Welcome to

What is a Secure Network

PROSA August 2025

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

prosa-secure-network-2025.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teacher and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

You are welcome to drop me an email

Code of Conduct

I subscribe to having a Code of Conduct for events, we need them still! Usually I say the BornHack code of conduct apply whenever I teach! https://bornhack.dk/conduct/

Today we talk about networking, so I recommend this also: RIPE Code of Conduct Publication date: 05 Oct 2021

Rationale Our goals in having this Code of Conduct are:

- **To help everyone feel safe and included.** Many people will be new to our community. Some may have had negative experiences in other communities. We want to set a clear expectation that harassment and related behaviours are not tolerated here. If people do have an unpleasant experience, they will know that this is neither the norm nor acceptable to us as a community.
- **To make everyone aware of expected behaviour.** We are a diverse community; a CoC sets clear expectations in terms of how people should behave.

Source: https://www.ripe.net/publications/docs/ripe-766

Time schedule

- 17:00 - 17:40 Introduction and basics for the subject
- 17:40 - 18:05 Exercise in groups: example secure network
- 30min break Eat with your family if you like, I will be around most of the break, available for questions
- 18:45 - 19:30 Further teaching and exercises in the subject for the evening
- 15min break Stretch your legs, get some more water
- 19:45 - 20:30 Further teaching and exercises in the subject for the evening, Opal router, questions and more
- 20:30 - 21:00 May contain exercises to be done on your own, with input from me

I will try to keep this plan for all evenings! So you hopefully can plan family life better

Will also try to make smaller breaks/exercises during the slidesshows, check for questions etc.

About Equipment and Exercises

- Bringing a laptop is not required, but welcome.
- Exercises booklets are available for many of my courses, see Github
  but it is expected that participants will do any exercises on their own later or at the scheduled hacker days
- The hacker days will be announced in various places
- Events like BornHack are excellent places to arrange hacker days in the network warrior village, or other places
- I announce mine at https://nwwc.dk

Invite a few friends, make a hacker day and work together!

Hvad er et sikkert netværk? (Onlinemodul 1 af 3)

Systemsikkerhed, forensics, hændelseshåndtering og softwaresikkerhed samt netværkssikkerhed med et holistisk blik Første af tre online-aftenkurser om værktøjer, der får netværk og drift til at spille sammen for at give et løft til IT-sikkerheden i din organisation. Med udgangspunkt i netværkssikkerhed gennemgår vi, hvordan du kan være med til at sikre din organisation gennem design, arkitektur, værktøjer, processer og tiltag indenfor netværkslagene. Der vil være elementer af systemsikkerhed, forensics og hændelseshåndtering og softwaresikkerhed men hovedvægten er på netværkssikkerhed med et holistisk blik.

Keywords: CIA modellen, CVE sårbarheder, switch, router, firewall, ACL, DoS/DDoS, VLAN, segmentering, logning, monitoring, Netflow, Zeek, Suricata, Nmap, Elasticsearch, IEEE 802.1x, IPv4, IPv6, NTP, DNS

- Man kan godt nøjes med en aften
- Materialet er open source, I kan hente det hele – og spørg gerne på email eller chat
- Sidste tal fra Lulu var 86 tilmeldte – hvilket gør interaktion lidt udfordrende – async hvor I skriver spørgsmål i chatten virker typisk godt

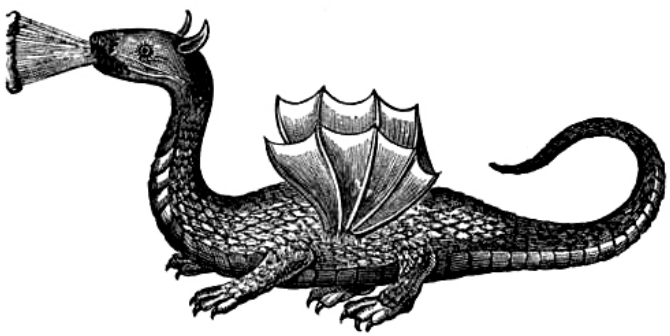
Goals for today

- What is a secure network
- Confidentiality, Integrity og Availability (CIA) model
- Look at network security with a *holistic approach*
- Move down and up in the network layers
- Discuss design, architecture and technical capabilities
- Show tools that can help along the way

Exercises

- Larger exercise in groups: example secure network
- Router exercise near end: Opal router inspiration

Networks are trouble



Internet here be dragons

- Networks are constantly evolving
- Threats are constantly increasing
- Vulnerabilities are found daily
- Even more vulnerabilities are *developed* and *installed*
  Sorry developers, but some of you don't care, and it shows!

Internet is based on Open Standards and collaboration!

> We reject kings, presidents, and voting.
> We believe in rough consensus and running code.
> – The IETF credo Dave Clark, 1992.

- Request for comments - RFC – series of documents describing internet standards
- RFC, BCP, FYI, informational
  First ones from 1969
- Never changed but status changed to Obsoleted when a never version or document superseeds it
  (Errata exist and are published though)
- Standards track:
  Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard
- Open standards gurantee transparency, but not security

What is a Secure Network

A controlled environment with a purpose and goal which is designed, implemented and monitored to be sufficiently secure – according to the policies and wishes of the owner and operator

Example networks

- Home network – should support a *family typically*
- Factory network – should support machines, robots, production of things
- Office network – should be available for employees and without malware and data leaks

Network Security as a Holistic Approach

holistic adjective

1 : of or relating to holism

2 : relating to or concerned with wholes or with complete systems rather than with the analysis of, treatment of, or dissection into parts
holistic medicine attempts to treat both the mind and the body
holistic ecology views humans and the environment as a single system

Source: https://www.merriam-webster.com/dictionary/holistic

- The network spans the whole organisation and we use *the network* – the Internet for many things
- Network security affects the whole organisation
- When improving network security, we often improve overall security

Networks are Built from Components

Photo by Eugen Str on Unsplash

Knowledge and insight

- Networks have end-points and conversations on multiple layers
- Wireshark is advanced, try right-clicking different places
- Name resolution includes low level MAC addresses, and IP - names

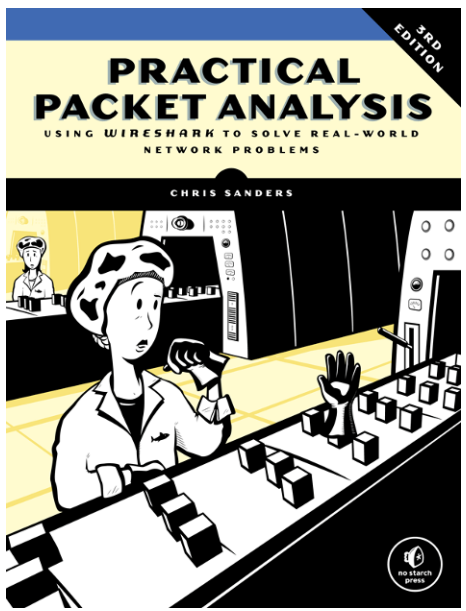
- Tcpdump format, built-in to many network devices
- Remote packet dumps, like `tcpdump -i eth0 -w packets.pcap`
- Story: tcpdump was originally written in 1988 by Van Jacobson, Sally Floyd, Vern Paxson and Steven McCanne who were, at the time, working in the Lawrence Berkeley Laboratory Network Research Group https://en.wikipedia.org/wiki/Tcpdump

Great network security comes from knowing networks!

Course Materials

- This material is in multiple parts:
- Kickstart document – basic information `kickstart-prosa-secure-network.pdf`
- Slide show - the presentation - this file `prosa-secure-network-2025.pdf`
- Exercise for today: example secure network `exercise-secure-network-example.pdf`
- Exercise/inspiration for today: `kickstart-2-opal-router.pdf`
- Exercise booklet – large PDF with many exercises, stuff to do if you want to learn networks on your own `prosa-secure-network-2025-exercises.pdf`
- Additional resources from the internet like `firewall-book-10-DRAFT-PROSA.pdf`

Book: Practical Packet Analysis (PPA3)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1

https://nostarch.com/packetanalysis3 but also sometimes in https://www.humblebundle.com/books

Exercises and Prerequisites

Exercise theme: Virtual Machines allows us play with things

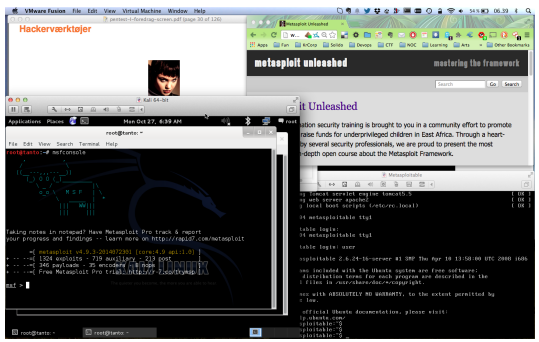
This course includes exercises and getting the most of the course requires the participants to carry out these practical exercises

One VM based on Debian, running various tools
https://codeberg.org/kramse/kramse-labs

Network security and most internet related security work has the following requirements:

- Network experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill** for infosec work
  – too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- **Hackersoftware: Kali Virtual Machine https://www.kali.org/**

Demo: output from running a git clone

```
user@Projects:tt$  git clone https://codeberg.org/kramse/kramse-labs.git
Cloning into 'kramse-labs'...
remote: Enumerating objects: 283, done.
remote: Total 283 (delta 0), reused 0 (delta 0), pack-reused 283
Receiving objects: 100% (283/283), 215.04 KiB | 898.00 KiB/s, done.
Resolving deltas: 100% (145/145), done.

user@Projects:tt$  cd kramse-labs/

user@Projects:kramse-labs$  ls
LICENSE  README.md  core-net-lab  lab-network  suricatazeek  work-station
user@Projects:kramse-labs$ git pull
Already up to date.
```

- Skills like these will allow you to run 100s or 1000s of applications, tools etc.!
- In the *docker-install* directory are Ansible YAML files to install Docker on Debian easily!

Look for *awesome lists* on various subjects

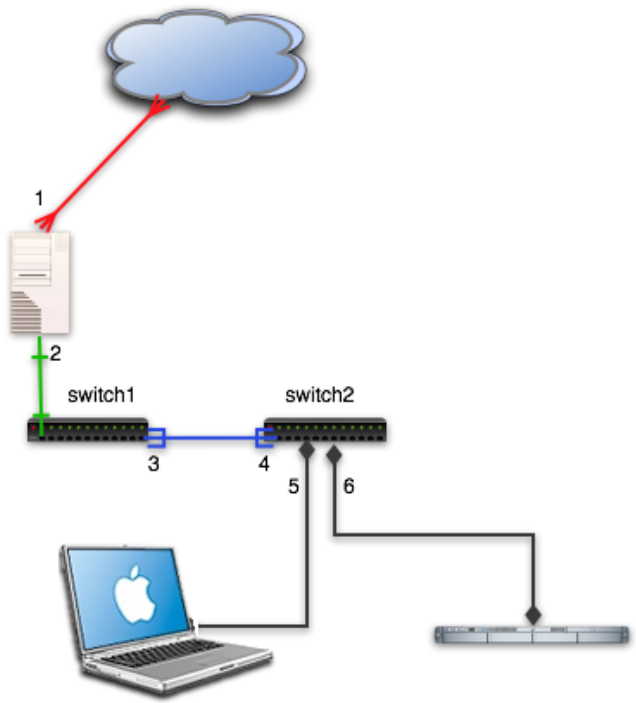
Your Network

.

