Unknown Title

Esta es una de las prácticas más seguras en la administración de sistemas, conocida como **"Denegación por defecto" (Default Drop)**. En lugar de intentar adivinar qué ataques bloquear, cierras todas las puertas y solo abres las que realmente necesitas.

Para implementar esto en `iptables`, el comando clave es definir la **Policy** de la cadena de entrada (`INPUT`).

Cómo configurar la política por defecto

Para bloquear todo el tráfico entrante de forma predeterminada, debes ejecutar:

```
sudo iptables -P INPUT DROP
```

⚠️ ¡Cuidado antes de ejecutarlo!

Si estás conectado por **SSH** a un servidor remoto y ejecutas ese comando sin haber permitido antes tu conexión actual, **perderás el acceso al servidor de inmediato** y quedarás bloqueado.

Configuración mínima recomendada

Para que el equipo sea funcional tras aplicar la política de "no dejar entrar nada", generalmente se siguen estos pasos en orden:

1. **Permitir el tráfico de bucle local (loopback):** Necesario para que las aplicaciones internas se comuniquen entre sí.

```
sudo iptables -A INPUT -i lo -j ACCEPT
```

2. **Mantener conexiones ya establecidas:** Permite que las respuestas a peticiones que tú iniciaste (como navegar por una web) puedan entrar.

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT
```

3. **Abrir puertos específicos (Opcional):** Por ejemplo, si necesitas SSH o un servidor Web.

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

4. **Aplicar la política por defecto:**

```
sudo iptables -P INPUT DROP
```

Resumen de Políticas Comunes

Cadena	Política	Descripción
INPUT	`DROP`	Bloquea todo lo que intenta entrar al equipo.
FORWARD	`DROP`	No permite que el equipo actúe como router (seguridad extra).
OUTPUT	`ACCEPT`	Permite que el equipo envíe datos al exterior (común en entornos estándar).

¿Te gustaría que te ayude a redactar un script completo para que estas reglas se mantengan activas incluso después de reiniciar el equipo?