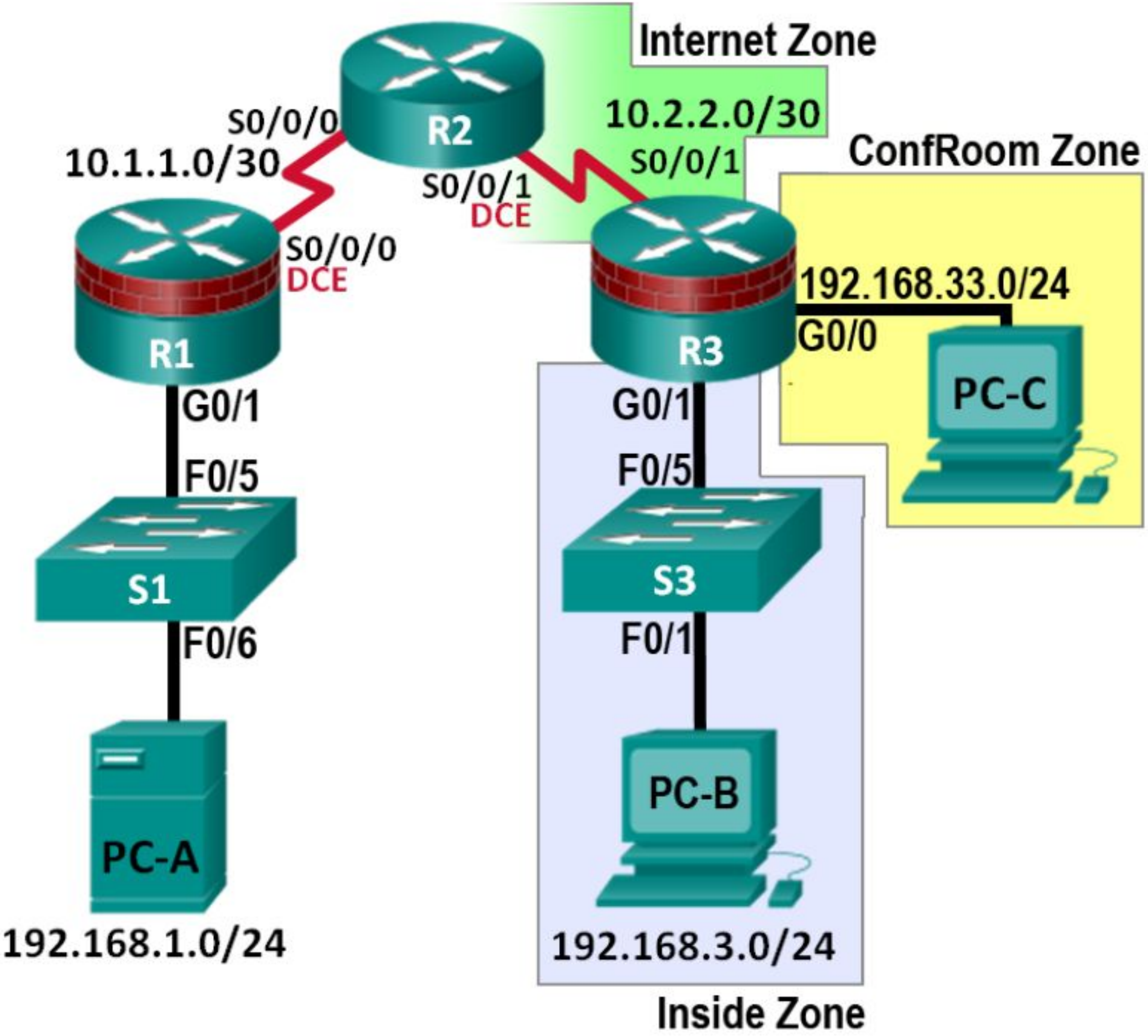
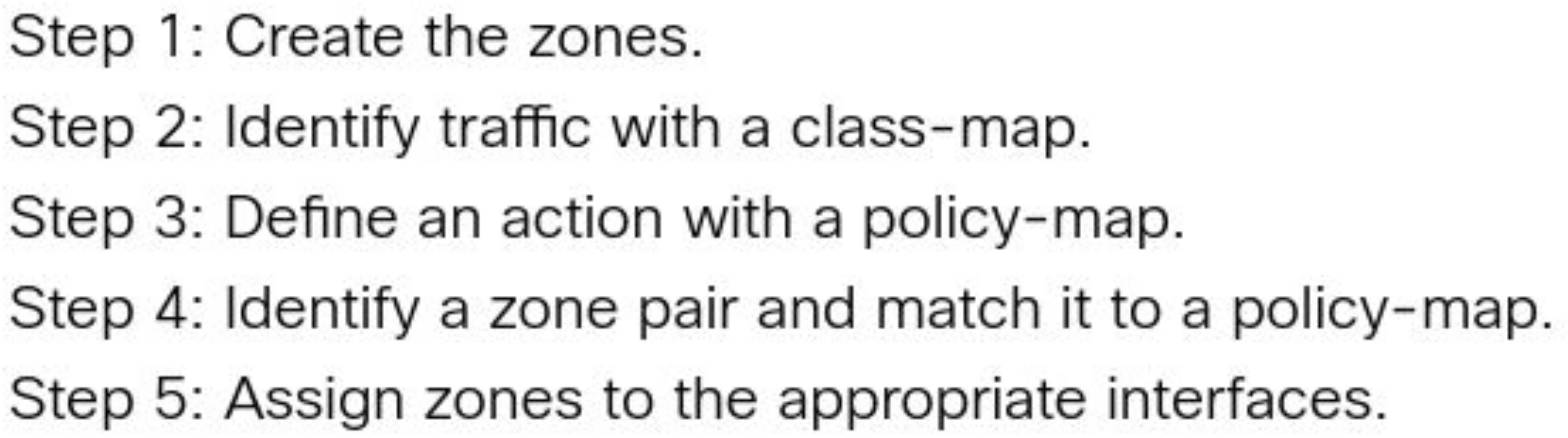
Zone-Based Policy Firewall (ZPF)

