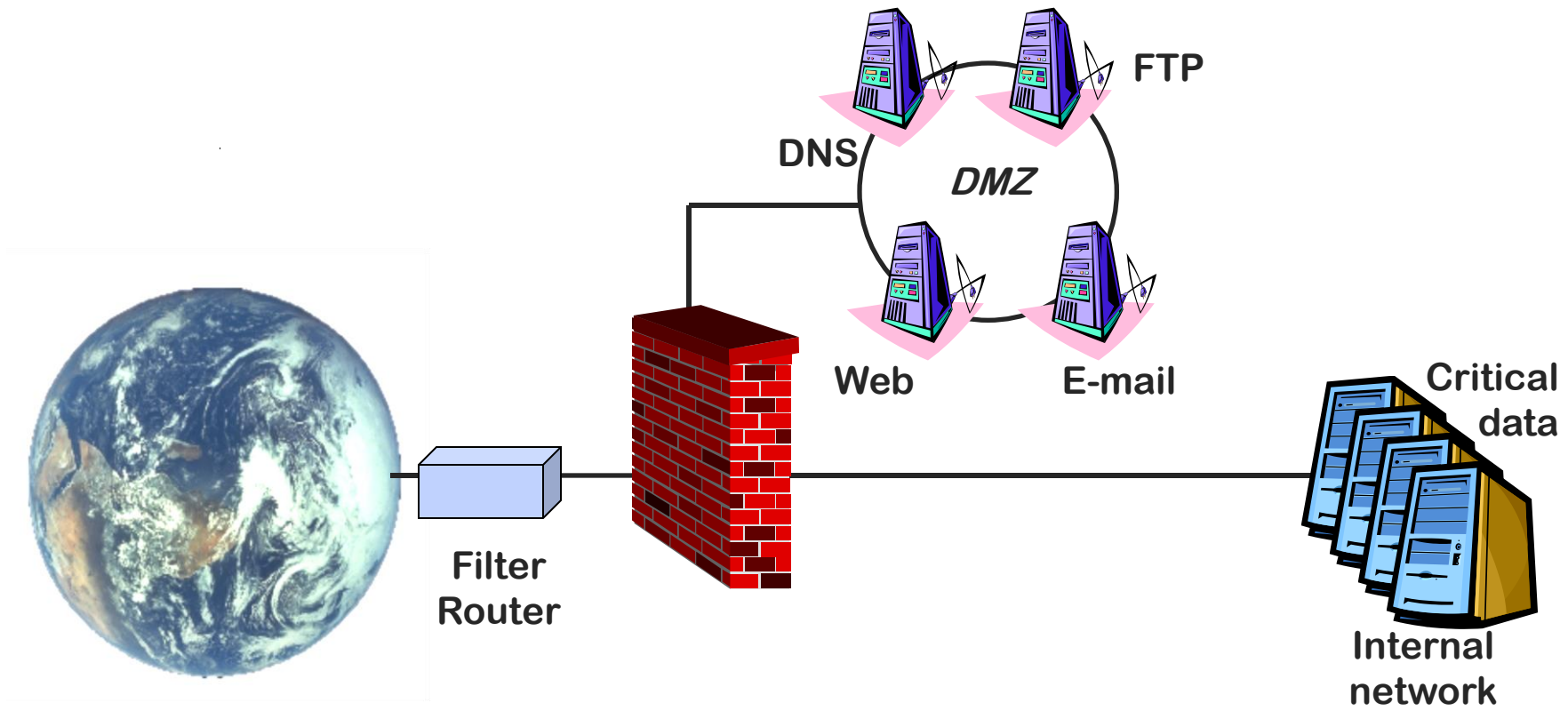
The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

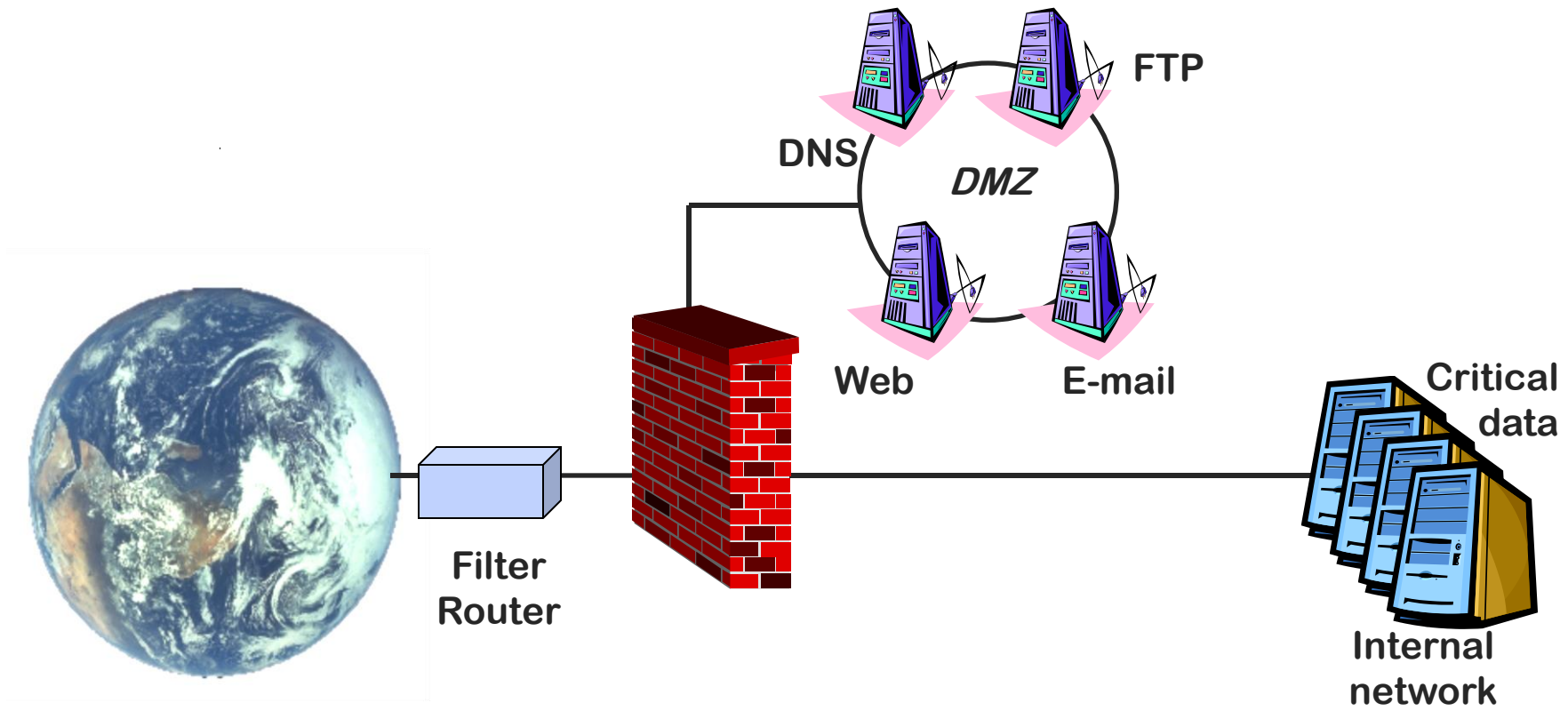
Typical firewall problems

- Mistakes in configuration
  (The FW does not protect as you think)
- Too many open ports (Access or DoS)
- Too many protocols allowed - ping etc.
- Changes in configuration never fixed
- Management services available on FW

Typical setup



Typical setup



Typical DNS issues

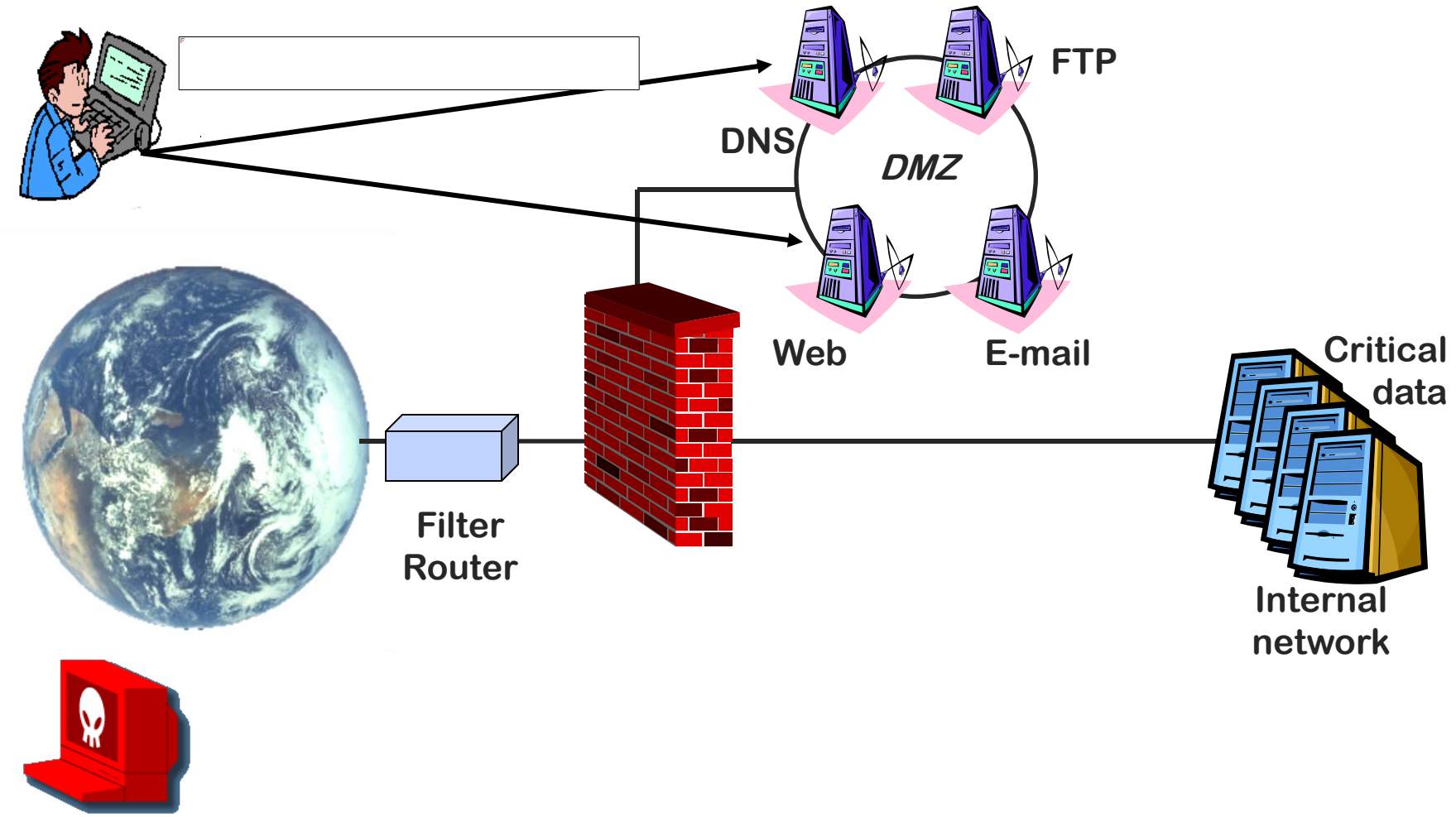
DoS

Re-direct traffic to other IP-addresses (Hijacking/Man-in-the-Middle)

