

Securizando Redes con Firewalls

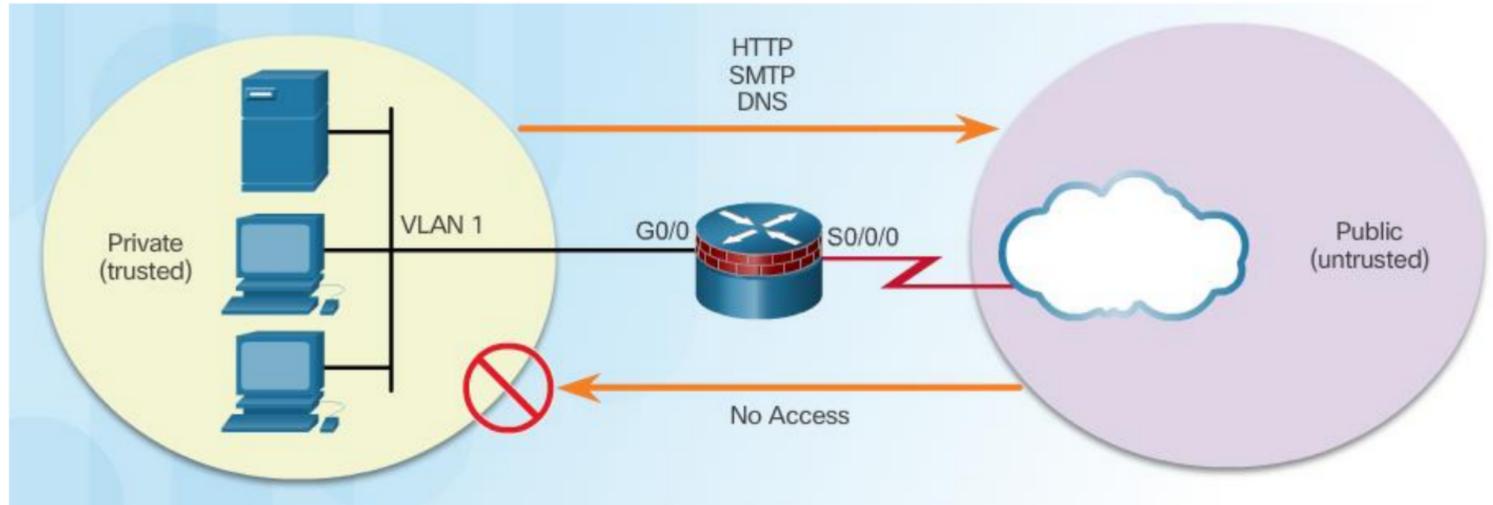
CCNA Security v2.0



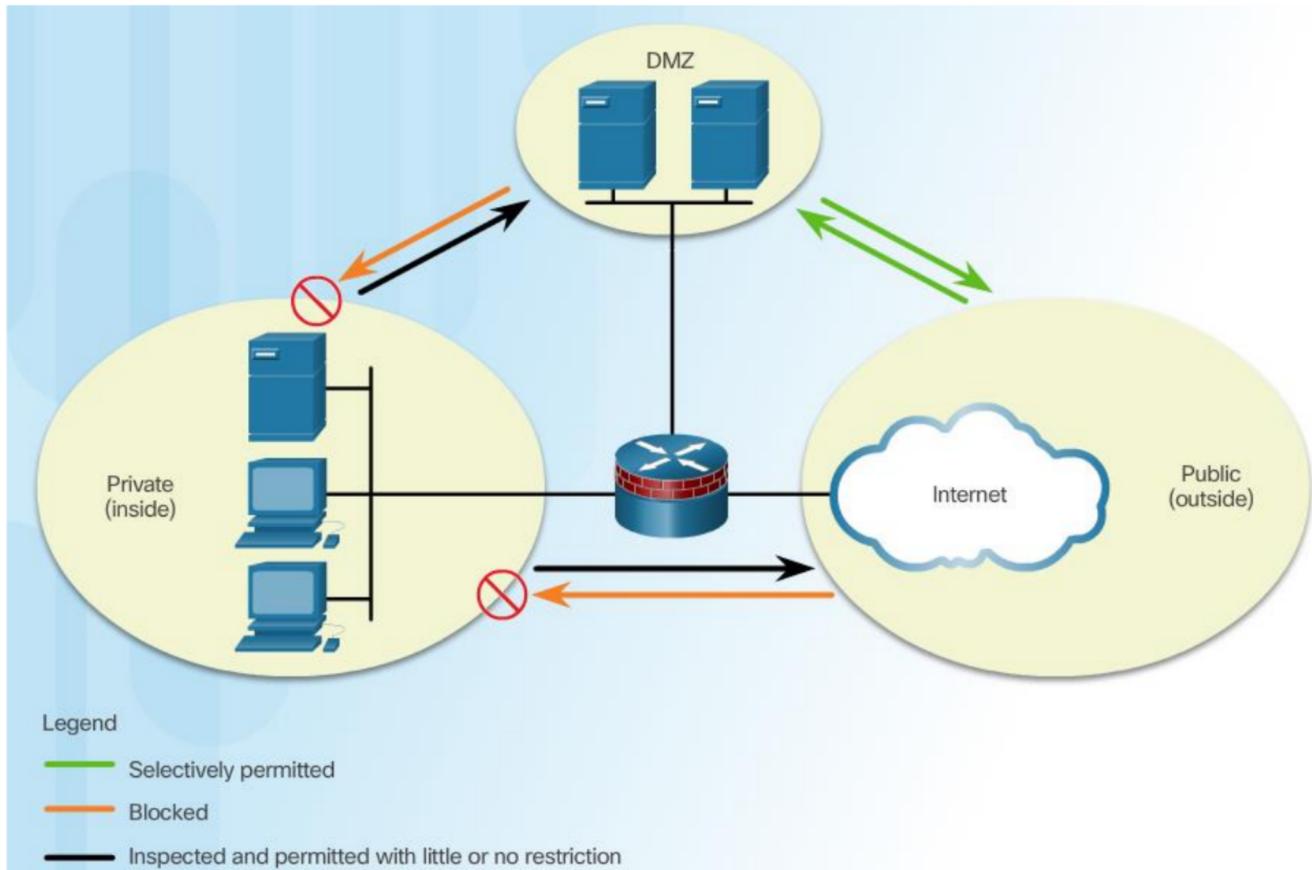
