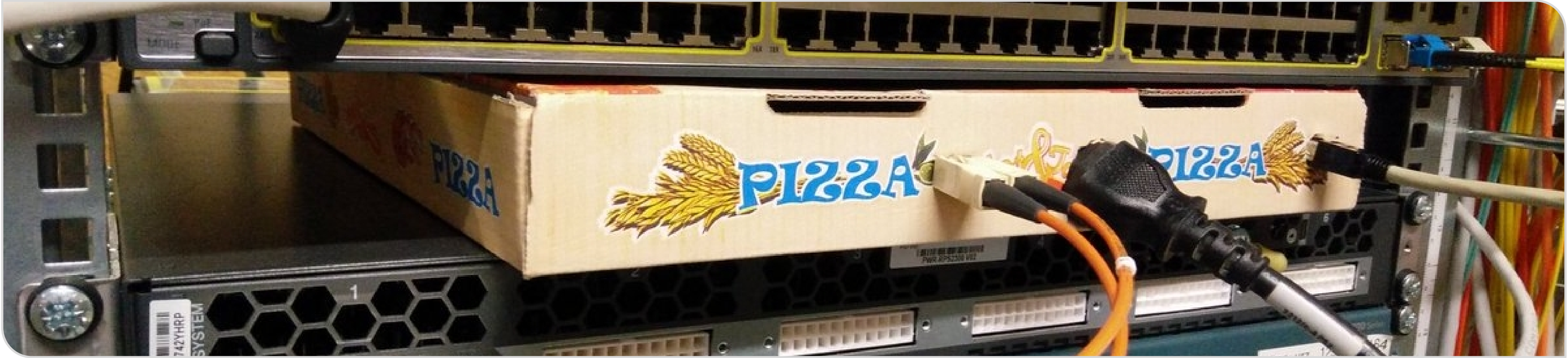
Karlsruhe Institute of Technology

Steinbuch Centre for Computing

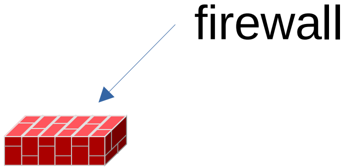
Providing firewalled network segments within an EVPN fabric using a routed approach

Benedikt Neuffer



Firewalls - definition

- Middle box working on IP layer and transport layer
- Stateful packet inspection
- No DPI
- No SSL inspection



Why Firewalls? - campus network

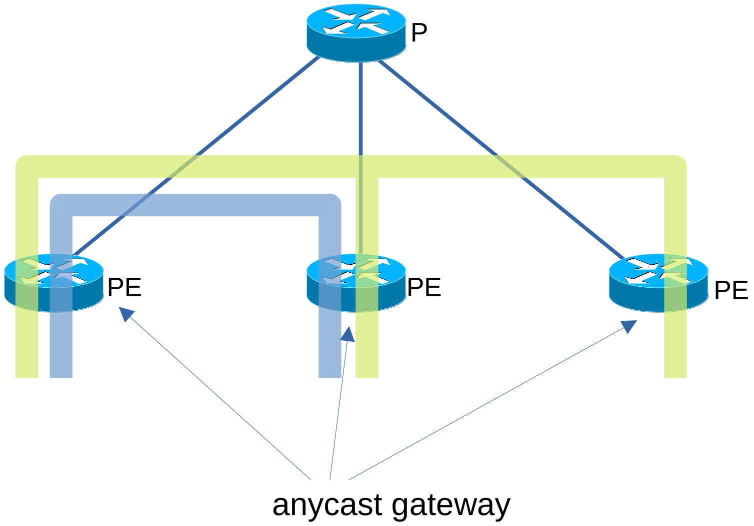
- Campus / enterprise network: basic security with stateful firewalls
  - Offices
  - BYOD
  - IoT, building automation, VoIP
  - Labs

Why Firewalls? - datacenter

- Datacenter: basic security with stateful firewalls
  - IoT, sensors, PDU, UPS
  - IPMI
  - Appliances
  - User / customer requests
  - Certification / requirements

