CENTRO PAULA SOUZA

**FACULDADE DE TECNOLOGIA DE AMERICANA**

**Curso de Segurança da Informação**

Alan Marchini

# A SEGURANÇA DA INFORMAÇÃO EM VPNS (REDE PRIVADAS VIRTUAIS)

**Americana, SP**

**2014**

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Segurança da Informação

Alan Marchini

# A SEGURANÇA DA INFORMAÇÃO EM VPNS (REDE PRIVADAS VIRTUAIS)

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação da Fatec-Americana, sob a orientação do Prof. Me. Henri Alves Godoy.

Área de concentração: Tecnologia da Informação

**Americana, S. P.**

**2014**

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS**
**Dados Internacionais de Catalogação-na-fonte**

Marchini, Alan
M265s A segurança na informação em VPNs (Redes privadas virtuais). / Alan Marchini. – Americana: 2014.
80f.

Monografia ( Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Henri Alves de Godoy

1. Segurança em sistemas de informação I. Godoy, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:681.518.5

Alan Marchini

# A SEGURANÇA DA INFORMAÇÃO EM VPNS (REDE PRIVADAS VIRTUAIS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Tecnologia da Informação.

Americana, 01 de dezembro de 2014.

**Banca Examinadora:**

Prof. Me. Henri Alves Godoy (Presidente)
Analista de Redes
Fatec - Americana

Prof.ª Me. Maria Cristina da Luz Fraga Moreira Aranha
Fatec - Americana

Prof.ª Me. Maria Elizete Luz Saes
Fatec - Americana

## AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado a oportunidade de chegar até aqui e por estar concluindo mais um processo em minha vida. Também pela capacidade que me deu para aprender todos os devidos conhecimentos adquiridos ao decorrer de meu curso.

Ao prof. Me. Henri Alves Godoy, por estar me auxiliando e orientando nesse Trabalho Técnico Cientifico, bem como ao Prof. Rossano, que possibilitou que eu entendesse o Linux com suas aulas.

Aos meus amigos de classe que formei durante todos os semestres de aprendizado nesta faculdade, pelo apoio e cooperação em todos as atividades feitas e trabalhos em grupos, além dos bons momentos passados juntos.

Aos diversos professores com os quais tive aulas que dedicaram seu tempo e empenho, me auxiliando para que eu obtivesse o conhecimento, tanto teórico como prático, que possuo hoje.

## DEDICATÓRIA

Primeiramente queria dedicar este trabalho a Deus, pois Ele que nos deu inteligência e concede cada dia o fôlego de vida para enfrentarmos todos os nossos desafios.

Segundo, aos meus pais, que sempre se sacrificaram por mim, e se hoje estou aqui, tenho que agradecer somente a eles, pois foram meu apoio nos momentos mais difíceis da minha vida e me possibilitaram realizar este sonho de fazer uma faculdade e agora me formar.

## RESUMO

Com o avanço na área da Tecnologia da Informação, o explosivo crescimento da Internet, e a necessidade das empresas se comunicarem e trocarem informações de forma cada vez mais rápida e confiável constatou-se que a Internet pode ser uma ótima ferramenta como um meio conveniente para as comunicações corporativas de forma segura e íntegra com um custo muito mais baixo que outros possíveis métodos a serem utilizados. Para isso, é necessário o uso de uma tecnologia que torne esse meio realmente um meio confiável. Este projeto tem como objetivo dar uma visão global do que é uma *Virtual Private Network* (VPN), começando por origem, seu funcionamento detalhado, uma descrição dos protocolos que a mesmo utiliza, a importância de sua utilização no mundo corporativo atual, como é utilizada e questões relacionadas diretamente à Segurança da Informação na implementação de uma VPN, bem como os tipos de criptografia e certificados que poderão ser utilizados para integridade, confidencialidade e autenticidade efetiva na preservação dos dados. No estudo de caso, será apresentado uma implementação detalhada de dois tipos principais de conexões VPN utilizando-se da ferramenta OpenVPN em um meio virtualizado, baseando-se em cenários de redes exemplificados no trabalho. O teste de segurança se baseará no uso de serviços de autenticação inseguros atualmente mostrando as diferenças entre a VPN habilitada e desabilitada, como também o monitoramento de pacotes pela rede por um software sniffer. Os resultados obtidos mostram que a VPN é segura e será melhor abordada no decorrer dos testes de segurança e na conclusão.



**Palavras Chave:** Rede Privada Virtual, VPN, Segurança da Informação, OpenVPN.

## *ABSTRACT*

*With the advancement in the field of Information Technology, the explosive growth of the Internet, and the necessity of the companies to communicate and exchange information in increasingly fast and reliable, it was found that the Internet can be a great tool as a convenient means to corporate communications securely and full with a much lower cost than other possible methods to be used. For this it is necessary to use a technology that makes that really means a reliable means. This project aims to give an overview of what is a Virtual Private Network (VPN), starting at origin, its detailed operation, a description of the protocols that it uses, the importance of its use in today's corporate world, how it is used and related issues directly to Information Security in implementing a VPN, as well as the types of encryption and certificates that can be used for integrity, confidentiality and authenticity effective in the preservation of data. In the case study, a detailed implementation of two main types of VPN connections using the OpenVPN tool in a virtualized environment, based on network scenarios exemplified in the work. The safety test will be based on the use of insecure authentication services currently showing the differences between the VPN enabled and disabled, as well as the monitoring of packets on the network for a sniffer software.*
The results show that the VPN is secure and will be better addressed in the course of safety testing and conclusion.



**Keywords:** *Virtual Private Network, VPN, information security, OpenVPN.*

**SUMÁRIO**


**1 INTRODUÇÃO ..... 12**

**1.1 Objetivo ..... 13**

**2 REDES DE COMPUTADORES ..... 14**

**2.1 Classificações das redes ..... 14**

2.1.1 *Local Area Network* (LAN) ..... **14**

2.1.2 *Metropolitan Area Network (MAN)* ..... **15**

2.1.3 *Wide Area Network (WAN)* ..... **15**

**3 SEGURANÇA DA INFORMAÇÃO ..... 16**

**3.1 Conceito e atributos de Segurança ..... 16**

**3.2 Criptografia ..... 17**

3.2.1 Chave Simétrica ou Chave Privada ..... **18**

3.2.2 Chave Assimétrica ou Chave Pública ..... **19**

**3.3 Algoritmos de Criptografia ..... 20**

**3.4 Algoritmos de Integridade ..... 20**

**3.5 Algoritmo *Diffie-Hellman* ..... 21**

**4 VIRTUAL PRIVATE NETWORK (VPN) ..... 23**

**4.1 Introdução e definição ..... 23**

**4.2 Tipos de VPNs ..... 25**

4.2.1 Acesso remoto ..... **25**

4.2.2 Ponto-a-Ponto ..... **26**

**4.3 Princípios de segurança em VPN ..... 27**

4.3.1 Elementos de uma conexão VPN ..... **27**

**4.4 Segurança em VPN – *Firewall* ..... 29**

4.4.1 Posicionamento do *firewall* ..... **30**

4.4.1.1 Servidor VPN à frente do *firewall* ..... **30**

4.4.1.2 Servidor VPN atrás do *firewall* ..... **30**

4.4.1.3 Servidor VPN ao lado do *firewall* ..... **31**

4.4.1.4 Servidor VPN ao paralelo do *firewall* ..... **31**

**5 PROTOCOLOS E SOFTWARES VPN ..... 32**

**5.1 *Point-to-Point Tunneling Protocol* (PPTP) ..... 32**

**5.2 *Layer Two Forwarding* (L2F) ..... 33**

**5.3 *Layer Two Tunneling Protocol* (L2TP) ..... 34**

5.3.1 Funcionamento do L2TP ..... 35

**5.4 IP *Security* (IPSec) ..... 36**

5.4.1 *Security Association* (SA) ou Associates de Segurança ..... 38

5.4.2 Authentication Header (AH) - (Autenticação por Cabeçalho) ..... 39

5.4.3 *Encapsulation Security Payload* (ESP) - (Encapsulamento de Carga de Segurança) ..... 39

5.4.4 Gerenciamento de chaves ..... 40

**5.5 *Secure Socket Layer (SSL)* ..... 41**

**5.6 OpenVPN ..... 42**

**6 ESTUDO DE CASO ..... 44**

**6.1 Cenários de implementação do OpenVPN ..... 44**

**6.2 Instalação e implementação ..... 46**

**6.3 Configuração do OpenVPN ..... 47**

6.3.1 Cenário 1 – Ponto a Ponto ..... 47

6.3.2 Cenário 2 – Conexão Remota ..... 54

6.3.3 Instalando e configurando Cliente OpenVPN no Windows XP ..... 59

**6.4 Teste de Segurança ..... 60**

6.4.1 Conexão Remota - FTP ..... 61

6.4.2 Conexão Remota – Telnet ..... 65

6.4.3 Conexão Remota – Servidor Apache ..... 70

6.4.4 Ponto a Ponto – FTP ..... 73

**7 CONCLUSÃO ..... 76**

**REFERÊNCIAS BIBLIOGRÁFICAS ..... 78**

## LISTA DE FIGURAS E TABELAS

**Figura 1 – Cifragem e decifragem de uma mensagem ..... 18**
**Figura 2 - Esquema de chave simétrica ou privada..... 19**
**Figura 3 – Esquema de chave assimétrica ou pública ..... 19**
**Figura 4 – Explicação do funcionamento do algoritmo *Diffie-Hellman* ..... 21**
**Figura 5 - Rede privada ligando três locais diferentes..... 23**
**Figura 6 - Tunelamento..... 28**
**Figura 7 - Servidor VPN à frente do *firewall* ..... 30**
**Figura 8 - Servidor VPN atrás do *firewall* na rede de perímetro. ..... 31**
**Figura 9 - Canal de conexão PPTP Datagrama IP ..... 32**
**Figura 10 - Tunelamento PPTP..... 33**
**Figura 11 - Conexão L2TP ..... 35**
**Figura 12 - Encapsulamento L2TP..... 36**
**Figura 13 - IPSec modo transporte ..... 37**
**Figura 14 - IPSec modo túnel ..... 37**
**Figura 15 - Campos do cabeçalho AH ..... 39**
**Figura 16 - Pacote ESP ..... 40**
**Figura 17 - Ponto a Ponto Servidor Matriz e Filial ..... 45**
**Figura 18 - Conexão Remota entre servidor e estação matriz e cliente remoto 45**
**Figura 19 - Interface Interativa do pfSense 2.1 da matriz ..... 46**
**Figura 20 - Configuração IP Estação Matriz (esquerda) e IP Estação Filial (direita)..... 47**
**Figura 21 – Tela de login para a interface navegador do pfSense ..... 48**
**Figura 22 – Interface principal do pfSense ..... 49**
**Figura 23 – Tela de configuração menu OpenVPN – aba Server ..... 50**
**Figura 24 - Tela de configuração menu OpenVPN – aba Server 2..... 51**
**Figura 25 - Tela de configuração menu OpenVPN – aba Client ..... 52**
**Figura 26 - Tela de configuração menu OpenVPN – aba Client 2 ..... 53**
**Figura 27 – Criação de certificado de autoridade da Matriz..... 54**
**Figura 28 – Criação de certificado do usuário ..... 55**
**Figura 29 – Criação de usuário para autenticação e criação do túnel ..... 56**
**Figura 30 – Criação da conexão VPN remota..... 57**
**Figura 31 – Definição das rotas entre as redes diferentes..... 58**

**Figura 32 – Processo de salvar os certificados e configurações para repassar a outro dispositivo ..... 58**
**Figura 33 - Instalação do driver TAP-Win32 ..... 59**
**Figura 34 – Detalhes do arquivo de configuração *.ovpn* ..... 60**
**Figura 35 – Interface principal Wireshark ..... 61**
**Figura 36 – Logon no servidor FTP vindo da máquina remota ..... 62**
**Figura 37 – Momento de captura dos pacotes descriptografados pelo Wireshark ..... 63**
**Figura 38 – Exemplo de como se conectar ..... 63**
**Figura 39 - OpenVPN Conectado ..... 64**
**Figura 40 - Momento de captura dos pacotes criptografados pelo Wireshark .. 64**
**Figura 41 – Passo a passo da digitação no Prompt de comando ..... 65**
**Figura 42 - Momento de captura dos pacotes Telnet descriptografados ..... 66**
**Figura 43 – Detalhes da captura do Wireshark capturando o protocolo Telnet 67**
**Figura 44 – Captura do primeiro caractere do login ..... 67**
**Figura 45 – Abreviação de captura de pacotes mostrando caracteres descobertos ..... 68**
**Figura 46 - Momento de captura dos pacotes Telnet descriptografados ..... 69**
**Figura 47 – Página de autenticação do software Cacti utilizando o servidor Web Apache ..... 70**
**Figura 48 – Pacotes HTTP descriptografados capturados pelo Wireshark ..... 71**
**Figura 49 – Pacotes criptografados capturados pelo Wireshark ..... 72**
**Figura 50 – Interface do capturador de pacotes nativo do pfSense ..... 73**
**Figura 51 – Pacotes capturados ..... 74**
**Figura 52 – Pacotes todos criptografados, resultado da captura ponto a ponto ..... 75**

# 1 INTRODUÇÃO

Com o avanço da tecnologia da informação e dos meios de comunicação, a globalização e a alta necessidade de segurança para todos os meios digitais, grandes e inteligentes serviços e softwares precisaram ser criados a fim de que a troca de informações que inicialmente eram de meros papeis, disquetes e entregues pessoalmente, pudessem ser agora transferidos digitalmente entre simples usuários ou até grandes empresas multinacionais utilizando a maior rede disponível pra isso, que é a Internet, de forma segura, rápida e eficaz.

A Virtual Private Network (VPN) ou Rede privada Virtual surgiu com esse objetivo. Antes linhas privadas eram utilizadas para essa comunicação e troca de informações, porém elas podiam apenas se estender por uma determinada área de cobertura e seu custo tanto de implantação como de manutenção era caro. Com a VPN pode-se usar a Internet para isso, reduzindo grandemente os custos, além de manter a segurança, que é a principal e mais importante questão neste quesito (ROSSI, FRANZZIN, 2000).

O princípio chave de uma VPN é a criação de túneis virtuais pela Internet, e para isso usa se a criptografia, a fim de que as informações passem camufladas por redes alheias e mesmo que elas sejam capturadas, haja uma garantia de que não serão entendidas sem o algoritmo de origem e reveladas a terceiros. (ROSSI, FRANZZIN, 2000).

Uma VPN também tem como função permitir que redes mesmo distantes, possam ser enxergadas como locais. Isso através de conexões remotas como Intranets e Extranets, facilitando muito a troca de informações entre empresas ou mesmo filiais (TYSON, [s.d.]).

Este trabalho abordará as possíveis e seguras opções de VPN e quais os melhores tipos de VPN, bem como apresentará conceitos sobre os protocolos necessários e envolvidos para os diversos tipos de conexões VPN e suas vantagens e desvantagens. Noções de posicionamento de *Firewall* serão abordadas.

No estudo prático, será mostrado o uso de um software gratuito de VPN, bem como sua implementação, funcionalidade e segurança, com testes entre os dois lados da conexão entre empresas e usuários simulando um ambiente real de uma corporação.

## 1.1 **Objetivo**

O objetivo deste trabalho é analisar e estudar a Rede Privada Virtual visando mostrar sua utilidade para o meio corporativo e sua segurança, bem como apresentar uso dos diversos protocolos e tipos de VPN em meio a rede de computadores pública, a Internet.

Para atingir o objetivo geral estabelecido, este trabalho teve como objetivos específicos:

- Analisar aspectos da rede de computadores e também da segurança da Informação;
- Detalhar os diversos protocolos de VPN;
- Implementar uma VPN usando o software Open Source OpenVPN e comprovar que ele é eficaz e seguro.

A metodologia utilizada neste trabalho será através de pesquisas em sites da Internet e por meio da consulta em livros, cujos os autores são: especialistas, formados ou reconhecidos na área. Tudo isso com fontes que possam ser comprovadas no meio da comunidade acadêmica.

O estudo de caso sobre a implementação de uma VPN e teste da mesma será realizado através do software gratuito VirtualBox 4.3.18.r96516 e os Sistemas Operacionais FreeBSD pfSense 2.1 x86, Linux Debian 7.7 x86 e o Microsoft Windows XP Professional x86 SP3. O trabalho faz o estudo dos tipos de VPN, utilização, vantagens de sua implementação no meio corporativo, sua segurança e criptografia empregada. Analisa os tipos de protocolos existentes e quais são realmente seguros com algumas vantagens e desvantagens de sua utilização. Também explica formas de proteger a transferência de pacotes através da VPN.

# 2 REDES DE COMPUTADORES

Redes é um conjunto de computadores autônomos interconectados, trocando informações entre si (TANENBAUM, 2003, 4ª ed, p. 2). Uma rede consiste em dois ou mais dispositivos conectados uns aos outros por meio de um cabo ou mesmo sem cabeamento, para que se possam compartilhar dados. A estrutura de uma rede é composta basicamente por um emissor de algum tipo de informação (aquele que deseja se comunicar, também chamado como origem), o meio pela qual a informação trafega (o canal) e por fim um receptor (destino da informação). Com o passar do tempo, este processo teve inúmeras melhorias de forma que o processo de comunicação se tornou mais rápido, fácil e eficiente.

A ideia principal ao se desenvolver o conceito de “redes”, foi para o princípio militar. Estados Unidos e a Ex-União Soviética, atual Rússia, eram as duas principais potências da década de 60. Os Americanos, através de muitas pesquisas, desenvolveram um método de comunicação para que pudessem interconectar seus vários centros de comandos do país mesmo após uma eventual guerra que afetasse o país. Foi nesse período que foi criado o termo ***backbone***, que traduzido para o português, seria a espinha dorsal da rede. Por ele, várias outras mini redes se conectam e podem se comunicar com outras mini redes. Com o fim da guerra fria, esta estrutura passou a ser utilizada para uso científico e educacional.

## 2.1 **Classificações das redes**

As redes de computadores são classificadas de acordo com a dimensão geográfica que elas ocupam. Assim, os principais tipos de redes classificados são:

### 2.1.1 *Local Area Network* (LAN)

Entende-se por LAN a rede que alcança uma distância de poucas dezenas de metros e geralmente possuem taxas de transmissão de 100 Mbps nas estações e 1 Gbps para o servidor. Geralmente usado em casas, escritórios, escolas e empresas de pequeno porte.

### 2.1.2 *Metropolitan Area Network (MAN)*

Este tipo de rede alcança um perímetro maior de distância. Geralmente cidades pequenas ou grandes universidades. Possui uma taxa de transmissão de dados menor. Muito requisitado por empresas para se comunicarem com filiais.

### 2.1.3 *Wide Area Network (WAN)*

Este tipo é o maior em questões de distância. Atinge todos os países e atravessa continentes. Utilizam enlaces mais extensos como cabos submarinos e satélites. Sua taxa de velocidade é menor, porém tem como principal função interligar redes MAN.

# 3 SEGURANÇA DA INFORMAÇÃO

Com o passar do tempo e o grande aumento do número de redes compartilhadas, criou-se uma grande preocupação com a segurança dos dados, principalmente os privados. Empresas e instituições precisavam cada vez mais garantir que seus dados não estivessem nas mãos de terceiros, podendo, por exemplo, atrapalhar o crescimento das mesmas com o roubo de alguma inovação/descoberta exclusiva. Isso acontece até nos dias atuais, pois a informação possui um valor imenso e há várias tentativas de ataque conhecidas e usadas por quem quer sair lucrando com o acesso não autorizado de informações privilegiadas.

A segurança da Informação pode ser definida com a proteção de um conjunto de dados ou da informação em si, com a intenção de preservar o valor que os mesmos possuem para uma organização, empresa, entre outras. Seus principais atributos são confidencialidade, integridade, disponibilidade, autenticidade e não repúdio. A segurança da Informação não se refere a apenas arquivos de informações eletrônicas, mas também a sistemas computacionais e de armazenamento.

> Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do Padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos. (FERREIRA, ([s.d.]).

## 3.1 Conceito e atributos de Segurança

A Segurança da Informação tem como referência a proteção sobre informações, tanto pessoais, como corporativas. A preservação da informação pode ser afetada por diversos fatores e depende do agente causador. Exemplos destes fatores são pessoas mal intencionadas com o objetivo de furtar, destruir ou modificar; o ambiente em que a informação está armazenada, se é o ideal ou não; fatores comportamentais dos indivíduos (erro humano) e devida política de segurança empregada a respeito do controle de acesso da informação, como também a infraestrutura do local no qual a informação está.

Para chegar a esse nível de proteção, várias ferramentas são utilizadas e recursos como criptografias avançadas são empregados a fim de garantir os principais atributos da segurança da informação que seriam a Confidencialidade, Integridade e Autenticidade, como também não menos importantes, a disponibilidade e o não repúdio da informação, segundo Rossi; Franzin (2000):

> Confidencialidade
> Tendo em vista que estarão sendo utilizados meios públicos de comunicação, a tarefa de interceptar uma sequência de dados é relativamente simples. É imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos.
>
> Integridade
> Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e reencaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas por uma VPN, por exemplo.
>
> Autenticidade
> Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados em pôr um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

Segundo (Lucas, 2010):

**Disponibilidade**: Mesmo a informação sendo segura, não será tão útil assim se não estiver disponível para acesso ou restauração quando for necessário. Para uma informação estar sempre disponível, ela tem que ser armazenada e estar protegida, em um sistema à prova de falhas lógicas e físicas e também redundante.

**Não repúdio**: Ele pode ser definido como uma certa garantia de que o emissor da informação não tenha condições de negar que enviou ou alterou essa informação durante o caminho ao destinatário, ou seja, garantir que haja provas quando for necessário para provar que “alguém fez algo” com a informação.

## 3.2 **Criptografia**

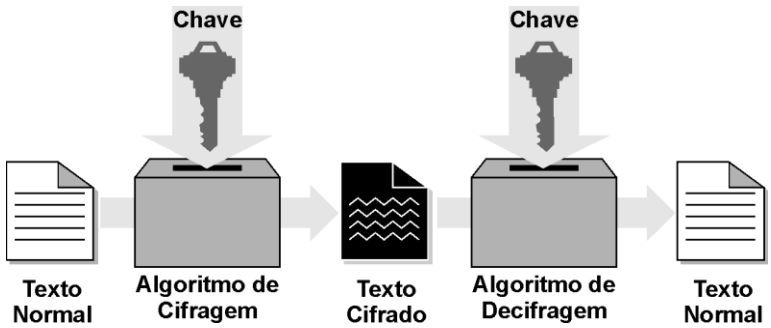
Com toda a preocupação sobre segurança da informação, surgiu uma maneira de se evitar o acesso a dados através da codificação do mesmo. Isso é conhecido como criptografia e permite que apenas quem tenha uma chave ou mais

chaves de acesso, como também o algoritmo de criptográfico possa compreender a informação.

> A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada **comumente** de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem (TRINTA; MACEDO, 1998).

A criptografia é gerada por um conjunto de técnicas de transformações dos dados empregando uma sequência de bits (chave) como padrão a ser utilizado. O objetivo é criar uma sequência de dados que não possa ser entendida por terceiros sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma chave. Todos esses dados serão transmitidos pela rede pública. São chamadas de Chave Simétrica e de Chave Assimétrica as tecnologias utilizadas para criptografar dados. Um exemplo dinâmico se encontra na Figura 1.

**Figura 1 – Cifragem e decifragem de uma mensagem**

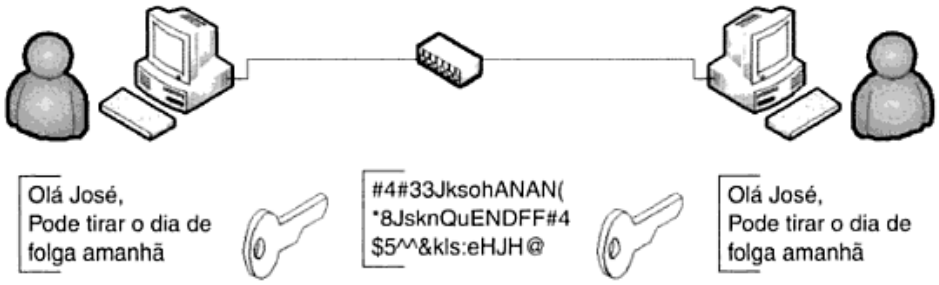



**Fonte: Trinta, Macedo (1998)**

### 3.2.1 Chave Simétrica ou Chave Privada

Neste tipo, é usada apenas uma chave, tanto para entrada na criptografia, quando para a saída na descriptografia, como na Figura 2. É fundamental neste caso que a chave seja bem guardada, para não haver violação da proteção dos dados.

