

Firewall Linux: 4 Soluções Para Facilitar O Processo De Implantação

pedrodelfino(<https://e-tinet.com/author/pedrodelfino/>)

Venus Williams at SIGNAL

One of sports' most influential women talks perseverance, success, equality.

Twilio



(<https://profissionaislinux.com.br/materiais/curso-linux-ubuntu/>)


JUNTE-SE A MAIS DE 110.000 PESSOAS QUE JÁ TEM UMA CÓPIA

Ubuntu: Iniciando Com Linux De Maneira Prática E Rápida

Qual é o seu email?

Receber





DigitalOcean® Free T

Save Up to 55% Compared to Other Providers. Learn Why Devs Love DigitalOcean.

DigitalOcean®

Compartilhe Este Post



Boa parte dos iniciantes no sistema Linux tem dúvidas quanto à importância do firewall, seja em ambientes domésticos, seja em corporativos (<https://e-tinet.com/carreira/firewall-corporativo-o-que-e/>). Se você convive com dúvidas a respeito do assunto, adianto: chegou ao lugar certo. Aqui, explico a função desse tipo de ferramenta e, também, apresento uma série de soluções de firewall Linux.

Começando pela definição dada por Wes Noonan (<https://e-tinet.com/carreira/firewall-corporativo-o-que-e/>), engenheiro de sistemas da Cisco e coautor do livro Firewall Fundamentals (<https://www.oreilly.com/library/view/firewall-fundamentals/1587052210/>) (disponível em inglês), muitas pessoas pensam o firewall como:

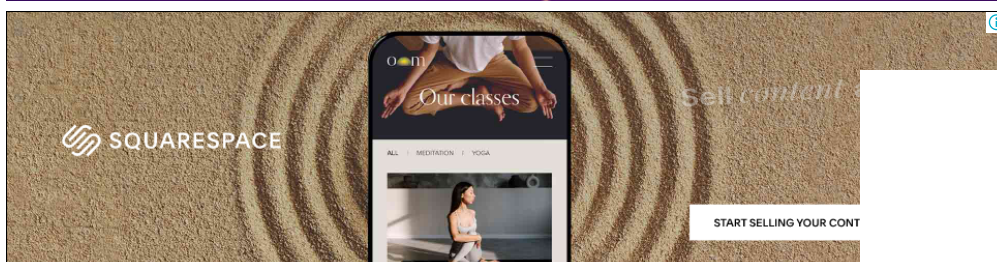
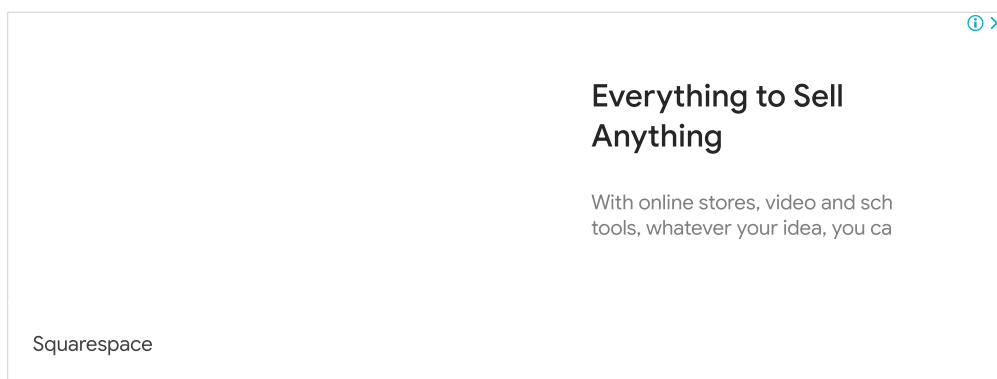
“Um dispositivo residente na rede e que controla o tráfego que passa por seus vários segmentos, mas ele pode, também, ser implementado nos sistemas em si — os chamados host-based firewalls. De qualquer forma, o objetivo é sempre o mesmo: fornecer um método de impor uma política de controle de acesso.”

Em outras palavras, o firewall é um mecanismo configurado pelo administrador da rede implementar regras e privilégios dos usuários em relação ao que se é permitido fazer no ambiente em questão, sem a necessidade de intervenção humana.

Agora que já temos uma definição básica para o firewall e sua principal função, que tal conhecermos as soluções disponíveis? Abaixo, listei quatro softwares de firewall Linux altamente úteis e completas em termos de recursos.



(https://profissionaislinux.com.br/materiais/curso-linux-ubuntu/?utm_source=e-tinet.com&utm_medium=referral&utm_campaign=content-blog)



1. Firewall Linux Com Iptables

O iptables é uma solução de firewall Linux bastante poderosa que, como o próprio nome diz, tem a sua estrutura composta por tabelas — para entender mais a lógica das tabelas do iptables, já temos um artigo em que abordo o assunto (<https://e-tinet.com/linux/tabelas-do-iptables-firewall-linux/>). Sem dúvidas, é um dos melhores programas de firewall à disposição.

