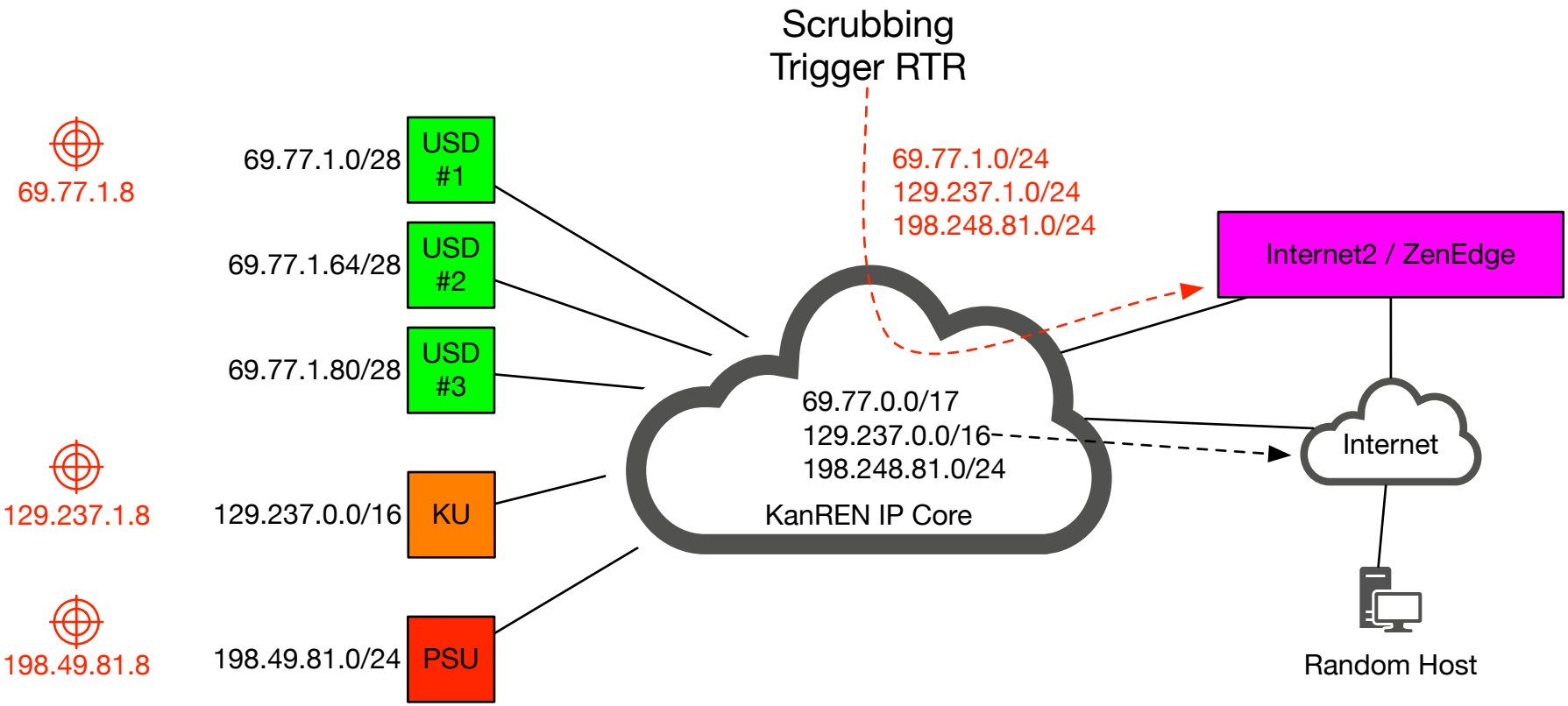
DDoS Scrubbing Routing Problems

Problem Statements

Author: Brad Fleming
Date: 2017-07-26
Email: bdfleming@kanren.net
Phone: 785-856-9805



Green hosts are no problem. We have a more specific OSPF route internally which can be used for delivery of clean traffic. Only caveat is that when we generate the 69.77.1.0/24 scrub route it impacts 3 sites (in this example), not just one.

