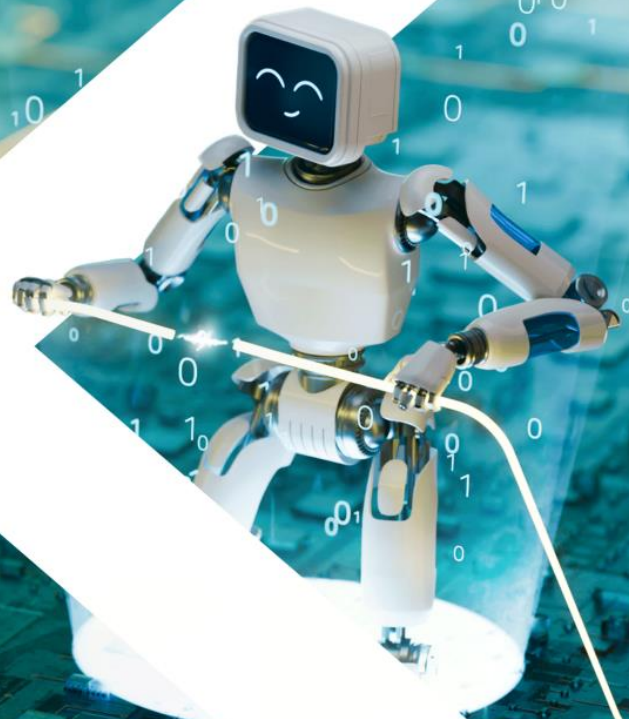


NOKIA

# Secure the future

Dominique Schaeffer  
Director IP Consulting Engineering EMEA

European Peering Forum  
Vienna, 16-18 September 2024



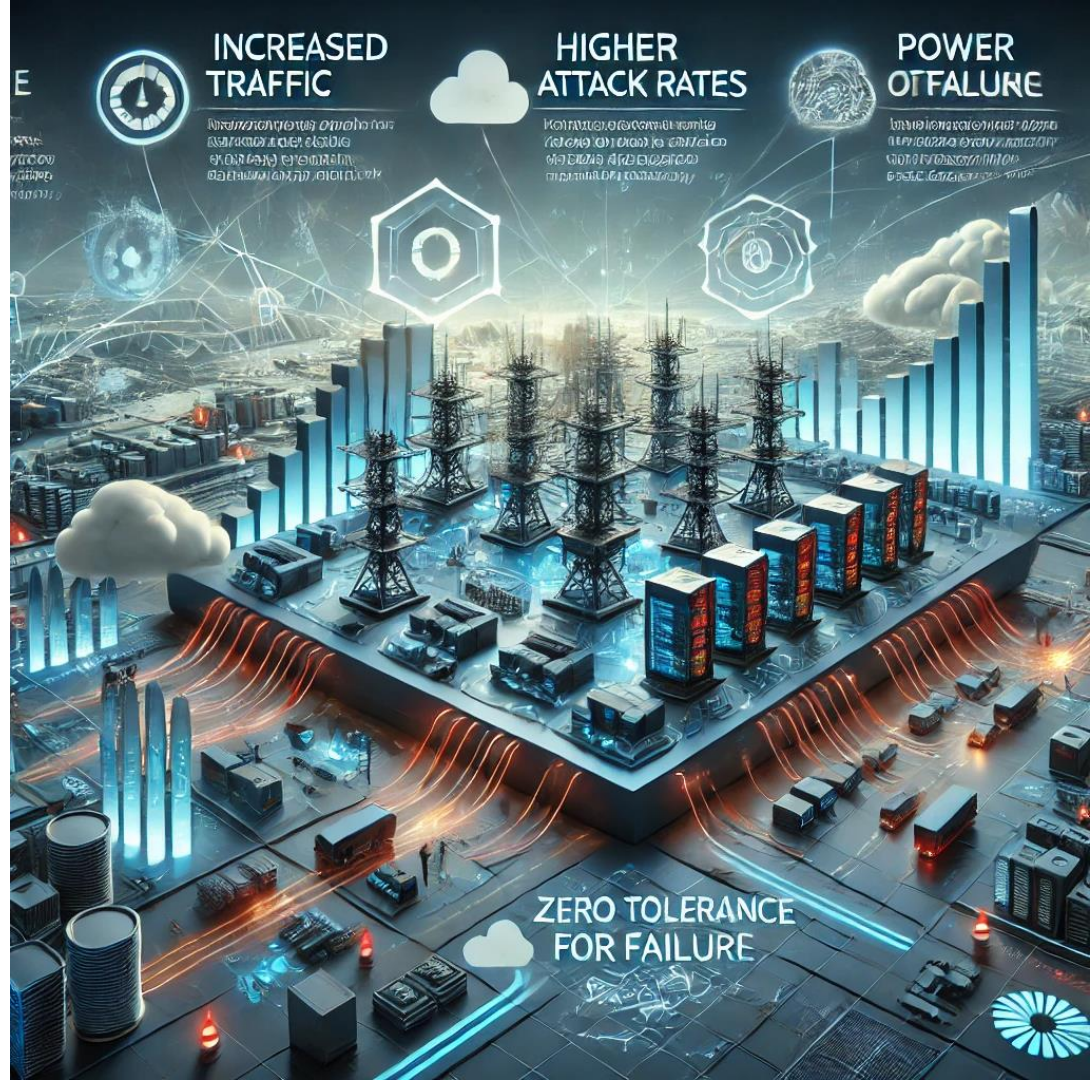
# Peering landscape

## Introduction

- More and more traffic
- More and more attacks
- Zero tolerance for failure
- Less power consumption per Gb

**Choosing the right peering router is key**

Disclaimer : Illustration pictures of this presentation have been generated with DALL-E 3

