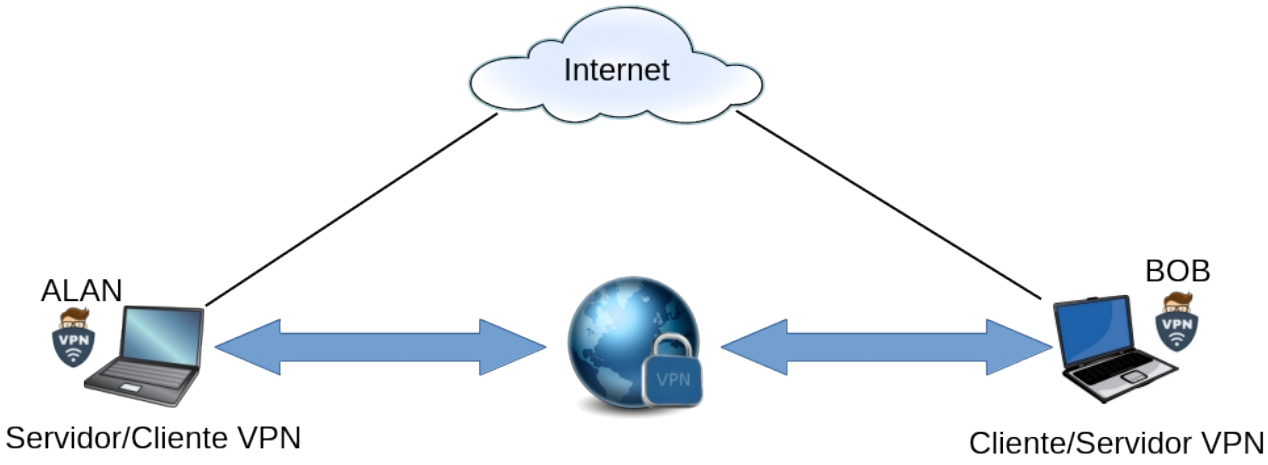
Configurações de VPN

Cenário 01

VPN sem criptografia. Máquinas autônomas se conectam diretamente.



Servidor/Cliente

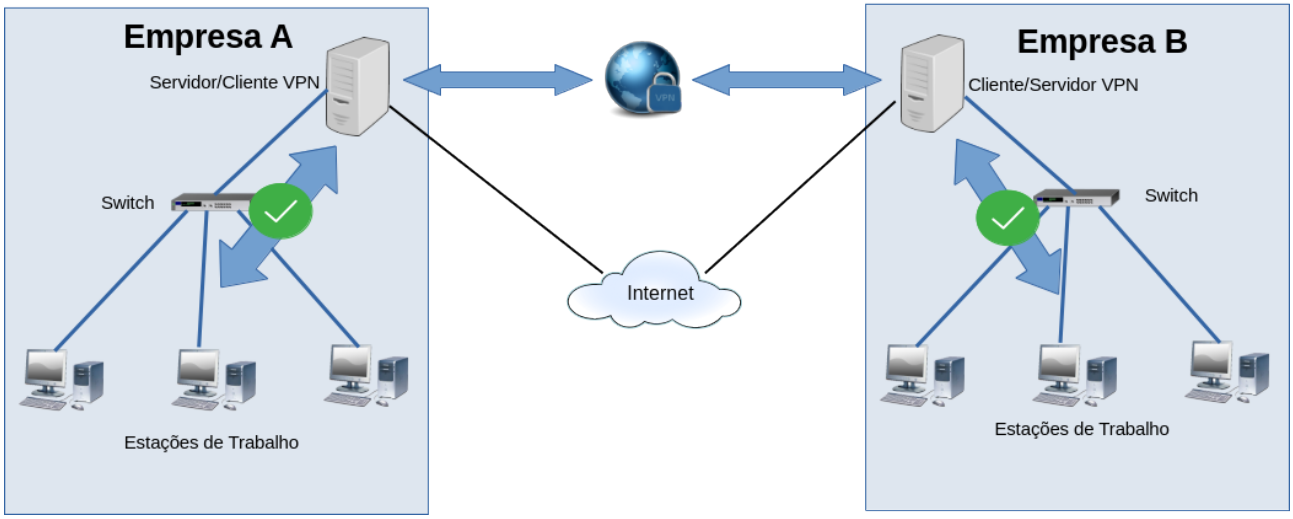
```
# openvpn --remote 10.3.1.6 --dev tun --ifconfig  172.16.0.5 172.16.0.6
```

Cliente/Servidor

```
# openvpn --remote 10.3.1.5 --dev tun --ifconfig  172.16.0.6 172.16.0.5
```

Cenário 02

VPN sem criptografia. Servidores autônomos se conectam diretamente e permitem que as máquinas internas das empresas também se comuniquem entre si.



Servidor/Cliente

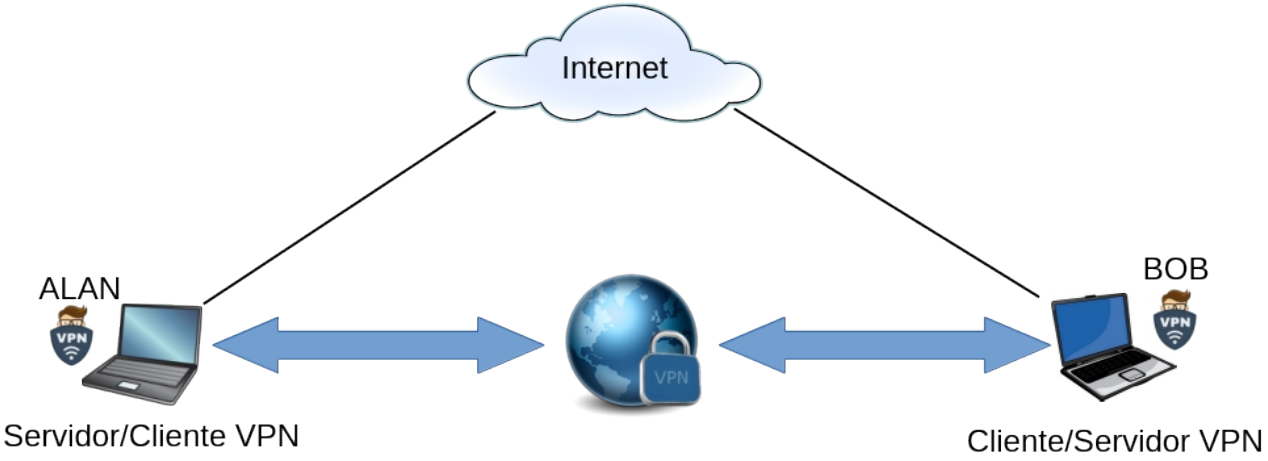
```
# openvpn --remote 10.3.1.6 --dev tun --ifconfig  172.16.0.5 172.16.0.6

# ip route add 192.168.6.0/24 via 172.16.0.6
```

Cliente/Servidor

```
# openvpn --remote 10.3.1.5 --dev tun --ifconfig  172.16.0.6 172.16.0.5

# ip route add 192.168.5.0/24 via 172.16.0.5
```

Cenário 03

VPN com criptografia simétrica. Máquinas autônomas se conectam diretamente.



Servidor/Cliente

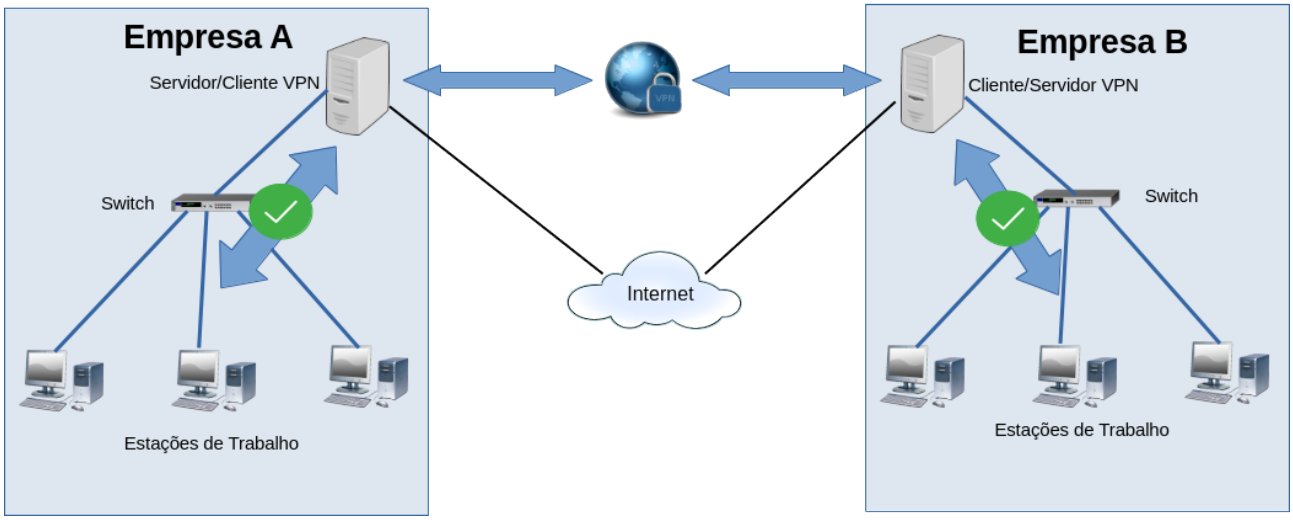
```
# openvpn --genkey secret chave-estatica.key

# openvpn --remote 10.3.1.6 --dev tun --ifconfig 172.16.0.5 172.16.0.6 --secret ./chave-estatica.key --cipher AES-256-CBC
```

Cliente/Servidor

```
# openvpn --remote 10.3.1.5 --dev tun --ifconfig 172.16.0.6 172.16.0.5 --secret ./chave-estatica.key --cipher AES-256-CBC
```

Cenário 04

VPN com criptografia simétrica. Servidores autônomos se conectam diretamente e permitem que as máquinas internas das empresas também se comuniquem entre si.



Servidor/Cliente

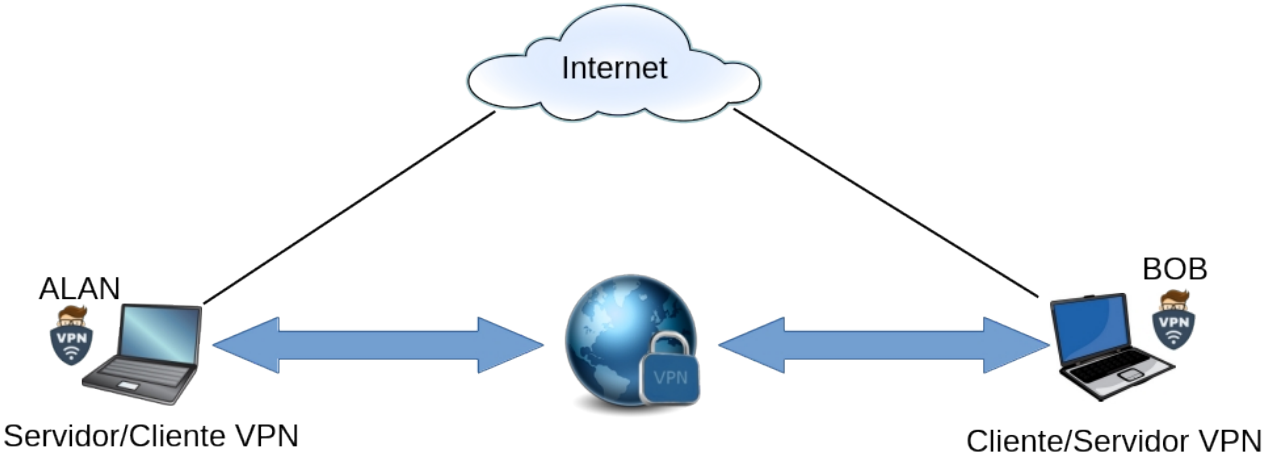
```
# openvpn --genkey secret chave-estatica.key

# openvpn --remote 10.3.1.6 --dev tun --ifconfig 172.16.0.5 172.16.0.6 --secret ./chave-estatica.key --cipher AES-256-CBC

# ip route add 192.168.6.0/24 via 172.16.0.6
```

Cliente/Servidor

```
# openvpn --remote 10.3.1.5 --dev tun --ifconfig 172.16.0.6 172.16.0.5 --secret ./chave-estatica.key --cipher AES-256-CBC

# ip route add 192.168.5.0/24 via 172.16.0.5
```

Cenário 05

VPN com criptografia assimétrica. Máquinas autônomas se conectam diretamente.



Servidor.conf

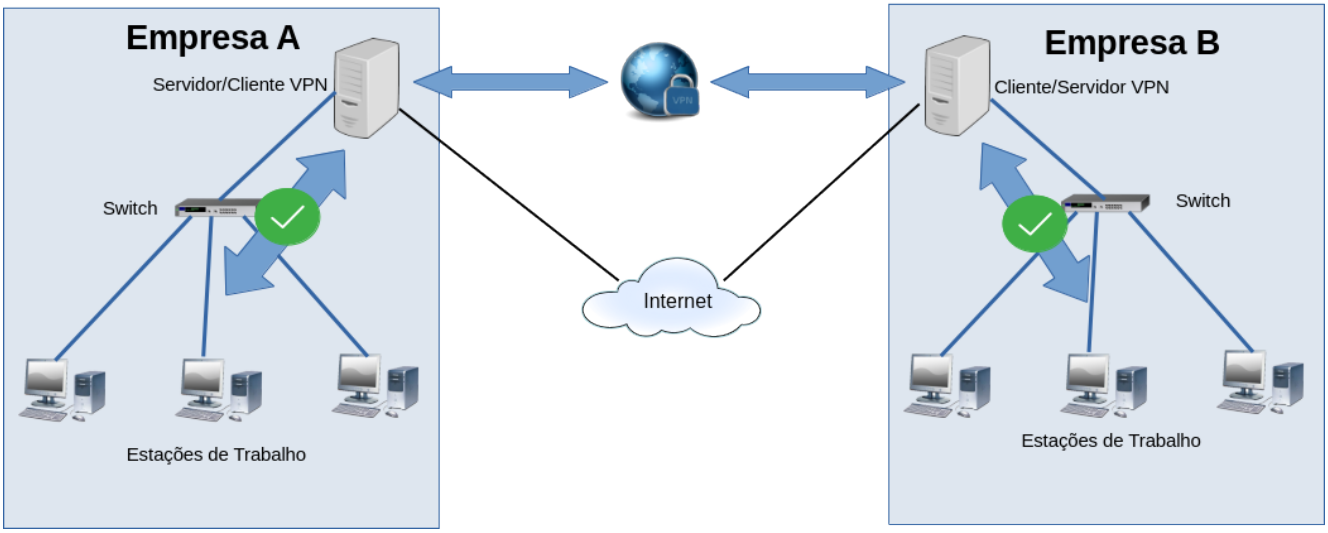
```
dev tun
ifconfig 172.16.0.5 172.16.0.6

# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
ifconfig 172.16.0.6 172.16.0.6

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cenário 06

VPN com criptografia assimétrica. Servidores autônomos se conectam diretamente e permitem que as máquinas internas das empresas também se comuniquem entre si.



Servidor.conf

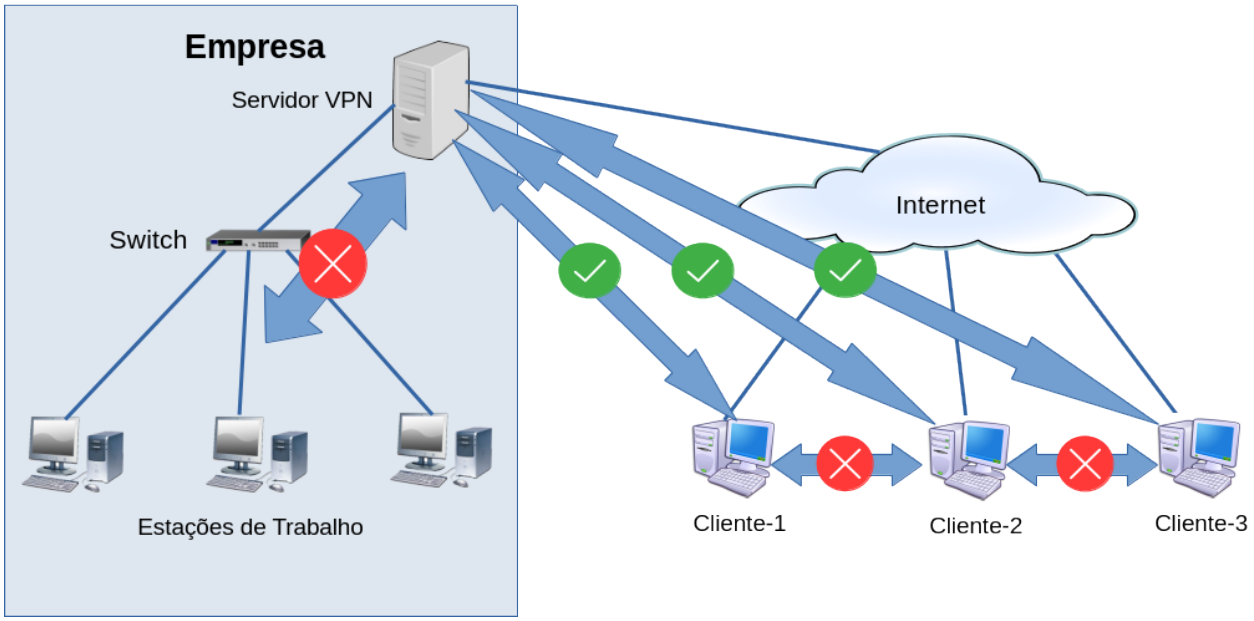
```
dev tun
ifconfig 172.16.0.5 172.16.0.6
push "route 192.168.5.0 255.255.255.0"
route 192.168.6.0 255.255.255.0

# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
ifconfig 172.16.0.6 172.16.0.5
pull

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Coreção para compatibilidade
cipher AES-256-GCM
```

Cenário 07

Clientes conseguem se conectar diretamente ao Servidor VPN mas não conseguem se comunicar entre si e nem com as máquinas internas da empresa.



Servidor.conf

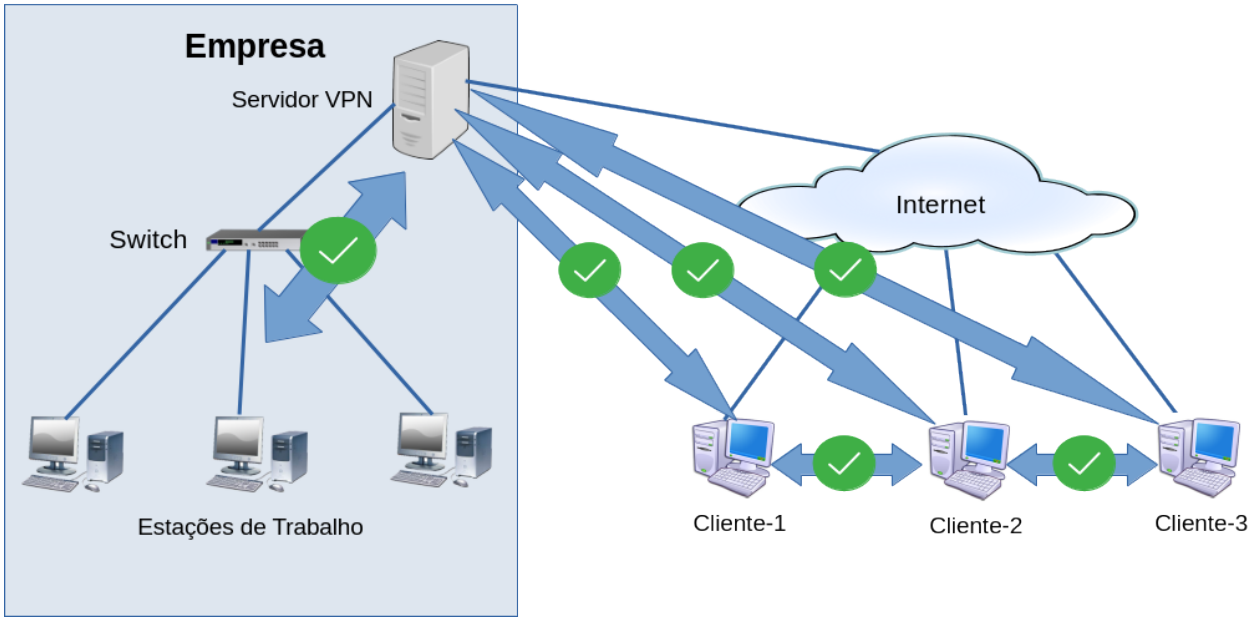
```
dev tun
server 172.16.5.0 255.255.255.0


# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
client

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cenário 08

Clientes conseguem se conectar diretamente ao Servidor VPN e também conseguem se comunicar entre si e com as máquinas internas da empresa.



