

Nftables-gui

José María Caballero Alba
caballeroalba@gmail.com

In real open source, you have the right to control your own destiny.

15 de abril de 2015

- 1 Problema
- 2 Solución aportada.
- 3 Estudio del arte
- 4 Requisitos
- 5 Diseño
- 6 Implentación
- 7 Trabajo futuro
- 8 Resultados
- 9 Conclusiones

Problema

Nftables es un nuevo framework que sustituye al antiguo iptables. Este nuevo software aun no esta desarrollado al 100 % pero ya es operativo en gran parte de sus funciones.

Problema

- Nftables pretende sustituir a Iptables en un futuro próximo.
- Nueva sintaxis
- Tiene una curva de aprendizaje.
- Aún en desarrollo
- Adaptación en servidores
- Desinterés del usuario

Problema

```
root@LUNA:/home/caballeroalba# nft list table filter -nn
table ip filter {
    chain input {
        type filter hook input priority 0; policy accept;
        ip saddr 192.168.1.0/24 ct state established accept
    }

    chain preroute {
        type filter hook prerouting priority 0; policy accept;
        dnat tcp dport map { 21 : 92.168.1.3, 80 : 192.168.1.2}
    }
}
root@LUNA:/home/caballeroalba#
```

Solución aportada

La solución aporta consistirá en una interfaz gráfica escrita en c y usando ncurses para poder manejar nftables y que de esta manera sea mas fácil su uso. Esto implica una mejora sustancial para aquellas personas que quieran dejar de usar iptables y puedan utilizar nftables con todas las características nuevas haciendo que la pendiente de la curva sea mas liviana.

Solución aportada

- Una interfaz gráfica que nos de la solución a:
 - Curva de aprendizaje
 - Adaptación final
 - Desinterés de usuario

Estudio del arte

Actualmente existen las siguientes aplicaciones que ofrecen una interfaz gráfica:

- Vuurmuur firewall
- Fwbuilder
- Ipmenu
- Easy firewall generator
- Turtle firewall project

Estudio del arte

Software	Facilidad de uso	Vida del proyecto
vuurmuur	3	5(aún en soporte)
ipmenu	5	1(sin soporte)
fwbuilder	4	4(ultima versión 2013)
easy firewall generator	5	1(2005, sin soporte)
turtlefirewall	5	3(ultima versión 2011)

La puntuación va desde 1 a 5, siendo 1 la peor y 5 la mejor

Estudio del arte

El problema viene dado por que ninguno de ellos esta hecho para nftables.

Requisitos

- Crear/borrar tablas de tipo ip, ip6, arp, bridge
- Crear/borrar cadenas de tipo base o personalizadas
- Crear/borrar reglas permitiendo personalizar el filtrado teniendo en cuenta:
 - Procotolo
 - Hook (INPUT, OUTPUT, PREROUTING, FORWARD, POSTROUTING)
 - Ip/red/puerto/interfaz origen y destino
 - Diccionarios
 - Zonas
 - NAT
 - Mapas

Modelo conceptual

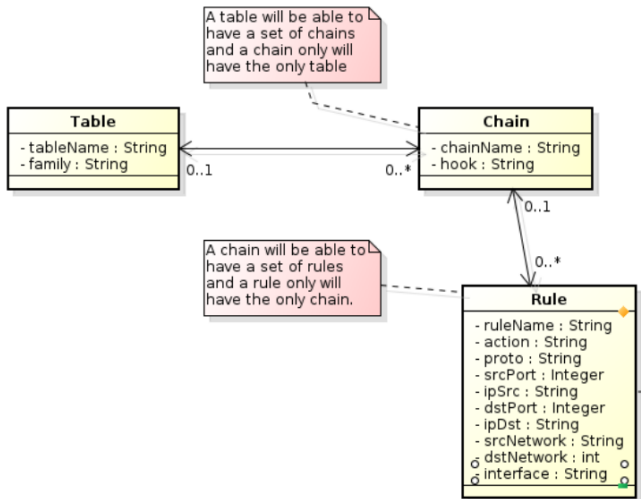


Diagrama navegabilidad

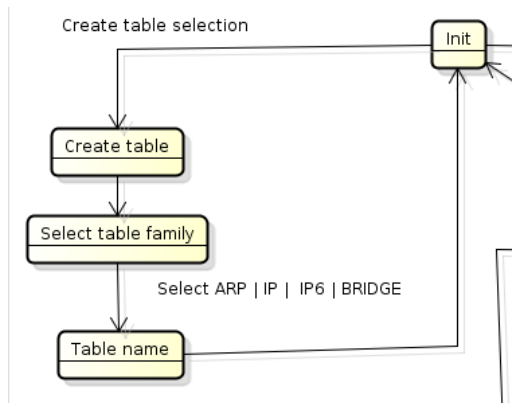


Diagrama navegabilidad

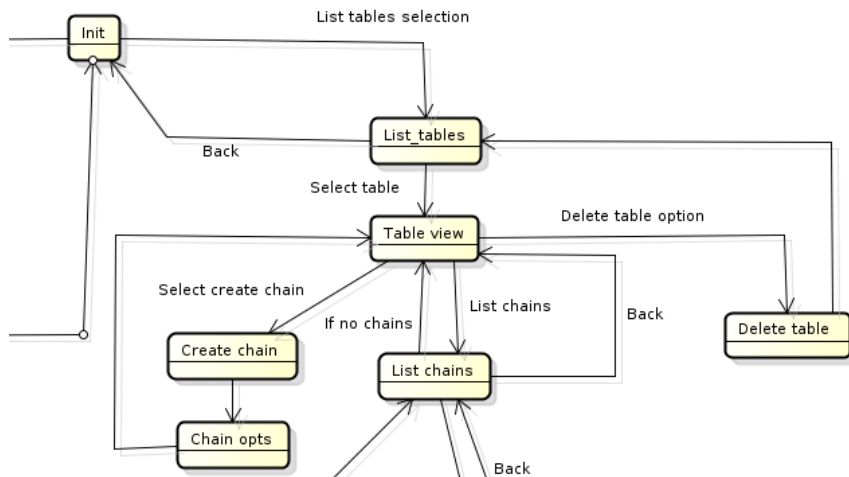
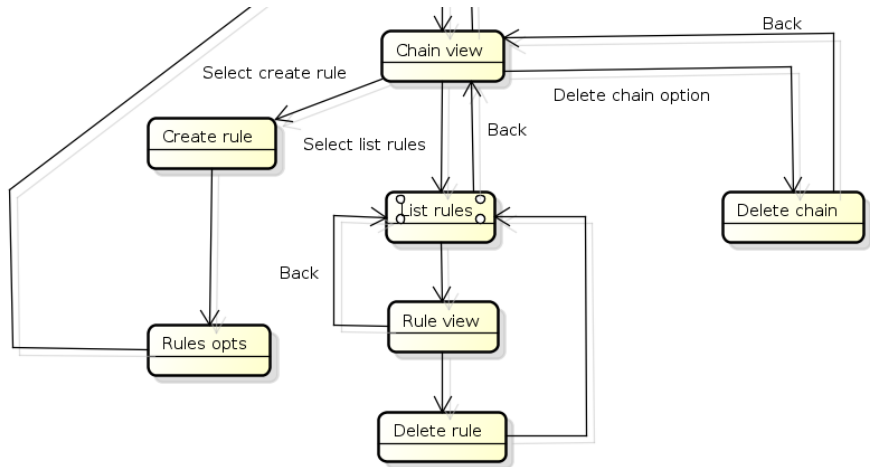


Diagrama navegabilidad



Diseño

Este software se ha llevado a cabo usando el modelo arquitectónico MVC, separando la lógica del software con la presentación al usuario en ncurses. Esto se ha llevado a cabo creando una api que permite mediante una serie de parámetros crear una vista sin que esta sepa de la lógica de negocio de la aplicación.

Implementación

- Lenguaje c
- Librería libncurses
- Utilidad de linea de comandos de espacio de usuario nft (utilidad para interactuar con nftables)
- GNU Build System (Autotools) para la construcción del software
- Git como control de versiones

¿Por que C y libncurses?

- TIOBE declara a C como el mejor lenguaje para programar.
- Ncurses provee una API que permite al programador escribir interfaces basadas en texto, TUIs.

Trabajo futuro

Este proyecto no termina aquí. En el futuro se pretende:

- Traducciones a otros lenguajes.
- Mejoras en la funcionalidad
- Inclusión en los repositorios oficiales de las distribuciones habituales

Resultados

Welcome to nftables-gui, please select a option

Create table
List tables

select a family

IP
ARP
IP6
BRIDGE

Resultados

Please fill values and press F2 to exit

Table name filter

Select a table for details

filter

Resultados

You are in filter table, please select a option

List chains
Create chain
Delete this table
Back

Please fill values and press F2 to exit

Chain name Internet
Hook input

Resultados

You are in filter table chain list,
plase select a chain for details

Internet

Please fill values and press F2 to exit

Rule name: _____
Action: _____
Protocol: _____
Src port: _____
Dst port: _____

Resultados

Please fill values and press F2 to exit

Rule name: test
Action: drop
Protocol: tcp
Src port: 80
Dst port: 80

Resultados

```
root@LUNA:/home/caballeroalba# nft list table filter
table ip filter {
    chain Internet {
        type filter hook input priority 0; policy accept;
        tcp sport http drop
    }
}
root@LUNA:/home/caballeroalba#
```

Conclusiones



[illegible]