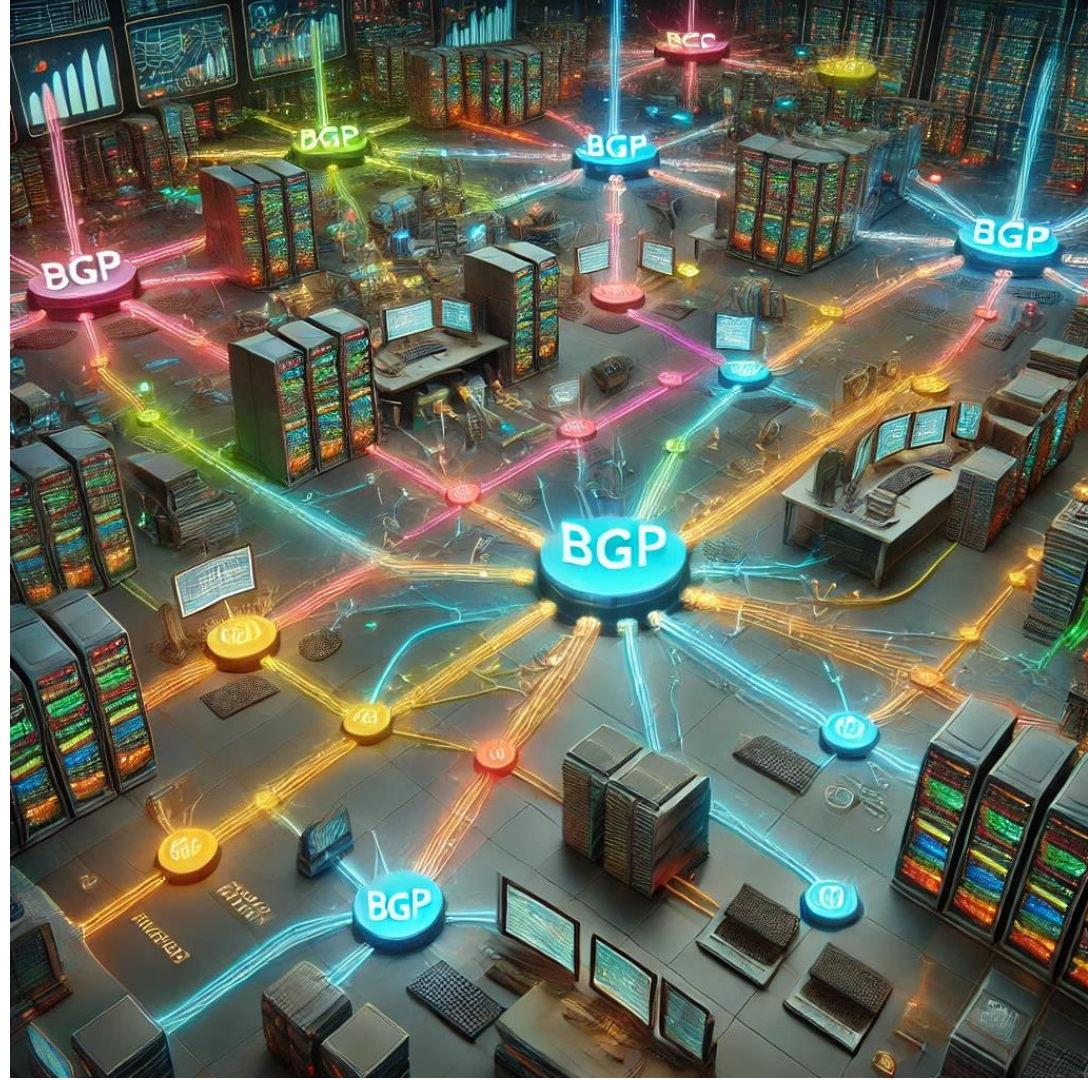


# BGP implementation

Robust and feature-rich

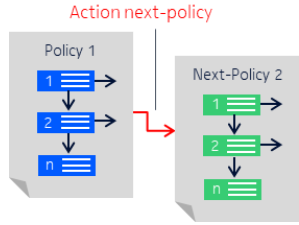
Best in class implementation includes :

- Scale
- Path visibility and reconvergence
- Robustness
- Error handling (RFC7606)
- Rib-out processing
- High availability
- Rapid BGP convergence leveraging multi-processing architecture

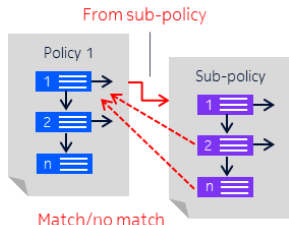


# Route policy framework

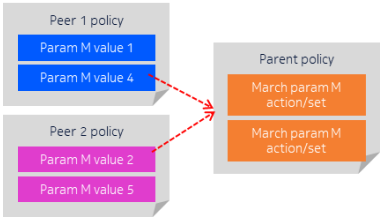
Flexible and scalable route policy language