Topology


Internet Zone
R2
S0/0/0
10.1.1.0/30
S0/0/1
DCE
10.2.2.0/30
S0/0/1
ConfRoom Zone
R1
S0/0/0
DCE
R3
192.168.33.0/24
G0/0
PC-C
G0/1
F0/5
S1
F0/6
PC-A
192.168.1.0/24
G0/1
F0/5
S3
F0/1
PC-B
192.168.3.0/24
Inside Zone

ZPF Configuration Steps



Step 1: Create the zones.

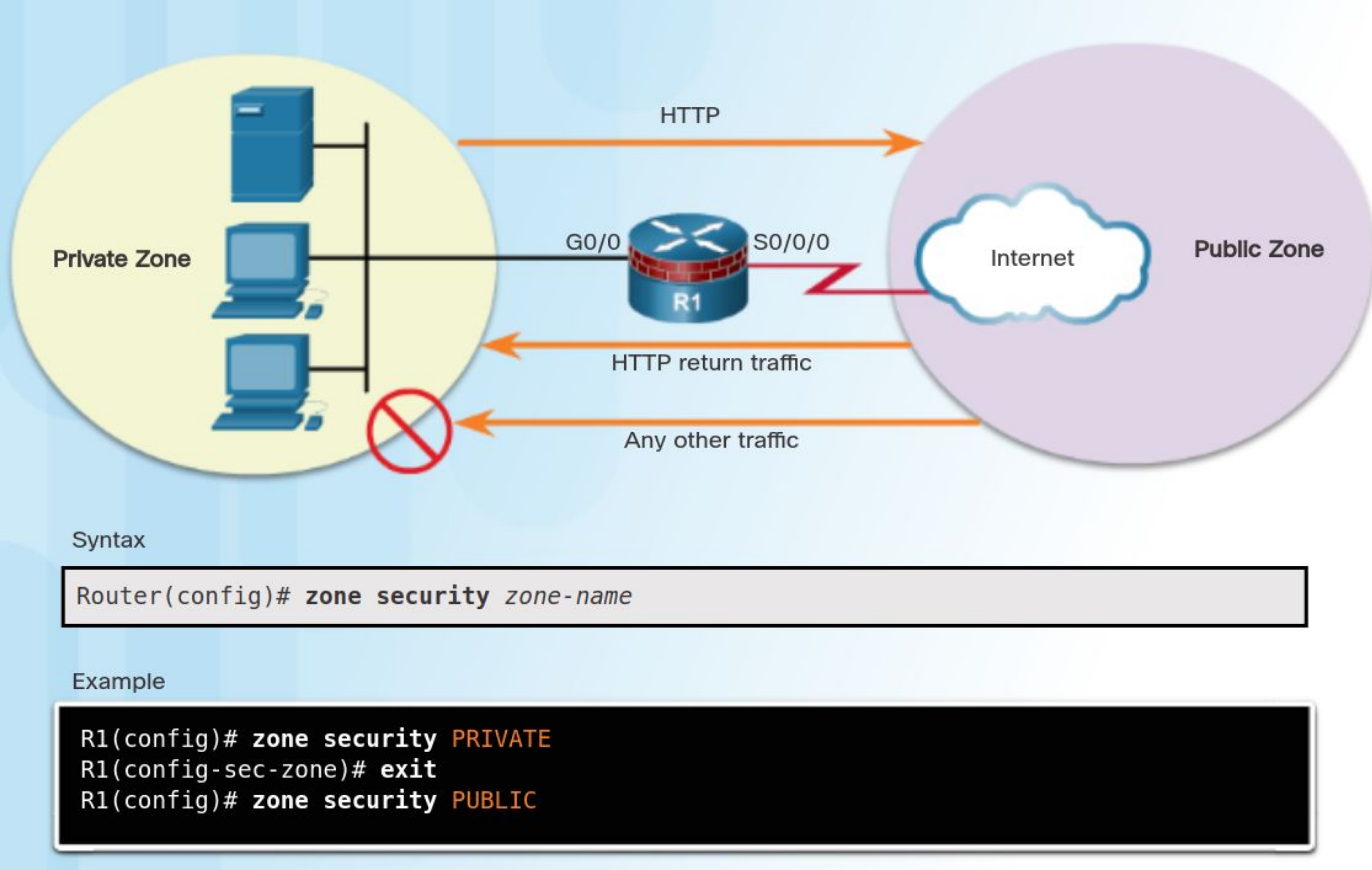
Step 2: Identify traffic with a class-map.

Step 3: Define an action with a policy-map.

Step 4: Identify a zone pair and match it to a policy-map.

Step 5: Assign zones to the appropriate interfaces.

ZPF Configuration Step 1



Syntax

```
Router(config)# zone security zone-name
