

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

IMPLANTAÇÃO DE UMA REDE VIRTUAL PRIVADA (VPN) NA
PROCURADORIA DA REPÚBLICA NO RN

**IMPLANTAÇÃO DE UMA REDE VIRTUAL PRIVADA (VPN) NA
PROCURADORIA DA REPÚBLICA NO RN**

Monografia apresentada ao curso de
Especialização em Redes de
Computadores da Faculdade Natalense
para o Desenvolvimento do Rio Grande
do Norte como requisito parcial para a
obtenção do título de Especialista em
Redes de Computadores.

Orientador: **João Fernandes Mitzcun**

Alaísio Pereira da Rocha Neto, MSc.

**NATAL/RN
2007**

JOÃO FERNANDES MITZCUN

**IMPLANTAÇÃO DE UMA REDE VIRTUAL PRIVADA (VPN) NA
PROCURADORIA DA REPÚBLICA NO RN**

**IMPLANTAÇÃO DE UMA REDE VIRTUAL PRIVADA (VPN) NA
PROCURADORIA DA REPÚBLICA NO RN**

Monografia apresentada ao curso de
Especialização em Redes de
Computadores da Faculdade Natalense
para o Desenvolvimento do Rio Grande
do Norte como requisito parcial para a
obtenção do título de Especialista em
Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto, M.Sc.

**NATAL/RN
2007**

RB 30.260

FARN
BIBLIOTECA

Nº Reg M000727

13 / 12 / 07

M

004.7

M6752

2007

12.07

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Mitzcun, João Fernandes

Implantação de uma Rede Virtual Privada (VPN) na Procuradoria da República do RN / João Fernandes Mitzcun. – Natal: FARN, 2007.

39 f.

Orientador: Aluizio Ferreira da Rocha Neto, M.Sc.

Monografia (Especialização em Redes de Computadores) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Rede Virtual Privada (VPN) – Monografia. 3. Ambiente de Rede da Procuradoria da República do RN. – Monografia. I. Título.

RN/FARN/BC

CDU 004.7

JOÃO FERNANDES MITZCUN

**IMPLANTAÇÃO DE UMA REDE VIRTUAL PRIVADA (VPN) NA
PROCURADORIA DA REPÚBLICA NO RN**

Trabalho final apresentado e aprovado em 25 de maio de 2007, pela banca examinadora formada pelos seguintes professores.

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Gleydson de Azevedo Ferreira Lima, M.Sc.
Examinador

*Com todo o respeito a Deus nosso pai todo
potente, dedico este trabalho a Sr. Glécia
Fernandes Mitzcun minha mãe, pelo apoio e
insistência a mim conferida.*

**NATAL/RN
2007**

AGRADECIMENTOS

Com todo o respeito a Deus nosso pai todo poderoso, dedico este trabalho a Sr^a. Glícia Fernandes Mitzcun minha mãe, pelo apoio e incentivo a mim conferido.

Jornada Acadêmica.

AGRADECIMENTOS

Agradeço a FARN e a todo o corpo docente do curso de especialização em redes de computadores desta faculdade, pois estes professores me acompanharam em mais esta jornada acadêmica.

RESUMO

Este trabalho aborda o conceito de VPN (*Virtual Private Network*) disponibilizando um referencial teórico sobre o assunto, como também descreve a implantação de um serviço de rede virtual privada (OpenVPN) na rede da Procuradoria da República no Rio Grande do Norte (PRRN). Tal serviço irá inicialmente beneficiar os Técnicos de Informática, dando novas condições na prestação de serviço de manutenção e acompanhamento à rede da PRRN a partir de um ambiente externo. Tudo isto é acompanhado de uma visão futura, onde se planeja a expansão destes serviços aos usuários (Procuradores), com a possibilidade de pesquisarem documentos que se encontram nos volumes da rede da procuradoria, a partir de qualquer ambiente externo, evitando assim o deslocamento dos mesmos ao prédio da procuradoria, apenas para este fim. Foram feitas também análise de resultados, com o intuito de observar o comportamento do serviço em diversas situações de uso, ressaltando suas potencialidades e desafios.

Fabiana Chaves: VPN, Rede Virtual Privada, OpenVPN.

***"As pequenas oportunidades são, freqüentemente,
o início de grandes empreendimentos."***

Demóstenes

RESUMO

Este trabalho aborda o conceito de VPN (*Virtual Private Network*) disponibilizando um referencial teórico sobre o assunto, como também descreve a implantação de um serviço de rede virtual privada (OpenVPN) na rede da Procuradoria da República no Rio Grande do Norte (PRRN). Tal serviço irá inicialmente beneficiar os Técnicos de informática, dando novas condições na prestação de serviço de manutenção e acompanhamento à rede da PRRN a partir de um ambiente externo. Tudo isto é acompanhado de uma visão futura, onde se vislumbra a expansão destes serviços aos usuários (Procuradores), com a possibilidade de pesquisarem documentos que se encontram nos volumes da rede da procuradoria, a partir de qualquer ambiente externo, evitando assim o deslocamento dos mesmos ao prédio da procuradoria, apenas para este fim. Foram feitas também análise de resultados, com o intuito de observar o comportamento do serviço em diversas situações de uso, ressaltando suas potencialidades e desafios.

Palavras Chaves: VPN, Rede Virtual Privada, OpenVPN.

ABSTRACT

This work approaches the concept of VPN (Virtual Private Network) offering a theoretical referencial on the subject, as well as it describes the implantation of a service of Virtual Private Network (OpenVPN) in the network of the Procuradoria da República no Rio Grande do Norte (PRRN). Such service will benefit the computer science Technicians initially, giving new conditions in the installment of maintenance service and accompaniment to the net of PRRN starting from an external place. Everything is accompanied by a future vision, where is shimmered the expansion of these services to the users (Procurators), with the possibility to research documents that are in the volumes of the network of the PRRN, starting from any external place, avoiding the displacement of the same ones to the building of the PRRN, just for this end. There were also made analysis of results, with the intention of observing the behavior of the service in several use situations, pointing out their potentialities and challenges.

Keywords: VPN, Virtual Private Network, OpenVPN.

SUMÁRIO

1. INTRODUÇÃO	10
1.1 A PRRN	10
1.2 O SERVIÇO	11
1.3 O OBJETIVOS	12
1.3.1 Objetivos Gerais	12
1.3.2 Objetivos Específicos	12
1.4 JUSTIFICATIVA	12
2. REFERENCIAL TEÓRICO	13
2.1 CRIPTOGRAFIA	13
2.1.1 Chave Simétrica ou Chave Privada	14
2.1.2 Chave Assimétrica ou Chave Pública	14
2.2 VPN - REDE VIRTUAL PRIVADA	15
2.2.1 Chaves de uma VPN	17
3. DESENVOLVIMENTO	19
3.1 ANÁLISE E ESCOLHAS DO SOFTWARE	19
3.2 TESTES EM LABORATÓRIO	19
3.2.1 Preparação do Servidor	19
3.2.2 Definição e Preparação dos Clientes	22
3.2.3 Testes no Ambiente Interno (LAN)	25
3.2.4 Testes no Ambiente Externo (WAN)	28
3.3 IMPLANTAÇÃO DO SERVIÇO	30
4. ANÁLISE DE RESULTADOS	31
5. CONCLUSÃO E RECOMENDAÇÕES	32
REFERÊNCIAS BIBLIOGRÁFICAS	33
ANEXOS	34

LISTA DE FIGURAS

Figura 1 – Prédio da PRRN	10
Figura 2 – Cenário VPN	11
Figura 3 – Tunelamento.....	17
Figura 4 – Logomarca OpenVPN.....	19
Figura 5 – Arquivos de configuração do servidor OpenVPN	20
Figura 6 – Exemplo de chaves estáticas de 2048 bits.....	21
Figura 7 – Visualização do ifconfig	22
Figura 8 – Visualização do ipconfig /all.....	23
Figura 9 – Arquivo de configuração Windows.ovpn	24
Figura 10 – Ícone do arquivo BAT.....	24
Figura 11 – Arquivo BAT	24
Figura 12 – Seqüência de inicialização do OpenVPN co CMD.....	25
Figura 13 – Visualização do ipconfig /all tunelado	26
Figura 14 – Visualização do ping no cliente	26
Figura 15 – Visualização do ping do servidor no 1º cliente	27
Figura 16 – Visualização do ping do servidor no 2º cliente	27
Figura 17 – Processo incompleto de conexão externa do OpenVPN.....	28
Figura 18 – Processo completo de conexão externa do OpenVPN	29
Figura 19 – Ping no IP da VPN com resposta positiva	29

1.2 O SERVIÇO

1 INTRODUÇÃO

1.1 A PRRN

A PRRN faz parte do Ministério Público Federal, que por sua vez faz parte do Ministério Público da União, que também, é composto pelo Ministério Público do Trabalho, pelo Ministério Público Militar e pelo Ministério Público do Distrito Federal e Territórios (MPDFT). Juntos, o MPU e os ministérios públicos estaduais formam o Ministério Público brasileiro.

As atribuições e os instrumentos de atuação do Ministério Público estão previstos no artigo 129 da Constituição Federal, dentro do capítulo "Das funções essenciais à Justiça". As funções e atribuições do MPU estão na Lei Complementar nº 75/93.

O Ministério Público não faz parte de nenhum dos três Poderes – Executivo, Legislativo e Judiciário. O MP possui autonomia na estrutura do Estado, não pode ser extinto ou ter as atribuições repassadas a outra instituição. Os procuradores e promotores têm a independência funcional assegurada pela Constituição. Assim, estão subordinados a um chefe apenas em termos administrativos, mas cada membro é livre para atuar segundo sua consciência e suas convicções, baseado na lei. Os procuradores e promotores podem tanto defender os cidadãos contra eventuais abusos e omissões do Poder Público quanto defender o patrimônio público contra ataques de particulares de má-fé. Uma foto do prédio da PRRN pode ser visto na Figura 1.



