

Linux tambien como Firewall

Boris Quiroz Q.

<http://boris.penguin.cl>

CC by- nc- nd/2.0/cl



Conceptos basicos

- La seguridad no es un problema tecnico.
- Defectos de diseño y/o programacion.
- Ningun sistema es seguro por si mismo.
- Una red sera tan segura como su eslabon mas debil.
- Preguntas clave:
 - ¿Que asegurar?
 - ¿Por que asegurarlo?

¿Que es un firewall?

- Dispositivo capaz de manejar las conexiones que entran y salen de una red.
- Proporciona dos tipos de proteccion:
 - Ataques o accesos no autorizados.
 - Proteccion a la informacion.
- Forwarding de paquetes.

Tipos de firewall

- Firewalls de capa de Red.
 - Filtrado según direcciones de origen y destino.
- Firewalls de capa de Aplicacion.
 - Filtrado basado en protocolos.
- Firewalls de usuario.
- Cisco Pix.
 - Finesse.
 - Algoritmo ASA.

Políticas de Seguridad

- Permitir todo:
 - Filtra lo explícitamente especificado.
 - Fácil de administrar.
 - Poco control de puertos abiertos.
- Denegar todo:
 - Deja pasar solo lo especificado.
 - Administración compleja.
 - Mayor control.

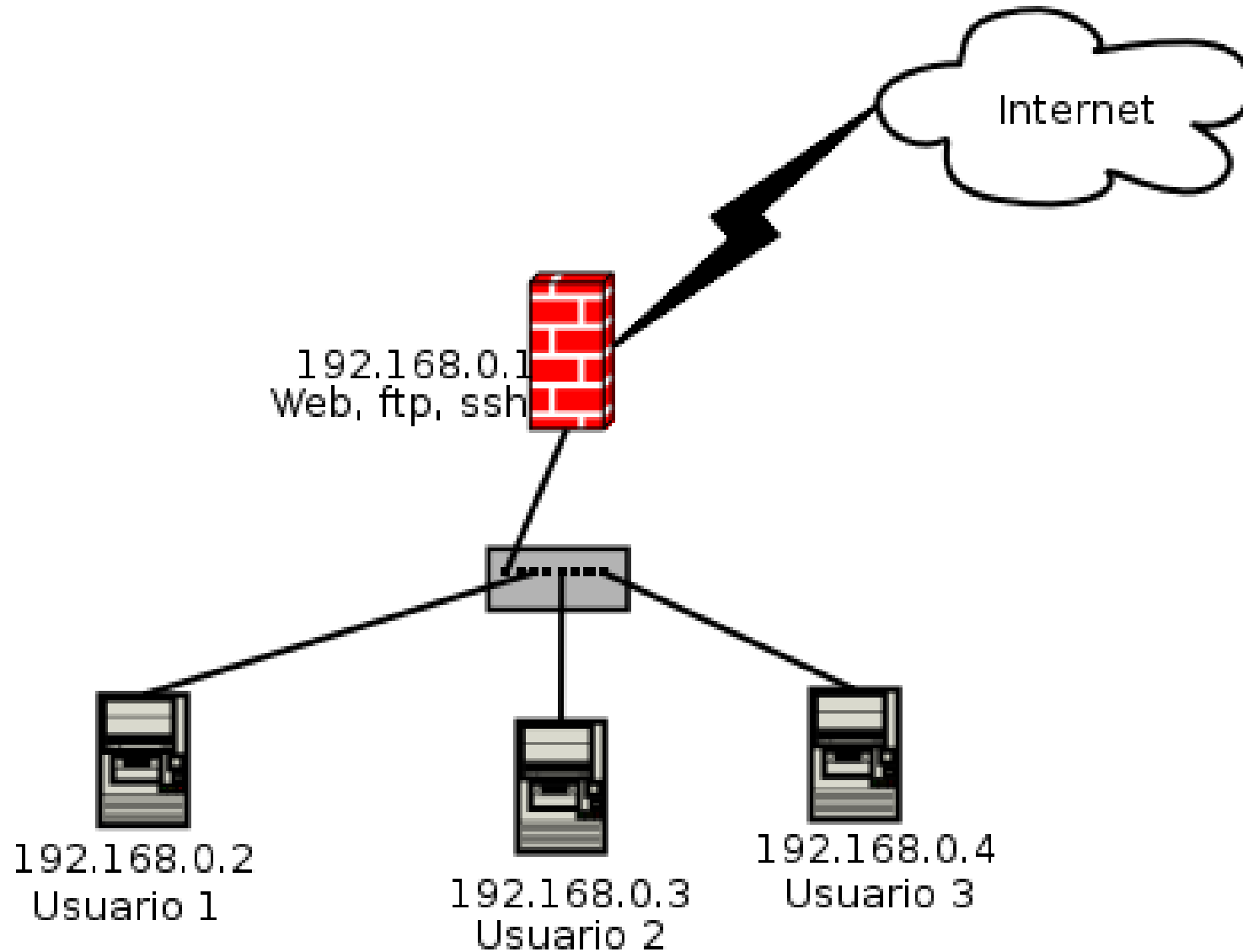
Linux como Firewall

- Puede garantizar un determinado nivel de seguridad.
- Open source, facil de auditar.
- No es necesario esperar un nuevo release.
- Principal herramienta: Iptables.

¿Que es Iptables?

- Herramienta de filtrado y revision TCP/IP.
- Sucesor de Ipchains.
- Desarrollado por Rusty Russell.
- Es parte del modulo Netfilter del kernel 2.4 en adelante.

Ejemplo Practico



Ejemplo Practico

- NAT para permitir a los usuarios acceso a Internet.
- Bloquear ping al firewall.
- Permitir acceso ftp y ssh solo al Usuario 3.
- Bloquear puertos conflictivos de Windows.
- Bloquear salida a Internet por el puerto 23.

Esfuerzos adicionales

- Shorewall:
 - “Iptables made easy”.
- M0n0wall:
 - Basado en FreeBSD.
- Exec Shield:
 - Desarrollado por RedHat, usa bit NX.
- SELinux:
 - Desarrollado por la NSA.

Lo que viene...

- ¿Que pasara con las direcciones cuando llegue ipv6?
- ¿Necesitaremos firewalls?
- ¿Necesitaremos NAT?

¿Preguntas?

