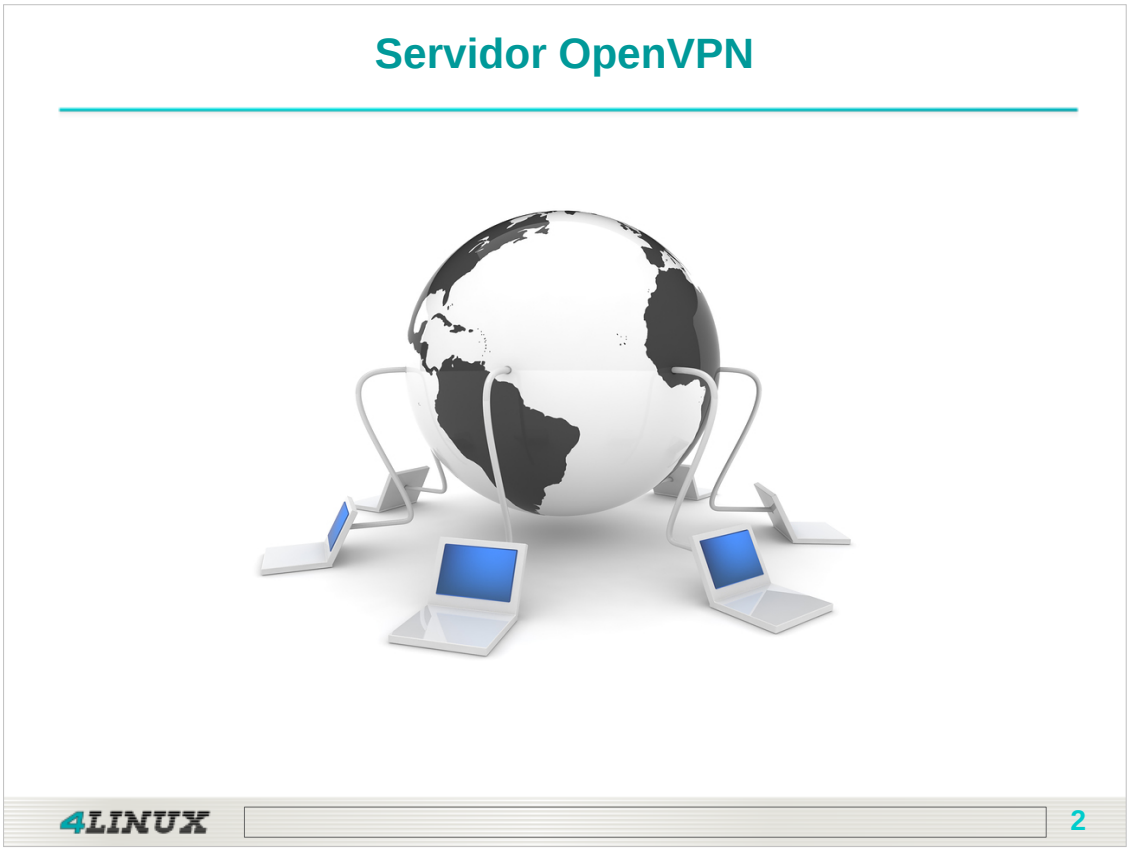
Curso 452

Linux Security Servers in Cloud

Versão 2015_3.0

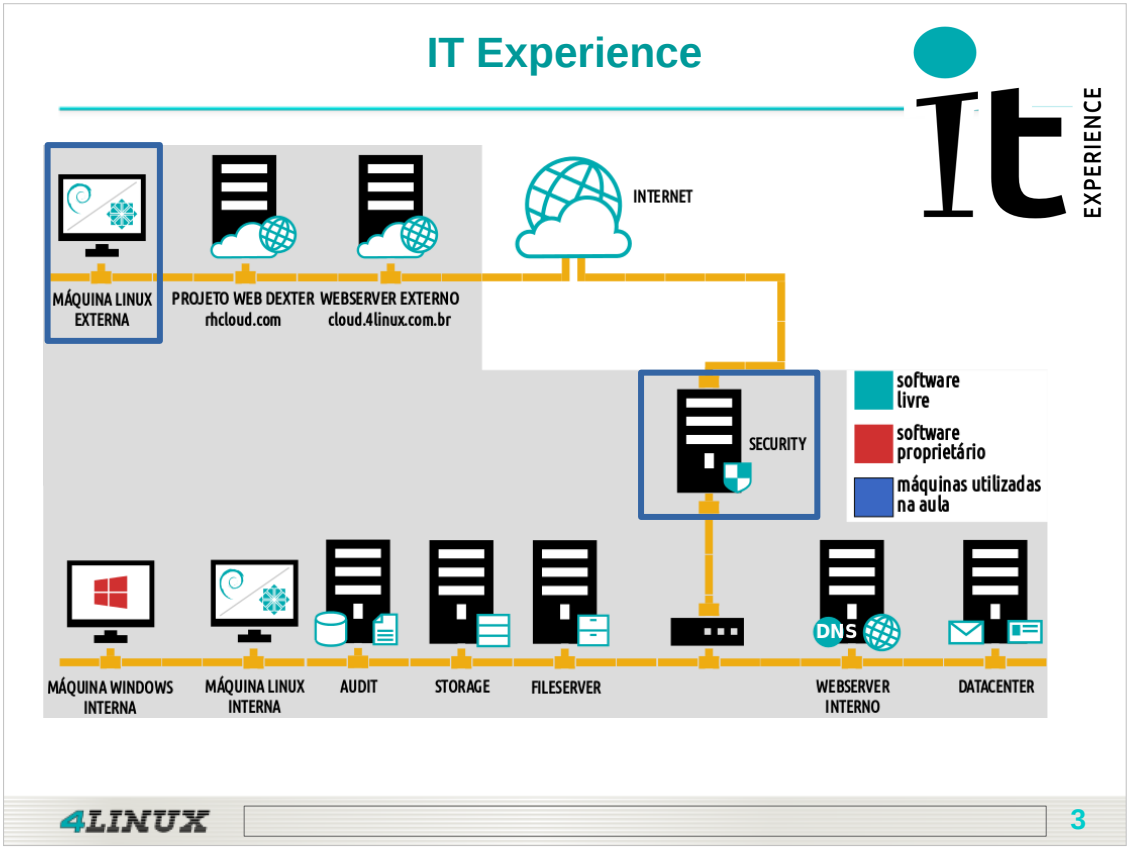


Cenário

Visto que a empresa DEXTER COURIER possui alguns colaboradores fora do ambiente corporativo (home-office), ela precisa de uma forma segura para que eles possam acessar a rede da empresa.

Proposta de solução

Com a flexibilidade das conexões proporcionadas com Internet hoje em dia, vimos um crescente aumento de colaboradores que necessitam estar em muitos lugares e ao mesmo tempo conectados na empresa. Para isto devemos montar uma estrutura de VPN com autenticação criptografada, elevando assim a segurança dos acessos externos.