Servidor.conf

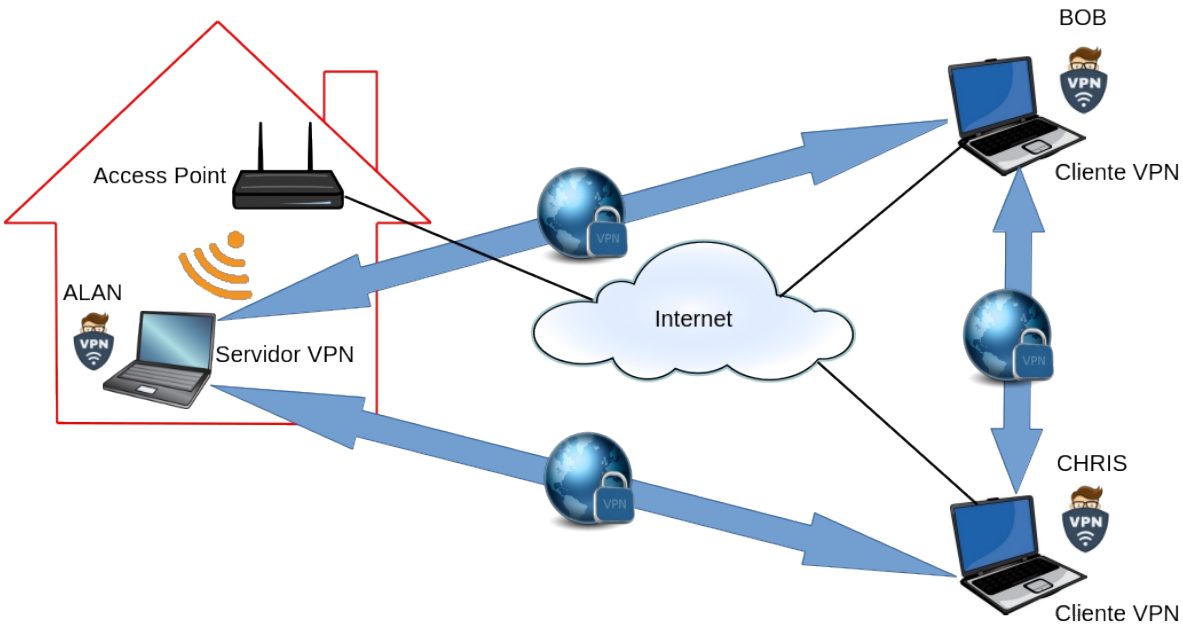
```
dev tun
server 172.16.5.0 255.255.255.0
topology subnet
push "route 192.168.5.0 255.255.255.0"

# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
client
pull

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cenário 09

Clientes conseguem se conectar ao Servidor VPN passando pelo Firewall do Acces-Point e também conseguem se comunicar entre si.



Servidor.conf

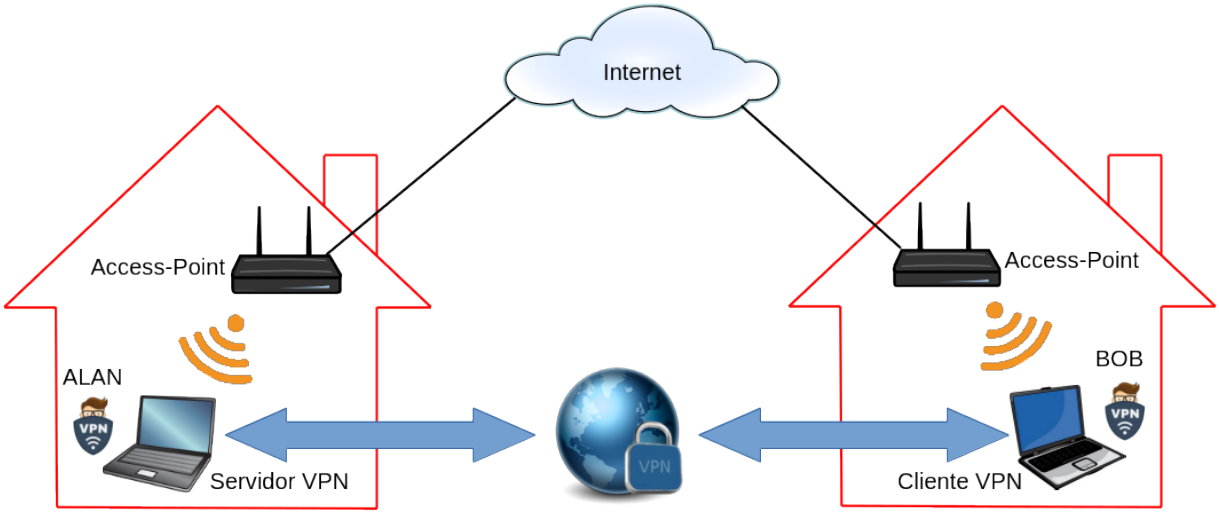
```
dev tun
server 172.16.5.0 255.255.255.0
topology subnet

# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
client

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cenário 10

Servidor e Cliente VPN conseguem se conectar passando pelo Firewall do Acces-Point e conseguem se comunicar com as máquinas internas das duas casas.



Servidor.conf

```
dev tun
ifconfig 172.16.0.5 172.16.0.6
push "route 192.168.5.0 255.255.255.0"
route 192.168.6.0 255.255.255.0

# Criptografia
tls-server
dh /etc/openvpn/keys/dh.pem
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada5.crt
key /etc/openvpn/keys/bancada5.key

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Correção para compatibilidade
cipher AES-256-GCM
```

Cliente.conf

```
remote 10.3.1.5
dev tun
ifconfig 172.16.0.6 172.16.0.5
pull

# Criptografia
tls-client
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/bancada6.crt
key /etc/openvpn/keys/bancada6.key

# Autenticação
askpass /etc/openvpn/client/auth.txt

# Ajuste fino
keepalive 10 60
comp-lzo
persist-key
persist-tun
float

# Coreção para compatibilidade
cipher AES-256-GCM
```