**Figura 2 - Esquema de chave simétrica ou privada**

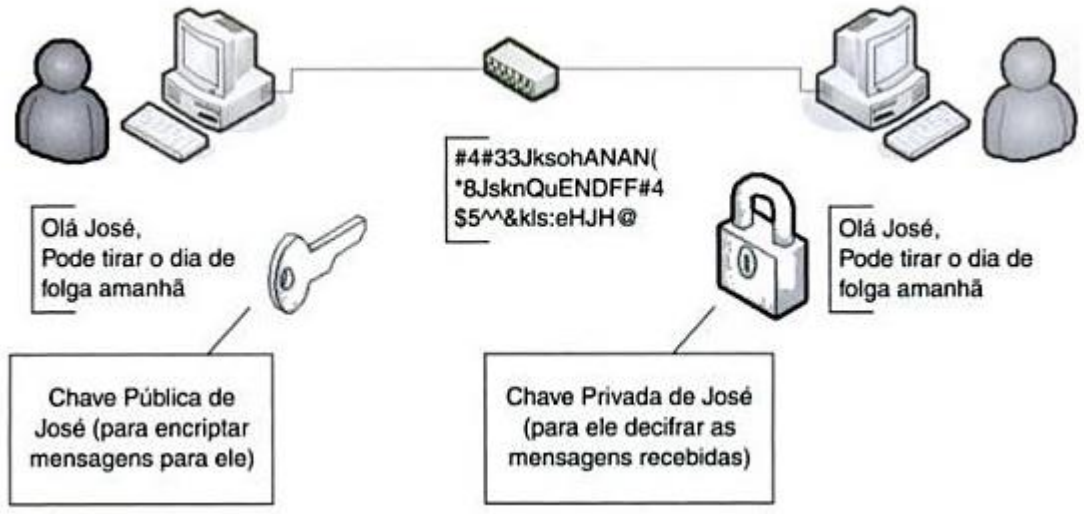



**Fonte: Carvalho (5. ed., 2013, p. 455)**

### 3.2.2 Chave Assimétrica ou Chave Pública

Neste outro tipo exemplificado na Figura 3, a criptografia de chave pública funciona através de uma junção da chave privada com a pública. Quem conhece a chave privada é apenas o computador de origem, porém ele concede uma chave pública a todos que querem se comunicar com ele. Para poder descriptografar uma mensagem, outro computador deve pegar a chave pública já disponibilizada e juntar com sua chave privada que é somente dele. Assim não há como os dados se perderem.

**Figura 3 – Esquema de chave assimétrica ou pública**




**Fonte: Carvalho (5 ed., 2013, p. 459)**

## 3.3 **Algoritmos de Criptografia**

Resumidamente, há alguns algoritmos de criptografia. Eles servem tanto para chave simétrica, como para assimétrica. Primeiro, uma chave criada pelo algoritmo é considerada mais segura ou não devido ao seu tamanho em bits e também a fórmula matemática usada para se gerar a informação criptografada. Serão citados os 3 principais simétricos existentes. Eles são: **DES**, **3DES** (Triple DES) e o **AES** (mais recente). A agência que aprovou comercialmente os três foi a United States Department of Homeland Security, abreviado como DHS, conhecida como Departamento de Segurança Nacional dos Estados Unidos. Muitos *firmwares* de equipamentos e softwares utilizam estes algoritmos.

O DES usa chaves de 40 ou 56 bits. Com este tamanho de criptografia, o algoritmo já pode ser quebrado hoje em dia até que facilmente. Surgiu então o 3DES, que usava o triplo de 56 bits que resultava em 168 bits. Era criptografado três vezes, porém esse processo deixava ele lento. Foi então que surgiu o AES, que originalmente possuía 128 bits de encriptação. Hoje já possui 256 bits. Amplamente utilizado atualmente, como por exemplo, em aparelhos de rede sem fio (CARVALHO, 2013).

## 3.4 **Algoritmos de Integridade**

Também existem algoritmos para integridade dos pacotes, para garantir que as informações que saem não cheguem ao destino adulteradas. Esses algoritmos geram códigos binários únicos com uma sequência de bits que são encapsulados junto aos pacotes. Se chegarem no destinatário adulterados, serão identificados, pois uma verificação é feita antes de enviar e outra no momento da chegada e são comparados os mesmos códigos binários (MIRANDA, 2002).

Os principais algoritmos são:

**SHA-1**: O *Secure Hash Algorithm* (SHA-1), gera uma combinação binaria de 160 bits. Apesar de um tanto considerável de bits, descobriu-se falhas em seu algoritmo em 2005.

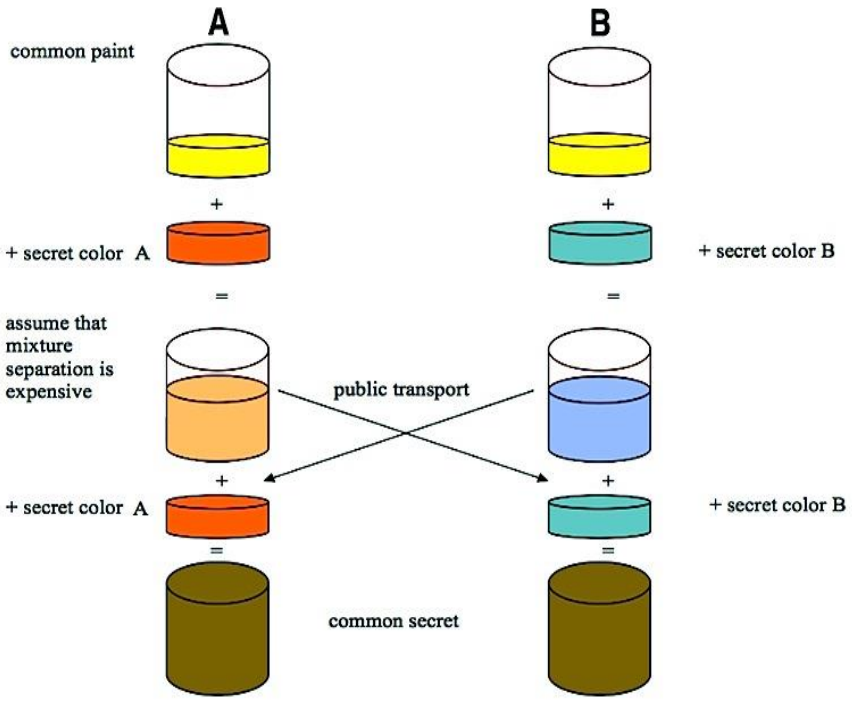
**SHA-2**: Atualização do SHA-1 com correções e uma forma diferente de gerar o *hash*. De acordo com Oliveira (2012, p. 7), “O (SHA-2) executa duas funções *hash* similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512.”

**MD5**: Foi criado em 1991 e o significado das siglas MD é *message digest*. Este algoritmo *hash* utiliza de um valor de 128 bits. Seu objetivo de criação foi com a intenção de ser rápido, seguro e simples. Atualmente, apesar de terem descoberto uma pequena fraqueza, continua sendo utilizado globalmente. Sua maior desvantagem mesmo é utilizar 128 bits. Recomenda-se utilizar *hashs* com mais bits para completa segurança.

## 3.5 Algoritmo *Diffie-Hellman*

Este algoritmo não tem como objetivo criptografar. Sua função é prover rapidez, otimização e eficiência para a troca das chaves privadas e públicas por meio da rede insegura entre os pontos (origem e destino) que querem se comunicar.

**Figura 4 – Explicação do funcionamento do algoritmo Diffie-Hellman**




**Fonte: Vinck (2012, p. 16)**

Além da Figura 4, para uma melhor explicação sobre o assunto, segundo Silva (2002, p. 36),

> O usuário A gera uma chave composta da chave privada dele e a chave pública do usuário B. O usuário B faz o inverso, ou seja, gera uma chave composta da chave privada dele mais a chave pública do usuário A.
> Por meio de um processo matemático, a chave gerada pelo usuário A serve para criptografar os dados a serem enviados ao usuário B e a chave gerada pelo usuário B serve para descriptografar. Inversamente, a chave gerada pelo usuário B serve para criptografar os dados a serem enviados ao usuário A, e a chave gerada pelo usuário A serve para descriptografar.

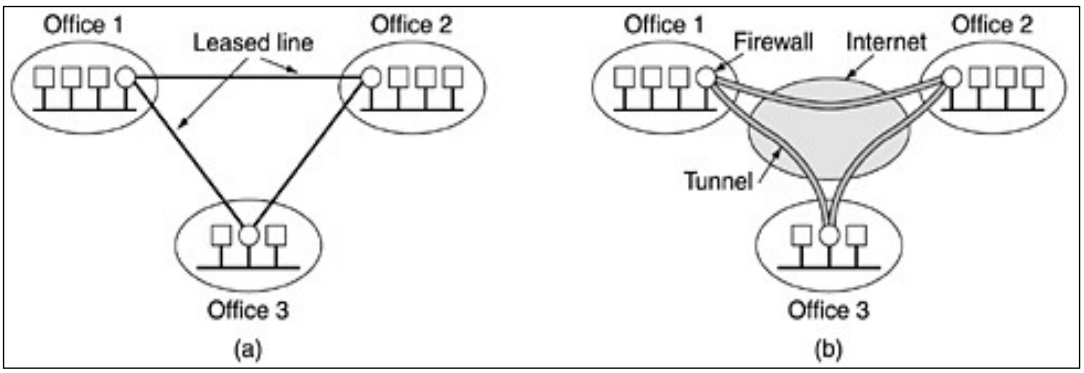
# 4 VIRTUAL PRIVATE NETWORK (VPN)

Este capitulo abrangerá sobre o que é uma VPN, seu funcionamento, função, utilidade e princípios de segurança.

## 4.1 Introdução e definição

Com o passar do tempo, muitas empresas e companhias, foram crescendo e se modernizando. O que era apenas uma matriz, dividiu-se em várias filiais. Às vezes, geograficamente perto umas das outras, porém em alguns casos, até em outros países e continentes, o que criou sérios problemas para uma eficiente e rápida comunicação de dados entre elas. Ainda hoje, quando não há tanta distância entre um local e outro, uma **rede privada** é construída. Um exemplo de rede privada ocorre quando um servidor de alguma empresa se comunica e troca dados com outro servidor de sua filial usando um cabo para conexão entre eles. São separados e não estão nem diretamente, nem indiretamente ligados à Internet e não trafegam pelos mesmos cabos e sim por cabos próprios e exclusivos para a empresa. Esta conexão se assemelha a uma rede ponto a ponto na qual, através de um cabo ou mesmo via *Wireless*, dois computadores se conectam (Rossi, Franzzin, 2000). A seguir na Figura 5, uma demonstração de rede privada conectando três locais distintos.

**Figura 5 - Rede privada ligando três locais diferentes**




**Fonte: Tanenbaum (2003, 4 ed., p. 585)**

Esse tipo de rede é considerado bem segura, porém seu custo é alto e não compensa financeiramente. Há um valor para manutenção destes cabos e equipamentos, podendo acontecer o rompimento dos mesmos devido a alguma

situação, além de em alguns casos, empresas de terceiros serem contratadas somente para administrar essa questão. Foi então que com o surgimento e popularização da Internet, que apresenta um custo bem mais baixo, muitas empresas deixaram as redes privadas e optaram pelo tráfego de seus dados pela rede pública, porém com a mesma possível segurança. Essas empresas contratam planos de Internet não dedicados (compartilhados) ou dedicados, ou seja, contrata-se um plano com o provedor de Internet, que vai disponibilizar uma quantidade x de Mbps de velocidade e largura de banda (limite de dados a serem transferidos). Se torna dedicado quando a conexão é totalmente destinada a quem a contratou, cuja prestadora de serviço tem a obrigação de oferecer no mínimo 99% de velocidade da conexão contratada, sendo que normalmente em uma conexão compartilhada, divide-se com todos os usuários comuns e até algumas empresas menores. Quanto mais usuários ao mesmo tempo acessando e usando, mais lento irá ser o tráfego. Outra diferença, é que nas conexões dedicadas, caso haja alguma falha na rede, as operadoras garantem a máxima disponibilidade possível, com punições caso houver um descumprimento deste contrato. Diferentemente de uma rede compartilhada, que pode haver uma demora maior para se reestabelecer uma conexão.

Segundo Guimarães; Lins; Oliveira (2006, p. 75), “ VPNs (*Virtual Private Networks*) são redes sobrepostas as redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não e memoria real ”. Em outras palavras, VPNs é uma extensão de uma rede privada, mas que atravessa uma rede pública como a Internet. Ela possibilita um computador/servidor enviar e receber dados por meio dessa rede pública ou compartilhada como se estivesse conectada por uma rede privada direta com os mesmo benefícios, funcionalidades e segurança. O que permite tudo isso são os túneis criados pelo caminho desde a origem até o destino e o uso da criptografia ou uma combinação dos dois.

Dentre as principais funcionalidades de uma VPN, está a possiblidade de funcionários de alguma empresa acessar a Intranet da mesma, mesmo que estejam viajando por exemplo.

De acordo com Tyson [s.d.], engenheiro de sistemas certificado pela Microsoft, os principais benefícios de uma rede VPN se resumem em:

- Aumentar a segurança dos dados transmitidos
- Reduzir custos operacionais (em relação a uma rede WAN)
- Reduzir tempo de locomoção e custo de transporte dos usuários remotos
- Aumentar a produtividade
- Simplificar a topologia da rede
- Proporcionar melhores oportunidades de relacionamentos globais
- Prover suporte ao usuário remoto externo
- Prover compatibilidade de rede de dados de banda larga.
- Prover retorno de investimento mais rápido do que a tradicional WAN
- Ampliar a área de conectividade

## 4.2 **Tipos de VPNs**

As VPNs podem ser classificadas em dois tipos de conexão: *usuário-Gateway* (Acesso Remoto) e *Gateway-Gateway* (Ponto a Ponto). A segunda opção é dividida em Intranet e Extranet.

### 4.2.1 Acesso remoto

A **VPN de acesso remoto** é uma conexão usuário-LAN que permite aos usuários estabelecer conexões seguras com uma rede privada. Os usuários podem acessar os recursos de segurança independentemente de onde estiverem como se estivessem conectados diretamente dentro da empresa com o servidor. Um exemplo que pode explicar melhor como funciona essa forma de VPN, seria uma grande empresa que possua vários vendedores espalhados por vários lugares e que necessitam acesso de qualquer local aos dados da empresa, fazendo consulta ao servidor. VPN de acesso remoto também era chamado antigamente de **Virtual Private Dial-up Network** (VPDN), sendo que era necessário discar para um servidor usando um sistema telefônico analógico.

Existem dois componentes necessários para o correto funcionamento da VPN de acesso remoto. O primeiro seria o **Network Access Server (NAS),** também

chamado de Media ***Gateway***, **Network-Attached Storage** ou **Remote-Access Server** (**RAS**)**.** Um NAS pode ser tanto um servidor totalmente dedicado, como também funcionar por meio de um software em um servidor ou máquina. É ele quem permite o acesso de uma VPN através do uso das credenciais do usuário e um processo de autenticação de um servidor de autenticação separado rodando na rede.

O segundo componente vital para o funcionamento dessa VPN é um software cliente. Esse vai possibilitar que os funcionários mantenham acesso com o servidor NAS da empresa. Este software precisa ser instalado em cada computador que quer estabelecer e manter uma conexão com a empresa. A maioria dos sistemas operacionais de hoje já possuem incluídos nativamente o recurso, ainda assim, alguns tipos de VPNs ou mesmo dependendo da política de segurança, softwares específicos precisam ser utilizados. O software cliente configura a conexão encapsulada para um NAS, que o usuário indica por seu endereço na Internet (IP). O software também gera a criptografia necessária para manter a ligação segura. As grandes corporações ou empresas que possuam pessoal especializado costumam comprar, implantar e manter os seus próprios VPNs de acesso remoto. As empresas também podem optar por terceirizar seus serviços de VPN de acesso remoto através de um **Provedor de Serviços Corporativos (ESP).** O ESP configura um NAS e mantém ele funcionando perfeitamente e será explicado ainda neste trabalho (TYSON, [s.d.]).

### 4.2.2 Ponto-a-Ponto

Uma VPN Ponto a Ponto funciona com um princípio diferente do de acesso remoto. Ela possibilita que vários escritórios ou empresas, por exemplo, que estejam em lugares fixos estabeleçam uma conexão segura e confiável entre si, para então a troca de dados através de uma rede pública, no caso a Internet. Esta VPN cria uma conexão entre as redes como se fosse uma só, mesmo estando separadas, permitindo que todos possuam acesso a todas as redes, de acordo com sua permissão/autorização de acesso. Um exemplo de uma empresa que precisa de VPN de ponto a ponto seriam empresas com diversas filiais espalhadas por vários lugares.

Esta topologia de VPN pode ser dividida entre dois outros:

**Intranet** - Se uma empresa pretende que escritórios ou departamentos que pertencem a ela acessem a uma única rede privada mesmo estando em locais diferentes, ela pode criar uma Intranet VPN para conectar cada LAN separada como uma única WAN.

**Extranet** - Quando uma empresa tem uma relação com outra empresa (como um parceiro, fornecedor ou cliente), pode-se construir uma Extranet VPN que conecta LANs dessas empresas. Esta Extranet VPN permite às empresas a trabalhar junto em um ambiente de rede seguro e compartilhado, enquanto impede o acesso a suas Intranets separadas, caso possuam.

Algo que também diferencia a VPN de acesso remoto de Ponto a Ponto é o fato que não se costumam usar os mesmos softwares e equipamentos que os de acesso remoto. Geralmente a Intranet e tanto a Extranet são acessadas pelo navegador de um computador na empresa. Ainda assim existem softwares próprios que podem ser instalados nas máquinas que irão usar o recurso de VPN Ponto a Ponto, porém este método não é o melhor.

## 4.3 **Princípios de segurança em VPN**

Neste tópico serão apresentados os princípios e recursos necessários para o funcionamento e uso de uma Rede Privada Virtual de forma segura.

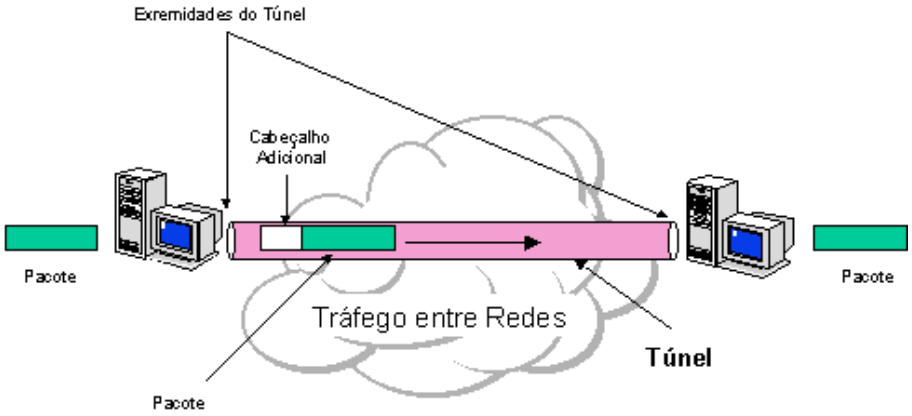
### 4.3.1 Elementos de uma conexão VPN

Os principais elementos de uma conexão VPN são:

- **Tunelamento** – Todas as VPNs atuais precisam usar um recurso chamado de tunelamento para garantir a melhor eficiência no transporte de um pacote. “Tunelamento é o processo de encapsular um tipo de pacote dentro de outro para facilitar algum tipo de vantagem no transporte de uma informação dentro da rede” (Guimarães; Lins; Oliveira, 2006, p. 81). Um túnel pode ser denominado como um caminho lógico criado aonde o pacote irá trafegar ao longo de uma rede pública. O tunelamento possui uma forma de ser feito. Primeiramente, antes de encapsular o pacote que será transportado, ele é criptografado para caso o mesmo seja

interceptado por algum agente exterior desde a sua origem até seu destino. O pacote já criptografado e encapsulado percorre todo seu caminho pela rede pública Internet até chegar ao seu destino quando é desencapsulado e descriptografado para enfim voltar ao seu estado original. Segue exemplo Figura 6.

**Figura 6 - Tunelamento**




**Fonte: Chin (1998)**

Um detalhe importante é que pacotes de um determinado protocolo também podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX (protocolo que trata cada pacote como entidade individual) podem ser encapsulados e transportados dentro de pacotes TCP/IP (CHIN, 1998).

Além disso, o protocolo que é utilizado no tunelamento, encapsula todos os pacotes com um cabeçalho adicional que contém informações de roteamento, possibilitando a entrega o mais corretamente possível durante a viagem pela rede.

• **Autenticação das Extremidades** – Este processo visa garantir que a autenticação das extremidades de uma conexão VPN ocorra de forma íntegra e ainda com verificação por algoritmos de *hash* como o MD5 nas mensagens. Assim somente usuários realmente válidos estarão conectados. O algoritmo MD5 é utilizado para verificar a integridade dos arquivos e *logins* (RUELAS, 2014).

- **Transporte Subjacente**: Segundo Fagundes (2007, p. 38),

> Devido ao protocolo TCP/IP ser a base da Internet, ele é amplamente utilizado para a comunicação entre redes. Entretanto, ele é muito inseguro. Por isso, uma VPN utiliza a infraestrutura da rede já existente do TCP/IP

> para transmitir os seus pacotes pela Internet adicionando alguns cabeçalhos, o que possibilita a instalação destes em qualquer parte da rede.

## 4.4 **Segurança em VPN – *Firewall***

Outro recurso totalmente indispensável em uma eficiente VPN é o *firewall*. Segundo Pinheiro (2004),

> *Firewall* pode ser definido como uma coleção de componentes ou mesmo um sistema colocado entre duas redes de comunicação e que possui as seguintes propriedades:
>
> - Todo o Trafego de dentro para fora dessa rede e vice-versa deve passar pelo f*irewall*.
> - Só o trafego definido pela política de segurança da rede é permitido a passar pelo f*irewall*.
> - O próprio sistema do *firewall* deve ser altamente resistente a qualquer tentativa de invasão

Ele pode ser tanto implementado via software instalado em um servidor ou mesmo dedicado, como um hardware separado. É capaz de controlar o acesso e evitar os acessos não autorizados em uma rede local de alguma organização. Assim, ele protege a rede interna da externa, sendo que todas as requisições obrigatoriamente necessitam passar por ele.

Ainda segundo Pinheiro (2004), existe três tipos de f*irewall*:

- Filtros de pacotes – Este é o tipo mais comum utilizado. Sua função é simples. Ele permite ou nega que determinados pacotes entrem na rede, de acordo com o endereço IP e portas de origem e destino;

- Inspeção de pacotes com informações de estado - além de possuir as mesmas funções do filtro de pacotes, este tipo sempre verifica o estado da conexão, ou seja, apenas permanecem válidas aquelas conexões previamente estabelecidas que cumprem as condições configuradas pelo *firewall*;

- Aplicativos de *Firewall* e de Proxy - são os mais complexos e precisam ser melhor configurados para uma boa efetividade, pois verificam todos os dados que entram e saem da rede, descartando os perigosos ou não autorizados, não permitindo que a rede interna fique exposta.

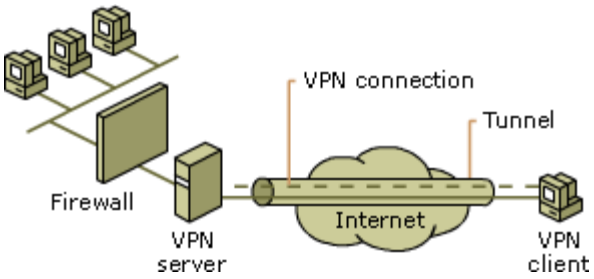
### 4.4.1 Posicionamento do *firewall*

Segundo Figueiredo (2001), há quatro maneiras de se utilizar um *firewall* juntamente com um servidor VPN e é de suma importância, já que os *firewall*s não conseguem aplicar suas regras a pacotes cifrados.

#### 4.4.1.1 Servidor VPN à frente do *firewall*

Se ele está à frente do *firewall* e conectado diretamente a rede externa (Internet), pode apresentar uma possível falta de otimização e segurança. Os pacotes que vierem de fora poderão vir de forma cifrada ou não cifrada, ou melhor dizendo, nem todos os pacotes seriam destinados ao *Gateway* VPN diretamente, sendo que ainda pacotes já decifrados acabam sendo filtrados novamente pelo *firewall*. O *Gateway* VPN também pode ser invadido e comprometido, já que não tem o *firewall* para o proteger. O exemplo de rede com servidor VPN a frente do *firewall* se encontra na Figura 7.

**Figura 7 - Servidor VPN à frente do *firewall***




**Fonte: TechNet [s.d].**[1]

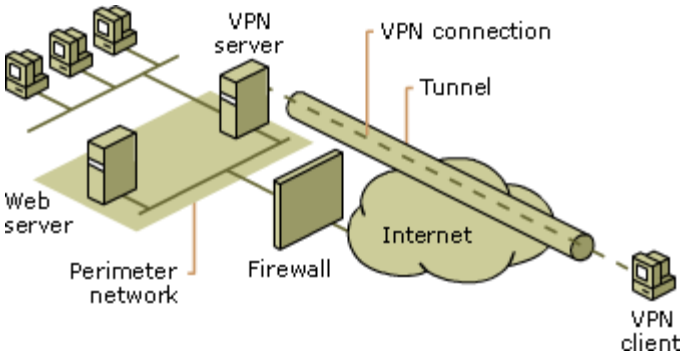
#### 4.4.1.2 Servidor VPN atrás do *firewall*

Neste caso, o funcionamento é bem diferente. As regras do *firewall* precisam permitir que os tráfegos dos arquivos cifrados passem por ele. A porta 50 (AH), 51 (ESP) e pacotes UDP na porta 500 (IKE) precisam estar liberados. O *Firewall* em si não conseguirá filtrar as partes cifradas que já foram endereçadas ao *Gateway* VPN.

[1] Disponível em: http://technet.microsoft.com/pt-br/library/cc753364(v=ws.10).aspx. Acessado em: 15 out. 2014.

Este é seu ponto de falha, pois o trafego da VPN vai entrar na rede passando abertamente no *firewall* antes. Mais detalhes na Figura 8 a seguir.

**Figura 8 - Servidor VPN atrás do *firewall* na rede de perímetro.**




**Fonte: Technet [s.d][2]**

#### 4.4.1.3 Servidor VPN ao lado do *firewall*

Quando um *Gateway* VPN está implementado ao lado de um *firewall*, ocorre a seguinte situação: O *firewall* primeiro recebe o tráfego cifrado e o envia direto ao *Gateway* VPN. Após isso o *Gateway* VPN decifra e manda de volta ao *firewall* que analisa os dados decifrados manda ao devido destino dentro da rede. É umas das melhores formas de usar o *Gateway* VPN, pois o protege dos ataques de redes não confiáveis e ainda cifra todo os dados, que são decifrados e mandados para ele. A interface externa do *Gateway* VPN deve ser configurada para aceitar somente pacotes cifrados.