Los Firewalls en el diseño de red



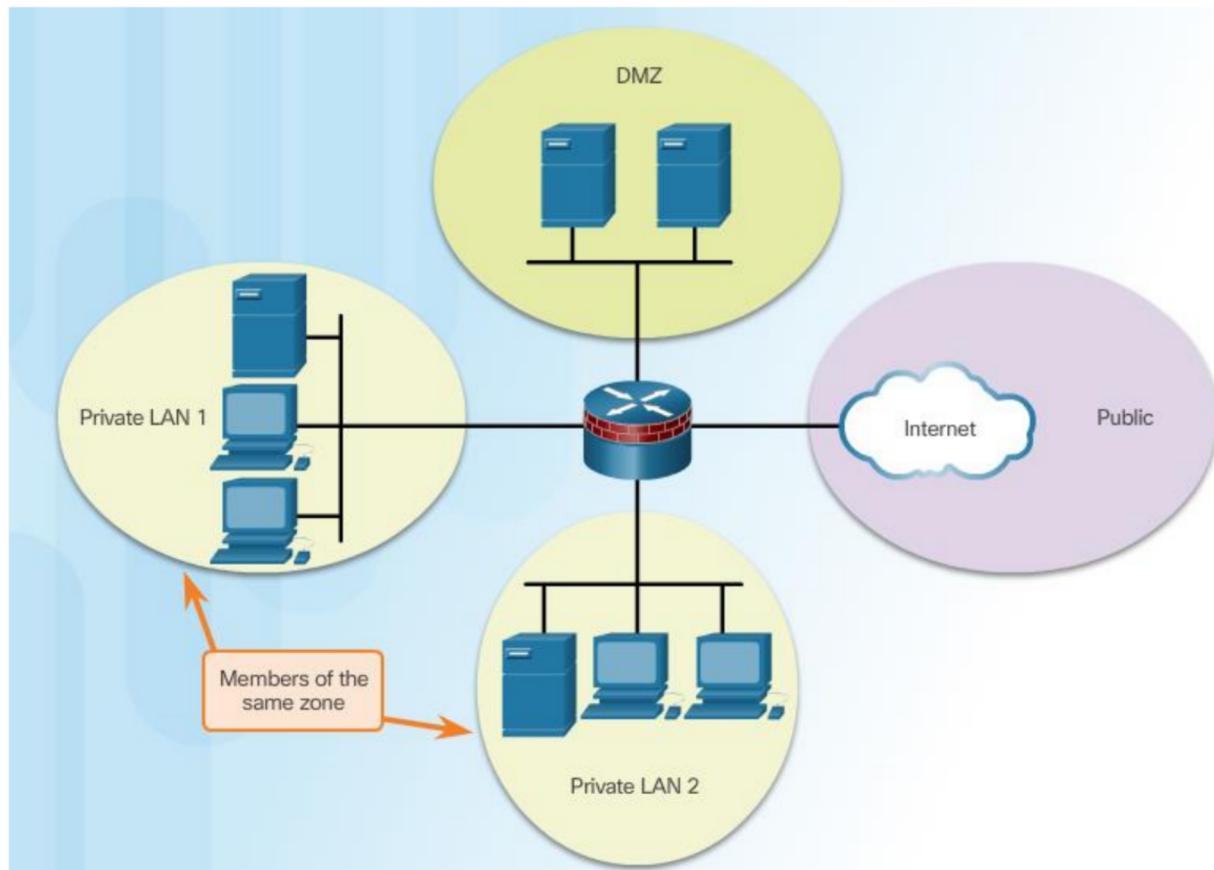
Redes internas y redes externas



Zonas desmilitarizadas (DMZ's)