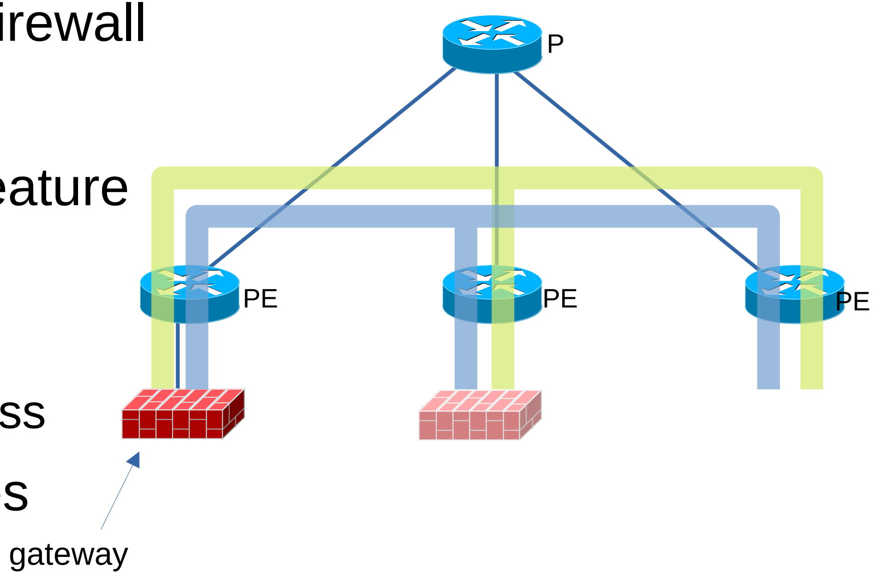
EVPN - basics

- Standardized BGP based “toolkit” for network virtualization
- L2VPN and L3VPN combined
- Uses e.g. MPLS or VXLAN for tunnels
- Anycast gateway



Classic firewall integration

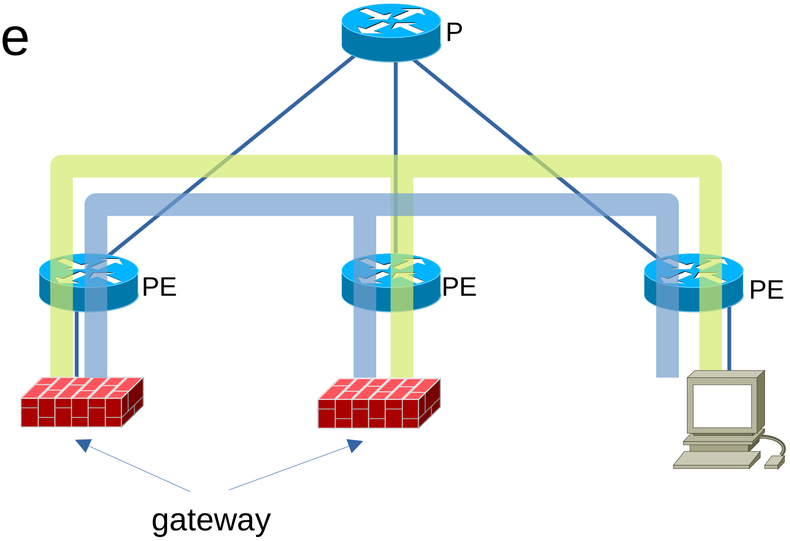
- L2 stretching to firewall, active/standby
- Gateway behaves inconsistent between anycast gateway and gateway on firewall
  - NDP / ARP
- Gateway on firewall has different feature set
  - Suppor for DHCPv6 PD
  - RA options, RA from link-local address
- Failover leads to a lot of mac moves



Classic firewall integration with active/active

- New firewalls should be active/active
- VRRP for L3 redundancy
- Both Firewalls send RA
  - But if one firewall fails, clients may use stale default route
- Still L2 stretching
- Still inconsistent gateway behavior for firewalled and non-firewalled network segments