Ministério Público Federal

Procuradoria da República no
Rio Grande do Norte

Figura 1 – Prédio da PRRN.

1.2 O SERVIÇO

VPN significa *Virtual Private Network*, usada amplamente para fazer um túnel seguro entre duas redes distantes, separadas pela Internet. Os dados são criptografados antes de entrar no túnel e apenas a outra ponta conhece a chave para descriptografar o mesmo, criando um canal de comunicação relativamente seguro.

Inicialmente o serviço VPN será prestado apenas para dois notebook oficiais do setor de informática. Mas este serviço poderá se estender a outras máquinas no futuro. O cenário de utilização deste serviço pode ser visto na Figura 2.

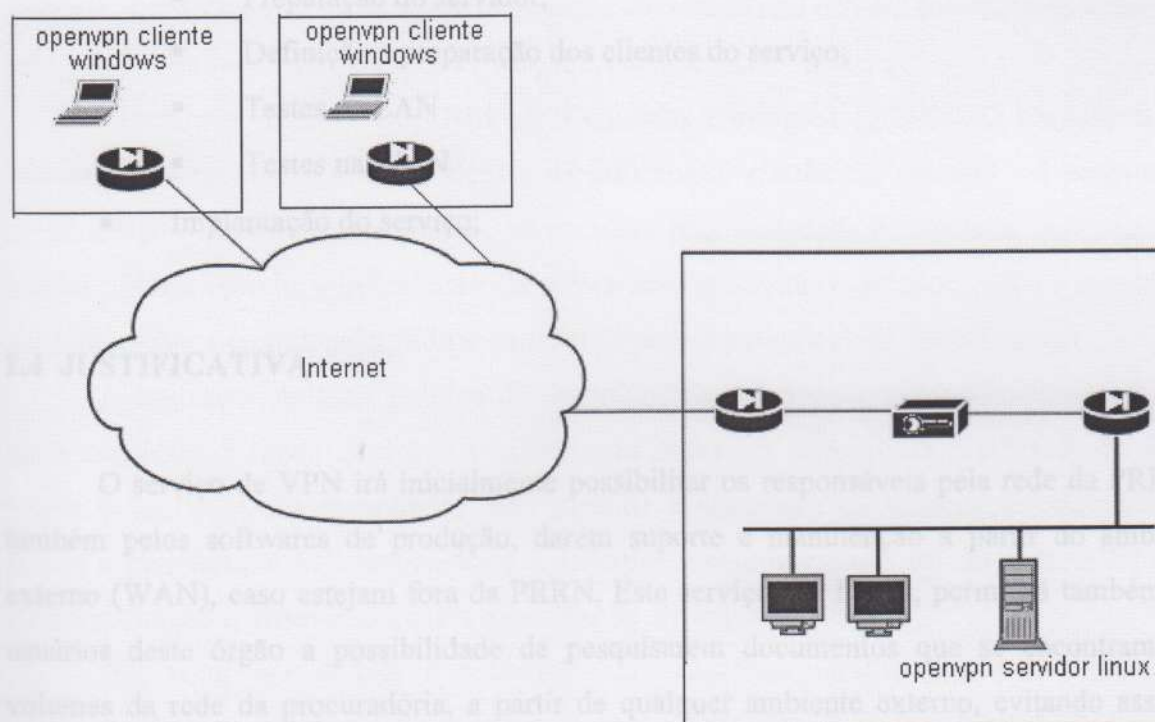


Figura 2 – Cenário VPN

2 REFERENCIAL TEÓRICO

1.3 OBJETIVOS

1.3.1 Objetivos Gerais

Este trabalho tem como objetivo a implantação de um serviço de rede virtual privada (VPN) na rede da Procuradoria da República no Rio Grande do Norte.

1.3.2 Objetivos Específicos

- Analisar e escolher os softwares a serem utilizados;
- Testes em laboratório;
 - Preparação do servidor;
 - Definição e preparação dos clientes do serviço;
 - Testes na LAN
 - Testes na WAN
- Implantação do serviço;

1.4 JUSTIFICATIVA

O serviço de VPN irá inicialmente possibilitar os responsáveis pela rede da PRRN e também pelos softwares de produção, darem suporte e manutenção a partir do ambiente externo (WAN), caso estejam fora da PRRN. Este serviço, no futuro, permitirá também aos usuários deste órgão a possibilidade de pesquisarem documentos que se encontram nos volumes da rede da procuradoria, a partir de qualquer ambiente externo, evitando assim o deslocamento dos mesmos ao prédio da procuradoria, apenas para este fim.

Foi escolhido este serviço pelo baixo custo que ele representa.

2 REFERENCIAL TEÓRICO

2.1 CRIPTOGRAFIA

Segundo WEBER (1998), “A necessidade de comunicação é algo inerente à sociedade humana, assim como o impulso para desvendar segredos também está profundamente enraizado em nossa natureza. Durante anos e anos a humanidade procurou formas de manter parte da sua comunicação segura e confidencial e foi durante a busca dessa confienciabilidade que surgiram os primeiros métodos para encriptar mensagens. Os primeiros registros de técnicas de encriptar mensagens são atribuídas aos gregos em meados do século VI A.C.”.

Hoje com a evolução da tecnologia a necessidade de comunicar esta cada vez mais presente, a utilização de meios de comunicação em tempo real como a Internet está realizando uma verdadeira revolução em todos os aspectos da sociedade moderna.

Segundo a Câmara Brasileira de Comercio Eletrônico (2007), “O paradigma que emerge dessa revolução é a prevalência da informação eletrônica, gerando um conjunto de novas relações econômicas e sociais, vivenciadas pela sociedade de maneira cada vez mais natural”. Neste sentido, a informação eletrônica deve ter alguns requisitos, como a integridade da informação, a confienciabilidade da informação e a autenticidade da informação.

A utilização de uma política de segurança da informação adequada deve atender a esses requisitos fazendo com que a informação possa ser transmitida e utilizada de forma ampla e confiável. As tecnologias para garantir a segurança da informação são variadas, porém a proliferação de computadores e sistemas comunicacionais trouxe grande demanda para a utilização e disseminação dos conceitos de criptografia.

Um texto que é lido e entendido sem nenhuma modificação é um texto não criptografado, a metodologia utilizada para ocultar o conteúdo do texto garantindo assim a sua confienciabilidade é chamado de encriptação. O processo inverso da encriptação é a desencriptação.

A criptografia é constituída por métodos e técnicas destinadas a proteger o conteúdo de uma informação. A confienciabilidade de uma informação é garantida quando forem empregados métodos para que o texto seja cifrado. Assim o emissor do documento pode enviá-lo para o receptor que vai decifrar a informação, transformando-a, novamente, na informação inicial.

Segundo a Câmara Brasileira de Comércio Eletrônico (2007), “o conjunto de regras que determina as transformações do texto claro é chamado de algoritmo (uma sequência de operações) e o parâmetro que determina as condições da transformação é chamado de chave”.

“A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma sequência de bits (chave) como padrão a ser utilizado na criptografia. Partindo dos dados que serão transmitidos, o objetivo é criar uma sequência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma chave”.

ROSSI e FRANZIN (2000)

Chamamos de chave simétrica e de chave assimétrica as tecnologias utilizadas para criptografar dados.

2.1.1 Chave Simétrica ou Chave Privada

A criptografia simétrica ou chave privada é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto cifrado. Nesse método apenas o receptor e o emissor da informação devem conhecer as chaves para garantir a confiabilidade da informação.

2.1.2 Chave Assimétrica ou Chave Pública

É a técnica de criptografia onde as chaves utilizadas para criptografar e decriptografar são diferentes, sendo, no entanto relacionadas. A chave utilizada para criptografar os dados é formada por duas partes, sendo uma pública e outra privada, da mesma forma que a chave utilizada para decriptografar.

Segundo WEBER (1998), “Nos criptosistemas de chave pública, uma das chaves é de conhecimento público, e somente a outra é que deve ser mantida secreta. O problema de distribuição de chaves é eliminado, pois as chaves públicas podem circular livremente, e não existe nenhuma necessidade de enviar a chave secreta a qualquer outro participante do sistema”.

2.2 VPN - REDE VIRTUAL PRIVADA

“VPN (*Virtual Private Network*), ou rede virtualmente privada, como o próprio nome exprime, disponibiliza através de uma rede pública um caminho que se comporta como uma linha privativa para conectar dois equipamentos ou redes que querem se comunicar entre si.

Esse caminho simula ser privativo, sem compartilhamento, de forma a dar segurança à conexão. Desta forma podemos utilizar a infra-estrutura da Internet para uma comunicação que se comporta como uma linha privativa.”

SOUSA (2006)

O termo VPN esteve associado no passado a serviços remotos de conectividade, como o a rede de telefonia pública comutada (RTPC) ou os PVCs (*Permanent Virtual Circuits/Channel*) do Frame Relay, mas hoje já está associado ao uso de infra-estruturas públicas de comunicação para simular redes privadas IP. Antes da utilização deste novo conceito de VPN, as corporações gastavam grandes quantias de recursos para montar complexas redes privadas, chamadas Intranets, entre suas diversas unidades. Essas redes utilizavam serviços caros, como linhas privadas, Frame Relay e ATM para incorporar filiais à rede interna da companhia. Para escritórios ou usuários móveis, eram utilizados servidores de acesso remoto (com modens e linhas de discagem gratuita como o 0800) ou conexões RDSI (Rede Digital de Serviços Integrados). Ao mesmo tempo, empresas pequenas ou médias, que não tem recursos para manter conexões dedicadas tão caras, utilizavam serviços de comutação de circuito de baixa velocidade.

