



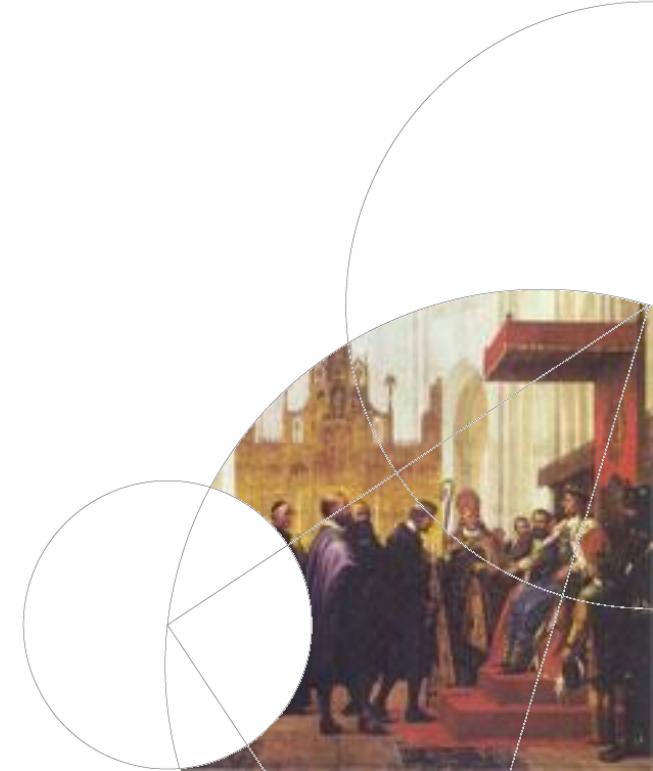
# Security architecture and firewalls

## Old-school vs new world

### DoS and DDoS

Carsten Jørgensen  
Department of Computer Science

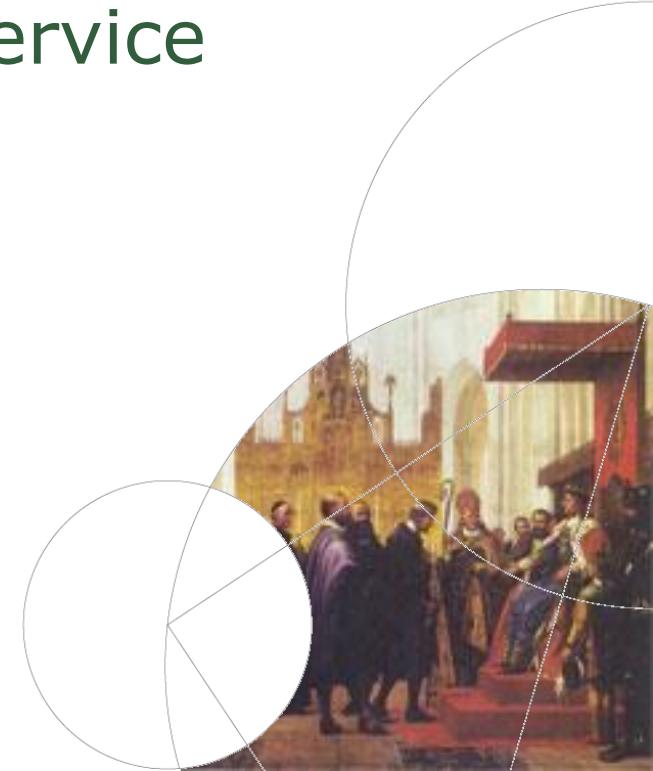
DIKU 20. september 2019





DoS: Denial of Service

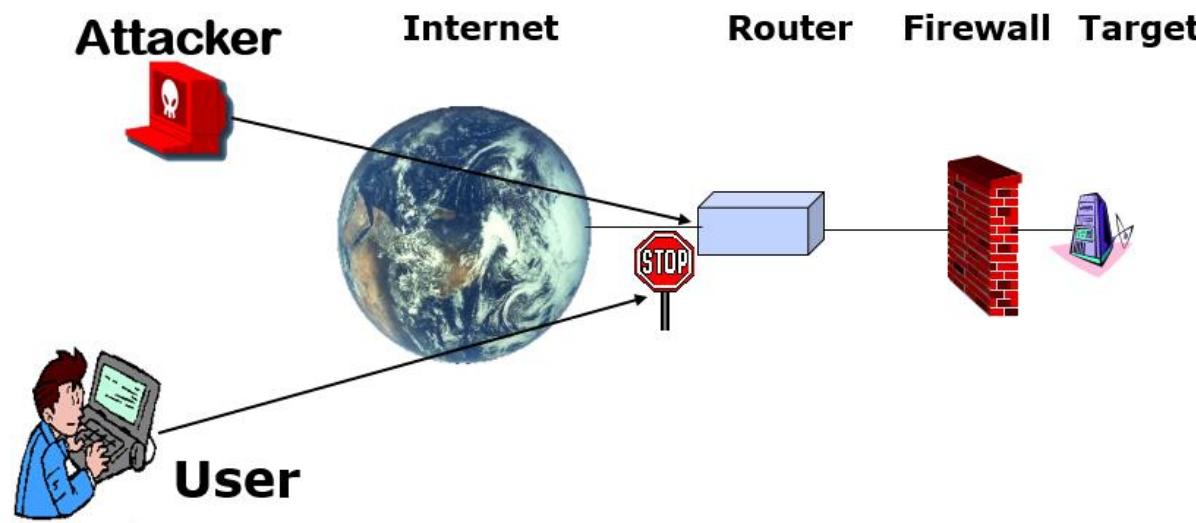
DDoS: Distributed Denial of Service



## What is DoS

Taking out sites – even large sites - with little computing work

## DoS vs. DDoS



## What is DoS

# DSB udsat for cyberangreb

14. maj. 2018, 05:36



<https://nyheder.tv2.dk/samfund/2018-05-14-dsb-udsat-for-cyberangreb>



## What is DoS

### Attacks against availability

Two basic classes:

**Magic packets (Poison packets)** – protocol attacks or design flaw that allows one machine to disrupt a service

**DoS Flood** – botnet used to generate flood of data

Amplification and reflection – small number of packets from attacker -> big effect



DoS works (very well), but it is not sophisticated

The Internet is not designed to handle DDoS attacks



You Retweeted

**Simon Roth** @SimoRoth · 29 Dec 2014

DDOS attacks are not hacking, nor do they expose security flaws.  
They are as sophisticated as blocking a toilet by jamming your head  
into it

2.1K 1.7K

Nothing new:

*If you have a router with a 10Gbps port and an attacker sends you 11Gbps of attack traffic, no amount of intelligent software or hardware will allow you to stop the attack if the network link is completely saturated*



## Why?

### Attacks against availability

Extortion: Online gambling, florists on Valentines day etc.

Often an initial low-level attack and a warning that a larger attack will be carried out unless Bitcoin ransom is paid

### Cloud computing cost-attacks



Why?

SAMFUND

# Pakkefirma ramt af cyberangreb på årets travleste pakkedag

19. dec. 2017, 20:40



MEST



Why?

Part of serious attacks, hiding tracks

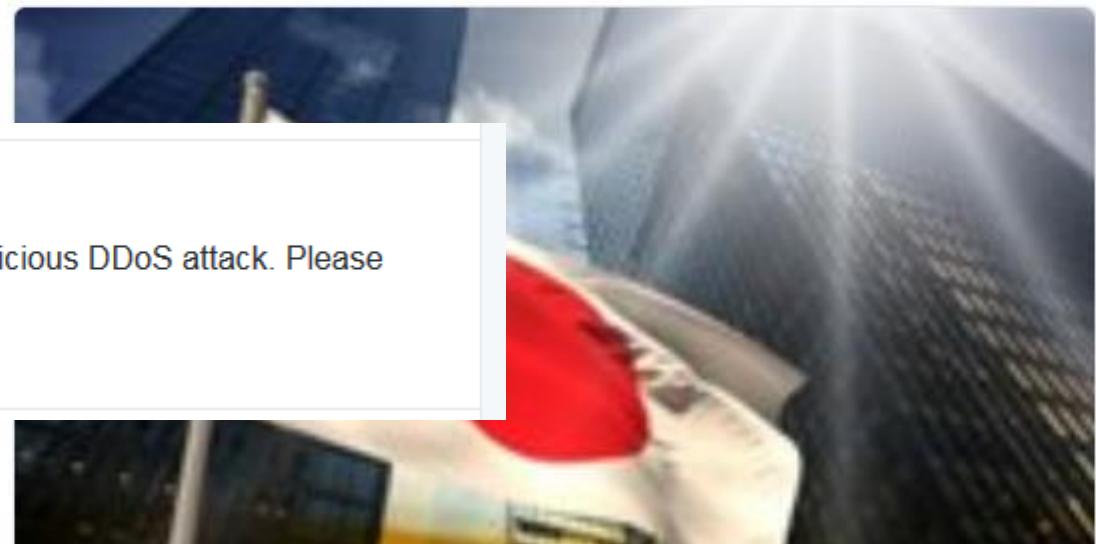
Anger or "Fun"

Curiosity

Not understanding how DoS (or the internet) works



"Japanese teen's #DoS attack takes out 444 school websites" [oak.ctx.ly/r/4p551](http://oak.ctx.ly/r/4p551)  
via [@SCMagazine](#) #DDoS



You Retweeted

**reddit status** @redditstatus · 19 Apr 2013

We are still working on mitigating a malicious DDoS attack. Please stay tuned.



161

17

...

# Hacktivism



IT-NYHEDER

BLOGS

IT-JOB

IT-FIRMAER

WHITEPAPERS

KURSER

EMNER *Hacking*

Se kommentarer (27)

## 3F's hjemmeside kæmper mod gentagne DDoS-angreb

Hos fagforeningen 3F kæmper man i øjeblikket en hård kamp mod et DDoS-angreb mod hjemmesiden, som begyndte onsdag aften.

*Af Theis Holtz Hansen Fredag, 20. juli 2012 - 11:04*

Fagforeningen 3F's hjemmeside bliver i øjeblikket oversvømmet med forespørgsler, der har til formål at lægge siden ned. Altså et såkaldt DDoS-angreb.

Angrebet er angiveligt sat i værk af Twitter-brugeren Elan0r1, som med en statusopdatering tager ansvaret for angrebet. Ifølge opdateringen sker angrebet i sympati for Restaurant Vejlegården, som 3f har blokeret i en overenskomstkonflikt.



# DoS is cheap - and easy for the attacker

NEM ID

PRIVAT | ERHVERV | MYNDIGHEDER | [OM NEMID](#) | DIGITAL SIGNATUR

## Om NemID

Forside / Om NemID / Aktuelt

▼ Aktuelt

- Nyhedsarkiv
- ▶ Nyhedsbrev om NemID
- Statistik om NemID
- Driftsstatis
- Driftsstatis for NemID

▶ Hvad er NemID?

Hvem kan få NemID?

Er NemID obligatorisk?

Her kan du bruge NemID

▶ Sikkerhed

▶ Regler

▶ Videreudvikling af NemID

▶ Om dette websted

Ofte stillede spørgsmål

### NemID udsat for DDoS-angreb

11. april 2013

Publiceret af: Digitaliseringsstyrelsen

Torsdag morgen fra ca. kl. 5-8 har det været svært eller umuligt at logge på med NemID i både netbanken og på offentlige og private hjemmesider.

Lignende hændelser fandt sted den 24. og 25. marts.

Adgangen er stadig ustabil, og der arbejdes på at løse problemerne.

Årsagen til problemerne skyldes, at it-kriminelle udfører det, der kaldes et DDoS-angreb mod NemID.

DDoS-angreb betyder kort fortalt, at it-kriminelle via et stort netværk af computere sender så mange forespørgsler til NemID-systemet, at systemet



## DoS is easy for the attacker

The image shows two screenshots of network stress testing tools. On the left is the Pandora DDoS Stresser interface, featuring a large title 'Pandora DDoS' and sections for 'Main' and 'Statistics'. It displays bot counts ('Today bots: 0', 'Online bots: 0') and configuration options for threads, timeout, and mode. On the right is the RussKill interface, with a title 'RussKill' and a status bar showing 'Online: 293'. It has fields for 'URL:' and 'Flows HTTP-flood:' (set to 0). Both interfaces include a 'Launch Stress Test' button at the bottom.

**Pandora DDoS**

Main Statistics

Today bots: 0 Online bots: 0

Threads Timeout Mode

Save

**RussKill**

Online: 293

URL:

Flows HTTP-flood: 0 Flows SYN-flood:

Start Save

**Stresser**

**Layer 4 (Transport Layer)**

Method:  DRDoS  UDP  UDP-Lag  SYN

Protocol:  DNS  CHARGEN

Host 1 (www.example.com or 1.1.1.1):  Add Host

Port (valid range: 1025 - 65535; 0 = randomize each packet):

Duration:  Seconds (5.00 Minutes)

Bandwidth:  Mbps (200.00 Mbps per host)

Launch Stress Test

# DoS is cheap - and easy for the attacker

## PACKAGES

**Bronze Packages**

⌚ 600 seconds	\$ 4.99
📅 1 month	

⌚ 600 seconds	\$ 13.99
📅 3 month	

**Silver Packages**

⌚ 1200 seconds	\$ 8.99
📅 1 month	

⌚ 1200 seconds	\$ 24.99
📅 3 month	

**Diamond Packages**

⌚ 7200 seconds	\$ 34.99
📅 1 month	

⌚ 7200 seconds	\$ 99.99
📅 3 month	

At NetSpoof, we're committed to bringing you the best product at the best prices, but also allowing you the **flexibility to choose what works for you**. Doing some stress-testing on your new site? Want to take a target offline, and keep them offline? We provide **all sorts of packages** to suit you! Simply choose the length of time you want to have a license for, the time you'd like each boot to last, and click the button below to **make your automatic purchase** - there's no waiting around!

**BUY NOW- CLICK!**

### HOW TO PAY

**PayPal**  
Autobuy with PayPal

**OR**

**Bitcoin**  
Autobuy with Bitcoin



# Stressers and booters

## "Stressers" and "booters"

STRESSER

Host:	127.0.0.1 [INSE]
Port:	<ul style="list-style-type: none"><li>UDP</li><li>SSYN</li><li>UDP-Lag</li><li>Slowloris</li><li>RUDY</li><li>ARME</li><li>Layer 7 GET</li><li>Layer 7 POST</li><li>Layer 7 HEAD</li></ul>
Time:	
Method:	UDP

**Stress**

SERVER STATUS

Alpha: Online

---

Echo: Online

---

Foxtrot: Online

---

Sierra: Online

STATISTICS

Online Users: 9 Users Online

---

Total Users: 33301

---

Total Stresses: 780998

---

Attacks Running: 5

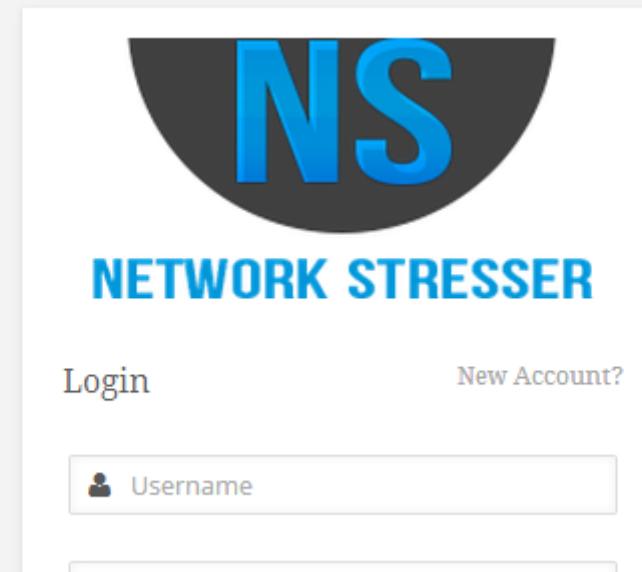


## Stressers and booters

### "Stressers" and "booters"



**Network Stresser the best IP  
Stresser money can buy!  
Voted #1 Booter all booter rating  
sites!**



## What is DoS

DoS can take place at any layer

**Most common:**

IP/TCP/UDP/ICMP

(Layer 3 and 4 – transport and network)

Applications  
(Layer 7 attacks)



# **Denial-of-Service (DoS): “Magic packets/ Poison packets”**



DoS: “Magic Packets”

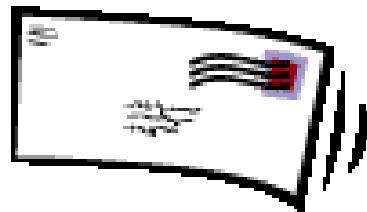
## **Unexpected and unwanted traffic**

Malformed packets:  
overlapping, fragmented, too large,  
too small, ‘strange’ options

Result: Crashing host or service  
or high CPU load so other requests  
cannot be serviced



## "Magic Packets" - Land



To: Peter  
From: Peter



DoS: "Magic Packets"

## Land - same sender and recipient:

**Expected:** TO: A:port 80, FROM **B**:port 2304



**Recieves:** TO: A:port 80, FROM **A**:port 80



DoS: “Magic Packets”

## **ICMP ‘Ping of Death’:**

ICMP-packet max length:



Packet longer than max length after assembly:



DoS: "Magic Packets"

## TearDrop: Overlapping packets:

Expected: large packet, reassembled:



Received: large overlapping packet:



## DoS: “Magic Packets”

Don't fragment flag set, + 'more fragments follows' flag set:



## DoS and DDoS

Modern operating systems are (currently)  
not vulnerable

Internet of Things etc could change that

Currently flooding attacks are much  
more common





# Bandwidth Saturation

## DoS: Bandwidth Saturation

Sending more traffic than the network/server can handle

Smurf, Fraggle, SYN-flooding, Stream, UDP-flood, etc, etc, etc

Saturates network router or network uplink

Stopping others from accessing the network or host



## Distributed Denial of Service and BotNets

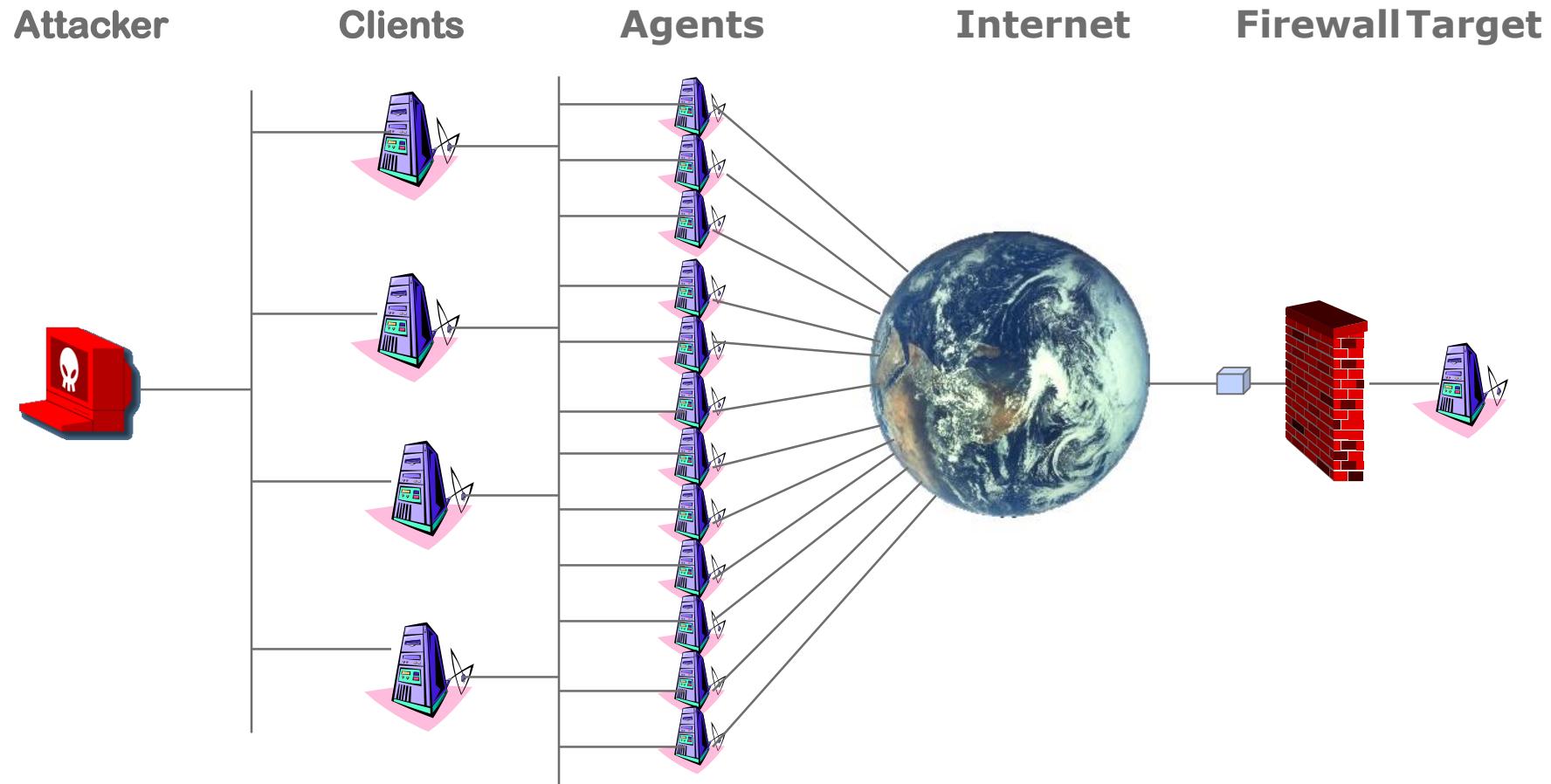
Can be groups of individuals working together  
(hacktivism)

Most commonly:

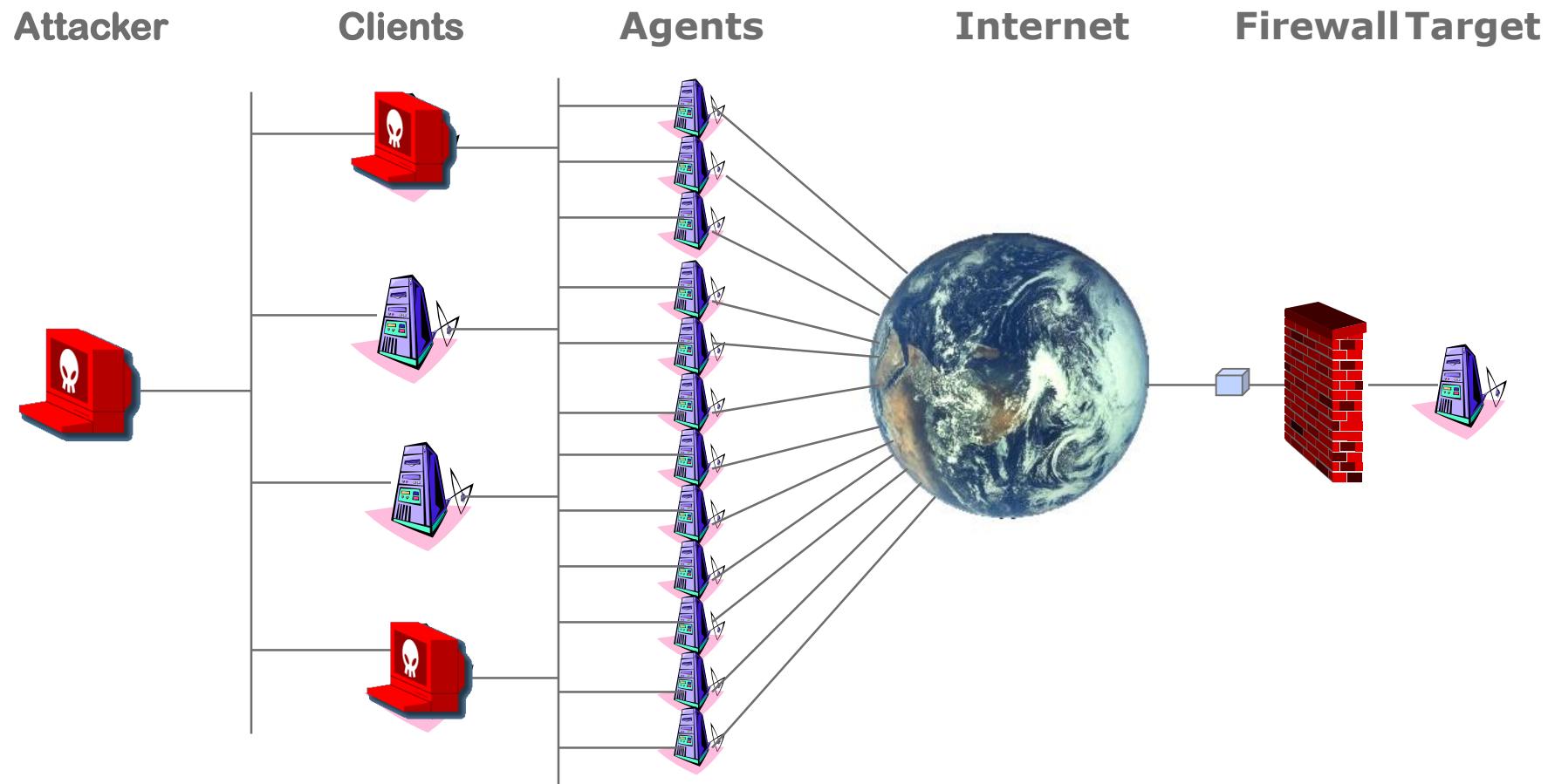
Botnets of compromised PCs or compromised servers