Por meio das camadas do firewall (ao todo são três), o sysadmin consegue estabelecer regras avançadas para ~~proteger a rede~~ ^(https://e-tinet.com) e controlar os pacotes que por ela trafegam e, de quebra, pode instalar extensões. Em contrapartida às suas funcionalidades de alto nível e flexibilidade, dominar o iptables requer dedicação e estudo.

Instalação do iptables no CentOS

Baseado no Red Hat Enterprise Linux, o CentOS é um dos principais sistemas operacionais voltados a ambientes de trabalho. Sendo assim, aprender a instalação do iptables nessa distro é uma atividade, no mínimo, conveniente.



(https://profissionaislinux.com.br/materiais/curso-linux-ubuntu/?utm_source=e-tinet.com&utm_medium=referral&utm_campaign=content-blog)

Leia também: [Vamos usar o Shell do Ubuntu Linux ?](https://e-tinet.com/linux/shell-ubuntu/)
(<https://e-tinet.com/linux/shell-ubuntu/>)

O único pré-requisito para a implementação é a habilitação de uma conta com privilégios sudo. Caso tenha algum firewall instalado na máquina, desative-o. A solução padrão do CentOS é o Firewalld — que conheceremos mais adiante. Para desativá-lo, digite a sequência de comandos (<https://e-tinet.com/linux/comandos-linux-mais-utilizados/>):

```
sudo systemctl stop firewalld #encerrará o processo
sudo systemctl disable firewalld #desativará a
inicialização automática junto ao boot do sistema
sudo systemctl mask --now firewalld #impedirá que outros
processos acionem o Firewalld
```

Concluídas as etapas preliminares, vamos começar a instalação dos pacotes do iptables e, em seguida, iniciar a aplicação. Digite:

```
sudo yum install iptables-services
sudo systemctl start iptables
```

Agora, você pode usar o comando **-nvL** para verificar as regras correntes do firewall. Quaisquer alterações passam a vigorar após a reinicialização do sistema operacional.

2. Firewalld: Firewall Linux No Padrão RedHat

Aproveitando que já o mencionamos, o Firewalld segue presente na lista como uma das melhores e mais utilizadas soluções de firewall Linux. Como falamos no tópico anterior, ele vem instalado por padrão no CentOS ([Privacidade - Termos](https://e-</p></div><div data-bbox=)

tinet.com/linux/centos-distribuicao-linux/) — e em todas as distros baseadas no Red Hat Enterprise Linux (RHEL) (<https://e-tinet.com/linux/red-hat-oque-saber/>).

Para aprender mais sobre a implementação do FirewallD (<https://e-tinet.com/linux/firewall-firewalld/>), veja também o artigo abaixo;

- **Firewalld: Como Utilizar a Solução de Firewall Para Linux Padrão Da RedHat** (<https://e-tinet.com/linux/firewall-firewalld/>)

Com suporte aos protocolos IPv4 e IPv6, fora os diversos recursos, o FirewallD traz vantagens como a aplicação imediata de novas configurações. Ou seja, as mudanças não requerem reboot. Isso é possível graças à função runtime configuration, a qual permite que novas regras sejam aplicadas instantânea e temporariamente.

Elucidando melhor a questão, o FirewallD é separado por dois tipos de configurações: **runtime** e **permanent**. A runtime estabelece as alterações junto ao kernel, porém não as salva na configuração permanente, bastando o encerramento do firewall para que sejam desfeitas.

O mais legal disso é que o administrador tem condições de realizar testes e, se quiser, tornar definitivas as configurações experimentais. A conversão de runtime para permanent é realizada por meio do comando firewall-cmd, como no exemplo:

```
firewall-cmd --runtime-to-permanent
```

Gostei, mas como faço para instalá-lo no Linux?

Se você utiliza o Ubuntu, por exemplo, é necessário, primeiramente, desinstalar o UFW — seu firewall padrão. Para remover o UFW e suas dependências, digite:

```
sudo apt remove --auto-remove ufw
```

ou

```
sudo ufw disable #isso apenas desativará o firewall
```

Tendo o caminho livre de conflitos para a recepção do FirewallD, digite a seguinte sequência de comandos:

```
sudo apt install firewalld
```

```
sudo systemctl enable firewalld #habilitará o FirewallD e fará com que o firewall abra durante o boot do sistema
```

```
sudo systemctl start firewalld
```

```
sudo firewall-cmd --state #este comando apenas confirmará se o FirewallD está funcionando
```

3. UFW: O Firewall do Ubuntu

Reiterando, assim como o FirewallD para sistemas baseados no RHEL, o UFW também é um firewall padrão, mas do Ubuntu (<https://e-tinet.com/linux/comecando-ubuntu-linux/>). O seu nome é um acrônimo para

