Preguntas iptables

GSyC, Universidad Rey Juan Carlos

5 de marzo de 2021

En la figura 1 se muestra la conexión de dos pequeñas empresas a Internet a través de un proveedor de servicios de Internet (ISP). Estas entidades quedan representadas en la figura de la siguiente forma:

- Empresa1: tiene las siguientes máquinas `e1-pc1` y `e1-pc2` que pertenecen a una subred privada, `e1-pc3` y `e1-pc4` que pertenecen a una zona DMZ y el *router firewall* `e1-fw`.
- Empresa2: tiene las siguientes máquinas `e2-pc1`, `e2-pc2` que pertenecen a una subred privada y el *router firewall* `e2-fw`.
- ISP: tiene un único *router* `isp-r1`.
- Internet: tiene las siguientes máquinas `i-pc1`, `i-pc2` y los siguientes *routers* `i-r1` y `i-r2`.

Las máquinas `e1-fw` y `e2-fw` están funcionando como *firewalls* a los que se sabe que se les ha configurado únicamente las siguientes reglas:

- Políticas por defecto para las cadenas de entrada y reenvío (`INPUT` y `FORWARD`) configuradas para **descartar** paquetes.
- Política por defecto para la cadena de salida (`OUPUT`) configurada para **aceptar** paquetes.

---

1. Partiendo de la situación inicial, se ha realizado una configuración tanto en la tabla `nat` como en la tabla `filter` en `e2-fw` para permitir la siguiente comunicación:

```
e2-fw~:# cat /proc/net/ip_conntrack
tcp      6 431933 ESTABLISHED src=20.0.6.20 dst=20.0.2.1  sport=36303 dport=7     packets=4 bytes=221
                              src=10.0.0.20 dst=20.0.6.20 sport=7     dport=36303 packets=3 bytes=169 [ASSURED]
```

   Las reglas definidas en la tabla `filter` de `e2-fw` no son objeto de esta pregunta.

   Con respecto a la tabla `nat` de `e2-fw` se sabe que se han definido las siguientes reglas:

   - Regla1:

     ```
     iptables -t nat -A PREROUTING -p tcp --dport 7 -s 20.0.6.20 -d 20.0.2.1 -j DNAT --to-destination 10.0.0.20
     ```

   - Regla2:

     ```
     iptables -t nat -A POSTROUTING -p tcp --sport 7 -s 10.0.0.20 -d 20.0.6.20 -j SNAT --to-source 20.0.2.1
     ```

   Justo después de mostrar la información anterior de `/proc/net/ip_conntrack`, se consulta la tabla `nat`de `e2-fw`. Indica cuántas veces indicará dicha tabla que se ha aplicado cada una de esas reglas:

   (A) Indicará que se ha aplicado la Regla1 4 veces y la Regla2 3 veces.

   (B) Indicará que se ha aplicado la Regla1 3 veces y la Regla2 4 veces.

   (C) Indicará que se ha aplicado la Regla1 1 vez y que no se ha aplicado la Regla2.

   (D) Indicará que se ha aplicado la Regla1 4 veces y que no se ha aplicado la Regla2.

2. Partiendo de la configuración inicial se consulta la tabla `filter` de `e1-fw`:

```
Chain INPUT (policy DROP 2 packets, 168 bytes)
pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2 packets, 168 bytes)
pkts bytes target     prot opt in     out     source               destination
```

Indica cuál de las siguientes situaciones explicaría el contenido de la tabla anterior:

(A) `e1-fw` ha reenviado 2 paquetes de `e1-pc4` hacia un pc de Internet y ha reenviado 2 paquetes desde ese pc de Internet dirigidos a `e1-pc4`.

(B) `e1-fw` ha reenviado 2 paquetes de `e1-pc4` hacia un pc de Internet y ha descartado 2 paquetes desde ese pc de Internet dirigidos a `e1-pc4`.

(C) `e1-fw` ha enviado 2 paquetes hacia un pc de Internet y ha descartado 2 paquetes desde un pc de Internet dirigidos a `e1-fw`.

(D) `e1-fw` no ha recibido, enviado, ni reenviado ningún paquete.