IT Experience
IT EXPERIENCE
INTERNET
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
SECURITY
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
STORAGE
FILESERVER
DNS
WEBSERVER INTERNO
DATACENTER
4LINUX
3

Anotações:

Objetivos da Aula

Aula 08

- Introdução a VPN;
- Conhecer os tipos de VPN;
- Implementar VPN Host-to-gateway;
- Configurar certificado para servidor e clientes;
- Revogar certificado na VPN.

Anotações:

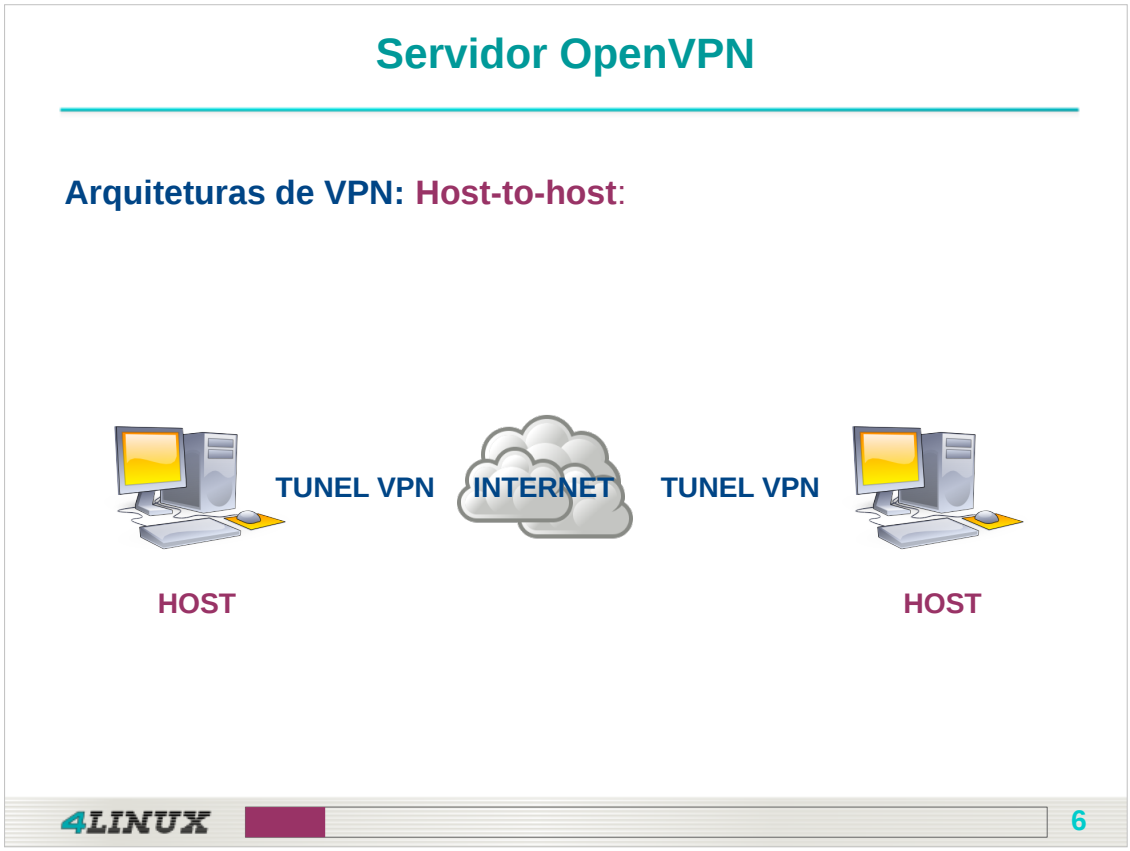
Servidor OpenVPN

Introdução a VPN:

A VPN (Virtual Private Network) é uma rede de comunicação particular, geralmente utilizando canais de comunicação inseguros, como a "LAN" ou mesmo a WAN (Internet).

O que torna esta rede de comunicação particular é o fato das ferramentas de "VPN" empregarem métodos e protocolos de criptografia, criando um túnel para prover acesso seguro a partes da rede ou mesmo ligação entre "LAN's" geograficamente separadas.

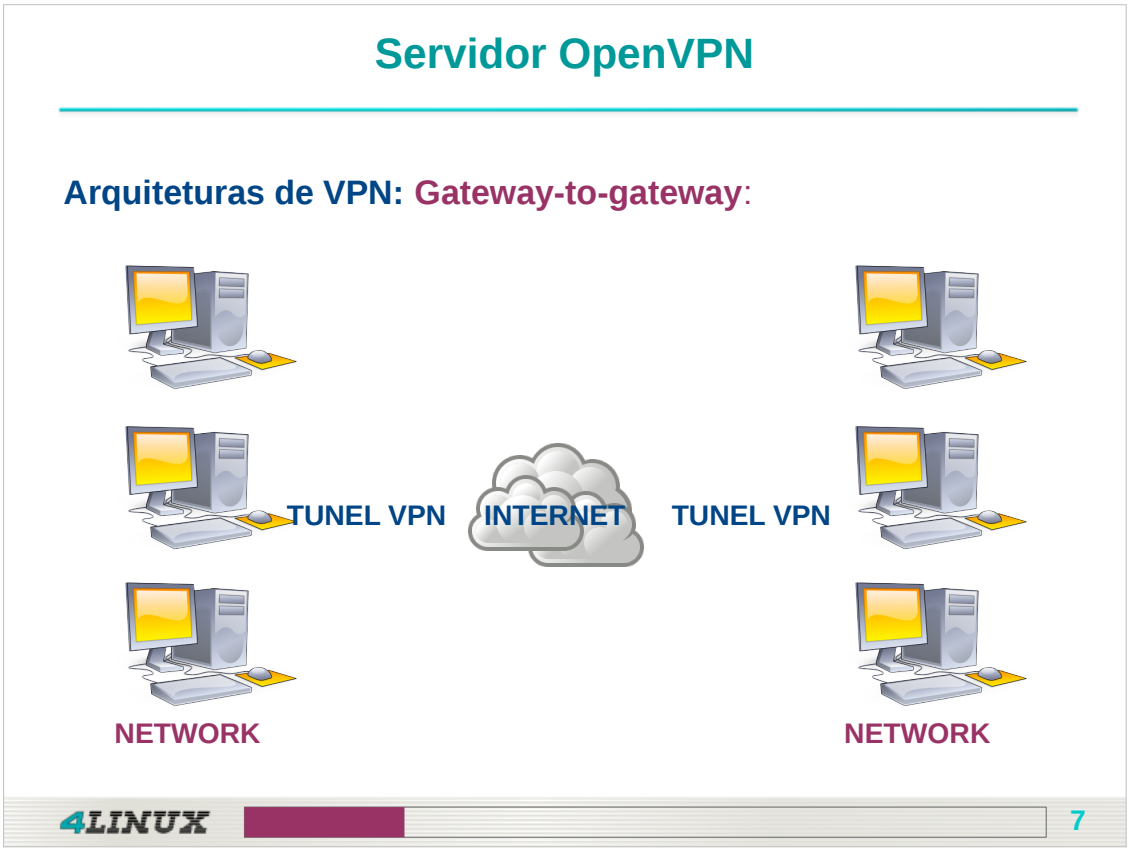
Anotações:



