Contents

Introduction

ZBFW is a feature set of IOSFW where we assign the router interfaces into different zones depending upon the requirement. This way we are applying inspection to the traffic moving between zones not interfaces. While using ZBFW we have more flexibility as compared to CBAC.In CBAC we configure inspection policies with ACL rules to define the IOSFW feature set however these inspection policies and ACL rules are applicable to all the traffic leaving or entering a respective interface of the router. In ZBFW we can use object-groups or ACLS to perform inspection of interested traffic along with class-maps and policy-maps which in turns provide more flexibility as compared to CBAC.Also multiple inspection rules and ACL on several interfaces of router make it more difficult to correlate the policies that will be applied to traffic flow between multiple interfaces as in case of CBAC.

ZBFW offers following features

- Application inspection
- Statefull inspection
- Local URL filtering
- Transparent firewall

Things to remember about ZBFW

- The policies configured from one zone to another are unidirectional in nature.
- By default the traffic flow between the inter-zones is ?DENY ALL?.
- By default the traffic flow to or from ?SELF? zone to another zone is ?ALLOW ALL? and we can restrict the same with the help of class-maps along with respective actions.
- By default the traffic flow between the intra-zones is ?Allow ALL? and we can?t restrict or apply any kind of inspection to the same.
- An interface can be assigned to only one security zone.
- Traffic cannot flow between a zone-member interface and any interface which is not a *zone-member, so that means every interface should be assigned to a zone.
- We can apply multiple classes along with respective action per zone-pair.

Steps to configure ZBFW

- Identify and define network zones.
- Determine the traffic flow between the respective zones.
- Define class-maps to describe traffic between zones.
- Associate class-maps with policy-maps to define actions to the respective traffic flow.
- Set up zone pairs for any policy other than deny all.
- Assign policy-maps to zone-pairs.
- Now assign interfaces to zones.
- The final step would be validate the configuration by passing some interested traffic.

Design

Server??R1(ZBFW)?-Client Client :- 10.10.10.2 R1 LAN interface:- 10.10.10.1 R1 WAN interface:- 2.2.2.1 Server :- 2.2.2.2

Configuration

```
ZBFW(config)#zone sec out

ZBFW(config-sec-zone)#exit

ZBFW(config)#zone sec in

ZBFW(config-sec-zone)#exit

ZBFW(config)#ip access-list exte insp-traffic

ZBFW(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any

ZBFW(config-ext-nacl)#exit

ZBFW(config)#class-map type inspect match-any insp-traffic

ZBFW(config-cmap)#match access-group name insp-traffic

ZBFW(config-cmap)#exit


ZBFW(config)#class-map type inspect match-any insp-traffic-protocol

ZBFW(config-cmap)#match protocol tcp

ZBFW(config-cmap)#match protocol udp

ZBFW(config-cmap)#match protocol icmp

ZBFW(config-cmap)#exit


ZBFW(config)#class-map type inspect match-all inspection-outbound

ZBFW(config-cmap)#match class insp-traffic

ZBFW(config-cmap)#match class insp-traffic-protocol

ZBFW(config-cmap)#exit



ZBFW(config)#policy-map type inspect outbound

ZBFW(config-pmap)#class inspection-outbound

ZBFW(config-pmap-c)#insp

ZBFW(config-pmap-c)#inspect

ZBFW(config-pmap-c)#exit
```

```
ZBFW(config-pmap)#exit


ZBFW(config)#zone-pair sec in-out source in destination out

ZBFW(config-sec-zone-pair)#service-policy type inspect outbound

ZBFW(config-sec-zone-pair)#exit

ZBFW(config)#


ZBFW(config)#int f0/0

ZBFW(config-if)#zone-member security out

ZBFW(config-if)#exit


ZBFW(config)#int f0/1

ZBFW(config-if)#zone-member security in

ZBFW(config-if)#exit

ZBFW(config)#
```

Related show Commands

This section provides information you can use to confirm your configuration is working properly.

Certain show commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of show command output.

ZBFW#sh policy-map type inspect zone-pair in-out sessions Zone-pair: in-out

```
 Service-policy inspect : outbound

   Class-map: inspection-outbound (match-all)
     Match: class-map match-any insp-traffic
       Match: access-group name insp-traffic
         4 packets, 135 bytes
         30 second rate 0 bps
     Match: class-map match-any insp-traffic-protocol
       Match: protocol tcp
         1 packets, 28 bytes
         30 second rate 0 bps
       Match: protocol udp
         2 packets, 67 bytes
         30 second rate 0 bps
       Match: protocol icmp
         1 packets, 40 bytes
         30 second rate 0 bps
     Inspect
       Established Sessions
        Session 669F65F4 (10.10.10.2:1086)=>(2.2.2.2:23) tcp SIS_OPEN
         Created 00:00:18, Last heard 00:00:13
```

```
        Bytes sent (initiator:responder) [45:84]
       Session 669F6064 (10.10.10.2:8)=>(3.3.3.1:0) icmp SIS_OPEN
        Created 00:02:14, Last heard 00:00:00
         ECHO request
        Bytes sent (initiator:responder) [4320:4288]

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    1 packets, 219 bytes
```

Related Information

Technical Support & Documentation - Cisco Systems