Building a firewall

S-38.153 Security of Communication Protocols

29.4.2003

Toni Henttonen

Overview

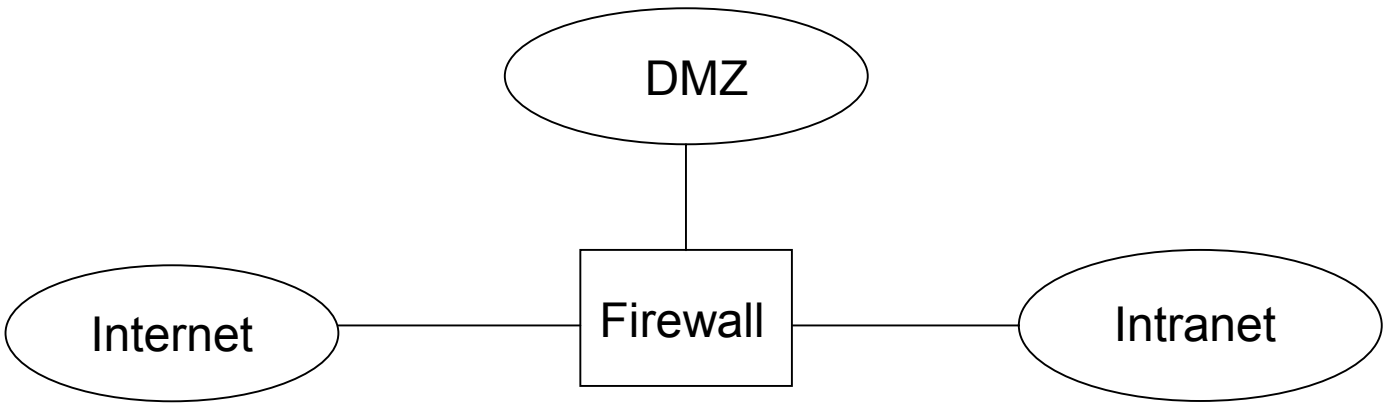
- Different possibilities
- Real life case: Building a firewall for company X
- Eventually, does firewall give you safety?

Different possibilities

- The simplest solution
- Only two networks: The bad Internet and the good intranet
- Mostly used at home where you usually only have your own computer in the intranet

Different possibilities

- More sophisticated solution
- Should be used when running servers in your own network
- Servers are placed in DMZ (DeMilitarized Zone)
- Used (usually) in small and medium size companies