=> Solution is unsatisfactory

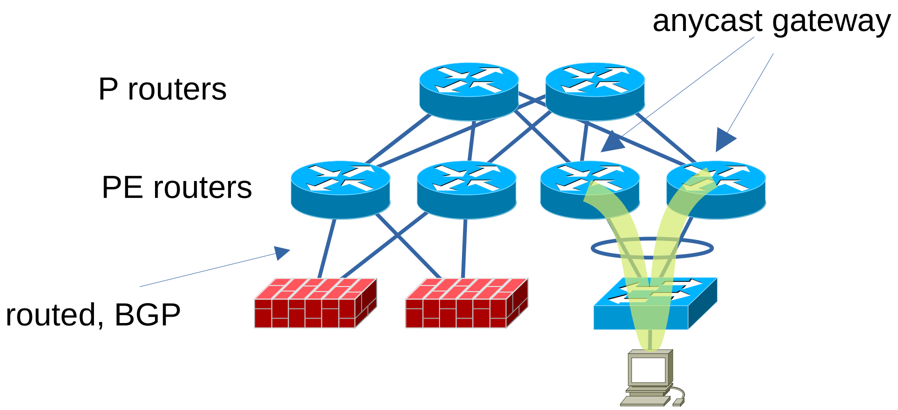


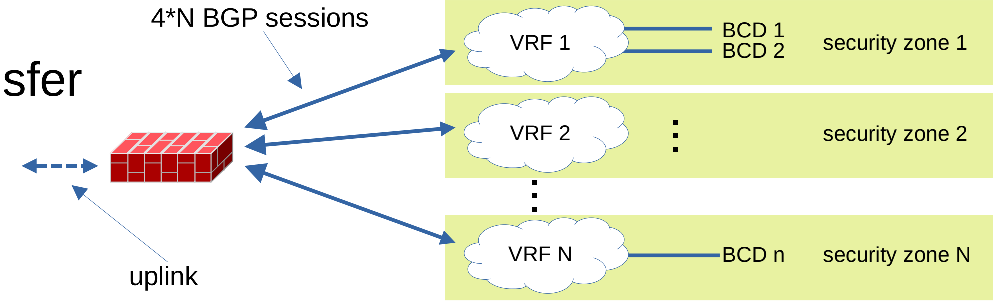
```
route learned via RA:
default via
    fe80:5a:49:3bff:febc:3c10
    fe80:5a:49:3bff:feba:c410
```

First routed-only approach

- One VRF per security zone (N)
- Multiple network segments per security zone possible
- Consistent gateway behavior!
- BGP connections per security zone
  - A lot of sub-interfaces and transfer networks needed (4*N)
  - A lot of BGP sessions (4*N)