A medida em que a Internet (*web*) tornou-se mais e mais acessível, e a capacidade de transmissão disponível aumentou, as companhias passaram a migrar suas Intranets para a *web*, criando as chamadas Extranets, ligando usuários internos e externos. Apesar do baixo custo e a grande disponibilidade da Internet, há um problema fundamental: a segurança das informações que trafegam na rede.

As VPN aparecem para superar o problema de segurança. Usando protocolos de **tunelamento e procedimentos de encriptação**, a integridade e autenticidade dos dados é garantida. Como as operações ocorrem sobre uma rede pública, a implementação e manutenção de uma VPN custa significativamente menos do que os serviços dedicados descritos acima.

Os dados que trafegam por esse caminho (também chamado de "túnel") são criptografados de forma que teoricamente somente o transmissor e o receptor conseguem entendê-los, por isso a segurança e o sentimento de que o canal de comunicação funciona como se fosse privativo.

Podemos assim interligar redes locais distantes entre si, utilizando a Internet como meio de transmissão, fazendo com que a interligação entre as redes comporte-se como uma rede privada (não compartilhada por estranhos à rede da empresa). A vantagem desse tipo de solução é que uma empresa pode montar uma rede corporativa com baixo investimento em canais de comunicação, utilizando a Internet como meio de comunicação de seus dados.

Uma VPN permite assim uma comunicação entre computadores e redes distantes entre si, utilizando uma rede pública de comunicação de dados, com a segurança que as redes privadas com LPs dedicadas fornecem.

O conceito de VPN é criar um túnel privativo lógico virtual entre dois pontos, com criptografia dos dados entre a origem e o destino final (criptografia *end-to-end*), de forma que ninguém possa interceptar os dados ao longo do caminho. Soluções VPN podem ser implantadas em *firewalls*¹ da rede.

A vantagem do uso de VPNs por uma empresa é principalmente econômica, pois não utiliza links dedicados (LPs) nem redes de pacotes como Frame-relay ou X.25 para conectar redes remotas. Utiliza neste caso a Internet, por meio de um provedor, a um custo menor e com um alcance mundial.

E mesmo utilizando a Internet, uma rede pública, podemos dizer que estamos na verdade na rede privada da empresa, devido à privacidade fornecida pelos túneis. Apesar do termo túnel parecer se referir a um caminho fixo entre a origem e o destino, ele se comporta como qualquer outro tráfego na Internet, que pode passar por diferentes caminhos para chegar a um destino. O que faz da transmissão VPN um túnel é o fato de apenas o destino, no final do túnel, poder ver a informação original.

As tecnologias de tunelamento encriptam e encapsulam um determinado protocolo de rede dentro de um pacote IP. Desta forma, ele pode ser roteado, filtrado e serem aplicados dispositivos para controle de custo da mesma forma que é feitos com WAN tradicionais.

O exemplo de cenário onde um túnel VPN é utilizado, pode ser visto na Figura 3.

¹ É uma aplicação que isola redes distintas e permite que se controle o tráfego entre elas.

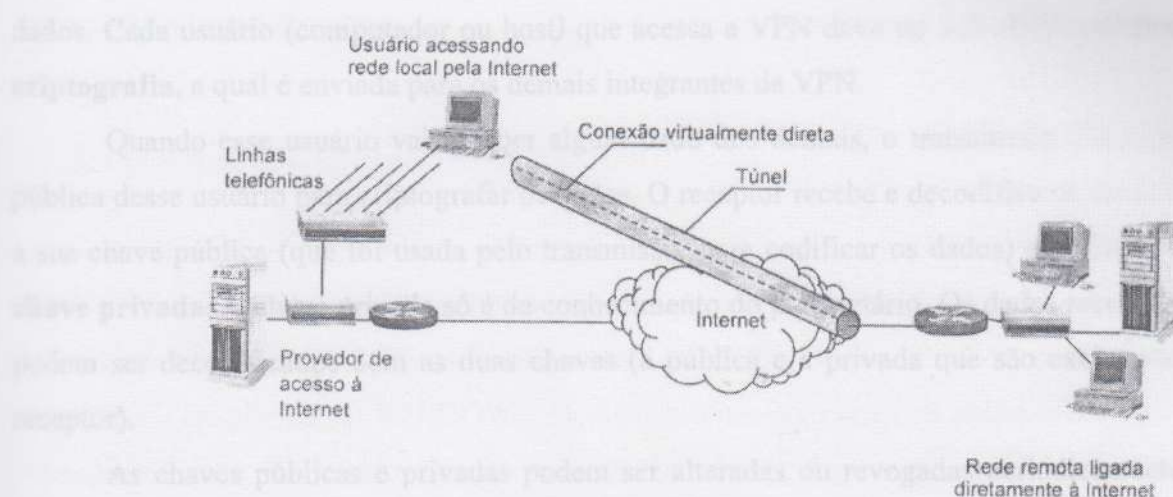


Figura 3 – Tunelamento

A VPN utiliza protocolos que fazem a criptografia dos dados antes de transmiti-los, de forma a fornecer segurança na transmissão dos dados contra intrusos. Os protocolos de segurança e criptografia mais utilizados são:

- IPSec (*Internet Protocol Security*)
- L2TP (*Layer 2 Tunneling Protocol*)
- L2F (*Layer 2 Forwarding*)
- PPTP (*Point to Point Tunneling Protocol*)

Numa transmissão por VPN segura, o datagrama IP é codificado (criptografado) pelo protocolo de VPN, antes de ser enviado pela rede WAN. No receptor é feita a operação inversa na qual o protocolo VPN do receptor decodifica os dados do pacote IP, retornando-os ao formato original.

2.2.1 Chaves de uma VPN

A VPN oferece segurança e privacidade às transmissões dos dados, encriptando-os automaticamente, tornando-os incompreensíveis para os equipamentos e usuários que não façam parte da rede privada. Para que um equipamento possa fazer parte da rede privada virtual, é preciso passar por uma certificação para ter acesso ao sistema e assim decriptar os

dados. Cada usuário (computador ou host) que acessa a VPN deve ter sua **chave pública de criptografia**, a qual é enviada para os demais integrantes da VPN.

Quando esse usuário vai receber algum dado dos demais, o transmissor usa a chave pública desse usuário para criptografar os dados. O receptor recebe e decodifica os dados com a sua chave pública (que foi usada pelo transmissor para codificar os dados) associada à sua **chave privada**. A chave privada só é de conhecimento do proprietário. Os dados recebidos só podem ser decodificados com as duas chaves (a pública e a privada que são exclusivas do receptor).

As chaves públicas e privadas podem ser alteradas ou revogadas periodicamente de acordo com o protocolo de segurança utilizado.

Deve ser feita uma certificação de que a chave pública é realmente do receptor verdadeiro que vai receber a mensagem, e não de um impostor. Essa certificação é feita por cartórios eletrônicos (ou autoridades certificadoras) que confirmam, pelos dados cadastrais do receptor que vai receber a mensagem, se a chave pública enviada por ele é realmente dele ou não. A certificação é feita por meio de uma chave e um PIN (*Personal Identification Number*).

Caso uma chave pública tenha sido enviada por alguma outra pessoa que queira se passar pelo verdadeiro receptor, a certificação deve detectar e não autorizar o envio dos dados.

Finalmente é importante ressaltar que em redes heterogêneas os equipamentos podem possuir diferentes sistemas operacionais e os comandos de configuração variam.

Para cada fabricante temos uma forma diferente de configuração de equipamentos. Assim, os endereços IP, máscaras, sub-redes e demais definições lógicas de uma rede devem ser definidos em um projeto de rede e depois configurados especificamente nos hardwares (roteadores, *switchs*, *gateways* e outros equipamentos), sistemas operacionais e softwares, de acordo com as características de cada equipamento ou sistema utilizado.

3 DESENVOLVIMENTO

3.1 ANÁLISE E ESCOLHAS DO SOFTWARE

Após análise dos softwares disponíveis para o serviço de VPN, foi escolhido o OPENVPN, pois além de ser um software livre (disponível para download e uso sem custo de licenciamento), ele disponibiliza o servidor em LINUX (como o pretendido, pois também é sem custo) e um cliente em WINDOWS, facilitando o uso por parte dos usuários(clientes) que normalmente não tem conhecimento em LINUX. A imagem que representa o software OpenVPN pode ser vista na Figura 4.



Figura 4 – Logomarca OpenVPN

3.2 TESTES EM LABORATORIO

Após a escolha da ferramenta, montou-se uma máquina para ser o servidor VPN e preparou-se dois notebook(s), para serem os futuros usuários, ou seja os futuros clientes VPN.

3.2.1 Preparação do Servidor

Foi preparado um computador com sistema operacional LINUX da distribuição UBUNTU versão 6.06 LTS com Kernel versão 2.6.15, pois nesta versão do kernel já vem o suporte ao drive TUN/TAP (device para tunelamento). Neste equipamento foi baixado do repositório e instalado, o pacote OpenVPN, conforme o comando:

```
# apt-get install openvpn
```

Após isto foram gerados dois arquivos através de um editor de texto, com os seguintes nomes, **notebook0.conf** e **notebook1.conf**, conforme Figura 5, para configurar o serviço OpenVPN no servidor, com intuito de prepará-lo entre outras coisas para escutar nas devidas portas que serão dedicadas aos futuros clientes. Estes arquivos ficarão localizados no subdiretório **/etc/openvpn**.