Uncomplicated Firewall, ou seja, o projeto UFW visa proporcionar facilidades ao usuário iniciante. (<https://e-tinet.com>)

Leia também: **[Proxy com Squid3 + SquidGuard no Ubuntu - Controle a sua internet com Linux](https://e-tinet.com/linux/proxy-squid3-squidguard-ubuntu-linux/)** (<https://e-tinet.com/linux/proxy-squid3-squidguard-ubuntu-linux/>)

Aproveite também para ver um **tutorial completo do UFW** (<https://e-tinet.com/linux/firewall-com-ufw/>) no artigo:

- **Firewall Com UFW: Descomplicando a Configuração De Firewall No Linux (Debian / Ubuntu)** (<https://e-tinet.com/linux/firewall-com-ufw/>)

Na prática, ele é uma versão descomplicada do iptables, visto que sua estrutura é composta por uma das interfaces do iptables, a qual simplifica o processo de configuração do firewall.

Em comparação ao iptables, que é uma ferramenta (<https://e-tinet.com/linux/30-ferramentas-para-hackers-kali-linux/>) complexa e pouco amigável para iniciantes, o UFW é consideravelmente mais fácil de utilizar e, ao mesmo tempo, embora com menos recursos, pode garantir ótima proteção a uma rede de computadores.

Aliás, se você prefere iniciar o contato com um firewall Linux a partir de uma interface gráfica, baixe o GFW. Trata-se da versão gráfica do mesmo firewall — ótima para usuários que estão migrando do Windows e, naturalmente, adaptando-se ao Linux.

Como instalar o UFW?

Se você chegou a desinstalar o UFW de seu Ubuntu, apenas digite o comando `apt install ufw -y` — o mesmo vale para o Debian (<https://e-tinet.com/linux/debian-gnu-linux/>). Agora, caso pretenda instalar no CentOS, é necessário não apenas desinstalar o Firewallld, mas baixar o repositório EPEL em seu sistema. Digite:

```
yum install epel-release -y
```

Assim que instalado o repositório, utilize o seguinte comando para instalar o UFW:

```
yum install --enablerepo="epel" ufw -y
```

Finalizando, digite o comando `ufw enable` para habilitar o firewall para inicializar automaticamente, junto ao sistema operacional.

4. Nftables

O nftables é um framework compatível com o iptables que tem como propósito ser uma alternativa otimizada a este. De acordo com a wiki dos desenvolvedores, problemas envolvendo inconsistências no código, atualizações e sintaxe são algumas das correções promovidas pelo nftables.

Caso você precise de um **material mais completo sobre o NfTables** (<https://e-tinet.com/linux/firewall-nftables/>), acesse o artigo abaixo:

- **NfTables: Aprenda Como Utilizar o Firewall Universal Para Linux** (<https://e-tinet.com/linux/firewall-nftables/>)

Leia também: [9 mitos do Sistema Linux que você precisa ignorar \(urgentemente\)](https://e-tinet.com/linux/9-mitos-sistema-linux/)
(<https://e-tinet.com/linux/9-mitos-sistema-linux/>)

Em face disso, o usuário pode notar diferenças na sintaxe, que é mais simples e intuitiva no nftables, na flexibilidade, pois ele permite que especifique várias ações em uma só regra, e nas possibilidades de aplicar configurações avançadas de tabelas.

Qual é o procedimento de instalação?

Antes de seguir com a implantação do nftables, é necessário instalar uma série de dependências, sendo elas:

- **init-system-helpers:** sudo apt install -y init-system-helpers;
- **libc6:** sudo apt install -y libc6;
- **libgmp10:** sudo apt install -y libgmp10;
- **libmnl0:** sudo apt install -y libmnl0;
- **libnftnl4:** sudo apt install -y libnftnl-dev; e
- **libreadline6:** sudo apt install -y libreadline6.

Todavia, por mais que estejamos falando de um firewall robusto, a instalação do nftables é muito simples. No Ubuntu, certifique-se de que nenhum firewall esteja ativo e, então, abra o terminal (<https://e-tinet.com/linux/terminal-linux/>) e digite:

```
sudo apt-get install -y nftables
```

Curtiu as sugestões de firewall Linux listadas no conteúdo? Uma das lições importantes que aprendemos ao conhecê-las é que o iptables é a base para a maioria das soluções, sendo ela a mais difícil de dominar, enquanto as demais tendem a oferecer menos obstáculos ao usuário.

No mais, se você deseja se tornar um especialista em Linux (<https://e-tinet.com/linux/o-mercado-de-trabalho-esta-pronto-para-especialistas-em-linux-veja/>) capaz de configurar todas as ferramentas de firewall Linux abordadas até aqui, recomendo que visite a página Profissionais Linux (<https://e-tinet.com/profissionais-linux/acesso-nivel-1/>)!

Artigos Relacionados: