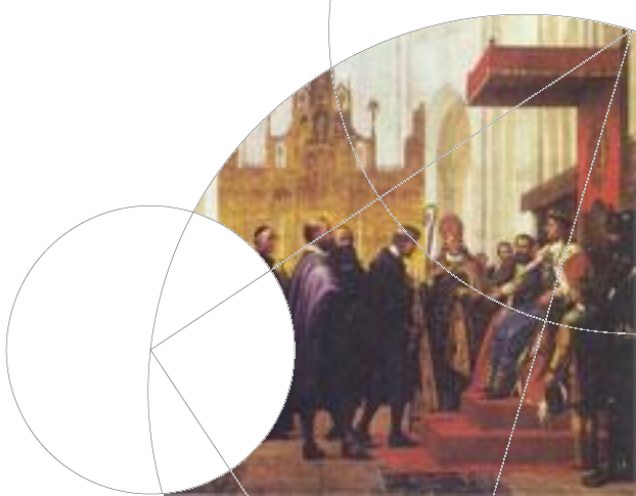
Security architecture and firewalls
Old-school vs new world

DoS and DDoS

Carsten Jørgensen
Department of Computer Science

DIKU 20. september 2019

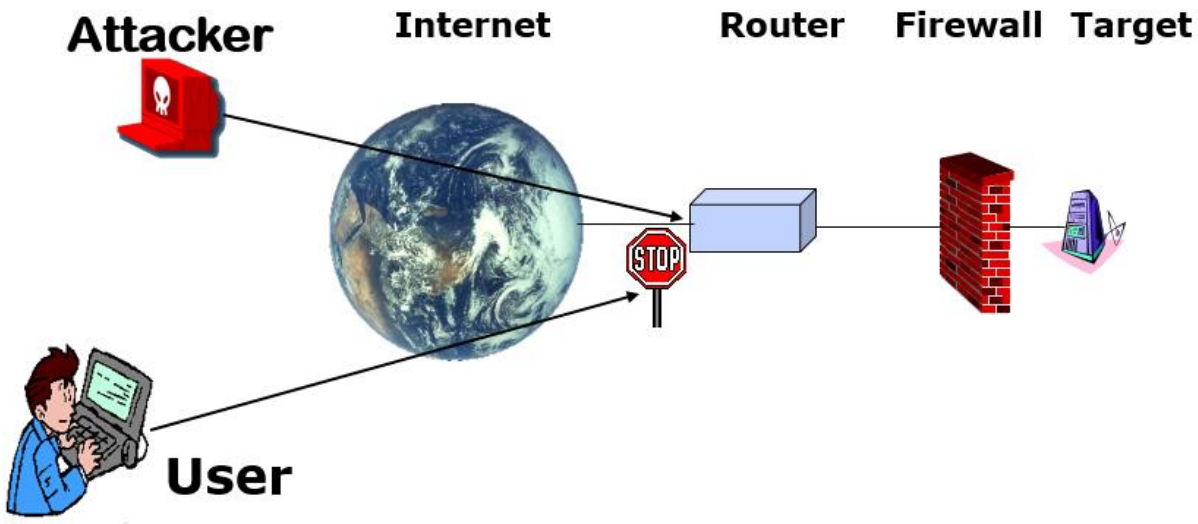
DoS: Denial of Service
DDoS: Distributed Denial of Service



What is DoS

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

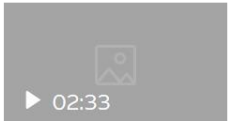
DoS vs. DDoS

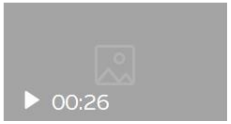


What is DoS

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

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

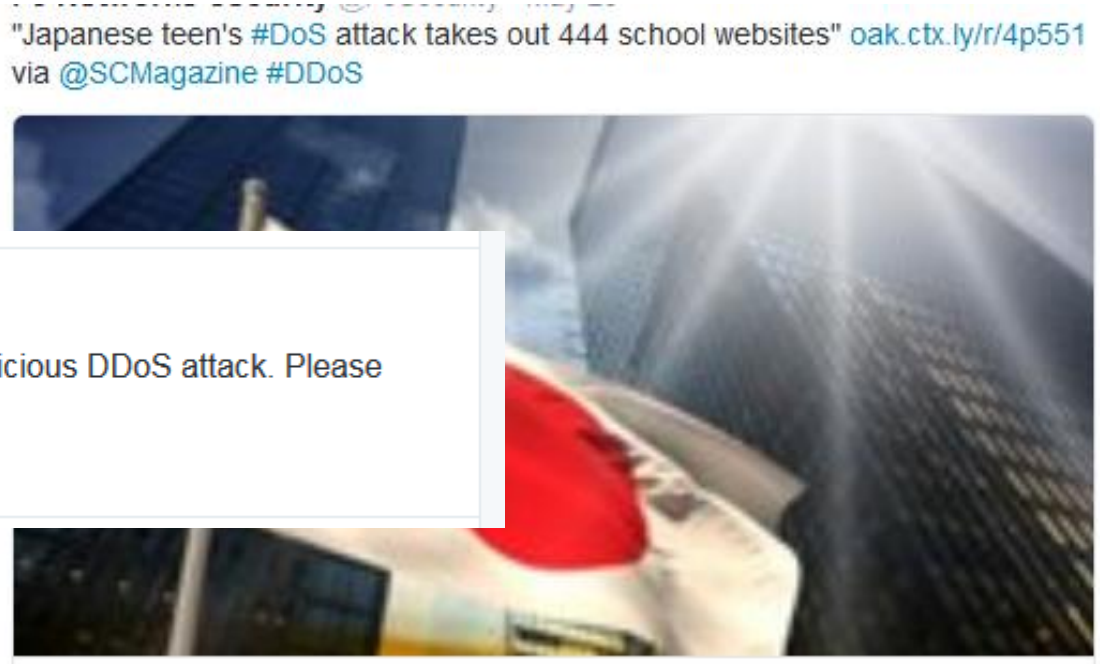
Why?

Part of serious attacks, hiding tracks

Anger or “Fun”

Curiosity

Not understanding how DoS (or the internet) works



Hacktivism

version2

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
  - Driftsstatus
  - Driftsstatistik 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.

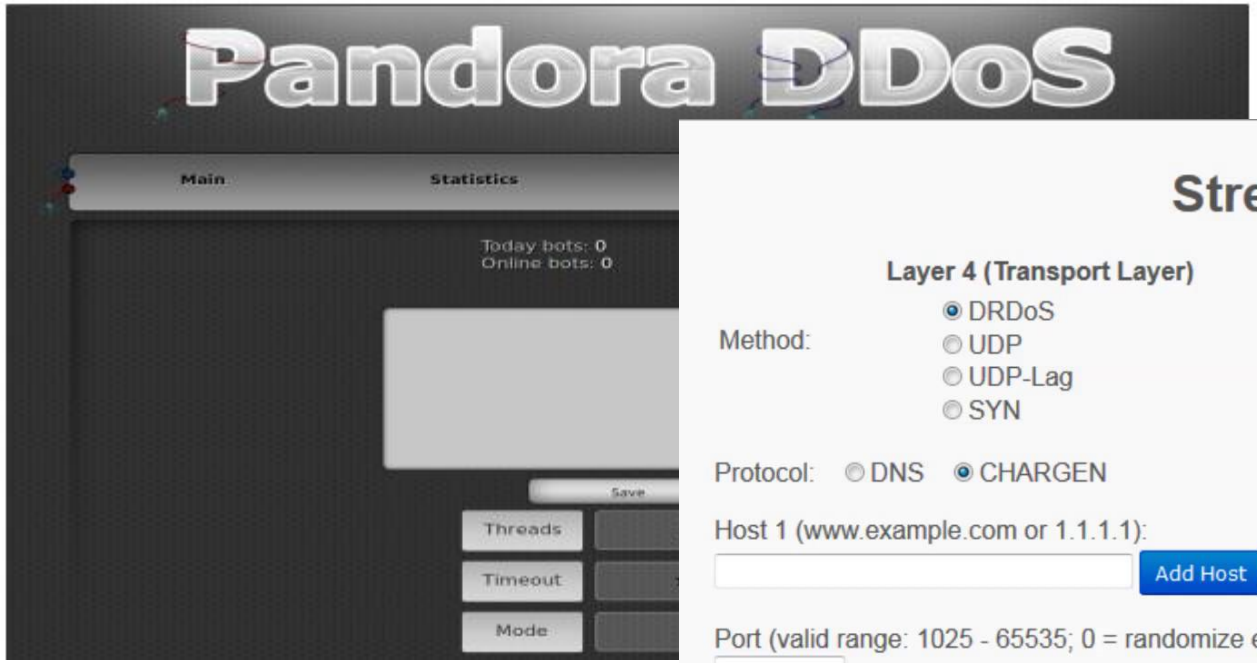
Lignende hændelser fandt sted den 24. og 25. marts.

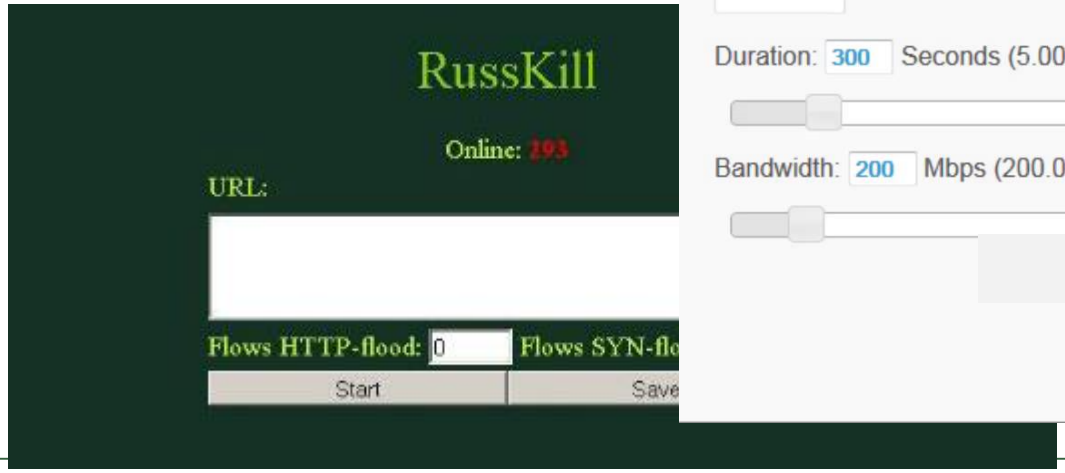
Adgangen er stadig ustabil, og der arbejdes på at løse problemerne.

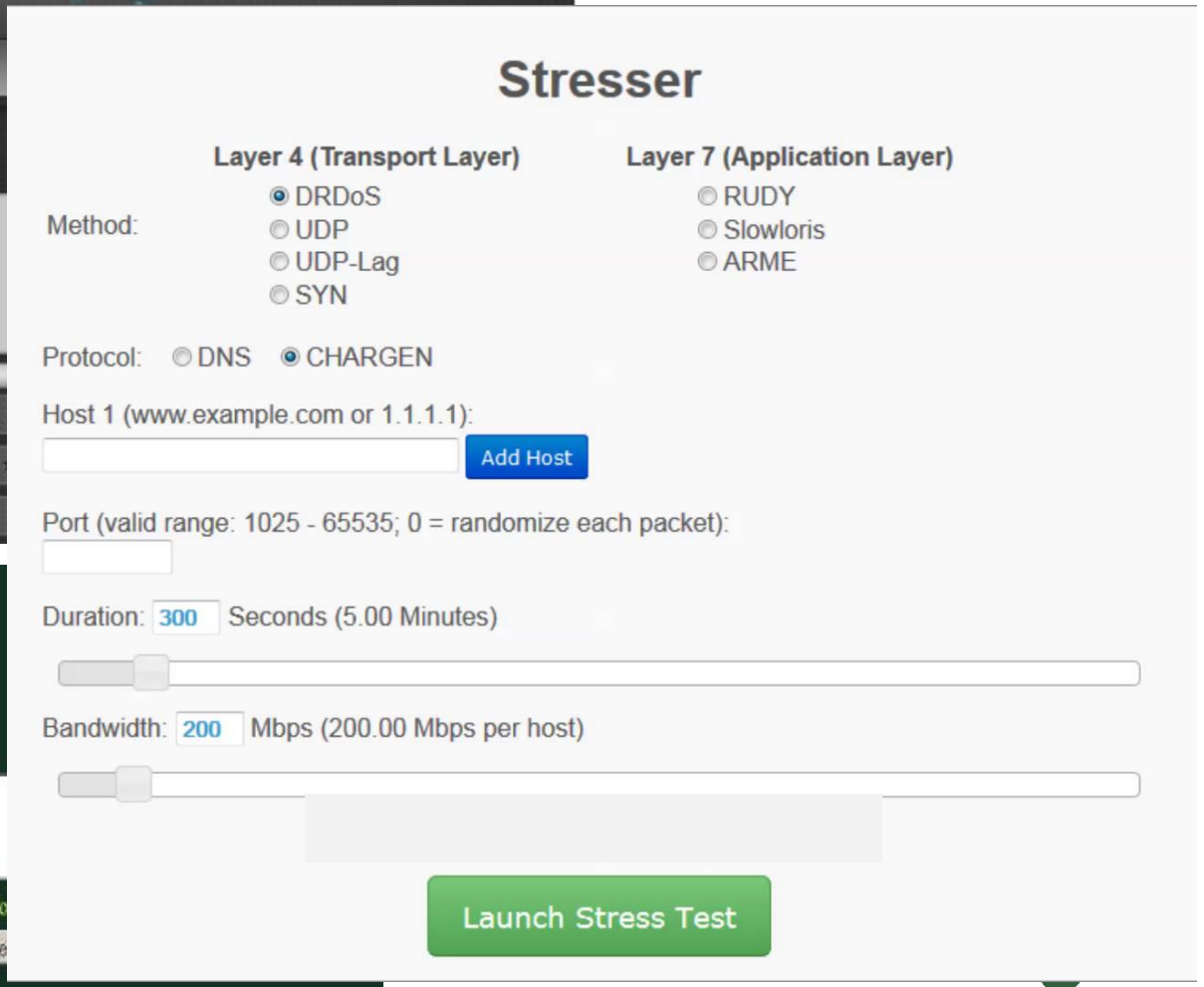
Årsagen til problemerne skyldes, at it-kriminelle udfører det, der kaldes et DDoS-angreb mod NemID.

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

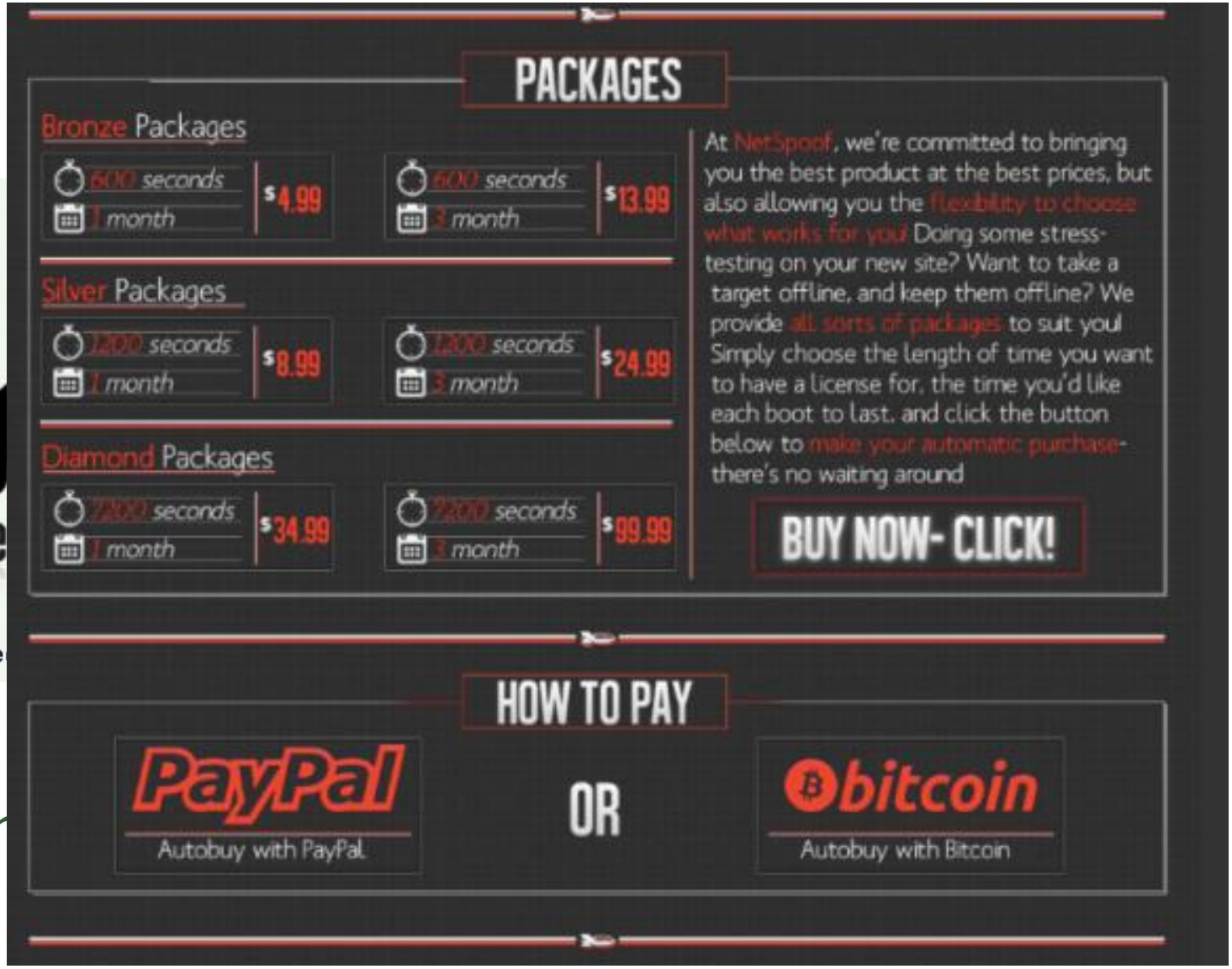
DoS is easy for the attacker





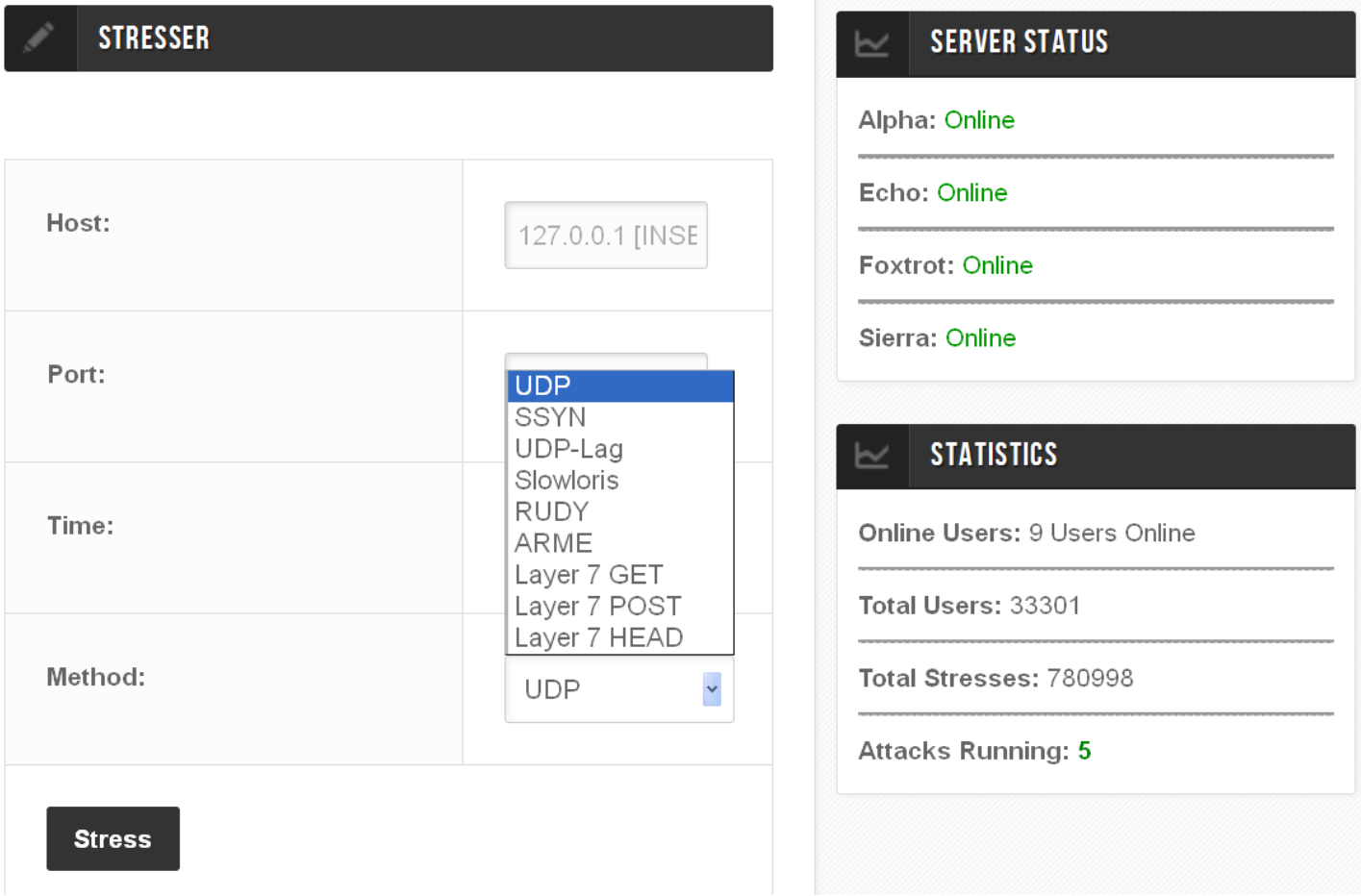


DoS is cheap - and easy for the attacker



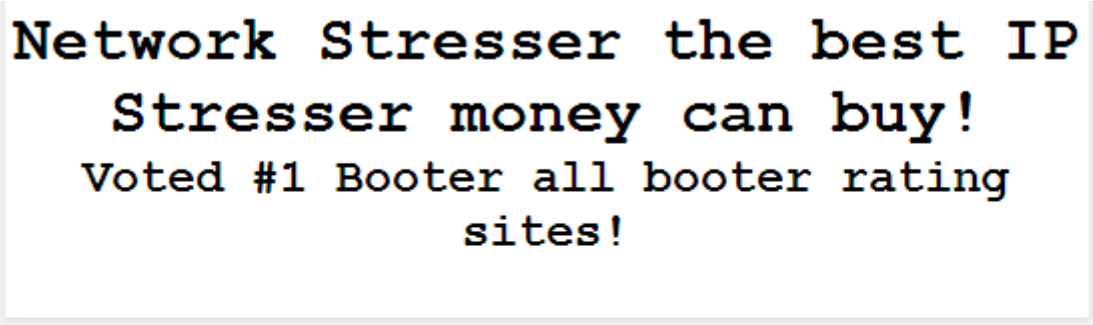
Stressers and booters

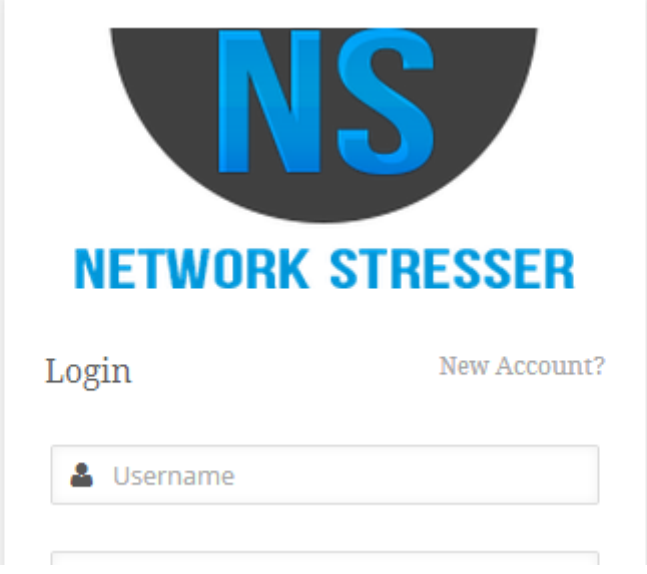
”Stressers” and ”booters”



Stressers and booters

”Stressers” and ”booters”





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

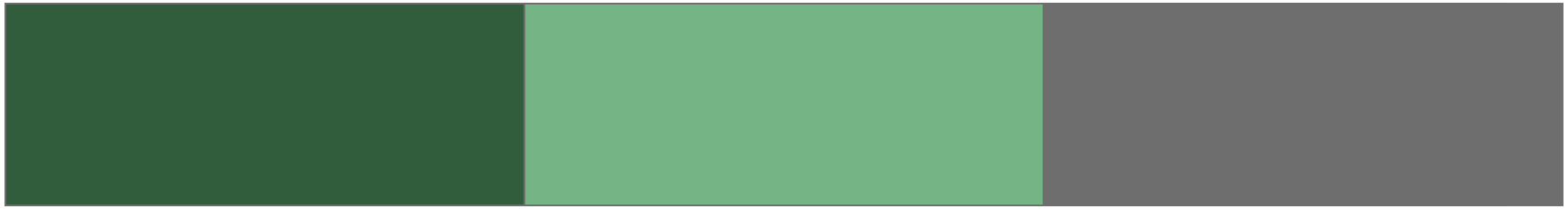
Recieves: TO: A:port 80, FROM **A**:port 80

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:

“Packet is NOT fragmented”

“NEXT fragment follows”

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

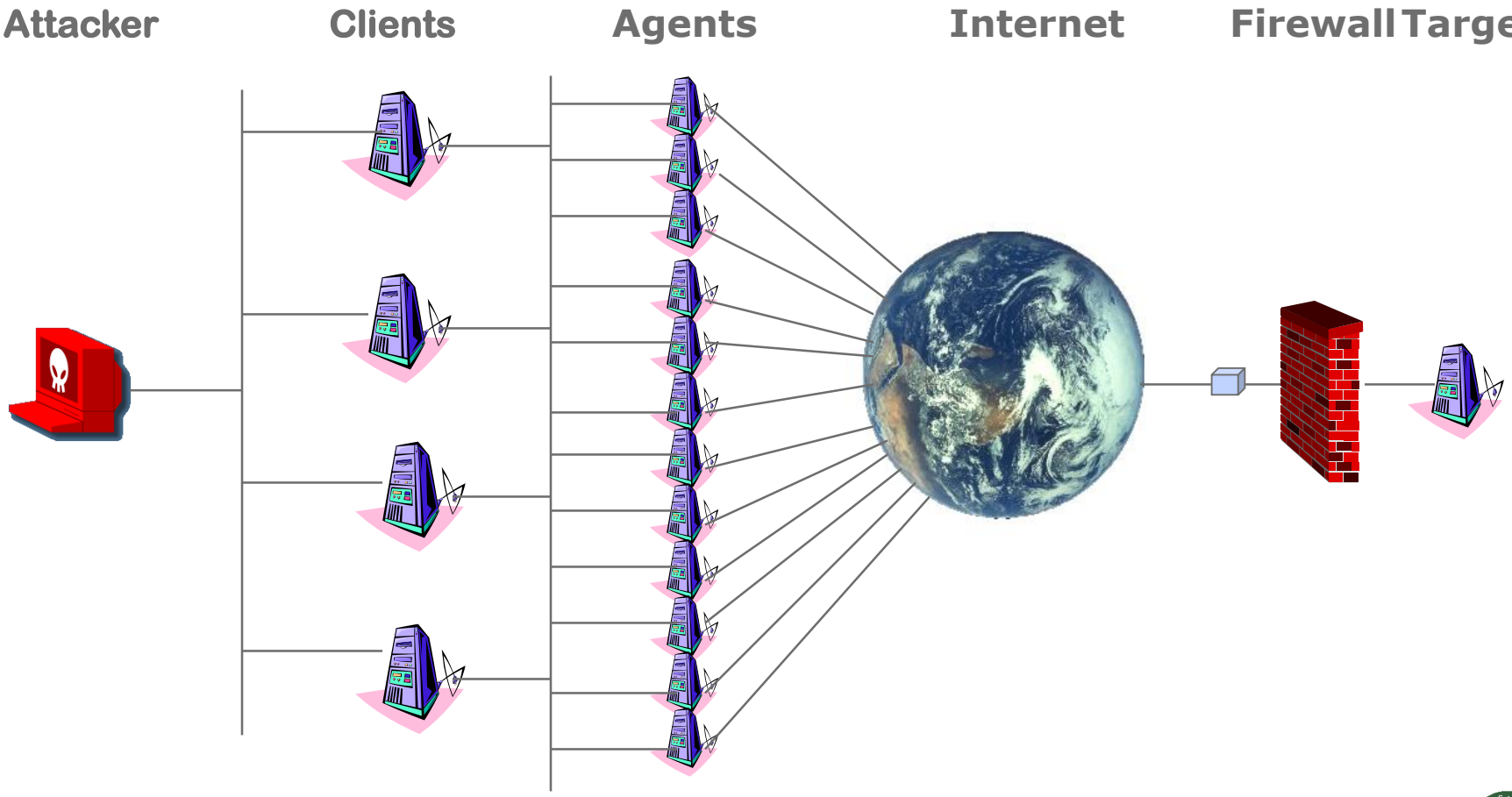
Stopping others from accessing the network or host

