CONTROL PLANE PROTECTION

Melchior Aelmans Juniper Networks



Engineering Simplicity

ANATOMY OF A ROUTER



A router consists, functionally, of two planes:

1- <u>The Control Plane</u>: The function of the control plane is to discover the network's topology and compute loop-free, optimal routes. It is where routing protocols, such as OSPF, ISIS and BGP, and signaling protocols, such as RSVP and LDP, run and where the routing tables (also called Routing Information Bases or RIBs), including multicast reverse path checking tables and VRF tables, are instantiated and populated. It is where the kernel reins and daemons live. The control plane also provides an interface for configuring and monitoring the router.

The control plane, usually implemented on a Routing Engine (RE), among other names, is based on an operating system, called a Network Operating System (NOS), such as Junos, running on a general propose processor because the computational and memory resources it requires are of such a complexity that only a software implementation is feasible. The control plane is the router's brain and its computational element.

2- <u>The Forwarding Plane</u>: The function of the forwarding plane is to transfer packets from an ingress interface (port) to an egress interface (port) so as to move each packet a hop closer to its ultimate destination. By traversing a chain of forwarding plane instances, each contained within a router, a packet completes its voyage from source to destination. Unlike the control plane, which only looks at control (such as OSPF Link State Updates and RSVP-TE PATH and RESV messages) and management packets (such as SNMP messages), each and every packet arriving at the router is processed by the forwarding plane. The forwarding plane is a router's muscles and its communication element.

Source: https://forums.juniper.net/t5/Routing/An-Informal-Guide-to-the-Engines-of-Packet-Forwarding/ta-p/401192

© 2020 Juniper Networks



WHY CONTROL PLANE PROTECTION (COPP)?

- Prevent control plane overload with invalid data. For example:
 - DoS/DDoS
 - TCP injection/replay attacks in protocol updates
 - Forming of invalid protocol adjacencies (BGP/OSPF/etc)
- Only allow authorized sources to be able to login ex. prevent brute force.
- Rate limit valid traffic ex. icmp pings.



Summary:

"CoPP is used to only allow legitimate traffic to reach Control Plane."



WHAT MECHANISMS ARE AVAILABLE? 1/2

- Embedded Control Plane DDoS Protection based on two main components
 - The classification of host-bound control plane traffic
 - A hierarchical set of individual- and aggregate-level policers
 - Hierarchically applied at PFE, FPC (linecard), Routing Engine
- "Good old" firewall filters to regulate traffic to Routing Engine
 - Allow only configured BGP neighbours. "Easy button" available: prefix-list bgp-neighbors { apply-path "protocols bgp group <*> neighbor <*>"; #apply-path works with lots of protocols }
 - Allow TCP 22 (SSH) from management network only
 - Allow VRRP single well-known multicast address prefix-list vrrp { 224.0.0.18/32;



WHAT MECHANISMS ARE AVAILABLE? 2/2

• Manually configured policers

```
- Limit Management traffic to 1 Mbps
policer management-1m {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 625k;
    }
    then discard;
}
```

• Another "automagic" rate-limiting example

To prevent CPU overloading, ARP packets destined for the Routing Engine are rate-limited.

- Block insecure protocols and tools (procedures / human factor)
 - Don't allow operators to use FTP, telnet, etc. Instead allow SCP and SSH



WHERE TO APPLY CONTROL PLANE FILTERS





MULTILAYER CONTROL PLANE PROTECTION



© 2020 Juniper Networks



LOOPBACK FILTER AND CONTROL PLANE PROTECTION COMPARISON

	Loopback Filter	Control Plane DDoS Protection
Traffic Classification	User configurable	Embedded, not configurable
Policing	User configurable	User configurable
Rate limit enforcement level	ASIC	ASIC Line Card Routing Engine

Summary

Control Plane DDoS Protection limits traffic sent to the control plane components

Loopback filters may enforce lower limits to specific flows at ASIC level



WHAT'S NEXT? THERE'S MORE THAT IMPACTS CONTROL PLANE

 Secure BGP routing operations by deploying RPKI Origin Validation <u>https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-187-bgp-rpki-tn.pdf</u>

 There's a book about Deploying BGP Routing Security <u>https://www.juniper.net/documentation/en_US/day-one-books/DO_BGP_SecureRouting2.0.pdf</u>

 Scoop: Junos 20.3R1 will have TCP Authentication Option (TCP-AO) to secure BGP sessions. Further reading: <u>https://github.com/TCP-AO/</u> More protocols to follow that will leverage TCP-AO.



RESOURCES AND FURTHER READING

- Day One book: Securing the Routing Engine <u>https://kb.juniper.net/library/CUSTOMERSERVICE/Securing_RouteEngine2.pdf</u>
- O'Reilly Juniper MX DDoS Protection Case Study <u>https://www.oreilly.com/library/view/juniper-mx-series/9781449358143/ch04s02.html</u>
- Control Plane Distributed Denial-of-Service (DDoS) Protection Overview <u>https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-management-dos-protection.html</u>
- Configuring Control Plane DDoS Protection <u>https://www.juniper.net/documentation/en_US/junos/topics/topic-map/configuring-ddos-protection.html</u>
- Juniper Control Plane Protection

https://howdoesinternetwork.com/2017/juniper-control-plane-protection