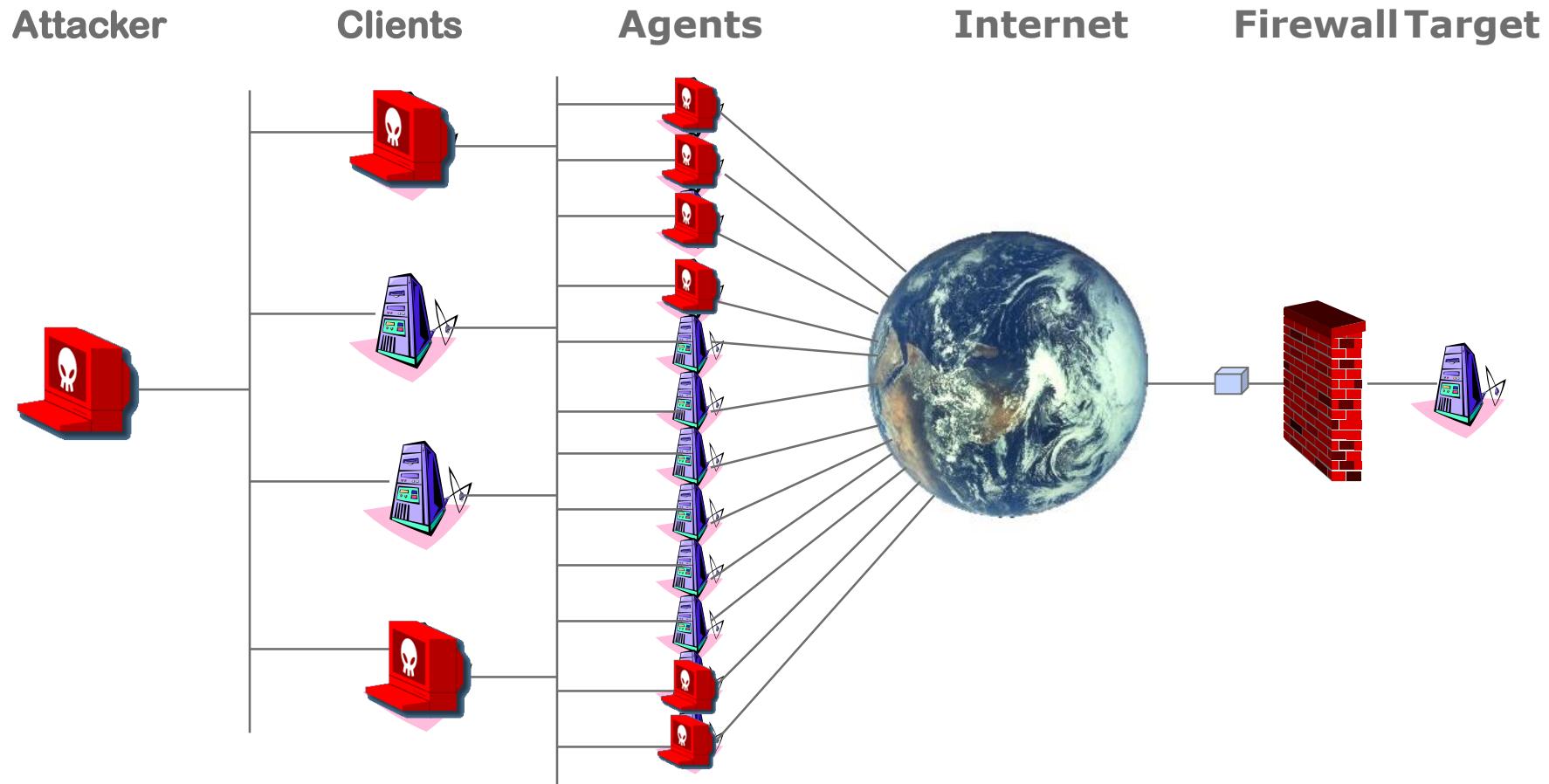
# Distributed Denial-of-Service Attack



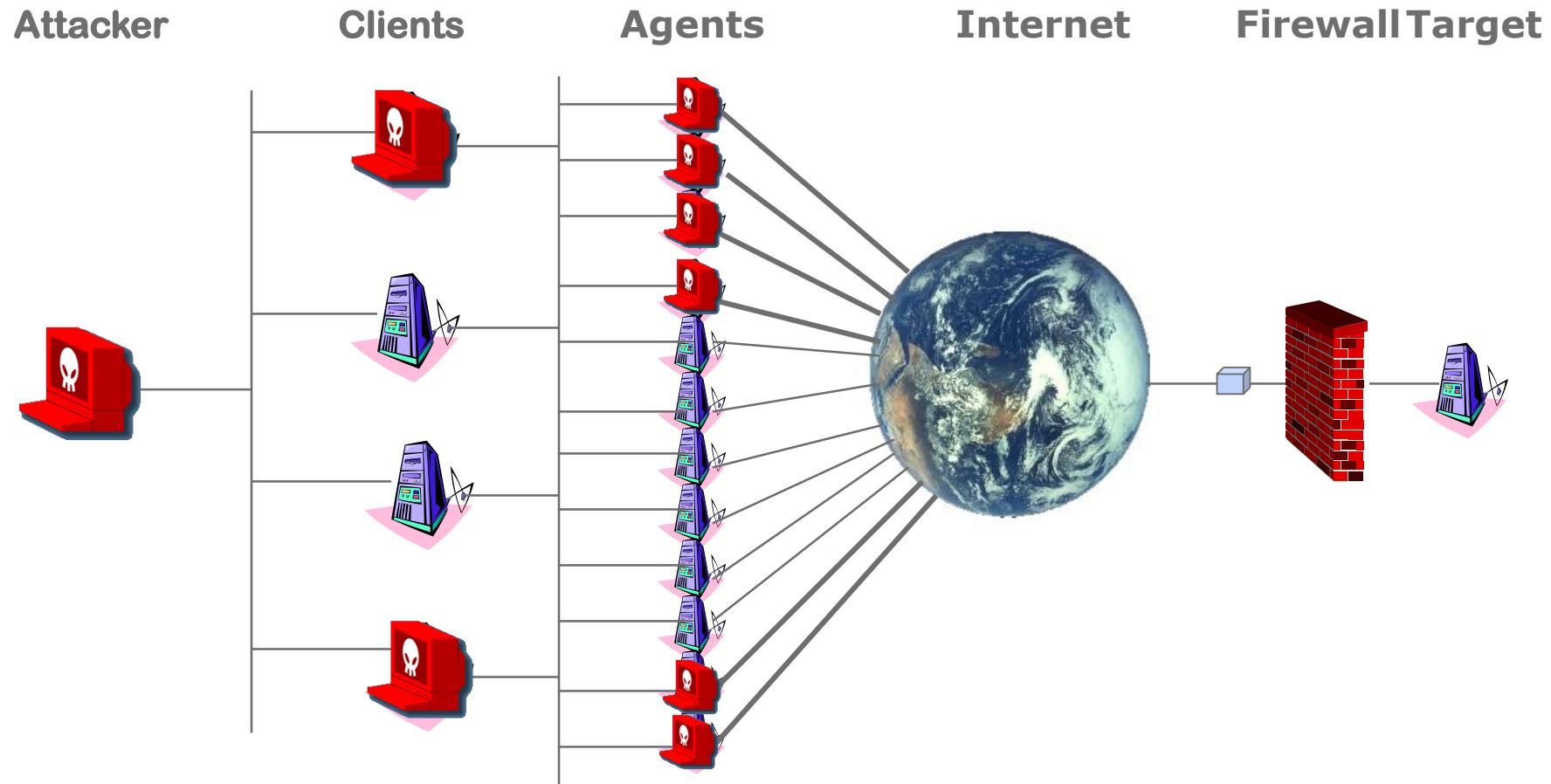
# Distributed Denial-of-Service Attack



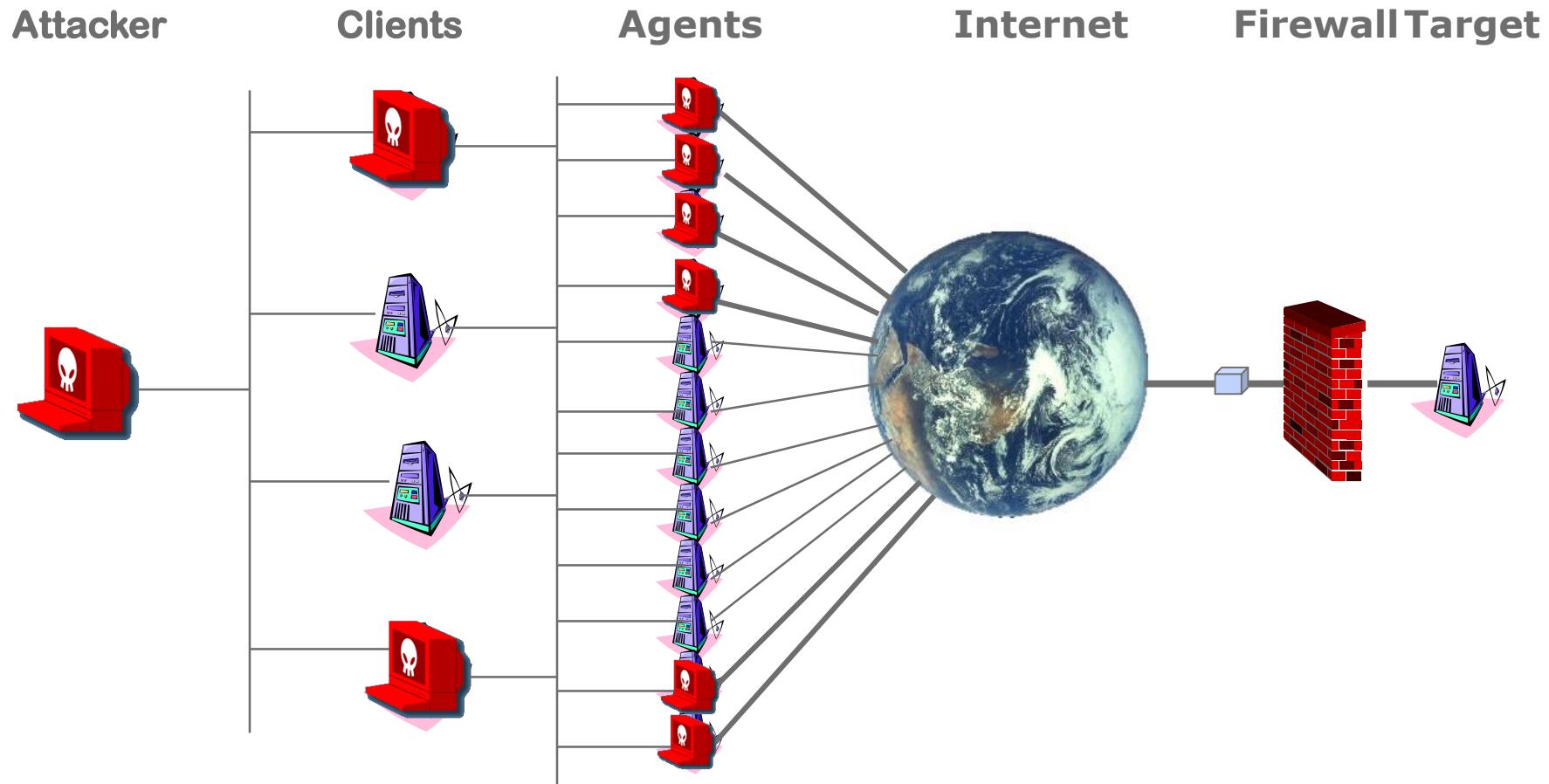
# Distributed Denial-of-Service Attack



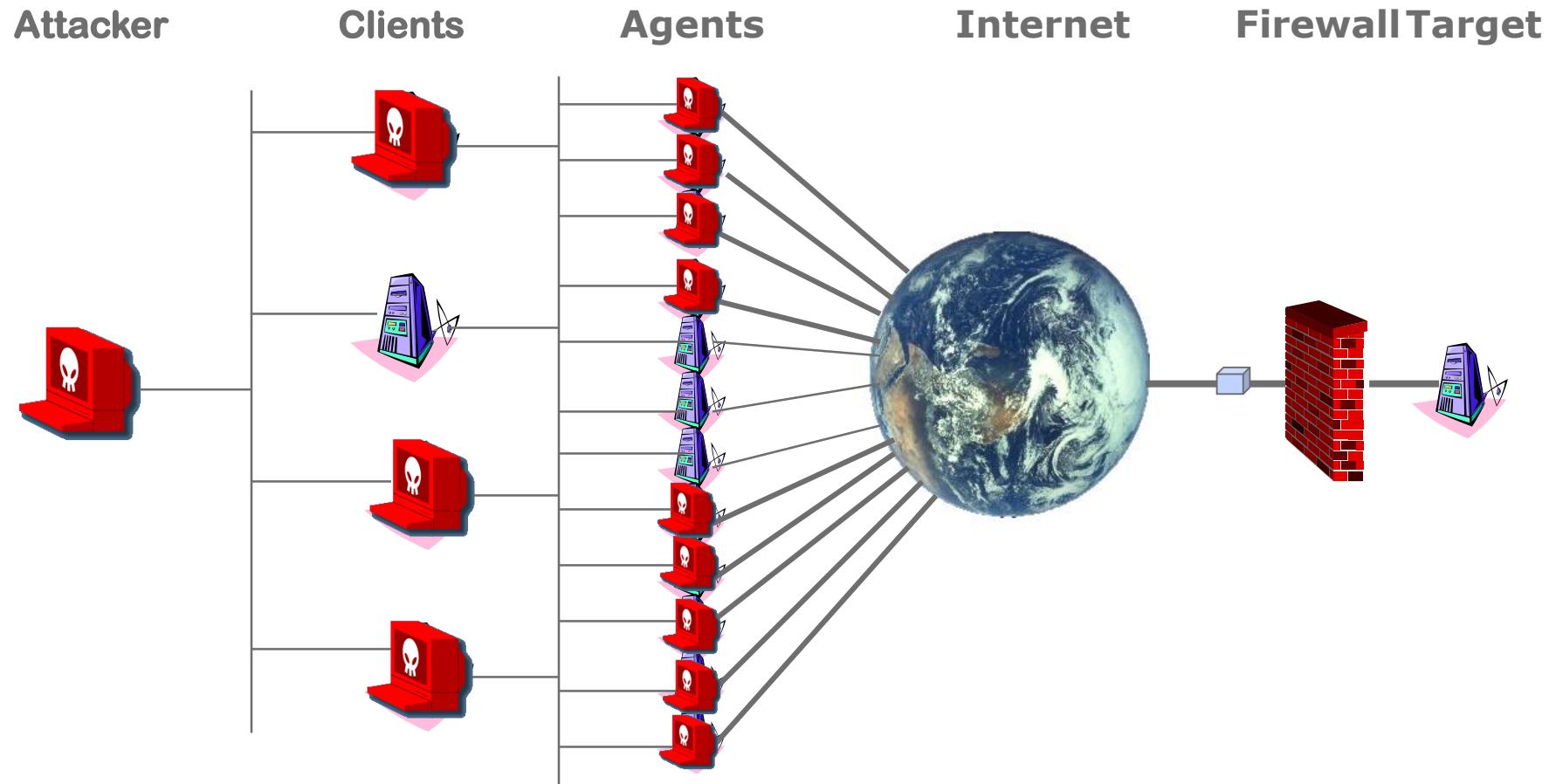
# Distributed Denial-of-Service Attack



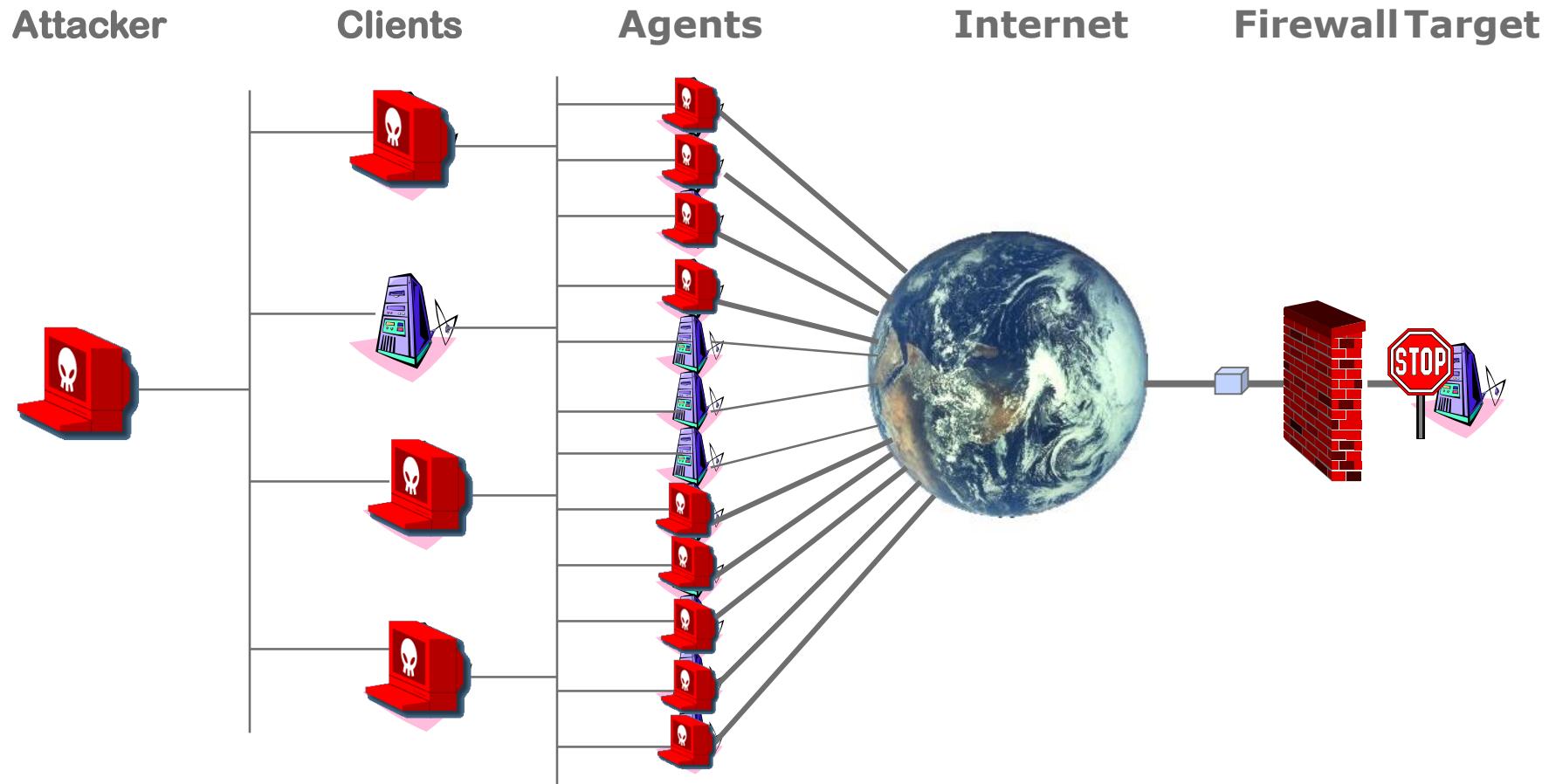
# Distributed Denial-of-Service Attack



# Distributed Denial-of-Service Attack



# Distributed Denial-of-Service Attack



# Tribe Flood Net 2000

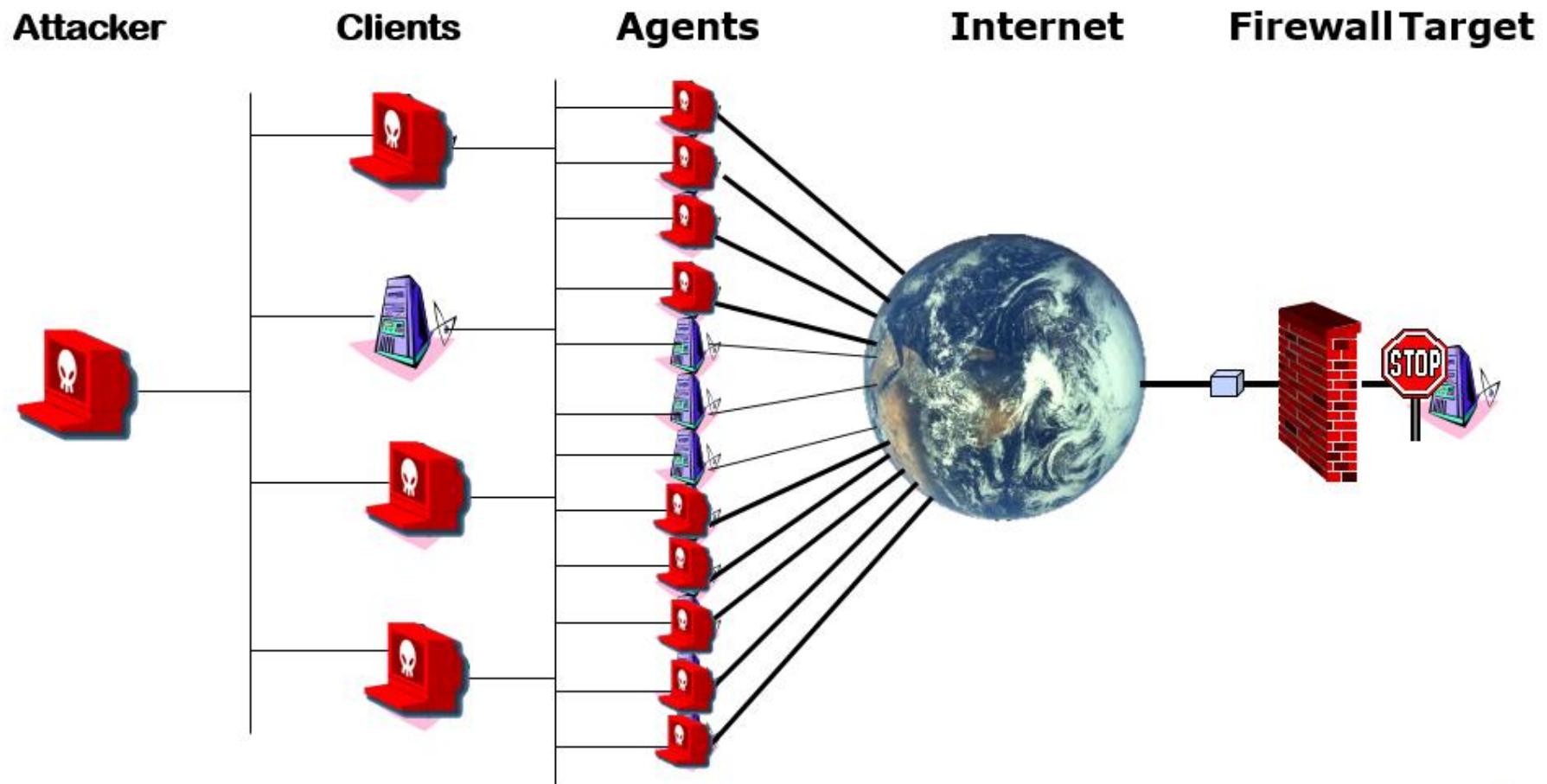
```
Terminal <4>
Fil Indstillinger Hjælp

[root@t3 tfn2k]# ./tfn
usage: ./tfn <options>
[-P protocol] Protocol for server communication. Can be ICMP, UDP or TCP.
              Uses a random protocol as default
[-D n]         Send out n bogus requests for each real one to decoy targets
[-S host/ip]   Specify your source IP. Randomly spoofed by default, you need
              to use your real IP if you are behind spoof-filtering routers
[-f hostlist]  Filename containing a list of hosts with TFN servers to contact
[-h hostname]  To contact only a single host running a TFN server
[-i target string] Contains options/targets separated by '!', see below
[-p port]       A TCP destination port can be specified for SYN floods
<-c command ID> 0 - Halt all current floods on server(s) immediately
                  1 - Change IP antispoof-level (evade rfc2267 filtering)
                      usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
                  2 - Change Packet size, usage: -i <packet size in bytes>
                  3 - Bind root shell to a port, usage: -i <remote port>
                  4 - UDP flood, usage: -i victim0!victim2!victim3...
                  5 - TCP/SYN flood, usage: -i victim0... [-p destination port]
                  6 - ICMP/PING flood, usage: -i victim0...
                  7 - ICMP/SMURF flood, usage: -i victim0!broadcast0!broadcast2...
                  8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim0...
                  9 - TARGA3 flood (IP stack penetration), usage: -i victim0...
                 10 - Blindly execute remote shell command, usage -i command

[root@t3 tfn2k]#
```



## Problems for the attacker?



Attacker risk assessment...



# Source Address Spoofing

## Using forged source addresses

- Usually via the raw socket interface on operating systems
- Makes attacking systems harder to identify

Attacker generates large volumes of packets that have the target system as the destination address



## Spoofing

DoS and DDoS often use spoofed traffic to target, including spoofed source IPs

Random attack source IPs looks like real SYNs.  
Source IP spoofing looks as if attack is coming from virtually infinite number of sources

Since packet data can be fully randomized upstream IP filtering techniques is generally useless



## Spoofing

UDP and ICMP attacks are most popular since they don't require a handshake and therefore works well with spoofed source address

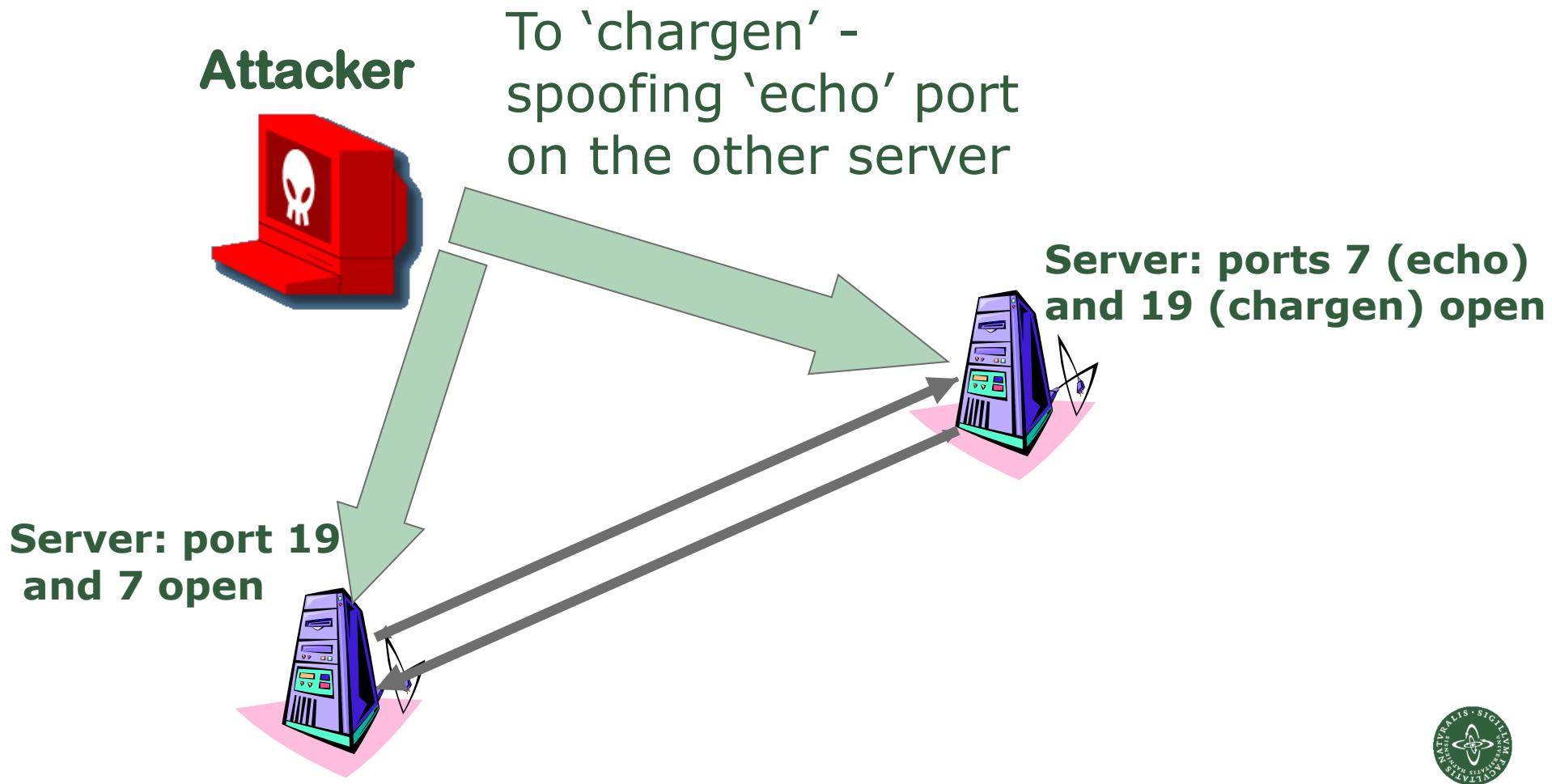
Attackers not interested in receiving responses to the requests they send - the packets do not have to be accurate or correctly formatted