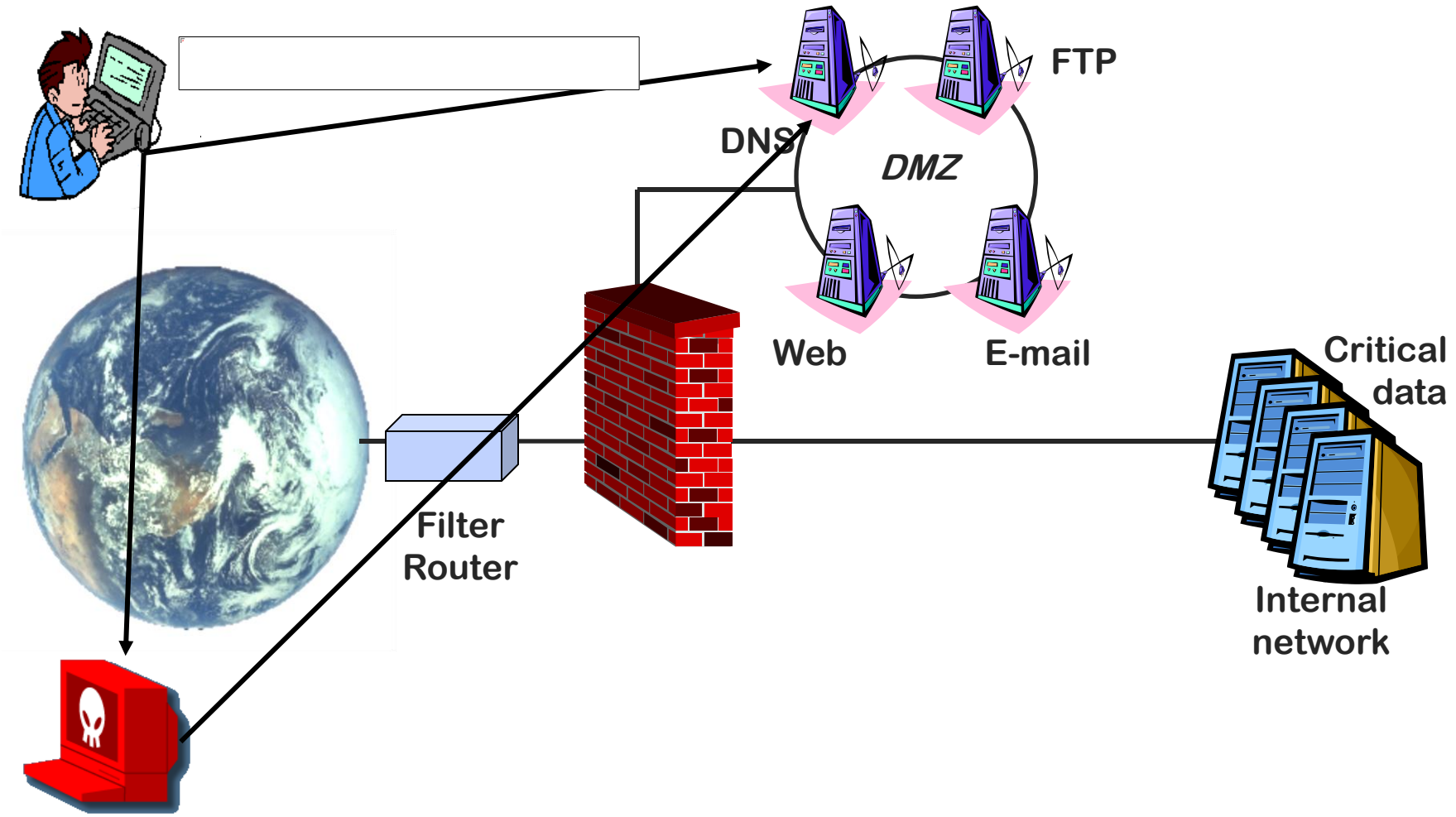
Execute commands on the server

Stepping Stone

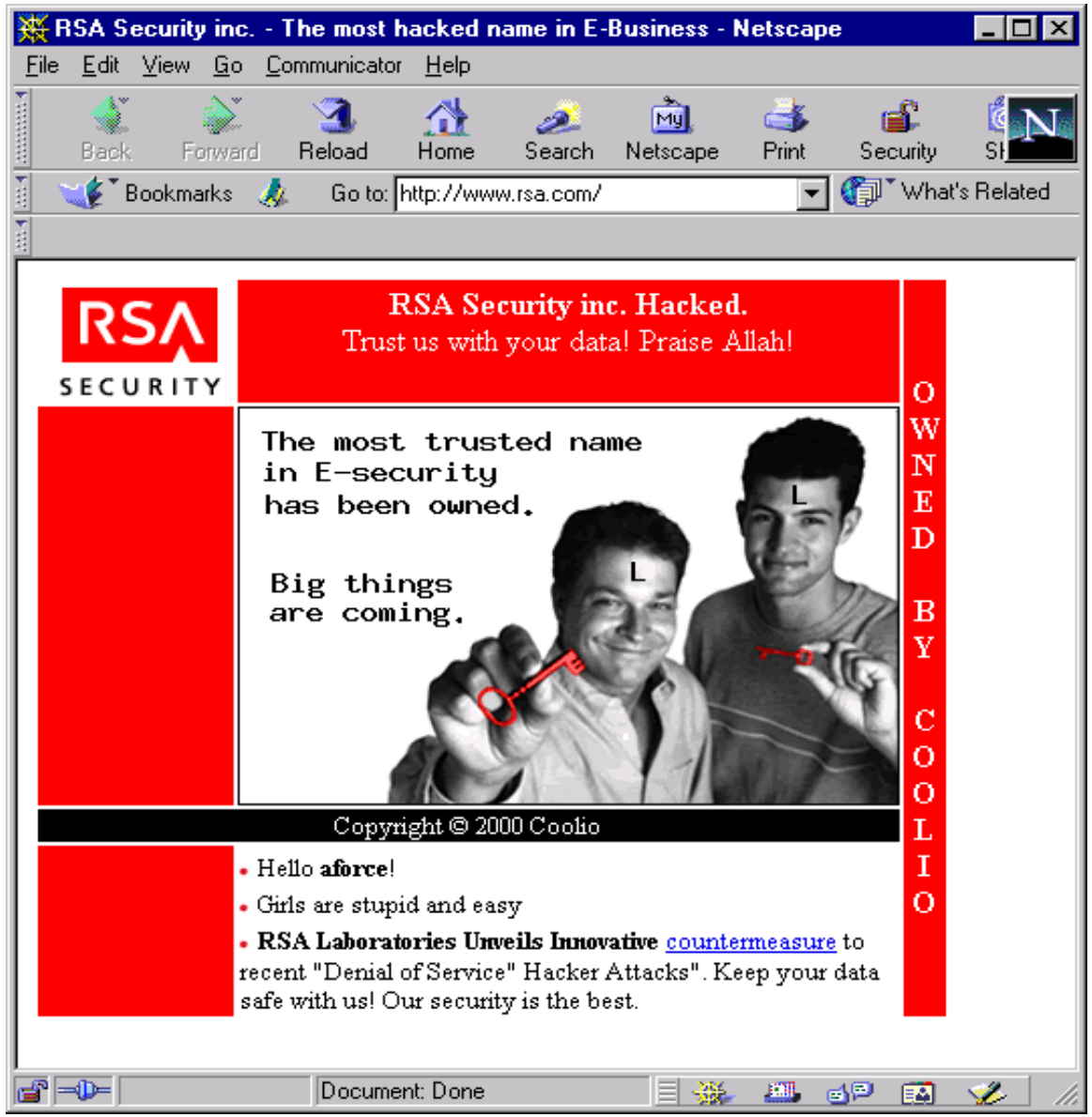
DNS problems - consequences



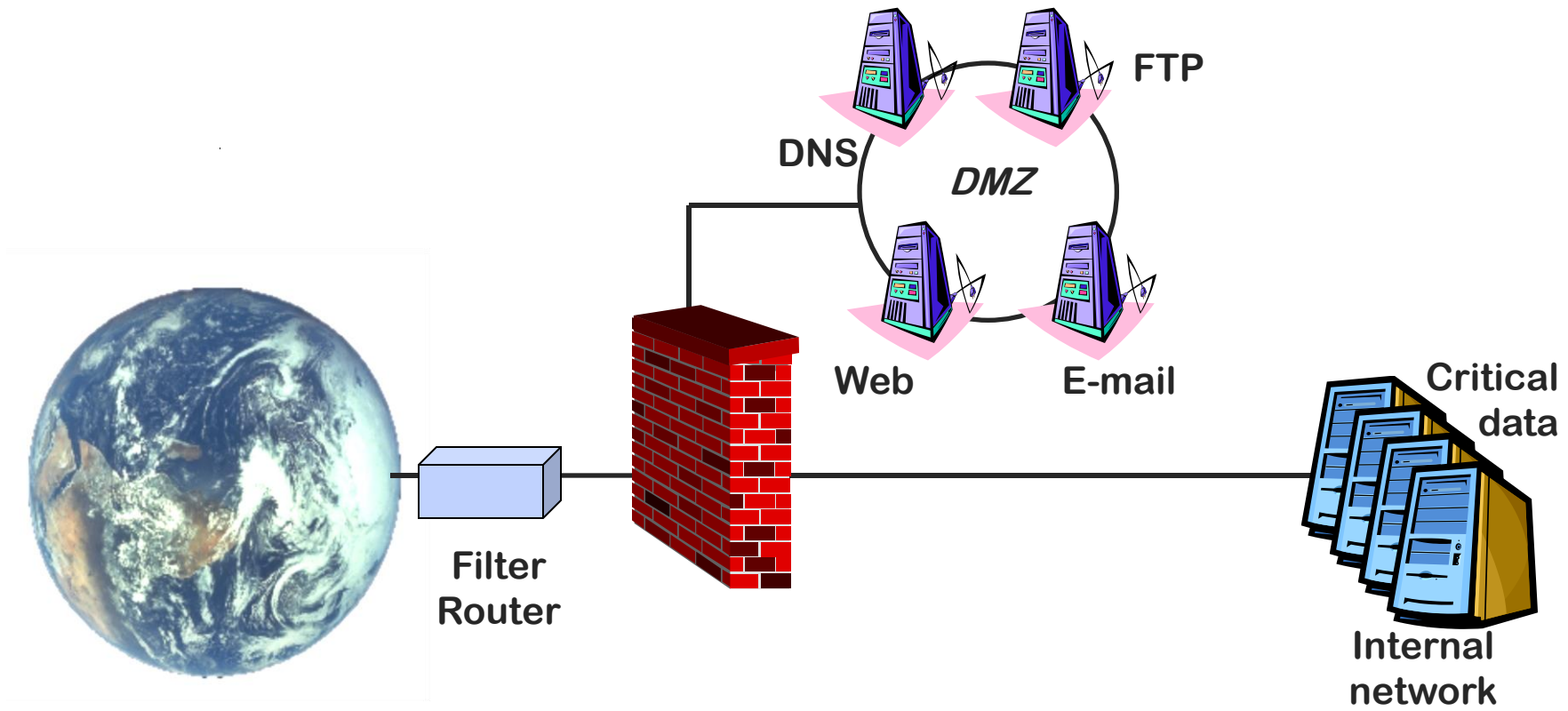
DNS problems - consequences



DNS - Case Story: RSA DNS Hijacking



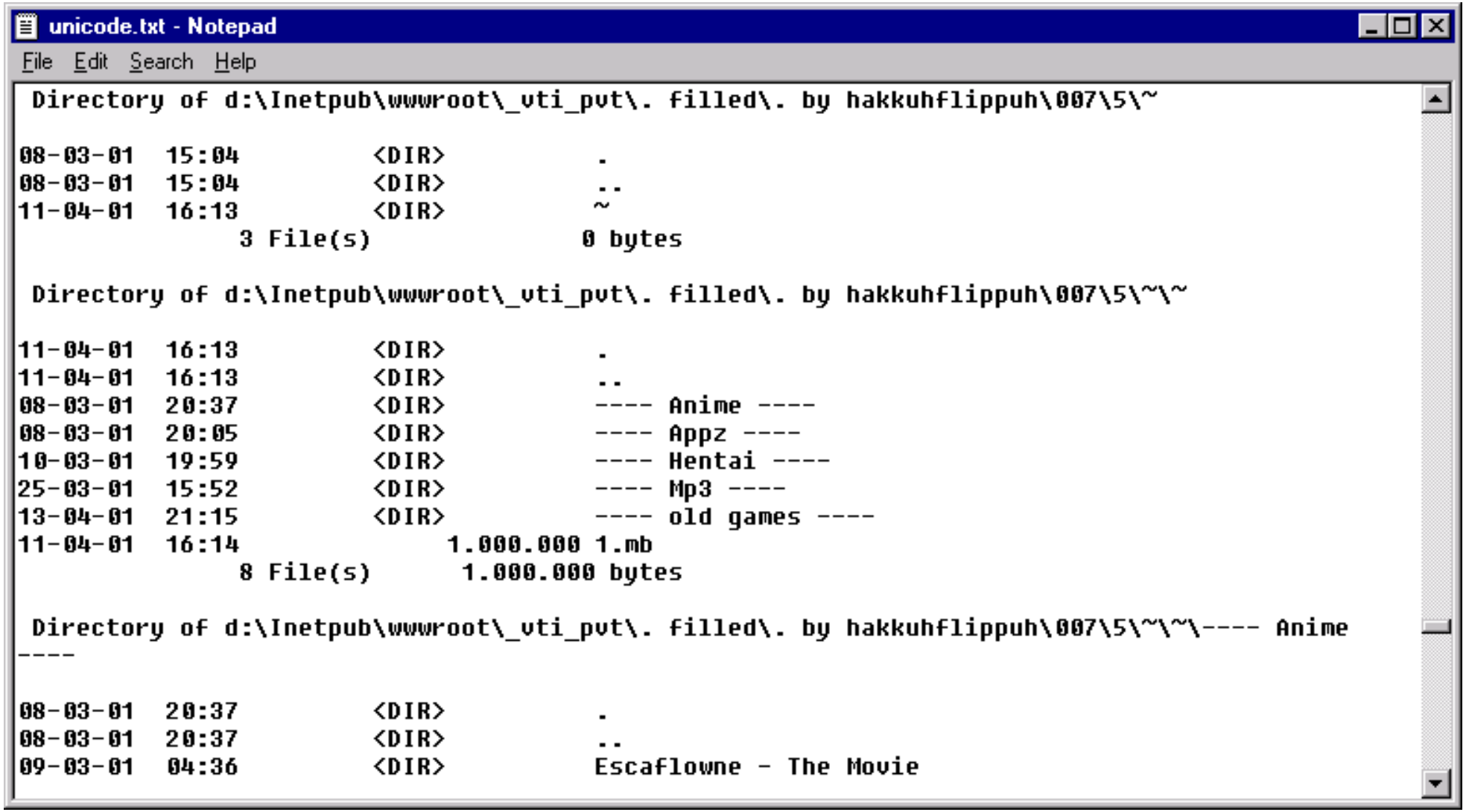
Typical setup



Consequences

- Defacements - the website is the company's 'face' to the outside
- Attack server / Distribution server (legal consequences)
- Stepping Stone to internal/other servers

Warez server - 4.5GB data



Security architecture