#### 4.4.1.4 Servidor VPN ao paralelo do *firewall*

Quando o servidor está em paralelo ao *firewall*, há duas formas de conexão com a rede insegura exterior, que seria pelo *firewall* e pelo VPN. O trafego cifrado apenas é direcionado ao VPN. Como ele está separado do *firewall*, tem que se defender dos ataques externos também, o que não é considerado o ideal.

[2] Disponível em: http://technet.microsoft.com/pt-br/library/cc753364(v=ws.10).aspx. Acessado em: 15 out. 2014.

# 5 PROTOCOLOS E SOFTWARES VPN

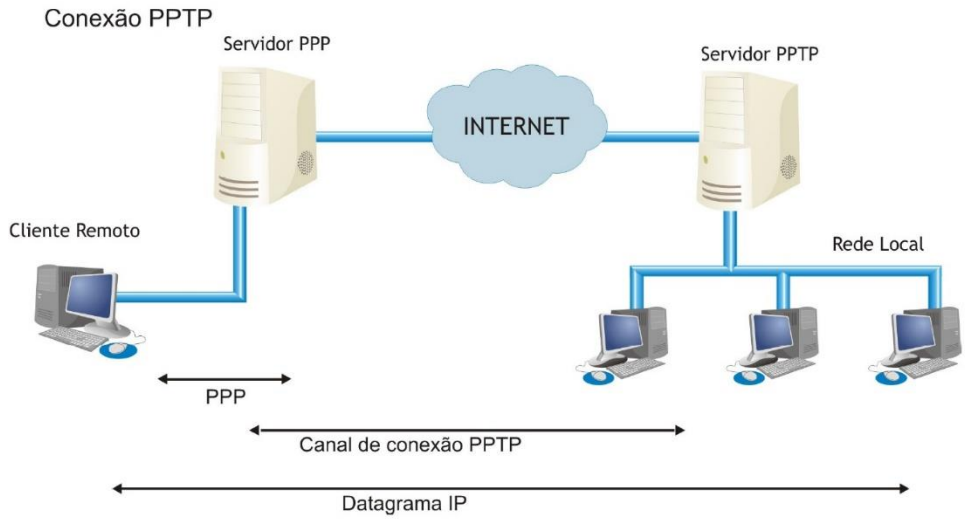
Os protocolos de VPN são os responsáveis pela abertura e também o gerenciamento das sessões de túneis em uma VPN.

## 5.1 *Point-to-Point Tunneling Protocol* (PPTP)

Este protocolo foi originalmente desenvolvido por um fórum de empresas denominado PPTP Fórum, e tinha como principal objetivo possibilitar um fácil acesso de computadores remotos a uma rede privada através de uma rede pública (Internet) baseada em IP, no caso a Internet. É considerado como sendo um dos primeiros protocolos de VPN que surgiram.

O protocolo é nativo do Windows e está implementado desde o Windows NT 4.0 e Windows 95. No Linux apenas se tornou nativo em algumas distribuições atuais, pois é necessário baixar um pacote para usá-lo. O PPTP encapsula pacotes PPP utilizando o protocolo *Generic Routing Encapsulation* (GRE). Este protocolo é definido pela RFC 2784 e sua função é realizar o tunelamento em uma conexão. Foi desenvolvido pela CISCO e a JUNIPER. Assim ele usa o *Point-to-Point Protocol* (PPP) para utilizar o recurso do túnel. Na Figura 9, vê-se como funciona uma conexão PPTP.

**Figura 9 - Canal de conexão PPTP Datagrama IP**

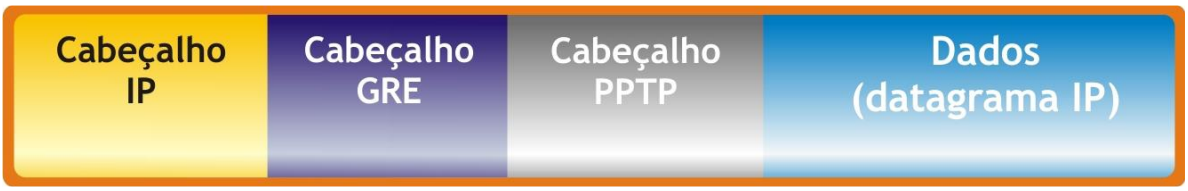



**Fonte: Fagundes (2007, p. 42)**

Para que haja uma conexão PPTP, há processos em sequência que são necessários:

Primeiramente o cliente utiliza do protocolo PPP para se conectar à Internet. Para isso precisa usar um Serviço chamado *Internet Service Provider* (ISP), que seria nosso provedor de Internet. É neste momento que o mesmo protocolo PPP se autentica no *host* destino. O PPP então abre uma conexão com o servidor PPTP pela Internet através de um túnel PPTP utilizando pacotes TCP nos quais todos os detalhes da conexão são definidos. Assim criptografa os dados, encapsula um cabeçalho PPP e um cabeçalho GRE. Logo, é encapsulado com um cabeçalho IP que contém os endereços de origem e destino da conexão PPTP (Fagundes, 2007, p. 41-42). A Figura 10 apresenta um exemplo mais fácil de entendimento sobre o tunelamento PPTP.

**Figura 10 - Tunelamento PPTP.**




**Fonte: Fagundes (2007, p. 43)**

Existem três desvantagens neste protocolo:

> O processo de negociação dos parâmetros de conexão e feito com criptografia muito fraca. As mensagens do canal de controle são transmitidas sem qualquer forma de autenticação ou proteção de integridade. Não existe autenticação no período de negociação dos parâmetros da conexão. (FAGUNDES, 2007, p. 44-45).

## 5.2 ***Layer Two Forwarding*** **(L2F)**

Este protocolo surgiu nos primórdios da tecnologia VPN e foi criado pela Cisco. O L2F é um pouco diferente do PPTP, pois seu tunelamento não necessariamente precisa do IP para funcionar. Por isso ele consegue trabalhar com o ATM e Frame Relay (Estes dois últimos itens são explicados a seguir).

Funcionamento: Primeiro o usuário estabelece uma conexão PPP com o servidor de acesso à rede (NAS) do ISP, então o NAS estabelece um túnel L2F com o *Gateway*. Finalmente o *Gateway* autentica o nome do usuário e a senha e estabelece a conexão PPP. A autenticação e feita quando uma sessão VPN-L2F e estabelecida, o cliente, o NAS e o *Gateway* da Internet usam um sistema triplo de autenticação via CHAP (FAGUNDES, 2007, p. 45-46).

CHAP: *Challenge-Handshake Authentication Protocol* é um método de autenticação seguro usado por protocolos de VPN. Sua principal vantagem de uso é que a cada certo período de tempo determinado nas configurações, ele verifica a identidade do usuário através de um reconhecimento em três etapas com o servidor (*three-way handshake*).

> Após a etapa de estabelecimento da conexão, o servidor RADIUS envia um desafio para o usuário. O usuário então emite uma resposta que contém o hash do segredo compartilhado. O servidor de Autenticação então verifica o valor do hash enviado e o compara com o hash gerado por ele mesmo. Caso o valor esteja correto, o servidor envia um Reconhecimento positivo (ACK). Caso contrário, o servidor finaliza a conexão. Em intervalos de tempo aleatórios, o servidor realiza novamente um desafio para o usuário. (CARVALHO, 2008);

> Logo, o ATM (*Asynchronous Transfer Mode*) é uma arquitetura de transmissão de dados criada com o objetivo de permitir a transmissão eficiente de diversos tipos de dados, como texto, vídeo e áudio. Uma outra arquitetura de rede, o Frame Relay, se caracteriza por transmitir os dados dividindo-os em quadros de tamanho variável. Ao serem enviados, esses quadros percorrem diversos switches da rede, que formam circuitos virtuais. No Frame Relay, a verificação de erros é realizada apenas nas extremidades. Uma forma de baratear os custos para a criação de redes corporativas mantendo a característica autônoma das redes privadas convencionais é através de VPNs que utilizem a infraestrutura de redes Frame Relay ou ATM. (MENDONÇA; ROMEIRO; BAZEIRO, 2009, item 3.1.1.).

## 5.3 ***Layer Two Tunneling Protocol*** **(L2TP)**

O protocolo de tunelamento da Camada 2 foi criado para reunir o que havia de melhor entre os dois protocolos PPTP e L2F. Ele oferece bons recursos de privacidade e está preparado para o crescimento da rede e o intenso uso dela. Também funciona com o *Frame Relay* ou *ATM.*

Há dois modos de tunelamento que este protocolo permite (FAGUNDES, 2007, p. 47):

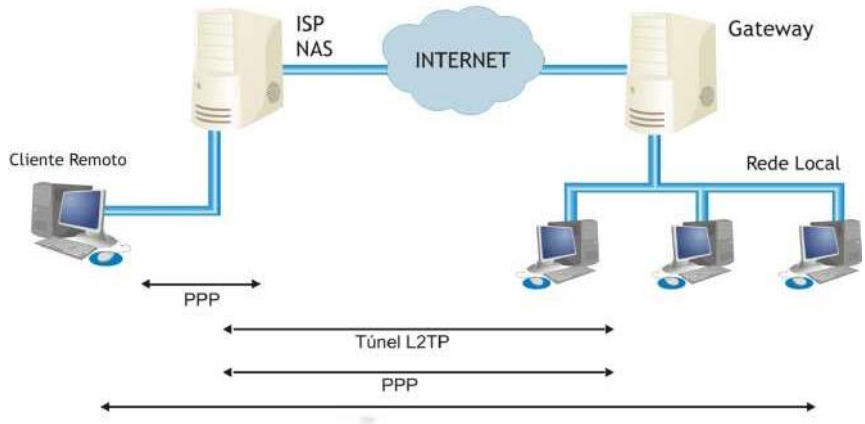
Na forma **voluntária**, as requisições do túnel são iniciadas de um computador/usuário remoto. Não necessita que um servidor as crie e é o melhor para usuários que estão utilizando-o em ambientes externos.

Pela forma **compulsória**, o túnel é criado pelo servidor, porém todas as devidas configurações do mesmo necessitam ser pré configuradas para o tunelamento.

### 5.3.1 Funcionamento do L2TP

Primeiramente o cliente L2TP faz uma requisição ao servidor, para então se conectar e se autenticar. Após esse processo inicial, o concentrador de acessos LAC (*L2TP Access Concentrator*) troca mensagens PPP com o servidor L2TP para a criação dos túneis. O L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão. Os quadros enviados pelo usuário são aceitos pelo ISP, encapsulados em pacotes L2TP e encaminhados pelo túnel. No *Gateway* de destino os quadros L2TP são desencapsulados e os pacotes originais são processados para interface apropriada (FAGUNDES, 2007, p. 47), como mostrado na Figura 11.

**Figura 11 - Conexão L2TP**




**Fonte: Fagundes (2007, p. 47).**

Segue exemplo na Figura 12, o cabeçalho L2TP sendo ilustrado:

**Figura 12 - Encapsulamento L2TP**


**Fonte: Fagundes (2007, p. 49)**

Desvantagens:

O L2TP, apesar de ser melhor que o PPTP, ainda não é seguro sozinho. Não é recomendado seu uso em redes públicas como a Internet, pois a não possui processos para gerenciamento de chaves criptográficas, tornando seguro apenas com a junção do IPSec ou outros protocolos, por exemplo. Ainda também é vulnerável a ataques de DoS (Ataque de Negação de Serviço) (FAGUNDES, 2007).

## 5.4 **IP *Security* (IPSec)**

Devido a uma falta de segurança que existia no protocolo IP, em 1995, foi criado pelo IETF (Internet Engineering Task Force), um grupo de segurança do protocolo IP, o IPSec (*IP Security*). O IPSec já está contido no IPv6, porém como a adoção dessa versão está bem devagar, ele também foi adaptado na versão IPv4.

O IPSec apresenta algumas características especiais. Além de ser mais fácil configurá-lo, pois pode ser implementado com políticas de segurança, ele pode se aliar a outros protocolos tornando a informação muito mais segura. A criptografia é um dos elementos principais do IPSec. Ele pode ser usado no modo túnel como padrão ou em associação com o protocolo L2TP, aonde o L2TP fica responsável pela criptografia dos dados. Este método é chamado de modo de transporte. No modo túnel, somente se consegue utilizar o IPSec em redes baseadas em IP. Como o L2TP é um protocolo de nível de transporte, esse conjunto possibilita transportar não apenas pacotes IP, porém IPX, NetBEUI, entre outros.

O IPSec pode trabalhar de dois modos diferentes, no modo transporte e no modo túnel.

No **modo transporte** somente a parte principal do Datagrama IP, que seria o *Payload* é gerenciado e criptografado pelo IPSec após a adição de um cabeçalho IPSec logo após o cabeçalho IP original, como Figura 13, de modo que apenas os protocolos superiores podem ser cifrados/autenticados (BRAGHETTO; SILVA; BARBOSA, 2003, p. 7). Este modo é mais usado em comunicação *host-to-host*.

Nesse modo, somente a mensagem (*payload*)[3] é criptografada. O roteamento permanece intacto, desde que o cabeçalho do IP não seja modificado e nem cifrado; entretanto, quando o cabeçalho da autenticação é usado, os endereços IP não podem ser traduzidos, porque isto invalida o valor de hash. As camadas de transporte e de aplicação são fixas sempre pelo hash, assim, não podem sofrer nenhuma modificação. O modo transporte é usado para comunicações de host-a-host.

**Figura 13 - IPSec modo transporte**


**Fonte: Fagundes (2007, p. 50)**

No **modo túnel**, segundo (BRAGHETTO; SILVA; BARBOSA, 2003, p. 7), no modo túnel o datagrama inteiro incluindo cabeçalhos são cifrados e um novo cabeçalho IP é criado. Isto permite "escondermos" o endereço IP de origem e destino originais, impedindo a alteração ou conhecimento do atacante das partes envolvida. Exemplo, Figura 14.

**Figura 14 - IPSec modo túnel**


**Fonte: Fagundes (2007, p. 50)**

[3] É a parte mais importante de um dado em uma transmissão, excluindo cabeçalhos, ou origem e destino do IP, por exemplo.

### 5.4.1 *Security Association* (SA) ou Associates de Segurança

Este recurso contém todas as informações como o algoritmo de criptografia, chaves secretas ou sequências de números, funções *hash,* modo de funcionamento (túnel ou transporte), porta de comunicação e outras, necessárias para a correta conexão e configuração entre as entidades do IPSec.

O IPSec usa dois bancos de dados para armazenamento de algumas configurações:

***Security Police Database*** **(SPD)** – Neste banco de dados, estão armazenadas as políticas de segurança dos pacotes, já pré estabelecidas pelo administrador da rede. Se o pacote a trafegar na conexão de rede passar por esse filtro de políticas, ele poderá ser aceito e o IPSec será aplicado sobre ele ou recusado, caso alguma regra seja violada. Há casos também que o pacote tem permissão de entrar mesmo sem o IPSec.

***Security Association Database*** **(SAD)** – Segundo Guimarães, Lins e Oliveira (2006, pág. 115), o SAD contém todos os conjuntos de parâmetros associados à AS, como algumas das seguintes informações:

- Índice dos parâmetros de segurança (SPI);
- Tipo de protocolo AH ou ESP;
- Modo túnel ou modo transporte;
- Sequencial do pacote IP dentro da SA;
- Número máximo de unidades de transmissão;
- Endereço IP de origem da SA;
- Endereço IP de destino da SA;
- Algoritmo de autenticação e sua chave;
- Algoritmo de criptografia e sua chave;
- Tempo de vida das chaves;
- Tempo de vida da AS.

O IPSec apresenta três características principais apresentadas abaixo:

### 5.4.2 Authentication Header (AH) - (Autenticação por Cabeçalho)

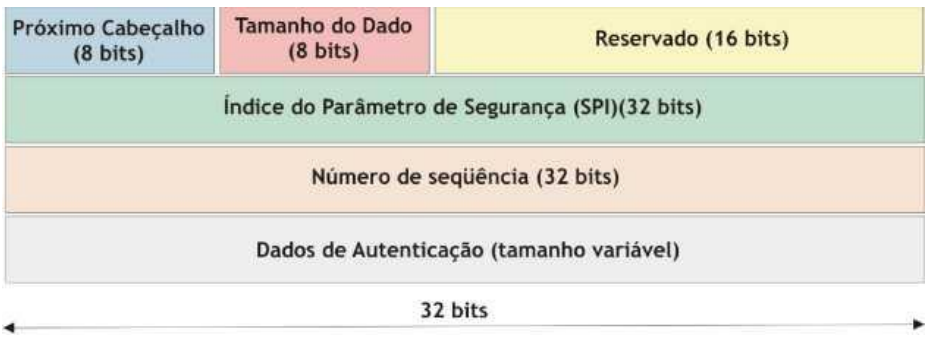
Segundo Fagundes (2007), a utilização do protocolo AH previne ataques do tipo *replay, spoofing* e *hijacking.* Isso porque o protocolo faz uso de mecanismos de autenticação. Para proteger um pacote, o AH insere um cabeçalho dentro do pacote a ser protegido, utiliza um número sequencial, que é zerado a cada estabelecimento de uma nova associação segura e adiciona funções de *hash* ao AH.

Sobre os tipos de ataque citados, segundo Lopez (2003),

> *Replay*, quando o atacante intercepta um pacote válido e autenticado pertencente a uma conexão, replica-o e o reenvia mais tarde, atrapalhando a comunicação. *Spoofing*, quando o atacante assume o papel de uma máquina confiável para o destino e, dessa forma, ganha privilégios na comunicação. "Roubo de conexões" (*connection hijacking*), quando o atacante intercepta um pacote no contexto de uma conexão e passa a participar da comunicação.

A Figura 15 abaixo descreve os campos do protocolo AH.

**Figura 15 - Campos do cabeçalho AH**




**Fonte: Fagundes (2007, p. 51)**

### 5.4.3 *Encapsulation Security Payload* (ESP) - (Encapsulamento de Carga de Segurança)

Responsável por garantir a confidencialidade, assim como também oferecer as características do AH. Ele adiciona em cabeçalho ESP logo após o cabeçalho

AH. Sua função é criptografar a parte referente aos dados *Payload* com um algoritmo que é escolhido ao estabelecimento de uma SA. Segue o exemplo na Figura 16.

**Figura 16 - Pacote ESP**


**Fonte: Fagundes (2007, p. 52).**

### 5.4.4 Gerenciamento de chaves

Existe algumas formas de gerenciamento de chaves dentro do IPSec. Ele pode ser de modo manual ou automático. O IPSec utiliza um protocolo padrão para gerenciamento, o Internet *Key Exchange Protocol* (IKE). Este protocolo é uma combinação de outros dois. O primeiro é o ISAKMP (***Internet Security Association and Key Management Protocol).*** Este possui a função de prover serviços de autenticação e barganha de chaves. O segundo protocolo é o de *Oakley.* Este, descreve os vários modos de trocas de chaves de criptografia (Martins, 2000).

O ***IKE*** opera em duas fases:

Segundo Martins (2000, p. 9-10),

> na fase um, dois pares estabelecem um canal seguro para realizar as operações do ISAKMP (o ISAKMP SA). Na fase dois, os dois pares negociam os SA de propósito geral. O protocolo Oakley prove três modos para a troca de informação de chaves e estabelecimento das SA ISAKMP. O modo Principal (*main mode*) faz a fase um de troca do ISAKMP para estabelecimento de um canal seguro. O modo Agressivo (*agressive mode*) é outra forma de realizar a fase um de troca. Este segundo modo é mais simples e rápido que o modo principal, mas em compensação não protege as identidades dos nós envolvidos na negociação, porque ele transmite suas identidades antes do estabelecimento do canal seguro de comunicação. O modo Rápido (*quick mode*) faz a segunda fase de troca negociando um AS para comunicação de uso geral. O IKE possui ainda um outro modo, chamado Novo Grupo (*new group mode*), o qual não se ajusta à fase um ou dois. Ele segue a fase um de negociação, e é utilizado para

> prover um mecanismo que define grupos privados para troca do tipo Diffie-Hellman.

## 5.5 ***Secure Socket Layer (SSL)***

Desenvolvido pela Netscape Communications, sua principal função era cuidar da segurança entre aplicações cliente/servidor. Ao ser padronizado recebeu o nome de *Transport Layer Security* (TSL) que também pode ser descrito como SSL 3.0. Ele atua entre as camadas de transporte e Aplicação.

Segundo Fagundes (2007, p. 55), os objetivos do protocolo SSL em ordem de prioridade são:

> Garantir o sigilo e a segurança dos dados de uma conexão entre duas partes através do uso de criptografia;
>
> Permitir que programadores pudessem desenvolver aplicações utilizando o SSL/TLS independente de sua plataforma de trabalho, garantindo sua interoperabilidade;
>
> Prover uma estrutura adequada para incorporar novos métodos de criptografia e chave pública quando necessário, sem a necessidade de criar um novo protocolo ou uma nova biblioteca de segurança interna, garantindo assim a extensibilidade do protocolo;
>
> Disponibilização de um esquema opcional para armazenamento temporário de dados das sessões estabelecidas, o que ajuda a diminuir o tráfego entre as partes, logo influencia em um melhor desempenho do protocolo.

O Protocolo SSL e dividido em duas partes:

*SSL Handshake Protocol**:*  Esse protocolo tem como função ser o mediador para uma conexão entre o servidor e o cliente*.* Ele também oferece suporte para o funcionamento do SSL Record.

As mensagens do handshake são feitas trocadas usando um *Message Authentication Code* (MAC) a fim de tornar mais seguro o processo desde o início. O protocolo de *handshake* possui duas fases, numa e feita uma escolha de chave que será utilizada entre o cliente e o servidor, a autenticação do servidor e a troca da chave mestra, já na segunda é feita uma autenticação do cliente, sendo que esta fase pode não ser requerida (Fagundes, 2007).

*SSL Record*

Para a eficiente comunicação deste protocolo, primeiro ocorre o estabelecimento de uma sessão, que é caracterizada por um estado de conexão e sessão. Só é possível este estabelecimento após a conclusão das funções do protocolo *handshake*.

> O protocolo *SSL record* recebe os dados da camada superior e os fragmenta em tamanhos fixos para que possam ser melhor "manuseados" posteriormente, então dependendo dos parâmetros recebidos da fase de negociação do protocolo de *handshake* os dados são ou não compactados, em seguida aplica-se um MAC com uma das funções de *hash.* Agora os dados são encriptados com o algoritmo definido e finalmente transmitidos. A outra extremidade da conexão executa a operação inversa, junta os fragmentos e entrega a mensagem completa para os protocolos da camada superior.
>
> Como vantagens temos:
>
> - Um dos protocolos mais convenientes e utilizados para implementação de transações seguras;
> - Simples implantação;
> - Trabalho independente das aplicações utilizadas e, após o *handshake* inicial, comporta-se como um canal seguro;
> - Possui uma padronização do IETF (FAGUNDES, p. 58, 2007).

## 5.6 **OpenVPN**

O OpenVPN é um software destinado a VPN utilizando criptografia OpenSSL para isso. Possui uma Interface acessada pelo navegador *WEB* e é bastante intuitiva, semelhante a configuração de um roteador comum.

Segundo Marques (2012),

> *O OpenVPN foi desenvolvido por James Yonan e é publicado pela GNU (General Public Licence). É um software destinado a VPN, o qual tem muitos recursos para administração da VPN. Ele utiliza extensivamente a criptografia OpenSSL. Usa também os protocolos SSLv3/TLSv1. Se encontra disponível para vários sistemas operacionais, entre eles: Mac OS X, Windows Server/XP/7/8, Linux, Solaris, FreeBSD e outros. O OpenVPN não é compatível com o protocolo IPsec. Ele trabalha com chaves secretas compartilhadas, autenticação de usuários com senha e autenticação com certificados. Existe uma vantagem na utilização desse software que é a forma de transmissão dos pacotes, que pode utilizar o protocolo UDP ou TCP, sendo que o UDP é o mais adequado, porque este protocolo transmite os pacotes diretamente, sem repetição, o que é melhor para o desempenho da rede.*

Um outro pacote deve ser instalado junto ao OpenVPN para aumentar a gama de segurança para este tipo de VPN, que seria o OpenSSL no Linux. Ele possibilita usar os recursos do SSL e TLS nas configurações do software, já que estes dois protocolos servem para criptografar promovendo a integridade e privacidade dos dados entre a comunicação das duas partes envolvidas (MARQUES, 2012).

Existem dois tipos básicos de túneis que podem ser criados com o OpenVPN:

**Túneis IP Roteáveis** – ideal para rotear túneis IP ponto-a-ponto sem broadcast. Ligeiramente mais eficientes que túneis ethernet em ponte e mais fáceis de se configurar.

**Túneis Ethernet em Ponte** – pode ser usado em túneis que rodam tanto IP quanto protocolos não IP. Esse tipo de túnel é apropriado para aplicações que rodam via broadcasts, como redes Windows e jogos em LAN. Ele é um pouco mais complexo de se implementar (YONAN, 2004).

# 6 ESTUDO DE CASO

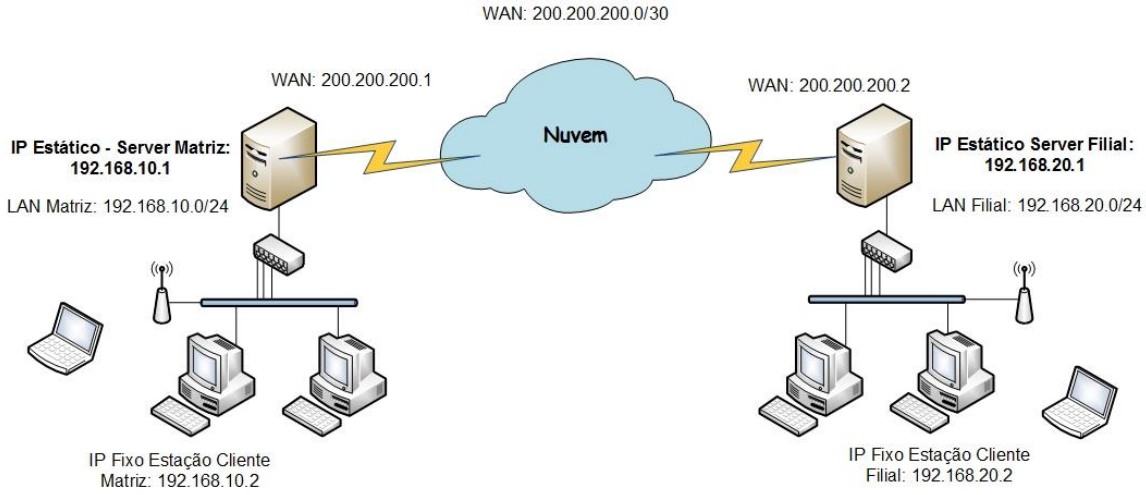
Este trabalho traz como parte prática uma implementação em uma máquina virtual de uma VPN utilizando o OpenVPN, bem como testes de segurança e integridade. Os cenários criados foram baseados nas conexões principais de VPN, ponto a ponto e conexão remota e serão explicados a seguir. Foi utilizado o Wireshark, que seria um *software* de capturas de pacotes individuais que trafegam na rede para monitoramento e levantamento de dados para a conclusão.

## 6.1 **Cenários de implementação do OpenVPN**

Cenário 1: Ponto a ponto

Neste cenário vamos demonstrar como seria uma instalação e implementação de uma VPN entre a matriz de uma empresa e sua filial. A matriz precisa se comunicar e transferir dados para sua filial, bem como para uma estação local da filial e vice-versa. Para isso, é necessário que ambas possuam rede locais (LAN), no caso, a rede da matriz seria 192.168.10.0/24 e da Filial 192.168.20.0/24. O **Servidor Matriz** está com IP Fixo: 192.168.10.1 e o **Servidor Filial**: 192.168.20.1. A Estação local da Matriz está com o IP Fixo atribuído: 192.168.10.2 e a Estação Local da filial com IP Fixo atribuído: 192.168.20.2. Será utilizada a conexão VPN Ponto a Ponto.
Tanto a filial como a matriz, estão utilizando em seus servidores o sistema operacional BSD pfSense 2.1 e cada servidor possui duas interfaces de rede. A em0 (para Internet) e em1 (para rede local). Uma conexão FTP será executada entre a estação da Matriz e a estação da filial. Na Figura 17, está exemplificado melhor o modelo ponto a ponto de conexão entre os servidores.

**Figura 17 - Ponto a Ponto Servidor Matriz e Filial**

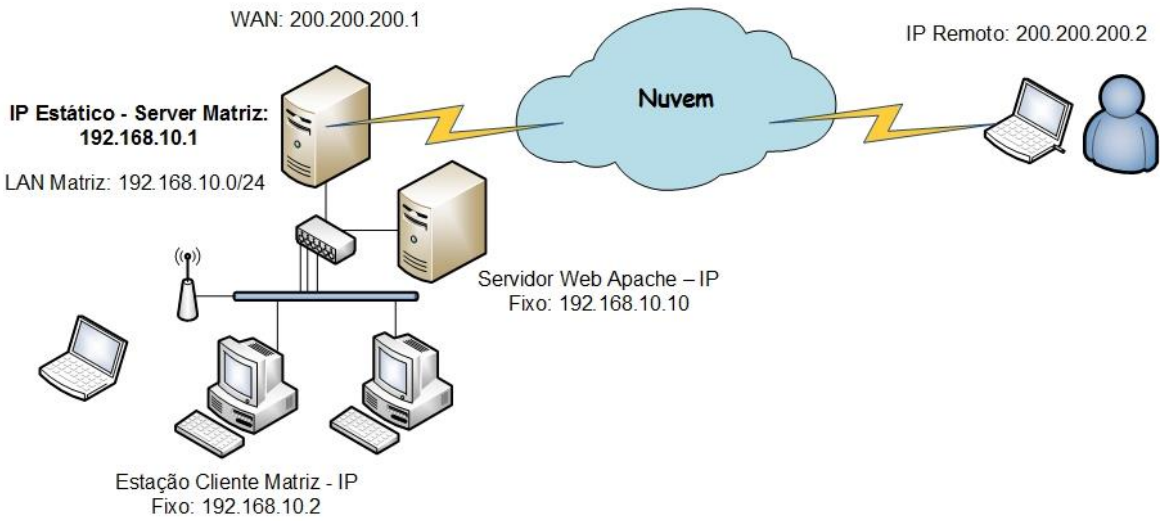



**Fonte: Próprio Autor**

Cenário 2: Conexão remota

Neste cenário há uma diferença entre o da Matriz e da filial. O servidor Matriz é mantido, porém quem vai se conectar a ele é uma máquina remota cliente, provavelmente um *notebook*, por exemplo. Imagine uma empresa, com vários funcionários trabalhando em diversos locais ou mesmo, alguns deles atendendo um cliente enquanto faz uma venda pelo *notebook*, que está conectado através de uma conexão 3G e precisa que o pedido seja repassado com segurança para reduzir o tempo de entrega ao comprador. Exemplo a seguir na Figura 18:

**Figura 18 - Conexão Remota entre servidor e estação matriz e cliente remoto**



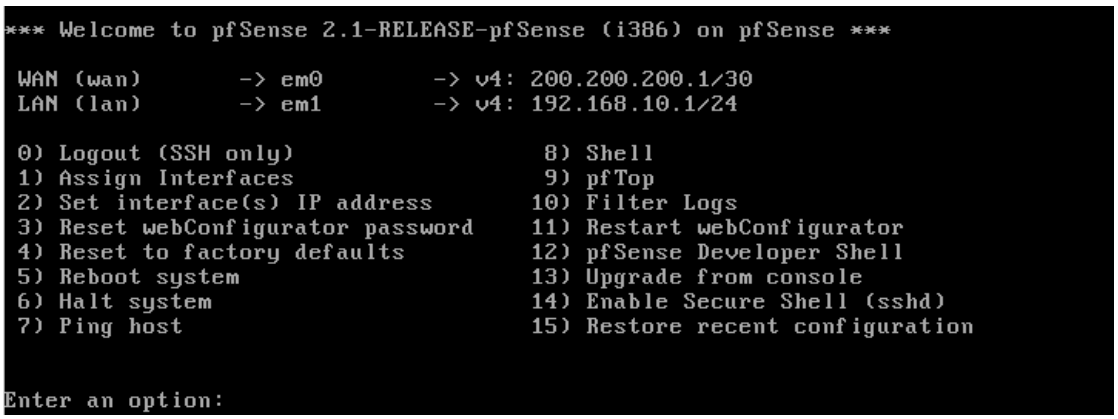

**Fonte: Próprio Autor**

Neste caso, o servidor da matriz possui o mesmo BSD pfSense 2.1 e o cliente estará utilizando o Windows XP SP3 com uma conexão por modem 3G utilizando um IP fixo simulado 200.200.200.2. O **Servidor Matriz** continua com IP Fixo: 192.168.10.1 e também será utilizado uma estação da Matriz com endereço fixo: 192.168.10.2 e um Servidor de Web Apache com o Endereço IP Fixo: 192.168.10.10. Será simulada uma conexão via FTP, Telnet e Web através do servidor Apache com autenticação entre está estação e o notebook remoto do funcionário.

## 6.2 **Instalação e implementação**

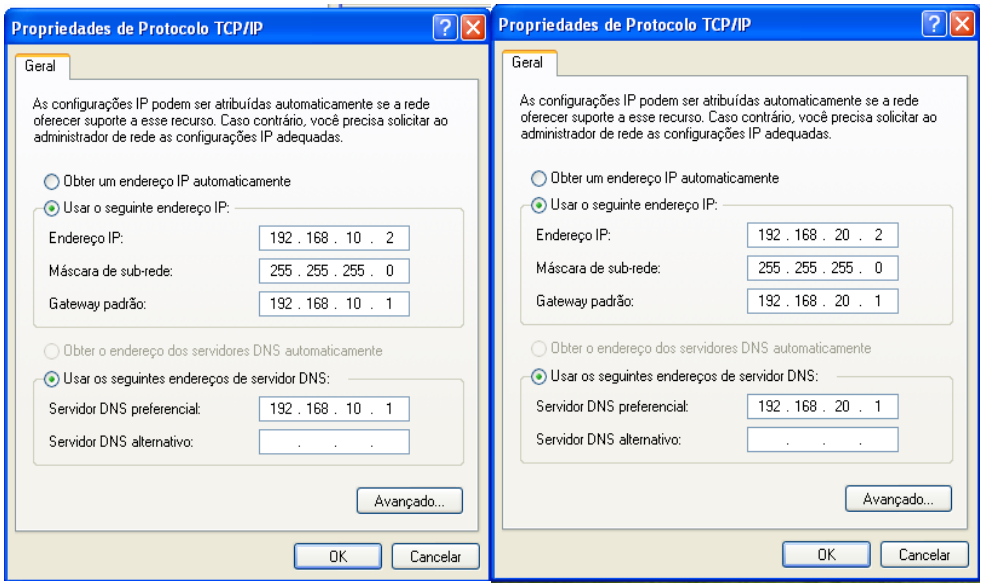
Após a instalação do Sistema Operacional FreeBSD pfSense 2.1 (o que não será comentado aqui devido a não ser o foco do trabalho), é necessário a atribuição dos endereços IPs ao servidor matriz. O pfSense possui uma interface bastante interativa. Primeiro é necessário nomear como WAN: em0 e LAN: em1. Após atribuir a interface em0 o endereço IP fixo da WAN e a interface em1 o endereço IP Fixo da LAN, faremos igualmente na Máquina Virtual da Filial. Após isso serão configurados ambas as estações, tanto da Matriz, como da filial, com seus endereços IPs Fixos. Na Figura 19, encontra-se uma foto da tela interativa inicial pfSense 2.1. Na Figura 20, os IPs configurados nas máquinas locais da matriz e da filial.

**Figura 19 - Interface Interativa do pfSense 2.1 da matriz**




**Fonte: Próprio Autor**

**Figura 20 - Configuração IP Estação Matriz (esquerda) e IP Estação Filial (direita).**




**Fonte: Próprio Autor**

O pfSense possui uma Interface Web para acessar suas configurações, bem como todos os recursos de redes, *firewall*, VPNs, *logs*, entre outros. Devido a ele não possuir uma interface gráfica de acesso, será necessário configurar diretamente da máquina virtual da Estação da Matriz pelo navegador

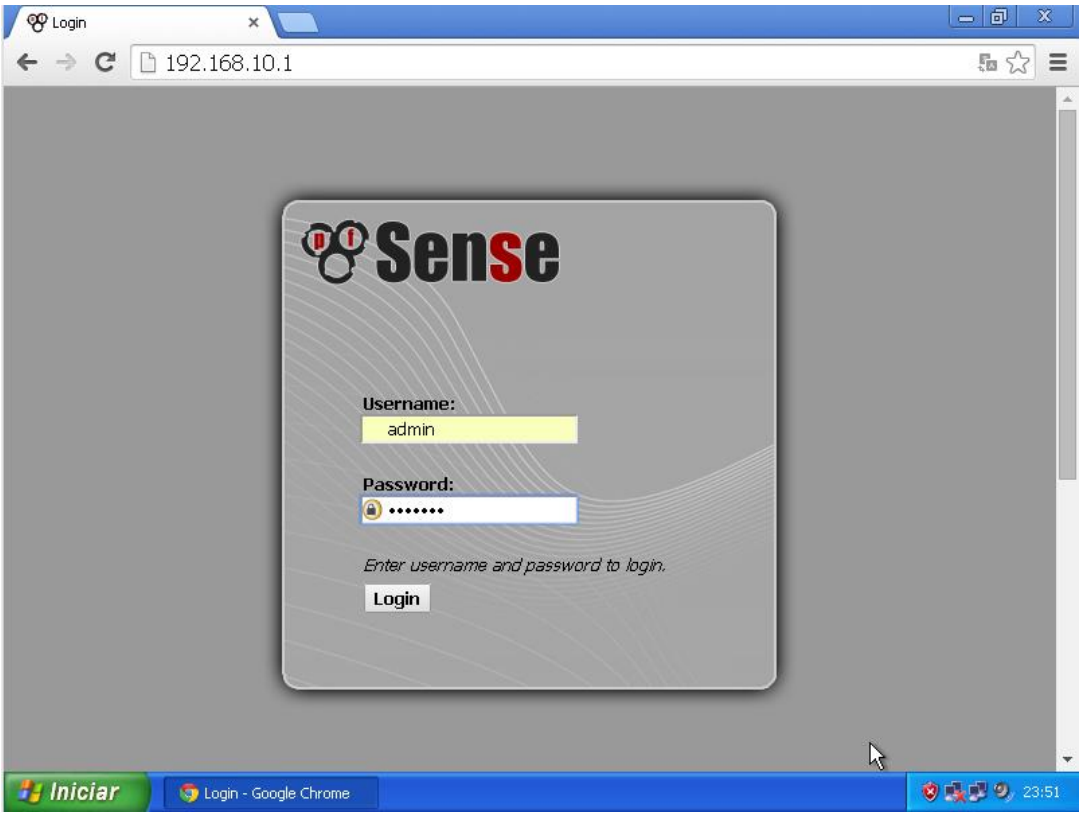
## 6.3 Configuração do OpenVPN

Conectado com um usuário padrão com direitos administrativos necessários, vamos abrir o navegador Chrome (devido a ser mais recente e seguro que o Internet Explorer 6 que vem instalado nativamente no Windows XP) e digitar o IP do servidor da Matriz na barra de endereços.

### 6.3.1 Cenário 1 – Ponto a Ponto

Lembrando que por padrão, o usuário (*username*) padrão é “admin” e a senha (*password*) padrão é “pfsense”. Segue exemplo Figura 21.

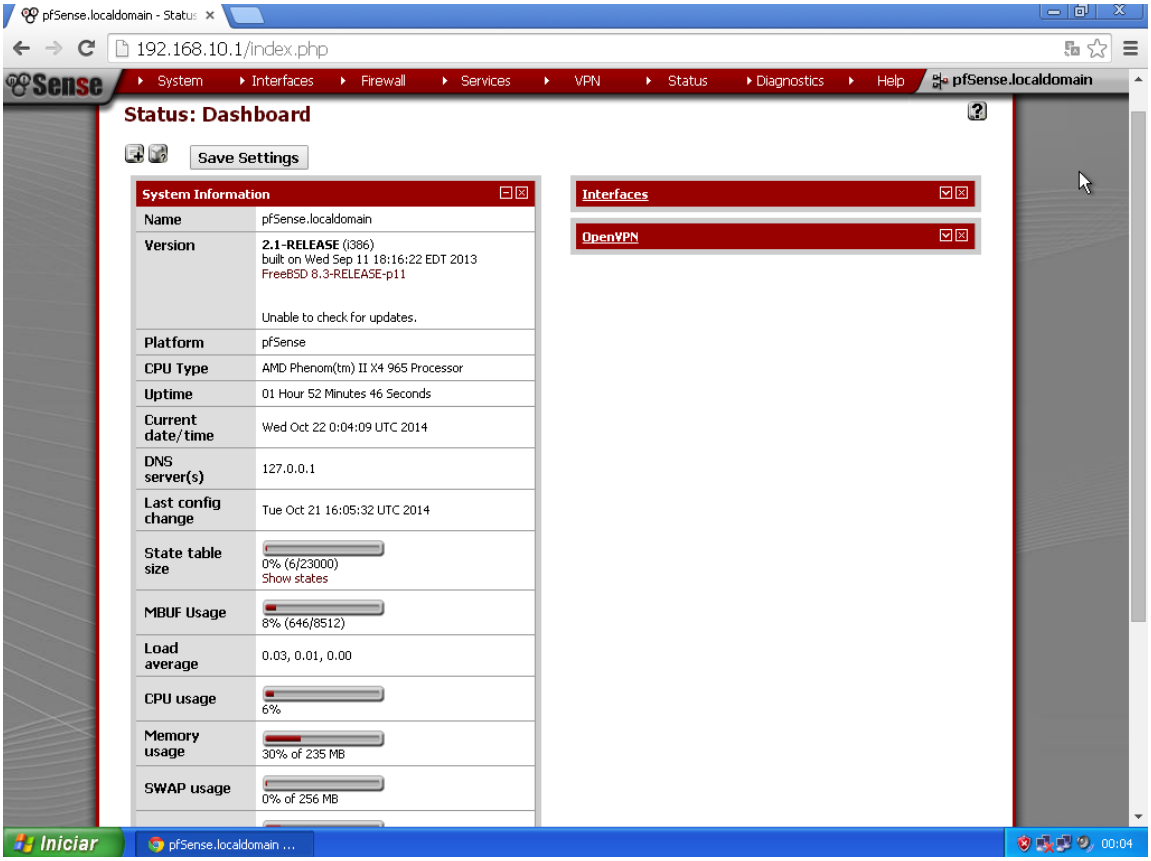
**Figura 21 – Tela de login para a interface navegador do pfSense**




**Fonte: Próprio Autor**

Após o *login*, a interface principal do pfSense será mostrada, como na Figura 22.

**Figura 22 – Interface principal do pfSense**

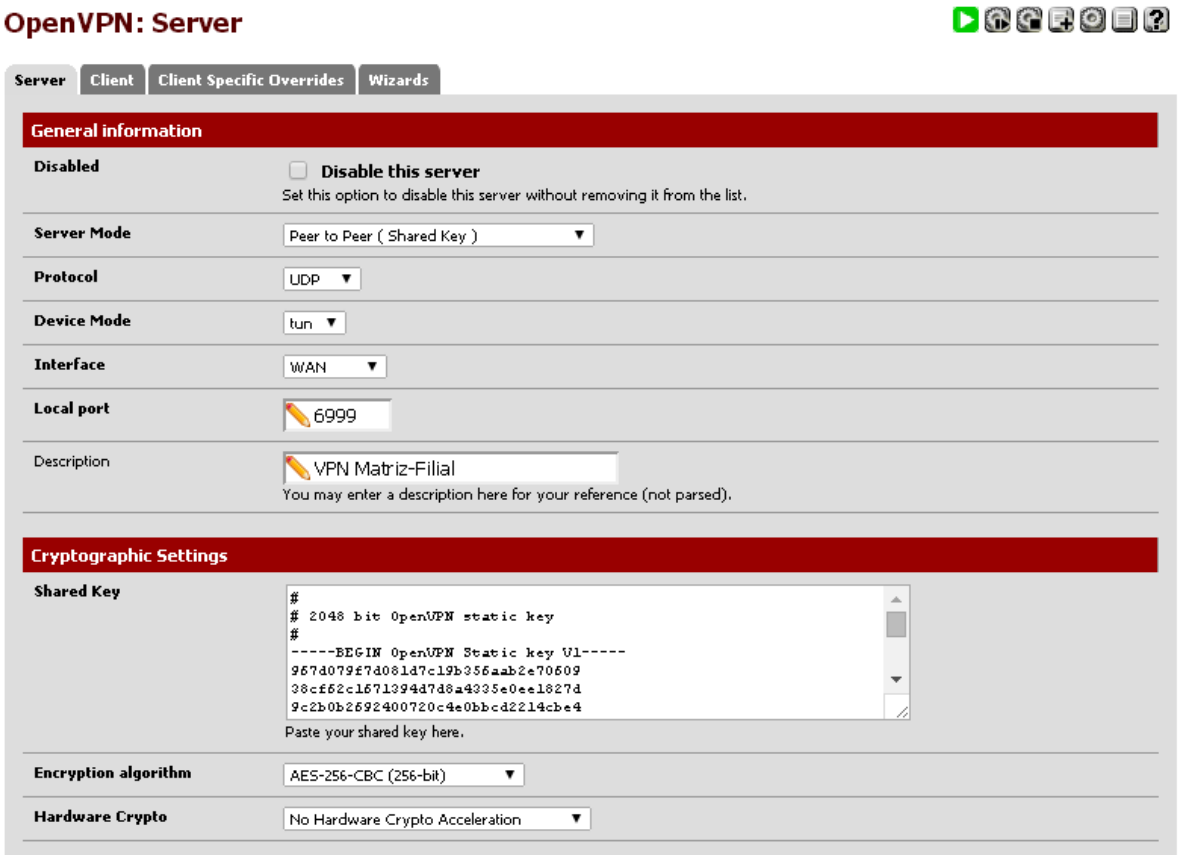



**Fonte: Próprio Autor**

Proximo passo é ir no menu Interfaces e em seguida clicar em LAN. As configurações dos IPs estarão definidas igual ao do servidor. Se não estiverem, altere ou verifique porque do erro.

Após este procedimento, é necessário voltar ao menu principal para então ser configurado a VPN. Apenas clique no ícone pfSense do lado superior esquerdo. Procurar o menu VPN e clicar em OpenVPN. Depois clicar na aba *server* – *add server*.

**Figura 23 – Tela de configuração menu OpenVPN – aba Server**



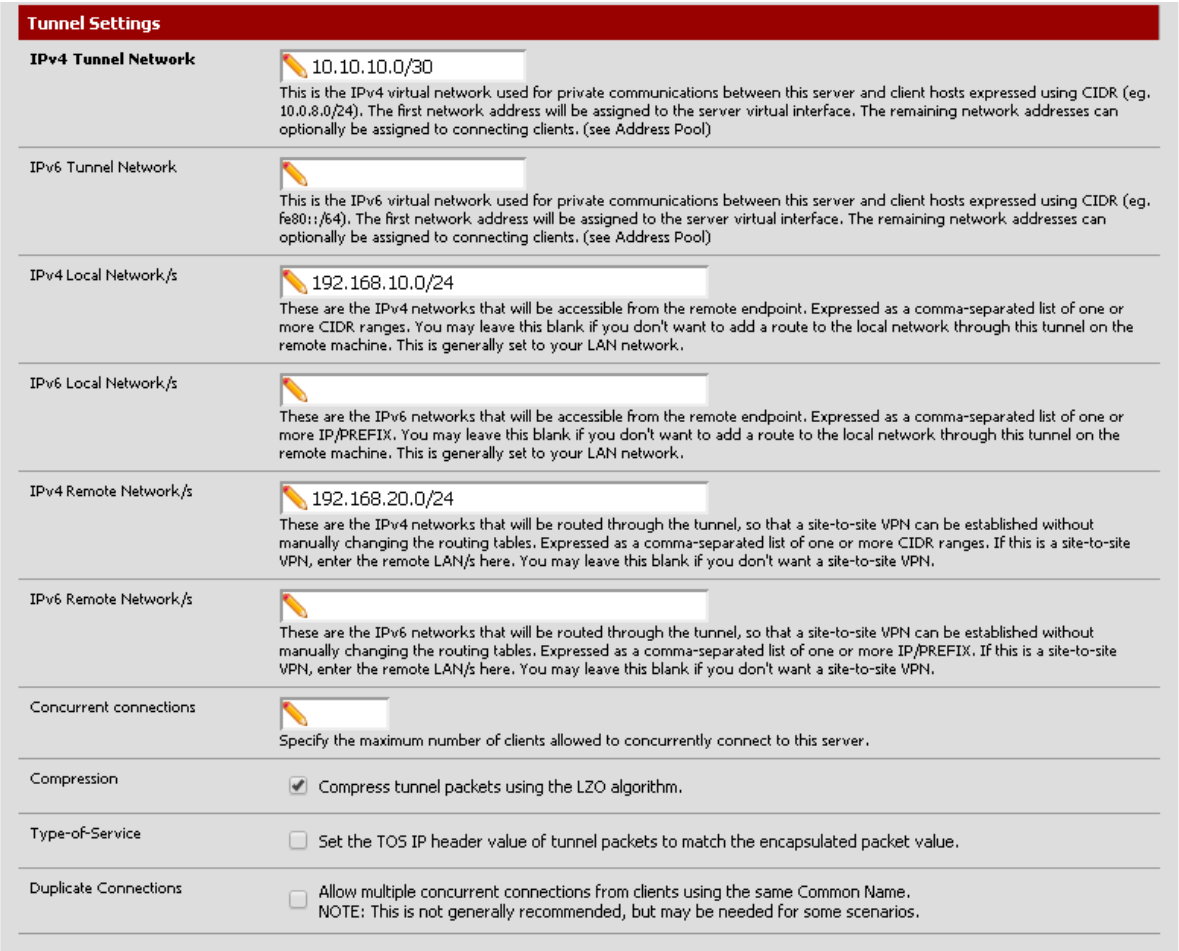

**Fonte: Próprio Autor**

Será aberta uma nova página, como mostra Figura 23. Para configuração foi usado em *Server Mode*, o modelo *Peer to Peer* (Ponto a Ponto), o protocolo UDP por ser mais rápido, modo de tunelamento (tun), utilizando a interface WAN para a ligação, que é a de Internet, a porta 6999 (padrão é 1194), a chave que será compartilhada entre as pontas do túnel é a *Static Key* de 2048 bits. Ela é gerada automaticamente ou pode ser alterada por outra modificando o mesmo campo chamado *Shared Key*. A criptografia utilizada no túnel será a AES-256-CBC (256-bit). Muito segura. *Hardware Crypto* não será necessário alterar.

Segundo Morimoto, (2008): “A diferença entre o modo de tunelamento tun e o tap é que no tun o tráfego da rede é roteado (o que elimina os pacotes de broadcast), enquanto no tap tudo é transmitido, incluindo pacotes de broadcast e pacotes de outros protocolos de rede (como o IPX/SPX).”