Nootebook0.conf

```
# Usar como interface o driver TUN
dev tun0
# 10.0.0.1 ip que será assumido no servidor
# 10.0.0.2 ip remoto, ou seja, esse será o ip do
#notebook
ifconfig 10.0.0.1 10.0.0.2
# Entra no diretório onde se encontram os arquivos
#de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de
#criptografia
secret notebook0.key
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
port 5000
# Usuário e grupo que rodará o daemon do
#OpenVPN
user nobody
group nobody
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé.
ping 15
# Nível de log
verb 3
```

Nootebook1.conf

```
# Usar como interface o driver TUN
dev tun1
# 10.0.0.101 ip que será assumido no servidor
# 10.0.0.102 ip remoto, ou seja, esse será o ip do
#notebook
ifconfig 10.0.0.101 10.0.0.102
# Entra no diretório onde se encontram os arquivos
#de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de
#criptografia
secret notebook1.key
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
port 50001
# Usuário e grupo que rodará o daemon do
#OpenVPN
user nobody
group nobody
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé.
ping 15
# Nível de log
verb 3
```

Figura 5 – Arquivos de configuração do servidor OpenVPN

No mesmo subdiretório **/etc/openvpn** foram criadas duas chaves de segurança estáticas de 2048 bits, **Notebook0.key** e **Notbook1.key**.

Estas chaves foram criadas com os seguintes comandos:

```
# openvpn --genkey --secret /etc/openvpn/notebook0.key
```

```
# openvpn --genkey --secret /etc/openvpn/notebook1.key
```

Futuramente estas chaves devem ser levadas com toda a discrição para os devidos clientes, ou seja, os notebooks. Na Figura 6, exemplo de uma chave criada somente para ilustração, pois estas chaves não devem ser divulgadas.

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
5cf5ad8488b132e976281d55bd403ba7
cbcd574fdcd7d94e262f887991bc602
3f0bd04d878f9038327d5e5a6a63e7f4
7c4ccb483e9332c6ef98af676523cee1
01d819b306237973a0f433c75270c453
1fc7e10e45073947e89c70f97d182423
8fe6ba8e75f2607ae71ab1c1455fa385
55a0e8e2f61cd5750b82af82bd917c93
f4dlbc54d35b68235c46029049f335c2
057537c73c5f0f69b552f4eb7faa0b3b
02782c6bb2911ed326869abd80bc0850
27429celbfcc3d9elf4585406ael14438
fe8f74c24edf8a09cb93e2343861061e
8667c6e2b6bb2866f2b2b976fdlac05f
22bdd7a9280b50371ae7fbdee3db1c4d
ed3364d07332c3934f2bb230026dea48
-----END OpenVPN Static key V1-----
```

Figura 6 – Exemplo de chaves estáticas de 2048 bits

Por fim, quando o OpenVPN é instalado, é criado um Deamon, chamado **openvpn** que reside no subdiretório **/etc/init.d** e é executado toda vez que o servidor for inicializado.

Aproveitando o Deamon do OpenVPN, foi colocado dentro dele, para ativar o roteamento e gerar regra de NAT² respectivamente, os seguintes comandos:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING -s 10.50.0.0/16 -o eth0 -j MASQUERADE
```

Para verificar se o servidor está pronto, executa-se o comando:

```
# ifconfig
```

O resultado deste comando é a exibição das interfaces de rede do serviço, onde devem ser observadas as interfaces **tun0** e **tun1**, correspondendo aos túneis dos clientes 0 e 1, respectivamente, como mostrado na Figura 7.

² Tradução de Endereço de Rede

```

eth0      Encapsulamento do Link: Ethernet  Endereço de HW 00:50:8D:70:03:48
inet end.: 200.142.13.142  Bcast:200.142.13.255  Masc:255.255.255.128
endereço inet6: fe80::250:8dff:fe70:348/64  Escopo:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
pacotes RX:1324 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:76 erros:2 descartados:0 excesso:0 portadora:2
colisões:0 txqueuelen:1000
RX bytes:125048 (122.1 KiB) TX bytes:7758 (7.5 KiB)
IRQ:209  Endereço de E/S:0xb000

lo        Encapsulamento do Link: Loopback Local
inet end.: 127.0.0.1  Masc:255.0.0.0
endereço inet6: ::1/128  Escopo:Máquina
UP LOOPBACK RUNNING  MTU:16436  Métrica:1
pacotes RX:7 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:7 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:448 (448.0 b) TX bytes:448 (448.0 b)

tun0      Encapsulamento do Link: Não Especificado  Endereço de
HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet end.: 10.50.0.1  P-a-P:10.50.0.2  Masc:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Métrica:1
pacotes RX:0 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:0 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

tun1      Encapsulamento do Link: Não Especificado  Endereço de
HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet end.: 10.50.0.101  P-a-P:10.50.0.102  Masc:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Métrica:1
pacotes RX:0 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:0 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

```

Figura 7 – Visualização do ifconfig

Como estas interfaces tun0 e tun1 ativas, o servidor está pronto, mas para testá-lo será necessário preparar os clientes (notebooks).

3.2.2 Definição e Preparação dos Clientes

Foram preparados dois notebooks de uso da Coordenação de Informática, com sistema operacional Microsoft Windows XP Home Edition. Neles foram baixados e implantados o software OpenVPN Client para Windows, conforme **Anexo 1**.

Será relatado os procedimentos apenas do primeiro notebook, pois os demais são de procedimento idêntico.

Após esta instalação, se for dado o comando:

```
> ipconfig /all
```

No Prompt de comando, poderá se visto o adaptador para o tunelamento, conforme destacado na Figura 8.

```

C:\>ipconfig /all

Configuração de IP do Windows

    Nome do host . . . . . : mtzxp
    Sufixo DNS primário. . . . . : 
    Tipo de nó . . . . . : desconhecido
    Roteamento de IP ativado . . . . . : não
    Proxy WINS ativado . . . . . : não

Adaptador Ethernet Conexão local 6:

    Estado da mídia . . . . . : mídia desconectada
    Descrição . . . . . : TAP-Win32 Adapter V8
    Endereço físico . . . . . : 00-FF-11-60-5A-1D

Adaptador Ethernet Conexão local 5:

    Sufixo DNS específico de conexão . . . . . : 
    Descrição . . . . . : SiS 900-Based PCI Fast Ethernet Adapter
    Endereço físico . . . . . : 00-0C-6E-4F-3E-DE
    DHCP ativado . . . . . : Não
    Endereço IP . . . . . : 200.142.13.141
    Máscara de sub-rede . . . . . : 255.255.255.128
    Gateway padrão . . . . . : 200.142.13.129
    Servidores DNS . . . . . : 200.142.58.2
                                200.142.58.20

C:\>_

```

Figura 8 – Visualização do ipconfig /all

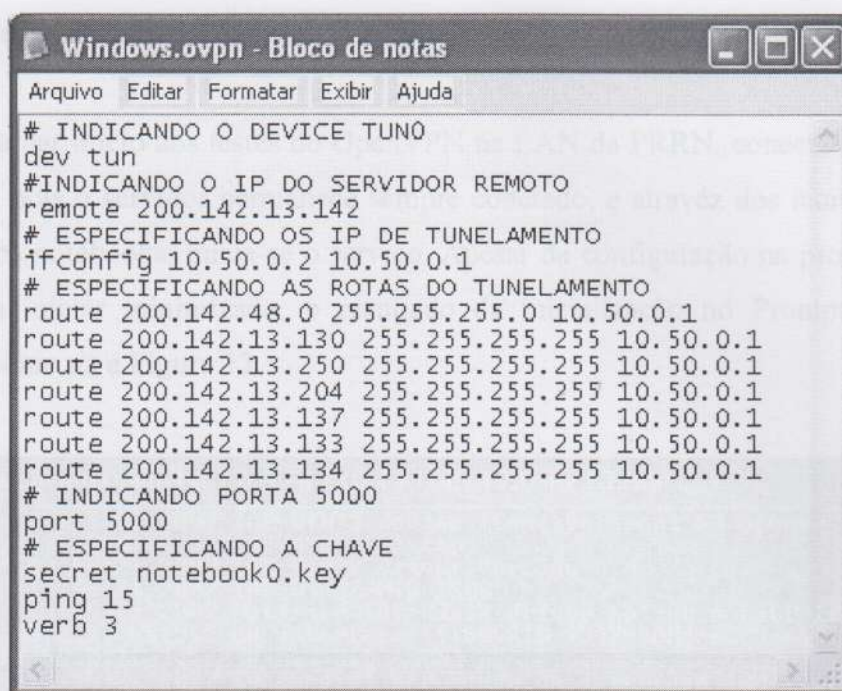
Será preciso agora, levar discretamente como foi dito anteriormente, o arquivo de chave, gerado no servidor, para os seus respectivos notebooks, colocando-os na pasta criada na instalação, que por padrão é:.

