



# Estácio

OUTROS TRABALHOS EM:

[www.projetoederedes.com.br](http://www.projetoederedes.com.br)

**UNIVERSIDADE ESTÁCIO DE SÁ**  
**Campus Praça XI**  
**Curso de Engenharia Elétrica**

## **Redes III**

### **- Projeto para VPN -**

**Professor Alexandre**

**Turma 3008**

**Alunos:**

**Teo Pires Marques**  
**Erivaldo Gomes de Oliveira**  
**Rafael Cossetti**  
**Julio C. Francisco**

**Rio de Janeiro**

**Novembro 2010**

## ÍNDICE:

I. LISTA DE FIGURAS.....	2
II. LISTA DE TABELAS.....	2
1. CONCEITOS DE VPN.....	3
2. DEFINIÇÃO DO PROJETO.....	3
2.1. SITUAÇÃO ATUAL.....	3
2.2. SITUAÇÃO PROPOSTA.....	3
2.3. JUSTIFICATIVA.....	4
3. DETALHAMENTO DE RECURSOS ALOCADOS.....	5
3.1. PROJETO.....	5
3.1.1. INFRA-ESTRUTURA.....	5
3.1.2. DISTRIBUIÇÃO DE PONTOS NAS FILIAIS.....	5
3.2. ESPECIFICAÇÕES DOS MATERIAIS DE CABEAMENTO ESTRUTURADO.....	5
3.3. HARDWARE.....	6
3.3.1. AQUISIÇÃO DE EQUIPAMENTOS.....	7
4. DIAGRAMA DO PROJETO.....	8
5. DISTRIBUIÇÃO DOS IP'S.....	8
6. SOFTWARES.....	9
6.1. IMPLANTAÇÃO DO VPN.....	9
7. CUSTO TOTAL DO PROJETO.....	15
8. CONSIDERAÇÕES FINAIS.....	15

## LISTA DE FIGURAS

FIGURA 1: REDE DE ACESSO REMOTO.....	4
FIGURA 2: CONEXÃO DE LANS VIA INTERNET.....	4
FIGURA 3: CONEXÃO DE COMPUTADORES NUMA INTERNET.....	4
FIGURA 4 – CABO MULTILAN.....	5
FIGURA 5 – TOMADAS E CONECTORES RJ-45.....	5
FIGURA 6: TW100-BRV304.....	6
FIGURA 7: D-LINK / DSL-500B.....	7
FIGURA 8: DIAGRAMA DO PROJETO.....	8
FIGURA 9: LOGO BIGLINUX.....	9
FIGURA 10: LOGO OPENVPN.....	9

## LISTA DE TABELAS

TABELA 1 – PLANILHA DE CUSTO DOS EQUIPAMENTOS.....	7
TABELA 2 – PLANILHA DE CUSTO DOS EQUIPAMENTOS.....	8
TABELA 3 – PLANILHA DE CUSTO DOS EQUIPAMENTOS.....	8
TABELA 4 - PLANILHA DE CUSTO TOTAL DO PROJETO.....	15

## **Proposta de projeto de uma VPN para a empresa Mfrena informática**

### **1. CONCEITOS DE VPN**

Uma VPN (virtual private network) é uma rede de computadores que utiliza infra-estrutura pública de telecomunicações, como a Internet para fornecer acesso seguro a rede privada de uma organização dos seus escritórios ou usuários individuais. O objetivo é evitar um dispendioso sistema de circuitos alugados ou proprietário que pode ser usado por uma única organização. O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

### **2. DEFINIÇÃO DO PROJETO**

#### **2.1. SITUAÇÃO ATUAL**

A empresa Mfrena informática é uma pequena que remanufatura cartuchos para impressora de diversas marcas e modelos e deseja que seus funcionários tenham acesso aos arquivos da empresa e programas através da Internet. A empresa possui duas lojas instaladas no Rio de Janeiro uma no bairro do Santo Cristo e outra na Ilha do Governador. A empresa possui apenas alguns funcionários e os trabalhadores tipicamente executam muitas funções diferentes.