Arquitetura de VPNs

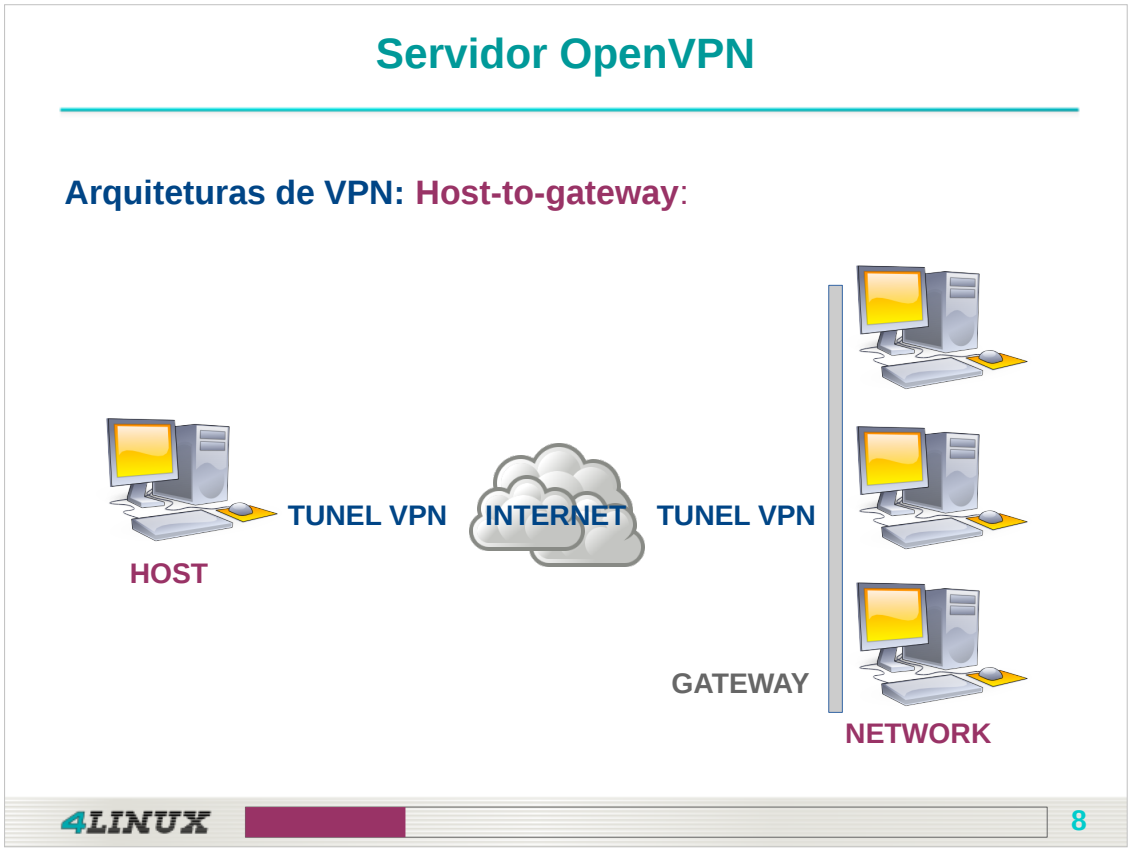
Host-to-host: VPN criada para proteger a comunicação entre dois computadores específicos.

Utilizada, geralmente, quando pequeno numero de usuários têm que administrar remotamente um sistema;



Arquitetura de VPNs

Gateway-to-gateway: VPN criada para proteger a comunicação entre 2 redes, por exemplo a rede da matriz de uma companhia interligada a rede de um escritório da mesma companhia.



Arquitetura de VPNs

Host-to-gateway: VPN criada para a proteção da conexão entre um ou mais usuários e uma rede específica, por exemplo, entre os funcionários longe da sede da empresa e a rede da empresa.

Servidor OpenVPN

Implementando VPN Host-to-gateway:

```
1# apt-get install openvpn
2# cp -r /etc/openvpn /etc/openvpn.bkp
3# rm -rf /etc/openvpn/*
4#    cp    -a    /usr/share/doc/openvpn/examples/easy-rsa/2.0
/etc/openvpn/
5# cp /etc/openvpn.bpk/update-resolv-conf /etc/openvpn/
6# cd /etc/openvpn/2.0 ; mkdir keys
7# apt-get install openssl
```


Anotações:

Servidor OpenVPN

Servidor: Security

Implementando VPN Host-to-gateway:

```
1# vim vars
export KEY_SIZE=2048
export KEY_COUNTRY="BR"
export KEY_PROVINCE="SP"
export KEY_CITY="SaoPaulo"
export KEY_ORG="Dexter Courier"
export KEY_OU="TI"
export KEY_EMAIL="admin@dexter.com.br"
export KEY_CN="security"
export KEY_NAME="Dexter CA"
```


Anotações:

Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Criação do CA:

```
1# source vars
2# ./clean-all
3# ./build-ca
....
Country Name (2 letter code) [BR]:(Tecle Enter)
State or Province Name (full name) [SP]:(Tecle Enter)
Locality Name (eg, city) [SaoPaulo]:(Tecle Enter)
```


Anotações:

Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Criação do CA:

```
Organization Name (eg, company) [Dexter Courier]:(Tecle Enter)
Organizational Unit Name (eg, section) [TI]:(Tecle Enter)
Common Name (eg, your name or your server's hostname)[Dexter CA]: (Tecle Enter)
Name [Dexter CA]: (Tecle Enter)
Email Address [admin@dexter.com.br]:(Tecle Enter)
State or Province Name (full name) [SP]:(Tecle Enter)
```


Anotações:

Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Certificado do servidor:

```
1# ./build-key-server security
Country Name (2 letter code) [BR]:(Tecle Enter)
State or Province Name (full name) [SP]:(Tecle Enter)
Locality Name (eg, city) [SaoPaulo]:(Tecle Enter para)
Organization Name (eg, company) [Dexter Courier]:(Tecle Enter)
Organizational Unit Name (eg, section) [TI]:(Tecle Enter)
Common Name (eg, your name or your server's hostname) [server]:
(Tecle Enter)
```


Anotações:

Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Certificado do servidor:

```
Name [Dexter CA]: (Tecle Enter)

Email Address [admin@dexter.com.br]: (Tecle Enter)

A challenge password []: (Tecle Enter)

An optional company name []: (Tecle Enter)

Certificate is to be certified until Aug 16 08:41:49 2022 GMT
(3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
```


Anotações:

Melhorando a segurança na VPN

Servidor: Security

- Para aumentar a segurança na VPN os parâmetros Diffie-Hellman são utilizados para a troca das chaves criptografadas durante a execução do OpenVPN.
- Use o script abaixo para gerar os parâmetros:

```
1# ./build-dh
2# ls -l keys/
```


Anotações:

Servidor OpenVPN

Servidor: Security

Arquivo de configuração do servidor VPN:

```
1# vim /etc/openvpn/security.conf
dev tun
proto udp
server 10.0.0.0 255.255.255.0
push "dhcp-option DNS 192.168.200.30"
push "dhcp-option DNS 8.8.8.8"
push "route 192.168.200.0 255.255.255.0"
push "route 192.168.200.128 255.255.255.128"
```

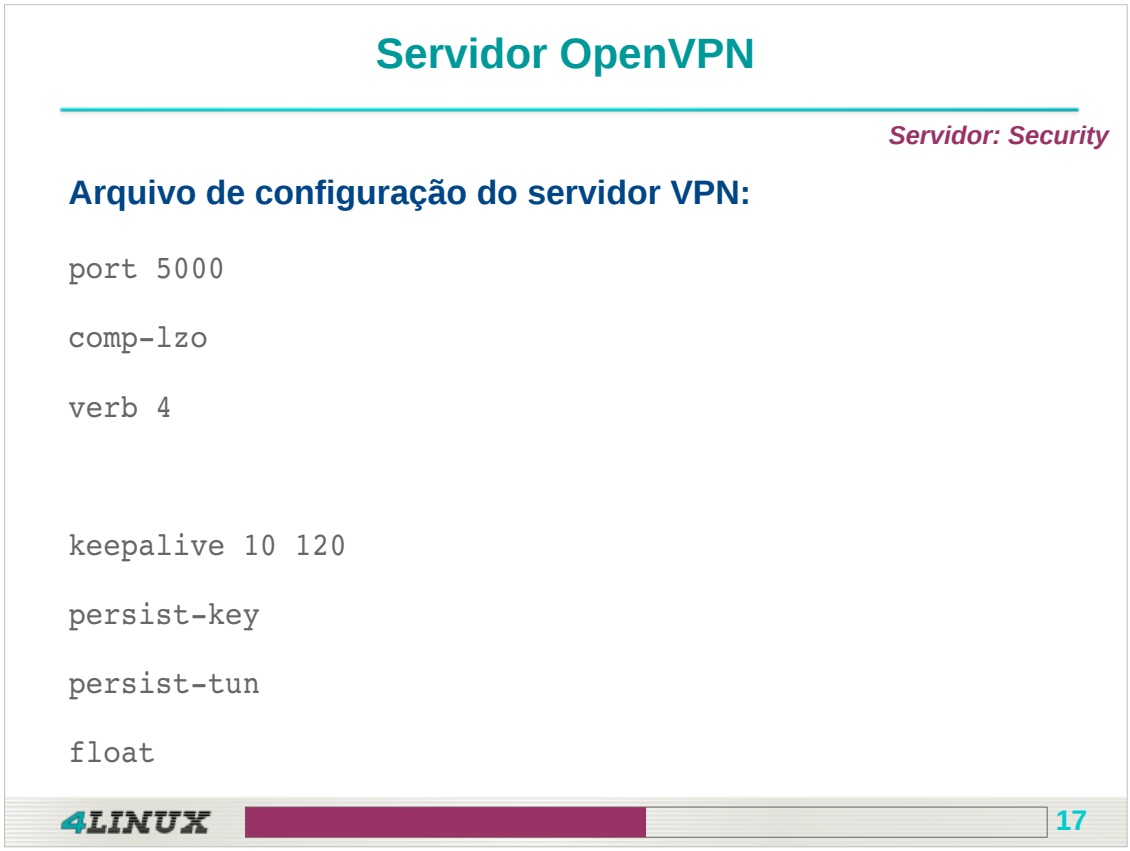

Descrição da diretivas:

dev: Habilita suporte ao driver TUN/TAP;

proto: Define qual protocolo o servidor ira escutar na porta;

server : Define uma faixa de endereços IP para a VPN, e permite que o servidor atribua endereços para os clientes conforme eles se conectam. Esta configuração permite que vários clientes se conectem simultaneamente à VPN.

push: Permite que o servidor inclua uma regra de roteamento na configuração do cliente no momento da conexão. A rota sera definida da rede Classe A para rede Classe C.