3. Partiendo de la situación inicial, se ha realizado una configuración adicional en `e1-fw` para permitir las siguientes comunicaciones:

```
e1-fw:~# cat /proc/net/ip_conntrack
tcp      6 431946 ESTABLISHED src=10.0.0.20 dst=20.0.6.20 sport=7000 dport=8000 packets=3 bytes=169 \
         src=20.0.6.20 dst=20.0.1.1 sport=8000 dport=7000 packets=2 bytes=112 [ASSURED] mark=0 use=1
tcp      6 431943 ESTABLISHED src=20.0.4.10 dst=20.0.0.40 sport=7000 dport=8000 packets=3 bytes=169 \
         src=20.0.0.40 dst=20.0.4.10 sport=8000 dport=7000 packets=2 bytes=112 [ASSURED] mark=0 use=1
```

Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas se han tenido que añadir en `e1-fw` para que dichas comunicaciones hayan podido tener lugar:

(A)
```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -p tcp --dport 8000 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth2 -s 10.0.0.20 -p tcp --dport 8000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(B)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 8000 -j DNAT --to-destination 10.0.0.20
iptables -t filter -A FORWARD -o eth2 -d 10.0.0.20 -p tcp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 8000 -j DNAT --to-destination 20.0.0.40
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -p tcp --dport 8000 -j SNAT --to-source 20.0.1.1
```

(D)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 8000 -j DNAT --to-destination 20.0.0.40
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -p tcp --dport 8000 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -j ACCEPT
```

4. Partiendo de la configuración inicial descrita del escenario, se ha aplicado en `e1-fw` **exclusivamente** la siguiente configuración:

```
iptables -t filter -A FORWARD -s 10.0.0.10 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -s 20.0.0.30 -p tcp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Indica cuál de las siguientes afirmaciones es correcta:

(A) La configuración:
- NO permite a un cliente TCP lanzado en la zona Internet intercambiar mensajes con un servidor lanzado en `e1-pc3` escuchando en el puerto 7000 TCP
- NO permite a un cliente TCP lanzado en `e1-pc1` intercambiar mensajes con un servidor lanzado en la zona Internet escuchando en el puerto 7000 TCP.

(B) La configuración:
- SÍ permite a un cliente TCP lanzado en la zona Internet intercambiar mensajes con un servidor lanzado en `e1-pc3` escuchando en el puerto 7000 TCP
- NO permite a un cliente TCP lanzado en `e1-pc1` intercambiar mensajes con un servidor lanzado en la zona Internet escuchando en el puerto 7000 TCP.

(C) La configuración:
- SÍ permite a un cliente TCP lanzado en la zona Internet intercambiar mensajes con un servidor lanzado en `e1-pc3` escuchando en el puerto 7000 TCP
- SÍ permite a un cliente TCP lanzado en `e1-pc1` intercambiar mensajes con un servidor lanzado en la zona Internet escuchando en el puerto 7000 TCP.

(D) La configuración:
- NO permite a un cliente TCP lanzado en la zona Internet intercambiar mensajes con un servidor lanzado en `e1-pc3` escuchando en el puerto 7000 TCP
- SÍ permite a un cliente TCP lanzado en `e1-pc1` intercambiar mensajes con un servidor lanzado en la zona Internet escuchando en el puerto 7000 TCP.

5. Partiendo de la situación inicial, se desea permitir, simultáneamente:

- Que las máquinas de Internet puedan intercambiar mensajes con un servidor TCP instalado en `e1-pc2` en el puerto 80
- Que desde el *firewall* `e1-fw` se pueda hacer *ping* a todas las máquinas de la organización.

Indica cuál de los siguientes conjuntos de reglas se han tenido que añadir en `e1-fw` para que dichas comunicaciones hayan podido tener lugar:

(A)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
iptables -t filter -A FORWARD -i eth0 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A OUTPUT -o eth1 -j ACCEPT
iptables -t filter -A OUTPUT -o eth2 -j ACCEPT
```

(B)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
iptables -t filter -A FORWARD -i eth0 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth1 -j ACCEPT
iptables -t filter -A INPUT -i eth2 -j ACCEPT
```

(C)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
iptables -t filter -A INPUT -i eth1 -j ACCEPT
iptables -t filter -A INPUT -i eth2 -j ACCEPT
```

(D)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A OUTPUT -i eth1 -j ACCEPT
iptables -t filter -A OUTPUT -i eth2 -j ACCEPT
```

6. Partiendo de la configuración inicial descrita del escenario, se ha aplicado en `e1-fw` **exclusivamente** la siguiente configuración:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -j DROP
iptables -t filter -A FORWARD -d 20.0.0.30 -p tcp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Indica cuál de las siguientes afirmaciones es correcta:

(A) La configuración permite a cualquier máquina de Internet intercambiar mensajes con un servidor TCP instalado en `e1-pc3` en el puerto 7000.

