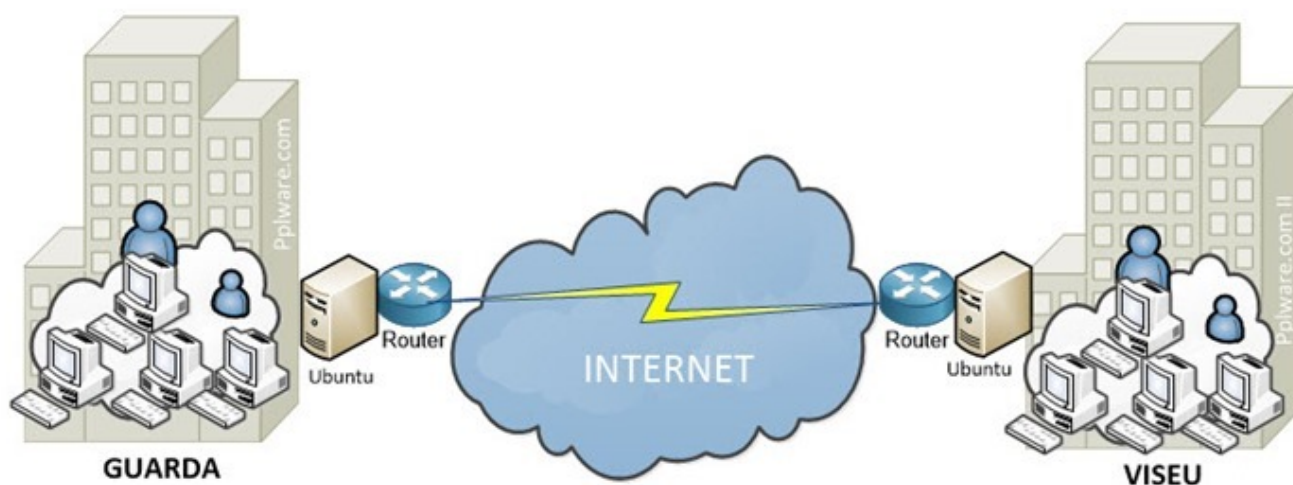


## Aprenda como interligar dois locais através de uma VPN

Date : 14 de Maio de 2015

Imagine por exemplo que tem uma empresa na Guarda e uma filial em Viseu e pretende constituir uma única rede privada (Guarda+Viseu) sem contratar circuitos dedicados ou algum tipo de ligação adicional. Na prática, pretende-se que as duas redes privadas (da Guarda e Viseu) se “unam” podendo um utilizador que se encontre em Viseu aceder localmente aos serviços da rede da Guarda (ex. um utilizador da Guarda poderá imprimir numa impressora localizada em Viseu, entre outros serviços).

Para a implementação de um cenário deste tipo, hoje vamos ensinar como poderão implementar uma VPN (Site-toSite VPN) entre dois locais, recorrendo ao OpenVPN e [desta vez](#) com o Ubuntu.



As organizações que usam VPNs beneficiam com um aumento de flexibilidade e escalabilidade a nível de comunicações e até produtividade. As VPN's permite “trazer” as máquinas remotas para dentro da rede interna, garantindo de certa forma uma nível de segurança idêntico como se o utilizador estivesse dentro da organização.

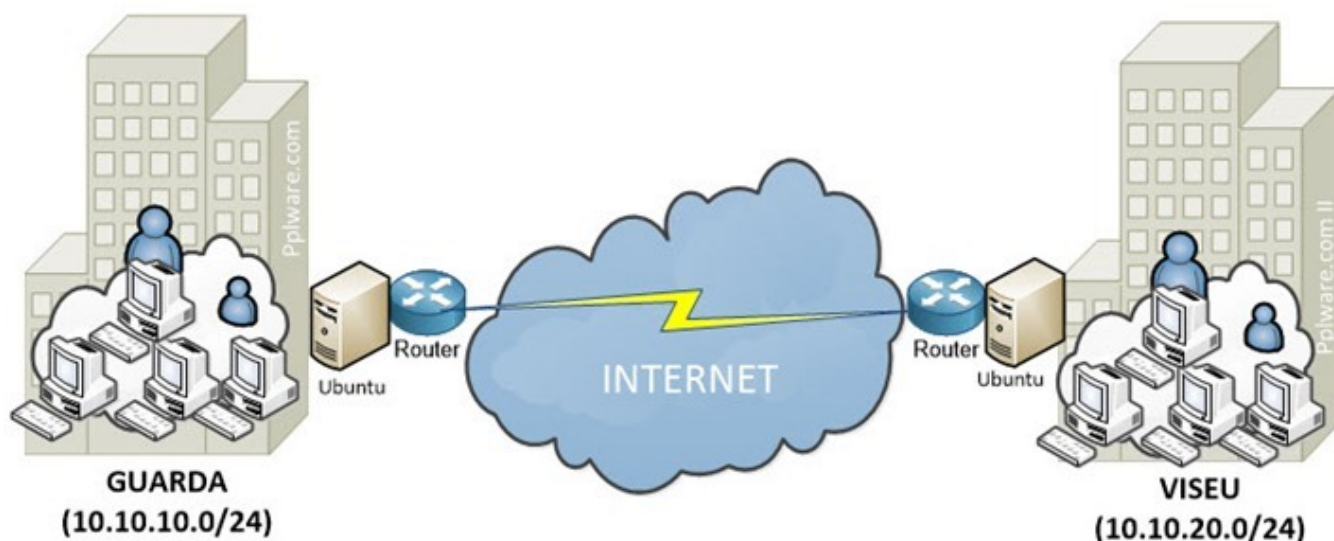
Além dos benefícios referidos, realçar também a poupança de custos a nível de comunicações (já que não é necessário contratar circuitos dedicados). Para quem exerce tele-trabalho, as VPNs são sem duvida uma forma de estar ligado à organização/empresa remotamente e de forma segura.

## Requisitos para a implementação deste tutorial

- As máquinas que vão estabelecer a VPN deverão ter um IP Público (num cenário real)
- As máquinas deverão ter instalado o Linux Ubuntu (deverá funcionar em outras versões)

**Nota:** Para a realização deste artigo vamos considerar os nomes **Pplware-Guarda** (Sede) e **Pplware-Viseu** (Filial). Vamos considerar também as seguintes redes privadas:

- **Pplware-Guarda** – 10.10.10.0/24
- **Pplware-Viseu**– 10.10.20.0/24



## Instalação do Openvpn

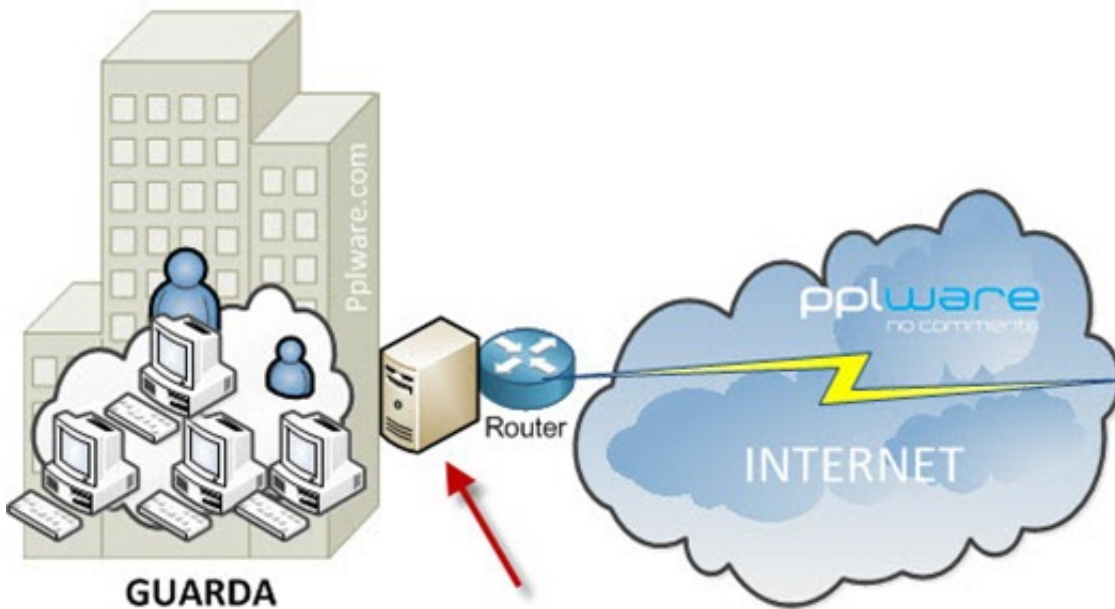
O OpenVPN é um software multi-plataforma que permite a criação de uma VPN entre várias máquinas com sistemas operativos diferentes.

