



Welcome to

13. Running a Modern Network

Communication and Network Security 2023

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

Slides are available as PDF, [kramse@Github](#) 

13-Running-a-Modern-Network.tex in the repo [security-courses](#)

Plan for today



Subjects

- BCP38 RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- Mutually Agreed Norms for Routing Security (MANRS)
- Testing security, evaluating and reporting
- Hardened network device configurations
- Jump hosts and management networks
- DDoS protection
- Check you network from outside RIPEstat, BGPmon

Exercises

- Look at your own networks, from the outside

Reading Summary



Browse

<https://www.manrs.org/>

and read this

https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf

Browse / skim this:

<https://tools.ietf.org/pdf/bcp38.pdf>

RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks

Infrastrukturer i praksis



Vi vil nu gennemgå netværksdesign med udgangspunkt i vores setup

Vores setup indeholder:

- Routere
- Firewall
- Wireless
- DMZ
- DHCPD, BIND, BGPD, OSPFD, ...

Den kunne udvides med flere andre teknologier vi har til rådighed:

- VLAN inkl VLAN trunking/distribution, WPA Enterprise

Hvad taler for og imod - de næste slides gennemgår nogle standardsetups

En slags patterns og anti-patterns for networking

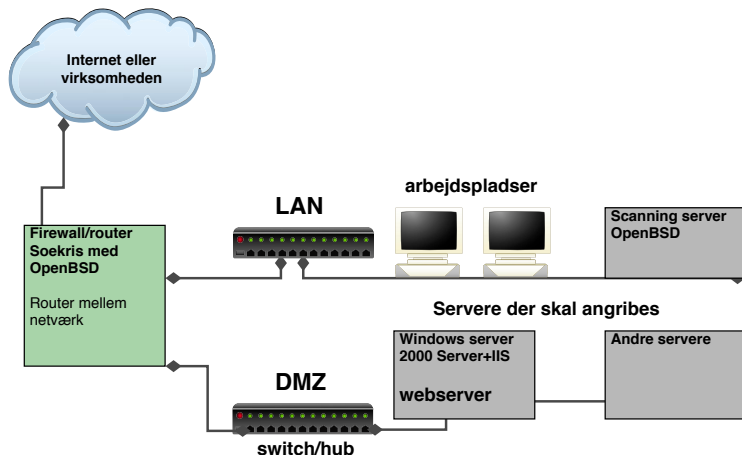
Husk følgende slides er min mening



Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche – managed switche med monitorering, logning og administration
- Opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Basic Network Security Pattern Isolate in VLANs



Du bør opdele dit netværk i segmenter efter trafik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Pattern use IDS to get flow, connections and data



Use Intrusion Detection Systems - IDS

Angrebsværktøjerne efterlader spor

Det anbefales at have IDS og flow opsamling som minimum

Hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

Network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

Drift og Planlægning af sikre miljøer



Før installationen scope

- Hvad er formålet - reaktion eller "statistik"
- Hvor skal der måles - hele netværket eller specifikke dele
- Hvad skal måles og hvilke operativsystemer og servere/services

Implementationen

- Er infrastrukturen i orden som den er
- Er der gode målepunkter - monitorporte
- Et målepunkt eller flere, Hvor meget trafik skal måles

Selve idriftsættelsen

- Ændringer af infrastrukturen
- Installation af udstyret og test af udstyret udenfor drift
- Installation i driftsmiljøet
- Test af udstyret i driftsmiljøet

Eksempel Opsætning og konfiguration af IDS miljøer



Vælg en simpel installation til at starte med!