Nested policies

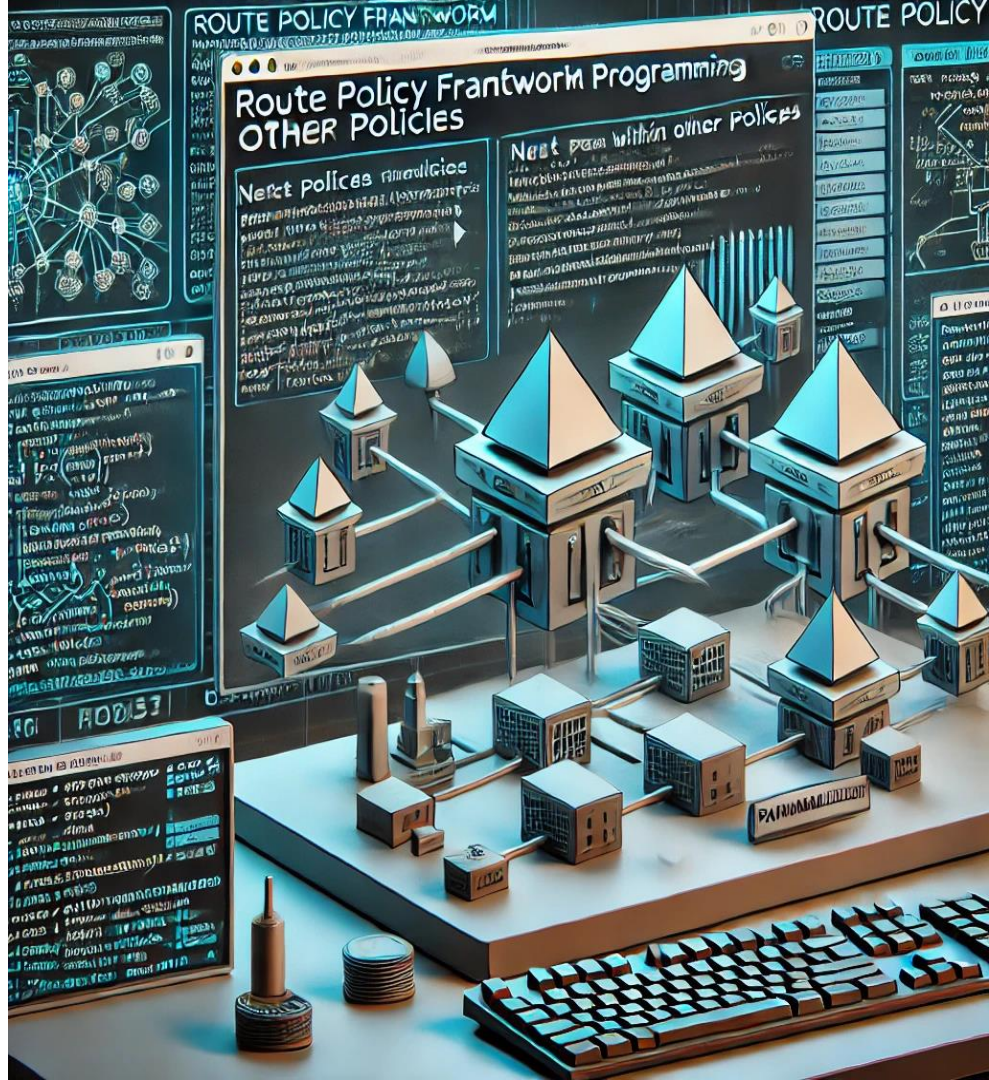


Scaling with sub-routines



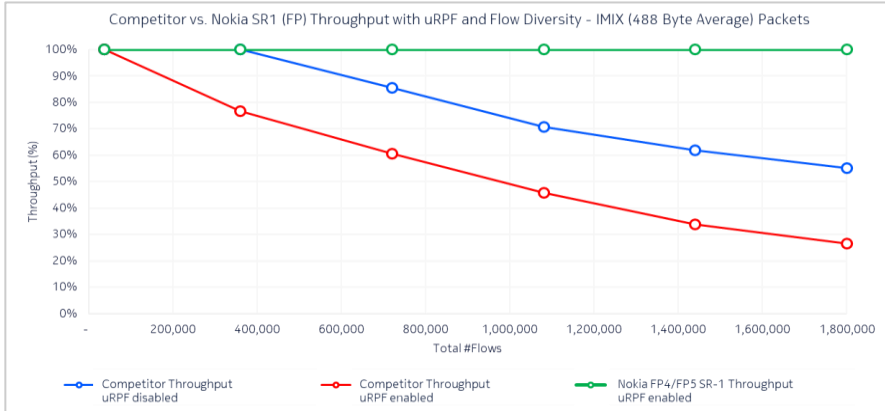
Simplification with parameterization

Possibility to allow for test evaluation of policy before applying



# Determinist performance

## Performant silicon and memory architecture



- High number of flows result in performance degradation due to cache miss
- Enabling uRPF (loose mode) results in a further ~25% decline in throughput for IMIX traffic
- Fully buffered architecture for determinist performance



