Welcome to

Webinar: DDoS - hvad er det, og hvad kan du gøre ved det?

KEA 2023

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Github

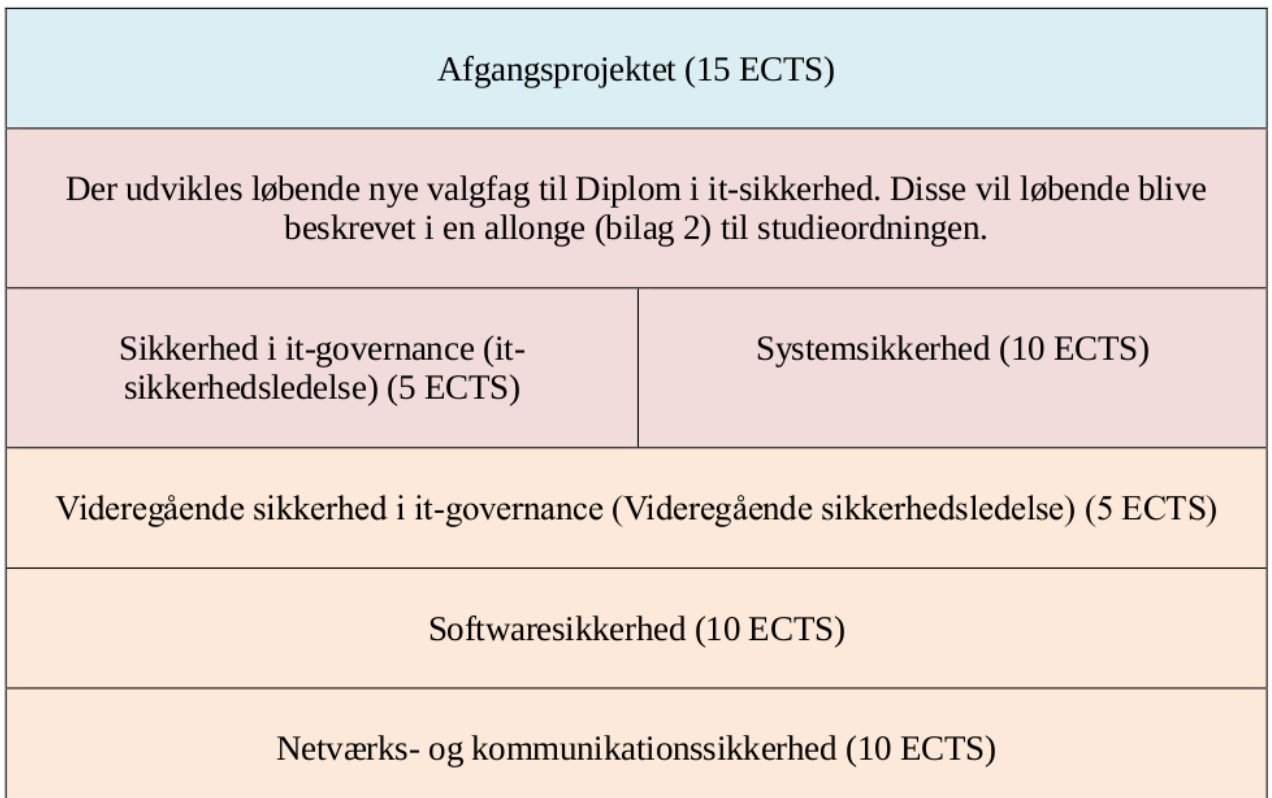
webinar-ddos-2023.tex in the repo security-courses

Kontaktinformation

- Henrik Kramselund, han/ham internet samurai, primært netværk og sikkerhed
- Netværk og it-sikkerhedskonsulent Zencurity, underviser på KEA og aktivist
- Cand.scient. fra Datalogisk Institut ved Københavns Universitet (DIKU)
- Email: hlk@zencurity.com Mobil: +45 2026 6000

I er velkomne til at sende email

Overview Diploma in IT-security



Course Description

OB1 Netværks- og kommunikationssikkerhed (10 ECTS)

Indhold:

Elementet går ud på at forstå og håndtere netværkssikkerhedstrusler samt implementere og konfigurere udstyr til samme.

Elementet omhandler forskellig sikkerhedsudstyr (IDS) til monitorering. Derudover vurdering af sikkerheden i et netværk, udarbejdelse af plan til at lukke eventuelle sårbarheder i netværket samt gennemgang af forskellige VPN teknologier.

STUDIEORDNING Diplomuddannelse i it-sikkerhed

https://kompetence.kea.dk/studieordninger/Studieordning_Diplom_IT-sikkerhed_2022_03.pdf

What is this presentation about

When **connecting to the Internet we immediately receive traffic from unknown sources**. We should consider **testing our infrastructure using active pentest methods**, to verify robustness.

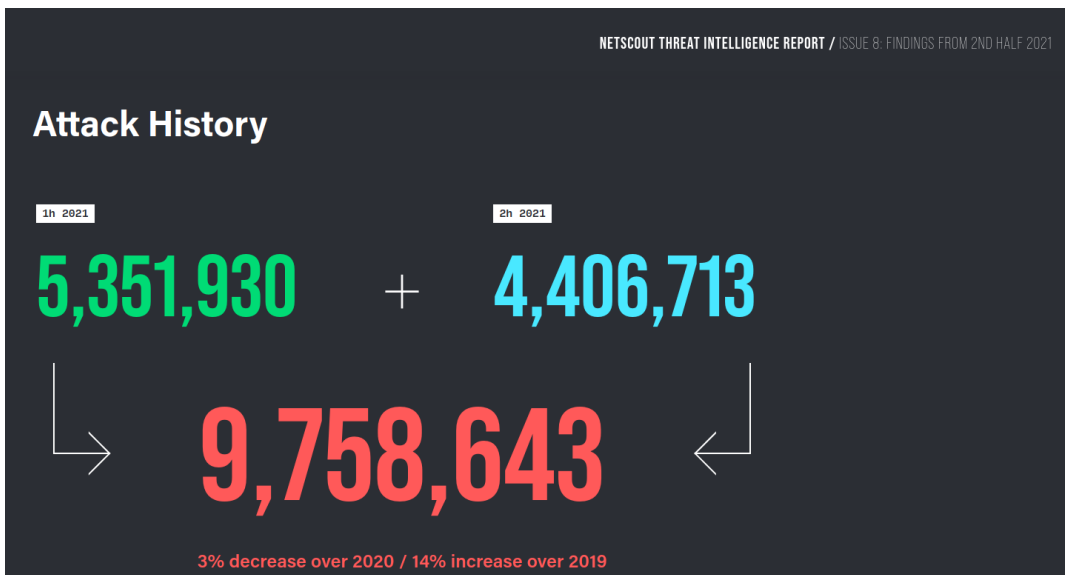
You will learn:

- This talk will be about DDoS
- What is DDoS
- What happens
- How can we start testing your infrastructures
- My advice for protection using your existing devices and networks

Note: The attack tools will be already developed and possibly known tools, but with a lot of focus on the process and experiences. I also have some opinions and experiences to share.

The Internet and DDoS is trouble

Security attacks and DDoS is very much in the media



Source: Netscout Global DDoS Threat Intelligence Report 2nd half 2021

https://www.netscout.com/threatreport/global-ddos-attack-trends/

Also in Denmark

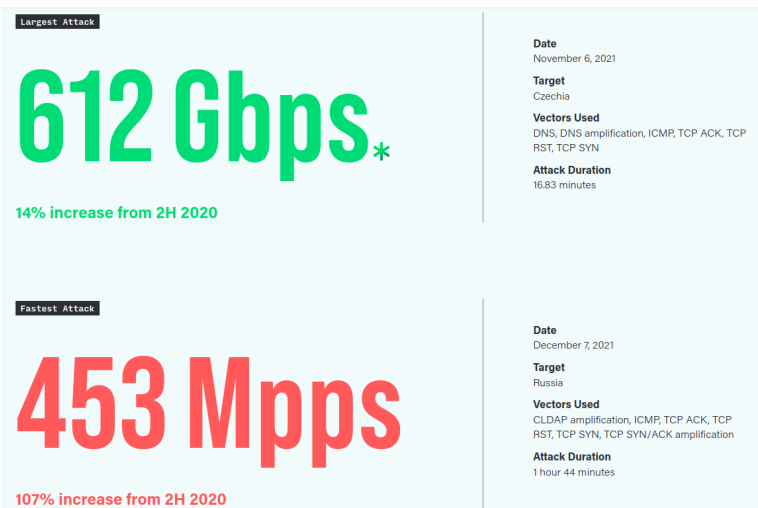
> 8. december 2022 blev Forsvaret ligeledes ramt af et 11 timer langt DDoS-angreb, der også gjorde flere hjemmesider utilgængelige. I begyndelsen af januar 2023 blev en række danske banker, herunder Nationalbanken, ofre for DDoS-angreb, ligesom Bankdata, der er it-leverandør til flere danske pengeinstitutter, blev ramt gentagne gange.
> »Vi kommer også fremover til at se overbelastningsangreb ramme danske netværk. Det er en del af normalbilledet, sådan som det nuværende trusselsbillede ser ud,« udtalte CFCS i midten af januar til mediet FinansWatch.

Source: Version2.dk

- 16. januar Banker og finansielle institutioner over flere omgange
- 30. januar Forsvarsministeriet og 8.dec 2022 forsvaret
- 1. februar Flere ministerier via Statens IT
- 23. februar Københavns lufthavn og Roskilde Lufthavn

DDoS Attacks are HUGE

Extremely hard to protect against from a small network



Source: Netscout Global DDoS Threat Intelligence Report 2nd half 2021

https://www.netscout.com/threatreport/global-ddos-attack-trends/

We can do a lot to improve our infrastucture – Don't give up!

Taxonomy of DDoS Attacks - quick

RioRey Taxonomy of DDoS Attacks

		Attack Types	Attack Matrix Dimensions									
			Nature of IP	Handshake	Source IP Range	Packet Rate	Packet Size	Packet Content	Fragmenting	Session Rate	Session Duration	VERB Rate
TCP BASED	1	SYN Flood	Spoofed	None	Large	High	Small	---	---	---	---	---
	2	SYN-ACK Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	3	ACK & PUSH ACK Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	4	Fragmented ACK	Spoofed	None	Large	Moderate	Large	---	High	---	---	---
	5	RST or FIN Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	6	Synonymous IP	Spoofed	None	Single IP	High	---	---	---	---	---	---
	7	Fake Session	Spoofed	None	Large	Low	---	---	---	---	---	---
	8	Session Attack	Non-Spoofed	Yes	Small	Low	---	---	---	Low	Long	---
	9	Misused Application	Non-Spoofed	Yes	Small	Variable	---	---	---	High	Short	---

HTTP

TCP HTTP BASED	10	**HTTP Fragmentation**	Non-Spoofed	Yes	Small	Very Low	Small	Valid	High	Very Low	Very Long	Very Low
	11	**Excessive VERB**	Non-Spoofed	Yes	Small	High	---	Valid	---	High	Short	High
	12	**Excessive VERB Single Session**	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Moderate	High
	13	**Multiple VERB Single Request**	Non-Spoofed	Yes	Small	Very Low	Large	Valid	---	Low	Long	High
	14	**Recursive GET**	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low
	15	**Random Recursive GET**	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low
	16	**Faulty Application**	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low

NOT a complete list, but examples, see another example
https://en.wikipedia.org/wiki/Slowloris_(computer_security)

UDP

UDP BASED	17	**UDP Flood**	Spoofed	---	Very Large	Very High	Small	Not Valid	---	---	---	---
	18	**Fragmentation**	Spoofed	---	Moderate	Very High	Large	Not Valid	High	---	---	---
	19	**DNS Flood**	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---
	20	**VoIP Flood**	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---
	21	**Media Data Flood**	Spoofed	---	Very Large	Very High	Moderate	Valid	---	---	---	---
	22	**Non-Spoofed UDP Flood**	Non-Spoofed	---	Small	Very High	---	Valid	---	---	---	---

UDP is not used in most Web applications. My advice is to bandwith limit UDP flow into parts of the network with HTTP/HTTPS servers.

ICMP

ICMP BASED	23 **ICMP Flood**	Spoofed	---	Very Large	Very High	Variable	Not Valid	---	---	---	---
	24 **Fragmentation**	Spoofed	---	Moderate	Very High	Large	Not Valid	High	---	---	---
	25 **Ping Flood**	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---

ICMP is a control protocol for sending messages about a problem. It does not carry data for web applications, so could be restricted and bandwidth limited in most network.

If you have a 10Gigabit connection, having 1Gbit UDP and 100Mbit ICMP is often enough.

What about the firewall – vendors can protect against DDoS, right?!

Definition of firewalls – multiple definitions exist

We define a firewall as **a collection of components** placed between two networks that collectively have the following properties:

- All traffic from inside to outside, and vice-versa, must pass through the firewall.
- Only authorized traffic, as defined by the **local security policy**, will be allowed to pass.
- The firewall itself is immune to penetration.

We should note that these are design goals; a failure in one aspect does not mean that the collection is not a firewall, simply that it is not a very good one.

We will consider this a firewall, but we know today that **both inside and outside at meaningless**, since we have **multiple networks inside, we have partner network connections etc.**

Source: *Firewalls and Internet Security; Repelling the Wily Hacker.* by Cheswick and Bellovin 1994

Definition of firewalls – Wikipedia

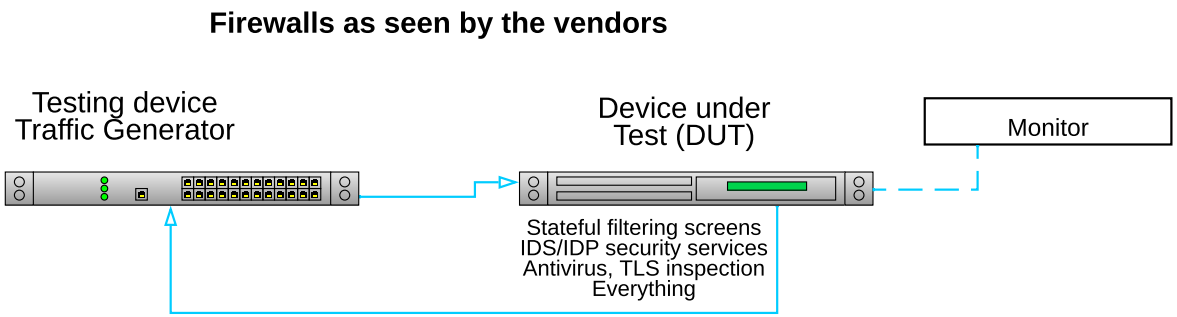
Another short definition that encapsulates this is found on Wikipedia, and may suffice in many situations. Again there will typically be multiple networks, zones or areas of the networks with varying degrees of trust.

> In computing, a firewall is a **network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules**.[1] A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.[2]

Source: Wikipedia https://en.wikipedia.org/wiki/Firewall_(computing)

TL;DR Not necessarily a single device

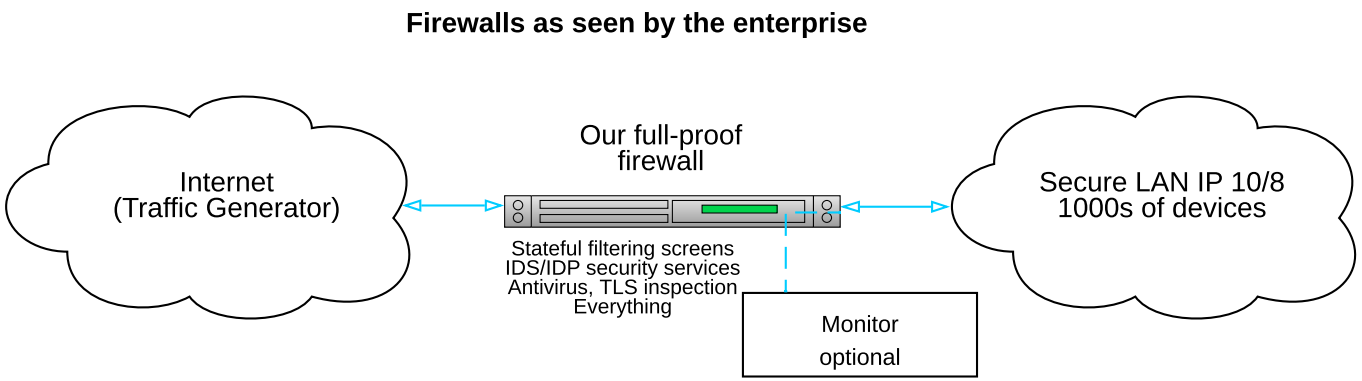
A firewall – in the vendor eyes



"**Can your firewall flex in the face of change?**
Does it harmonize your network, workload, and application security? Does it protect apps and employees in your hybrid or multicloud environment? Make sure you're covered."

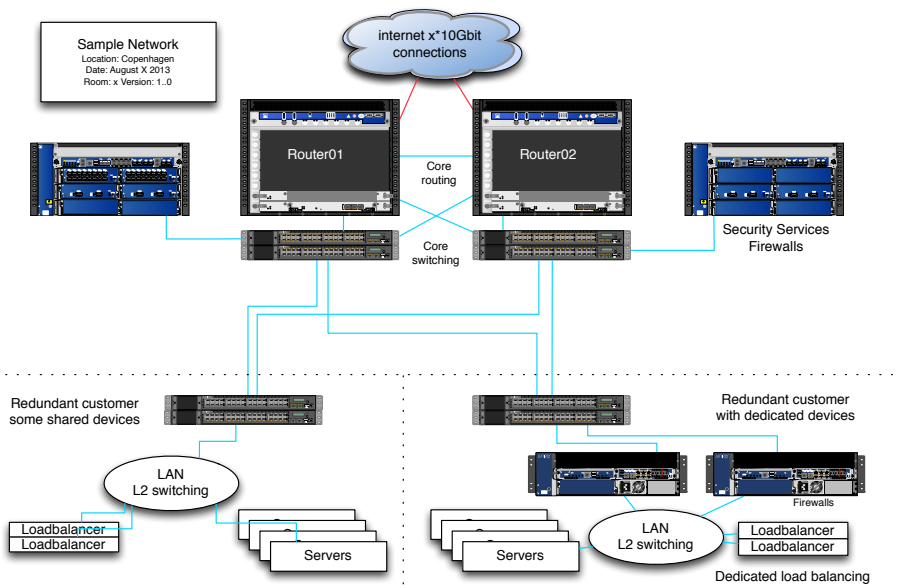
Source: not shown to protect the audience from further marketing speak

A firewall – in the enterprise mindset



- Even though some vendors suggest they can do everything in a single box, I don't believe them!
- Truth – yes, we can do almost anything in software
- Realization **Your infrastructure is based on multiple components and or devices**

Bottlenecks exist, but where



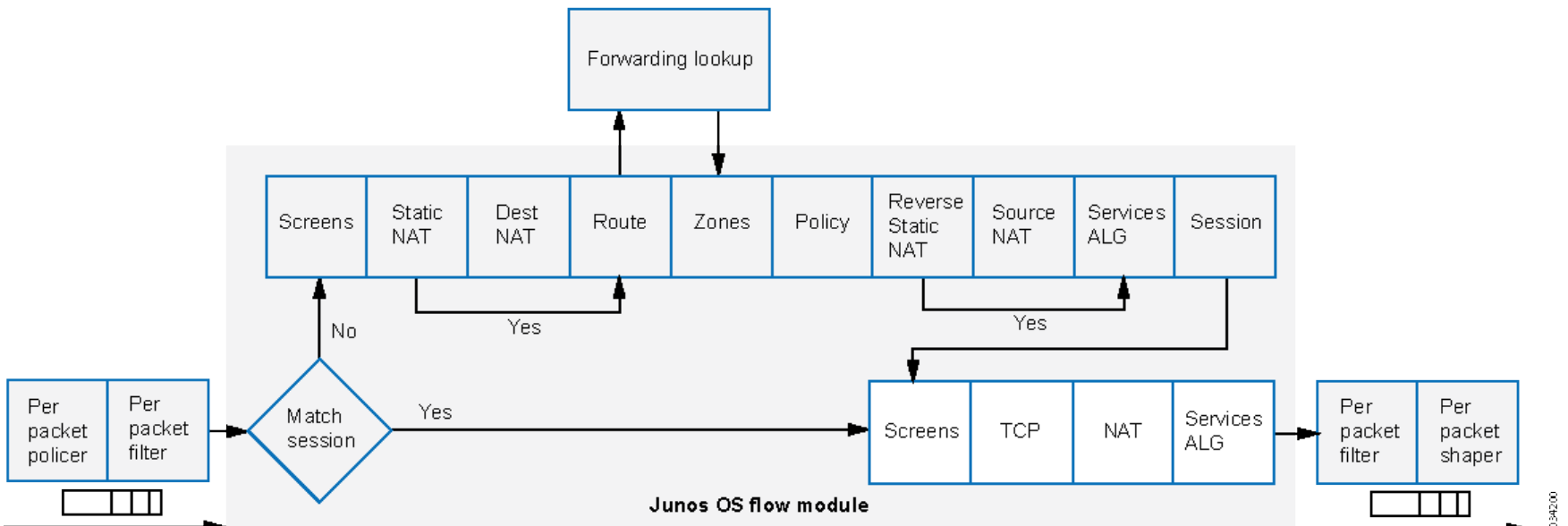
- Lower layer attacks Transport Layer Attacks TCP SYN flood – packet based
- Higher layer attacks like Slowloris and web attacks – keep sessions running
- Protect everything without loosing functionality or creating administrative nightmare

Availability and Network flooding attacks

The attacks we are discussing today are:

- **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 popular targets – more similar ones exist
- Special packets and protocols – anything that can create *load on systems* work
- 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 (pps)
- **CPU processing** in firewalls, pps
- CPU processing in server software
- **Bandwidth** - megabits per second (mbps)
- Typically source is spoofed or amplification attacks abusing devices on the Internet

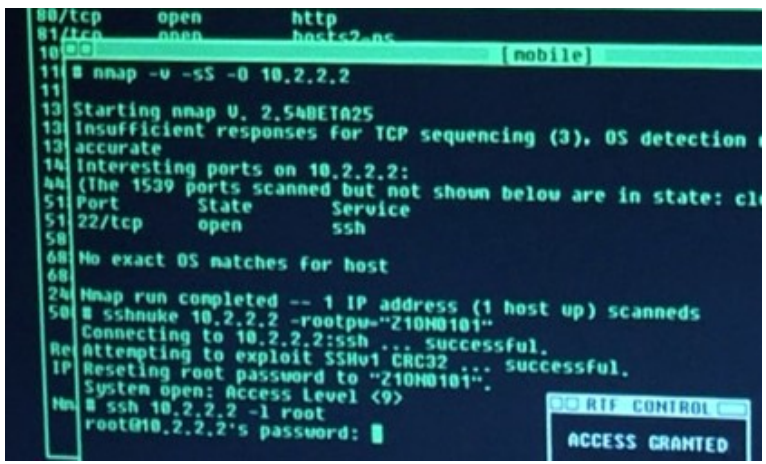
Packet processing in firewalls – detailed view



Traffic Processing on SRX Series Devices Overview

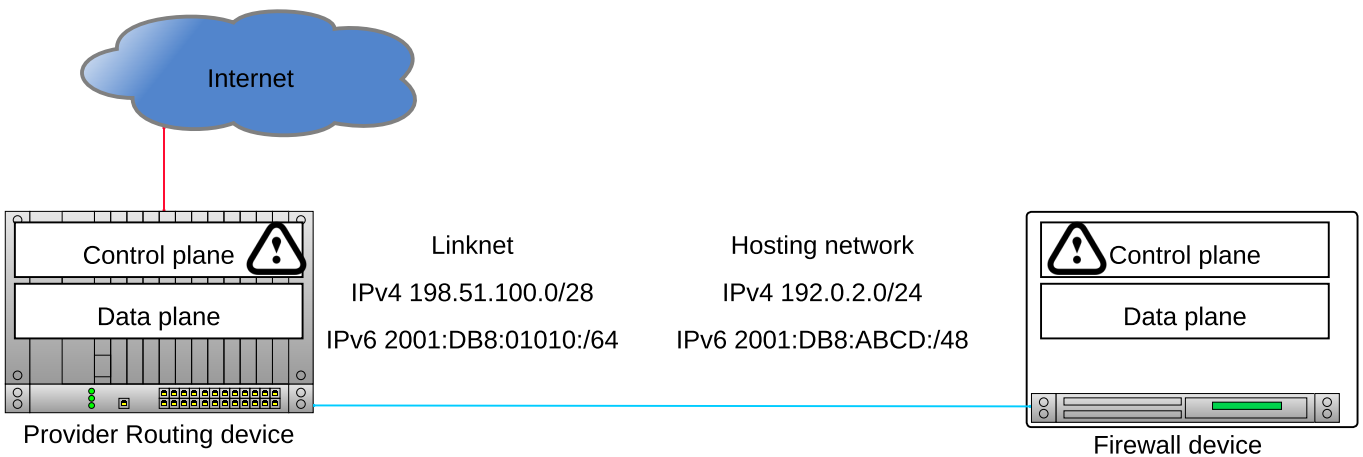
https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-srx-devices-processing-overview.html

Prepare for the testing



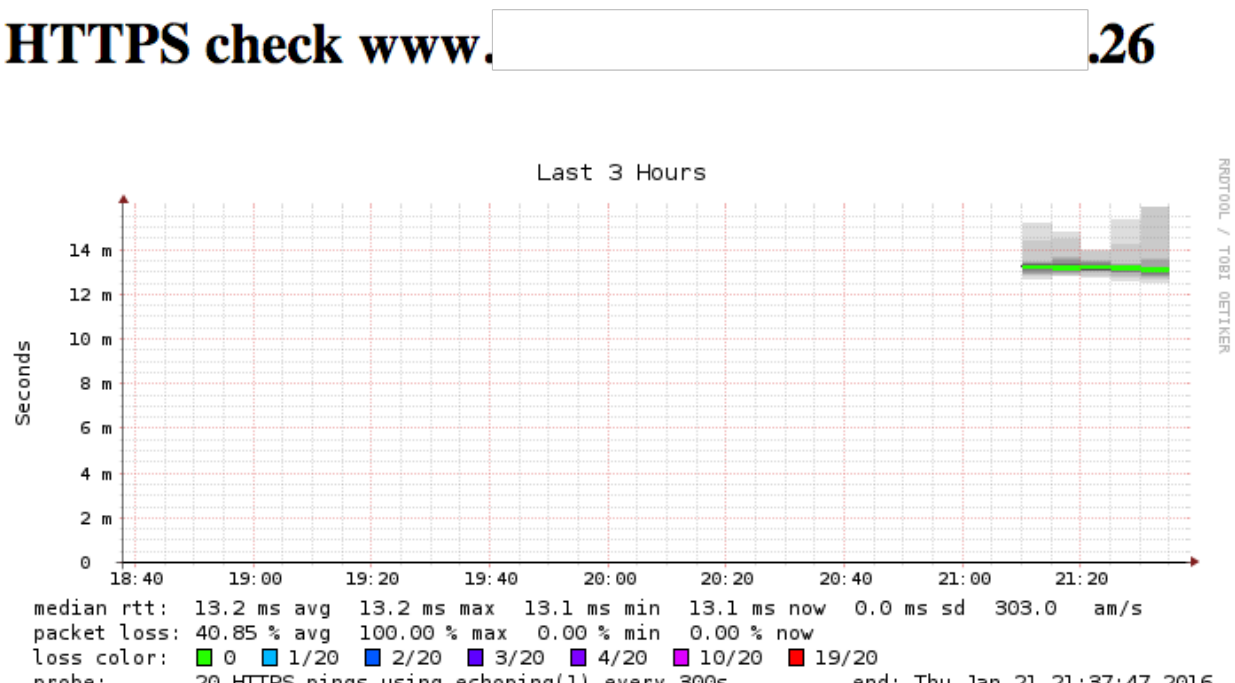
- Portscan the whole linknet and hosting range in IPv4
- Ask about IPv6 ranges in use, specific subnets and IPv6 addresses
  We can guess from traceroute, Nmap test first 100 addresses in each subnet etc. but easier to ask
- Portscan the whole linknet - identify provider devices, hosting network devices, type of device router/firewall
- Also Thank you Fyodor (Gordon Lyon) and contributors for Nmap!

Scanning and Attacking – Pressure Points and Scope



- In scope for me is everything that could adversely affect the network
- Typical scope IPv4: Link network /28 or /26 and a hosting network /24 or even /22
- Typical scope IPv6: Link network /64 (bad) or /127 (RFC9099) and a hosting network /48 with subnets

Before testing: Smokeping



Before DDoS testing use Smokeping software

Performing the DDoS test

So lets break this task down into:

- Use Nmap to port scan the network
- Run testing tool `hping3`, `t50` or `penguinping`
- Go through all scenarios before making changes to environment
- Expect things to break, investigate, repeat failed scenarios

- BTW we usually schedule this for night time! There WILL be interruptions

- How do you run the tools, since they all have so many options?
  `man nmap | enscript -o test.ps` result in 54 pages, `hping3` has about 80 options and `t50` has even more

Running full port scan on network

Hint: use a variable to keep the target address, carefully enter it and avoid mystyping it later

```
# export  CUST_NET4="192.0.2.0/24"
# export CUST_NET6="2001:DB8:ABCD:1000::/64"
# nmap -p 1-65535 -Pn -A -oA full-scan  $CUST_NET4

# export CUST_IP=192.0.2.138
# date;time hping3 -q -c 1000000  -i u60 -S -p 80 $CUST_IP
```

Better yet, script it all – but most likely you will want to repeat specific steps.

Nmap port sweep for TCP services, full TCP scan

Goal is to enumerate the ports that are allowed through the network.

```
#  nmap -Pn -A -p 1-65535 -oA full-tcp-customer-ipv4 $CUST_NET4
...
Nmap scan report for 192.0.2.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
#  nmap -Pn -A -p 1-65535 -oA full-tcp-customer-ipv6 $CUST_NET6
#  nmap -Pn -A -p 1-65535 -oA full-tcp-linknet-ipv4 $LINK_NET4
#  nmap -Pn -A -p 1-65535 -oA full-tcp-linknet-ipv6 $LINK_NET6
```

Note: Pretty harmless, if something dies, then it is *vulnerable to normal traffic* - and should be fixed!

```
Options:
-Pn -- Scan all IPs, dont use ping or TCP ping to check alive    -A advanced -- perform full TCP connection and grab banner
-p 1-65535 -- full portscan all ports  -oA filename -- Saves output in "all formats" normal, XML, and grepable formats
```

Nmap port sweep for SNMP port 161/UDP

Perform some UDP scanning, cannot do full scan, but often SNMP is there, example:

```
# nmap -A -sU -p 161 --script "snmp-info" -oA snmp-scan $LINK_NET4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 20:20 CEST
Nmap scan report for 192.0.2.10
Host is up (0.00082s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    Cisco SNMP service; ciscoSystems SNMPv3 server
| snmp-info:
|   enterprise: ciscoSystems
|   engineIDFormat: mac
|   engineIDData: 00:08:4f:xx:yy:zz
|   snmpEngineBoots: 4
|_  snmpEngineTime:  732d07h09m04s
Too many fingerprints match this host to give specific OS details
Network Distance: 6 hops
```

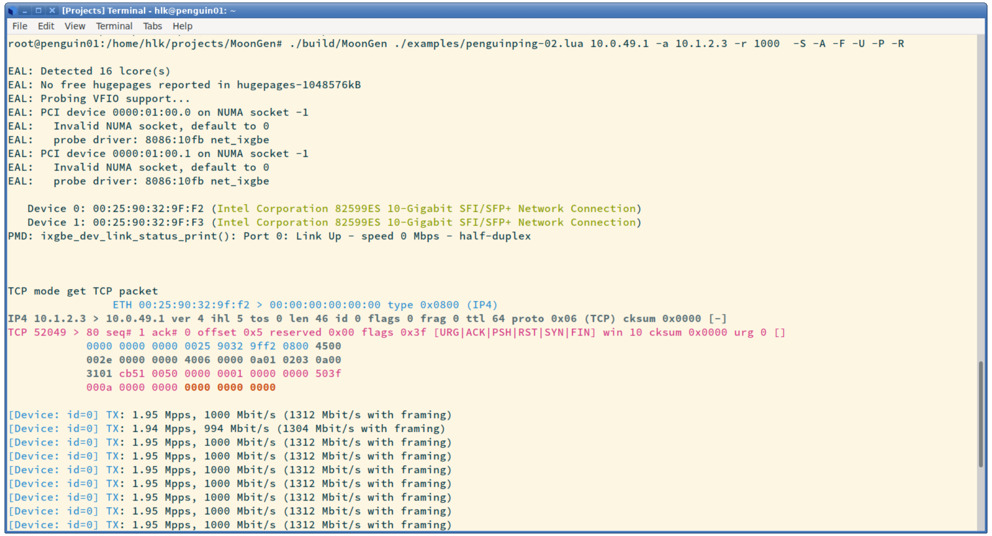
More reliable to use Nmap script with probes like –script=snmp-info

Packet generators – multiple options

```
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.
UDP/TCP
  -s  --baseport   base source port             (default random)
  -p  --destport   [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -L  --setack     set TCP ack
  -F  --fin        set FIN flag
  -S  --syn        set SYN flag
...
```

- Hping3 packet generator is a very flexible tool to produce simulated DDoS traffic with specific charateristics
- Home page: http://www.hping.org/hping3.html Source repository https://github.com/antirez/hping
- My fork with IPv6 and VXLAN branches added https://github.com/kramse/hping-2018
- Used to be my primary DDoS testing tool, now I am moving to PenguinPing / MoonGen
- Another great option: T50 packet generator http://t50.sourceforge.net/resources.html

Penguingping packet generator



- 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

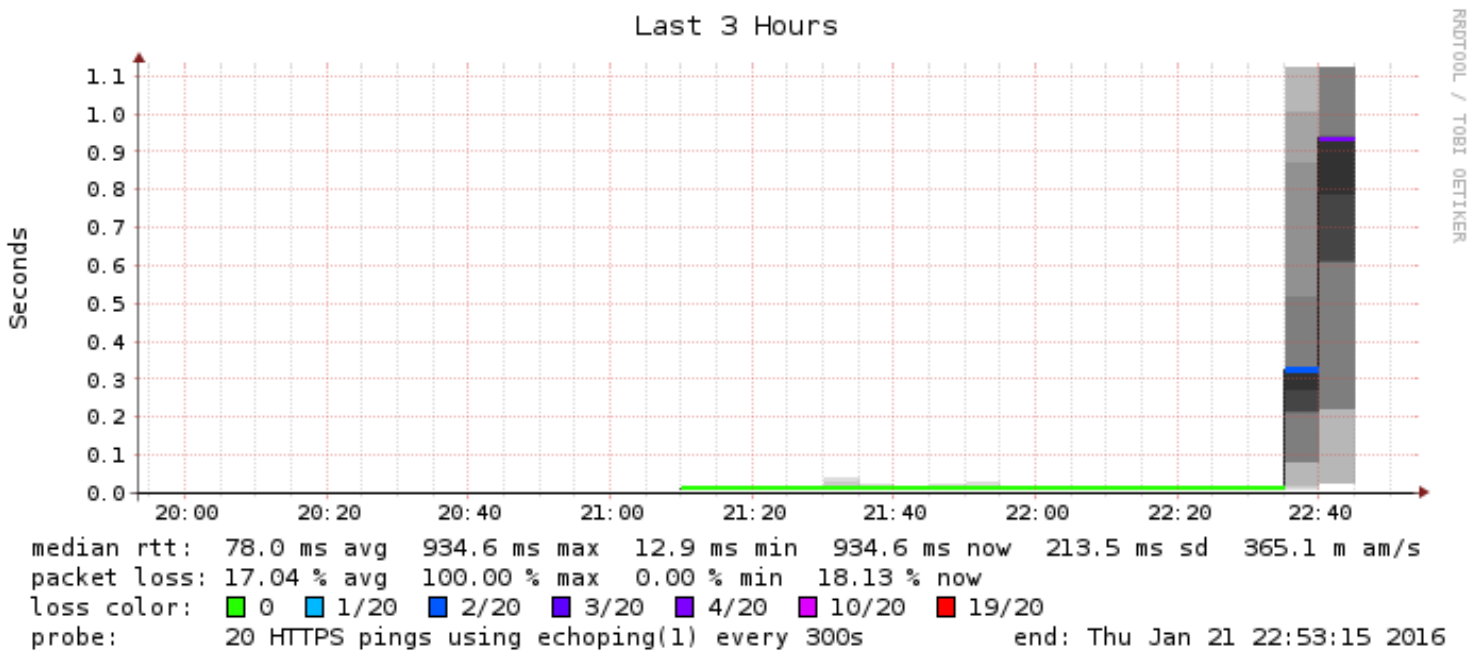
- Start small, run with delays between packets
- Turn up until it breaks, decrease delay - until using full bandwidth / max pps
- Monitor speed of attack on your router interface pps/bandwidth
- Give it up to maximum speed
  `hping3 --flood -1` and `hping3 --flood -2` – probably about 1mpps / core/process
  `penguinping -r 10000` if you have it – rate 10Gbit using one CPU core!
- Have a common chat with network operators/customer to talk about symptoms and things observed
- Any information resulting from testing is good information

Running the tools

A basic test would be:

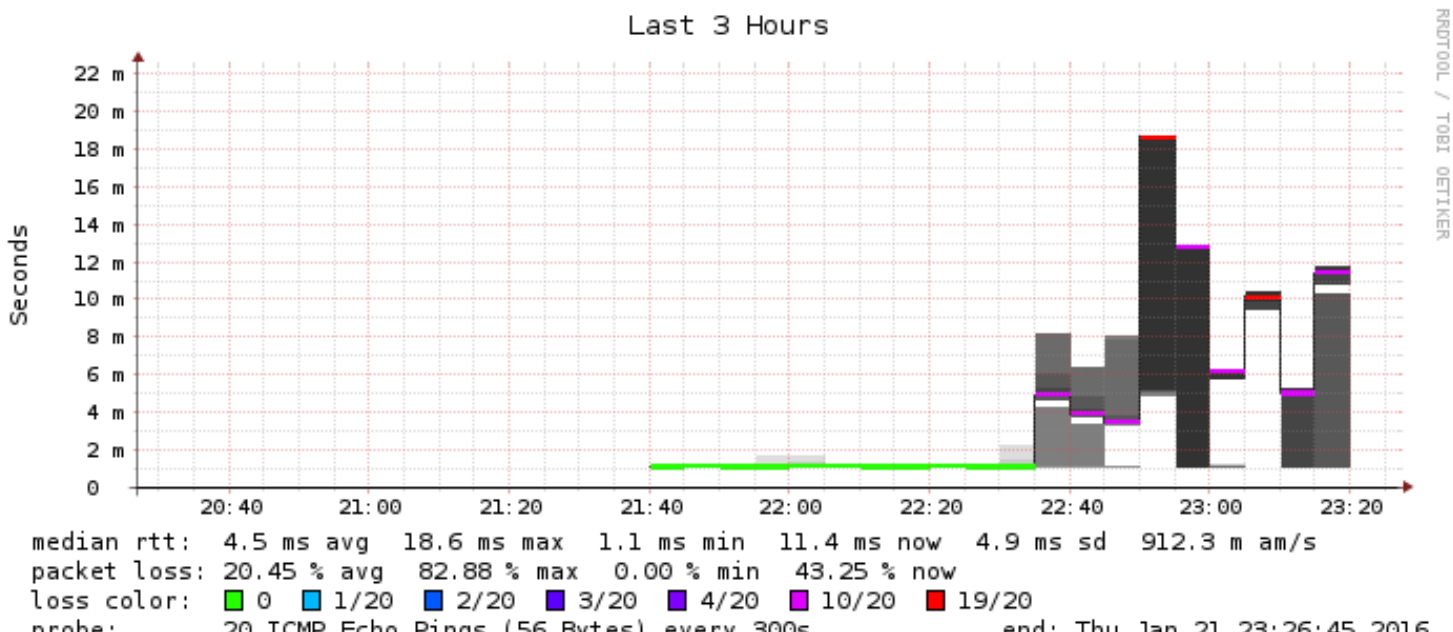
- TCP SYN flooding
- TCP other flags, PUSH-ACK, RST, ACK, FIN
- ICMP flooding
- UDP flooding
- Spoofed packets src=dst=target ☺
- Small fragments
- Bad fragment offset
- Bad checksum
- Be creative
- Mixed packets - like `t50 --protocol T50`
- Perhaps esoteric or unused protocols, GRE, IPSec

Rocky Horror Picture Show - 1



Really does it break from 50.000 pps SYN attack?

Rocky Horror Picture Show - 2



Oh no 500.000 pps UDP attacks work?

Advanced and High Performance Testing

- We DO want to test maximum speed at some point, full 10Gbit and 14.8Million pps (Mpps)
- Data Plane Development Kit (DPDK) open source software
  https://en.wikipedia.org/wiki/Data_Plane_Development_Kit
- Modern computer with modern CPU and PCIe x8 or better
  Cheap Dell devices Precision 3240 Compact shown (not a recommendation)
- Supported card - I am using the old Intel 82599 based 10Gbit cards
- DPDK and software – I use MoonGen https://github.com/emmericp/MoonGen
- Maybe the easiest way to use DPDK currently – "Craft all packets in user-controlled Lua scripts"

Running MoonGen

```
root@penguin01:~/projects/MoonGen#  ./build/MoonGen ./examples/l3-tcp-syn-flood.lua 0 -d 192.0.2.138
[INFO]  Initializing DPDK. This will take a few seconds...
EAL: Detected 16 lcore(s)
[INFO]  Found 1 usable devices:
   Device 0: 00:25:90:32:9F:F3 (Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection)
PMD: ixgbe_dev_link_status_print():  Port 0: Link Down
[INFO]  Device 0 (00:25:90:32:9F:F3) is up: 10000 MBit/s
[INFO]  Detected an IPv4 address.
...
[Device: id=0] TX: 14.88 Mpps, 7619 Mbit/s (9999 Mbit/s with framing)
[Device: id=0] TX: 14.48 Mpps, 7414 Mbit/s (9730 Mbit/s with framing)
[Device: id=0] TX: 14.88 Mpps, 7619 Mbit/s (10000 Mbit/s with framing)
```

- Installed Debian Linux – little bit of disable secure boot, RAID/AHCI settings, ...
- After install – tuning and enabling Hugepages
- Clone the repository https://github.com/emmericp/MoonGen build and run
- **Note: the full 14.8Mpps is done using a single core!**

Turn up and down as you please with the -r rate option

```
root@penguin01:~/projects/MoonGen#  ./build/MoonGen ./examples/l3-tcp-syn-flood.lua 0 -r 5000 -d 192.0.2.138
[INFO]  Initializing DPDK. This will take a few seconds...
EAL: Detected 16 lcore(s)
[INFO]  Found 1 usable devices:
   Device 0: 00:25:90:32:9F:F3 (Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection)
PMD: ixgbe_dev_link_status_print():  Port 0: Link Down
[INFO]  Device 0 (00:25:90:32:9F:F3) is up: 10000 MBit/s
[INFO]  Detected an IPv4 address.

[Device: id=0] TX: 9.77 Mpps, 5000 Mbit/s (6562 Mbit/s with framing)
[Device: id=0] TX: 9.68 Mpps, 4955 Mbit/s (6504 Mbit/s with framing)
[Device: id=0] TX: 9.77 Mpps, 5000 Mbit/s (6562 Mbit/s with framing)
```

IPv6 and UDP, replace tcp with udp in example:

```
./build/MoonGen ./examples/l3-tcp-syn-flood.lua 0 -r 5000 -d 2001:DB8:ABCD:0053::138 -i 2001:DB8:ABCD:0053::1

./build/MoonGen ./examples/l3-udp-flood-hlk.lua 0 -r 5000 -d 2001:DB8:ABCD:0053::138 -i 2001:DB8:ABCD:0053::1
```

PenguinPing – re-implementing hping3 with Lua

```
root@penguin01:~/projects/MoonGen#  ./build/MoonGen ./examples/penguinping-02.lua 10.0.49.1 -a 10.1.2.3 -r 10000 -S -p 80
[INFO]  Initializing DPDK. This will take a few seconds...
[INFO]  Found 2 usable devices:
   Device 0: 00:25:90:32:9F:F2 (Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection)
[INFO]  Device 0 (00:25:90:32:9F:F2) is up: 10000 MBit/s
TCP mode get TCP packet
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 0x02 [-|-|-|-|SYN|-] win 10 cksum 0x0000 urg 0 []
  0x0000:   0000 0000 0000 0025 9032 9ff2 0800 4500
  0x0010:   002e 0000 0000 4006 0000 0a01 0203 0a00
  0x0020:   3101 cb51 0050 0000 0001 0000 0000 5002
  0x0030:   000a 0000 0000 0000 0000 0000

[Device: id=0] TX: 14.88 Mpps, 7619 Mbit/s (9999 Mbit/s with framing)
[Device: id=0] TX: 14.78 Mpps, 7568 Mbit/s (9933 Mbit/s with framing)
[Device: id=0] TX: 14.88 Mpps, 7619 Mbit/s (10000 Mbit/s with framing)
```

- Using Lua we can implement the same attacks from Hping3 easily
- Only about 230 lines of Lua using MoonGen and libmoon
- Can run at specific rate up to full 10Gbps / 14.8 Million packets per second using a single CPU core

Comparable to real DDoS?

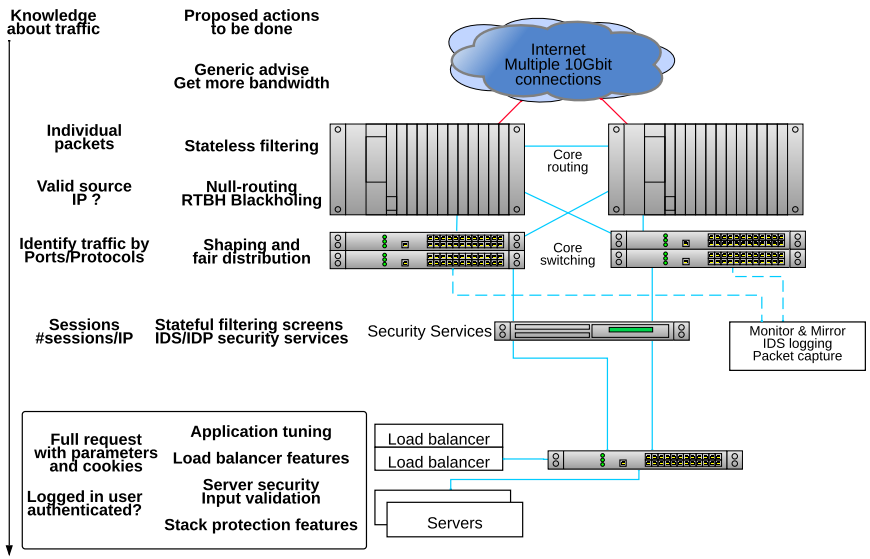
Tools are simple and widely available but are they actually producing same result as high-powered and advanced criminal botnets. We can confirm that the attack delivered in this test is, in fact, producing the traffic patterns very close to criminal attacks in real-life scenarios.

- We can also monitor logs when running a single test-case
- Gain knowledge about supporting infrastructure
- Can your syslog infrastructure handle 800.000 events in $<$ 1 hour?

Main difference are that attackers are free to switch attack types and mix them. While we try specifically to keep using one type, to see the worst and which ones that hurt the most.

I also start at the bottom, and work my way up – while an attacker may begin attacking HTTP/HTTPS directly.

Protection – Enable More Packet filtering



- Packet filtering can be done one single packets – stateless filtering
- We can save information about direction and ongoing traffic – stateful filtering/firewalling
- *Filtering* can also be setting a maximum number of packets for a protocol – rate limit by protocol

Designing the protection – bandwidth and rate limit

Protocol	Mbps	Prefix
TCP	Up to full bandwidth 10Gbps	192.0.2.0/25
UDP	Less than 1Gbps	192.0.2.128/25
ICMP	Less than 10Mbps	192.0.2.0/24

- Create an address plan for your services
- Monitor your traffic – how much UDP and TCP do you have, roughly
- Above is a simplified example – dig deeper into your traffic

Designing the protection – address families & protocols

Address family	Protocol	Services and ports	Prefix
IPv4	TCP	25, 80, 8003, 443, 4443	192.0.2.0/25
IPv4	UDP	53	192.0.2.128/25
IPv6	UDP	53	2001:DB8:ABCD:0053::/60
IPv6	TCP	80 443	2001:DB8:ABCD:1000::/56

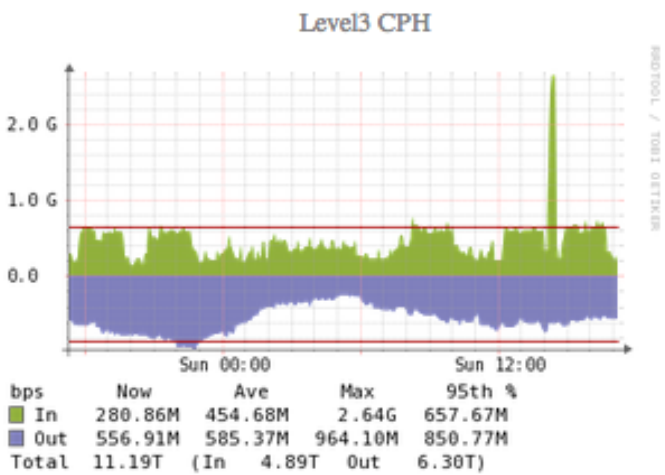
- Direction is also very important – servers that never initiate connections have fewer requirements
- How much traffic do you have that uses IPv6 yet? Should an IPv6 DDoS take up all resources?
- Maybe let IPv4 only use a part, so at least some customers can visit using IPv6?
- Maybe you can do an allow list for allocated networks, since not all is used yet

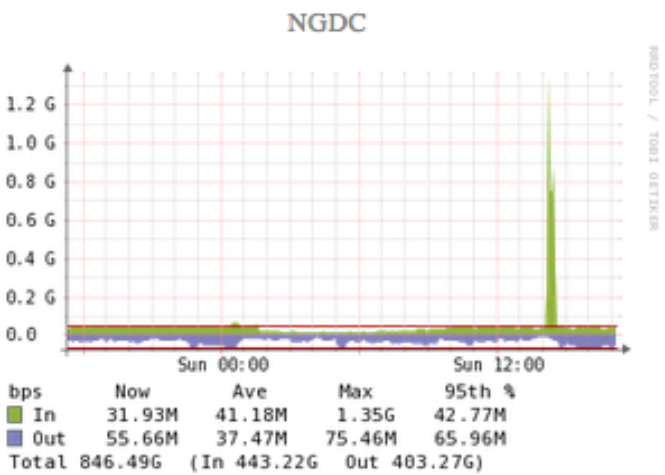
Strict filtering for some servers, still stateless!

```
term some-server-allow {
    from {
        destination-address {
            192.0.2.0/25;
        }
        protocol tcp;
        destination-port [ 25 80 8003 443 4443 ];
    } then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            192.0.2.0/25; }
        protocol-except icmp;  }
    then { count some-server-block; discard;
    }
}
```

