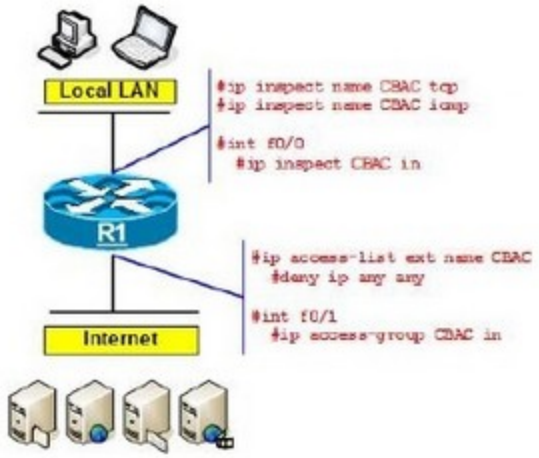
Micronics NETWORKING & TRAINING INC

Legacy Cisco IOS Firewall (CBAC)

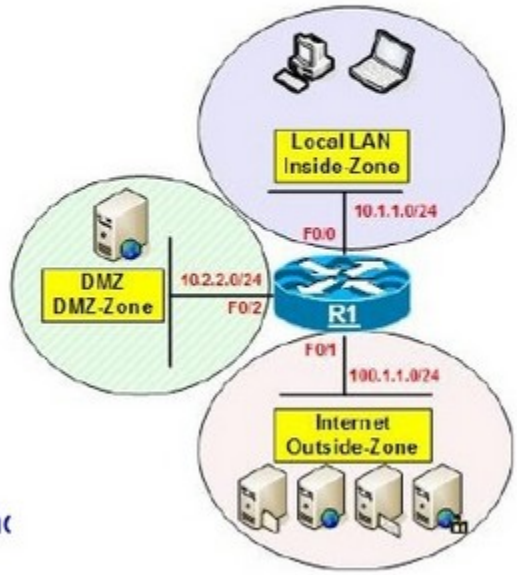
- Cisco IOS Stateful Inspection (formerly CBAC) offered interface-based firewall service
- Inspection policy and ACL policy combined to define firewall policy
- Very little inspection policy granularity
- Inspection relies too heavily on ACLs



Micronics NETWORKING & TRAINING INC

Zone-Based Policy Firewall (ZFW)

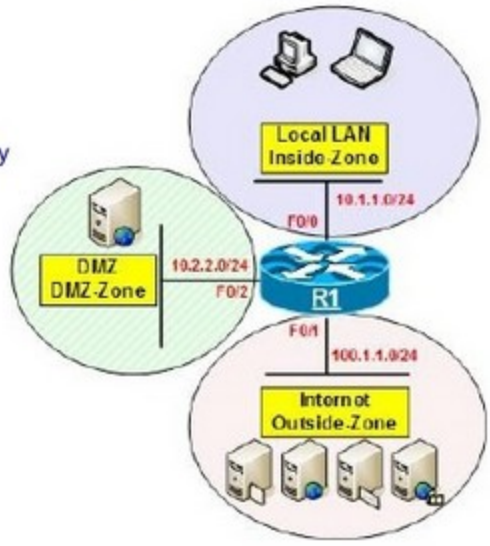
- Zone-Based Policy introduces a new firewall configuration model
- Policies are applied to traffic moving between zones, not interfaces
- Subnet-and host-specific policies
- Firewall policies can be more clearly understood
- CBAC and ZFW can be used concurrently on the same router, but nc combined on interfaces