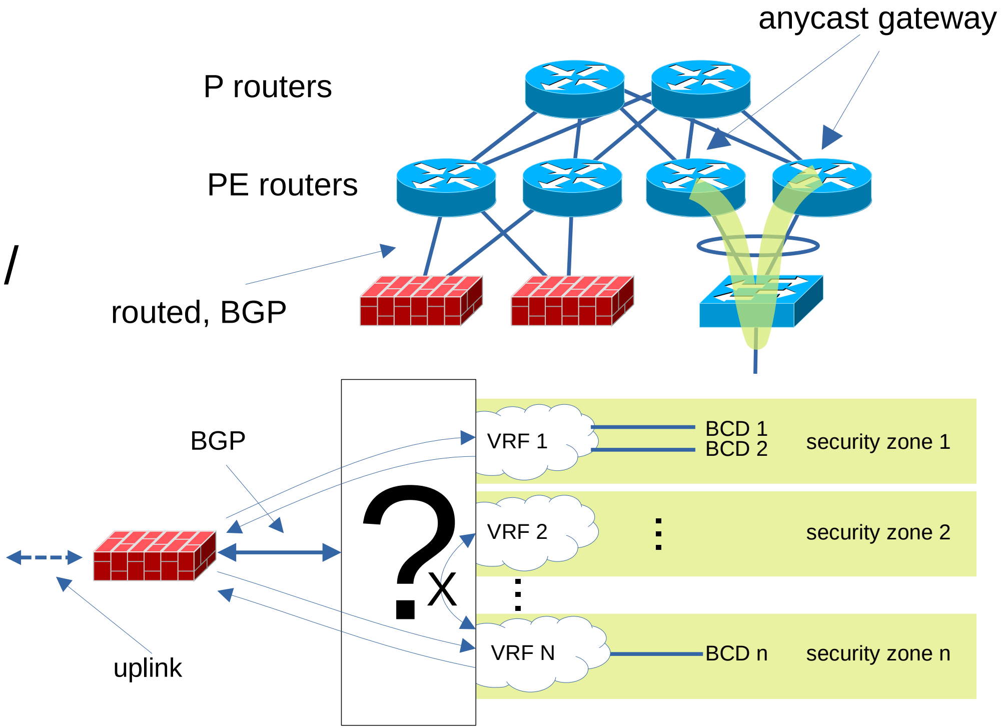
=> Solution does not scale





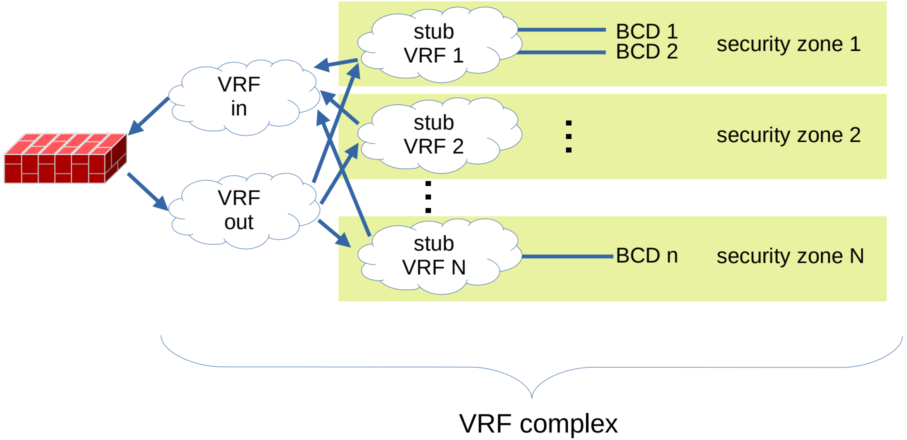
Optimal routed-only approach

- Statically configured interconnection between firewalls and EVPN fabric
- Traffic leaving a security zone / vrf is routed to the firewall
- Traffic between security zones / vrfs is routed through the firewall