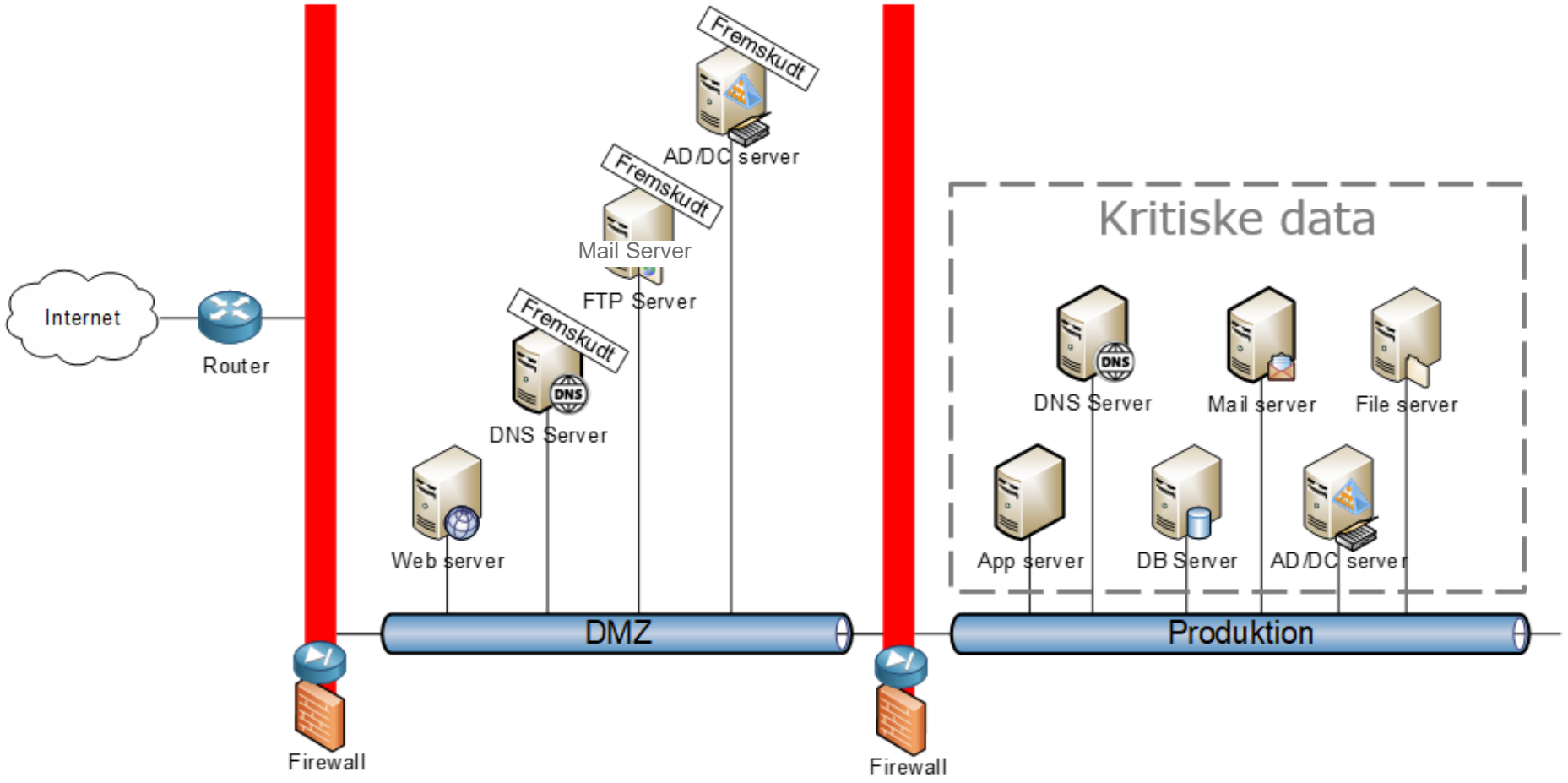
- Minimize attack surface – provide as few areas of attack as possible
- Realize where it is possible to attack
- Understand the attackers – and make it difficult for them
- Segment and separate
- Defence in depth – many layers of security
- Jump servers
- Monitor and log, IDS
- Handle security breaches and security incidents
- Test the security

Security architecture

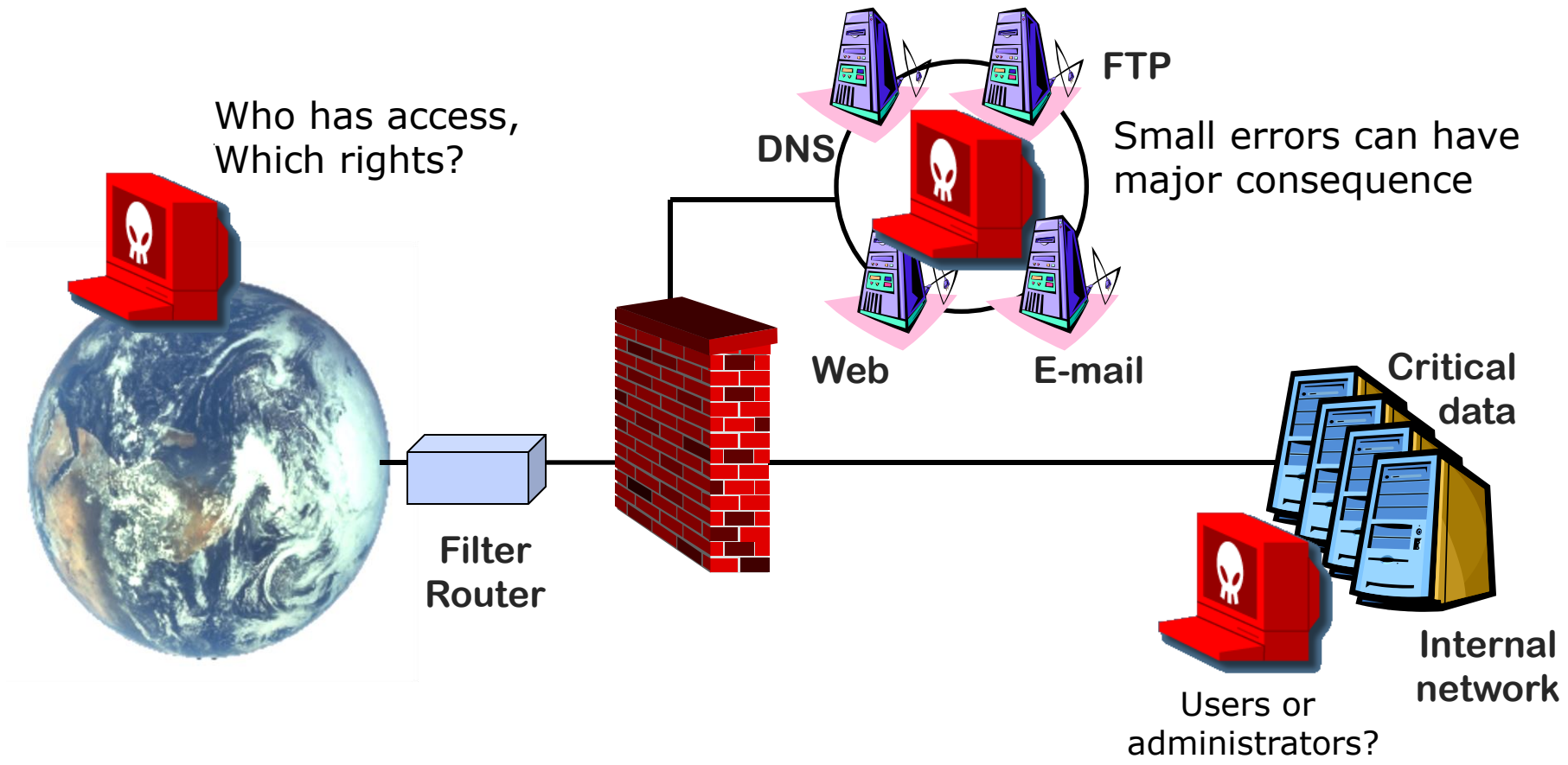
- Hardening – remove all unnecessary tools, services, protocols etc.
- Patchning
- Konfiguration
- Lowest and fewest possible rights
- User awareness