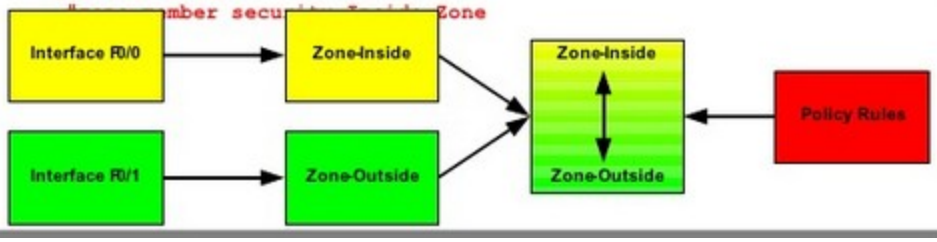


Micronics NETWORKING & TRAINING INC

Steps to ZFW Configuration

1. Define zones.
```
#zone security Inside-Zone
```
3. Define zone-pairs.
```
#zone-pair ZP source Inside-Zone destination
Outside-Zone
```
5. Define class-maps that describe traffic that must have policy applied as it crosses a zone-pair.
```
#class-map type inspect match-all CMAP
 #match protocol tcp
```
8. Define policy-maps to apply action to your class-maps' traffic.
```
#policy-map type inspect PMAP
 #class CMAP
  #inspect
```
12. Apply policy-maps to zone-pairs.
```
#zone-pair ZP source Inside-Zone destination
Outside-Zone
 #service-policy type inspect PMAP
```
15. Assign interfaces to zones.
```
#interface f0/0
```





Micronics NETWORKING & TRAINING INC

ZFW Basic Rules

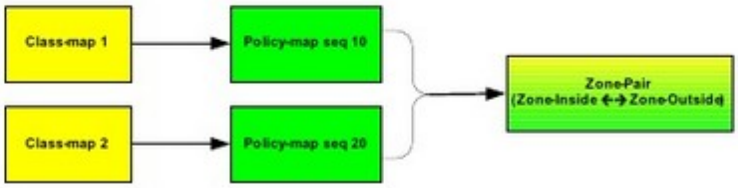
- ✓ Unidirectional policy is applied between zones
- ✓ Default policy for inter-zone traffic is DENY ALL
- ✓ Multiple traffic classes and actions can be applied per zone-pair
- ✓ If two interfaces are not in zones, traffic flows freely between them
- ✓ If one interface is in a zone, and another interface is not in a zone, traffic may never flow between them
- ✓ If two interfaces are in two different zones, traffic will not flow between the interfaces until a policy is defined to allow the traffic

Micronics NETWORKING & TRAINING INC

How to build a policy?

Applies C3PL (Cisco Common Classification Policy Language) framework based on existing MQC framework in Cisco IOS Software using 3 simple steps:

- Class-map - Specifies interesting traffic via "match" conditions
- Policy-map - Associates actions with the above specified traffic
- Service-policy - Associates policy map with the zone-pair (applies policy)



Micronics NETWORKING & TRAINING INC

The „inspect" type class-map

- Applies logical qualifiers 'match-all' and 'match-any'; determines the way a packet is matched against filters in a class-map

- Applies three types of match statements (filters)
  - match protocol <protocol-name>
  - match access-group <number | name>
  - match class <class-map-name>

Example

```
class-map type inspect match-all CMAP1
 match protocol http
 match access-group 120

class-map type inspect match-any CMAP2
 match protocol http
 match protocol ftp
 match protocol smtp

class-map type inspect match-all CMAP3
 match access-group 199
 match class CMAP2
```

Micronics NETWORKING & TRAINING INC

The „match protocol" filter

- Matches the protocol in the packet headers against the specified protocol
  - L4 protocols - match protocol <tcp | udp | icmp>
  - L7 protocols - match protocol <http | smtp | telnet|…>
- In case of L7 protocols, the ports associated with the protocol are dictated by the existing PAM feature
- Determines the protocol for which the packet will be inspected, if 'inspect' action is configured in the policy-map

Example

```
class-map type inspect match-any CMAP1
 match protocol tcp
 match protocol http

class-map type inspect match-all CMAP2
 match protocol tcp
 match protocol http
```

When HTTP packets comes it will be inspected as TCP

When HTTP packets comes it will be inspected as HTTP

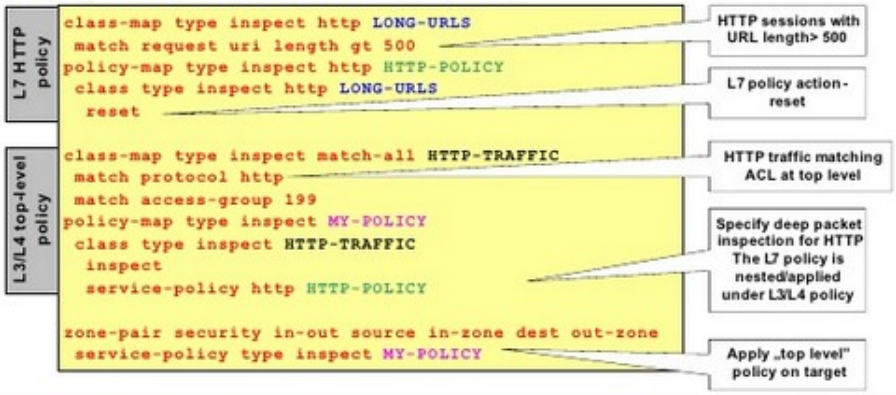
Micronics NETWORKING & TRAINING INC

ZFW Policy Action

- Inspect
  - Monitor outbound traffic according to permit/deny policy
  - Anticipate return traffic according to session table entries
- Drop
  - Siliently drops packets
- Pass
  - Requires manually-configured ACL for reflexive policy
  - No stateful capability
- Interface ACLS are still applicable, in addition to Zone-Based Policy
  - 'ip access-group in' is applied before ZFW
  - 'ip access-group out' is applied after ZFW

ZFW Policy Types: Layer 3/4/7

- L3/L4 policy is a “top level” policy which is attached to the zone-pair; applies “high level” actions like drop, inspect, urlfilter and deep-inspection to the traffic matched by the class-map
- L7 or application policy is optional and is typically applied to control details of an application ie: http, smtp etc. It is contained in an L3/L4 policy and cannot be directly attached to a target
- L3/L4 policy suffices for basic inspection; application level inspection id performed by nesting an L7 policy under the L3/L4 policy



Local traffic inspection

- 'Local' traffic provisioned through concept of 'self' zone
- 'self' zone is system-defined
- 'self' can appear as source or destination zone in a zone-pair
- Validations are performed to check that only allowed protocols (tcp, udp, icmp, H323) can be configured for inspection when self zone is involved

Example

```
class-map type inspect LOCAL-TCP
 match protocol tcp
policy-map type inspect MY-LOCAL-POLICY
 class type inspect LOCAL-TCP
  inspect
zone-pair security Inside-to-Local source in-zone dest self
 service-policy type inspect MY-LOCAL-POLICY
```

ZFW DoS Protection

- 'parameter maps' are used to specify inspection behavior like TCP connections, session timers, audit trail logging setting and DoS Protection
- 'parameter map' can be used in defining matching criteria in the class map
- Can also be used in policy map to define application-specific behavior like HTTP objects and POP3/IMAP authentication requirements

Example

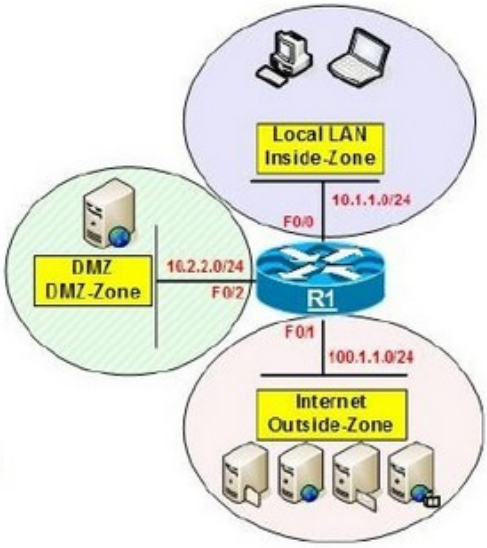
```
parameter-map type inspect PARAM1
 max-incomplete low 100
 max-incomplete high 200
 tcp max-incomplete host 100 block-time 10
parameter-map type regex PARAM2
 pattern .*delete

class-map type inspect http HTTP-CMAP
 match request uri regex PARAM2

policy-map type inspect http HTTP-PMAP
 class type inspect http HTTP-CMAP
   reset

policy-map type inspect MY-POLICY
 class type inspect CMAP1
  inspect PARAM1
 class type inspect CMAP2
  inspect
  service-policy http HTTP-PMAP
```


ZFW Configuration – In/Out/DMZ

Network consistes of three zones

- Inside-Zone: private network, 10.1.1.0/24
- Outside-Zone: Internet
- DMZ-Zone: 10.2.2.0/24

3. Inspect tcp, http, icmp from the Inside-Zone to the Outside-Zone.
4. Does not allow users to connect to the mail.google.com and mail.yahoo.com websites.
5. Allow and inspect HTTP to hosted Web Server on DMZ (10.2.2.2).
6. Enable DoS Protecton so that it does not allow more than 500 half-open connections (delete the oldest 200 entries when the limit is reached) from the Internet to the Web Server.



ZFW Configuration: Step #1

Create the policy : Inside-Zone - Outside-Zone

Step #1

```
class-map type inspect match-any CMAP-L3-ICMP-TCP-In-Out
 match protocol icmp
 match protocol tcp

class-map type inspect match-all CMAP-L3-HTTP-In-Out
 match protocol http

parameter-map type regex DENY-SITES
 pattern .*mail.google.com
 pattern .*mail.yahoo.com

class-map type inspect http CMAP-L7-In-Out
 match req-resp header host regex DENY-SITES

policy-map type inspect http PMAP-L7-In-Out
 class type inspect http CMAP-L7-In-Out
   reset


policy-map type inspect PMAP-L3-In-Out
 class type inspect CMAP-L3-HTTP-In-Out
  inspect
  service-policy http PMAP-L7-In-Out
class type inspect CMAP-L3-ICMP-TCP-In-Out
 inspect
```

Create L3/L3 class map to match ICMP and TCP

Create L3/L3 class map to match HTTP only

Create parameter map to match domain names using regex

Create L7 class map to match host field in HTTP header
Host: mail.google.com

Create L7 policy map and assign L3/L4 class map to it Set action to „reset" for packets matching L7 class map

Create L3/L4 policy map and assign previously configured class maps Set action to „inspect" Remeber that L7 policy map must be nested

ZFW Configuration: Step #2

Create the policy : Outside-Zone - DMZ-Zone

Step #2

```
access-list 120 permit tcp any host 10.2.2.2 eq 80

class-map type inspect match-all CMAP-L3-Out-DMZ
 match protocol http
 match access-group 120

parameter-map type inspect PM-DMZ-PROTECTION
 max-incomplete low  300
 max-incomplete high 500

policy-map type inspect PMAP-L3-Out-DMZ
 class type inspect CMAP-L3-Out-DMZ
  inspect PM-DMZ-PROTECTION
```

ACL should match Web Server's IP address

Create L3 class map to match HTTP along with ACL

Create paramater map for DoS Protection

Create L3/L4 policy map and attach previously configured L3/L4 class map. Set the action to „inspect" with custom parameters defined

ZFW Configuration: Step #3

Step #3 — Create zones and zone pairs . Assign policy.

```
zone security Inside-Zone
zone security Outside-Zone
zone security DMZ-Zone

zone-pair security Inside-to-Outside source Inside-Zone destination Outside-Zone
 service-policy type inspect PMAP-L3-In-Out
zone-pair security Outside-to-DMZ source Outside-Zone destination DMZ-Zone
 service-policy type inspect PMAP-L3-Out-DMZ

int f0/0
 zone-member security Inside-Zone
int f0/1
 zone-member security Outside-Zone
int f0/2
 zone-member security DMZ-Zone
```

Create zones

Attach policy to the zone pair

Attach policy to the zone pair

Assign interface to the zones

ZFW Verification

- show policy-map type inspect zone-pair
- show policy-map type inspect http
- show zone security
- show zone-pair security