**SUMARIO**

**INSTALAR PACOTES E CONFIGURAR O LADO SERVIDOR OPENVPN**

**CONFIGURAR O LADO CLIENTE DO OPENVPN**

**CONFIGURAR INTERFACE GRÁFICA PARA GERENCIAMENTO DA VPN**

**------------------------------------------------------------------------------------**

**NO SERVIDOR**

**INSTALAR OS PACOTES NECESSÁRIOS.**

yum install -y epel-release openvpn easy-rsa --enablerepo=epel

**FAZER UMA CÓPIA DO EXEMPLO DO ARQUIVO DE CONFIGURAÇÃO**

cp /usr/share/doc/openvpn-\*/sample/sample-config-files/server.conf /etc/openvpn

**EDITAR O ARQUIVO DE CONFIGURAÇÃO DO SERVIDOR**

vi /etc/openvpn/server.conf

**#Descomente a linha abaixo**

dh dh2048.pem

**#Configure o endereço de DNS**

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 8.8.8.8"  
push "dhcp-option DNS 8.8.4.4"

**#Copie a linha abaixo.**

cipher AES-256-CBC

**#Configure o usuário e grupo**

user nobody  
group nobody

**#Crie um diretório para as chaves**

mkdir -p /etc/openvpn/easy-rsa/keys

cp -rf /usr/share/easy-rsa/2.0/\* /etc/openvpn/easy-rsa

**#Edite a arquivo com as informações da chave.**

vi /etc/openvpn/easy-rsa/vars

Exemplo : . . .  
  
**# These are the default values for fields  
# which will be placed in the certificate.  
# Don't leave any of these fields blank.**  
export KEY\_COUNTRY="BR"  
export KEY\_PROVINCE="SP"  
export KEY\_CITY="São Paulo"  
export KEY\_ORG="Organização"  
export KEY\_EMAIL="alvkennedy@gmail.com"  
export KEY\_OU="Community"  
  
**# X509 Subject Field**  
export KEY\_NAME="server"  
  
. . .  
  
export KEY\_CN=openvpn.example.com  
  
. . .

**#Faça uma cópa do arquivo .cnf para o diretório de chaves**

cp /etc/openvpn/easy-rsa/openssl-1.0.0.cnf /etc/openvpn/easy-rsa/openssl.cnf

**#Entre no diretório do easy-rsa e recarregue o arquivo alterado agora pouco.**

cd /etc/openvpn/easy-rsa  
source ./vars

**#Limpa as chaves que já estão no diretório para gerarmos nossas novas chaves.**

./clean-all

**#Gerando o certificado, como já preenchemos o arquivo vars, basta pressionar enter nas opções.**

./build-ca

**#Gerando a chave para o servidor.**

./build-key-server server

**#Gerando o chave diffie-hellman**

./build-dh

**#Entre no diretório de chaves e copie as chaves para o diretório raiz da openvpn**

cd /etc/openvpn/easy-rsa/keys  
cp dh2048.pem ca.crt server.crt server.key /etc/openvpn

**#Gere a chave ta.key, no arquivo de configuração do lado server deve adicionar a linha tls-auth ta.key 0**

**#No lado cliente tls-auth ta.key 1**

openvpn --genkey --secret ta.key

vim /etc/openvpn/server.conf

...

tls-auth ta.key 0

...

**#Entre no diretório easy-rsa e gere as chaves para o cliente.**

cd /etc/openvpn/easy-rsa  
./build-key client

**#Instalando os pacotes e configurando as regras de firewall**

yum install iptables-services -y  
systemctl mask firewalld  
systemctl enable iptables  
systemctl stop firewalld  
systemctl start iptables  
iptables --flush

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE  
iptables-save > /etc/sysconfig/iptables

**#Edite o arquivo sysctl.conf e habilite o redirecionamento de pacotes**

vi /etc/sysctl.conf

net.ipv4.ip\_forward = 1

**#Reinicie a placa de rede e habilite a openvpn para iniciar automaticamente e inicie o serviço**

systemctl restart network.service

systemctl -f enable openvpn@server.service

systemctl start openvpn@server.service

**CLIENTE**

**#Copie os arquivos que estão no servidor para a máquina cliente.Os arquivos a serem copiados são:**

/etc/openvpn/easy-rsa/keys/ca.crt  
/etc/openvpn/easy-rsa/keys/client.crt  
/etc/openvpn/easy-rsa/keys/client.key