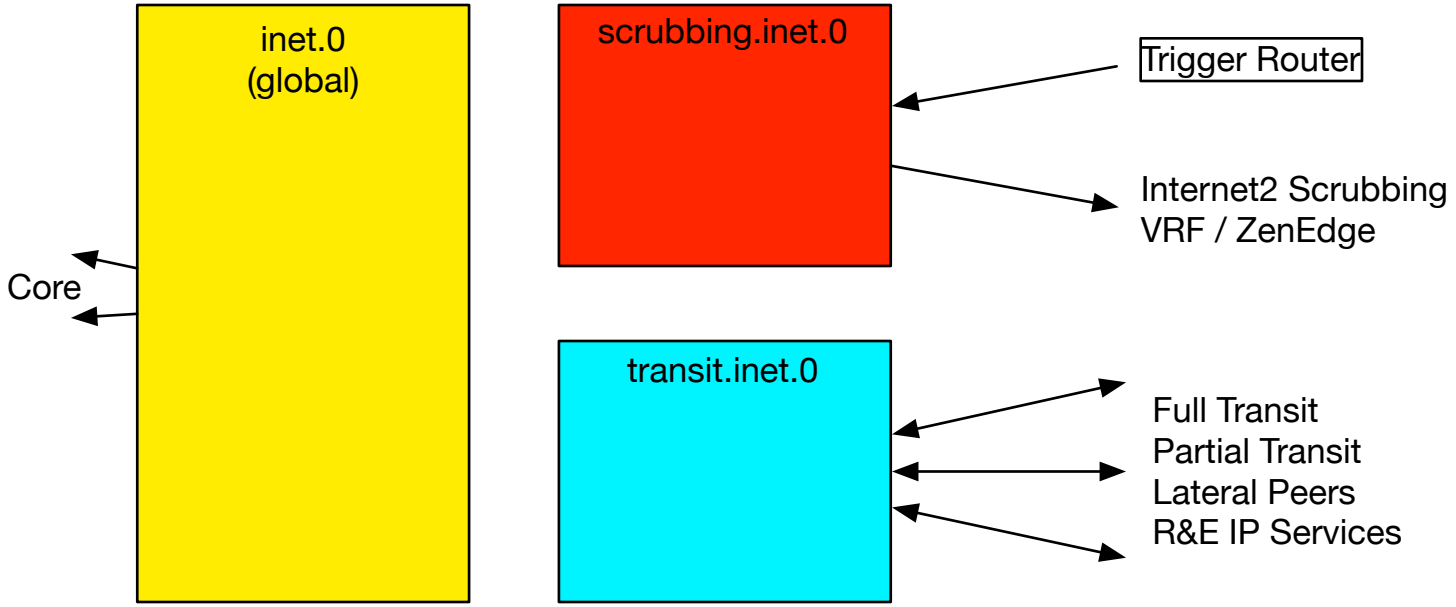
Orange networks are a problem. If site signals the scrub route, no problem.. we forward to the campus like any other route. But we have to assume most of our BGP speaking members are not that sophisticated and KanREN will have to generate the scrub route on their behalf. Problem is next-hop.. can't send traffic to the Scrubbing Trigger RTR; and many (most?) of these sites are dual-homed so we can't predict the current next-hop. This is especially true during DDoS events where squishy things at the border of their networks fall over and the network goes into a fault mode. This same basic problem exists for any site with a >/24 subnet inside our OSPF area as well; e.g.: if we've assigned a /23 to a USD we can't generate a more specific /24 to scrub one of their hosts without causing delivery problems.

Red networks have ALL THE SAME problems from the orange PLUS the added problem that we must withdraw their /24 advertisement from transit paths. If we don't withdraw the route from transits we run the risk of networks still sending us traffic via full transit links because the AS Path will be shorter than the I2/Zenedge path.

DDoS Scrubbing Routing Problems

Solution - RIB Outline

Author: Brad Fleming
Date: 2017-07-26
Email: bdfleming@kanren.net
Phone: 785-856-9805



Source RIB

Destination RIB

	inet.0	scrubbing.inet.0	transit.inet.0
inet.0		Import BGP routes with community 2495:400 (members) and perform origination	Import BGP routes with community 2495:400 (members) and perform origination
scrubbing.inet.0	Static default route		Import BGP routes with community <scrubbing-active>, elevate local-pref to 999, NH to inet.0
transit.inet.0	All BGP routes except <scrubbing-active> and <scrubbing-cooldown>	no route exchange needed	