CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE SANTA CATARINA
UNIDADE FLORIANÓPOLIS
NIS – NÚCLEO DE INFORMÁTICA E SISTEMAS
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Frederico Gendorf

REDES VIRTUAIS PRIVADAS EM AMBIENTE COOPERATIVO: UMA ABORDAGEM PRÁTICA

Trabalho de Conclusão de Curso submetido ao Centro Federal de Educação Tecnológica de Santa Catarina como parte dos requisitos para a obtenção do grau de Tecnólogo em Redes de Computadores

Orientador: Prof. MSc. Júlio César da Costa Ribas

Florianópolis, Junho de 2006

REDES VIRTUAIS PRIVADAS EM AMBIENTE COOPERATIVO: UMA ABORDAGEM PRÁTICA

Frederico Gendorf

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Graduação no Curso Superior de Tecnologia em Redes de Computadores e aprovado em sua forma final pelo Núcleo de Informática e Sistemas – Curso Superior de Tecnologia em Redes de Computadores.

_____

Prof. MSc. Júlio César da Costa Ribas
Orientador

_____

Profª. Meng. Rosemeri Coelho Nunes
Coordenadora do CST em Redes de Computadores

Banca Examinadora:

_____

Prof. MSc. Júlio César da Costa Ribas
Presidente

_____

Prof. Dr. Antônio Pereira Cândido

_____

Prof. Meng. Ilson Gripa

Dedico este trabalho à minha mãe, Darlene Polimene Caires que sempre me incentivou a ir atrás dos meus sonhos e nunca desistir em horas de dificuldades.

Agradeço ao professor MSc. Júlio César da Costa Ribas, por sua orientação, que foi muito útil para o desenvolvimento deste trabalho.

A minha noiva, Daiane Kunst, pela compreensão e incentivo nos momentos necessários.

Ao Gustavo Coral Xavier, por seu auxilio com conhecimento em línguas estrangeiras.

A todos, que de alguma forma, contribuíram para a concretização deste objetivo.

Resumo

A necessidade da troca de informações e o compartilhamento de recursos computacionais de forma segura e com baixos custos tornaram-se uma necessidade para a maioria das empresas que possuem seus dados estruturados através de redes de computadores. O avanço e a criação de tecnologias que buscam solucionar estas questões têm sido um dos maiores desafios na área da computação. Algoritmos criptográficos, protocolos de segurança, meios de comunicação seguros, são alguns dos ítens primordiais para que esta informação possa trafegar em ambientes livres de interferências externas.

A VPN (Rede Privada Virtual) veio para tentar suprir esta lacuna, sendo uma das soluções mais viáveis no atual mercado da informática. Este trabalho apresenta uma solução de acesso remoto para compartilhamento de recursos computacionais de forma segura, utilizando uma abordagem prática em uma empresa do ramo de engenharia, adotando-se a tecnologia de VPN.

Será abordado todo o processo, desde a seleção da tecnologia de VPN e os critérios que levaram à escolha da mais adequada, até a implementação e a análise de uso, em um ambiente cooperativo distribuído.

Palavras chaves: VPN, Criptografia, Linux, Redes, Internet.

Abstract

The need for data exchange and share computational data in a safe way with low cost became a real need for most of the companies which have the majority of their data structured in computer networks. The advance and creation of new technologies which allows solving these issues have been one of the biggest challenges in the computational field. Cryptographic algorithms, security protocols, safe data exchange are some of the main items which allows the information to be traded in free environments rid of outside interferences.

VPN (Virtual Private Network) came to try to supply this gap, being one of the solutions most viable in the current market of computer science. This document presents a solution of remote access for sharing of computational resources of safe form, using a practical boarding in a company of the engineering branch, adopting itself it VPN technology.

The process will be boarded all, since the election of the technology of VPN and the criteria that had led to the most adjusted choice of, until the implementation and the analysis of use, in a distributed cooperative environment.

Key Words: VPN, Cryptographic, Linux, Network, Internet.

Resumen

La necesidad del cambio de informaciones y el intercambio de recursos computacionales de manera segura y con bajos costos se transformaron en una necesidad para la mayoría de las empresas que poseen sus datos estructurados a través de redes de computadores. El avanzo y la creación de tecnologías que buscan solucionar esos temas tienen sido uno de los mayores desafíos en el área de la computación. Algoritmos criptográficos, protocolos de seguridad, medios de comunicación seguros, son algunos de los ítems primordiales para que esa información pueda trasegar en ambientes libres de interferencias externas.

VPN (Red Privada Virtual) vino intentar proveer este boquete, siendo una de las soluciones más viables del mercado actual de la informática. Este documento presenta una solución del acceso alejado para compartir de recursos de cómputo de la forma segura, usando subir práctico en una compañía del rama de la ingeniería, adoptándose él tecnología de VPN.

El proceso será subido todos, puesto que la elección de la tecnología de VPN y los criterios de los cuales había conducido a la opción ajustada, hasta la puesta en práctica y el análisis del uso, en un ambiente cooperativo distribuido.

Palabras claves: VPN, Criptográfico, Linux, Red, Internet.

Lista de Tabelas

Lista de Figuras

Listas de abreviaturas e siglas

AES	Advanced Encryption Standard
AH	Authentication Header
ANSI	American National Standards Institute
ARPA	Advanced Research Projects Agency
ASP	Application Server Provider
ATM	Asynchronous Transfer Mode
BOOTP	Bootstrap Protocol
CA	Certificate Authority
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
ESP	Encapsulated Security Payload
ESSS	Engineering Simulation and Scientific Software Ltda
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Security
IETF	Internet Engineering Task Force
IMAPS	Internet Message Access Protocol Security
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
MPPE	Microsoft Point-To-Point Encryption Protocol
NCP	Network Control Protocol
NFS	Network File System
NIST	National Institute of Standard and Technology
NSF	National Science Foundation
OSI	Open Systems Interconection
PKI	Public Key Infrastructure
POP	Post Office Protocol
POPS	Post Office Protocol Security
PPP	Point to Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RAS	Remote Access Service
RFC	Request For Coments
RSA	Ron **R**ivest, Adi **S**hamir e Len **A**dleman.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TI	Tecnologia de Informação

TLS	Transport Layer Security
UDP	User Datagram Protocol
VNC	Virtual Network Computing
VPN	Virtual Private Network
VPNC	Virtual Private Network Consortium
VPDN	Virtual Private Dial Network
WAN	Wide Area Network
IMAP	Internet Message Access Protocol

Sumário

1. Introdução

Na atualidade os ambientes corporativos mundiais estão cada vez mais dependentes da informática para a execução das mais variadas atividades em seu cotidiano e para que haja uma maior interação entre os hosts dos usuários, tanto em compartilhamento de informações, quanto em compartilhamento de recursos como: impressora, disco, equipamento de captura de dados e vários outros, foram criadas tecnologias que possibilitam a criação de redes locais.

Estas redes locais geralmente possuem alta velocidade para transferência de informações dentro da empresa. Quando uma empresa começa expandir geograficamente, para atender uma maior demanda, geralmente ela tem necessidade de se interligar às outras filiais para compartilhamento de resultados ou recursos utilizados, porém, esta interligação, por se tratar de uma longa distância, é feita com uma tecnologia diferente da rede local e quase sempre é mais lenta, mas o suficiente para troca dos dados necessários.

Existe uma série de tecnologias que proporcionam esta interligação, porém, algumas delas necessitam de um grande investimento para implantação ou para manutenção, como o caso da fibra óptica, banco de modens e links Frame Relay. Existe uma tecnologia que permite a interligação de filiais nas mais diferentes posições geográficas por um custo relativamente mais atraente para empresas. Esta tecnologia é chamada VPN (Virtual Private Netowork ou Rede Privada Virtual).

A VPN é constituída por um túnel virtual criptografado que por meio de algumas regras, interliga duas redes distantes usando a internet como meio de transmissão.

> Antes do surgimento de VPN, as comunicações dentro de uma empresa e entre empresas eram feitas através de serviços de Frame Relay, linhas privadas, servidores de acesso remoto e modens. Apesar de serem seguras e apresentarem grande disponibilidade, estas tecnologias são caras e pouco escaláveis. A cada nova filial a ser conectada à rede interna da empresa, ou um novo fornecedor que deva acessar um servidor interno, uma nova conexão dedicada deveria ser acionada. [RAP 03]

Por geralmente utilizar a internet como meio de conexão, interligar uma nova filial à rede da empresa é significativamente simples e sem maiores investimentos, pois basta que a mesma tenha acesso à internet e que seja configurado um gateway VPN. Esta será a abordagem apresentada neste trabalho.

1.1. Objetivos

1.1.1. Objetivo Geral

A proposta do TCC é demonstrar uma solução de acesso remoto para compartilhamento de recursos computacionais de forma segura, utilizando uma abordagem prática em uma empresa do ramo de engenharia.

Será abordado todo o processo, desde a seleção da tecnologia de VPN e os critérios que levaram à escolha da mais adequada, até a implementação e a análise de uso, em um ambiente cooperativo distribuído.

1.1.2. Objetivos Específicos

Os objetivos específicos a serem alcançados com este TCC são:

- Realizar um estudo bibliográfico aprofundado sobre o tema em estudo, o qual dará suporte e fundamentação para o desenvolvimento da proposta do TCC em questão;
- Implementação de rede em um ambiente cooperativo no qual existe a necessidade de uma estrutura de VPN para interligação de filiais, uso remoto de recursos computacionais da matriz e acesso remoto para funcionários em trânsito;
- Utilização e análise da solução aplicada na empresa.

1.2. Abrangência

Este trabalho foi concebido de acordo com a necessidade da empresa ESSS (Engineering Simulation and Scientific Software Ltda.) em ter uma maior integração entre matriz, filiais e funcionários em deslocamento. O modelo da ESSS é comumente encontrado em diversas empresas que necessitam prover uma comunicação segura, eficiente e com baixo custo de investimento para filiais e usuários móveis (vendedores, diretoria, analistas de TI, etc).

Implementar uma VPN entre matriz e filial pode parecer bastante simples em uma primeira impressão, porém existe uma série de regras e cuidados que devem ser analisados antes da implantação. Deve-se analisar a estrutura na qual se

encontram as partes envolvidas e visualizar no futuro como a empresa pretende se expandir.

"A simples escolha do protocolo a ser utilizado, portanto não implica em sucesso no projeto da VPN, pois um protocolo sozinho não garante a segurança do sistema" [NAK 02], e muito menos a aquisição de dispositivos VPN por alguns milhares de dólares irá garantir o sucesso da solução. O conceito de Virtual Private Networks em nada se assemelha com o conceito de plug-and-play.

Este trabalho propõe atingir uma área geográfica, usando topologia de VPN rede-rede, abrangendo a matriz localizada em Florianópolis e as filiais localizadas nas cidades de São Paulo e Rio de Janeiro.

A topologia a ser utilizada, bem como a representação da WAN da empresa é mostrada na figura 1.

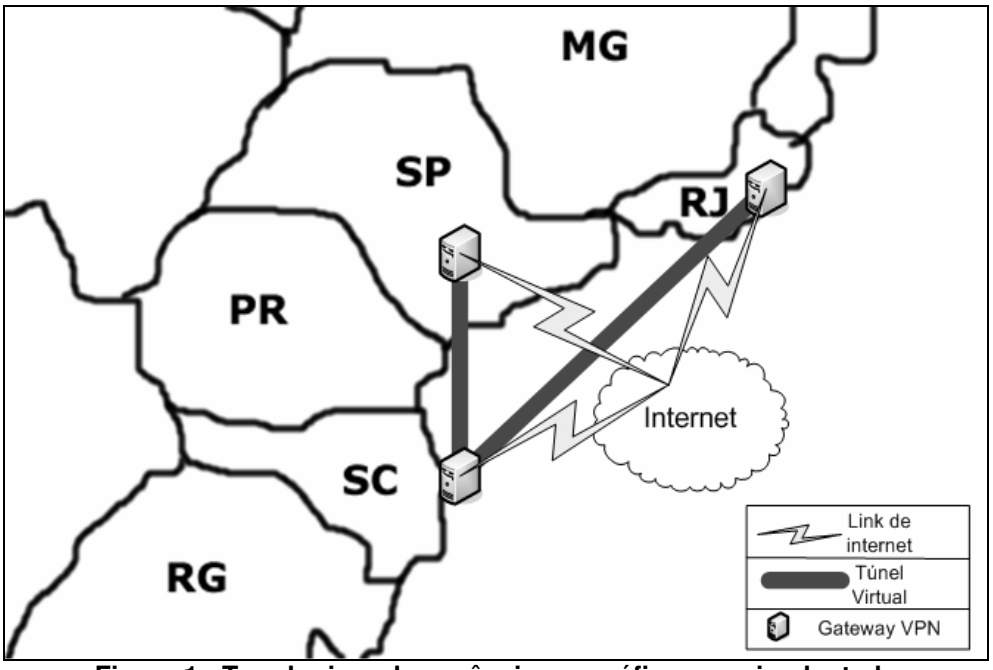


Figura 1 - Topologia e abrangência geográfica a ser implantada

1.3. Organização do trabalho

Baseado nas etapas de desenvolvimento deste trabalho, os itens necessários para a utilização de uma rede WAN com VPN em um ambiente cooperativo foram agrupados e discutidos na seqüência apresentada a seguir.

