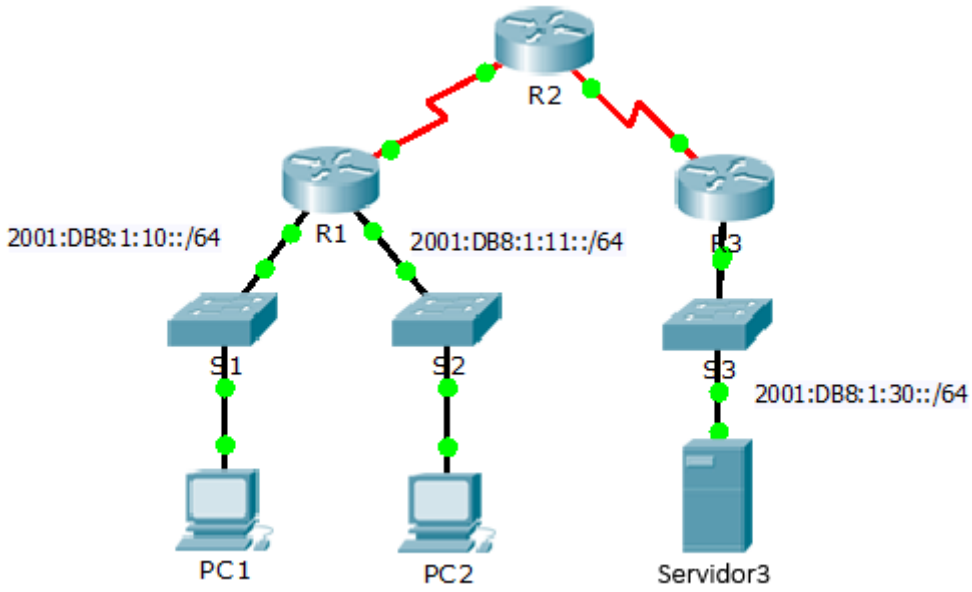
# Packet Tracer: configuración de ACL de IPv6

## Topología




## Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección/Prefijo IPv6 | Gateway predeterminado |
|---|---|---|---|
| Servidor3 | NIC | 2001:DB8:1:30::30/64 | FE80::30 |

## Objetivos

**Parte 1: configurar, aplicar y verificar una ACL de IPv6**

**Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6**

# Parte 1: configurar, aplicar y verificar una ACL de IPv6

Según los registros, una computadora en la red 2001:DB8:1:11::0/64 actualiza repetidamente su página web, lo que ocasiona un ataque por denegación de servicio (DoS) contra el **Servidor3**. Hasta que se pueda identificar y limpiar el cliente, debe bloquear el acceso HTTP y HTTPS a esa red mediante una lista de acceso.

### Paso 1: configurar una ACL que bloquee el acceso HTTP y HTTPS.

Configure una ACL con el nombre **BLOCK_HTTP** en el **R1** con las siguientes instrucciones.

a. Bloquear el tráfico HTTP y HTTPS para que no llegue al **Servidor3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Permitir el paso del resto del tráfico IPv6.

### Paso 2: aplicar la ACL a la interfaz correcta.

Aplique la ACL a la interfaz más cercana al origen del tráfico que se desea bloquear.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

### Paso 3: verificar la implementación de la ACL.

Realice las siguientes pruebas para verificar que la ACL funcione de manera correcta:

- Abra el **navegador web** de la **PC1** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. Debería aparecer el sitio web.
- Abra el **navegador web** de la **PC2** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. El sitio web debería estar bloqueado.
- Haga ping de la **PC2** a 2001:DB8:1:30::30. El ping debería realizarse correctamente.

## Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Ahora, en los registros se indica que su servidor recibe pings de diversas direcciones IPv6 en un ataque por denegación de servicio distribuido (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

### Paso 1: crear una lista de acceso para bloquear ICMP.

Configure una ACL con el nombre **BLOCK_ICMP** en el **R3** con las siguientes instrucciones:

a. Bloquear todo el tráfico ICMP desde cualquier host hasta cualquier destino.

b. Permitir el paso del resto del tráfico IPv6.

### Paso 2: aplicar la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier origen. Para asegurar que el tráfico ICMP esté bloqueado, independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL lo más carca posible del destino.

### Paso 3: verificar que la lista de acceso adecuada funcione.

a. Haga ping de la **PC2** a 2001:DB8:1:30::30. El ping debe fallar.

b. Haga ping de la **PC1** a 2001:DB8:1:30::30. El ping debe fallar.

Abra el **navegador web** de la **PC1** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. Debería aparecer el sitio web.