Distributed Denial of Service and BotNets

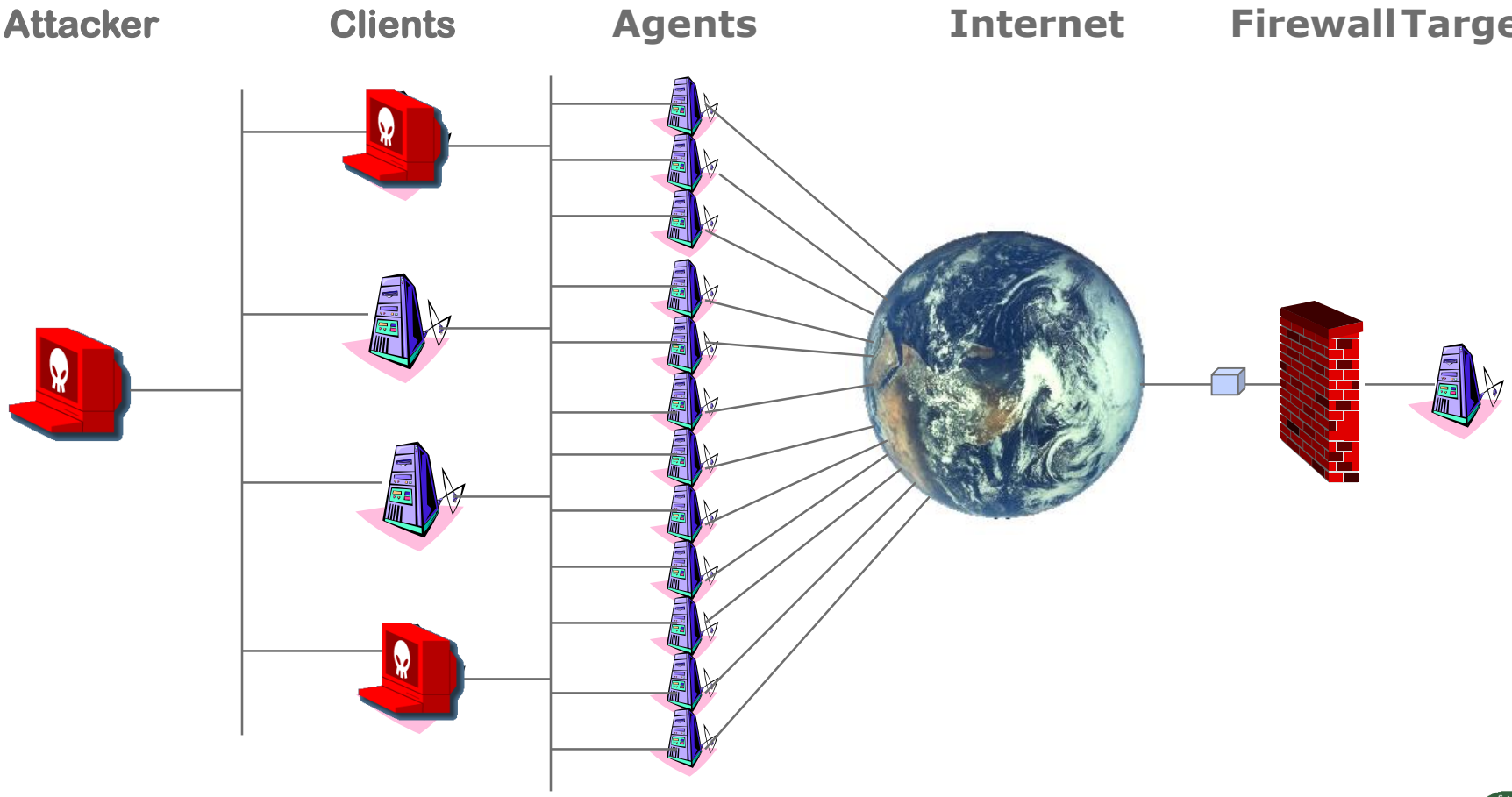
Can be groups of individuals working together (hacktivism)