No capítulo 2 serão apresentados os principais protocolos de comunicação necessários para utilização de uma VPN nos moldes da que será discutida neste trabalho. Este capítulo é um dos requisitos necessários para se entender como funciona uma VPN.

No capítulo 3 serão abordados os aspectos de segurança necessários ao se implantar uma VPN em um ambiente cooperativo. Serão comentados alguns riscos para a empresa e alguns métodos de defesa.

O capítulo 4 abordará especificamente o tema VPN. Nele será descrito o funcionamento da VPN, um comparativo entre VPNs e outras tecnologias utilizadas para interligar redes.

O capitulo 5 será referente à descrição do método utilizado para implementação da VPN na empresa ESSS.

No capitulo 6 será descrito como foi efetuado o processo de seleção da tecnologia de VPN que foi adotada para instalação na empresa ESSS.

No capítulo 7 será descrito todo o procedimento executado dentro da empresa ESSS para a implantação de uma rede WAN entre matriz, filiais e acesso remoto para funcionários fora da empresa, com a utilização de VPN. Neste capítulo será descrito também as ferramentas que serão utilizadas bem como as suas configurações necessárias.

O capítulo 8 serão abordadas as análises feitas sobre as conexões de clientes VPN, como seus números de acessos, médias de transferências e perfil de utilização.

O último capítulo conclui os estudos ressaltando as contribuições obtidas com a implantação da Rede Privada Virtual, seus benefícios e perspectivas futuras. Finalizando seguem as referências bibliográficas e o glossário.

2. TCP/IP

2.1. Protocolos de Comunicação

O Conjunto de protocolos da Internet TCP/IP é o padrão mundial para interconexão de sistemas abertos. Nenhum outro conjunto de protocolos proporciona tanta interoperabilidade ou abrange sistemas de tantos fornecedores. E, o que é mais importante, o TCP/IP é executado em mais tecnologias de rede do que qualquer outro conjunto de protocolos. A internet global conecta escolas, instituições governamentais, organizações com e sem fins lucrativos e indivíduos ao redor do mundo.

Além das conexões à internet, muitas organizações empregam o TCP/IP em suas redes internas. Uma rede privada que utiliza TCP/IP é conhecida como uma intranet; embora a maioria das empresas não divulgue informações sobre suas intranets, algumas delas são amplas. Por exemplo, empresas dos setores aeroespacial, automotivo, eletrônico, de hotelaria, petroleiro, de imprensa, farmacêutico, e outros possuem intranets que incluem sites em diversos paises. Tais empresas usam o TCP/IP para conectar todas as suas redes remotas e locais [COM 99].

2.2. Histórico

TCP/IP *(Transmission Control Protocol/Internet Protocol) é* o protocolo formal baseado em dois subprotocolos: TCP, um protocolo da camada 4 do modelo OSI, e o IP, um protocolo da camada 3. A história do TCP/IP está ligada à ARPANET, que estava baseada no *Network Control Protocol* (NCP). O projeto inicial da ARPANET estava centrado em dois princípios: A rede física não era confiável, e os protocolos não podiam depender de software ou hardware proprietário. A idéia de se ter uma rede não-confiável parecia fora de senso a princípio, mas a ARPANET era um projeto do Ministério da Defesa, onde se admitia que um evento catastrófico poderia interromper a rede física. Isso alavancou o desenvolvimento do TCP/IP. O princípio de software e hardware não-proprietário, juntamente com o sucesso da ARPANET, tornou o TCP/IP disponível em várias plataformas de software e hardware.

Vint Cerf e Robert Kahn auxiliaram o desenvolvimento do TCP/IP. No início dos anos 70, ambos desenvolveram a idéia de gateways como parte do programa de interconectar a ARPA e fizeram a primeira especificação do TCP/IP. A idéia principal do desenvolvimento do TCP/IP era possibilitar que redes de pacotes distintos fossem interconectadas, de forma que os computadores não precisassem ter conhecimento sobre as redes intermediárias para poder usá-las. Em 1982, a ARPA estabeleceu como protocolo para a ARPANET, o TCP/IP', que também passou a ser o padrão para uso militar. Este fato impulsionou uma das primeiras definições de "internet" como um conjunto de redes interconectadas, e especialmente aquelas que usavam o TCP/IP foram denominadas "Internet". A idéia da Internet era a ligação de vários tipos de redes chaveadas por pacotes. Tal objetivo foi facilitado pela robustez do TCP/IP, que possibilitava a

comunicação de dados através de linhas analógicas, pacotes de rádio, conexões com satélite, redes Ethernet e outros.
A ARPANET cresceu nos anos 80 na mesma proporção da interconexão de computadores. A popularidade das redes de computadores foi impulsionada com a proliferação de PCs e estações de trabalho – usuários queria conectar seus sistemas. Com o reconhecimento do potencial de mercado, popularidade da interconexão levou ao desenvolvimento de vários protocolos de rede proprietários. Isso também levou a problemas de interoperabilidade. Este não era o caso, entretanto, em uma rede heterogênea.
Nesta época, o Departamento de Ciência da Computação da University of California em Berkeley estava melhorando a versão original do sistema operacional UNIX, chamado de BSD UNIX. Uma das suas novidades foi a incorporação do protocolo TCP/IP. Este software foi distribuído gratuitamente e logo se tornou bastante popular nas universidades dos EUA. Dado que o TCP/IP foi incorporado ao UNIX e que estava sendo usado com sucesso em rede de tempo real (ARPANET), a NSF (National Science Foundation) ordenou que todos os seus centros de supercomputação e suas redes na NSFNET usassem o TCP/IP como protocolo de comunicação. Desta forma, a NSF estabeleceu o TCP/IP como um padrão [GAL 03].

2.3. Modelos de Referência

2.3.1. Modelo OSI

O modelo de Referência OSI (*Open Systems Interconection*) foi desenvolvido pela *International Standards Organization* (ISO) e, geralmente utiliza-se o paradigma do Modelo OSI para descrever outros padrões e protocolos normalmente utilizados para a rede. O modelo OSI divide as tarefas da rede em sete camadas hierárquicas. Estas camadas são hierárquicas porque as camadas superiores dependem das camadas inferiores para sua operação [SOA 97].

A figura 2 apresenta a organização do modelo de referência OSI.

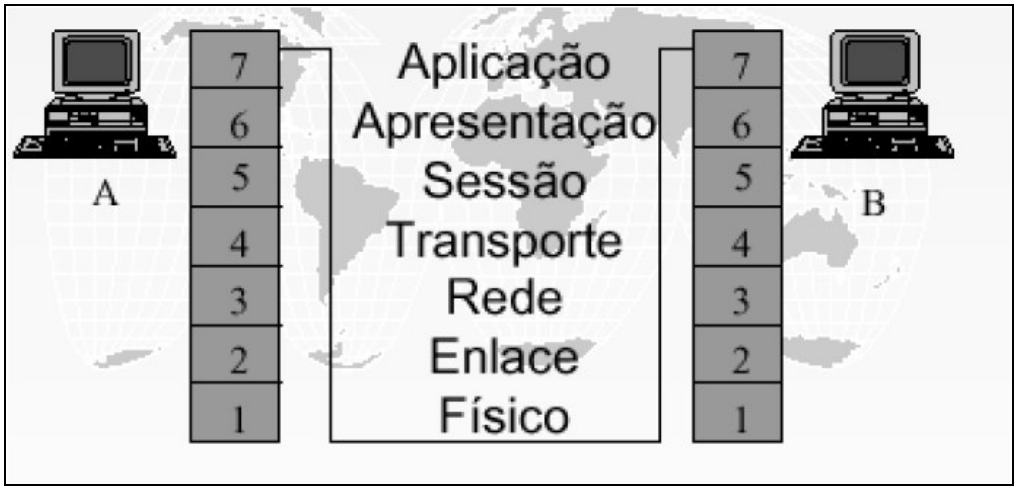


Figura 2 - As sete camadas do modelo OSI

2.3.2. Modelo TCP/IP

> TCP/IP é um acrônimo para o termo *Transmission Control Protocol/Internet Protocol Suite*, ou seja, é um conjunto de protocolos, onde dois dos mais importantes (o IP e o TCP) deram seus nomes à arquitetura. O protocolo IP, base da estrutura de comunicação da Internet é um protocolo baseado no paradigma de chaveamento de pacotes (*packet-switching*) [COM 99].

Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa. Como exemplo, pode-se empregar estruturas de rede como Ethernet, Token-Ring, FDDI, PPP, ATM, X.25, Frame-Relay, barramentos SCSI, ligações telefônicas discadas e várias outras como meio de comunicação do protocolo TCP/IP.

A arquitetura TCP/IP, assim como a OSI, realiza a divisão de funções do sistema de comunicação em uma estrutura de camadas. A figura 3 ilustra esta estrutura.

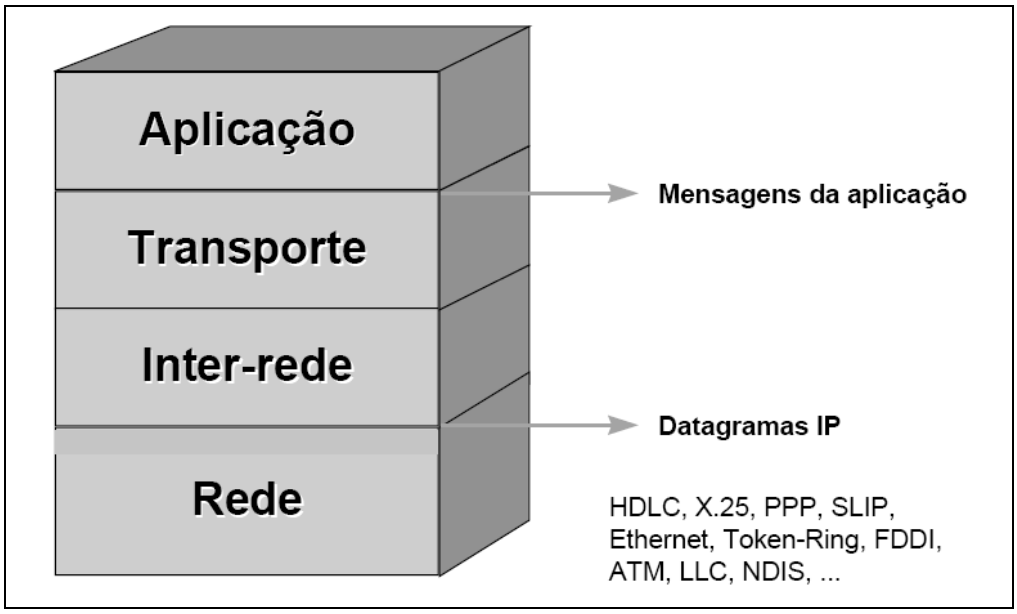


Figura 3 - Camadas do protocolo TCP/IP

2.4. A Arquitetura Internet

Esta arquitetura segue o modelo de referencia TCP/IP, com as mesmas definições de camadas.

2.4.1. A camada Host/Rede

A camada de rede é responsável pelo envio de datagramas construídos pela camada Inter-Rede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-rede para um endereço físico ou lógico do nível de Rede. A camada Inter-Rede é independente do nível de Rede [PIN 01].

