BGP Flowspec

4. atnog Stammtisch

Christoph Loibl (next layer)
Martin Bacher (T-Mobile)

DAS VERBINDET UNS.

Attacks

- Volumetric
  - high bandwidth
  - UDP amplification/reflection (NTP, SSDP, DNS, …)
  - TCP amplification/reflection (i.e. multiple RST or SYN/ACK)
- Protocol Attacks
  - Medium to low bandwidth
  - Syn Flood, Fragmentation, ICMP
- Application Level Attacks
  - Low bandwidth
  - Hard to detect/migigate

Countermeasures

- Platform hardening (avoid insecure implementations)
- NIF/NEF
  - RPF
  - Border ACLs
- Blackhole
  - D-RTBH
  - S-RTBH
- Scrubbing Center
- Cloud based solution
- BGP FlowSpec
- Netconf/Yang
- SDN

BGP Flowspec

- Intra-Domain
  - Injection from routing daemon
  - Validation turned off
- Inter-Domain
  - Upstreams
  - Customer
  - IXP
  - PNI

BGP Flowspec Inter-Domain

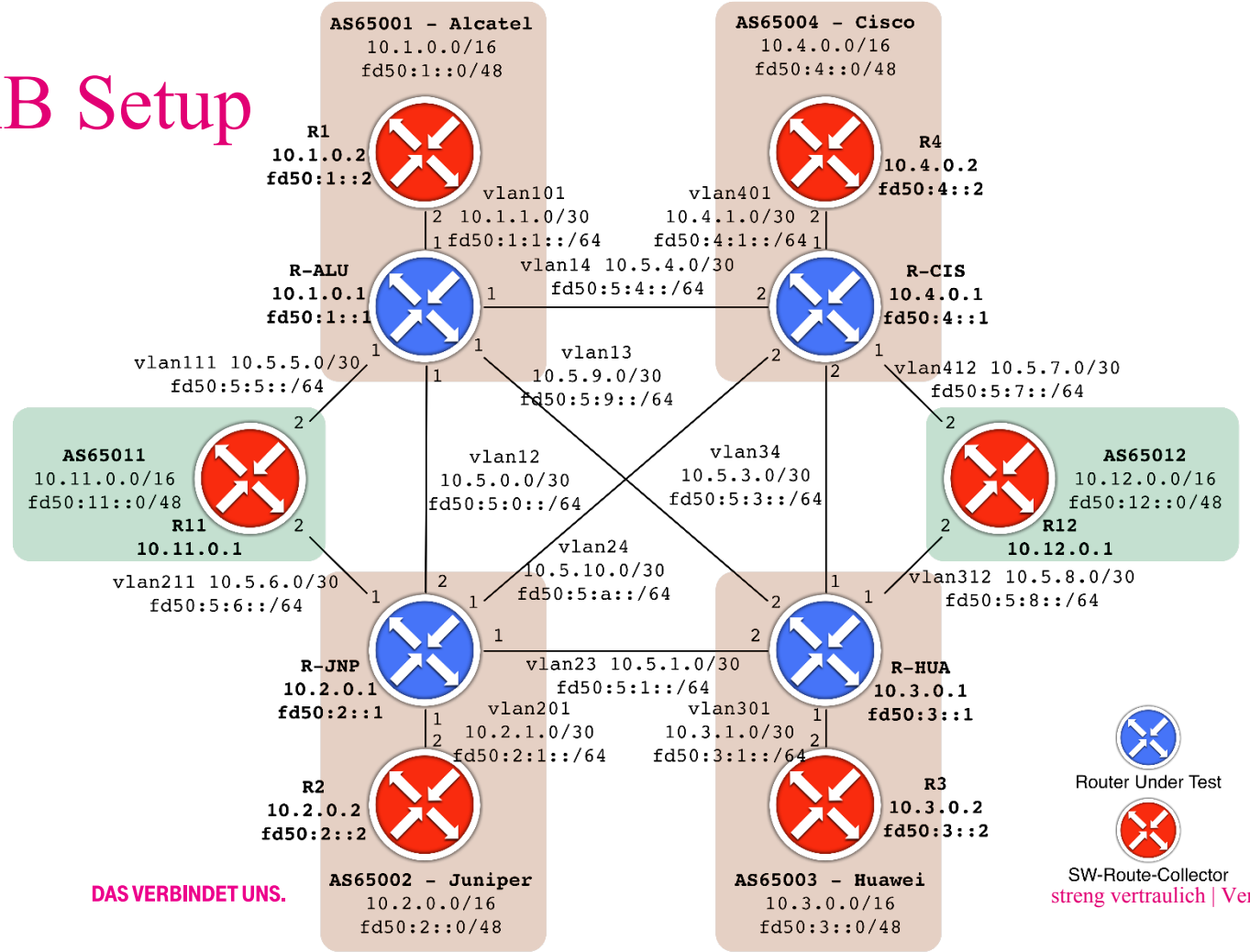
- Missing Interop
- Scalability 3k – 150K
- May not work (duplicate announcements)
- Filtering options unclear
- Possibly abuseable

Interop LAB

- ALU
- Cisco
- Huawei
- Juniper

- next layer
- T-mobile

LAB Setup


AS65001 - Alcatel
10.1.0.0/16
fd50:1::0/48
AS65004 - Cisco
10.4.0.0/16
fd50:4::0/48
R1
10.1.0.2
fd50:1::2
R4
10.4.0.2
fd50:4::2
vlan101
10.1.1.0/30
fd50:1:1::/64
vlan401
10.4.1.0/30
fd50:4:1::/64
vlan14 10.5.4.0/30
fd50:5:4::/64
R-ALU
10.1.0.1
fd50:1::1
R-CIS
10.4.0.1
fd50:4::1
vlan111 10.5.5.0/30
fd50:5:5::/64
vlan13
10.5.9.0/30
fd50:5:9::/64
vlan412 10.5.7.0/30
fd50:5:7::/64
AS65011
10.11.0.0/16
fd50:11::0/48
R11
10.11.0.1
vlan12
10.5.0.0/30
fd50:5:0::/64
vlan34
10.5.3.0/30
fd50:5:3::/64
AS65012
10.12.0.0/16
fd50:12::0/48
R12
10.12.0.1
vlan211 10.5.6.0/30
fd50:5:6::/64
vlan24
10.5.10.0/30
fd50:5:a::/64
vlan312 10.5.8.0/30
fd50:5:8::/64
R-JNP
10.2.0.1
fd50:2::1
vlan23 10.5.1.0/30
fd50:5:1::/64
R-HUA
10.3.0.1
fd50:3::1
vlan201
10.2.1.0/30
fd50:2:1::/64
vlan301
10.3.1.0/30
fd50:3:1::/64
R2
10.2.0.2
fd50:2::2
R3
10.3.0.2
fd50:3::2
AS65002 - Juniper
10.2.0.0/16
fd50:2::0/48
AS65003 - Huawei
10.3.0.0/16
fd50:3::0/48
Router Under Test
SW-Route-Collector

Many problems

- VRF support (Internet in a VRF application)
- Parsing problems
- Display problems (large filters)
- Notifications (various reasons)
- Encoding (large filters)
- Ignoring Flowspec routes at BGP level
- Validation timing issues
- Transitivity of Flowspec Extended communities