#### **2.2. SITUAÇÃO PROPOSTA**

Utilizar uma rede pública como a Internet para implementar a rede corporativa da empresa. As transferências de informações serão realizadas de modo seguro, entre redes corporativas ou usuários remotos. A rede permitirá que os funcionários tenham acesso às ordens de entrada de compra e venda do escritório em casa ou outro local remoto. A encomenda pode ser enviada para um fornecedor e ser enviada ao cliente no mesmo dia. Durante uma reunião, um cliente pode pedir o seu histórico de compras, e você pode fornecê-la, enquanto no local ao invés de fazer o cliente esperar até que você esteja no escritório.

A segurança será a primeira e mais importante função da VPN implementada. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

### 2.3 JUSTIFICATIVA

Uma das grandes vantagens será a redução de custos com comunicações corporativas, pois serão eliminadas as necessidades de *links* dedicados de longa distância que serão substituídos pela Internet. As LANs poderão, através de *links* dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet. Esta solução pode ser bastante interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. Outro fator que simplifica a operacionalização da WAN é que a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.

Haverá conexão entre corporações (Extranets) através da Internet, além de possibilitar conexões *dial-up* criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

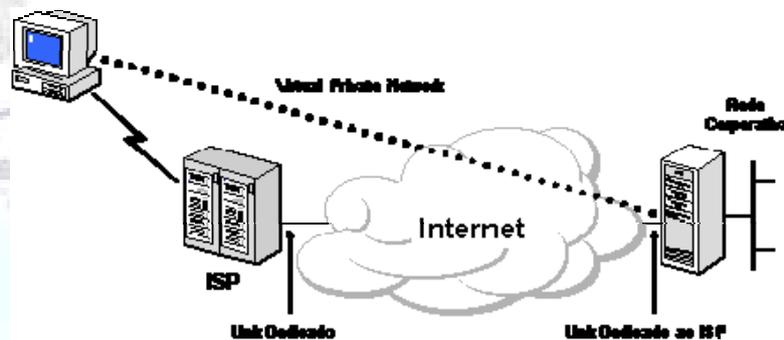


Figura 1: Rede de Acesso Remoto / Fonte: [http://www.gta.ufrj.br/grad/06\\_1/vpn/uso.html](http://www.gta.ufrj.br/grad/06_1/vpn/uso.html)

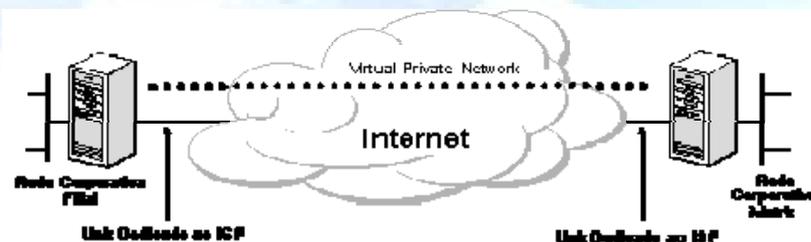


Figura 2: Conexão de LANs via Internet / Fonte: [http://www.gta.ufrj.br/grad/06\\_1/vpn/uso.html](http://www.gta.ufrj.br/grad/06_1/vpn/uso.html)

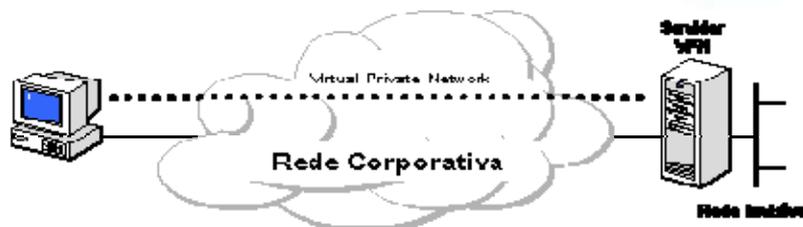


Figura 3: Conexão de Computadores numa Internet / Fonte: [http://www.gta.ufrj.br/grad/06\\_1/vpn/uso.html](http://www.gta.ufrj.br/grad/06_1/vpn/uso.html)

### **3. DETALHAMENTO DE RECURSOS ALOCADOS**

#### **3.1. PROJETO**

##### **3.1.1. INFRA – ESTRUTURA**

Como foi solicitado será feito apenas o necessário de obras para não interferir no funcionamento da empresa. Os novos cabos passarão por baixo do piso elevado Dimopiso, tipo “40”, estrutura tipo “A”. Deverão ser previstas, nas placas de piso, os furos da posição das tomadas e cabos para computadores e demais equipamentos. Instalação das canaletas de passagem dos cabos em todas as salas que terão pontos de rede.