Most commonly:
Botnets of compromised PCs or compromised servers

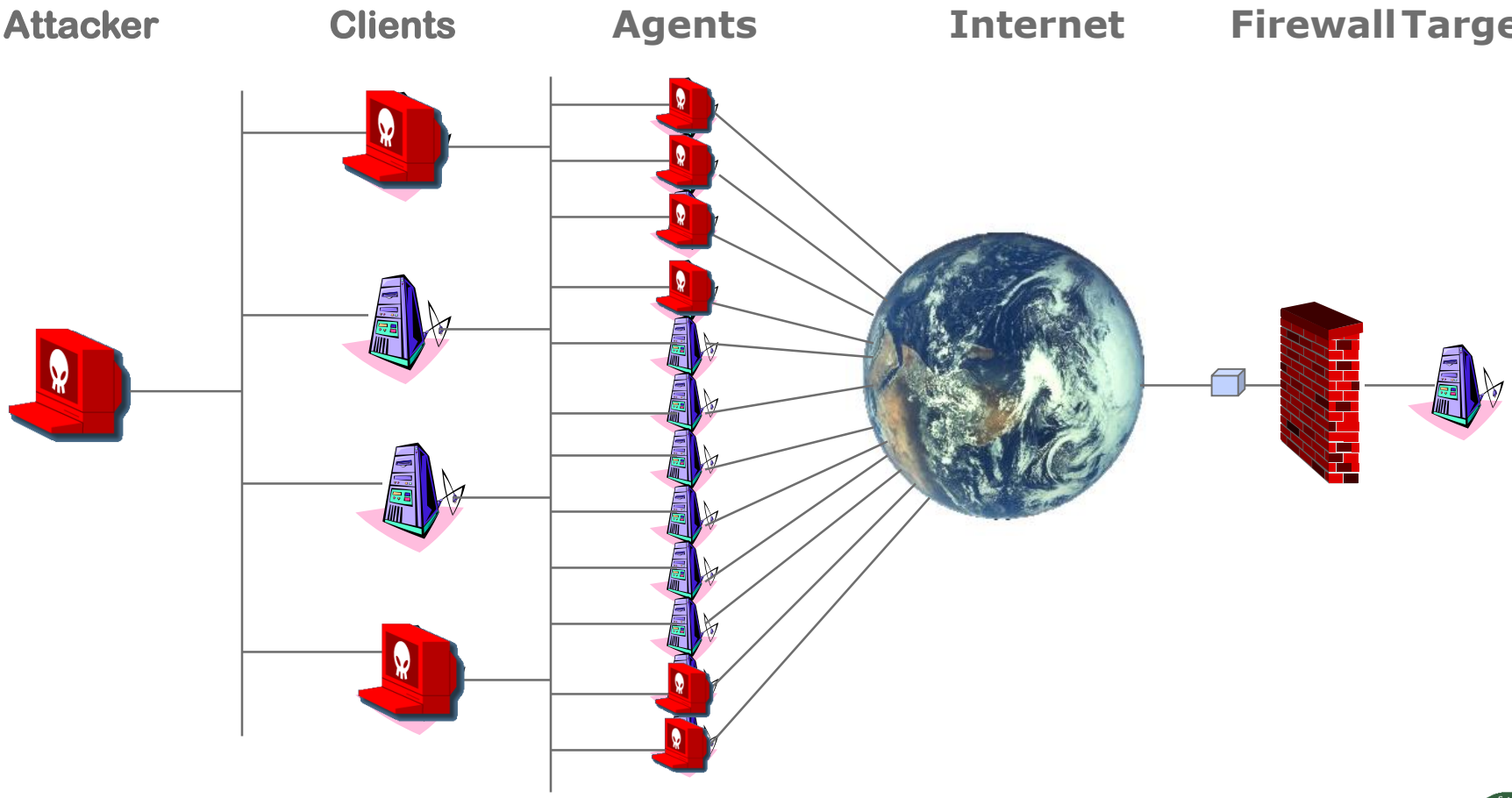
Distributed Denial-of-Service Attack



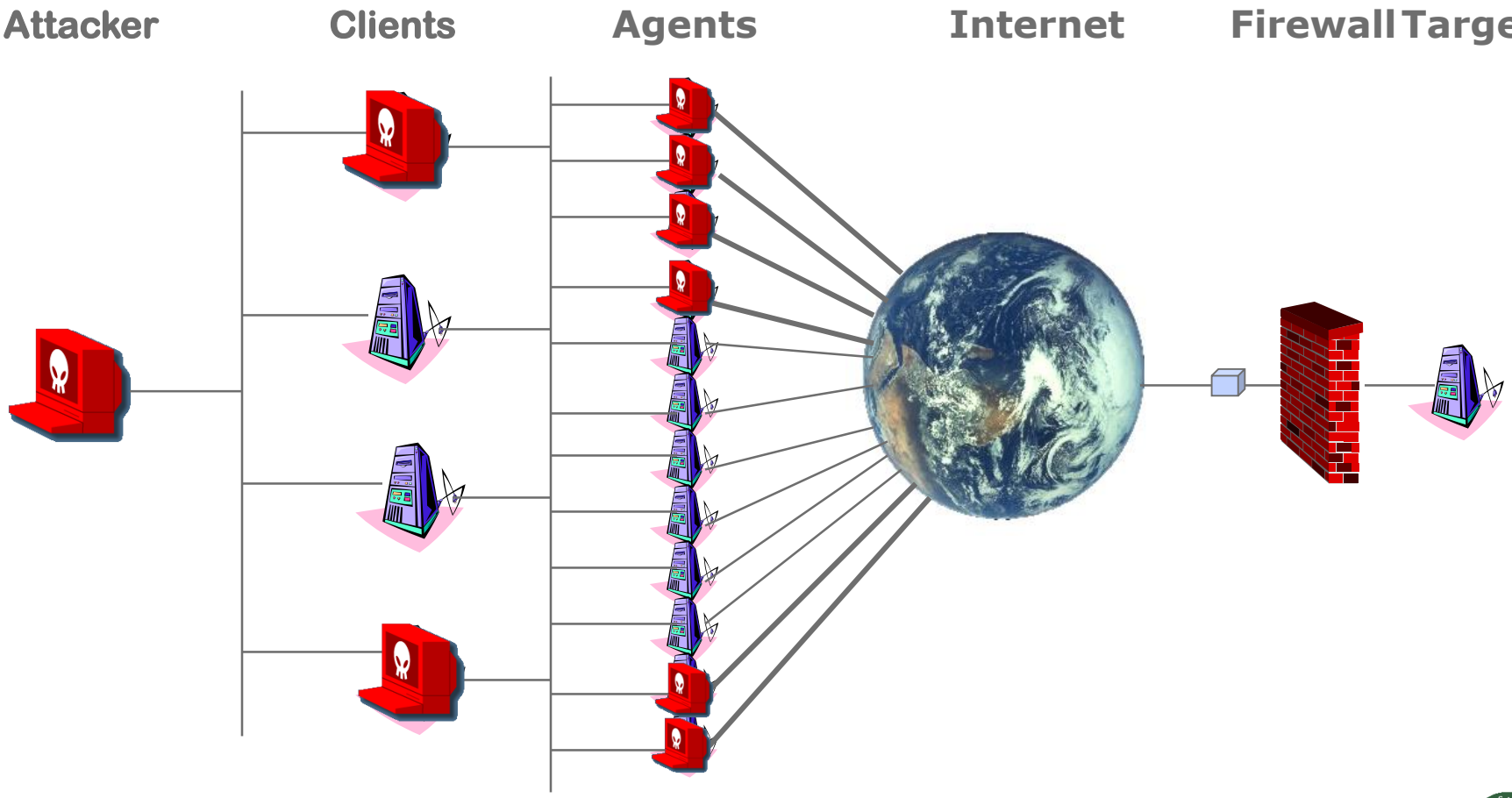
Distributed Denial-of-Service Attack



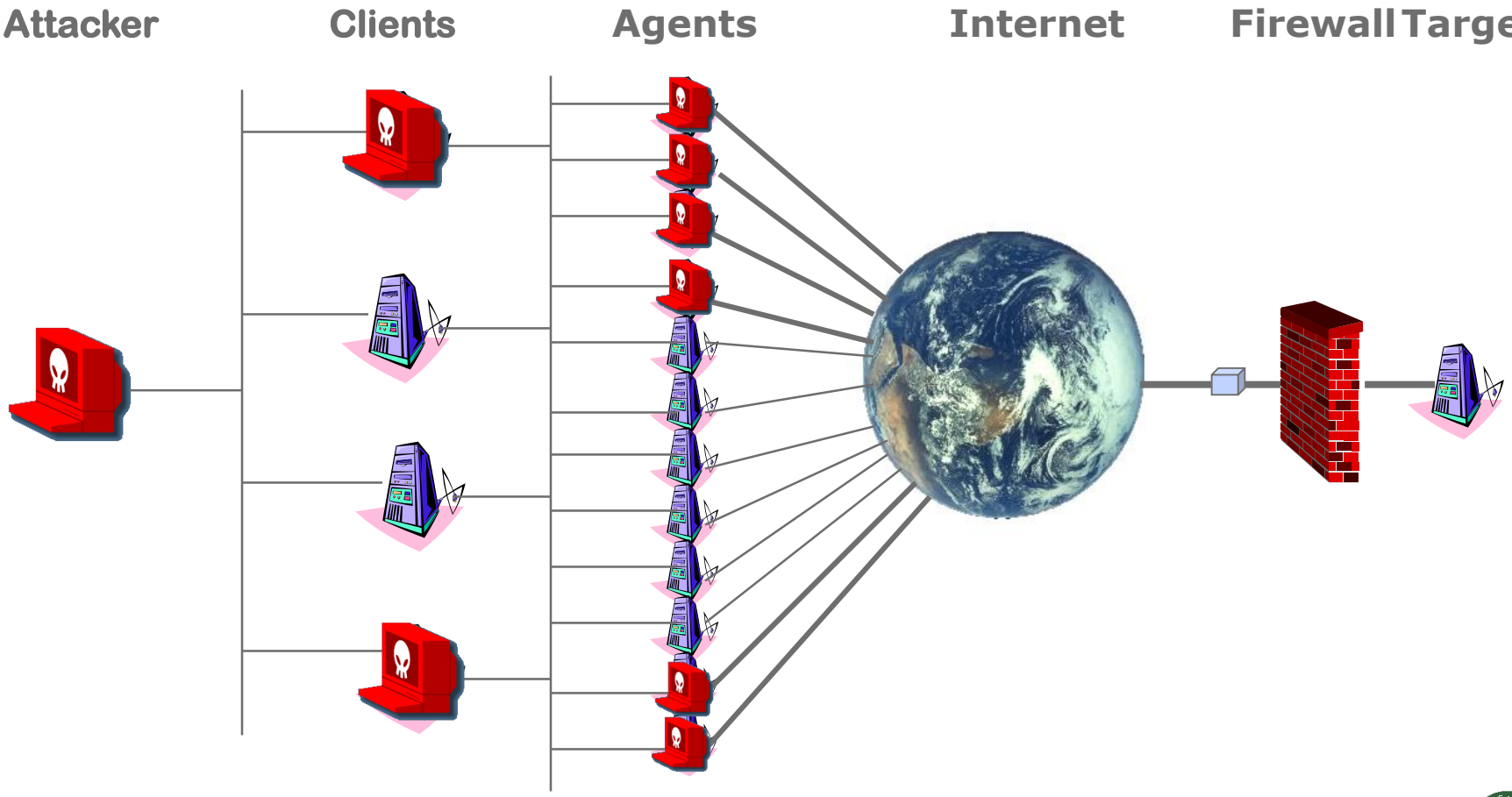
Distributed Denial-of-Service Attack



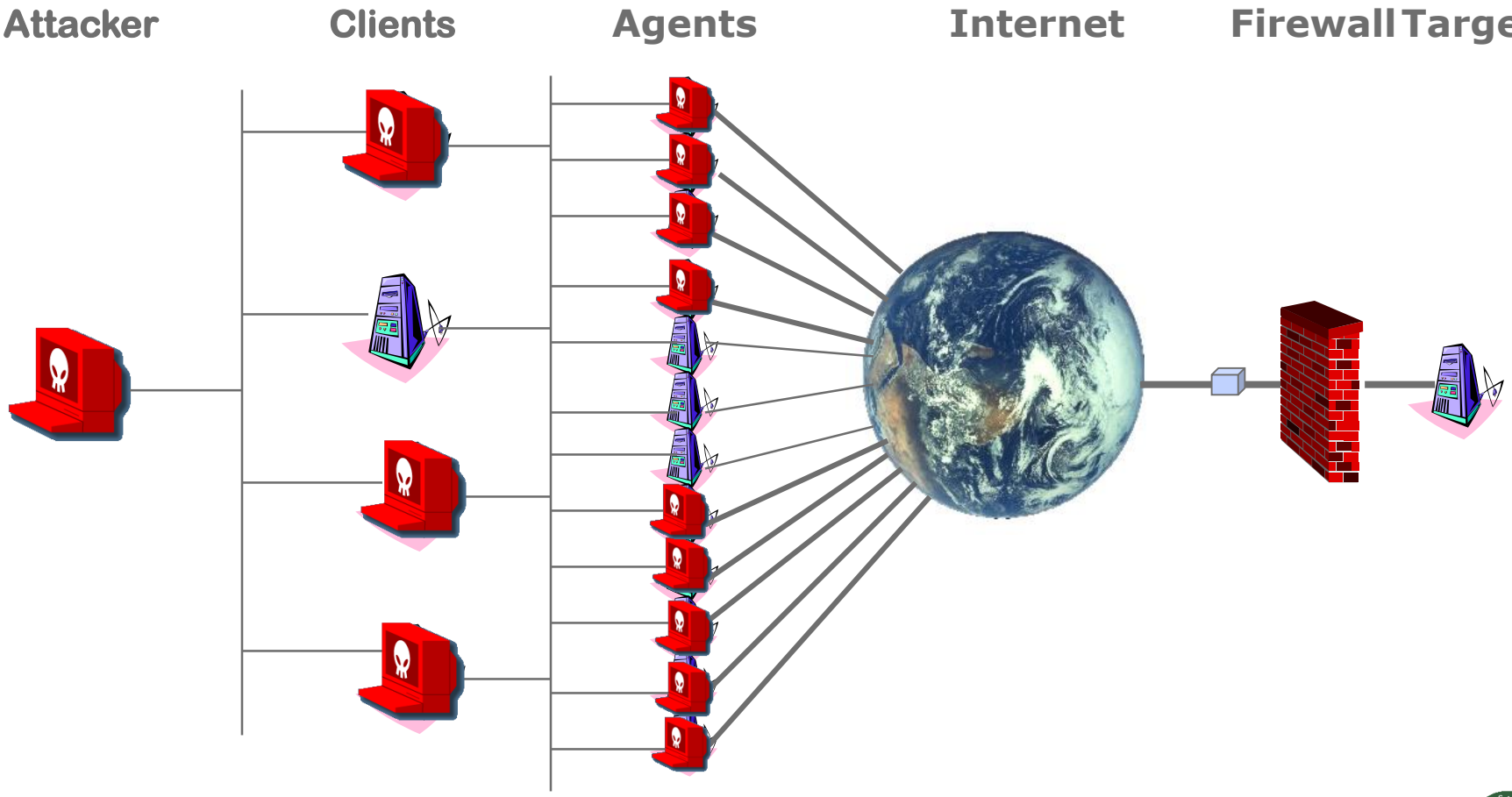
Distributed Denial-of-Service Attack



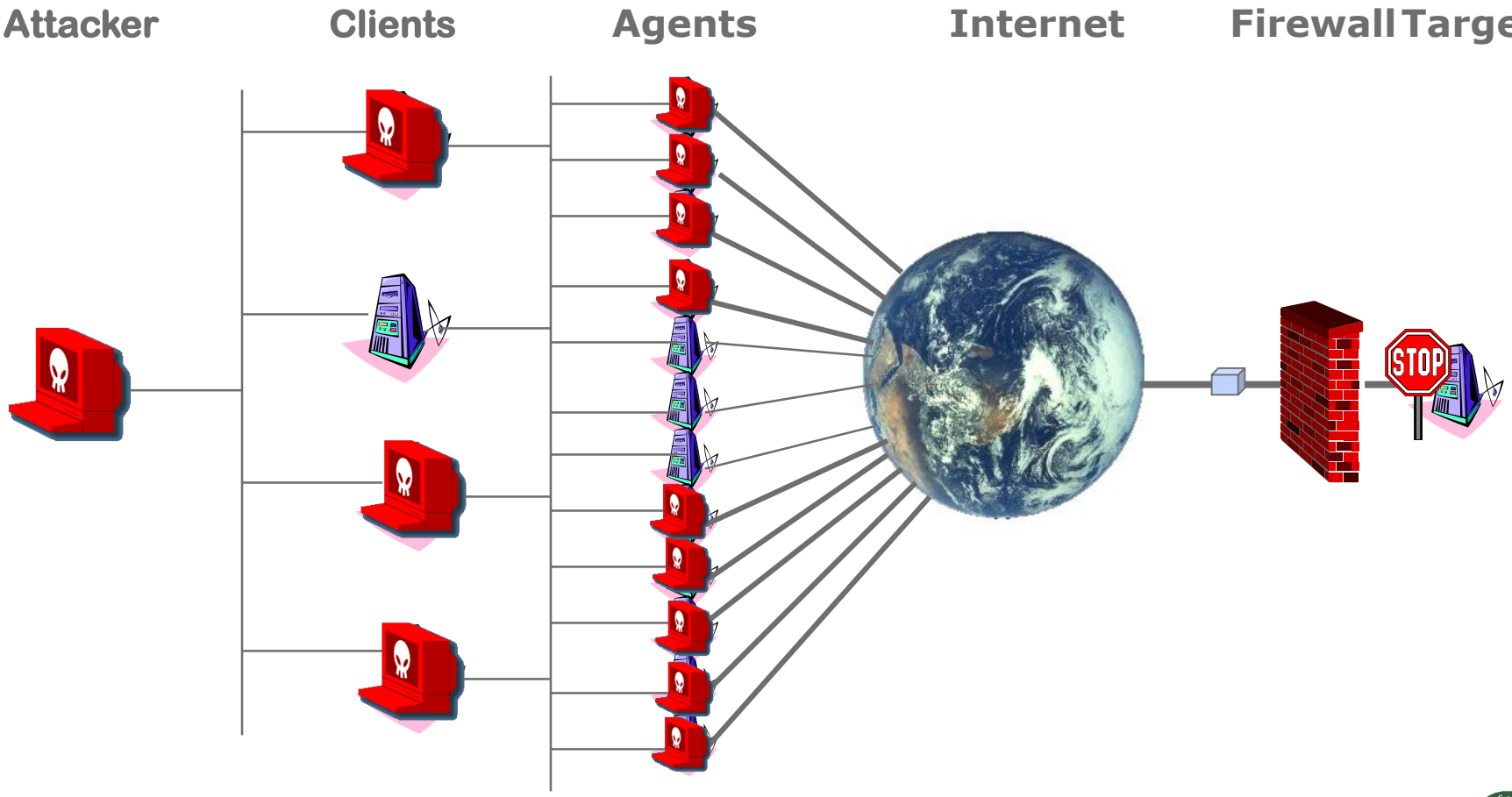
Distributed Denial-of-Service Attack



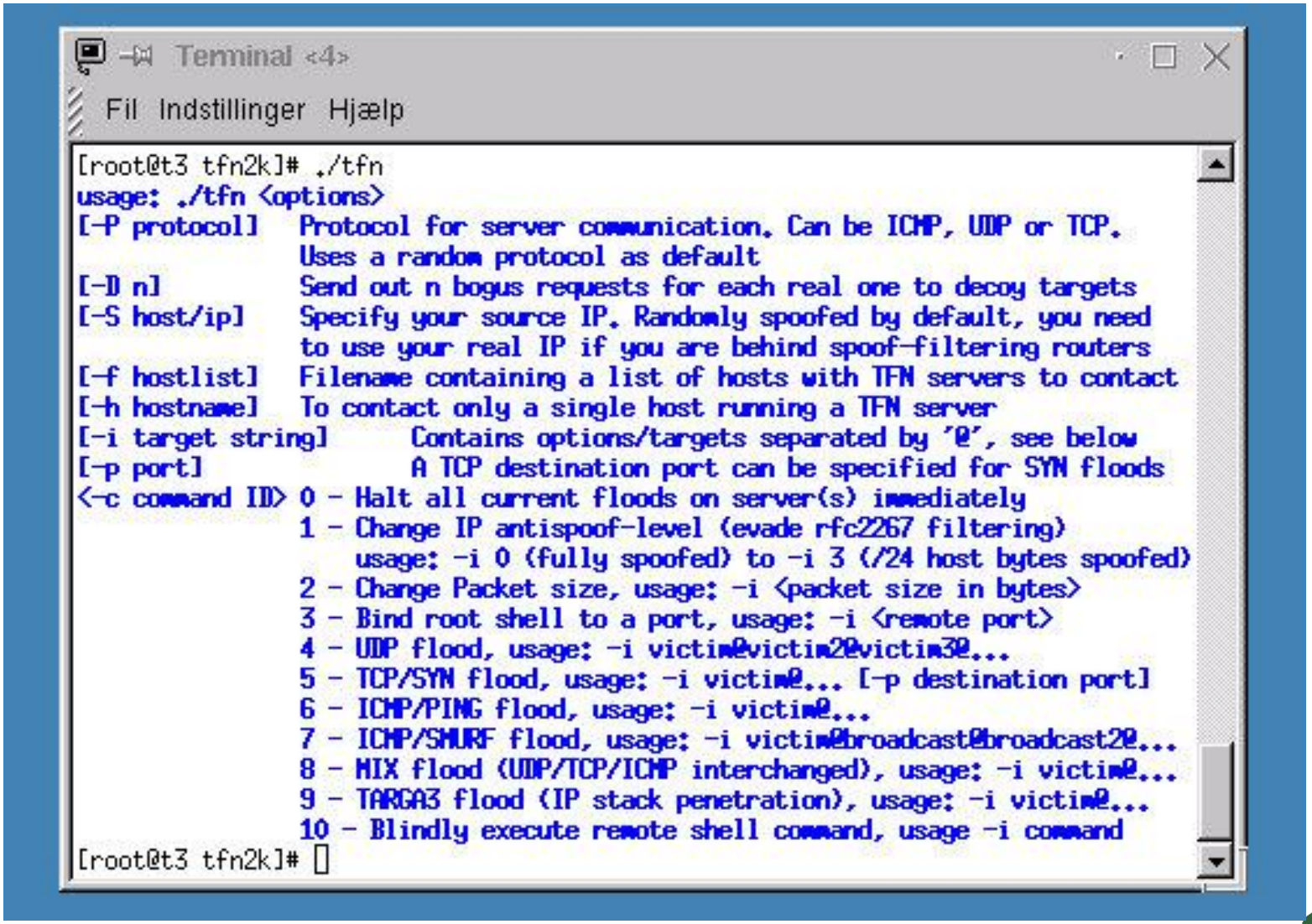
Distributed Denial-of-Service Attack



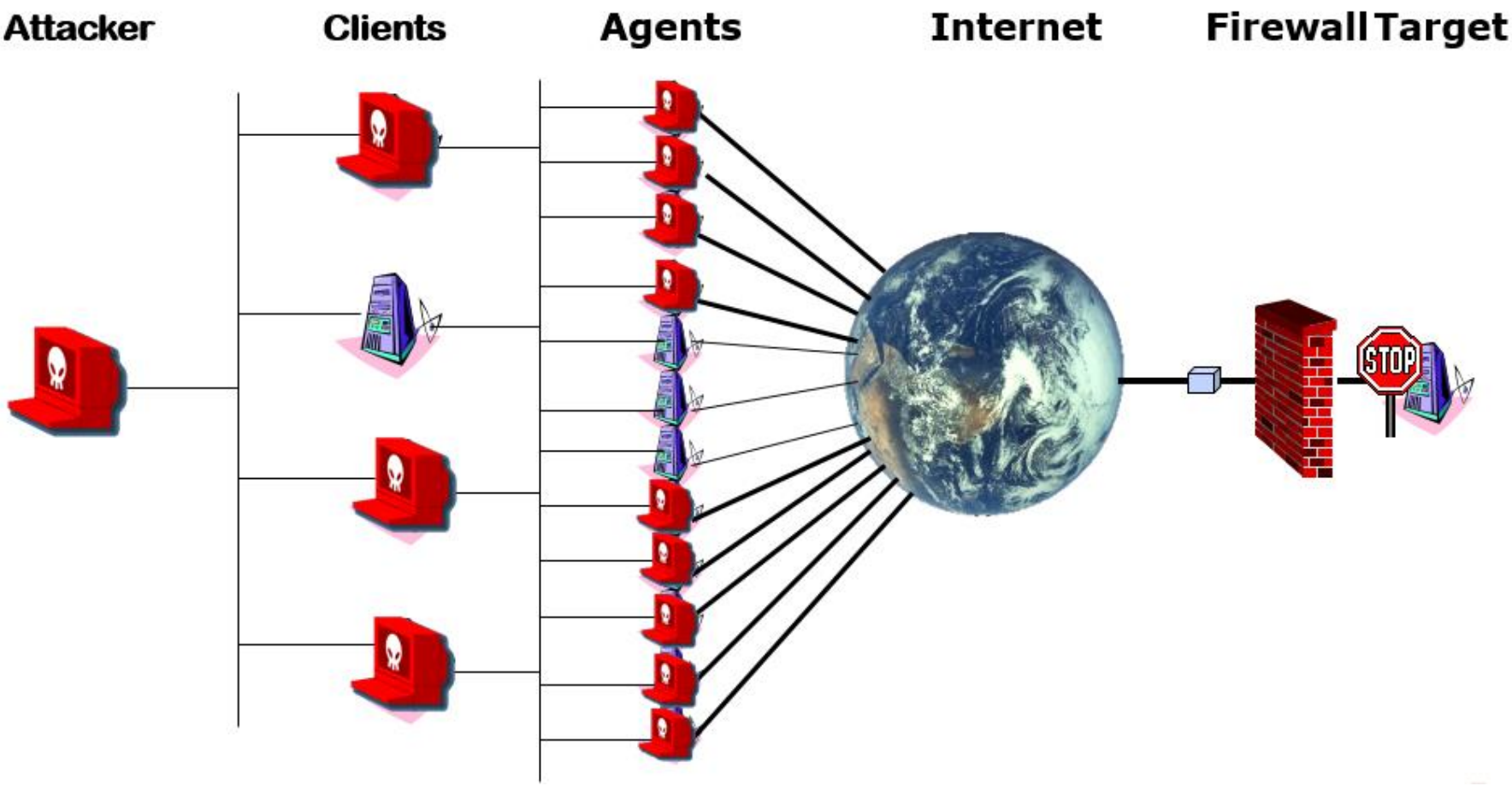
Distributed Denial-of-Service Attack



Tribe Flood Net 2000



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

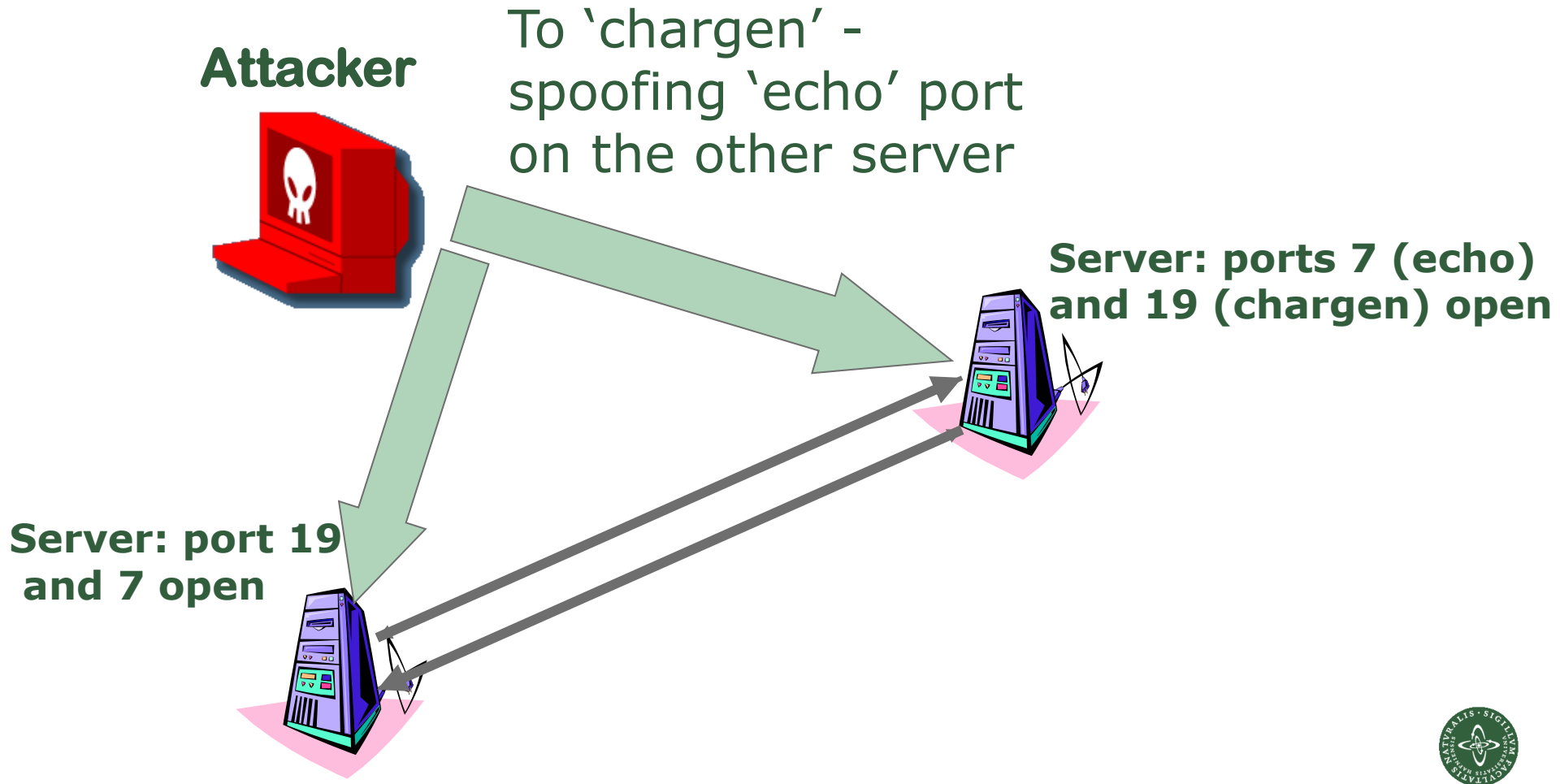
Spoofing

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

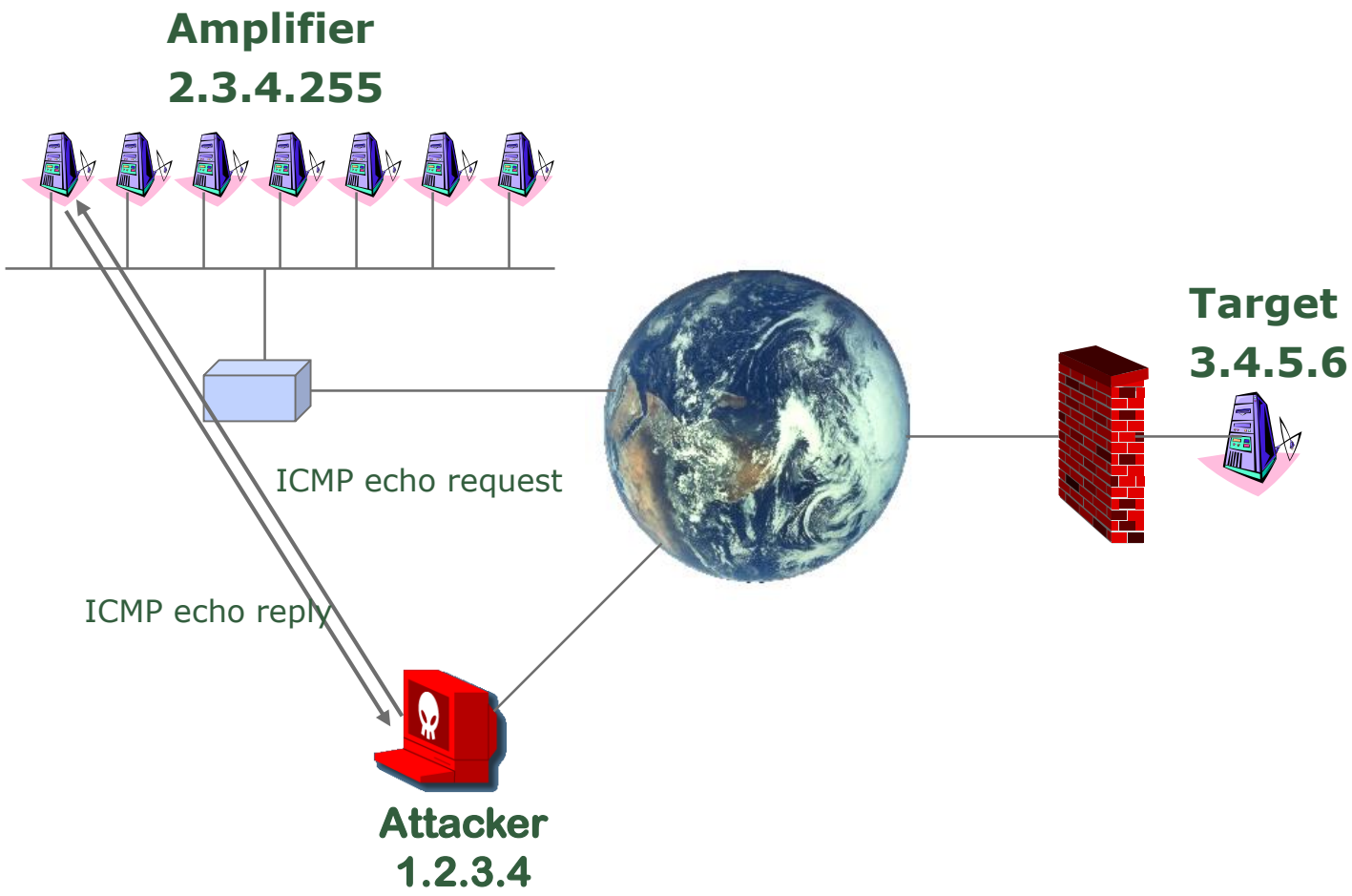
Attackers not interested in receiving responses to the requests they send - the packets do not have to be accurate or correctly formatted

Amplification DDoS

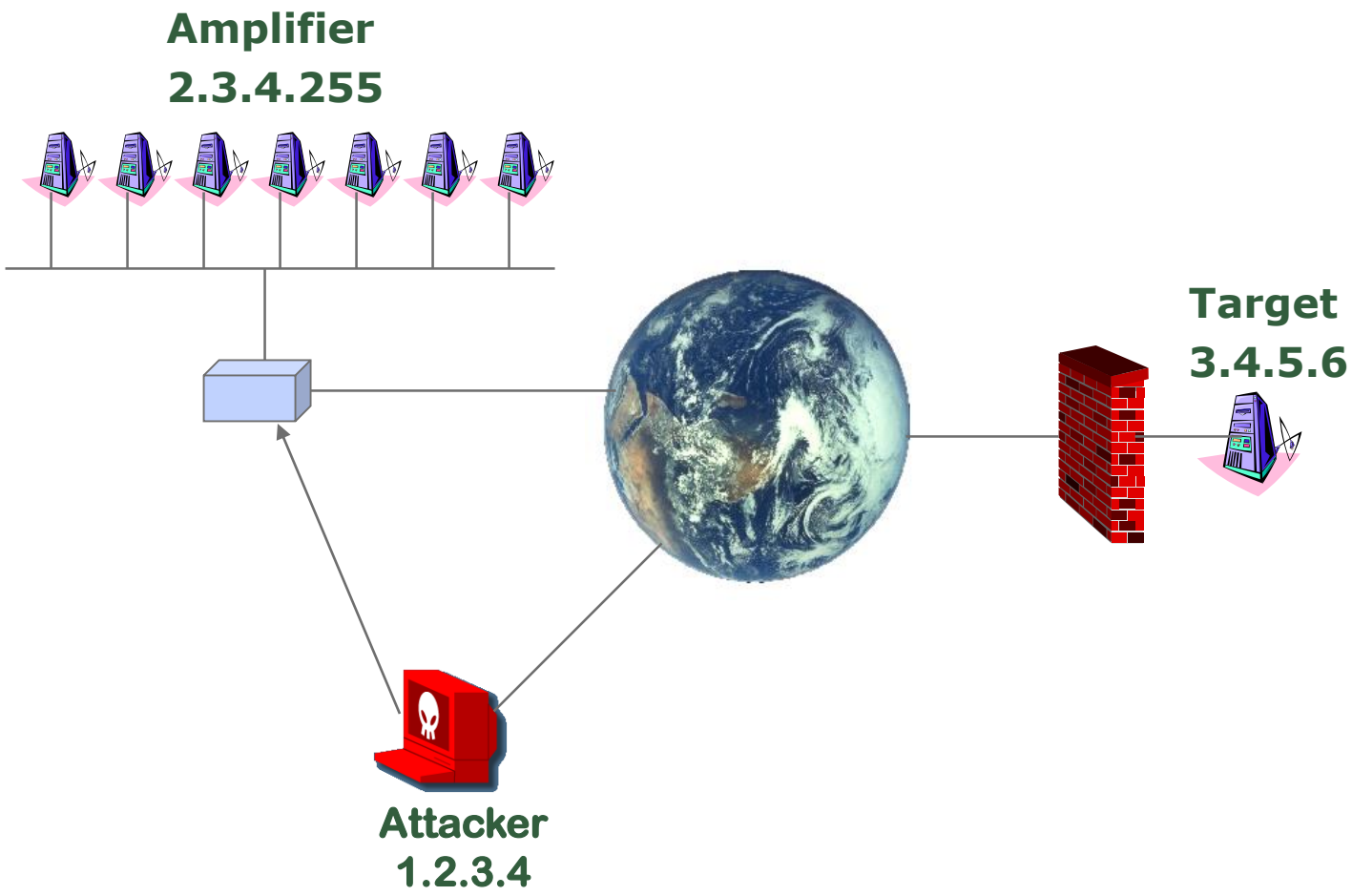
Chargen, echo etc



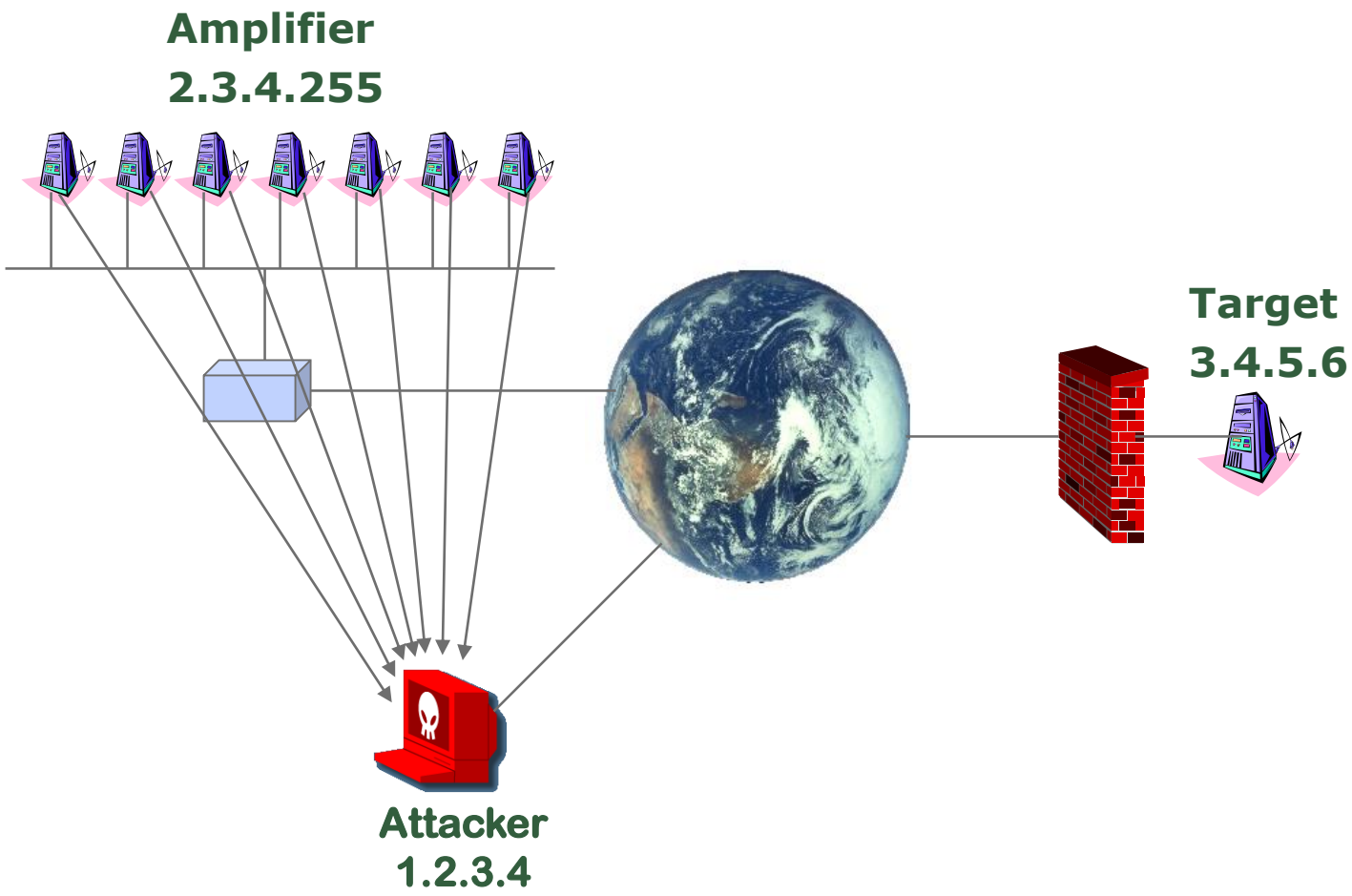
Smurf (and Fraggle):



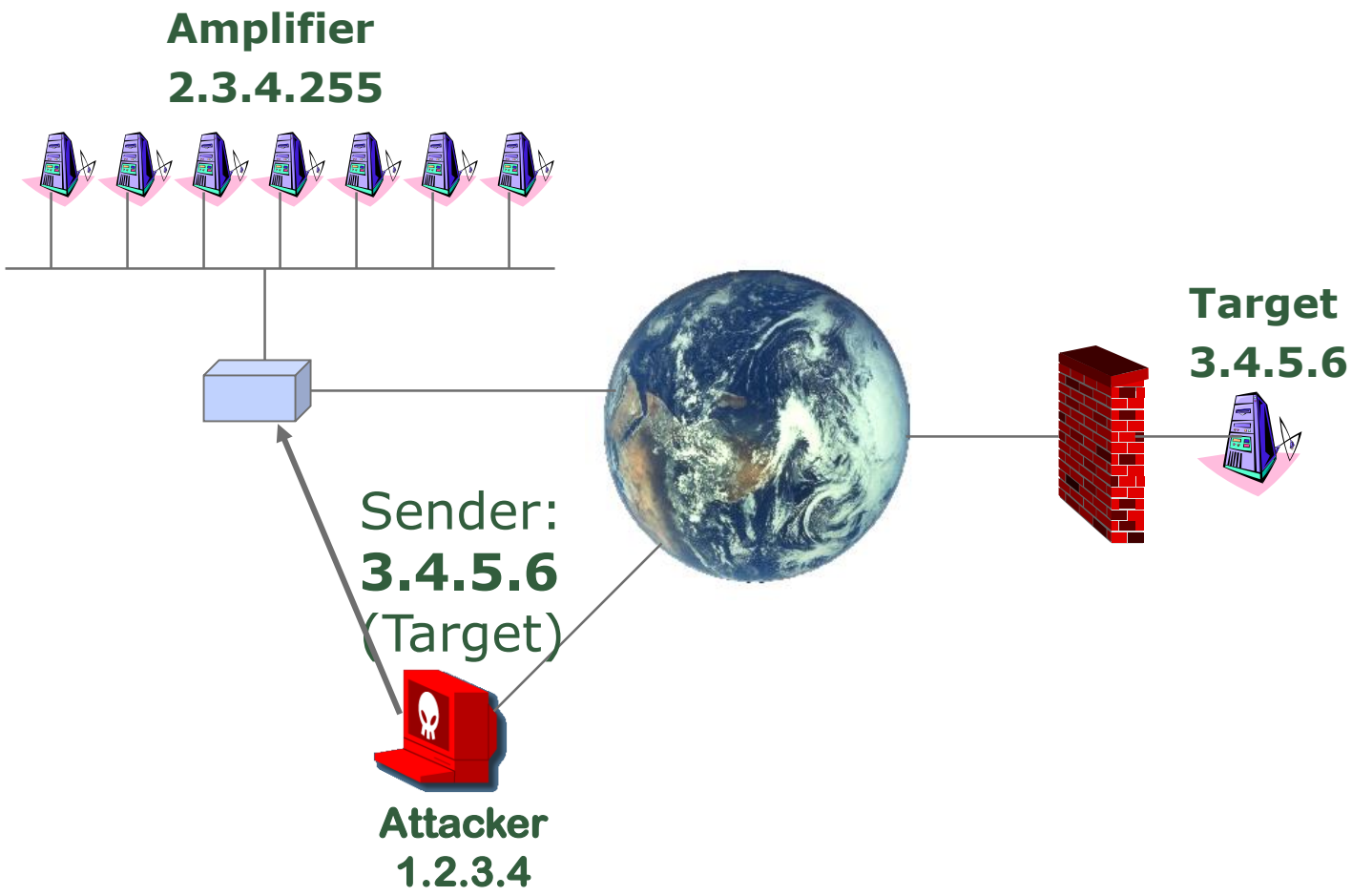
Smurf (and Fraggle):



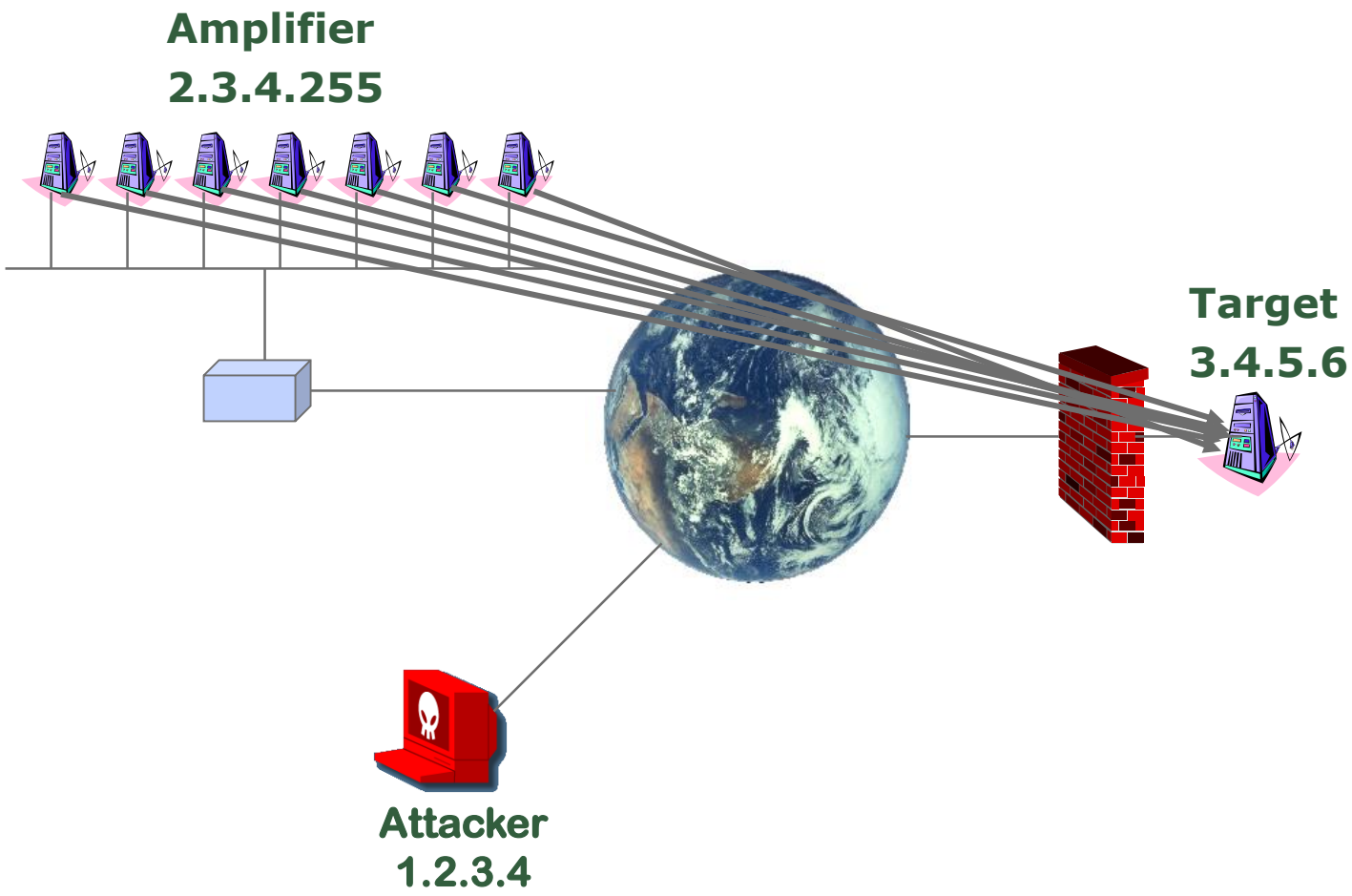
Smurf (and Fraggle):



Smurf (and Fraggle):



Smurf (and Fraggle):



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

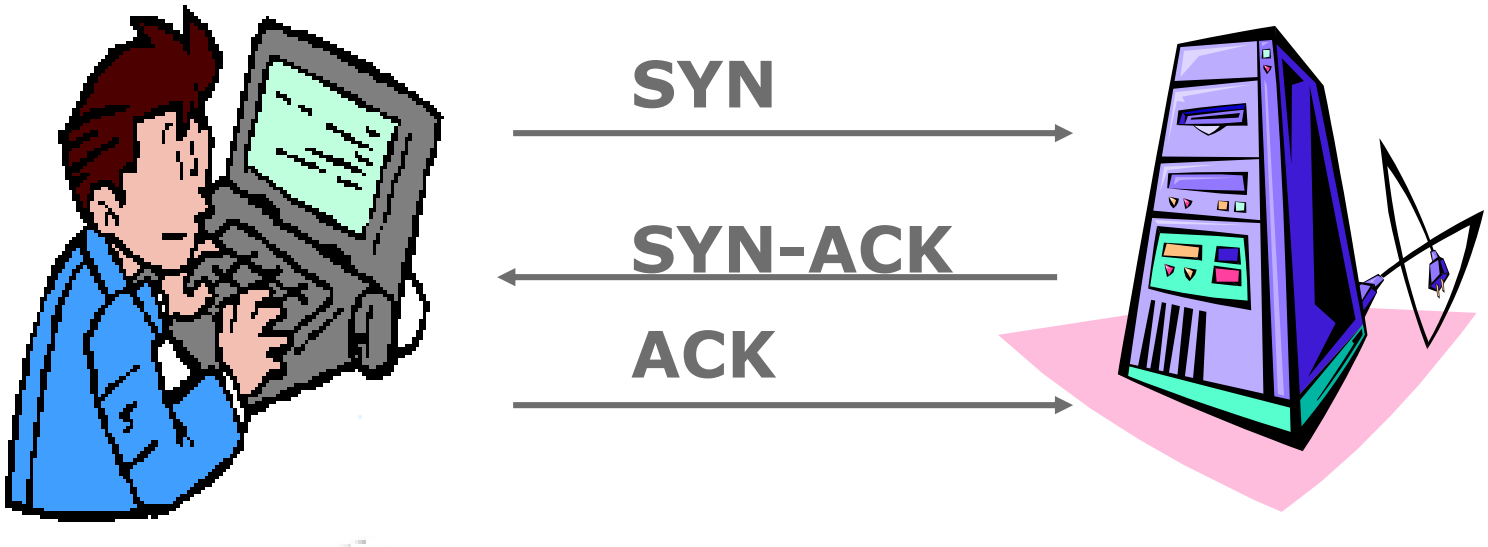
December 2015: 500 Gbps (several – DNS amplification)
January 2016 : 602 Gbps against BBC
21.Sep 2016: 665 Gbps against Brian Krebs
24. Sep 2016: 1Tbps (1000 Gbps) against Brian Krebs
25. Sep 2016: 1.1 Tbps against OVH (hosting provider)
February 28. 2018: 1.35 Tbps against GitHub

Internet of Things…

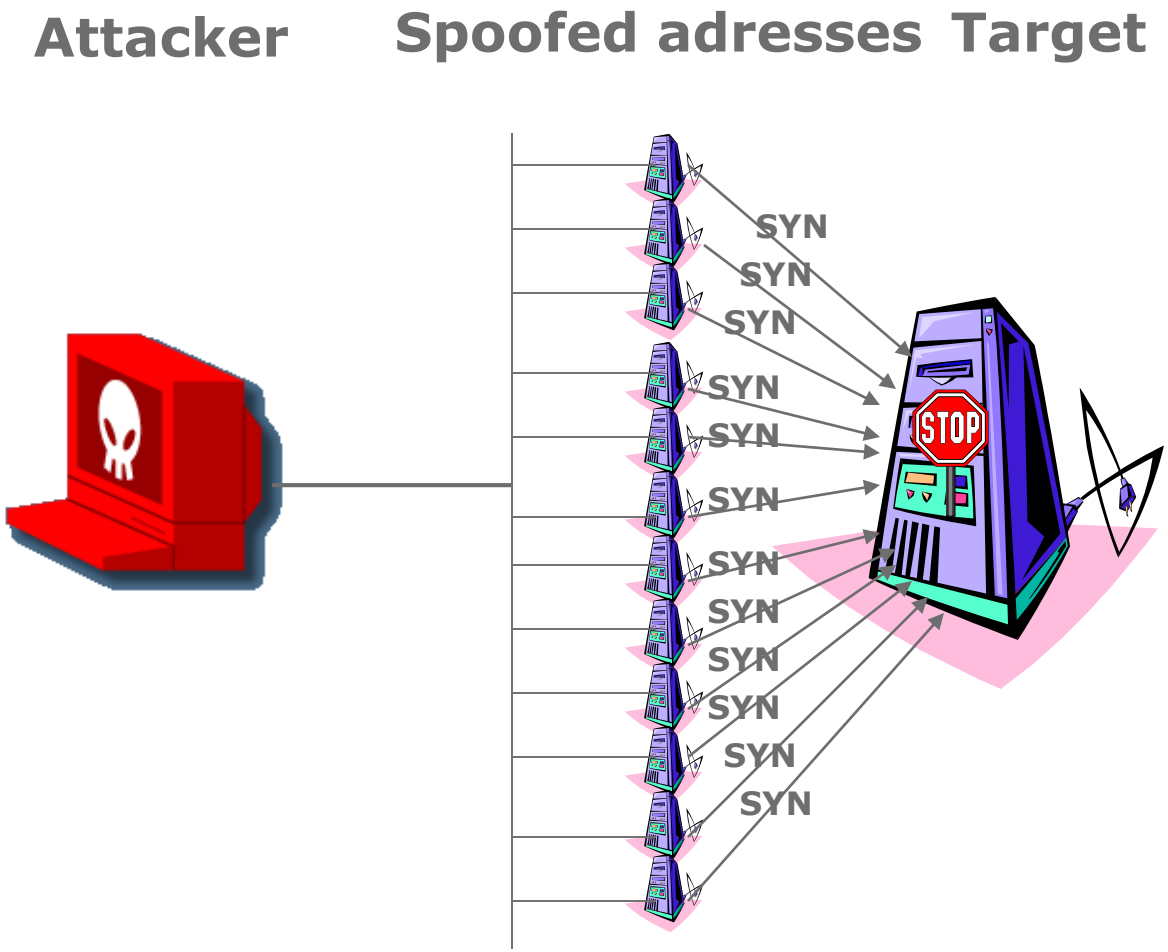
In Q1 2019, there was an increase of 967% for attacks sized 100 Gbps or higher, compared to Q1 2018

Other common flood-techniques

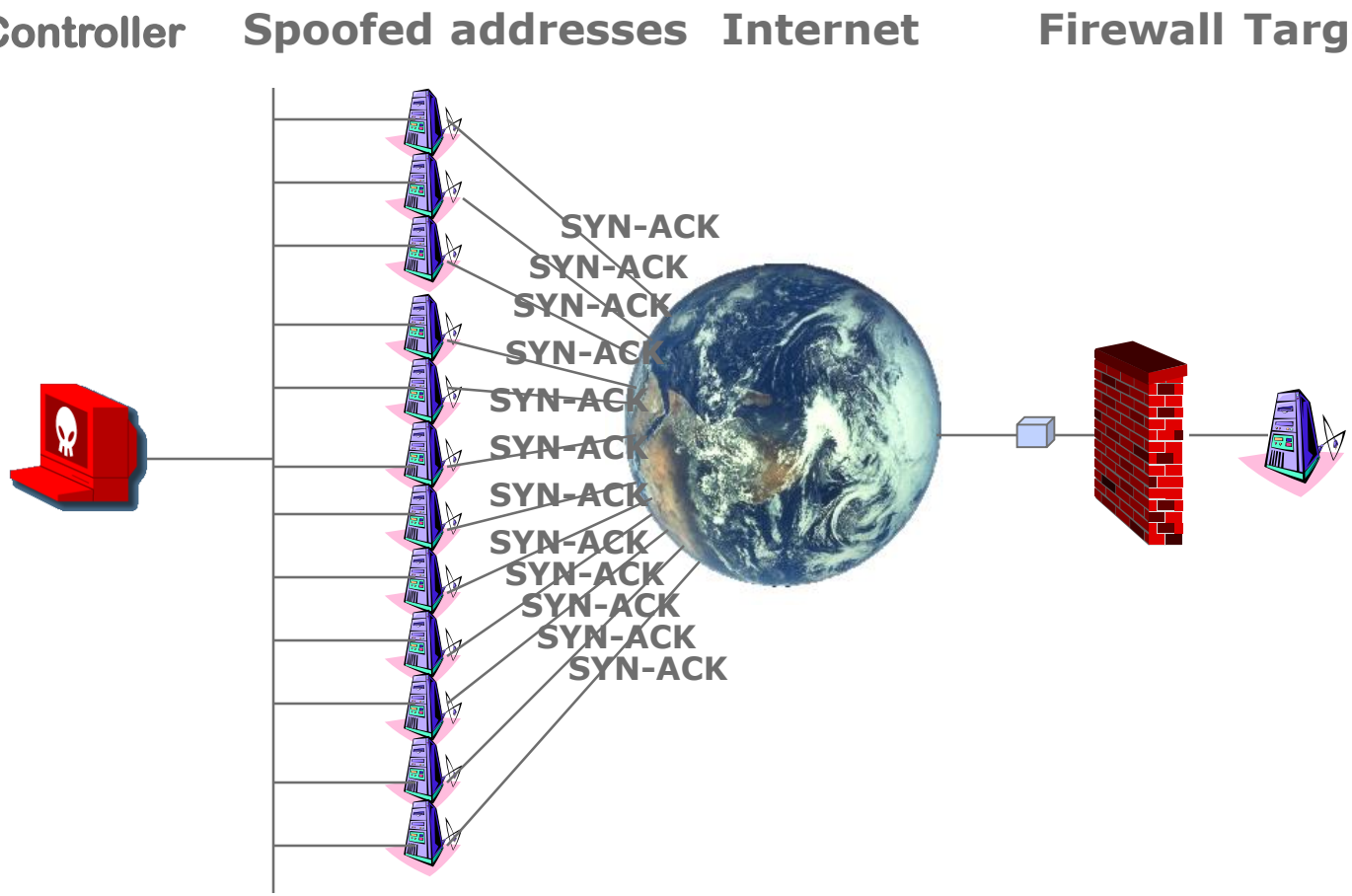
3-way handshake:



SYN-flood:


Attacker
Spoofed adresses
Target
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
STOP

Stream Attack



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.

