



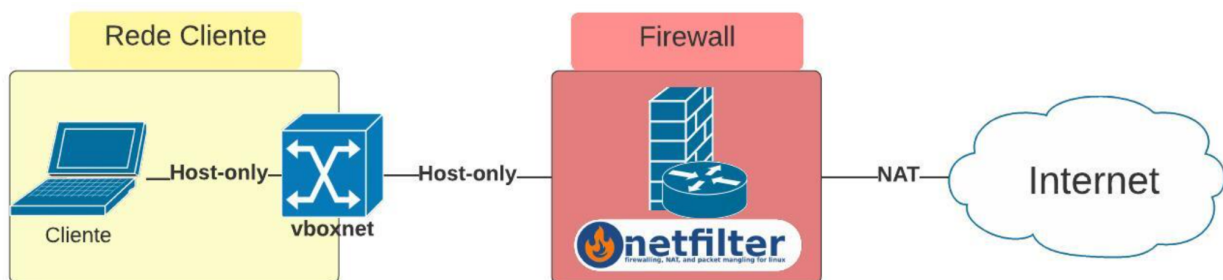
# Universidade Federal do Ceará

Disciplina: Segurança

Professor: Marcos Dantas Ortiz

## Exercícios – Iptables

- 1) Explicar o que as seguintes regras fazem:
  - a) iptables -t filter -A INPUT -s 192.168.0.0/24 -i eth1 -j ACCEPT
  - b) iptables -A INPUT -j LOG --log-prefix "FW INPUT"
  - c) iptables -I FORWARD -s 192.168.0.0/24 -d www.facebook.com -j DROP
  - d) iptables -A OUTPUT -o lo -j ACCEPT
  - e) iptables -D FORWARD -s 192.168.13.0/24 -d www.google.com -j REJECT
- 2) Criar regras necessárias para implantar as seguintes políticas de segurança no Firewall, utilizando cenário de rede virtualizado (virtualbox) abaixo:  
**Obs.: adicione nas respostas as regras e os prints dos tráfegos (quando possível)**



- a) Por padrão, o Firewall deve descartar todos os pacotes

### **Política DROP - INPUT, OUTPUT e FORWARD**

- b) Permitir o tráfego loopback no host do firewall.

Testar com ping (ICMP) para o próprio host - 127.0.0.1

- c) Permitir o acesso remoto via SSH ao Firewall.

*ssh user@ip\_do\_firewall*

d) Permitir a realização de ping ao Firewall (ICMP echo(8) e ICMP echo reply(0)).

*ping ip\_do\_firewall*

e) Permitir que o host do firewall faça requisições DNS.

*Testar com nslookup*

f) Permitir que a **rede cliente** faça requisições HTTP.

*Testar com wget*

g) Permitir que a **rede cliente** faça requisições HTTPS.

*Testar com wget*

h) Permitir que a **rede cliente** faça requisições DNS.

*Testar com nslookup*

d) Permitir a realização de ping pela **rede cliente** (ICMP echo(8) e ICMP echo reply(0)).

*ping ip\_externo*

**Bom Trabalho!**