DDoS hybrid protection

Pedja Radoicic

25.11.2015.

telenor

Agenda

1	Telenor Group overview
2	DDoS attacks overview
3	DDoS protection system solution
4	DDoS protection system as a service
5	Q&A

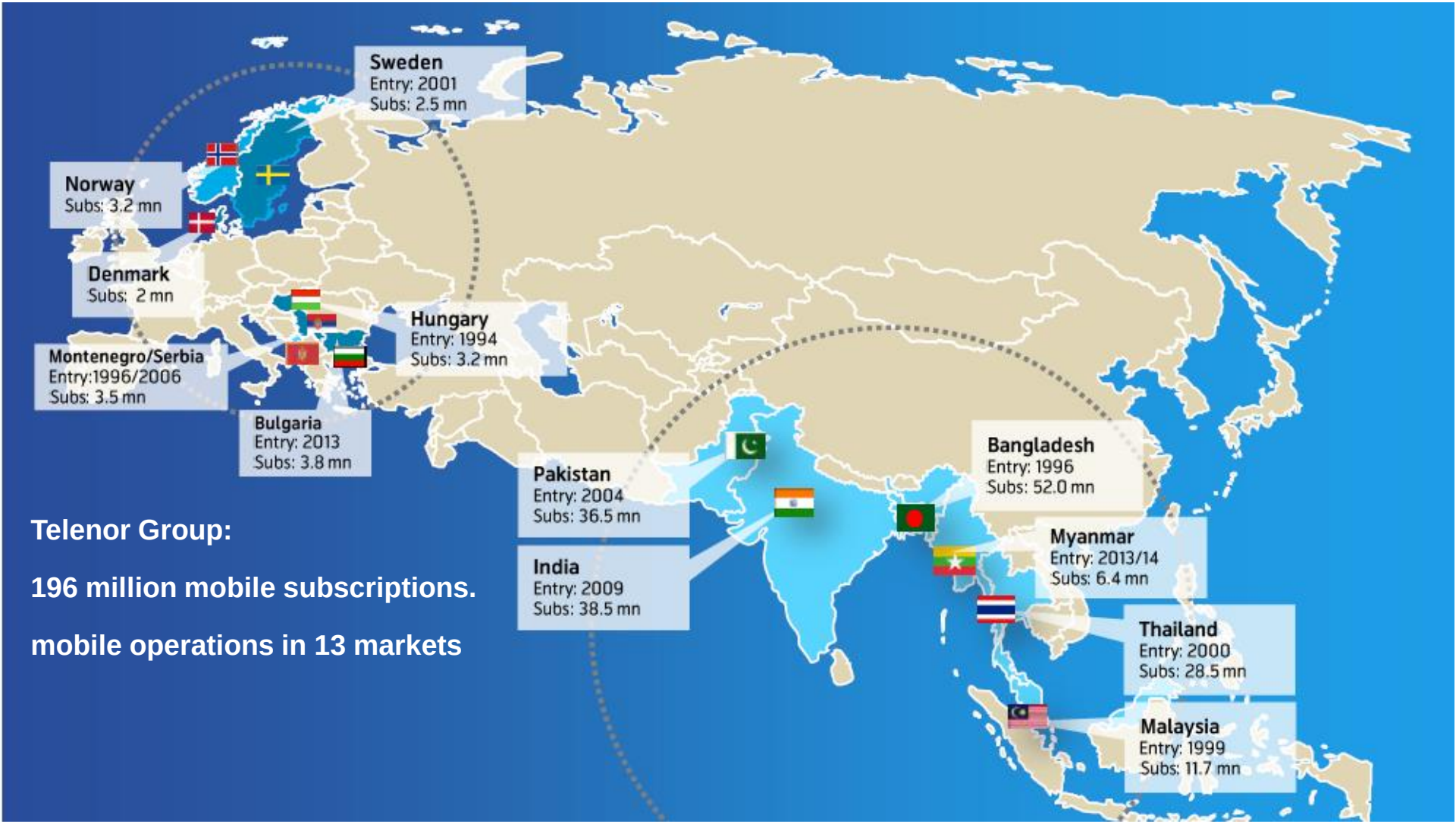
telenor

Agenda

1	Telenor Group overview
2	DDoS attacks overview
3	DDoS protection system solution
4	DDoS protection system as a service
5	Q&A

telenor

1 Telenor Group overview



Telenor Group:

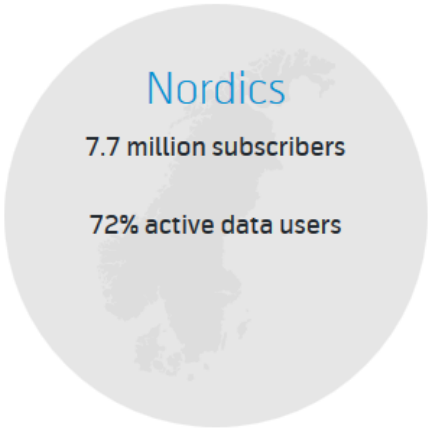
196 million mobile subscriptions.

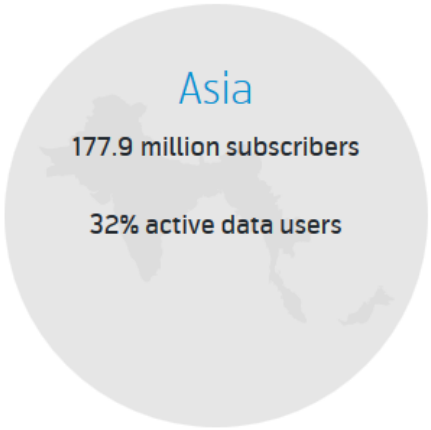
mobile operations in 13 markets

telenor

1 Internet for All

- Telenor Group aims to enable the digital transformation of the societies by extending internet connectivity to as many people as possible.
- About 40% of the world's population has access to the internet.
- Telenor Group has set an ambition of 200 million active internet users by 2017.





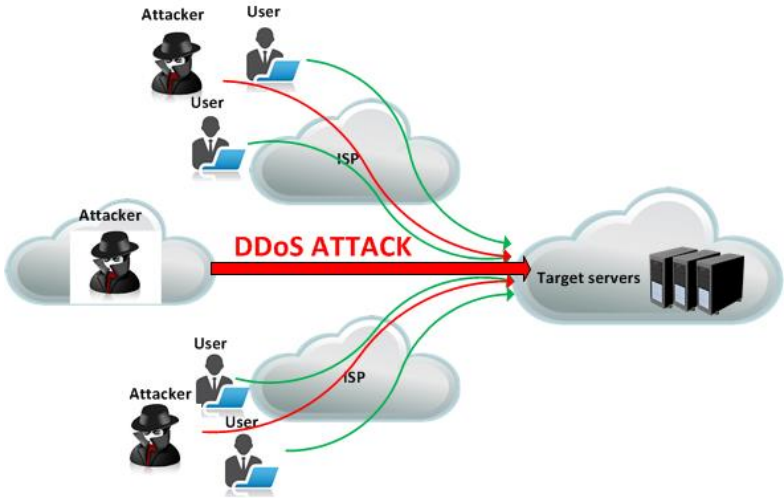
Agenda

1	Telenor Group overview
2	**DDoS attacks overview**
3	DDoS protection system solution
4	DDoS protection system as a service
5	Q&A

telenor

2 DDoS attacks overview

- **DDoS - Multiple compromised host targeting single one**
  - Most terrifying attacks on the Internet
  - Cannot be prevented
  - Suspend data services

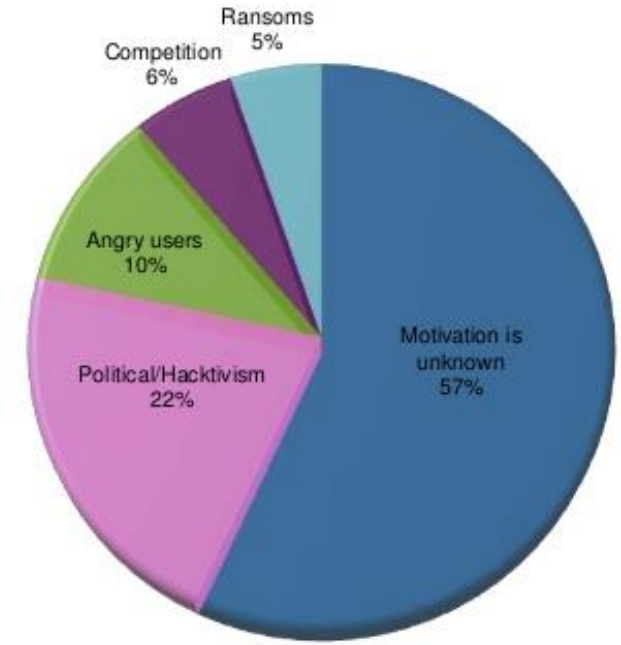


- **Telenor as ISP needs to keep data service availability as high as possible**
- **Telenor customers experienced both major attack families**
  - Volumetric & Application
- **DDoS Lifecycle - the time to detect and mitigate**
- **All service providers are faced with the same threat**