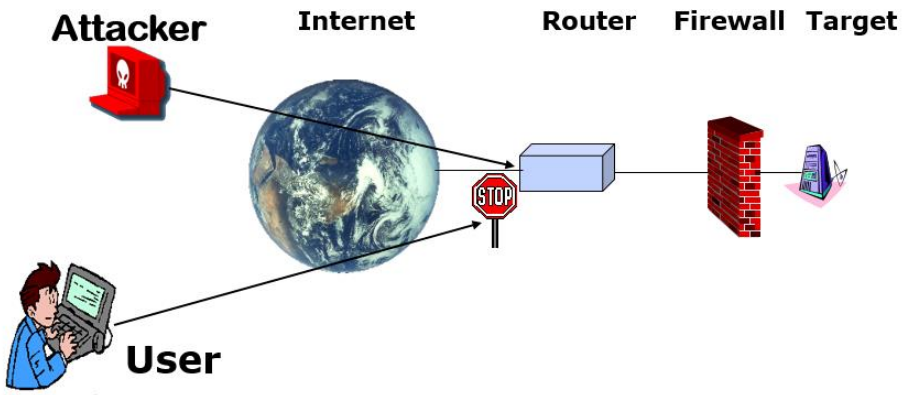
Slow Read attacks then sends packets slowly across multiple connections.

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 colateral 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

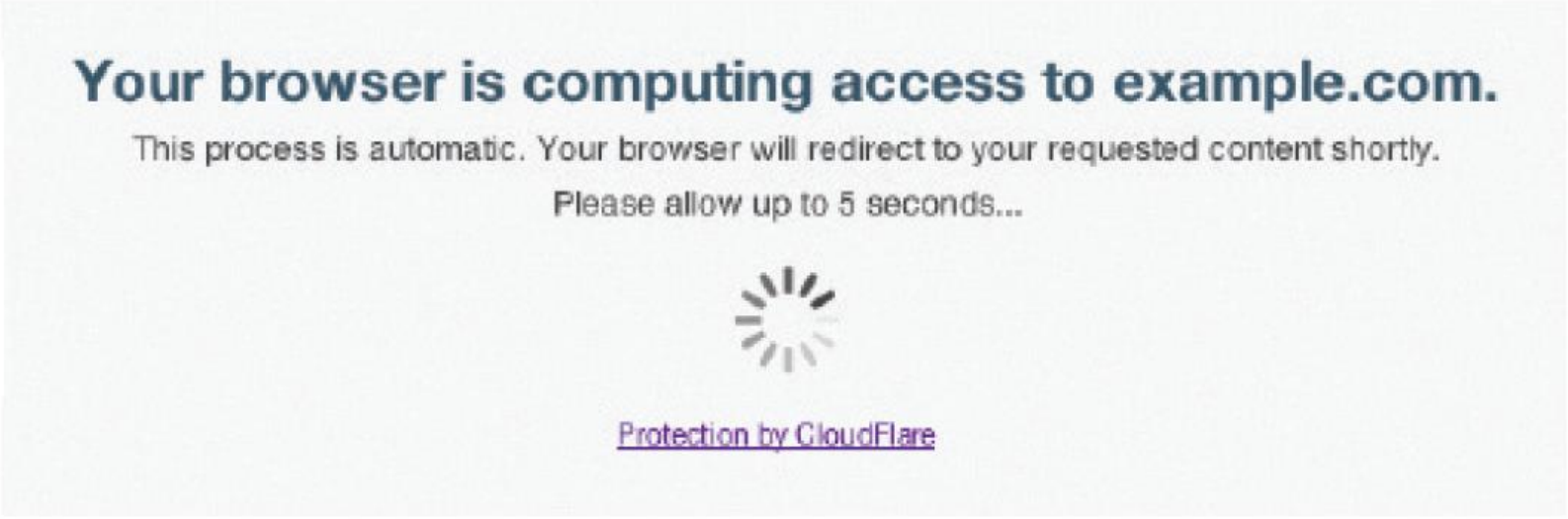
GitHub called in assistance from Akamai Prolexic, which rerouted traffic to GitHub through its "scrubbing" centers, which removed and blocked data deemed to be malicious. Following eight minutes of the assault, the attackers called it off and the DDoS stopped.

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



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

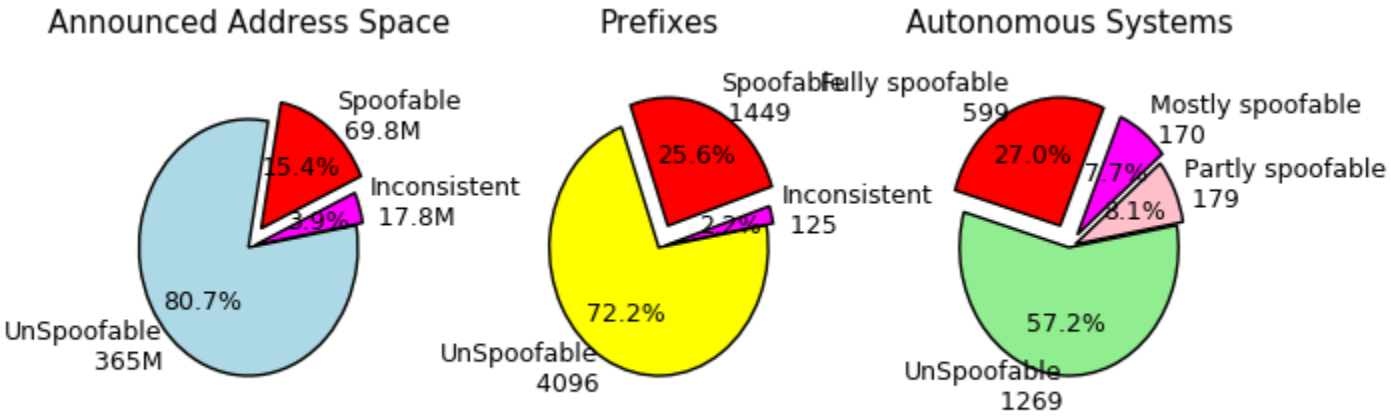
Source IP identification to block attacks at the source

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

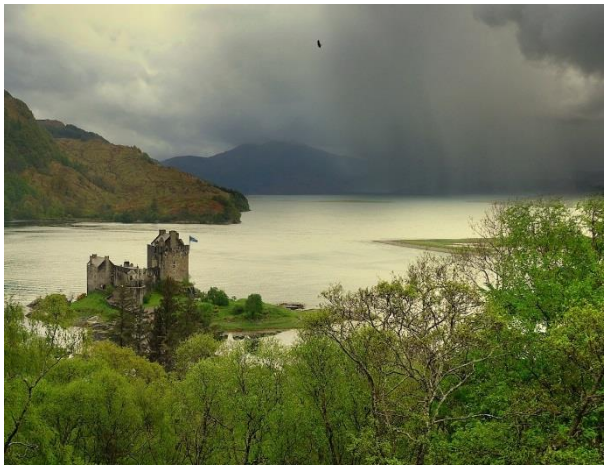


Defence

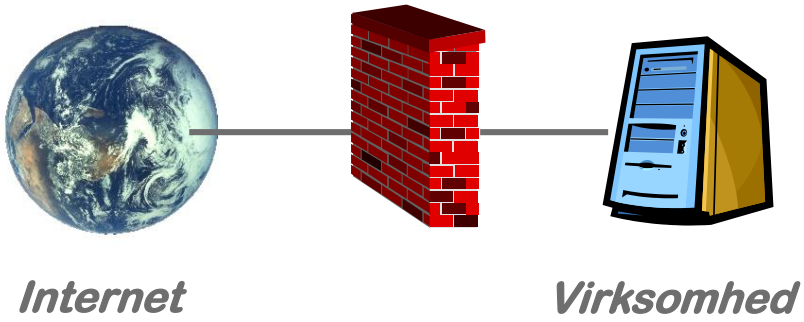
Core Internet redesign (many good proposals)

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?

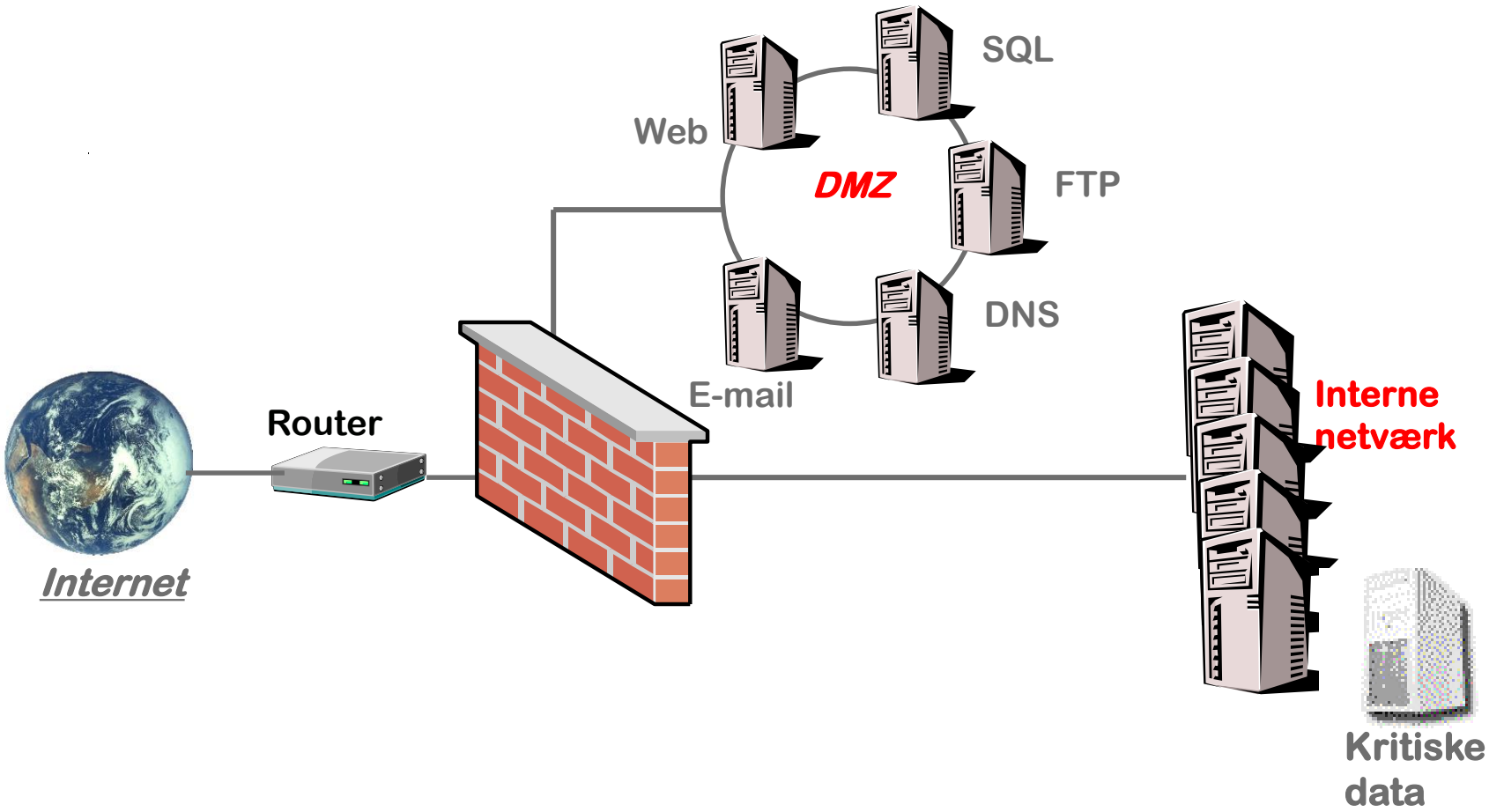
Policies can be anything and can do anything

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

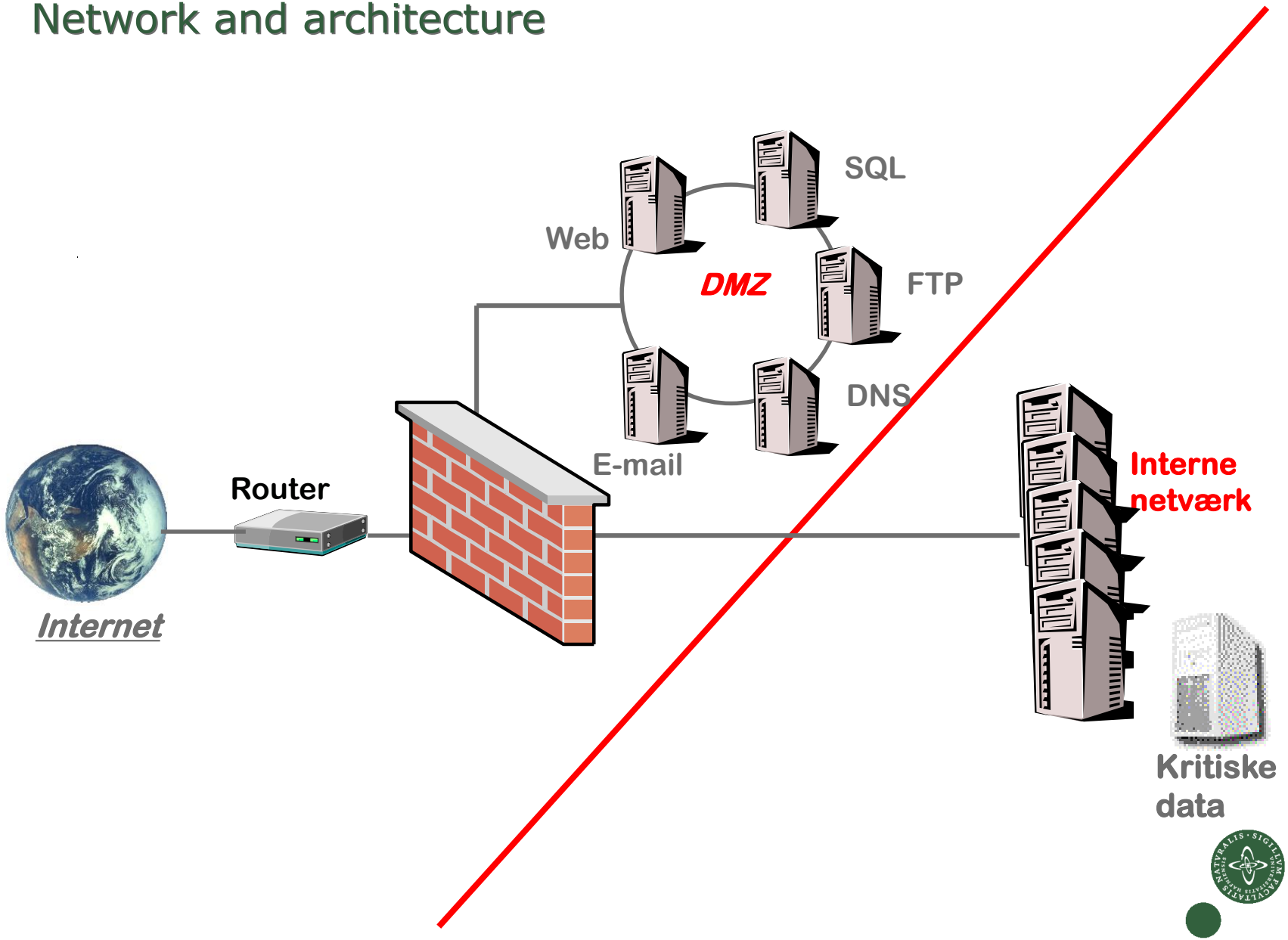
Firewall typer

- **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**

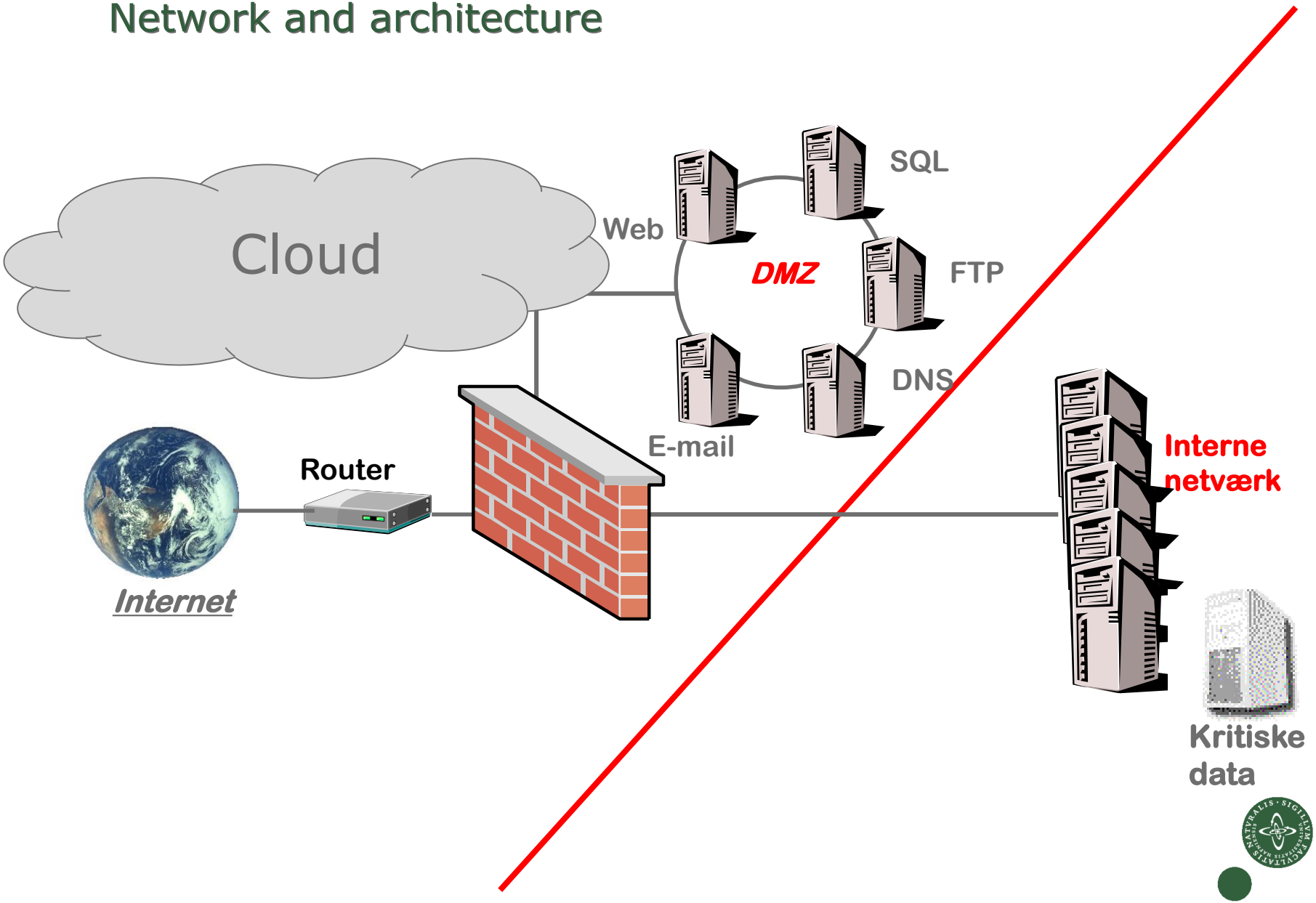
Network and architecture



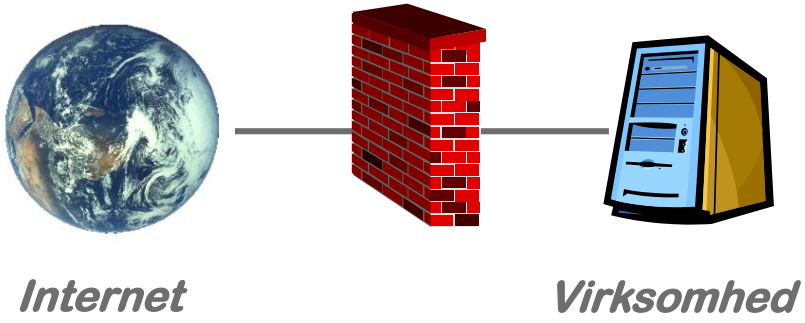
Network and architecture



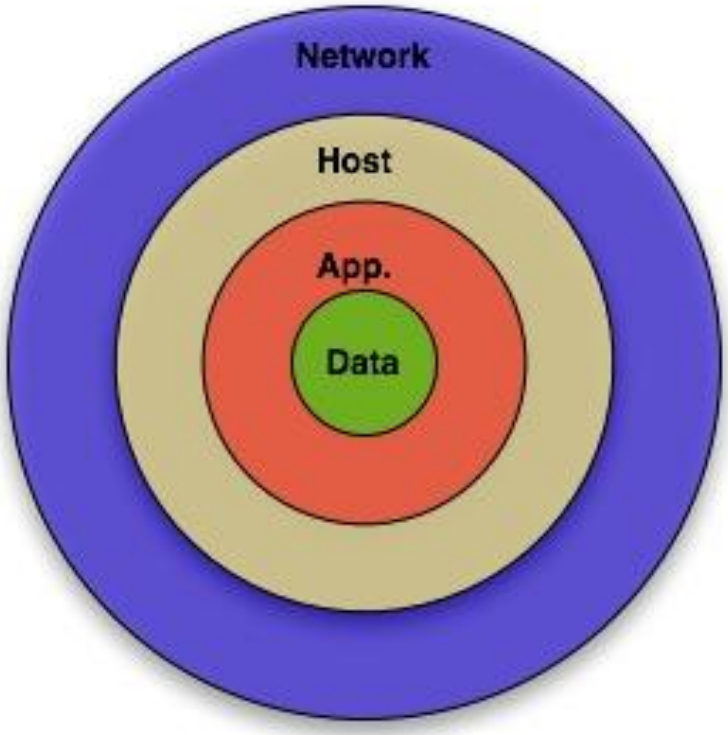
Network and architecture



Opening ports in the firewall



After opening?



Defense in Depth

Remember your risk assessment basics

Eliminate/Mitigate

Minimize (compensate)

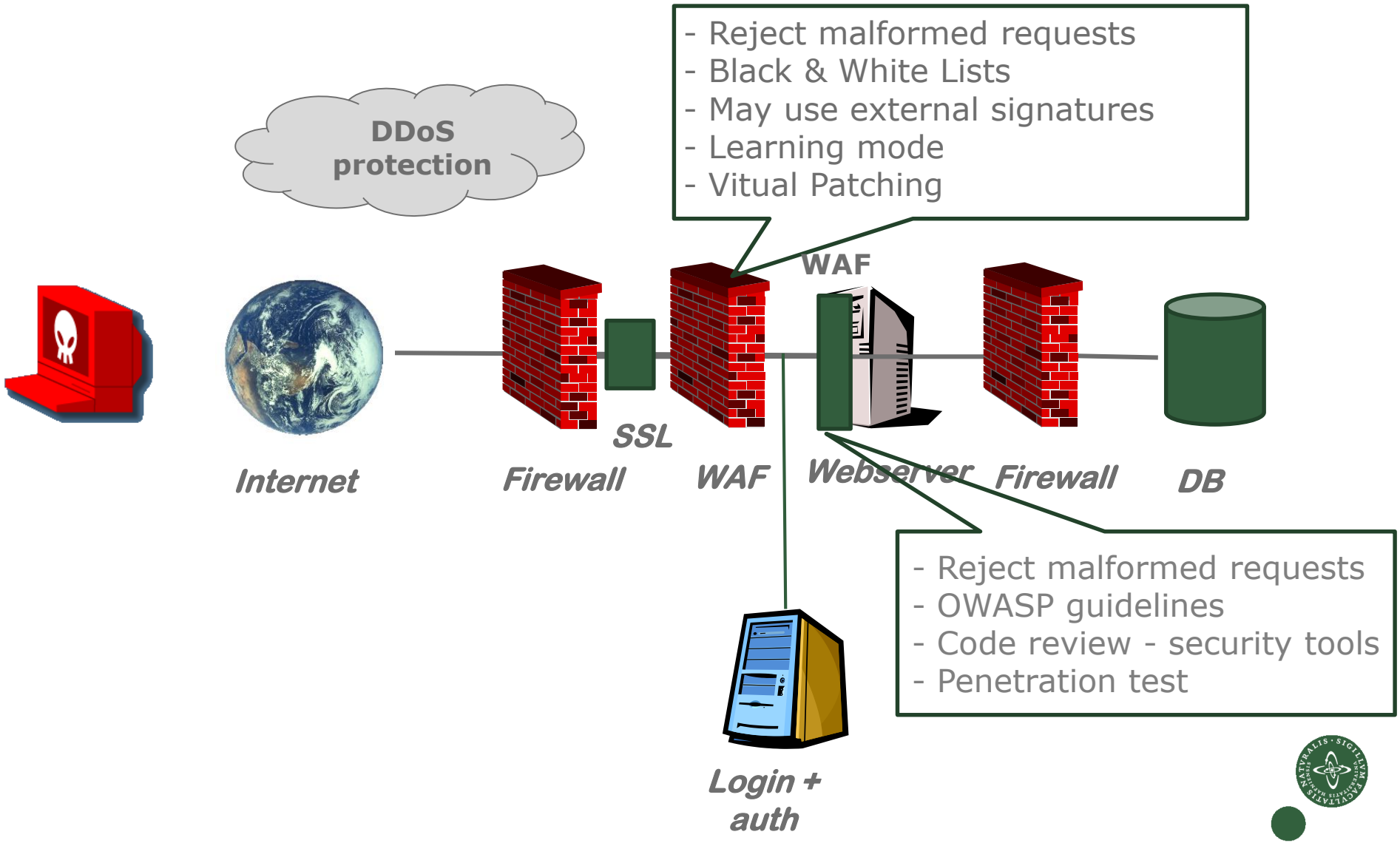
Transfer

Accept

~~Ignore~~

Prevent – Detect - Respond

Layers of security and the firewall



Which is “Best”?

