Configurar nftables servidores

El archivo de nftables se encuentra en /etc/nftables.conf

Para activar el servicio ejecutaremos

```
systemctl enable nftables
```

Para iniciarlo, ejecutaremos

```
systemctl start nftables
```

O bien

```
service nftables start
```

Ejemplo práctico de configuración de nftables para un servidor

Ejemplo de nftables que permite web y correo desde cualquier IP, y bloquea el ssh a una serie de IP predefinidas.

```
#! /usr/sbin/nft -f

flush ruleset

# `inet` applies to both IPv4 and IPv6.
table inet filter {
   set management_ips_ipv4 {
  type ipv4_addr
flags interval
  elements = {A. B. C. D/26,
F. G. H. I/23,
J. K. L. M/24,
N. O. P. R}
```

```
    }

    chain input {
        type filter hook input priority 0;

        # accept any localhost traffic
        iif lo accept

        # no ping floods:
        ip protocol icmp icmp type echo-request limit rate over 10/second burst 4 packets drop
        ip6 nexthdr icmpv6 icmpv6 type echo-request limit rate over 10/second burst 4 packets
drop

        # accept traffic originated from us
        ct state established,related accept

        # accept ICMP & IGMP
        ip6 nexthdr icmpv6 icmpv6 type { echo-request, destination-unreachable, packet-too-
big, time-exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-listener-
reduction, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-neighbor-advert, ind-
neighbor-solicit, ind-neighbor-advert, mld2-listener-report } accept
        ip protocol icmp icmp type { echo-request, destination-unreachable, router-
solicitation, router-advertisement, time-exceeded, parameter-problem } accept
        ip protocol igmp accept

        # ssh
        #tcp dport 22 accept
        tcp dport {22} ip saddr @management_ips_ipv4  accept

        # http/https
        tcp dport 80 accept
        tcp dport 443 accept

        # smtp/submission
        tcp dport 25 accept
        tcp dport 587 accept
□□tcp dport 465 accept

        # pop3/pop3s
        tcp dport 110 accept
```

```
        tcp dport 995 accept

        # imap/imaps
        tcp dport 143 accept
        tcp dport 993 accept

        # count and drop any other traffic
        counter drop
    }

    chain output {
        type filter hook output priority 0;
        policy accept;
    }

    chain forward {
        type filter hook forward priority 0;
        policy drop;
    }
}
```

En el caso de querer abrir otro puerto pondríamos en cualquiera de las líneas a partir de la 37 para tcp

```
 tcp dport puerto-a-abrir accept
```

Para UDP

```
udp dport puerto-a-abrir accept
```

En el caso de querer abrir el puerto solo a determinadas IP

```
 tcp dport {puerto-a-abrir} ip saddr @management_ips_ipv4  accept
```

Referencia de nftables. https://www.netfilter.org/projects/nftables/manpage.html

---

Revision #9
Created 17 May 2022 18:20:02 by Admin
Updated 19 October 2023 12:04:10 by Admin