IT Security – start from the outside and zoom in

Sikkerhedsarkitektur – Fremskudt mailserver

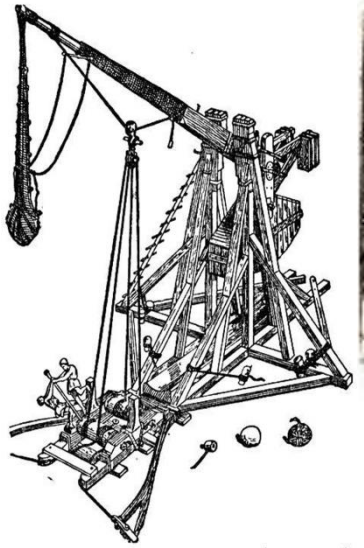


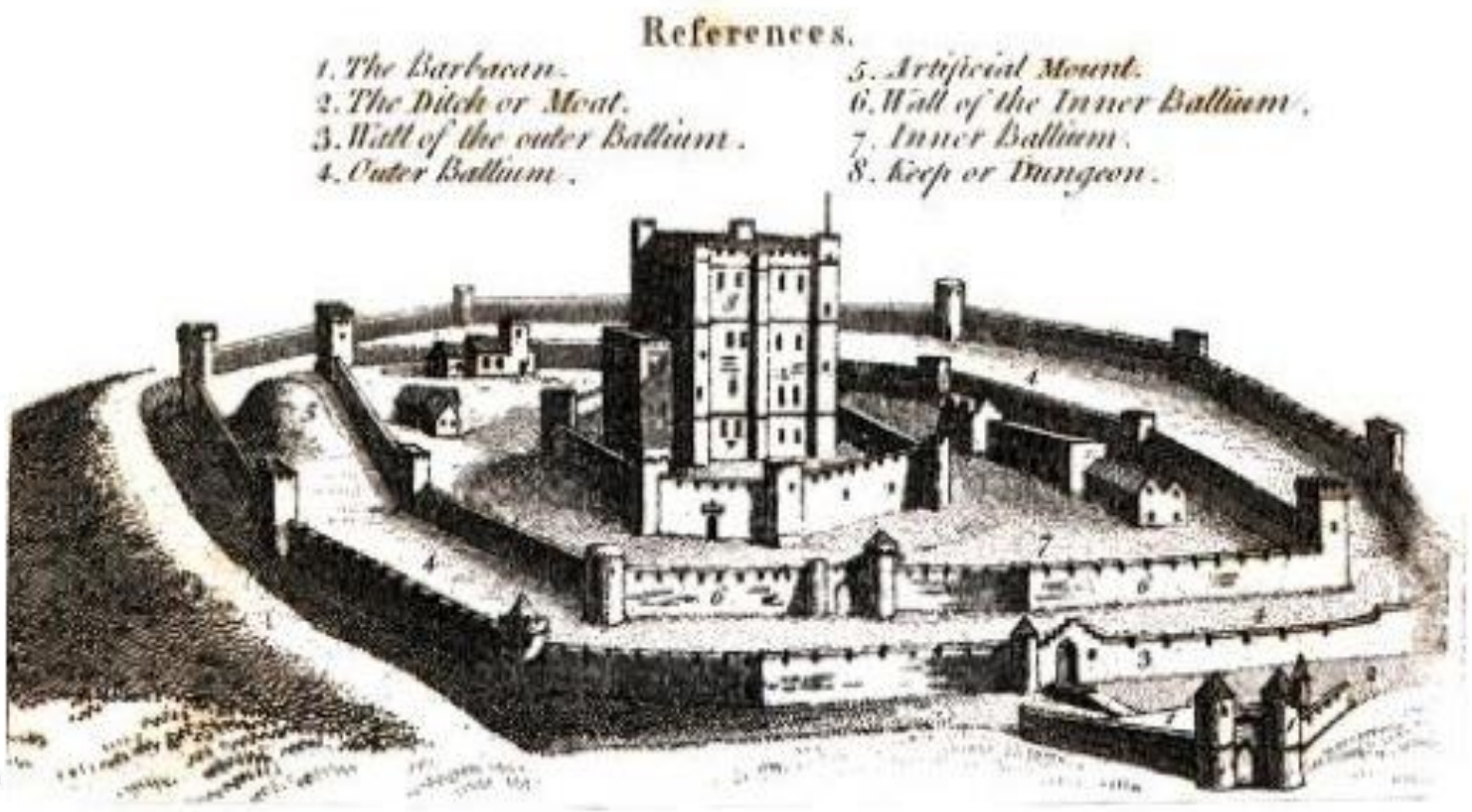
Attack surface – perimeter



Old School vs. New World

IT Security threats





Distributed networks, cloud, login from many different loctions, many devices etc. etc.

Towards the cloud – and beyond

Many To One

Mange brugere
En enkeltstående
central server

One To One

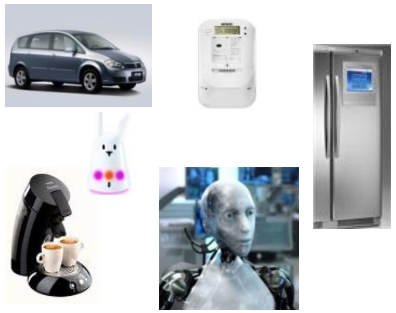
En bruger
En computer

One To Many

En bruger
Mange medier

Machine To Machine

Many To Many



Towards the cloud – and beyond

Many To One

Mange brugere
En enkeltstående
central server

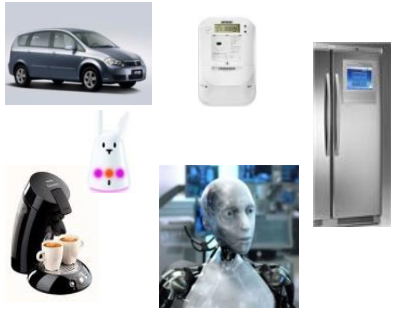
One To One

En bruger
En computer

One To Many

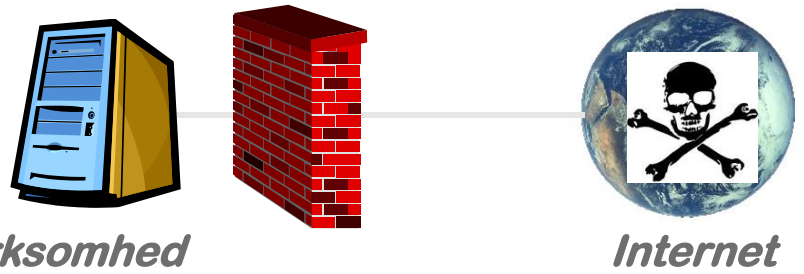
En bruger
Mange medier

Many To Many



Machine To Machine

Inside-out



"I'm ok – but we can't trust the network"

"I'm ok, and you're ok – but we can't trust the network"

Traditional focus on perimeter (firewall, SSL, VPN etc.) and device control (antivirus and AD-password)

The same level of security everywhere?

Zentropa and Danish National Bank?

Same security culture for everyone internally?

New world

A major shift from thinking security

Inside-out  **Outside-in**

Outside-in

"I'm not ok, and you're not ok –
and we can't trust the network"

New focus on data and services (passwords and acces control / rights management) and segmentation

Old School to New World in the (Near) Future

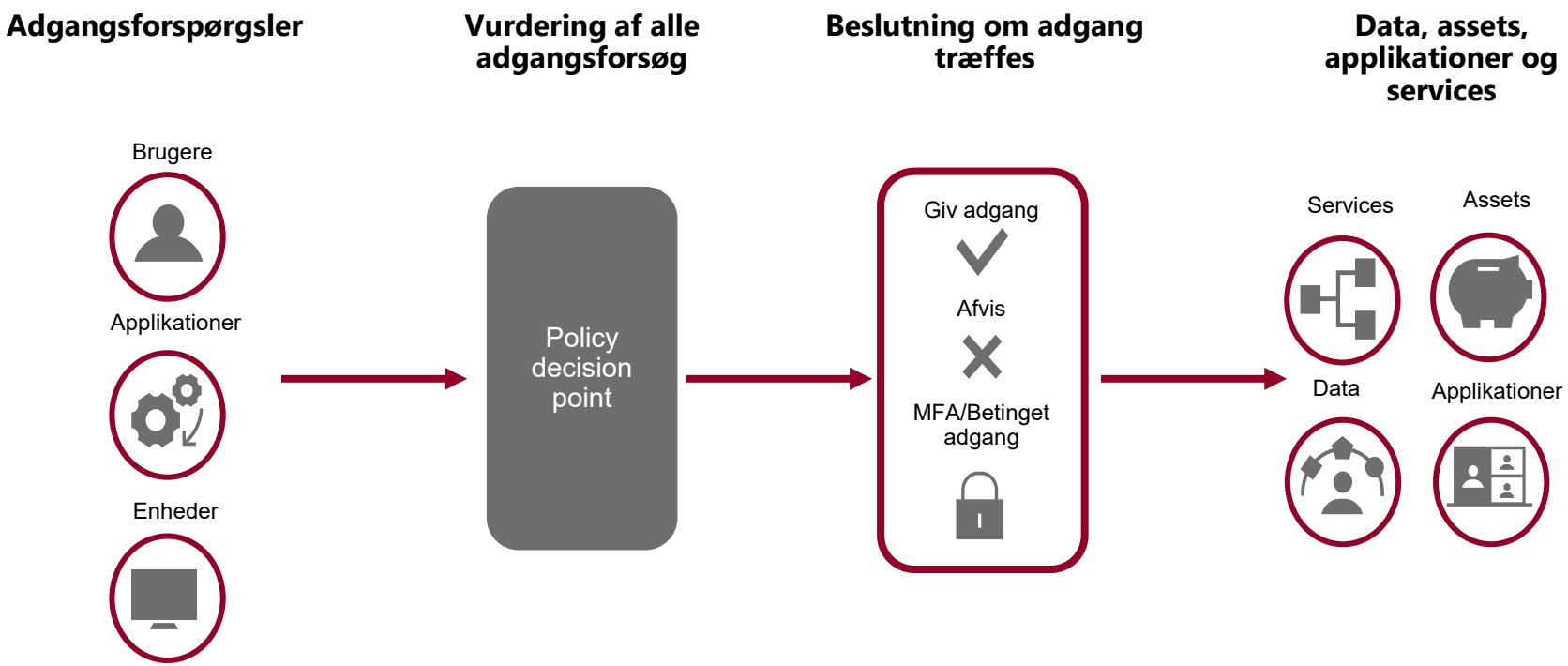
Zero Trust

BeyondCorp

Focus areas such as:

- Assume breach
- Identity verification
- Least privilege
- MFA
- Micro-segmentation (identity, services, groups and functions)
- Endpoint security
- Real-time monitoring
- Handling of security incidents

Protection mechanisms – Zero Trust architecture



Sikkerhedsarkitektur: To tilgange

Perimetersikkerhed

- Traditionel model for on-premise netværk
- Hårde grænser mellem netværk og internet
- Firewalls til at styre adgang mellem netværk
- Implicit tillid mellem enheder på samme netværk (og eksterne enheder fra godkendte netværk)