Descrição da diretivas:

port: Define a porta que o OpenVPN vai rodar;

comp-lzo: Ativa suporte a compressão;

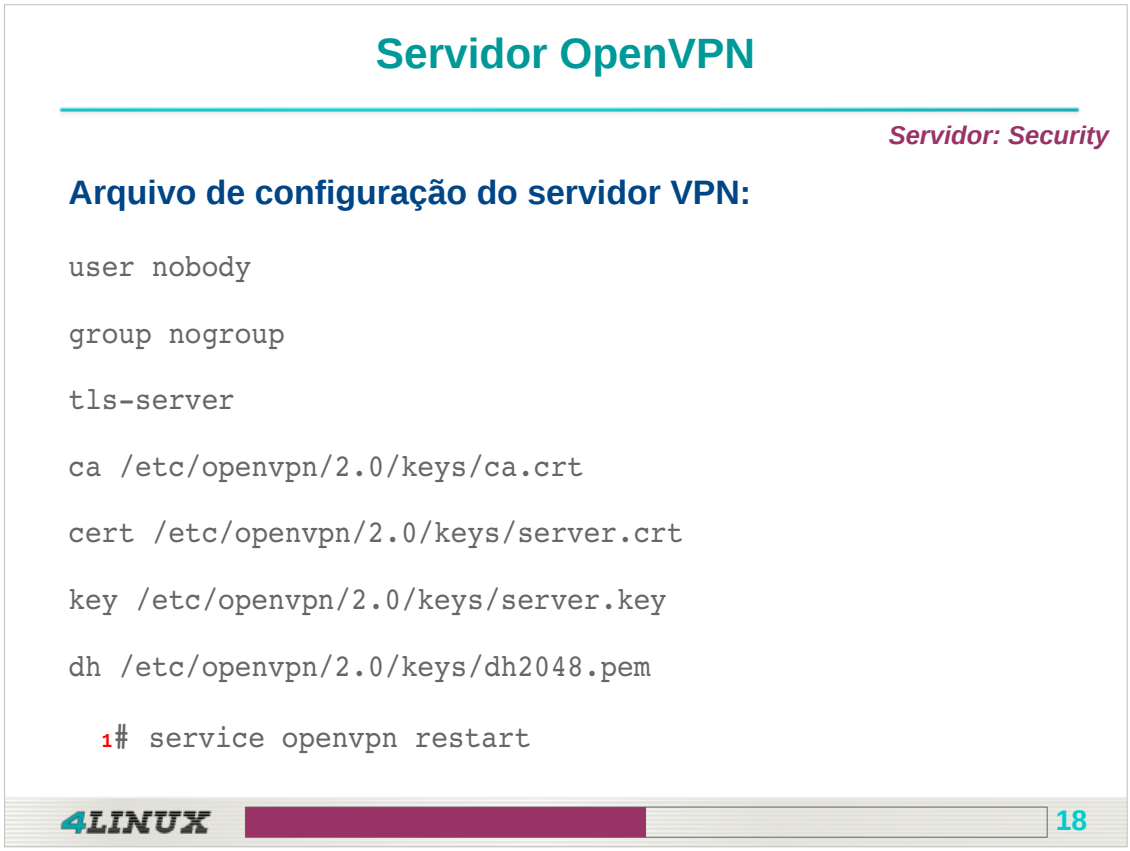
verb: Nível para depuração de erros;

keepalive: Envia um ping a cada 10 segundos sem atividade e a VPN é reiniciada depois de 120 segundos sem respostas;

persist-key: Assegura que o daemon mantenha as chaves carregadas, quando a VPN é restabelecida depois de uma queda de conexão;

persist-tun: Assegura que o daemon mantenha a interface tun aberta, quando a VPN é restabelecida depois de uma queda de conexão;

float: Permite que o túnel continue aberto mesmo que o endereço IP da outra máquina mude.



Descrição da diretivas:

user: Remoção dos privilégios de root na conexão VPN para usuário;

group: Remoção dos privilégios de root na conexão VPN para grupo;

tls-server: Ajuda a bloquear ataques DoS e flooding na porta do OpenVPN;

ca: Certificado de autoridade (CA) que usa as bibliotecas do OpenSSL;

cert: Certificado do servidor;

key: have RSA de 2048 do servidor;

dh: Parâmetros Diffie-Hellman utilizado para a troca das chaves criptografadas durante a execução.

Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Certificado do cliente:

```
1# ./build-key linux-externa
```

```
Country Name (2 letter code) [BR]:(Tecle Enter)
State or Province Name (full name) [SP]:(Tecle Enter)
Locality Name (eg, city) [SaoPaulo]:(Tecle Enter)
Organization Name (eg, company) [Dexter Courier]:(Tecle
Enter)
Organizational Unit Name (eg, section) [TI]:(Tecle Enter)
Common Name (eg, your name or your server's hostname)
[linux-externa]:(Tecle Enter)
```


Anotações:

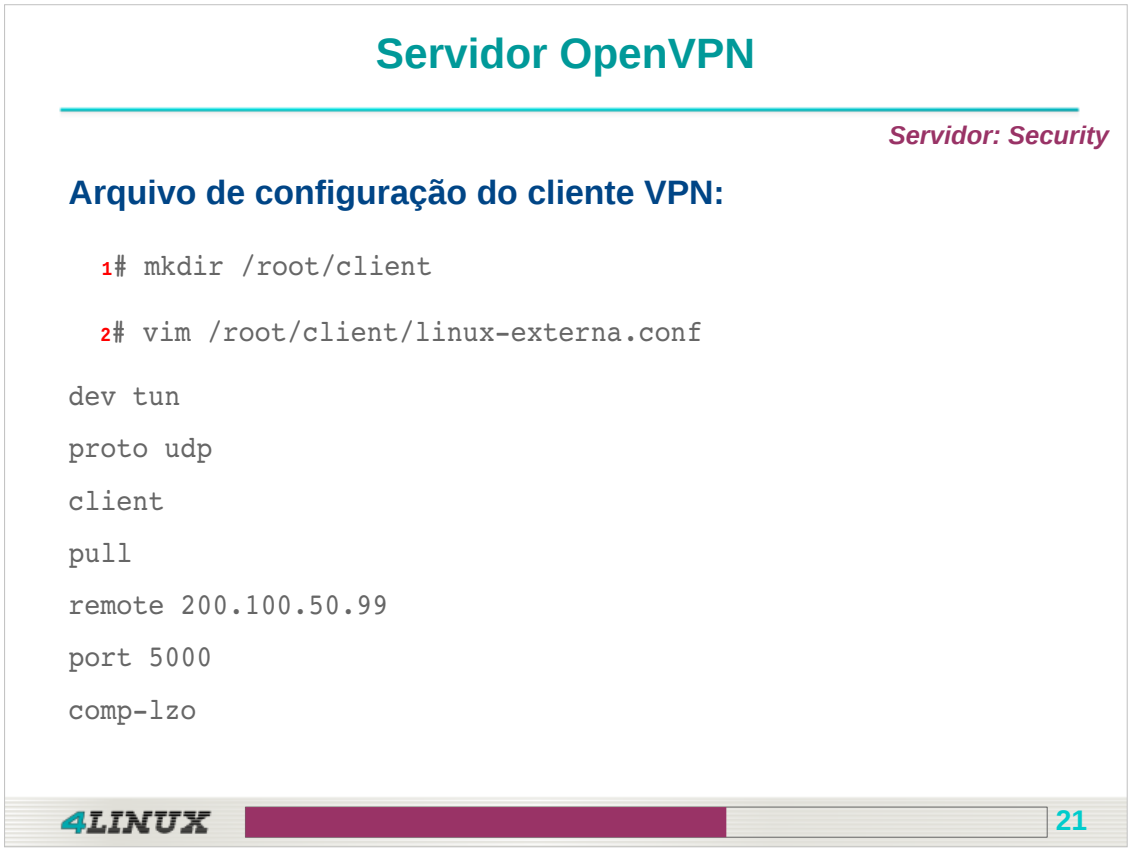
Servidor OpenVPN

Servidor: Security

VPN Host-to-gateway: Certificado do cliente:

```
Name [Dexter CA]:(Tecle Enter)

Email Address [admin@dexter.com.br]:linux-externa@dexter.com.br

A challenge password []: (Tecle Enter)

An optional company name []: (Tecle Enter)

Certificate is to be certified until Aug 16 08:41:49 2022 GMT
(3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
```


Anotações:



Descrição da diretivas:

client: Define que a maquina é um cliente VPN;

pull: Define que o cliente aceite configurações fornecidas pelo servidor; **remote** : Define o hostname/IP do servidor VPN (endereço publico);

