Cloud Computing

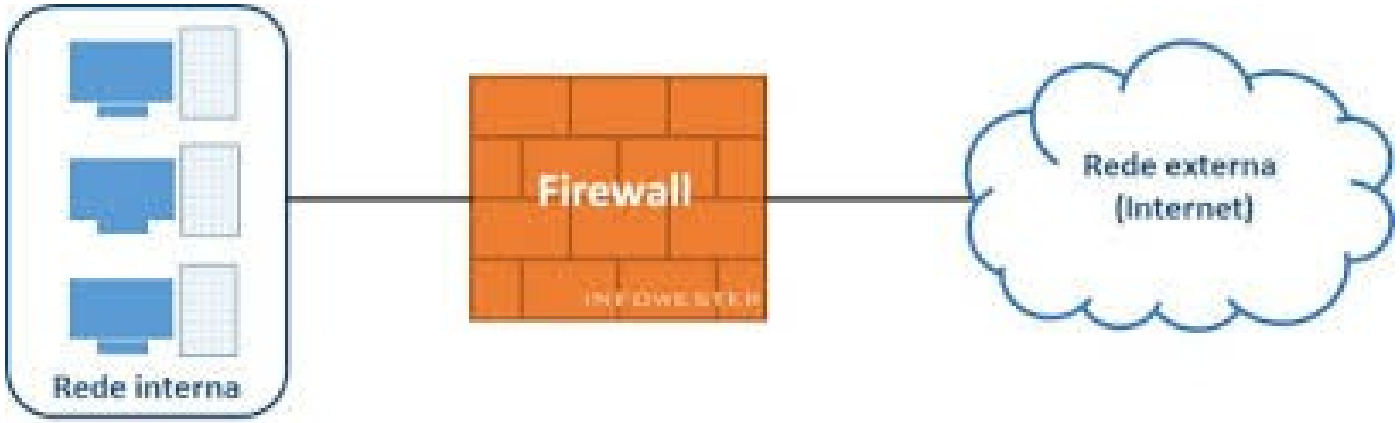
Gledson Scotti

Firewall Prática

SATC EDUCAÇÃO E TECNOLOGIA | Engenharia da Computação

UFW

O UFW, ou Uncomplicated Firewall (Firewall Descomplicado), é uma interface para iptables desenvolvida para simplificar o processo de configuração de um firewall. Apesar da iptables ser uma ferramenta sólida e flexível, pode ser difícil para os iniciantes aprender como usá-la para configurar corretamente um firewall.



Engenharia da Computação

UFW e iptables

UFW é um “host-based firewall”, um programa que, rodando em um servidor, pode restringir o tráfego de dados e a atividade da rede naquele servidor em específico prevenindo investidas em fragilidades de acessos ao Sistema Operacional.

A ferramenta de configuração de firewall padrão para o Ubuntu é o ufw. Desenvolvido para facilitar a configuração do iptables, o ufw fornece um jeito fácil de criar um firewall IPv4 ou IPv6. Por padrão, o UFW é desativado.

UFW Sintaxe Básica e Exemplos

Habilitar o UFW

$ sudo ufw enable

Para verificar o estado do UFW:

$ sudo ufw status verbose

Desabilitar o UFW

$ sudo ufw disable

Engenharia da Computação

UFW Sintaxe Básica e Exemplos

Note que por padrão, os pacotes de entrada estão sendo recusados. Existem exceções, as quais podem ser visualizadas com o comando:

$ sudo ufw show raw

Podemos ler os arquivos de regras em /etc/ufw (os arquivos cujos nomes terminam em .rules (regras)).