##### **3.1.2. DISTRIBUIÇÃO DE PONTOS NAS FILIAIS**

A empresa possui duas filiais cada uma com 3 computadores e 1 impressora.

### **3.2. ESPECIFICAÇÕES DOS MATERIAIS DO CABEAMENTO ESTRUTURADO**

#### **Cabos**



Figura 4 – Cabo multilan / Fonte: [http://user.img.todaoferta.uol.com.br/H/4/WG/LVTL2X/bigPhoto\\_0.jpg](http://user.img.todaoferta.uol.com.br/H/4/WG/LVTL2X/bigPhoto_0.jpg)

Os cabos são da marca multilan, padrão EIA/TIA , Categoria 5E de 4 pares e não blindados (UTP). São formados por 8 vias constituídas por condutores de cobre isolados em polietileno com capa externa na cor azul.

#### **Conectores (DADOS)**



Figura 5 – tomadas e conectores RJ-45 / fonte: <http://ikem.files.wordpress.com/2008/02/rj45x4001.jpg>

RJ-45 (Fêmea/Macho)

CAT 5 e 10/100BASE-TX;

Fabricada em PVC;

Cor Branca/Transparente; e

1 entrada/1 saída.

### **3.3. HARDWARE**

## Roteador Firewall VPN Avançado Cabo/DSL



Figura 6: TW100-BRV304 / Fonte: <http://www.trendware.com.br/products/TW100-BRV304.htm>

O TW100-BRV304 Roteador Firewall VPN Avançado Cabo/DSL proporciona a usuários segurança avançada para banda larga com um Firewall SPI (Stateful Packet Inspection) que filtra o tráfego no nível dos pacotes e incorpora proteção contra populares ataques de hackers. Ele inclui criptografia VPN com suporte para até 70 túneis VPN simultâneos através de configuração pc cliente-ao-pontofinal ou pontofinal-ao-pontofinal. Para permitir acesso direto a um servidor web ou PC a partir do firewall, o roteador inclui uma porta DMZ dedicada. Instalação e configuração da VPN de forma simples e rápida.

Especificações	
<b>Hardware</b>	
<b>Padrões</b>	<ul style="list-style-type: none"><li>IEEE 802.3 (10-Base T)</li><li>802.3u (100-Base TX)</li></ul>
<b>Protocolos</b>	NAT, PPPoE, NTP, SMTP, HTTP, TFTP, DHCP, TCP/IP, PAP, CHAP, RIP1, RIP2, DDNS
<b>WAN</b>	1 Porta 10/100 Mbps (Internet)
<b>LAN</b>	3 Portas 10/100 Mbps Auto-MDIX
<b>DMZ</b>	1 Porta 10/100 Mbps Auto-MDIX
<b>LEDs Indicadores</b>	<ul style="list-style-type: none"><li>Unidade: Power, Status, PPPoE</li><li>Portas LAN /Porta DMZ : Link/Act, 100</li></ul>
<b>Adaptador de Tensão</b>	12 VDC, 800 mA
<b>Dimensões</b>	170 x 147 x 27 mm
<b>Peso</b>	0.6 kg
<b>Temperatura</b>	<ul style="list-style-type: none"><li>Operação: 0° a 40° C (32° a 104° F)</li><li>Armazenagem: -10° a 70° C (14° a 158° F)</li></ul>
<b>Umidade</b>	<ul style="list-style-type: none"><li>Operação: 0 % a 80 % (sem condensação)</li><li>Armazenagem: 0% a 95% (sem condensação)</li></ul>
<b>Certificados</b>	FCC, CE e VCCI
<b>Roteador</b>	
<b>Firewall</b>	Firewall NAT e Firewall SPI
<b>Segurança</b>	Filtro URL, Controle de Acesso, Proteção por Senha, Email de Alerta e Logs
<b>VPN (IPSec)</b>	Autenticação MD5-HMAC/SHA1-HMAC, Criptografia DES-CBC, 3DES-CBC, Internet Key Exchange e Manual Key Negotiation
<b>Túneis VPN</b>	70 (IPSec), 10 (PPTP)
<b>VPN Pass-Through</b>	IPSec, PPTP e L2TP (100 Sessões)

