Laboratório Avançado de Produção Pesquisa e Inovação em Software

# Relatório #01 de atividade da equipe de segurança

Rodolfo Cabral Neves

Brasília, aos 12 de Julho de 2024

## 1. Introdução

Este presente documento consiste no relatório de atividades que compreendeu a semana de 8 a 12 de julho de 2024, cujo objetivo é apresentar as vulnerabilidades encontradas, os impactos causados e as possíveis soluções e recomendações. O time é atualmente composto por Rodolfo Cabral Neves, o escopo da atividade é o ambiente de homologação do projeto **Brasil Participativo** - BP e foi avaliado toda a rede, incluindo o servidor **Wireguard**. A metodologia usada foi *grey box*, uma combinação de *black box* e *white box*.

## 1. Vulnerabilidades/riscos encontrados

Durante o processo de avaliação, foi identificado que todos os usuários da VPN podem se comunicar livremente com quaisquer servidores presentes, o que pode nos levar as seguintes vulnerabilidades:

- Acesso não autorizado
- Propagação de ameaças internas
- Dificuldade na detecção de atividades
- Comprometimento de dados sensíveis

## 2. Medidas de correção

Para a correção destas falhas, as configurações do firewall do servidor Wireguard foram atualizadas, e o RBAC - Role Based Access Control foi implementado usando a ferramente *iptables* , o que faz com que cada usuário se comunique com determinados servidores, segundo as suas funções. Eis a tabela de referência.

Eis o arquivo *postup.sh* onde estão todas as configurações:

```
# Como gerar script "/etc/wireguard/wg0_postdown.sh"
# grep "iptables" /etc/wireguard/wg0_postup.sh | grep -v "#" | sed -e "s/-A/-D/" | tee /etc/wireguard/wg0_postdown.sh
# Como listar regras
# iptables -L -v

# Regra padrao para FORWARD (nao precisa estar em postdown)
iptables -P FORWARD DROP

# Criar logs em /var/logs/iptables
iptables -A FORWARD -i wg0 -o ens192 -j LOG --log-prefix='[netfilter] '

# Usar ip do proprio Wireguard para acessar as outras maquinas
iptables -t nat -A POSTROUTING -o ens192 -j MASQUERADE -s 192.168.200.0/24

# Accept related or established traffic
iptables -A FORWARD -o wg0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT


# Acesso ping ao 192.168.3.1
```

```
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.1/24 -d 192.168.3.1 -p icmp --icmp-type echo-request

# Infra JoaoNobrega (exemplo de acesso em homolog)
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.8/32 -d 192.168.3.20
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.8/32 -d 192.168.3.21
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.8/32 -d 192.168.3.22
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.8/32 -d 192.168.3.30

# Brisa
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.31/32 -d 192.168.3.30
# GabrielZaranza
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.33/32 -d 192.168.3.30
# Isaque
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.39/32 -d 192.168.3.30
# GabrielScheidt
# iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.32/32 -d 192.168.3.30




# Equipe infra-lider
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.2/32 -d 192.168.3.0/24 # Francisco
iptables -A FORWARD -i wg0 -s 192.168.200.20/32 -d 192.168.3.0/24 -j ACCEPT # Francisco
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.12/32 -d 192.168.3.0/24 # Renato Coral
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.3/32 -d 192.168.3.0/24 # Leonardo
```

```
###
================================================================
================================================

### Equipe dados

# Criar o grupo dos ip's dos servidores de dados, por questões de organização
ipset create servidores_dados hash:ip -exist
ipset add servidores_dados 192.168.3.2
ipset add servidores_dados 192.168.3.20
ipset add servidores_dados 192.168.3.22

iptables -A FORWARD -i wg0 -s 192.168.200.4/32 -m set --match-set
servidores_dados dst -j ACCEPT # Isaque
iptables -A FORWARD -i wg0 -s 192.168.200.5/32 -m set --match-set
servidores_dados dst -j ACCEPT # Nitai
iptables -A FORWARD -i wg0 -s 192.168.200.6/32 -m set --match-set
servidores_dados dst -j ACCEPT # Paulo Goncalves
iptables -A FORWARD -i wg0 -s 192.168.200.7/32 -m set --match-set
servidores_dados dst -j ACCEPT # Joao Amoedo
iptables -A FORWARD -i wg0 -s 192.168.200.23/32 -m set --match-set
servidores_dados dst -j ACCEPT # lucasmaretti
iptables -A FORWARD -i wg0 -s 192.168.200.25/32 -m set --match-set
servidores_dados dst -j ACCEPT # Eric
iptables -A FORWARD -i wg0 -s 192.168.200.26/32 -m set --match-set
servidores_dados dst -j ACCEPT # wolfgang
###
================================================================
================================================

# Equipe DEX
iptables -A FORWARD -i wg0 -s 192.168.200.10/32 -m set --match-set
servidores_dados dst -j ACCEPT # matheusbeltrami
```

```
# Equipe pencillabs
# Criar o grupo dos ip's dos servidores da pencillabs, por questões de organização
ipset create servidores_pencillabs hash:ip -exist
ipset add servidores_pencillabs 192.168.3.2
ipset add servidores_pencillabs 192.168.3.20

iptables -A FORWARD -i wg0 -s 192.168.200.21/32 -m set --match-set servidores_pencillabs dst -j ACCEPT # davidcarlos

# Equipe segurança
iptables -A FORWARD -i wg0 -j ACCEPT -s 192.168.200.22/32 -d 192.168.3.0/24 # roddascabral, o pai grande
```

## 3. Conclusão

Após a configuração do *RBAC* por meio do *iptables*, a rede VPN de homologação está um pouco mais segura e as atividades de cada usuário terão rastreamento melhor, além do fato de que cada servidor só poderá responder as requisições dos endereços IP’s permitidos, entretanto é importante que as permissões de cada usuário estejam bem definidas.