telenor

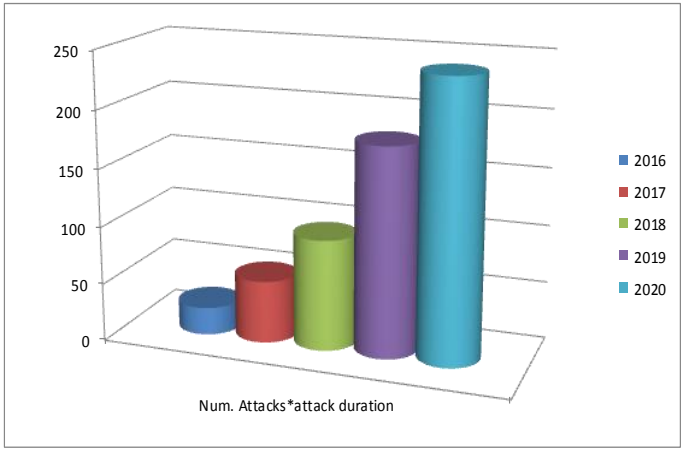
2 DDoS attacks overview

- **DDoS - Motivation for the attack?**
  - Business competition – do some damage to the competing company and make profit indirectly
  - „Hacktivism“ – express your critisism to an organization by taking down their website
  - Extortion, ransom, racketeering
  - Vandalism and Fun



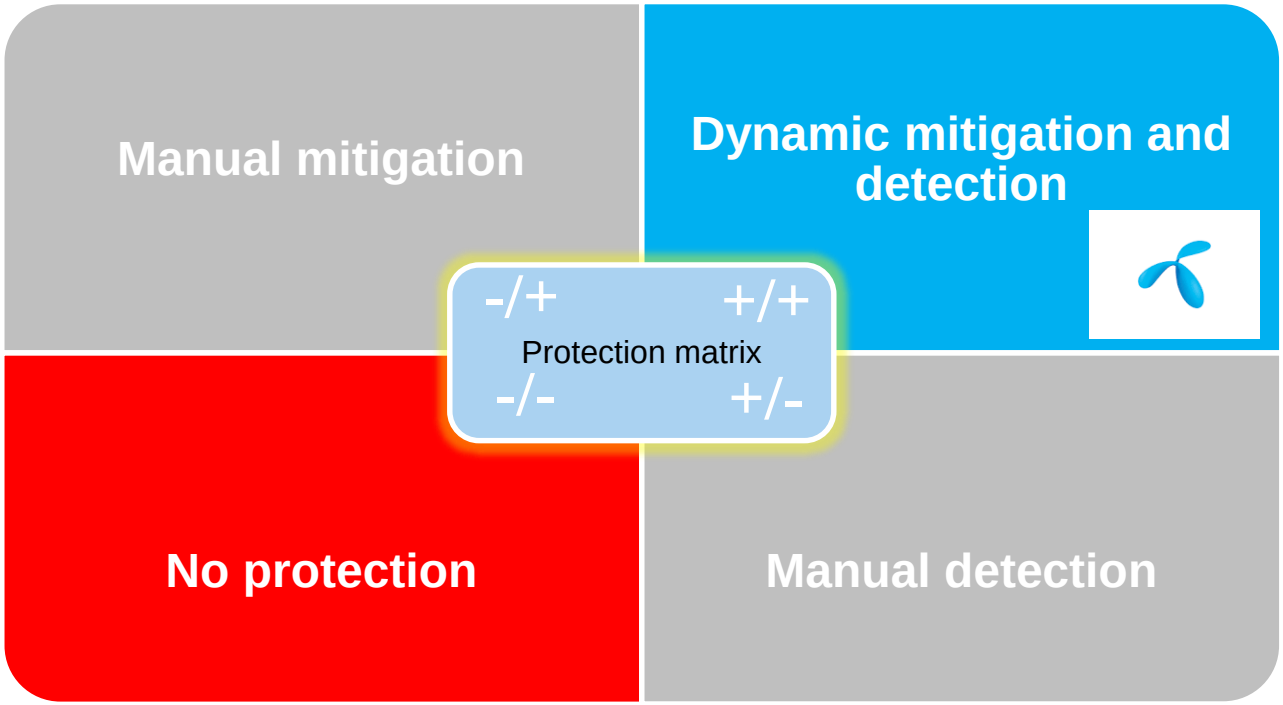
2 DDoS attacks overview – exponential growth