I have a home network which has the following systems:

- OpenBSD router
- Juniper and small TP-Link switches
- UniFi wireless access-point

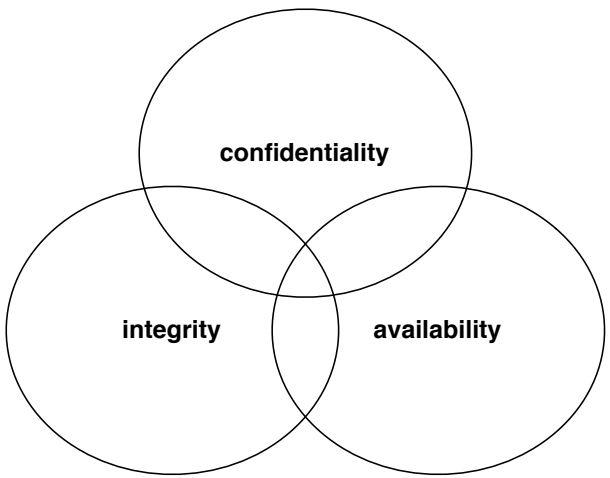
Due to online remote teaching - we will investigate other networks and scan across the internet to *my servers*!



Lab Networks

- When learning and investigating it is nice to have a *lab network* – make changes, play with settings, break things
- If you live alone, and are not in a remote meeting – play with you own network!
- I recommended the small GL-Inet Opal (GL-SFT1200) Wireless Travel Router
  https://store.gl-inet.com/products/opal-gigabit-wireless-pocket-sized-openwrt-ipv6-sft1200
- It has 2 LAN ports for connecting, 1 WAN port for Internet or can act as a Wi-Fi client. All powered by USB-C etc.
- Manual and documentation https://docs.gl-inet.com/router/en/4/user_guide/gl-sft1200/

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data kept secret

Integrity - data is not subject to unauthorized changes

Availability - data and system are available when needed

Unencrypted data protocols

Examples

- TFTP use UDP and is unencrypted
- TFTP still used for configuration files and firmwares
- FTP sends data in cleartext
  USER username
  PASS password
  Stop using FTP on the internet!
- DNS sending unencrypted on UDP and TCP
  Use DNS over HTTPS (DoH) or DNS over TLS (DoT)

Person in the middle attacks

ARP spoofing, ICMP redirects, the classics

Used to be called Man in The Middle (MiTM)

- ICMP redirect
- ARP spoofing
- Wireless listening and spoofing higher levels like airpwn-ng https://github.com/ICSec/airpwn-ng

Usually aimed at unencrypted protocols or redirecting clients to wrong sites

Recommended Reading

So to get started in network security I recommend learning the basics:

- Chapter 1: Packet Analysis and Network Basics
- Chapter 2: Tapping into the Wire
- Chapter 3: Introduction to Wireshark

Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition

TCP/IP Protocol Suite

Security Problems in the TCP/IP Protocol Suite

*S.M. Bellovin**
smb@ulysses.att.com

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

Skim if you like:

- *Security problems in the TCP/IP protocol suite*, S. M. Bellovin April 1989, https://www.cs.columbia.edu/~smb/papers/ipext.pdf
- *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 2004, https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

Still TCP/IP Problems?

Recent example from 2020:

> The JSOF research lab has discovered a series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Treck, Inc. The 19 vulnerabilities, given the name Ripple20, affect hundreds of millions of devices (or more) and include multiple remote code execution vulnerabilities.
>
> **Pre-emptive traffic filtering is an effective technique that can be applied as appropriate to your network environment.**

Source: https://www.jsof-tech.com/ripple20/

- I highly recommend mature and known technologies like firewalls – both network and hosts
- Isolation into different VLANs and zones
- Layer 2 attacks only work if you are in the same L2 zone!

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication

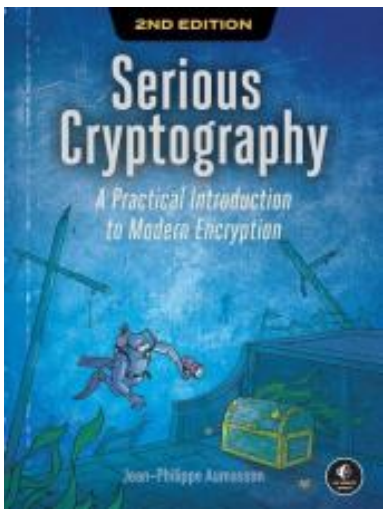
Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key, to ensure confidentiality, example algorithm AES

Public-key cryptography (like RSA) uses two related keys, a key pair of a public key and a private key. This allows for easier key exchanges, and can provide confidentiality, and methods for signatures and other services

Source: https://en.wikipedia.org/wiki/Cryptography

Serious Cryptography



Serious Cryptography, 2nd Edition A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson August 2024, 376 pp ISBN-13: 9781718503847 https://nostarch.com/serious-cryptography-2nd-edition

SMTP TLS

> The STARTTLS command for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 3207, for XMPP in RFC 6120 and for NNTP in RFC 4642. For IRC, the IRCv3 Working Group has defined the STARTTLS extension. FTP uses the command "AUTH TLS"defined in RFC 4217 and LDAP defines a protocol extension OID in RFC 2830. HTTP uses upgrade header.

SMTP was extended with support for Transport Layer Security TLS

Also called **Opportunistic TLS**, where the quote is also from:
https://en.wikipedia.org/wiki/Opportunistic_TLS

Now we have MTA Strict Transport Security (MTA-STS) RFC 8461
so we can announce that we only accept encrypted email!

It is 2025 you should ALL turn off unencrypted SMTP 🚩

DNS over TLS vs DNS over HTTPS - DNS encryption

- Protocols exist that encrypt DNS data
- Today we have competing standards:
- *Specification for DNS over Transport Layer Security (TLS)* (DoT), RFC7858 MAY 2016
  https://en.wikipedia.org/wiki/DNS_over_TLS
- *DNS Queries over HTTPS (DoH)* RFC8484
- How to cofigure DoT
  https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients

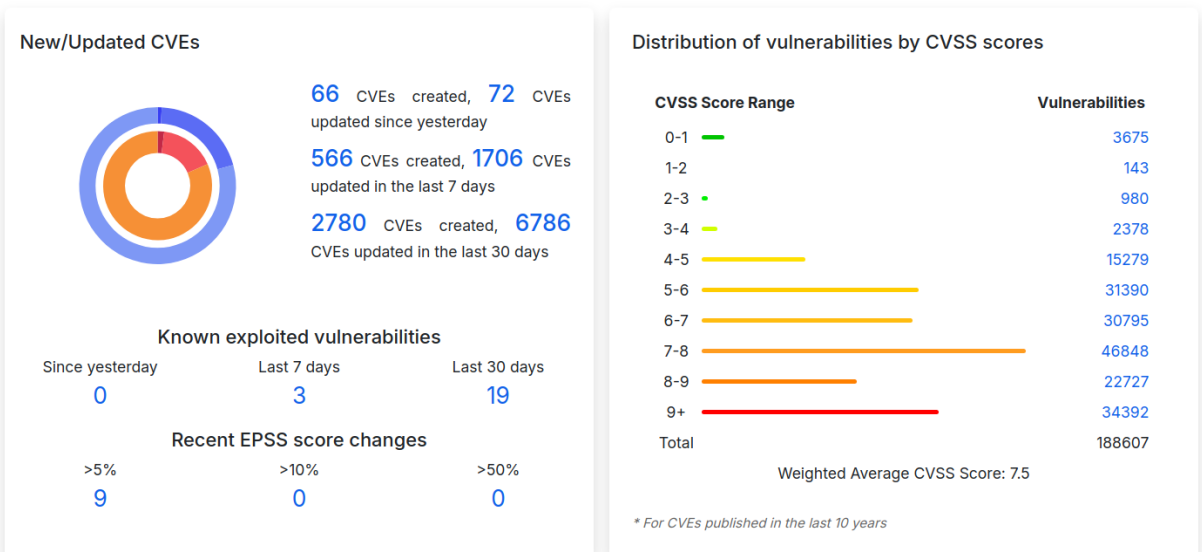
Linux Wireguard VPN

> WireGuard is a secure network tunnel, operating at layer 3, implemented as a kernel virtual network interface for Linux, which aims to replace both IPsec for most use cases, as well as popular user space and/or TLS-based solutions like OpenVPN, while being more secure, more performant, and easier to use.

Description from https://www.wireguard.com/papers/wireguard.pdf

- Very easy to setup!
- single round trip key exchange, based on NoiseIK
- Short pre-shared static keys—Curve25519
- strong perfect forward secrecy
- Transport speed is accomplished using ChaCha20Poly1305 authenticated-encryption
- encapsulation of packets in UDP
- WireGuard can be simply implemented for Linux in less than 4,000 lines of code, making it easily audited and verified

Security Vulnerabilities Have Dependencies



So you read about a new security vulnerability, it is bad!

- New vulns all the time, every day, week, month – year round

CVE-2025-49704 SharePoint Remote Code Execution July 2025

Bornholms Regionskommune under hackerangreb 22. juli 2025

Kommunens hjemmesider og intranet bliver lukket i fire timer, mens ny software bliver installeret for at stoppe angrebet.

Bornholms Regionskommune har været udsat for et omfattende hackerangreb.

Helt konkret er der tale om et angreb via en såkaldt zero day-sårbarhed i programmet **SharePoint fra Microsoft**, som benyttes til kommunens hjemmesider og intranet.

En zero day-sårbarhed er et sikkerhedshul, som endnu ikke er blevet lukket af virksomheden bag softwaren – i dette tilfælde Microsoft – og som derfor kan udnyttes af hackere til at opnå adgang.

– Vi er virkelig under et stort pres, men Microsoft har reageret hurtigt og er kommet med en opdatering, der kan løse problemet, siger Claus Munk, leder af Digitalisering, IT og AI i Bornholms Regionskommune.

Source: https://www.dr.dk/nyheder/bornholms-regionskommune-under-hackerangreb

- Probably CVE-2025-49704 see https://www.cvedetails.com/cve/CVE-2025-49704/ and CVE-2025-49706

CVE-2025-49706 & CVE-2025-49704 to get unauthorised RCE

On the evening of July 18, 2025, Eye Security was the first in identifying large-scale exploitation of a SharePoint remote code execution (RCE) vulnerability chain in the wild. Demonstrated just days before on X, this exploit is being used to compromise on-premise SharePoint Servers across the world. The chain we uncover in this blog combines CVE-2025-49706 & CVE-2025-49704 to get unauthorised RCE on unpatched SharePoint Servers.

After we learned about this chain being exploited in the wild, our team scanned over 23000 SharePoint servers worldwide. In total, we discovered more then 400 systems actively compromised during four confirmed waves of attack:

- confirmed initial wave on 17th of July at 12:51 UTC from 96.9.125[.]147 (probably testing)
- confirmed wave #1 on 18th of July at 18:06 UTC from 107.191.58[.]76 (widely successful)
- confirmed wave #2 on 19th of July at 07:28 UTC from 104.238.159[.]149
- confirmed multiple waves on and after 21th of July

Source: https://research.eye.security/sharepoint-under-siege/

Exploit Public-Facing Application

> Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.
>
> Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet-accessible open sockets.[1][2][3][4][5] On ESXi infrastructure, adversaries may exploit exposed OpenSLP services; they may alternatively exploit exposed VMware vCenter servers.[6][7] Depending on the flaw being exploited, this may also involve Exploitation for Defense Evasion or Exploitation for Client Execution.

Source: https://attack.mitre.org/techniques/T1190/

- Part of the Mitre ATT&CK Framework https://attack.mitre.org/

Weak password allowed hackers to sink a 158-year-old company

One password is believed to have been all it took for a ransomware gang to destroy a 158-year-old company and put 700 people out of work.