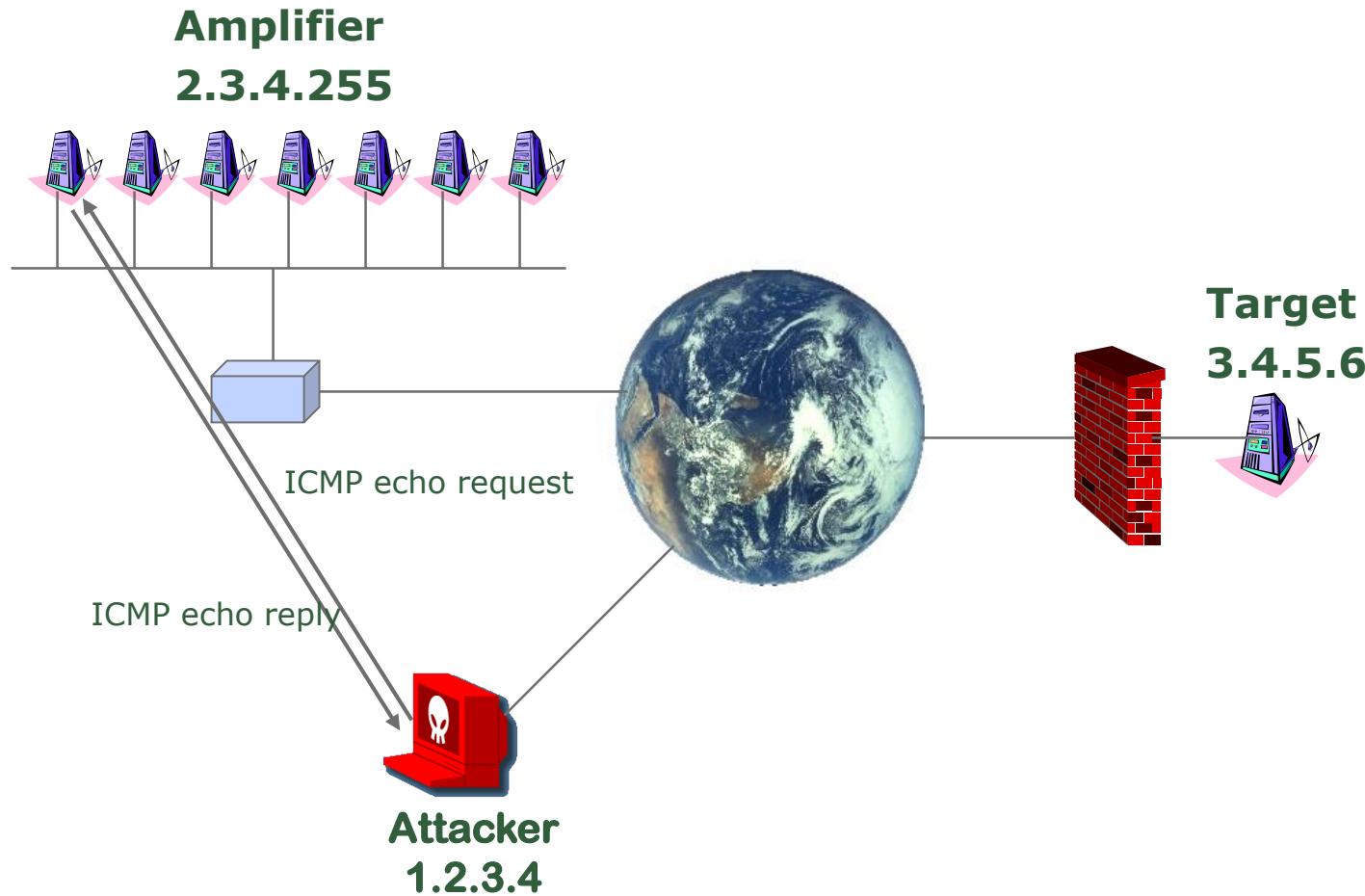


# Amplification DDoS

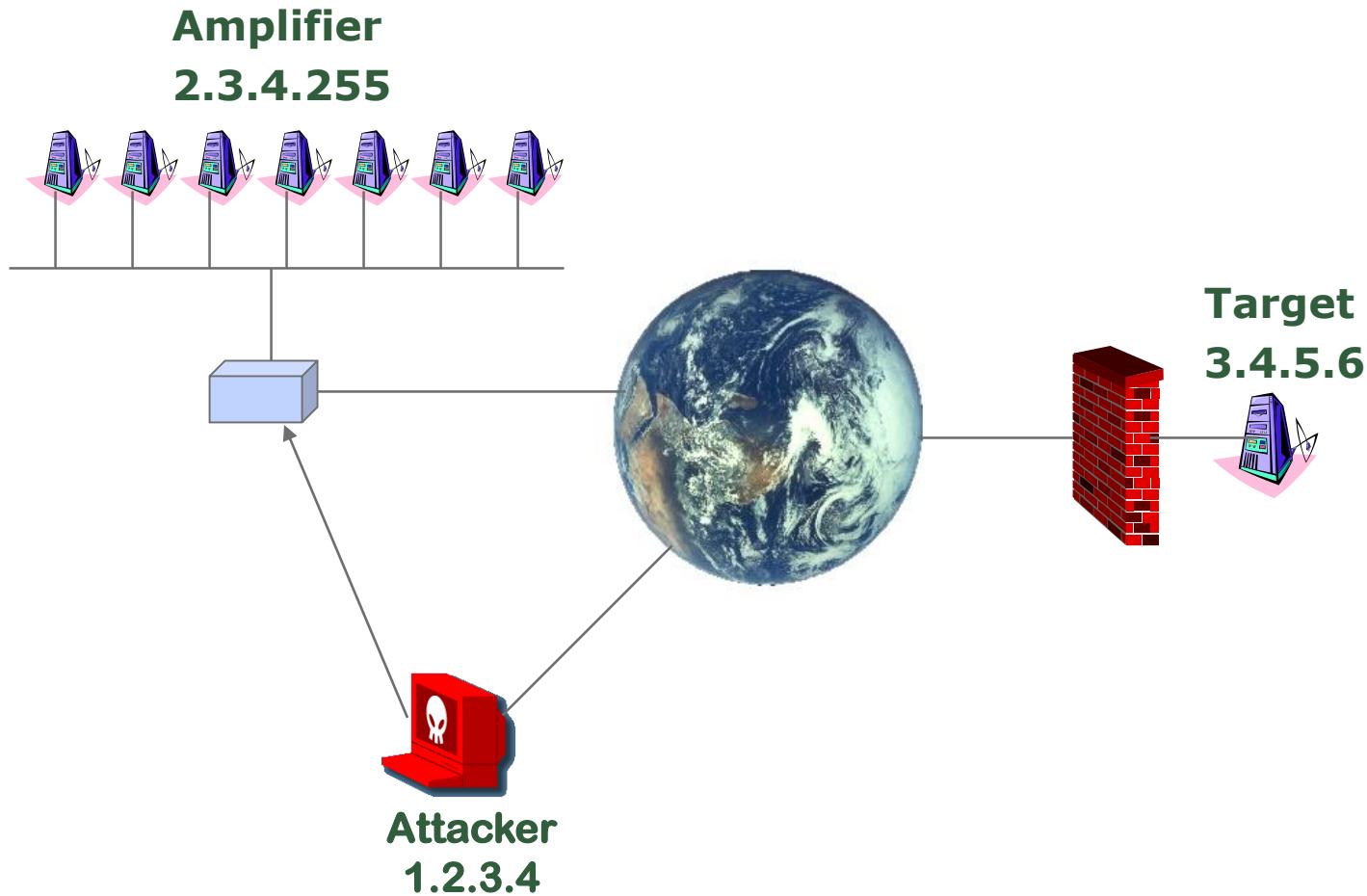
## Chargen, echo etc



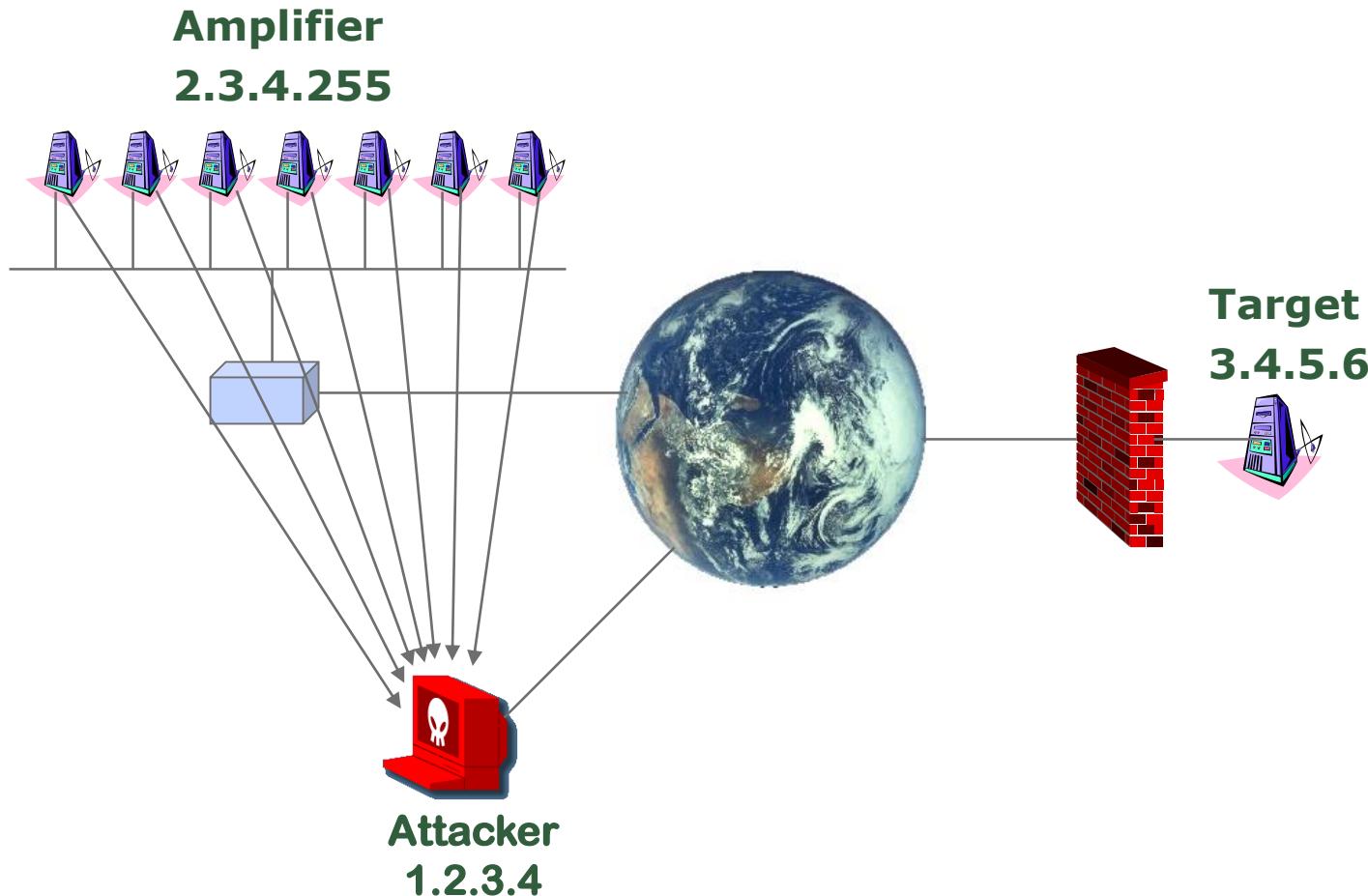
# Smurf (and Fraggle):



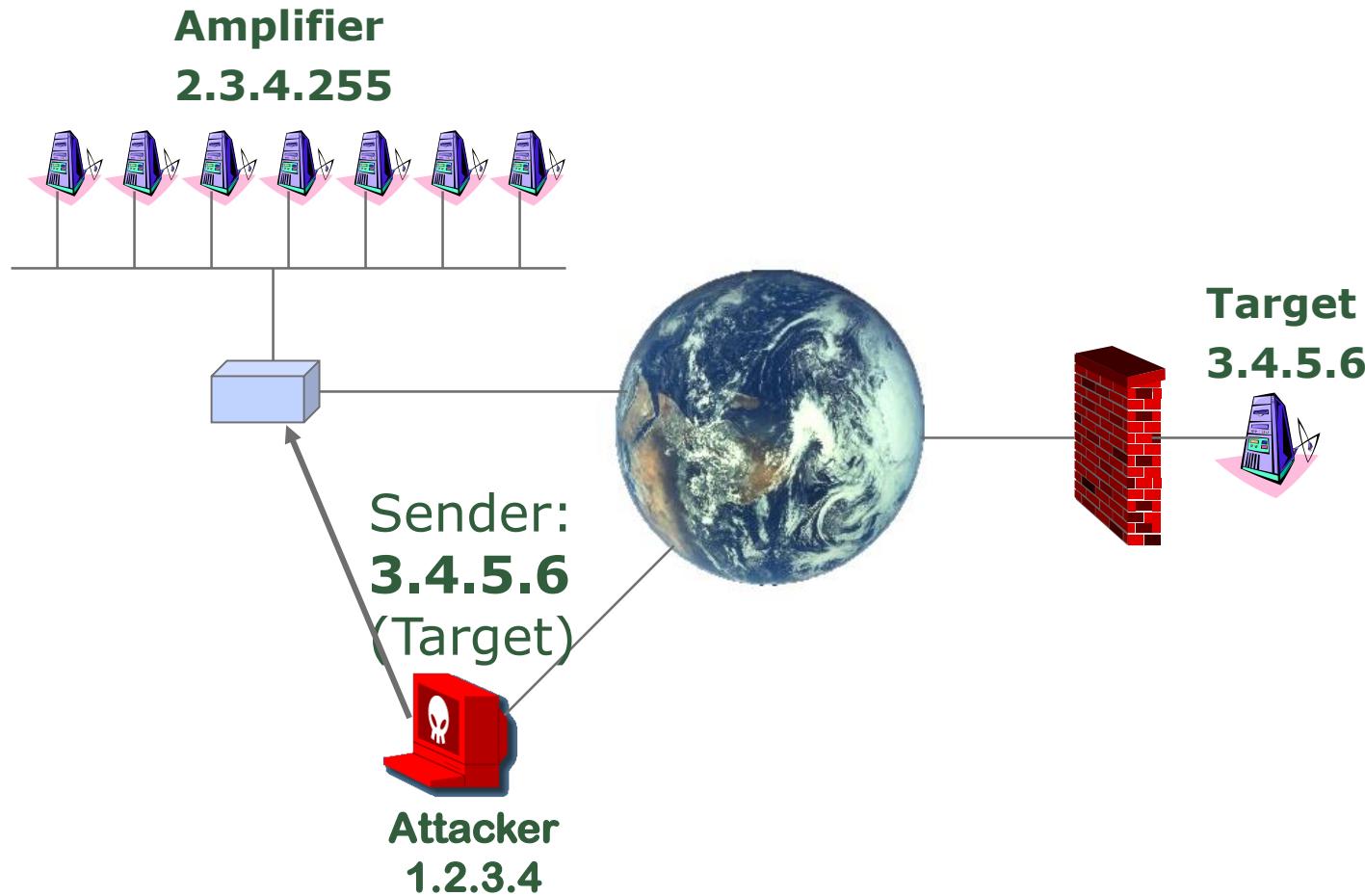
## Smurf (and Fraggle):



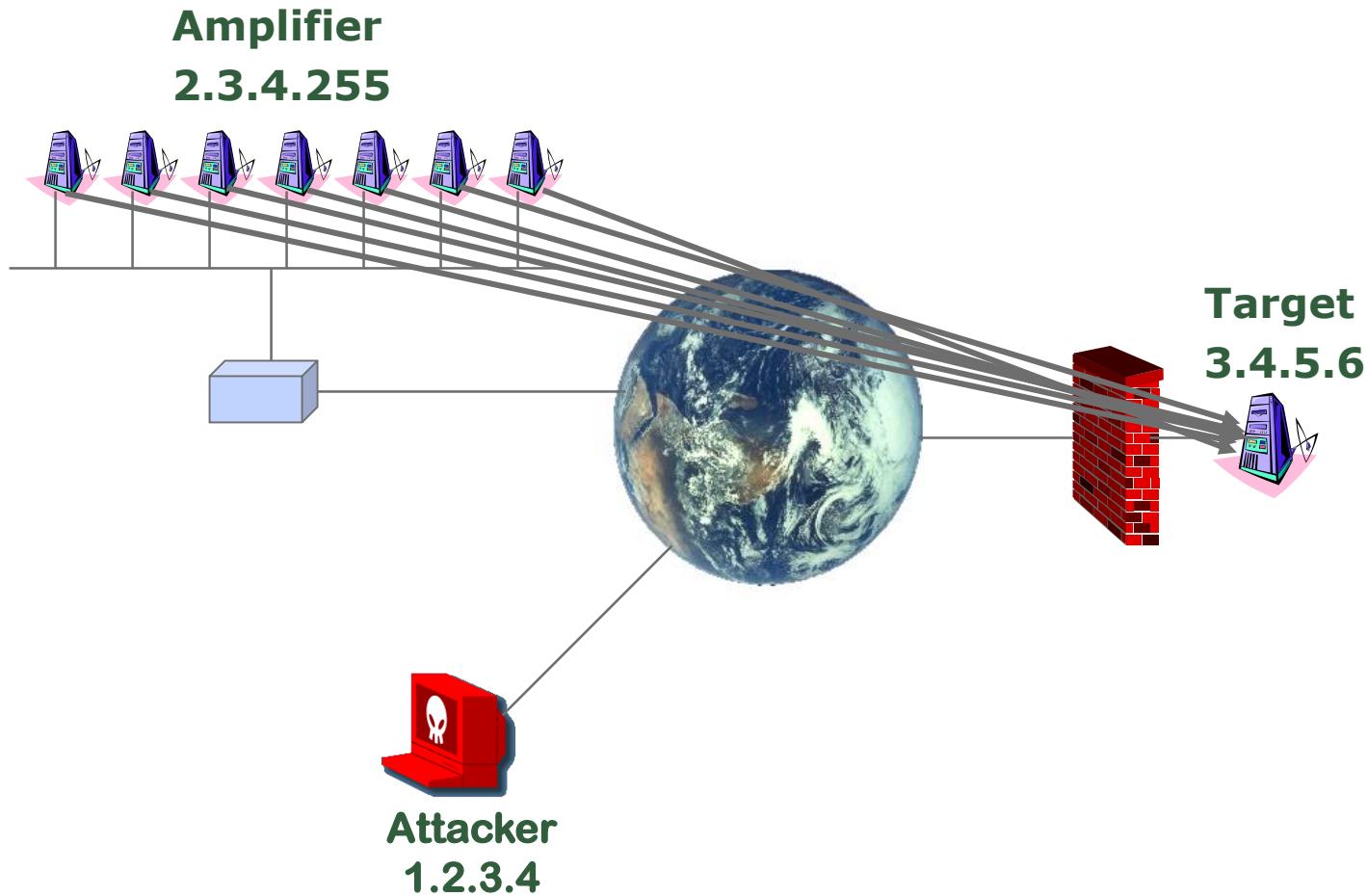
## Smurf (and Fraggle):



## Smurf (and Fraggle):



## Smurf (and Frabble):



## Smurf attack

768 kb/s, 100 computers = 76.8 Mb/s



## DNS amplification attacks

A 64 byte query results in a 3,223 byte zone response (50-times amplification)

```
dig ANY isc.org @x.x.x.x +edns=0
```

Query is sent with a spoofed source address.  
DNS queries are most often UDP



Amplification attacks are very common

(Smurf: 768 kb/s, 100 computers = 76.8 Mb/s)

DNS: 100 to 500 Gbps is now common

NTP – Network Time Protocol

SSDP – Simple Service Discovery protocol

Internet of Things cameras etc.



Use your risk assessment knowledge

Record for largest DDoS attack

December 2015: 500 Gbps (several – DNS amplification)

January 2016 : 602 Gbps against BBC

21.Sep 2016: 665 Gbps against Brian Krebs

24. Sep 2016: 1Tbps (1000 Gbps) against Brian Krebs

25. Sep 2016: 1.1 Tbps against OVH (hosting provider)

February 28. 2018: 1.35 Tbps against GitHub

Internet of Things...

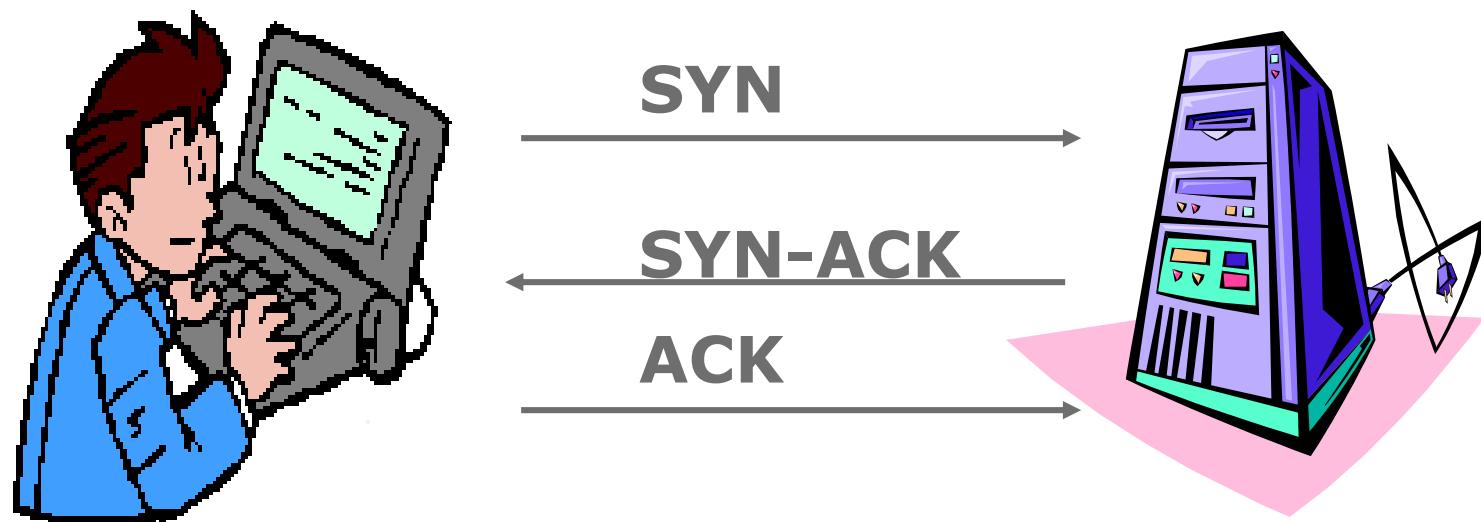
In Q1 2019, there was an increase of 967% for attacks sized 100 Gbps or higher, compared to Q1 2018





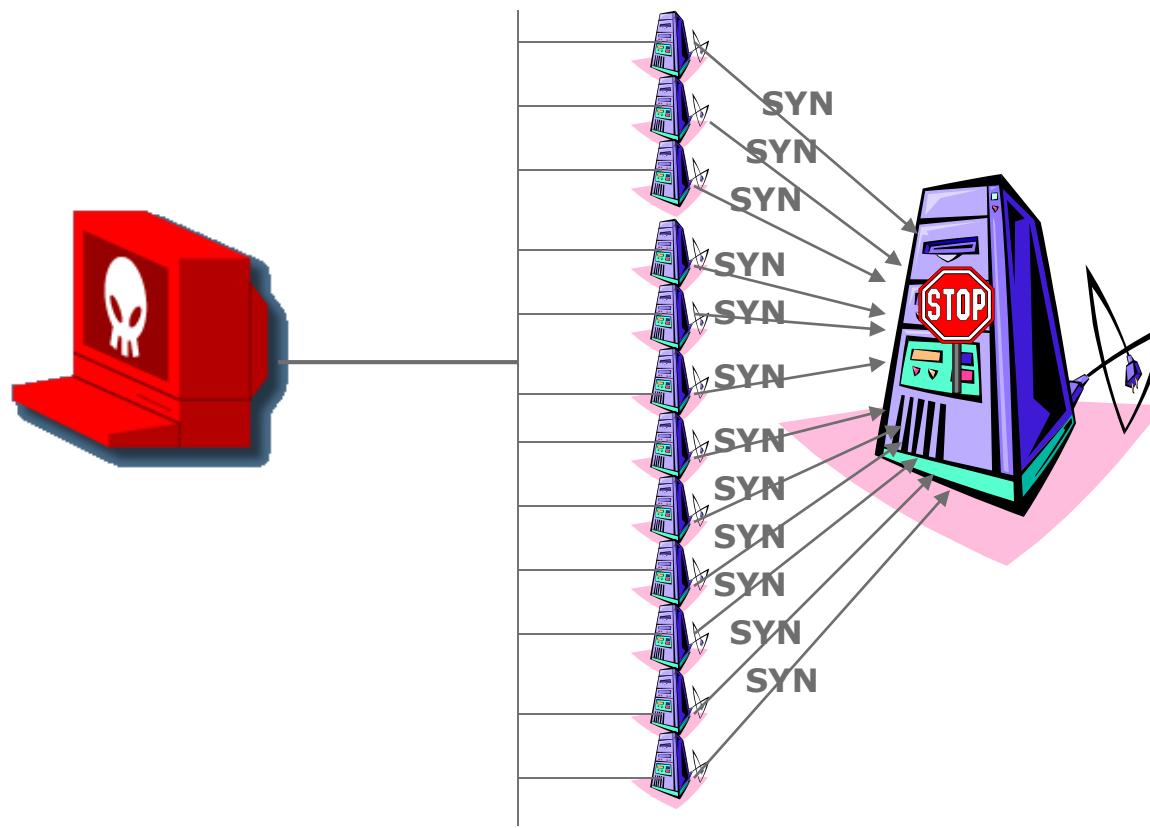
# Other common flood-techniques

## 3-way handshake:



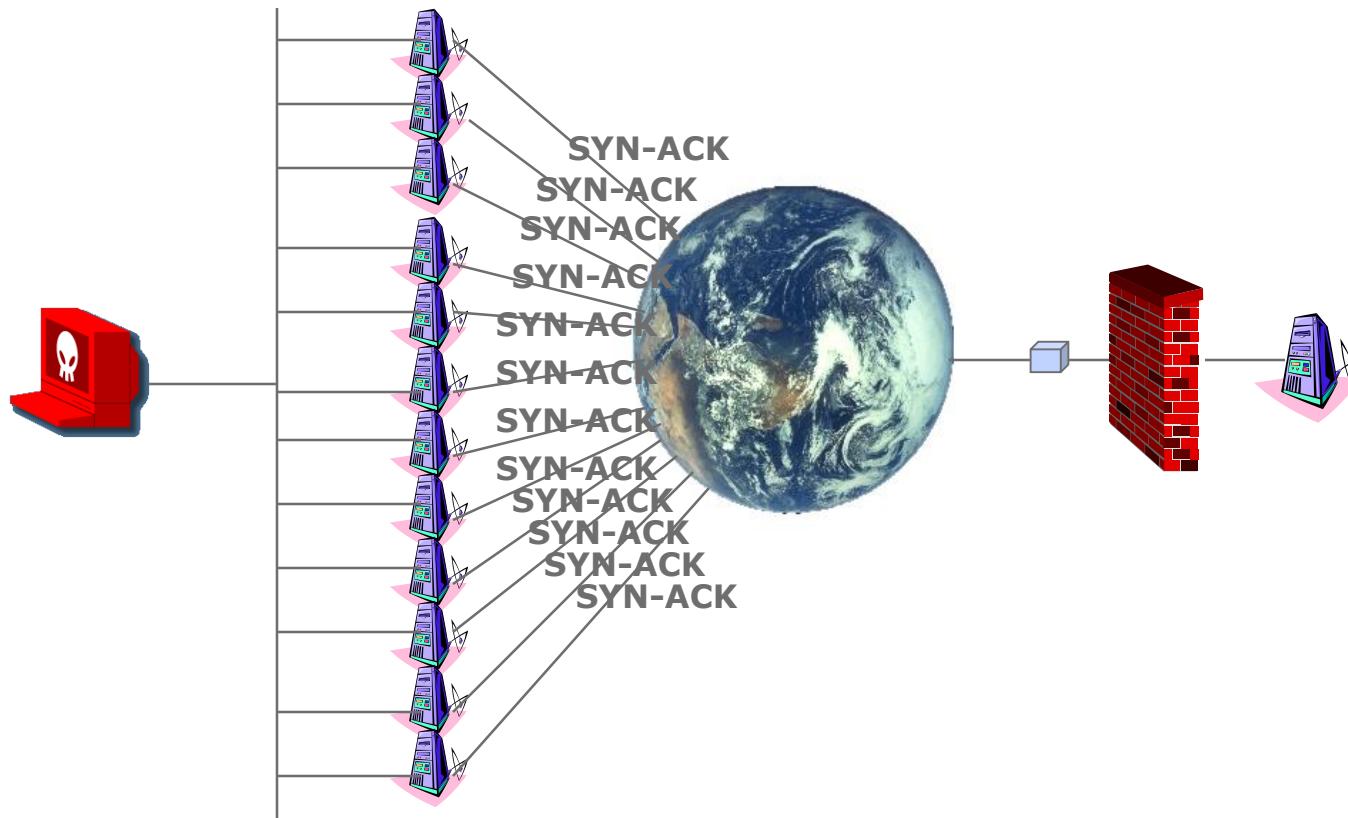
## SYN-flood:

**Attacker      Spoofed addresses      Target**



# Stream Attack

Controller    Spoofed addresses    Internet    Firewall Target



## Reflection attack

Spoofed SYN-ACK flood - uses **CPU** on target computer **AND bandwidth**:

In addition to flood of SYN-ACK packets, target sends TCP RST to non-existent IP-addresses.

Routers will then send back 'ICMP host/network unreachable' adding to bandwidth consumption

Not amplification, this type is known as **reflection attacks**



## Other 'flag' and 'header' flooders

ACK-flood

RST-flood

NULL-flood (like SYN-flood, but with TCP flags set to 0)

Random flag-flood

Random TCP-headers flood

IP-header flood

Fragment-flood

Mixed-flood attacks





# Application DDoS (Layer 7 attacks)

# Application DDoS

Focus is focus on specific characteristics of web applications that create bottlenecks



# Hypertext Transfer Protocol (HTTP) Based Attacks

## HTTP flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources
- Website searches
  - Resource heavy searches – target specific
- Spidering
  - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

## HTTP POST/GET targets logical resources, not CPU or network

Sends a complete, legitimate HTTP POST header, including a 'Content-Length' field to specify size of message body to follow.

Attacker then sends message body slowly (1 byte/110 seconds). Entire message is correct and complete - target server will obey the 'Content-Length' field in header: waits for the entire body of the message  
Attacker establishes hundreds or thousands of connections -> using all resources for incoming connections on victim



## Slow Read

Slow reading attacks advertise a very small number for the TCP Receive Window size while emptying clients' TCP receive buffer slowly.

That naturally ensures a very low data flow rate.

Slow Read attacks then sends packets slowly across multiple connections.

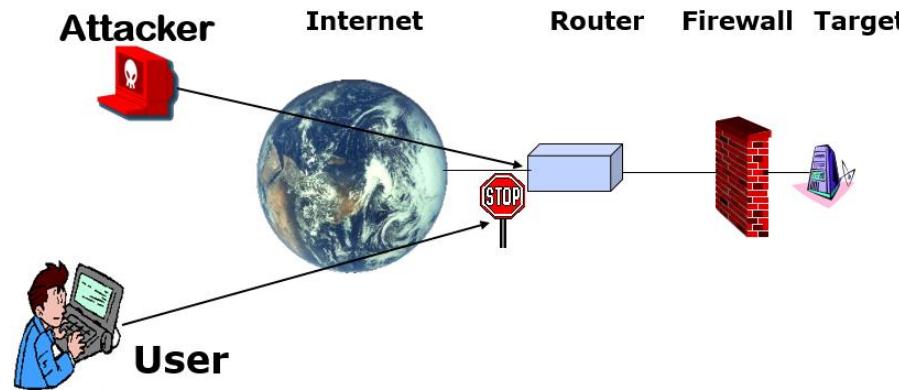
Apache opens a new thread for each connection, and since connections are maintained as long as there is traffic being sent, an attacker can overwhelm a web server by exhausting its thread pool relatively quickly.



## Slow Read and HTTP POST/GET – no spoofing

These types of attack bypass flood protection proxies but:

The attacker can no longer spoof or use random source IPs  
This reveals location of the bot zombies and *proxies can then block or rate-limit bots*





# DoS/DDoS defence

## DoS consequences

Attacking specific (web)servers or the entire company infrastructure including DNS and mail.

Datacenters and core internet components.

Sometimes DDoS attacks leads to collateral damage – ISP hosting DNS-servers often victim to Target DNS-floods because of random source IP addresses



Use your risk assessment knowledge

Consider the consequences of a DDoS-attack, what would happen?

Consider your setup, would an attacker be able to DoS more than is actually necessary ?

Consider how an attacker would identify which addresses they need to attack.



## Defence

- On-site – before, and during an attack
- ISP
- Upstream filtering services (scrubbers)

## Threat Analysis and Risk Assessment



## Defence

Magic packets: Patch OS and applications - if possible

Onsite boxes and applications

Is it possible to block traffic from outside Denmark?

Only forward established TCP connections to site/network

Flooding attacks are difficult — if not impossible — to mitigate with an on-premise solution



# Responding to DoS Attacks

## Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Implementing anti-spoofing, directed broadcast, and rate limiting filters
- Network monitors and IDS to detect and notify abnormal traffic patterns



# Responding to DoS Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling



## Defence

Global networks of scrubbing centres

Junk packets are dropped by proxy/scrubber

Filtering - drop unmatched ACKs, malformed packets etc.