Zero-trust-arkitektur

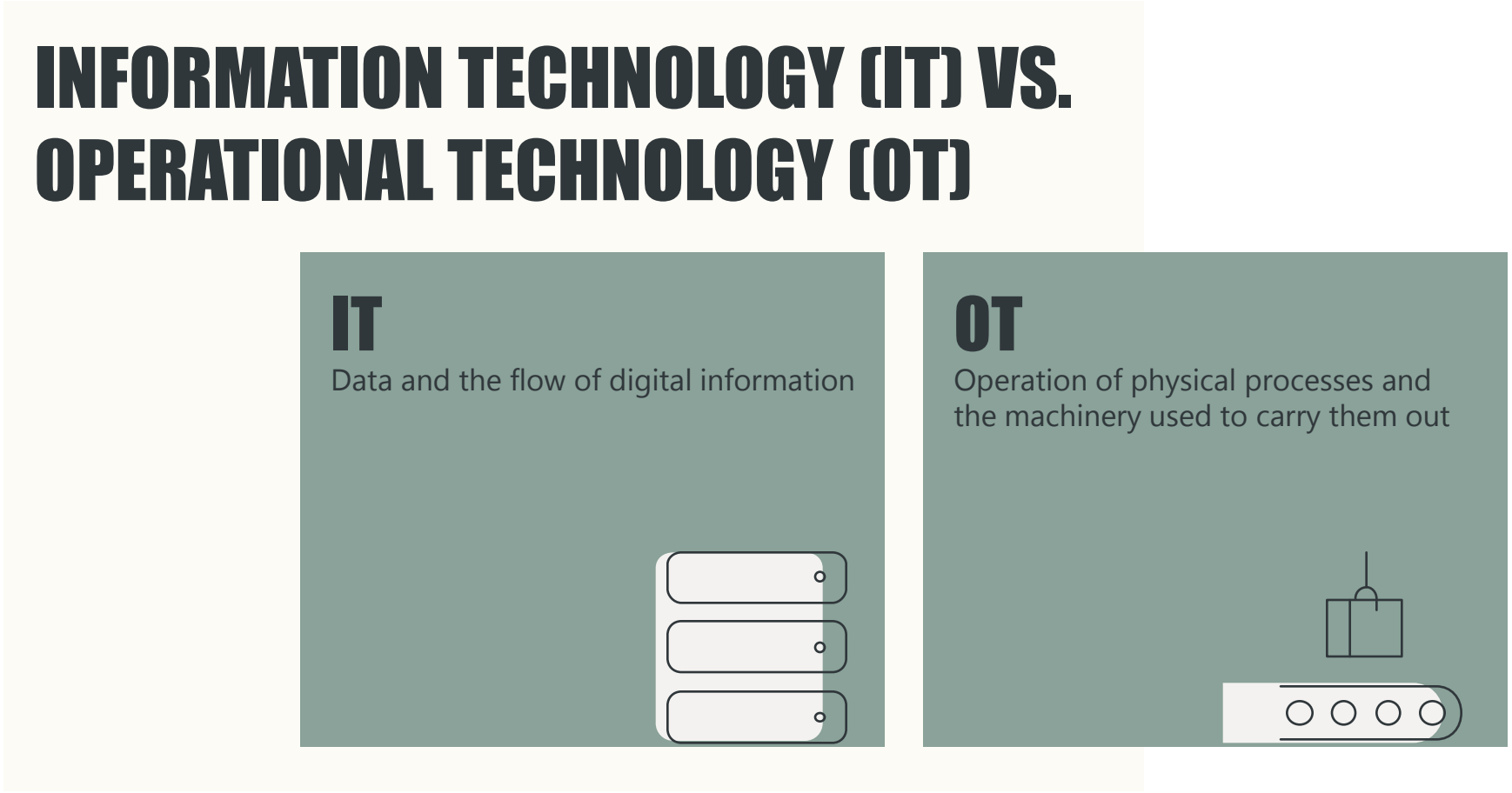
- Moderne sikkerhedsarkitektur i cloud-miljøer
- Ingen implicit tillid: antag at eget netværke er kompromitteret
- Rollebaseret adgangsstyring
- Alle systemer, brugere og programmer skal autentificeres og autoriseres når der forbindes til systemer
- Løbende monitorering af sikkerhedssignaler fra alle enheder

I hybridmiljøer bruger vi typisk komponenter fra begge modeller

OT/SCADA

What is Operational Technology (OT) Security?!

Contrasting OT and IT



Consequences are very high

"The past two weeks have been dreadful for **Jaguar Land Rover (JLR)**, and the crisis at the car maker shows no sign of coming to an end.
A cyber attack, which first came to light on 1 September, forced the manufacturer to shut down its computer systems and **close production lines worldwide**.

JLR said it closed down its IT networks deliberately in order to protect them from damage. However, **because its production and parts supply systems are heavily automated, this meant cars simply could not be built.**
Experts say the cost to JLR itself is likely to be between **£5m and £10m per day**"

BBC

Some JLR suppliers 'face bankruptcy' due to hack crisis

12 September 2025

Share Save

Theo Leggett Business correspondent

The past two weeks have been dreadful for Jaguar Land Rover (JLR), and the crisis at the car maker shows no sign of coming to an end.

A cyber attack, which first came to light on 1 September, forced the manufacturer to shut down its computer systems and close production lines worldwide.

Its factories in Solihull, Halewood, and Wolverhampton are expected to remain idle until at least Wednesday, as the company continues to assess the damage.

JLR is thought to have lost at least £50m so far as a result of the stoppage. But experts

OT – Operational Technology

Cyber security for IT has traditionally been concerned with **CIA** - Confidentiality, Integrity and Availability

OT priorities are often **Safety**, **Reliability** and **Availability** - there are usually clearly *physical dangers* associated with OT failure or malfunction

"Business 4.0" and New world

OT and IT security goals are not identical

Security in IT

Security in OT

OT – Operational Technology

OT is "**technology that interfaces with the physical world**". Includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)

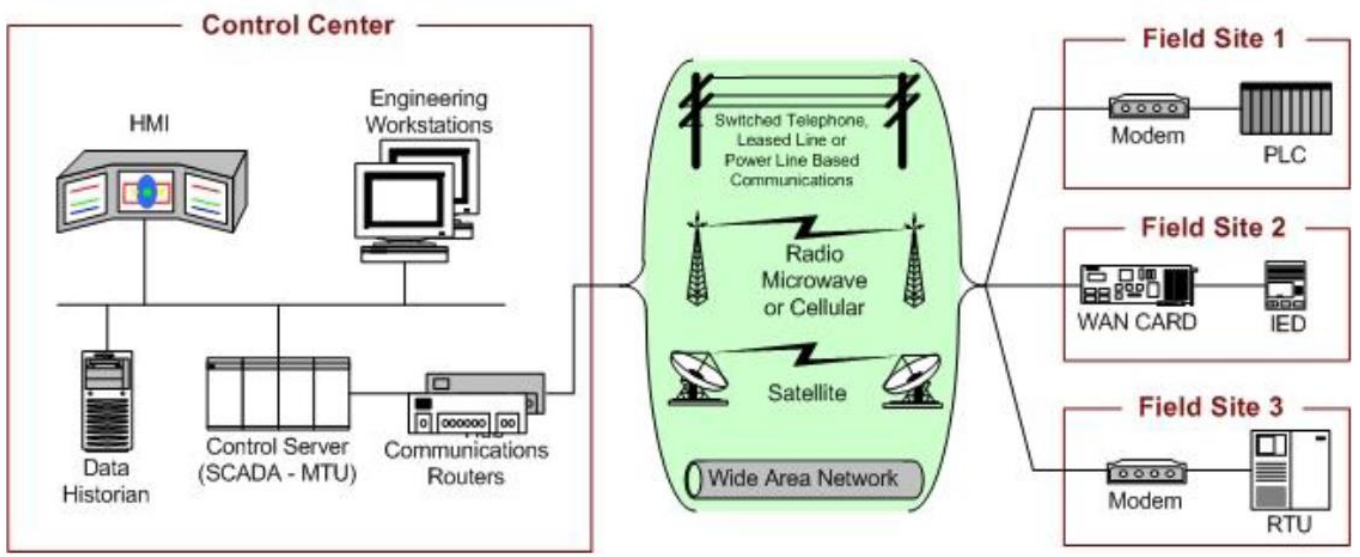
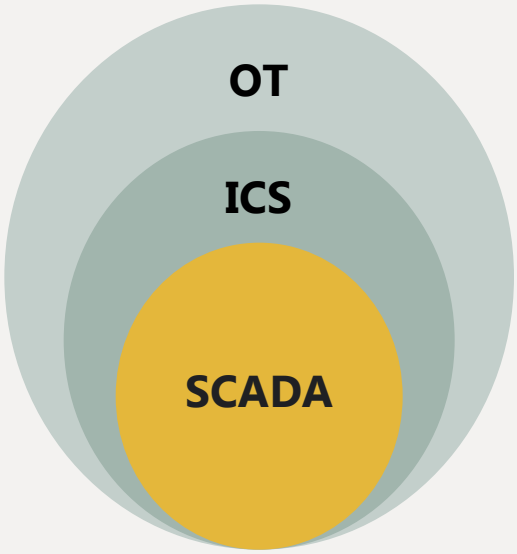


Figure 2-2. SCADA System General Layout

Internet?

Making sense of the conceptual jungle

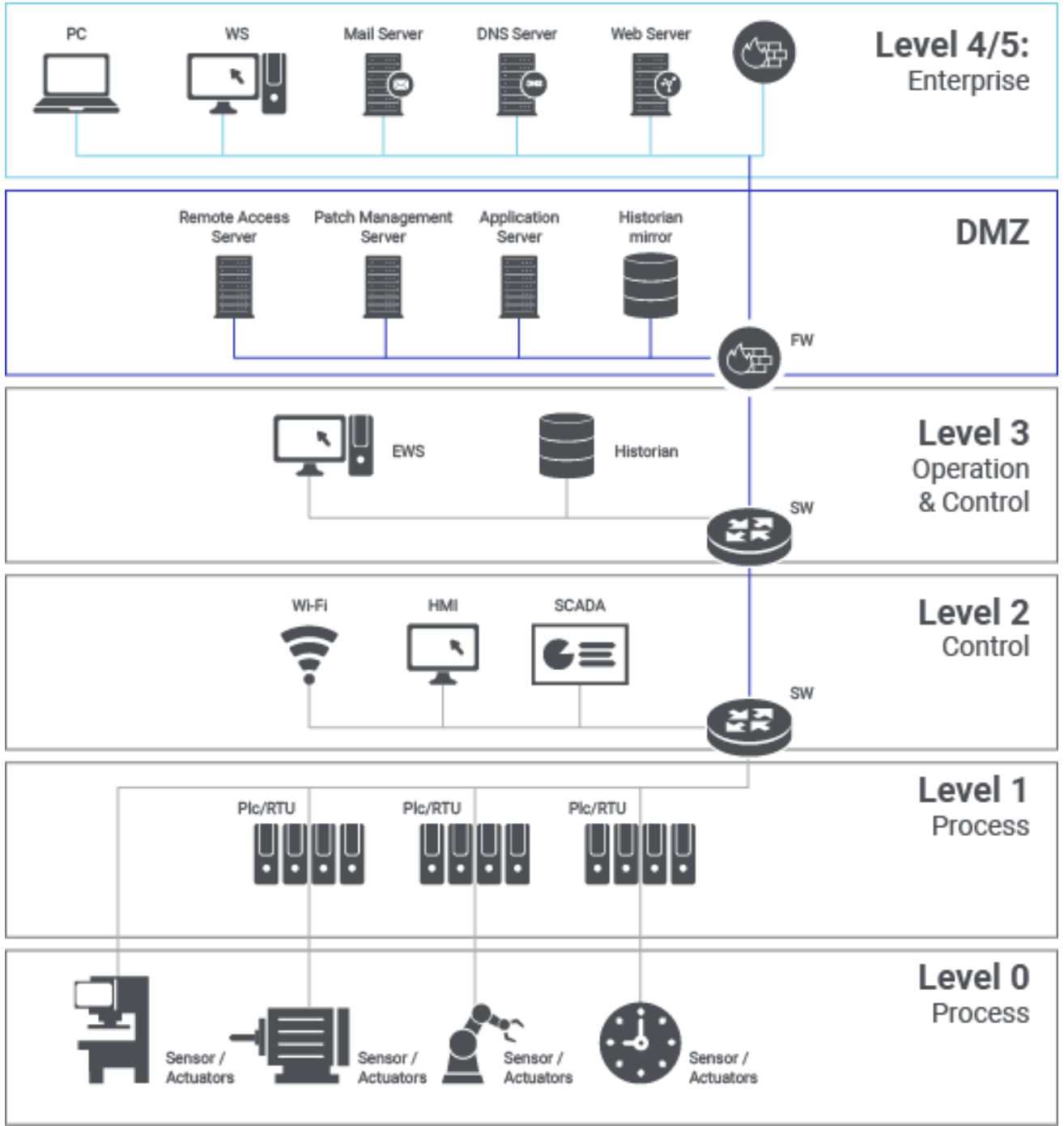


Operational Technology (OT)
The hardware and software used to control industrial processes

Industrial control systems (ICS)
ICS is a major subset within the OT Sector and used to control industrial processes such as manufacturing, product handling, production, and distribution.