KNP - a Northamptonshire transport company - is just one of tens of thousands of UK businesses that have been hit by such attacks.

Big names such as M&S, Co-op and Harrods have all been attacked in recent months. The chief executive of Co-op confirmed last week that all 6.5 million of its members had had their data stolen.

In KNP's case, it's thought the hackers managed to gain entry to the computer system by guessing an employee's password, after which they encrypted the company's data and locked its internal systems.

KNP director Paul Abbott says he hasn't told the employee that their compromised password most likely led to the destruction of the company.

Source: https://www.bbc.com/news/articles/cx2gx28815wo July 2025

How to react to zero-days in zero-time?!

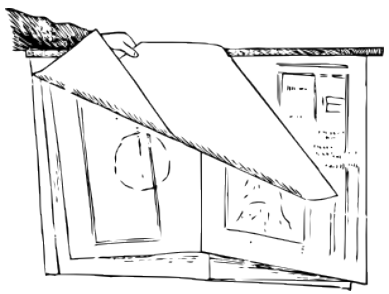
There will be vulnerabilities in the products you use – especially over a time frame of years!

So maybe, just maybe:

- Lock down administration
  Do NOT put your administrative interfaces directly on the Internet
  We can see ESXi web administration, router administration – on the internet
- Update your systems
  We see hacker exploiting known vulnerabilities much more than using *super advanced hitech state of the art exploits*
- Change default passwords
- Monitor your systems

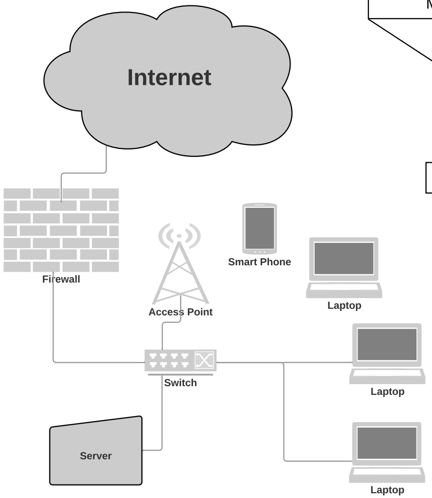
Essentially this boils down to design, architecture and defense in depth

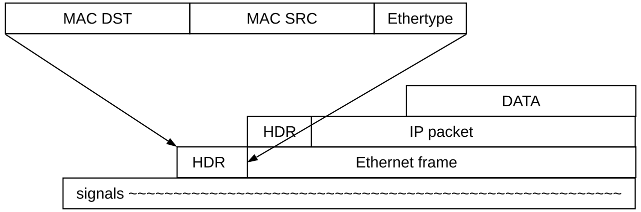
Design and Architecture



- Which systems need to communicate, which departments
- How strict are you allowed to make things
- Default allow – permissive, or default block – restrictive
- and what are the constraints, budgets, resources, time, money, ...
- I recommend using tools like Decision Records for making sure alternatives are considered etc. https://github.com/joelparkerhenderson/decision-record/blob/main/template/template.md

Protection, building secure and robust networks





Ethernet frames contain packets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

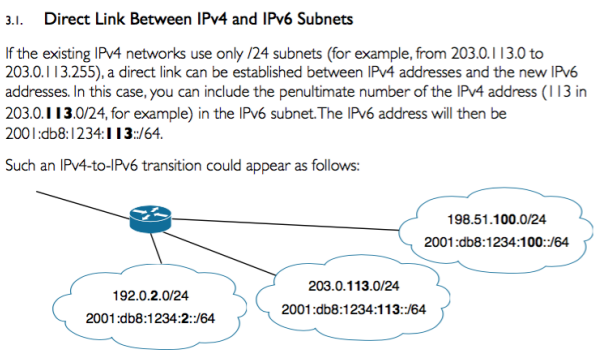
Address planning – helps security for both IPv4 and IPv6!

> IPv6 address allocations and overall architecture are important parts of securing IPv6. Initial designs, even if intended to be temporary, tend to last much longer than expected. Although IPv6 was initially thought to make renumbering easy, in practice, it may be extremely difficult to renumber without a proper IP Address Management (IPAM) system. [RFC7010] introduces the mechanisms that could be utilized for IPv6 site renumbering and tries to cover most of the explicit issues and requirements associated with IPv6 renumbering. **A key task for a successful IPv6 deployment is to prepare an addressing plan. Because an abundance of address space is available, structuring an address plan around both services and geographic locations allows address space to become a basis for more structured security policies to permit or deny services between geographic regions**. [RFC6177] documents some operational considerations of using different prefix sizes for address assignments at end sites.

Source: RFC 9099

- You have space, use it!

Network Architecture and Address planning



3.1. **Direct Link Between IPv4 and IPv6 Subnets**

If the existing IPv4 networks use only /24 subnets (for example, from 203.0.113.0 to 203.0.113.255), a direct link can be established between IPv4 addresses and the new IPv6 addresses. In this case, you can include the penultimate number of the IPv4 address (113 in 203.0.**113**.0/24, for example) in the IPv6 subnet. The IPv6 address will then be 2001:db8:1234:**113**::/64.

Such an IPv4-to-IPv6 transition could appear as follows:

Source: picture from Surfnet Preparing and IPv6 Address Plan

- Take the opportunity to re-design your network! Create a design, consider it green field, work towards it!
- Use /127 for point-to-point links, add loopback addresses on routers, allows filtering of access to management
- You can also make parts IPv6-only, Veronika McKillop at TROOPERS19 *Microsoft IT (secure) journey to IPv6-only* https://troopers.de/troopers19/agenda/h7sv7v/

Modern Firewall Infrastructures

A firewall blocks traffic on a network

A firewall allows traffic on a network

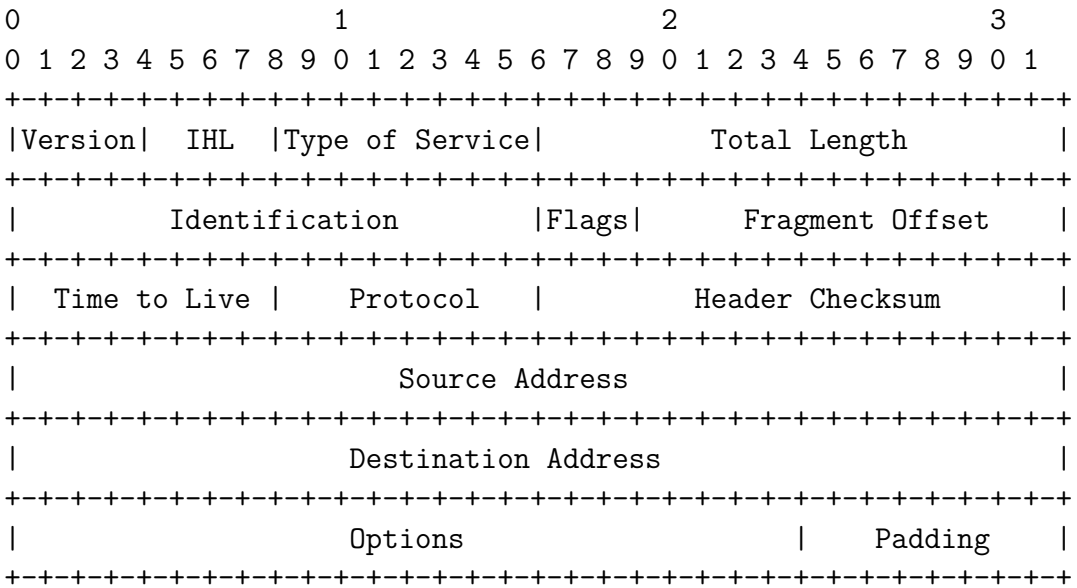
The interesting part is typically what it allows!

A firewall infrastructure must:

- Prevent attackers from entering
- Prevent data exfiltration
- Prevent worms, malware, virus from spreading in networks
- Be part of an overall solution with ISP, routers, other firewalls, switched infrastructures, intrusion detection systems and the rest of the infrastructure

Difficult – and requires design and secure operations

Packet Filtering



Packet filtering are firewall devices filtering on single packet

Most *specialized firewall devices* do stateful filtering and more

Don't forget IPv6 – even though you haven't turned it on, it is there

Modern Firewalls

Basically some filtering between networks or network segments

Typically they contain:

- Some interface, maybe web interface, often command line interface
- TCP/IP filtering options – packets flowing in and out, direction, protocol, ports etc.
- Should be able to handle both IPv6 and legacy IPv4
- Often they have predefined rules for common use-cases
  Is this really a good thing if you can easily configure a bad protocol like Server Message Block to and from the Internet?
- Most legacy setups use Network Address Translation (NAT) – NAT is a kludge and bad!
- Most platforms have extra network related features DHCP servers, DNS caching servers etc.

The firewall devices are mostly allowing some **stateful filtering** which are much easier to configure than a pure network packet filter

Goal is to implement rules – a security policy for isolation and data flow

Sample Rules from OpenBSD PF

```
# Gateway config inspired from https://www.openbsd.org/faq/pf/example1.html
set block-policy drop
set loginterface egress
set skip on lo0
wired = "em1"
table <martians> { 0.0.0.0/8 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0 169.254.0.0/16  }
match in all scrub (no-df random-id max-mss 1440)
match out on egress inet from !(egress:network) to any nat-to (egress:0)
antispoof quick for { egress $wired $wifi }
block in quick on egress from <martians> to any
block return out quick on egress from any to <martians>

block all
pass out quick inet
pass out quick inet6

pass in on { $wired } inet
pass in on { $wired } inet6
```

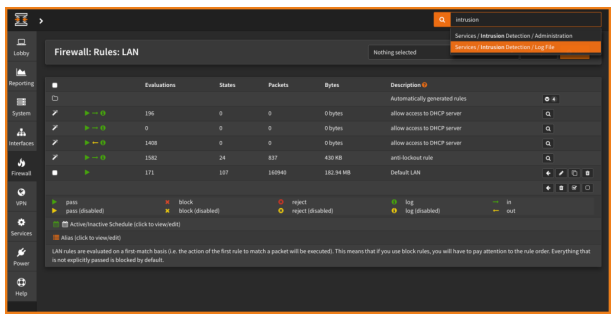
Note: the line with `block all` – default deny

Example Firewall Products

- Checkpoint Firewall-1 http://www.checkpoint.com
- Cisco ASA http://www.cisco.com
- Juniper SRX http://www.juniper.net
- Palo Alto https://www.paloaltonetworks.com/
- Fortinet https://www.fortinet.com/