Firewalls basados en políticas de zonas (ZPF Zone-Based Policy Firewalls)



Defensa por capas

Consideraciones para la defensa de la red:

- Seguridad de la red core
- Seguridad Perimetral
- Seguridad de los dispositivos finales (End-Points)
- Seguridad de las comunicaciones

Prácticas de seguridad recomendadas en los Firewalls:

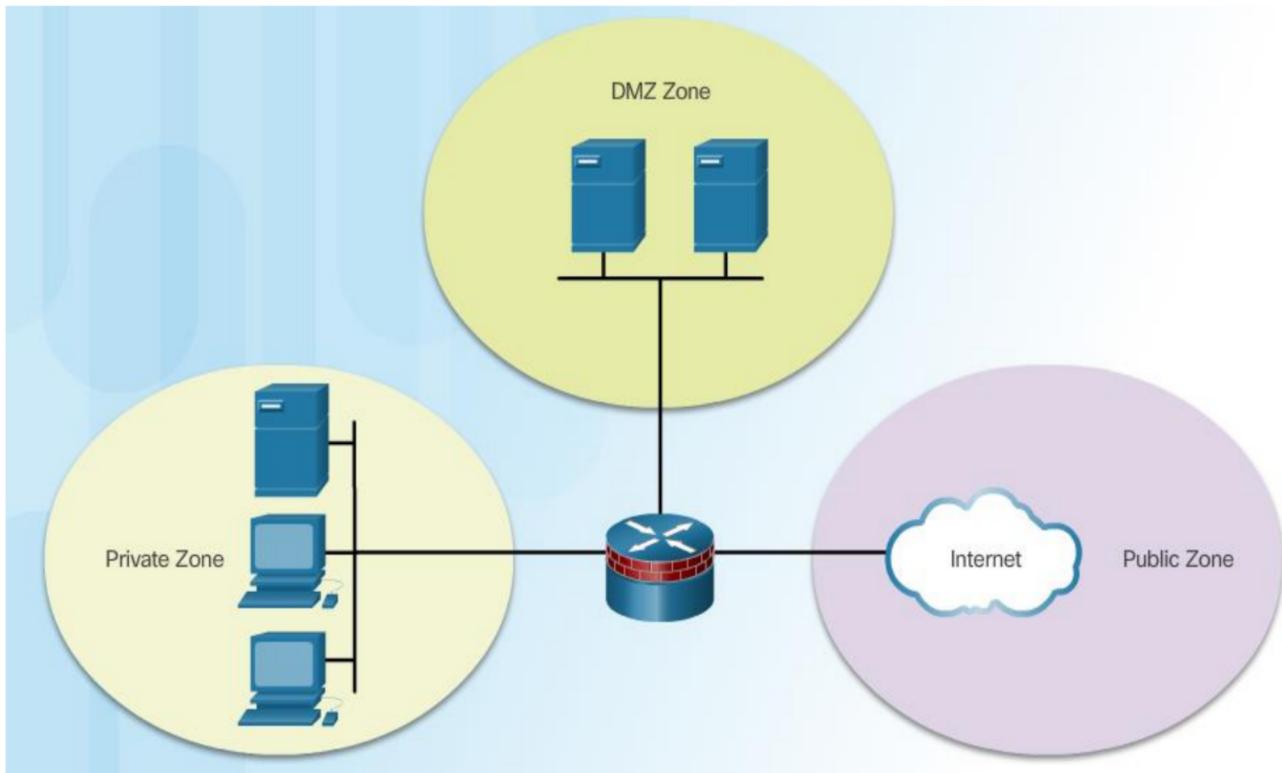
- Posición de los Firewalls en el perímetro de seguridad.
- No es prudente confiar exclusivamente en un servidor de seguridad para la seguridad.
- Por defecto denegaremos todo el tráfico. Solo permitiremos los servicios que sean necesarios.
- Asegurarse que el acceso físico al firewall está protegido/controlado.
- Monitorizar los logs del Firewall.
- Gestionar el cambio de administración cuando haya cambios de configuracion en el FW.
- Recuerda que los FW principalmente protegen de los ataques técnicos procedentes del exterior.