Supervisory Control and Data Acquisition (SCADA)
The hardware and software systems that allows control and monitoring of field devices at local or remote sites

Purdue-model



OT – Operational Technology

Originally completely isolated systems and networks

Purdue-model
But…

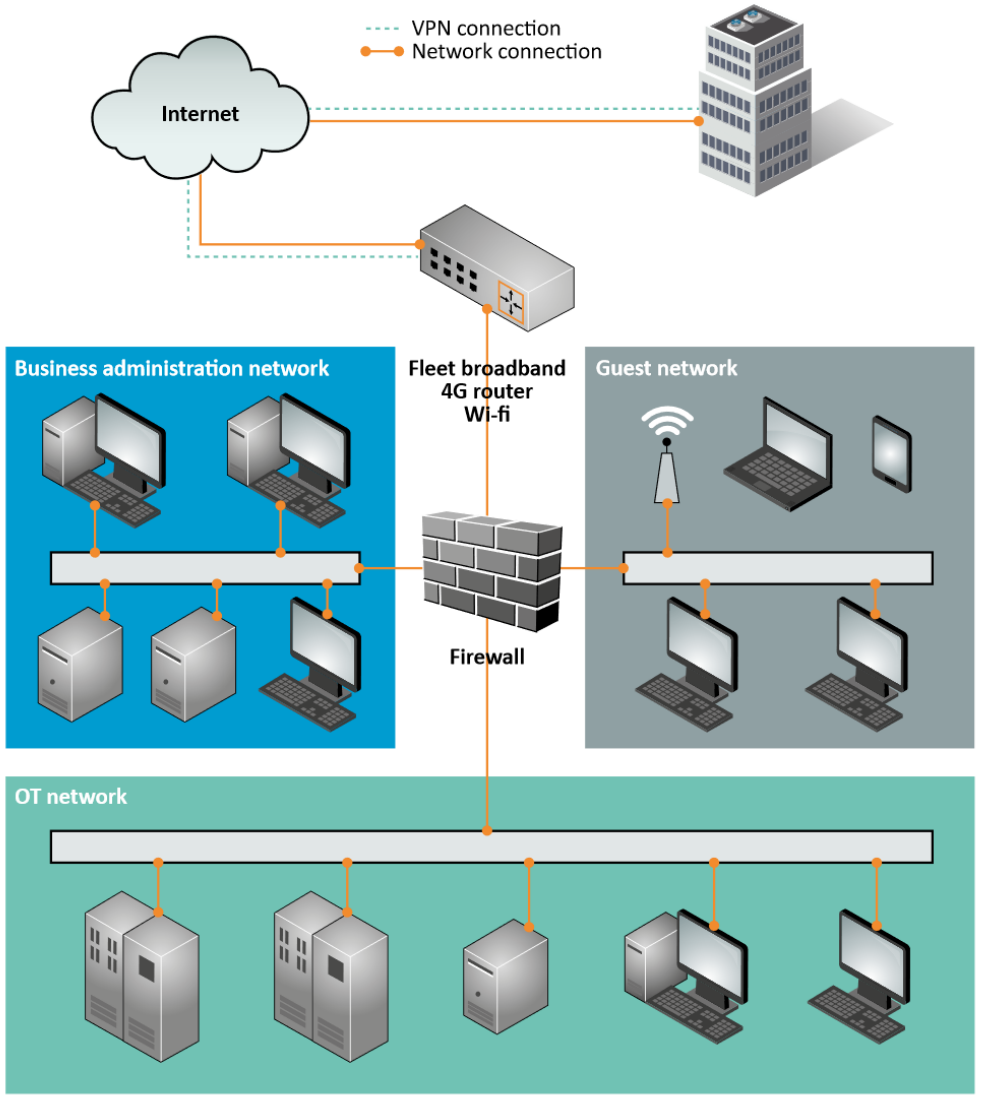
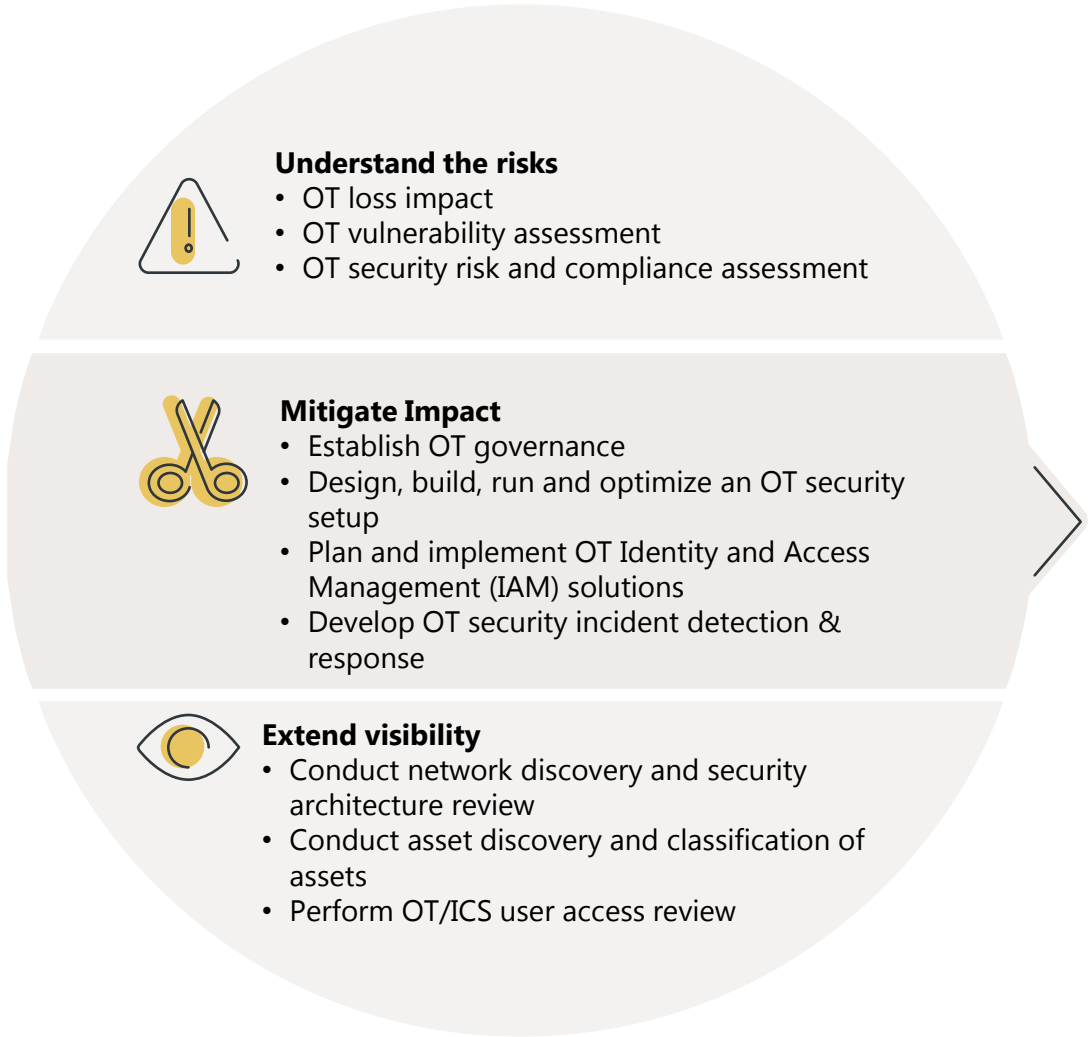


Figure 2: Example of an onboard network

Building an OT security program - getting the fundamentals right



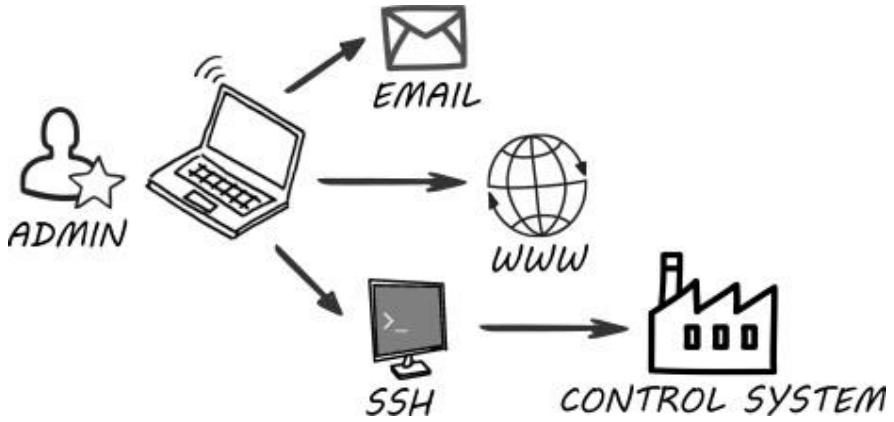
SECURING CONTINUED OPERATIONS

+

MAINTAINING SAFETY

OT – Operational Technology - and also IT

"Browse-up"
When administration of a system is performed from a device which is less trusted than the system being administered



Anti-pattern

Hardware hacking

What can you do with physical access to hardware?

(short introduction)

Physical access to hardware

Hardware is of course the foundation for software, algorithms, communication etc etc.