2.4.2. A Camada Inter-redes

A camada Inter-Rede realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede, onde estas estão situadas é definido um identificador, chamado endereço IP, que é independente de outras formas de endereçamento que possam existir nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP em um endereço deste nível. O protocolo IP realiza a função mais importante desta camada que é a própria comunicação inter-redes. Para isto ele realiza a função de roteamento que consiste no transporte de mensagens entre redes e na decisão de qual rota uma mensagem deve seguir através da estrutura de rede para chegar ao destino [DER 95].

2.4.3. A Camada de Transporte

A camada de Transporte reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários.
A camada de transporte possui dois protocolos que são o UDP (*User Datagram Protocol*) e TCP (*Transmission Control Protocol*) [PIN 01].

2.4.4. A Camada de Aplicação

A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário e faz a comunicação entre os aplicativos e o protocolo de transporte. Existem vários protocolos que operam nesta camada como: HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), DNS (Domain Name System) e o Telnet [PIN 01].

2.5. Principais Protocolos e Serviços

A arquitetura internet se baseia praticamente em um serviço de rede não orientado à conexão (datagrama não confiável, UDP), o Internet Protocol (IP) e em um serviço de transporte orientado à conexão, oferecido pelo Transmission Control Protocol (TCP). Juntos, estes

protocolos se completam, oferecendo um serviço confiável de uma forma simples e eficiente.
"Os três protocolos-chave da internet que temos hoje – TCP, UDP, IP – já estavam conceitualmente disponíveis no final da década de 70" [TAM 97].

2.5.1. UDP

O UDP (User Datagrama Protocol) é um protocolo livre de conexão que provê um serviço de datagrama não-confiável. Ele não faz detecção ou correção de erros entre pontos terminais de transmissão, não retransmite os dados que não foram recebidos e nem tem a habilidade de lidar com erros ou controle de fluxo. Isso implica que todos os programas de aplicação baseados no UDP devem prover mecanismos para lidar com erros e controle de fluxo e para recuperar os pacotes perdidos. Em resumo, todas as questões que envolvem confiabilidade e segurança devem ser providas pelos programas de aplicação que usam o UDP? Isso faz o UDP ter um desempenho melhor que o TCP, quando a rede não está congestionada, porque ele não faz tantas verificações quanto o TCP. Contudo, quando a rede está congestionada, as aplicações baseadas em UDP apresentam baixo desempenho. Os protocolos de aplicação baseados no UDP incluem o Trivial File Transfer Protocol (TFTP), o Network File System (NFS), Simple Network Management Protocol (SNMP), o Bootstrap Protocol (BOOTP) e o Name Service (DNS) [GAL 03].

2.5.2. IP

Este protocolo pertence à camada de Internet. A tarefa do IP é fornecer a melhor forma de transportar datagramas da origem ao destino, independente se as máquinas estão na mesma rede ou em redes intermediárias. Como está mostrado na figura 4, um datagrama de IP é composto de várias partes. O cabeçalho é composto de informações variadas, incluindo endereços de IP de origem e de destino. Estes elementos juntos formam um cabeçalho completo. A parte restante do datagrama contém os dados que estão sendo enviados. O que surpreende no protocolo de Internet é que, os datagramas podem ser fragmentados durante sua viagem e mais tarde montados no seu destino [LES 00].

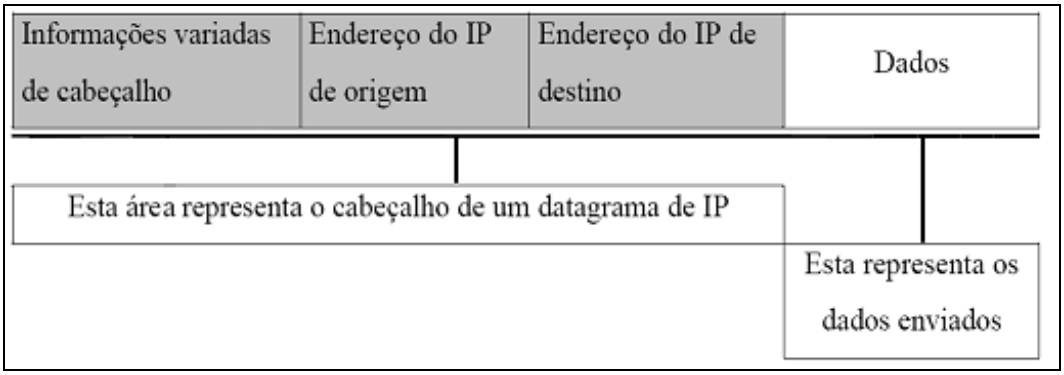


Figura 4 - Datagrama IP

2.5.3. TCP

> Protocolo de Controle de Transmissão (Transmission Control Protocol) é o TCP do TCP/IP. É um protocolo duplex completo orientado por conexão que desempenha várias funções, incluindo: transmissão confiável de dados com detecção e correção de erros; garantia de transmissão de dados corretos e na ordem adequada; retransmissão de dados não recebidos no ponto destino e garantia de não-duplicação de dados entre os nós origem e destino.
> Protocolos de aplicação que usam o TCP incluem: Telnet, Protocolo de Transferência de Arquivos (FTP), Protocolo Simples de Transferência de Correio (SMTP) e Protocolo de Correio (POP) [GAL 03].

2.6. Resumo do capítulo

Neste capítulo foram revisados alguns conceitos sobre o que é o protocolo TCP/IP, seu histórico, alguns modelos de referências para desenvolvimento de rede e a descrição da arquitetura da internet, que segue o modelo de referência do TCP/IP.

3. Aspectos de segurança

> Segurança da informação é um item indispensável dentro de uma corporação e a VPN se encaixa perfeitamente devido as suas premissas de funcionamento, que são: Privacidade, Integridade, autenticidade, Não-repudio e Facilidade [SAR 03].

Cada uma destas premissas será discutida mais a frente no capítulo quatro, que abordará conceitos de VPN.

Ao deixar de fazer um redirecionamento no gateway para um serviço na rede interna da empresa, ou de colocar um serviço na internet e ainda assim estar possibilitando a um usuário se conectar a este serviço contribui e muito com a segurança do sistema e dos dados dentro de um ambiente cooperativo e é assim que a VPN aumenta a segurança.

Mesmo não expondo a rede externamente, a VPN pode sofrer com alguns problemas de segurança. Algumas ameaças e ataques serão discutidos à frente.

3.1. Ameaças

Apesar de aumentar a segurança dos dados disponibilizado a funcionários fora da empresa ou entre filiais e matriz, a VPN, como qualquer serviço disponibilizado na internet, pode sofrer várias ameaças vindo de várias origens.

> As ameaças mais comuns à rede da empresa são: hackers, antigos funcionários ou funcionários insatisfeitos, parceiros extranet e usuários curiosos que querem ter posse de determinada informação para uso pessoal ou para benefício próprio [SAR 03].

Por estes e outros motivos há sempre a necessidade de se ter um acompanhamento de atualizações de softwares, uma política de utilização bem definida e restrições a serem impostas aos usuários. Este item será discutido mais à frente em métodos de defesas.

3.2. Ataques

As VPNs, por proporcionar uma conectividade entre filiais e possibilitar que funcionário possam acessar a seus postos de trabalho como se estivessem dentro da empresa, é bastante passiva de ataques, tanto externa quanto internamente.

Alguns dos ataques mais comuns são:

> **Denial of Service (Negação de Serviços) –** DoS são ataques que visam interromper ou negar completamente um serviço a usuários

legítimos, congestionando redes, sistemas ou outros recursos. Existem várias formas de promover um ataque DoS, como por exemplo número excessivo de tentativas de conexões, ataques por pacoteamento excessivo (flood) e etc [NAK 02].

IP Spoofing – É uma técnica na qual o endereço real do atacante é mascarado, de forma a evitar que ele seja encontrado. A intenção deste tipo de ataque é fazer com que se pense que a origem do ataque esta vindo de outro lugar.Uma Organização pode proteger sua rede contra o IP spoofing de endereços IP da rede interna por meio da aplicação de filtros, de acordo com as interfaces de rede.Por exemplo, se a rede interna da organização tem endereços do tipo 100.200.200.0, então o firewall deve bloquear tentativas de conexão originadas externamente, onde a origem tem endereços da rede interna. Firewall será discutido um pouco mais a frente [NAK 02].

Ataques de força bruta - É a forma de ataque mais básica. Consiste em adivinhar uma cominação de ID de usuário e senha pelo método de tentativa e erro (força bruta). Qualquer par de ID de usuário/senha pode ser descoberto por força bruta se o atacante dispuser de tempo suficiente. Os sistemas de segurança procuram tornar este tempo suficientemente longo (centenas/milhares de anos). De forma a tornar este tipo de ataque ineficaz [SAR 03].

Ataque Sniffing – Também conhecida como passive eavesdropping, esta técnica consiste na captura de informações valiosas diretamente pelo fluxo de pacotes na rede. Diversos softwares podem ser encontrados, inclusive o snoop, fornecido com o Solaris (Sistema operacional da SUN), e o tcpdump, fornecido com o linux, que são originalmente utilizados para auxiliar na resolução de problemas de rede. Com o uso da criptografia da VPN este tipo de ataque não é possível diretamente no túnel VPN, porém pode ocorrer em suas extremidades [NAK 02]

A vulnerabilidade que a empresa tem se dá pela falta de uma política de segurança (regras e métodos de proteção a serem usados dentro da empresa), sistemas desatualizados (principalmente versões antigas com furos de proteção conhecidos e ainda não corrigidos), gestão inadequada dos softwares e dispositivos existentes praticadas por pessoas sem o conhecimento necessário para tal [SAR 03].

3.3. Métodos de defesas

Existem várias métodos para se defender um ambiente cooperativo de ameaças comumente encontradas em um ambiente ligado em rede. A VPN pode trabalhar com vários deles ao mesmo tempo, proporcionando assim um aumento substancial no nível de segurança alcançado. Vejamos agora alguns métodos de se proteger uma VPN de certas ameaças.

3.3.1. Firewall

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

> Há mais de uma forma de funcionamento de um firewall, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem dois tipos básicos de conceitos de firewalls: o que é baseado em filtragem de pacotes e o que é baseado em controle de aplicações. Ambos não devem ser comparados para se saber qual o melhor, uma vez que cada um trabalha para um determinado fim, fazendo que a comparação não seja aplicável [ALE 04].

O firewall de modo geral fica localizado entre a internet e a rede interna, funcionando como se fosse uma muralha (ver figura 5) barrando trafego e conexões indesejadas.

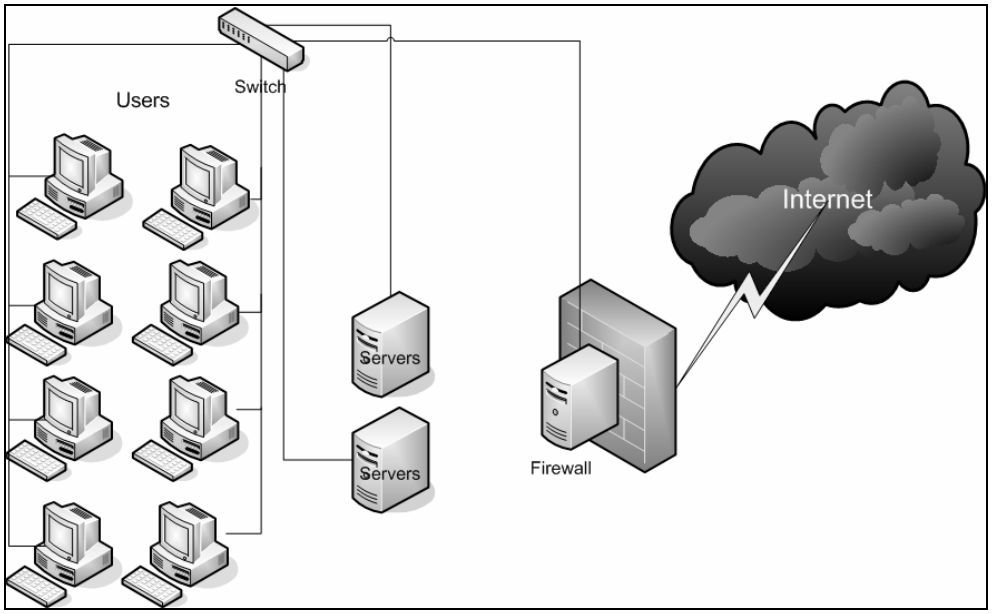


Figura 5 - Representação de um Firewall corporativo

3.3.1.1. Firewall e VPN

O firewall é um item de segurança que pode auxiliar e muito uma VPN, tanto para restrição de conexões de determinados hosts, como em conjunto com a VPN restringindo que alguns usuários acessem determinadas máquinas e serviços dentro da empresa.

“Existem basicamente cinco maneiras de se posicionar o firewall e a VPN em uma rede” [NAK 02], [SAR 03], são elas:

a. VPN junto ao Firewall

A localização da VPN junto ao Firewall (figura 6) possibilita que o gerenciamento e a administração sejam mais simplificados, havendo a possibilidade de uma ação em conjunto das duas ferramentas.

Alguns autores citam a unificação dos dois itens em um único equipamento como uma diminuição no fator de segurança, pois caso exista a possibilidade de falha, isto está presente apenas em um único ponto da rede. Já outros autores dizem este ser o posicionamento ideal, pois o firewall pode atender a todas as necessidades da VPN, além de haver a possibilidade de uma maior interação entre os dois.

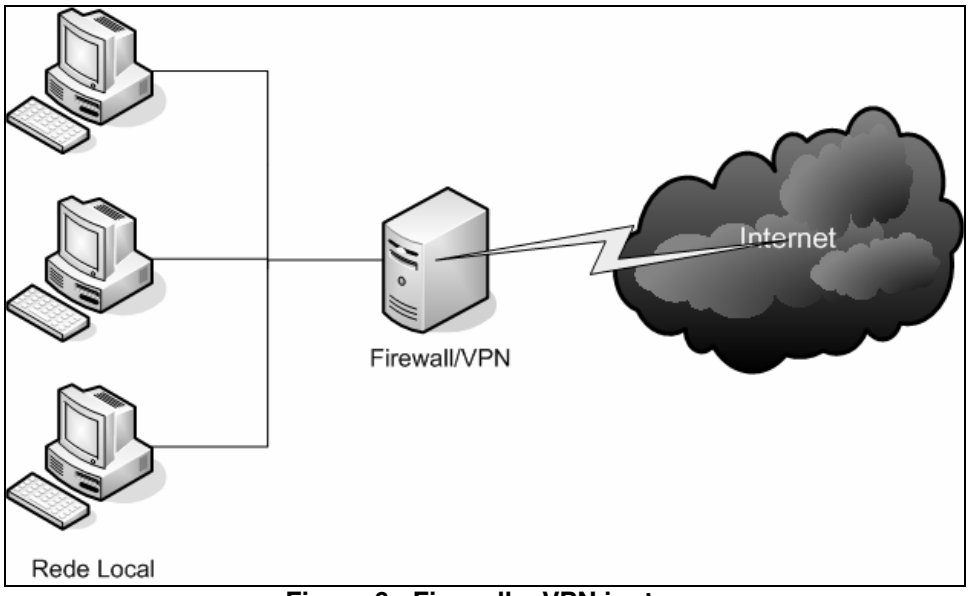


Figura 6 - Firewall e VPN juntos

b. VPN em frente ao Firewall

A localização da VPN em frente ao firewall (ver figura 7) visa permitir que o tráfego que sai da VPN seja verificado pelo firewall depois que os pacotes forem descriptografados. Porém, pelo servidor de VPN estar localizado frente ao firewall ele é obrigado a deixar passar todo o tráfego como se fosse um gateway, além de ficar diretamente exposto à internet comprometendo assim a sua segurança.

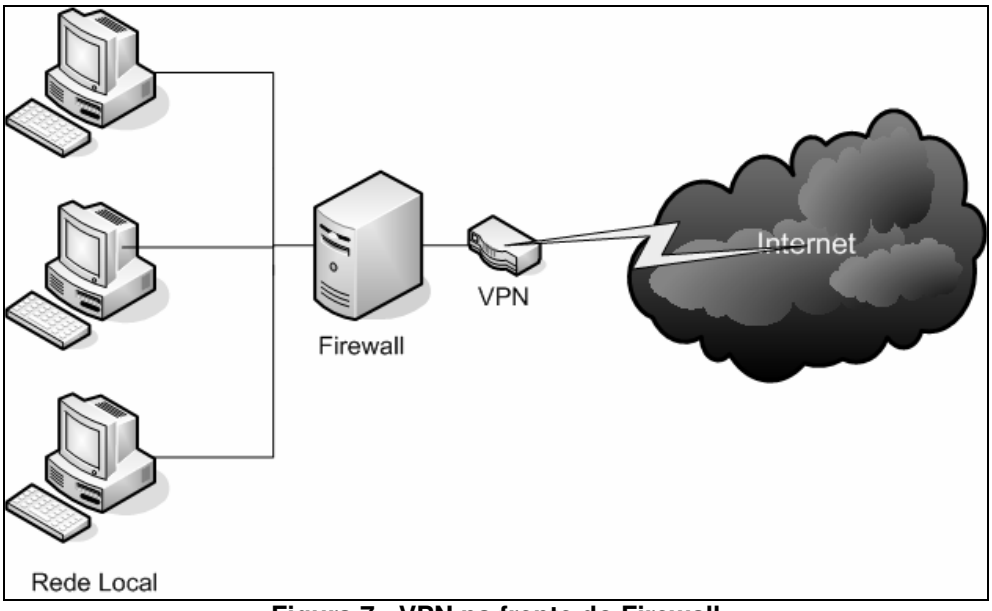


Figura 7 - VPN na frente do Firewall

c. VPN atrás do Firewall

Este posicionamento (ver figura 8) resolve o problema de o servidor VPN ficar exposto, porém, para que o servidor VPN possa funcionar de maneira correta o firewall é obrigado a deixar passar todo o tráfego com destino ao serviço de VPN, deixando o servidor VPN vulnerável a ataques de negação de serviços ocasionando a indisponibilidade do serviço.

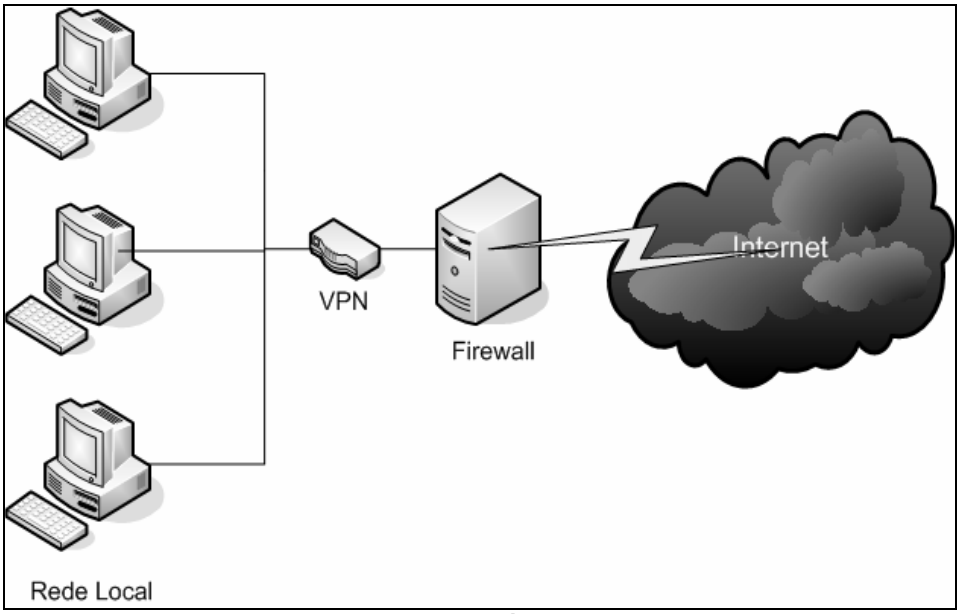


Figura 8 - VPN atrás do Firewall

d. VPN em paralelo com o Firewall

Este posicionamento (Ver figura 9) tem a função de dividir o que é tráfego de VPN e o que são os outros tráfegos, ou seja, a conexão VPN não passa pelo firewall.

O fato das conexões VPN não passarem pelo firewall cria uma grande probabilidade de que se um indivíduo que conseguir atravessar o servidor VPN, caia diretamente dentro da rede interna da empresa. Além desta desvantagem, este tipo de posicionamento requer complicado esquema de roteamento para separar os pacotes com destino a VPN dos outros pacotes, causando grandes aborrecimentos ao administrador da rede.

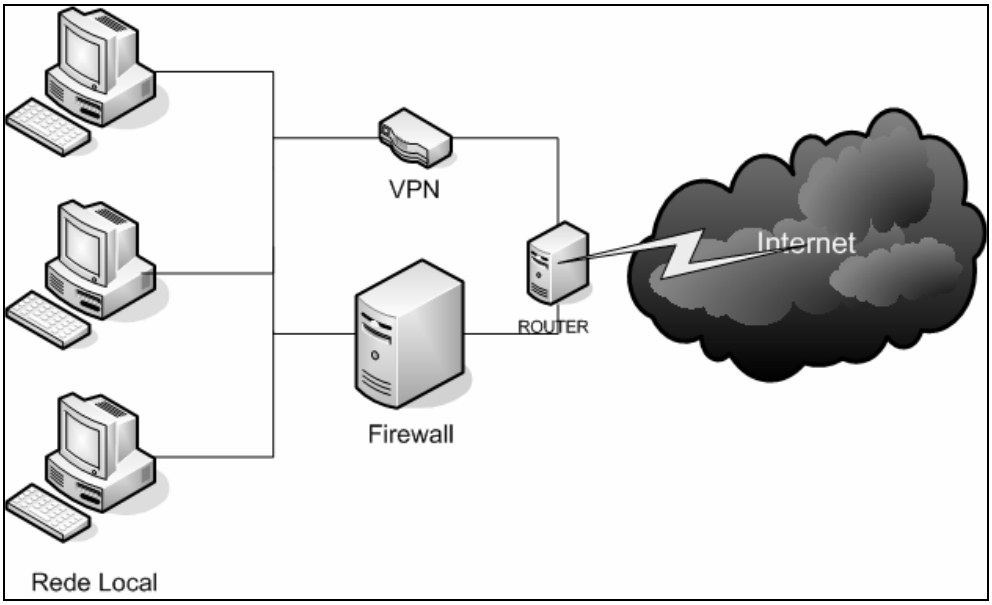


Figura 9 - VPN em paralelo ao firewall

e. VPN em uma interface do Firewall

A VPN em uma interface do Firewall (ver figura 10), também conhecida como DMZ (**de**-**m**ilitarized **z**one) que é uma interface do firewall que não está localizada fora da rede interna, porém, protegida pelo firewall. Os autores pesquisados concordam que em princípio este posicionamento é o mais seguro, pois, todo tráfego direcionado à VPN é desviado para esta interface externa, autenticado e depois retorna ao firewall que irá encaminhá-lo para a rede interna.

> Em uma necessidade de grande performance esta solução requer que o firewall tenha uma grande capacidade de processamento, pois se formos analisar todos os dados antes de atingirem seu destino final passam duas vezes pelo firewall, antes e depois de autenticados [SAR 03].

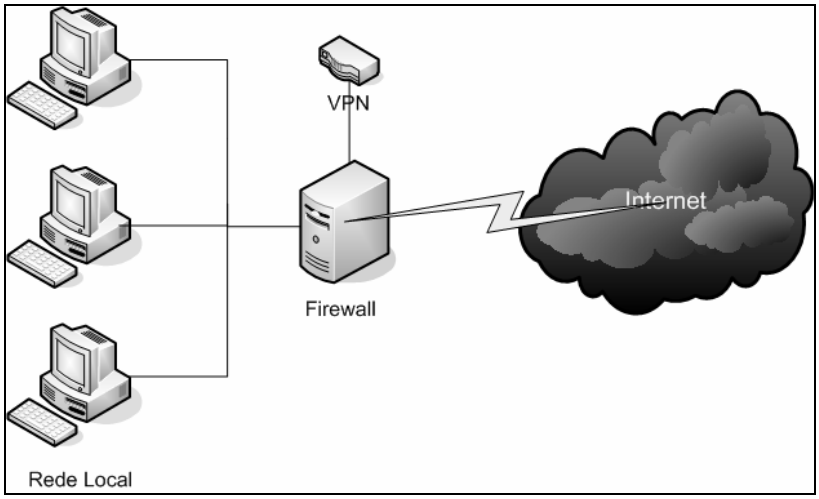


Figura 10 - VPN em uma interface DMZ

3.3.2. Criptografia

A privacidade no mundo virtual seguro esta diretamente ligada às técnicas de criptografia utilizadas, diferente da privacidade real a que estamos acostumados; tentar impedir que alguém capture um pacote que trafega em vários equipamentos como roteadores, switches e computadores é extremamente difícil, se não impossível, e só nos resta garantir certa privacidade na informação, embaralhando a informação de uma forma bem eficiente.