Threat modeling – the 5 questions

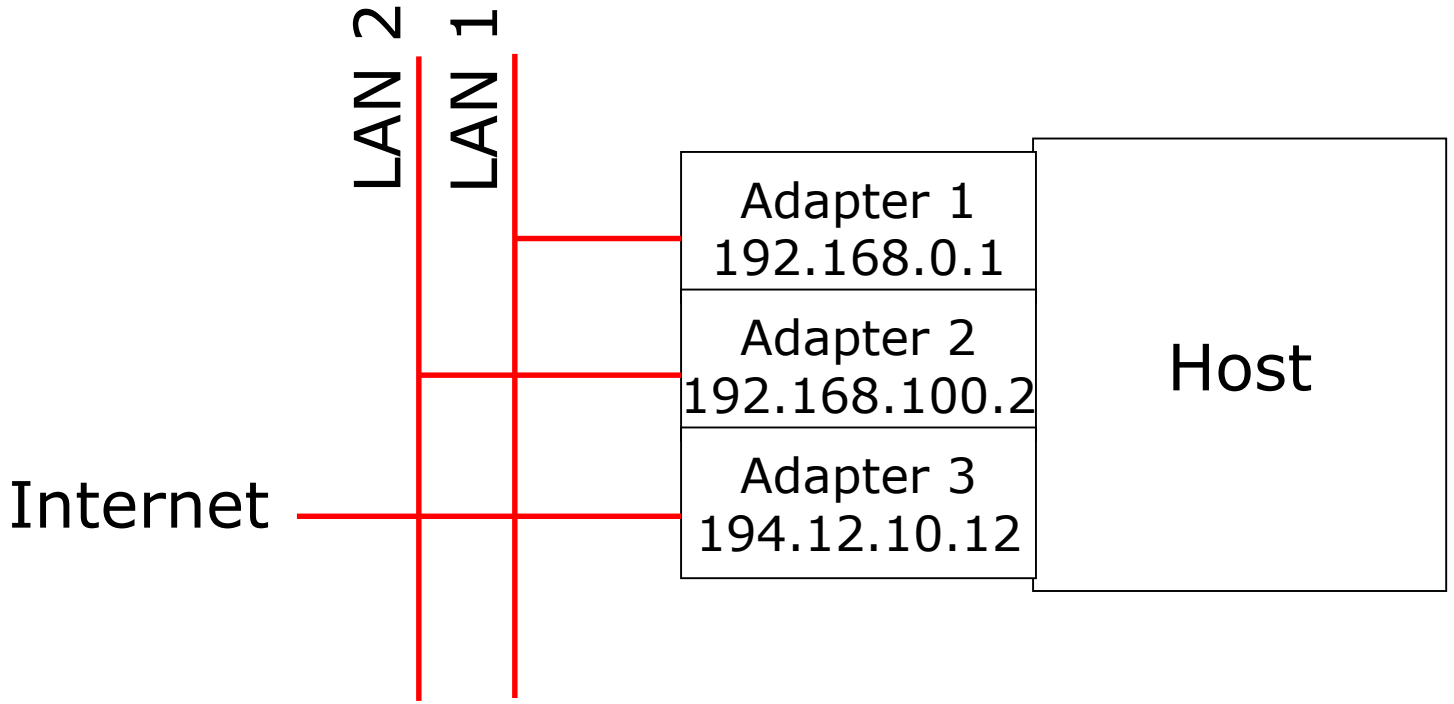
1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent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

Ports and firewalls

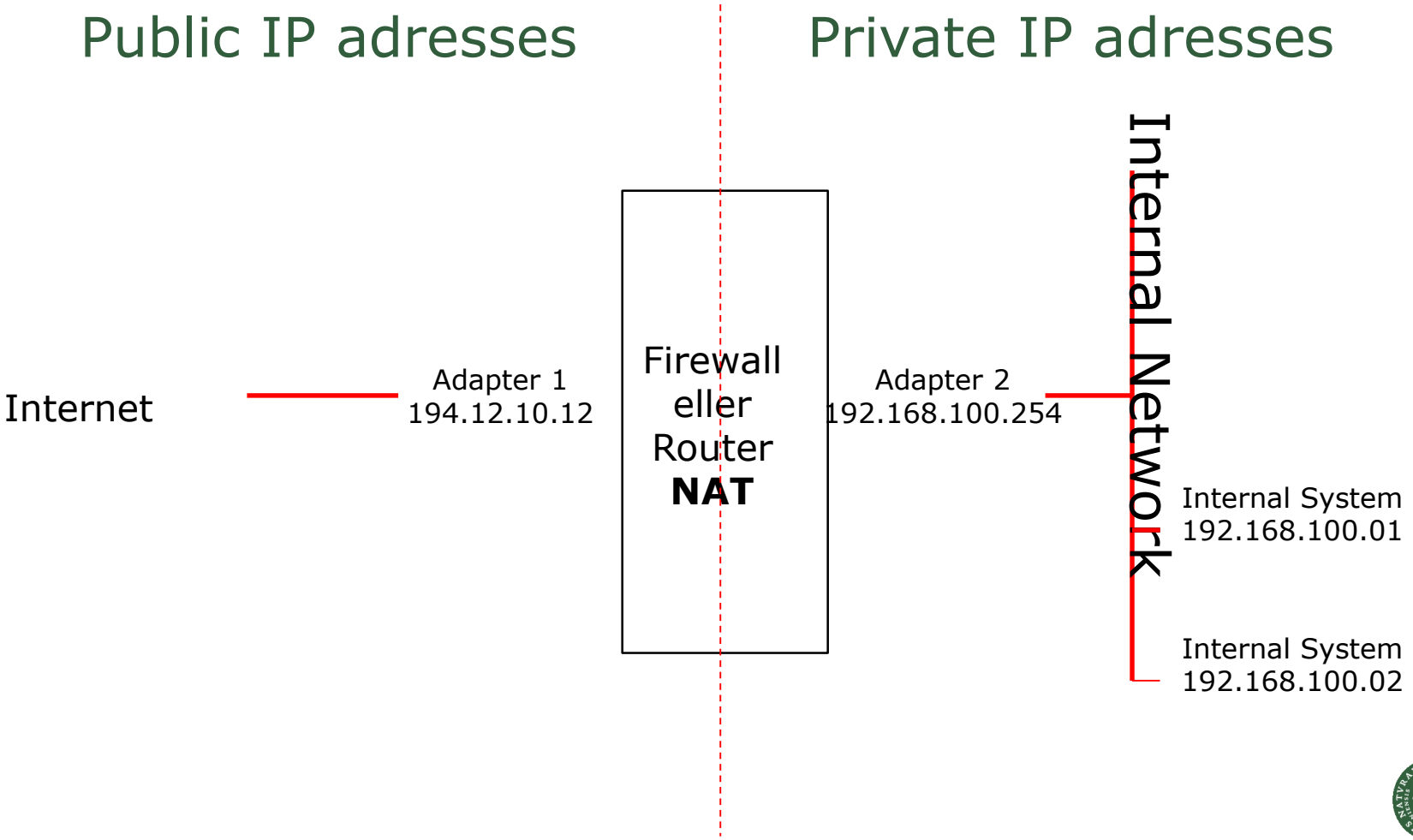
Firewalls

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: Registred 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

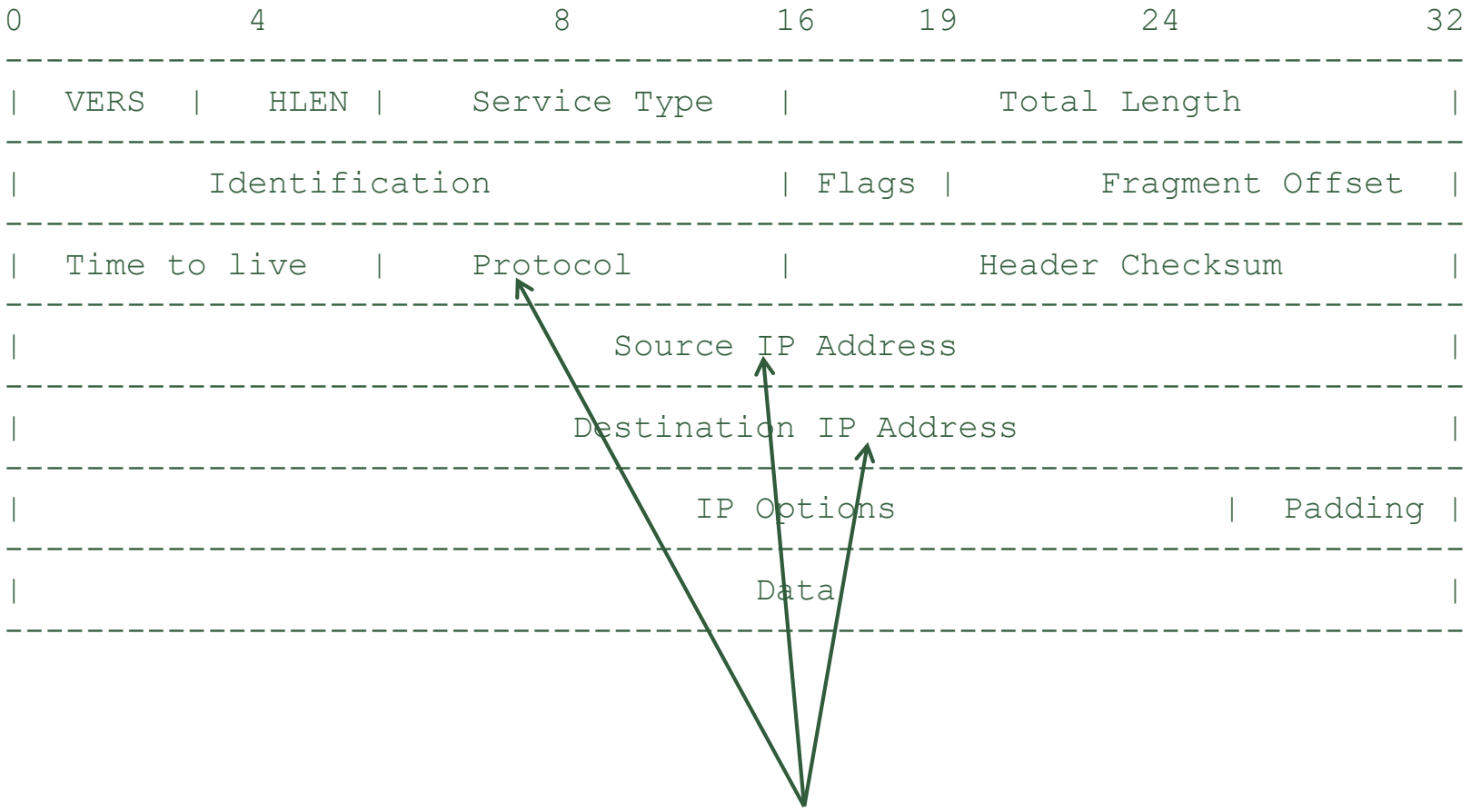
Service	Port	Protocol
FTP	21	TCP
Telnet	23	TCP
Simple Mail Transfer Protocol (SMTP)	25	TCP
Domain Name	53	UDP
HTTP (web server)	80	TCP
POP3 (mail box)	110	TCP
NetBios loc-srv	135	TCP
NetBios Name	137	TCP
NetBios Datagram	138	TCP
NetBios Session	139	TCP

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.

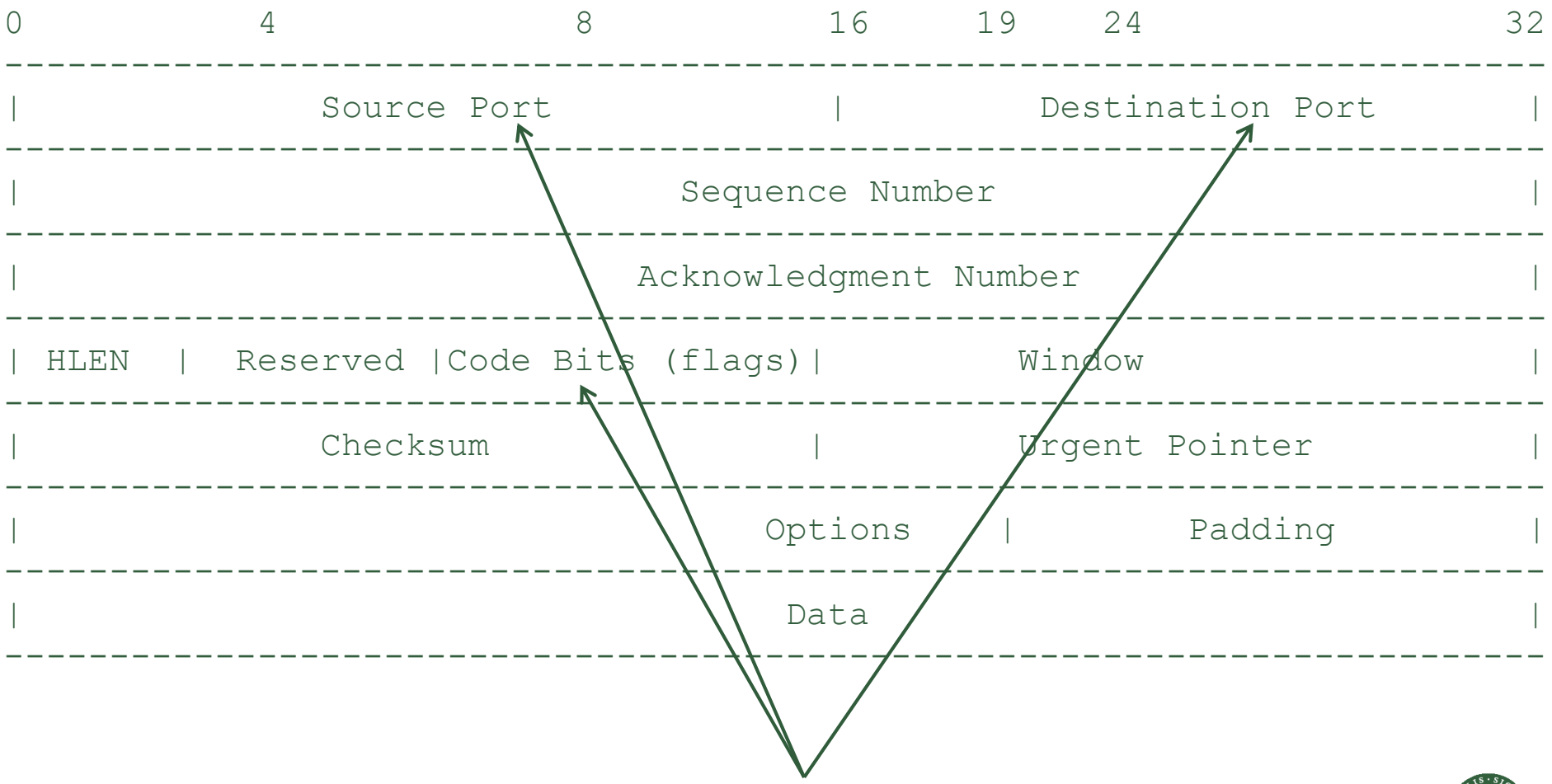
TCP - Transmission Control Protocol

IP Header



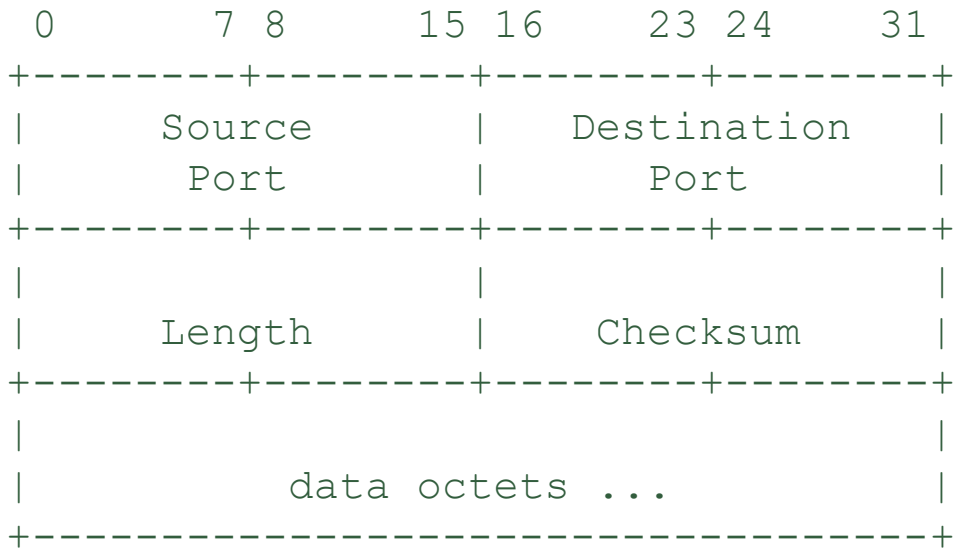
Typiske felter for filtrering

TCP Header



Typiske felter for filtrering

UDP header


0 7 8 15 16 23 24 31
Source Port
Destination Port
Length
Checksum
data octets ...

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

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

iptables -F INPUT *(flush)*

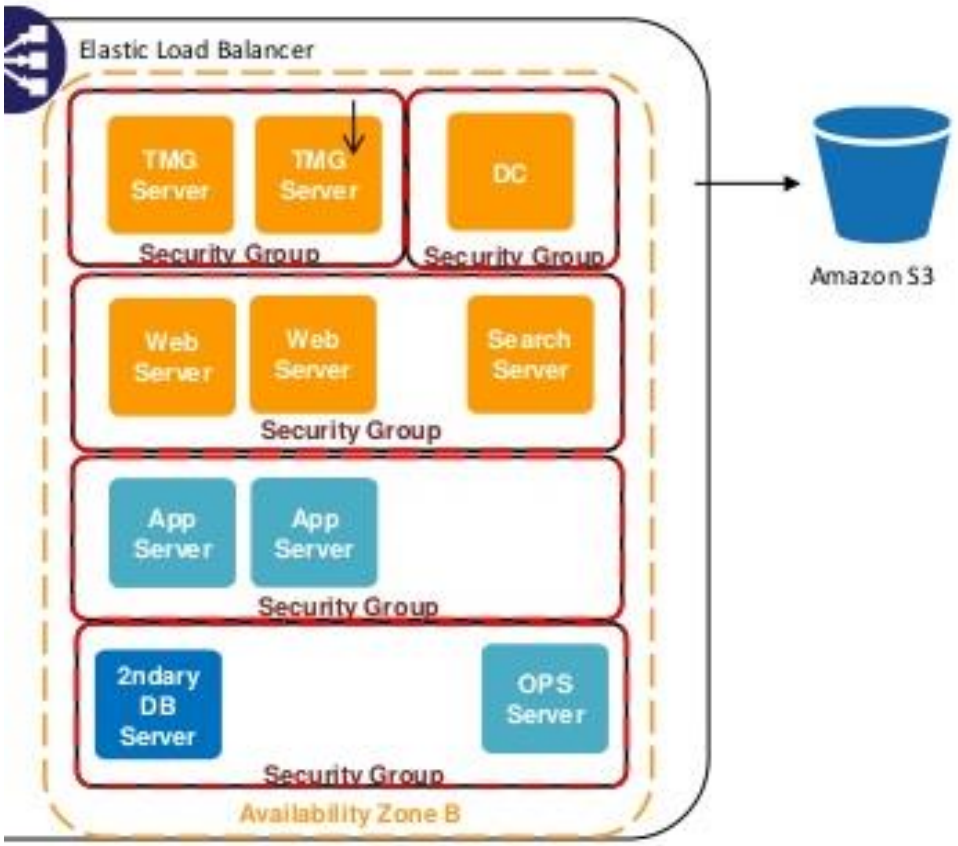
iptables -A INPUT -i eth0 -j DROP *(append)*

Firewalls and Security Groups

Security Groups

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

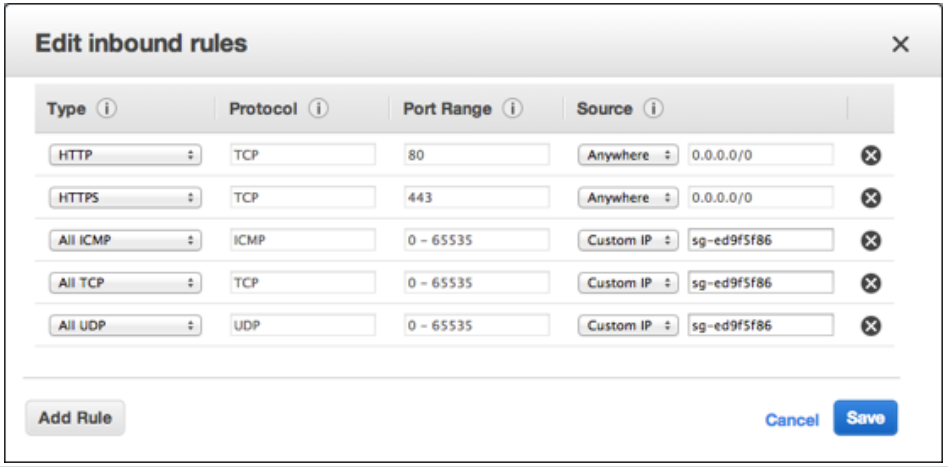
A Security Group is a container for security group rules. Works as firewalls – isolating traffic to VMs, controlling traffic to and from ports and instances



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

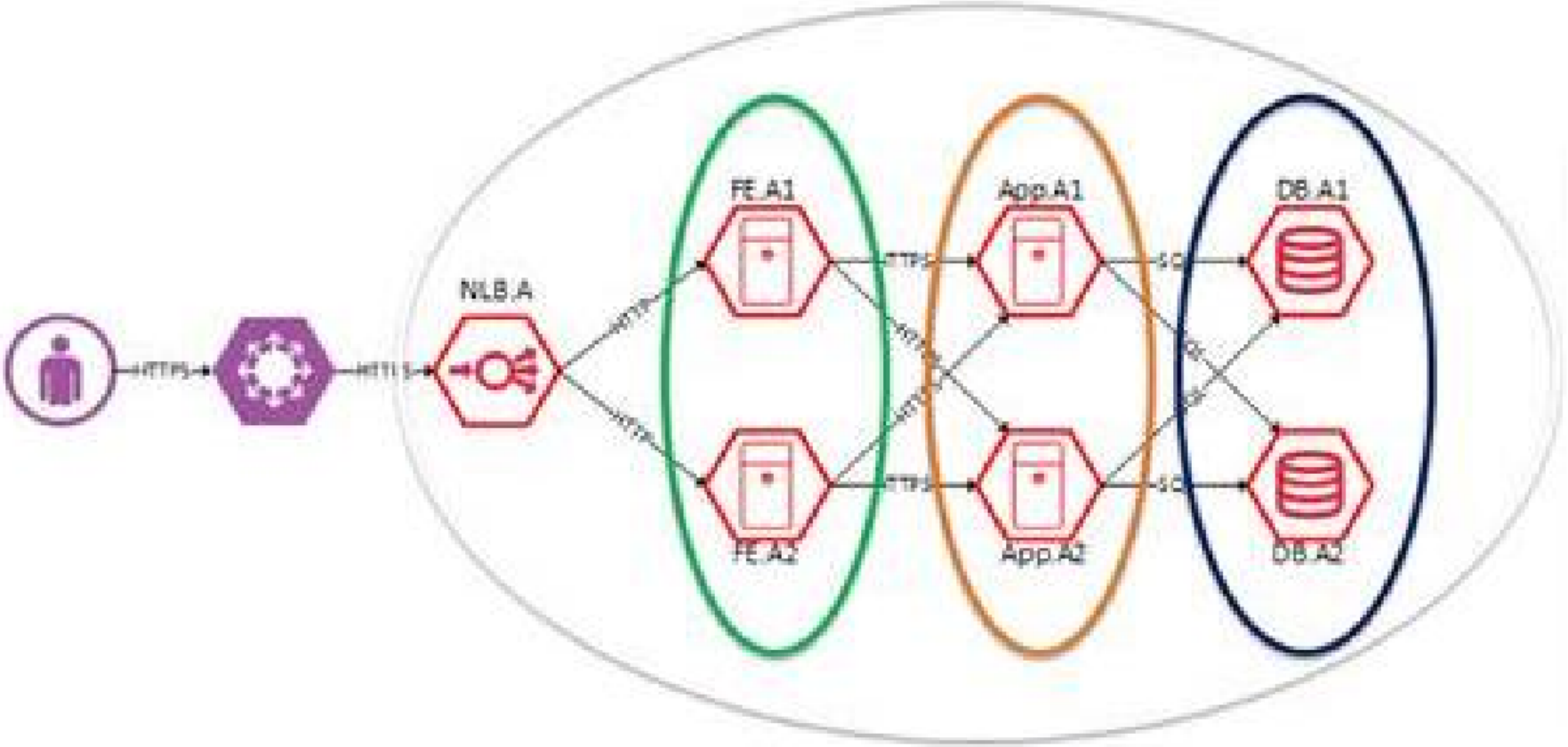
Instances in a Security Group cannot communicate with other instances unless specifically allowed.

"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.

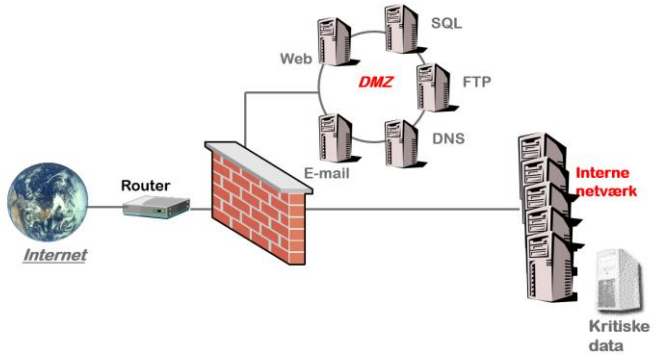
Security Groups should not allow any form of internet access outside the webserver group). Administrative access should be limited to known IP-addresses such as jump servers or own internal IP-addresses

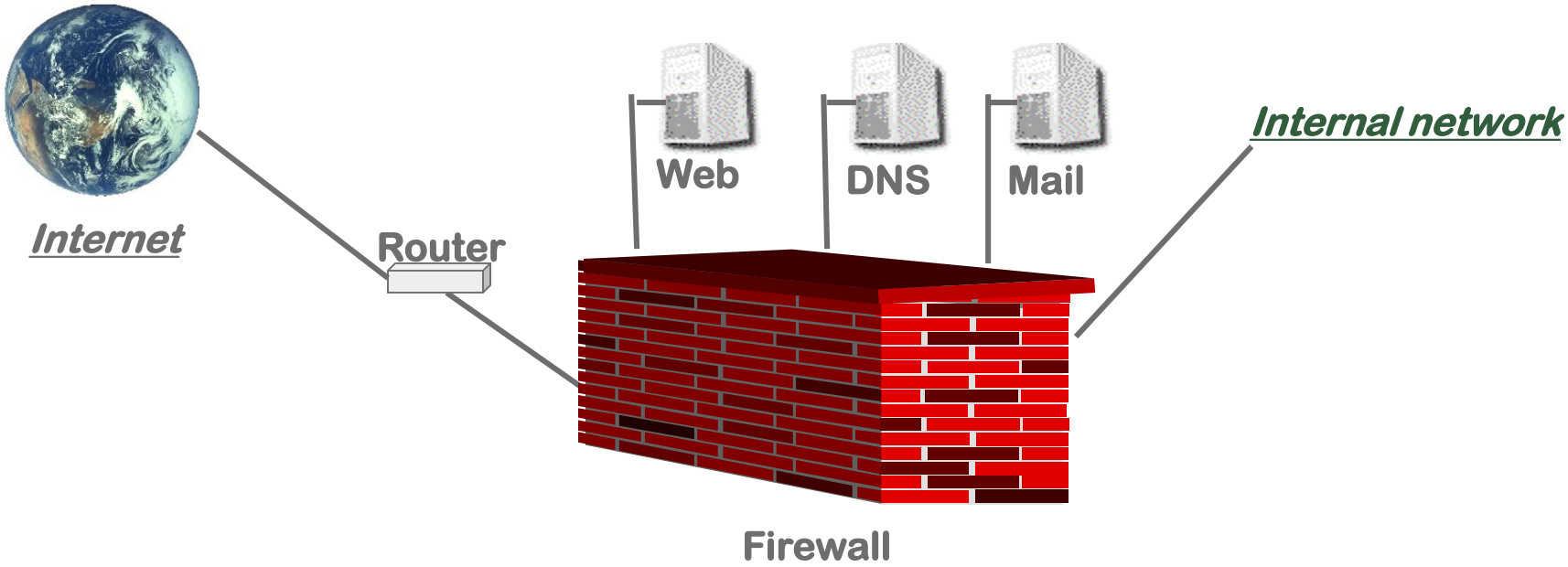
Pause


SECURITY CHECK
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!