Undgå for alt i verden for meget information

- Start med en enkelt sensor
- Byg en server med database og "brugerværktøjer"
- Start med at overvåge dele af nettet
- Brug et specifikt regelsæt i starten - eksempelvis kun Windows eller kun UNIX
- Lav nogle simple rapporter til at starte med

Gør netværket mere sikkert før du lytter på hele netværket

Brug tcpdump/Wireshark til at se på trafik, lær IP pakker at kende

Brug Suricata og Zeek til at opsamle og evaluere trafikken – baseline af netværket

- Husk at man kan starte med vilkårligt værktøj og senere skifte til andre produkter, evt. kommercielle
- Praktisk erfaring med eget netværk er nødvendigt og værdifuldt

Honeypots



Man kan udover IDS installere en honeypot

En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger trafik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i

Forslag undgå standard indstillinger



Giv jer selv mere tid til at patche og opdatere

Tiden der går fra en sårbarhed annonceres på internet til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist

NB: ingen garanti

Brug krypterede forbindelser



```
root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jnaan ja
an ja
```

Især på utroværdige netværk kan det give problemer at benytte sårbare protokoller

Mission 1: Kommunikere sikkert



Du må ikke bruge ukrypterede forbindelser til at administrere netværk eller servere

Du må ikke sende kodeord i ukrypterede e-mail beskeder

Telnet daemonen - telnetd må og skal dø!

FTP daemonen - ftpd må og skal dø!

POP3 daemonen port 110 må og skal dø!

IMAPD daemonen port 143 må og skal dø!

væk med alle de ukrypterede forbindelser!

Pattern: erstat Telnet med SSH



Telnet er død!

Brug altid Secure Shell fremfor Telnet

Opgrader firmware til en der kan SSH, eller køb bedre udstyr næste gang

Selv mine små billige Linksys switcher forstår SSH!

Pattern: erstat FTP med HTTP



Hvis der kun skal distribueres filer kan man ofte benytte HTTP istedet for FTP

Hvis der skal overføres med password er SCP/SFTP fra Secure Shell at foretrække

FTP File Transfer Protocol



File Transfer Protocol - filoverførsler

Bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP

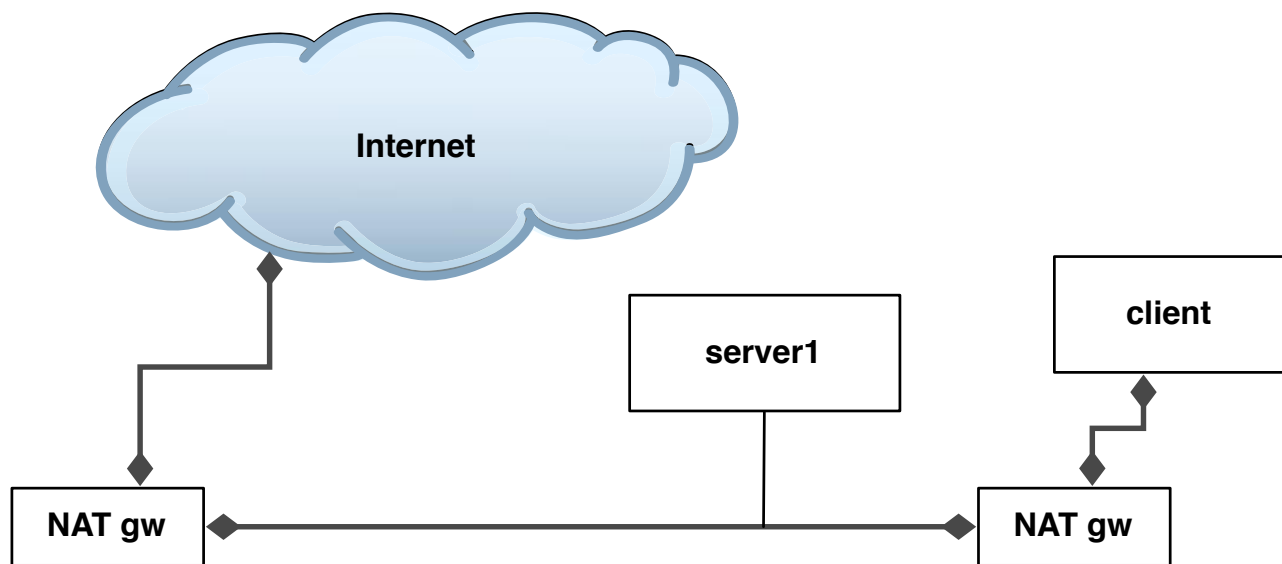
FTP sender i klartekst

USER brugernavn og

PASS hemmeligt-kodeord

Der findes varianter som tillader kryptering, men brug istedet SCP/SFTP over Secure Shell protokolle

Anti-pattern dobbelt NAT i eget netværk



Det er nødvendigt med NAT for at oversætte trafik der sendes videre ud på internet.
Der er ingen som helst grund til at benytte NAT indenfor eget netværk!

