

A person wearing a dark hoodie is shown from the chest up, sitting at a desk and using a laptop. The background is a dark blue color with a vertical stream of white binary code (0s and 1s) falling from the top, reminiscent of the 'Matrix' effect. The text is overlaid on this background.

NFTABLES

para Proteção de

Servidores Linux

ROTEIRO

1. O nftables
2. Tradução das regras iptables para nftables
3. Aplicações e contextos
4. O básico da sintaxe
5. Demonstração: um servidor LAMP com nftables
6. Bônus: firewall de rede com nftables

O NFTABLES

O que é?

- É uma nova estrutura de classificação de pacotes do kernel do Linux.
- O iptables (iptables, ip6tables, arptables e ebtables) será descontinuado e você vai necessitar dessa nova ferramenta de manipulação do **netfilter**.
- Há ferramentas automatizadas que auxiliam o processo de conversão do iptables para nftables.

TRADUÇÃO IPTABLES - NFTABLES

- Crie as regras

```
iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

- Salve as regras

```
iptables-save > regras_iptables.txt
```

- Traduza as regras para a sintaxe nft

```
iptables-restore-translate -f regras_iptables.txt > regras_nftables.nft
```

TRADUÇÃO IPTABLES - NFTABLES

A tradução ficará assim:

```
# Translated by iptables-restore-translate v1.8.9 on Tue Aug 8 14:44:40 2023
```

```
add table ip filter
```

```
add chain ip filter INPUT { type filter hook input priority 0; policy drop; }
```

```
add chain ip filter FORWARD { type filter hook forward priority 0; policy accept; }
```

```
add chain ip filter OUTPUT { type filter hook output priority 0; policy drop; }
```

```
add rule ip filter INPUT tcp dport 22 ct state new,related,established counter accept
```

```
add rule ip filter OUTPUT tcp sport 22 ct state related,established counter accept
```

```
# Completed on Tue Aug 8 14:44:40 2023
```

TRADUÇÃO IPTABLES - NFTABLES

Para utilizar um formato mais simples:

1) Carregue as regras no sistema:

```
nft -f regras_nftables.nft
```

2) Na sequência, liste as regras para um arquivo:

```
nft list ruleset > nftables.conf
```

TRADUÇÃO IPTABLES - NFTABLES

```
Arquivo  Editar  Ver  Pesquisar  Ferramentas  Documentos  Ajuda
+  📄  📄  |  ↶  ↷  |  ✂  📄  📄  |  🔍  ✎
nftables.conf ×
1 table ip filter {
2     chain INPUT {
3         type filter hook input priority filter; policy drop;
4         tcp dport 22 ct state established,related,new counter accept
5     }
6
7     chain FORWARD {
8         type filter hook forward priority filter; policy accept;
9     }
10
11    chain OUTPUT {
12        type filter hook output priority filter; policy drop;
13        tcp sport 22 ct state established,related counter accept
14    }
15 }
16
```

Texto sem formatação ▾ Espaços: 4 ▾ Lin 16, Col 1 INS

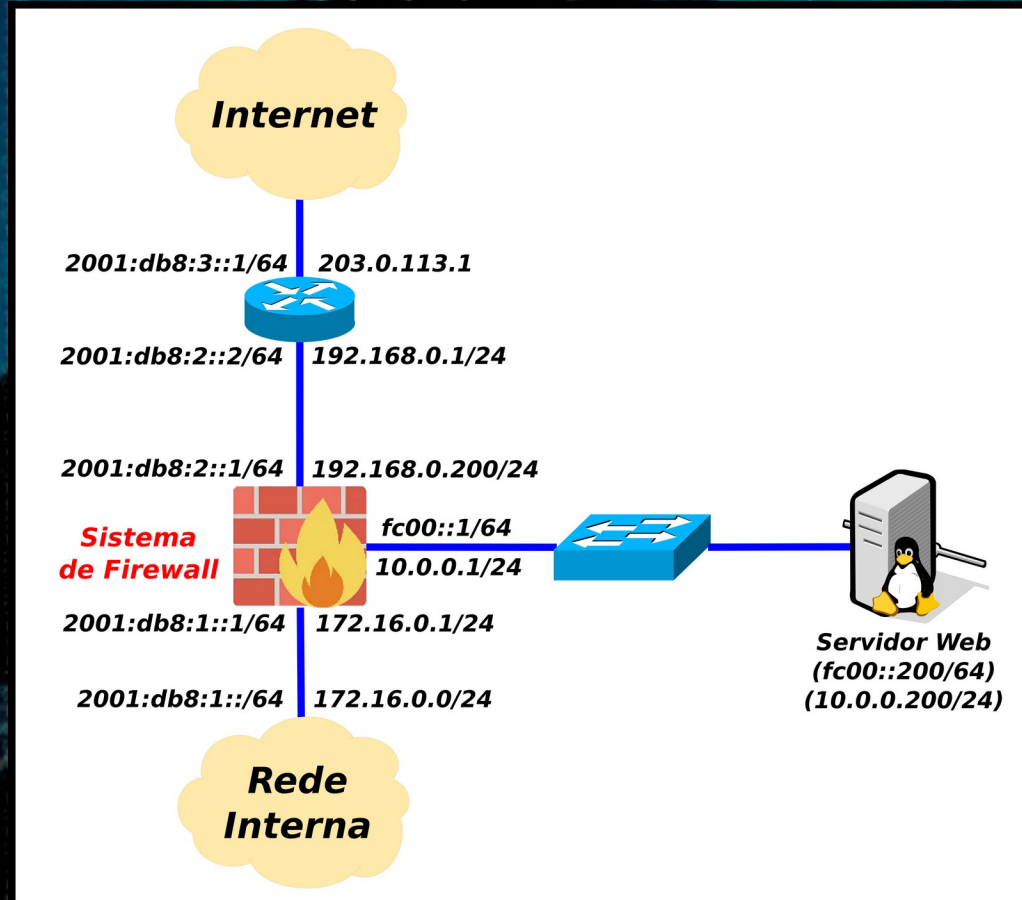
APLICAÇÕES E CONTEXTOS

- ISPs não deveriam utilizar firewall de rede na borda, para não ter problemas de performance e não bloquear tráfegos legítimos inadvertidamente.
- O firewall de rede deve estar na borda de um segmento de rede, mas ele é apenas um dos componentes de um sistema de firewall (IPS, IDS, firewall de pacotes, firewall de estados, proxies etc.).
- Toda máquina deve ter seu próprio firewall ativado.
- Não se esqueça do IPv6! Todas as suas máquinas já usam IPv6 e não vai adiantar muito proteger IPv4 e esquecer do IPv6! Os atacantes agradecem.

O BÁSICO DA SINTAXE

- Address families: ip, ip6, inet, arp, bridge e netdev.
- Hooks para ip, ip6, inet e bridge: prerouting, input, forward, output, postrouting e ingress (novidade).
- Hooks para arp: input e output.
- Hooks para netdev: ingress e egress.
- Tabelas são identificadas por nome e um address family.

DEMONSTRAÇÃO



BÔNUS

Os arquivos [nftables.conf](#) da demonstração e do firewall de rede estão disponíveis no link [Palestras](#) do meu site:

<https://www.nivio.eti.br>

A person wearing a dark hoodie is shown from the chest up, holding a laptop. The background is a dark blue gradient with vertical columns of white binary code (0s and 1s) falling from the top, creating a digital rain effect. The person's face is obscured by the hood and shadows.

CONCLUSÃO

OBRIGADO!

contato@nivio.eti.br

REFERÊNCIAS

DEBIAN.org. **NFTables**. Disponível em <https://wiki.debian.org/nftables>.

GENTOO.org. **NFTables**. Disponível em <https://wiki.gentoo.org/wiki/Nftables>.

Manual do comando nft: [man nft](#).

NFTABLES.org. **Wiki do nftables**. Disponível em <https://wiki.nftables.org/>.