Global load-balancing



## Defence

# The world's largest DDoS attack took GitHub offline for fewer than 10 minutes

Jon Russell @jonrussell 7 months ago

 Comment

GitHub called in assistance from Akamai Prolexic, which rerouted traffic to GitHub through its “scrubbing” centers, which removed and blocked data deemed to be malicious. Following eight minutes of the assault, the attackers called it off and the DDoS stopped.

In total, GitHub was offline for five minutes between 17:21 to 17:26 UTC, with intermittent connectivity between 17:26 to 17:30 UTC.



## Defence against Layer 7 attacks

### JavaScript computational challenge tests

Real visitors are allowed to access the site after verification as legitimate

**Your browser is computing access to example.com.**

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...



[Protection by CloudFlare](#)



## Defence

CAPCHAs per source IP address verifies that the visitor is a human

Web application firewalls  
Cookie challenges



## Defence

General changes across networks on the Internet

Smurf is almost removed today:

Routers blocks ICMP relay from broadcast addresses and

Firewalls are default configured to block external ICMP packets to broadcast addresses



## Defence

### Tracebacks

Source IP identification to block attacks at the source

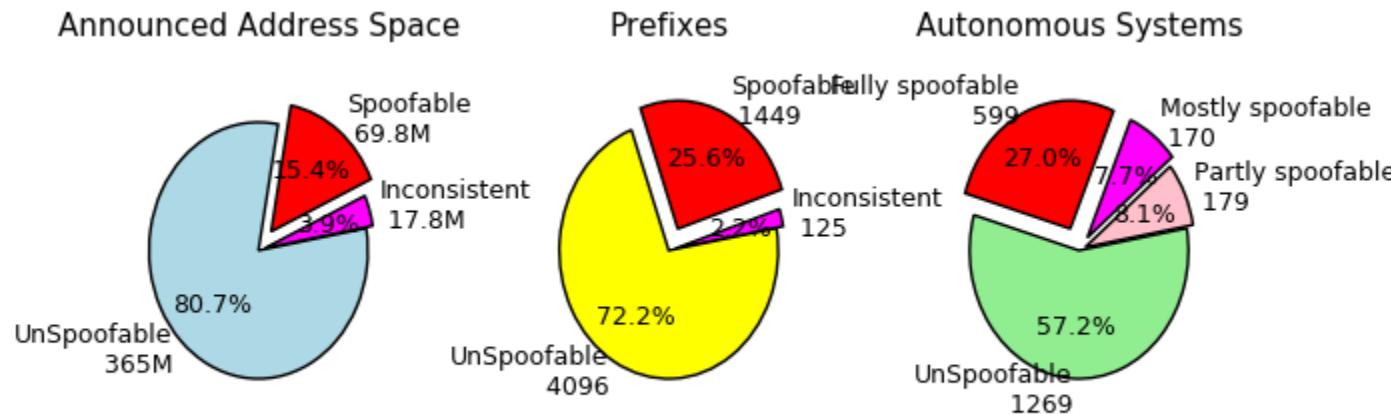
Since DDoS uses spoofed source IPs the ISPs must implement ingress filtering to only forward packets with legitimate source IPs



## Defence

ISPs should drop all spoofed packets  
But all ISPs must do this

No defense if just 10% of ISPs does not implement  
No incentive for deployment



## Defence

Core Internet redesign (many good proposals)



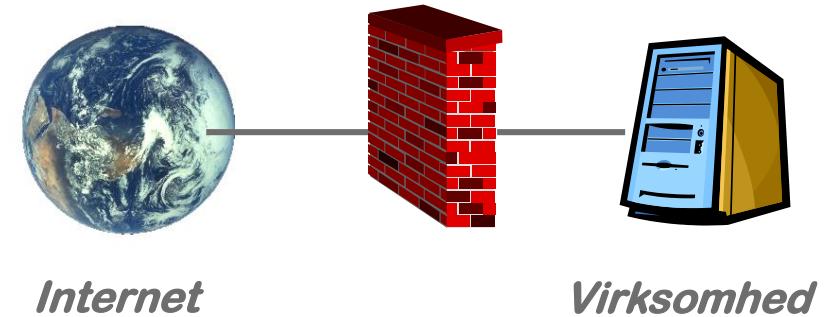


# Security architecture, ports and firewalls

# What is a firewall ?



Perimeter protection



## Firewalls

Hardware or software designed to prevent unauthorized access through perimeter protection

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

Modern firewalls are hybrids and typically use multiple methods



## Firewall types

**Stateless:** Do I like this packet?

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

Policies can be anything and can do anything

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

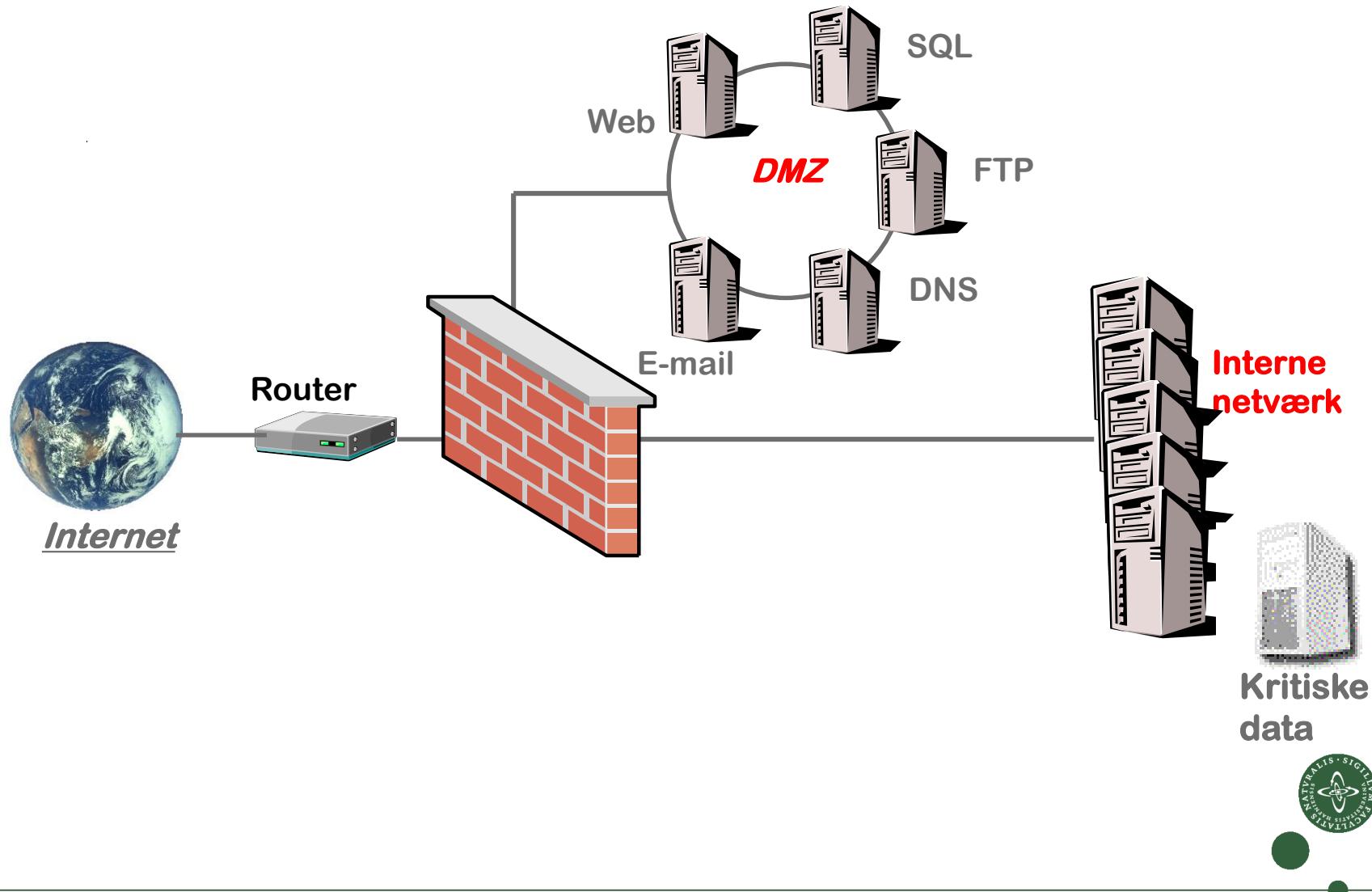


## Firewall typer

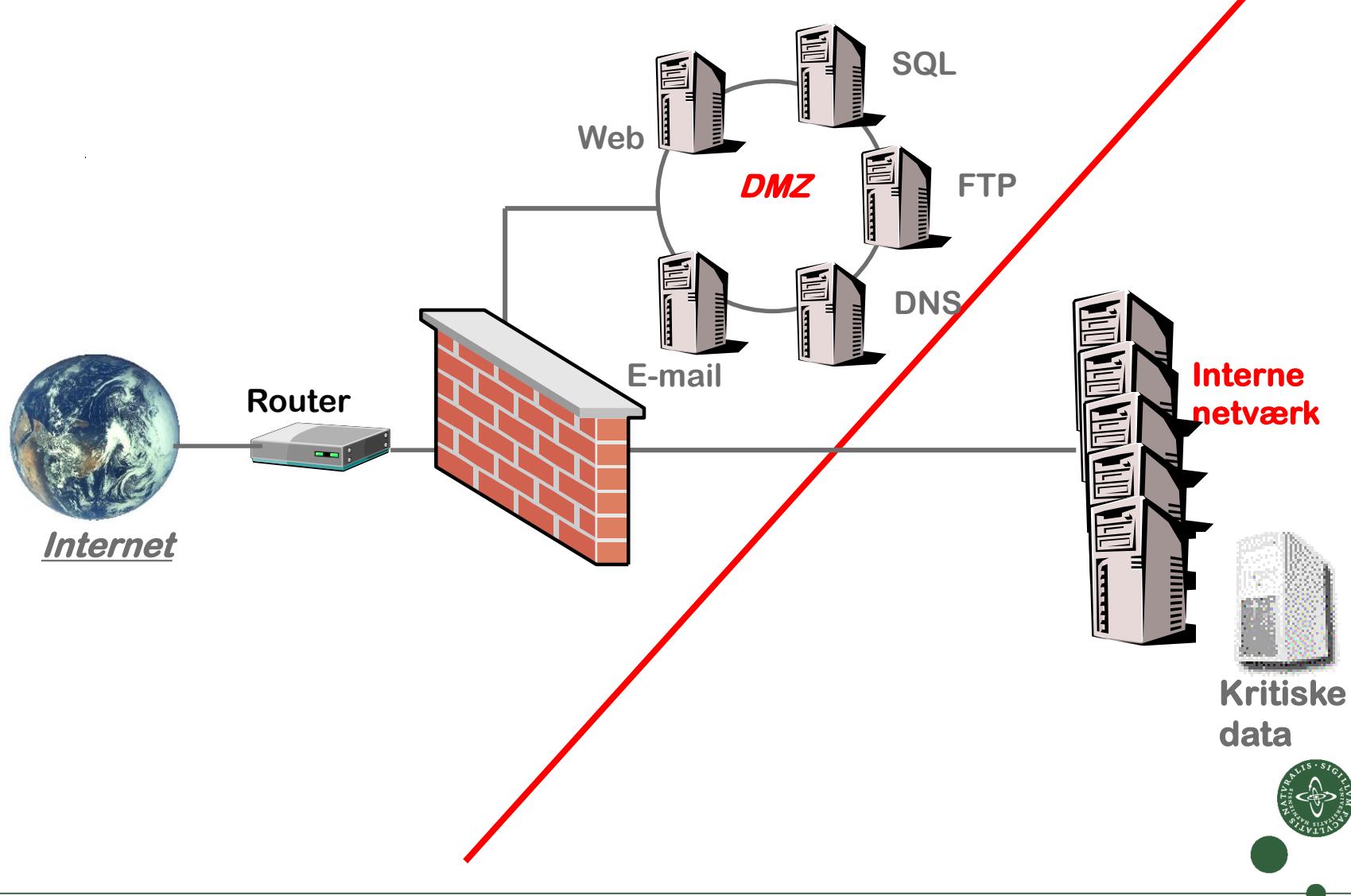
- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on defined filter rules (addresses and port numbers). Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- **Stateful inspection / Circuit-level gateway:**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



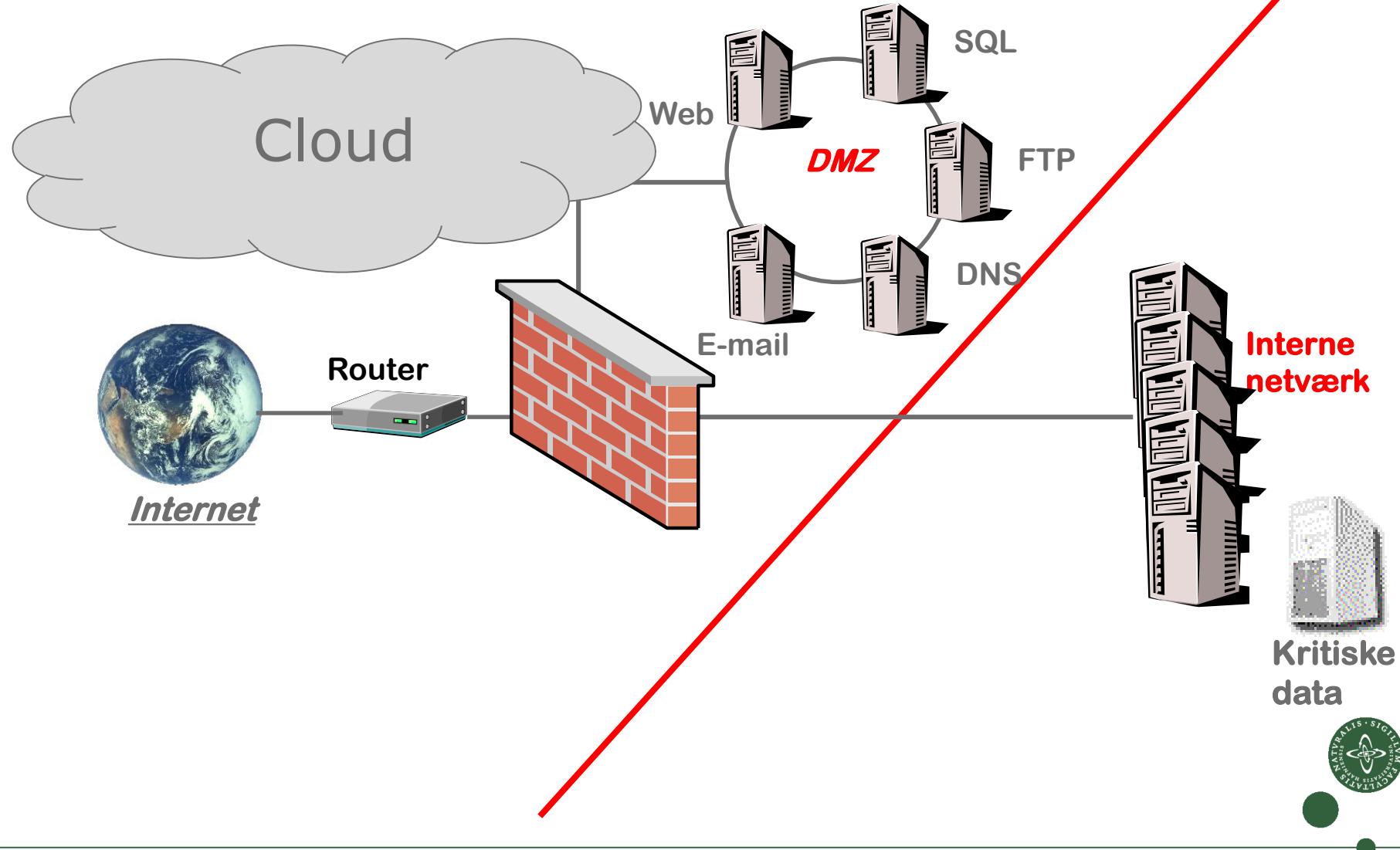
# Network and architecture



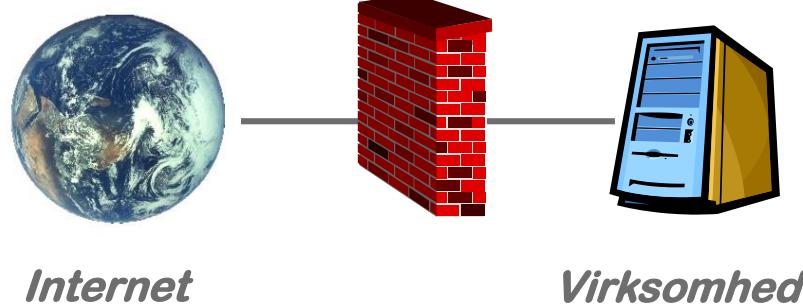
# Network and architecture



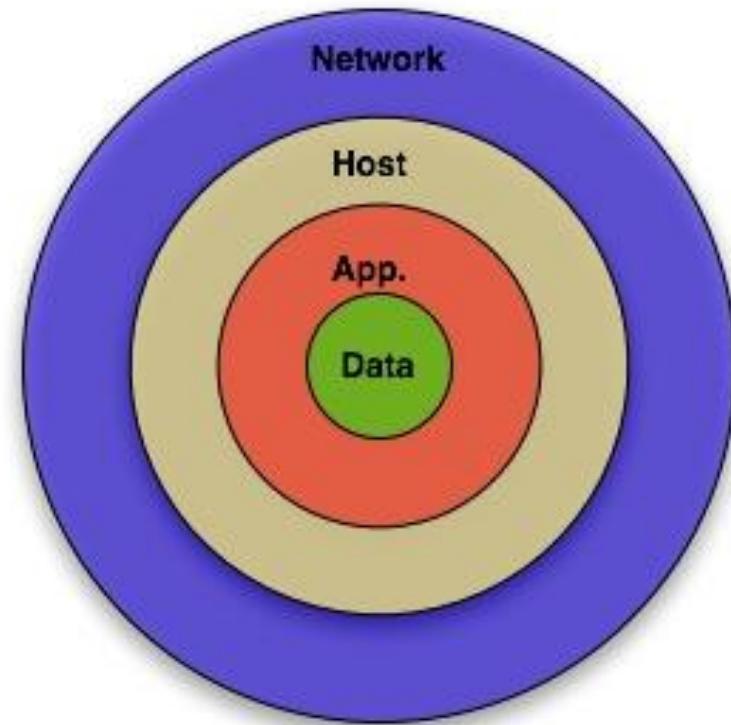
# Network and architecture



## Opening ports in the firewall



After opening?



**Defense in Depth**



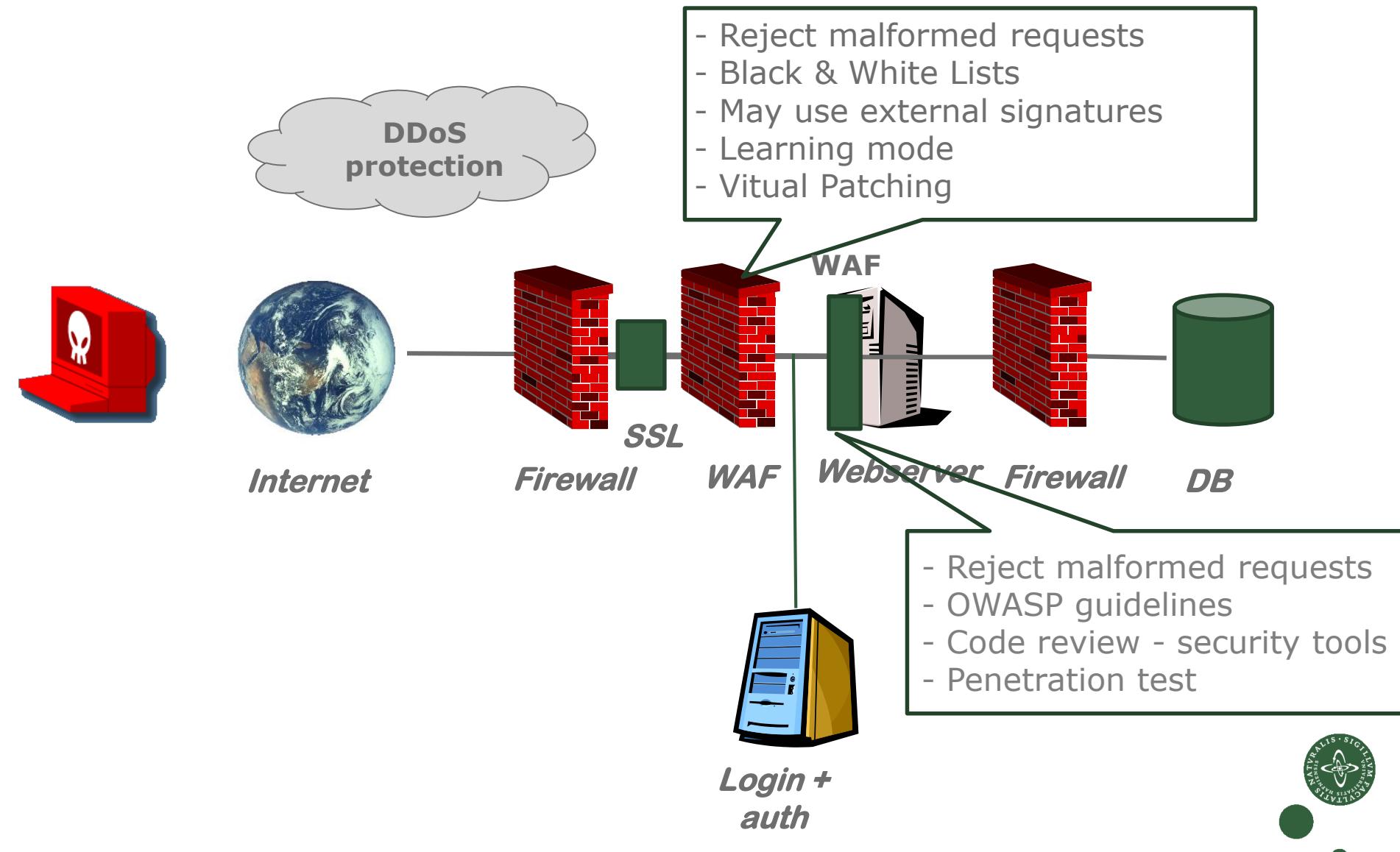
Remember your risk assessment basics

Eliminate/Mitigate  
Minimize (compensate)  
Transfer  
Accept  
~~Ignore~~

Prevent - Detect - Respond



# Layers of security and the firewall





# Which is “Best”?



## Threat modeling – the 5 questions

1. What do you want to protect?  
**Assets**
2. Who do you want to protect it from?  
**Adversaries and threats**
3. How likely is it that you will need to protect it?  
**Probability**
4. How bad are the consequences if you fail?  
**Risk**
5. How much trouble are you willing to go through in order to try to prevent those?  
**Value**



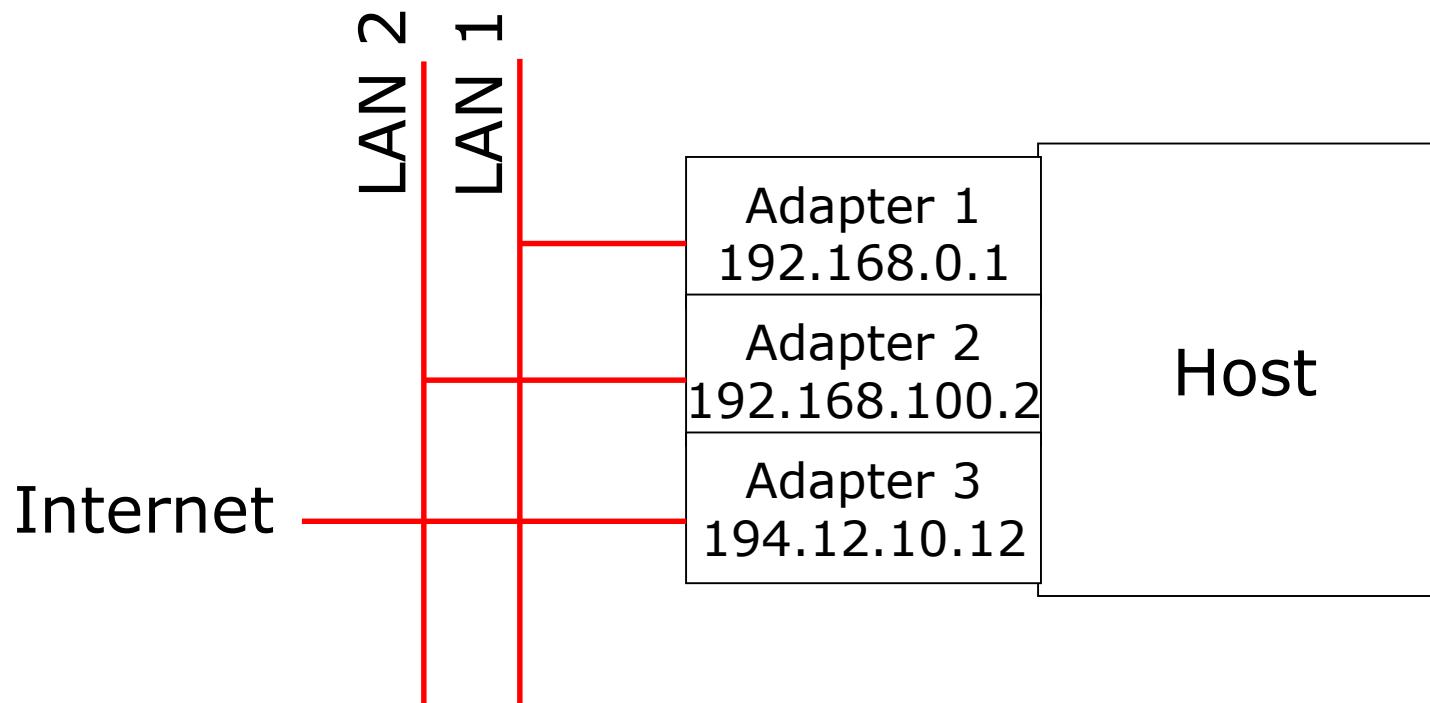


# Ports and firewalls

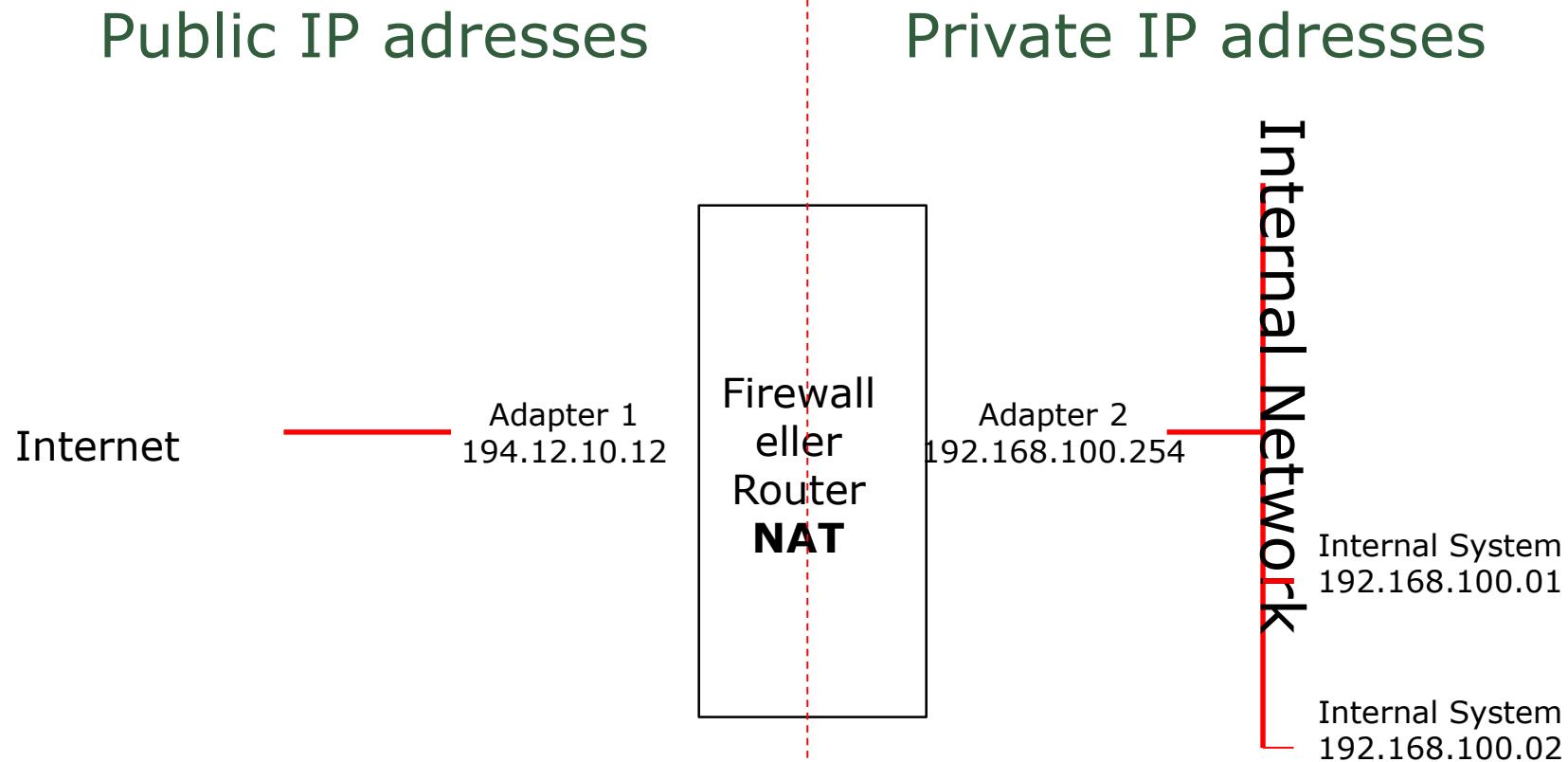
## Firewalls

IP addresses are associated with adapters,  
not CPUs

A single host can have many IP addresses



## Network Address Translation (NAT)



## 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

<u>Service</u>	<u>Port</u>	<u>Protocol</u>
FTP	21	TCP
Telnet	23	TCP
Simple Mail Transfer Protocol (SMTP)	25	TCP
Domain Name	53	UDP
HTTP (web server)	80	TCP
POP3 (mail box)	110	TCP
NetBios loc-srv	135	TCP
NetBios Name	137	TCP
NetBios Datagram	138	TCP
NetBios Session	139	TCP