Anti-pattern blokering af ALT ICMP



```
# Allow ICMPv6 destination unreachable (don't filter it out)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 1
# Allow NS/NA/toobig (don't filter it out)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 2
# Allow timex Time exceeded (don't filter it out)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 3
# Allow parameter problem (don't filter it out)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 4
# IPv6 ICMP - echo request (128) and echo reply (129)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 128,129
# IPv6 ICMP - router solicitation (133) and router advertisement (134)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 133,134
# IPv6 ICMP - neighbour discovery solicitation (135) and advertisement (136)
    $fwcmd6 add pass ipv6-icmp from any to any icmptypes 135,136
```

- Lad være med at blokere for alt ICMP, så ødelægger du funktionaliteten i dit net
- Eksemplet viser ICMPv6 – hvor nogle NDP pakker er kritiske at have tilladte

ICMPv4 beskedtyper



Type

- 0 = net unreachable;
- 1 = host unreachable;
- 2 = protocol unreachable;
- 3 = port unreachable;
- 4 = fragmentation needed and DF set;
- 5 = source route failed.

Tillad disse ICMP types:

- 3 Destination Unreachable
- 4 Source Quench Message
- 11 Time Exceeded
- 12 Parameter Problem Message

Lad være med at blokere for alt ICMP, så ødelægger du funktionaliteten i dit net

Anti-pattern blokering af DNS opslag på TCP



Det bliver (er) nødvendigt med DNS opslag over TCP

Store svar kræver TCP

Det betyder at firewalls skal tillade DNS opslag via TCP

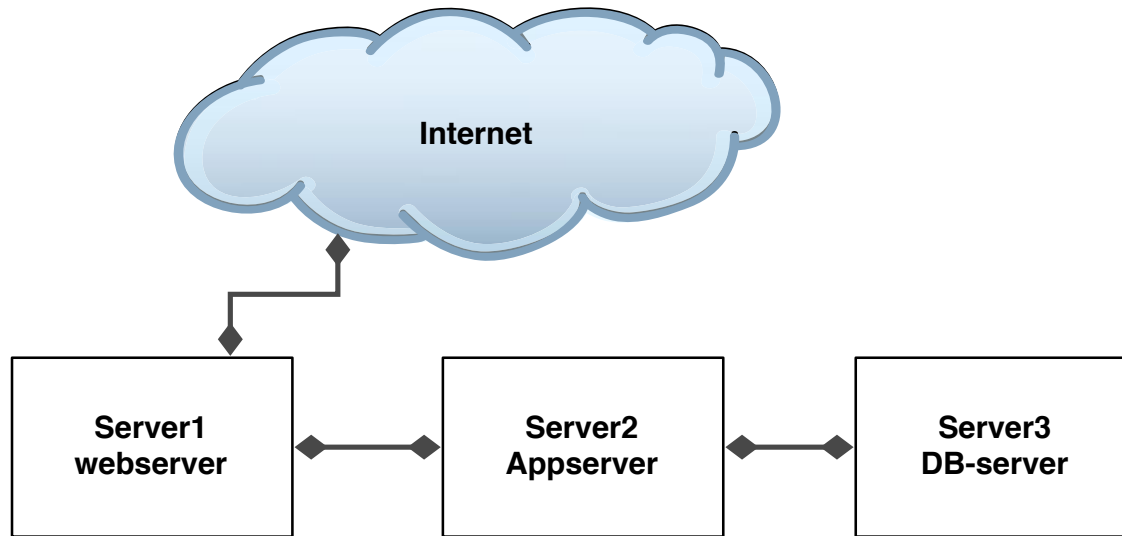
De nye forslag DNS over TLS (DoT) og DNS over HTTPS (DoH)

