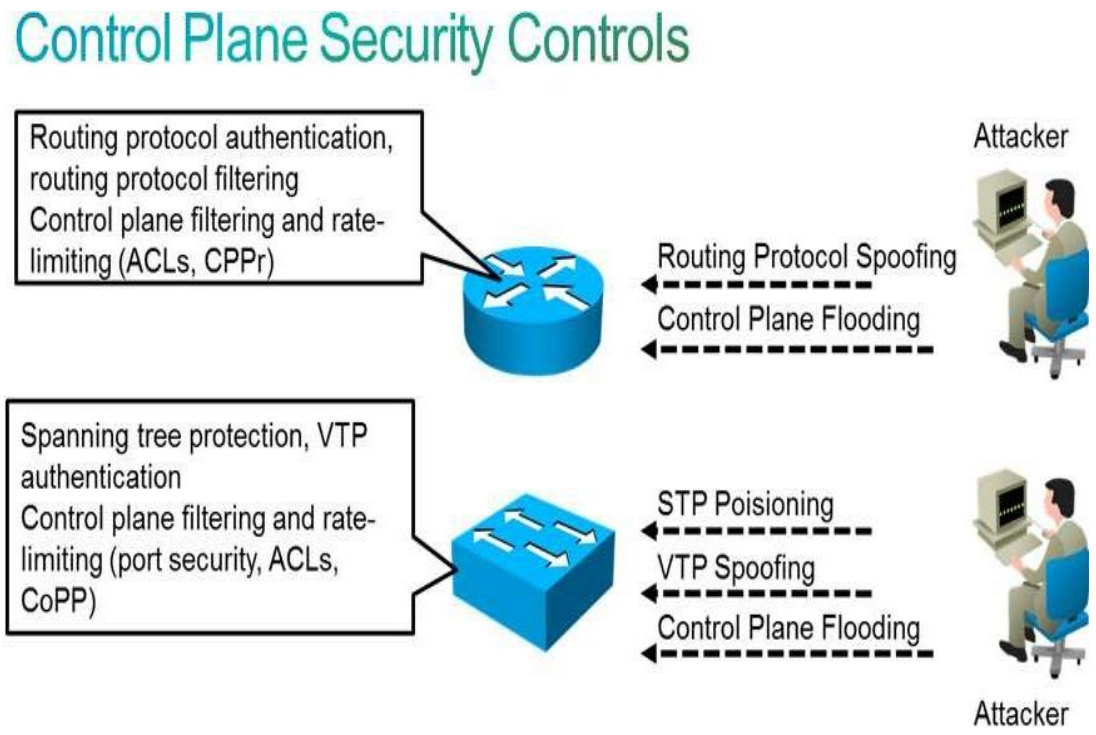
Control Plan:

- Control Plan traffic is the traffic which is from the device to the device traffic.
- Control plane traffic is traffic that is originated by or destined to the Router itself.
- Traffic that network devices send between each other for automatic network discovery.
- Protocols and traffic that network devices use on their own without direct interaction.
- For example, a routing protocol that can dynamically learn and share routing information.
- That the Cisco Router can then use to maintain an updated the routing table etc.
- If failure occurs in control plane, router might lose the capability to share routing info.
- For security of Control Plan use CoPP, CPPr, Authenticated routing protocol updates.
- Includes routing protocols and even Inter Control Message Protocol (ICMP) messages.
- Control Plan protocol example are such as CDP, LLDP, ARP, OSPF, RIP, BGP, EIGRP etc.

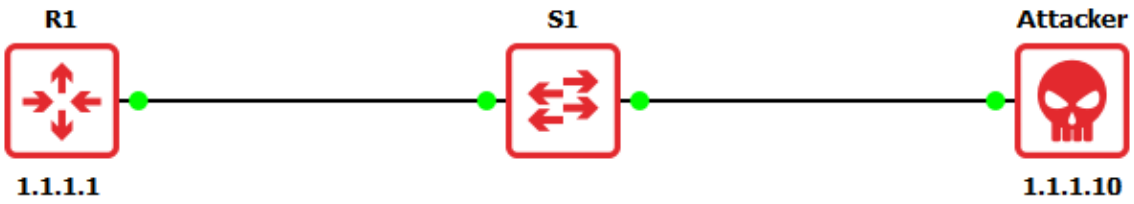


Best Practices for Protecting Control Plane.