## TCP/IP

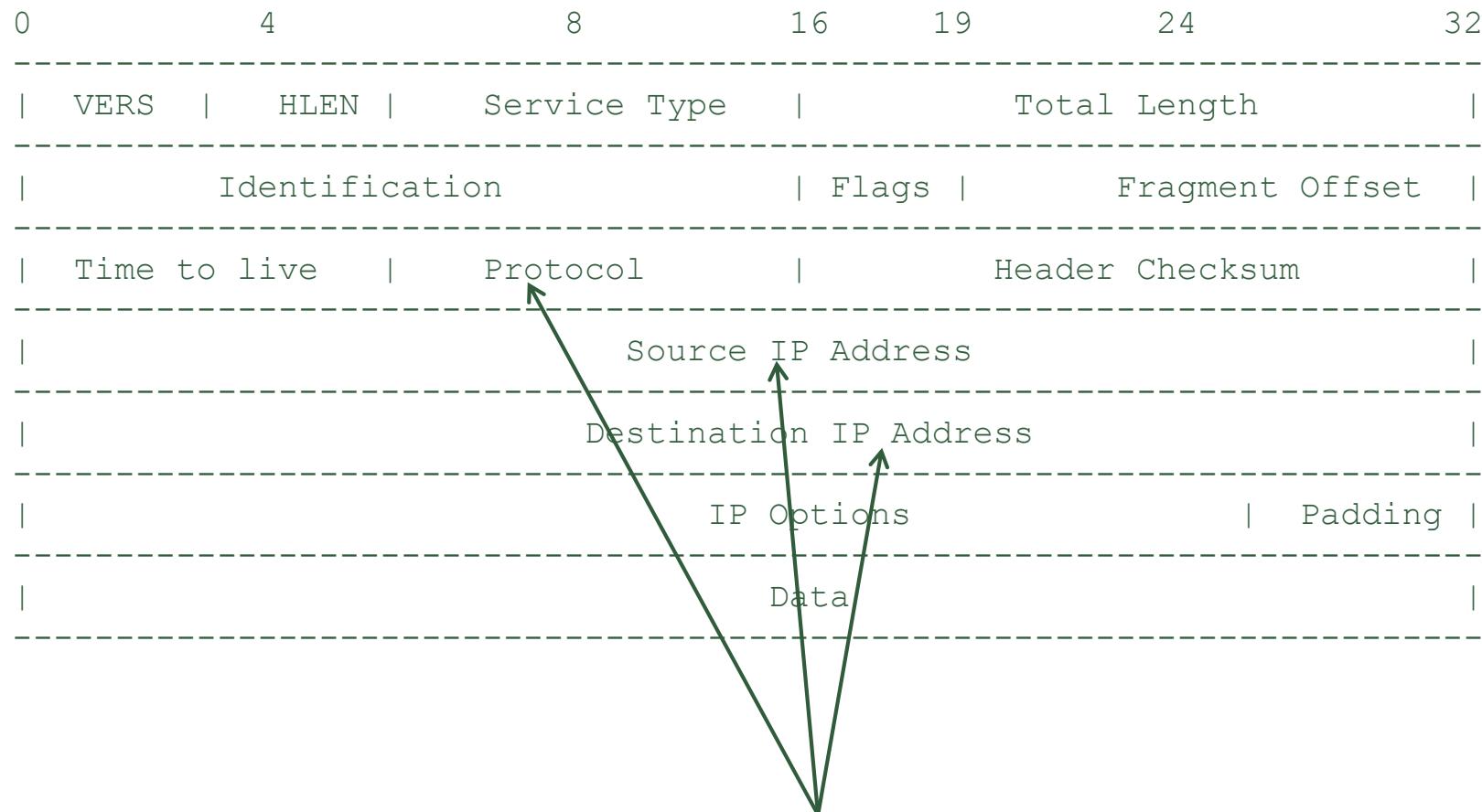
- TCP - Transmission Control Protocol
- IP - Internet Protocol
- UDP - User Datagram Protocol (postcard)
- ICMP - Internet Control Message Protocol
- Many other protocols: IGMP, OSPF etc.





# TCP - Transmission Control Protocol

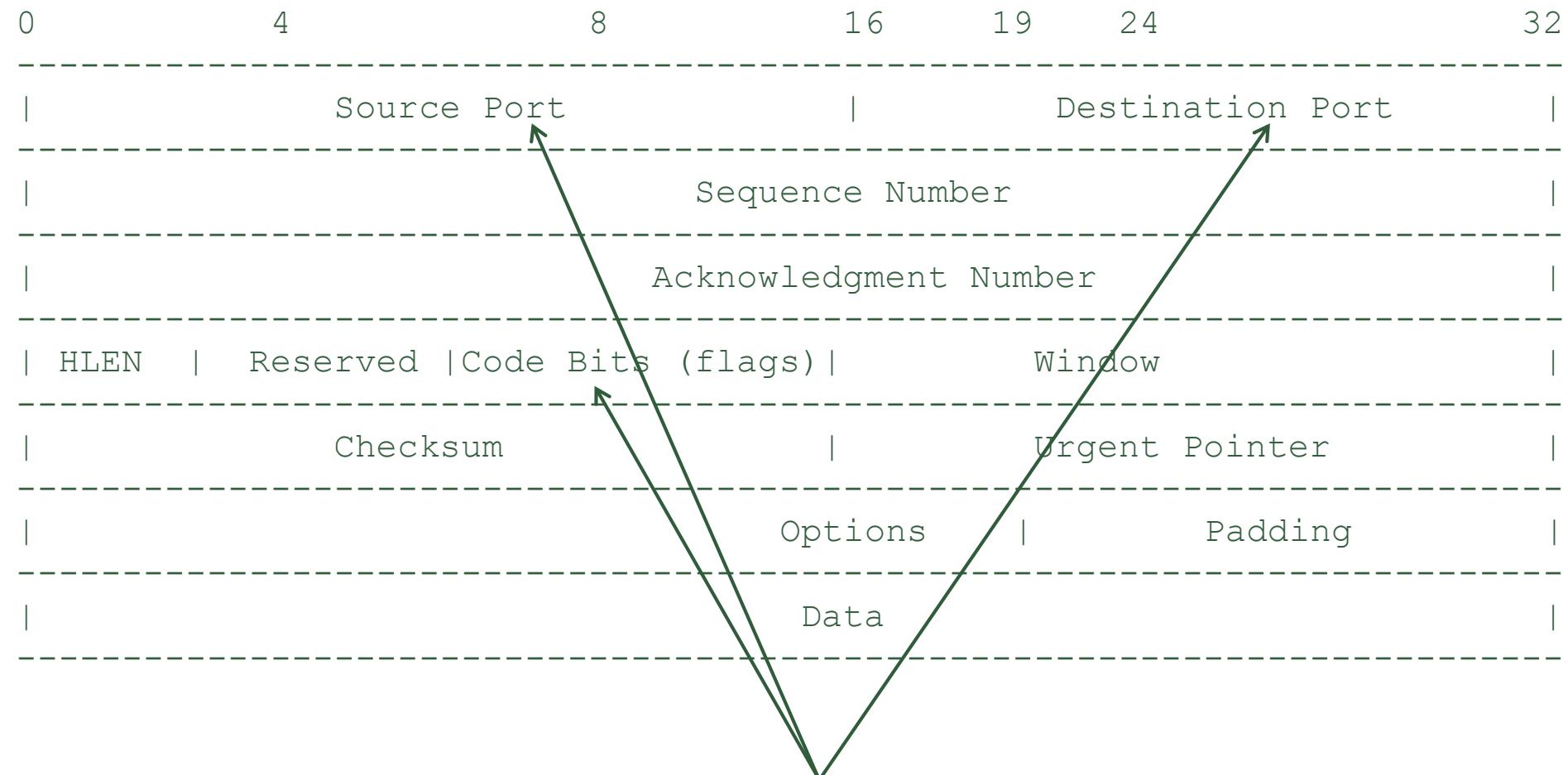
# IP Header



Typiske felter for filtrering



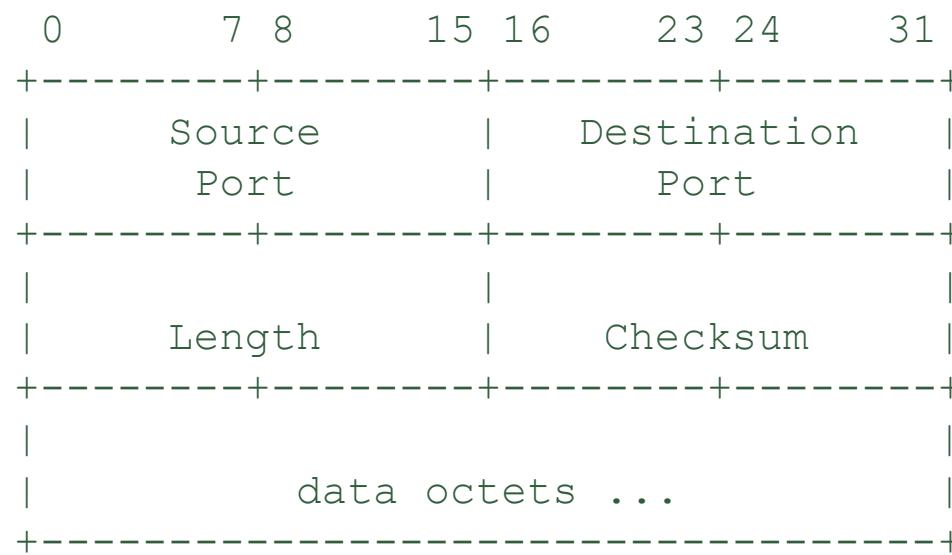
# TCP Header



Typiske felter for filtrering



# UDP header



## Firewall

- Firewall policy
- Firewall rules

### Protocol Source Port Destination Port Action

TCP	194.1.1.1	Any	180.2.2.2	80	Accept
TCP	Any		Any		Deny

Block unwanted traffic, direct incoming traffic to internal nodes,  
Hide vulnerable nodes from external threats, log traffic to and  
from the network



## Firewall rules

<b>Rule #</b>	<b>Source</b>	<b>Destination</b>	<b>Protocol</b>	<b>Destination port</b>	<b>Action</b>
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:  
deny/forbid/disallow/drop/block/refuse



# Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny



# 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



## IPtables

<https://www.frozenthux.net/iptables-tutorial/iptables-tutorial.html#HOWARULEISBUILT>

iptables -F INPUT (*flush*)

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



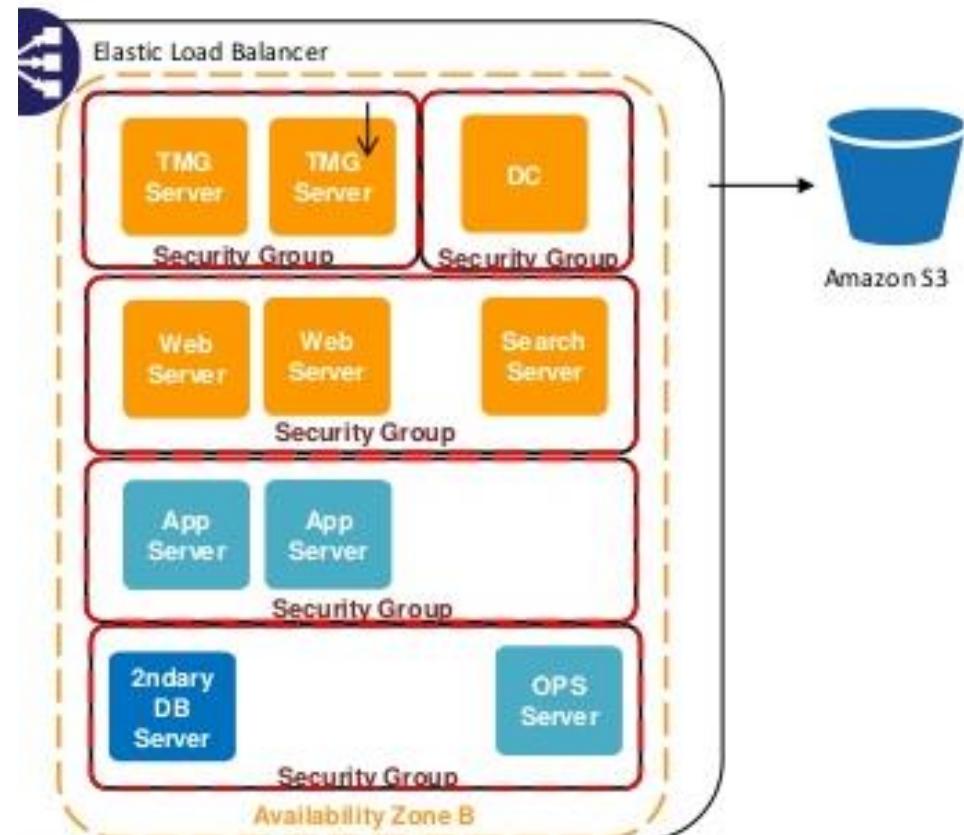


# Firewalls and Security Groups

# Security Groups

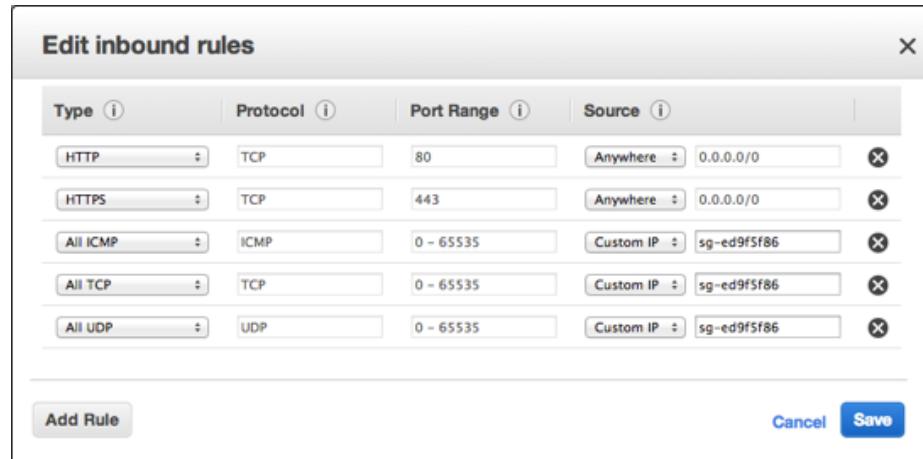
A *Security Group* is like a ‘basic stateless firewall’

A Security Group is a container for security group rules. Works as 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.

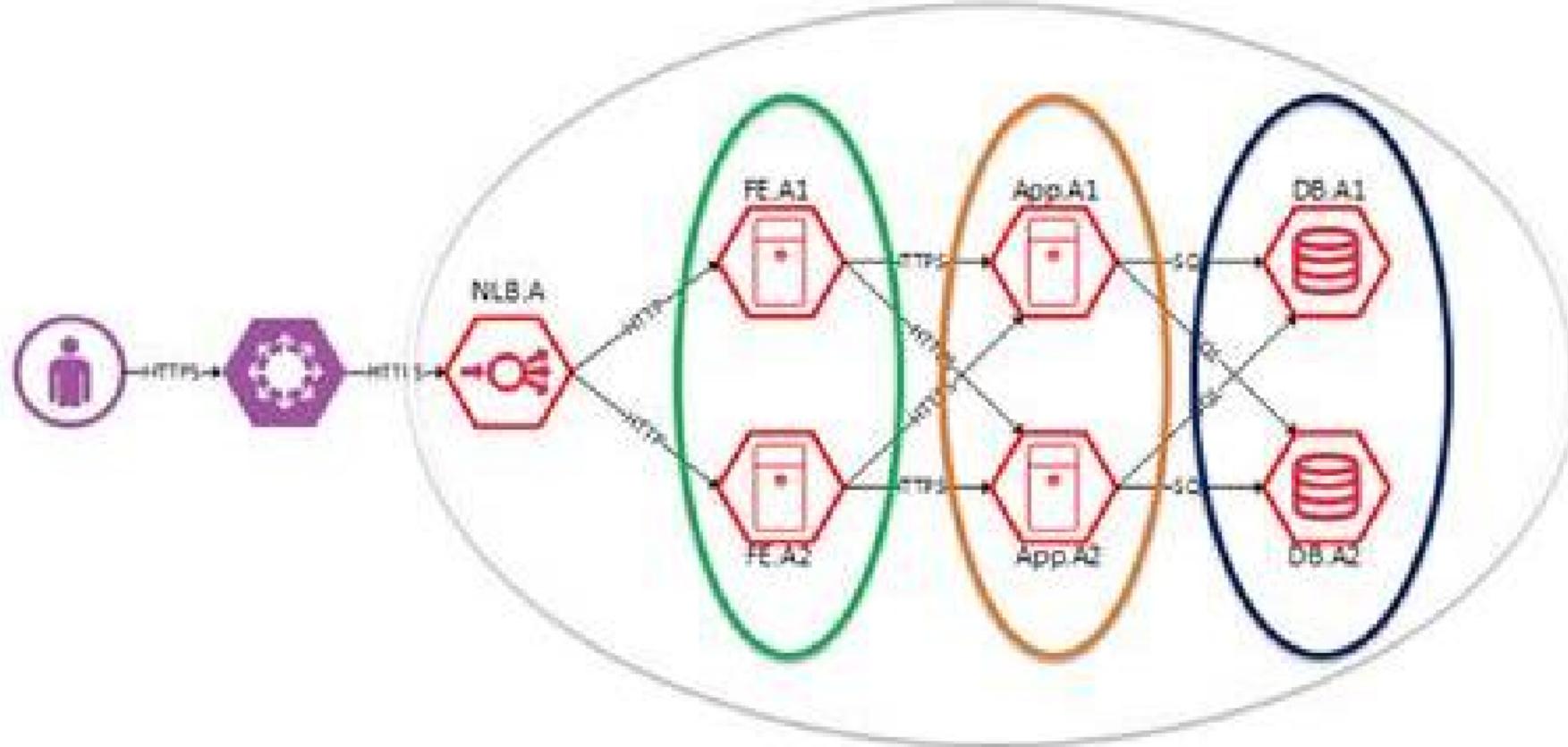
“Small cheap firewalls” in front of every single server/system.

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 Groups

If a solutions has a number of web-, application and database servers each group is placed in a Security Group that only allows communication with layers directly above and below.

Security Groups should not allow any form of internet access outside the webserver group). Administrative access should be limited to known IP-addresses such as jump servers or own internal IP-addresses





# Pause

**SECURITY CHECK**

Is there your card in the hackers database?  
You can easily check here, just enter your card info:

Card number:

CVC@ (CW2):

**Check!**

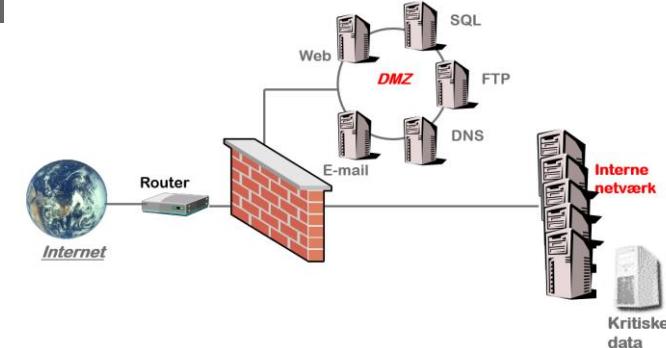
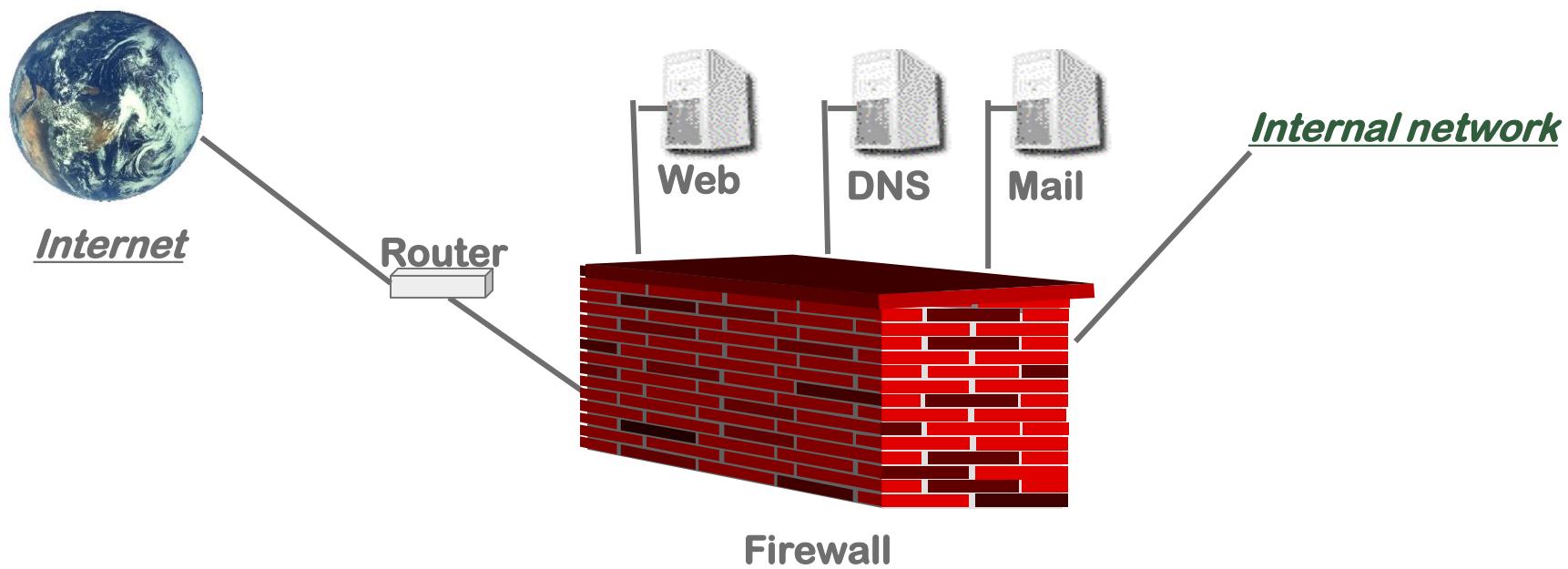


The slide features a large central box containing a security check form. At the top right of this box are the VISA and MasterCard payment method logos. Below the logos, there is a question about checking a card's presence in a hacker's database, followed by fields for entering a card number and CVC code. A prominent 'Check!' button is at the bottom of the form.