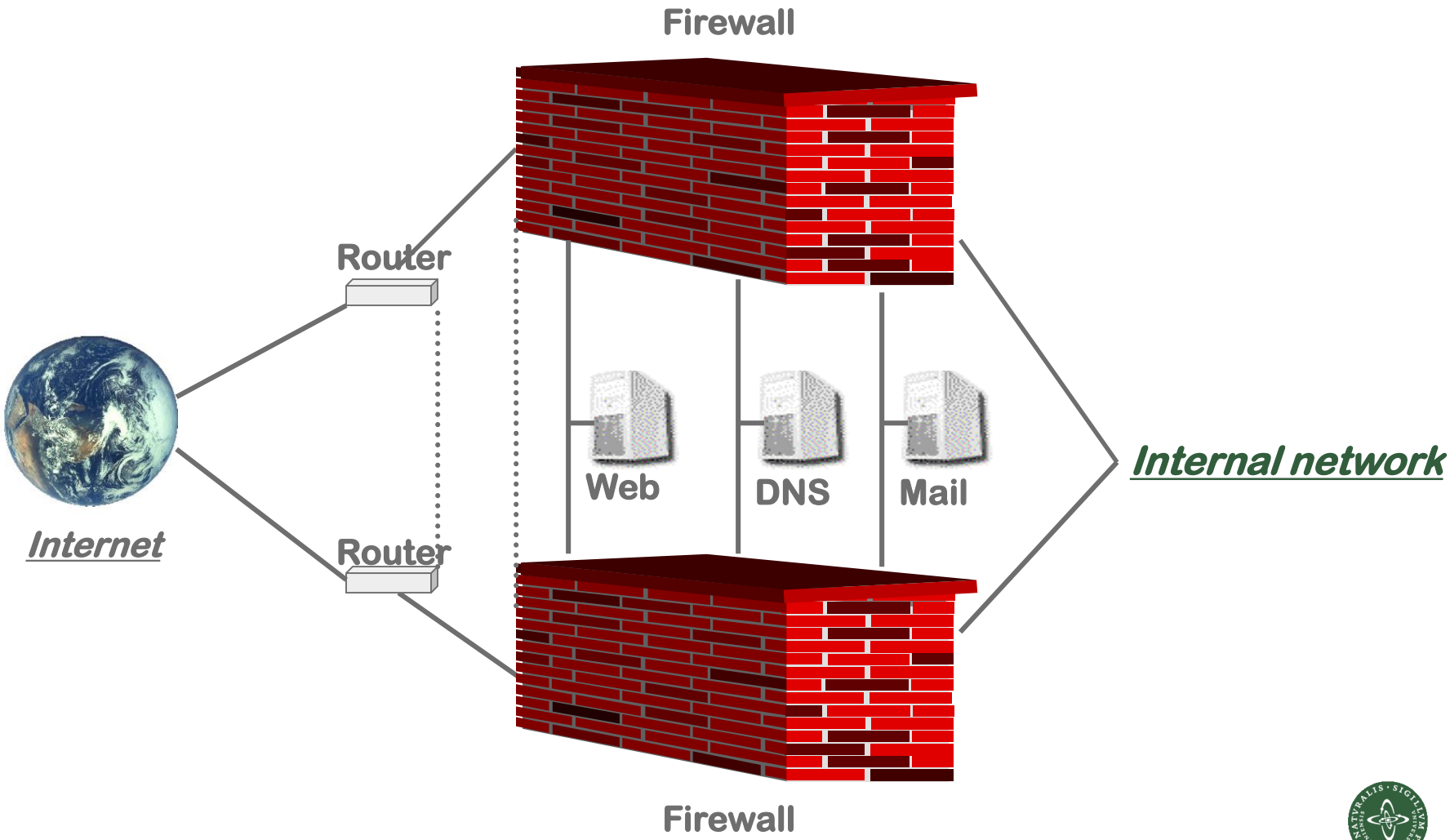
Classic security measures

Multiple DMZ

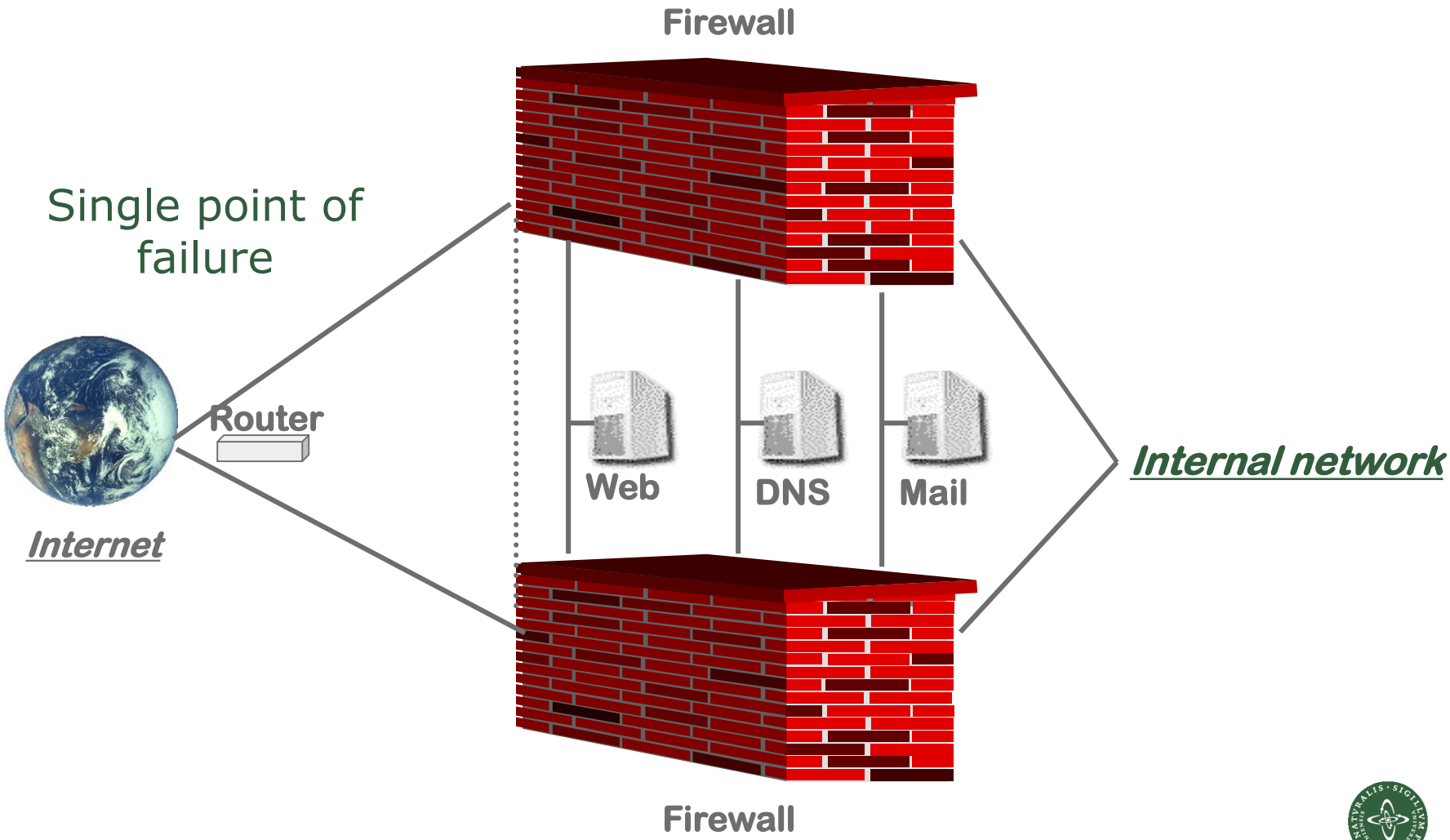




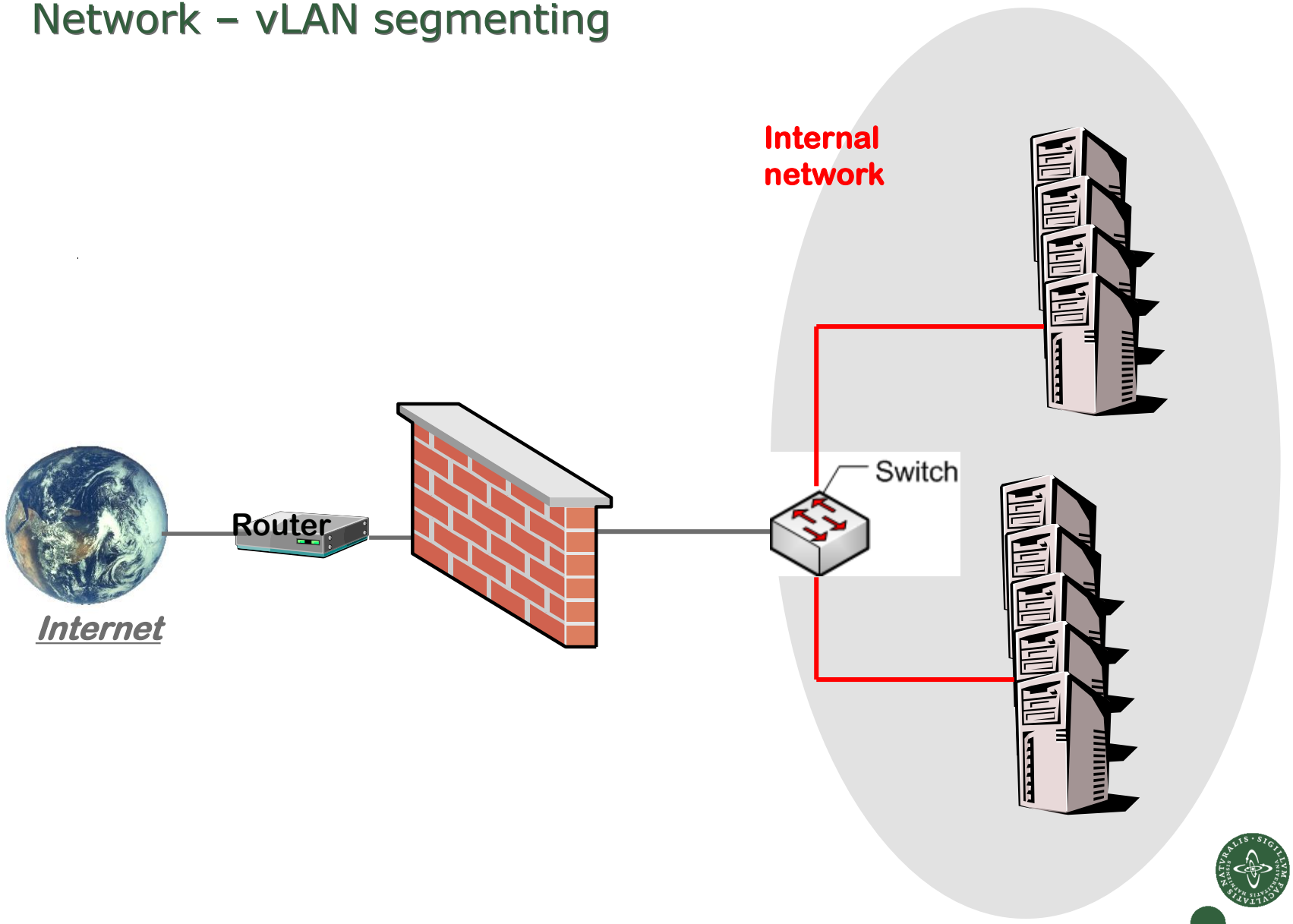
Multiple firewalls



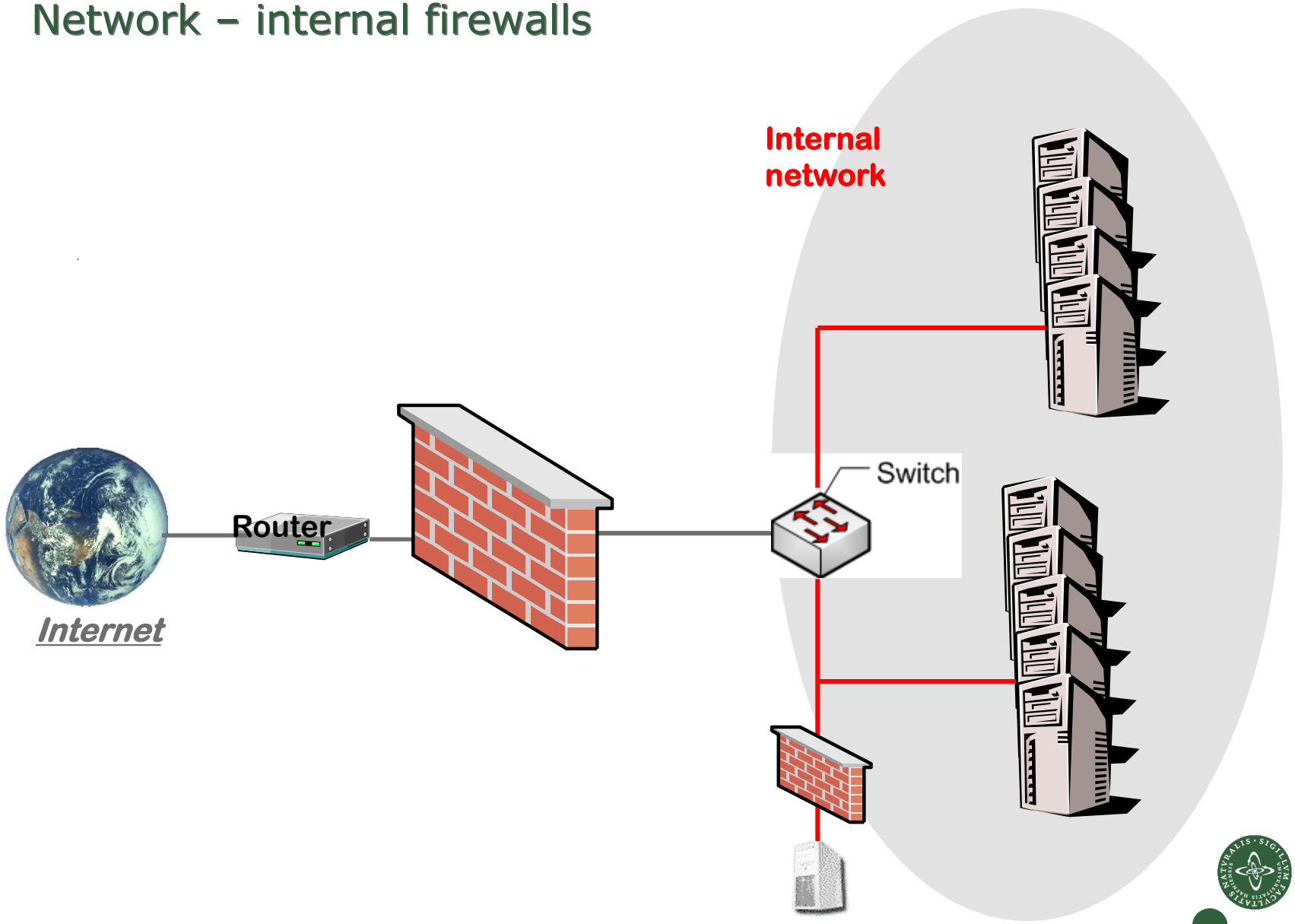
Multiple firewalls



Network – vLAN segmenting



Network – internal firewalls



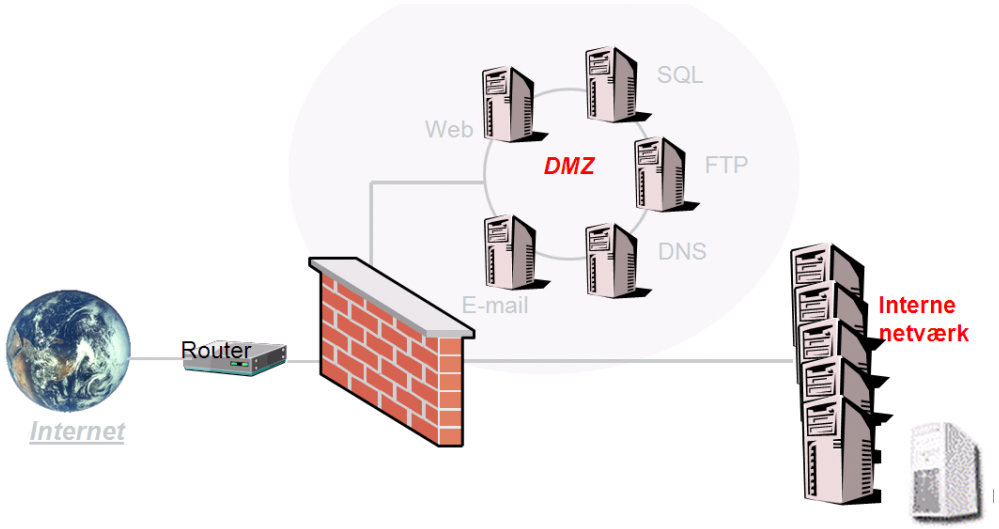
Intrusion Detection Systems (IDS)
Intrusion Protection Systems (IPS)

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

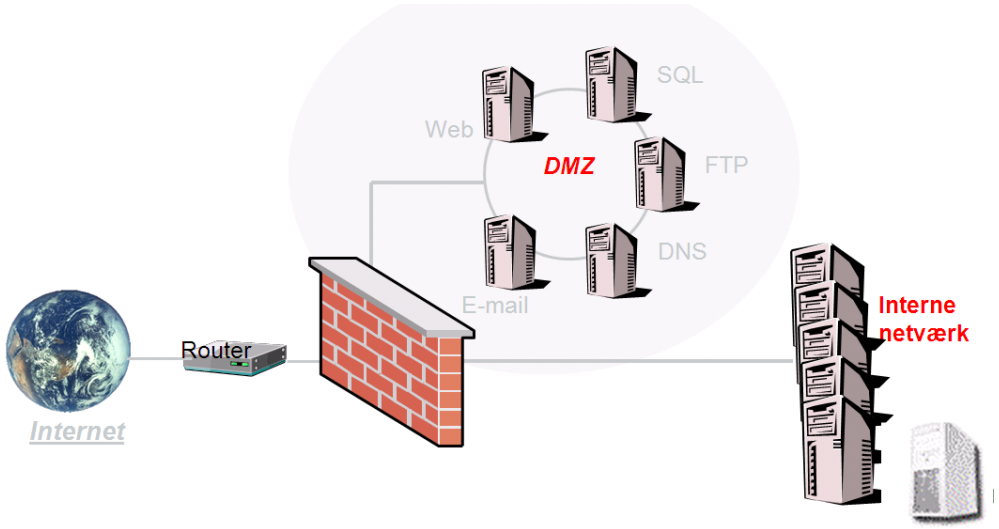
- IDS/IPS
- Scanning for virus and webtraffic
- Central loghost
- Many DMZ's
- VLAN, internal firewalls, segmentation
- DDoS protection
- …



Prevent – Detect - Respond

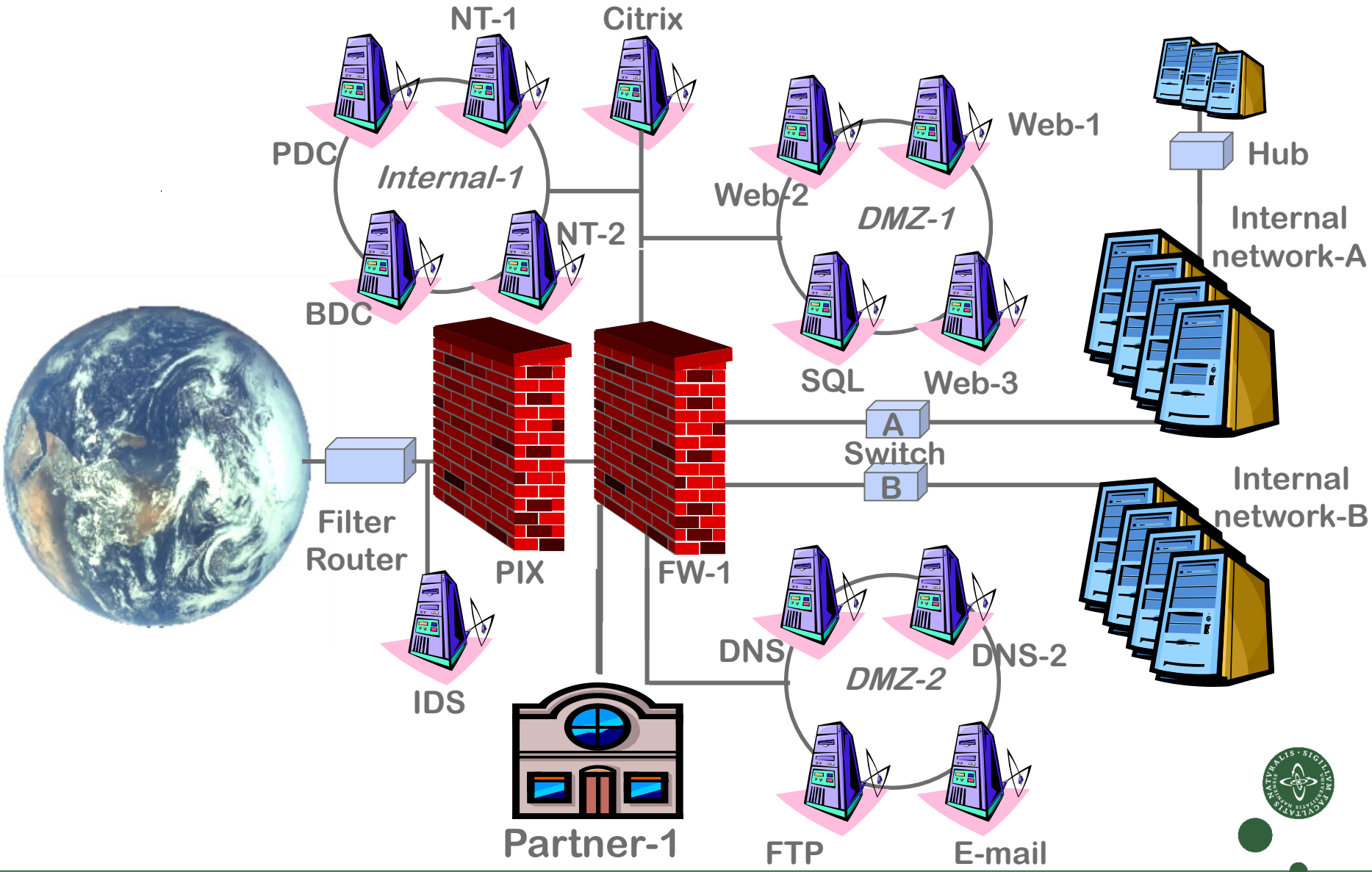
More examples of security measures

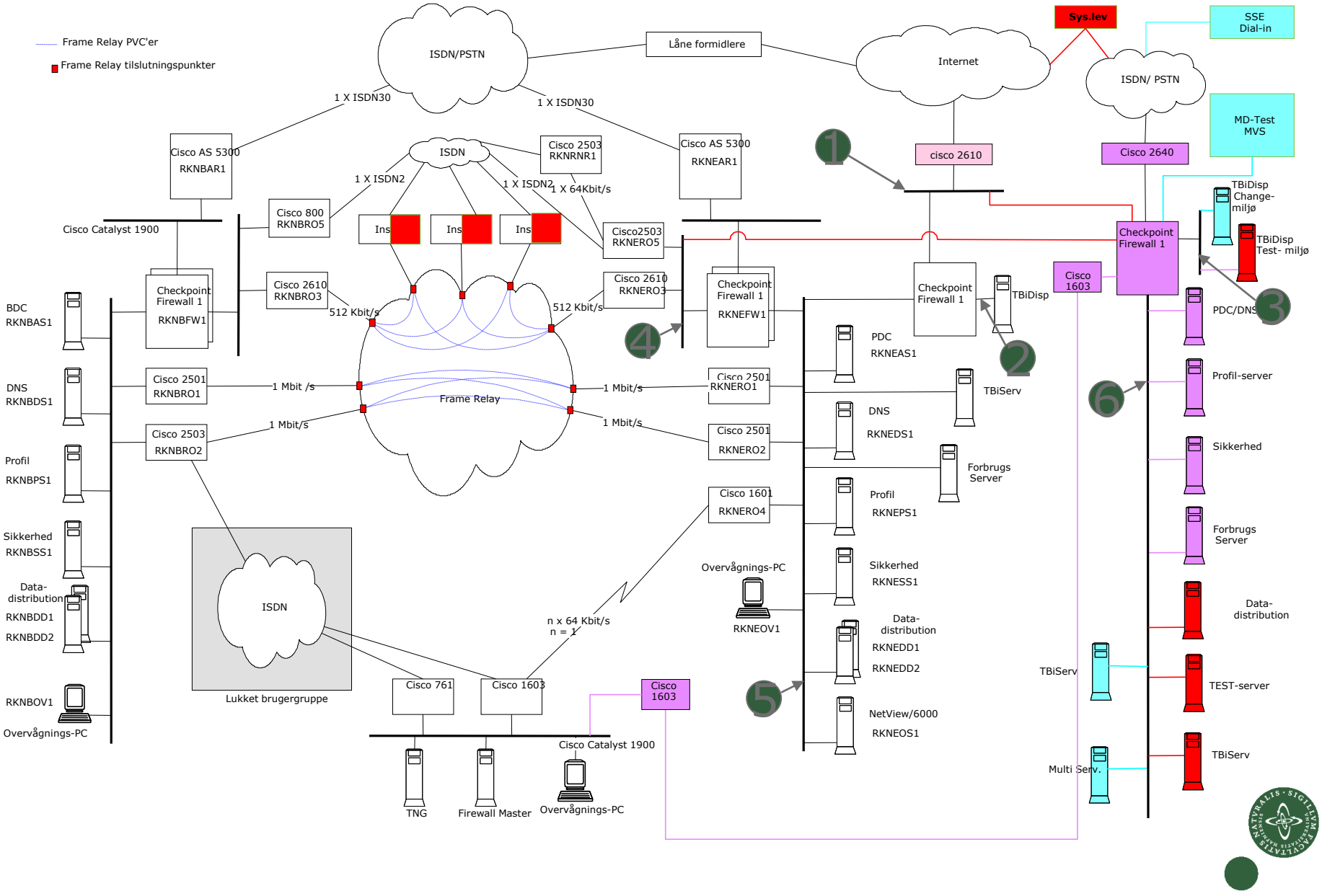
- Patching/updating
- Configuration management
- Filtering outgoing traffic
- Minimizing number of services (hardening)
- Whitelist/blacklist
- …



Prevent – Detect - Respond

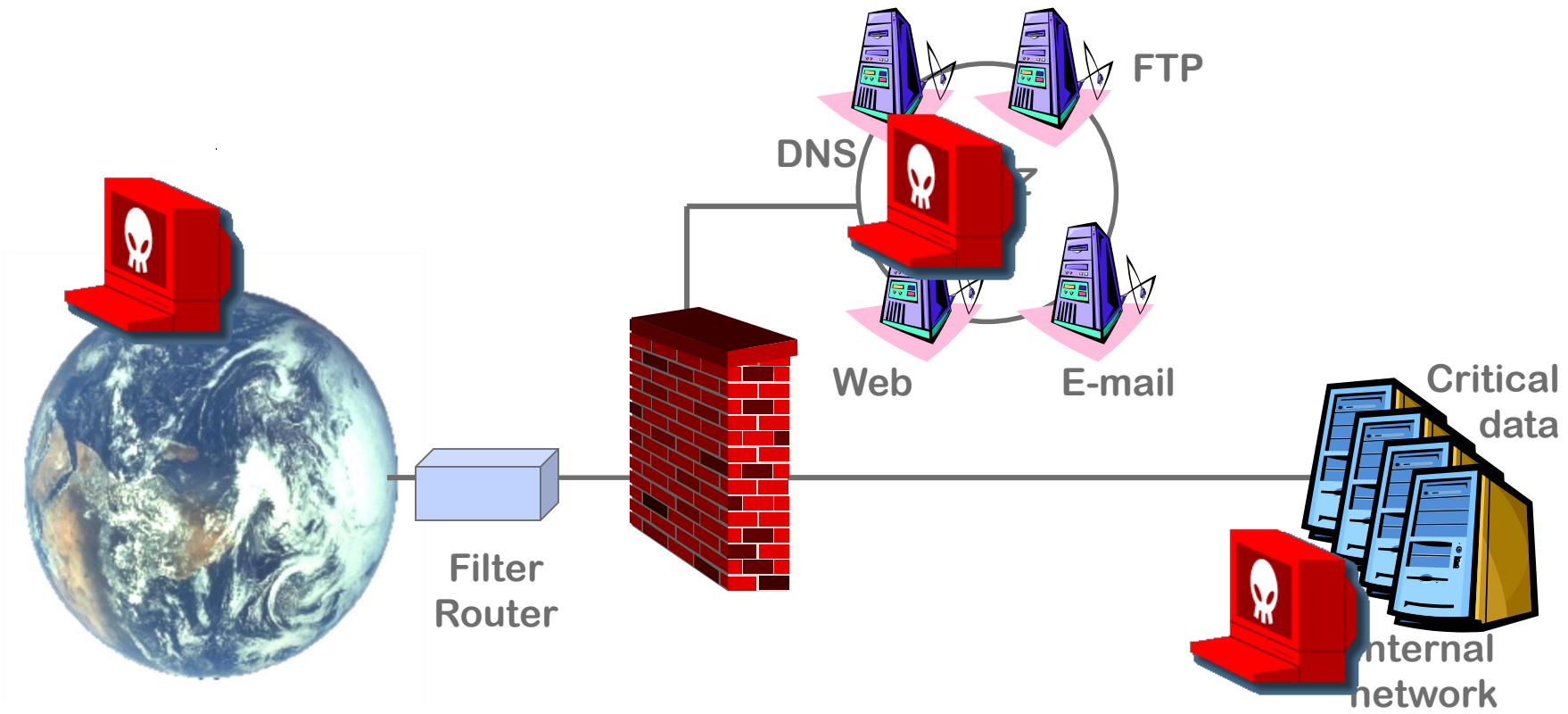
Large network (example)



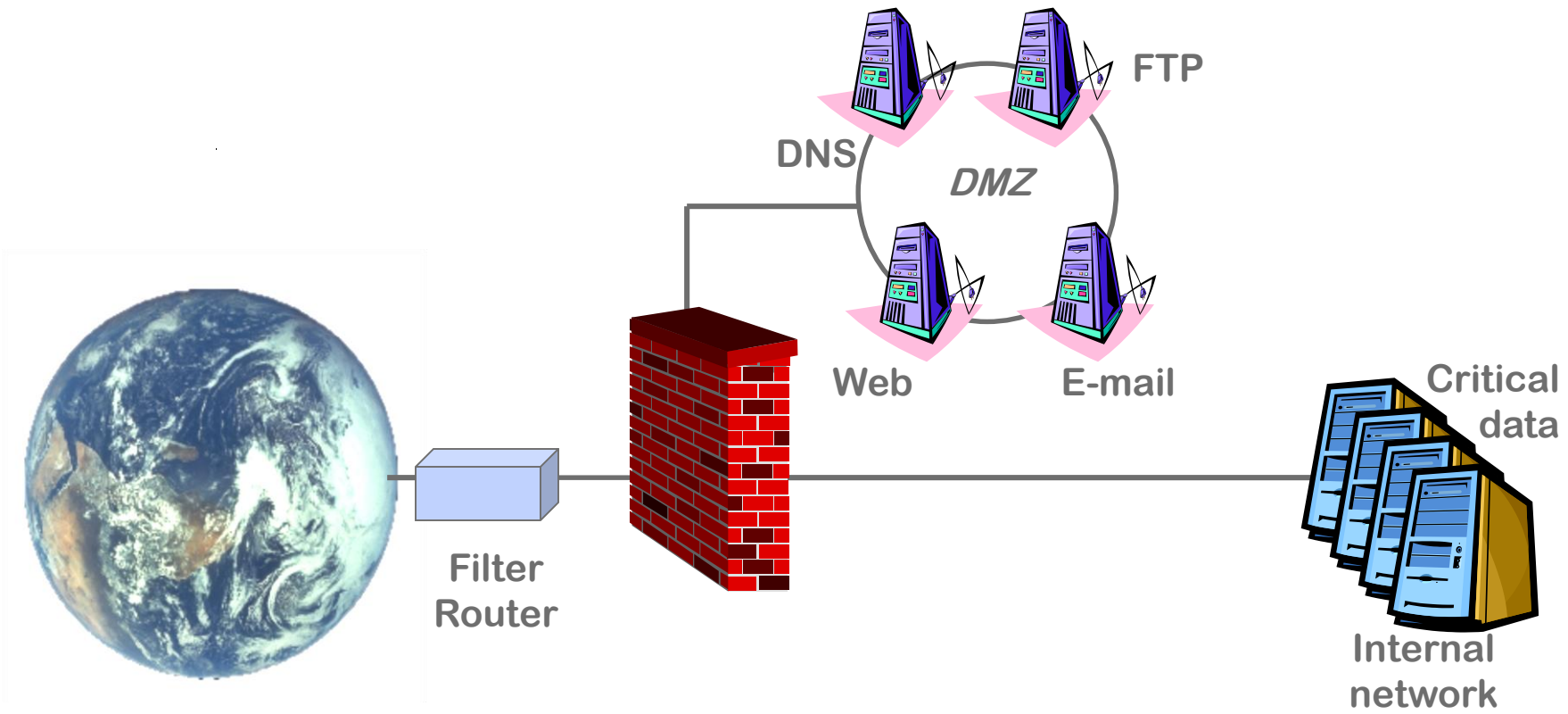

Frame Relay PVC'er
Frame Relay tilslutningspunkter
ISDN/PSTN
Låne formidlere
Internet
Sys.lev
SSE
Dial-in
ISDN/ PSTN
MD-Test
MVS
1 X ISDN30
1 X ISDN30
Cisco AS 5300
RKNBAR1
ISDN
Cisco 2503
RKNRNR1
Cisco AS 5300
RKNEAR1
cisco 2610
Cisco 2640
1 X ISDN2
1 X ISDN2
1 X 64Kbit/s
TBiDisp
Change-
miljø
TBiDisp
Test- miljø
Cisco Catalyst 1900
Cisco 800
RKNBRO5
Cisco2503
RKNERO5
Checkpoint
Firewall 1
Cisco
1603
Checkpoint
Firewall 1
BDC
RKNBAS1
Checkpoint
Firewall 1
RKNBFW1
Cisco 2610
RKNBRO3
512 Kbit/s
512 Kbit/s
Cisco 2610
RKNERO3
Checkpoint
Firewall 1
RKNEFW1
Checkpoint
Firewall 1
TBiDisp
PDC/DNS
PDC
RKNEAS1
DNS
RKNBDS1
Cisco 2501
RKNBRO1
1 Mbit /s
Frame Relay
1 Mbit/s
Cisco 2501
RKNERO1
TBiServ
Profil-server
DNS
RKNEDS1
Profil
RKNBPS1
Cisco 2503
RKNBRO2
1 Mbit/s
1 Mbit/s
Cisco 2501
RKNERO2
Forbrugs
Server
Sikkerhed
Profil
RKNEPS1
Sikkerhed
RKNBSS1
Cisco 1601
RKNERO4
Forbrugs
Server
Overvågnings-PC
Sikkerhed
RKNESS1
Data-
distribution
RKNBDD1
RKNBDD2
ISDN
Data-
distribution
RKNEDD1
RKNEDD2
Data-
distribution
n x 64 Kbit/s
n = 1
RKNEOV1
TBiServ
TEST-server
RKNBOV1
Overvågnings-PC
Lukket brugergruppe
Cisco 761
Cisco 1603
Cisco
1603
NetView/6000
RKNEOS1
Cisco Catalyst 1900
Multi Serv.
TBiServ
TNG
Firewall Master
Overvågnings-PC