- Create and enable Control Plane Policing (CoPP) on devices.
- Identify type & rate of traffic reaches control plane of Cisco IOS device.
- Allow users to manage the flow of traffic handled by the route processor.
- Prevent unnecessary traffic from overwhelming the route processor.
- Create and enable CPPr (Control Plane Protection) on network devices.
- Create and enable Port-filtering feature on network devices to protect.
- Limits the number of packets for a specific protocol in network device.
- Securing the Routing Protocols use password authentication method.

Function of Control Plane Policing:

- Security function that is used to protect the control plane of Cisco Routers.
- IOS feature that enables to manage the flow of traffic handled by the CPU.
- This feature prevent unnecessary traffic reducing the processing power of Router.
- Configure this as a filter for any traffic destined to the IP address of an IOS device.
- For example, specify management traffic is rate-limited down to a specific level.
- If attack occurs that involves an excessive amount of this type of traffic.
- The excess traffic specified threshold simply be ignored & not processed by CPU.



Before Control Plan Policy, let's do UDP DoS attack from Kali Linux to on R1 Router.

root@kali:~# hping3 --flood --rand-source --udp -p 445 1.1.1.1

Create ACL	Identify the Traffic create Access Control List
Class Map	Identify the Traffic Use already created ACL
Policy Map	Policy Map take Action on Class Map
Control Plan	Apply the Policy Map using Service Policy

Control Plan Policy Stop UDP DoS Attack
R1(config)#ip access-list extended test R1(config-ext-nacl)#permit udp any any
R1(config)#class-map cmap R1(config-cmap)#match access-group name test
R1(config)#policy-map pmap R1(config-pmap)#class cmap R1(config-pmap-c)#police 8000 conform-action transmit exceed-action drop R1(config-pmap-c-police)#exit R1(config-pmap-c)#log R1(config-pmap-c)#exit R1(config-pmap)#exit
R1(config)#control-plane R1(config-cp)#service-policy input pmap
R1#show policy-map control-plane

Before Control Plan Policy, let's do UDP DoS attack from Kali Linux to on R1 Router.

root@kali:~# hping3 --flood --rand-source --icmp -p 445 1.1.1.1

Control Plan Policy Stop Ping Flood
R1(config)#ip access-list extended test R1(config-ext-nacl)#permit icmp any any
R1(config)#class-map cmap R1(config-cmap)#match access-group name test
R1(config)#policy-map pmap R1(config-pmap)#class cmap R1(config-pmap-c)#police 8000 conform-action transmit exceed-action drop R1(config-pmap-c-police)#exit R1(config-pmap-c)#log R1(config-pmap-c)#exit R1(config-pmap)#exit
R1(config)#control-plane R1(config-cp)#service-policy input pmap
R1#show policy-map control-plane

Due to Control Plan Policy its drop the UDP DoS flooding Attack.

```
R2#
*May 11 15:50:03.971: %CP-6-IP: DROP Control-plane Policing  1.1.1.10 -> 1.1.1.1
 icmp
*May 11 15:50:03.971: %CP-6-IP: DROP Control-plane Policing  1.1.1.10 -> 1.1.1.1
 icmp
*May 11 15:50:03.975: %CP-6-IP: DROP Control-plane Policing  1.1.1.10 -> 1.1.1.1
 icmp
*May 11 15:50:03.975: %CP-6-IP: DROP Control-plane Policing  1.1.1.10 -> 1.1.1.1
 icmp
*May 11 15:50:03.975: %CP-6-IP: DROP Control-plane Policing  1.1.1.10 -> 1.1.1.1
 icmp
```