Aalto University
School of Electrical
Engineering

Evolved NAT and TCP SYNProxy

#Evonat

Jesús Llorente Santos <jesus.llorente.santos@aalto.fi>
Juha-Matti Tilli <juha-matti.tilli@aalto.fi>
15-03-2018

Evolved NAT / Realm Gateway

- **Redefine the concept of NAT and carrier-grade gateway**
- **Novel dynamic NAT traversal based on standard DNS queries**
  - *Allows multiple same-service instances running in the private network*
- **Local reputation system for DNS and data sources**
  - *Fair resource allocation*
- **Security features**
  - *Stateful firewall and third party integration*
  - *Assured communications for DNS and TCP flows*
  - *Strict definition of data services*
- **Linux kernel packet forwarding**
- **Interoperable with TCP SYNProxy for optimal data rates**

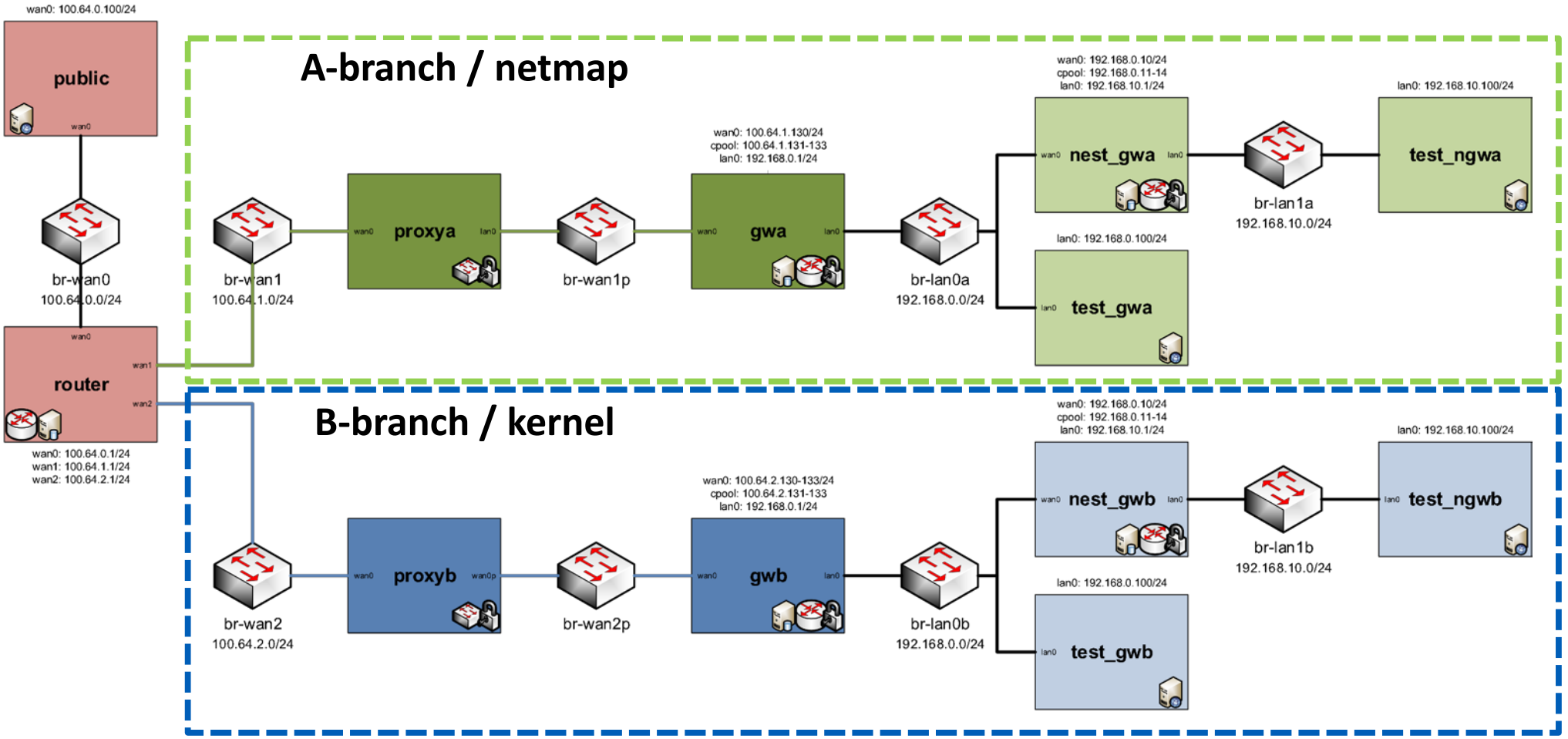
TCP SYNProxy via Linux kernel

- **Built-in kernel protection against TCP SYN flood attacks**
- **High data rates and low CPU consumption**
- **Custom deployment as an in-line layer-2 element**
  - *Suitable for virtualized environments*
  - *Benefits from checksum and segmentation offloading*
- **Drawbacks**
  - *Rudimentary mitigation of reflection attacks!!*
  - *Inherent flaws due to intended use as end-host mechanism (connection reuse and client stalling)*

TCP SYNProxy via netmap

- **Extremely high data rates and low CPU count requirement**
  - *Most suitable for physical NICs (40 Gbps link saturation with 3 cores)*
  - *Benefits from multiple queues*
- **Originally designed as an in-line layer-2 element**
  - *Solves connection reuse and client stalling*
- **Improved security and robustness**
  - *Revolving secrets and secure hash functions*
  - *Improved mitigation of reflection attacks*
- **Drawbacks**
  - *Poor performance with virtualized NICs!!*

Demo architecture



Demo contents

- **Realm Gateway**
  - *Carrier-grade NAT traversal with public IP address reuse*
  - *Enhanced security due to stricter service definition - SFQDN*
  - *Policy Based Resource Allocation algorithm and reputation system*
  - *Suricata integration and suspicious flow removal*

- **TCP SYNProxy(ies)**
  - *Interworking with Realm Gateway for throughput optimization*
  - *Performance evaluation*
  - *Advances in mitigation of reflection attacks*