DNS kryptering bliver med TCP

Anbefaling i enterprise netværk:

Brug en caching nameserver, således at det kun er den som kan lave DNS opslag ud i verden

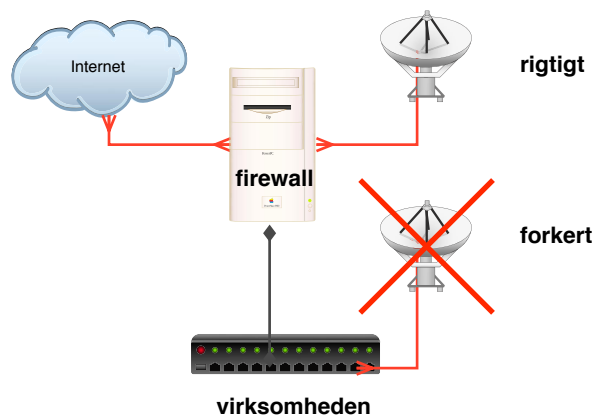
Anti-pattern daisy-chain



Daisy-chain af servere, erstat med firewall, switch og VLAN

Det giver et væld af problemer med overvågning, administration, backup og opdatering

Anti-pattern WLAN forbundet direkte til LAN



WLAN AP'er forbundet direkte til LAN giver risiko for at sikkerheden brydes, fordi AP falder tilbage på den usikre standardkonfiguration

Ved at sætte WLAN direkte på LAN risikerer man at eksterne får direkte adgang

Tegningen skal forstås som den logiske kobling. Typisk placeres APs ofte i eget VLAN, og dermed adskilt fra LAN

Pattern individuel autentificering!



ssh root@server1



Mange systemer administreres fejlagtigt ved brug af root-login eller andet delt administrator login

Undgå direkte root-login eller administrator

Insister på sudo eller su

Hvorfor?

- Sporbarheden mistes hvis brugere logger direkte ind som root
- Hvis et kodeord til root gættes er der direkte adgang til alt!

Centralized management SSH, Jump hosts



A jump server, jump host or jumpbox is a computer on a network used to access and manage devices in a separate security zone. The most common example is managing a host in a DMZ from trusted networks or computers.

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

Mutually Agreed Norms for Routing Security (MANRS)



Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

Problems related to incorrect routing information

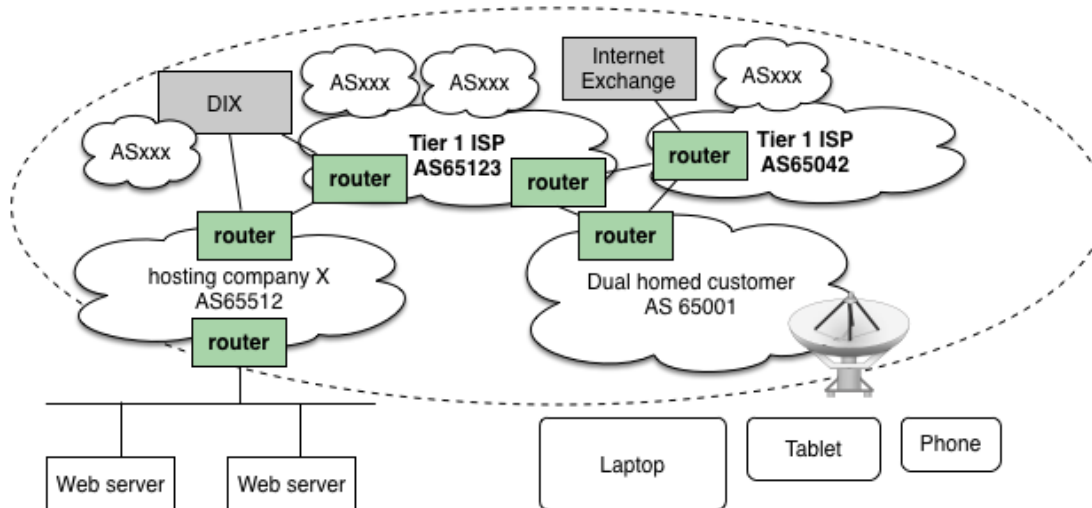
Problems related to traffic with spoofed source IP addresses