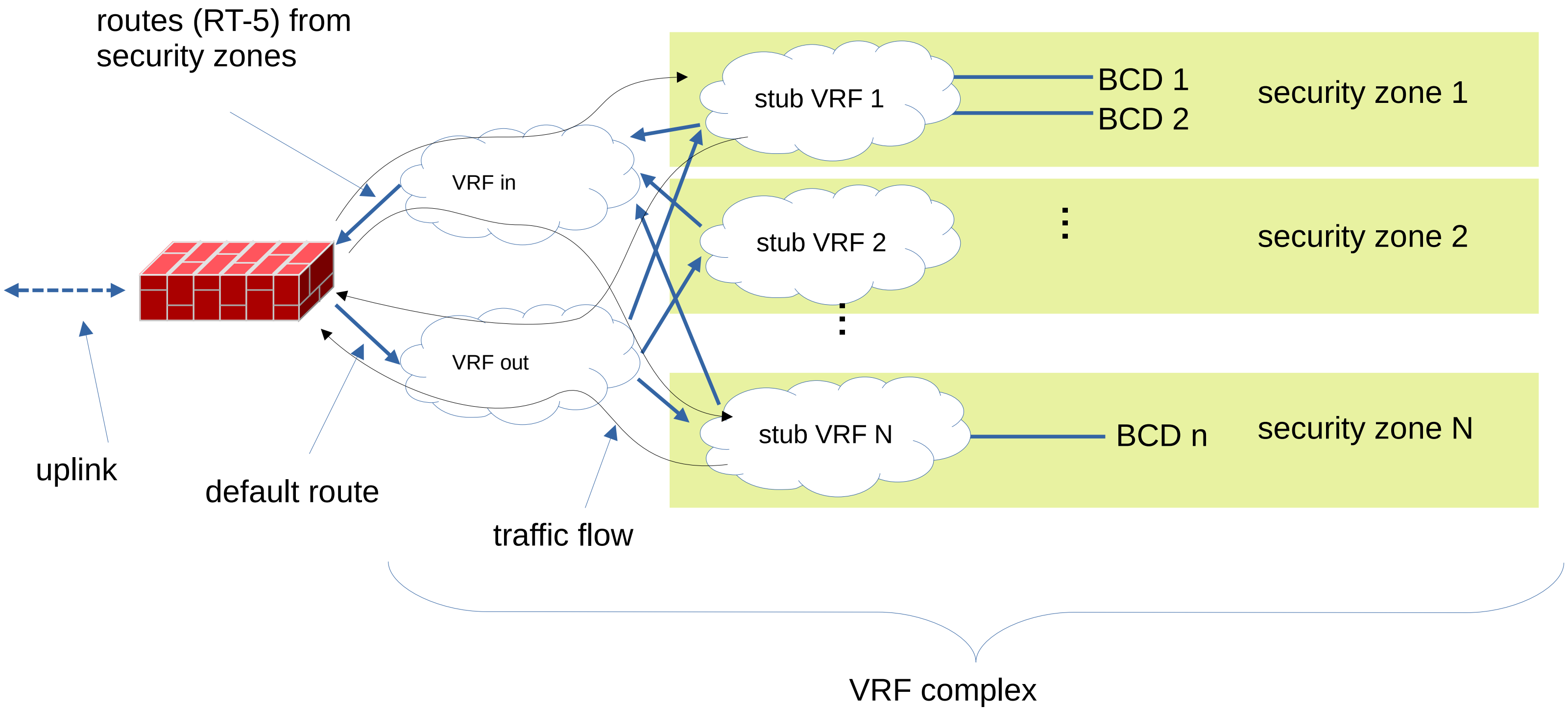


Routed-only approach with route leaks

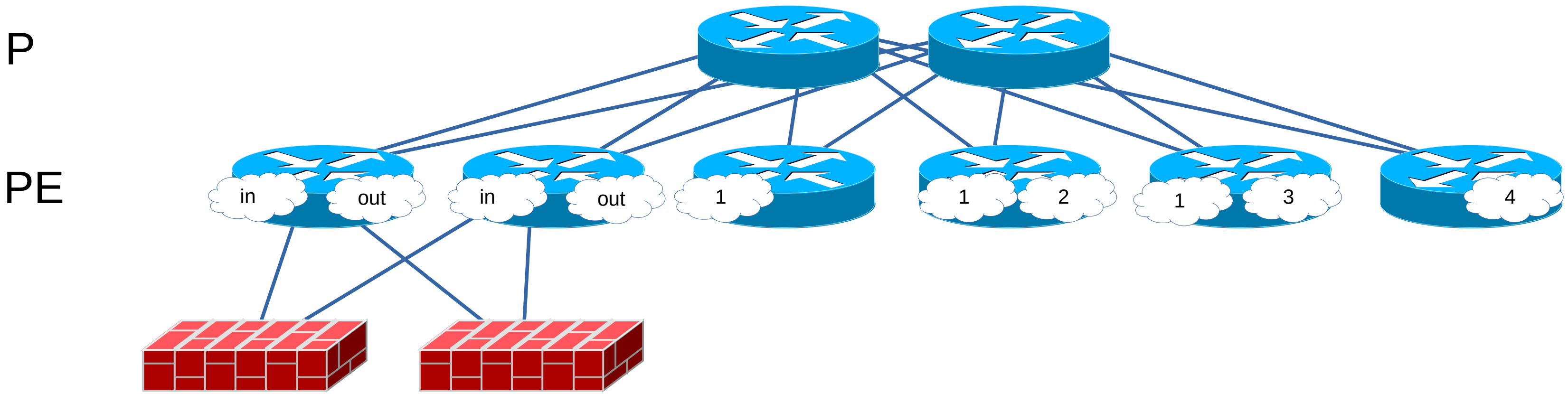
- One stub VRF per security zone
- Two additional VRFs
  - VRF in: imports all routes from stub VRFs and announces rt-5 to firewall
  - VRF out: learns default route from firewall and exports default route to stub VRFs
- VRF complex = set of stub vrfs + in VRF + out VRF



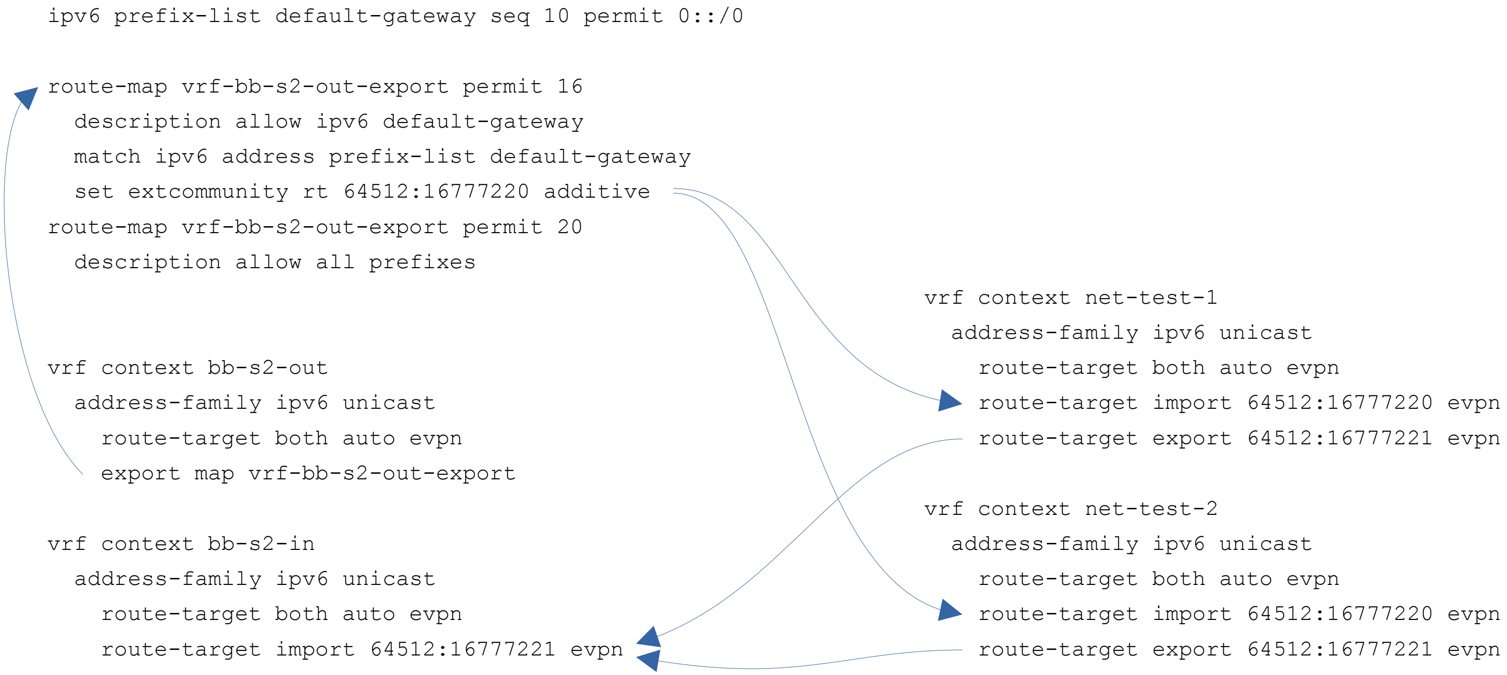
Routed-only approach with route leaks (detail)



VRFs in EVPN topology



Example cisco style configuration



```
ipv6 prefix-list default-gateway seq 10 permit 0::/0

route-map vrf-bb-s2-out-export permit 16
  description allow ipv6 default-gateway
  match ipv6 address prefix-list default-gateway
  set extcommunity rt 64512:16777220 additive
route-map vrf-bb-s2-out-export permit 20
  description allow all prefixes


vrf context bb-s2-out
  address-family ipv6 unicast
    route-target both auto evpn
    export map vrf-bb-s2-out-export

vrf context bb-s2-in
  address-family ipv6 unicast
    route-target both auto evpn
    route-target import 64512:16777221 evpn
```

```
vrf context net-test-1
  address-family ipv6 unicast
    route-target both auto evpn
    route-target import 64512:16777220 evpn
    route-target export 64512:16777221 evpn

vrf context net-test-2
  address-family ipv6 unicast
    route-target both auto evpn
    route-target import 64512:16777220 evpn
    route-target export 64512:16777221 evpn
```

Day to day firewall operations

- Firewall behaves like perimeter firewall
  - Interface based rules not applicable for security zones
  - Source / destination has to be used for rule matching
  - Security zone consists of one or more prefixes
  - Source / destination “any” considered harmful
- Good Documentation required
- Automation recommended

Conclusion

- Separation of concerns
  - Firewall: policy enforcement only
  - Router: gateway with modern and consistent feature set
- Operational advantage: gateway is always in EVPN fabric
- Scaling depends on VRF scaling of EVPN fabric
- Firewall can be replaced easily
- No L2 stretching needed

Q&A

?&!

Benedikt Neuffer

mail: benedikt.neuffer@kit.edu

matrix: @iv4011:kit.edu