Those listed are the most popular commercial ones I see in Denmark

OPNsense GUI based and easy to install



OPNsense https://opnsense.org/

Firewall built on FreeBSD with web interface

Originally thoughts from m0n0wall and later https://www.pfsense.org/

Danish companies have been using these for many years now

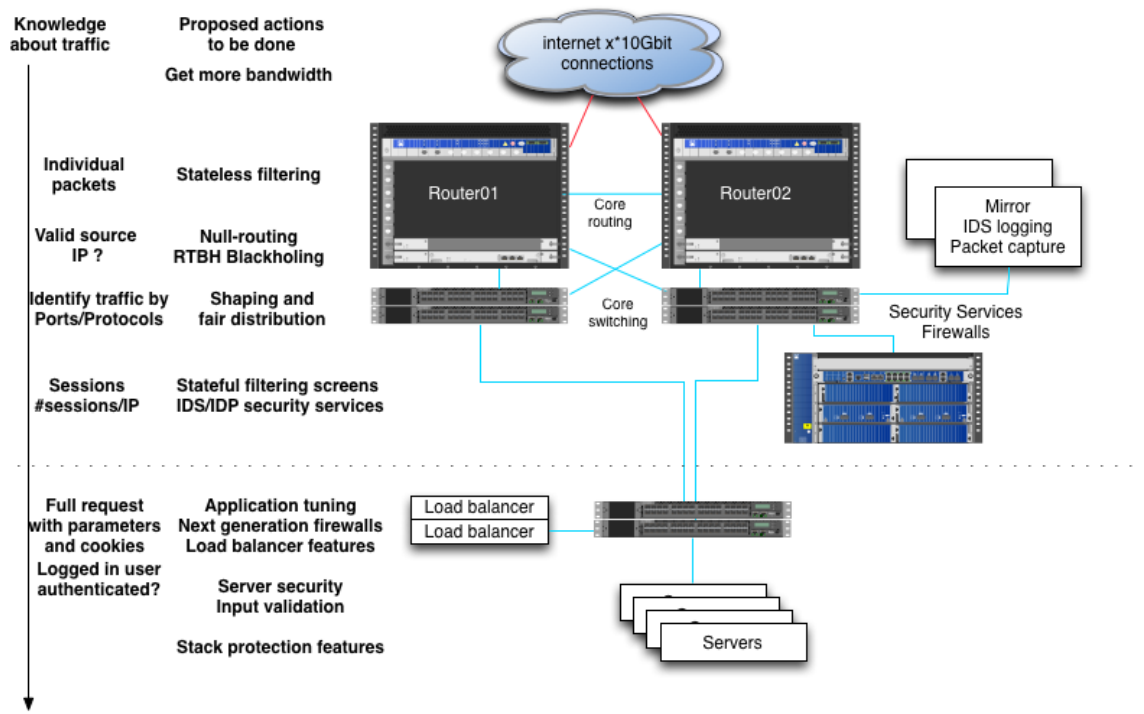
Uncomplicated Firewall (UFW)

```
root@debian01:~# apt install ufw
...
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

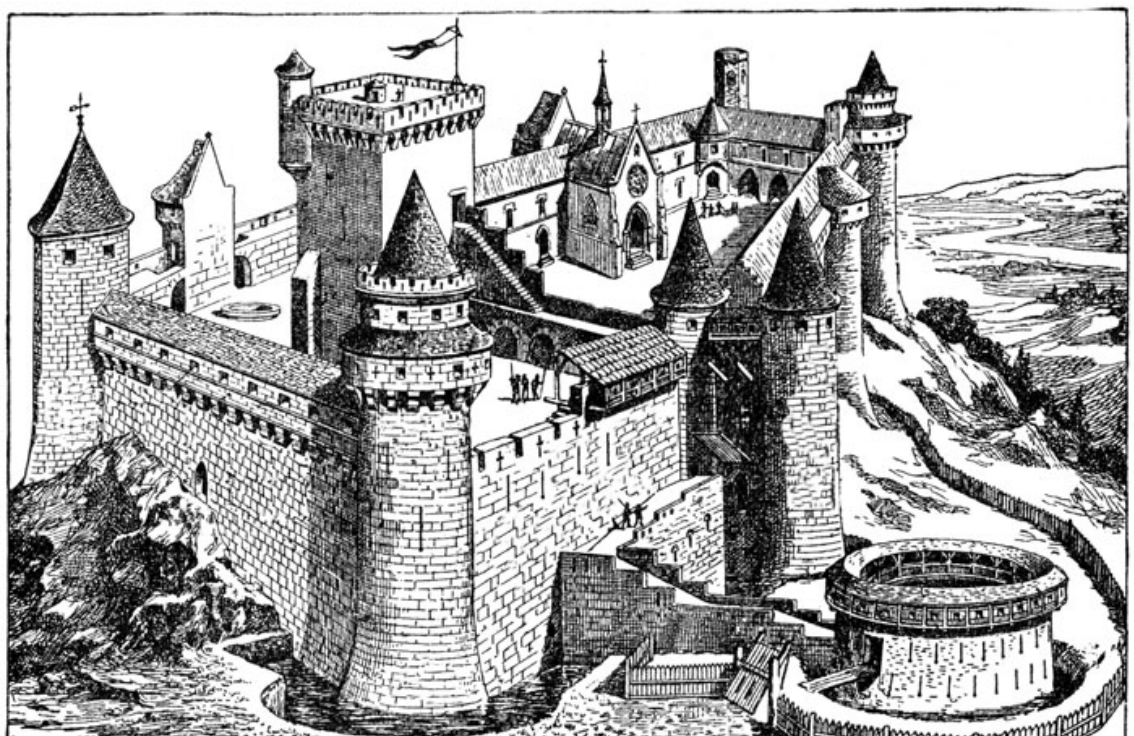
- Extremely easy to use – I recommend and use the (Uncomplicated Firewall) UFW
- All systems, Microsoft Windows, Unix etc. should have firewall enabled by now!

Specialized Firewall devices are NOT Alone



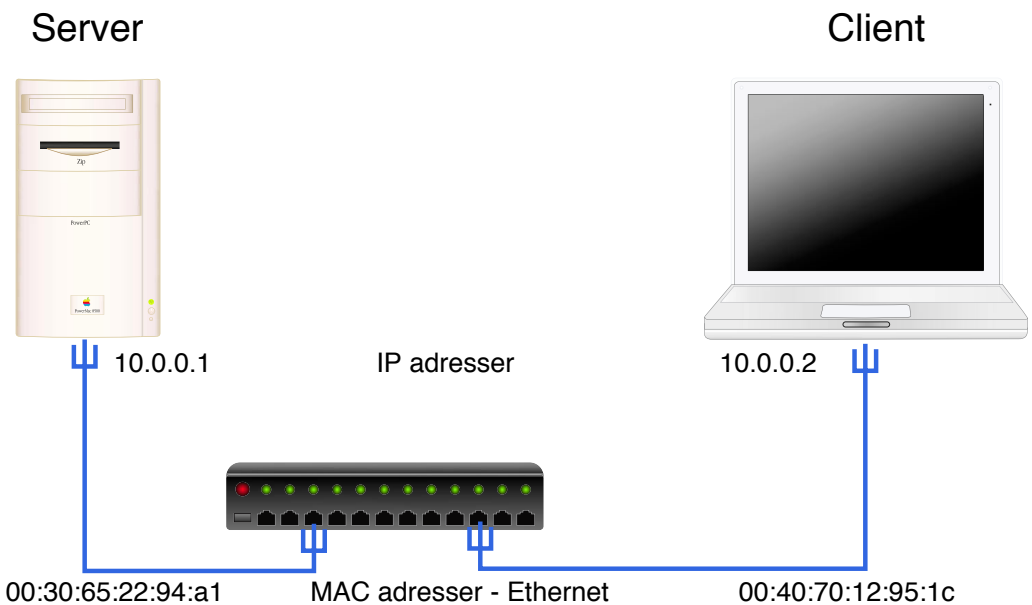
Use Defense in Depth – all layers have features

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

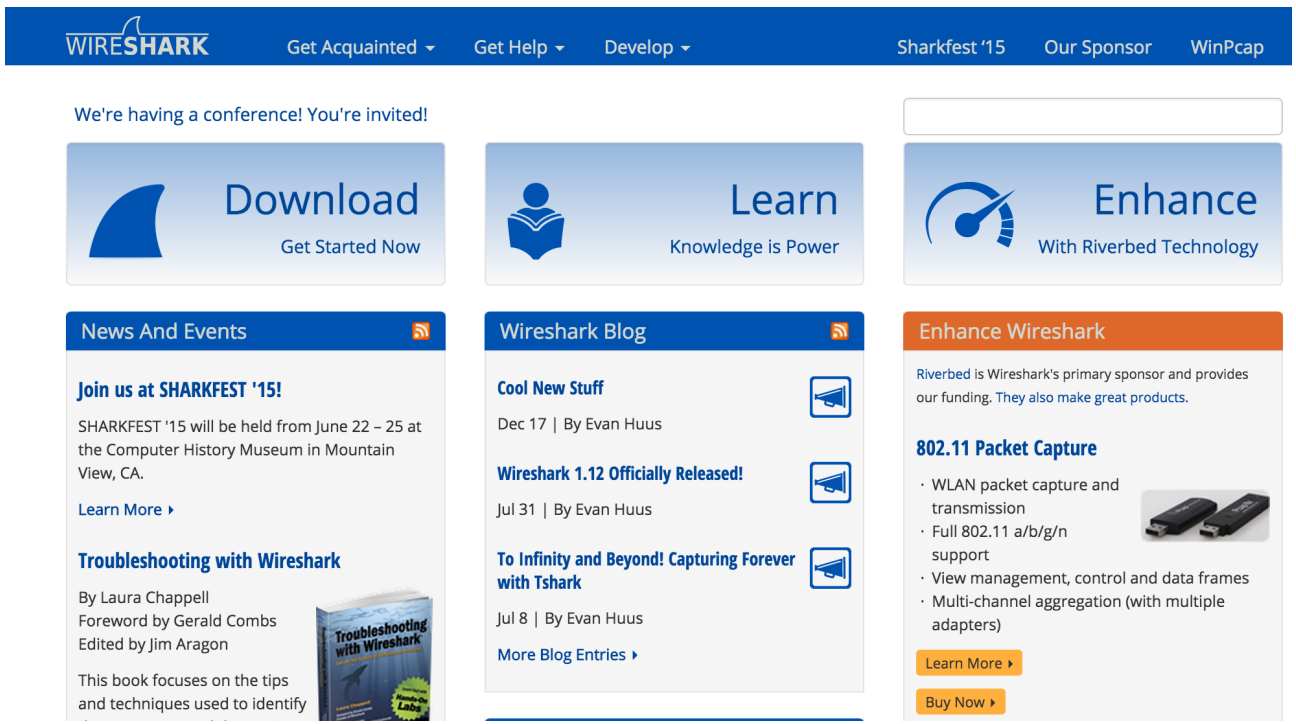
Address Resolution Protocol (ARP)



Systems that can communicate allow attackers access

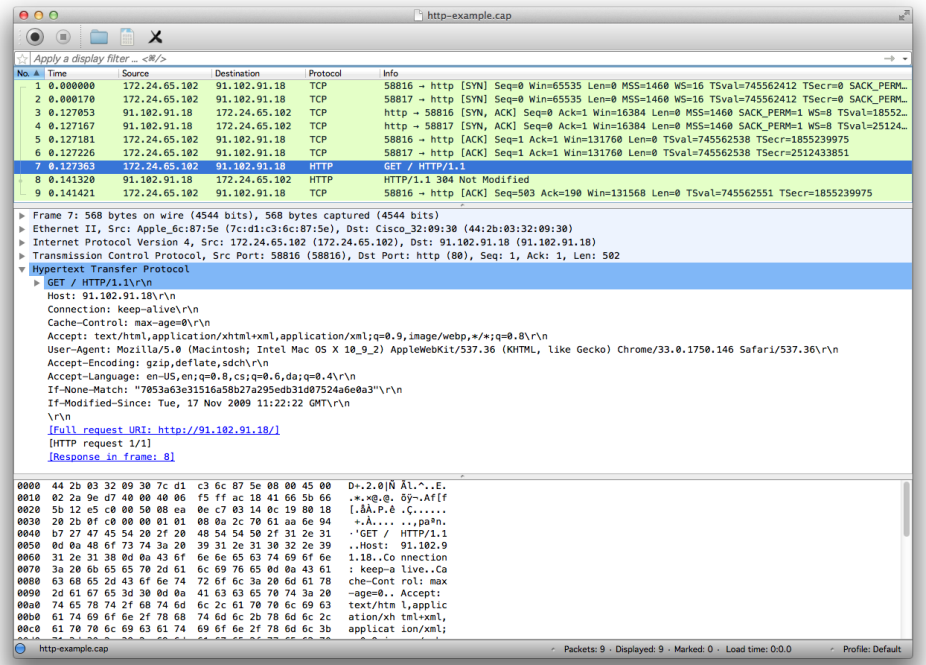
Hacking is not magical – if malware cannot *connect home* it cannot be controlled

Wireshark - graphical packet dump and analysis



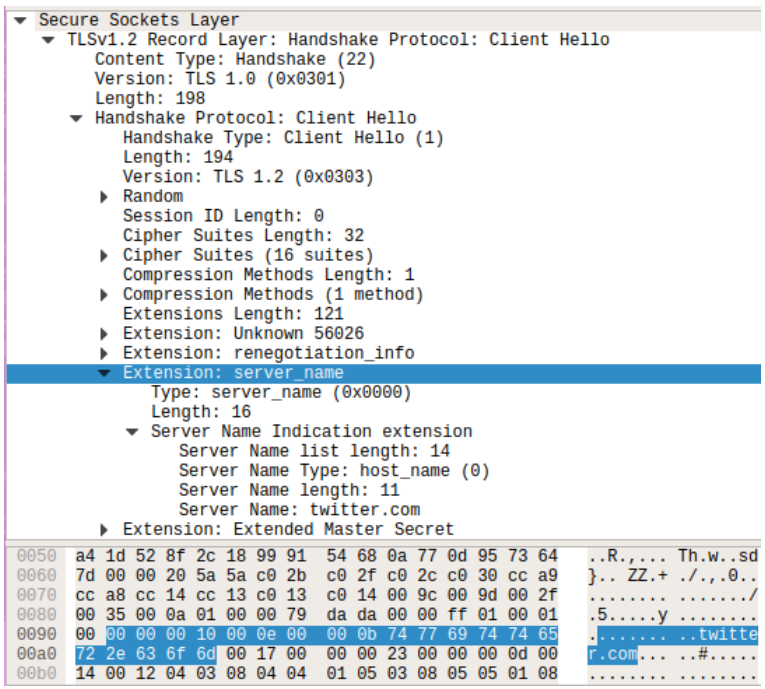
http://www.wireshark.org
Available for Windows and UNIX

Using Wireshark



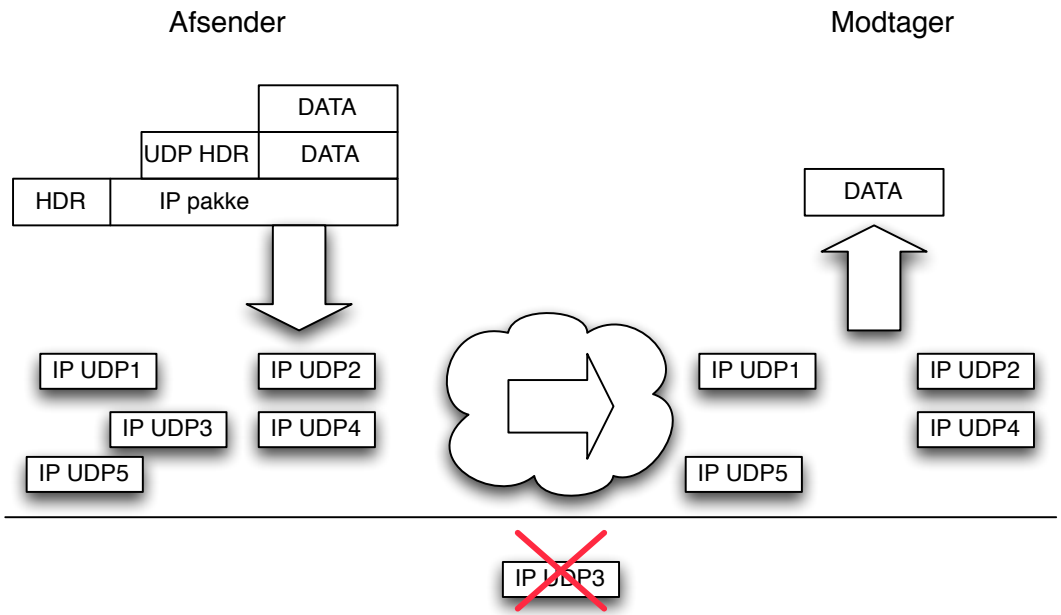
Capture - Options

What about encrypted traffic



Current TLS version 1.2 used in HTTPS show the name!

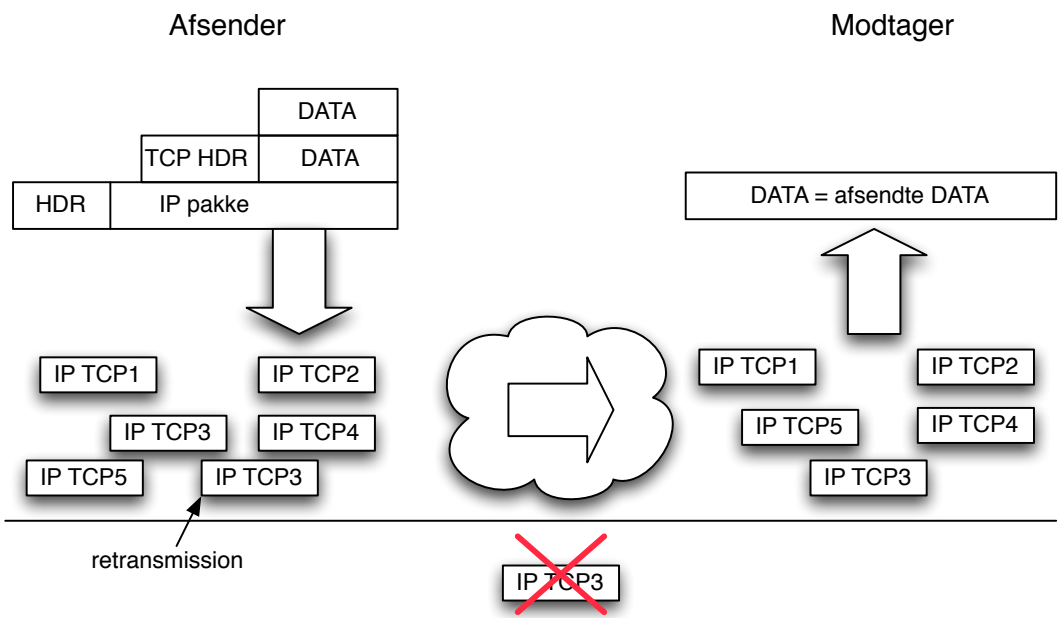
UDP User Datagram Protocol



RFC-768, *connection-less*

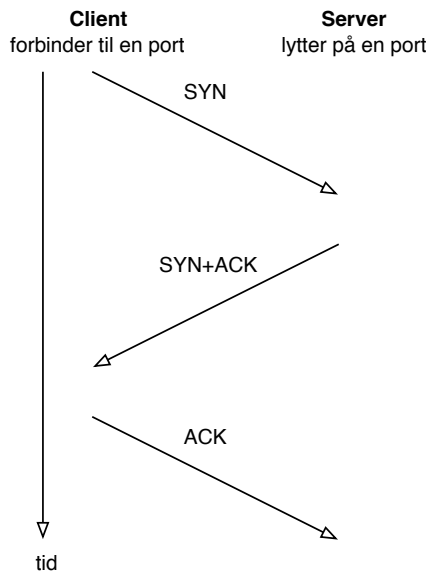
Source IP in UDP attacks may be *spoofed*

TCP Transmission Control Protocol



RFC-791 September 1981, *connection-oriented*

TCP three way handshake



- PPA chapter 8: Transport Layer Protocols
- **TCP SYN half-open** scans
- If the three way handshake is established – the source IP can be trusted in logs

Basic port scanning

What is a port scan

Testing all values possible for port number from 0/1 to 65535

Goal is to identify open ports, listening and vulnerable services

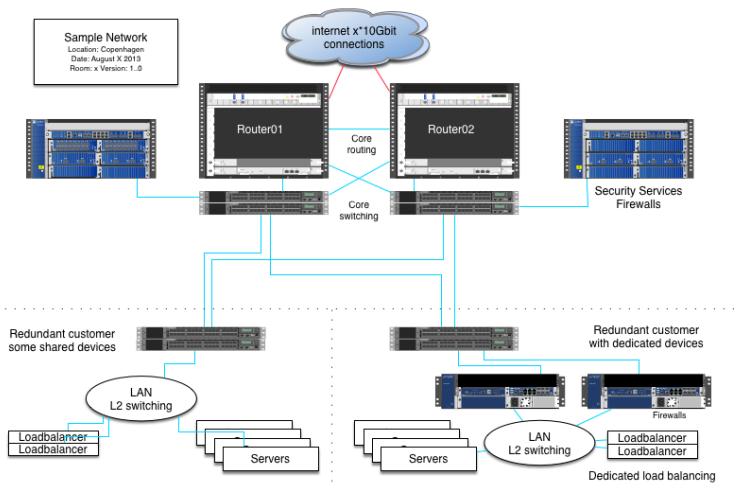
Most often TCP og UDP scan

TCP scanning is more realiable than UDP scanning

TCP handshake must respond with SYN-ACK packets

UDP applications respond differently – if they even respond
so probes with real requests may get response, no firewall they respond with ICMP on closed ports

Scope: select systems for testing



- Routers in front of critical systems and networks - availability
- Firewalls – are traffic flows restricted
- Mail servers – open for relaying
- Web servers – remote code execution in web systems, data download

Well-Known Port Numbers

IANA maintains a list of magical numbers in TCP/IP

Lists of protocl numbers, port numers etc.

A few notable examples:

- Port 25/tcp Simple Mail Transfer Protocol (SMTP)
- Port 53/udp and 53/tcp Domain Name System (DNS)
- Port 80/tcp Hyper Text Transfer Protocol (HTTP)
- Port 443/tcp HTTP over TLS/SSL (HTTPS)

Source: http://www.iana.org

Ping and port sweep

Scans across the network are named sweeps

Ping sweeps using ICMP Ping probes

Port sweep trying to find a specific service, like port 80 web

Quite easy to see in network traffic:

- Selecting two IP-adresser not in use
- Should not see any traffic, but if it does, its being scanned
- If traffic is received on both addresses, its a sweep – if they are a bit apart it is even better, like 10.0.0.100 and 10.0.0.200

Pro tip: a Great network intrusion detection engine (IDS), is Suricata suricata-ids.org

what is Nmap today

> Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

Initial release September 1997;

Today a package of programs for Windows, Mac, BSD, Linux, ... source

Flexible, powerful, and free! Includes other tools!

Lets check release notes: http://seclists.org/nmap-announce/

Bonus info: you can help Nmap by submitting fingerprints

Nmap port sweep for web servers

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap port sweep for SNMP port 161/UDP

```
root@cornerstone:~# nmap -sU -p 161 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:30 CET
Nmap scan report for 172.29.0.1
Host is up (0.00015s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00011s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:0C:29:46:22:FB (VMware)
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

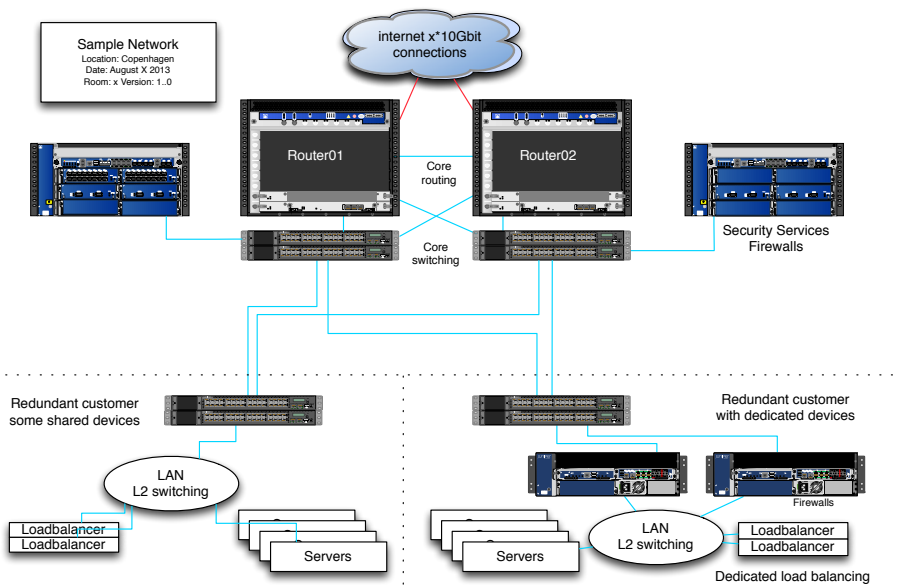
More reliable to use Nmap script with probes like –script=snmp-info

Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Low-level way to identify operating systems, also try/use `nmap -A`
- Send probes and observe responses, lookup in table of known OS and responses
- Techniques known since at least: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

DDoS protection and flooding



- Transport Layer Attacks TCP SYN flood TCP sequence numbers
- High level attacks like Slowloris - keep TCP/HTTP connection for a long time.