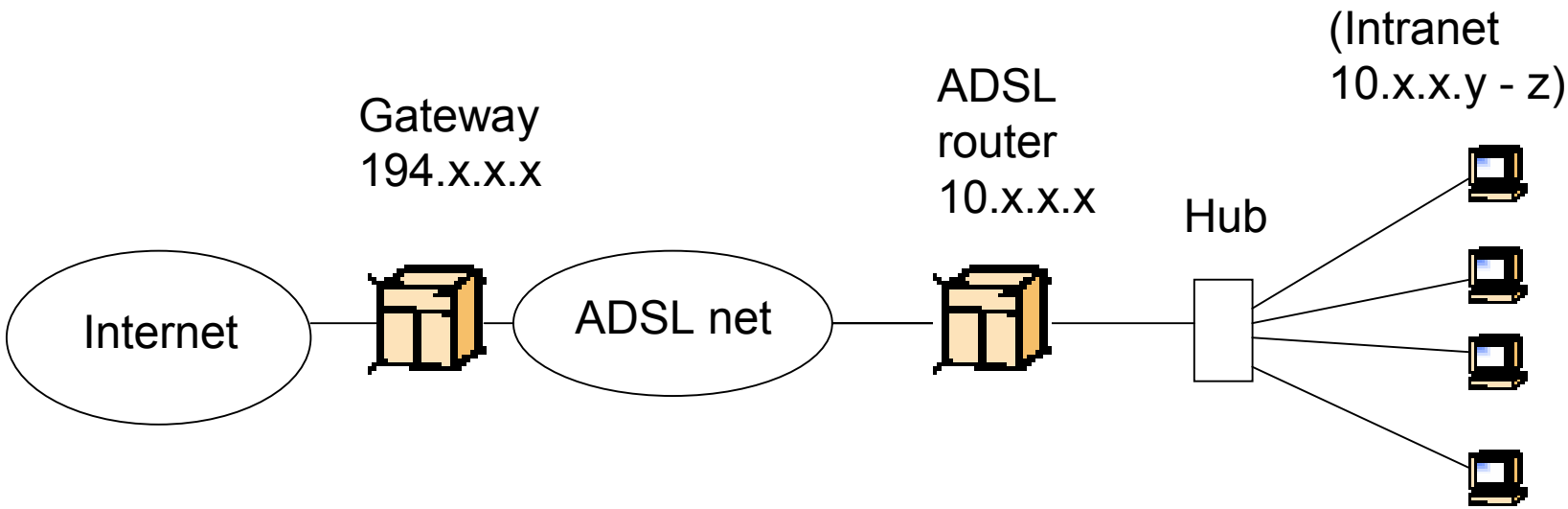


Different possibilities

- More complicated solutions exist
- Depends really on the network and on company policy
- Basic principle: When running (public) servers, place them on a network separated from the intranet

Real life case

- Company has an Internet connection via ADSL
- All PCs connected directly to Internet through a hub
- One PC acting also as a server (http, ftp, database)



Real life case

- Company has a deal with a network operator for connecting to the Internet and for redirecting requests coming from Interner to their server
- The company does not have public IPs, only the IPs provided from the private ADSL net
- Therefore, since there is a NAT in the gateway, redirecting is needed to reach the server from the Internet

Real life case

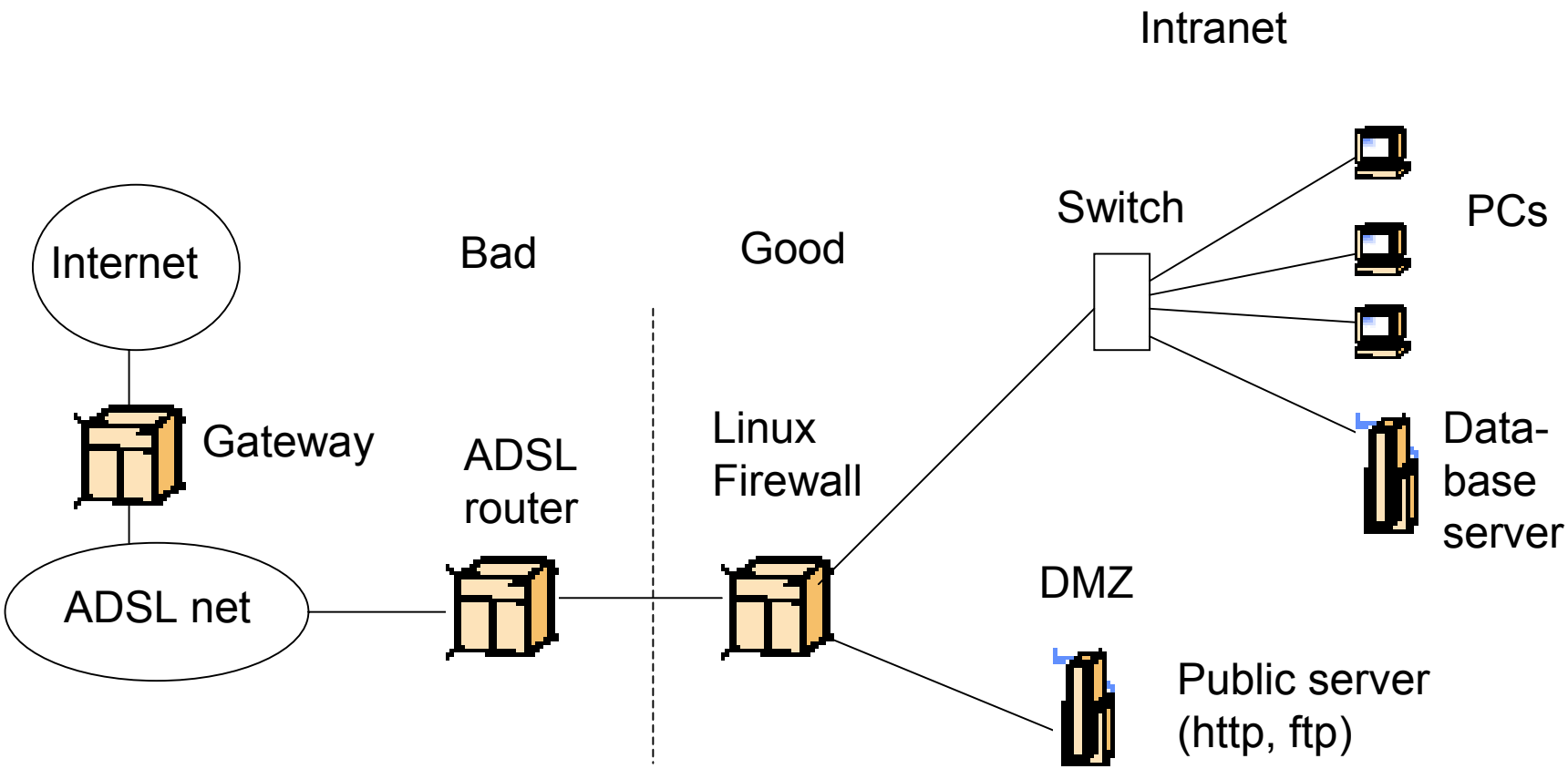
- Modifications definitely needed
- System protected in principal from the bad outside world (Internet) but not protected from threats from the ADSL net
- Firewall needed and servers needed to be separated from production machines (PCs)

Real life case

- Funding agreed for two servers and for one PC-based firewall
- Most important data in database, no need for public access
- Separate database server from http and ftp servers and place database server to intranet
- Outside access to database server allowed only from DMZ

Real life case

- Planned solution

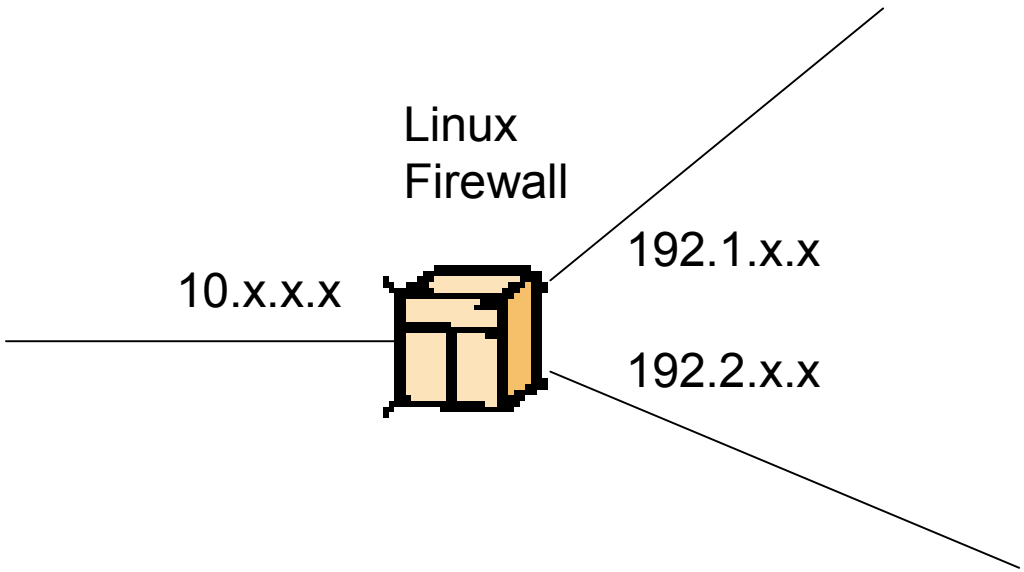


Real life case

- What do we need for the Linux firewall?
- First an old PC to act as firewall, in this case 533 MHz Pentium with 128 MB ram
- Need three network interfaces: either one network card with several interfaces or three normal nertwork cards
- Normal cards much cheeper, use them

Real life case

- Taking a closer look at the firewall we can see that it has three different IP-addresses since it is connected to three different networks
- Getting all these interfaces working correctly can cause some problems



Real life case

- What about the firewall itself?
- There are many softwares that could be used, but…
- Linux has built-in firewall in the Kernel
- IPChains or IPTables depending on the Kernel version
- This Kernel built-in firewall is very fast, reliable and rather tamper proof plus relatively easy to use

Real life case

- There are three different tables (chains) in IPTables
- Input: Defines which packets are allowed to enter the machine
- output: Defines which packets are allowed exit the machine
- Forward: Defines which packets should be forwarded through the firewall from one interface to another
- Rules can be given as command line commands or preferably in a shell script

Real life case

- Some examples of IPTables commands:
- Input:

```
# local interface, local machines, going anywhere is valid
IPTABLES -A INPUT -i $INTIF -s $INTNET -d $UNIVERSE -j accept-and-log-it
IPTABLES -A INPUT -i $DMZIF -s $DMZNET -d $UNIVERSE -j accept-and-log-it

# remote interface, claiming to be local machines, IP spoofing, get lost
IPTABLES -A INPUT -i $EXTIF -s $INTNET -d $UNIVERSE -j drop-and-log-it
IPTABLES -A INPUT -i $EXTIF -s $DMZNET -d $UNIVERSE -j drop-and-log-it
```

Real life case

- Output:

```
# local interface, any source going to local net is valid
IPTABLES -A OUTPUT -o $INTIF -s $INTIP -d $INTNET -j accept-and-log-it
IPTABLES -A OUTPUT -o $DMZIF -s $INTIP -d $DMZNET -j accept-and-log-it
IPTABLES -A OUTPUT -o $INTIF -s $DMZIP -d $INTNET -j accept-and-log-it
IPTABLES -A OUTPUT -o $DMZIF -s $DMZIP -d $DMZNET -j accept-and-log-it

# outgoing to local net on remote interface, stuffed routing, deny
IPTABLES -A OUTPUT -o $EXTIF -s $UNIVERSE -d $INTNET -j drop-and-log-it
IPTABLES -A OUTPUT -o $EXTIF -s $UNIVERSE -d $DMZNET -j drop-and-log-it
```

Real life case

- Forward:

```
#   This will forward ALL port 80 and 21 traffic from the external IP address
#   to port 80 or 21 on the 192.x.x.x machine
PORTFWIP="192.x.x.x"
IPTABLES -A FORWARD -i $EXTIF -o $DMZIF -p tcp --dport 80 -m state --state NEW,
ESTABLISHED,RELATED -j accept-and-log-it
IPTABLES -A FORWARD -i $EXTIF -o $DMZIF -p tcp --dport 21 -m state --state NEW,
ESTABLISHED,RELATED -j accept-and-log-it

IPTABLES -A PREROUTING -t nat -p tcp -d $EXTIP --dport 80 -j DNAT –to
$PORTFWIP:80
IPTABLES -A PREROUTING -t nat -p tcp -d $EXTIP --dport 21 -j DNAT –to
$PORTFWIP:21
```

Real life case

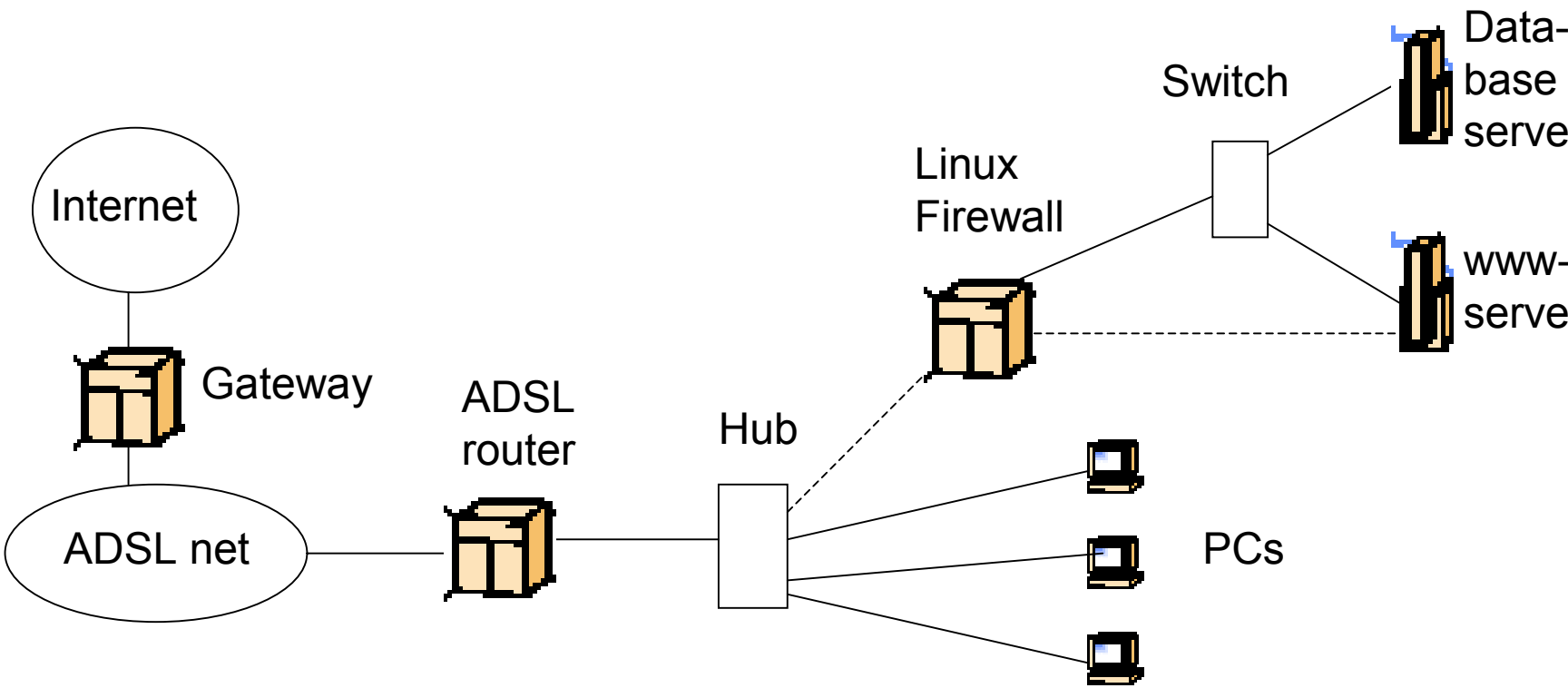
- Creating own chains:

```
# Creating a drop chain that logs all traffic
IPTABLES -N drop-and-log-it
IPTABLES -A drop-and-log-it -j LOG --log-level info
IPTABLES -A drop-and-log-it -j DROP

# Creating an accept chain that logs all traffic
IPTABLES -N accept-and-log-it
IPTABLES -A accept-and-log-it -j LOG --log-level info
IPTABLES -A accept-and-log-it -j ACCEPT
```

Real life case

- Temporary solution for testing the firewall and network:



Real life case

- First problem: Get the network and cards working
- Resulting from some testing different cards had several addresses which were in conflict with each other
- Second problem: IPTables does not start
- Third problem: How to tell the firewall to direct incoming traffic to the www-server?

Real life case

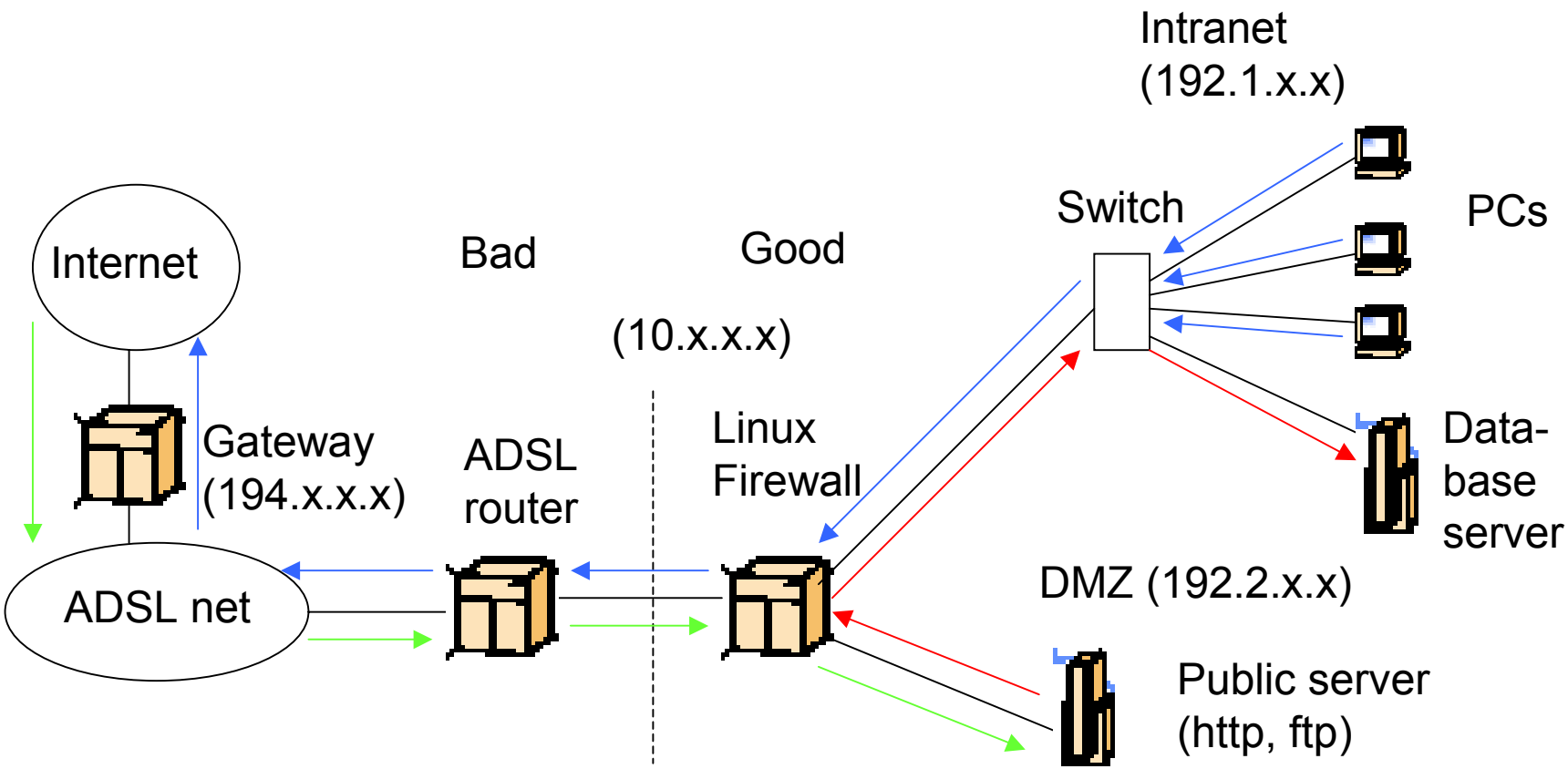
- After getting the basic version running the real configuration work starts
- Making the policy for the traffic
- Logging needs to be arranged
- Defining backup policy

Real life case

- The Policy:
- Only the necessary ports to www-server from firewall are opened
- Traffic generated from intranet allowed (trusted) and responding traffic to intranet allowed
- Only www-server from DMZ has access to DB-server in intranet plus access from intranet allowed
- Everything else denied (i.e. ping, UDP…)

Real life case

Final situation



Eventually, does firewall give you safety?

- Firewall not really a wall, holes needed
- In most cases the basic presumption is that people on the inside are trustworthy...
- New viruses discovered daily, a virus aimed especially against firewalls?!?
- If performance is not high enough the firewall can be vulnerable to DoS

Eventually, does firewall give you safety?

- Technology is developing at incredible speed
- If not kept very tightly up to date a hacker with a newly found bug may be able to break through the wall
- So eventually firewall does give you rather good protection allthough you can never be 100 % secure unless you pull the net plug…

Questions?

Thank you