Servidor OpenVPN

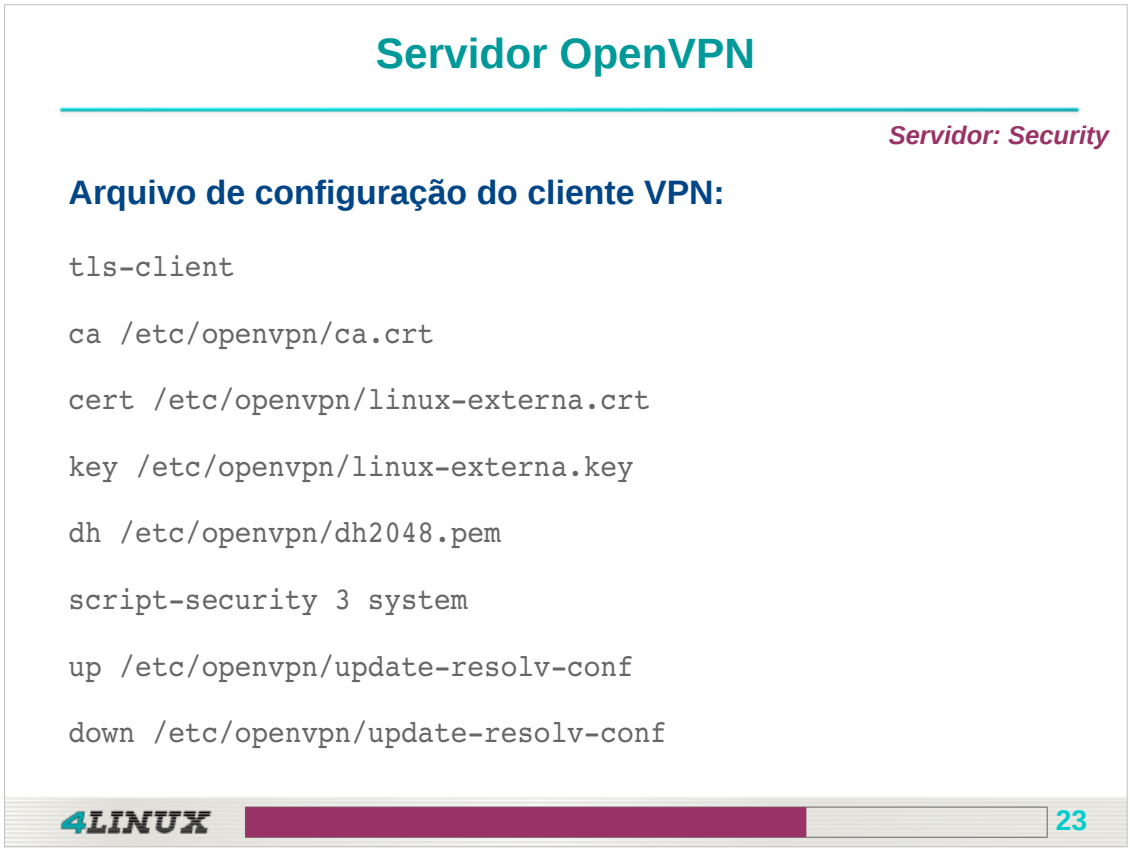
Servidor: Security

Arquivo de configuração do cliente VPN:

```
verb 4

keepalive 10 120

persist-key

persist-tun

float

user nobody

group nogroup

ns-cert-type server
```


Descrição da diretivas:

dns-cert-type: Indica que certificado foi assinado pelo servidor;



Descrição da diretivas:

tls-client: Habilita conexão TLS, ajudando a bloquear ataques DoS e flooding na porta do OpenVPN;

script-security: Permite executar scripts personalizados.

Servidor OpenVPN

Servidor: Security

Preparando o pacote de configuração do cliente VPN:

```
1# cd keys
2# cp ca.crt dh2048.pem linux-externa.crt linux-externa.key
/root/client/
3# cd /root/client/
4# tar czvf linux-externa.tar.gz *
```


Anotações:

Servidor OpenVPN

Servidor: Audit

Liberar acesso dos clientes VPN no DNS da DEXTER:

```
1# vim /etc/bind/named.conf.options
....
allow-query      {      200.100.50.0/24;      192.168.200.0/24;
192.168.200.128/25; 10.0.0.0/24; 127.0.0.1; };
allow-recursion    {    192.168.200.0/24;    192.168.200.128/25;
10.0.0.0/24; 200.100.50.0/24; 127.0.0.1; };

2# service bind9 restart
```


Anotações:

Servidor OpenVPN

Servidor: Linux Externa

Preparando o pacote de configuração do cliente VPN:

```
1# apt-get install openvpn resolvconf
2# scp  200.100.50.99:/root/client/linux-externa.tar.gz .
3# tar xzvf linux-externa.tar.gz -C /etc/openvpn
4# service openvpn restart && service resolvconf restart
5# ifconfig tun0
6# ping -c4 10.0.0.1 && ping -c4 192.168.200.30 && ping -c4
192.168.200.130
7# ping intranet.dexter.com.br
```


Anotações:

Servidor OpenVPN

Revogação de certificado no servidor:

A revogação de um certificado é um método para invalidar um certificado previamente assinado, de modo que o mesmo não pode ser utilizado para fins de autenticação.

Razões típicas para revogar um certificado de cliente:

- **A chave privada ao certificado é comprometida ou roubada;**
- **O usuário esquece a senha da chave;**
- **Você precisa encerrar o acesso de um usuário a VPN.**

Anotações:

Servidor OpenVPN

Servidor: Security

Revogação de certificado no servidor:

```
1# cd /etc/openvpn/2.0
2# source vars
3# ./revoke-full linux-externa
4# cp keys/crl.pem /etc/openvpn/
5# vim /etc/openvpn/server.conf
.....
crl-verify /etc/openvpn/crl.pem
6# service openvpn restart
```


Anotações:

Servidor OpenVPN

Qual é diretiva utilizada na revogação de certificados no OpenVPN?

A. crl-verify

B. comp-lzo

C. persist-key

D. keepalive

Anotações:

Servidor OpenVPN

Qual é a diretiva utilizada na revogação de certificados no OpenVPN?

A. crl-verify

B. comp-lzo

C. persist-key

D. keepalive

Resposta: alternativa A

Anotações:

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!