Ainda no mesmo menu OpenVPN, como na Figura 24, em *Tunnel settings,* aparece a rede do túnel IPv4 que será utilizada no túnel: 10.10.10.0/30, depois a rede IPv4 local da LAN e também a rede IPv4 da LAN que esta rede irá se comunicar, que seria a rede da Filial. Em *Compression,* será utilizada o algoritmo LZO para compressão de pacotes. Ele comprime blocos de dados sem perder velocidade. *Concurrent Connections* significa o número de conexões ao mesmo tempo. Em branco é ilimitada.

**Figura 24** - **Tela de configuração menu OpenVPN – aba Server 2**

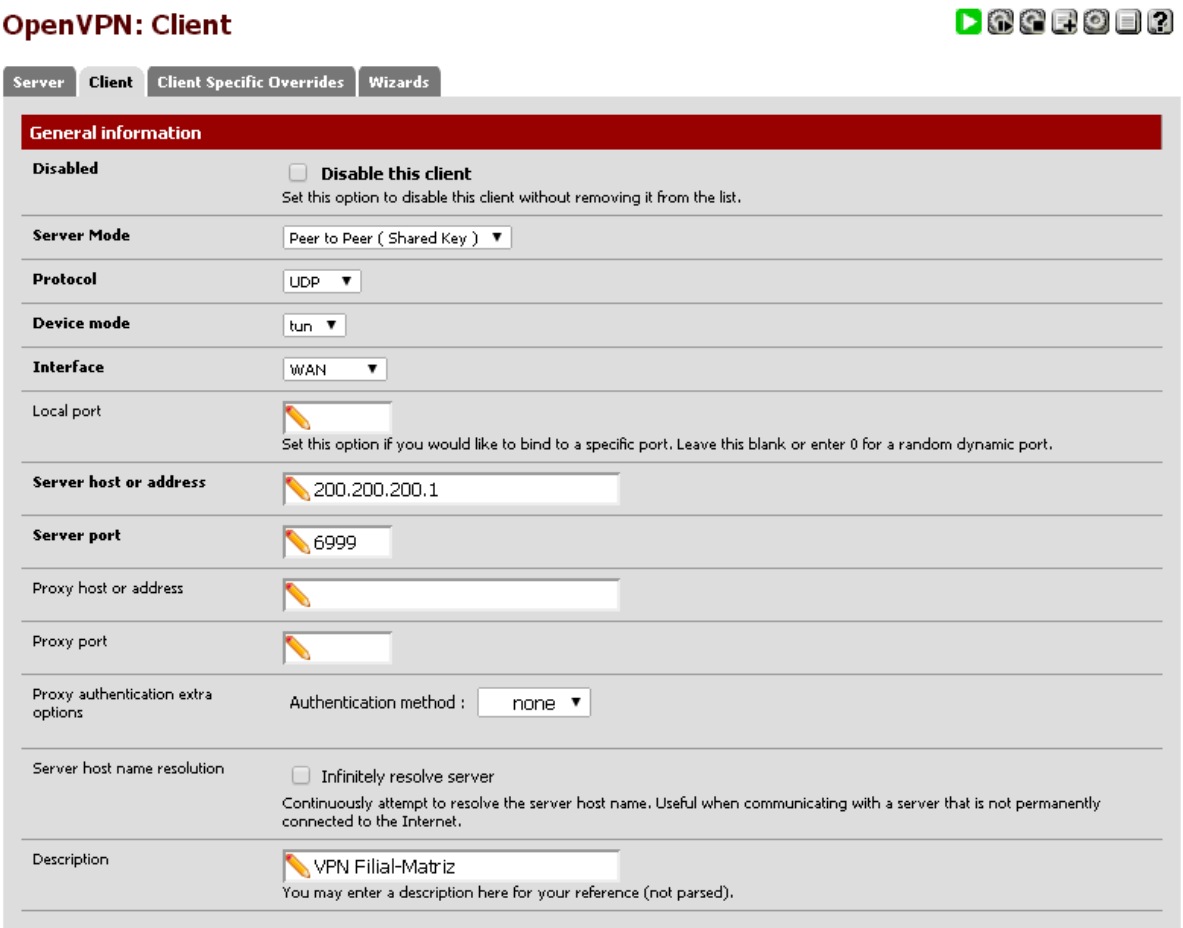



**Fonte: Próprio Autor**

Ao encerrar esse procedimento de configuração do servidor da Matriz, é necessário ir a estação local da filial e acessar via barra de endereços do navegador o IP do servidor da filial (192.168.20.1), e assim seguir o procedimento já descrito para configurar o servidor da Filial. Fazer o *login* padrão conforme a Figura 21. No

menu principal, ir então em VPN - OpenVPN, porém clicar na aba *Client* desta vez. Então, no botão *Add Client*. Exemplo, Figura 25.

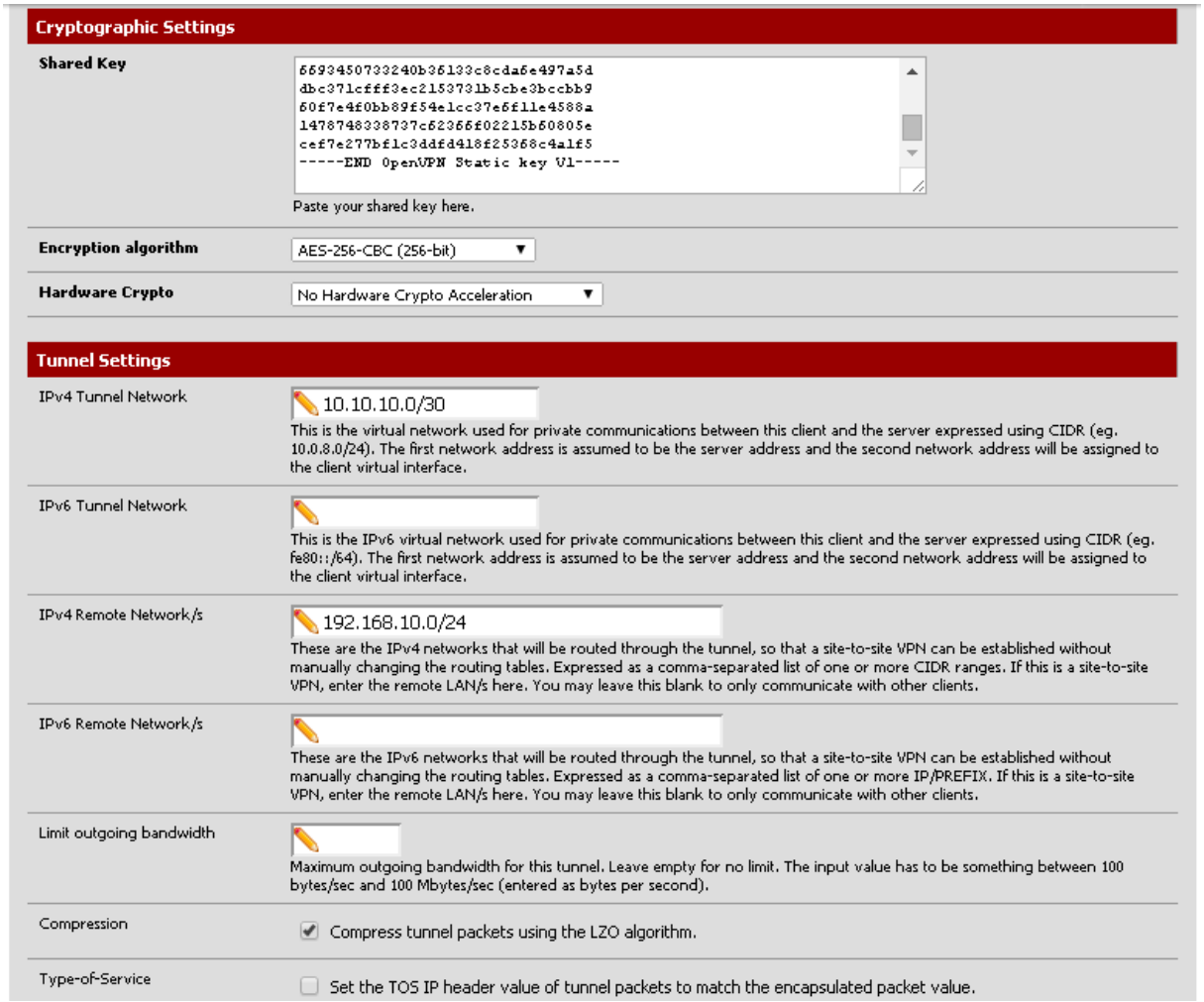
**Figura 25 - Tela de configuração menu OpenVPN – aba Client**




**Fonte: Próprio Autor**

Conforme a Figura 25, os campos iguais precisam ser preenchidos com os mesmos valores do servidor, porém apenas com a mudança do *server host*, que será o endereço IP WAN de origem do servidor da Matriz. Não será utilizado *Proxy*.

**Figura 26 - Tela de configuração menu OpenVPN – aba Client 2**




**Fonte: Próprio Autor**

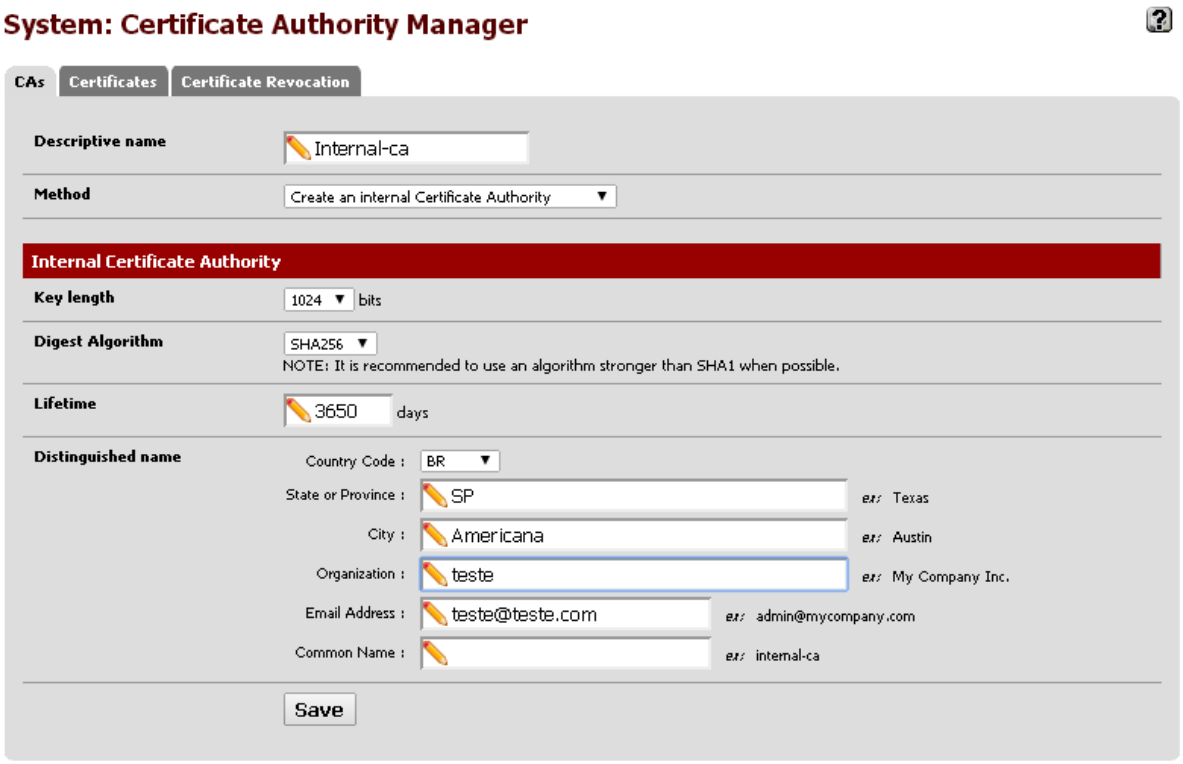
Na Figura 26, a *Static Key* terá que ser copiada igualmente com a do servidor. Por isso utilize um meio seguro para o transporte do mesmo. Recomenda-se salvar em um bloco de notas e transportar por um pen drive, por exemplo. Mesmo esquema de Criptografia AES-256 e mesmo túnel de rede (*Tunnel Network*). Mudança apenas para a rede remota (*Remote Network*), que agora será a do servidor Matriz. Novamente utilizar a compressão com o algoritmo LZO. Sempre lembrar de apertar *Save* para sair em todas as telas.

### 6.3.2 Cenário 2 – Conexão Remota

Utilizando as mesmas configurações da máquina virtual do servidor Matriz e também da estação XP do servidor Matriz e agora acrescentando uma estação remota, vamos seguir com o procedimento da Figura 21 acessando pela estação XP da Matriz. Mesmo IP: 192.168.10.1.

Este é o passo principal de uma conexão remota. A criação dos CA (certificado de autoridade), o qual torna o servidor como uma autoridade certificadora e dos certificados dos clientes da VPN. Vamos no menu *System* e *Cert Manager*. Após *Add or Import ca*. A Figura 27 mostra o que será aberto a seguir.

**Figura 27 – Criação de certificado de autoridade da Matriz**



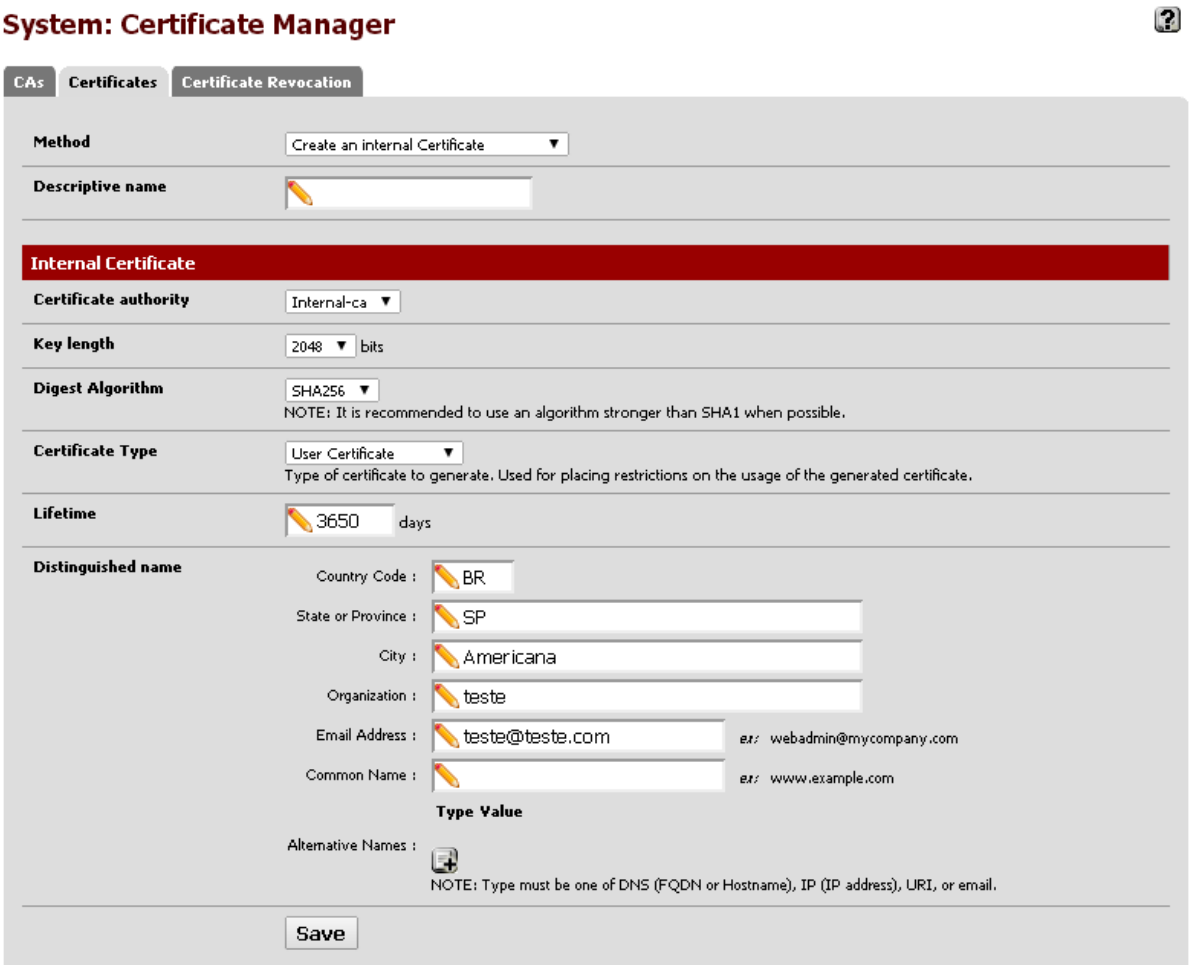

**Fonte: Próprio Autor**

Aqui preenche-se o nome descritivo (*descriptive name*) como uma Internal-ca. O método (*method*) seria uma criação de um novo certificado interno de autoridade.

*Key Lenght* como o número de bits de criptografia desse CA utilizando o algoritmo hash SHA256. Dias de expiração (*Lifetime*) do certificado padrão são 3650 dias ou 10 anos. As outras opções são aleatórias. Devem ser preenchidas com as informações da empresa. Clique *Save* para salvar o que foi digitado.

No mesmo menu, entra-se agora na aba Certificados (*certificates*). Após *Add or import certificates.*

**Figura 28 – Criação de certificado do usuário**

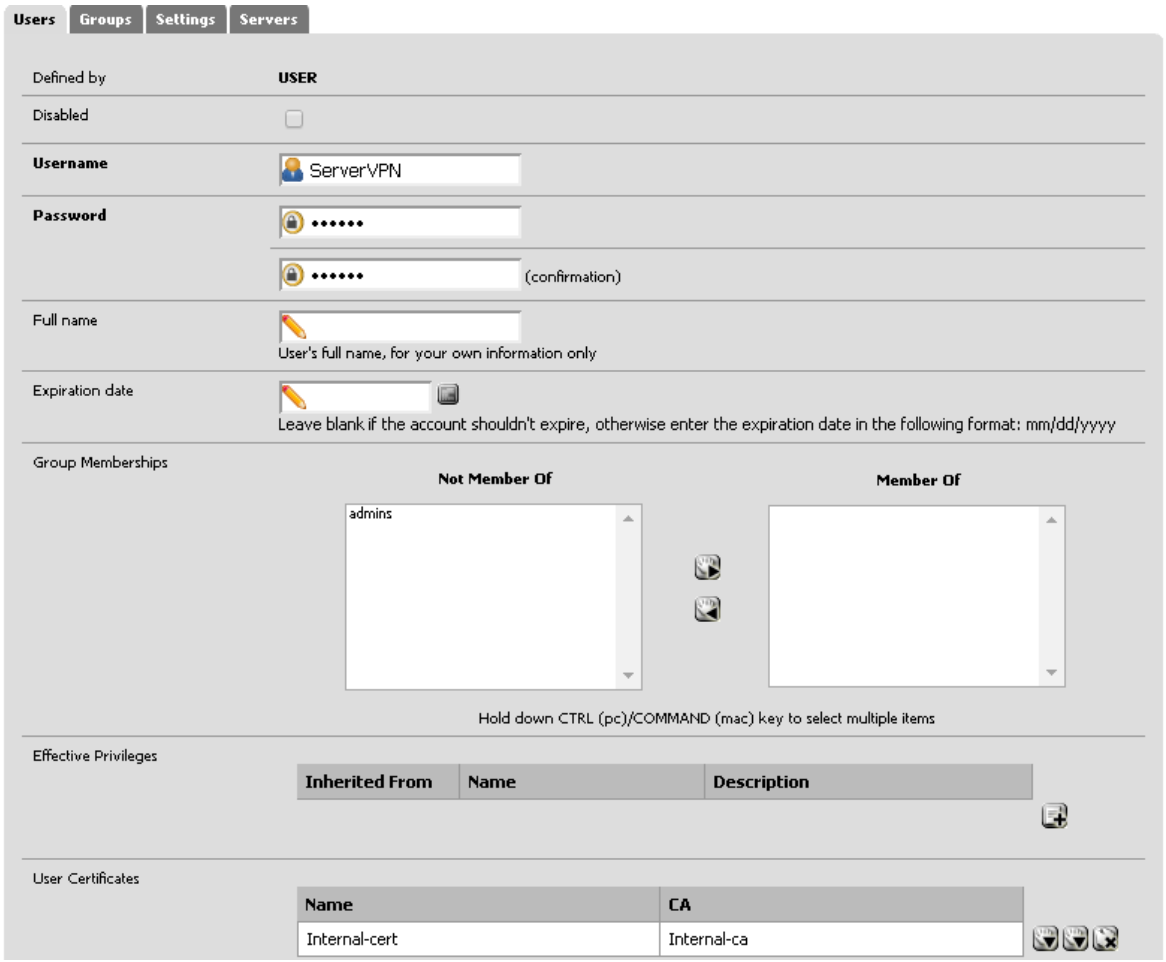



**Fonte: Próprio Autor**

Como mostrado da Figura 28, será criado um novo certificado (*Create an internal certificate*). Automaticamente todos os dados já serão preenchidos devido ao Internal-ca já ter sido configurado. Única mudança será a parte do tipo de certificado (*Certificate Type*), que será definido como certificado de usuário (*User Certificate*).

Neste momento, será criado um usuário para a VPN. Este usuário e sua senha serão requisitados no momento da conexão da estação remota com o servidor da Matriz. Clique no menu *System* e depois *User Manager*. Após *Add User*. Exemplo, Figura 29.

**Figura 29 – Criação de usuário para autenticação e criação do túnel**

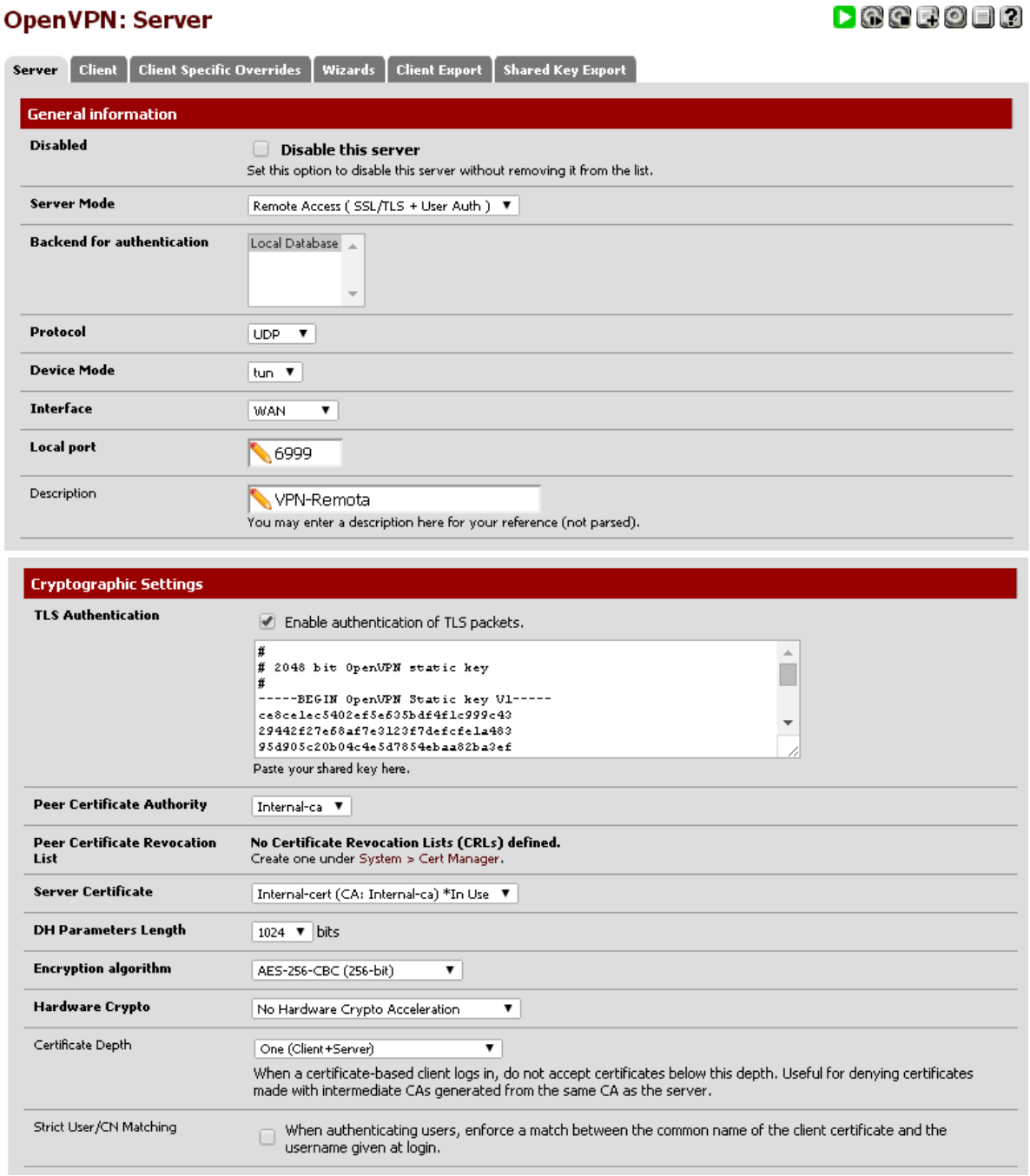



**Fonte: Próprio Autor**

O usuário “ServerVPN” foi criado e a senha “123456” configurada. Note que automaticamente o Internal-cert foi atribuído a este usuário. Se houvesse mais certificados, eles seriam mostrados ou seria necessário importar do lugar aonde estivesse através do botão importar certificados (*Import Certificate*).

Agora para criar a conexão OpenVPN, é necessário ir ai menu VPN – OpenVPN - add server.

**Figura 30 – Criação da conexão VPN remota**



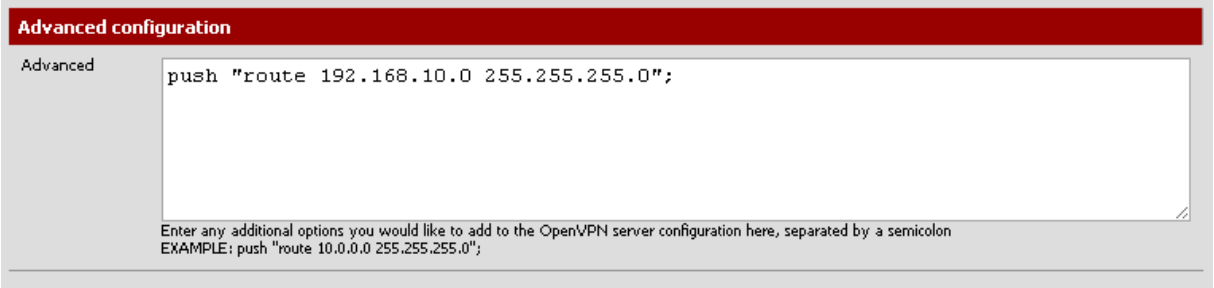

**Fonte: Próprio Autor**

Igual a Figura 30, em *server mode*, será definido como *Remote Access*, utilizando SSL/TLS e um certificado do usuário. Definição do certificado *Internal-ca*.

Detalhe para o algoritmo DH (*Diffie Hellman*) e também para o certificado do servidor (*Server Certificate*) definido como o certificado já criado *Internal-cert*. As demais configurações iguais a Figura 23.

Em IPv4 Tunnel Network ficará a rede do túnel 10.10.10.0/24. E em IPv4 Local Network a rede local 192.168.10.0/24. Compressão com LZO ativado.

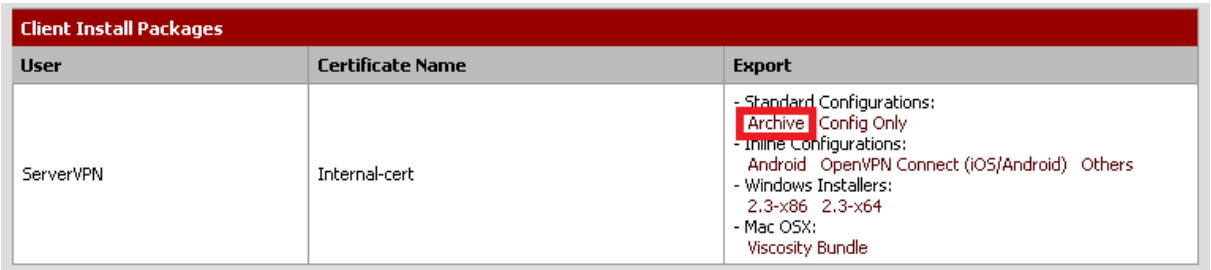
**Figura 31 – Definição das rotas entre as redes diferentes**




**Fonte: Próprio Autor**

Por fim, a rota da conexão VPN definida, para acesso a rede interna 10.10.10.0/24. Deve ser preenchida exatamente como a Figura 31. A VPN agora já está configurada. Só é preciso exportar o certificado para a máquina Windows XP remota. Para isso utiliza-se um recurso do próprio pfSense. Ainda no menu VPN – OpenVPN, vai-se na aba *Client Export*. Após abrir, localizar *Client Install Packpages* e em *Stardard Configurations*, clique em *Archive*, conforme Figura 32.

**Figura 32 – Processo de salvar os certificados e configurações para repassar a outro dispositivo**




**Fonte: Próprio Autor**

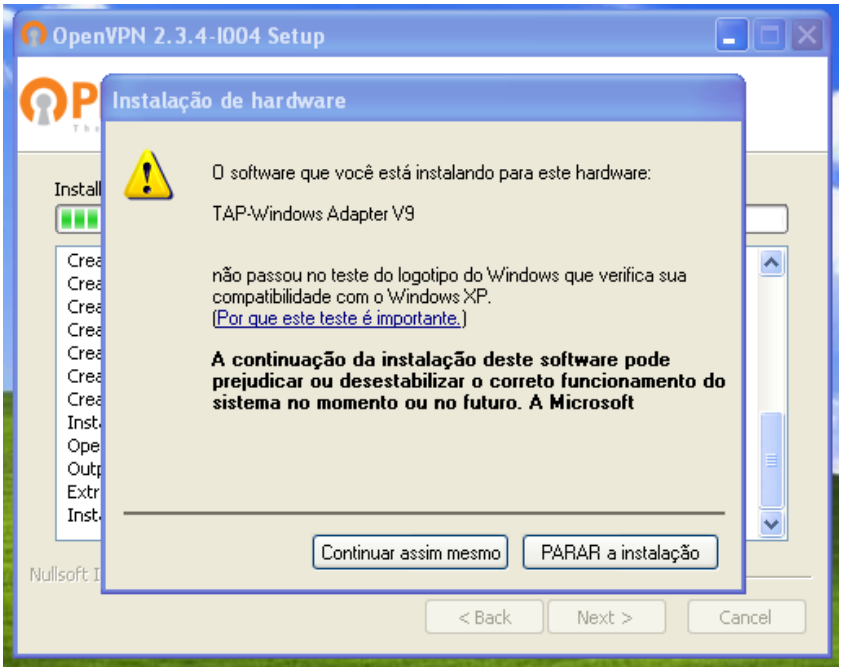
Após isso, só copiar o arquivo zipado com o nome pfSense-udp-6999-ServerVPN e colocar em um meio seguro para poder depois passar e extrair na máquina remota.

### 6.3.3 Instalando e configurando Cliente OpenVPN no Windows XP

Como o servidor já foi configurado, existe um cliente para Windows que apenas precisa ser instalado na máquina remota como um software executável. Ele se encontra no site oficial do OpenVPN[4]. A versão baixada foi a 2.3.4, a mais recente.

1- Após o *download* da aplicação, execute-a;
2- Irá abrir uma janela e apenas é necessário clicar no botão "*Next*";
3- Na próxima janela, clique no botão "*I agree*" para aceitar os termos de utilização do software;
4- Pode marcar todas as opções e clicar "Next" novamente;
5- Após isso, clique em "*Install*" e aguarde o final da instalação. É para aparecer um aviso de *driver* incompatível, conforme exemplificado na Figura 33. Clique no botão "Continuar assim mesmo";
6-Depois só desmarcar a opção "*Show Readme*", clicar em "*Finish*" e o cliente OpenVPN estará instalado.

**Figura 33 - Instalação do driver TAP-Win32**

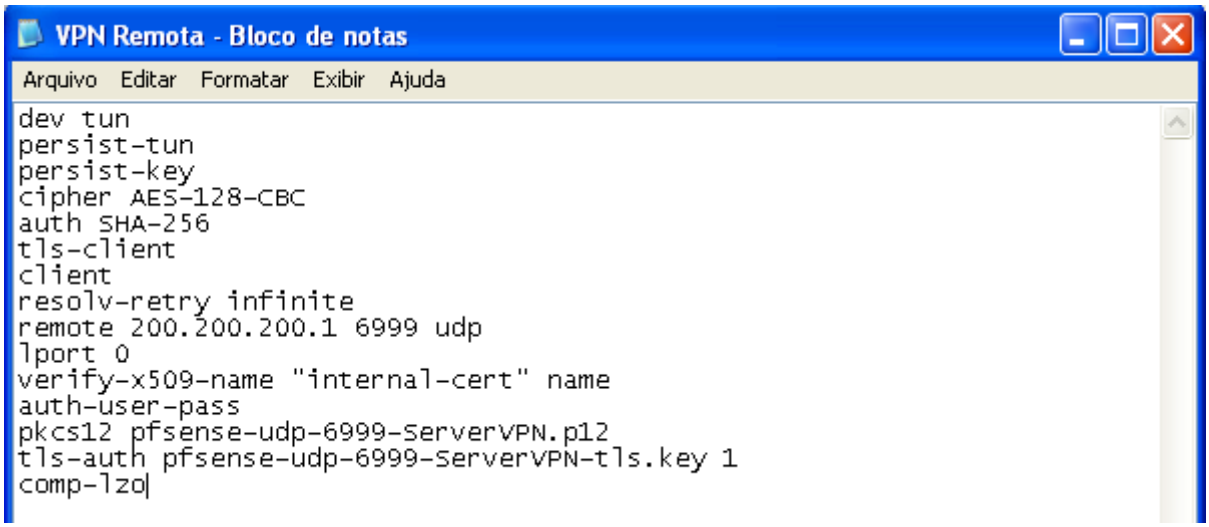



**Fonte: Próprio Autor**

[4] Disponível em: https://openvpn.net/index.php/download/community-downloads.html. Acessado em: 15 abr. 2014.

Após a instalação do cliente, é necessário configurar a conexão para correto funcionamento. Primeiramente, extraia os arquivos do pfsense-udp-6999-ServerVPN.zip dentro do diretório C:\Arquivos de programas\OpenVPN\config. Os arquivos extraídos são: um certificado de autoridade, pfsense-udp-6999-ServerVPN.key (chave do servidor), certificado do cliente pfsense-udp-6999-ServerVPN.crt e também as configurações da conexão OpenVPN, armazenados no arquivo com a extensão .ovpn. Para verificar as configurações do cliente, deve-se abrir o bloco de notas indo em Iniciar > Executar e digitando *notepad*. Clique em OK. Uma nova janela do Bloco de Notas do Windows vai se abrir. A partir disso, Arquivo – abrir e selecione o arquivo .ovpn. O arquivo aberto será igual a Figura 34.

**Figura 34 – Detalhes do arquivo de configuração .ovpn**




**Fonte: Próprio Autor**

## 6.4 **Teste de Segurança**

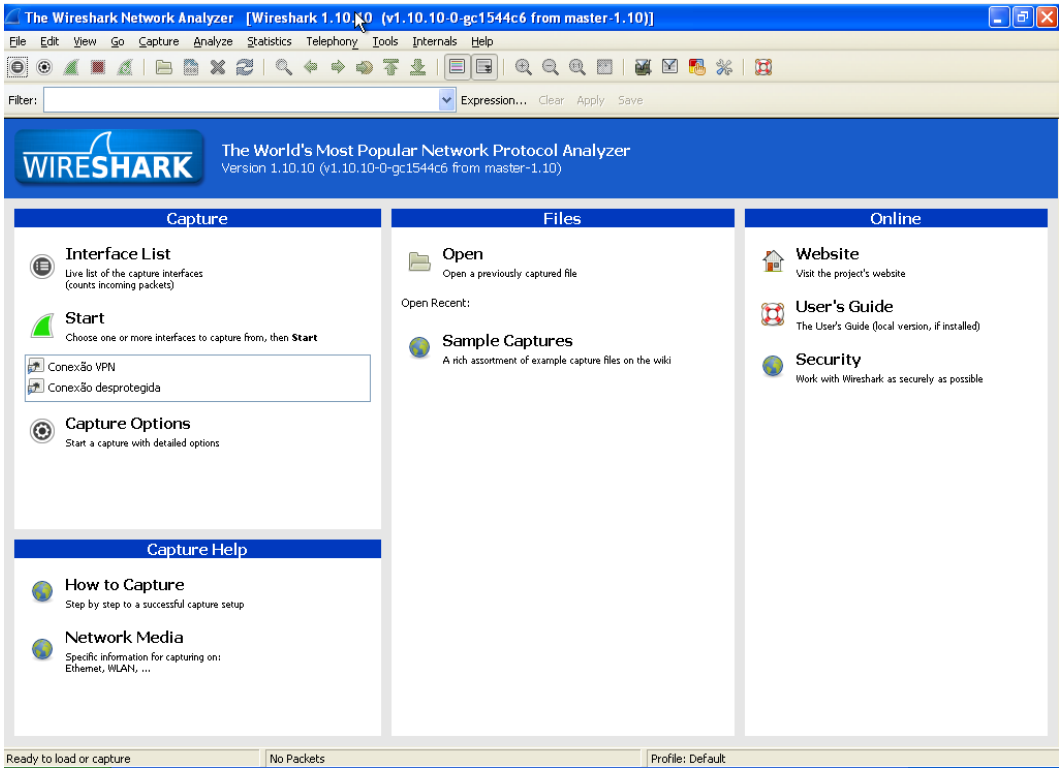
Abaixo os dois principais modos de conexão VPN e seus devidos testes efetuados. O primeiro através de uma conexão FTP (*File Transfer Protocol*), protocolo usado para transferir dados e considerado inseguro, mostrando uma autenticação entre o servidor e cliente. O segundo teste, com o protocolo de rede Telnet, que é um comunicador em texto de dados interativo baseado no TCP. O terceiro teste utilizando o Servidor Web Apache, juntamente com o monitor que gráfico de redes, Cacti. O quarto teste com uma versão ponto a ponto de conexão via FTP também. Todos os testes utilizaram como princípios de segurança a

autenticação nos serviços. Lembrando que a maioria dos testes foi executado pelo cenário Acesso Remoto, devido a ser possível a amostragem com e sem a conexão VPN estar ativa, diferentemente do cenário ponto a ponto que já inicia o S.O. com a conexão criptografada, porém o princípio de segurança é o mesmo.

### 6.4.1 Conexão Remota - FTP

Para verificação e garantia da integridade e confidencialidade de todos os arquivos que serão transportados e acessados pela Conexão VPN, será feito um teste com o software de *sniffer* Wireshark v.1.10.106[5] para ver se ele captura os pacotes trafegando pela rede no momento de uma autenticação de um servidor FTP. O teste será feito pela máquina Windows XP de conexão remota, encontrada fora da rede. Primeiro foi criado um servidor FTP padrão do Windows na máquina Windows XP local da matriz, que está localizada dentro da rede da matriz. A Figura 35 mostra como é a interface principal do Wireshark.

**Figura 35 – Interface principal Wireshark**

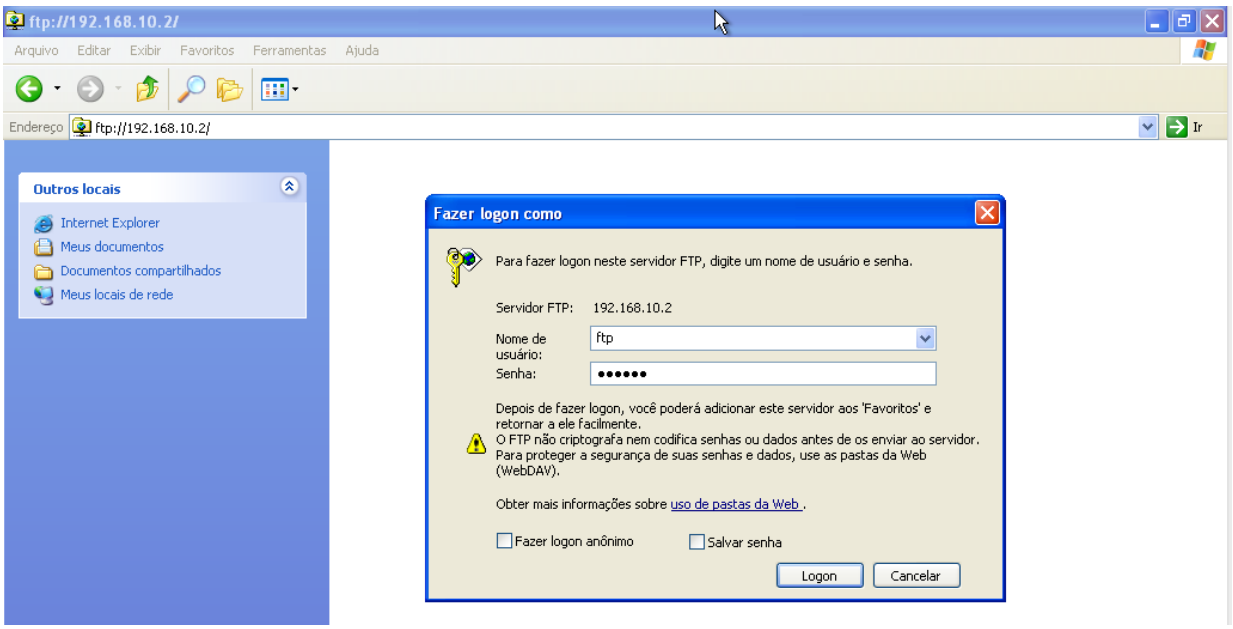



**Fonte: Próprio Autor**

[5] Disponível em: https://www.wireshark.org/download.html. Acessado em: 23 set. 2014.

Primeiro será demonstrado sem o túnel VPN aberto. Vamos selecionar a conexão desprotegida (Conexão Local padrão) e clicar em *Start a new live capture*. Os dados passarão a ser capturados. Iremos agora nos conectar via FTP. Abra o meu computador e digite o IP da estação Windows XP da rede do servidor Matriz. Após botão direito em qualquer parte branca da janela e fazer logon como. Digite no nome de usuário “FTP” e senha “123456”, conforme Figura 36. Clique em *Logon* depois.

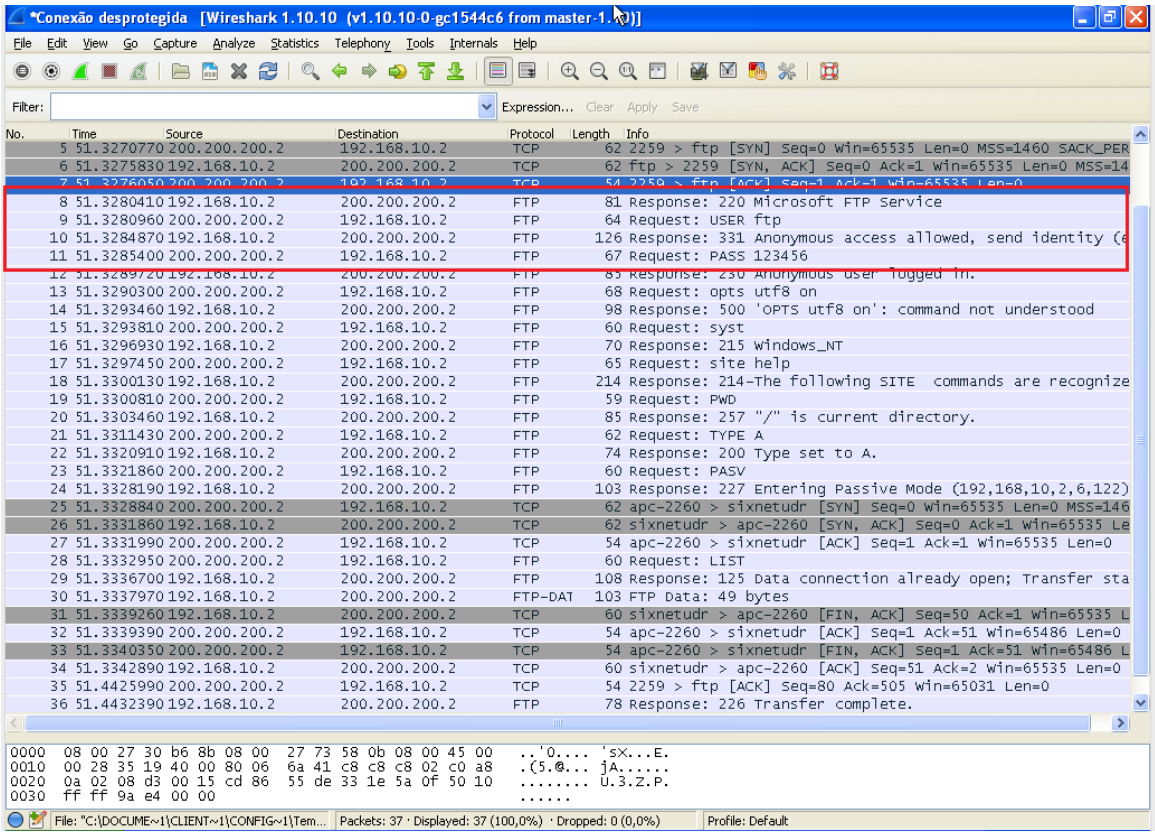
**Figura 36 – Logon no servidor FTP vindo da máquina remota**




**Fonte: Próprio Autor**

Como é mostrado na Figura 37, os pacotes de autenticação foram capturados e mostrados pelo *sniffer*. Tanto a senha, como o usuário, além do IP de origem e destino.

**Figura 37 – Momento de captura dos pacotes descriptografados pelo Wireshark**




**Fonte: Próprio Autor**

Após esse passo, é necessário abrir o *software* cliente VPN através do ícone criado na área de trabalho com o nome OpenVPN GUI. Um novo ícone aparecerá na barra de tarefas semelhante a uma conexão local. Apenas clique com o botão direito e conectar seguindo o exemplo da Figura 38.

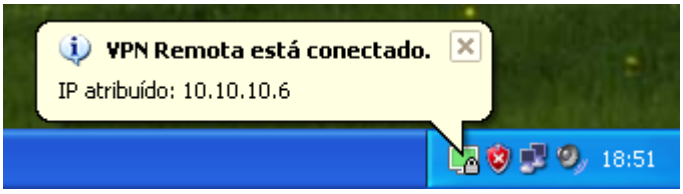
**Figura 38 – Exemplo de como se conectar**


**Fonte: Próprio Autor**

Ao clicar em conectar, uma janela com configurações detalhada da conexão se abrirá, porém será pedido uma autenticação. Digite “ServerVPN” para usuário e

senha “123456”. Se tudo estiver certo, o resultado será conforme a Figura 39 a seguir. Um túnel será criado na rede 10.10.10.0/24 entre os dispositivos.

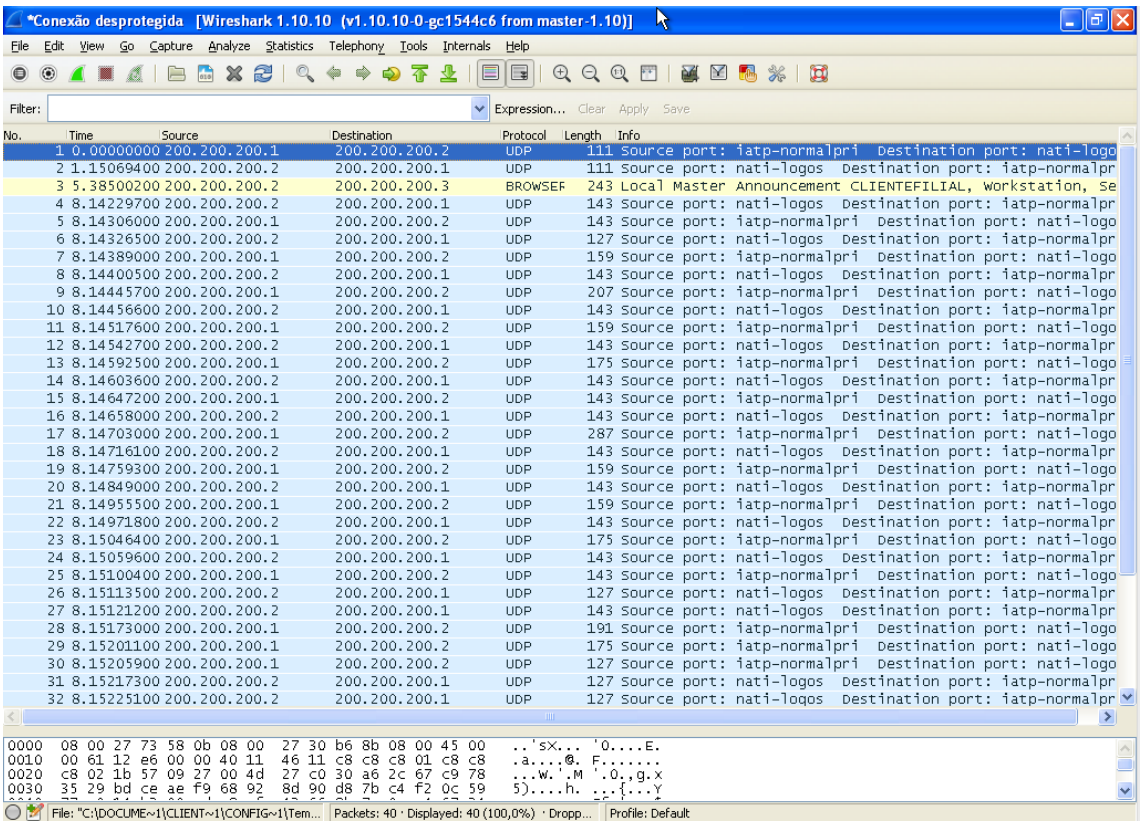
**Figura 39 - OpenVPN Conectado**




**Fonte: Próprio Autor**

Agora, ligando-se a conexão VPN selecionando a conexão desprotegida (Conexão Local) novamente e fizermos a mesma coisa.

**Figura 40 - Momento de captura dos pacotes criptografados pelo Wireshark**



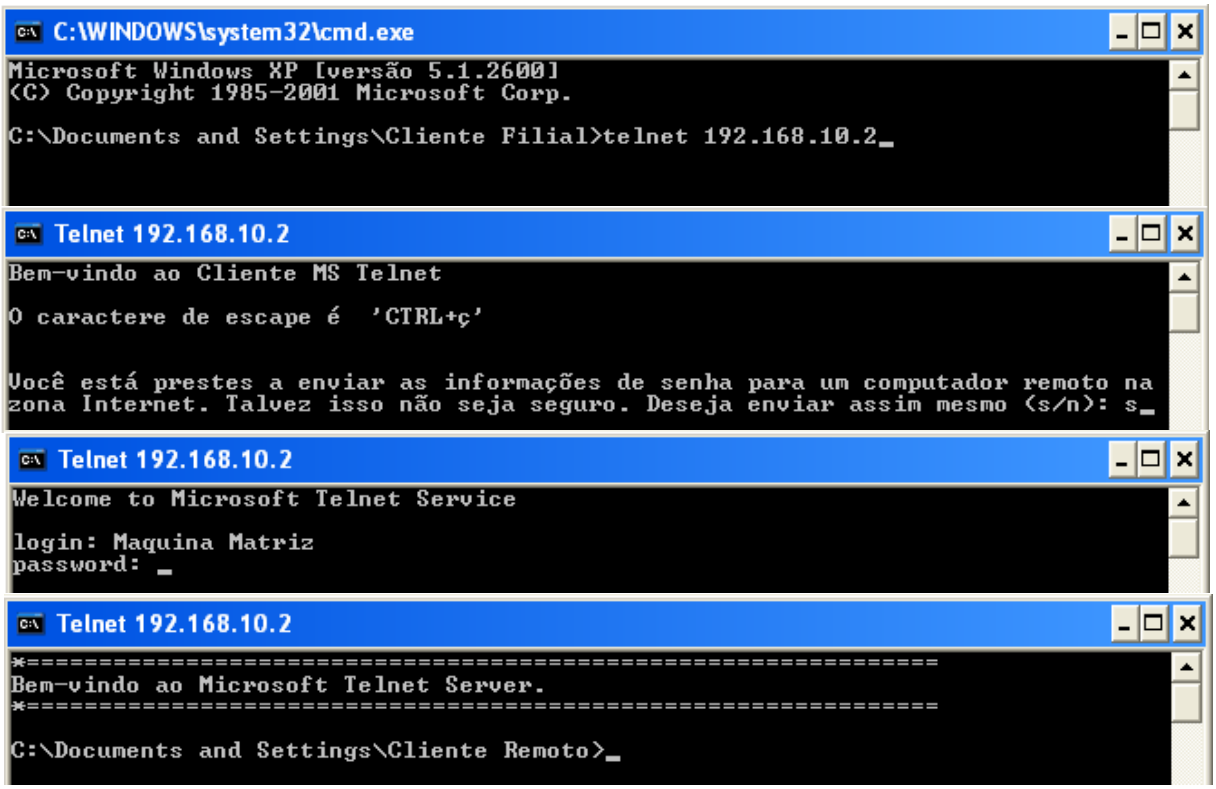

**Fonte: Próprio Autor**

Segundo a Figura 40, agora nenhum pacote é sequer identificado. Nem a máquina origem da estação da Matriz e nem a destino remota.

### 6.4.2 Conexão Remota – Telnet

Neste teste, será efetuada uma autenticação utilizando o protocolo Telnet entre a máquina da matriz e a máquina remota. Na máquina Windows XP remota (fora da rede), será aberto o programa Wireshark semelhantemente a Figura 35, então selecionar a conexão desprotegida (sem VPN habilitada), clicar em *Start new live capture* e abrir o Prompt de Comando do Windows XP, em Iniciar – Todos os programas – Acessórios. Após, digitar o comando, conforme o primeiro passo da Figura 41. Relembrando que o IP que vamos acessar é o da máquina local da Matriz, que possui o IP Definido como 192.168.10.2.

**Figura 41 – Passo a passo da digitação no Prompt de comando**

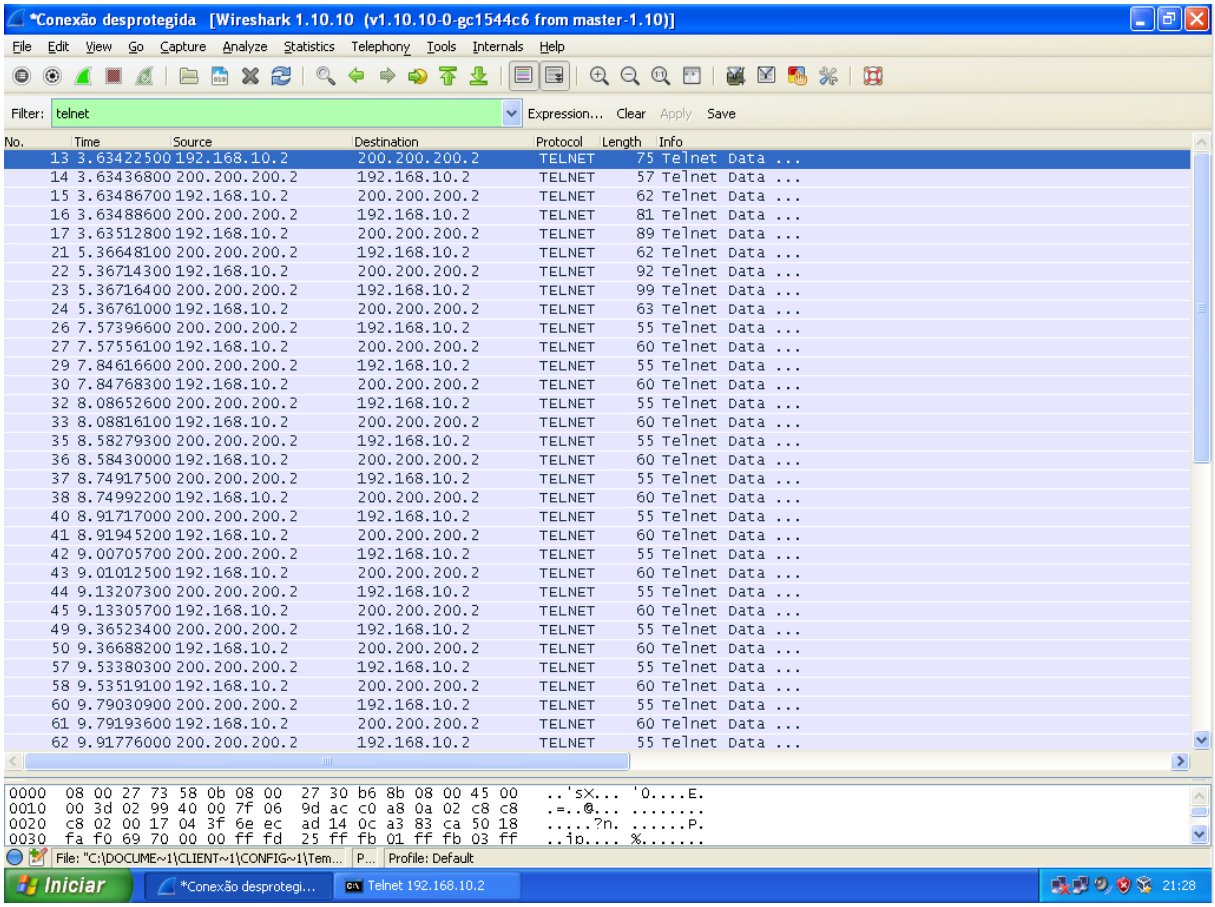



**Fonte: Próprio Autor**

Uma confirmação de insegurança é apresentada pelo Windows. Coloque sim (s). O usuário (*login*) da Máquina Matriz era “Máquina Matriz” mesmo e a senha (*password*) era “123456”. A senha encontra-se oculta devido a ser camuflada pelo Prompt ao ser digitada. Assim obtem-se acesso a um computador remoto.

Após esses passos, será preciso abrir novamente o *software* Wireshark e parar o monitoramento. O resultado após este processo se encontra logo a seguir, na figura 42.

**Figura 42 - Momento de captura dos pacotes Telnet descriptografados**

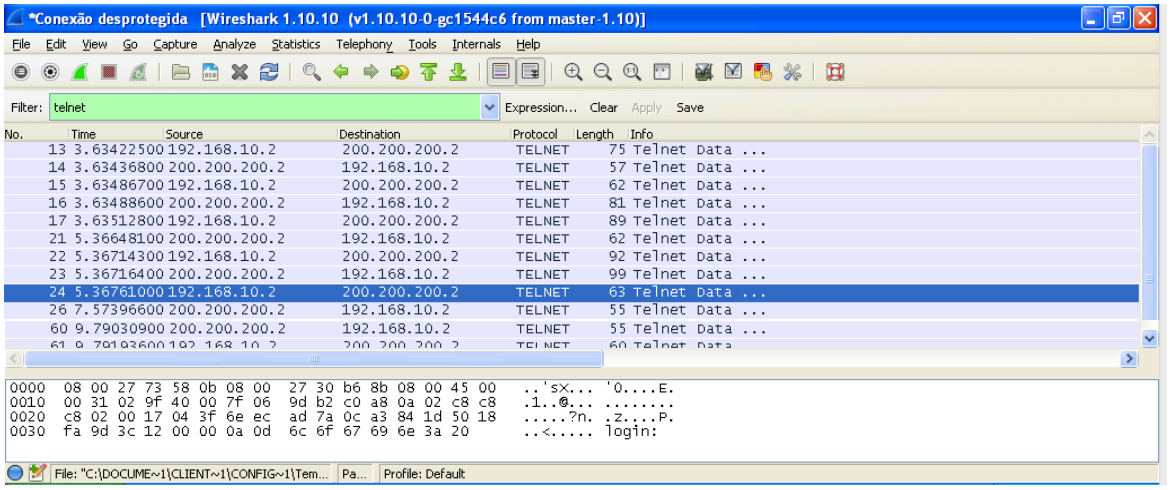



**Fonte: Próprio Autor**

Em *Filter* (filtro de protocolos do Wireshark), coloca-se somente o protocolo Telnet. Vê-se que todos os pacotes trocados entre as máquinas foram capturados.

A partir do pacote 24 da análise, percebe-se que em seu conteúdo, foi capturado o "*login*:", conforme Figura 43. Lembrando que apenas é analisado os pacotes com *destination* (destino) ao IP remoto 192.168.10.2.

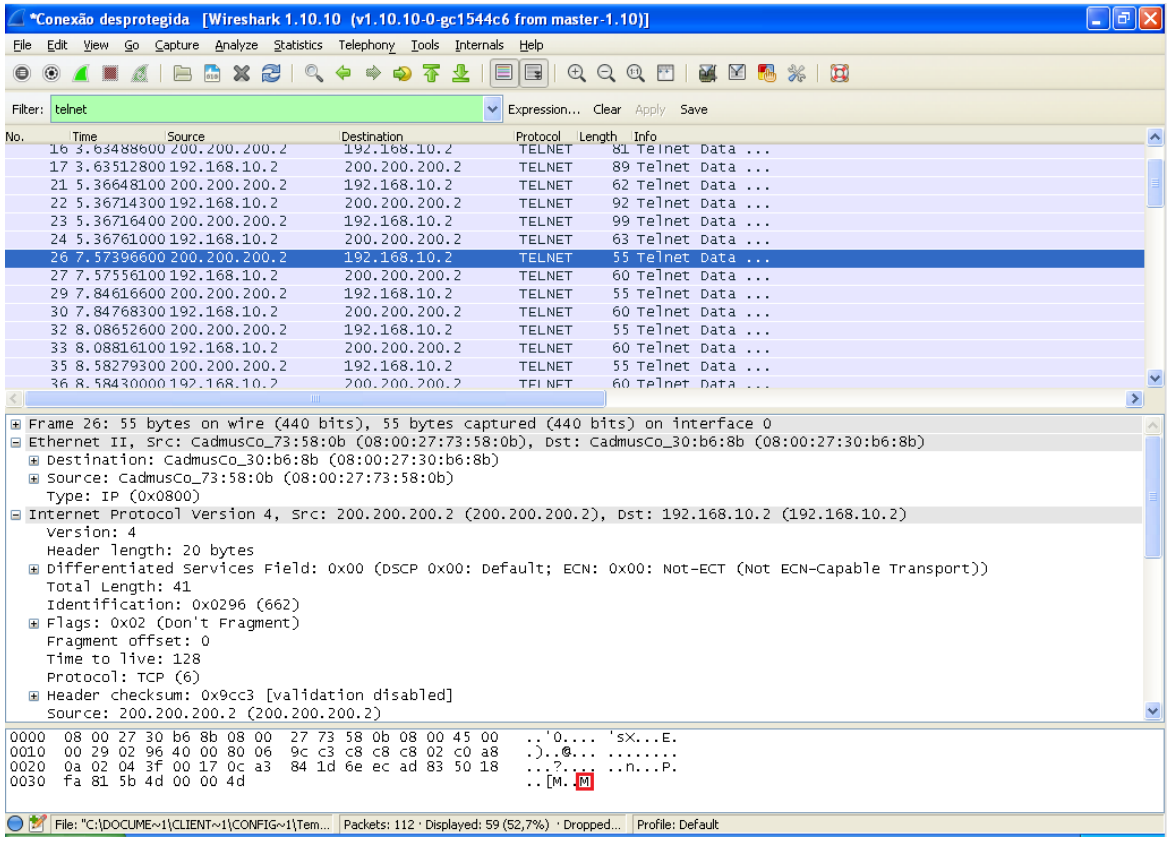
**Figura 43 – Detalhes da captura do Wireshark capturando o protocolo Telnet**




**Fonte: Próprio Autor**

Localiza-se agora o próximo pacote 26, nota-se que o caractere “M” foi capturado, conforme Figura 44.

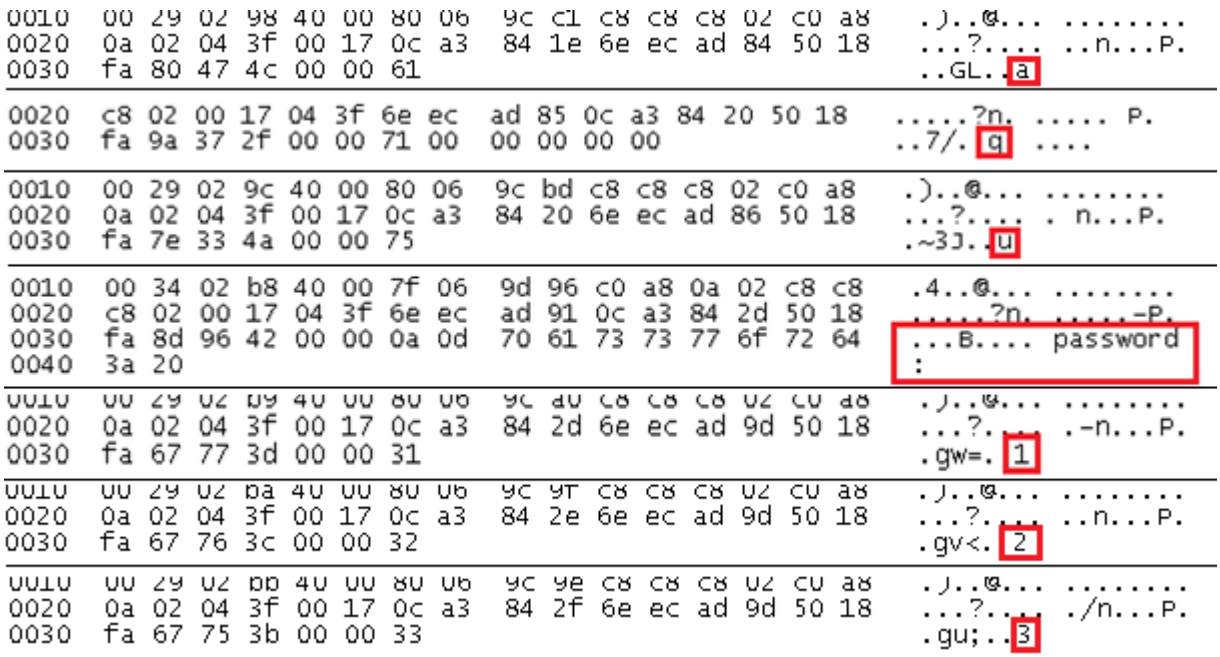
**Figura 44 – Captura do primeiro caractere do login**




**Fonte: Próprio Autor**

Ao selecionarmos o pacote 29, o caractere “a“ foi capturado. Ao irmos pro pacote 30, ele captura o “q” e assim por diante, como mostrado na Figura 45.

**Figura 45 – Abreviação de captura de pacotes mostrando caracteres descobertos**

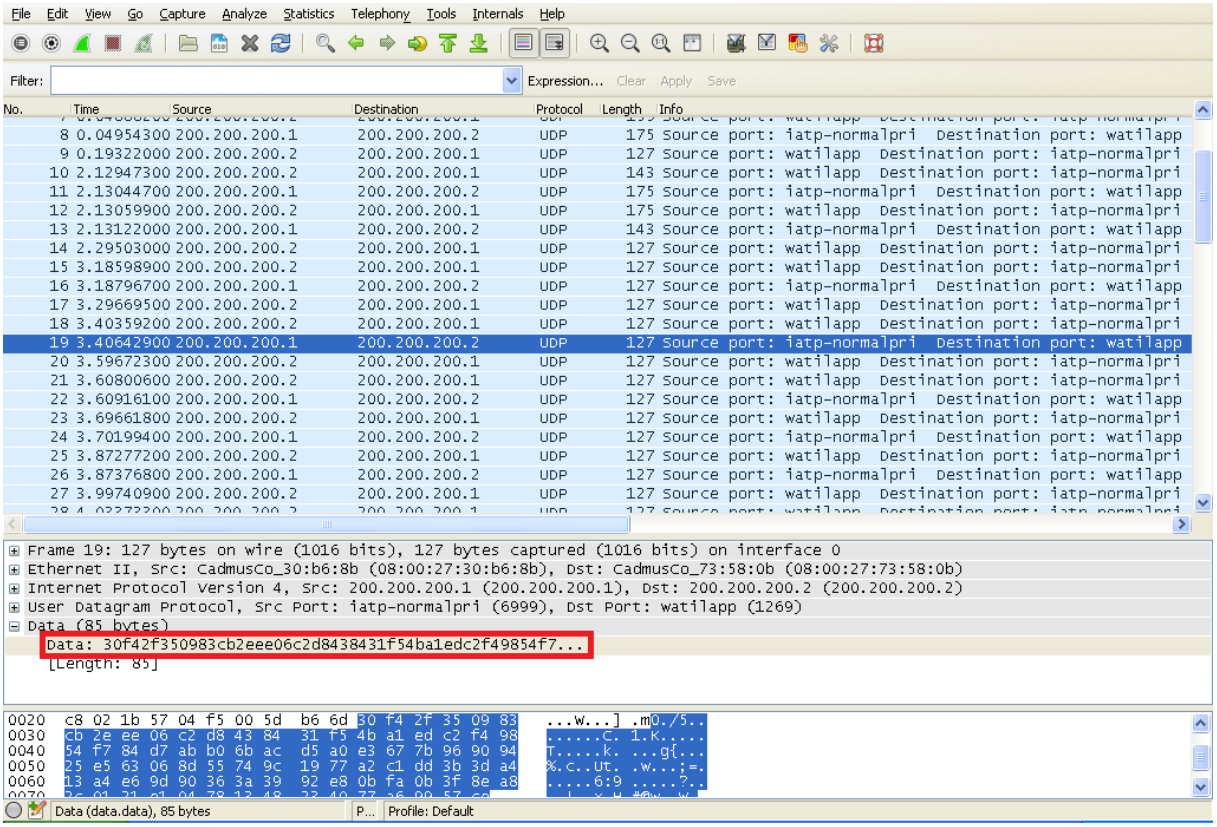



**Fonte: Próprio Autor**

Podemos ver na Figura 45, uma junção dos pacotes que apesar de nem todas as imagens estarem sendo mostradas, os caracteres do usuário remoto de Telnet, Máquina Matriz, saem um a um em sequência, pacote a pacote, bem como a descrição de *password* e os números da senha 1, 2, 3, ..., 6 também.

Agora habilita-se a conexão VPN diretamente da máquina matriz como já exemplificado na Figura 38 e 39 e colocaremos o Wireshark para monitorar os pacotes clicando em *Start new live capture*. Então, precisamos repetir os mesmos passos da Figura 41 e ao voltar ao Wireshark, parar a captura. Iremos ver o resultado da captura. Será conforme a Figura 46 a seguir.

**Figura 46 - Momento de captura dos pacotes Telnet descriptografados**



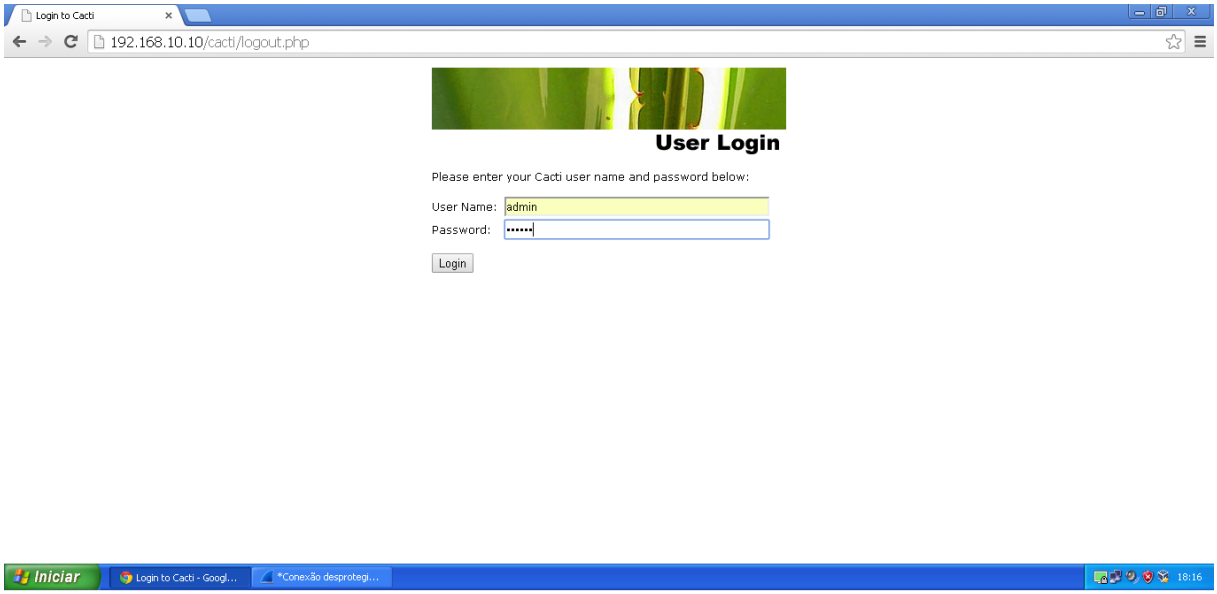

**Fonte: Próprio Autor**

Através disto, pode-se perceber que todos os dados foram criptografados em UDP, assim como no teste de segurança do FTP. Note que em “Data:”, que antes mostrava as letras alternadas do usuário e senha, agora vem com um número alfanumérico todos aleatórios, o que indica a criptografia.

### 6.4.3 Conexão Remota – Servidor Apache

Neste teste foi utilizado um servidor Web Apache com configurações padrões versão 2.4.3 instalado no sistema operacional Linux Debian 7.7. Também usa-se o sistema de autenticação do Cacti[6], que é um software livre responsável por monitorar redes utilizando gráficos. O Cacti trabalha em conjunto com apache disponibilizando acesso ao navegador. Acessando pela máquina Windows XP remota, ao se digitar o endereço do servidor 192.168.10.10/cacti na URL do navegador, obtemos o resultado a seguir, conforme a Figura 47. O usuário definido nas configurações do cacti foi: “admin” e a senha: “123456”

**Figura 47 – Página de autenticação do software Cacti utilizando o servidor Web Apache**



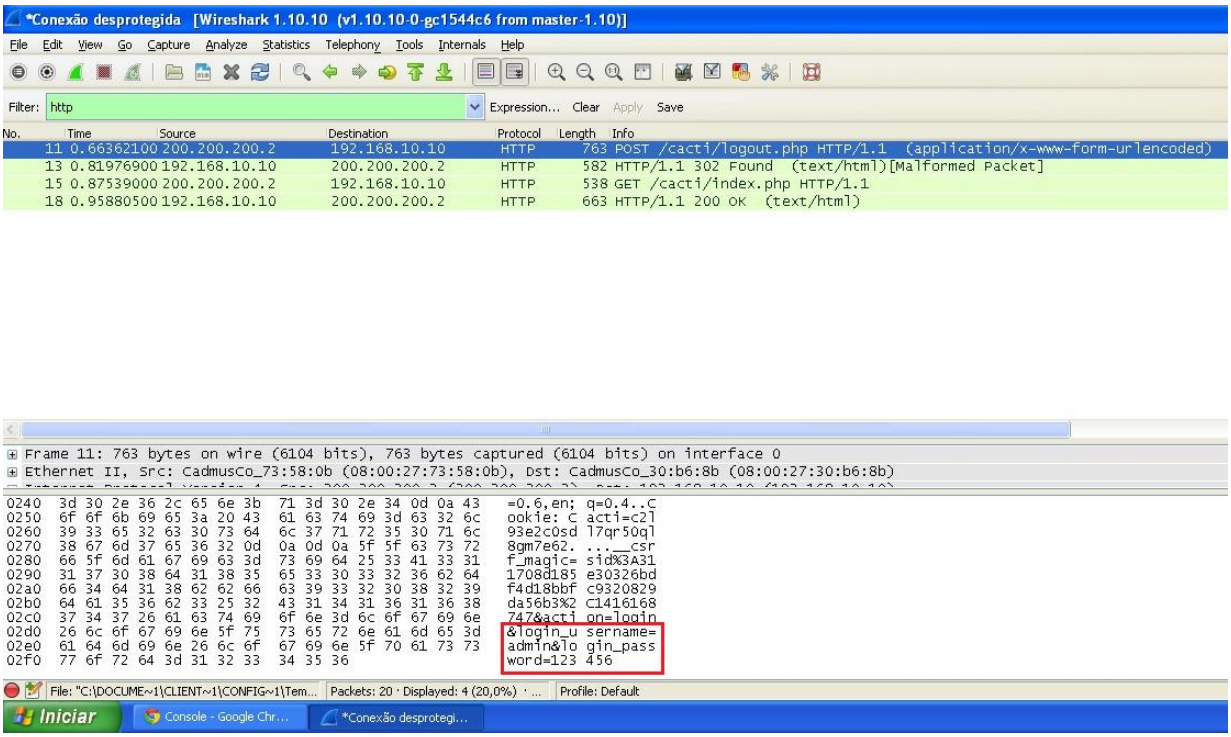

**Fonte: Próprio Autor**

Antes de clicar em *login*, será necessário abrir o programa Wireshark, selecionar a conexão desprotegida (Conexão Local) conforme Figura 35 e clicar em *Start New capture*. Agora clica-se em *Login* e em seguida volta-se ao Wireshark para pararmos o monitoramento clicando em *Stop the running Capture.*

[6] Disponível em: http://www.cacti.net/download_cacti.php. Acessado em: 12 nov. 2014.