\arquivos de programas\openvpn\config

Ficando assim:

\arquivos de programas\openvpn\config\notebook0.key

Será ainda preciso criar com um editor de texto, nesta mesma pasta, um arquivo de configuração para o OpenVPN, que será chamado de **Windows.ovpn**. O mais interessante neste arquivo, é que se pode filtrar as máquinas as quais se quer liberar para o túnel, através do comando **route**, conforme Figura 9.



```
# INDICANDO O DEVICE TUN0
dev tun
#INDICANDO O IP DO SERVIDOR REMOTO
remote 200.142.13.142
# ESPECIFICANDO OS IP DE TUNELAMENTO
ifconfig 10.50.0.2 10.50.0.1
# ESPECIFICANDO AS ROTAS DO TUNELAMENTO
route 200.142.48.0 255.255.255.0 10.50.0.1
route 200.142.13.130 255.255.255.255 10.50.0.1
route 200.142.13.250 255.255.255.255 10.50.0.1
route 200.142.13.204 255.255.255.255 10.50.0.1
route 200.142.13.137 255.255.255.255 10.50.0.1
route 200.142.13.133 255.255.255.255 10.50.0.1
route 200.142.13.134 255.255.255.255 10.50.0.1
# INDICANDO PORTA 5000
port 5000
# ESPECIFICANDO A CHAVE
secret notebook0.key
ping 15
verb 3
```

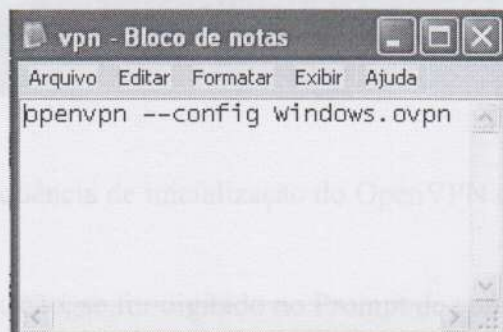
Figura 9 – Arquivo de configuração Windows.ovpn

Finalmente para facilitar a inicialização do tunelamento, pois normalmente o OpenVPN é acionado através de linha de comando no cliente, será criado um arquivo VPN.bat na mesma pasta e um atalho na pasta Desktop, este atalho será chamado pelo ícone da Figura 10.



Figura 10 – Ícone do arquivo BAT

O conteúdo deste arquivo pode ser visto na Figura 11.



```
openvpn --config windows.ovpn
```

Figura 11 –Arquivo VPN.BAT

Agora os dois notebooks também estão prontos para testes.

3.2.3 Testes no Ambiente Interno (LAN)

Para dar início aos testes do OpenVPN na LAN da PRRN, conecta-se na rede os dois notebooks, pois o servidor permanece sempre conectado, e através dos ícones no Desktop de cada um dos notebooks, inicia-se o serviço. Apesar da configuração na propriedade do ícone esteja para iniciar minimizado, o resultado da inicialização no Prompt de comando se apresenta como na a Figura 12.

```
[Windows.ovpn] OpenVPN 2.0.9 F4:EXIT F1:USR1 F2:USR2 F3:HUP
Thu May 24 13:55:21 2007 TAP-WIN32 device [Conexão local 6] opened: \\.\Global\{11605A1D-933E-40B4-8CC3-4642745BE6E5}.tap
Thu May 24 13:55:21 2007 TAP-Win32 Driver Version 8.4
Thu May 24 13:55:21 2007 TAP-Win32 MTU=1500
Thu May 24 13:55:21 2007 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.50.0.2/255.255.255.252 on interface {11605A1D-933E-40B4-8CC3-4642745BE6E5} [DHCP-serv: 10.50.0.1, lease-time: 31536000]
Thu May 24 13:55:21 2007 Successful ARP Flush on interface [2] {11605A1D-933E-40B4-8CC3-4642745BE6E5}
Thu May 24 13:55:21 2007 Data Channel MTU parms [ L:1544 D:1450 EF:44 EB:4 ET:0 EL:0 ]
Thu May 24 13:55:21 2007 Local Options hash (VER=U4): 'db1fb5f1'
Thu May 24 13:55:21 2007 Expected Remote Options hash (VER=U4): 'a86a87f8'
Thu May 24 13:55:21 2007 UDPv4 link local (bound): [undef]:5000
Thu May 24 13:55:21 2007 UDPv4 link remote: 200.142.13.142:5000
Thu May 24 13:55:32 2007 Peer Connection Initiated with 200.142.13.142:5000
Thu May 24 13:55:33 2007 TEST ROUTES: 7/7 succeeded len=7 ret=1 a=0 u/d=up
Thu May 24 13:55:33 2007 route ADD 200.142.48.0 MASK 255.255.255.0 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.130 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.250 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.204 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.137 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.133 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 route ADD 200.142.13.134 MASK 255.255.255.255 10.50.0.1
Thu May 24 13:55:33 2007 Route addition via IPAPI succeeded
Thu May 24 13:55:33 2007 Initialization Sequence Completed
```

Figura 12 – Sequência de inicialização do OpenVPN com CMD

Após esta inicialização, se for digitado no Prompt de comando:

> ipconfig /all

Figura 14 – Visualização do ping ao cliente

Poderá se ver a interface de rede para o túnel de VPN no clienten conforme Figura 13.

```

C:\>ipconfig /all

Configuração de IP do Windows

    Nome do host . . . . . : mtzxp
    Sufixo DNS primário. . . . . : 
    Tipo de nó . . . . . : desconhecido
    Roteamento de IP ativado . . . . . : não
    Proxy WINS ativado . . . . . : não

Adaptador Ethernet Conexão local 6:

    Sufixo DNS específico de conexão . . : 
    Descrição . . . . . : TAP-Win32 Adapter V8
    Endereço físico . . . . . : 00-FF-11-60-5A-1D
    DHCP ativado . . . . . : Sim
    Configuração automática ativada . . : Sim
    Endereço IP . . . . . : 10.50.0.2
    Máscara de sub-rede . . . . . : 255.255.255.252
    Gateway padrão . . . . . : 
    Servidor DHCP . . . . . : 10.50.0.1
    Concessão obtida . . . . . : segunda-feira, 16 de abril de 2007
    Concessão expira . . . . . : terça-feira, 15 de abril de 2008 1

Adaptador Ethernet Conexão local 5:

    Sufixo DNS específico de conexão . . : 
    Descrição . . . . . : SiS 900-Based PCI Fast Ethernet Ad
    Endereço físico . . . . . : 00-0C-6E-4F-3E-DE
    DHCP ativado . . . . . : Não
    Endereço IP . . . . . : 200.142.13.141
    Máscara de sub-rede . . . . . : 255.255.255.128
    Gateway padrão . . . . . : 200.142.13.129
    Servidores DNS . . . . . : 200.142.58.2
    200.142.58.20
  
```

Figura 13 – Visualização do ipconfig /all tunelado

Para confirmar-se o tunelamento digita-se o comando:

> **ping 10.50.0.1** (este é o IP próprio do tunelamento, que está no servidor)

No Prompt de comando do cliente, verifica-se o resultado visto na Figura 14.

```

C:\>ping 10.50.0.1

Disparando contra 10.50.0.1 com 32 bytes de dados:

Resposta de 10.50.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=1ms TTL=64

Estatísticas do Ping para 10.50.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 1ms, Média = 1ms
  
```

Figura 14 – Visualização do ping no cliente

Pode-se ainda confirmar o tunelamento a partir do servidor através dos comandos,

```
# ping -c 4 10.50.0.2
```

e

```
# ping -c 4 10.50.0.102.
```

Os resultados são vistos nas Figuras 15 e 16, respectivamente.

```
PING 10.50.0.2 (10.50.0.2) 56(84) bytes of data.
64 bytes from 10.50.0.2: icmp_seq=1 ttl=128 time=0.998 ms
64 bytes from 10.50.0.2: icmp_seq=2 ttl=128 time=0.964 ms
64 bytes from 10.50.0.2: icmp_seq=3 ttl=128 time=0.963 ms
64 bytes from 10.50.0.2: icmp_seq=4 ttl=128 time=0.988 ms

--- 10.50.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 0.963/0.978/0.998/0.026 ms
```

Figura 15 – Visualização do ping do servidor no 1º cliente

```
PING 10.50.0.102 (10.50.0.102) 56(84) bytes of data.
64 bytes from 10.50.0.102: icmp_seq=1 ttl=128 time=0.987 ms
64 bytes from 10.50.0.102: icmp_seq=2 ttl=128 time=0.744 ms
64 bytes from 10.50.0.102: icmp_seq=3 ttl=128 time=0.723 ms
64 bytes from 10.50.0.102: icmp_seq=4 ttl=128 time=0.748 ms

--- 10.50.0.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.723/0.800/0.987/0.111 ms
```

Figura 16 – Visualização do ping do servidor no 2º cliente

Os teste em laboratório no ambiente interno (LAN), foram terminados com sucesso.

3.2.4 Testes no Ambiente Externo (WAN)

Como existe um firewall na rede da PRRN nacional em São Paulo, barrando o tráfego desconhecido e indejejado, foi necessário pedir liberação do trafico de VPN para o IP do servidor nas portas 5000 e 5001 de escuta, especificando o protocolo UDP.

Sem esta liberação a tentativa de conexão externa não obteve sucesso e o estabelecimento do túnel ficou incompleto, conforme pode ser visto na Figura 17.



```
[Windows.ovpn] OpenVPN 2.0.9 F4:EXIT F1:USR1 F2:USR2 F3:HUP
start or --ping-exit
Wed May 09 14:43:16 2007 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 09 14:43:16 2007 Static Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 09 14:43:16 2007 Static Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 09 14:43:16 2007 Static Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 09 14:43:16 2007 TAP-WIN32 device [Conexão local 6] opened: \\.\Global\{11605A1D-933E-40B4-8CC3-4642745BE6E5}.tap
Wed May 09 14:43:16 2007 TAP-Win32 Driver Version 8.4
Wed May 09 14:43:16 2007 TAP-Win32 MTU=1500
Wed May 09 14:43:16 2007 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.50.0.2/255.255.255.252 on interface {11605A1D-933E-40B4-8CC3-4642745BE6E5} [DHCP-serv: 10.50.0.1, lease-time: 31536000]
Wed May 09 14:43:16 2007 Successful ARP Flush on interface [2] {11605A1D-933E-40B4-8CC3-4642745BE6E5}
Wed May 09 14:43:16 2007 Data Channel MTU parms [ L:1544 D:1450 EF:44 EB:4 ET:0 EL:0 ]
Wed May 09 14:43:16 2007 Local Options hash (VER=U4): 'db1fb5f1'
Wed May 09 14:43:16 2007 Expected Remote Options hash (VER=U4): 'a86a87f8'
Wed May 09 14:43:16 2007 UDPv4 link local (bound): [undef]:5000
Wed May 09 14:43:16 2007 UDPv4 link remote: 200.142.13.142:5000
```

Figura 17 – Processo incompleto de conexão externa do OpenVPN

Isto porque o protocolo usado UDP não é orientado a conexão, e então não se teve uma confirmação do estabelecimento ou não da conexão, pois uma vez perdido o pacote não se pode esperar qualquer retorno.

