Trabalho prático 1 de Segurança em Redes de Computadores

Autores

- Ana Vidal (118408)
- Simão Andrade (118345)

Objetivo

Apresentar um relatório dos **testes de configuração** e de **funcionamento** dos cenários descritos nos pontos `9` e `10` do guia laboratorial "High-Availability Firewall Scenarios".

Temos as seguintes tarefas a serem realizadas:

- [ ] Firewall and load-balancers deployment (2 valores).
- [ ] Network routing and connectivity (2 valores).
- [ ] Devices state synchronization (3 valores).
- [ ] Zones definition (3 valores).
- [ ] Inter-zone rules (6 valores).
- [ ] Report (4 valores).

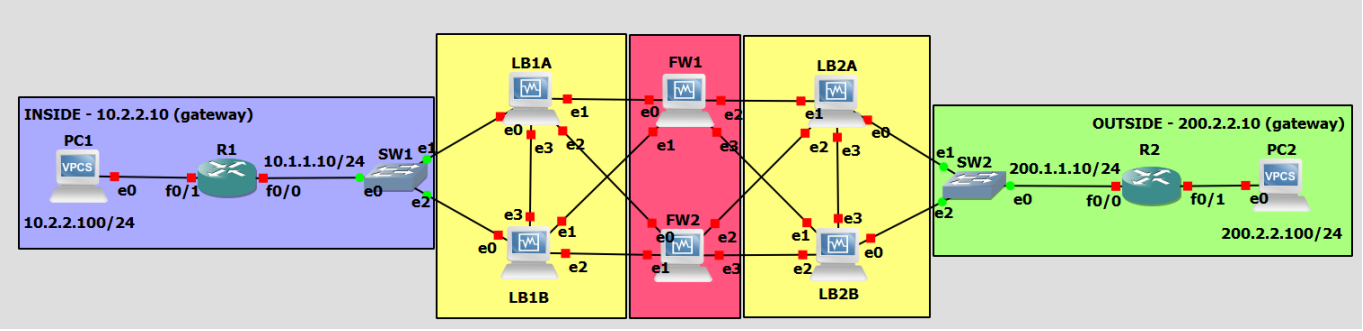
Estado-de-Arte

Explicar os seguintes conceitos:

- **Firewall**;
- **Zonas e Regras**;
- **Load Balancer**;
- **State Synchronization**;
- **Redundancy Synchronization**;

Ponto 9

Topologia



Configuração Inicial

Vamos começar por atribuir os endereços IP às interfaces dos routers e aos computadores de acordo com o enunciado.

PC1 (computador interno):

```
ip 10.2.2.100/24 10.2.2.10
save
```

PC2 (computador externo):

```
ip 200.2.2.100/24 200.2.2.10
save
```

R1 (*router* interno):

```
conf t
ip route 0.0.0.0 0.0.0.0 (ip por definir)
ip route 0.0.0.0 0.0.0.0 (ip por definir)
int f0/1
ip add 10.2.2.10 255.255.255.0
no shut
int f0/0
ip add 10.1.1.10/24
no shut
end
write
```

R2 (*router* externo):

```
conf t
ip route 192.1.0.0 255.255.254.0 (ip por definir)
ip route 192.1.0.0 255.255.254.0 (ip por definir)
int f0/1
ip add 200.2.2.10 255.255.255.0
no shut
int f0/0
ip add 200.1.1.10 255.255.255.0
no shut
end
write
```

LB1A (*load balancer* superior interno):

```
set system host-name LB1A
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)
commit
save
```

LB1B (*load balancer* inferior interno):

```
set system host-name LB1B
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)
commit
save
```

FW1 (*firewall* superior):

```
set system host-name FW1
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)

set nat source outbound-interface eth0
set nat source rule 10 source address 10.0.0.0/8
set nat nat source rule 100 translation address 192.1.0.1-192.1.0.10

commit
save
```

FW2 (*firewall* inferior):

```
set system host-name FW2
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)

set nat source outbound-interface eth0
set nat source rule 10 source address 10.0.0.0/8
set nat nat source rule 100 translation address 192.1.0.1-192.1.0.10
```

```
commit
save
```

LB2A (*load balancer* superior externo):

```
set system host-name LB2A
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)

commit
save
```

LB2B (*load balancer* inferior externo):

```
set system host-name LB2B
set interfaces ethernet eth0 address (ip por definir)
set interfaces ethernet eth1 address (ip por definir)
set interfaces ethernet eth2 address (ip por definir)
set interfaces ethernet eth3 address (ip por definir)

commit
save
```

Rotas e Conectividade da Rede

Sincronização de Estados (*State Synchronization*)

Definição de Zonas

Regras entre Zonas

Questões finais

1. Explain why the synchronization of the load-balancers allows the nonexistence of firewall synchronization.

R: A sincronização feita nos load balancers permite que os pedidos do cliente atinjam sempre o mesmo servidor, evitando que o firewall tenha de sincronizar estados entre os servidores.

Isto é feito através do conceito de *sticky sessions*, que permite que os pedidos do cliente sejam sempre encaminhados para o mesmo servidor, evitando que o firewall tenha de sincronizar estados entre os servidores.

2. Which load balancing algorithm may also allow the nonexistence of load-balancers synchronization?
3. Explain why device/connection states synchronization may be detrimental during a DDoS attack

Ponto 10 (Ainda não chegámos aqui)