Descripción general de los ZPF (Zone-Based Policy Firewalls)



Zonas que define el ZPF

Un ZPF basa su funcionamiento en distinguir distintas zonas, cada una de ellas con un tratamiento específico.



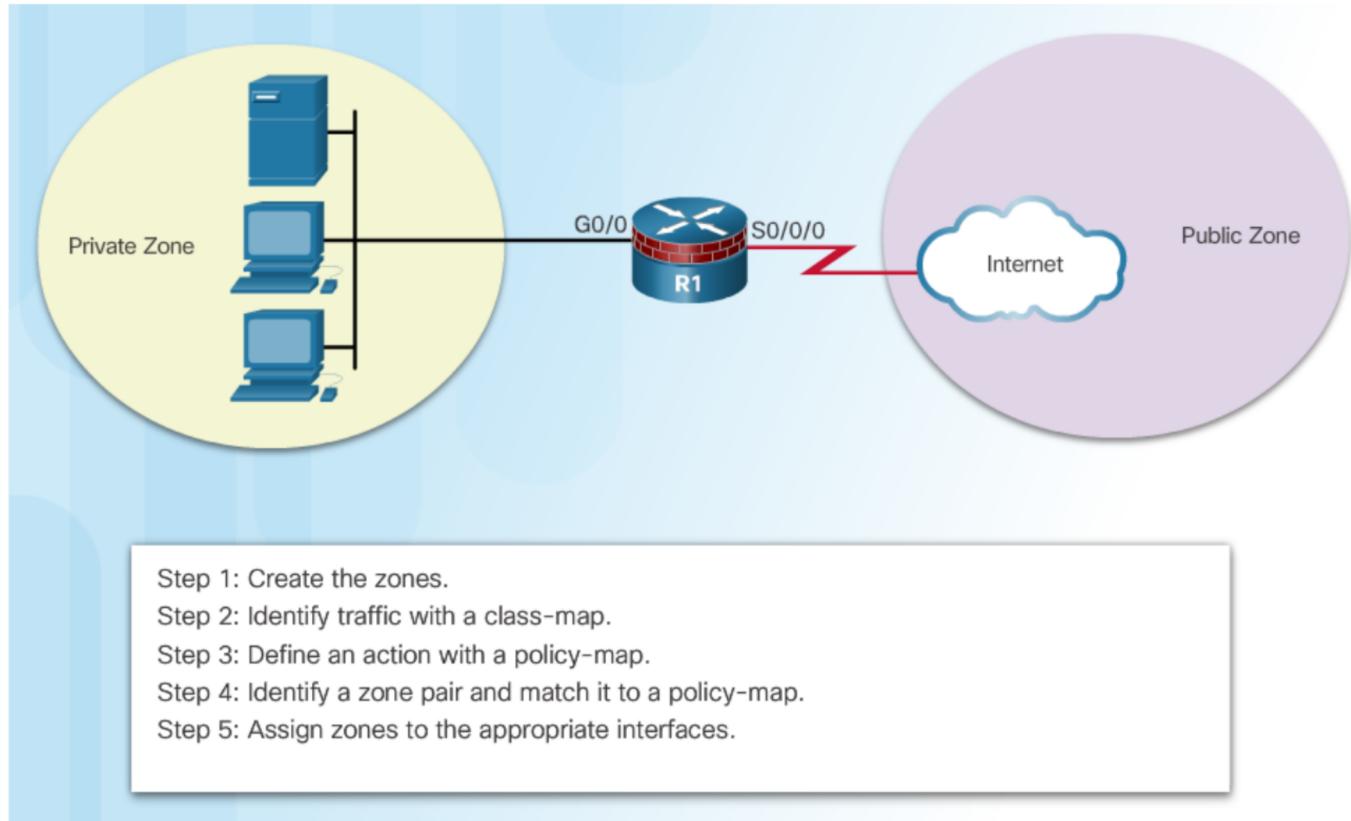
Acciones ZPF

- **Inspect** – Configura la inspección de paquetes de estado(es decir registra las sesiones generadas dentro de la zona interna).
- **Drop** – Similar al “DENY” de las ACL. Existe una opción log que permite registrar los paquetes que son rechazados.
- **Pass** - Similar al “PERMIT” de las ACL. La acción pass no hace un seguimiento del estado de las conexiones o sesiones dentro de los paquetes.