Common security issues

3 major areas of attack



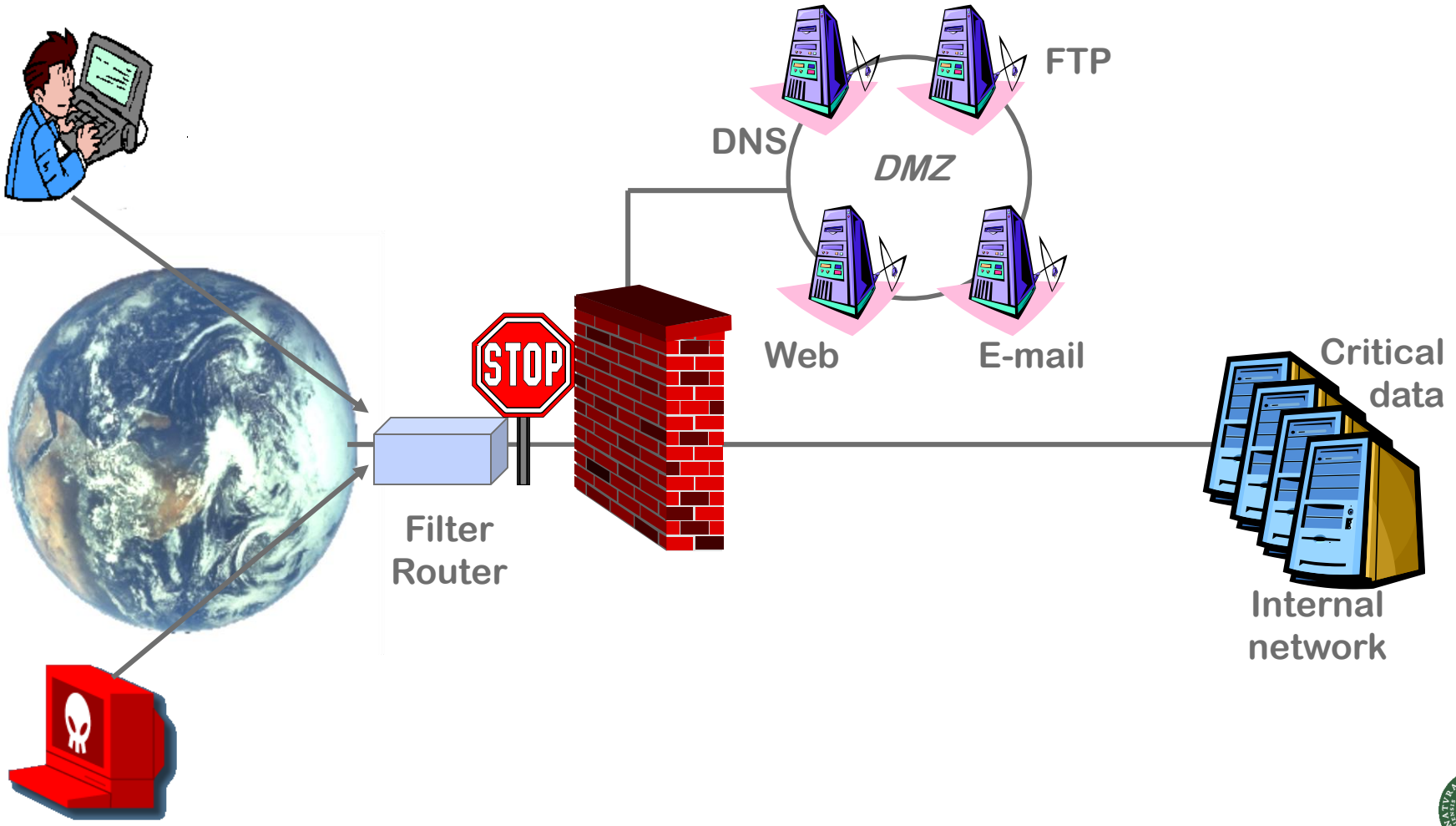
The network


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

Router problems - consequences

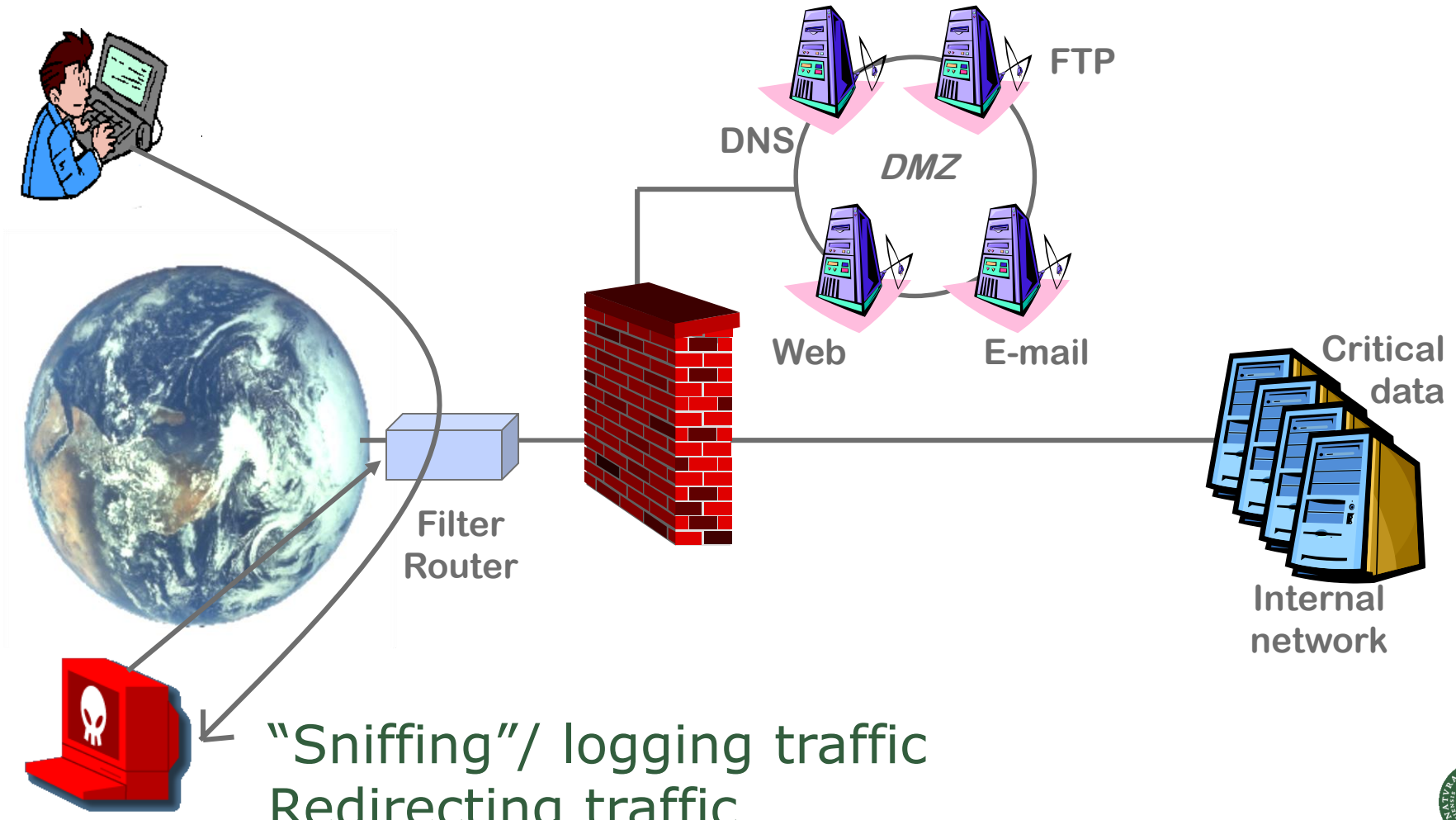


Router - Case Story: Microsoft

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

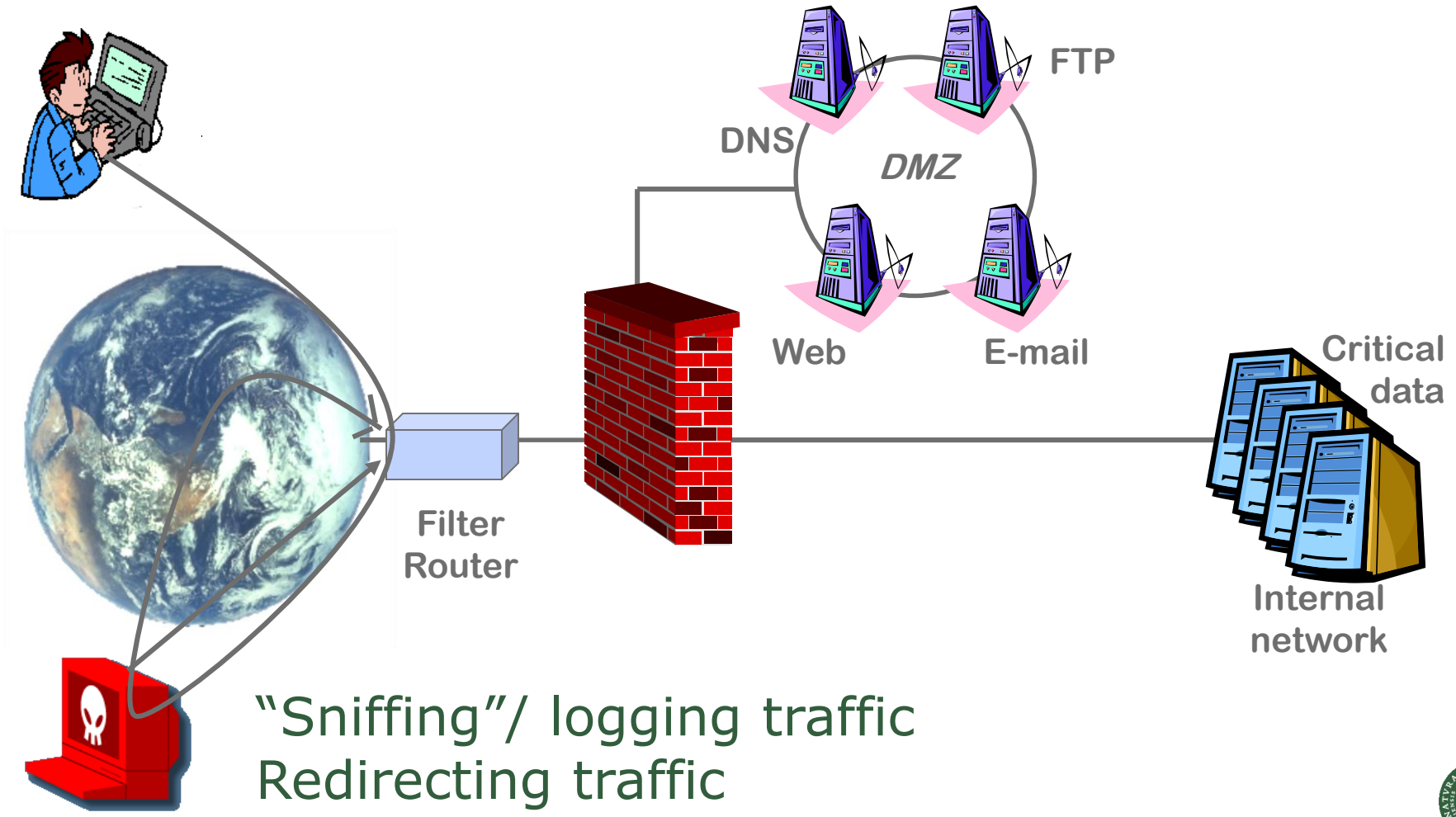
DoS attack against the router meant that all Microsoft's DNS-servers were uncapable of resolving domain names.

Router problems – consequences



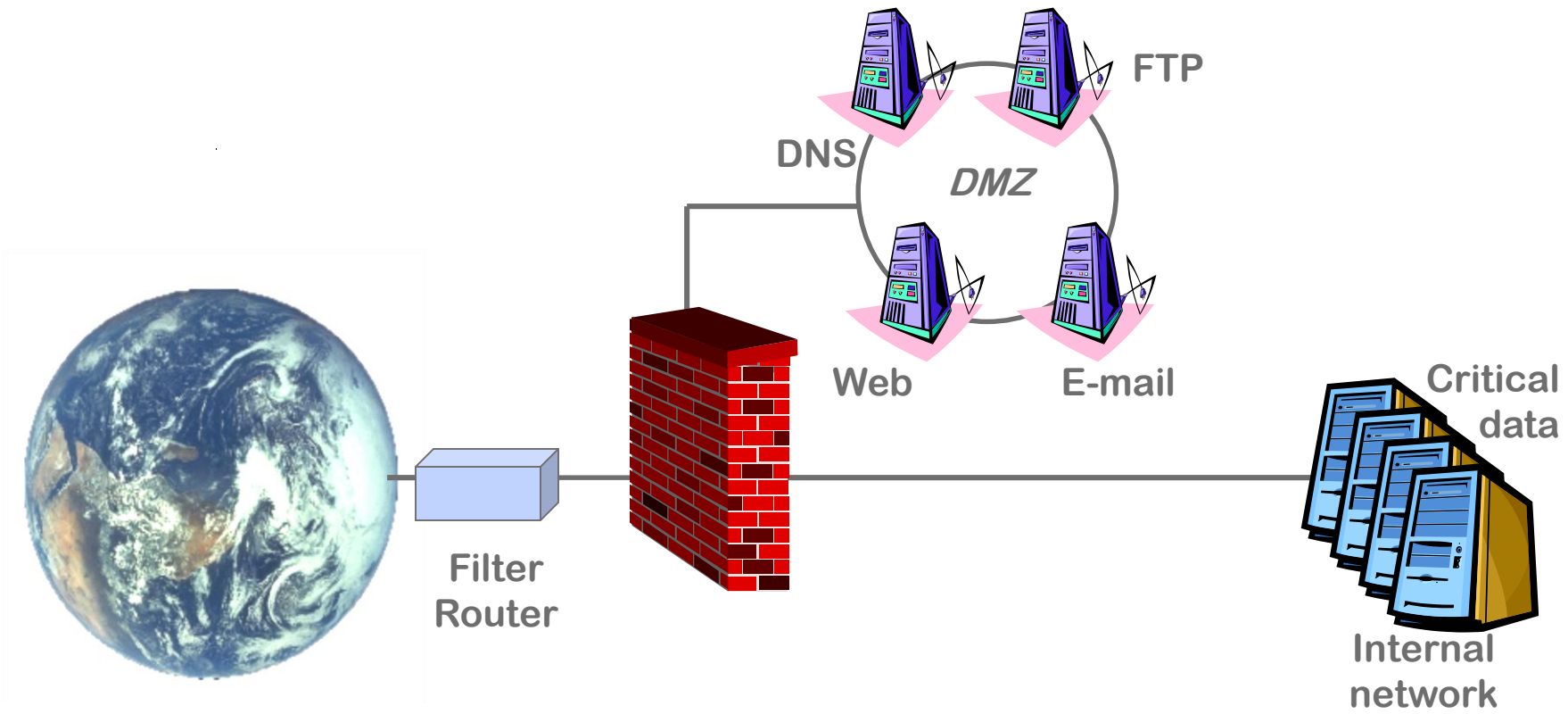
"Sniffing"/ logging traffic
Redirecting traffic