## Modem D-Link / DSL-500B (Geração II)



Figura 7: D-Link / DSL-500B / Fonte: <http://www.boadica.com.br/produtos/f428/55669.html>

### Características principais

Compartilha o acesso à Internet  
Fácil de Conectar e Configurar  
Suporta alta velocidade de conexão  
Firewall embutido  
Suporta ADSL2 e ADSL2+

### Especificações

Padrões suportados:

- RFC 1483 (Ethernet Bridge), RFC 1577 (IP sobre ATM), RFC 1661 (PPP), RFC 2516 (PPP sobre Ethernet), RFC 2364 (PPP sobre ATM)
- RFC 1994 (CHAP), RFC 1334 (PAP)
- RFC 1631 (NAT)
- RFC 1877 (Atribuição automática de IP)

Suporta RFC 2131 e RFC 2132 (DHCP)

Suporta ATM FORUM UNI V3.1 PVC

Suporta ADSL, ADSL2 e ADSL2+

Suporte a G.dmt full rate: velocidades de até 8Mbps/640Kbps para Downstream/Upstream

Suporte a G.lite: velocidades de até 1.5Mbps/512Kbps para Downstream/Upstream

Portas:

- 1 x RJ-11 para conexão com a linha telefônica
- 1 x RJ-45 10/100BASE T para conexões Ethernet

Funções: DHCP, DDNS, IP QoS

Segurança: NAT e Firewall integrado

Dimensões: 144 x 117 x 31 mm

Temperatura de Operação: 0° a 40° C

Temperatura de Armazenamento: -20° C a 70° C

Umidade: 5% a 45% não condensada

## 3.3.1. AQUISIÇÃO DE EQUIPAMENTOS

### Planilha de custo

equipamento	fabricante	modelo	quantidade	valor unidade (R\$)	total (R\$)
Roteador	TRENDnet	TW100-BRV304	2	R\$ 472,00	R\$ 944,00
Modem	D-Link	DSL-500B	2	R\$ 100,00	R\$ 200,00
Custo Total					R\$ 1.144,00

Tabela 1 – planilha de custo dos equipamentos

Os valores foram cotados em: [WWW.BOADICA.COM.BR](http://WWW.BOADICA.COM.BR)