Mas a partir da liberação solicitada, a nova tentativa de conexão logrou sucesso, estabelecendo a conexão, como mostra a Figura 18.

Figura 18 – Ping no IP da VPN com resposta positiva

```

C:\Arquivos de programas\OpenVPN\config>openvpn --config windows.ovpn
Tue May 15 19:35:46 2007 OpenVPN 2.0.9 win32-MinGW [SSL] [LZO] built on Oct 12 2006
Tue May 15 19:35:46 2007 WARNING: --ping should normally be used with --ping-res
start or --ping-exit
Tue May 15 19:35:46 2007 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bi
t key
Tue May 15 19:35:46 2007 Static Encrypt: Using 160 bit message hash 'SHA1' for H
MAC authentication
Tue May 15 19:35:46 2007 Static Decrypt: Cipher 'BF-CBC' initialized with 128 bi
t key
Tue May 15 19:35:46 2007 Static Decrypt: Using 160 bit message hash 'SHA1' for H
MAC authentication
Tue May 15 19:35:46 2007 TAP-WIN32 device [Conexão local 3] opened: \\.\Global\{
B0DB08A1-0714-4048-8346-2E8B2C9620B3}.tap
Tue May 15 19:35:46 2007 TAP-Win32 Driver Version 8.4
Tue May 15 19:35:46 2007 TAP-win32 MTU=1500
Tue May 15 19:35:46 2007 Notified TAP-win32 driver to set a DHCP IP/netmask of 1
0.50.0.2/255.255.255.252 on interface {B0DB08A1-0714-4048-8346-2E8B2C9620B3} [DH
CP-serv: 10.50.0.1, lease-time: 31536000]
Tue May 15 19:35:46 2007 Successful ARP Flush on interface [3] {B0DB08A1-0714-40
48-8346-2E8B2C9620B3}
Tue May 15 19:35:46 2007 Data Channel MTU parms [ L:1544 D:1450 EF:44 EB:4 ET:0
EL:0 ]
Tue May 15 19:35:46 2007 Local Options hash (VER=V4): 'db1fb5f1'
Tue May 15 19:35:46 2007 Expected Remote Options hash (VER=V4): 'a86a87f8'
Tue May 15 19:35:46 2007 UDPv4 link local (bound): [undef]:5000
Tue May 15 19:35:46 2007 UDPv4 link remote: 200.142.13.142:5000
Tue May 15 19:35:55 2007 Peer Connection Initiated with 200.142.13.142:5000
Tue May 15 19:35:55 2007 TEST ROUTES: 1/1 succeeded len=1 ret=1 a=0 u/d=up
Tue May 15 19:35:55 2007 route ADD 200.142.0.0 MASK 255.255.255.0 10.50.0.1
Tue May 15 19:35:55 2007 Route addition via IPAPI succeeded
Tue May 15 19:35:55 2007 Initialization Sequence Completed

```

Figura 18 – Processo completo de conexão externa do OpenVPN

Para complementar o teste, pingou-se o IP do túnel 10.50.0.1, e o resultado obtido foi positivo, conforme Figura 19.

```

Prompt de comando
Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Mitzcun>ping 10.50.0.1

Disparando contra 10.50.0.1 com 32 bytes de dados:

Resposta de 10.50.0.1: bytes=32 tempo=190ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=165ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=156ms TTL=64
Resposta de 10.50.0.1: bytes=32 tempo=174ms TTL=64

Estatísticas do Ping para 10.50.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 156ms, Máximo = 190ms, Média = 171ms

C:\Documents and Settings\Mitzcun>

```

Figura 19 – Ping no IP da VPN com resposta positiva

3.3 IMPLANTAÇÃO DO SERVIÇO

A implantação do serviço se deu de forma simples e natural, pois mesmo ainda a nível de testes, tanto o computador determinado para o papel do servidor já teria sido preparado e dimensionado para ser o servidor definitivo a ser implantado, como também os notebooks dos clientes já eram os próprios de uso da informática. Desta maneira, como todos os testes, tanto de LAN como de WAN foram finalizados com sucesso, foi considerado então, a partir deste momento a VPN implantada.

Mas existe a intenção futura de re implantar a fase final do serviço, ou seja o uso do mesmo pelos procuradores, a partir da total segurança do pessoal especializado, no serviço de VPN.

4 ANÁLISE DE RESULTADOS

Foram feitos vários teste de uso do serviço VPN, como emulação de Host, transferência de arquivos, gerenciamento remoto e outros. Os resultados destes testes foram satisfatório e de acordo com os objetivos previamente traçados.

O serviço está considerado implantado na fase inicial, onde está disponível para o pessoal da informática, e está sendo usado não só para o dia a dia, como também para esgotar qualquer dúvida sobre o mesmo, pelo pessoal especializado.

Mas existe a intenção futura de se implantar a fase final do serviço, ou seja o uso do mesmo pelos procuradores, a partir da total segurança do pessoal especializado, no serviço de VPN.

5 CONCLUSÃO E RECOMENDAÇÕES

O serviço VPN enfim está em uso e também está sendo considerado de grande eficácia, além de barato é de fácil manuseio. Pode-se concluir que foi um acerto, a opção pelo serviço VPN e pela ferramenta OpenVPN.

A recomendação mais importante a ser ressaltada, é como será tratado o serviço de firewall da rede, pois as regras aplicadas devem ser precisas para não vir a causar problema ao serviço, como também devem servir para dar mais confiabilidade ao mesmo. Estas regras vão variar, dependendo da situação e necessidade de cada VPN implantada.

NEWMITH, DON; SNYDER, GARTH; HEIN, TONY R. *Manual Completo do Linux*. 1ª ed. São Paulo: Pearson Makron Books, 2004.

STARLIN, Gorki. *TCP/IP Manual Completo*. 3ª ed. Rio de Janeiro: Starline Press, 2001.

STARLIN, Gorki. *Netware 3 Completo*. 2ª ed. Rio de Janeiro: Book Express, 1999.

HUNT, Craig. *Servidores de Redes com Linux*. 1ª ed. São Paulo: Market Books Brasil, 2000.

TORRES, Gabriel. *Redes de Computadores Curso Completo*. 1ª ed. Rio de Janeiro: Anel Books, 2001.

UNIVERSIDADE DE HELSINKI. FI 2007. Disponível < [www.helsinki.fi/itk/english/ty-pojhy-vpn](http://www.helsinki.fi/fi/itk/english/ty-pojhy-vpn) >. Acesso em: 16 abril 2007.

VIVA O LINUX. BR 2007. Disponível < www.vivaolinux.com.br/artigos/verArtigo.php?codig=2601 >. Acesso em: 12 abril 2007.

Câmara Brasileira de Comércio eletrônico -- camara .x.net -- disponível em http://www.leonnet.com.br/ed/ed_guia.pdf acesso em 15 de maio de 2007.

ROSSI, Marco Antonio G; FRANZIN Oswaldo. - VPN - Virtual Private Network (Rede Privada Virtual) - GPr Sistemas/ASP Systems - Agosto/2000.

WEBER, Raul Fernando -- *Criptografia Contemporânea*. 1998 -- Instituto de Informática -- UFRGS -- Porto Alegre RS.

REFERÊNCIAS BIBLIOGRÁFICAS ANEXOS

TANENBAUM, A. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Campus, 2003.

SOUSA, Lindeberg Barros. **TCP/IP Básico & Conectividade em Redes**. 3ª ed. São Paulo: Érica, 2006.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 3ª ed. São Paulo: Pearson Addison Wesley, 2006.

NEMETH, Evi; SNYDER, Garth; HEIN, Trent R. **Manual Completo do Linux**. 1ª ed. São Paulo: Pearson Makron Books, 2004.

STARLIN, Gorki. **TCP/IP Manual Completo**. 5ª ed. Rio de Janeiro: Starlicon Press, 2001.

STARLIN, Gorki. **Netware 5 Completo**. 2ª ed. Rio de Janeiro: Book Express, 1999.

HUNT, Craig. **Servidores de Redes com Linux**. 1ª ed. São Paulo: Market Books Brasil, 2000.

TORRES, Gabriel. **Redes de Computadores Curso Completo**. 1ª ed. Rio de Janeiro: Axcel Books, 2001.

UNIVERSIDADE DE HELSINK. FI 2007. Disponível < www.helsinki.fi/atk/english/hy-ppp/hy-vpn >. Acesso em: 16 abril 2007.

VIVA O LINUX. BR 2007. Disponível < www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2602 >. Acesso em: 12 abril 2007.

Câmara Brasileira de Comercio eletrônico – camara – e.net – disponível em http://www.iconenet.com.br/cd/cd_guia.pdf acesso em 15 de maio de 2007.

ROSSI, Marco Antonio G; FRANZIN Oswaldo. - **VPN - Virtual Private Network (Rede Privada Virtual)** - GPr Sistemas/ASP Systems - Agosto/2000.