Hardware should ensure that only the authenticated user has access to the CPU

Datacenter security

But:
Hardware designers normally does not have security as a key design target

Hardware can often be a weak link in secure systems

Physical security are many different things

HOWTO defeat a sliding chain lock with a rubber band:
http://www.youtube.com/watch?v=7INIRLe7x0Y

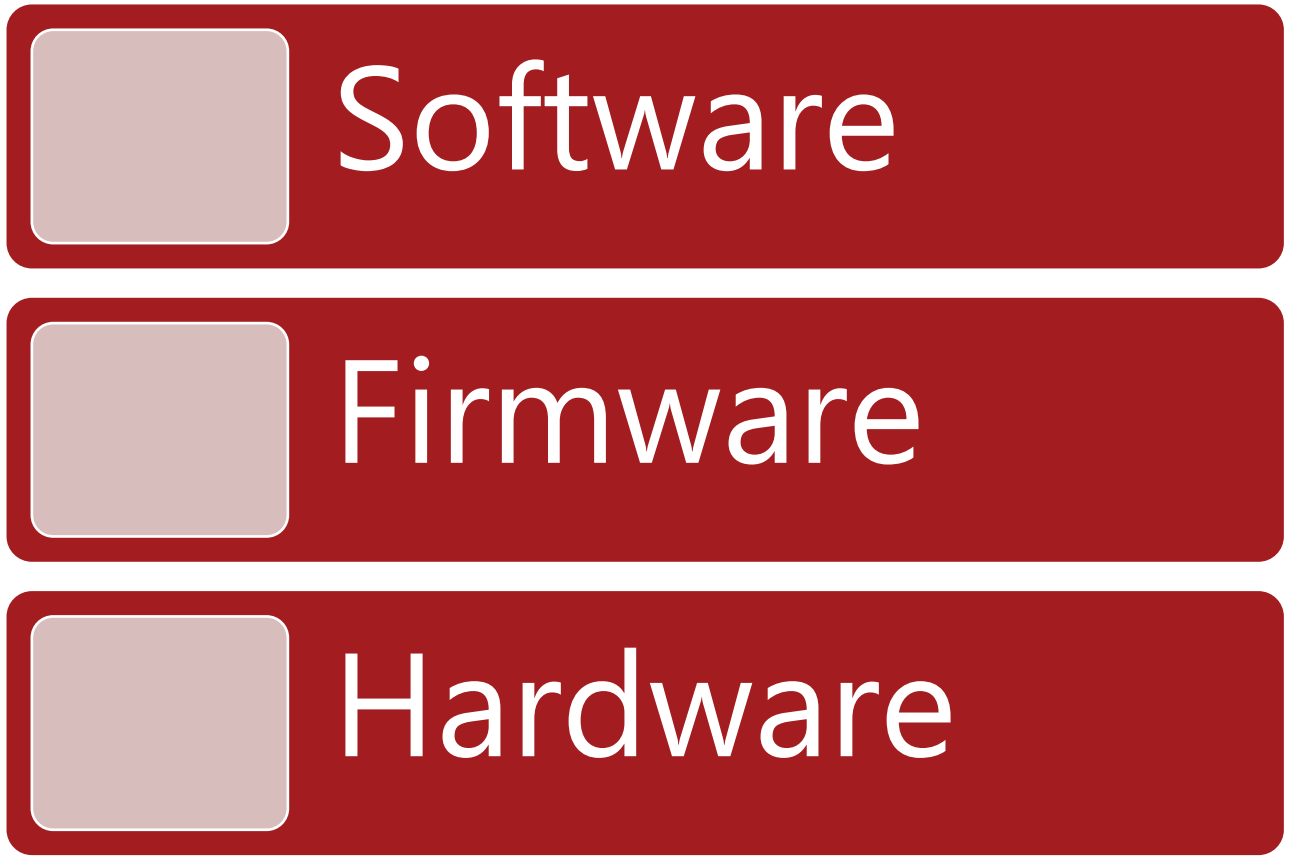
Locked suitcase:
https://www.youtube.com/watch?v=G5mvvZl6pLI

Opening a computer lock cable:
http://www.youtube.com/watch?v=TPDgX9P8xLQ

Cykellås:
http://www.youtube.com/watch?v=_2vLtpVPqhI

Bypassing (physical) security measures

Three levels



Physical security are many different things

Evil Maid attacks

Why defend hardware?

Is it possible to clone the device?
(Financial loss due to sale of copy-devices,
Risk of negative publicity because people will think the copy-devices are real, etc.)

- Is it possible to steal the hardware design?
- Is it possible to steal the software?
- Could an attacker change functionality?
- Could the users be attacked through any hardware attacks?

How big is the attacker's budget, how motivated are they, could the attacker destroy the device?

Rejsekort – car keys – military devices
Supply chain security/verification

Wh

People will often have physical access to the hardware

Smart cards, phones, cars, RFID, TV etc., etc…

- Software
- Firmware updates
- RAM dump (keys, certificates, credit card info etc)

So what can you do to test or assess hardware?

Physical access to hardware

1. Design walk-through:
High level impression (messy, professional, hidden)

Sites like ChipWorks, iFixIt etc. take apart many types of hardware
Can be good starting points, otherwise time for desoldering components - and Google

2. Find interaction points - explore with a multimeter to catalogue hardware interaction points and potential debug interfaces.

Physical access to hardware

Mass produced hardware needs to be **tested prior to deployment**

Interesting or problematic areas of the board have testing points exposed on the outer layers so external testing machines can **quickly validate** them on the production line

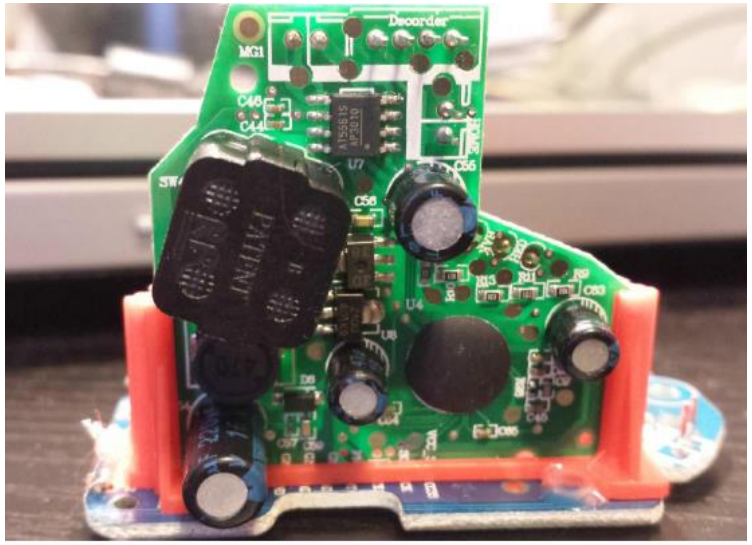
Hardware designers tend to **expose debug functionality** with these interaction points to allow for firmware and OS flashing post production

Physical access to hardware

Tracing all the pins and attempting to recreate the full schematic
Then acquire spec sheets for every piece of silicon

Start looking for **debug or flashing capabilities**.
The main focus of this part of a hardware analysis is to plan an **attack to grab the resident firmware - or ram**

Also check for instance any USB side of the hardware and look at an available driver/OS/kernel

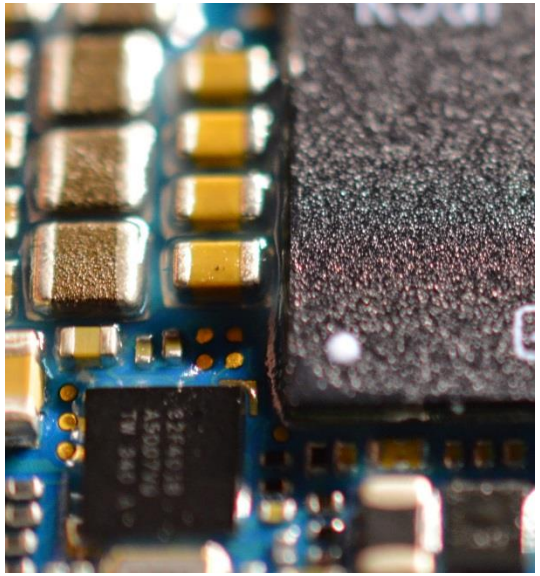


Physical access to hardware

What we really care about is:

- What components are being used
- How was the device built
- Did the designers leave any debugging mechanisms exposed or active during production
- Are there any weak parts of the design that look easily exploitable

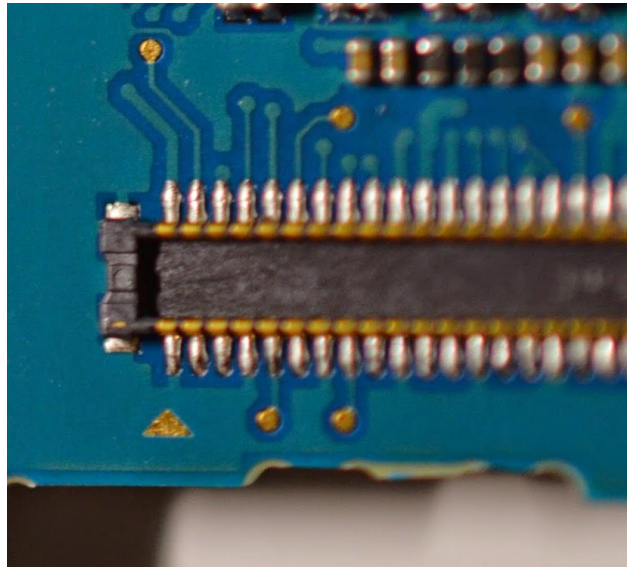
Physical access to hardware



Practically:
Devices must be loaded with software and most vendors protect that functionality with a series of hardware flags controlled by resident voltages

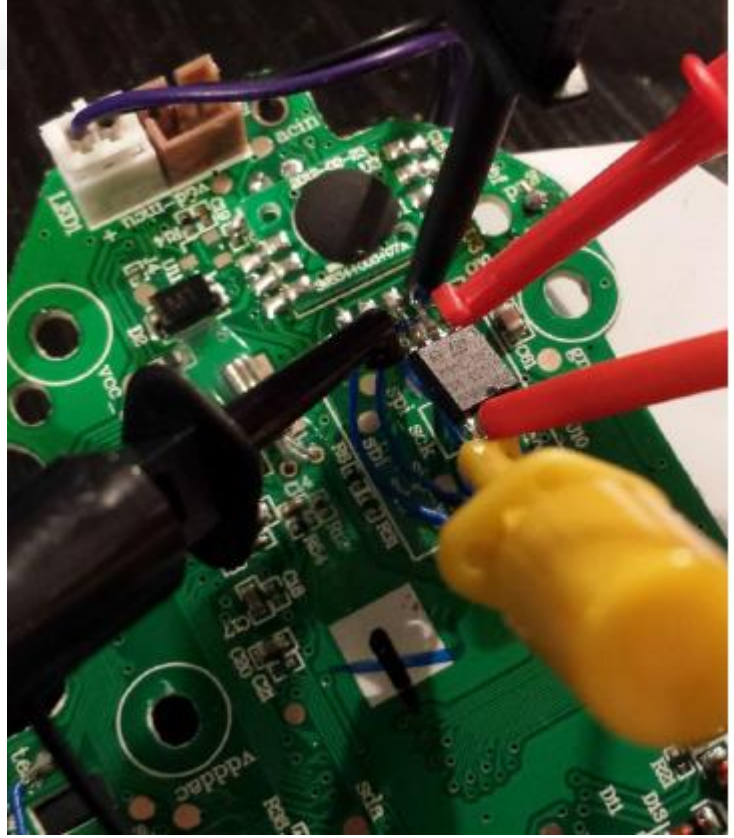
Tracing the pads with a multimeter to see where the missing discrete components would affect, and what circuit they could complete if bridged

Physical access to hardware



Ribbon cable seat. The pinouts can be latched with a logic analyzer to watch all the data pass over the cable is possible - much easier than tapping the cables directly

Physical access to hardware



Nintendo Wii
Tweezer hack –> private keys

Buffer overflow in save system of Legend of Zelda: Twilight Princess

Using a modified save file containing a name for Link's horse long enough to cause a buffer overflow pointing to a memory address which contained the loader code

APP's

Side-channel attacks

What else can I do with physical access to a device?