#### 4. DIAGRAMA DO PROJETO

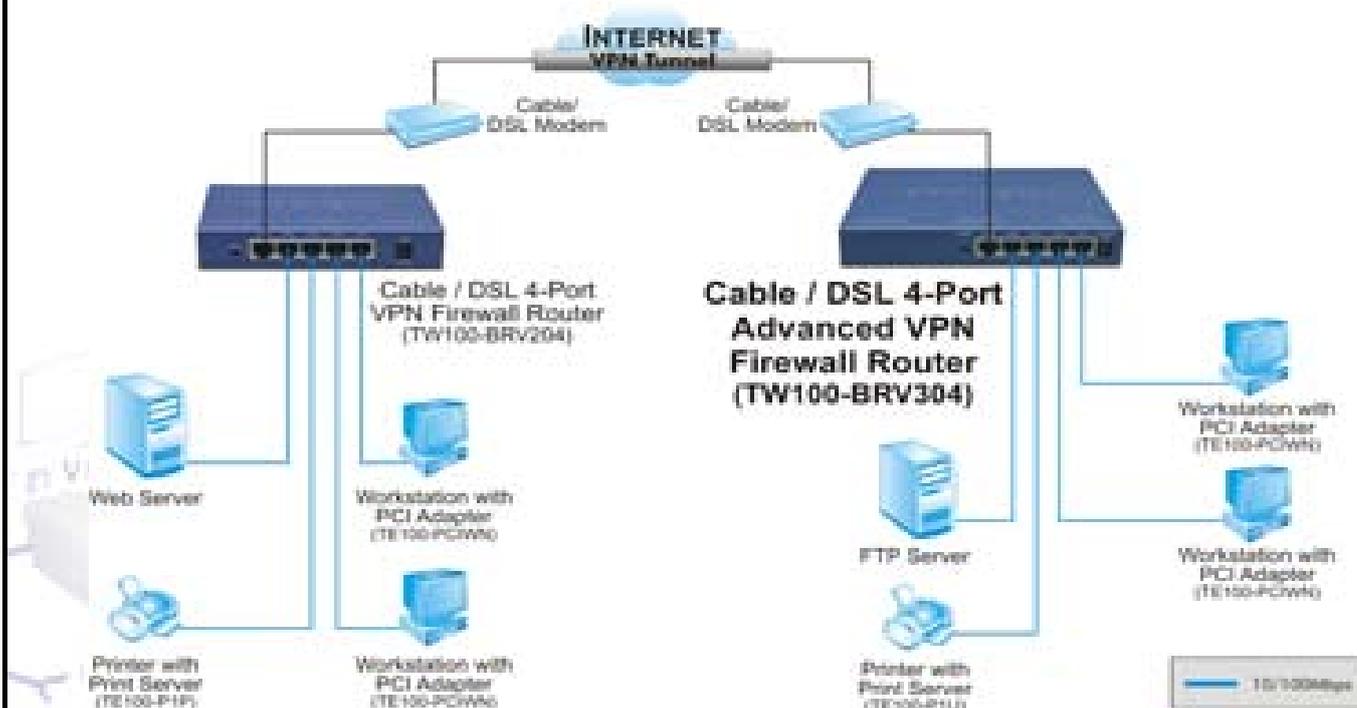


Figura 8: diagrama do projeto / Fonte:

[http://www.trendware.com.br/lab/VPNVideoSeries\\_po.htm](http://www.trendware.com.br/lab/VPNVideoSeries_po.htm)

#### 5. DISTRIBUIÇÃO DOS IPs

Filial Santo Cristo	
IP Classe A	Máscara 255.0.0.0
Equipamento	IP
Roteador1	20.1.1.1
Web Server	20.1.1.2
Impressora1	20.1.1.3
Workstation1	20.1.1.4
Workstation2	20.1.1.5

Tabela 2 – planilha de custo dos equipamentos

Filial Ilha do Governador	
IP Classe A	Máscara 255.0.0.0
Equipamento	IP
Roteador2	20.1.2.1
FTP Server	20.1.2.2
Impressora2	20.1.2.3
Workstation3	20.1.2.4
Workstation4	20.1.2.5

Tabela 3 – planilha de custo dos equipamentos

## **6. SOFTWARES**

A empresa utiliza software livre.

**Sistema Operacional Big Linux.**



Figura 9: logo Biglinux / Fonte: <http://www.biglinux.com.br/>

**Software OpenVPN**



Figura 10: logo OpenVPN / Fonte: [http://marciods.files.wordpress.com/2010/05/openvpn\\_logo.png](http://marciods.files.wordpress.com/2010/05/openvpn_logo.png)

### **6.1. IMPLANTAÇÃO DO VPN**

Ofereceremos duas opções de protocolo para o tunelamento do VPN a primeira em Pass-Through baseado em IPSec, PPTP e L2TP (100 Sessões) original do roteador com configuração simples e autoexplicativa e a segunda como cada filial da empresa possui uma conexão ADSL rodando Linux como servidor utilizaremos o OpenVPN que é um software livre e open-source para criar redes privadas virtuais. Permite autenticação ponto-a-ponto através de chaves secretas compartilhadas, certificados digitais ou autenticação com usuário e senha. Quando utilizado em modo multicient-server ele permite que cada cliente utilize a autenticação pública com certificados digitais, fazendo isto através de assinaturas digitais e certificados de autoridade. Ele utiliza extensivamente a criptografia OpenSSL. Usa também os protocolos SSLv3/TLSv1. Esta disponível para Solaris, Linux, OpenBSD, FreeBSD, NetBSD, Mac OS X, e Windows 2000/XP/Vista. Ele contém muitos recursos de segurança. Ele não é um cliente VPN baseado em web, não é compatível com IPsec ou qualquer outro tipo de pacote VPN. Todo pacote do OpenVPN consiste em apenas um binário tanto para conexões do lado do cliente quanto para conexões do lado do servidor, você vai encontrar mais alguns arquivos e chaves dependendo do tipo e método de autenticação utilizado.

