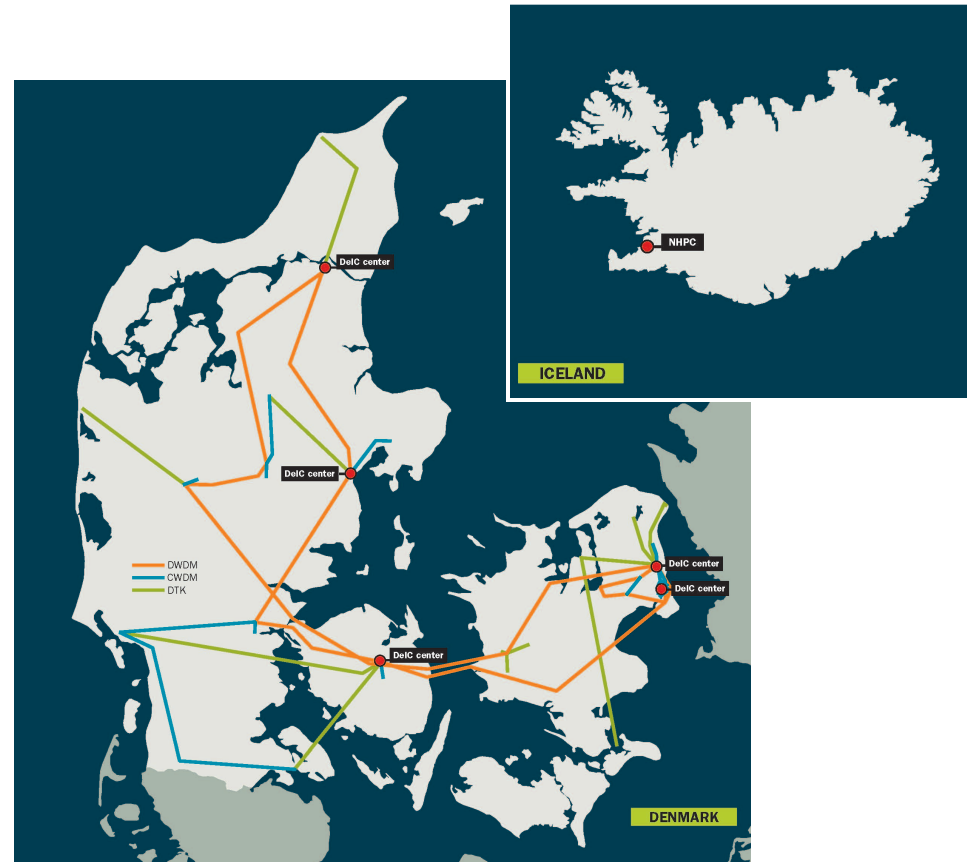


SIG-ISM (&TF-MSP) workshop:
DDoS Mitigation
in the NREN environment
Why is this important?

Vienna, 18th March 2015

Martin Bech, martin.bech@deic.dk
Head of NREN





19-05-2014

Service Management



Our (NREN) world is full of services...

- Look at the GÉANT Service Matrix at compendium.geant.org
- Here, we can see what services are offered by all the NRENs

What if we don't supply a service or the institutions just want to get it elsewhere?

When we look at all the services...

IP connectivity
Eduroam
Anti-spam solution
Web SSO Federation
CERT/CSIRT
IPv6
Certificate service
Interfederation
Consultancy/training
Filesender
Videoconferencing
Virtual circuit/VPN
Domain name registration
IP address allocation/LIR
Multicast
NTP service
Provision of content portal/s
Optical wavelength
VLE
Email server hosting
Web/desktop conferencing
PERT
Housing/co-location
Web hosting
DDoS r

...conferencing
Housing/co-location
Web hosting
DDoS mitigation
User conferences
Journal access
Project collaboration tools
Quality of Service
Dissemination
VoIP
DNS hosting
Vulnerability scanning
Archival storage
Procurement/brokerage
Software licenses
Network monitoring
SDN testbed
Event recording/streaming
Cloud storage (end user)
Virtual machines/laaS
User portals
Hosted campus AAI
Remote access VPN service
Mailing lists
Netnews/USENET
Hot stand

...us AAI
Remote access VPN service
Mailing lists
Netnews/USENET service
Hot standby
Nameserver services
National IX operation
Managed router service
Content delivery hosting
Scheduling tool
Software development
Survey/polling tool
3G/4G data service
CMS
Instant messaging
Database services
Network troubleshooting
TV/radio streaming
Web filtering
SMS messaging
Web development
Disaster recovery
Media post production
Open Lightpath Exchange
Plagiarism detection
Netflow tool
Intrusion
PC

...y hosting
ing tool
Software development
Survey/polling tool
3G/4G data service
CMS
Instant messaging
Database services
Network troubleshooting
TV/radio streaming
Web filtering
SMS messaging
Web development
Disaster recovery
Media post production
Open Lightpath Exchange
Plagiarism detection
Netflow tool
Intrusion detection
PGP key server
Security auditing
Finance/admin systems
Class registration tool
Firewall-on-demand
Online payment connectiv
Identifier registry
e-portfolio
SaaS

Our institutions can get most services elsewhere!

- Out of a total of 77 services
- We only have a monopoly on 6:
 - IP Connectivity
 - IPv6
 - Optical Wavelengths
 - DDoS Mitigation
 - QoS
- The users can not get these 6 services from other providers than us without leaving the NREN

By DDoS protection I mean broad coverage of a network block – not just a proxy for a selected web service



Affordable advanced DDoS protection

For business and enterprise customers

Denial-of-service (DoS) attacks are on the rise and have evolved into complex and overwhelming security challenges for organizations large and small. Although DoS attacks are not a recent phenomenon, the methods and resources available to conduct and mask such attacks have dramatically evolved to include distributed (DDoS) and, more recently, distributed reflector (DRDoS) attacks—attacks that simply cannot be addressed by traditional on-premise solutions.

CloudFlare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of such threats, and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks. This document explains the anatomy of each attack method and how the CloudFlare network is designed to protect your web presence from such threats.

19-05-2014

Below you will find detailed information on these attacks and how the CloudFlare network protects

against them:

Service Management

Get in touch

[Contact our team](#)

1 (888) 99 FLARE

1 (888) 993 5273

UK callers:

+44 (0)20 3514 6970

Singapore callers:

+65 3158 3954

International callers:

+1 (650) 319 8930

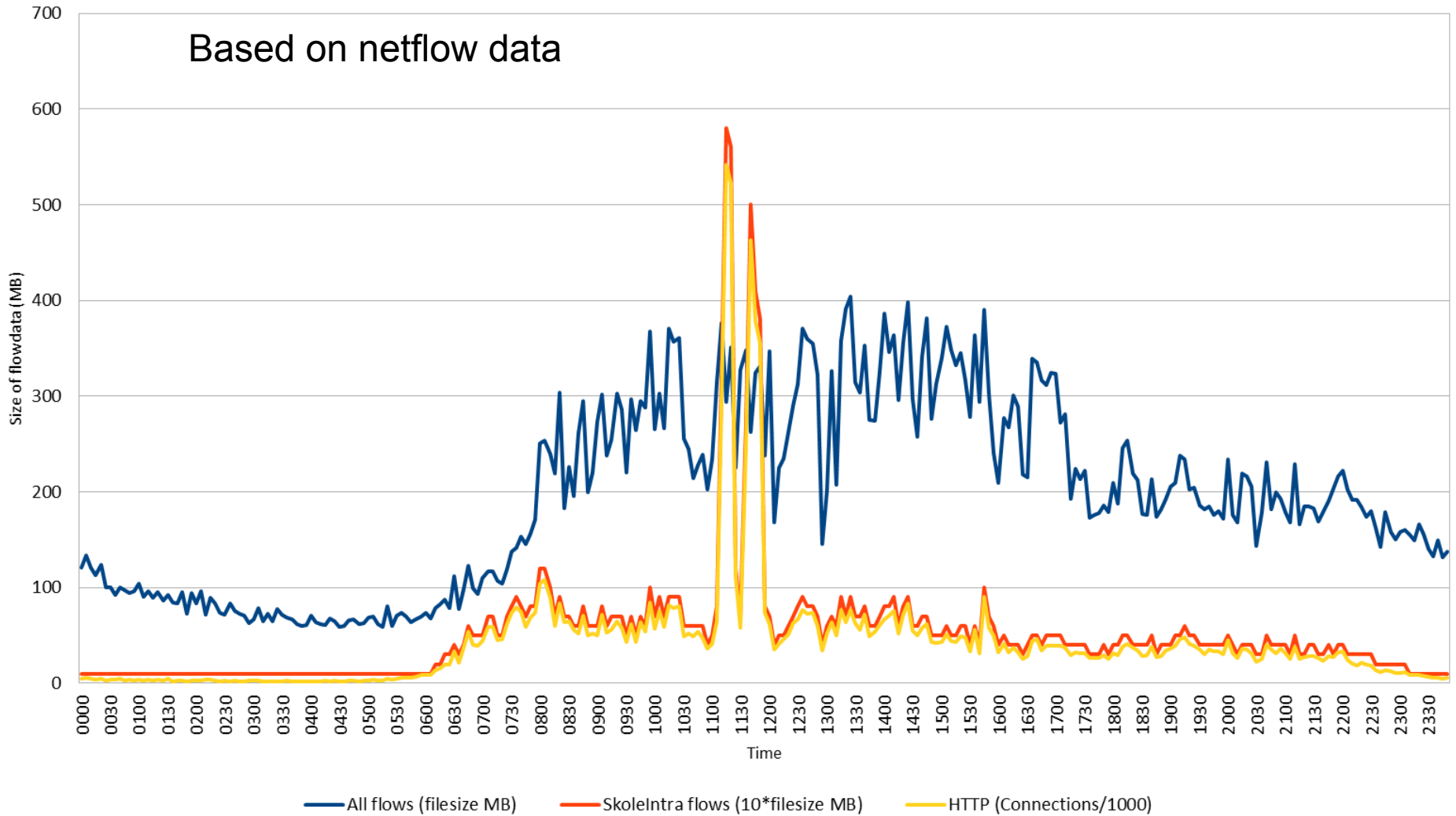
[Under DDoS attack?](#)

Can we handle this problem as part of general NOC operation?

- Why not just look at traffic volumes as part of the on-going general network monitoring?
- ...and manually add filters
- Will not work because we do not have the data at the NOC level