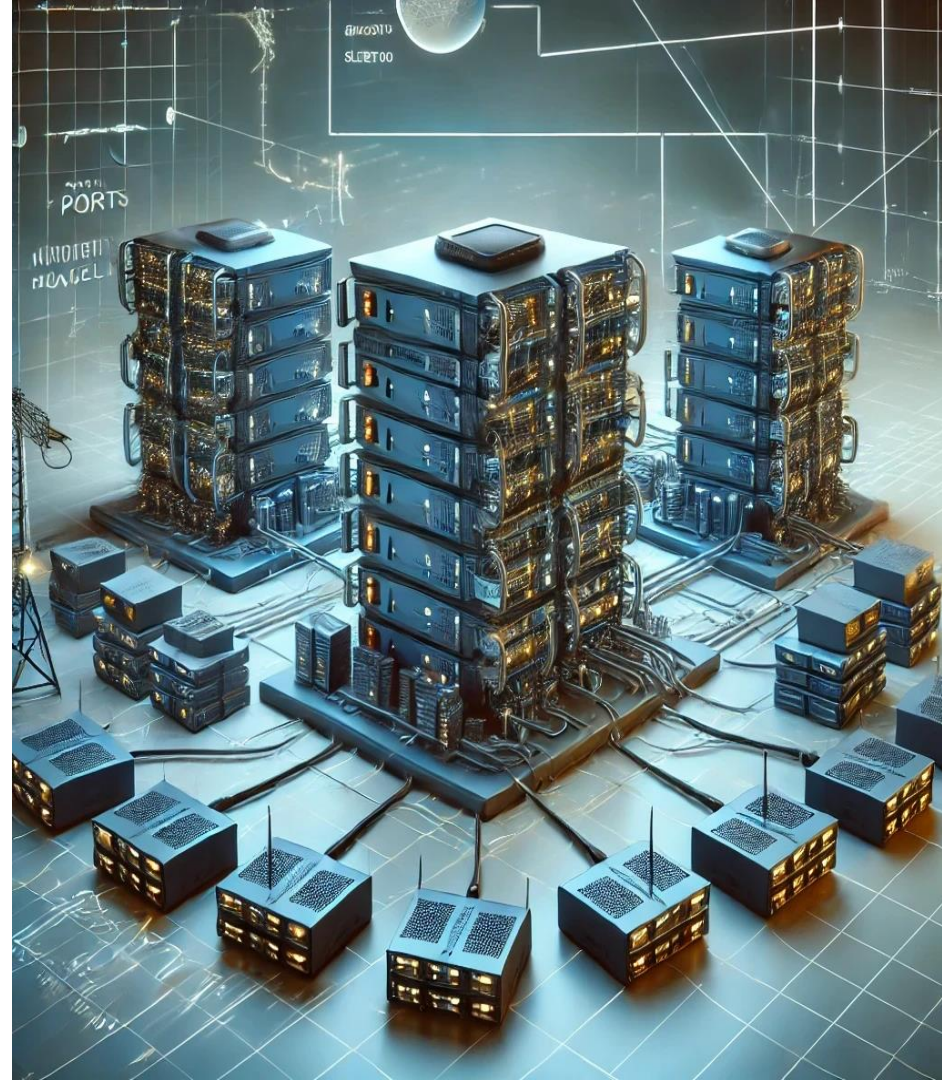
# High slot capacity with low speeds ports fanout

## Cost optimized architecture

Consider 800Gb/s ports for backbone links with breakout possibility allowing power optimization and investment protection

Consider using satellite for client links

- Cost effective solution
- Only host is configured
- Satellite is seen as port extender
- Can be local or remote



# Full security implementation

Robust and feature-rich

Best in class implementation includes :

- Secure Boot
- CPU protection with hardware queues
- Protocol encryption
- RPKI implementation
- RTBH, GTSM
- Flowspec
- Unparalleled ACL scale



# The DDoS problem is shifting

## New detection approach needed

2000 – 2020  
Spoofed

2020 – 2024  
Botnet

2024+  
AI

More volume / more automation

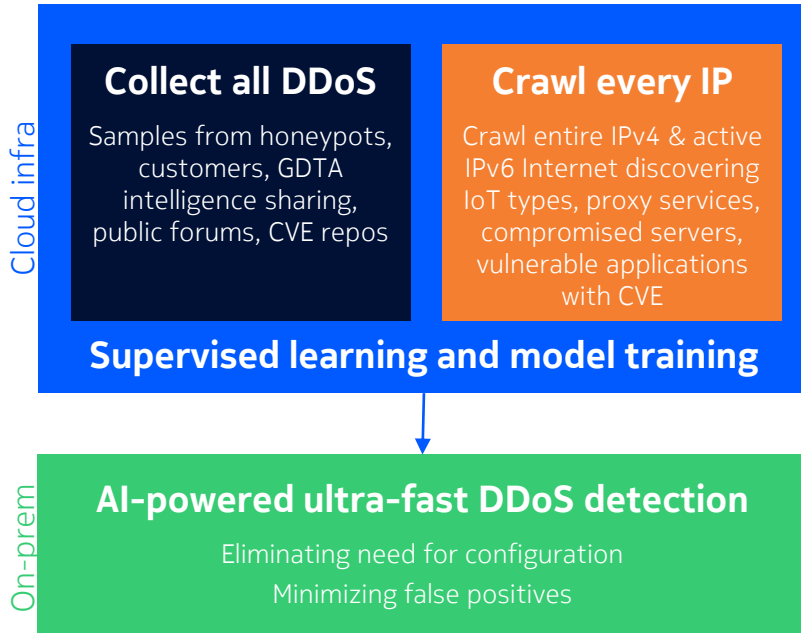
- Botnet and proxy-based attacks increasing
  - 1M active IoT bot devices, >10M residential proxies
  - >100 Tb/s aggregate capacity
- Cost of attacking is very low
- Increasing level of automation
  - Attack variability (bursts, carpet bombs, ...)
  - Realistic HTTP/DNS/VoIP requests





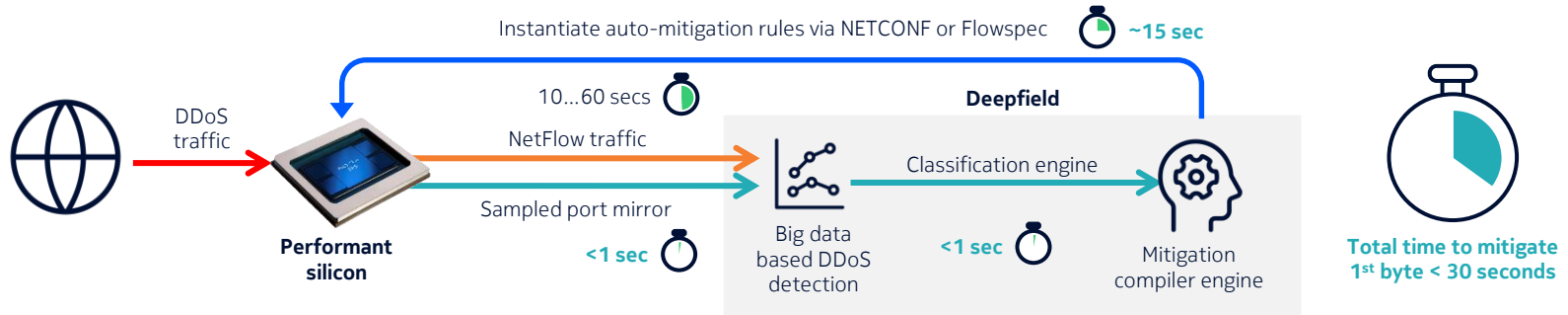
# Best in class DDoS detection engine

AI-powered detection without complex threshold configuration & maintenance



# Using silicon ACL power to protect against DDoS

Combined forces for cost-effective DDoS protection



## AI-powered intelligence

- Zero-touch big-data based DDoS detection
- Real-time compilation of optimal filter list

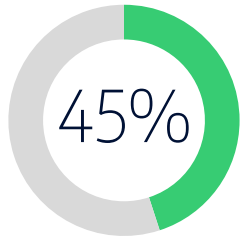


## Performant silicon

- Large-scale ACLs to block large/complex DDoS attacks
- Line-rate filtering with no performance impact
- Fast filter-population for fastest possible mitigation