- **DDoS attacks in general**
  - Grow exponentially
  - More unpredictable than ever
  - More data users - more attack attractiveness
- **Zombie army for hire as cheap as ever**
- **Telenor experienced first large attack in 2014**
  - 3 major attacks in 2014
  - 9 attacks in five months 2015
  - 15 more till today



telenor

2 DDoS attacks overview – protection models



Dynamic protection solutions

Purpose-built on-premises system

+

Cloud / managed service

=

Hybrid

telenor

2 DDoS attacks overview – purpose-built system

- **DDoS attacks cannot be mitigated by**
  - Firewall
  - IDS
  - IPS
  - WAF
- **DDoS attacks look like legitimate and cannot be detected**

telenor

2 DDoS attacks overview – Hybrid model

Hybrid model provides Telenor with possibility to:

- **STOP** high capacity volumetric attacks
- **PROTECT**
  - Resources from attacks coming from all ingress points
  - Telenor ISP reputation
- **BE FLEXIBLE** in terms of DDoS protection service levels

telenor

Agenda

1	Telenor Group overview
2	DDoS attacks overview
3	**DDoS protection system solution**
4	DDoS protection system as a service
5	Q&A

telenor

3 DDoS protection system – Hybrid solution

- **Telenor hybrid DDoS protection is based**
  - Local netflow based DDoS protection segment
  - Cloud based Internet pipe protection segment

- **Local netflow based segment**
  - Telenor SOC - Security Operation Centre
  - Multitenat Radware DefencePro element
  - Volumetric and application attack protection

- **Cloud attack protection segment**
  - ERT – Emergency Response team monitor the pipe utilization
  - Volumetric attacks protection upto 1T (today)

telenor radware

- Telenor and Radware design
- Monitored and controlled by Telenor SOC

telenor

3 DDoS protection system – Cloud solution

Volumetric DDoS attack that blocks the Internet pipe

On-premises system mitigates the attack

Clean traffic

ERT with the Telenor SOC decide to divert the traffic

Defense Messaging
Includes traffic baselines

Protected objects
-Internal
- Mobile users
- Fixed customers

Pipe Saturation Alert includes essential information for attack mitigation

ERT monitors both cloud and on-premises devices

radware

SOC monitors on-premises devices

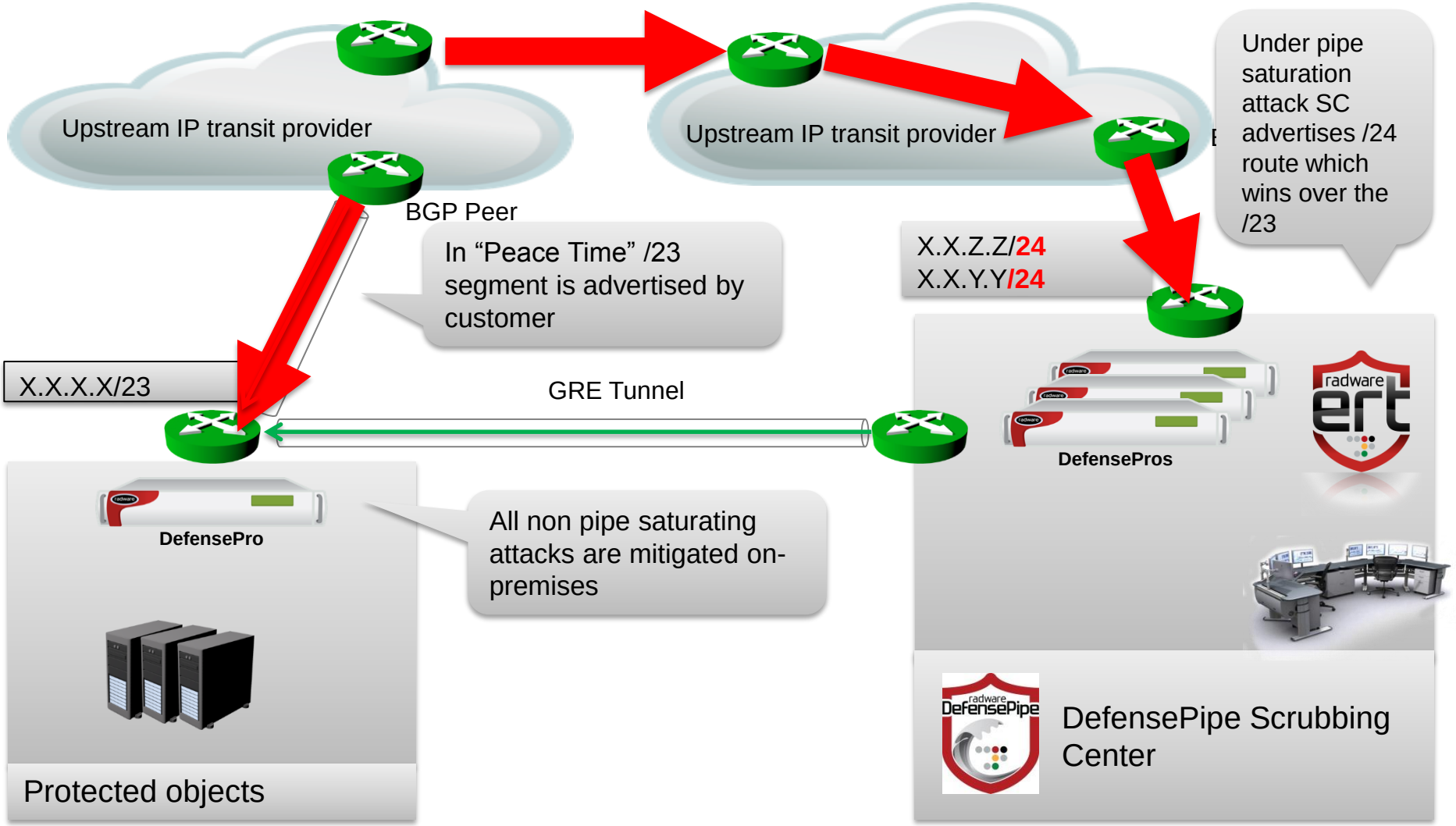
telenor

DefensePipe Scrubbing Center

telenor

Supported by Radware

3 DDoS protection system – Cloud solution