A real-life DDoS attack from our network

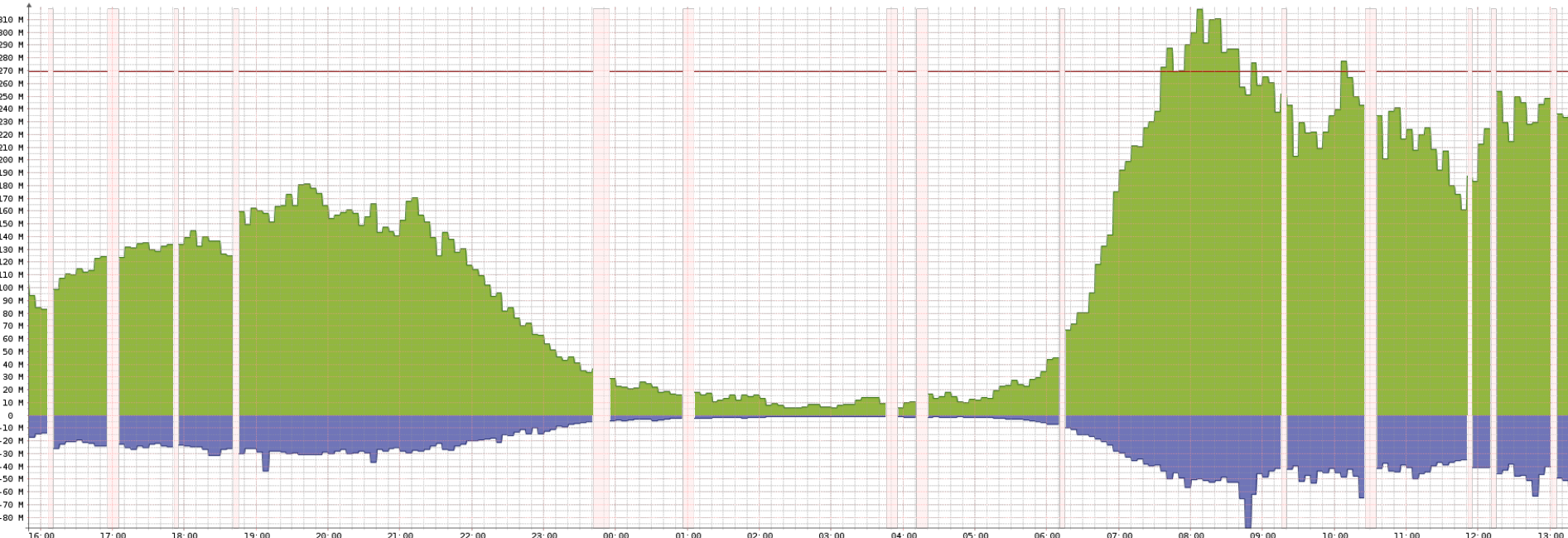
Based on netflow data



19-05-2014

Service Management

If we look at traffic volumes, we see nothing



Bits/s	Last	Avg	Max	95th
In	171.97M	131.18M	318.09M	269.04M
Out	31.93M	24.46M	88.30M	51.09M
Total	1.48T	(In 1.27T Out 239.85G)		

DDoS is here ↑



We do not necessarily see DDoS attacks as part of normal NOC operation

- The only parties who will surely see the attack are the targets (and their users)
- We need to enable users (user institutions) to report the attacks online and real-time

The commercial ISPs offer DDoS protection



DDoS Prote

Beskyt jer mod ar

Døgnet rundt monitorere
øjeblikkeligt, hvis it-krim
tjenester ned

Alle virksomheder med online



DDoS Beskyttelse

- beskyt din virksomhed mod angreb

Virksomheder og institutioner verden over oplever en eksplosiv stigning i antallet og i styrken af DDoS-angreb. Et DDoS-angreb forsøger enten at oversvømme dit netværk via kolossale trafikmængder, at bringe enkelte dele af dit netværk i knæ eller at udnytte svagheder og derigennem trænge ind i

ZEN SECURE

- ▶ Firewall
- ▶ BGP - ISP In A Box
- ▶ DDoS Beskyttelse
- ▶ Rådgivning
- ▶ Anti-Spam



DDoS Protection

Data Protection Suite | Backup og restore | Disaster Recovery | DDoS Protection | Hosted Firewall

Effektiv beskyttelse mod DDoS-angreb

Er DDoS-angreb noget, I bekymrer jer om? Bare rolig - I er ikke alene. Mange virksomheders hverdag og kræver en løsning, der er hurtig og



Vil du vide mere? Kontakt
Zen Systems

Indtast email

Skriv besked...

DDoS protection

- We need special tools to deal with this problem
- We need online, real-time reporting from the users
- Our users expect us to do it – they can not produce it themselves – they can not get it from another service provider
- All the commercial providers have it
- NRENs look old-fashioned when not offering it

So: Let's do it and do it as a community



Deic