Universidade do Minho
Serviços de Comunicações

Jornadas FCCN 2017

Infra-estrutura NETFLOW

Marco Teixeira
(marco@scom.uminho.pt)

2017-04-21

Agenda

1 – Introdução

2 – Infra-estrutura NetFlow (Anterior)

3 – Requisitos da Área de Segurança

4 – Infra-estrutura NetFlow (Actual)

5 – Trabalho futuro

6 – Questões

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

(art. 32º do Regulamento Orgânico das Unidades de Serviços da Universidade do Minho)

1. Os Serviços de Comunicações da Universidade, adiante designados por SCOM, fornecem serviços e infraestrutura de comunicações à Universidade.

2. Compete aos SCOM a conceção, implementação e exploração de infraestruturas e serviços de comunicação basilares, nomeadamente o fornecimento dos recursos necessários ao desenvolvimento e manutenção da infraestrutura de comunicações e serviços básicos de apoio aos projetos a Universidade, designadamente:

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

a) A gestão técnica das infraestrutura de voz e dados na Universidade;
b) A administração dos serviços básicos de comunicações de voz e dados;
c) A gestão das comunicações;
d) Os serviços de segurança na área das comunicações;
e) Gestão técnica e apoio às salas de access grid existentes nos campi da Universidade;
f) Assegurar o estabelecimento e monitorização de acordos de nível de serviço com os utentes, garantindo o atendimento e apoio técnico associado à configuração de portáteis e outros equipamentos, gestão de incidentes, pedidos de alterações de

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

Mais informações em:

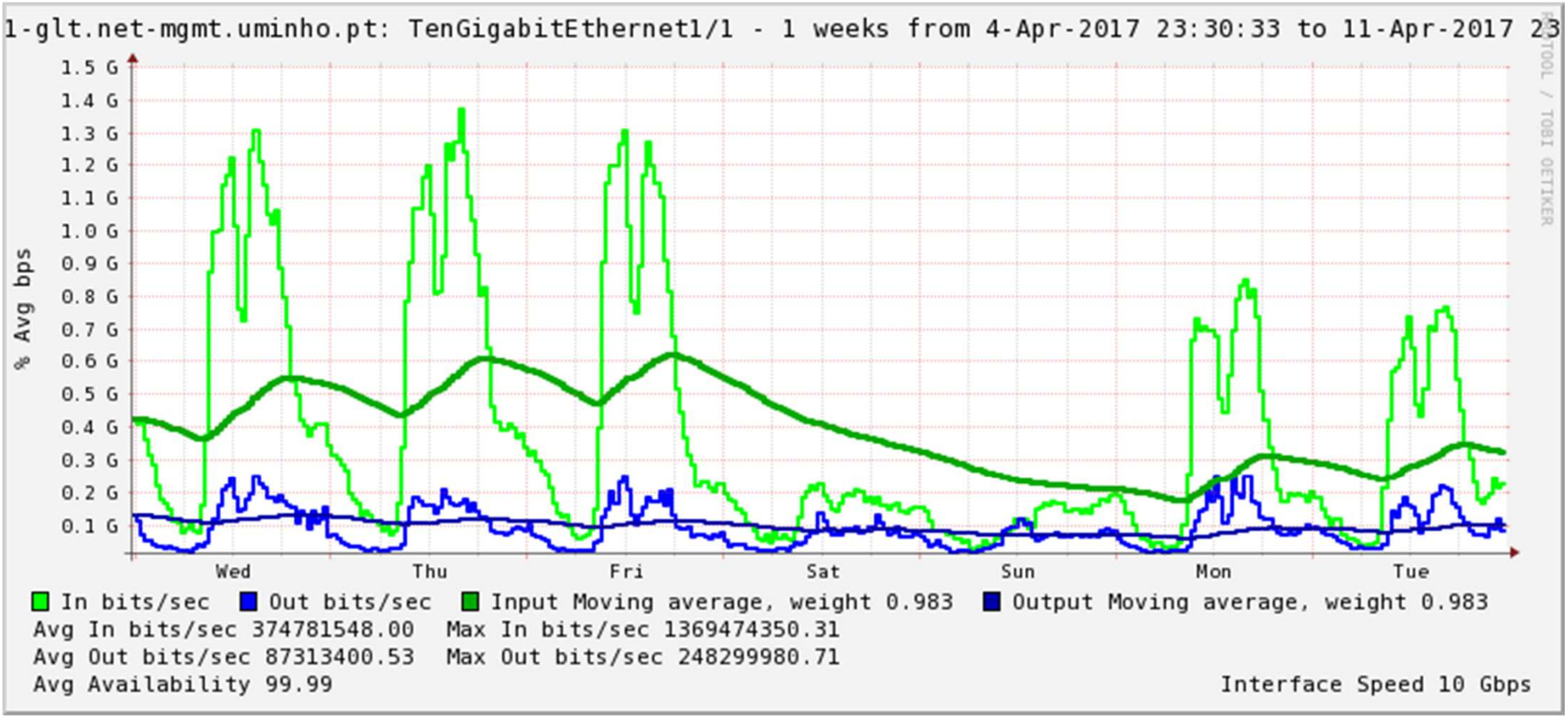
http://www.scom.uminho.pt

Onde podem encontrar, entre outros:

- Catálogo de Serviços
- Relatórios de Atividades
- Dados sobre a infra-estrutura gerida

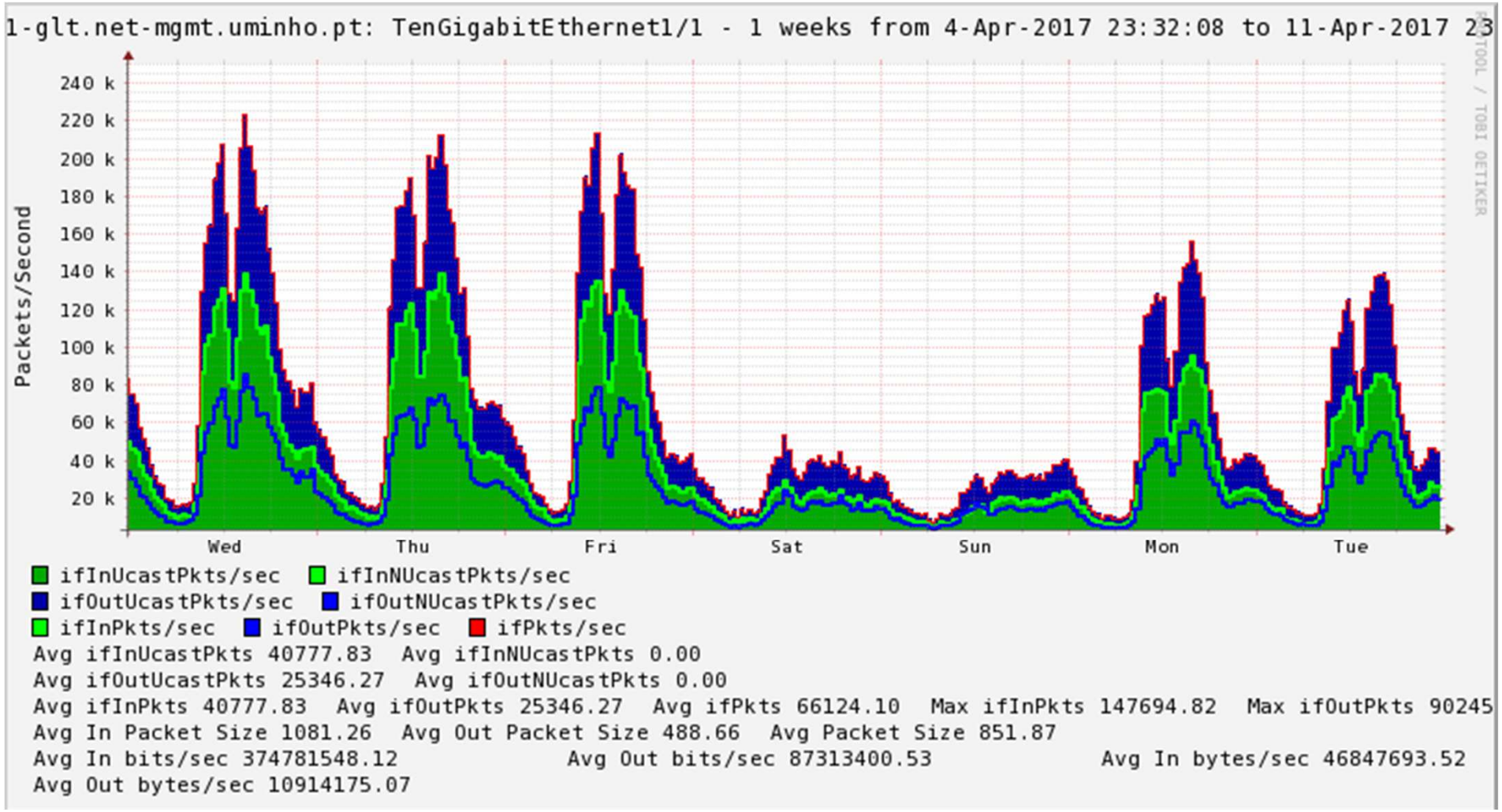
Introdução

Padrão de Tráfego

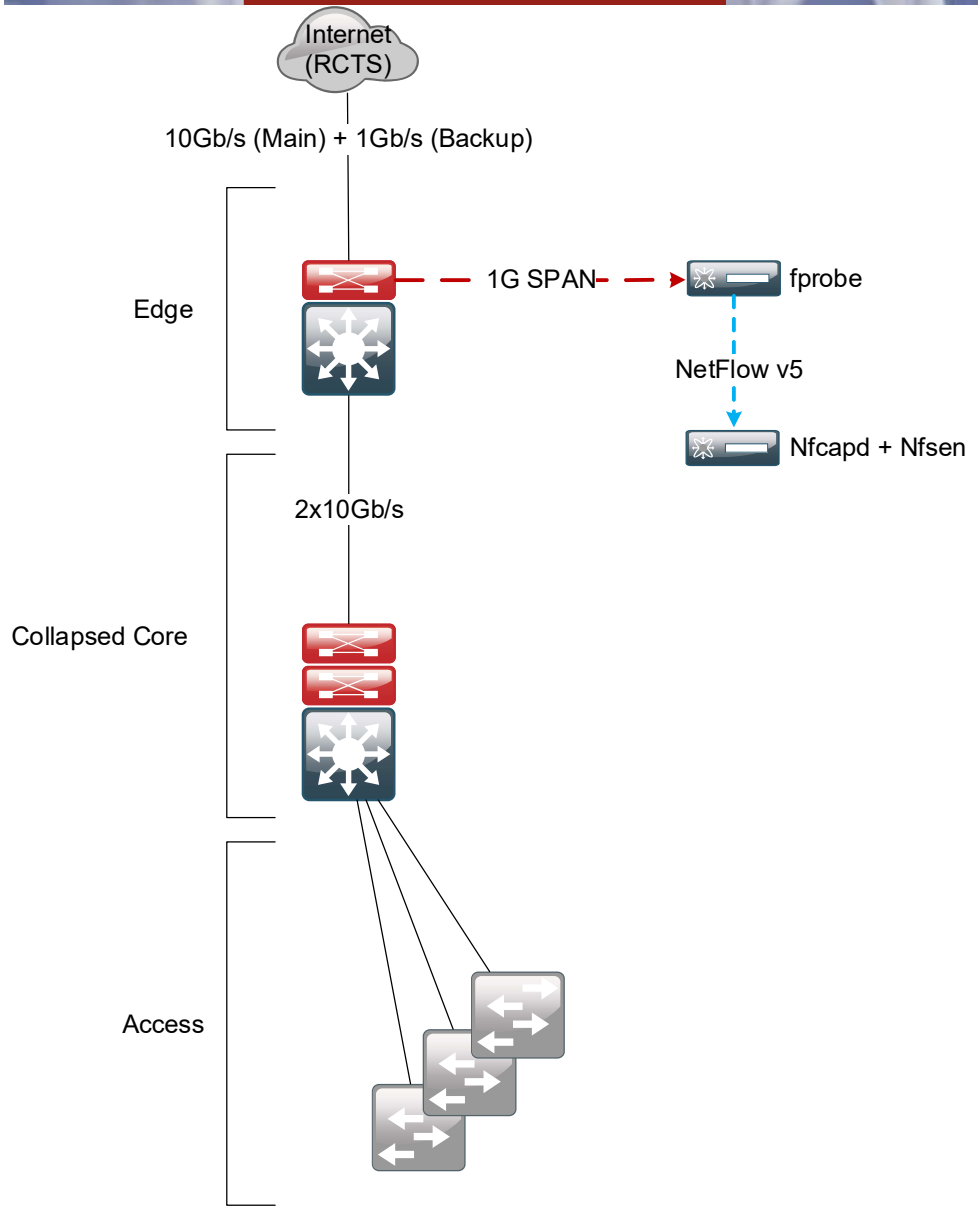


Introdução

Padrão de Tráfego



Infra-estrutura NetFlow



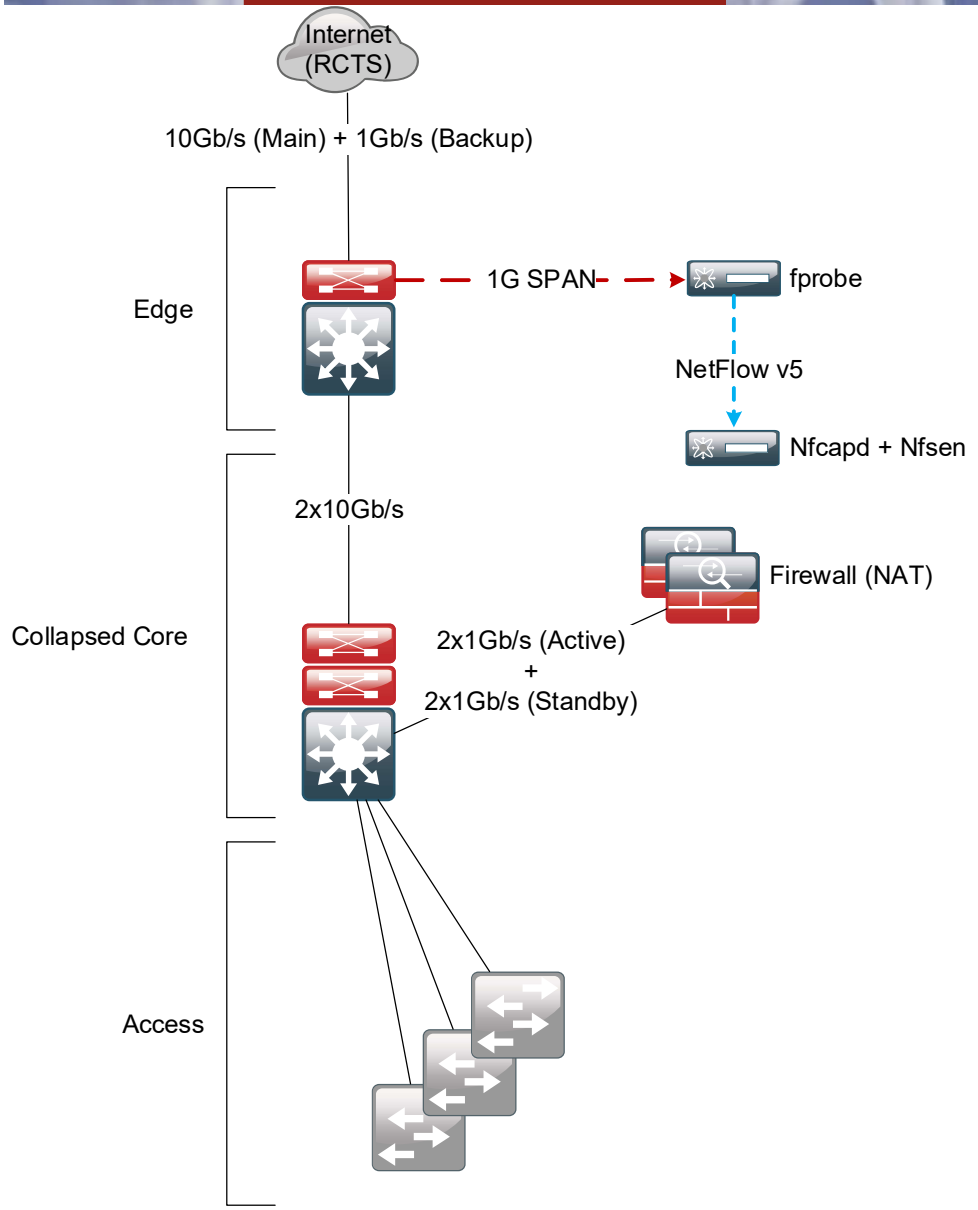
Pontos Fortes:

- Simplicidade
- Poucos recursos

Pontos fracos:

- Visibilidade apenas até ao "primeiro" Gb/s
- Falta de visibilidade sobre "flows" IPv6
- Visibilidade apenas na "fronteira"
- Gerava "Flows" sobre tráfego descartado pela ACL de fronteira

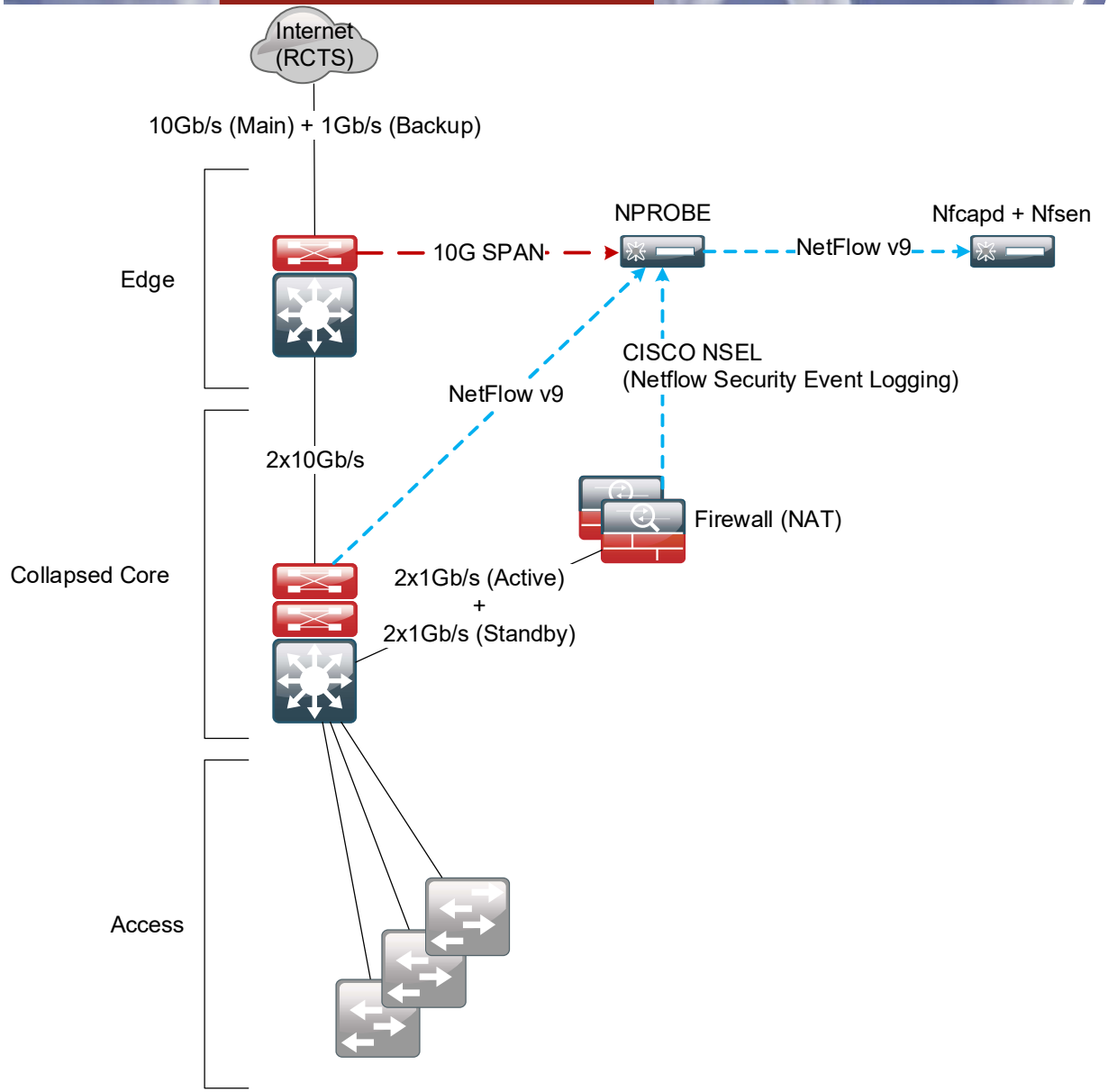
Requisitos da Área de Segurança



Requisitos:

- Alcançar visibilidade total sobre o tráfego de entrada
- Ganhar visibilidade sobre o tráfego entre o "Edge" e (no) "Core"
- Ganhar visibilidade sobre o tráfego IPv6
- Ganhar visibilidade sobre o tráfego cursado com recurso a NAT (dispensando a consulta de logs)
- Alcançar melhor performance nas operações de consulta sobre os Flows
- Alcançar maior tempo de retenção dos NetFlow

Infra-estrutura
NetFlow



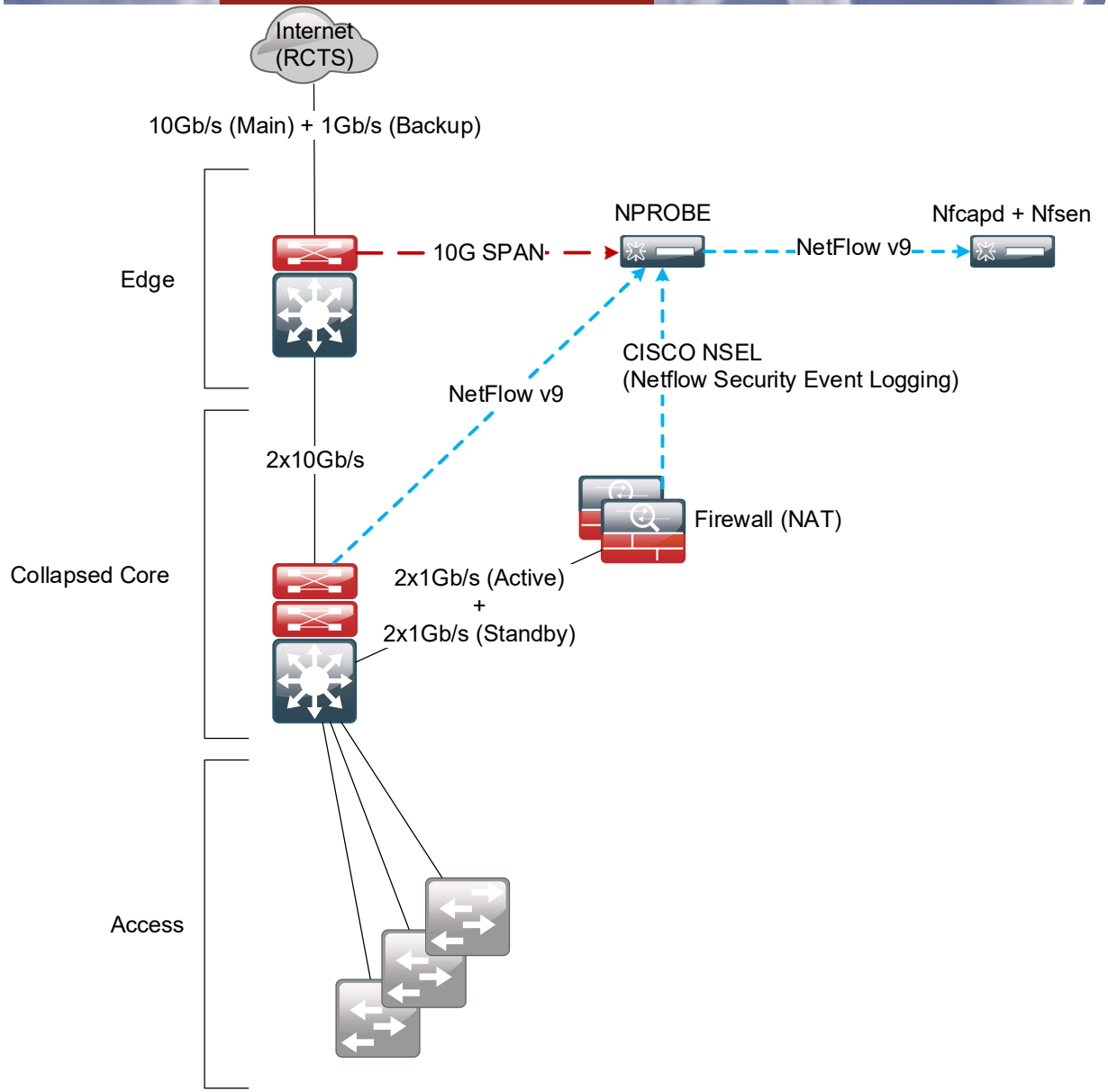
Pontos fracos:

- Mais complexidade
- Mais recursos

Pontos fortes:

- Resposta a todos os requisitos da Área de Segurança

Infra-estrutura NetFlow



Adcionalmente:

- Serve de sonda à plataforma SIEM (AlienVault) e ao NTOP-NG (JSON over ZQM)
- Permite com mínimo esforço, adicionar destinos para testar/implementar novas soluções (Kibana)
- Permite converter e exportar várias versões (CISCO NSEL, Netflow v5/v9, IPFIX)
- Vários plugins

Infra-estrutura NetFlow

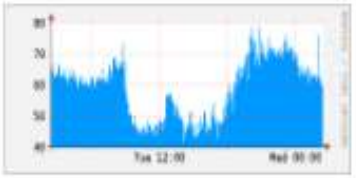
Home | Graphs | Details | Alerts | Stats | Plugins | continuous | Bookmark URL | Profile: swb-s0-glt ▼

Profile: swb-s0-glt

TCP

UDP

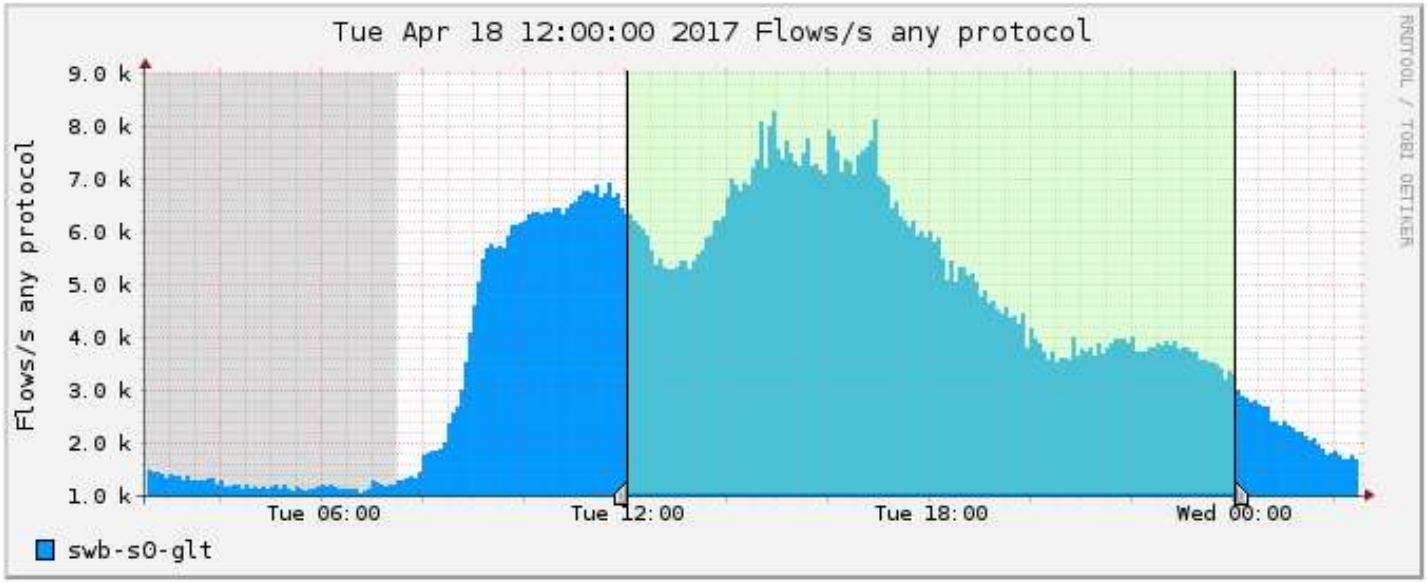
ICMP



other

Profileinfo:

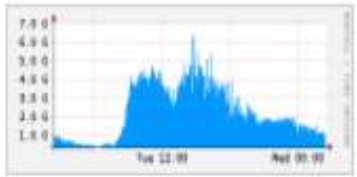
Type: continuous
Max: 20.0 GB
Exp: 60 days 0 hours
Start: Apr 18 2017 - 06:30 WEST
End: Apr 19 2017 - 01:35 WEST



t_{start} 2017-04-18-12-00
t_{end} 2017-04-19-00-00

Packets

Traffic



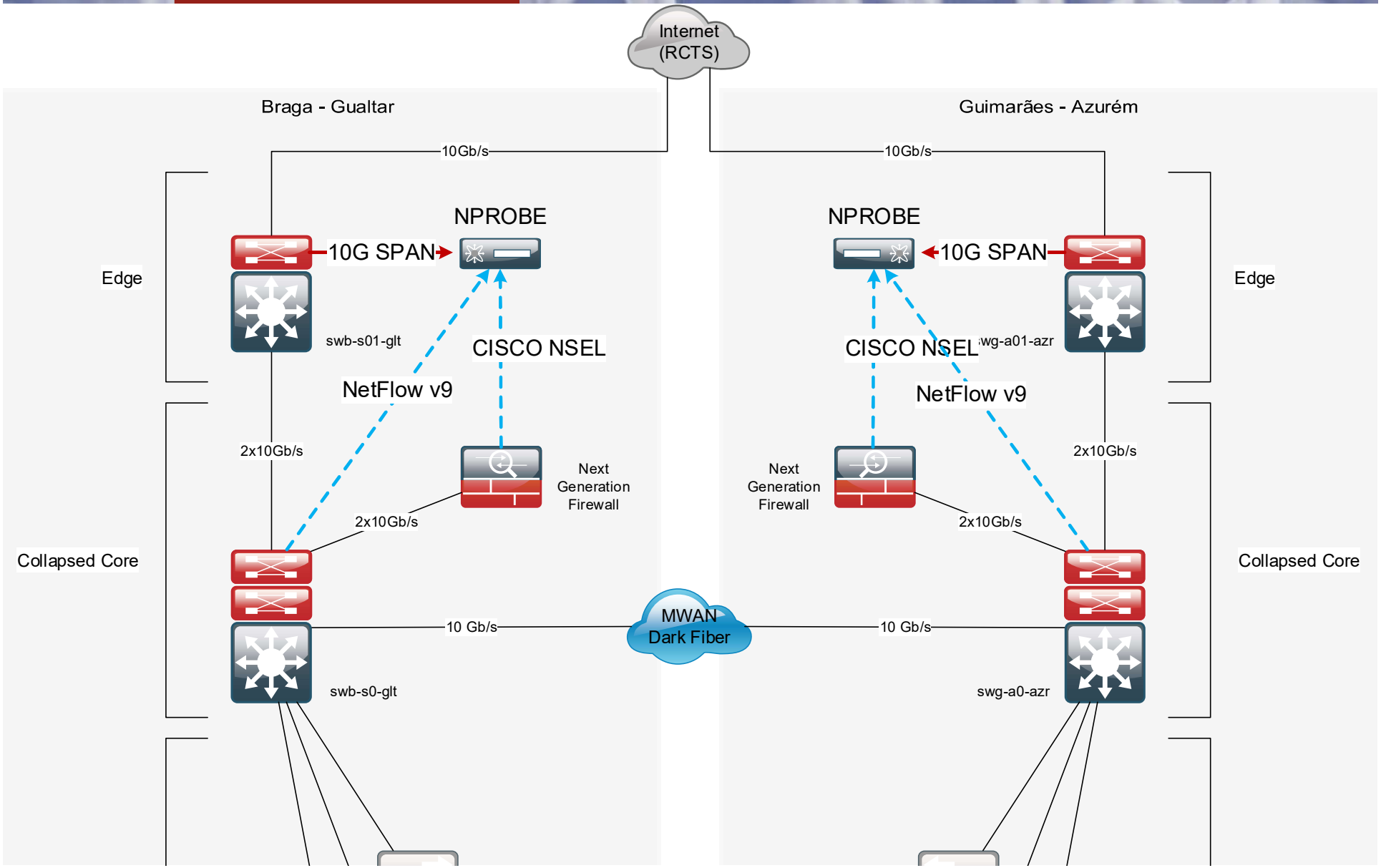
Select Time Window ▼ Display: 1 day ▼ << < | ^ > >> >|

◉ Lin Scale ◉ Stacked Graph
○ Log Scale ○ Line Graph

Trabalho Futuro

- Implementar redundância (geográfica)
- Pensar a escalabilidade
- Tirar partido da tecnologia PF_Ring ZC (ZERO-COPY)
- Configurar novos “profiles” no NFSen
- Avaliar o impacto na performance e implementar plugins no NFSen (para)
- Passar da reatividade semanal, aos relatórios do CERT.FCCN, para uma postura proactiva (também precisamos de acesso a feeds de qualidade ☺)
- Implementar a abertura automática de incidentes no RTIR com base no ponto anterior
- Pensar a anonimização dos dados, para que possam ser usados fora da esfera de confidencialidade do serviço, p.e. na investigação cientifica
- Detecção de (D)DoS com base em Packet Headers (IPFIX)

Trabalho Futuro



Questões?

marco@scom.uminho.pt
www.scom.uminho.pt