Wut - no UDP, yes only TCP service is used on these servers

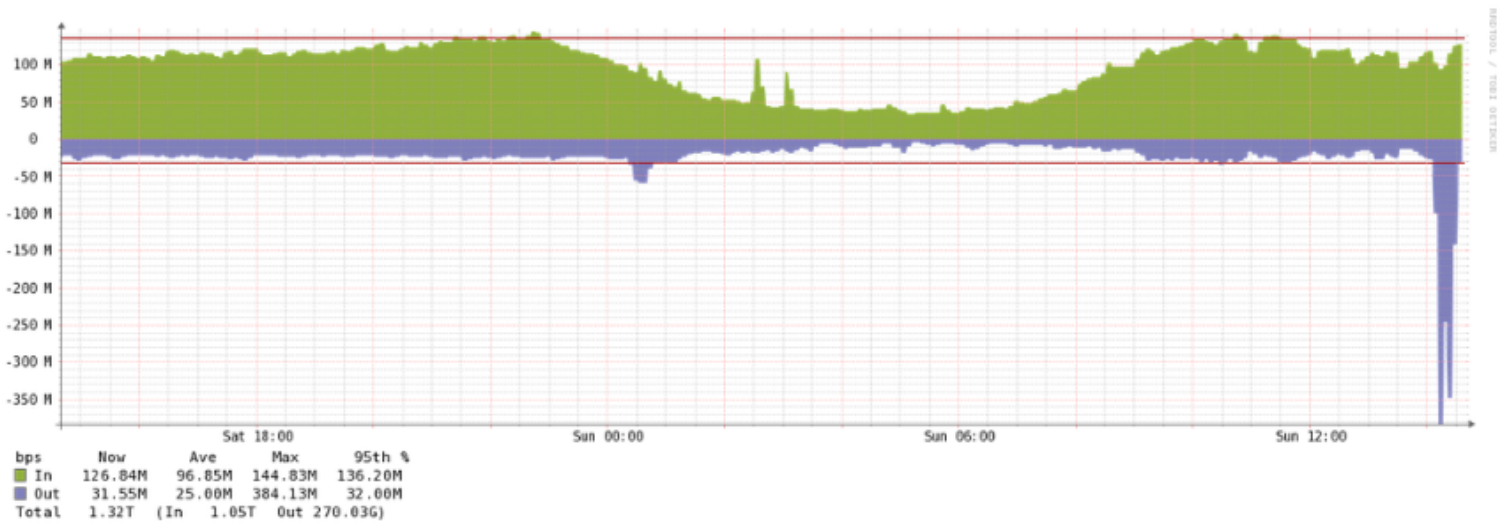
Results from implementing – DDoS traffic before filtering





Only two links shown, at least 3Gbit incoming for this single IP

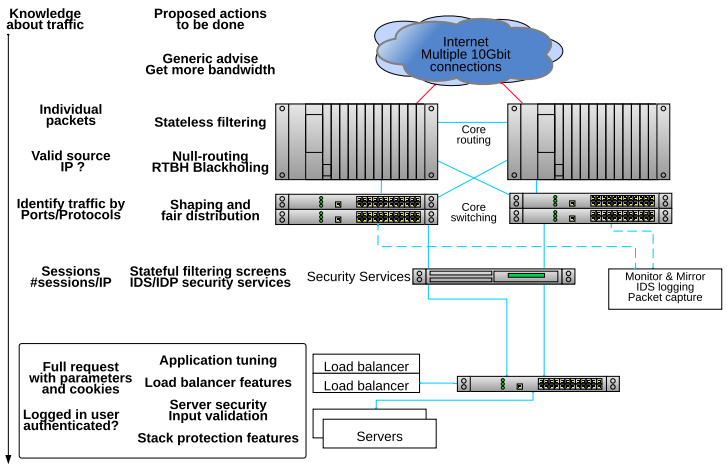
DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Knowing what it going on, is half the battle

Conclusion DDoS and network attacks



- You really should try testing, and investigate your existing devices all of them
- Choose which devices does which part – discard early to free resources for later devices to dig deeper
- This is just one small part of your security posture, extra slides has my take on enterprise network security

Questions?

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

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

Capture data and logs!

- Run DNS query logs – when client1 is infected with malware from domain malwareexample.com, then search for more clients i nfected
- Run Zeek and gather information about all HTTPS sessions – captures certificates by default, and we can again search for certificate related to malwareexample.com
- Run network logging – session logs in enterprise networks are GREAT
  (country wide illegal logging is of course NOT)

  Make sure to check with employees, inform them!

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

DROP SOME TRAFFIC NOW

kea

- 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

Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, better to use BGP flowspec or BGP based RTBH */
term edgeblocker {
    from {
        source-address {
            84.xx.xxx.173/32;
...
            87.xx.xxx.171/32;
        }
        destination-address {
            192.0.2.16/28;
        }
        protocol [ tcp udp icmp ];
    }
    then {
        count edge-block;
        discard;
    }
}
```

Example how to do it wirespeed – with Junos Hint: can also leave out protocol and then it will match all protocols

Stateless firewall filter limit protocols

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

Routers also have extensive Class-of-Service (CoS) tools today

Strict filtering for some servers, still stateless!

```
term some-server-allow {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol tcp;
        destination-port [ 80 443 ];
    }
    then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol-except icmp;
    }
    then {
        count some-server-block;
        discard;
    }
}
```

Wut - no UDP, yes UDP service is not used on these servers

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-echange to any port 25/tcp
# Unknown, remove when phased out
pass out on egress inet proto tcp from smtp-internal 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?

Zeek is a framework and platform

The Zeek Network Security Monitor

While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

https://www.Zeek.org/ Does useful things out of the box using more than 10.000 script lines

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

http://suricata-ids.org/ http://openinfosecfoundation.org

Suricata, Zeek og DNS Capture – it a nice world, use it!

https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop

Routing Security

- Use MD5 passwords or better authentication for routing protocols 🚩
- TTL Security – avoid routed packets
- Max prefix – of course, only allow expected networks
- Prefix filtering – only parts of IPv6 space is used
- TCP Authentication Option [RFC 5925] replaces TCP MD5 [RFC 2385]
- Turn ON RPKI for both IPv4 and IPv6 prefixes, 🚩
  https://nlnetlabs.nl/projects/rpki/about/
- Drop bogons on IPv4 and IPv6, article with multiple references YMMV
  https://theinternetprotocolblog.wordpress.com/2020/01/15/some-notes-on-ipv6-bogon-filtering/

Mutually Agreed Norms for Routing Security (MANRS)

kea

> 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.

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

- Problems related to incorrect routing information
- Problems related to traffic with spoofed source IP addresses
- Problems related to coordination and collaboration between network operators
- Also BCP38 RFC2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

You should all ask your internet providers if they know about MANRS, and follow it. We should ask our government and institutions to support and follow MANRS and good practices for network on the Internet