Problems related to coordination and collaboration between network operators

<https://www.manrs.org/isps/>

https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf

Hosting og internet-udbydere



- Data krydser mange internetudbydere
- Det er stadig muligt at spoofe mange steder fra
- Din sikkerhed er afhængig af andres sikkerhed

Expected Actions in MANRS for Network Operators



1. Prevent propagation of incorrect routing information

Clear routing policies and systems for correctness, route import filters

2. Prevent traffic with spoofed source IP addresses

Validate source address from end-users and infrastructure, use BCP38

3. Facilitate global operational communication and coordination between network operators

Maintain contact information in databases like Whois, PeeringDB <https://www.peeringdb.com/>

Advanced

4. Facilitate validation of routing information on a global scale

Use RPSL https://en.wikipedia.org/wiki/Routing_Policy_Specification_Language



RFC-2142 Mailbox Names for Common Services, Roles and Functions

Du BØR konfigurere dit domæne til at modtage post for følgende adresser:

- postmaster@domæne.dk
- abuse@domæne.dk
- webmaster@domæne.dk, evt. www@domæne.dk

Du gør det nemmere at rapportere problemer med dit netværk og services

E-mail best current practice



MAILBOX	AREA	USAGE
-----	-----	-----
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries
...		
MAILBOX	SERVICE	SPECIFICATIONS
-----	-----	-----
POSTMASTER	SMTP	[RFC821], [RFC822]
HOSTMASTER	DNS	[RFC1033-RFC1035]
USENET	NNTP	[RFC977]
NEWS	NNTP	Synonym for USENET
WEBMASTER	HTTP	[RFC 2068]
WWW	HTTP	Synonym for WEBMASTER
UUCP	UUCP	[RFC976]
FTP	FTP	[RFC959]

Kilde: RFC-2142 Mailbox Names for Common Services, Roles and Functions. D. Crocker. May 1997

RIPE NCC abuse-c



The RIPE NCC began implementing a new policy in 2013 to ensure that all resources allocated and assigned by the RIPE NCC include an "abuse-c:" attribute. The idea behind the policy is to make it easier for end users to find abuse contact information to report abuse to the appropriate resource holder, and to give resource holders a single, consistent place to include this information in the RIPE Database.

The "abuse-c:" attribute is contained within the **organisation** object, and references a **role** object containing abuse contact information in an "abuse-mailbox:" attribute. All the **organisation** objects linked by the resources you manage (both IPv4 and IPv6) must contain an "abuse-c:" attribute.



Relationship between RIPE Database objects involved in abuse-c

<https://www.ripe.net/manage-ips-and-asns/resource-management/abuse-c-information>

Resource Public Key Infrastructure RPKI



- 1997 - AS7007 mistakenly (re)announces 72,000+ routes (becomes the poster-child for route filtering).
- 2008 - ISP in Pakistan accidentally announces IP routes for YouTube by blackholing the video service internally to their network.
- 2017 - Russian ISP leaks 36 prefixes for payments services owned by Mastercard, Visa, and major banks.
- 2018 - BGP hijack of Amazon DNS to steal crypto currency.

Source: <https://blog.cloudflare.com/rpki/>

RPKI https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

Authenticated routing protocols passwords, secrets etc.

Use RPKI



Routinator is RPKI Relying Party software, also known as an RPKI Validator. It is designed to have a small footprint and great portability.

Routinator connects to the Trust Anchors of the five Regional Internet Registries (RIRs) — APNIC, AFRINIC, ARIN, LACNIC and RIPE NCC — downloads all of the certificates and ROAs in their repositories and validates the signatures. It can feed the validated information to hardware routers supporting Route Origin Validation such as Juniper, Cisco and Nokia, as well as serving software solutions like BIRD and OpenBGPD. Alternatively, Routinator can output the validated data in a number of useful formats, such as CSV, JSON and RPSL.