Neste momento ve-se todos os pacotes capturados nesse curto espaço de trafego de pacotes. Vamos em *Filter* e digitar HTTP, que é o tipo de protocolo que o Cacti utilizada. Os resultados serão iguais a Figura 48 abaixo.

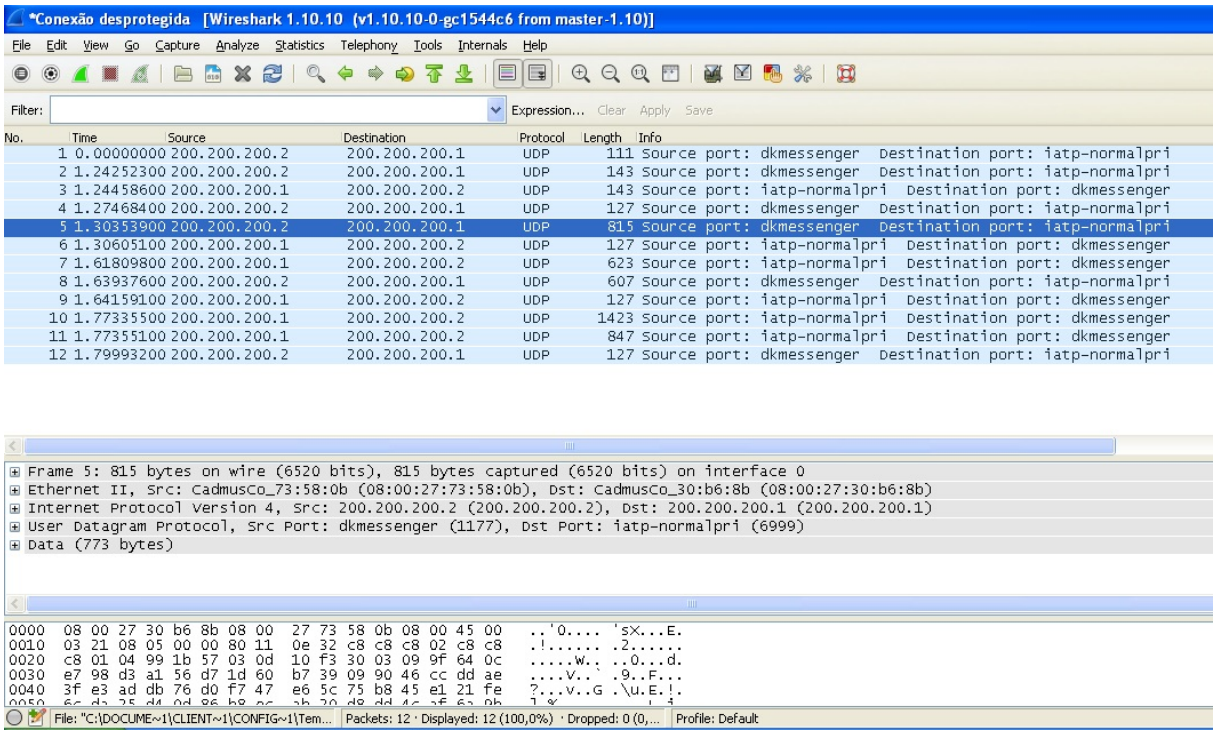
**Figura 48 – Pacotes HTTP descriptografados capturados pelo Wireshark**




**Fonte: Próprio Autor**

Pode-se perceber que o usuário (*username*) = “admin” e a senha (*password*) = “123456” foram capturados em um dos pacotes que trafegaram pela rede. Neste momento é comprovado que a autenticação do cacti é insegura. Agora será testado com conexão VPN ligada. Seguem-se exemplos da Figura 38 e 39 para habilitar a conexão VPN em nossa máquina remota. Após habilitado, será aberto o programa Wireshark novamente e será necessário clicar para capturar pacotes como já demonstrado. O *login* será feito conforme a Figura 47 e vamos parar o monitoramento logo após. O resultado será apresentado na Figura 49 a seguir.

**Figura 49 – Pacotes criptografados capturados pelo Wireshark**



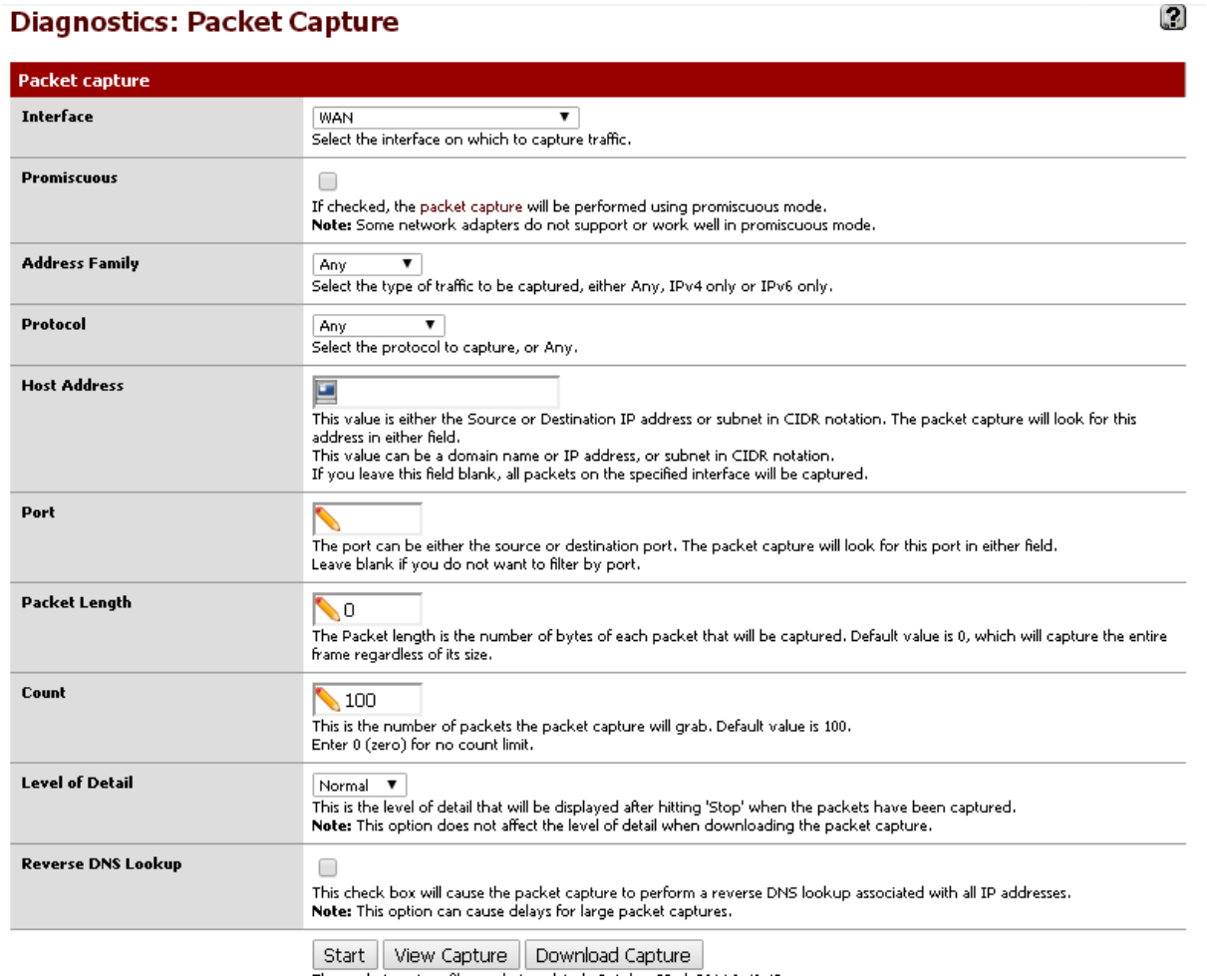

**Fonte: Próprio Autor**

Mais uma vez pode-se ver que os pacotes trafegam pela rede criptografados e todos por UDP, conforme configurado pela VPN. Os pacotes ainda podem ser vistos, porém com dados todos embaralhados devido a criptografia.

### 6.4.4 Ponto a Ponto – FTP

Utilizando o mesmo servidor FTP instalado na estação Windows XP da matriz vamos fazer o teste agora na rede ponto a ponto. Como a conexão VPN ponto a ponto foi feita entre os servidores da matriz e da filial, vamos utilizar um capturador de pacotes nativo do pfSense. Utilizando a máquina local da matriz também, primeiro será preciso logar com o IP 192.168.10.1 conforme a Figura 21. Após ir no menu *Diagnostics – Packet Capture.* Aparecerá essa interface igual a Figura 50.

**Figura 50 – Interface do capturador de pacotes nativo do pfSense**

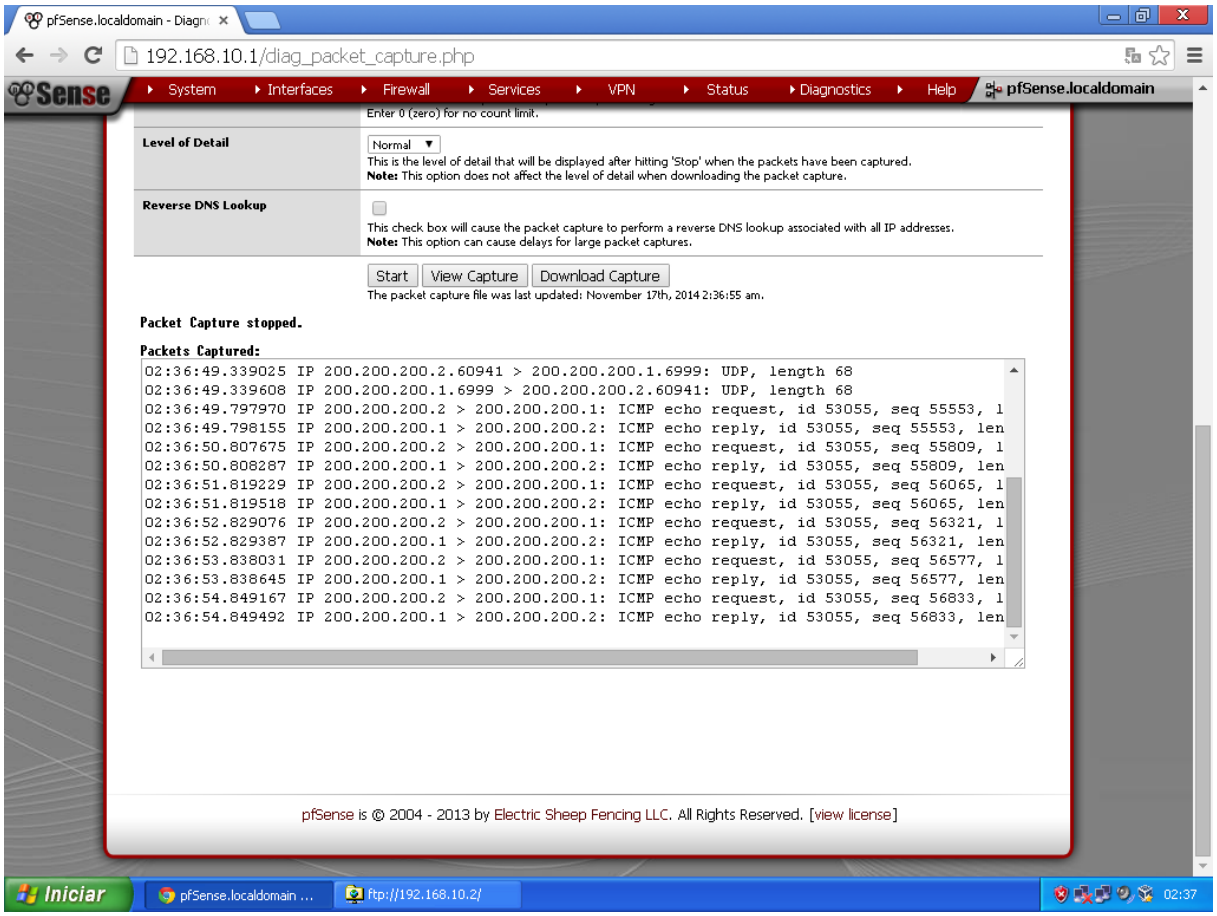



**Fonte: Próprio Autor**

Podemos ver aqui algumas opções de configurações. Seleciona-se o *WAN*, pois se trata do túnel que será criptografado. Colocar *Start*.

Agora através da estação local da matriz, igual o explicado na Figura 36, efetue o *logon* no FTP. Após o logon ser efetuado. Volte ao navegador e a página de capturas de pacotes do PfSense e de *Stop*. Efetue o *download* em *Download Capture,* como na Figura 51.

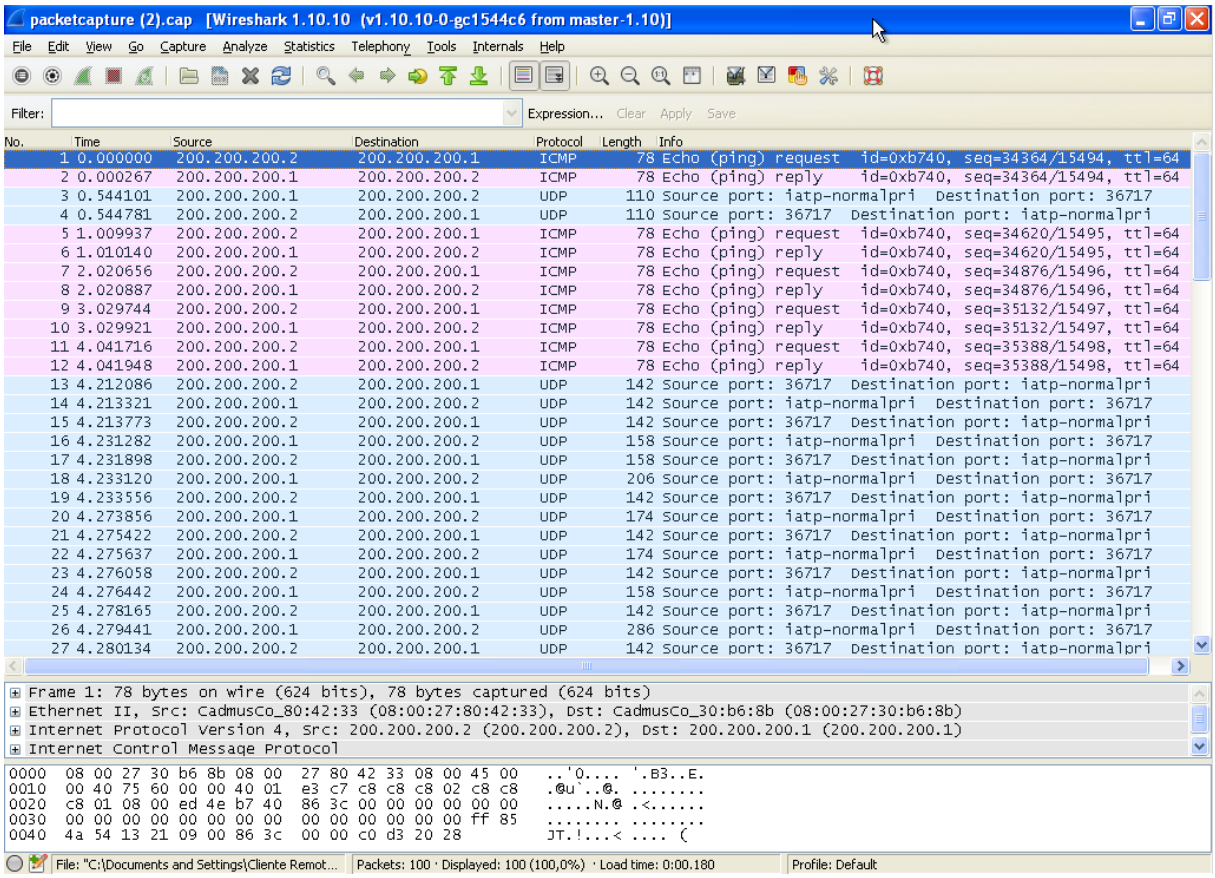
**Figura 51 – Pacotes capturados**




**Fonte: Próprio Autor**

Com o *download* do arquivo completo e salvo, se o Wireshark estiver instalado, ao dar um duplo clique sobre ele, o Wireshark vai se abrir e o resultado será semelhante a esse mostrado na Figura 52.

**Figura 52 – Pacotes todos criptografados, resultado da captura ponto a ponto**




**Fonte: Próprio Autor**

Como se pode ver, todos os pacotes estão criptografados e mais uma vez a VPN se provou criptografada.

# 7 CONCLUSÃO

Neste trabalho pode-se perceber que a tecnologia de rede, internet e segurança tem se aprimorado grandemente nos últimos anos. Percebemos que antes serviços que eram complicados, caros de se manter e com deficiência de segurança, como a comunicação entre duas empresas distantes, tem se tornando um serviço habitual e oferecido por diversas prestadoras de serviços. A concepção das pessoas, principalmente empresários, em aceitar a proteção de suas informações como o algo de extrema importância ajudou o crescimento do mercado e pesquisas avançadas por soluções melhores. A segurança ainda não é perfeita, como dificilmente será um dia, pois perfeição em informática nem sempre é possível, mas com os recursos de segurança atuais e todos os conhecimentos necessários para isso, proteger nossas informações tornou-se algo quase perto dos 100% de confiança.

A respeito do estudo do caso empregado, também pode-se dizer, que a ferramenta *Open Source* OpenVPN é tem se mostrado segura e cumpre com o prometido. Basta conhecê-la e aplicar seus diversos recursos. Ela também é uma das mais fáceis formas de VPN para se implementar, ainda compatível com praticamente todos os sistemas operacionais usados atualmente. O pfSense é uma das formas mais fáceis e práticas que se pode utilizar para a implementação de uma OpenVPN, com recursos nativos de criptografias como SH2, AES de elevados bits de proteção, gerenciamento certificados eficiente e uma interface gráfica bastante intuitiva e de fácil manuseio.

Tanto ponto a ponto como por conexão remota, segundos os testes realizados, todos os dados tornam-se criptografados no momento que o túnel VPN está habilitado pela WAN, impossibilitando o software sniffer Wireshark obter os dados limpos e livres como no modo descriptografado. É importante ressaltar que somente uma conexão VPN também não resolve todos os problemas. Medidas corretas de controle de acesso, políticas de segurança e configurações de *Firewall* devem ser colocadas em prática. Outros protocolos também são bastante seguros,

como o IPSec, por exemplo. A implementação ou não em uma empresa se deve a uma análise e ao conhecimento do profissional responsável.

Por fim, podemos concluir que a VPN, especificamente o OpenVPN é uma ferramenta segura se corretamente configurada e associada com outros recursos de segurança. Hoje a VPN já é bastante utilizada no meio corporativo, pois não é algo tão novo. Sua ideia e criação já não são tão recentes, porém novas ferramentas de gerenciamento sempre inovam e facilitam sua implementação, aprimorando seus recursos a fim de possibilitar uma segurança sempre mais eficiente.

## REFERÊNCIAS BIBLIOGRÁFICAS


AMARAL, A. F. F. **Rede de computadores:** Curso Técnico de Informática. Instituto Federal Espírito Santo – Colatina – ES – 2012. Disponível em: <http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_inf/081112_rede_comp.pdf>. Acessado em: 26 set. 2013.

BORGES F.; FAGUNDES, B. A.; CUNHA G. N. **VPN:** protocolos e segurança. Disponível em: <http://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20 Seguranca.pdf>. Acessado em: 07 abr. 2014.

BRAGHETTO, L. F. B.; SILVA, S. C. DA; BARBOSA L. ALBERTO. M. **IPSec segurança de redes** – INF542 Disponível em: <http://www.braghetto.eti.br/files/IPSec%20-%20Versao%20Final.pdf>. Acessado em 16 set. 2014.

CARVALHO, J. A. **Informática para concursos.** 5º Ed. Rio de Janeiro: Elsevier Editora Ltda. 2013. p. 808.

CARVALHO, H. E. T. **Radius:** métodos de autenticação suportados: Challenge-Handshake Authentication Protocol (CHAP). Disponível em: <http://www.gta.ufrj.br/grad/08_1/radius/Challenge-HandshakeAuthenticationProtocol (CHAP).html>. Acessado em: 15 set. 2014.

CHIN, L. K. **Rede Privada Virtual** : VPN. Disponível em: <http://www.rnp.br/newsgen/9811/vpn.html#ng-introducao>. Acessado em: 03 mar. 2014.

FAGUNDES, B. A. **Uma Implementação de VPN**. Disponível em:<http://www.lncc.br/~borges/doc/Uma%20Implementa%E7%E3o%20de%20VPN .TCC.pdf> Acessado em: 15 abr. 2014.

FERREIRA, Milton. **O que vem ser segurança da informação?.** Disponível em**:** <http://www.apinfo.com/artigo81.htm>. Acessado em: 29 set. 2013.

FIGUEIREDO, F. **Colocação do VPN na configuração do *Firewall*.** Disponível em: <http://www.aurelio.pro.br/computacao/2001-SSI-francisco.figueiredo-VPN.*firewall*.pdf>. Acessado em 18 mai. 2014.

GUIMARÃES, A. G.; LINS, R. D.; OLIVEIRA. R. **Segurança com redes privadas virtuais VPNs**. Rio de Janeiro: Brasport, 2006. 210p.

LOPEZ, G. N. **AH**: **Authentication Header**. Disponível em: <http://www.gta.ufrj.br/grad/03_1/ip-security/paginas/ah.html>. Acessado em 23 out. 2014.

LUCAS, T. J. Linux, Networking & TI. Disponível em: <http://thiagolucas.wordpress.com/2010/11/18/principios-da-seguranca-da-informacao/>. Acessado em: 28 out. 2013.

MARQUES, L. **Montando uma VPN com o OpenVPN.** Disponível em: <http://www.devmedia.com.br/montando-uma-vpn-com-o-openvpn/26670>. Acessado em: 03 set. 2014.

MARTINS, D. L. F. **Redes privadas virtuais com IPSec**. Brasília/DF. 11/08/2000. Disponível em: <http://www.cic.unb.br/~rezende/trabs/vpn.pdf>. Acessado em: 20 abr. 2014.

MENDONÇA, G. G.; ROMEIRO, R. O.; BAREIRO, S. B. **Redes Privadas Virtuais**: VPN. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/vpn/ATM.FrameRelay.html.> Acessado em: 23 set. 2014.

MIRANDA, M.Sc/D.Sc A. D. A. **Introdução as redes de computadores**. ESAB: Escola Superior Aberta Do Brasil Ltda. Vila Velha/ES. 2008. Disponível em: <http://ftp.feb.unesp.br/autodesk/pos/Disciplina-1-redes.pdf>. Acessado em: 22 set. 2013.

MIRANDA, I. C. de. **VPN - Virtual Private Network**: Rede Privada Virtual. Disponível em: <http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana/>. Acessado em 03 out. 2014.

MORIMOTO, C. E. **OpenVPN avançado:** certificados e bridges**:** Ajustando a configuração e roteando pacotes. Disponível em < http://www.hardware.com.br/tutoriais/openvpn_2/pagina4.html >. Acessado em: 29 set. 2014.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica:** os principais algoritmos de cifragem. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevista segurancadigital2012.pdf>. Acessado em: 15 set. 2014.

PINHEIRO, J. M. S., **Projeto de *Gateway* VPN**. Disponível em: <http://www.projetoderedes.com.br/tutoriais/tutorial_projeto_de_gateway_vpn_01.php>. Acessado em: 24 abr. 2014.

ROSSI, M. A. G.; FRANZIN, O. **VPN: virtual private network**. GPr Sistemas/ASP Systems – Ago. 2000. Disponível em: <http://www.gpr.com.br/download/vpn.pdf>. Acessado em: 01 nov. 2013.

RUELAS, A. M. R. **Segurança em redes privadas virtuais.** Disponível em: http://www.dca.fee.unicamp.br/~marco/cursos/ia012_14_1/trabalhos_finais/tf_11_artigo.pdf>. Acessado em 25 set. 2014.

RUGGIERI, RUGGERO; **VPN e criptografia**. Disponível em: <http://www.tiespecialistas.com.br/2011/03/vpn-e-criptografia/#.UT0WJxzFWG8> Acessado em: 06 out. 2013.

SILVA, L. S. DA. **Virtual Private Network: VPN**. Aprenda a construir redes privadas virtuais em plataformas Linux e Windows. Disponível em: <http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/143139.pdf> Acessado em: 25 mai. 2014.

TANENBAUM, ANDREW S. **Redes de computadores**. 4º Ed. Rio de Janeiro. Campus, 2003.

TRINTA, F. A. M.; MACEDO R. C. de. **Um estudo sobre criptografia e assinatura digital.** Universidade Federal de Pernambuco. 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm> Acessado em: 18 jun. 2014.

TYSON, J. **Como funciona uma VPN**. Traduzido por HowStuffWorks Brasil. Disponível em <http://informatica.hsw.uol.com.br/vpn.htm>. Acessado em: 27 set. 2013.

VINCK, A. J. H. **Introduction to public key cryptography**. Disponível em: <http://www.exp-math.uni-essen.de/~vinck/crypto/script-crypto-pdf/add-to-3.pdf>. Acessado em: 18 out. 2014.