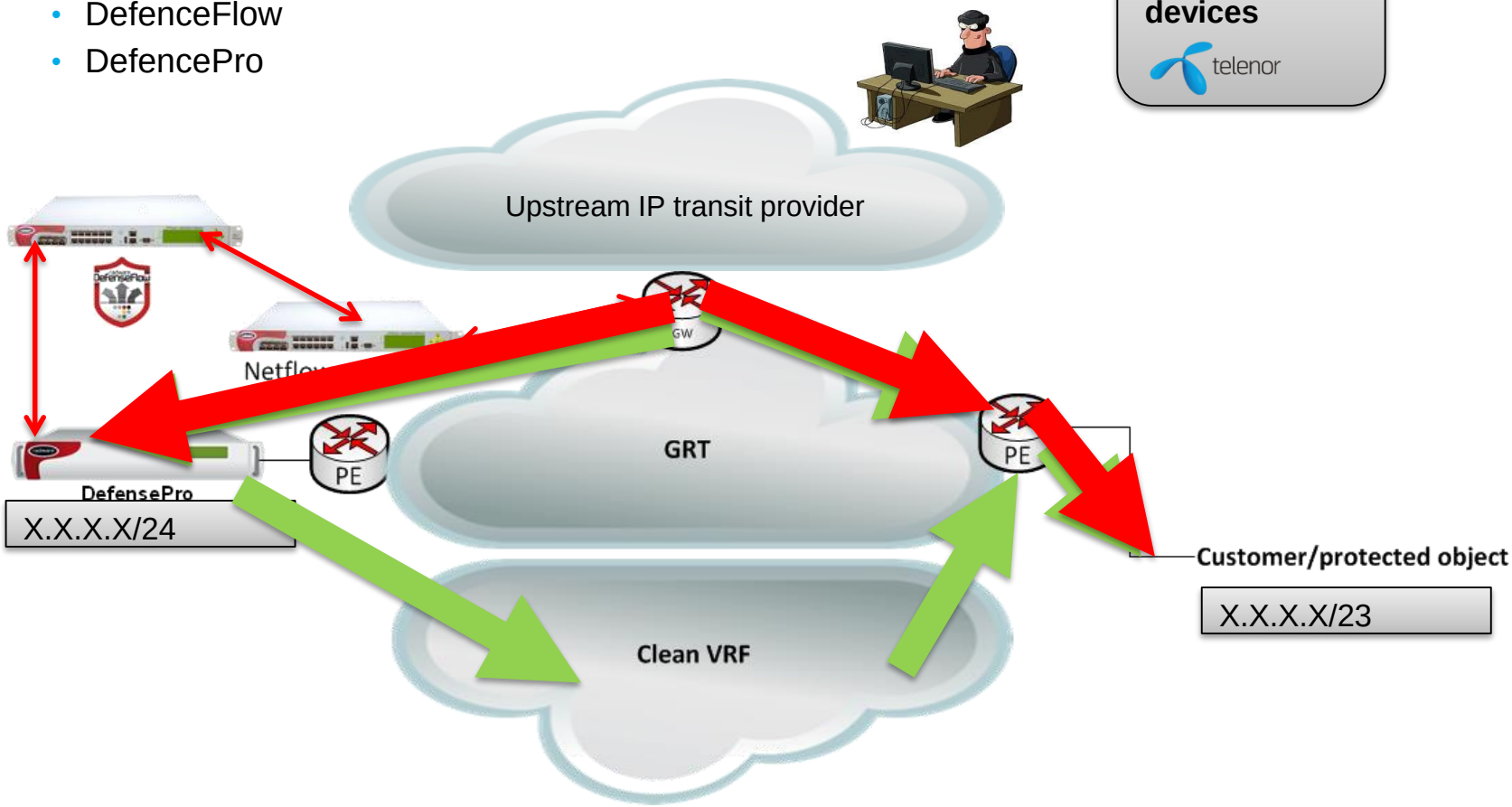
Supported by Radware

3 DDoS protection system – On-premises solution

- **Three step on-premises detection and mitigation**
  - Netflow collector
  - DefenceFlow
  - DefencePro

SOC monitors on-premises devices

telenor



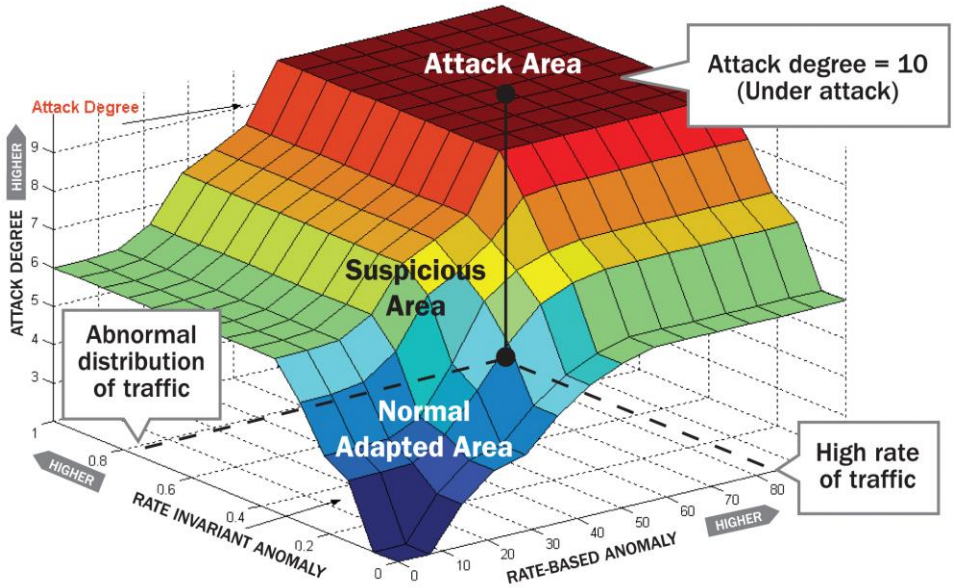
telenor

Supported by Radware

3 DDoS protection system – attack recognition solution

Both layers are built with same Radware DefencePro elements

- Algorithm for attack detection is same in local and cloud scrubbing centre



- The decision engine uses inputs of both rate-based and rate-invariant parameters to provide the degree of attack
- Different layers are used to construct different Telenor DDoS protection service packages