WEBER, Raul Fernando – **Criptografia Contemporânea**. 1998 – Instituto de Informática – UFRGS – Porto Alegre RS.

ANEXO I

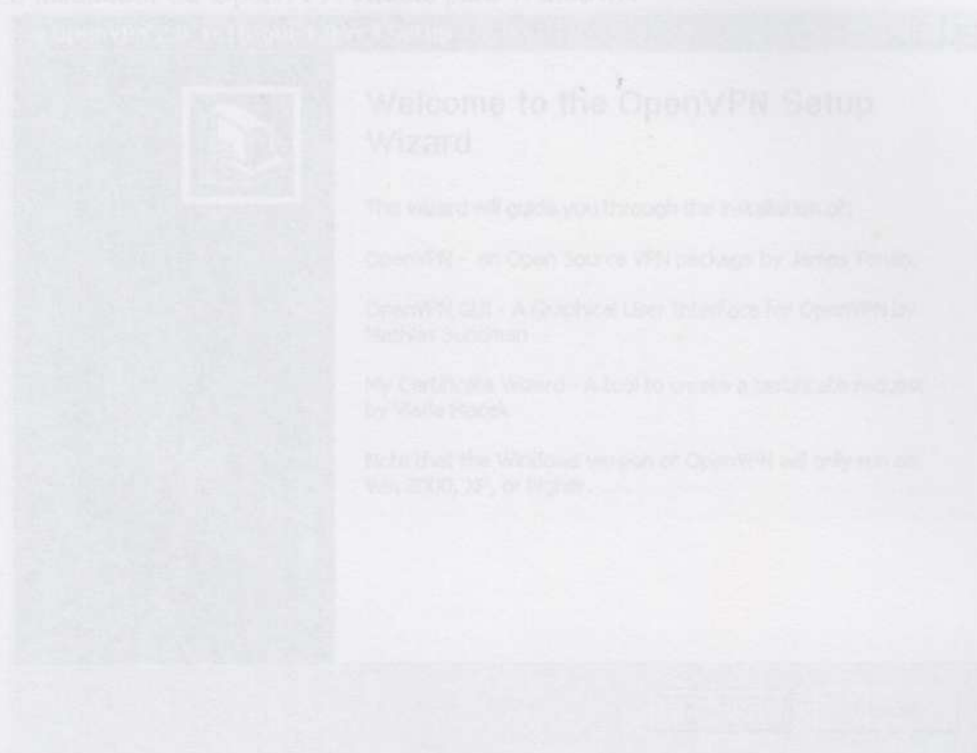
ANEXOS

Baixar o software OpenVPN Client: Para WINDOWS do Site:

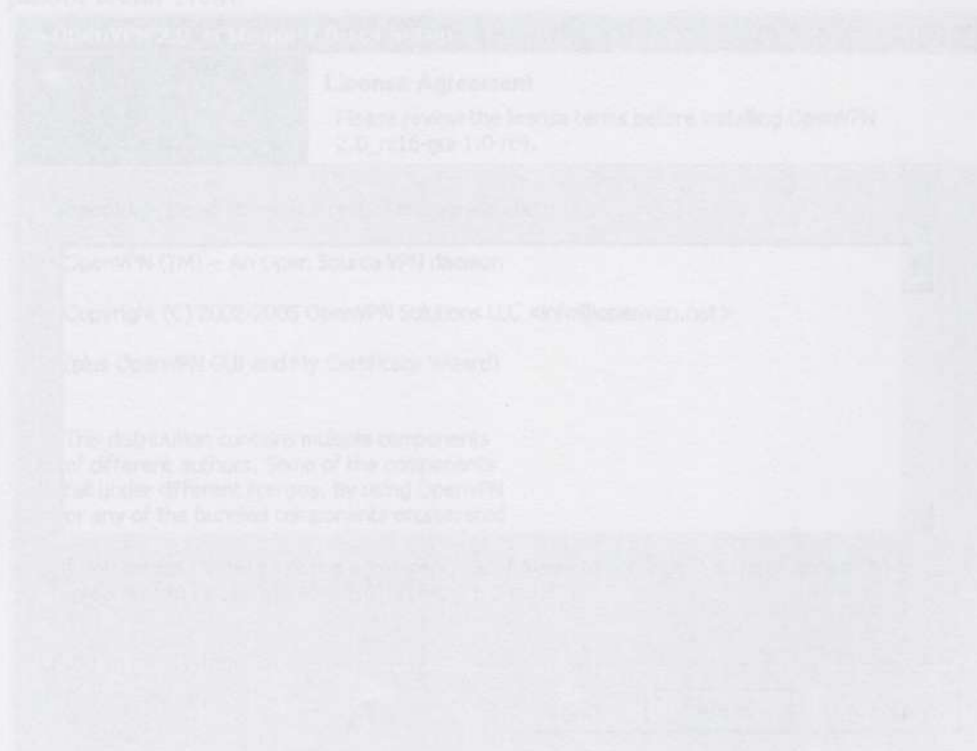
<http://openvpn.net/download.html>

Sequência de Instalação da OpenVPN Cliente Para WINDOWS

Executar o instalador do OpenVPN cliente para Windows.



Próximo passo, clicar Next.



ANEXO 1 Como instalar componentes e teclar Next

Baixar o software OpenVPN Cliente Para WINDOWS do Site:

<http://openvpn.net/download.html>

Seqüência de Instalação do OpenVPN Cliente Para WINDOWS

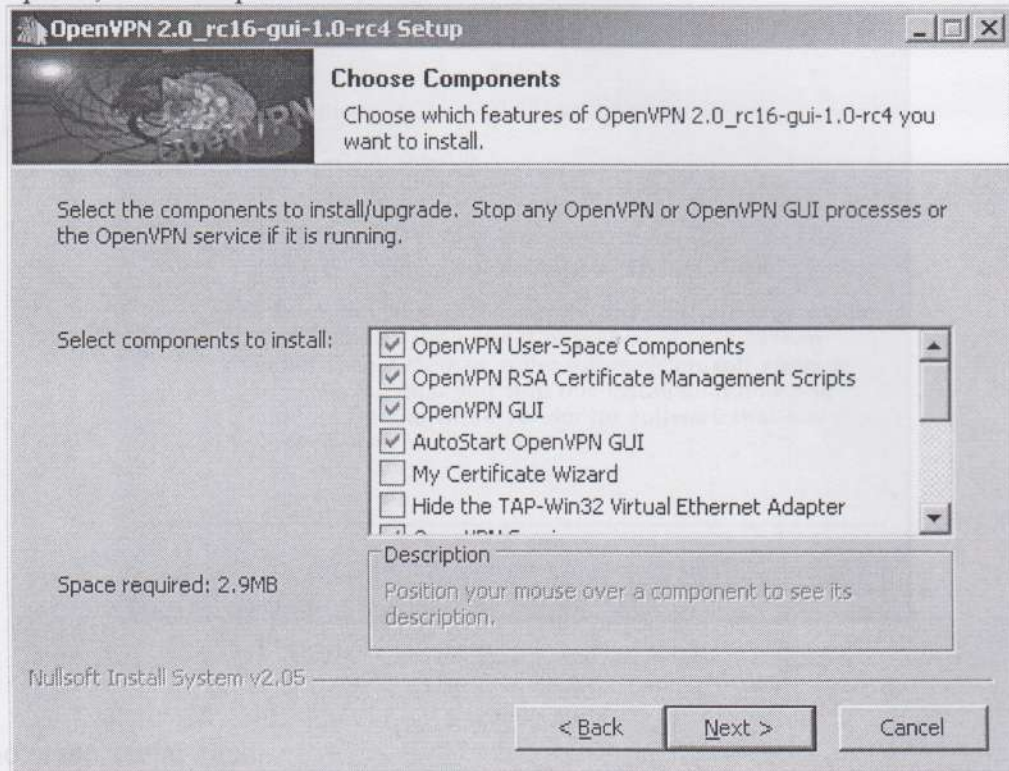
Executar o instalador do OpenVPN cliente para Windows.



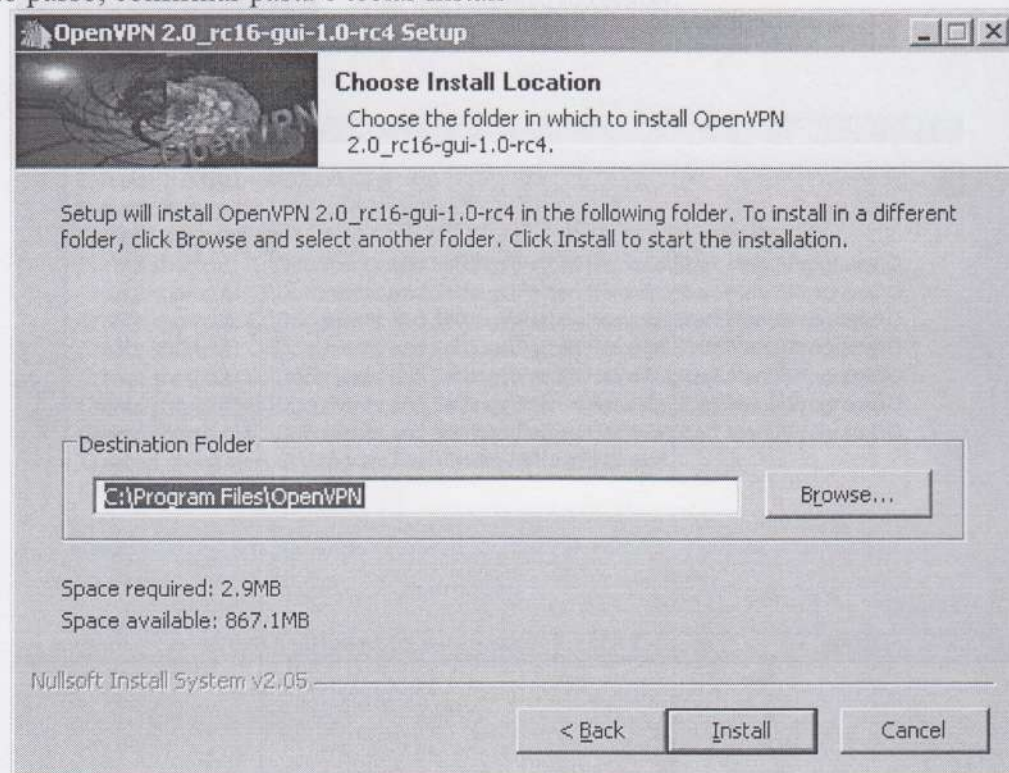
Próximo passo, teclar Next.