Quote from <https://www.nlnetlabs.nl/projects/rpki/routinator/>

Update your records in the Whois system, read about RIPE here:

<https://www.ripe.net/manage-ips-and-asns/resource-management/certification>

BCP38 RFC2827: Network Ingress Filtering



BCP38 RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

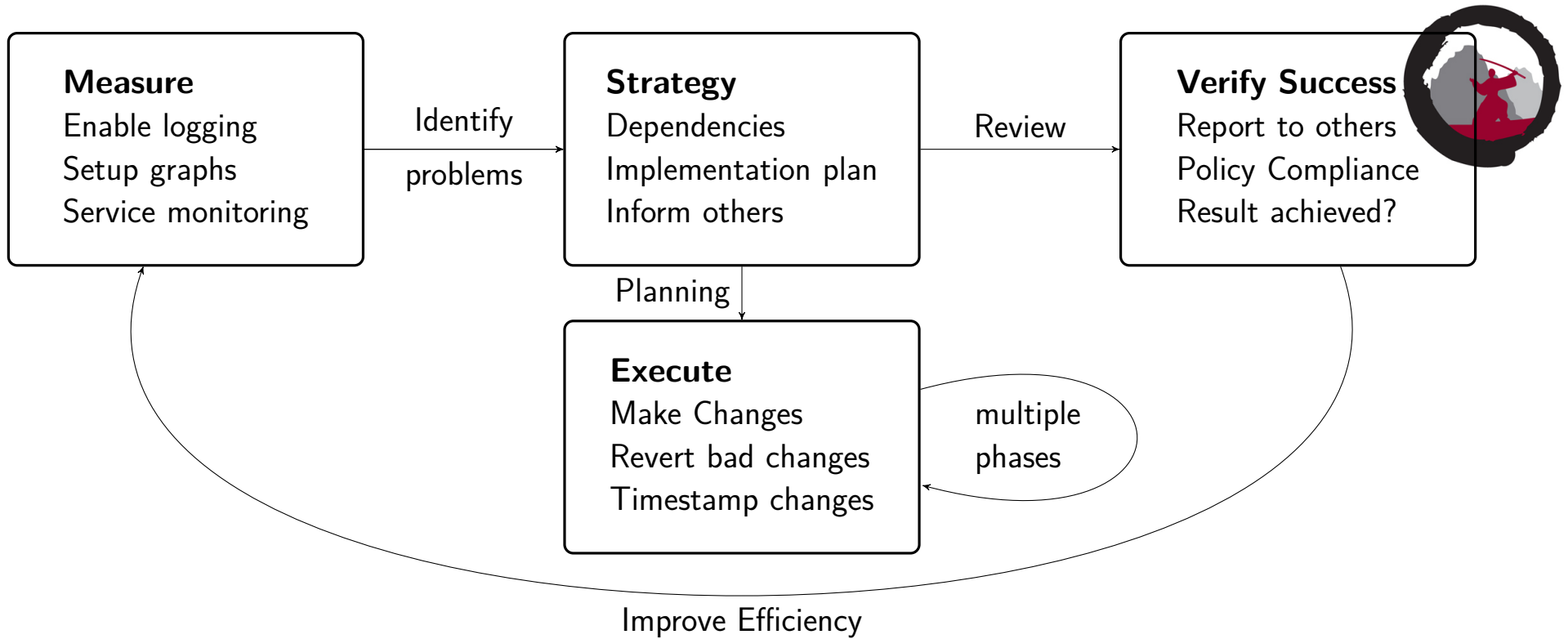
<https://tools.ietf.org/pdf/bcp38.pdf>

RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks

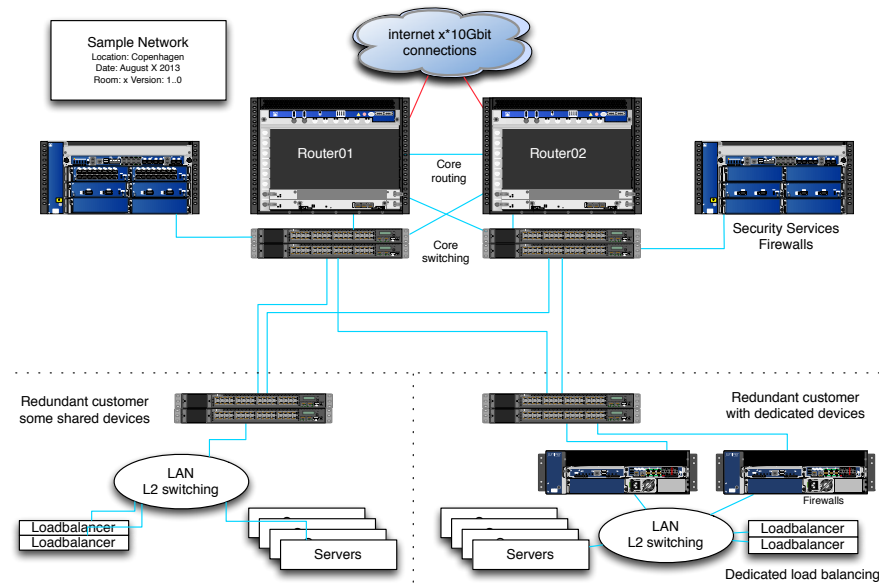
Testing security, evaluating and reporting



Make incremental changes



Example: 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.

Båndbredestyring og policy based routing



Mange routere og firewalls idag kan lave båndbredde allokering til protokoller, porte og derved bestemte services

Specielt relevant for DDoS beskyttelse

Findes på F5 BigIP, Cisco, Junos osv.

Mest kendte er i Open Source:

- OpenBSD - integreret i PF
- FreeBSD har dummynet
- Linux Traffic Control

Det kaldes også traffic shaping

hping3 packet generator



```
usage: hping3 host [options]
  -i --interval wait (uX for X microseconds, for example -i u1000)
  --fast      alias for -i u10000 (10 packets for second)
  --faster    alias for -i u1000 (100 packets for second)
  --flood     sent packets as fast as possible. Don't show replies.
...
hping3 is fully scriptable using the TCL language, and packets
can be received and sent via a binary or string representation
describing the packets.
```

- Hping3 packet generator is a very flexible tool to produce simulated DDoS traffic with specific characteristics
- Home page: <http://www.hping.org/hping3.html>
- Source repository <https://github.com/antirez/hping>

My primary DDoS testing tool, easy to get specific rate pps

t50 packet generator



```
root@cornerstone03:~# t50 -?
T50 Experimental Mixed Packet Injector Tool 5.4.1
Originally created by Nelson Brito <nbrito@sekure.org>
Maintained by Fernando Mercês <fernando@mentebinaria.com.br>
```

```
Usage: T50 <host> [/CIDR] [options]
```

Common Options:

```
--threshold NUM      Threshold of packets to send      (default 1000)
--flood               This option supersedes the 'threshold'
```

...

6. Running T50 with '--protocol T50' option, sends ALL protocols sequentially.

```
root@cornerstone03:~# t50 -? | wc -l
```

264

- T50 packet generator, another high speed packet generator can easily overload most firewalls by producing a randomized traffic with multiple protocols like IPsec, GRE, MIX

