UNIVERSITY OF AMSTERDAM

R. van der Gaag, M. Slotboom

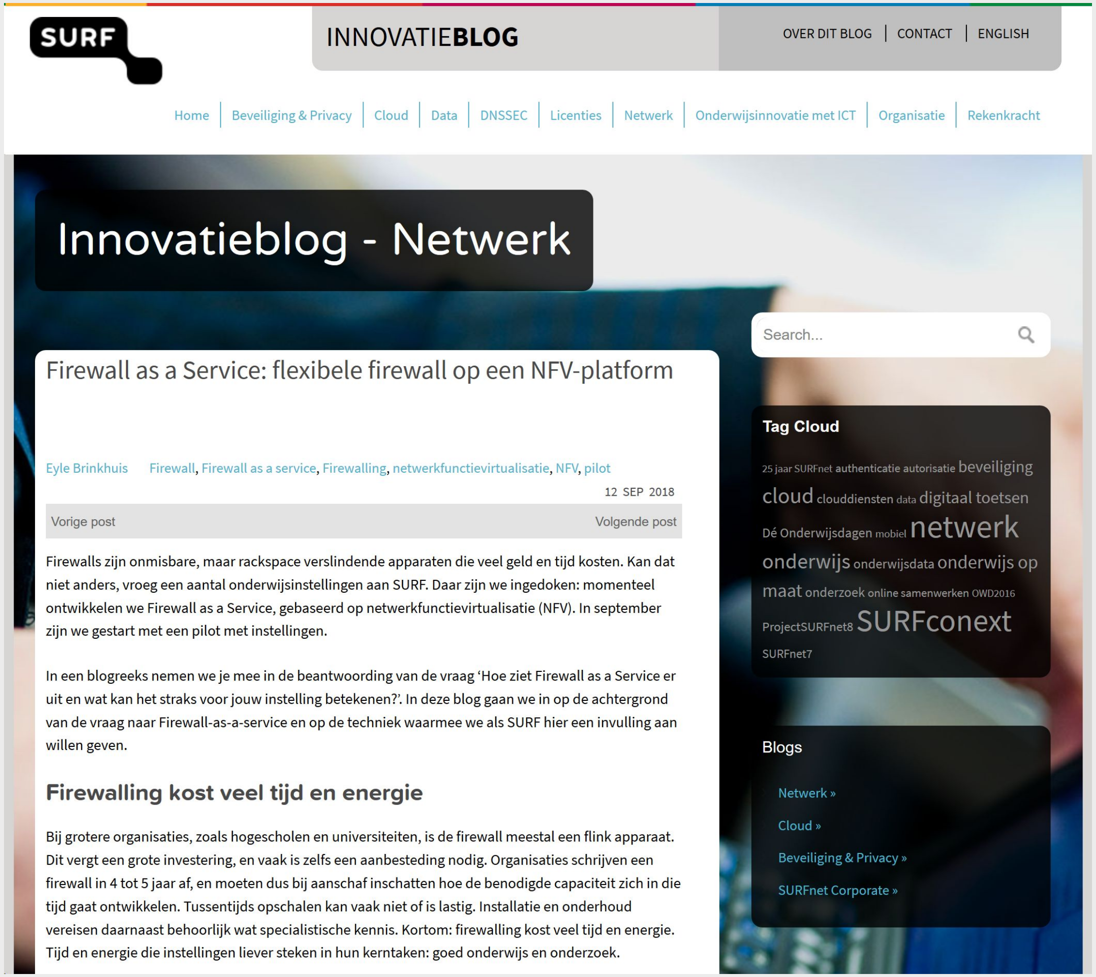
Technical feasibility of Segment Routing Traffic Engineering to steer traffic through VNFs

Research Project 1

SURF NET

SURF is the collaborative ICT organisation for Dutch education and research.

- Education institutions
- Universities
- Research institutions



SURF

INNOVATIEBLOG

OVER DIT BLOG | CONTACT | ENGLISH

Home | Beveiliging & Privacy | Cloud | Data | DNSSEC | Licenties | Netwerk | Onderwijsinnovatie met ICT | Organisatie | Rekenkracht

Innovatieblog - Netwerk

Firewall as a Service: flexibele firewall op een NFV-platform

Eyle Brinkhuis Firewall, Firewall as a service, Firewalling, netwerkfunctievirtualisatie, NFV, pilot

12 SEP 2018

Vorige post Volgende post

Firewalls zijn onmisbare, maar rackspace verslindende apparaten die veel geld en tijd kosten. Kan dat niet anders, vroeg een aantal onderwijsinstellingen aan SURF. Daar zijn we ingedoken: momenteel ontwikkelen we Firewall as a Service, gebaseerd op netwerkfunctievirtualisatie (NFV). In september zijn we gestart met een pilot met instellingen.

In een blogreeks nemen we je mee in de beantwoording van de vraag 'Hoe ziet Firewall as a Service er uit en wat kan het straks voor jouw instelling betekenen?'. In deze blog gaan we in op de achtergrond van de vraag naar Firewall-as-a-service en op de techniek waarmee we als SURF hier een invulling aan willen geven.

Firewalling kost veel tijd en energie

Bij grotere organisaties, zoals hogescholen en universiteiten, is de firewall meestal een flink apparaat. Dit vergt een grote investering, en vaak is zelfs een aanbesteding nodig. Organisaties schrijven een firewall in 4 tot 5 jaar af, en moeten dus bij aanschaf inschatten hoe de benodigde capaciteit zich in die tijd gaat ontwikkelen. Tussentijds opschalen kan vaak niet of is lastig. Installatie en onderhoud vereisen daarnaast behoorlijk wat specialistische kennis. Kortom: firewalling kost veel tijd en energie. Tijd en energie die instellingen liever steken in hun kerntaken: goed onderwijs en onderzoek.

Search...

Tag Cloud

25 jaar SURFnet authenticatie autorisatie beveiliging cloud clouddiensten data digitaal toetsen Dé Onderwijsdagen mobiel netwerk onderwijs onderwijsdata onderwijs op maat onderzoek online samenwerken OWD2016 ProjectSURFnet8 SURFconext SURFnet7

Blogs

- Netwerk »
- Cloud »
- Beveiliging & Privacy »
- SURFnet Corporate »

Network Function Virtualization Pilot

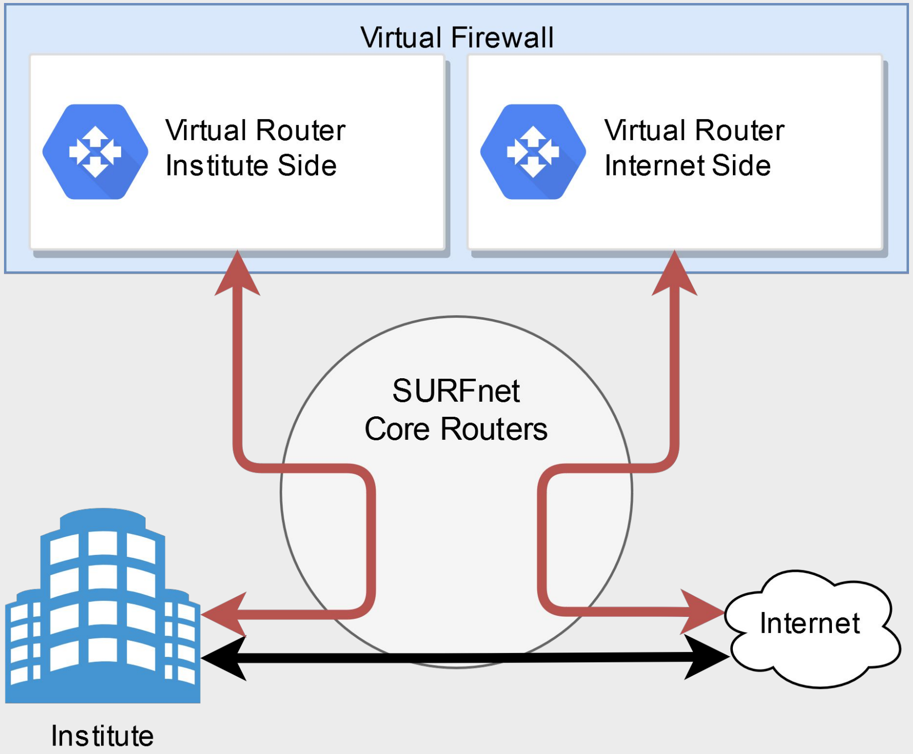
Firewall as a Service (FaaS) Outsourcing

Virtual Network Function (VNF)

Current Pilot solution

Using GRE tunnels and BGP

Added overhead and complexity per institute



Research questions

What are the **practical implications** and the **maturity** of **steering** network traffic through VNFs using **Segment Routing over MPLS** instead of the current GRE tunneling solution for SURFnet?

Two sub questions:

1. **practical implications**
2. **maturity**

Related work

Abdelsalam et. al gave an overview of SR components

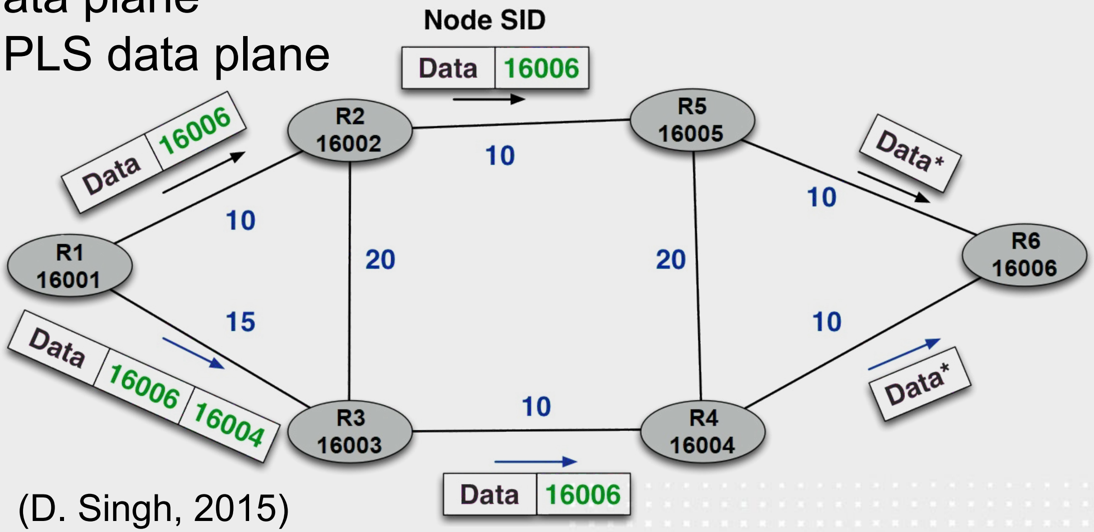
- SR-aware
- SR-unaware

Filsfils et. al conducted an experiment in 2015 for SR with Service Function Chaining

- Gave insight in different use cases

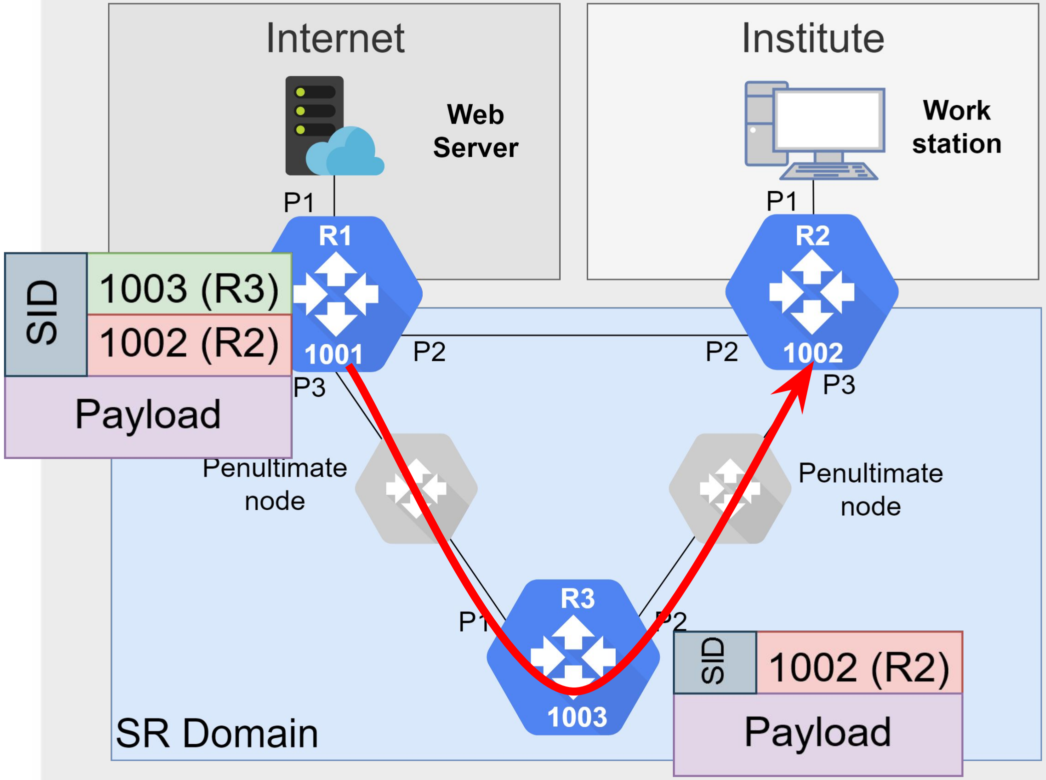
Background: What is Segment Routing?

- Source Routing Paradigm
- Point to ‘Segments’ in the network
- Segments identified with number (SID)
  - Nodes
  - Links (Adjacent Segment IDs)
  - Services
- SRv6 uses the IPv6 data plane
- SR-MPLS uses the MPLS data plane



(D. Singh, 2015)

Reference network - Segment Routing



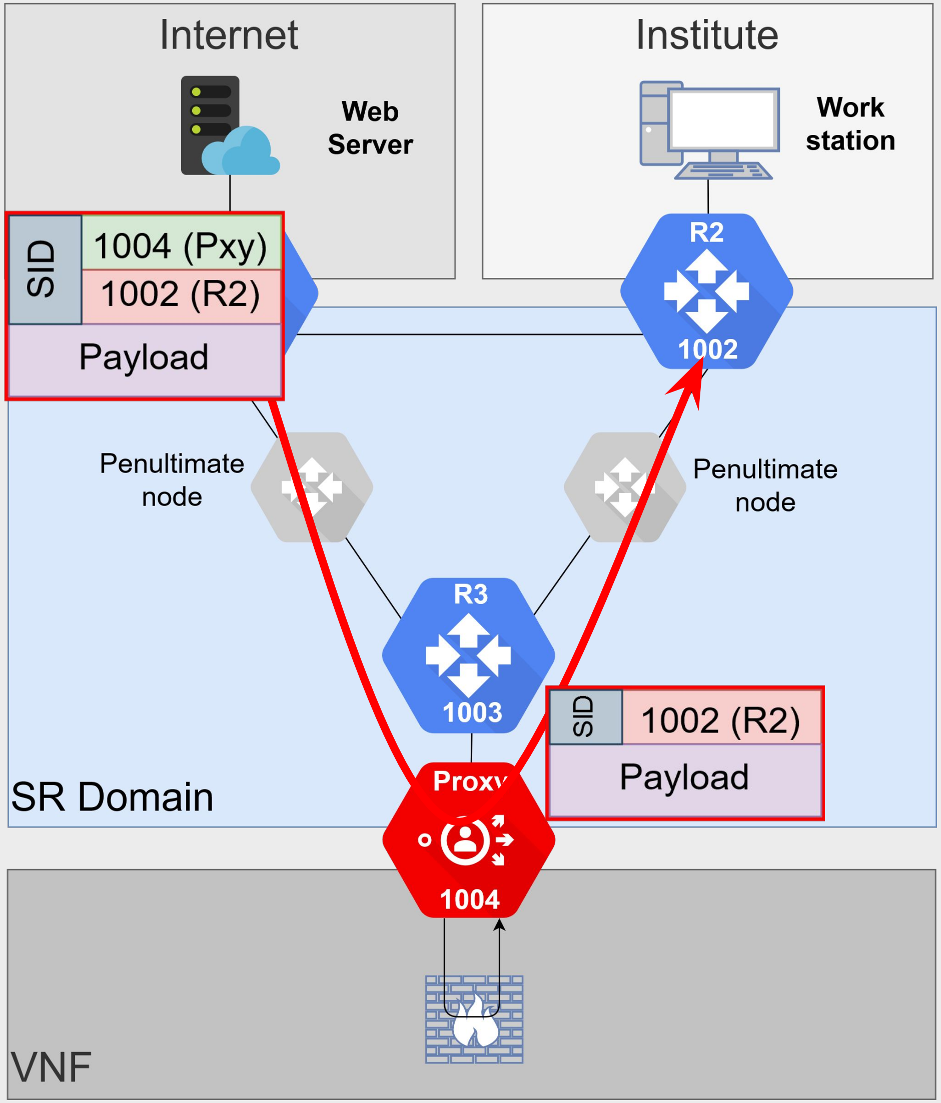
SURFnets new network uses SR-MPLS

Routers part of SR domain

Segment ID: Node, Adjacency

Penultimate node ‘pops’ label

Scenario A

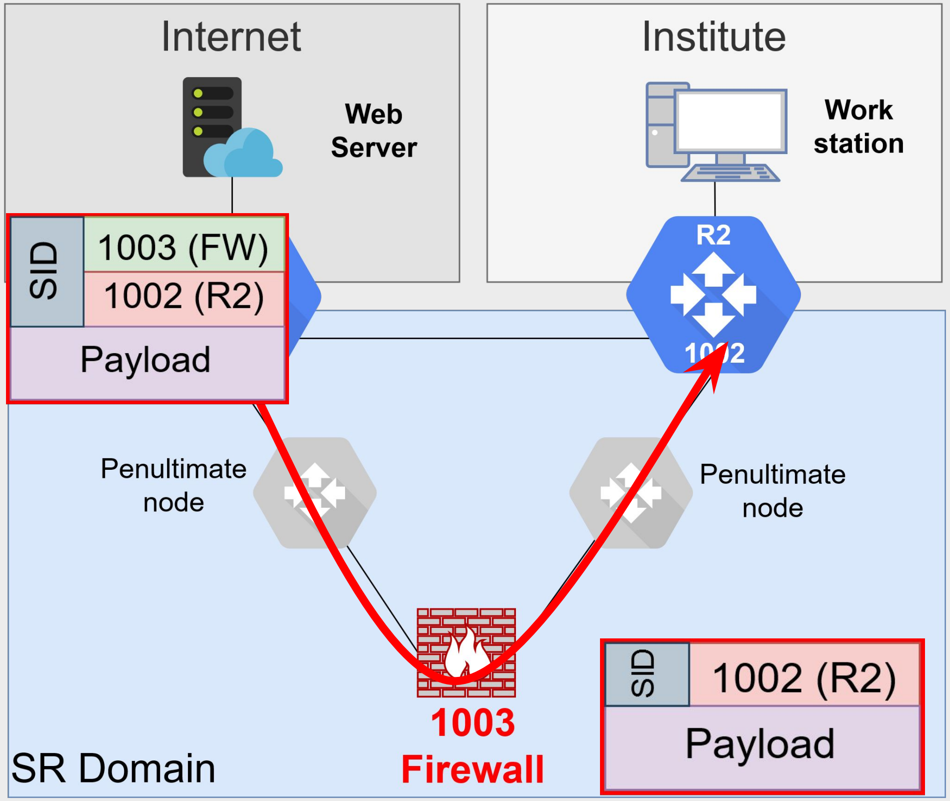


SR-unaware VNF
Dedicated SR-proxy

+ Every VNF can be used

- Extra device needed with own SID

Scenario B

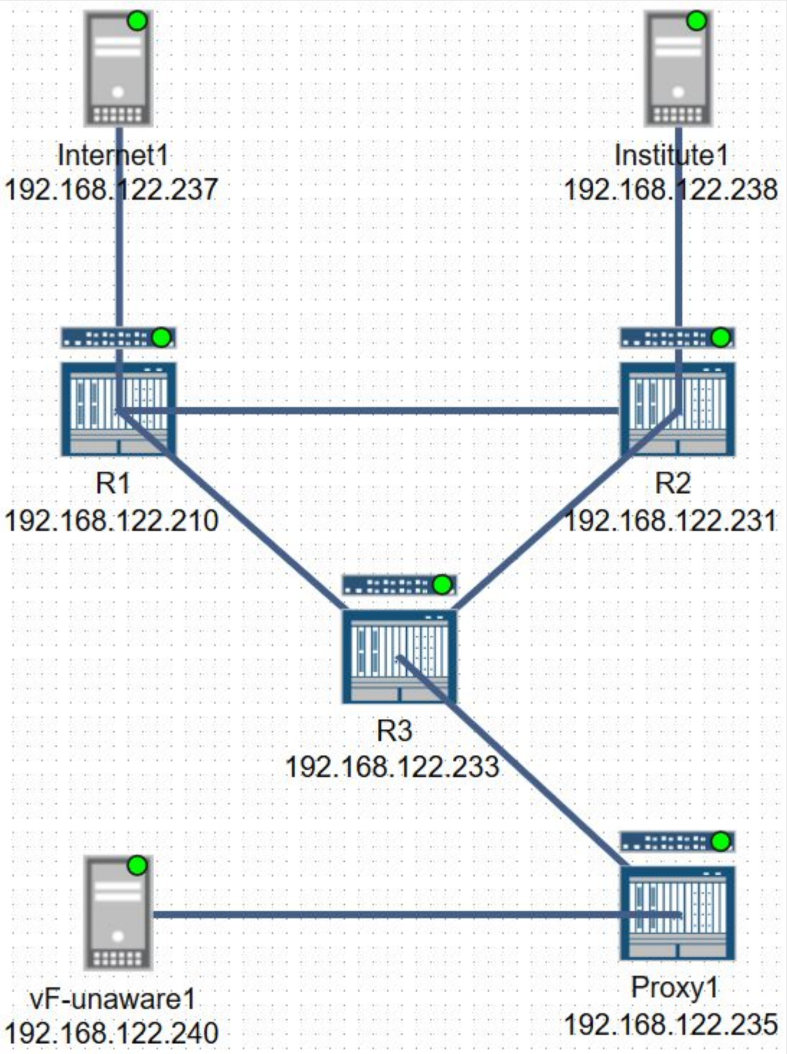


SR-aware VNF
VNF part of SR-domain

+ Most dynamic due to own SID
+ No proxy needed

- Every VNF needs to be SR-aware

Proof of Concept



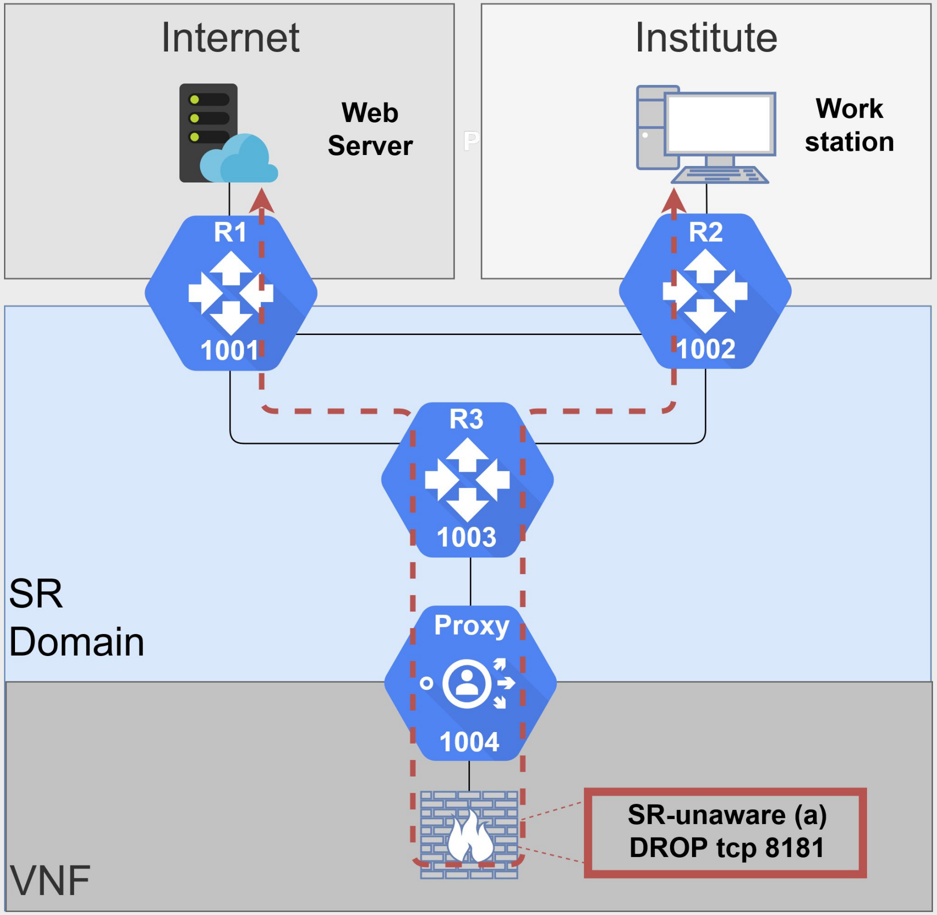
Virtual testbed containing:

- 3 Juniper vMX routers
- 1 Juniper vMX “proxy”
- 3 virtual machines (firewall appliance, web server and workstation)

Two scenarios:

- SR-unaware firewall (A)
- SR-aware firewall (B)

Proof of Concept (A)



Dedicated Proxy used

R3 is penultimate node due to the proxy

Only IP packets from R3 to Proxy

Demo Time

Conclusions

What are the **practical implications** and the **maturity** of **steering** network traffic through VNFs using **Segment Routing over MPLS** instead of the current GRE tunneling solution for SURFnet?

“Labelling” instead of static GRE tunneling

Two scenarios identified with their own characteristics:

SR-aware VNF

- Not mature, due to the lack of SR-MPLS aware VNFs
- Not fully tested in PoC, where a router was used as ‘firewall’

SR-unaware VNF with proxy

- Tested in PoC and mature with static proxy, but still in development
- Network traffic was steered through the firewall and filtered

Future work

- Performance testing of SR-MPLS in pilot including more Institutes
- Using SRv6 in SURFnets new network instead of SR-MPLS (data planes)
- Testing SR-aware functions in pilot based on SR-MPLS and SRv6