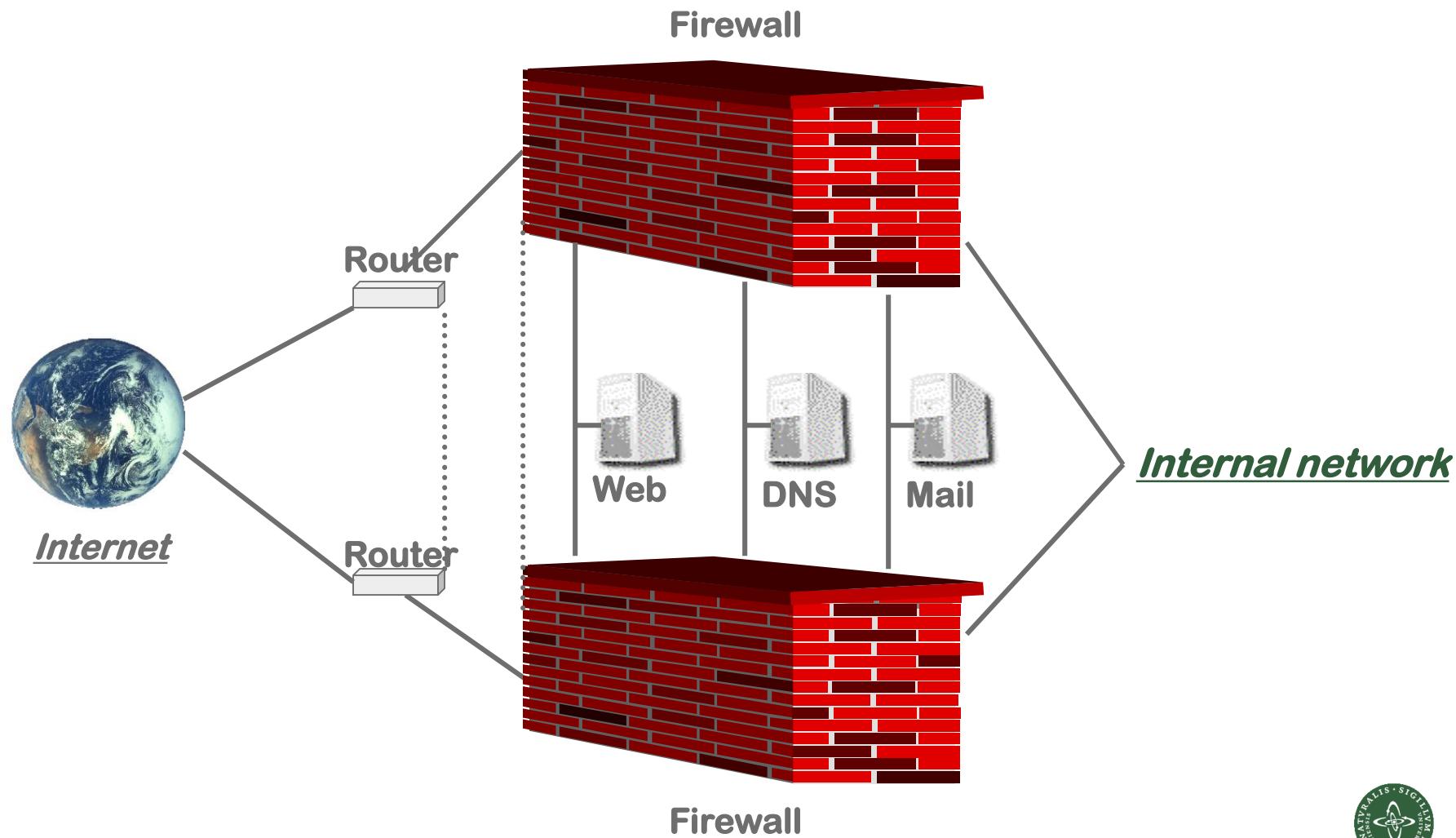


# Classic security measures

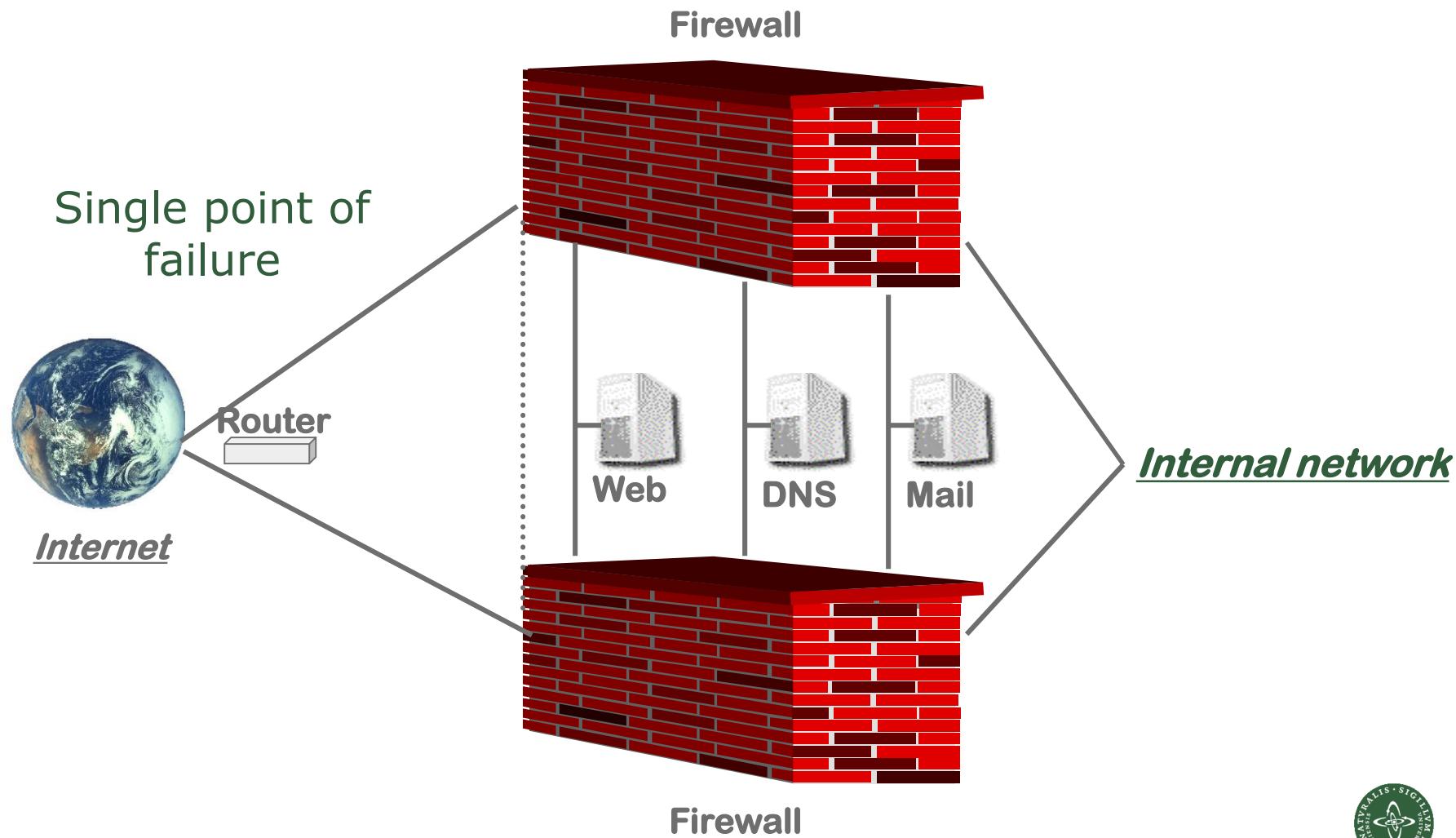
# Multiple DMZ



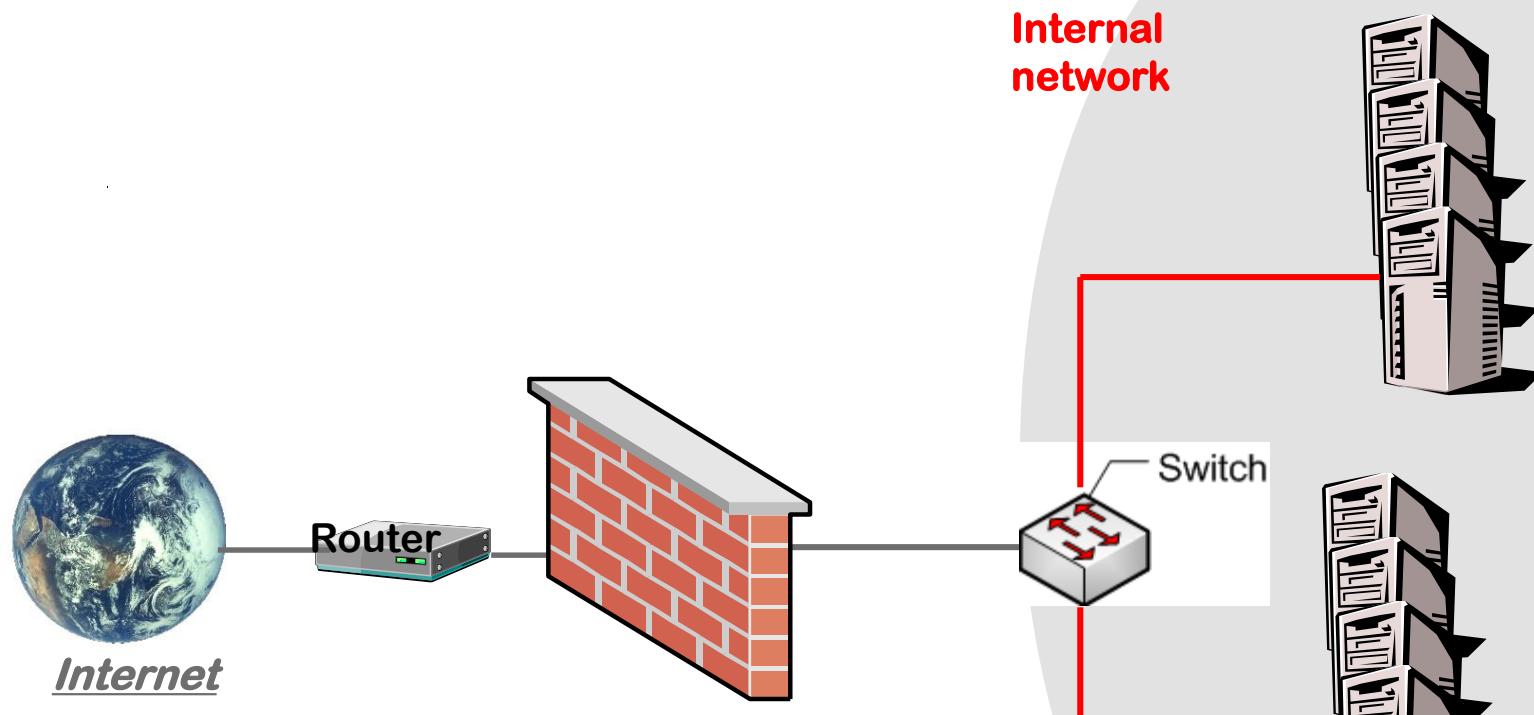
# Multiple firewalls



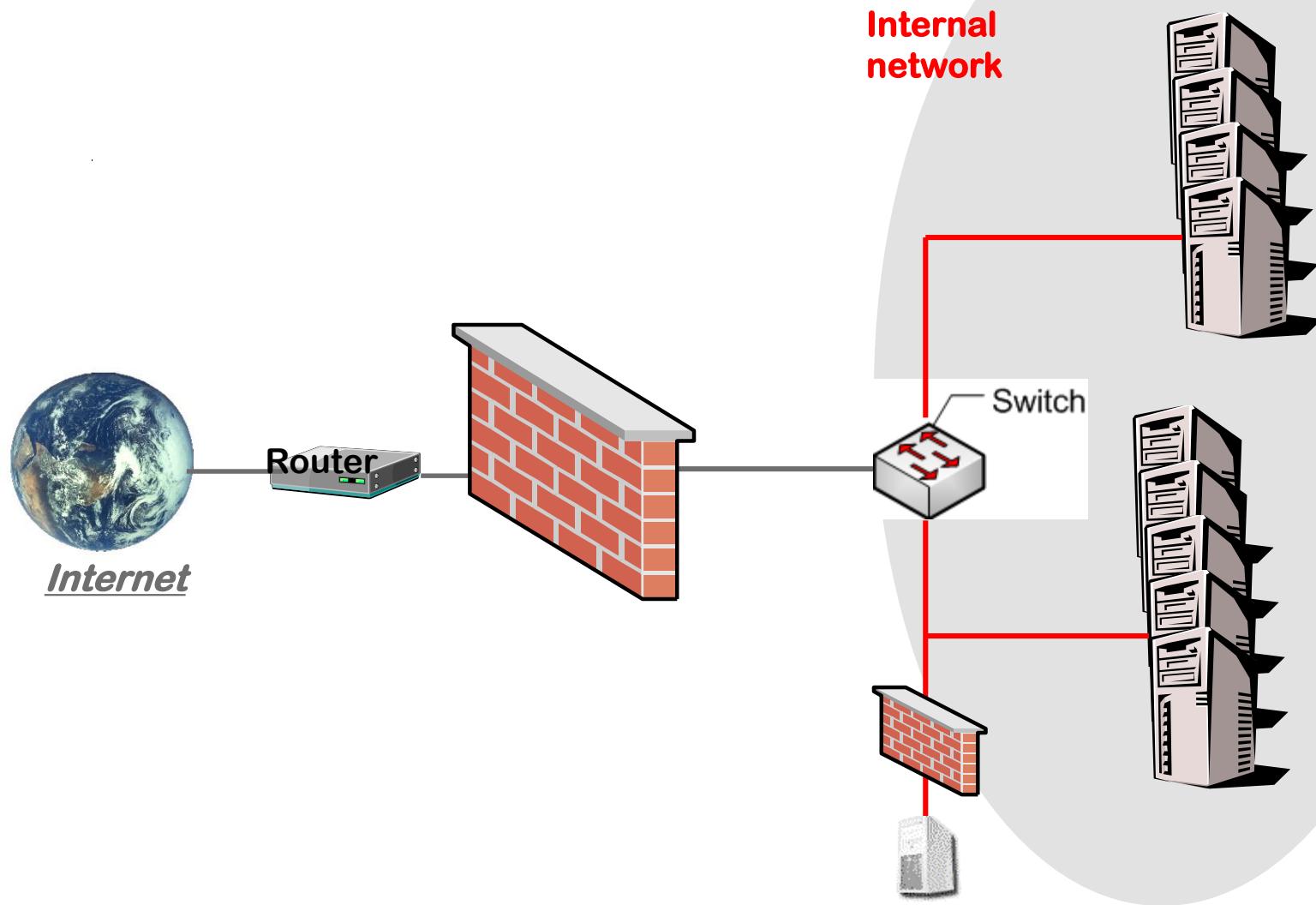
## Multiple firewalls



## Network – vLAN segmenting



## Network – internal firewalls



IDS

# Intrusion Detection Systems (IDS)

# Intrusion Protection Systems (IPS)



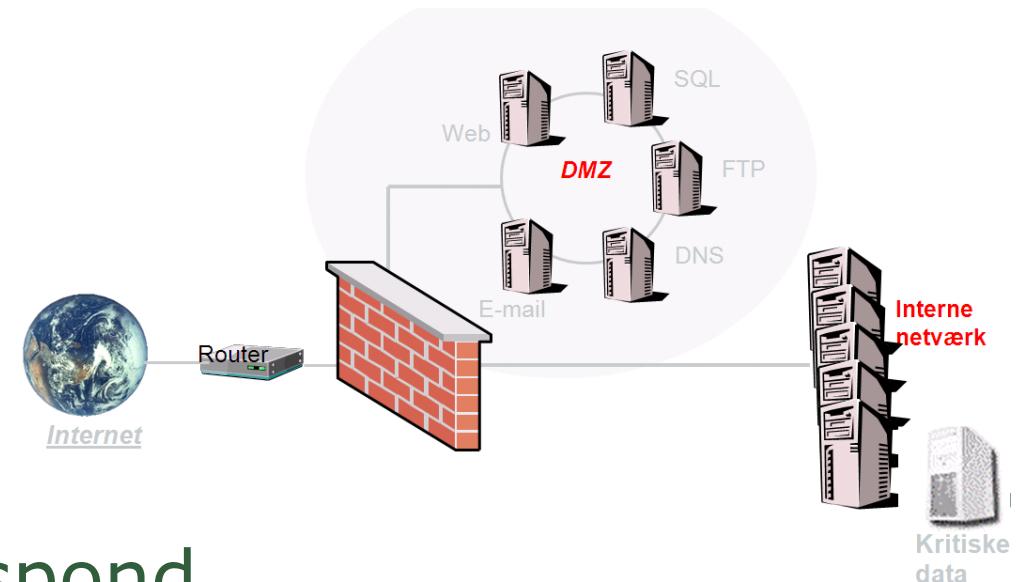
# Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so



## More examples of security measures

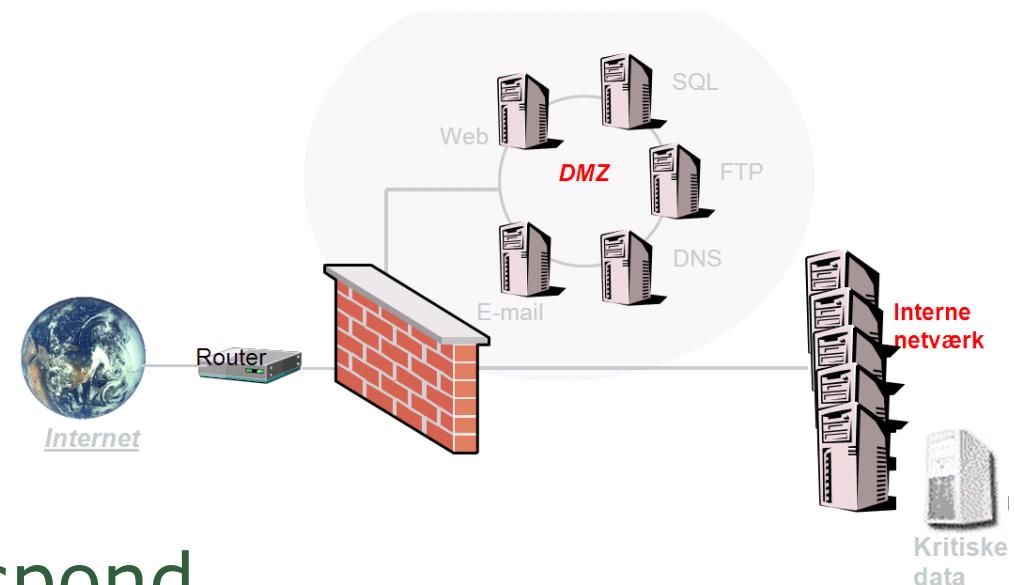
- IDS/IPS
- Scanning for virus and webtraffic
- Central loghost
- Many DMZ's
- VLAN, internal firewalls, segmentation
- DDoS protection
- ...



Prevent – Detect - Respond

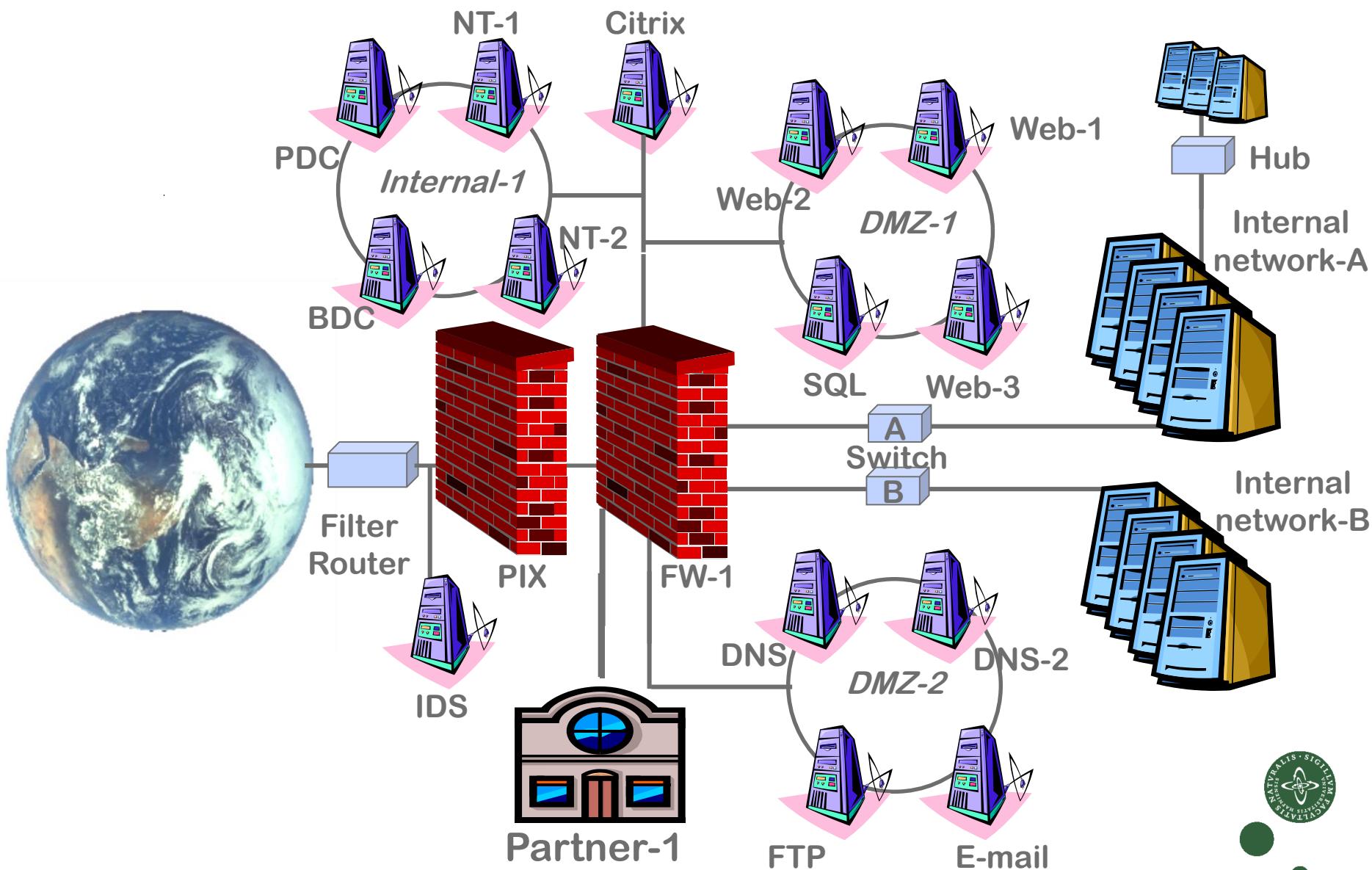
## More examples of security measures

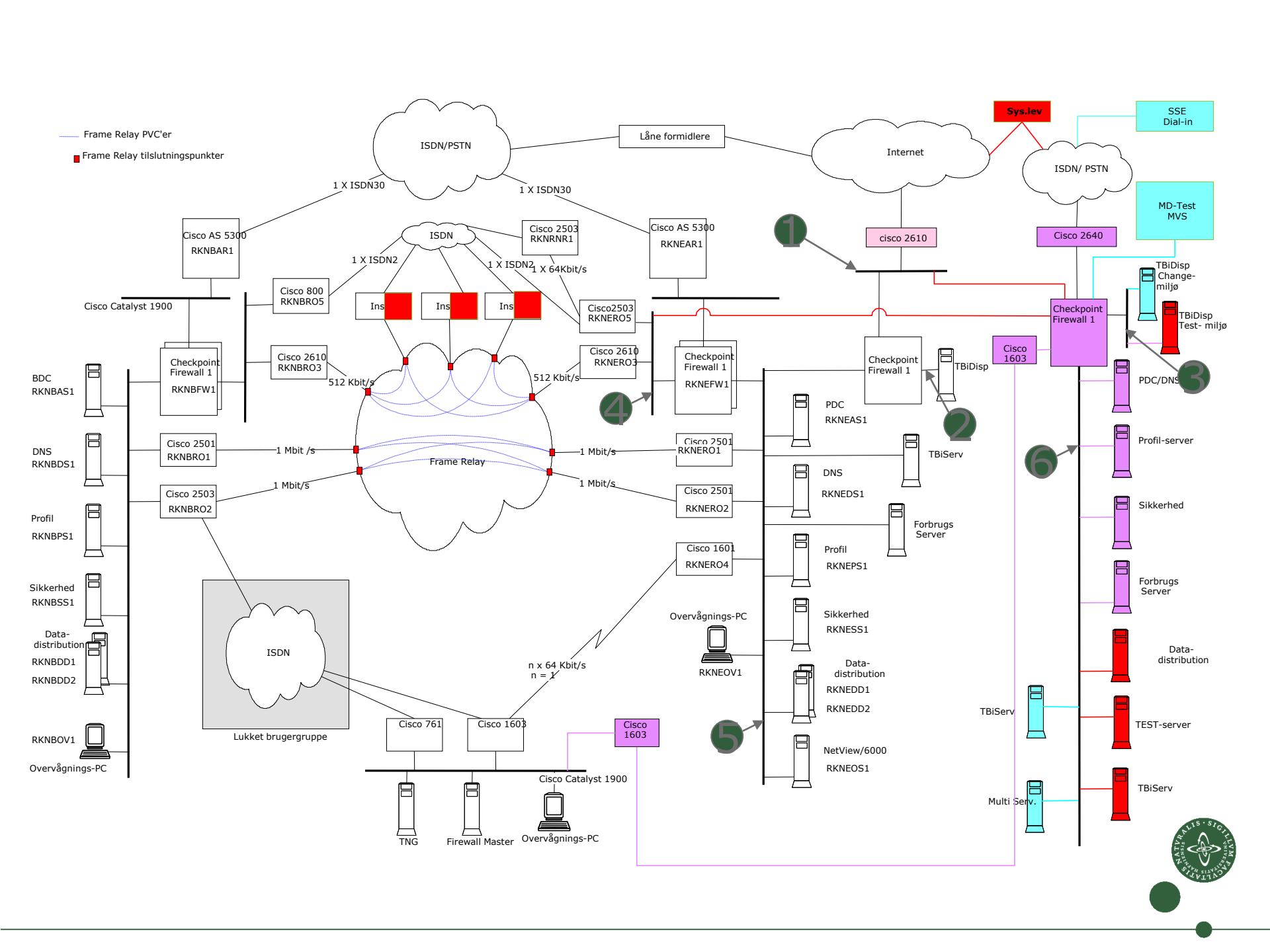
- Patching/updating
- Configuration management
- Filtering outgoing traffic
- Minimizing number of services (hardening)
- Whitelist/blacklist
- ...