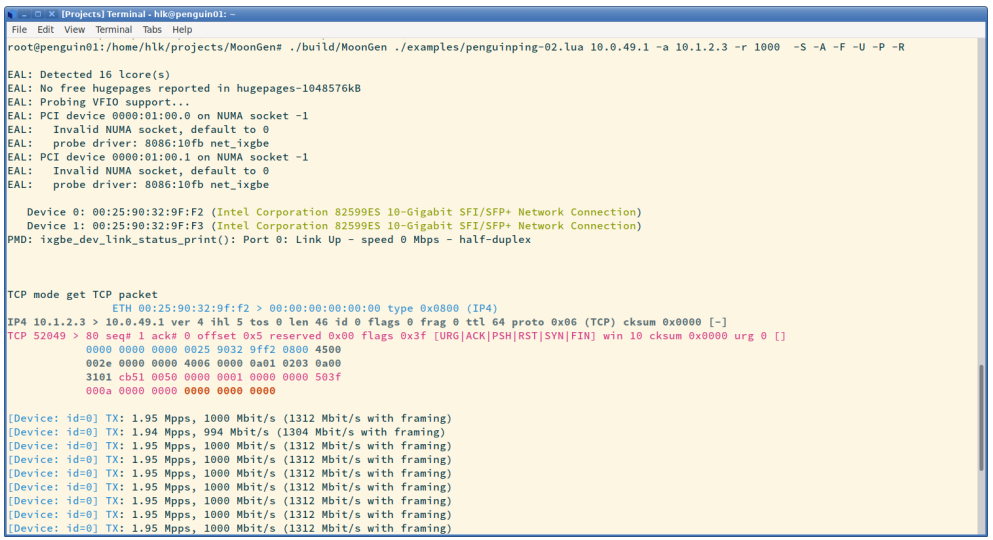
Availability and Network flooding attacks

- SYN flood is the most basic and very common on the internet towards 80/tcp and 443/tcp
- ICMP and UDP flooding are the next targets
- Supporting litterature is TCP Synfloods - an old yet current problem, and improving pf's response to it, Henning Brauer, BSDCan 2017
- All of them try to use up some resources
- Memory space in specific sections of the kernel, TCP state, firewalls state, number of concurrent sessions/connections
- interrupt processing of packets - packets per second
- CPU processing in firewalls, pps
- CPU processing in server software
- Bandwidth - megabits per second mbps

There are multiple resources about DDoS protection with more low level technical measures to implement at

https://codeberg.org/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing

Stress testing and DDoS



```
root@penguin01:/home/hlk/projects/MoonGen# ./build/MoonGen ./examples/penguinping-02.lua 10.0.49.1 -a 10.1.2.3 -r 1000  -S -A -F -U -P -R

EAL: Detected 16 lcore(s)
EAL: No free hugepages reported in hugepages-1048576kB
EAL: Probing VFIO support...
EAL: PCI device 0000:01:00.0 on NUMA socket -1
EAL:   Invalid NUMA socket, default to 0
EAL:   probe driver: 8086:10fb net_ixgbe
EAL: PCI device 0000:01:00.1 on NUMA socket -1
EAL:   Invalid NUMA socket, default to 0
EAL:   probe driver: 8086:10fb net_ixgbe

   Device 0: 00:25:90:32:9F:F2 (Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection)
   Device 1: 00:25:90:32:9F:F3 (Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection)
PMD: ixgbe_dev_link_status_print(): Port 0: Link Up - speed 0 Mbps - half-duplex



TCP mode get TCP packet
                ETH 00:25:90:32:9f:f2 > 00:00:00:00:00:00 type 0x0800 (IP4)
IP4 10.1.2.3 > 10.0.49.1 ver 4 ihl 5 tos 0 len 46 id 0 flags 0 frag 0 ttl 64 proto 0x06 (TCP) cksum 0x0000 [-]
TCP 52049 > 80 seq# 1 ack# 0 offset 0x5 reserved 0x00 flags 0x3f [URG|ACK|PSH|RST|SYN|FIN] win 10 cksum 0x0000 urg 0 []
            0000 0000 0000 0025 9032 9ff2 0800 4500
            002e 0000 0000 4006 0000 0a01 0203 0a00
            3101 cb51 0050 0000 0001 0000 0000 503f
            000a 0000 0000 0000 0000 0000

[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.94 Mpps, 994 Mbit/s (1304 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
[Device: id=0] TX: 1.95 Mpps, 1000 Mbit/s (1312 Mbit/s with framing)
```

- PenguinPing packet generator, my high speed packet generator home page: https://penguinping.org
- First versions are only about 230 lines of Lua code and implement basic command line to replace hping3
- Built on top of MoonGen/libmoon https://github.com/emmericp/MoonGen

Extremely fast and allows easy customization

Process: monitor, attack, break, repeat

- Pre-test: Monitoring setup - from multiple points
- Pre-test: Perform full Nmap scan of network and ports
- Start small, run with delays between packets
- Turn up until it breaks, decrease delay - until using `--flood`
- Monitor speed of attack on your router interface pps/bandwidth
- Give it maximum speed
  `hping3 --flood -1` and `hping3 --flood -2`
- Have a common chat with network operators/customer to talk about symptoms and things observed
- Any information resulting from testing is good information

Ohh we lost our VPN into the environment, ohh the fw console is dead

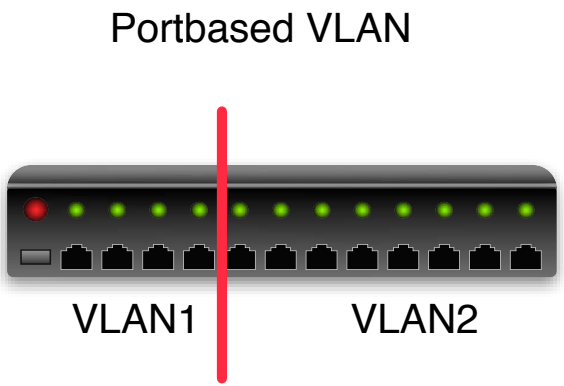
Best Current Practice

Lets get this documented, you should already be doing

- Network segmentation and filtering – we could write a book about this! 🚩
- Monitor your network – both bandwidth, error, netflow etc. 🚩
- Take control of your network, no more admin/admin logins on core devices 🚩
- Turn on authentication for protocols – routing protocols but also any http service within your org 🚩
- Configure host-based firewalls 🚩
- Control DNS – internally and externally, recursive, authoritative etc. 🚩

This goes for IPv4-only, IPv6-only, and mixed networks!

Together with Firewalls - Virtual LAN (VLAN)



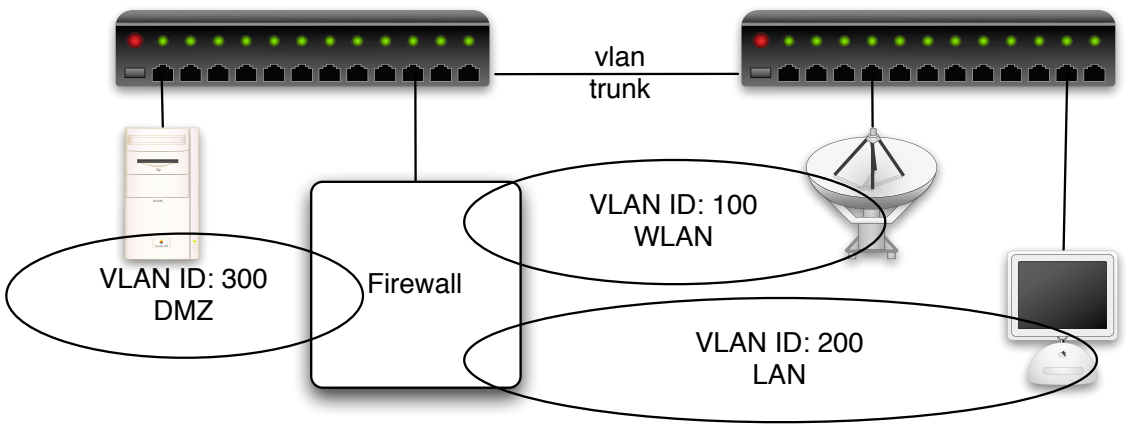
Managed switches often allow splitting into zones called virtual LANs

Most simple version is port based

Like putting ports 1-4 into one LAN and remaining in another LAN

Packets must traverse a router or firewall to cross between VLANs

Virtual LAN (VLAN) IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

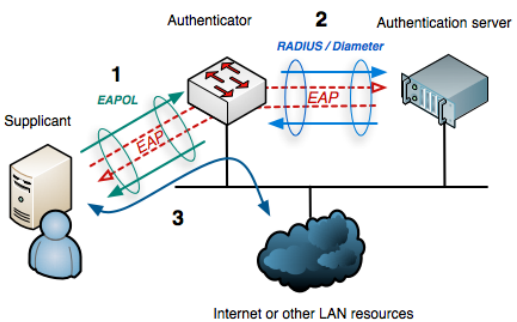
Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

Used in most, if not all, Wi-Fi networks – each SSID has a VLAN behind it

Network Access Control – Connecting clients more securely

Talking about standard, another useful one:
IEEE 802.1x – Port Based Network Access Control



Authentication protocol ensures user validation before port access

Can authenticate using username and then password or certificate

Typically RADIUS and 802.1x which can use LDAP or Active Directory

Already used in Wi-Fi networks, so can be turned on for wired Ethernet ports

Creating an Access Control List (ACL)

```
(config)#ipv6 access-list RA-GUARD
(config-ipv6-acl)#sequence 3 deny icmp any any router-advertisement
(config-ipv6-acl)#sequence 6 permit ipv6 any any
(config-ipv6-acl)#exit
(config)#interface FastEthernet0/5
(config-if)#ipv6 traffic-filter RA-GUARD in
```

Source: example copied from RIPE NCC IPv6 Security Training materials:
https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf

- Best practice, and not that hard to do – Layer 2 protection
- ACL, filtering and firewalling will create longer lasting protection
- Paired with a nice address plan you can easily put restrictions on traffic flow, without hurting functionality or the business
- Does ANY client in ANY office NEEEEEED to connect to ANY UPS, Virtualisation and printer across the world ...

