



ASA Deep Dive



Policy Maps & Class Maps



Policy Maps & Class Maps

- ▶ Class Maps are used to match traffic at Layer 3, Layer 3/4 or at Layer 7.
- ▶ Policy Maps are used to take action for certain types of traffic.
- ▶ ASA supports 2 types of class maps. (Layer 3/4 and Layer 7)
- ▶ ASA supports 2 types of policy maps. (Layer 3/4 and Layer 7)
- ▶ Layer 7 Class Maps
 - Used to match traffic at Layer 7 only.
 - It can only be called in a Layer 7 Policy map.
 - Command is class-map type inspect <Service> <Name>
- ▶ Layer 3/4 Class Maps
 - Used to match traffic at Layer 3/4 only.
 - It can only be called in a Layer 3/4 Policy map.
 - Command is class-map <Name>

Policy Maps & Class Maps

▶ Layer 7 Policy Maps

- Used to apply an action at Layer 7 only.
- It cannot be applied to interface.
- It is applied to Layer 3/4 Policy map.
- Command is policy-map type inspect <Service> <Name>

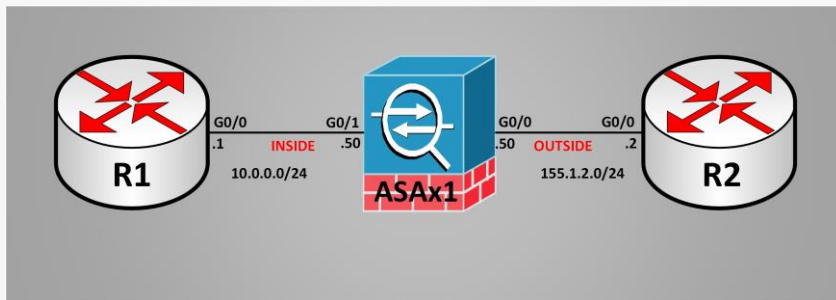
▶ Layer 3/4 Policy Maps

- Used to apply an action at Layer 3/4 only.
- It is be applied to interface.
- Command is policy-map <Name>

BGP through ASA

▶ BGP pre-requisites

- Reachability to neighbor
- Randomization of TCP sequence number should be disabled.
- Option 19 must be allowed.
- TCP port 179 needs to be permitted from lower security-level to higher security-level.



BGP through ASA

▷ BGP through ASA

- Example 1

```
class-map BGP  
  match port tcp eq bgp
```

```
tcp-map TMAP  
  tcp-options range 19 19 allow
```

```
policy-map P-Outside  
  class BGP  
    set connection random-sequence-number disable  
    set connection advanced-options TMAP
```

```
service-policy P-Outside interface OUTSIDE
```