# Network analytics for peering and CDN optimization

Reduce transit costs while improving customer experience



Internet Peering traffic sourced indirectly from paid transit\*



ISP traffic sourced from CDNs and internal caches\*

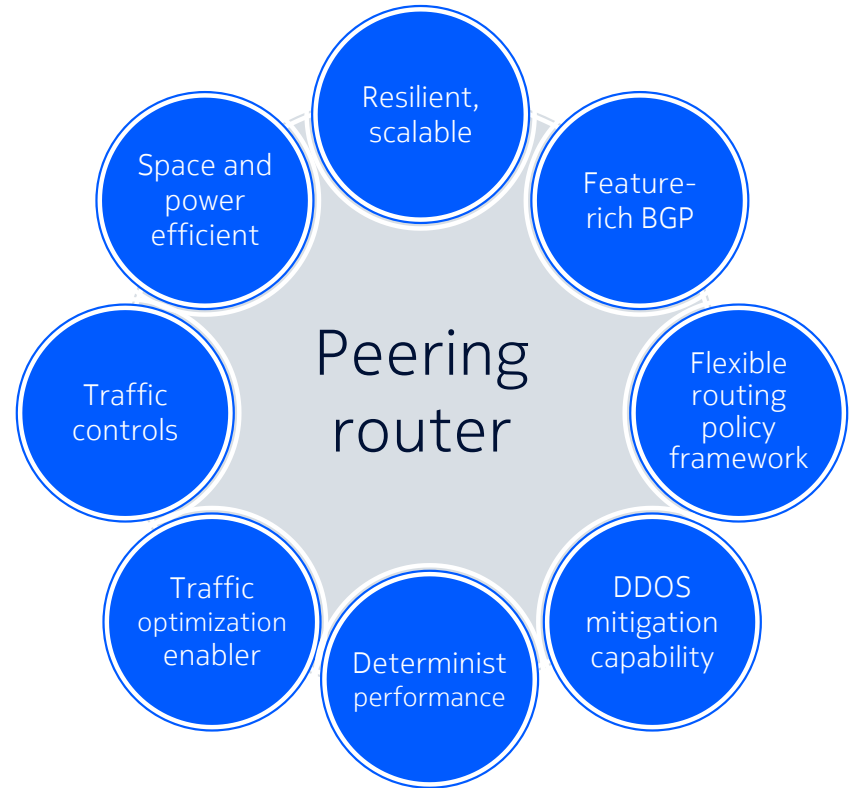
\*Data from several European ISPs



# Best in class peering router

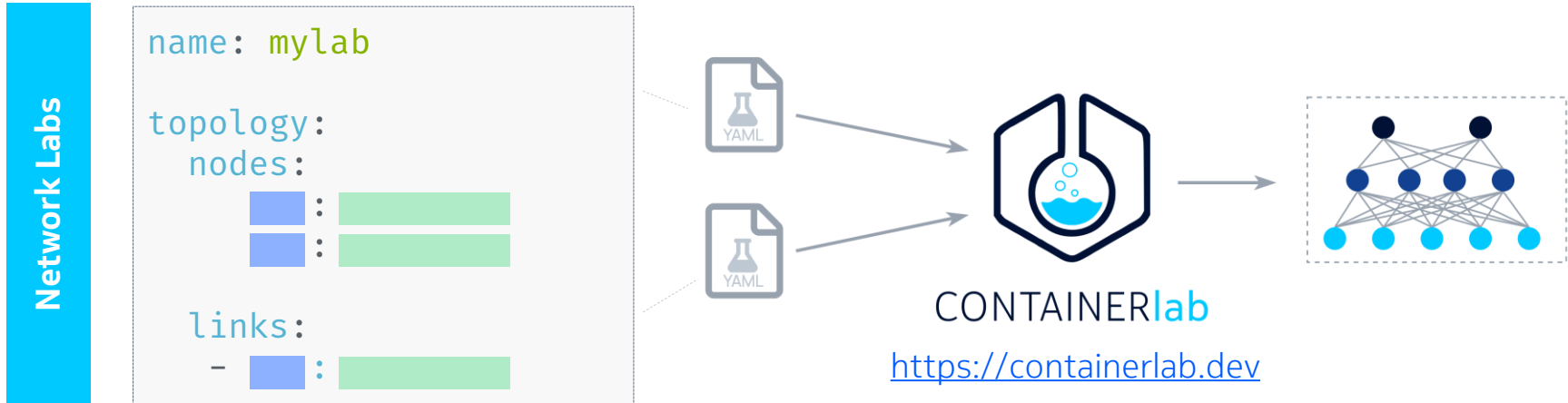
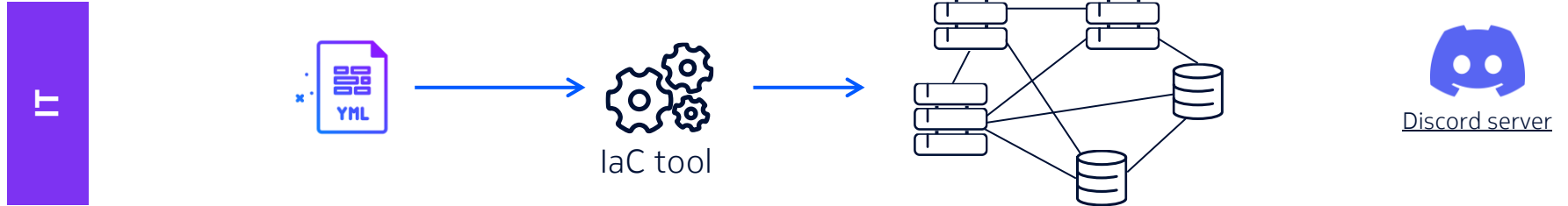
## Summary and takeaways

- Resilient, scalable, and feature-rich BGP process
- Flexible routing policy framework for frequent route policy updates
- Secure routing and DDoS mitigation on network entry
- Guaranteed performance for high number of flows and filters
- Traffic optimization enablers for moving prefixes across peering links
- Application traffic controls for peak load management
- Space and power efficient



