

Day of Firewall

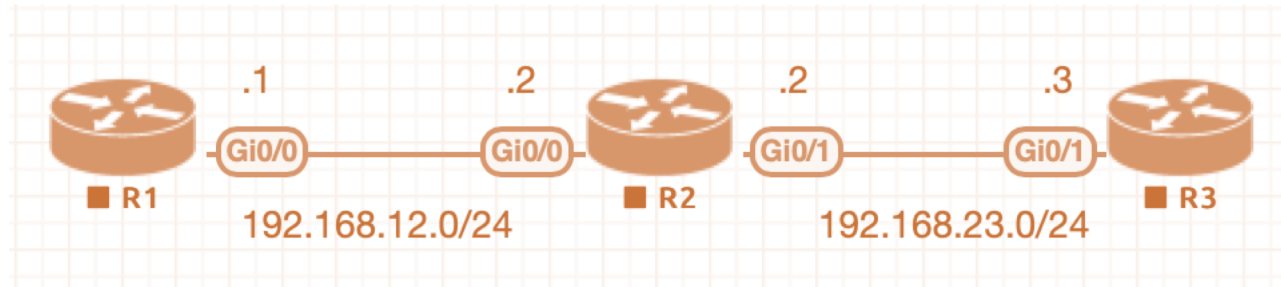
Nazrul Islam

nazrul13@gmail.com

Reflexive Access List

- Reflexive Access-list is an access-list which allows only the replies of the packets of the sessions initiated within the network (from the outside network) .
 - Reflexive Access-list should be nested inside the named Extended Access-list.
 - A temporary entry is generated when a session begins and automatically destroyed when session ends.
 - It does not have implicit deny at the end of Access-list.
 - Just like normal access-list, if one the condition matches then no more entries are evaluated.
 - Reflexive Access-list cannot be defined with named or numbered standard Access-list.

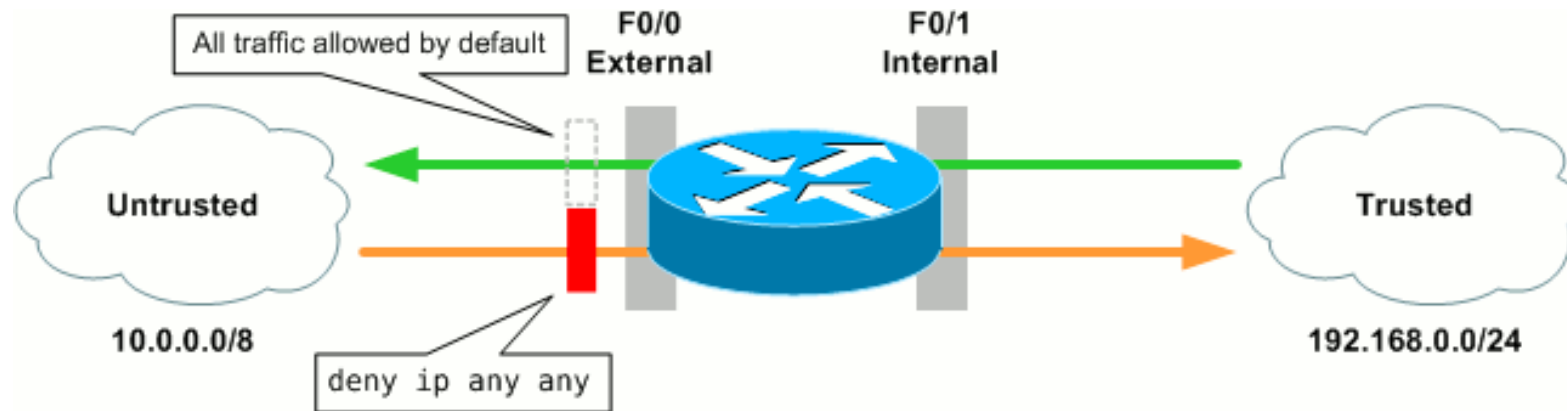
Reflexive LAB



- `R2(config)#ip access-list extended OUTBOUND`
- `R2(config-ext-nacl)#permit ip any any reflect EVALUATE`
- `R2(config)#interface fastEthernet 0/1`
- `R2(config-if)#ip access-group OUTBOUND out`
- `R2(config)#ip access-list extended INBOUND`
- `R2(config-ext-nacl)#evaluate EVALUATE`
- `R2(config)#interface fastEthernet 0/1`
- `R2(config-if)#ip access-group INBOUND in`

Context Based Access Control (CBAC)

- The ACLs provide traffic filtering and protection till the transport layer while on the other hand, CBAC provides the same function upto the application layer. With the help of CBAC configuration, the router can act as a firewall.