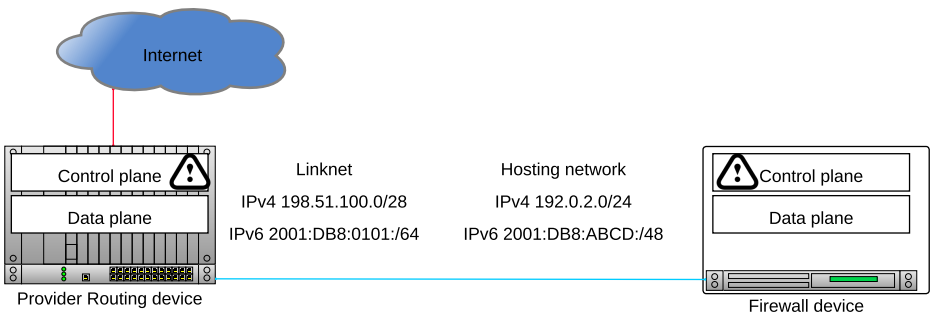
Example high level blueprint and process

- Create an address plan that matches the organisation, physical restrictions, cloud, on-premise etc.
- Create security policies from a high level, top-level mission, Information security management system (ISMS) if you have resources
- Map out the current network
- Implement changes that you can now
- Make procedures and requirements for new systems
- Start migration or phasing out older systems that do not follow guidelines and requirements

and for forensics purposes start logging!

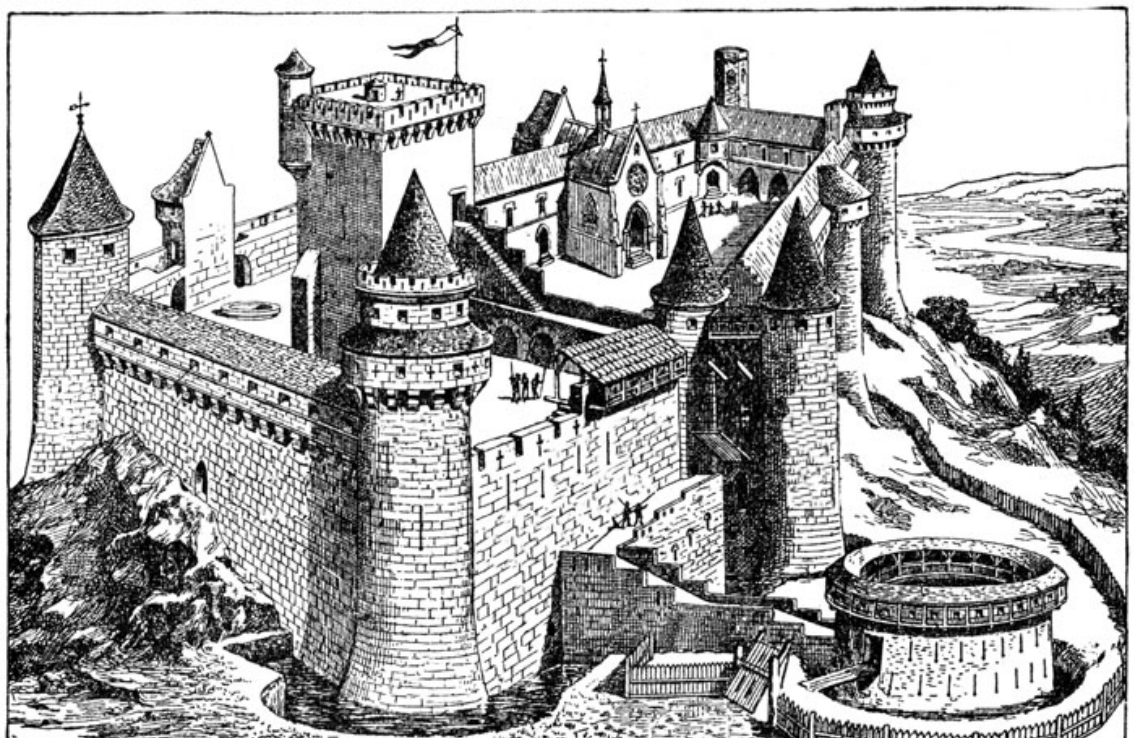
Note: I recommend logging in controlled networks, I do NOT condone mass sureveillance!

Lock down management



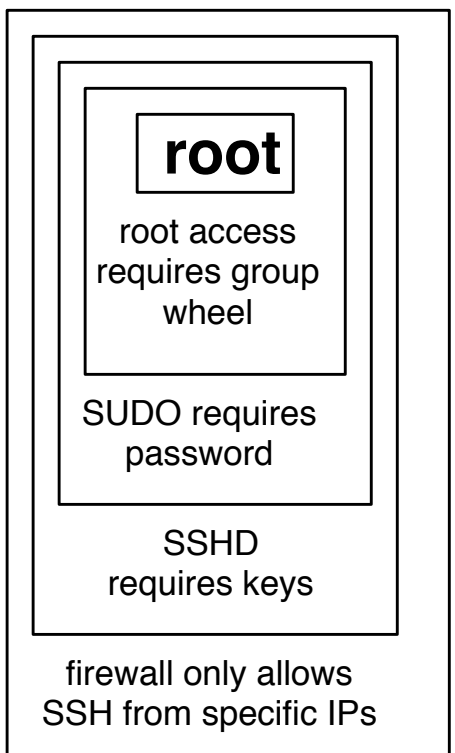
Routers often have a control plane and a data plane. The first is controlling the device, and provides management, while the data plane is forwarding and routing the packets. The data plane is mostly hardware based on high-end devices, and can forward at full wire speed.

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

Defense in depth - layered security



Multiple layers of security! Isolation!

Control-Plane Access Control Lists (CP-ACL)

Management of network devices can be done with Access Control lists, other systems may be put into a management VLAN

An example from a Cisco router using secure shell is shown below with a simple standard Access Control List (ACL) named 22 and then referenced for the virtual terminal (vty) secure shell (ssh):

```
ip access-list standard 22
10 permit 192.0.2.2
20 permit 172.13.22.10
30 permit 192.168.0.10
40 permit 203.0.113.10
line vty 0 4
  access-class 22 in
  transport input ssh
```

This will reduce the likelihood that an attacker can gain access to the administration using leaked username and passwords or because of vulnerabilities in the software.

Network Segmentation: Which VLANs to create

Using VLANs to segment networks we can extend it to the rest of the network, and an example of isolated segments could be:

- Guest network for cabled and Wi-Fi clients
- Client networks can be isolated per department, floor or building
- Server networks for multiple purposes – development, staging, testing, production, manufacturing, ...
- Internet servers in a demilitarized zone (DMZ)4 which would make it less likely that compromised internet server would affect the rest of the network
- Dedicated printer network
- Management network for virtualisation, one for network management, one for storage

Block outgoing traffic too

Some services should *not* cross firewalls, at least not to the internet

Some services are too *fragile*

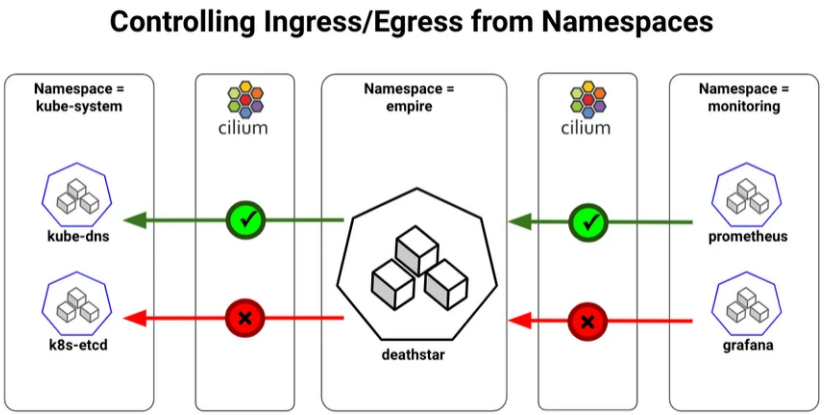
- Windows SMB file sharing is *only* for small internal networks
- Unix NFS is like-wise *only* for internal use
- Outgoing email should only go via dedicated relays
- LDAP outgoing, why?! See the log4j CVE-2021-44228
- Create a list, document them and consider them dead!

Making a positive list of allowed protocols would be best, but may require too many resources to implement and update

Proxy servers and Web Application Firewalls (WAF)

- Filtrering at higher layers is also possible
- Web proxies for clients can help security a lot – a centralized filter for everyone
- Reverse proxies for web applications are called Web Application Firewalls (WAF) – and filter incoming web requests, and outgoing answers. Can help with attacks like SQL injection and exfiltration of data
- Depending on your network it can replace or be combined with filtering on DNS servers, and I would prefer to filter domains with DNS
- I would also prefer blocking large prefixes of IP destinations using routers/stateless packet filters – maybe use BGP for distributing *lists*

Cloud Network Security: Cilium overview



Kubernetes provides Network Policies for controlling traffic going in and out of the pods. Cilium implements the Kubernetes Network Policies for L3/L4 level and extends with L7 policies for granular API-level security for common protocols such as HTTP, Kafka, gRPC, etc

Source: picture and text from https://cilium.io/blog/2018/09/19/kubernetes-network-policies/

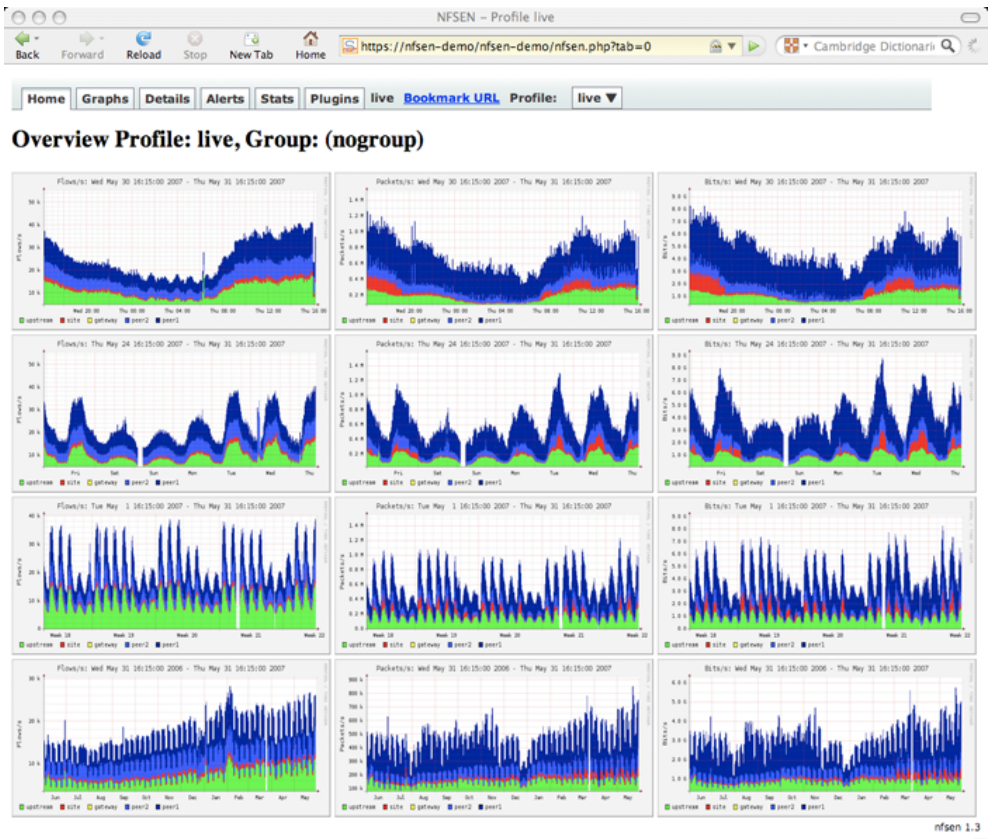
Logging and Monitoring

- This part is only a quick overview – next modules will dive deeper!

