INSTITUTO FEDERAL DE
EDUCAÇÃO CIÊNCIA E TECNOLOGIA
Telemática
Disciplina: Gerência e Segurança de Redes
Prof. José Roberto Bezerra

Atividade de Laboratório

1 Firewalls

Firewalls (FW) são dispositivos de *hardware* ou *software* essenciais para segurança de redes de computadores. Basicamente, um FW verifica a origem e o destino dos pacotes ao entrar ou sair da rede. A partir de um conjunto de regras pré-configuradas os pacotes têm seu fluxo permitido ou bloqueado. As regras fundamentam-se nos números de portas e IPs de origem e destino. A Tabela 1 apresenta alguns exemplos de regras que podem ser aplicadas.

Source Address	Source Port	Destination Address	Destination Port	Action
192.168.1.2	80	10.10.10.20	22	allow
10.0.0.0/24	any	192.168.0.0/24	22	deny
any	any	any	any	deny

Tabela 1: Exemplos de regras de FW.

A Tabela 2 apresenta alguns exemplos de soluções de FW em *hardware* e *software*. Existem diversas outras soluções disponíveis, especialmente para Linux.

Hardware	Software
CISCO ASA 5500	Net Gate pfSense
FortiNet FortiGate	Endian Firewall Community (EFW)
NetGear ProSafe	IPFire
SonicWall Network Security	Shorewall

Tabela 2: Soluções de *firewalls*.

2 Uncomplicated Firewall

O Ubuntu Linux conta com uma opção de FW bastante popular e de fácil configuração, o UFW (*Uncomplicated Firewall*). O UFW conta ainda com uma interface gráfica, o Gufw. A seguir são mostradas alguns comandos para o UFW.

```
$ sudo ufw enable                    # habilita o ufw, caso esteja instalado
$ sudo apt-get install ufw           # instala o ufw
$ sudo ufw status                    # verifica o estado atual do serviço
$ sudo ufw status numbered           # exibe um número para cada regra
$ sudo ufw delete [rule]             # apaga a regra especificada
$ sudo ufw reload                    # reinicializa o UFW apagando todas as regras
```

As portas podem ser abertas ou fechadas seguindo-se a sintaxe básica `sudo ufw allow/deny [porta/protocolo]`. Os protocolos permitidos são basicamente TCP ou UDP. Seguem alguns exemplos ilustrativos.

```
$ sudo ufw allow http                # abre para o serviço HTTP
$ sudo ufw allow 56/tcp              # permite que qualquer processo acesse a porta 56 via TCP
$ sudo ufw deny 56/tcp               # bloqueia o acesso de qualquer processo a porta 56 via TCP
$ sudo ufw deny 300:310/tcp          # fecha as portas 300 a 310
$ sudo ufw deny from 192.1.1.1       # bloqueia qualquer acesso originado do IP especificado
```

3 Atividades de Laboratório

1. Utilizando o Linux Ubuntu verifique se o UFW está instalado. Caso não esteja proceda com a instalação (a senha de *root* será necessária).
2. Inicialize o UFW e verifique seu status.
3. Quais as regras existentes? Quais serviços estão permitidos?
4. Descubra o IP do Security Onion e anote.

5. Descubra o IP da máquina cliente e anote.

6. Na máquina cliente, tente conectar com Security Onion via SSH. Use a linha de comando `ssh analyst@x.x.x.x` independente do sistema operacional. O que acontece?
7. Apague todas as regras e reinicialize o UFW.
8. Repita o comando do ítem 6. O que acontece agora? Observe que mesmo com o conjunto de regras vazio a conexão não é permitida.
9. Adicione uma regra que permite a máquina cliente conectar a qualquer serviço disponível no servidor e em seguida tente conectar via SSH. O que acontece?
10. Apague a regra criada no ítem anterior. Que é a única regra existente.
11. Permita o SSH através do comando `sudo ufw allow ssh`. (Existem alguns perfis de serviços pré-configurados que podem ser acessados via `sudo ufw app list`)
12. Agora adicione uma regra que NEGA o acesso via SSH a máquina cliente. O que acontece?
13. Mais uma vez apague todas as regras. Inicialmente, adicione a regra usada no ítem anterior. Em seguida adicione a regra geral que permite o SSH. O que acontece agora?

4 Questionário

1. A ordem em que as regras são cadastradas importa? Justifique.
2. Como corrigir o ”erro”que aconteceu no ítem 12?
3. O que acontece se regras conflitantes estiverem configuradas?
4. Qual a função dos arquivos de `log`?

5 Referências

- https://www.hostinger.com.br/tutoriais/firewall-ubuntu-ufw
- https://help.ubuntu.com/community/UFW