#### **Autenticação de Usuários**

O OpenVPN te possibilita autenticar entre os pontos de várias maneiras. O OpenVPN oferece chaves secretas compartilhadas, autenticação baseada em certificados e autenticação baseada em usuário e senha. O método de autenticação com chaves secretas compartilhadas é o mais simples, e combinando com certificados ele se torna o mais robusto e rico recurso de autenticação. A autenticação com usuário e senha é um recurso novo (disponível apenas na versão 2.0) que possibilita o uso de certificados no cliente, mas não é obrigatório (o servidor precisa de certificado). O código fonte em formato tarball inclui um exemplo de script Perl que verifica usuário e senha através do PAM e um plug-in em C chamado auth-pam-plugin.

## Criptografia de Dados

O OpenVPN utiliza a biblioteca OpenSSL para prover criptografia entre ambos os canais de controle de dados. Isto faz com que o OpenSSL faça funcionar toda a criptografia e autenticação, permitindo ao OpenVPN utilizar todas as cifras disponíveis no pacote do OpenSSL. Ele pode utilizar o pacote de autenticação HMAC para adicionar uma camada de segurança para a conexão. Ele pode também utilizar aceleração de hardware para obter uma melhor performance na criptografia.

## Gerenciamento de Chaves

O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

## Networking

O OpenVPN pode rodar sobre UDP (preferencial por padrão) ou TCP. Ele multiplexa toda a comunicação em cima de uma única porta TCP/UDP. Ele tem a habilidade de trabalhar com a maioria dos proxy servers (incluindo HTTP) e funciona muito bem trabalhando com NAT para passar por firewalls. As configurações do servidor tem a habilidade de fornecer certas configurações de rede para seus clientes, isto inclui endereços Ipv4, comandos de rotas e algumas poucas configurações de conexão. O OpenVPN oferece dois tipos de interfaces para rede via Universal TUN/TAP driver. Ele pode criar um túnel em layer-3 (TUN), ou pode criar um túnel em layer-2 baseado em ethernet TAP, o que pode carregar qualquer tipo de tráfego ethernet. O OpenVPN pode utilizar a biblioteca de compressão LZO para compactar o fluxo de dados. A porta 1194 é a numeração oficial IANA para o OpenVPN. As novas versões do OpenVPN já estão configuradas para utilizarem esta porta. Um novo recurso na versão 2.0 permite que um processo possa manipular e gerenciar vários túneis simultâneos como alternativa ao método original de um processo por túnel, o qual era uma restrição das versões 1.x.x. O OpenVPN usa como seus protocolos comuns o TCP e UDP como uma alternativa ao IPsec em situações onde o ISP pode ter bloqueado os protocolos específicos para VPN na tentativa de forçar os clientes a assinarem serviços mais caros.

## Security

O OpenVPN oferece vários recursos de segurança internos. Ele roda em userspace, ao invés de necessitar de uma ip stack operation. O OpenVPN tem a habilidade de bloquear os privilégios de acesso root, ele usa o mlockall para prevenir que dados sensíveis sejam colocados em swap no disco, e, após sua inicialização, ele roda em ambiente chroot.

O OpenVPN oferece suporte a smart card através de criptografia baseada em token PKCS#11. Este é um software estável, simples de configurar, além de ser um projeto que está sempre em desenvolvimento. **Como cada filial da empresa possui uma conexão ADSL rodando Linux como servidor e suas respectivas redes internas:**

Mfrena Santo Cristo:  
ADSL com IP 200.217.222.222  
LAN com a classe 20.1.1.0

Mfrena Ilha do Governador  
ADSL com ip 200.141.64.33  
LAN com a classe 20.1.2.0

Em nossa VPN, teremos como principal objetivo fazer com que qualquer máquina da rede interna da Matriz se conecte diretamente com qualquer máquina da rede interna da Filial (ou vice versa), deixando a impressão de que ambas as redes estão no mesmo meio físico.