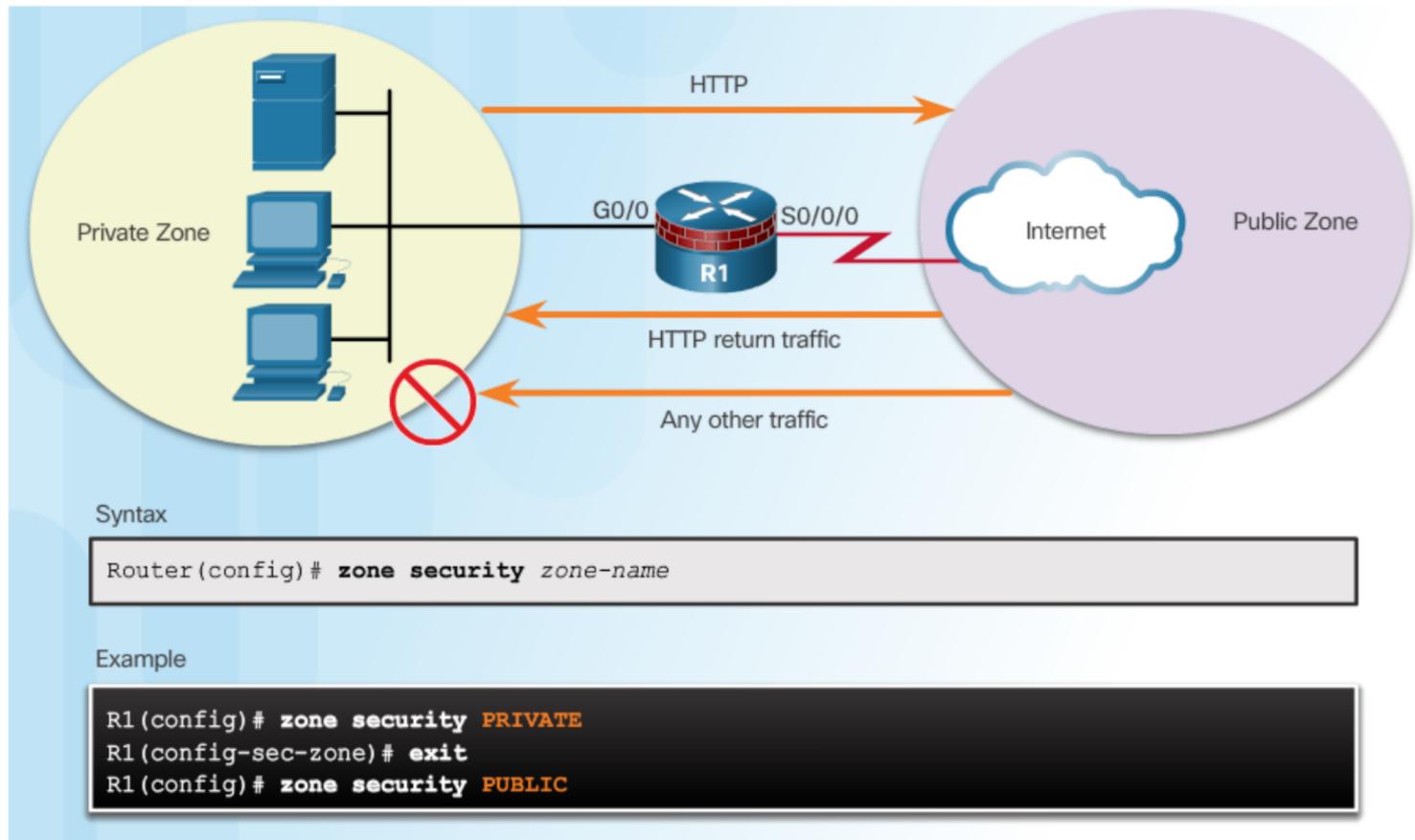
Pasos para diseñar un ZPF

1. Crear las zonas
2. Identificar el tipo de tráfico con un mapa de tipos (class-map)
3. Crear una política según la cual al tráfico identificado por el class-map le aplico una acción (inspect / drop / pass). Las políticas siempre se aplican a pares de zonas (más concretamente a la frontera entre un par de zonas).
4. Crear un par de zonas al que aplicar la política (policy-map)
5. Asignar interfaces físicas a las zonas que me he creado en el paso 1.