Router - consequences

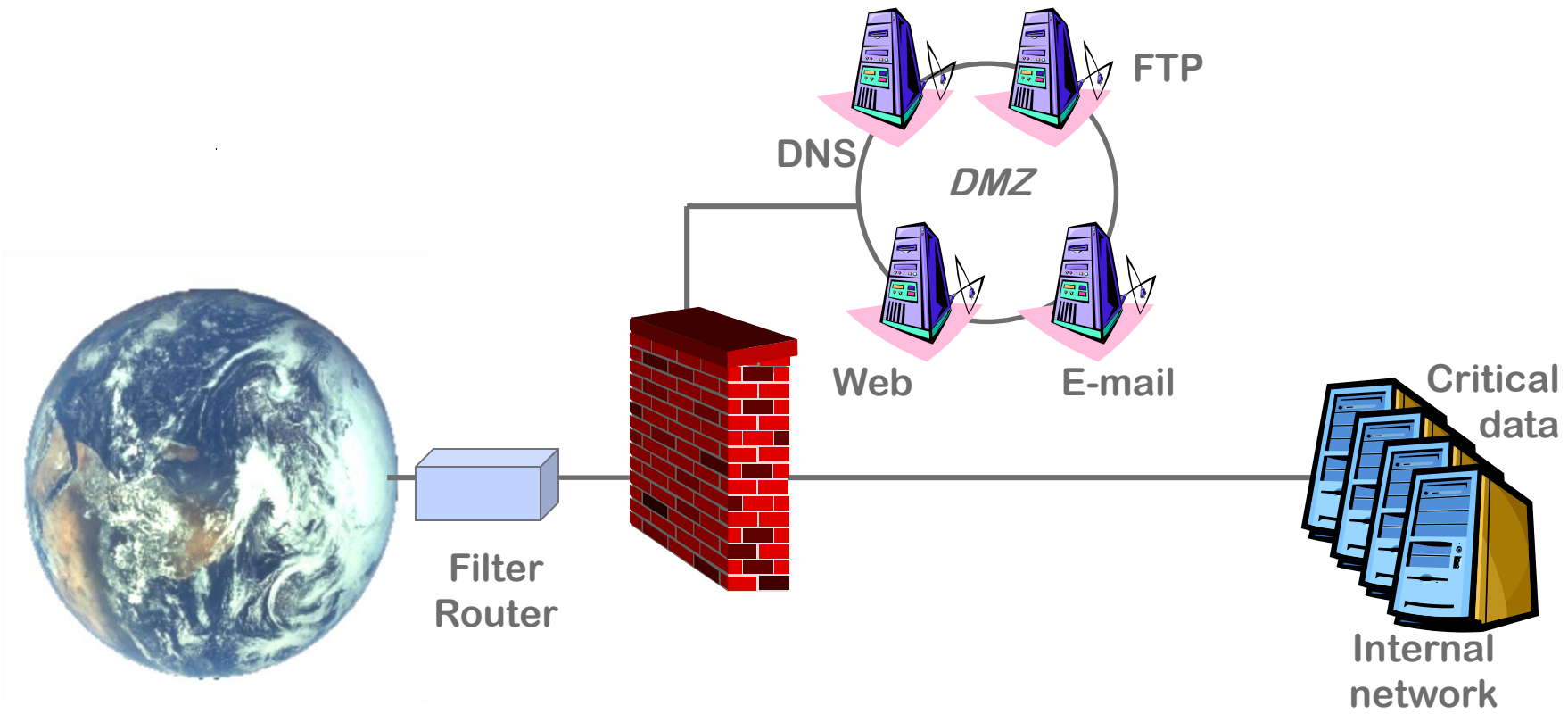


"Sniffing"/ logging traffic
Redirecting traffic

The network


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

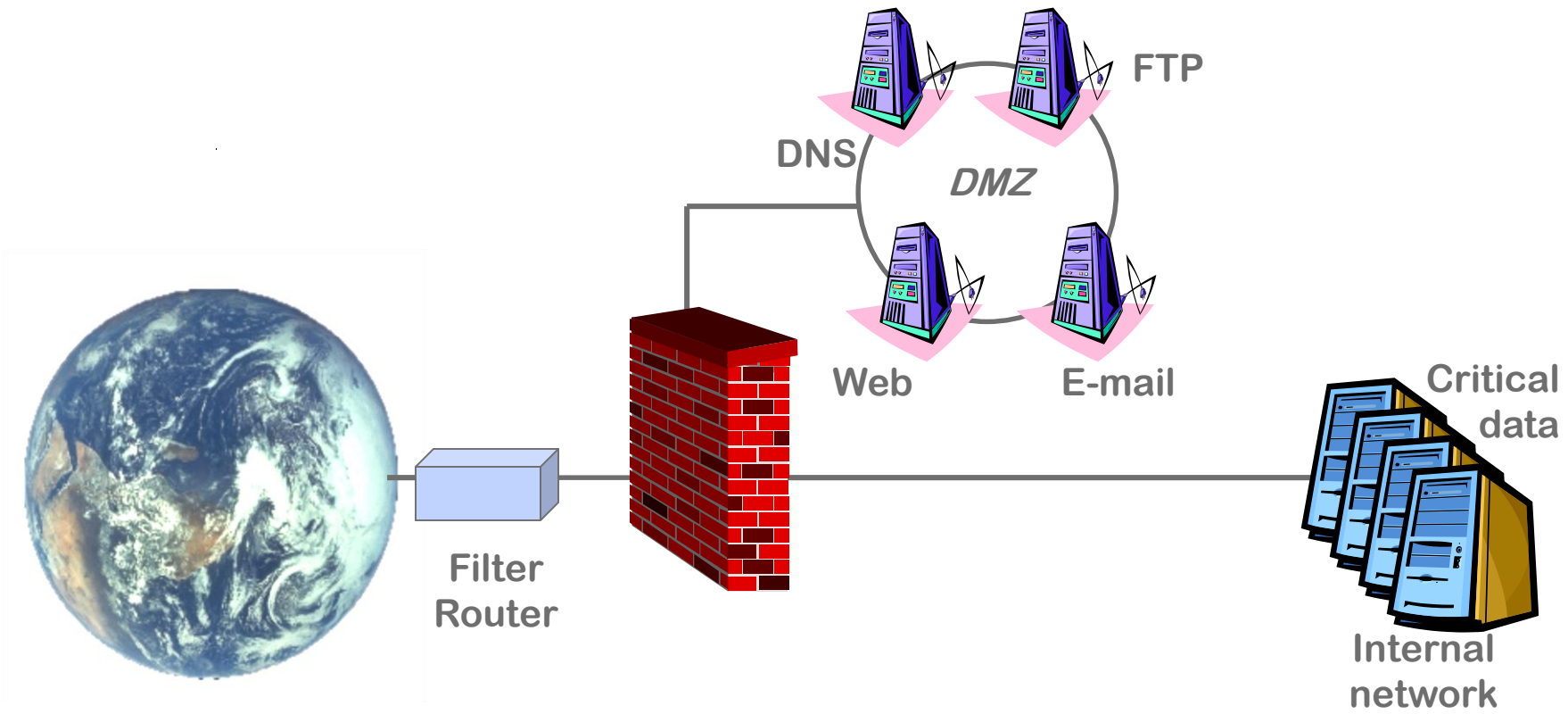
The network


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

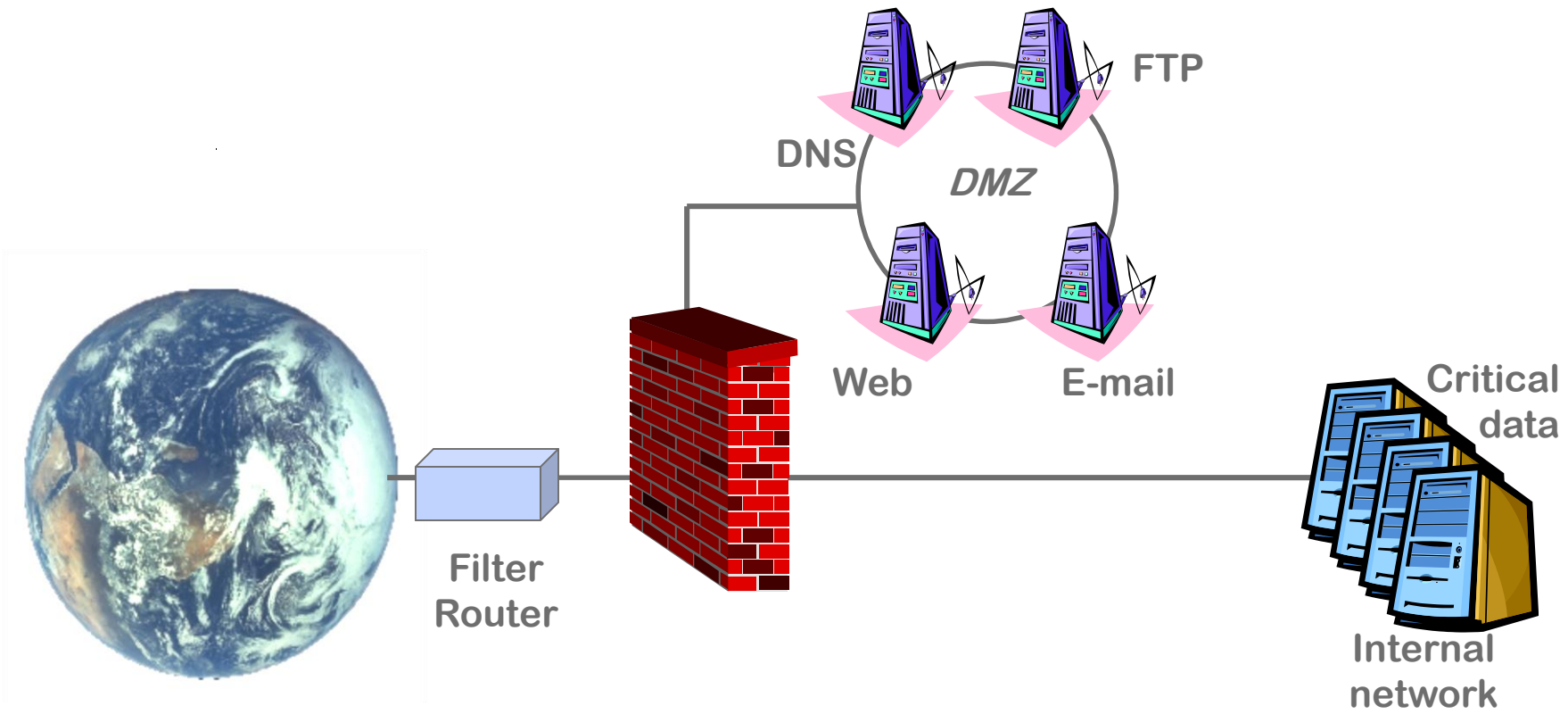
Typical firewall problems

- 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

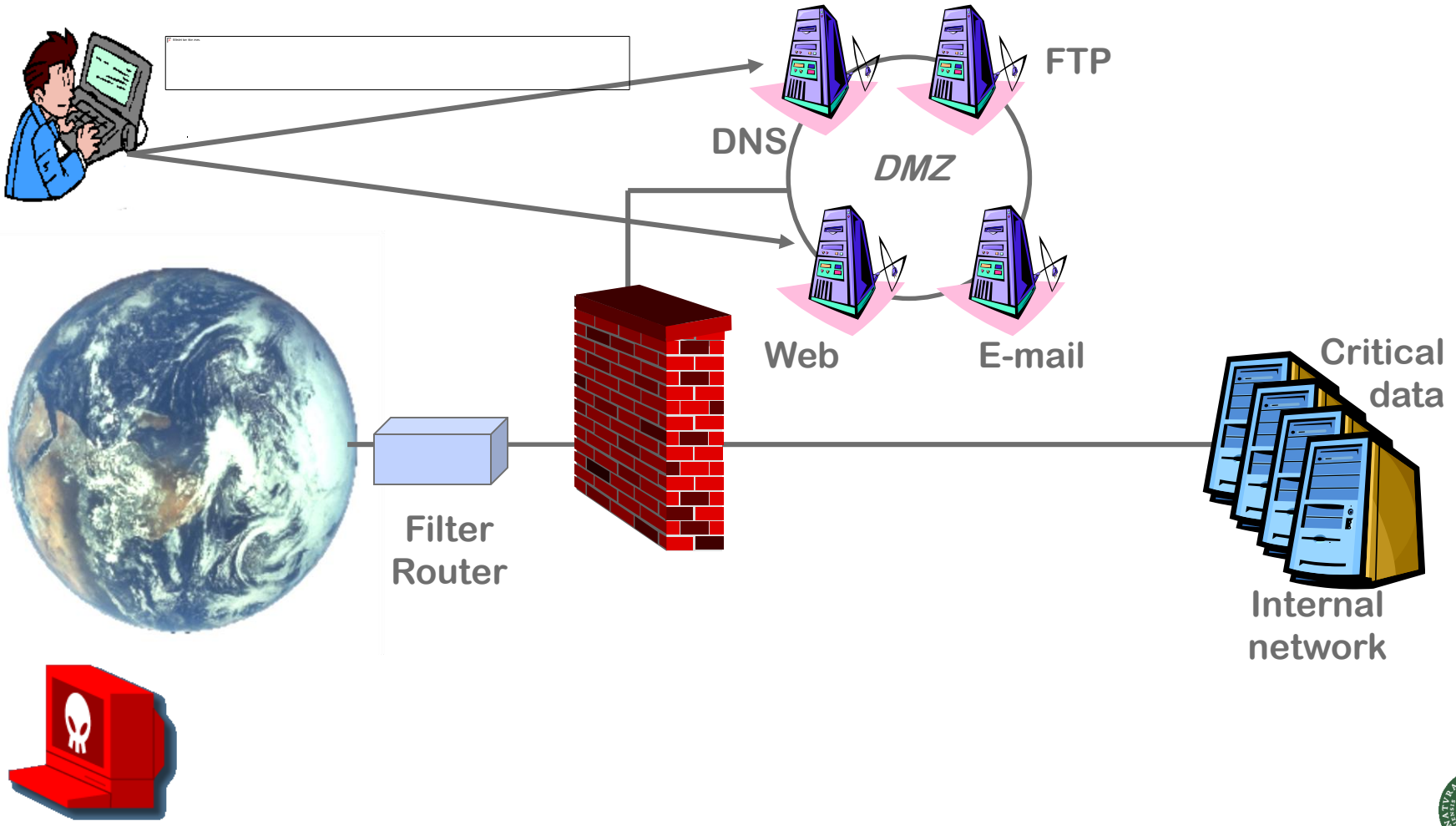
DoS

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

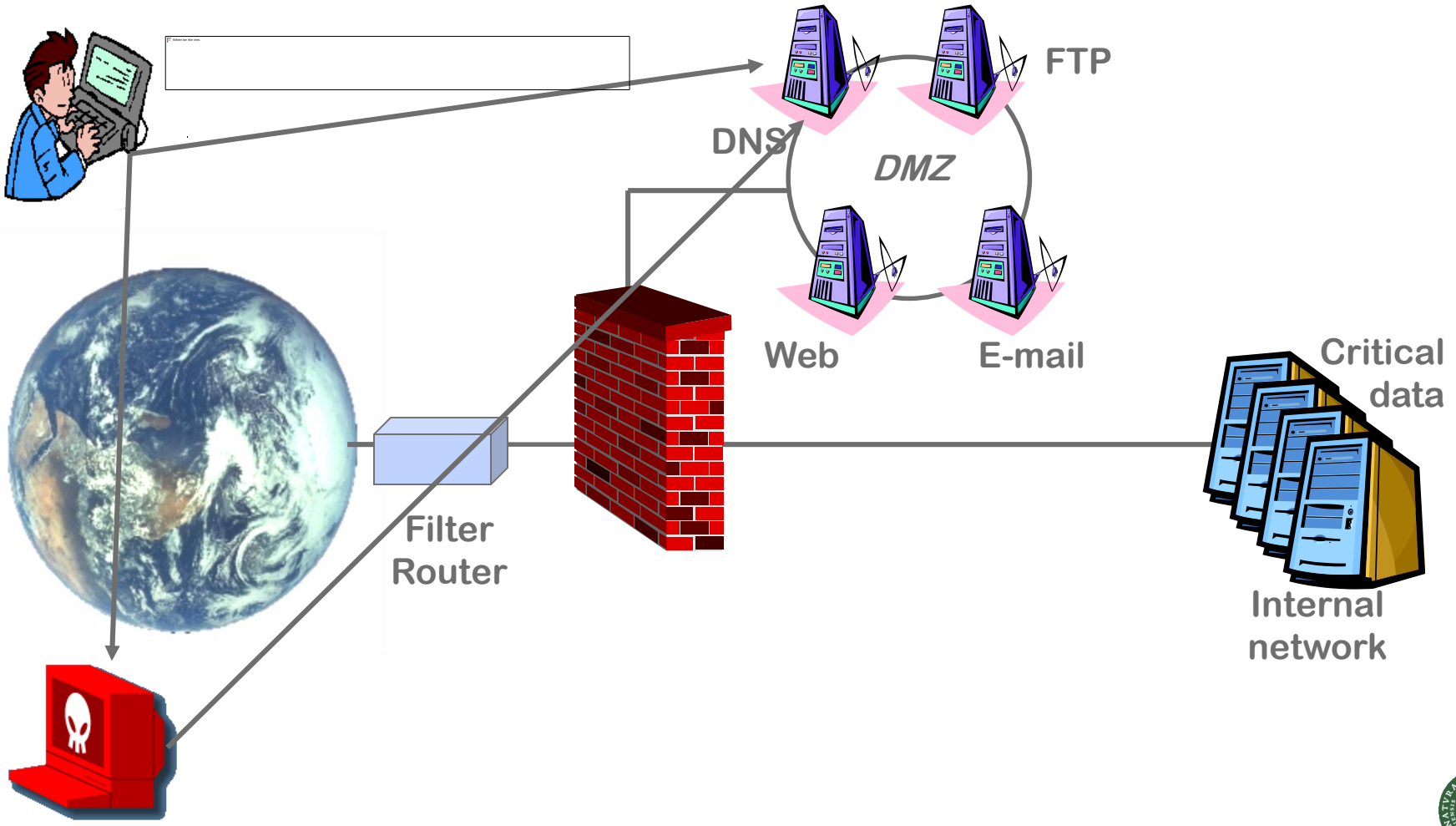
Execute commands on the server

Stepping Stone

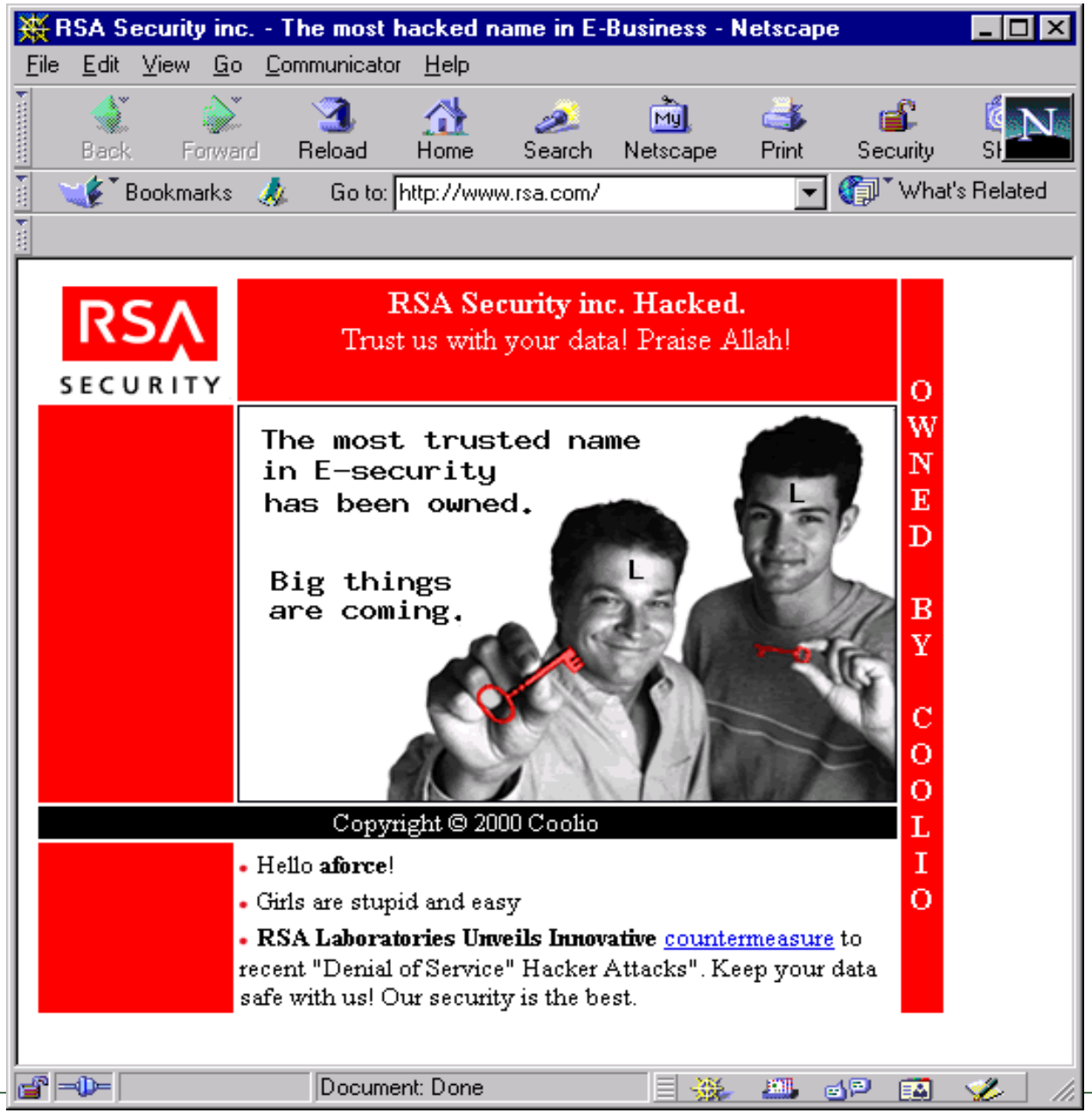
DNS problems - consequences



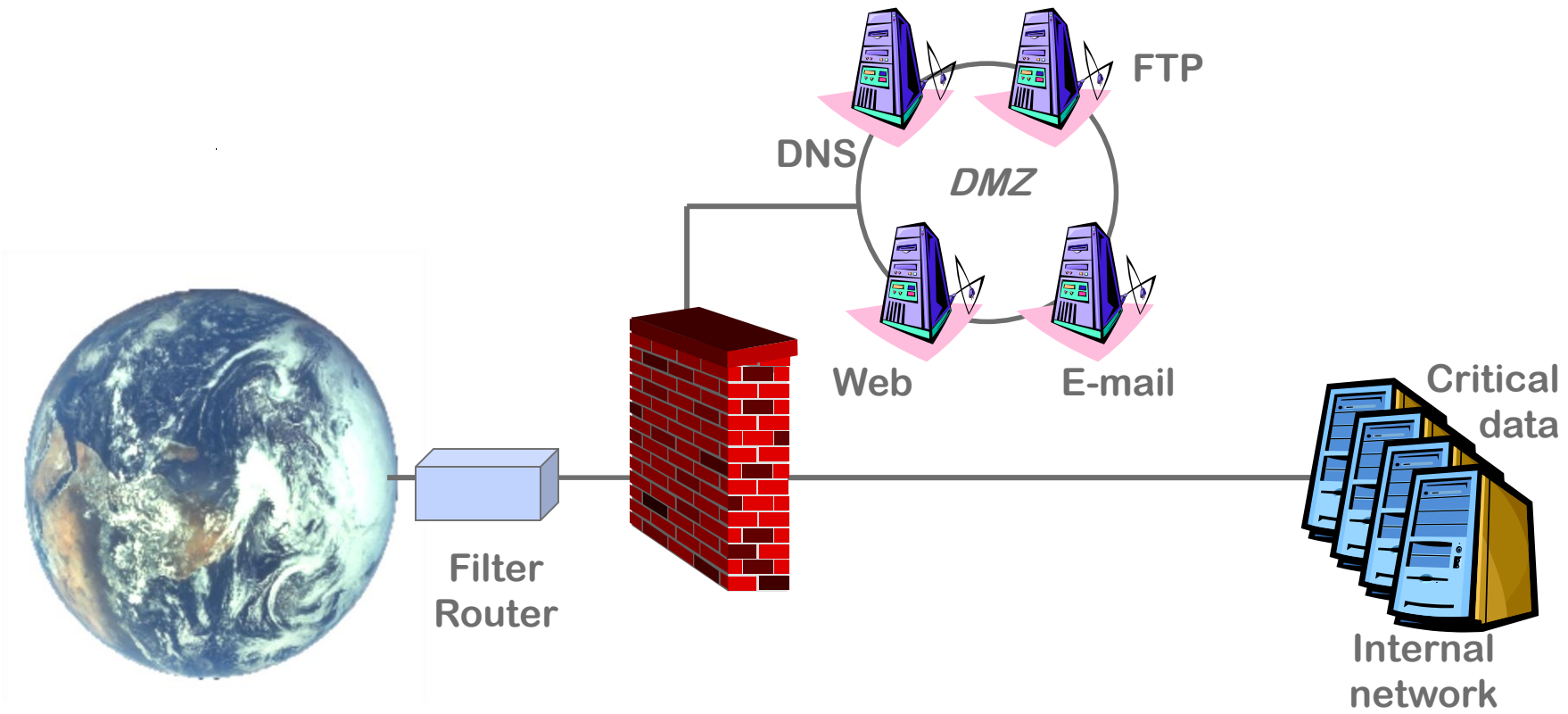
DNS problems - consequences



DNS - Case Story: RSA DNS Hijacking



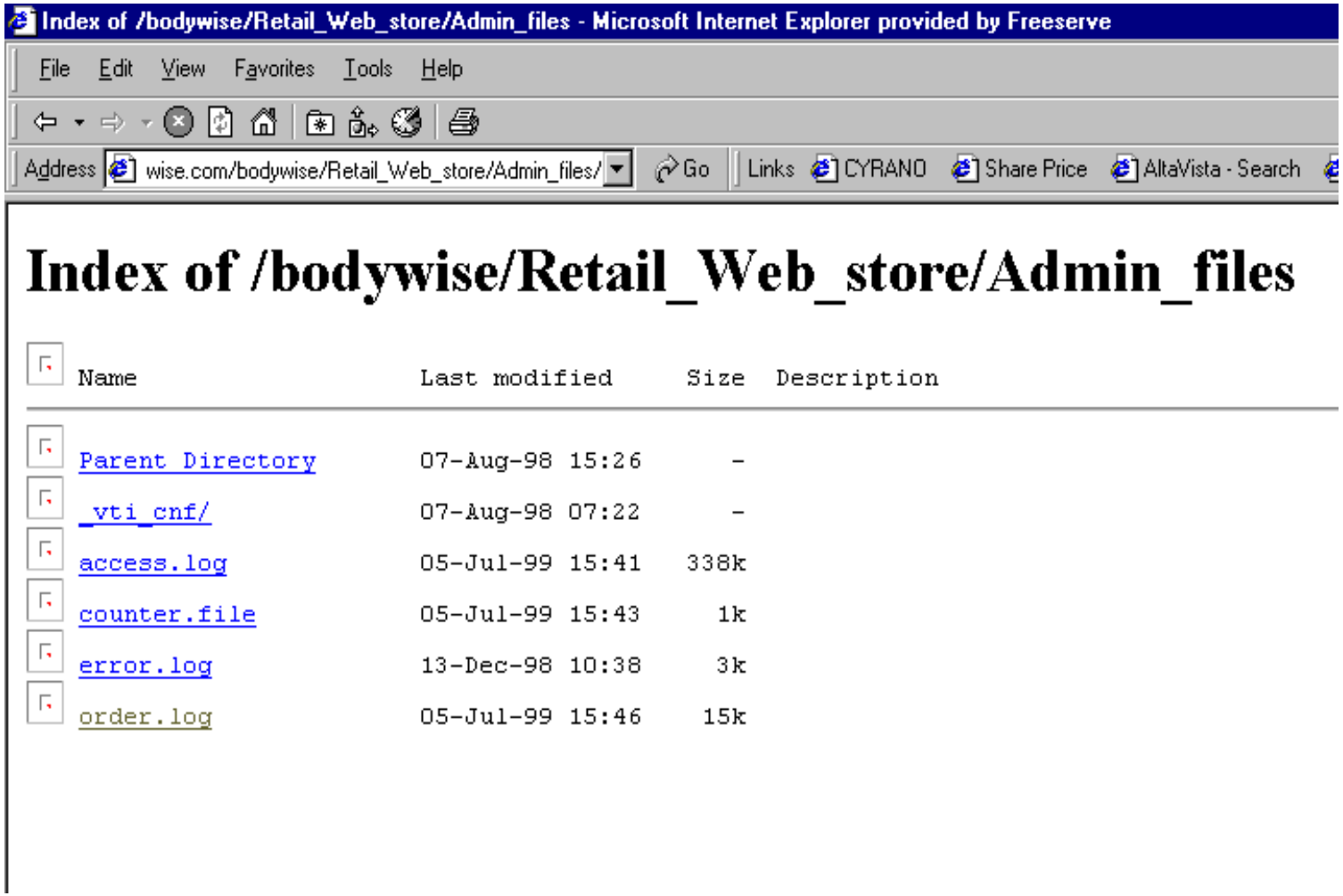
Typical setup



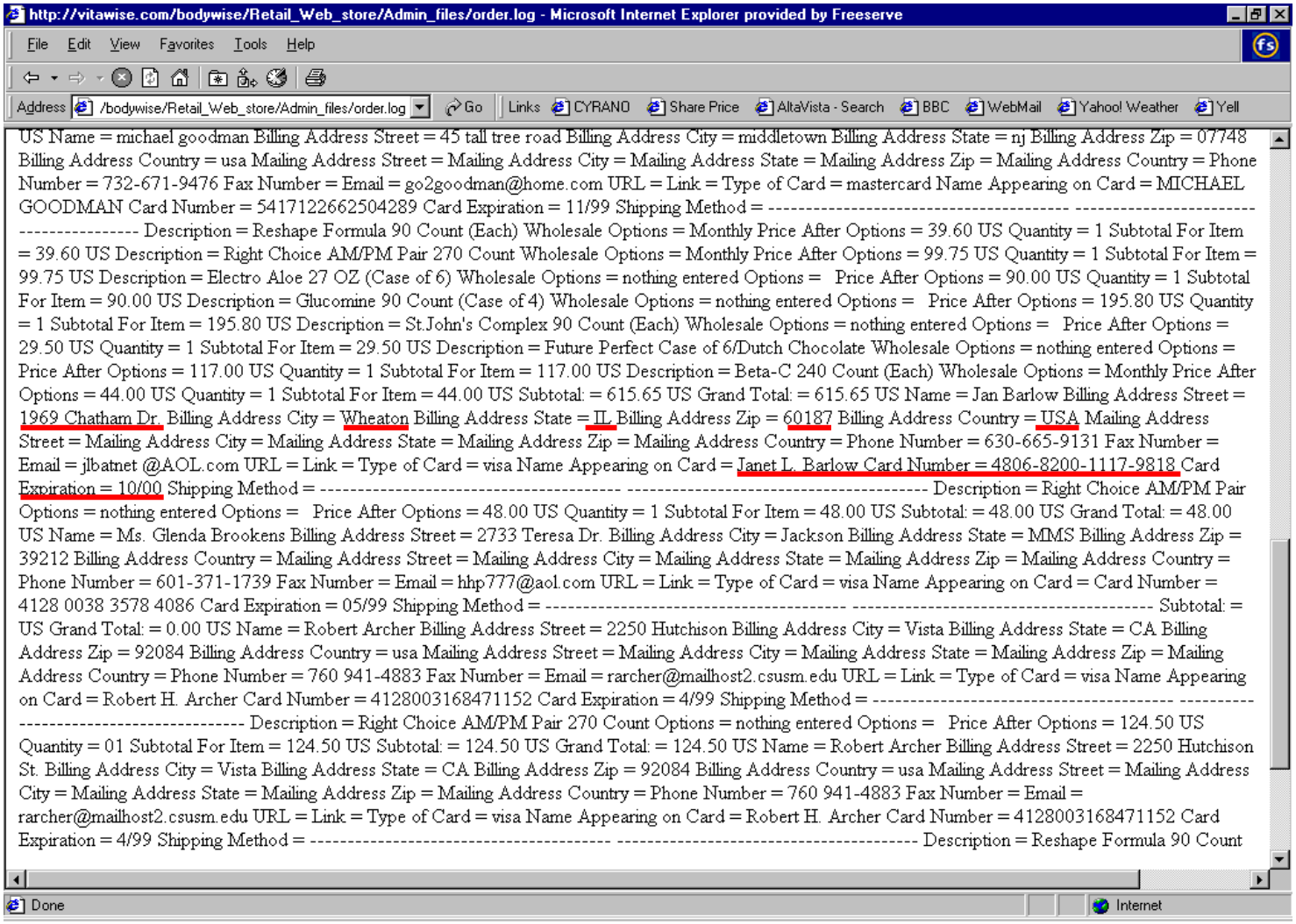
Consequences

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

Consequences



Consequences



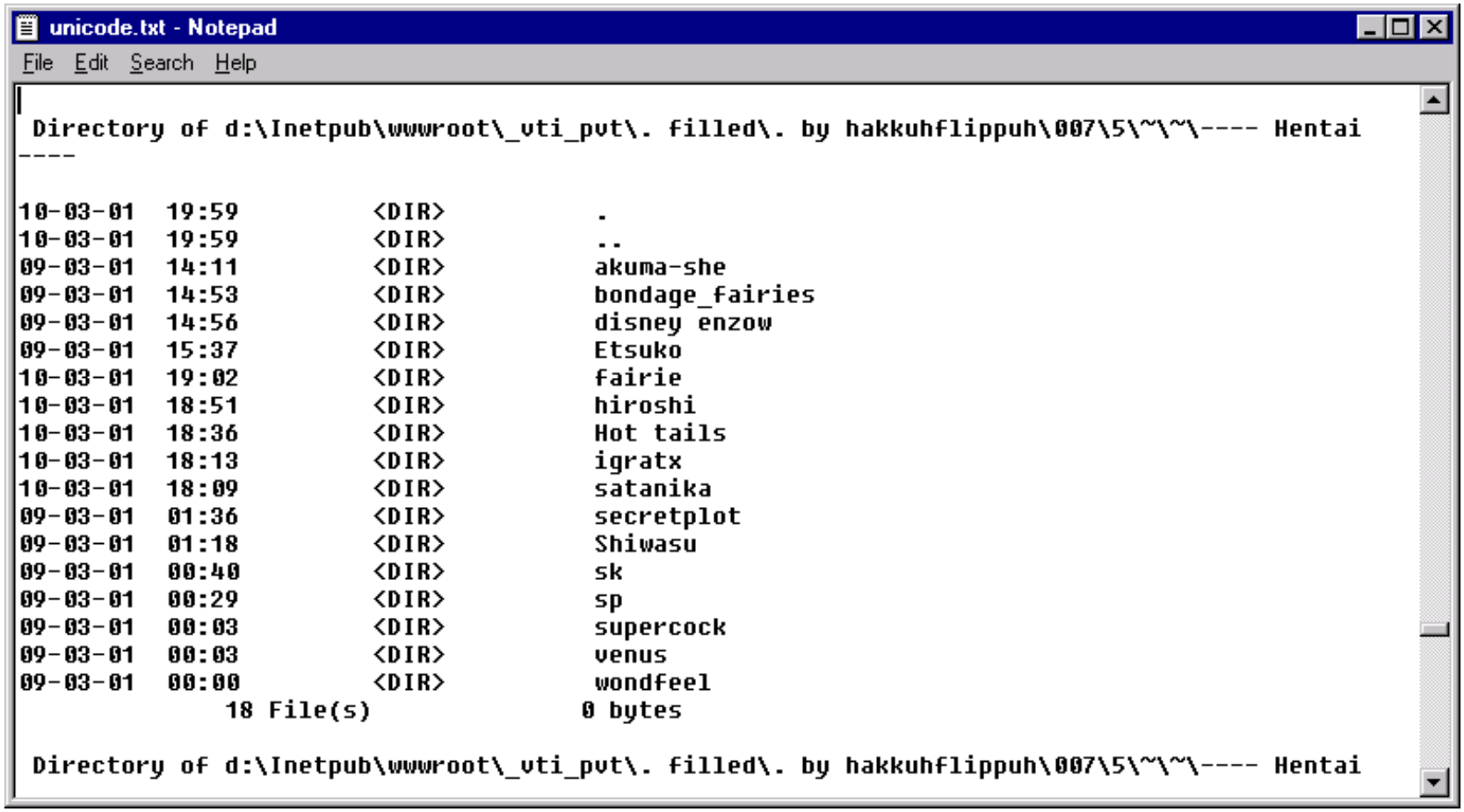
Warez server - 4.5GB data

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



Security architecture

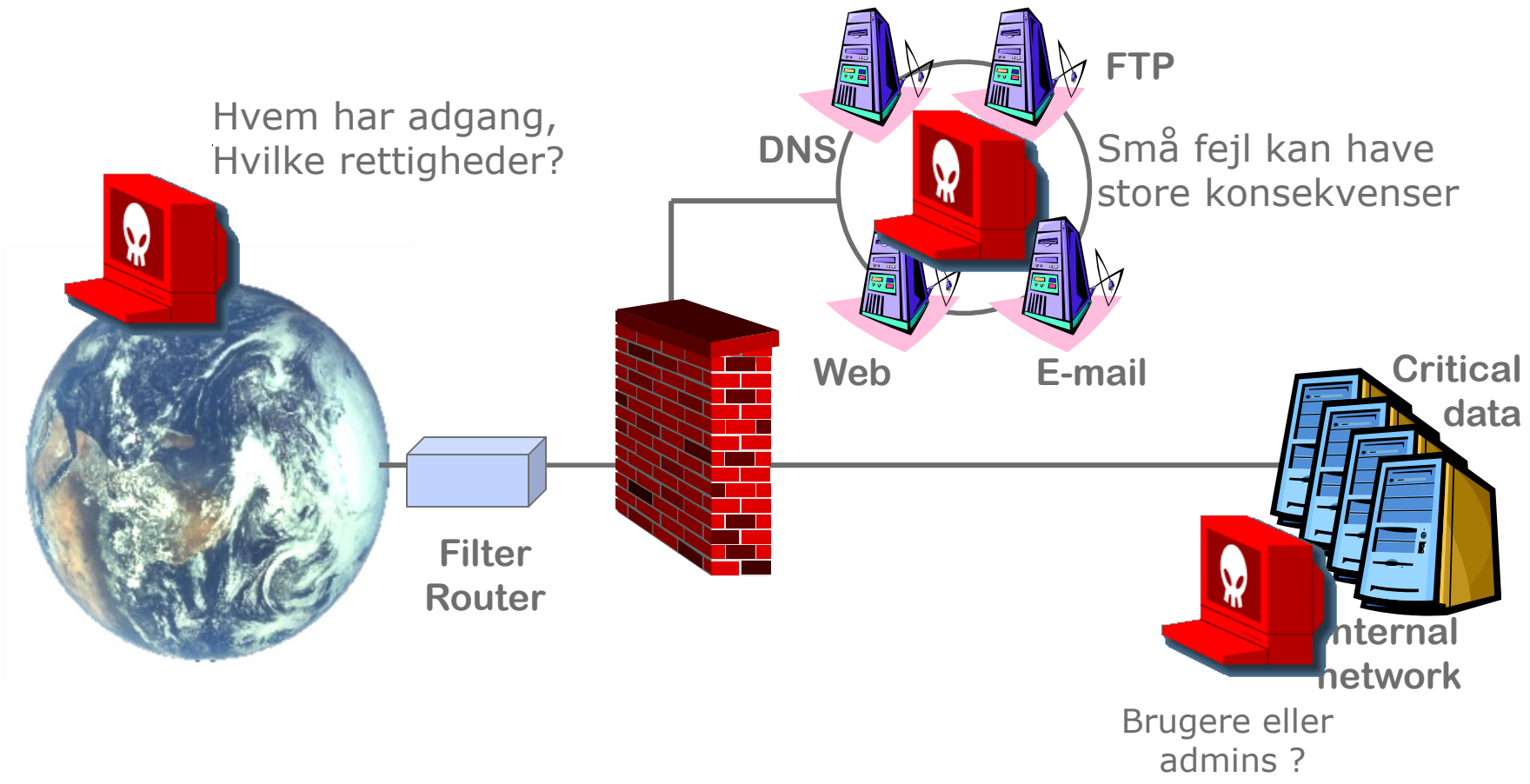
- Så få ”angrebssteder” som muligt (minimize attack surface)
- Vær opmærksom på at stederne findes
- Forså angriberne, gør det svært for dem
- Segmenter og adskil
- Defence in depth – mange lag af sikkerhed
- Jump servers
- Overvåg og log, IDS
- Håndtering af sikkerhedsbrud
- Test sikkerheden

Security architecture

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

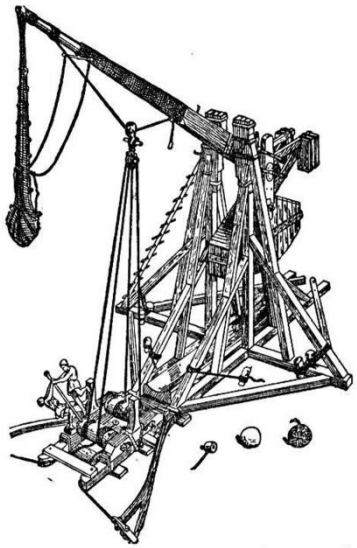
IT Security – start from the outside and zoom in

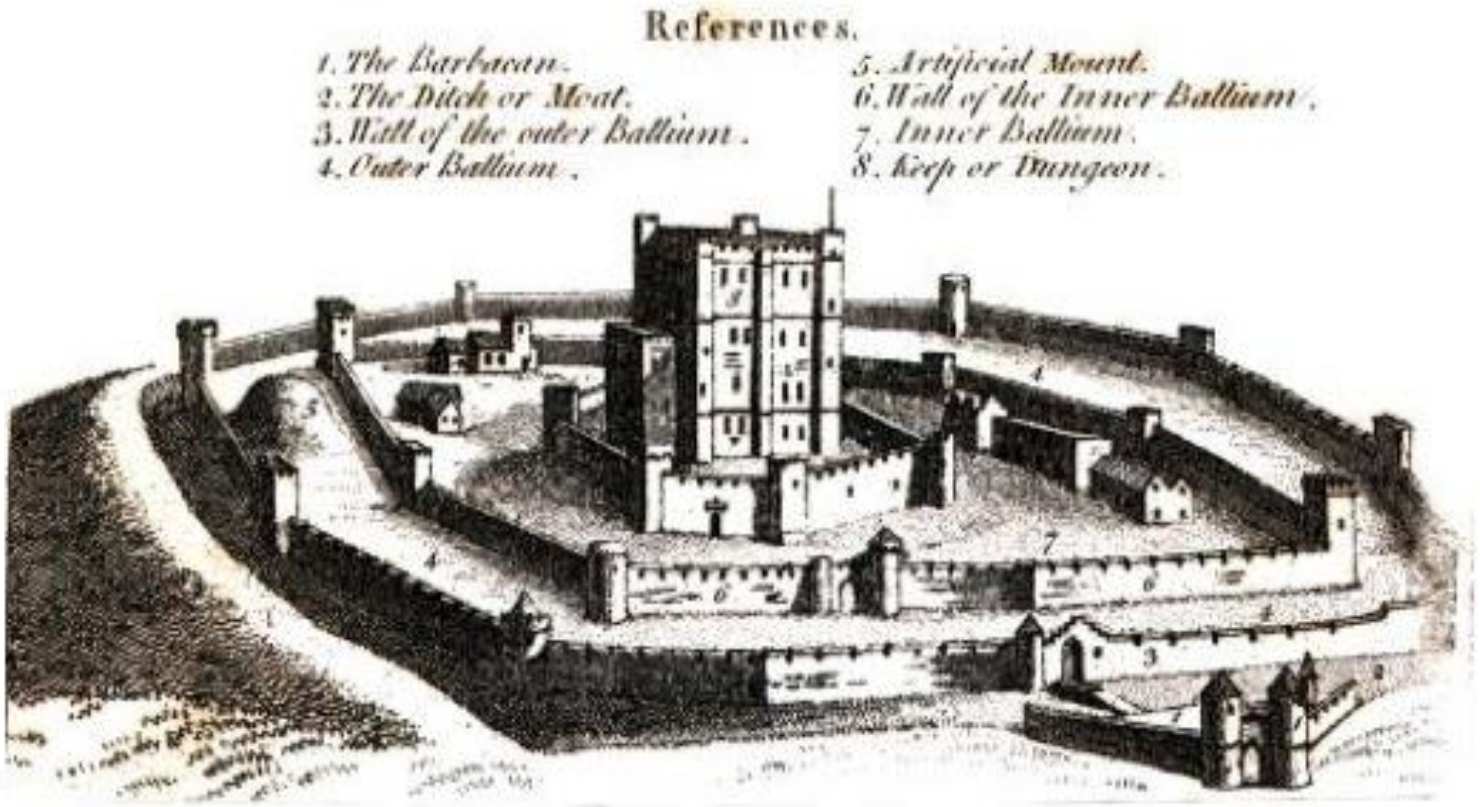
3 areas of attack



Old School vs. New World

IT Security threats





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

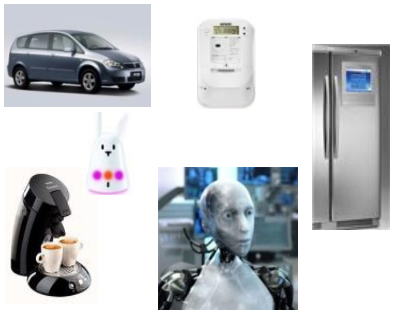
En bruger
Mange medier

I dag

Mobilitet

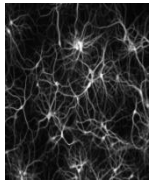
Machine To Machine

Many To Many



I morgen

Allesteds-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

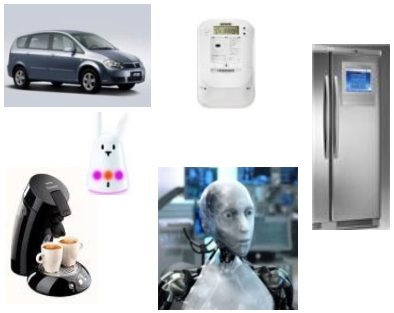
One To Many

En bruger
Mange medier

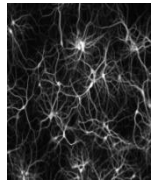
I dag

Machine To Machine

Many To Many



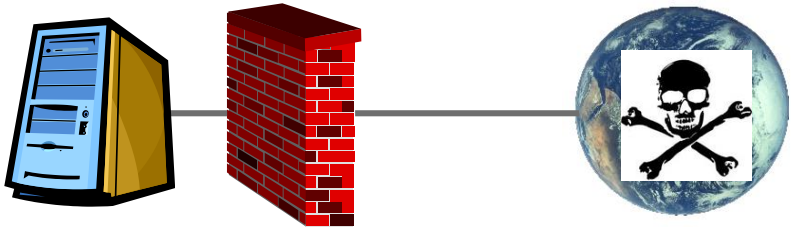
I morgen



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?

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