**Passo 1** - Para instalar o OpenVPN basta que execute o seguinte comando:

```
sudo apt-get install openvpn
```

```
ppinto@pplware: ~  
.11-2 [46,6 kB]  
Obter:2 http://pt.archive.ubuntu.com/ubuntu/ vivid/main openvpn i386 2.3.2-9ubun  
tu4 [426 kB]  
Obtidos 472 kB em 0s (773 kB/s)  
A pré-configurar os pacotes...  
A seleccionar pacote anteriormente não seleccionado libpkcs11-helper1:i386.  
(A ler a base de dados ... 181120 ficheiros e directórios actualmente instalados  
.)  
A preparar para desempacotar ../libpkcs11-helper1_1.11-2_i386.deb ...  
A descompactar libpkcs11-helper1:i386 (1.11-2) ...  
A seleccionar pacote anteriormente não seleccionado openvpn.  
A preparar para desempacotar ../openvpn_2.3.2-9ubuntu4_i386.deb ...  
A descompactar openvpn (2.3.2-9ubuntu4) ...  
A processar 'triggers' para man-db (2.7.0.2-5) ...  
A processar 'triggers' para ureadahead (0.100.0-19) ...  
A processar 'triggers' para systemd (219-7ubuntu3) ...  
A instalar libpkcs11-helper1:i386 (1.11-2) ...  
A instalar openvpn (2.3.2-9ubuntu4) ...  
* Restarting virtual private network daemon(s)...  
* No VPN is running.  
A processar 'triggers' para libc-bin (2.21-0ubuntu4) ...  
A processar 'triggers' para ureadahead (0.100.0-19) ...  
A processar 'triggers' para systemd (219-7ubuntu3) ...  
ppinto@pplware:~$
```