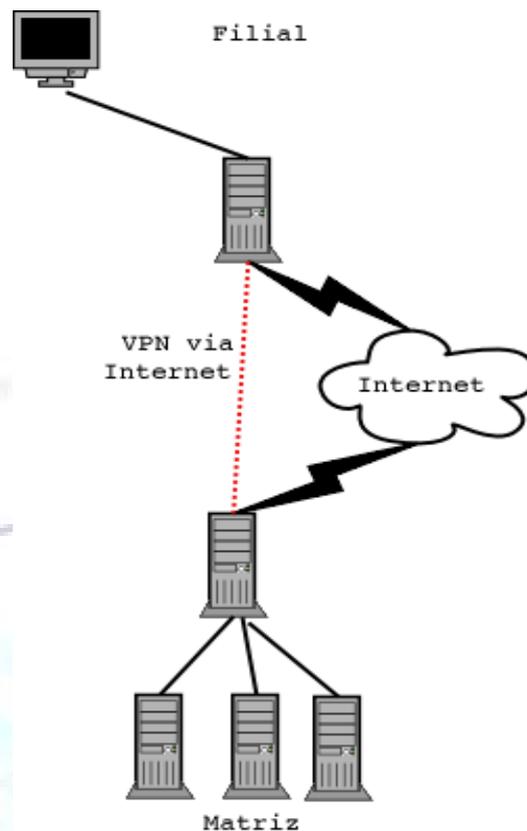


Figura 11: VPN via internet.

fonte: <http://www.vivaolinux.com.br/artigo/VPN-em-Linux-com-OpenVPN/?pagina=2>

### Implantação do OpenVPN:

**1-Checamos se o driver TUN/TAP se encontra no kernel.**

**2-Instalaremos os pacotes** lzo-1.08.tar.gz (biblioteca de compressão de dados) e o pacote openvpn-1.5.0.tar.gz.

3- Configuraremos nossa VPN na loja Santo Cristo:

O OpenVPN usaremos criptografia com chaves estáticas.

Com os seguintes comandos:

```
# mkdir /etc/openvpn
```

Criaremos o diretório onde estarão todos os arquivos de configuração.

```
# openvpn --genkey -secret /etc/openvpn/chave
```

Com isso geramos uma chave de criptografia, o nome de chave (pode ser qualquer nome de arquivo) dentro do diretório /etc/openvpn.

## # cat /etc/openvpn/chave

para visualizarmos o conteúdo da chave que geramos.

## # touch /etc/openvpn/matriz.conf

Crie esse arquivo com o seguinte conteúdo:

```
# Usar como interface o driver TUN
dev tun
# 10.1.0.1 ip que será assumido na loja Santo Cristo
# 10.1.0.2 ip remoto, ou seja, esse será o ip da filial
ifconfig 10.1.0.1 10.1.0.2
# Entra no diretório onde se encontram os arquivos de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de criptografia
secret chave
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000
# Usuário que rodará o daemon do OpenVPN
user nobody
# Grupo que rodará o daemon do OpenVPN
group nobody
Usa a biblioteca Izo
comp-izo
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé em firewall statefull
# Muito recomendado, mesmo se você não usa
# um firewall baseado em statefull.
ping 15
# Nível de log
verb 3
```

Em seguida, Iniciaremos a conexão no servidor, faltando apenas configurar a filial. Executaremos o seguinte comando no servidor da Matriz:

```
# openvpn --config /etc/openvpn/matriz.conf -daemon
```

```
# ifconfig tun0
```

```
tun0      Link encap:Point-to-Point Protocol
          inet addr:10.1.0.1  P-t-P:10.1.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1255  Metric:1
          RX packets:1383257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1144968 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:82865921 (79.0 Mb)  TX bytes:383951667 (366.1 Mb)
```

Se aparecer algo assim ou parecido, o túnel na Matriz já está pronto e a espera da conexão da filial.

## Configuração da Loja Ilha do Governador

Configurando nossa VPN na Filial:

Já na parte de configuração, não muda muita coisa, pois o maior trabalho é simplesmente copiar a chave que geramos na Matriz por um canal seguro até a filial. Executaremos os seguintes comandos e criaremos o mesmo diretório de configuração na filial:

```
# mkdir /etc/openvpn
```

Copiaremos a chave gerada na matriz para a filial com seguinte comando:

```
# scp /etc/openvpn/chave ip_filial:/etc/openvpn
```