(B) La configuración permite a un cliente TCP instalado en `e1-pc3` en el puerto 7000 comunicarse con servidores lanzados en cualquier máquina de Internet en cualquier puerto.

(C) La configuración permite a un cliente TCP instalado en `e1-pc3` en cualquier puerto comunicarse con servidores lanzados en cualquier máquina de Internet en el puerto 7000.

(D) El resto de afirmaciones son falsas.

7. Se desea conseguir en la Empresa1 una configuración que cumpla, simultáneamente:

   a) Cualquiera de los PCs de la Empresa1 debe poder acceder a servidores TCP de cualquier máquina de Internet

   b) Sólo `e1-pc3` y `e1-pc4` deben poder acceder a servidores UDP de cualquier máquina de Internet.

   c) Cualquier máquina de Internet debe poder comunicarse con un servidor de HTTP (puerto 80) arrancado en `e1-pc3` y con un servidor de HTTP (puerto 80) arrancado en `e1-pc4`.

   d) Ninguna máquina de Internet debe poder comunicarse con ningún otro servidor TCP ni UDP de la Empresa1.

   Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas en `e1-fw` lo permite:

(A)
```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -p udp -j DROP
iptables -t filter -A FORWARD -i eth0 -o eth2 -p udp -m state --state RELATED,ESTABLISHED -j DROP
iptables -t filter -A FORWARD -i eth2 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(B)
```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth2 -o eth0 -p UDP -j DROP
iptables -t filter -A FORWARD -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C)
```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -p udp -j DROP
iptables -t filter -A FORWARD -i eth0 -o eth2 -p udp -m state --state RELATED,ESTABLISHED -j DROP
iptables -t filter -A FORWARD -i eth2 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1 -p tcp --dport 80 -j DNAT --to-destination 20.0.0.30:80
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1 -p tcp --dport 81 -j DNAT --to-destination 20.0.0.40:80
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(D)
```
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -p udp -j DROP
iptables -t filter -A FORWARD -i eth0 -o eth2 -p udp -m state --state RELATED,ESTABLISHED -j DROP
iptables -t filter -A FORWARD -i eth2 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

8. Partiendo de la situación inicial,en un momento dado se ejectutan en e1-fw y e2-fw las siguientes órdenes, respectivamente:

```
e1-fw:~# cat /proc/net/ip_conntrack
tcp      6 431990 ESTABLISHED src=20.0.2.1 dst=20.0.0.40 sport=46162 dport=11000 packets=4 bytes=231 \
         src=20.0.0.40 dst=20.0.2.1 sport=11000 dport=46162 packets=3 bytes=164 [ASSURED] mark=0 use=1

e2-fw:~# cat /proc/net/ip_conntrack
tcp      6 431967 ESTABLISHED src=10.0.0.10 dst=20.0.0.40 sport=46162 dport=11000 packets=4 bytes=231 \
         src=20.0.0.40 dst=20.0.2.1 sport=11000 dport=46162 packets=3 bytes=164 [ASSURED] mark=0 use=1
```

Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas se han tenido que añadir en e1-fw y e2-fw para que dichas comunicaciones hayan podido tener lugar:

(A) En e1-fw:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.2.1
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(B) En e1-fw:

```
iptables -t nat -A PREROUTING -d 20.0.1.1 -p tcp --dport 11000 -j DNAT --to-destination 20.0.0.40:11000
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C) En e1-fw:

```
iptables -t nat -A PREROUTING -d 20.0.1.1 -p tcp --dport 11000 -j DNAT --to-destination 20.0.0.40:11000
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.2.1
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(D) En e1-fw:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t filter -A OUTPUT -o eth0 -p tcp -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

9. Partiendo de la configuración inicial, se establece en e1-fw el siguiente conjunto ordenado de reglas adicionales:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.1.1
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.10:80
iptables -t filter -A FORWARD -i eth2 -o eth0 -p udp -j DROP
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p udp -j ACCEPT
```

Indica cuál de las siguientes afirmaciones es correcta:

(A) Cualquiera de los pcs de la Empresa1 puede ejecutar un cliente que puede comunicarse con cualquier servidor TCP o UDP en cualquier máquina de Internet.

(B) Cualquier máquina de Internet puede ejecutar un cliente TCP capaz de comunicarse con un servidor TCP escuchando en el puerto 80 en e1-pc1.

(C) Cualquier máquina de Internet puede ejecutar un ping para comprobar si está encendido e1-fw.

(D) El resto de afirmaciones son falsas.

10. Partiendo de la configuración inicial, se desea que `e2-fw` permita cumplir simultáneamente las siguientes reglas:

   a) Cualquier máquina de Internet puede acceder a un servidor UDP escuchando en el puerto 1000 de `e2-pc1`.

   b) Desde `e2-fw` se puede ejecutar un `ping` para comprobar si está encendida cualquier máquina de Internet.

   Indica cuál de los siguientes conjuntos de reglas se tienen que añadir en `e2-fw` para poder cumplir, simultáneamente:

(A)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -d 20.0.2.1 -p icmp -j ACCEPT
```