## Configurar openvpn em Pplware-Guarda

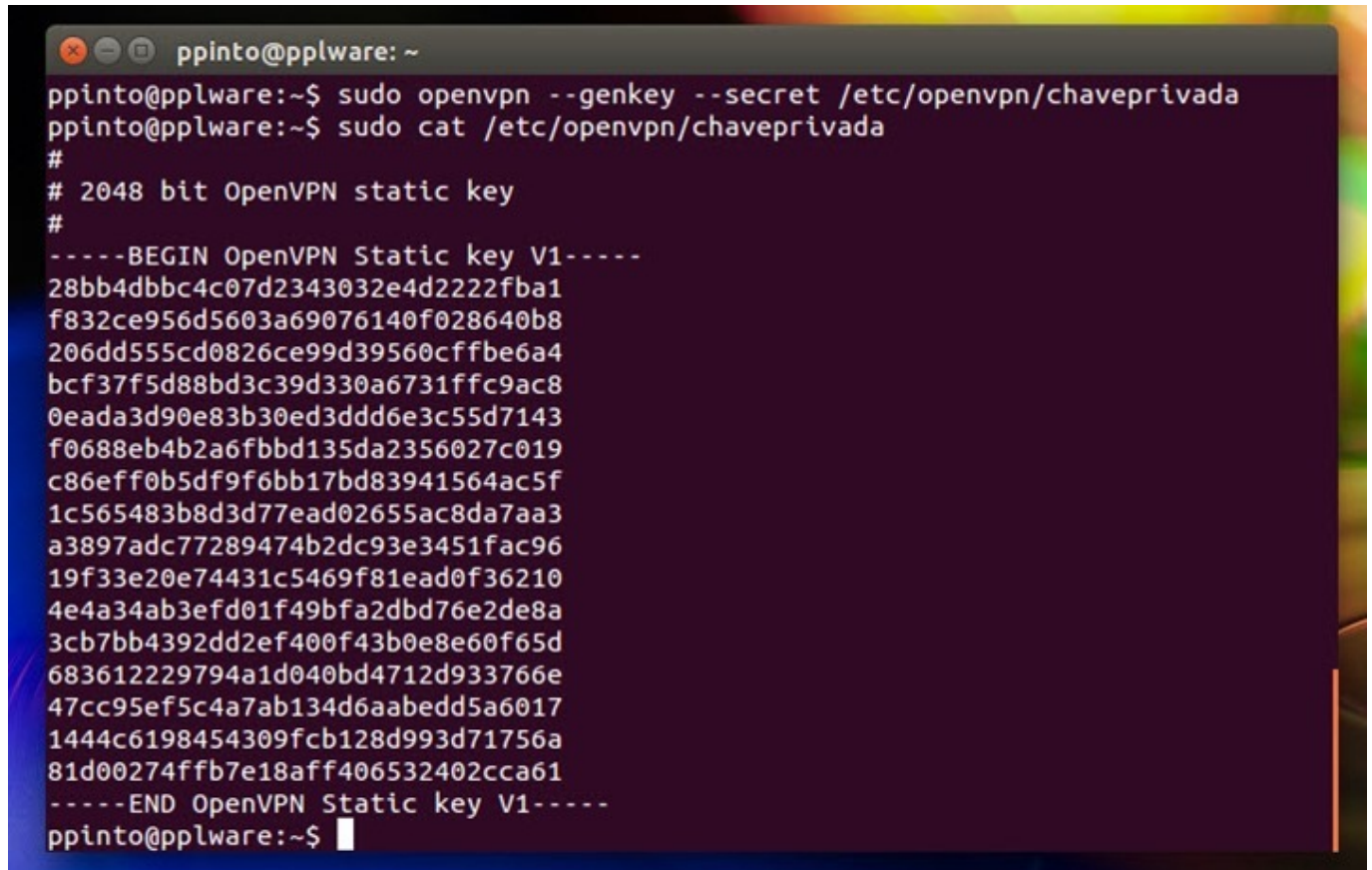


**Passo 2** - Vamos agora criar uma chave privada. Para isso basta que execute o seguinte comando:

```
sudo openvpn --genkey --secret /etc/openvpn/chaveprivada
```

Para verem o conteúdo da chave basta que executem o comando

```
sudo cat /etc/openvpn/chaveprivada
```



```
ppinto@pplware: ~
ppinto@pplware:~$ sudo openvpn --genkey --secret /etc/openvpn/chaveprivada
ppinto@pplware:~$ sudo cat /etc/openvpn/chaveprivada
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
28bb4dbbc4c07d2343032e4d2222fba1
f832ce956d5603a69076140f028640b8
206dd555cd0826ce99d39560cffbe6a4
bcf37f5d88bd3c39d330a6731ffc9ac8
0eada3d90e83b30ed3ddd6e3c55d7143
f0688eb4b2a6fbbd135da2356027c019
c86eff0b5df9f6bb17bd83941564ac5f
1c565483b8d3d77ead02655ac8da7aa3
a3897adc77289474b2dc93e3451fac96
19f33e20e74431c5469f81ead0f36210
4e4a34ab3efd01f49bfa2dbd76e2de8a
3cb7bb4392dd2ef400f43b0e8e60f65d
683612229794a1d040bd4712d933766e
47cc95ef5c4a7ab134d6aabedd5a6017
1444c6198454309fcb128d993d71756a
81d00274ffb7e18aff406532402cca61
-----END OpenVPN Static key V1-----
ppinto@pplware:~$
```

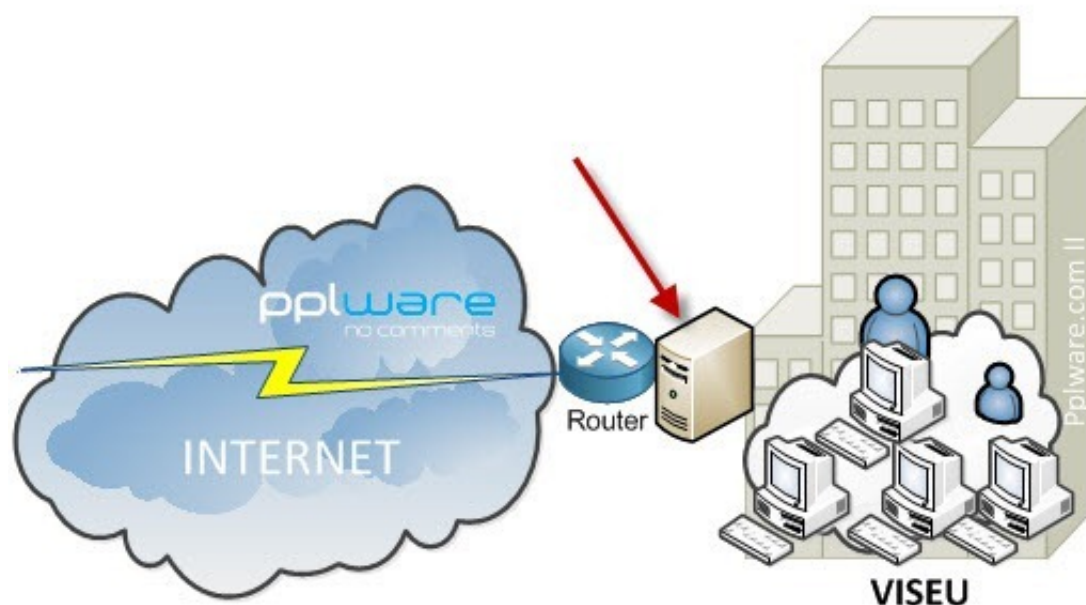
**Passo 3** – Criar o ficheiro `/etc/openvpn/pplware-guarda.conf` e acrescentar a seguinte informação:

```
# interface TUN remote 192.168.10.130 float dev tun ifconfig 10.0.
0.1 10.0.0.2 cd /etc/openvpn secret chaveprivada port 5000 persist
-tun persist-key persist-local-ip user nobody group nogroup comp-
lzo ping 15 verb 3
```