Prevent – Detect - Respond

# Large network (example)

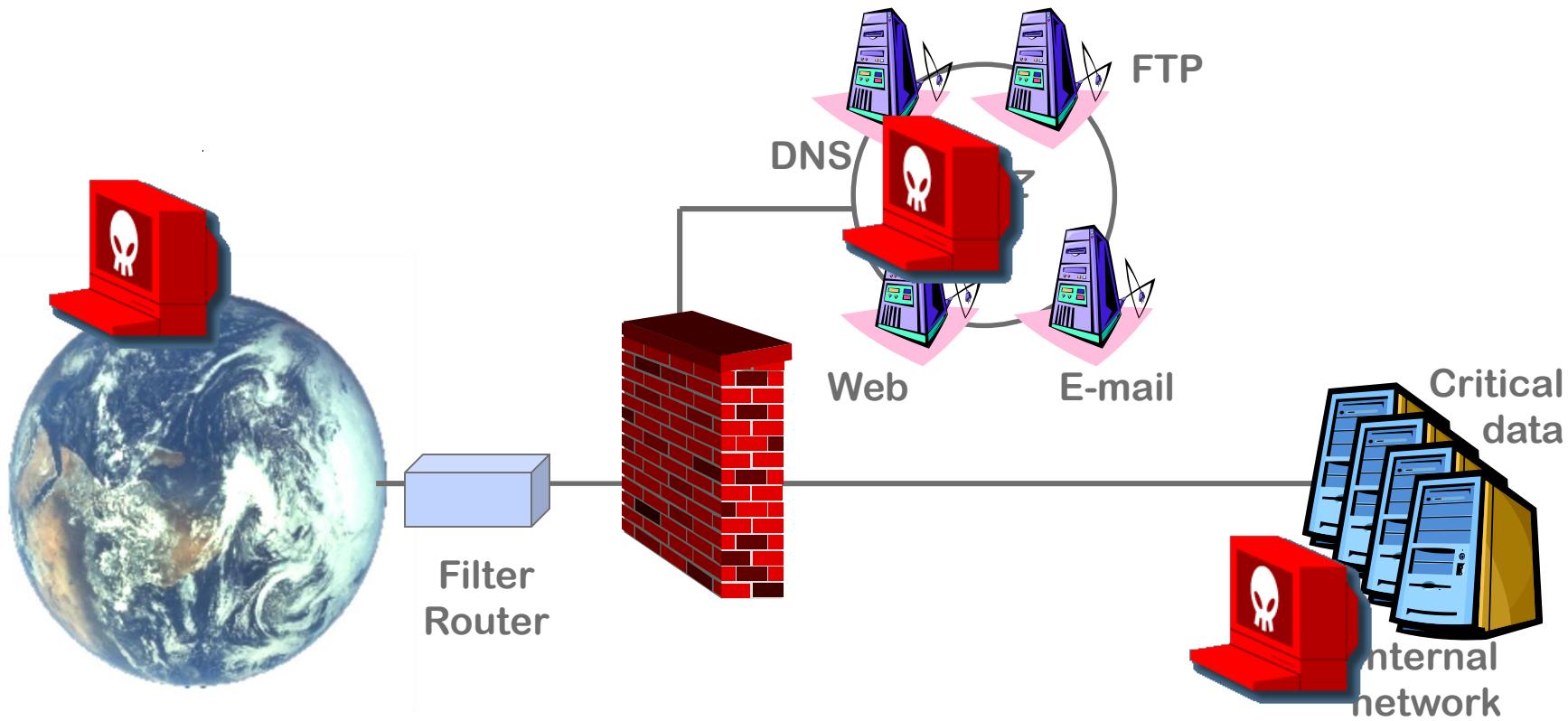




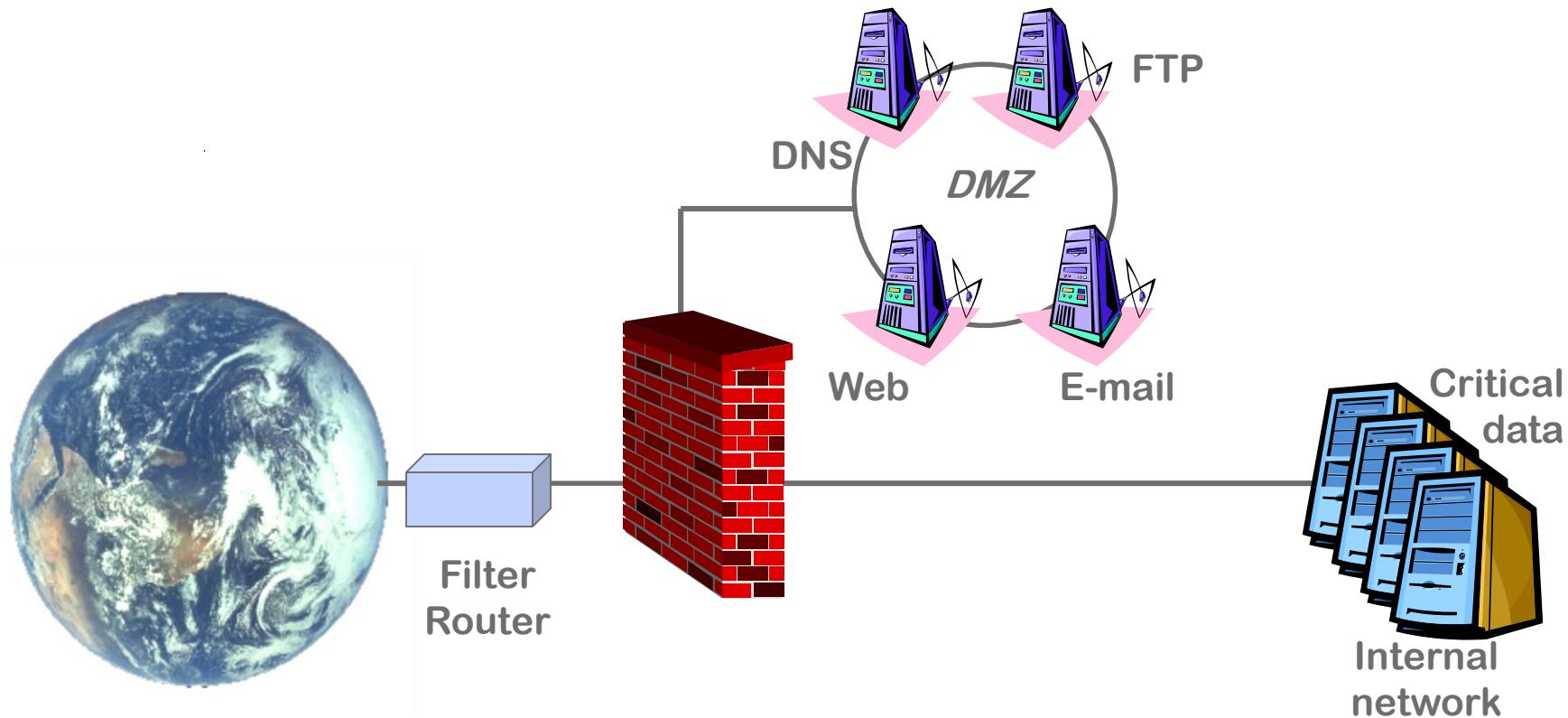


# Common security issues

## 3 major areas of attack



# The network

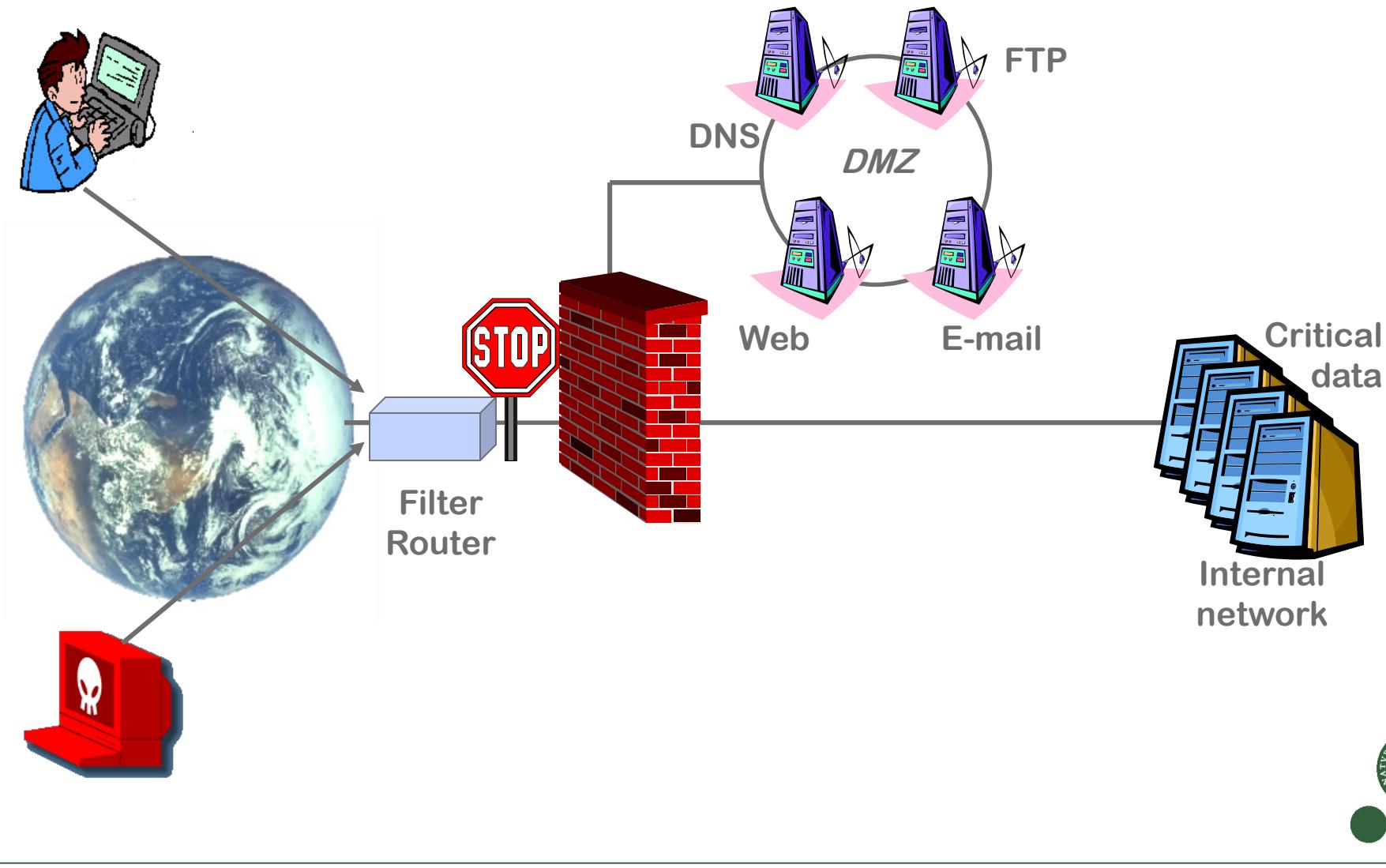


## Typical router problems

- Too many open ports (access or DoS)
- Router default accounts



## Router problems - consequences



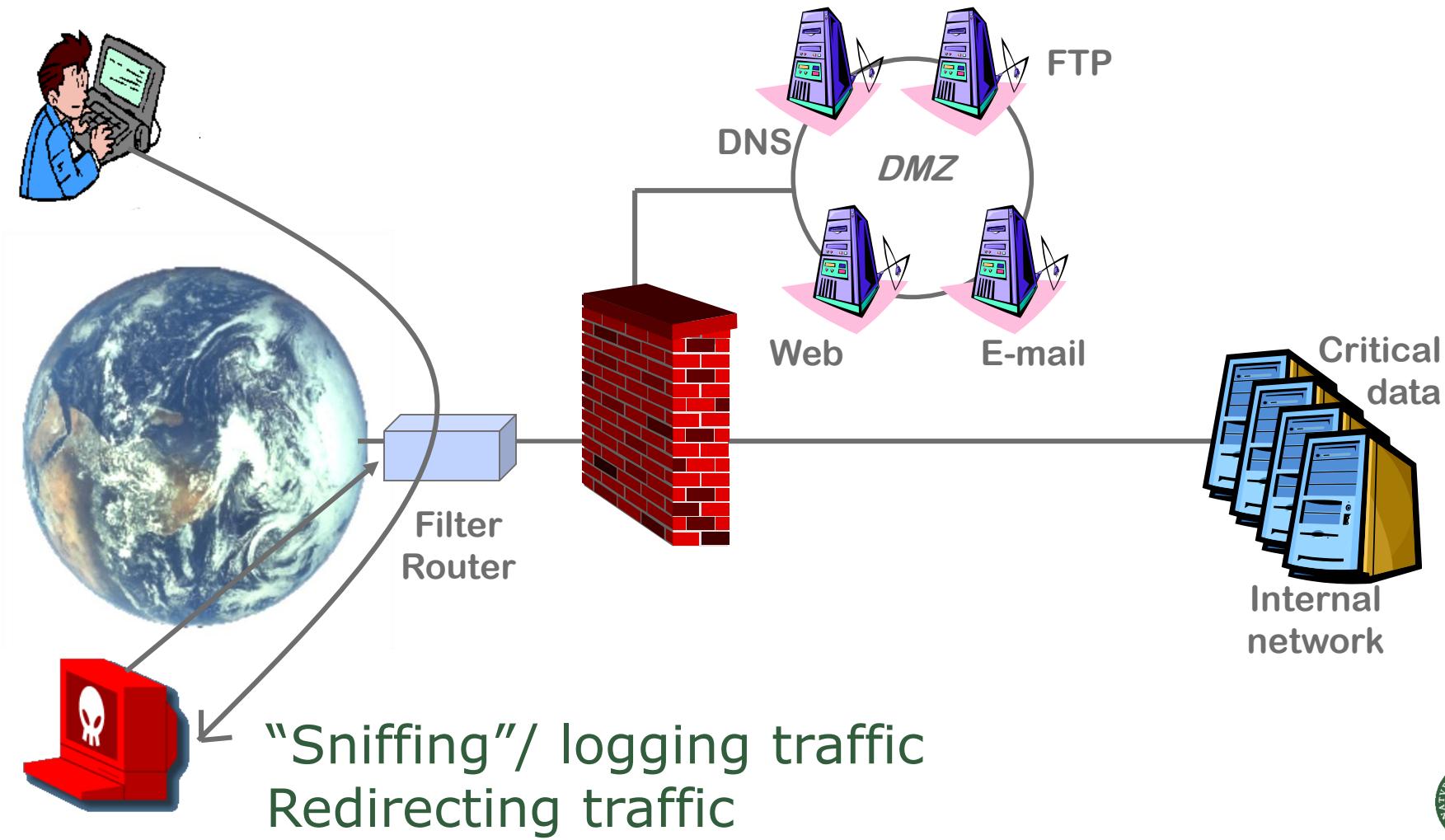
## Router - Case Story: Microsoft

4 primary DNS servers,  
But all behind the same router.

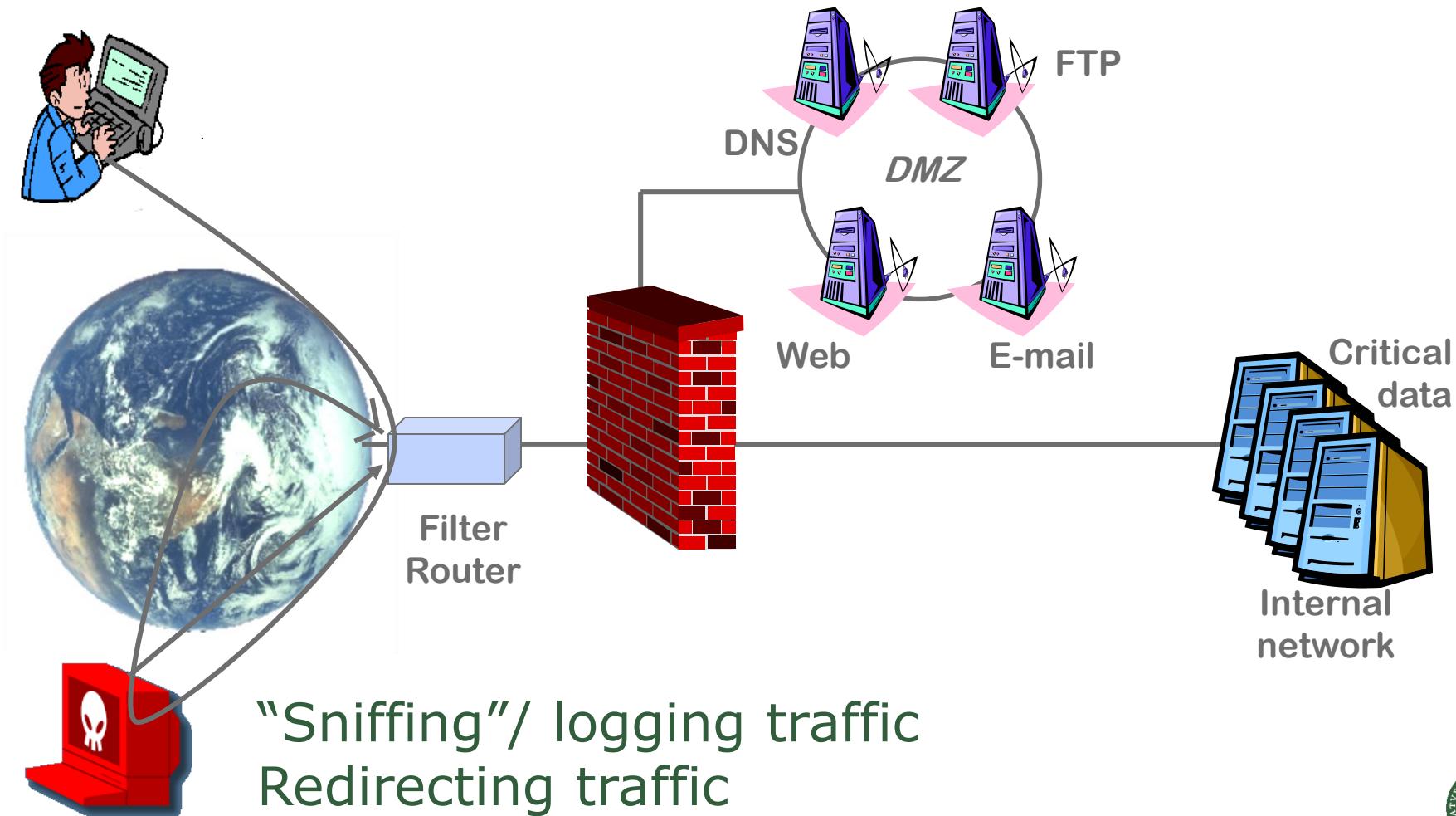
DoS attack against the router meant that all  
Microsoft's DNS-servers were uncapable of resolving  
domain names.



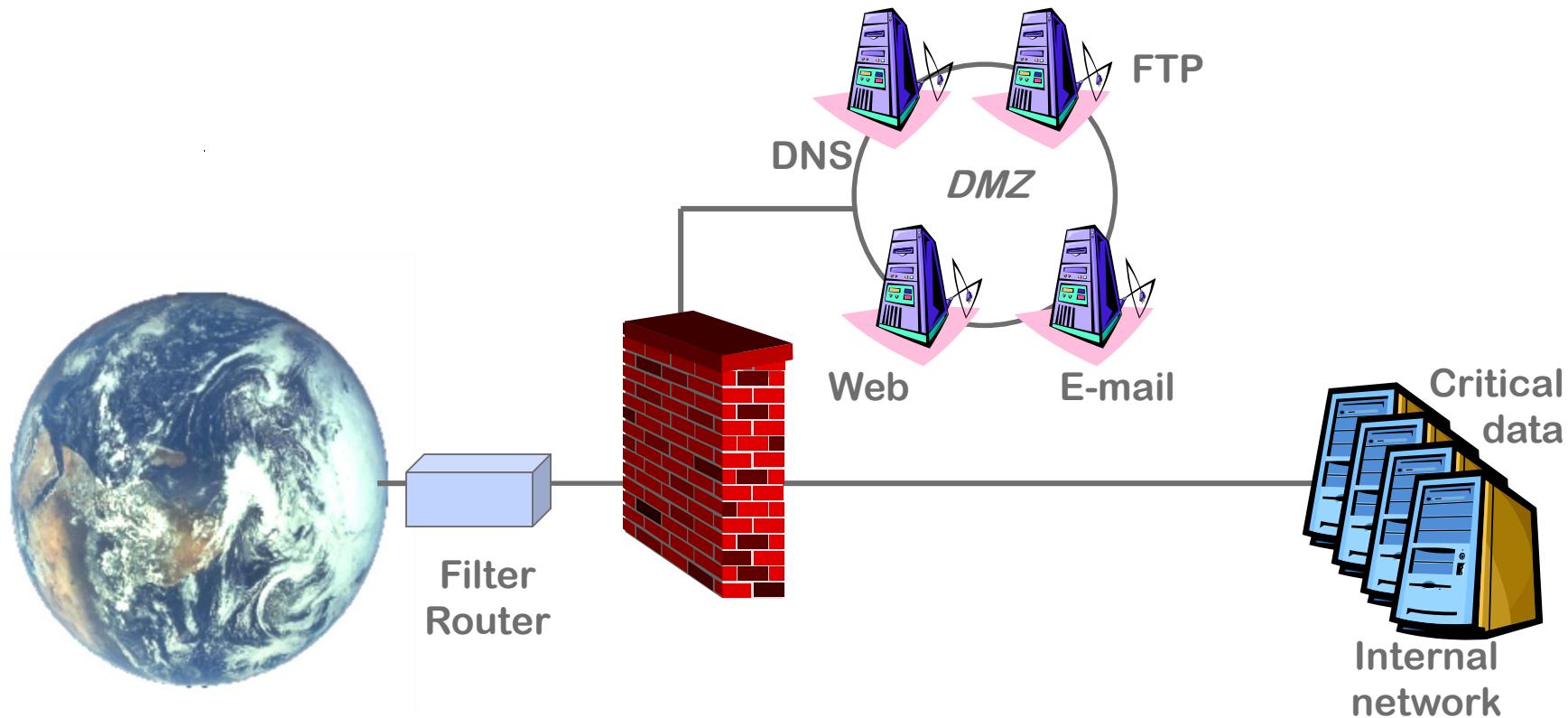
## Router problems – consequences



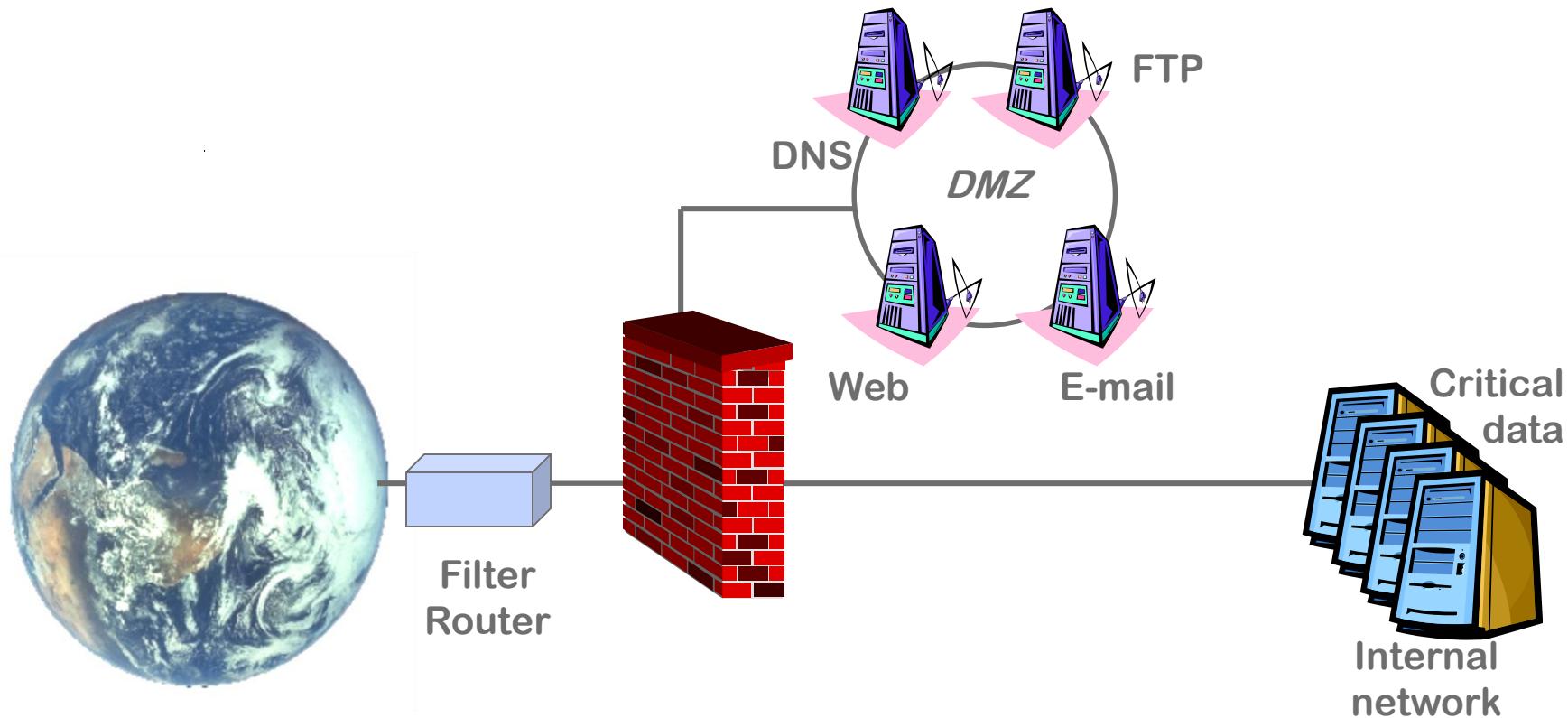
# Router - consequences



# The network



# The network

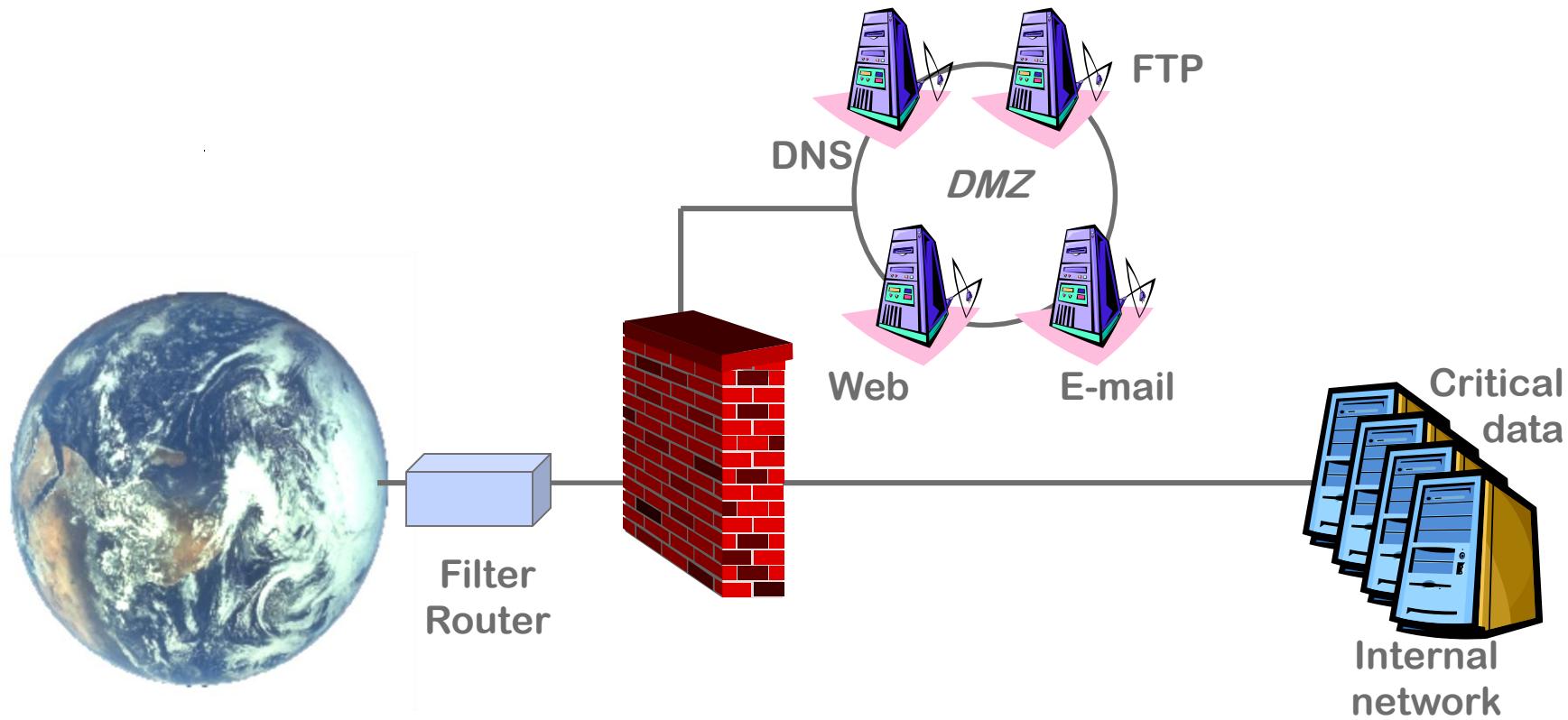


## Typical firewall problems

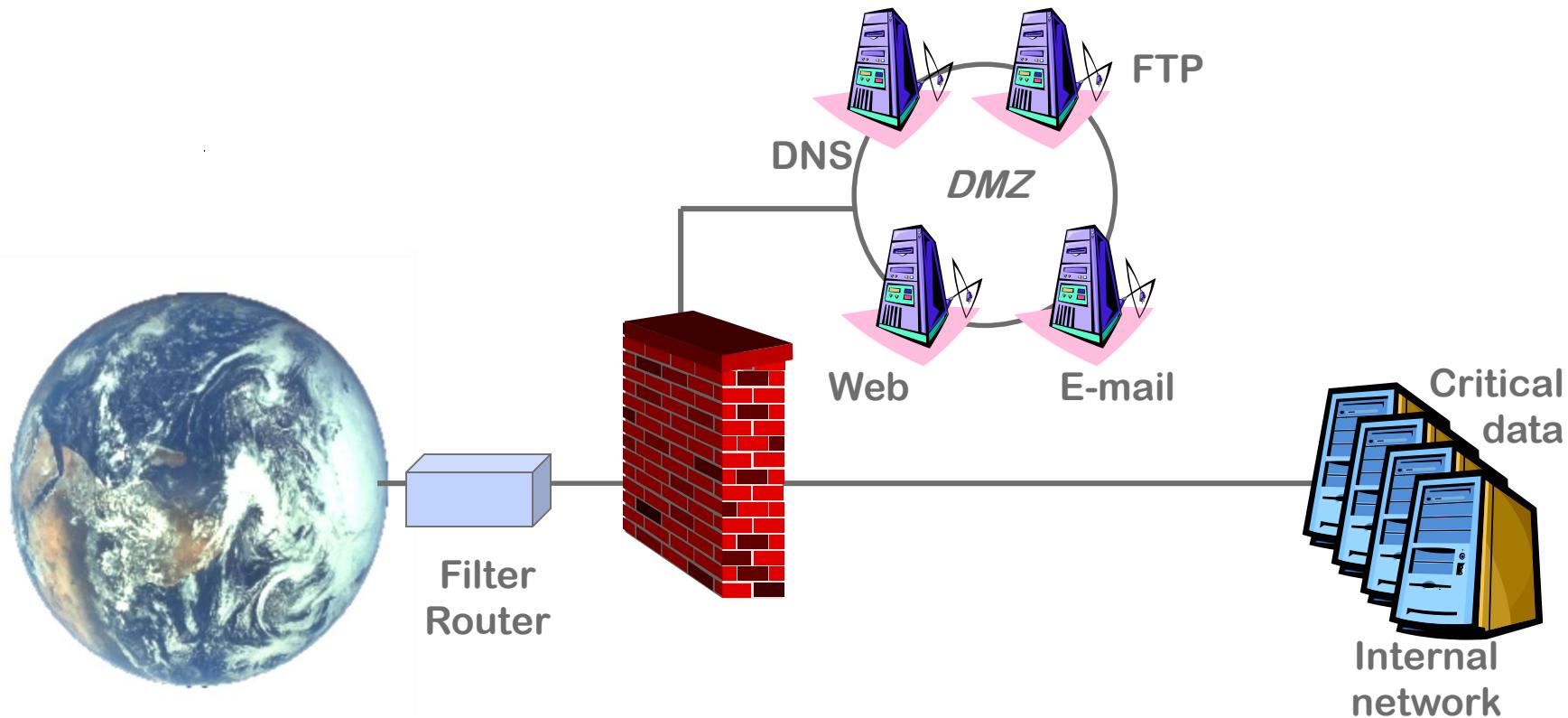
- Mistakes in configuration  
(The FW does not protect as you think)
- Too many open ports (Access or DoS)
- Too many protocols allowed - ping etc.
- Changes in configuration never fixed
- Management services available on FW



## Typical setup



## Typical setup



## Typical DNS issues

DoS

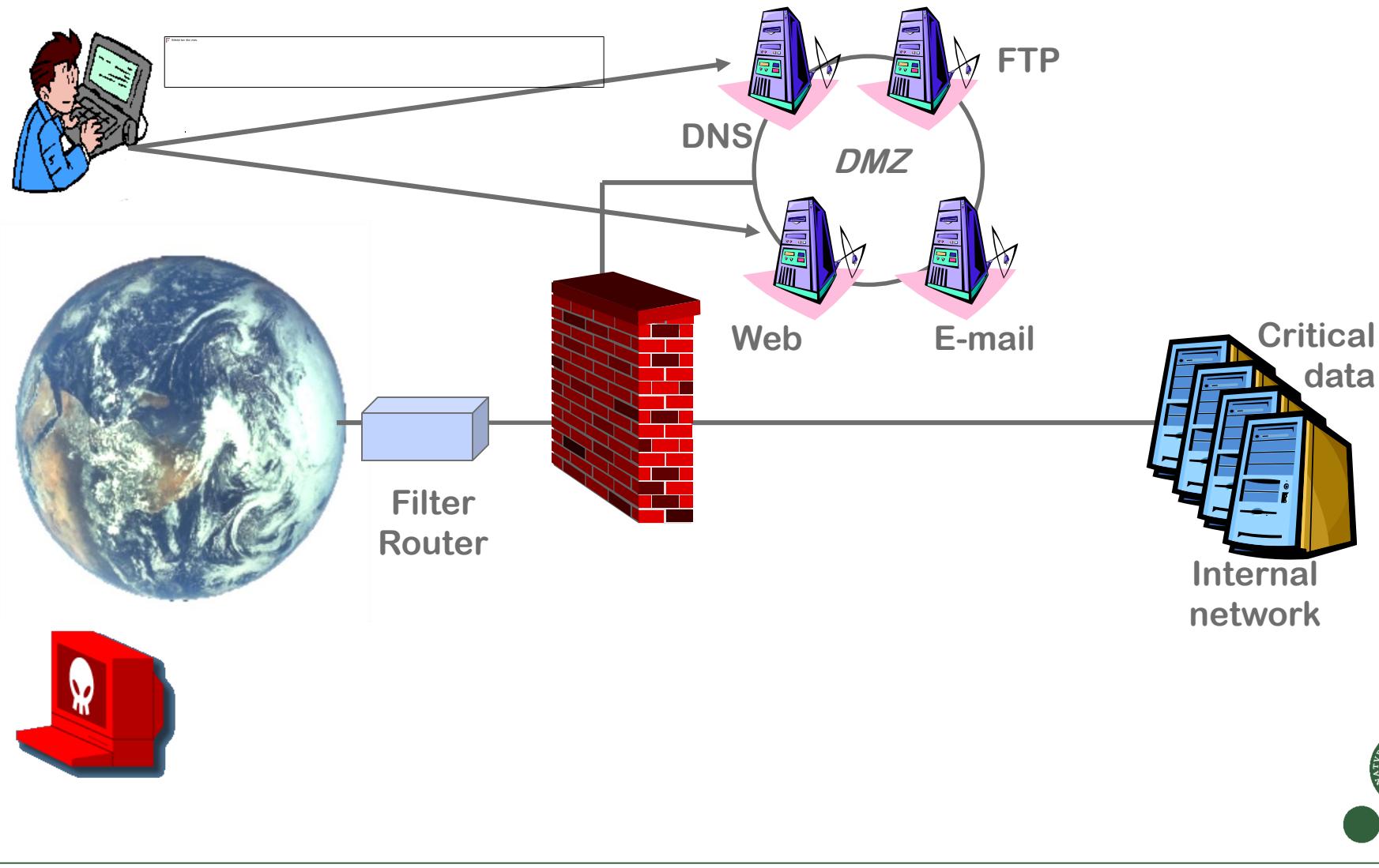
Re-direct traffic to other IP-addresses  
(Hijacking/Man-in-the-Middle)

Execute commands on the server

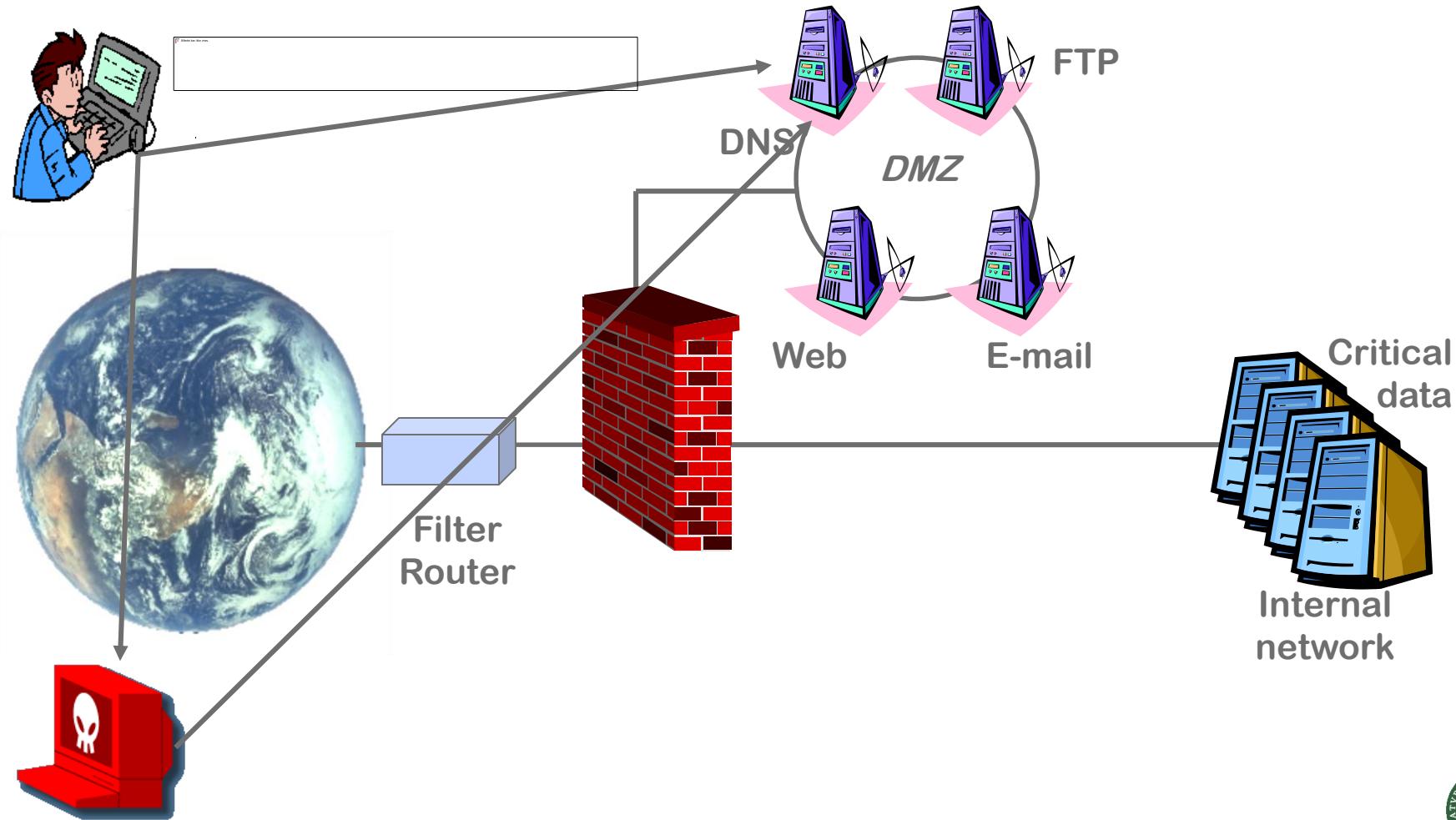
Stepping Stone



## DNS problems - consequences



## DNS problems - consequences



# DNS - Case Story: RSA DNS Hijacking

RSA Security inc. - The most hacked name in E-Business - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security SH

Bookmarks Go to: http://www.rsa.com/ What's Related

**RSA SECURITY**

**RSA Security inc. Hacked.**  
Trust us with your data! Praise Allah!

The most trusted name  
in E-security  
has been owned.