home page: <http://t50.sourceforge.net/resources.html>

Extremely fast and breaks most firewalls when flooding, easy 800k pps/400Mbps

Process: monitor, attack, break, repeat



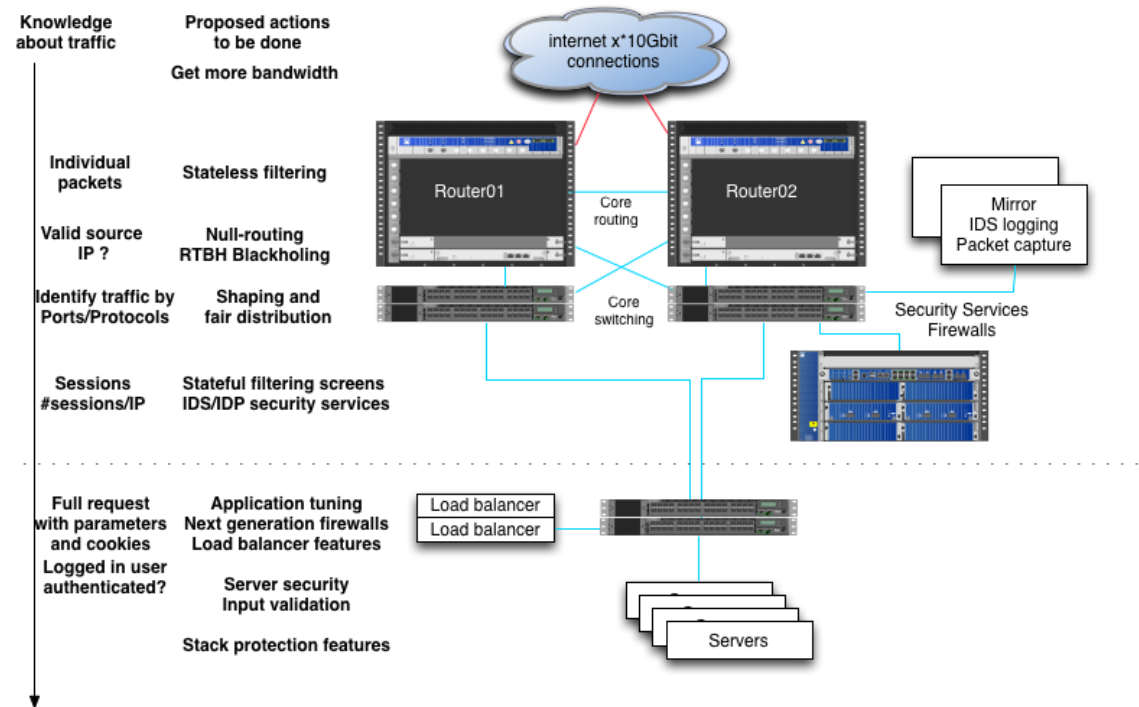
- Pre-test: Monitoring setup - from multiple points
- Pre-test: Perform full Nmap scan of network and ports
- Start small, run with delays between packets
- Turn up until it breaks, decrease delay - until using `--flood`
- Monitor speed of attack on your router interface pps/bandwidth
- Give it maximum 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

DDoS and network attacks



You really should try testing
Investigate your existing devices
all of them, RTFM, upgrade firmware
Choose which devices does which
part - discard early to free resources
for later devices to dig deeper



And dont forget that DDoS testing is as much a firedrill for the organisation

Fundamentet skal være iorden



Sørg for at den infrastruktur som I bygger på er sikker:

- redundans
- opdateret
- dokumenteret
- nem at vedligeholde

Husk tilgængelighed er også en sikkerhedsparameter

Hardened network device configurations



Alle services skal være konfigureret korrekt:

- Administration kun fra jump host og egne administrator netværk, SSH og HTTPS
- Alle protokoller med mulighed for *secrets* bør evalueres for om det skal benyttes
- Protokoller som BGP skal benytte route import filtre
- Protokoller som OSPF bør benytte policies OG secrets
- Brug Router protect filter således at kun relevant adgang tillades til services på udstyret
- Brug Reverse Path Forwarding uRPF / RPF

Check you network from outside



How does your network look like from the outside?

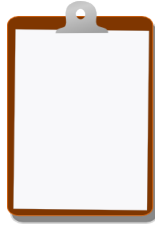
Check your network using:

<https://stat.ripe.net/>

Consider:

- Join the NLNOG RING <https://ring.nlnog.net/>
- <https://bgpmon.net/> - commercial tool, some alternatives exist
- <https://shadowserver.org/wiki/> sign up for Shadowserver - ASN & Netblock Alerting & Reporting Service

For Next Time



Think about the subjects from this time, write down questions

Next time is exam preparation

All books should be read by now

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools