VPS jun 03, 2022 Ariane G. 3min de leitura

Como Configurar um Firewall no Ubuntu 18.04 com UFW

Segurança é um assunto que deve ser levado a sério, principalmente nesta época em que crimes cibernéticos estão se tornando cada vez mais populares. Por isso, é altamente recomendável adotar medidas extras de segurança.

Uma das maneiras de proteger seus dados é configurando um firewall para supervisionar as conexões feitas com o **servidor**, incluindo uma VPS. Neste tutorial vamos ensinar como configurar um firewall no Ubuntu 18.04 com o UFW.

Utilizar Firewall para Proteger seu Servidor Ubuntu

Um firewall é um hardware ou software que controla o tráfego enviado e recebido de um servidor ou outra máquina. Em outras palavras, é um componente muito importante para a segurança de qualquer dispositivo que realiza conexões com a internet.

Mesmo o Linux tendo ótimas ferramentas de segurança pré-instaladas, quanto mais seguro, melhor.

O Ubuntu possui uma aplicação que facilita a instalação de firewall, o UFW (Uncomplicated Firewall). Esta ferramenta vem instalada por padrão na versão 18.04, mas é provável que esteja desabilitada. O UFW ainda possui uma interface gráfica chamada GUFW que pode ser instalada caso você tenha um ambiente desktop.

Configurar Firewall com UFW no Ubuntu 18.04

Como mencionado antes, o UFW está instalado por padrão no Ubuntu 18.04, mas não está habilitado. Então a primeira coisa que precisamos fazer é habilitá-lo.

Depois de conectar com o **SSH**, vamos executar o seguinte comando para habilitar o UFW:

Se você recebeu o erro de “comando não encontrado”, instale o UFW executando:

```
sudo apt-get install ufw
```

Em seguida, iremos verificar o status do UFW:

```
sudo ufw status
```

Neste momento o UFW deverá estar ativado.

Por padrão, o UFW nega qualquer conexão recebida e permite todas as conexões realizadas. Para muitos usuários, isto já é suficiente. Mas para quem possui serviços online ou aplicações, é preciso criar algumas regras.

Definir Regras de Firewall no Ubuntu 18.04 com UFW

Uma regra de firewall é uma instrução que define a maneira com que o firewall irá se comportar, por exemplo, quais conexões serão aceitas ou rejeitadas.

Vamos configurar algumas regras de firewall usando o UFW:

Abrir e Fechar Portas com UFW

As portas são interfaces de conexão utilizadas por aplicações para estabelecer uma conexão com o servidor.

Com o UFW é simples abrir ou fechar portas. Para abrir, basta utilizar o comando:

```
sudo ufw allow [porta/protocolo]
```

No caso dos protocolos, eles podem ser TCP ou UDP. Isso depende das nossas necessidades. Por exemplo:

```
sudo ufw allow 56/tcp
```

Isso significa que todas as aplicações ou serviços que tentarem conectar com nosso servidor usando a porta 56 serão permitidos.

Porém, podemos negar o uso desta mesma porta com o comando:

```
sudo ufw deny 56/tcp
```

Agora, todas as aplicações que utilizam TCP e tentarem conectar utilizando a porta 56 não irão conseguir.

Também conseguimos abrir ou fechar um intervalo de portas com um único comando, o que é perfeito para economizar tempo. A sintaxe básica fica assim:

```
sudo ufw allow/deny [Porta_inicial:Porta_final]/protocolo
```

Para abrir portas o comando fica assim:

```
sudo ufw allow 300:310/tcp
```

Para fechar:

```
sudo ufw deny 300:310/tcp
```

utilizada para fazer conexões com o servidor.

Por exemplo, o HTTP exige que a porta 80 esteja disponível, enquanto o HTTPS utiliza a porta 443.

Então, precisamos executar este comando para HTTP:

```
sudo ufw allow http
```

O comando é equivalente a abrir a porta 80, como explicado.

Portanto, só precisamos saber as portas usadas pelos serviços.

Permitir ou Negar Conexões com Endereços de IP

Também é possível negar o acesso de um endereço de IP específico.

Fazemos isto com o comando:

```
sudo ufw deny from ENDEREÇOIP
```

Por exemplo:

```
sudo ufw deny from 192.168.1.2
```

Ou, caso contrário, para permitir acesso desse mesmo IP:

```
sudo ufw allow from 192.168.1.3
```

Outra coisa que podemos fazer é definir que um IP possa conectar apenas com uma porta específica:

```
sudo ufw allow from [ENDEREÇOIP] to any port [PORTA]
```

O comando fica assim:

```
sudo ufw allow from 192.168.1.4 to any port 44
```

Dessa maneira, o IP só poderá realizar a conexão caso utilize a porta 44.

Deletar uma Regra Específica no Firewall Ubuntu

Podemos remover uma regra no UFW com um único comando! Mas primeiro temos que listar todas as regras. Para isso executamos o comando:

```
sudo ufw status numbered
```

```
sudo ufw delete 4
```

Essas são as principais funções que você precisa conhecer! Agora você está pronto para configurar a segurança do seu servidor da maneira que preferir. Para mais informações, consulte o manual do UFW com o comando:

```
sudo ufw –help
```

Resumo

O processo de configuração de um firewall no Ubuntu 18.04 é fácil graças ao UFW. Mas, a aplicação possui mais opções para tornar o servidor ainda mais seguro. Neste tutorial você aprendeu o básico para garantir a segurança dos seus dados. Esperamos que tenha sido útil!

O AUTOR

Ariane G.

A Ariane é SEO Team Leader com experiência em conteúdo, localização e SEO. Seu desafio é levar a Hostinger ao topo dos resultados no Brasil, França e Reino Unido. Eventualmente ela compartilha seu conhecimento no blog e nos tutoriais da Hostinger e no tempo livre ela gosta de explorar lugares novos e viver intencionalmente.

Mais de Ariane G.