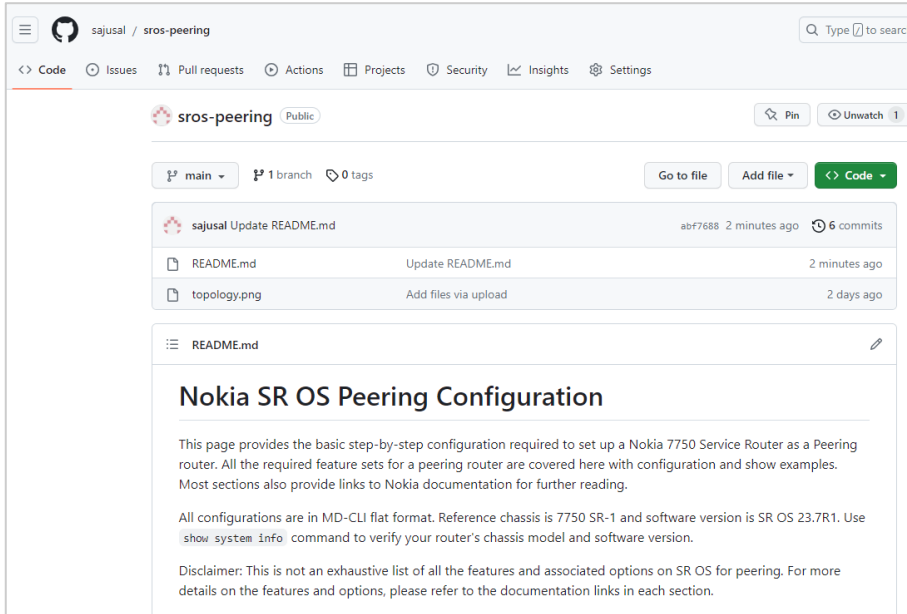
# Testing peering configuration with Containerlab

Bringing declarativeness to networking labs



# Peering reference configuration

<https://github.com/sajusal/sros-peering>



The screenshot shows the GitHub repository page for 'sajusal/sros-peering'. The repository is public and has a 'main' branch with 1 branch and 0 tags. The repository contains several files: README.md (updated 2 minutes ago), topology.png (uploaded 2 days ago), and another README.md file. The repository description is 'Nokia SR OS Peering Configuration'. The page provides a basic step-by-step configuration required to set up a Nokia 7750 Service Router as a Peering router. It mentions that all required feature sets for a peering router are covered here with configuration and show examples. Most sections also provide links to Nokia documentation for further reading. It notes that all configurations are in MD-CLI flat format, reference chassis is 7750 SR-1 and software version is SR OS 23.7R1. It also includes a disclaimer that this is not an exhaustive list of all the features and associated options on SR OS for peering, and for more details on the features and options, please refer to the documentation links in each section.

## Route Policies

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

For more details on route policy configuration and options, visit [SR OS Route Policies Documentation](#).

In these examples, we are creating AS path lists, community and prefix lists.

```
/configure policy-options as-path "PEERING" { expression "64503" }
/configure policy-options as-path-group "BOGON" { entry 10 expression ". * 0 .*" }
/configure policy-options as-path-group "BOGON" { entry 20 expression ". * [64496-64511] .*" }
/configure policy-options as-path-group "BOGON" { entry 30 expression ". * 65535 .*" }

/configure policy-options community "LARGE-PEER" { member "65100:100" }
/configure policy-options community "SMALL-PEERS" { member "65200:200" }
/configure policy-options community "SMALL-PEERS" { member "65400:.*" }
/configure policy-options community "SMALL-PEERS" { member "65500:.*" }
```

## RPKI

SR OS supports RPKI for BGP prefix origin validation.

In this example, we are configuring a RPKI session with an external server and then enabling prefix origin validation under the BGP group. We are also configuring BGP to not use any routes whose origin is invalid.

For more details on RPKI implementation, visit [SR OS RPKI Documentation](#).

```
/configure router "Base" origin-validation rpki-session 172.31.1.2 { admin-state enable }
/configure router "Base" origin-validation rpki-session 172.31.1.2 { local-address 10.10.1.4 }
/configure router "Base" origin-validation rpki-session 172.31.1.2 { port 8282 }
/configure router "Base" bgp group "eBGP-Peering" { origin-validation ipv4 true }
/configure router "Base" bgp group "eBGP-Peering" { origin-validation ipv6 true }
/configure router "Base" bgp best-path-selection { origin-invalid-unusable true }
```

NOKIA

# Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use by Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular

purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.