telenor

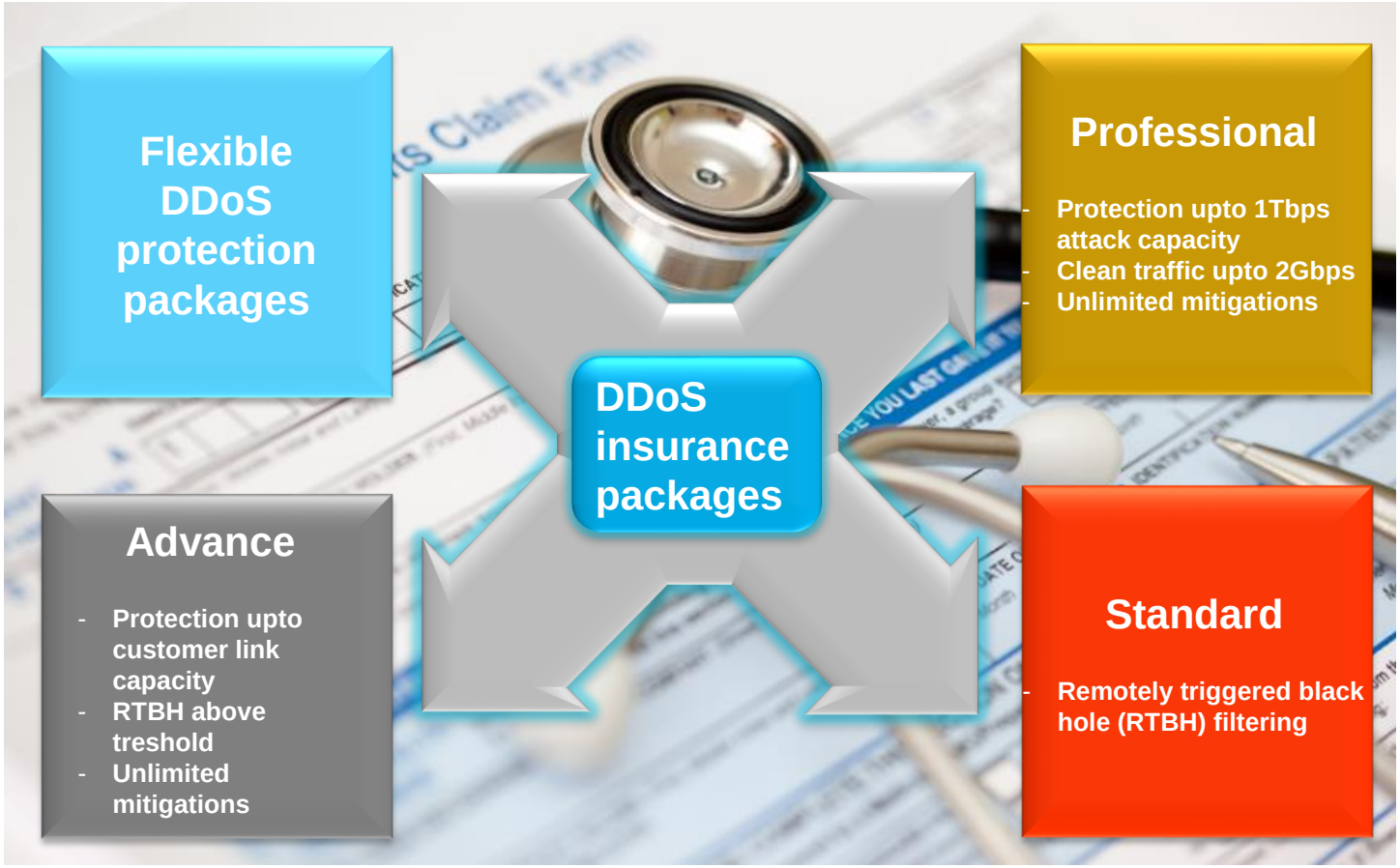
Supported by Radware

Agenda

1	Telenor Group overview
2	DDoS attacks overview
3	DDoS protection system solution
4	**DDoS protection system as a service**
5	Q&A

telenor

4 DDoS protection system as a service



telenor

5

telenor

Thank you

telenor