CBAC Features

- **Inspecting traffic**

- CBAC maintains TCP /UDP information which is needed to perform deeper inspection in packet payload.

- **Filtering traffic**

- CBAC filters the traffic which is originated from trusted network and goes out through the firewall and allow replies only if it has an entry in the state table. It has the ability to filter the traffic intelligently upto layer 7.

- **Detecting intrusion**

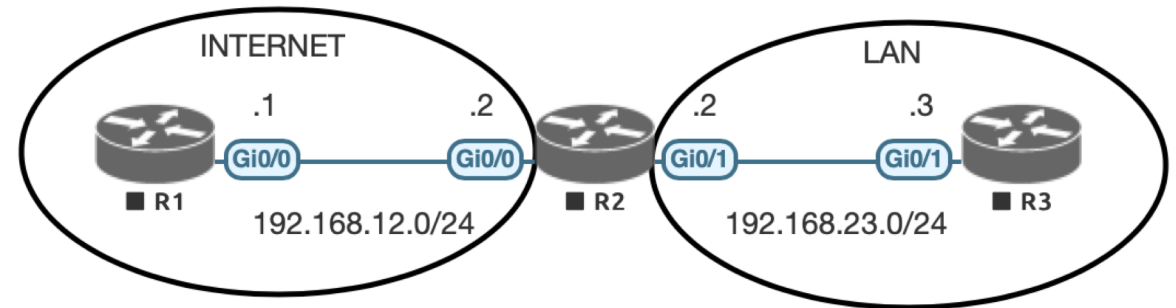
- CBAC examines the rate at which the connection has been established by which it can detect attacks like Dos attack, TCP syn attack etc. On the basis of this, CBAC mechanism can cause a connection to reestablish or drop malicious packets.

- **Generating alerts and audits**

- The router operating CBAC mechanism log information about connections established, number of bytes sent, source and destination IP address.

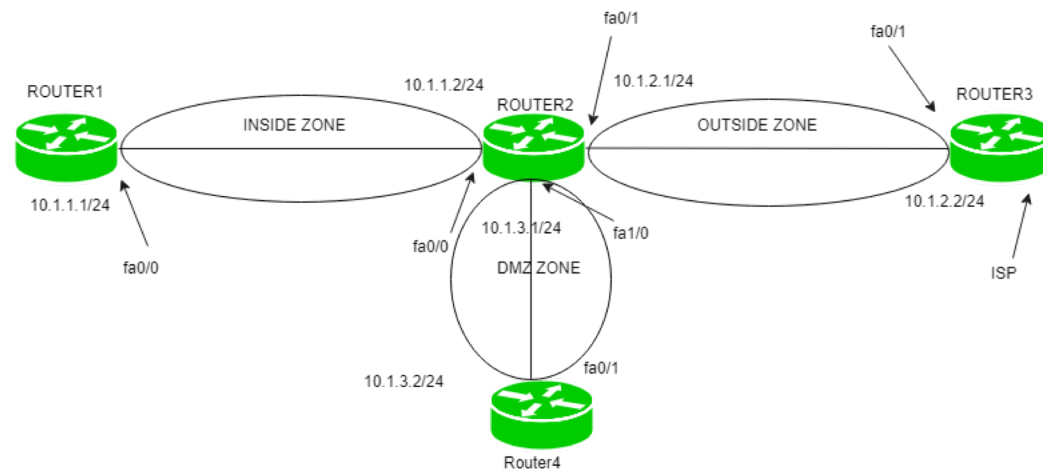
CBAC LAB

- R2(config)#ip access-list extended DENY_ALL_FROM_INTERNET
- R2(config-ext-nacl)#deny ip any any log
- R2(config)#interface fastEthernet 0/0
- R2(config-if)#ip access-group DENY_ALL_FROM_INTERNET in
- R2(config)#ip inspect name FIREWALL tcp
- R2(config)#ip inspect name FIREWALL udp
- R2(config)#ip inspect name FIREWALL icmp
- R2(config)#ip inspect name FIREWALL http
- R2(config)#interface fastEthernet 0/0
- R2(config-if)#ip inspect FIREWALL out



Zone Based Firewall

- A Zone-based firewall is an advanced method of stateful firewall. In stateful firewall, a stateful database is maintained in which source IP address, destination IP address, source Port number, destination port number is recorded. Due to this, only the replies are allowed.

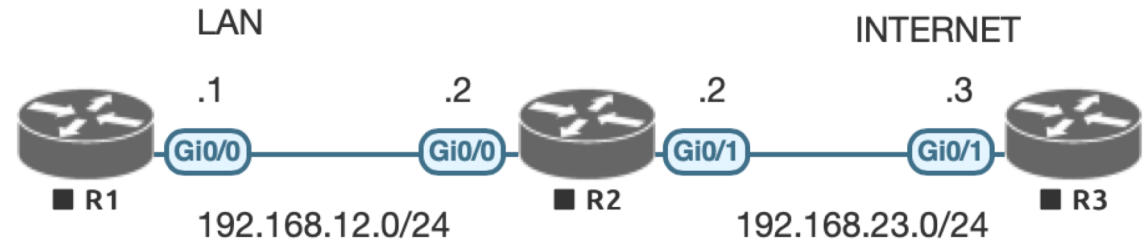


ZBF Terms

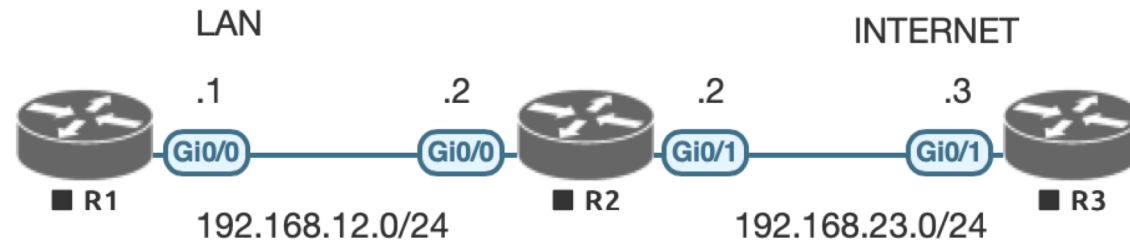
- **Zone** – A zone is a logical area in which the devices having same trust levels resides. After creating a zone, an interface is assigned to a zone. By default, traffic is not allowed from one zone to another.
- **Zone-pair** – Policies are defined in which traffic is identified (what type of traffic) then what action should be taken (Inspect Denied, permit). Then we have to apply this policies to a zone-pair. A zone-pair is always unidirectional. If we want to make it bidirectional then we have to create another zone-pair.
- **Self-zone** – Traffic destined to the router itself, irrespective of which device has send, is known as self zone. The traffic generated from router is known as traffic coming from self-zone. Traffic going to router is considered as traffic going to Self-zone. By default, the traffic to or from the Self-zone is allowed however it can be changed according to the policies applied.

ZBF LAB

- Zones Config:
- R2(config)#**zone security LAN**
- R2(config)#**zone security WAN**
- R2(config)#**interface fastEthernet 0/0**
- R2(config-if)#**zone-member security LAN**
- R2(config)#**interface fastEthernet**
- R2(config-if)#**zone-member security WAN**
- R2#**show zone security**



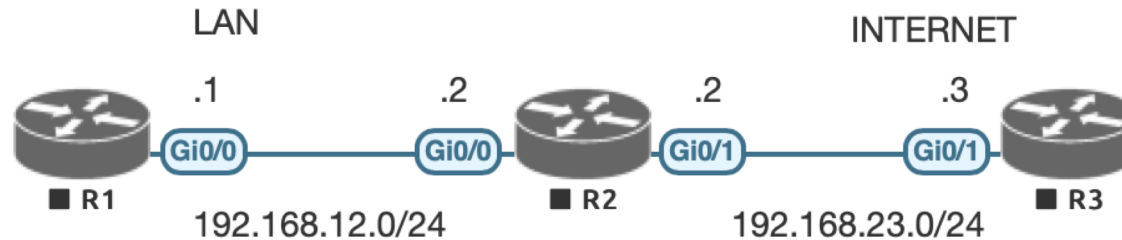
ZBF LAB



Zones Pair Config:

- `R2(config)#zone-pair security LAN-TO-WAN source LAN destination WAN`
- `R2(config-sec-zone-pair)#description LAN-TO-WAN TRAFFIC`
- `R2(config)#zone-pair security WAN-TO-LAN source WAN destination LAN`
- `R2(config-sec-zone-pair)#description WAN-TO-LAN TRAFFIC`
- `R2# show zone-pair security`

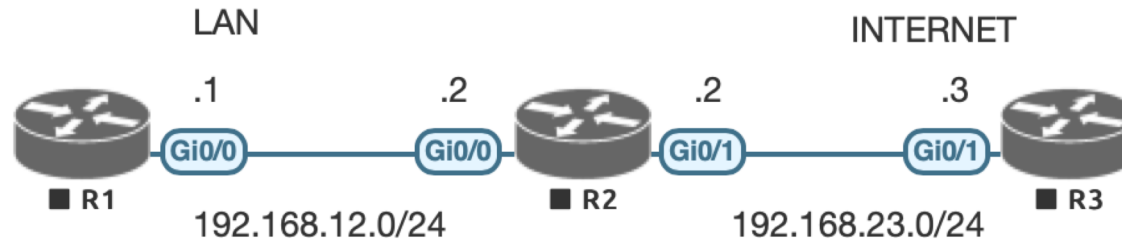
ZBF LAB



Security Policy Config:

- `R2(config)#class-map type inspect ICMP`
- `R2(config-cmap)#match protocol icmp`
- `R2(config)#policy-map type inspect LAN-TO-WAN`
- `R2(config-pmap)#class type inspect ICMP`
- `R2(config-pmap-c)#inspect`
- `R2(config)#zone-pair security LAN-TO-WAN`
- `R2(config-sec-zone-pair)#service-policy type inspect LAN-TO-WAN`
- `R2#show policy-map type inspect zone-pair`

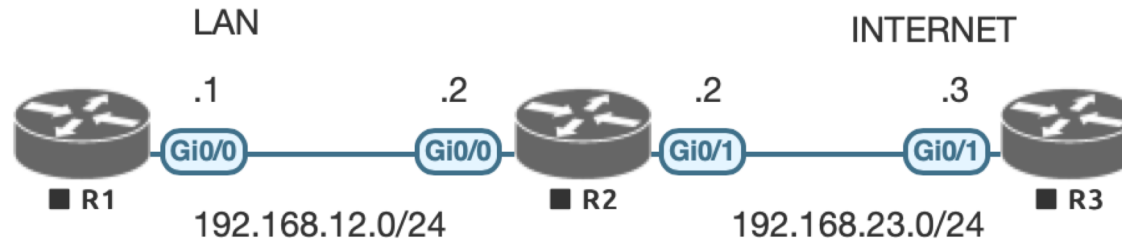
ZBF LAB



WAN-TO-LAN Policy Config:

- `R2(config)#class-map type inspect TELNET`
- `R2(config-cmap)#match protocol telnet`
- `R2(config)#policy-map type inspect WAN-TO-LAN`
- `R2(config-pmap)#class type inspect TELNET`
- `R2(config-pmap-c)#inspect`
- `R2(config)#zone-pair security WAN-TO-LAN`
- `R2(config-sec-zone-pair)#service-policy type inspect WAN-TO-LAN`

ZBF LAB



Self Zone Config:

- `R2(config)#policy-map type inspect WAN-TO-SELF`
- `R2(R2(config)#zone-pair security WAN-TO-SELF source WAN destination self`
- `R2(config-sec-zone-pair)#service-policy type inspect WAN-TO-SELF`
- `R2#show policy-map type inspect zone-pair WAN-TO-SELF`

ASA intro

- The firewall is the barrier between a **trusted and untrusted network**, often used between your LAN and WAN. It's typically placed in the forwarding path so that all packets have to be checked by the firewall, where we can drop or permit them.
- Cisco Adaptive Security Appliance (ASA) Software is the core operating system for the Cisco ASA Family. It delivers enterprise-class firewall capabilities for ASA devices in an array of form factors - standalone appliances, blades, and virtual appliances - for any distributed network environment

Major Function

- Stateful Filtering
 - Firewalls use stateful filtering. They keep track of all incoming and outgoing connections.
- Packet Inspection
 - Packet inspection means firewall can inspect up to layer 7 of the OSI model. This means it can look at application data and even the payload.
- Security Zones
 - Cisco routers, by default, will permit and forward all packets they receive, if they have a matching route in their routing table. Access list is to restrict this but it also become nightmare for an administrator and to avoid such situation ASA came with Security Zones.

ASA Basic Config

- ASA1(config)# **interface E0/0**
- ASA1(config-if)# **nameif INSIDE**
- ASA1(config-if)# **ip address 192.168.1.254 255.255.255.0**
- ASA1(config-if)# **no shutdown**

- ASA1(config)# **interface E0/1**
- ASA1(config-if)# **nameif OUTSIDE**
- ASA1(config-if)# **ip address 192.168.2.254 255.255.255.0**
- ASA1(config-if)# **no shutdown**

- ASA1(config)# **interface E0/2**
- ASA1(config-if)# **nameif DMZ**
- ASA1(config-if)# **security-level 50**
- ASA1(config-if)# **ip address 192.168.3.254 255.255.255.0**
- ASA1(config-if)# **no shutdown**