Configuración ZPF



Paso 1: Crear Zonas



Syntax

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

Example

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

Paso 2: Identificar Trafico

Sintaxis del comando
class-map

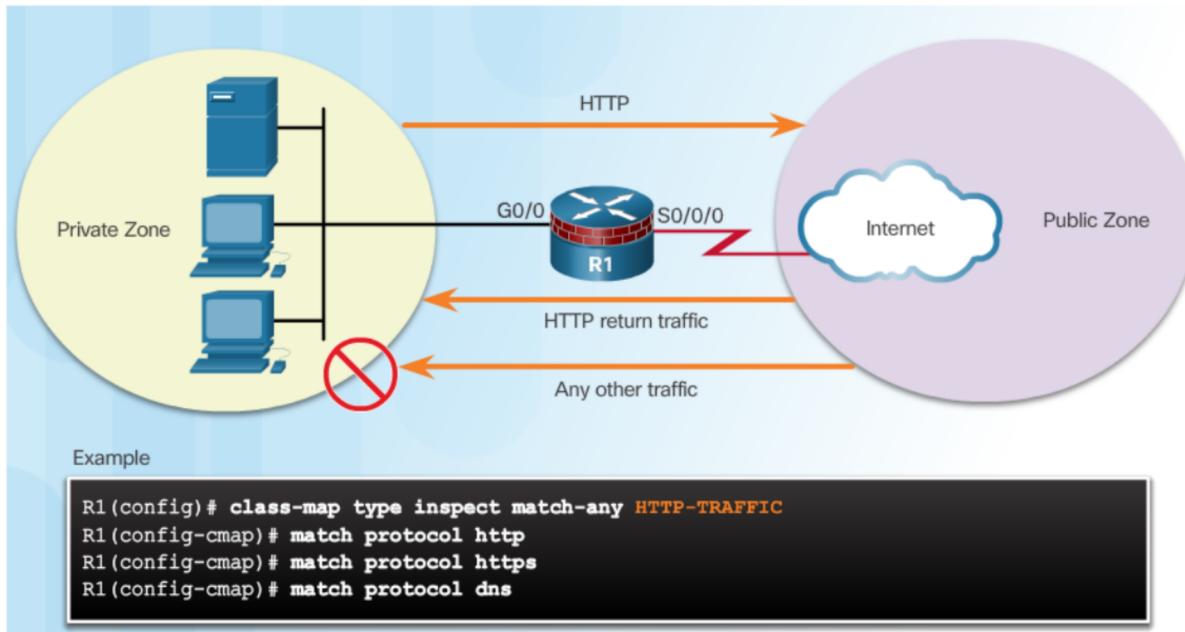
Router(config)# class-map type inspect [match-any match-all] class-map-name	
Parameter	Description
match-any	Packets must meet one of the match criteria to be considered a member of the class.
match-all	Packets must meet all of the match criteria to be considered a member of the class.
class-map-name	Name of the class-map used to configure the policy for the class in the policy-map.

Sintaxis de Sub-
Configuracion del
Comando
class-map

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	
Parameter	Description
match access-group	Configures the match criteria for a class-map based on the specified ACL number or name.
match protocol	Configures the match criteria for a class-map based on the specified protocol.
match class-map	Uses another class-map to identify traffic.

Paso 2: Identificacion del Trafico (Cont.)

Ejemplo de la configuración del comando `class-map`



Paso 3: Definir una Accion

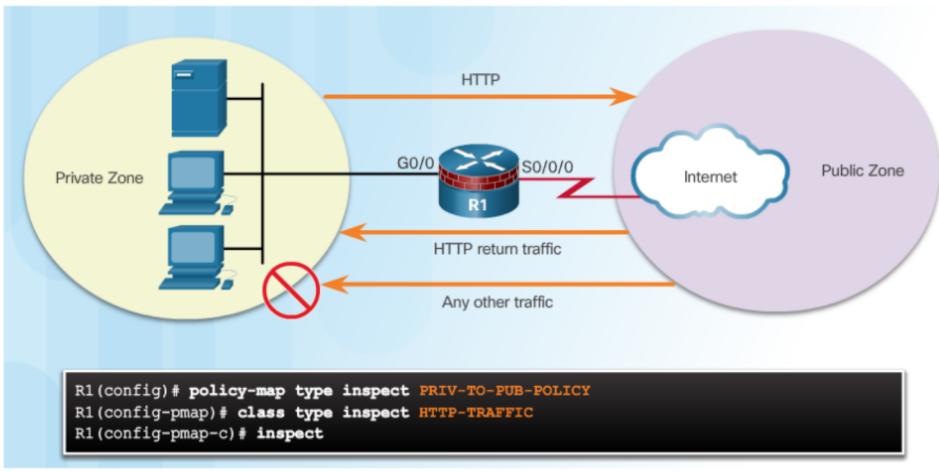
```
Router(config)# policy-map type inspect policy-map-name  
Router(config-pmap)# class type inspect class-map-name  
Router(config-pmap-c)# { inspect | drop | pass }
```

Sintaxis del comando
policy-map

Parameter	Description
inspect	An action that offers statebased traffic control. The router maintains session information for TCP and UDP and permits return traffic.
drop	Discards unwanted traffic
pass	A stateless action the allows the router to forward traffic from one zone to another