Engenharia da Computação

UFW Manutenção de Regras

Permitindo:

$ sudo ufw allow <**porta**>/<**opcional: protocolo**>

Exemplo: permitir pacotes tcp e udp de entrada na porta 53:

$ sudo ufw allow 53

Exemplo: permitir pacotes tcp de entrada na porta 53:

$ sudo ufw allow 53/tcp

Exemplo: Permitir pacotes udp de entrada na porta 53:

$ sudo ufw allow 53/udp

Engenharia da Computação

UFW Manutenção de Regras

Rejeitando:

$ sudo ufw deny <**port**>/<**optional: protocol**>

Exemplo: rejeitar pacotes de entrada tcp e udp na porta 53:

$ sudo ufw deny 53

Exemplo: rejeitar pacotes de entrada tcp na porta 53:

$ sudo ufw deny 53/tcp

Exemplo: rejeitar pacotes de entrada udp na porta 53:

$ sudo ufw deny 53/udp

Engenharia da Computação

UFW Manutenção de Regras

Apagarndo Regra Existente

Para apagar uma regra, execute o comando original com a palavra 'delete' como prefixo.

Por exemplo, se a regra original era:

$ ufw deny 80/tcp

Use o seguinte comando para apagá-la:

$ sudo ufw delete deny 80/tcp

UFW Manutenção de Regras

Serviços: permitir ou negar por nome de serviço visto que o ufw lê de /etc/service.

Para ver uma lista de serviços:

$ less /etc/services

Permitir por nome de serviço

$ sudo ufw allow <nome do serviço>

Exemplo: permitir ssh por nome:

$ sudo ufw allow ssh

Rejeitar por nome de serviço

$ sudo ufw deny <nome do serviço>

Exemplo: recusar ssh por nome:

$ sudo ufw deny ssh

Engenharia da Computação

UFW Manutenção de Regras

Habilitando o log no ufw e verificando o estado do seu firewall.

Para verificar o estado do ufw:

$ sudo ufw status

Para habilitar o registro, use:

$ sudo ufw logging on

Para desabilitar o registro, use:

$ sudo ufw logging off

Engenharia da Computação

UFW Manutenção de Regras

Sintaxe Avançada: pode ser permitido ou negado acesso utilizando endereços específicos da fonte ou do destino, portas e protocolos.

Permitir IP Específico:

sudo ufw allow from <endereço ip>

Permitir pacotes de 207.46.232.182

$ sudo ufw allow from 207.46.232.182

Permitir Sub-rede Específica

$ sudo ufw allow from 192.168.1.0/24

Engenharia da Computação

UFW Manutenção de Regras

Permitir por Porta e IP Específicos

$ sudo ufw allow from <endereço IP> to <protocolo> port <número da porta>

Exemplo: permitir acesso do endereço IP 192.168.0.4 à porta 22 para todos os protocolos:

$ sudo ufw allow from 192.168.0.4 to any port 22

Permitir por Porta, Endereço IP e Protocolo Específico

$ sudo ufw allow from <endereço ip> to <protocolo> port <número da porta> proto <nome do protocolo>

Exemplo: permitir acesso do endereço 192.168.0.4 à porta 22 usando TCP:

$ sudo ufw allow from 192.168.0.4 to any port 22 proto tcp

Engenharia da Computação

UFW Manutenção de Regras

Negar por IP Específico

$ sudo ufw deny from <ip address>

Exemplo: para bloquear pacotes de 207.46.232.182:

$ sudo ufw deny from 207.46.232.182

Negar por portas e endereço IP específicos

$ sudo ufw deny from <endereço ip> to <protocolo> port <número da porta>

Exemplo: negar endereço ip 192.168.0.1 de acessar a porta 22 para todos os protocolos:

$ sudo ufw deny from 192.168.0.1 to any port 22

Engenharia da Computação

UFW Exercícios

Cenário: Você quer bloquear acesso à porta 22 dos IPs 192.168.5.1 e 192.168.5.7 mas permitir todos os outros 192.168.0.x IPs para ter acesso à porta 22 usando tcp.

Mudança de cenário: Após feito seus bloqueios acima, você resolveu bloquear acesso à porta 22 também para 192.168.5.3, além dos ips acima.