```

Example

```
R1(config)# zone security PRIVATE
R1(config-sec-zone)# exit
R1(config)# zone security PUBLIC
```

ZPF Configuration Step 2

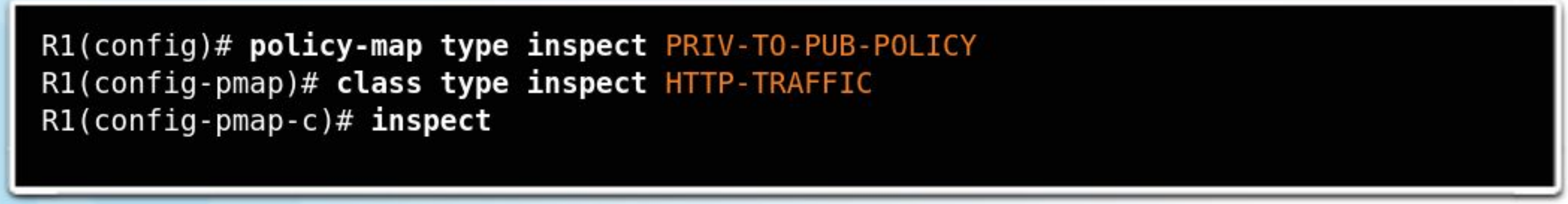
```
Router(config)# class-map type inspect [match-any | match-all] class-map-name
```

```
Router(config-cmap)# match access-group {acl-# | acl-name }
Router(config-cmap)# match protocol protocol-name
Router(config-cmap)# match class-map class-map-name
```

```
R1(config)# class-map type inspect match-any HTTP-TRAFFIC
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# match protocol dns
```

ZPF Configuration Step 3

```
Router(config)# policy-map type inspect policy-map-name
Router(config-pmap)# class type inspect class-map-name
Router(config-pmap-c)# { inspect | drop | pass }
```



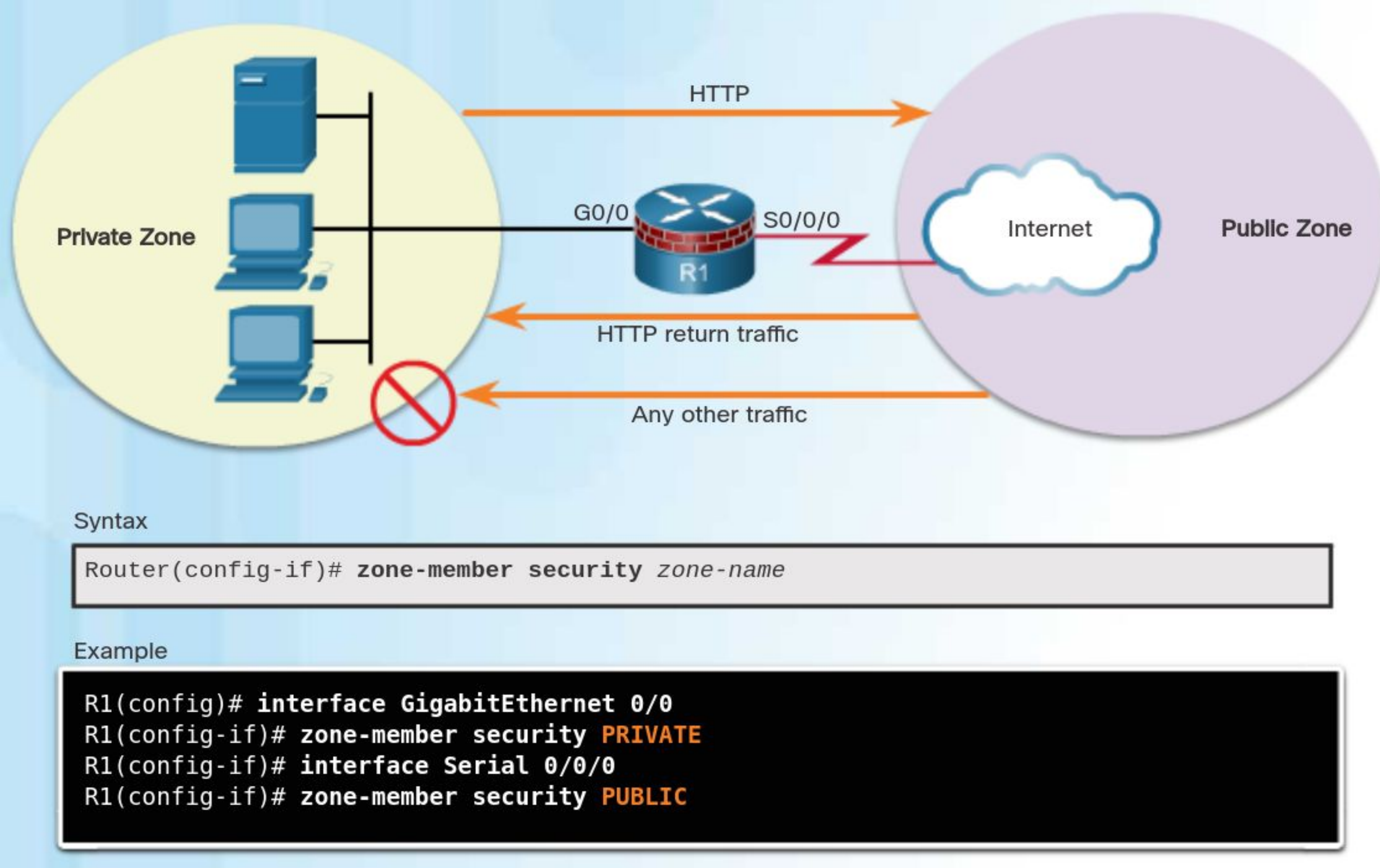
```
R1(config)# policy-map type inspect PRIV-TO-PUB-POLICY
R1(config-pmap)# class type inspect HTTP-TRAFFIC
R1(config-pmap-c)# inspect
```

ZPF Configuration Step 4

```
Router(config)# zone-pair security zone-pair-name source {source-zone-name | self
} destination {destination-zone-name | self }
Router(config-sec-zone-pair)# service-policy type inspect policy-map-name
```

```
R1(config)# zone-pair security PRIV-PUB source PRIVATE destination PUBLIC
R1(config-sec-zone-pair)# service-policy type inspect PRIV-TO-PUB-POLICY
```

ZPF Configuration Step 5



Syntax

```
Router(config-if)# zone-member security zone-name
```

Example

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# zone-member security PRIVATE
R1(config-if)# interface Serial 0/0/0
R1(config-if)# zone-member security PUBLIC
```

Security Zone

```
R3(config)# zone security INSIDE
R3(config)# zone security CONFROOM
R3(config)# zone security INTERNET
```

Inspect Class Map (1/2)

```
R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
```

Inspect Class Map (2/2)

```
R3(config)# class-map type inspect match-any CONFROOM_PROTOCOLS
R3(config-cmap)# match protocol http
R3(config-cmap)# match protocol https
R3(config-cmap)# match protocol dns
```

Inspect Policy Map (1/2)

```
R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
```

Inspect Policy Map (2/2)

```
R3(config)# policy-map type inspect CONFROOM_TO_INTERNET
R3(config-pmap)# class type inspect CONFROOM_PROTOCOLS
R3(config-pmap-c)# inspect
```

Zone Pair (1/2)

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET
```

Zone Pair (2/2)

```
R3(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination INTERNET
```

Show Zone Pair (1/2)

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
        Source-Zone INSIDE Destination-Zone INTERNET
        service-policy not configured
Zone-pair name CONFROOM_TO_INTERNET
        Source-Zone CONFROOM Destination-Zone INTERNET
        service-policy not configured
```

Apply Policy Map to Zone Pairs (1/2)

```
R3(config)# zone-pair security INSIDE_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET
```

Apply Policy Map to Zone Pairs (2/2)

```
R3(config)# zone-pair security CONFROOM_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect CONFROOM_TO_INTERNET
```

Show Zone Pair (2/2)

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
        Source-Zone INSIDE Destination-Zone INTERNET
        service-policy INSIDE_TO_INTERNET
Zone-pair name CONFROOM_TO_INTERNET
        Source-Zone CONFROOM Destination-Zone INTERNET
        service-policy CONFROOM_TO_INTERNET
```

Assign Interfaces to Security Zones

```
R3(config)# interface g0/0
R3(config-if)# zone-member security CONFROOM

R3(config)# interface g0/1
R3(config-if)# zone-member security INSIDE

R3(config)# interface s0/0/1
R3(config-if)# zone-member security INTERNET
```

Show Security Zone

```
R3# show zone security
zone self
  Description: System defined zone
zone CONFROOM
  Member Interfaces:
    GigEthernet0/0
zone INSIDE
  Member Interfaces:
    GigEthernet0/1
zone INTERNET
  Member Interfaces:
    Serial0/0/1
```

Secure Internal Security Zone

```
R3(config)#policy-map type inspect internet_to_self
R3(config-pmap)#class class-default
R3(config-pmap)#drop

R3(config)#zone-pair security INTERNET_to_Self source INTERNET destination self
R3(config-sec-zone-pair)#service-policy type inspect internet_to_self
```

Hint for some IOS versions

```
R3(config)# policy-map type inspect inside
R3(config-pmap)# class class-default
R3(config-pmap-c)# pass

R3(config)# zone-pair security INSIDE source INSIDE destination INSIDE
R3(config-sec-zone-pair)# service-policy type inspect inside
```

Questions