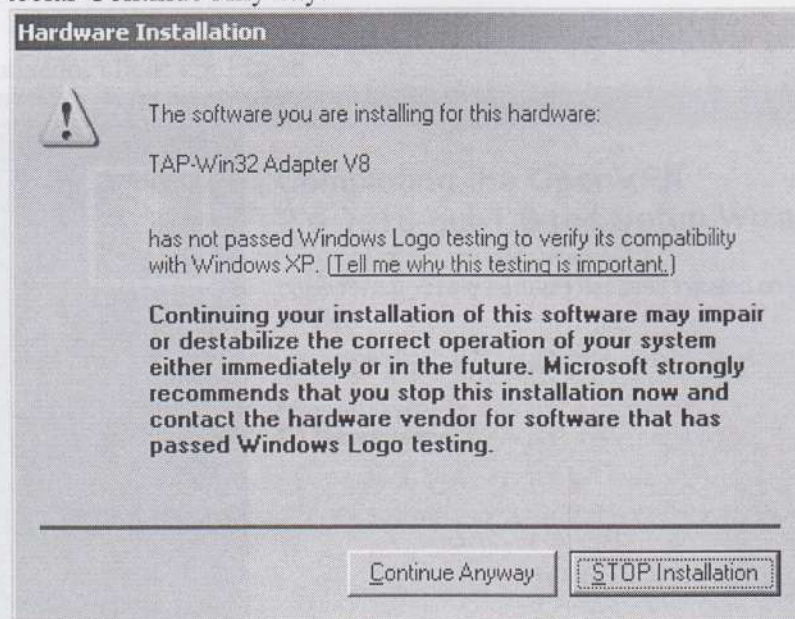
Próximo passo, setar componentes e teclar Next.



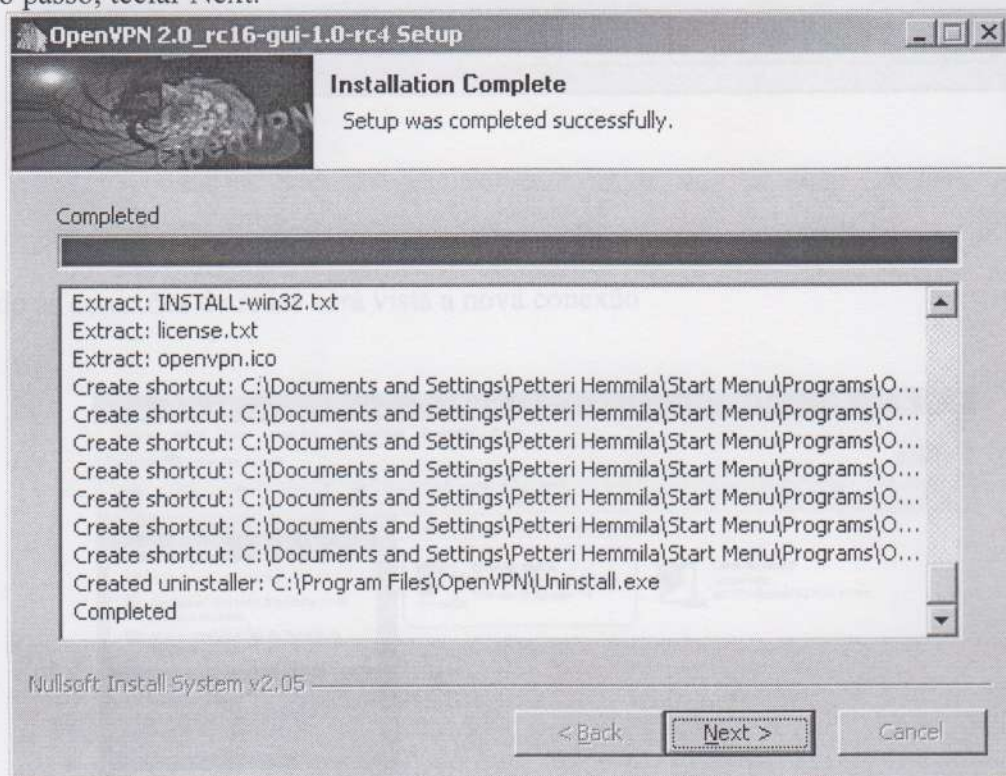
Próximo passo, confirmar pasta e teclar Install



Próximo passo, teclar Continue Anyway.



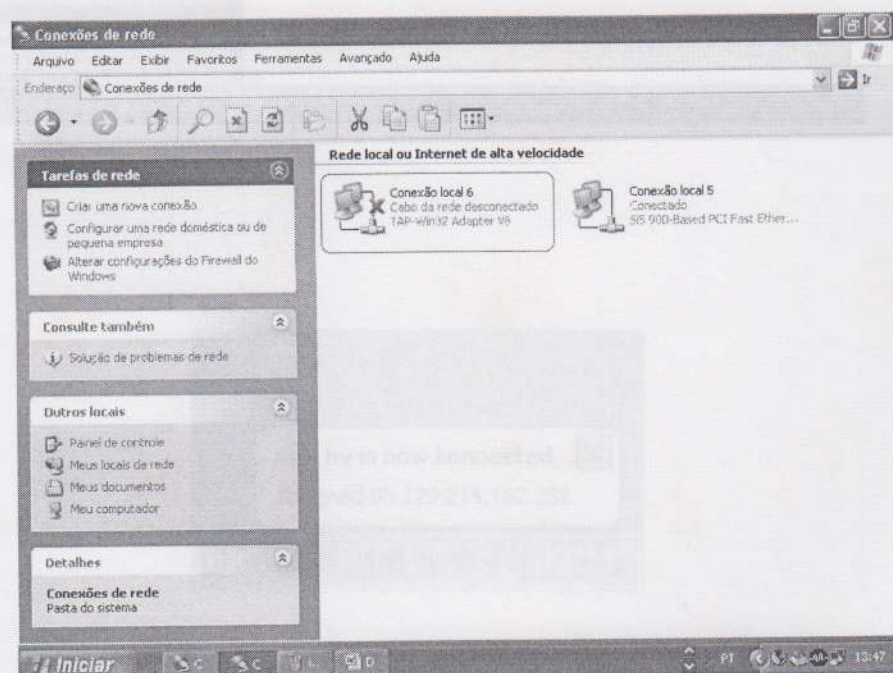
Próximo passo, teclar Next.



Terminar a instalação, clicar em Finish.



Olhando as conexões de redes será vista a nova conexão

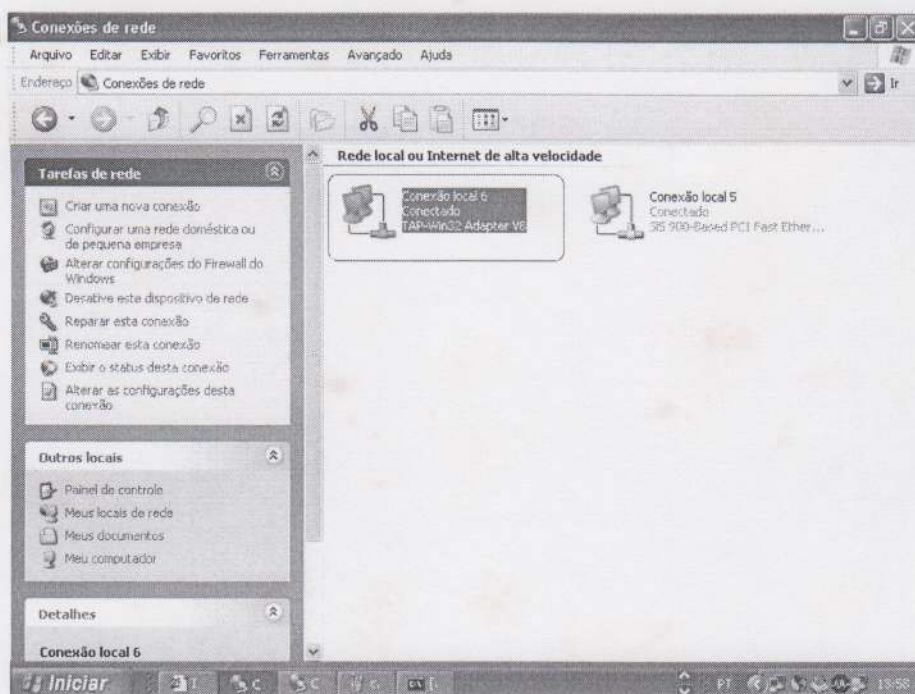


Caso esteja setada a opção mostrar ícone na área de notificação nas propriedades, será visto.



Quando o notebook se conectar ao servidor será visto a conexão ativa.

Tanto aqui.



Como aqui.