/etc/openvpn/ta.key

**#Adicione o conteúdo ao arquivo do cliente.**

vim /etc/openvpn/client.ovpn

client

dev tun

;proto tcp

proto udp

remote 179.228.51.168 1194

resolv-retry infinite

nobind

persist-key

persist-tun

;comp-lzo

cipher AES-256-CBC

verb 3

ca /etc/openvpn/keys/ca.crt

cert /etc/openvpn/keys/client.crt

key /etc/openvpn/keys/client.key

tls-auth /etc/openvpn/ta.key 1

**#Inicie a vpn no lado cliente**

sudo openvpn --config ~/path/to/client.ovpn

Regras de iptables atuais :

[root@localhost kalves]# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT udp -- anywhere anywhere udp dpt:domain

ACCEPT tcp -- anywhere anywhere tcp dpt:domain

ACCEPT udp -- anywhere anywhere udp dpt:bootps

ACCEPT tcp -- anywhere anywhere tcp dpt:bootps

Chain FORWARD (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere 192.168.122.0/24 ctstate RELATED,ESTABLISHED

ACCEPT all -- 192.168.122.0/24 anywhere

ACCEPT all -- anywhere anywhere

REJECT all -- anywhere anywhere reject-with icmp-port-unreachable

REJECT all -- anywhere anywhere reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

ACCEPT udp -- anywhere anywhere udp dpt:bootpc

[root@localhost kalves]#

----------------------------------------------------------------------------------------------------------------

[root@localhost kalves]# iptables -t nat -L

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

RETURN all -- 192.168.122.0/24 base-address.mcast.net/24

RETURN all -- 192.168.122.0/24 255.255.255.255

MASQUERADE tcp -- 192.168.122.0/24 !192.168.122.0/24 masq ports: 1024-65535

MASQUERADE udp -- 192.168.122.0/24 !192.168.122.0/24 masq ports: 1024-65535

MASQUERADE all -- 192.168.122.0/24 !192.168.122.0/24

RETURN all -- 192.168.122.0/24 base-address.mcast.net/24

RETURN all -- 192.168.122.0/24 255.255.255.255

MASQUERADE tcp -- 192.168.122.0/24 !192.168.122.0/24 masq ports: 1024-65535

MASQUERADE udp -- 192.168.122.0/24 !192.168.122.0/24 masq ports: 1024-65535

MASQUERADE all -- 192.168.122.0/24 !192.168.122.0/24

MASQUERADE all -- 10.8.0.0/24 anywhere

MASQUERADE all -- anywhere anywhere

MASQUERADE all -- anywhere anywhere

MASQUERADE all -- 10.8.0.0/24 anywhere

MASQUERADE all -- 10.8.0.0/24 anywhere

[root@localhost kalves]#

**CONFIGURAR ACESSO VIA WEB OPENVPN**

Fazer Download do pacote através do endereço

<https://openvpn.net/index.php/access-server/download-openvpn-as-sw/113.html?osfamily=CentOS>

#Instalar o pacote baixado

rpm -i openvpn-as-2.1.4-CentOS7.x86\_64.rpm

...

The Access Server has been successfully installed in /usr/local/openvpn\_as

Configuration log file has been written to /usr/local/openvpn\_as/init.log

Please enter "passwd openvpn" to set the initial

administrative password, then login as "openvpn" to continue

configuration here: https://192.168.0.112:943/admin

To reconfigure manually, use the /usr/local/openvpn\_as/bin/ovpn-init tool.

Access Server web UIs are available here:

Admin UI: https://192.168.0.112:943/admin

Client UI: https://192.168.0.112:943/

#Alterar a senha do usuário openvpn

passwd openvpn

Mudando senha para o usuário openvpn.

Nova senha:

Redigite a nova senha:

passwd: todos os tokens de autenticação foram atualizados com sucesso.

<https://192.168.0.112:943/admin>

user: openvpn

pass: \*\*\*\*\*\*\*