Protecting your peering edge.

Graham Beneke
AfPIF 2015
#include std-disclaimer
Expect to receive traffic not destined to your network.

You will need to protect your network!
FIB: NET_GREEN
NET_BLUE
NET_RED

FIB: NET_GREEN
NET_RED
route-map filter-to-my-peering-router
match criteria only_my_customers
permit only_my_customers
Whom are you protecting against?
1 2 3
• BGP advertisement classification

• QoS Policy Propagation via BGP (QPPB).
Step 1: Tag peer prefixes uniquely within BGP and FIB tables

- peer prefixes set with community attribute (P) and tag (P)

- customer prefixes are set with community attribute (C) and tag (C)

```text
route-policy qosgroup_map
if community matches-any (C1) then
  set qos-group 7
elseif community matches-any (C2) then
  set qos-group 2
else
  set qos-group 1
endif
end-policy
router bgp <your ASN>
  address-family ipv4 unicast
  table-policy qosgroup_map
```
Step 2: Tag external packets at peering locations based upon longest prefix match within FIB:

- tag (P) for packets received from peer and **destined** to a prefix in the FIB with tag (P),
- tag (C) for packets received from peer and **destined** to a prefix in the FIB with tag (C).

```
int Gig 0/0
ipv4 bgp policy propagation input qos-group destination
```
ISP forwards or discards packets that ingress peering interconnects based upon associated packet tag value:

- Packets with tag (P) are discarded
- Packets with tag (C) are forwarded

Step 3 (Packet classification via MQC):

```plaintext
int Gig 0/0
ipv4 bgp policy propagation input qos-group destination
  service-policy input qppb_set_dscp
```
handouts available for IOS, IOS-XR and JunOS
• Hardware forwarding platform.

• Classification is a key requirement.