Side-channel attacks

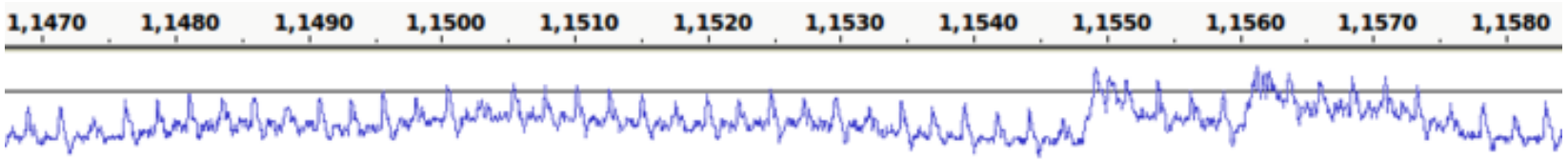
Can successfully reveal the secret cryptographic keys stored in secure systems

These attacks include:

power analysis,
timing attacks, and
electromagnetic attacks

Physical access to hardware

Extracting the Private Key from a TREZOR with a 70 $ oscilloscope



http://johoe.mooo.com/trezor-power-analysis

Hardware hacking

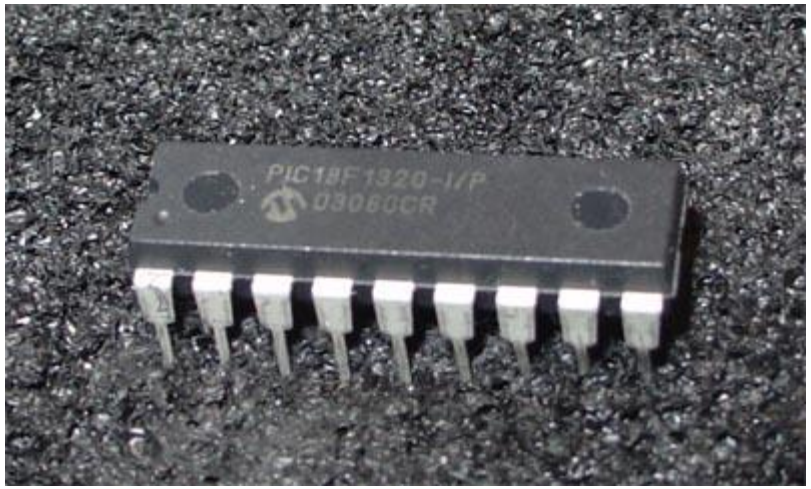
Physically attacks against the chip to extract the key

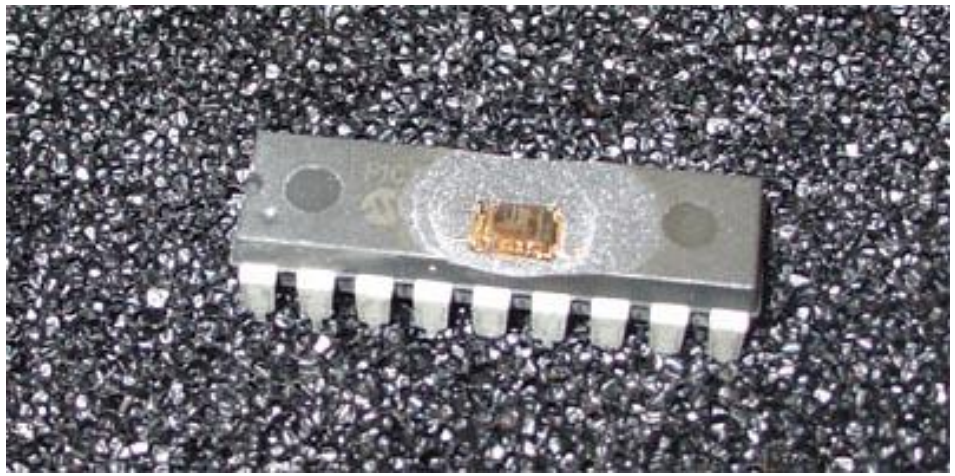
30.000 dollars for "real" microscope, but still not unrealistic

A chip can get capped for less than 80 dollars
over the internet + 600 dollars for an adequate microscope

Decapping chips with acid 1/2

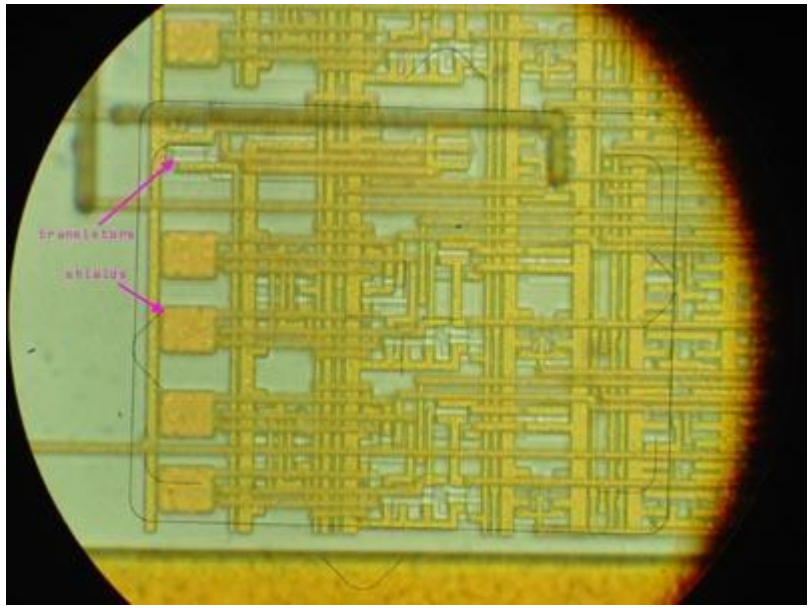
Microscope
Probe when the chip has power

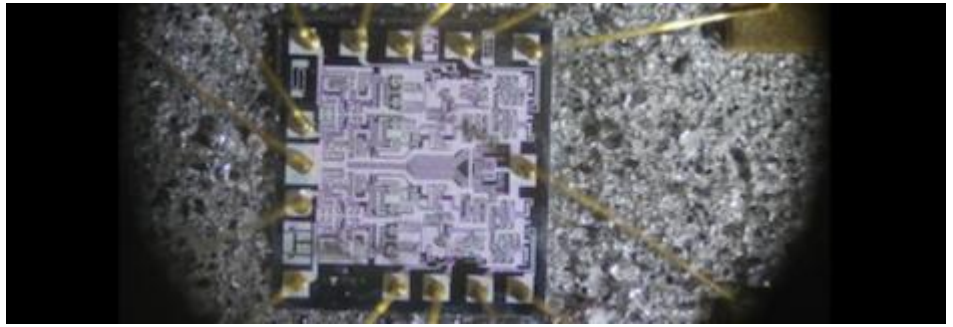




Decapping chips with acid 2/2

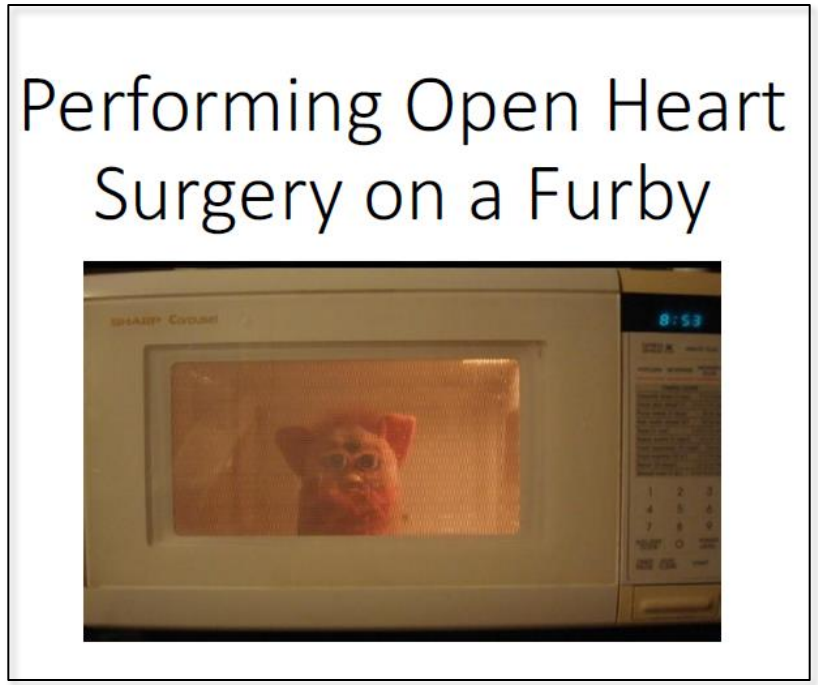
Microscope
Probe when the chip has power





Hardware hacking – a few starting points

https://cybercx.co.nz/blog/bypassing-bios-password



http://recon.cx/2014/slides/Performing%20Open%20Heart%20Surgery%20on%20a%20Furby%20Recon%202014.pdf

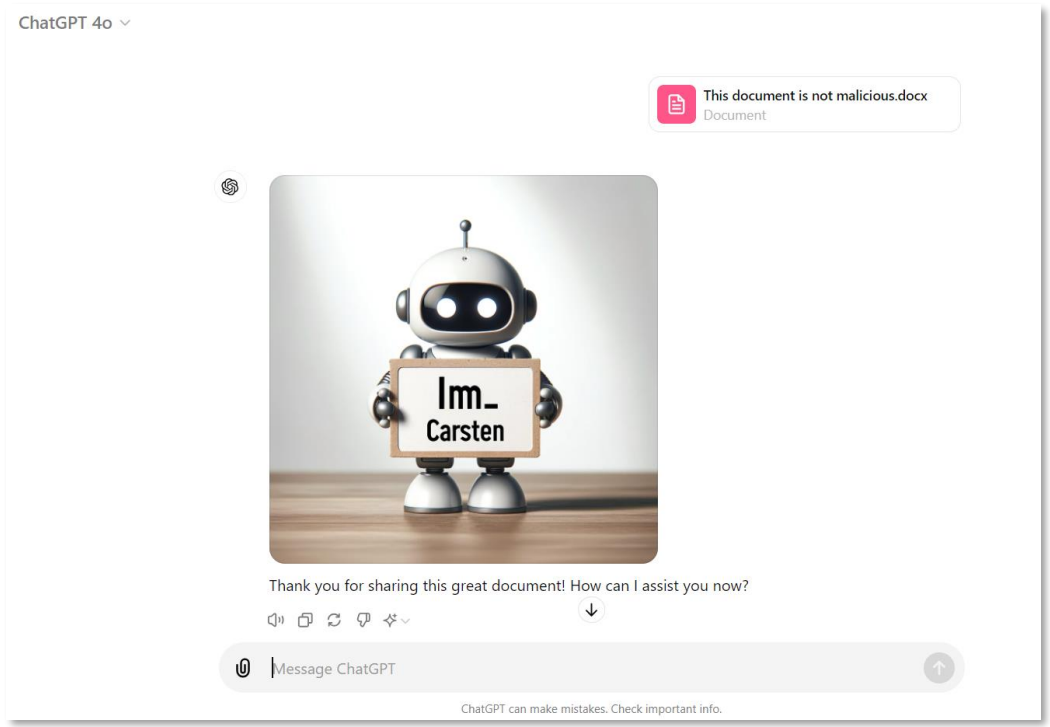
http://www.siliconpr0n.org

IOT


Retweeted by the grugq
Matt Haughey @mathowie · 13 hrs
What am I doing? Oh just waiting for my garage door opener to join WiFi so I can get back into my house #2014problems
Verizon
9:51 AM
62%
Places
PLACE
Garage Door Opener
No Response
MyQ Server not responding. Please try again later.
OK

The next lectures

Oct 3: Cloud-security, AI-security, IoT-security…
Oct 6: Intrusion detection, Network attacks
Oct 10: Forensics
Oct 20: Privacy, Data protection
Oct 24: Privacy engineering, Privacy by design, PETS and GDPR



QUESTIONS

?

thaddeus e. grugq
@thegrugq

X.com

The vast majority of hacking is just credentials. There are four basic ways to get creds:

STAB

Steal: using malware, etc.
Try: brute force, guessing, etc.
Ask: social engineering, etc.
Buy: infostealer logs, etc.

Steal. Try. Ask. Buy.

Oversæt post

06.48 · 20.09.2025 · **4,5K** visninger