Big things  
are coming.

Copyright © 2000 Coolio

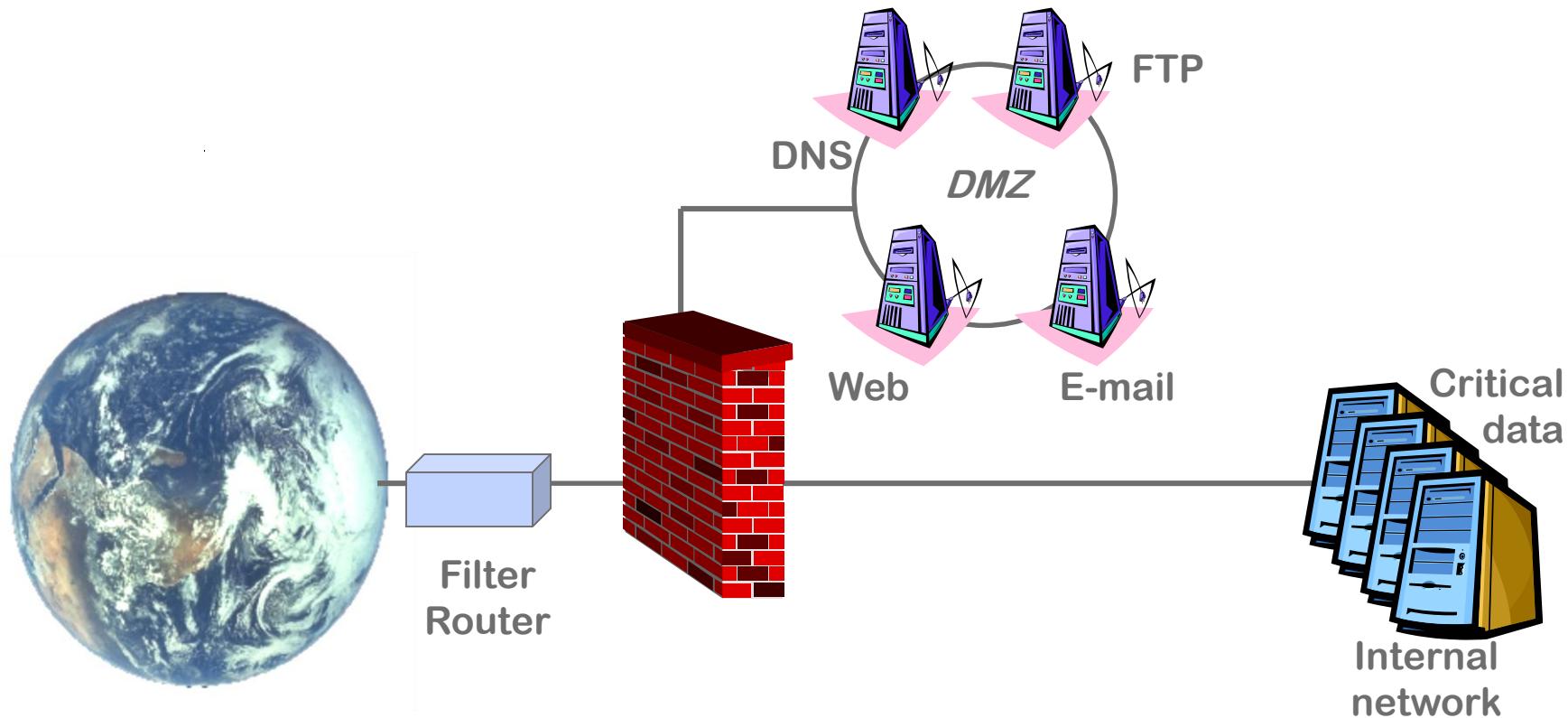
• Hello aforce!  
• Girls are stupid and easy  
• RSA Laboratories Unveils Innovative [countermeasure](#) to  
recent "Denial of Service" Hacker Attacks". Keep your data  
safe with us! Our security is the best.

O  
W  
N  
E  
D  
B  
Y  
C  
O  
O  
L  
I  
O

Document: Done



## 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



# Consequences

Index of /bodywise/Retail\_Web\_store/Admin\_files - Microsoft Internet Explorer provided by Freeserve

File Edit View Favorites Tools Help

Address wise.com/bodywise/Retail\_Web\_store/Admin\_files/ Go Links CYRANO Share Price AltaVista - Search

## Index of /bodywise/Retail\_Web\_store/Admin\_files

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	07-Aug-98 15:26	-	
<a href="#">vti_cnf/</a>	07-Aug-98 07:22	-	
<a href="#">access.log</a>	05-Jul-99 15:41	338k	
<a href="#">counter.file</a>	05-Jul-99 15:43	1k	
<a href="#">error.log</a>	13-Dec-98 10:38	3k	
<a href="#">order.log</a>	05-Jul-99 15:46	15k	



# Consequences

http://vitawise.com/bodywise/Retail\_Web\_store/Admin\_files/order.log - Microsoft Internet Explorer provided by Freeserve

File Edit View Favorites Tools Help

Address /bodywise/Retail\_Web\_store/Admin\_files/order.log Go Links CYRANO Share Price AltaVista - Search BBC WebMail Yahoo! Weather Yell

US Name = michael goodman Billing Address Street = 45 tall tree road Billing Address City = middletown Billing Address State = nj Billing Address Zip = 07748  
 Billing Address Country = usa Mailing Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 732-671-9476 Fax Number = Email = go2goodman@home.com URL = Link = Type of Card = mastercard Name Appearing on Card = MICHAEL GOODMAN Card Number = 5417122662504289 Card Expiration = 11/99 Shipping Method = -----  
 ----- Description = Reshape Formula 90 Count (Each) Wholesale Options = Monthly Price After Options = 39.60 US Quantity = 1 Subtotal For Item = 39.60 US Description = Right Choice AM/PM Pair 270 Count Wholesale Options = Monthly Price After Options = 99.75 US Quantity = 1 Subtotal For Item = 99.75 US Description = Electro Aloe 27 OZ (Case of 6) Wholesale Options = nothing entered Options = Price After Options = 90.00 US Quantity = 1 Subtotal For Item = 90.00 US Description = Glucominine 90 Count (Case of 4) Wholesale Options = nothing entered Options = Price After Options = 195.80 US Quantity = 1 Subtotal For Item = 195.80 US Description = St.John's Complex 90 Count (Each) Wholesale Options = nothing entered Options = Price After Options = 29.50 US Quantity = 1 Subtotal For Item = 29.50 US Description = Future Perfect Case of 6/Dutch Chocolate Wholesale Options = nothing entered Options = Price After Options = 117.00 US Quantity = 1 Subtotal For Item = 117.00 US Description = Beta-C 240 Count (Each) Wholesale Options = Monthly Price After Options = 44.00 US Quantity = 1 Subtotal For Item = 44.00 US Subtotal: = 615.65 US Grand Total: = 615.65 US Name = Jan Barlow Billing Address Street = 1969 Chatham Dr. Billing Address City = Wheaton Billing Address State = IL Billing Address Zip = 60187 Billing Address Country = USA Mailing Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 630-665-9131 Fax Number = Email = jlbatnet @AOL.com URL = Link = Type of Card = visa Name Appearing on Card = Janet L. Barlow Card Number = 4806-8200-1117-9818 Card Expiration = 10/00 Shipping Method = ----- Description = Right Choice AM/PM Pair Options = nothing entered Options = Price After Options = 48.00 US Quantity = 1 Subtotal For Item = 48.00 US Subtotal: = 48.00 US Grand Total: = 48.00 US Name = Ms. Glenda Brookens Billing Address Street = 2733 Teresa Dr. Billing Address City = Jackson Billing Address State = MMS Billing Address Zip = 39212 Billing Address Country = Mailing Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 601-371-1739 Fax Number = Email = hhp777@aol.com URL = Link = Type of Card = visa Name Appearing on Card = Card Number = 4128 0038 3578 4086 Card Expiration = 05/99 Shipping Method = ----- Subtotal: = US Grand Total: = 0.00 US Name = Robert Archer Billing Address Street = 2250 Hutchison Billing Address City = Vista Billing Address State = CA Billing Address Zip = 92084 Billing Address Country = usa Mailing Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 760 941-4883 Fax Number = Email = rarcher@mailhost2.csusm.edu URL = Link = Type of Card = visa Name Appearing on Card = Robert H. Archer Card Number = 4128003168471152 Card Expiration = 4/99 Shipping Method = ----- Description = Right Choice AM/PM Pair 270 Count Options = nothing entered Options = Price After Options = 124.50 US Quantity = 01 Subtotal For Item = 124.50 US Subtotal: = 124.50 US Grand Total: = 124.50 US Name = Robert Archer Billing Address Street = 2250 Hutchison St. Billing Address City = Vista Billing Address State = CA Billing Address Zip = 92084 Billing Address Country = usa Mailing Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 760 941-4883 Fax Number = Email = rarcher@mailhost2.csusm.edu URL = Link = Type of Card = visa Name Appearing on Card = Robert H. Archer Card Number = 4128003168471152 Card Expiration = 4/99 Shipping Method = ----- Description = Reshape Formula 90 Count

Done Internet



# Warez server - 4.5GB data

```
unicode.txt - Notepad
File Edit Search Help

Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~

08-03-01 15:04      <DIR>          .
08-03-01 15:04      <DIR>          ..
11-04-01 16:13      <DIR>          ~
               3 File(s)        0 bytes

Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~

11-04-01 16:13      <DIR>          .
11-04-01 16:13      <DIR>          ..
08-03-01 20:37      <DIR>          ---- Anime ----
08-03-01 20:05      <DIR>          ---- Appz ----
10-03-01 19:59      <DIR>          ---- Hentai ----
25-03-01 15:52      <DIR>          ---- Mp3 ----
13-04-01 21:15      <DIR>          ---- old games ----
11-04-01 16:14          1.000.000 1.mb
               8 File(s)        1.000.000 bytes

Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~\---- Anime
----

08-03-01 20:37      <DIR>          .
08-03-01 20:37      <DIR>          ..
09-03-01 04:36      <DIR>          Escaflowne - The Movie
```



# Warez server

```
unicode.txt - Notepad
File Edit Search Help

Directory of d:\Inetpub\wwwroot\vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~\---- Hentai
-----
10-03-01 19:59      <DIR>      .
10-03-01 19:59      <DIR>      ..
09-03-01 14:11      <DIR>      akuma-she
09-03-01 14:53      <DIR>      bondage_fairies
09-03-01 14:56      <DIR>      disney enzow
09-03-01 15:37      <DIR>      Etsuko
10-03-01 19:02      <DIR>      fairie
10-03-01 18:51      <DIR>      hiroshi
10-03-01 18:36      <DIR>      Hot tails
10-03-01 18:13      <DIR>      igratx
10-03-01 18:09      <DIR>      satanika
09-03-01 01:36      <DIR>      secretplot
09-03-01 01:18      <DIR>      Shiwasu
09-03-01 00:40      <DIR>      sk
09-03-01 00:29      <DIR>      sp
09-03-01 00:03      <DIR>      supercock
09-03-01 00:03      <DIR>      venus
09-03-01 00:00      <DIR>      wondfeel
                           18 File(s)          0 bytes

Directory of d:\Inetpub\wwwroot\vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~\---- Hentai
```



# Security architecture

- Så få "angrebssteder" som muligt (minimize attack surface)
- Vær opmærksom på at stederne findes
- Forså angriberne, gør det svært for dem
- Segmenter og adskil
- Defence in depth – mange lag af sikkerhed
- Jump servers
- Overvåg og log, IDS
- Håndtering af sikkerhedsbrud
- Test sikkerheden



# Security architecture

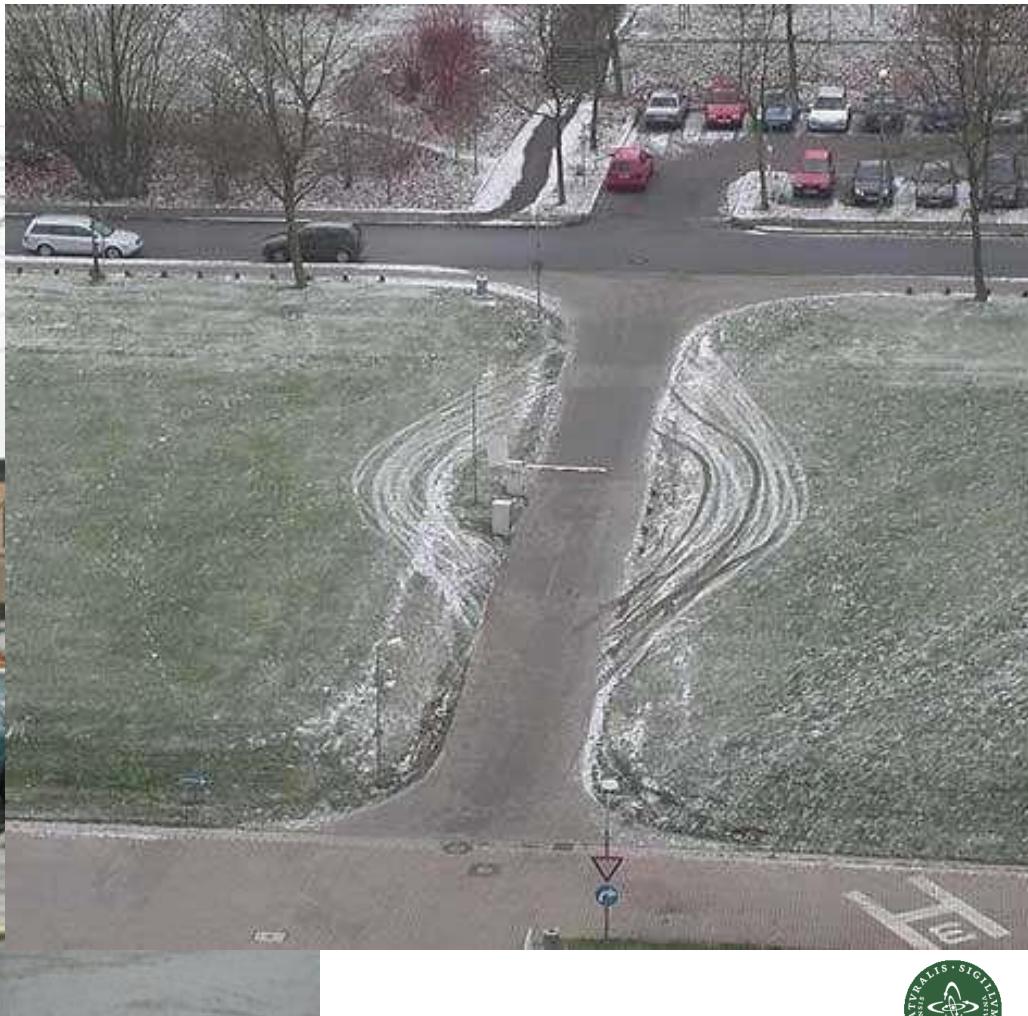
- Hærdning
- Fjern alle unødvendige tools og services etc.
- Patchning
- Konfigurering
- Lavest og færrest mulige rettigheder
- User awareness



## IT Security – start from the outside and zoom in

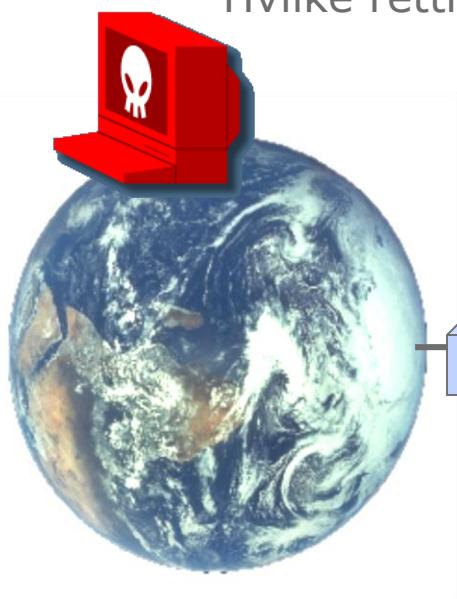


[failblog.org](http://failblog.org)



## 3 areas of attack

Hvem har adgang,  
Hvilke rettigheder?



Filter  
Router

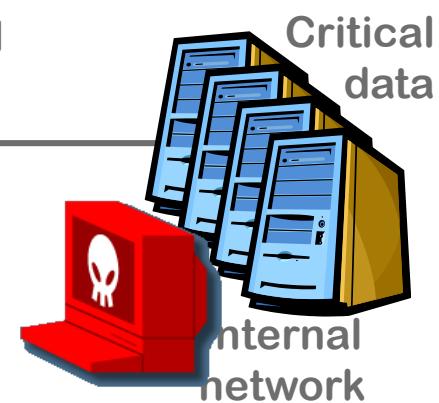


Web

E-mail

FTP

Små fejl kan have  
store konsekvenser



Brugere eller  
admins ?



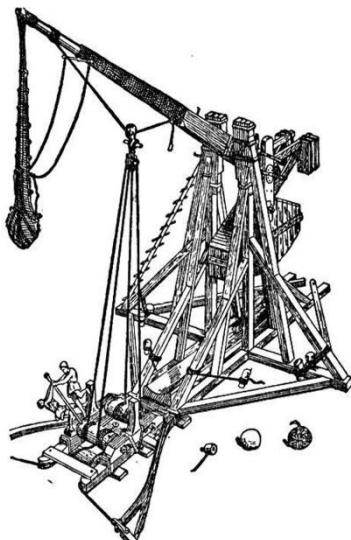
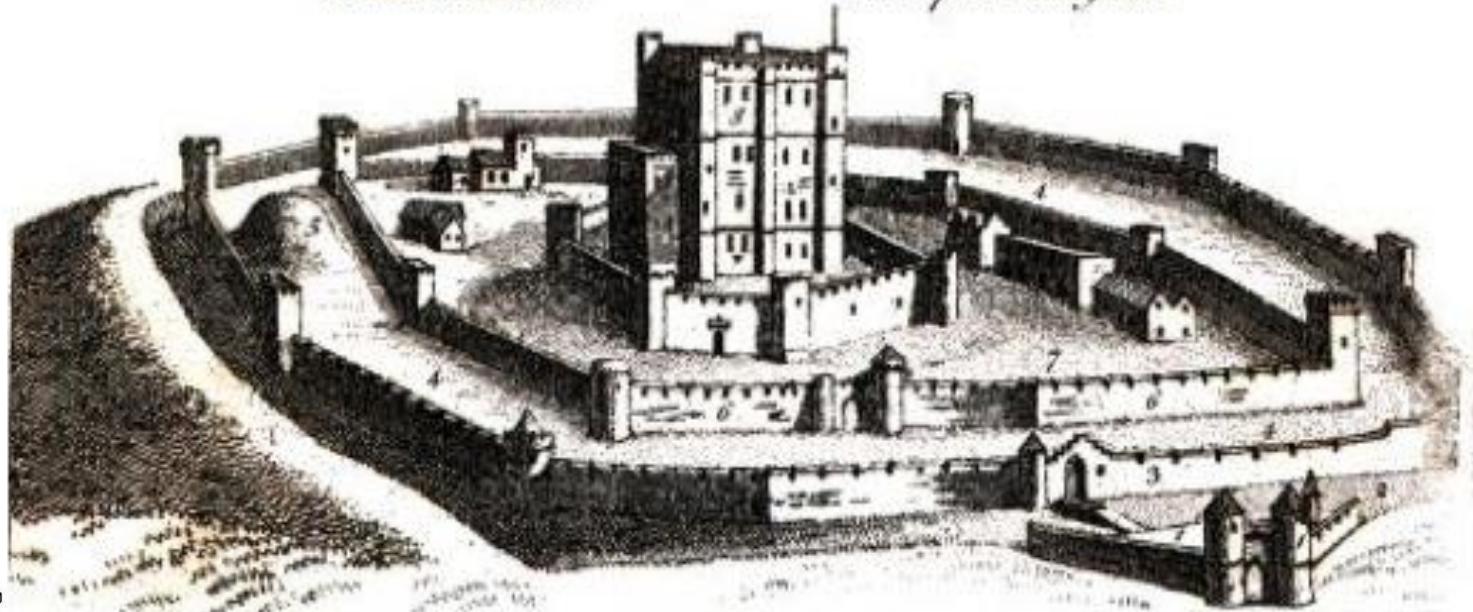
# Old School vs. New World



# IT Security threats

## References.

- 1. The Barbican.
- 2. The Ditch or Moat.
- 3. Wall of the outer Ballium.
- 4. Outer Ballium.
- 5. Artificial Mount.
- 6. Wall of the Inner Ballium.
- 7. Inner Ballium.
- 8. Keep or Dungeon.



# Towards the cloud – and beyond



## Many To One

Mange brugere  
En enkeltstående  
central server



I forgårs



## One To One

En bruger  
En computer



I går



## One To Many

En bruger  
Mange medier



I dag

## Mobilitet

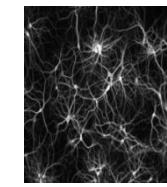
Machine To Machine



## Many To Many



I morgen  
Allestedts-  
nærværende



Neuro-  
Nano-  
technologier

I over-  
morgen



# Towards the cloud – and beyond



## Many To One

Mange brugere  
En enkeltstående  
central server



I forgårs



## One To One

En bruger  
En computer



I går



## One To Many

En bruger  
Mange medier



I dag



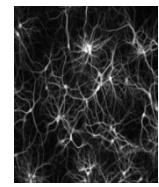
## Many To Many



Machine To Machine



I morgen

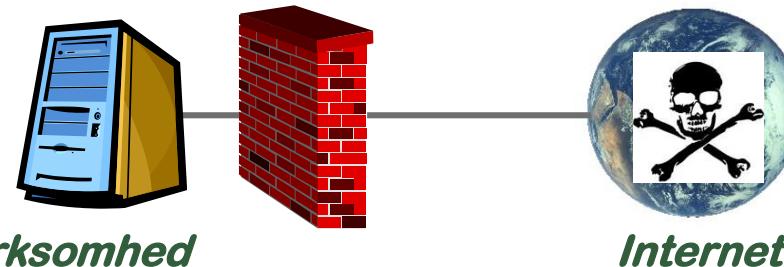


Neuro-  
Nano-  
technologier

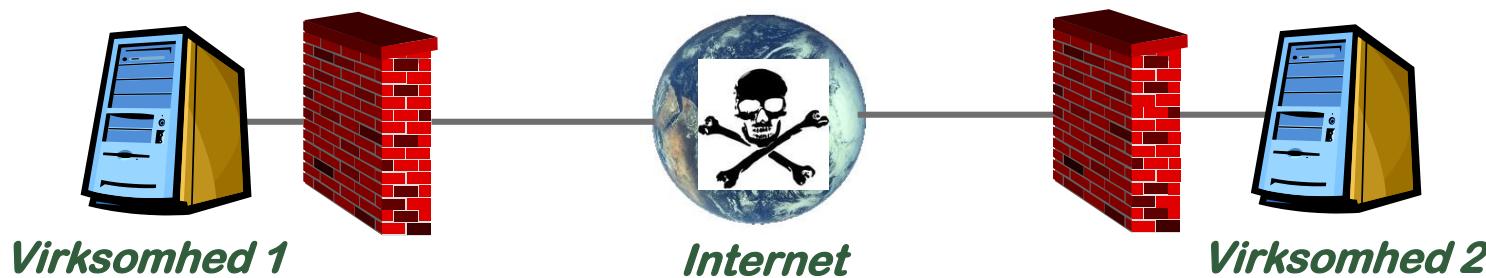
I over-  
morgen



## 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”

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



# The same level of security everywhere?



[Follow 3,234](#)

Kontakt Nyhedsbrev Language ▾  Seg

  
Kunde & Co

Branding | Strategisk marketing | Internationale kampagner | Digital | Corporate Religion | Cases | Om os

Få inspiration til, hvordan de mange nye muligheder kan spille sammen

Bestil ny casefolder



Bureau med speciale i **international markedsføring, branding og udvikling**

NYHEDSBREV  [Tilmeld her](#)

## Zentropa and Danish National Bank?



## Same security culture for everyone internally?

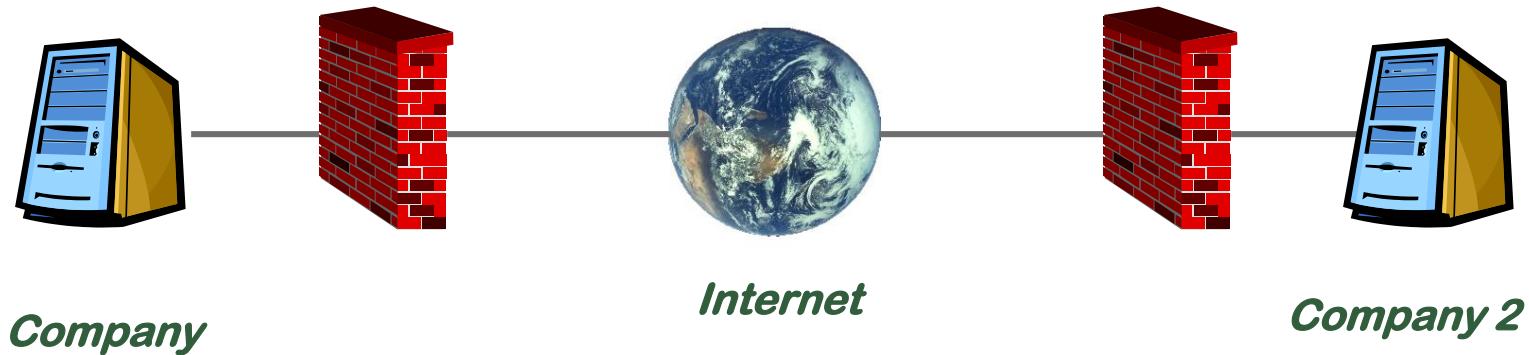


New world

Inside-out → Outside-in



# TCP/IP and secure communication over the Internet



“I’m ok, and you’re ok –  
but we can’t trust the network”

**Focus on data and services (passwords and acces control / rights management) and segmentation**



# Questions