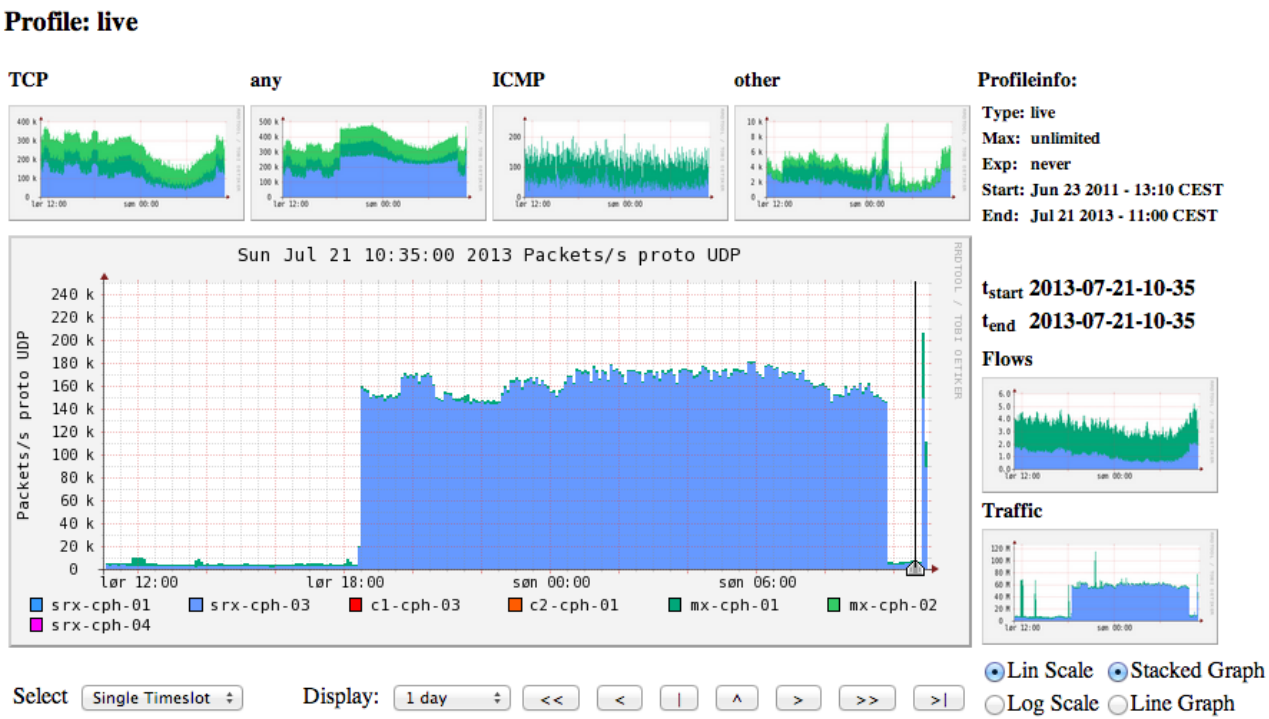
Netflow and Session Logging

- Netflow is getting more important, more data share the same links
- Accounting is important
- Detecting DoS/DDoS and problems is essential
- Netflow sampling is vital information - 123Mbit, but what kind of traffic
- NFSen is an old but free application http://nfsen.sourceforge.net/
- Currently also investigating sFlow - hopefully more fine grained
- sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model, https://en.wikipedia.org/wiki/SFlow

Netflow using NFSen



Netflow NFSen



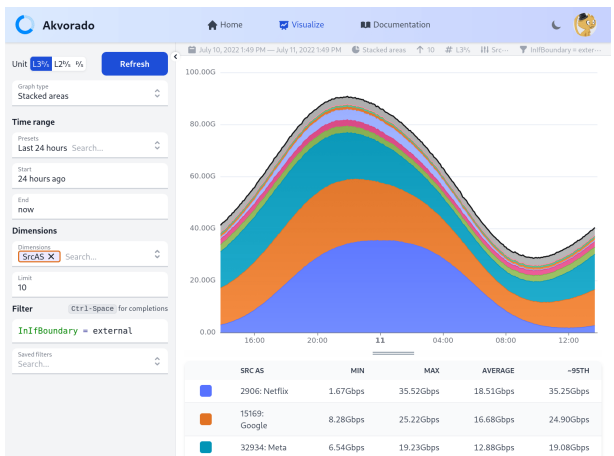
An extra 100k packets per second from this netflow source (source is a router)

ElastiFlow – Elasticsearch based

ElastiFlow™ provides network flow data collection and visualization using the Elastic Stack (Elasticsearch, Logstash and Kibana). It supports Netflow v5/v9, sFlow and IPFIX flow types (1.x versions support only Netflow v5/v9).

Source: Picture and text from https://github.com/robcowart/elastiflow

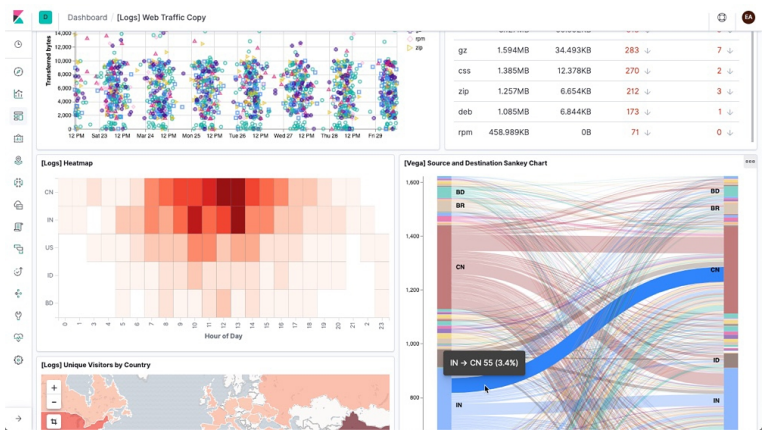
Akvorado: flow collector, enricher and visualizer



This program receives flows (currently Netflow/IPFIX and sFlow), enriches them with interface names (using SNMP), geo information (using IPinfo.io), and exports them to Kafka, then ClickHouse. It also exposes a web interface to browse the collected data.

Source: Picture and text from https://github.com/akvorado/akvorado

Big Data tools: Elasticsearch and Kibana



Elasticsearch is an open source distributed, RESTful search and analytics engine capable of solving a growing number of use cases.

https://www.elastic.co

DNS logging

Since most malware uses DNS today, to be able to switch to new command and control endpoints, we can leverage that to our advantage.

Domain Name System (DNS) depends on a query from the client, and a server that resolves this to a value.

- We can log any DNS traffic into a database
- We can look up if any clients have done a lookup for a specific name or IP during incident handling
- This can confirm if a client has ever *visited* a malicious site, because first it needs to lookup the name to IP address before it can make the TCP/HTTP connection, or send data

Unbound and NSD

Unbound is a validating, recursive, caching DNS resolver. It is designed to be fast and lean and incorporates modern features based on open standards.

To help increase online privacy, Unbound supports DNS-over-TLS which allows clients to encrypt their communication. In addition, it supports various modern standards that limit the amount of data exchanged with authoritative servers.

https://www.nlnetlabs.nl/projects/unbound/about/

My preferred local DNS server.

Also check out uncensored DNS and his DNS over TLS setup!
Even has pinning information available:
https://blog.censurfridns.dk/blog/32-dns-over-tls-pinning-information-for-unicastcensurfridnsdk/

Building Secure Infrastructures

A real-life setup of an infrastructure from scratch can be daunting!

You need:

- Policies
- Procedures
- Incident Response

Running systems which require

- Configurations
- Settings
- Supporting infrastructure – networks
- Supporting infrastructure – logging, dash boarding, monitoring

Building something *secure* is **hard work!**

Concrete advice for enterprise networks

- Portscanning - start using portscans in your networks, verify how far malware and hackers can travel, and identify soft systems needing updates or isolation
- Have separation – anywhere, starting with organisation units, management networks, server networks, customers, guests, LAN, WAN, Mail, web, ...
- Use Web proxies - do not allow HTTP directly except for a short allow list,
  do not allow traffic to and from any new TLD
- Use only your own DNS servers, create a pair of Unbound servers,
  point your internal DNS running on Windows to these
  Create filtering, logging, restrictions on these Unbound DNS servers
  https://www.nlnetlabs.nl/projects/unbound/about/ and also https://pi-hole.net/
- Only allow SMTP via your own mail servers, create a simple forwarder if you must

Allow lists are better than block list, even if it takes some time to do it

DROP SOME TRAFFIC NOW

- Drop some traffic on the border of everything
- Seriously do NOT allow Windows RPC across borders
- Border here may be from regional country office back to HQ
- Border may be from internet to internal networks
- Block Windows RPC ports, 135, 137, 139, 445
- Block DNS directly to internet, do not allow clients to use any DNS, fake 8.8.8.8 if you must internally
- Block SMTP directly to internet
- Create allow list for internal networks, client networks should not contact other client networks but only relevant server networks

You DONT need to allow direct DNS towards internet, except from your own recursive DNS servers

If you get hacked by Windows RPC in 2022, you probably deserve it, sorry for being blunt

Best would be to analyze traffic and create allow lists, some internal networks to not need internet at all

Default permit

One of the early implementers of firewalls Marcus J. Ranum summarized in 2005 The Six Dumbest Ideas in Computer Security https://www.ranum.com/security/computer_security/editorials/dumb/ which includes the always appropriate discussion about default permit versus default deny.

> **#1) Default Permit**
> This dumb idea crops up in a lot of different forms; it's incredibly persistent and difficult to eradicate. Why? Because it's so attractive. Systems based on "Default Permit" are the computer security equivalent of empty calories: tasty, yet fattening.
>
> The most recognizable form in which the "Default Permit" dumb idea manifests itself is in firewall rules. Back in the very early days of computer security, network managers would set up an internet connection and decide to secure it by turning off incoming telnet, incoming rlogin, and incoming FTP. Everything else was allowed through, hence the name "Default Permit." This put the security practitioner in an endless arms-race with the hackers.

- Allow all current networks today on all ports for all protocols *is* an allow list
  Which tomorrow can be split into one for TCP, UDP and remaining, and measured upon
- Measure, improve, repeat

We cannot do X

> We cannot block SMTP from internal networks, since we do not know for sure if vendor X equipment needs to send the MOST important email alert at some unspecific time in the future

Cool, then we can do an allow list starting today on our border firewall:

```
table <smtp-exchange> { $exchange1 $exchange2 $exchange3 }
table <smtp-unknown> persist file "/firewall/mail/smtp-internal-unknown.txt"
# Regular use, allowed
pass out on egress inet proto tcp from smtp-exchange to any port 25/tcp
# Unknown, remove when phased out
pass out on egress inet proto tcp from smtp-unknown to any port 25/tcp
```

Year 0 the unknown list may be 100% of all internal networks, but new networks added to infrastructure are NOT added, so list will shrink – evaluate the list, and compare to network logs, did networks send ANY SMTP for 1,2,3 years?

Conclusion

- Implement firewalls – take control over network packets
- Read the Fine manuals – your devices already has a lot to offer
- Make a policy for networks, make incremental changes, configure security for new parts and VLANs in the network
  Over time the older ones will be phased out, replaced or can have the same configuration applied with little trouble
- Start from the bottom and from client ports, or from server ports if you like
- Learn some Linux and use open source projects, really, will save you thosands of USD/EUR/DKK