ao fazer um **ifconfig**, deverá observar algo semelhante:

```
ppinto@pplware: /etc/openvpn
Thu May 14 12:06:35 2015 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [
EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Apr 13 2015
Thu May 14 12:06:35 2015 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bi
t key
Thu May 14 12:06:35 2015 Static Encrypt: Using 160 bit message hash 'SHA1' for H
MAC authentication
Thu May 14 12:06:35 2015 Static Decrypt: Cipher 'BF-CBC' initialized with 128 bi
t key
Thu May 14 12:06:35 2015 Static Decrypt: Using 160 bit message hash 'SHA1' for H
MAC authentication
Thu May 14 12:06:35 2015 Socket Buffers: R=[163840->131072] S=[163840->131072]
Thu May 14 12:06:35 2015 TUN/TAP device tun0 opened
Thu May 14 12:06:35 2015 TUN/TAP TX queue length set to 100
Thu May 14 12:06:35 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu May 14 12:06:35 2015 /sbin/ip link set dev tun0 up mtu 1500
Thu May 14 12:06:35 2015 /sbin/ip addr add dev tun0 local 10.0.0.1 peer 10.0.0.2
Thu May 14 12:06:35 2015 GID set to nogroup
Thu May 14 12:06:35 2015 UID set to nobody
Thu May 14 12:06:35 2015 UDPv4 link local (bound): [undef]
Thu May 14 12:06:35 2015 UDPv4 link remote: [AF_INET]192.168.10.130:5000
Thu May 14 12:07:47 2015 Peer Connection Initiated with [AF_INET]192.168.10.130:
5000
Thu May 14 12:07:47 2015 Initialization Sequence Completed
```

## Configurar Openvpn em Pplware-Viseu



**Passo 5** – Copie a chave privada que foi gerada no passo 2 para este servidor e coloque-a em

## **/etc/openvpn/chaveprivada**

Para esta acção poderá usar, por exemplo, a ferramenta [scp](#).

Exemplo:

```
sudo scp ppinto@192.168.1.5:/etc/openvpn/chaveprivada /etc/openvpn
```

**Passo 7** – Criar o ficheiro `etc/openvpn/pplware-viseu.conf` e acrescentar a seguinte informação:

```
# interface TUN remote 192.168.1.5 float dev tun ifconfig 10.0.0.2  
10.0.0.1 cd /etc/openvpn secret chaveprivada port 5000 persist-tu  
n persist-key persist-local-ip user nobody group nogroup comp-  
lzo ping 15 verb 3
```

**Passo 6** – Para colocar a VPN a funcionar no Pplware-Viseu, deverão executar o comando

```
openvpn --config /etc/openvpn/pplware-viseu.conf -daemon
```

Para testar se tudo funciona, experimente se consegue pingar o 10.0.0.1 a partir do Pplware-Viseu e assim confirmar se o tunel VPN foi estabelecido corretamente entre as máquinas e assim criado um ponto de ligação entre as redes.

```
ppinto@koala: /etc/openvpn
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00

inet addr:10.0.0.2  P-t-P:10.0.0.1  Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ppinto@koala:/etc/openvpn$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.63 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.37 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=1.31 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=1.91 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=1.28 ms
<64 bytes from 10.0.0.1: icmp_seq=7 ttl=64 time=1.68 ms
^C
--- 10.0.0.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 1.191/1.486/1.915/0.245 ms
ppinto@koala:/etc/openvpn$
```

### Criação de rotas

Depois de todas as configurações é importante que se criem as rotas para que o tráfego entre edifícios seja sempre encaminhado via tunel.

Para começar devem activar dos dois lados o encaminhamento IPV4 usando o comando:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

### Rota para Pplware-Guarda

Do lado da máquina Pplware-Viseu devem incluir a seguinte rota

```
route add -net 10.10.10.0 gw 10.0.0.2
```

## **Rota para Pplware-Viseu**

Do lado da máquina Pplware-Viseu devem incluir a seguinte rota

```
route add -net 10.10.20.0 gw 10.0.0.1
```

Alguma dúvida ou questão deixem as vossas mensagens nos comentários.