(B)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -d 10.0.0.10 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
```

(C)
```
iptables -t nat -A POSTROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
```

(D)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -o eth0 -p icmp -j ACCEPT
```

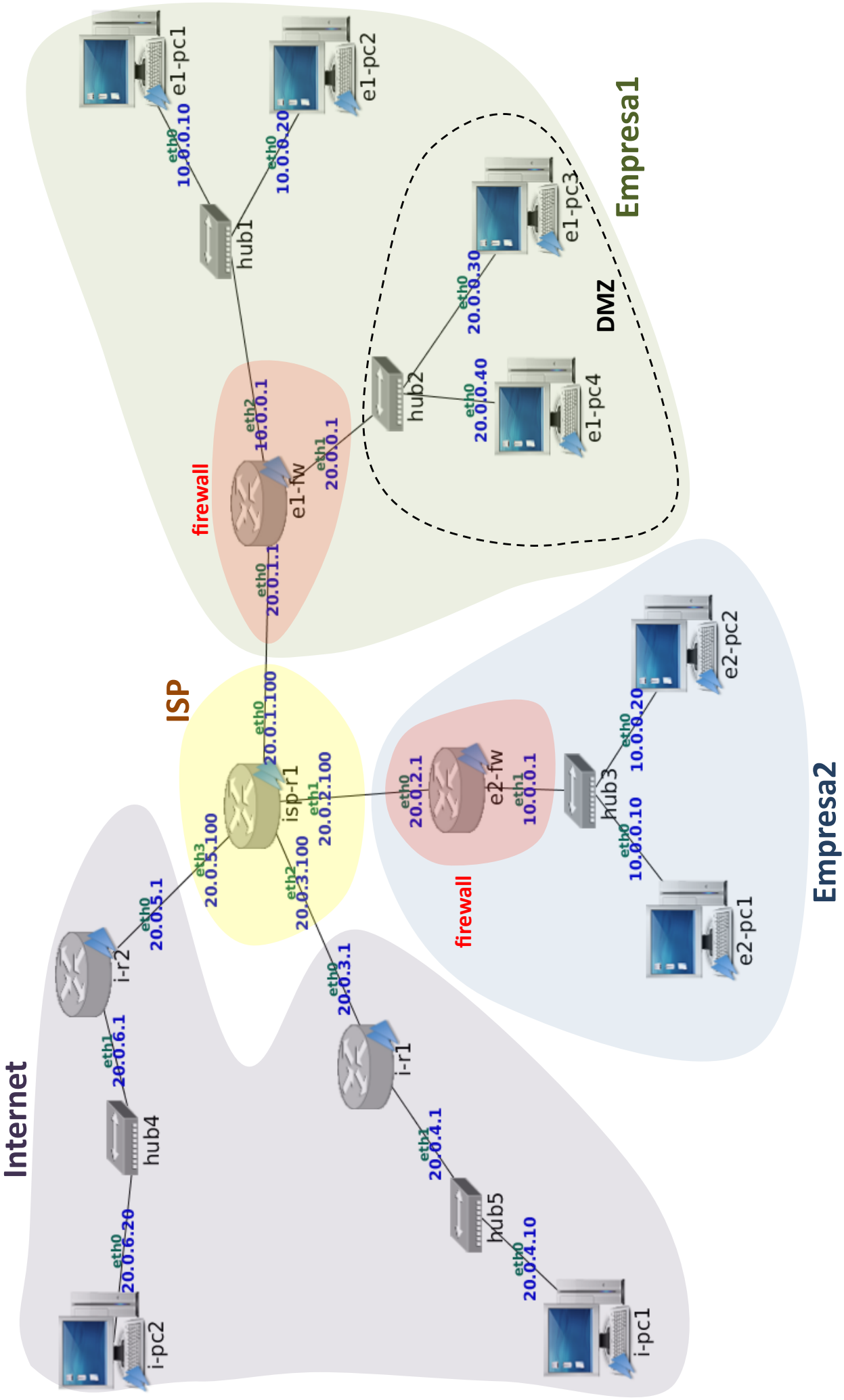

Figura 1: Seguridad