Ejemplo de
configuración del
comando

policy-map



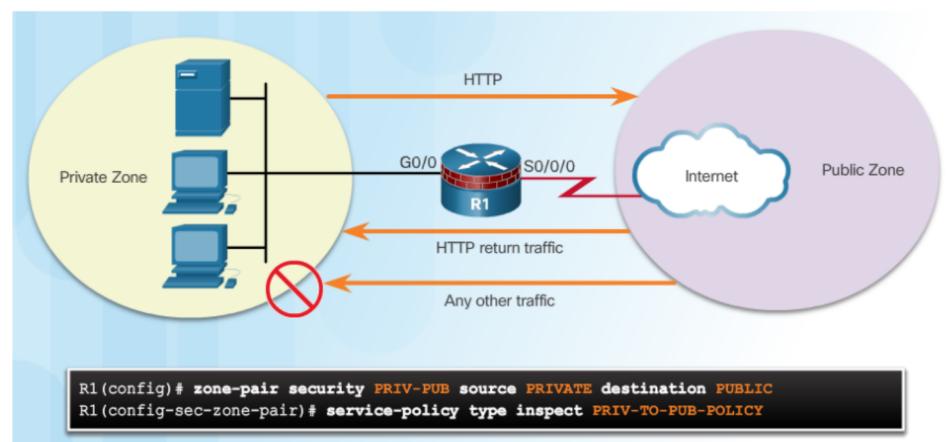
Paso 4: Identificar un par de zonas y asociarle una política

Sintaxis del comando:

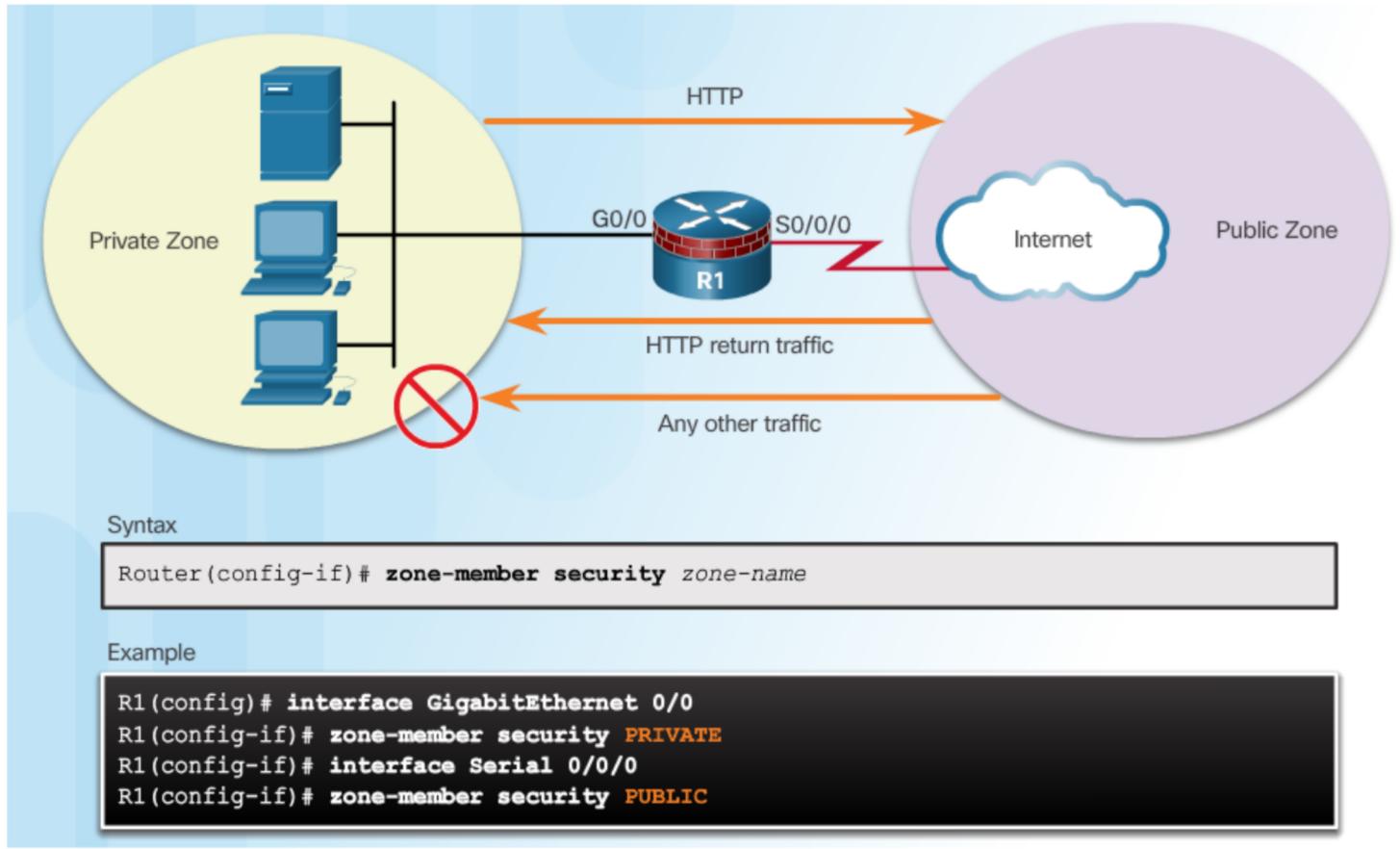
zone-pair y
service-policy

<pre>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</pre>	
Parameter	Description
source source-zone-name	Specifies the name of the zone from which traffic is originating.
destination destination-zone-name	Specifies the name of the zone to which traffic is destined.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from the router itself.

Ejemplo de configuración de
service-policy



Paso 5: Asignar Zonas a las Interfaces



Cómo comprobar la configuración del ZPF

- show run | begin class-map
- show policy-map type inspect zone-pair sessions
- show class-map type inspect
- show zone security
- show zone-pair security
- show policy-map type inspect

Consideraciones en la configuración del ZPF

- No se aplica ningún filtro para el tráfico intra-zone
- Sólo se permite que una interfaz pertenezca a una única zona.
- No puede existir en la misma interfaz un FW ZPF y un FW clásico.
- El tráfico entre una interfaz asignada a una zona y otra interfaz que no está asignada a ninguna zona se deniega.
- Sólo el tráfico permitido es reenviado entre zonas.
- El tráfico destinado a la SELF-ZONE no se filtra (SELF-ZONE es la zona a la que pertenece por defecto el tráfico que se crea en el propio Firewall)

Ejemplo de configuración de ZPF en Packet Tracer, paso a paso

Ejemplo de configuración consistente en inspeccionar el tráfico que va de la zona externa a la zona dmz para los protocolos HTTP y FTP

----- 1----- Crear las zonas

```
R1(config)# zone security PRIVADA
```

```
R1(config-sec-zone)# zone security PUBLICA
```

```
R1(config-sec-zone)# zone security DMZ
```

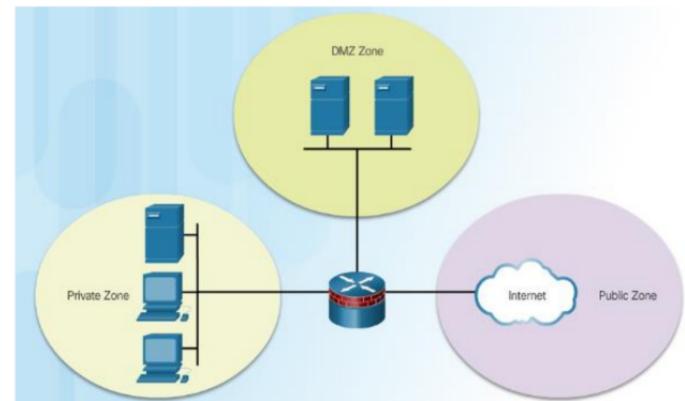
-----2---- Seleccionar tráfico (crear class-map)

```
R1(config)# class-map type inspect CMAP_publica_dmz
```

```
R1(config-cmap)# match protocol HTTP
```

```
R1(config-cmap)# match protocol FTP
```

```
R1(config-cmap)# exit
```



----3---- Crear una política según la cual al tráfico identificado por el class-map le aplico una acción (inspect / drop / pass). Las políticas siempre se aplican a pares de zonas (más concretamente a la frontera entre un par de zonas).

```
R1(config)# policy-map type inspect PMAP-publica-dmz
```

```
R1(config-pmap)# class type inspect CMAP-publica-dmz
```

```
R1(config-pmap-c)# inspect      (drop / inspect / pass, en este caso me piden inspeccionar que es inspect)
```

```
R1(config-cmap-c)# exit
```

```
R1(config-cmap)# exit
```

----4---- Crear un par de zonas al que aplicar la política (policy-map)

```
R1(config)# zone-pair security zp-publica-dmz source PUBLICA destination DMZ
```

```
R1(config-sec-zone-pair)# service-policy type inspect PMAP-publica-dmz
```

----5---- Asignar interfaces físicas a las zonas que me he creado en el paso 1.

```
R1(config)# interface Fa0/0
R1(config-if)# zone-member security PRIVADA
R1(config-if)# interface Fa0/1
R1(config-if)# zone-member security DMZ
R1(config-if)# interface ser0/0/0
R1(config-if)# zone-member security PUBLICA
```