Em seguida criaremos o arquivo de configuração chamado filial.conf:

```
# touch /etc/openvpn/filial.conf
```

com o seguinte conteúdo:

```
# Usar como interface o driver TUN
dev tun
# 10.1.0.1 ip que será assumido na matriz
# 10.1.0.2 ip remoto, ou seja, esse será o ip da filial
ifconfig 10.1.0.2 10.1.0.1
# Indica onde está o ip da Matriz (essa é a única linha que acrescentamos
# no arquivo de configuração da filial), o resto é tudo igual.
remote 200.217.222.222
# Entra no diretório onde se encontram os arquivos de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de criptografia
secret chave
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000
# Usuário que rodará o daemon do OpenVPN
user nobody
# Grupo que rodará o daemon do OpenVPN
group nobody
# Usa a biblioteca lzo
comp-lzo
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé em firewall statefull
# Muito recomendado, mesmo se você não usa
# um firewall baseado em statefull.
ping 15
# Nível de log
verb 3
```

Iniciaremos a conexão na filial com o seguinte comando:

```
# openvpn --config /etc/openvpn/filial.conf -daemon
```

## # ifconfig tun0

```
tun0      Link encap:Point-to-Point Protocol
          inet addr:10.1.0.2  P-t-P:10.1.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1255      Metric:1
          RX packets:1383257  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1144968  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:10
          RX bytes:82865921 (79.0 Mb)  TX bytes:383951667 (366.1 Mb)
```

Teste:

## # ping 10.1.0.1

```
PING 10.1.0.1 (10.1.0.1) 56(84) bytes of data:
64 bytes from 10.1.0.1: icmp_seq=1 ttl=63 time=11.9 ms
64 bytes from 10.1.0.1: icmp_seq=2 ttl=63 time=6.09 ms
64 bytes from 10.1.0.1: icmp_seq=3 ttl=63 time=5.93 ms
64 bytes from 10.1.0.1: icmp_seq=4 ttl=63 time=8.15 ms
64 bytes from 10.1.0.1: icmp_seq=5 ttl=63 time=6.19 ms
```

Adicionaremos as rotas para as redes internas se enxergarem.

## Adicionando rotas

NOTA: Antes de adicionarmos as rotas, é necessário ativar o roteamento no kernel em ambas as pontas (Matriz e Filial). Execute os seguintes comandos na matriz e filial:

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

Para adicionar a rota com destino a rede da Filial, execute de dentro do servidor da Matriz o seguinte comando: # route add -net 20.1.2.0 gw 10.1.0.2

Para adicionar a rota com destino a rede da Matriz, execute de dentro do servidor da Filial o seguinte comando: # route add -net 20.1.1.0 gw 10.1.0.1

Realizaremos o teste com o ping de dentro de uma máquina da LAN da loja Santo Cristo com destino a LAN da loja Ilha do Governador. Adicionaremos toda a seqüência de comandos acima no rc.local da distro Linux utilizada, para que a mesma carregue as configurações ao iniciar o sistema operacional.

Poderemos também configurar um servidor WINS com o Samba ou Windows NT/2000 para que ambos os micros das duas redes internas sejam visualizados no Ambiente de Rede do Windows.

## **7. CUSTO TOTAL DO PROJETO**

### **Planilha de custo total do projeto**

<b>EQUIPAMENTO</b>	<b>FABRICANTE</b>
HARDWARE	R\$1.144,00
ELABORAÇÃO DO PROJETO	R\$ 2.500,00
<b>TOTAL</b>	<b>R\$ 3.644,00</b>

*Tabela 4 – planilha de custo total*

## **8. CONSIDERAÇÕES FINAIS:**

As VPNs podem se constituir numa alternativa segura para transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os *links* dedicados de longa distância, de alto custo, na conexão de WANs.

Esclarecemos que em aplicações onde o tempo de transmissão é crítico, o uso de VPNs através de redes externas ainda deve ser analisado com muito cuidado, pois podem ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos.

A decisão de implementar ou não redes privadas virtuais requer uma análise criteriosa dos requisitos, principalmente aqueles relacionados a segurança, custos, qualidade de serviço e facilidade de uso que variam de acordo com o negócio da organização.

As VPNs oferecem:

- Confidencialidade ou privacidade: A informação só estará disponível para aqueles devidamente autorizados.
- Integridade: Os dados recebidos pelo cliente deverão ser os mesmos enviados pelo host
- Autenticidade: Assegurar-se que os usuários que acessam os serviços/recursos são verdadeiramente autorizados.
- Facilidade: O usuário deve ter acesso a vários recursos da maneira mais simples possível.