A criptografia foi uma técnica desenvolvida inicialmente pelos espartanos por volta do século V a.C. Eles cifravam e ocultavam a mensagem usando um pedaço de madeira, no formato de um bastão. Que se chamada skytalh (escútala) e uma tira de papel ou pano enrolada neste bastão onde a mensagem era escrita. A tira era desenrolada e enviava ao destinatário, que tinha outro bastão idêntico ao de origem. O receptor enrolava a tira no bastão que ele tinha e lia a mensagem. Se a tira ou a escútala fosse de tamanho diferente, a mensagem havia sido alterada e apareceria torta no destino.

O imperador romano Julio César, há mais de 2000 anos, inventou o método de criptografia por substituição. Ele passou a enviar mensagens a seus interlocutores trocando letras do alfabeto por três letras subseqüentes (A->D,B->E,C->F e assim por diante). Por exemplo, a mensagem:

Transmita esta mensagem à tropa, ficaria: Wudqvplwd hvwd phqvdjhp d wursd.

Isto foi possível, porque ele combinou com seu interlocutor antes a forma pela qual iria trocar cada caractere do alfabeto, ou seja, o segredo que iria utilizar para embaralhar a informação. Cada lado sabia como criptografar e descriptografar a informação. Como podemos perceber, esta técnica é extremamente simples, mas o importante aqui é o segredo ou chave de criptografia e como fazer com que os dois lados saibam como utilizá-la [SAR 03].

Existem dois tipos de chaves: chave simétrica ou chave secreta e chave assimétrica ou chave publica.

3.3.2.1. Criptografia simétrica

Na criptografia simétrica, a chave é compartilhada pelos dois pontos, ou seja, um destinatário sabe qual é a chave que utilizará para voltar a informação à sua forma original, ver figura 11.

Figura 11 - Representação de funcionamento da chave simétrica

A grande vantagem deste tipo de chave é a sua velocidade em relação ao uso de chave assimétrica.

Existe uma grande quantidade de algoritmos usados para criptografia, um dos mais antigos e conhecidos é o DES (Data Encryption Standard), padronizado pela ANSI (American National Standards Institute) em 1977, que utiliza chaves de comprimento de 64 bits, sendo 56 para a chave e 8 para paridade.

Desde a sua instituição oficial, até 1997, quase trinta anos se passaram em que o algoritmo do DES foi e tem sido submetido a todas as espécies de análises e ataques. Com exceção de duas quebras por força bruta, realizadas em ambiente puramente acadêmico, com isso pode se dizer que o DES cumpriu o seu papel para o qual foi destinado, até agora.

> Em 1997 o NIST (National Institute of Standard and Technology) iniciou um projeto chamado AES (Advanced Encryption Standard), que visa promover um substituto para o DES como modelo de algoritmo de criptografia padrão.
> E em 2 de dezembro de 2001 anunciou que o algoritmo selecionado seria um chamado Rijndael, dos belgas Joan Daemen e Vicent Rijmen, que obteve a maior pontuação obtida pelos engenheiros do NIST.
> Esta nova geração de criptografia agrega fatores como combinação de segurança, desempenho, eficiência facilidade de implementação e flexibilidade em diversas plataformas de software e hardware [SAR 03].

3.3.2.2. Criptografia assimétrica

Criptografia assimétrica, mais conhecida como chave pública, basicamente a chave é dividida em duas partes: uma única e privada e não pode ser compartilhada

com ninguém, ela é usada para descriptografar algum dado e a outra parte é a publica, que deve ser disseminada para qualquer pessoa que queira enviar dados criptografados ao dono da chave.

Quando é necessário o envio de algum dado criptografado para alguém, pega-se a parte publica da chave e faz-se a criptografia e encaminha para o dono da chave publica que ao receber os dados usará sua chave privada para retornar o dado ao seu estado original.

Existem dois algoritmos que fazem este trabalho, sendo eles:

Diffie-Hellman – Que leva o nome de seus criadores, Whitfield Diffie e Martin Hellman. O objetivo deste algoritmo é prover uma maneira rápida e eficiente de troca de chaves de criptografia, entre dois sistemas, baseada nas duas partes da chave (publica e privada) de cada interlocutor.

Por meio de um processo matemático a chave gerada por uma das partes usando sua chave privada e a chave publica de um outro interlocutor; serve para criptografar os dados a serem enviados e descriptografar os dados gerados por uma chave criada com a sua chave pública e a privada do outro interlocutor, ver figura 12.

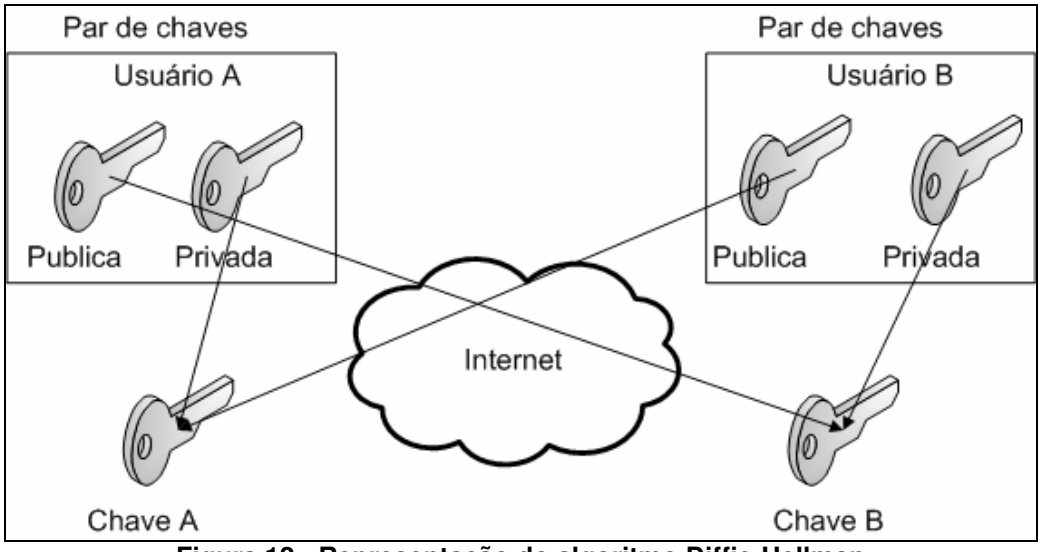


Figura 12 - Representação do algoritmo Diffie-Hellman

RSA – O RSA também leva o nome de seus inventores, Ron Rivest, Adi Shamir e Leonard Adleman. Este algoritmo é bastante utilizado na internet em diversos produtos, como browsers para acesso a páginas seguras, VPNs, serviços de E-mail (POPS, IMAPS) e outros. Este algoritmo não faz a geração de senhas, mas usa as chaves geradas previamente por uma infra-estrutura de chaves publicas

(PKI – Public Key Infrastructure), criptografando e descriptografando com o par de chaves de cada usuário, ver figura 13.

As chaves públicas podem ficar disponíveis na internet, administradas por órgãos certificadores ou CA (Certificate Authority), ou ficar em um servidor intranet para uso exclusivo de uma empresa [SAR 03].

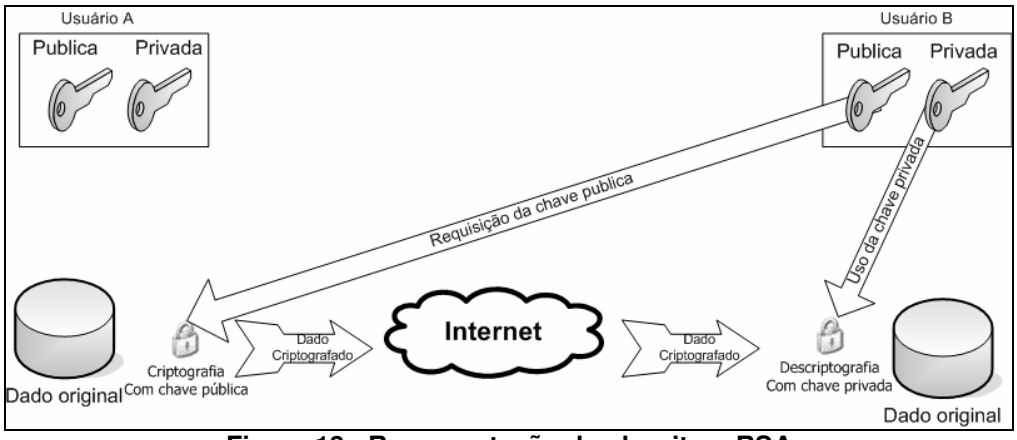


Figura 13 - Representação do algoritmo RSA

3.3.2.3. Assinatura digital

O modelo computacional que permita assinar digitalmente um documento deve permitir que o receptor possa verificar a identidade do emissor, deve controlar a assinatura de forma que o emissor não possa repudiar o conteúdo e possa evitar fraudes no próprio sistema. A assinatura digital utiliza a criptografia assimétrica, pois utiliza um par de chaves, uma pública e outra privada, a chave privada é usada para assinar o documento, enquanto a pública verifica a assinatura. Em termos práticos, todos os algoritmos de criptografia assimétrica podem ser utilizados para assinatura digital, porém o padrão adotado pelo mercado foi o RSA.

Para assinar um documento e mantê-lo em segredo e evitar que outros usuários possam lê-lo, é necessário não só assinatura digital, mas também a sua criptografia utilizando a chave pública do destinatário. Quando o documento é grande o processo de criptografia é demorado, isto aumenta o custo computacional. Para resolver este problema, utilizam-se funções Hashing que divide o documento em bloco fixo (128 a 512 bits) dependendo do algoritmo utilizado, gerando um Hash, criptografa-se o Hash gerado com uma chave privada, obtendo assim a assinatura digital.

A partir de um documento e sua assinatura digital, pode-se facilmente verificar sua autenticidade e integridade. Primeiro utiliza-se a mesma função Hashing aplicada ao documento na origem, obtendo assim o Hash do documento; depois se decifra a assinatura digital com a chave pública do remetente, que deve produzir o mesmo Hash gerado anteriormente. Com os valores Hash sendo iguais é determinado que o documento não foi modificado após a assinatura do mesmo, caso contrário, o documento ou a assinatura digital ou ambos foram modificados [JOA 03].

3.3.3. Certificado digital

Um certificado digital associa a identidade de uma pessoa ou processo, a um par de chaves criptográficas, uma pública e outra privada, que usadas em conjunto comprovam a identidade. O certificado digital é um arquivo assinado eletronicamente por uma entidade certificadora chamada Autoridade Certificadora (AC).
O conteúdo e a autenticidade de um certificado emitido por uma autoridade certificadora, podem ser examinados por qualquer entidade que conheça a chave pública da AC. O certificado digital é protegido pela assinatura digital do emissor, Autoridade Certificadora. No certificado existem 6 campos obrigatórios, número serial, algoritmo de assinatura, o emissor, validade, chave pública, assunto e campos opcionais, número da versão, dois identificadores e extensão.
A recomendação mais utilizada para emissão de certificados digitais é a X.509v3, descrita na [RFC 2459], formulada pela International telecommunication Union -
Telecommunication Standardization Sector (ITU-T), que introduziu as extensões (flags) que possibilita as autoridades certificadoras, utilizarem campos configuráveis [JOA 03].

3.4. Resumo do capítulo

Neste capítulo foram abordadas algumas ameaças que rondam a internet, as principais formas de defesas além de técnicas que reduzem os riscos como: firewall, criptografia de dados e certificados digital para proteção de informações.

4. Conceitos de VPN

Com o advento da internet, sua estrutura tem sido usada para interligar redes corporativas. O grande desafio está em garantir a segurança dos dados transmitidos, uma vez que a internet não prima pela segurança. Garantir principalmente que os dados não sejam modificados durante a transmissão, que as partes envolvidas na transmissão (origem e destino) sejam identificadas corretamente e manter o sigilo, isto é, não permitir que pessoas não autorizadas identifiquem o conteúdo da mensagem. A VPN surgiu com este propósito, garantir integridade, autenticidade, confidencialidade e controle de acesso, reduzindo o risco de ataques externos como, IP Spoofing e man-in-the-middle.

A VPN possui seus próprios protocolos de comunicação, dentre eles PPTP, L2TP e o IPSec, que atuam em conjunto com o TCP/IP, criando um túnel virtual onde os dados trafegam criptografados, garantindo a ilegibilidade dos mesmos à pessoas não autorizadas. Os protocolos de autenticação são usados, para garantir que as mensagens tenham vindo de usuários válidos e que se parte da mensagem for alterada, o pacote será descartado.

Algumas implementações de VPN utilizam software cliente nos computadores que se conectam a rede corporativa através da internet. Estas implementações são as chamadas VPDN (Virtual Private Dial Network), são ativadas pelo usuário após conexão com a internet através de software específico. Esta opção é muito usada por clientes móveis. Outras implementações utilizam criptografia entre gateways VPN, não sendo necessária intervenção do usuário e na maioria das vezes ele nem sabe que está usando VPN. Esta transparência permite que usuários, aplicações e computadores acessem recursos remotamente como se estivessem na rede local.

Pelo fato dos dados trafegarem criptografados em uma VPN, a localização de defeitos como, falhas de autenticação, a não sincronização das chaves, pacotes perdidos e sobrecarga do gateway VPN, pode ser um problema.

Outro ponto que deve ser bem planejado é a relação de confiança entre as redes, pois os recursos compartilhados de uma rede ficarão acessíveis à outra. Isso pode ocasionar falha de segurança na VPN, tornando-a vulnerável a ataques externos, caso uma das redes não possua uma segurança adequada.

As VPNs podem constituir uma alternativa segura na transmissão de dados através de redes públicas ou privadas, uma vez que oferecem recursos como autenticação e criptografia com níveis variados de segurança. Entretanto existem algumas aplicações em que o tempo de transmissão é crítico e que o uso de VPNs deve ser analisada com muito cuidado, pois podem ocorrer problemas com o desempenho ou atrasos na transmissão, comprometendo a qualidade do serviço oferecido [JOA 03].

4.1. Componentes de uma VPN

Uma rede VPN é formada geralmente por um conjunto de tecnologias, algumas das principais são:

4.1.1. Tunelamento

> O tunelamento foi desenvolvido inicialmente com o objetivo de possibilitar a comunicação entre organizações que utilizavam um determinado protocolo, por intermédio de um outro protocolo diferente. Por exemplo, pacotes IPX (Internet Packet Exchange) podem, pelo encapsulamento e pelo tunelamento, serem transmitidos por uma rede IP [NAK 02].

Os protocolos de tunelamento utilizados nas VPNs tratam o encapsulamento dos dados do usuário (payload) em pacotes IP. O tunelamento é importante, porque um túnel IP pode acomodar qualquer tipo de payload, e o usuário móvel pode utilizar a VPN para acessar, de modo transparente, a rede da organização, seja ela como base em IP, IPX ou em outros protocolos.

4.1.2. Criptografia dos dados

> A privacidade no mundo virtual seguro está diretamente ligada às técnicas de criptografia utilizadas diferentemente da privacidade real a que estamos acostumados. Tentar impedir que alguém capture um pacote que trafega em vários equipamentos como roteadores, switches e computadores é extremamente difícil, se não impossível, e só nos resta garantir certa privacidade na informação, embaralhando a informação de uma forma bem eficiente [SAR 03].

Os serviços de VPN utilizam a criptografia para criação de um túnel virtual entre os pontos de comunicação, proporcionando assim uma das premissas da VPN, que seria a privacidade.

Diversas tecnologias são empregadas para implementação do uso da criptografia, algumas requerem maiores recursos computacionais, isso depende um pouco do protocolo de VPN que se está utilizando, porém, o objetivo é sempre o mesmo.

4.1.3. Autenticação das extremidades

As mensagens são autenticadas para assegurar que elas vieram de usuários válidos, através da utilização de protocolos de autenticação, que geralmente implementam algoritmos hash. Desta forma, se alguma parte da mensagem for alterada durante a transmissão, o pacote é descartado.

Mesmo a mensagem estando encriptada, a razão de se autenticá-la deve-se ao fato da prevenção de ataques do tipo Replay.

4.2. Topologias

Basicamente existem três topologias possíveis para se implementar uma VPN, são elas:

4.2.1. Host-host

Esta é a topologia de VPN menos utilizada, serve para interligar dois computadores conectados à internet, de modo que as informações trocadas entre eles sejam protegias por um túnel. Sistemas operacionais Windows, versões Desktop, geralmente acompanham servidor e cliente para este tipo de VPN [SAR 03].

Ver figura 14 a seguir.

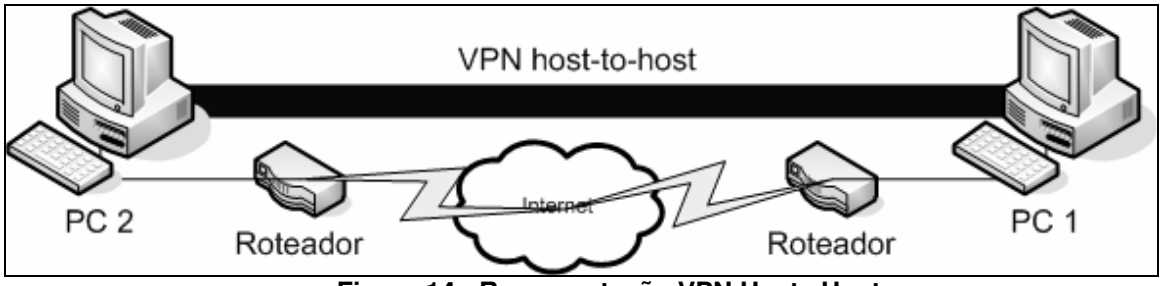


Figura 14 - Representação VPN Host –Host

4.2.2. Host-rede

Esta topologia, também chamada de client-to-gateway, esta VPN é usada para criar um túnel entre uma máquina de um colaborador, um laptop em um *hotspot (Acesso Wireless)* de aeroporto, por exemplo, à rede da empresa, neste caso o cliente inicia a conexão com o servidor VPN [NAK 02], [SAR 03].

Ver figura 15 a seguir.

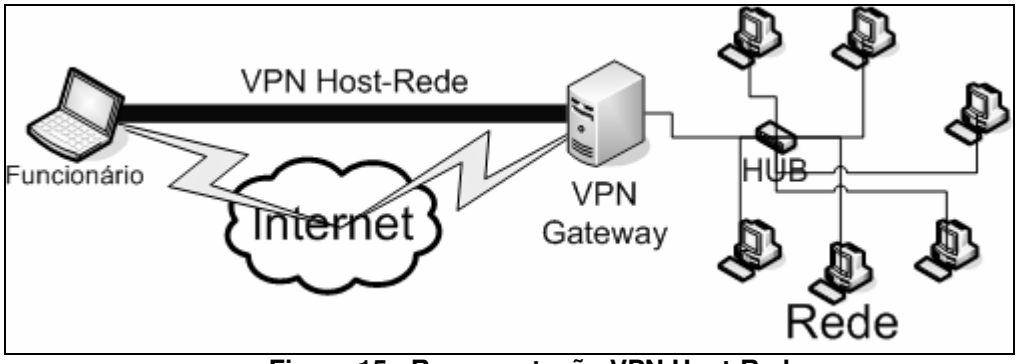


Figura 15 - Representação VPN Host-Rede

4.2.3. Rede-rede

> Topologia também é chamada de gateway-to-gateway e é usada para criar um túnel entre as redes da matriz e as filiais sendo que a conexão é transparente para os usuários [NAK 02], [SAR 03].

Ver figura 16, a seguir.

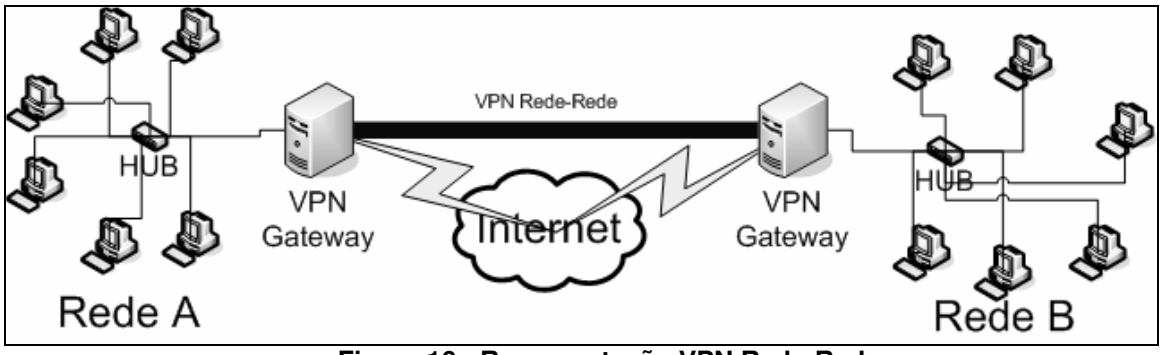


Figura 16 - Representação VPN Rede-Rede

4.3. Protocolos de VPN

> Os mecanismos de encapsulamento podem ser comparados no mundo real a uma carta com conteúdo, remetente e destinatário, porém, se esta carta estiver fora dos padrões dos correios, num padrão internacional por exemplo, ela precisa ser colocada dentro de um envelope devidamente preenchido para que chegue ao endereço destinatário e lá ser aberto e entregue [SAR 03].

Assim funciona a VPN, que encapsula os dados em um remetente como, por exemplo, IP inválido não roteável para a internet e o entrega a um destinatário que ira desempacotar os dados e entregar ao destinatário final.

Vários protocolos podem ser utilizados para se fazer uma rede baseada em VPN, alguns proprietários outros de código livre e disponível a qualquer um que necessite.

Existe um consórcio na internet chamado VPNC (Virtual Private Network Consortium) que foi fundado em 1999, que tem empresas conveniadas como: Microsoft, Broadcom, D-Link, SonicWall, Nokia, Nortel Juniper Networks e outros.

Este consórcio tem como objetivos principais a divulgação das tecnologias de VPN de seus membros e centralização de informações de tecnologias para futuros fabricantes.

De acordo com este consórcio, existem três principais protocolos de VPN que dominam o mercado, e que o VPNC comporta, são eles:

4.3.1. L2TP

L2TP é uma extensão do PPP (Point-to-Point Protocol), unindo características de outros dois protocolos proprietários: o L2F (Layer 2 Forwarding) da Cisco e o PPTP (Point-to-Point Tunneling Protocol) da Microsoft. É um padrão da IETF (Internet Engineering Task Force), descrito na [RFC 2661], que conta com a participação da Cisco e do PPTP fórum, entre outros líderes de mercado.

> O L2TP fornece a flexibilidade e escalabilidade do IP com a privacidade do Frame Relay ou ATM (Asynchronous Transfer Mode), permitindo que serviços de rede sejam enviados em redes roteadas IP. As decisões são tomadas nas terminações dos túneis ou VPNs, e comutadas sem a necessidade de processamento nos nós intermediários [RAP 03].

As seguintes vantagens são oferecidas pelo L2TP:

- Permite o transporte de protocolos que não o IP, como o IPX (Internetwork Packet Exchange, da Novell/Xerox) e o SNA, assim como outros protocolos dos terminais;
- Mecanismo simples de tunelamento para implementar funcionalidades de LAN e IP de forma transparente, possibilitando serviços de VPN IP de forma bastante simples;
- Simplifica a interação entre as redes do cliente e do provedor;
- Fácil configuração para o cliente.

Como mostra a figura 17, os roteadores R1 e R2 fornecem o serviço L2TP. Estes roteadores se comunicam por protocolo IP, através do caminho composto pela interface Int2, a rede IP e a interface Int3. Neste exemplo, os roteadores, R3 e R4 comunicam-se por interfaces POS (Packet-over-SONET) utilizando um túnel L2TP. O túnel Tu1 é estabelecido entre as interfaces Int1 de R1 e Int4 de R2. Qualquer pacote que chegue à interface Int1 de R1 é encapsulado pelo L2TP e enviado pelo túnel Tu1 para R2. R2. Então desencapsula o pacote e o transmite na interface Int4 para R4. Quando R4 precisa enviar um pacote para R3, o mesmo caminho, de forma inversa, é seguido.

Podemos fazer algumas observações a respeito da operação do L2TP:

- Todos os pacotes recebidos na interface Int1 serão redirecionados para R4. R3 e R4 não vêem a rede que está entre eles;
- O mesmo método é utilizado para interfaces Ethernet: qualquer pacote recebido da LAN1 por R1 na interface E1 será encapsulado

pelo L2TP e enviado pelo túnel Tu2 até a interface E2 de R2, ao que será transmitido para a LAN2.

- O mesmo vale para Frame-Relay: qualquer pacote recebido pela LAN1 por R1 em uma sub-interface será encapsulado pelo L2TP e enviado por um túnel até a sub-interface de R2, onde será transmitido na LAN2.

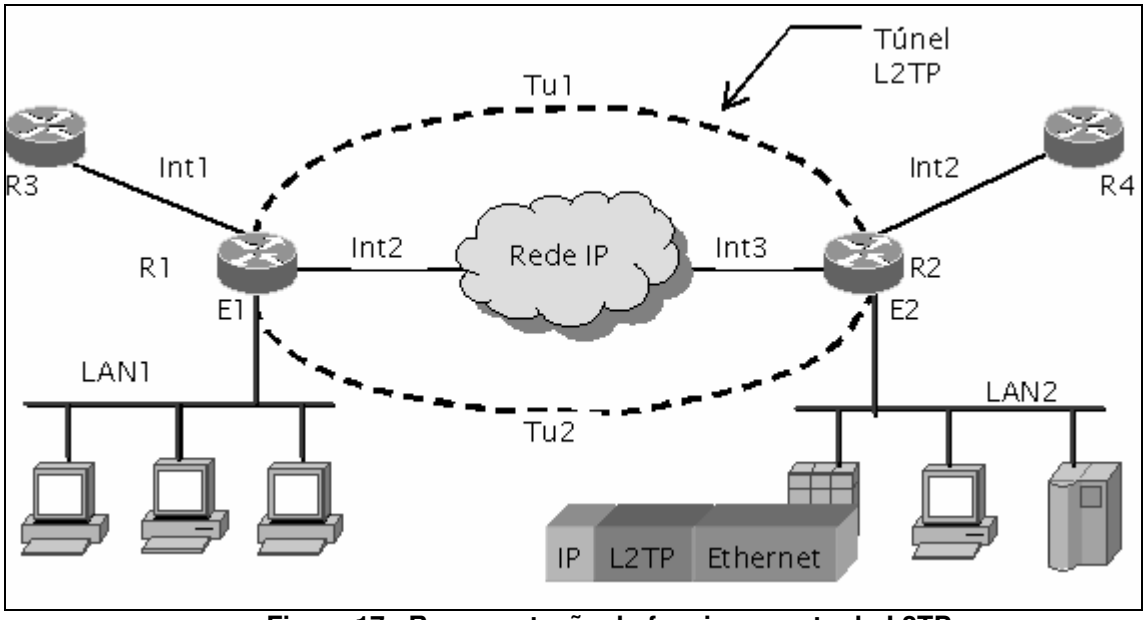


Figura 17 - Representação do funcionamento do L2TP

De acordo com este autor, o L2TP é um ótimo protocolo, que proporciona uma redução nos custos de comunicação entre a rede da empresa, filiais e fornecedores/consumidores.

4.3.2. IPsec

> O IPSec é um conjunto de padrões e protocolos para segurança relacionada com VPN sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security (IPSec) do IETF (Internet Engineering Task Force) descrito principalmente na [RFC 2401] e várias outras [ROS 00].

O IPSec especifica os cabeçalhos AH (Authentication Header) e ESP (Encapsulated Security Payload), que podem se utilizados independentemente ou em conjunto, de forma que um pacote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP) ou os dois cabeçalhos como mostra a figura 18.

Figura 18 - Estrutura do Pacote IPSec

Authentication Header (AH)

Utilizado para prover integridade e autenticidade dos dados presentes no pacote, incluindo a parte invariável do cabeçalho, no entanto, não provê confidencialidade.

Encapsulated Security Payload (ESP)

Provê integridade, autenticidade e criptografia à área de dados do pacote.

A implementação do IPSec pode ser feita tanto em Modo Transporte como em Modo Túnel.

4.3.3. SSL

Segundo [HOS 04], "há uma confusão entre a definição de um servidor de VPN SSL com túneis SSL". Os túneis criptografados que fazem a comunicação entre as aplicações, ele cita um dos casos mais comuns, o HTTPS.

Um servidor VPN SSL real não faz a comunicação de aplicações apenas na camada de aplicação e sim trabalha com o encapsulamento de todo o tráfego entre redes, trabalhando nas camadas 2 e 3 do modelo OSI.

Para as VPN SSL, não existe RFC específico, pois são usados todos os padrões impostos pela IETF no uso do SSL/TLS, [RFC 2246] e [RFC 4279].

Existem vários projetos atualmente que propõem uma VPN SSL real, como por exemplo: OpenVPN, VTun, Tinc, Cipe.

4.4. Vantagens e desvantagens

Uma das maiores vantagens em se implementar uma VPN é a redução de custo com o uso de serviços de rede oferecidos pelas

> operadoras de telecomunicações. Apesar disso, existem algumas desvantagens como consumir muito tempo para implementá-la, caso não haja um planejamento adequado, dificuldade na localização de defeitos, a relação de confiança entre as redes interconectadas e a disponibilidade da internet [ASS 04], [NAK 02], [SAR 03].

4.5. Comparação com outras tecnologias

Existem outras alternativas que antigamente eram mais utilizadas, porém, hoje seu uso é menos comum.

4.5.1. VPN x linhas dedicadas

As linhas dedicadas possuem um ótimo desempenho na transferência de informações entre a empresa e as filiais, porém seu custo, dependendo da disposição geográfica entre os pontos, pode chegar a um valor exorbitante e aumenta ainda mais quanto maior for a capilaridade da rede.

> Para a implantação de intercomunicações entre a matriz e as filiais com VPN e topologia rede-rede, o processo se torna muito mais barato, pois, atualmente grande parte das empresas possui um ponto de internet razoavelmente rápido, possibilitando assim a colocação de um gateway VPN para fechar um túnel entre as pontas. Com o uso de VPN, aumentar a capilaridade da WAN da empresa é muito mais simples e o custo é sensivelmente menor, pois basta ter um ponto de internet na filial para poder interligá-la a rede da empresa [SAR 03].

4.5.2. VPN x servidor de acesso remoto

Cada vez mais o uso de Servidor de Acesso Remoto (RAS) esta deixando de ser uma prática interessante para as empresas, pois além de um custo bastante elevado com o banco de modens, existe o custo com as ligações telefônicas para ter acesso à rede da empresa.

Com o uso de VPN e a topologia host-rede, para se ter acesso à rede da empresa, pode se usar uma conexão com um provedor local e fazer uma conexão virtual para o servidor de VPN da empresa, economizando assim também em custos de ligações no caso de colaboradores em viagem.

4.6. Resumo do capítulo

Este capítulo abordou conceitos gerais sobre VPN, comentando informações sobre seus componentes, tecnologias, principais protocolos, topologias utilizadas para implantação de VPN, suas principais vantagens e desvantagens e uma pequena comparação com outras tecnologias.

5. Método para implementação da solução proposta

Para desenvolvimento deste trabalho foi definido um método baseado em quatro etapas, são elas:

5.1. Etapa 1 - Pesquisas bibliográficas

Para o desenvolvimento do trabalho proposto houve a necessidade de uma pesquisa bibliográfica aprofundada em temas relacionados à conectividade via internet e com isso foi necessário resgatar conceitos vinculados, como protocolos de internet e segurança.

Além disso, depois de definida a situação problema, ou seja, a necessidade de prover acesso externo aos recursos computacionais da matriz, foi necessário fazer estudos de casos ocorridos em outras empresas com situação similar.

Foi observado que existem várias formas de se prover este tipo de acesso externo à rede interna da empresa como, por exemplo, Terminal Server, redirecionamento de portas no roteador para serviços internos (VNC, SSH, etc) e VPN.

5.2. Etapa 2 - Seleção da tecnologia

Para seleção da tecnologia mais apropriada foi criada uma lista de requisitos julgados indispensáveis para o uso na empresa.

Próximo passo executado para seleção foi à montagem de um ambiente de testes para testar a funcionalidade e características de cada uma das ferramentas elencadas.

O passo final foi à aplicação dos critérios para avaliação das ferramentas, a ferramenta que mais atendeu os critérios foi a escolhida.

5.3. Etapa 3 - Implementação da VPN

Definida a tecnologia a ser adotada na etapa anterior, foi dado início aos procedimentos para implementação da VPN.

Dentro da implementação alguns passos foram seguidos:

Primeiro passo foi a instalação do OpenVPN no servidor, nesta parte foi mostrada três formas de se fazer esta instalação, sendo duas em linux e uma em Windows.

Segundo passo foi a configuração dos servidores, dos gateways nas filiais e a configuração para usuários.

Terceiro passo foi a distribuição dos arquivos necessários para que os usuários pudessem acessar a VPN da empresa.

5.4. Etapa 4 - Análise de Utilização da VPN

Nesta etapa foram utilizadas algumas ferramentas de monitoramento e o desenvolvimento de uma ferramenta para análise de log de conexões, com isto foi possível analisar dois itens: transferências de dados e número conexões dos usuários.

5.5. Resumo do Capítulo

Neste capítulo, apresentou-se o método empregado para seleção, implementação e análise da VPN em um ambiente cooperativo. Este método está dividido em quatro etapas distintas e relacionadas entre si e utiliza um conjunto de procedimentos para estudo, seleção, implementação e avaliação da alternativa mais adequada de tecnologia de VPN, empregada na empresa ESSS.

6. Seleção da tecnologia mais adequada

Para selecionar uma solução adequada para implantação em ambiente cooperativo foram elencadas algumas tecnologias das que mais foram referenciadas na pesquisa a sites e fóruns de TI.

Em um ambiente de testes foram testados alguns requisitos.

6.1. Requisitos da solução adequada para ser implantada

Alguns requisitos testados:

- Total compatibilidade com os sistemas operacionais utilizados;
- Poucas ou nenhumas referências de falhas de segurança, nos sites que foram pesquisados;
- Facilidade de uso pelos usuários envolvidos;
- Segurança oferecida pela ferramenta;
- Facilidade de manutenção da ferramenta;

6.2. Características do ambiente de testes

Para não afetar máquinas ou servidores de trabalho que estão em produção dentro da empresa, foi criado um ambiente de testes isolado utilizando um computador com baixos recursos, como ambiente de teste com sistema operacional linux e em uma máquina com recursos relativamente bons. Foi instalado, em um ambiente Windows, um programa capaz de criar uma máquina virtual com a possibilidade de instalar um sistema completamente isolado, não causando assim nenhum impacto na máquina hospedeira.

Para que o sistema operacional que estava rodando dentro da máquina virtual criada pudesse ter conectividade para testes entre os sistemas operacionais linux e Windows, foi instalada uma segunda placa de rede no computador e interconectado ao computador com linux por meio de um cabo Cross-Over.

A máquina em que foi instalado o sistema operacional linux possuía a seguinte configuração:

- Processador Dual Pentium II 350MHz;
- 512Mb de RAM;
- Placa de rede;

- 20GB de disco;

- CD-ROM;

- Placa de vídeo.

Para manter uma compatibilidade com o servidor final onde foi implantado o gateway VPN, foi instalado o mesmo sistema operacional, Fedora Core 4 com as mesmas atualizações.

A máquina que possuía sistema operacional Windows e que foi instalado o software para criar uma máquina virtual possuía a seguinte configuração:

- Processador Athlon XP 2000+;

- 1GB de RAM;

- Duas placas de rede;

- 80GB de disco;

- Gravador de DVD;

- Placa de vídeo.

O sistema operacional já instalado na máquina que abrigou a máquina virtual utilizada para testes foi Windows XP, o mesmo instalado na máquina virtual, pois todos os usuários da empresa utilizam este sistema.

O Software utilizado para criação da máquina virtual no qual hospedou o ambiente Windows foi o software VMWare Workstation 5.0 [VMW 06]

6.3. Descrição das ferramentas elencadas

Foram selecionadas três ferramentas capazes de operar ambos em Windows e em linux, sistemas operacionais utilizados na empresa ESSS.

Segue abaixo a descrição de cada uma:

OpenSWAN – Solução baseada no protocolo IPSec para servidores baseados em sistemas UNIXs (Linux, FreeBSD, Solaris).

PoPToP – Solução baseada no protocolo PPTP para servidores linux.

OpenVPN – Solução de VPN baseada no protocolo SSL/TLS.

6.4. Aplicação dos critérios pré-estabelecidos

Com os critérios de avaliação pré-estabelecidos e o ambiente de testes que possuía os sistemas operacionais envolvidos, foram aplicados os critérios para a seleção da ferramenta mais apropriada.

Avaliação do OpenSWAN

Critério 1	**Total compatibilidade com os sistemas operacionais utilizados.**
	Como aplicação servidor, apesar de o OpenSWAN ter sido especialmente desenvolvido para sistemas operacionais Linux, foi observado que por ele ser uma aplicação que fica incorporada ao kernel do sistema é necessário aplicar um patch ao source do kernel linux e fazer uma compilação de kernel para sua utilização. Como aplicação cliente, no linux é necessário fazer os mesmos passos para utilização do server e em windows não existe compilação desta ferramenta, porém, é possível utilizar o próprio cliente de IPSec nativo do Windows, apesar de não ser uma tarefa trivial.
Critério 2	**Poucas ou nenhumas referências de falhas de segurança, nos sites que foram pesquisados.**
	Foram encontradas algumas vulnerabilidades conhecidas apenas em versões bem antigas, em versões mais recentes nada foi constatado.
Critério 3	**Facilidade de uso pelos usuários envolvidos.**
	Em sistemas operacionais linux: nada trivial o uso como cliente de VPN. No sistema operacional Windows: apesar de ser possível utilizar o cliente nativo de IPSec, existe uma série de procedimentos a serem realizados para se configurar o cliente.
Critério 4	**Segurança oferecida pela ferramenta.**
	Oferece toda a segurança estabelecida pelo protocolo IPSec, porém, [HOS 04] comenta que o IPSec pode ser bastante vulnerável se houver erros de configuração, que costuma ser bastante complexa.
Critério 5	**Facilidade de manutenção da ferramenta.**
	A ferramenta OpenSWAN propriamente dita, não possui empecilhos quanto a sua manutenção, a não ser o fato de a cada atualização de kernel do sistema operacional linux ser necessário a aplicação do patch de implementação do OpenSWAN.

Tabela 1 - Avaliação da ferramenta OpenSWAN

Esta ferramenta é bastante conhecida na área de TI com linux, porém, para o uso da empresa ESSS iria ser uma implantação árdua, principalmente para manutenção, já que a cada atualização do sistema operacional seria novamente necessária a aplicação do patch para o kernel.

Avaliação do PoPToP

Critério 1	**Total compatibilidade com os sistemas operacionais utilizados.**
	Como aplicação servidor, por ser uma implementação opensource de um protocolo proprietário da Microsoft, ele não vem de forma nativa em nenhuma distribuição linux encontrada e em sua instalação é necessário a compilação de um módulo de kernel. Como aplicação cliente, o poptop é apenas server, mas como é uma implementação do protocolo PPTP, no windows é possível se conectar a este servidor apenas criando uma nova conexão dial-up e escolhendo a opção de se conectar a um servidor de VPN.
Critério 2	**Poucas ou nenhumas referências de falhas de segurança, nos sites que foram pesquisados.**
	No site da [SEC 06] existe uma grande quantidade de vulnerabilidades encontradas no protocolo PPTP e também na ferramenta PoPToP
Critério 3	**Facilidade de uso pelos usuários envolvidos.**
	Em sistema operacional Windows, como implementa protocolo PPTP, a ferramenta cliente é nativa do sistema, em ambiente Linux existe uma ferramenta chamada pptp-client que se conecta com sucesso no servidor PoPToP.
Critério 4	**Segurança oferecida pela ferramenta.**
	Oferece autenticação de usuário e senha com o protocolo MS-CHAPv2, que utiliza método de pergunta e resposta para autenticar o usuário e oferece criptografia dos dados com MPPE (Microsoft Point to Point Encriptation).
Critério 5	**Facilidade de manutenção da ferramenta.**
	Apesar de a ferramenta requisitar um módulo que deve ser compilado junto ao kernel do linux, o autor da ferramenta disponibiliza uma série de programas que auxiliam nesta compilação, porém, é sempre necessário ter que refazer a compilação a cada atualização do kernel do linux.

Tabela 2 - Avaliação da ferramenta PoPToP

Apesar desta ferramenta ser comentada como insegura, se a utilização dela não for para casos que necessitem de segurança dos dados, sua utilização é bastante interessante pois é bem simples sua configuração tanto no servidor, quanto no cliente sendo utilizada até por universidades como [UFS 06].

Por questões de requisitos exigidos no planejamento é requerido um nível um pouco mais elevado de segurança. Portanto esta solução também não foi selecionada.

Avaliação do OpenVPN

Critério 1	**Total compatibilidade com os sistemas operacionais utilizados.**
	Por ser uma ferramenta de código aberta e desenvolvida com uma linguagem bastante popular, esta ferramenta é de fácil portabilidade em qualquer sistema operacional. Além disso, o autor da ferramenta disponibiliza compilações em Linux e Windows, sendo que em Windows a ferramenta tem total integração com o ambiente, facilitando assim sua utilização pelos usuários.
Critério 2	**Poucas ou nenhumas referências de falhas de segurança, nos sites que foram pesquisados.**
	Na versão 2.x não foi encontrada nenhuma referência de vulnerabilidade na ferramenta, a não ser no uso de uma ferramenta auxiliar para gerenciar conexões, que sua vulnerabilidade é aceitar conexões sem uso de autenticação, que pode ser contornada restringindo acesso a porta de comunicação por um determinado IP.
Critério 3	**Facilidade de uso pelos usuários envolvidos.**
	Esta solução é bastante simples de se utilizar existindo inclusive a possibilidade de customizar um pacote de instalação de acordo com as necessidades da empresa. Com o auxílio de um sistema para deployment dos certificados digitais e do arquivo de configuração para o usuário só precisa dar um duplo click e digitar seu usuário e sua senha.
Critério 4	**Segurança oferecida pela ferramenta.**
	Esta ferramenta possibilita todos os recursos do SSL (Secure Socket Layer), podendo oferecer criptografia dos dados com elevados níveis. Possibilita uso de certificados digitais para autenticação, uso de senha e uma versão, que na época deste trabalho estava em testes, possibilitava em ambiente Windows o uso de SmartCard para autorização dos clientes.
Critério 5	**Facilidade de manutenção da ferramenta.**
	Ferramenta completamente independente do sistema operacional em que esta instalada, não havendo necessidade de nenhum procedimento quando há atualização do kernel no Linux.

Tabela 3 - Avaliação da ferramenta OpenVPN

Por ter preenchido todos os requisitos estipulados e ainda ter oferecido recursos para a customização e distribuição da ferramenta aos usuários, o OpenVPN foi escolhido como a solução mais adequada a ser implementada empresa ESSS.

Os procedimentos de como instalar, configurar e o desenvolvimento de ferramentas auxiliares ao processo de implantação e gerência da VPN estão descritas no capitulo a seguir.

6.5. Resumo do Capítulo

Neste capítulo foram descritos os procedimentos para a seleção da tecnologia de VPN mais adequada e também os critérios que foram levados em consideração para a implantação dentro da empresa ESSS.

7. Implementação de uma VPN em um ambiente cooperativo

7.1. Cenário

Como representado na figura 19, o cenário encontrado na empresa ESSS conta com três escritórios localizados nas cidades de Florianópolis, São Paulo e Rio de Janeiro.

Na cidade de Florianópolis, onde é localizada a matriz, a empresa conta com uma estrutura bem desenvolvida em termos de recursos computacionais, incluindo um cluster com 12 máquinas com dois processadores cada, que são usadas por um software que faz processamento matemático de casos de mecânica de fluídos (CFD).

Além disso, nela se encontra servidores de arquivos, o servidor de intranet e outros servidores de aplicações usados no dia-a-dia da empresa. A empresa, por estar localizada em um parque tecnológico importante, possui um serviço de internet consideravelmente rápido, estando ligado diretamente no backbone da FAPESC (Fundação de Apoio a Pesquisa Científica).

No escritório de São Paulo, não existe nenhum recurso avançado para processamento matemático dos casos de CFD, logo o pessoal da área de engenharia necessita de alguma maneira acessar este cluster em Florianópolis. Por também estar localizado dentro de um centro empresarial, o escritório de São Paulo já possui um link de internet de 512Kbps.

O escritório do Rio de Janeiro foi montado dentro das dependências de um dos grandes clientes da empresa e usufruí das suas instalações, o que é certa comodidade, já que este cliente possui uma grande infra-estrutura de TI.

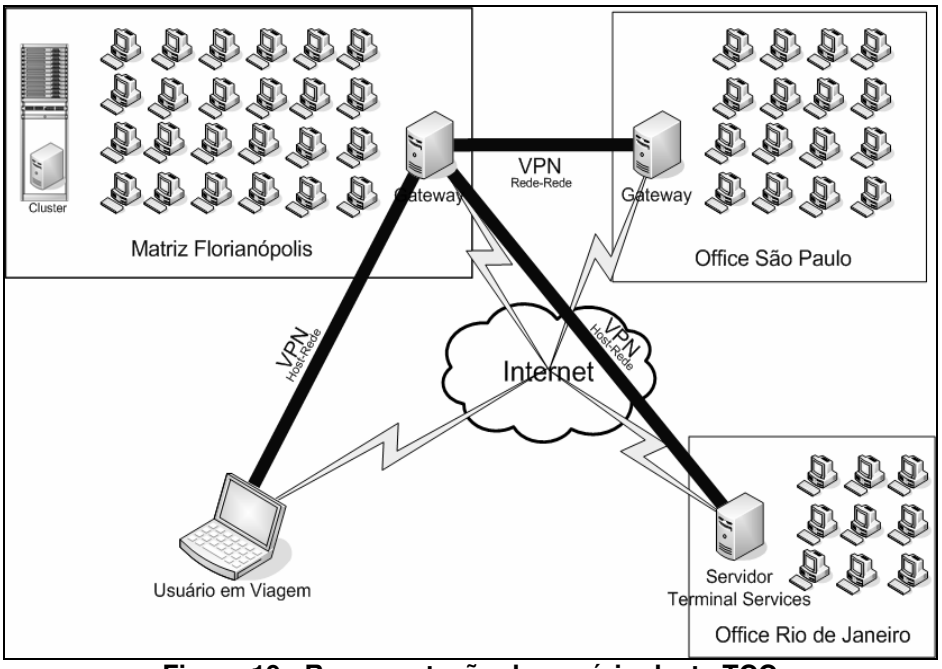


Figura 19 - Representação do cenário deste TCC

7.2. Implementação

Existem várias maneiras de se instalar o OpenVPN, tudo depende do sistema operacional no qual se está instalando ou da distribuição, caso se o sistema operacional seja Linux. Esta ferramenta pode ser baixada do site de seu desenvolvedor no formato de código fonte ou também em um pacote binário, pronto para instalação. Neste trabalho serão mostrados 3 formas de instalação do OpenVPN, sendo uma em Windows e duas em Linux.

O processo de implantação da VPN na empresa ESSS foi realizado em três etapas distintas: instalação, configuração e distribuição. Que serão descritas a seguir:

7.2.1. Instalação do OpenVPN a partir do código fonte

No ambiente de testes, descrito no capitulo anterior, foi usado o código fonte da aplicação, realizado download em [OPE 06], para isso foi necessário ter um compilador C++ e um conjunto de ferramentas necessárias, para efetuar a compilação do OpenVPN.

Para a compilação do OpenVPN foi necessário executar os procedimentos padrões na compilação de aplicações baseadas em “configure builds”, que é uma

script que monta o que é necessário na máquina em que o sistema vai ser compilado.

Os procedimentos para instalação do OpenVPN, usados na máquina de testes tiveram os seguintes passos:

a. Descompactando o código fonte da aplicação.

Após baixar a aplicação do site [OPE 06] e colocá-la no diretório /root, foi executado o seguinte comando para descompactar o pacote:

```
[root@fedora4 ~]# tar xzvf openvpn-2.0.7.tar.gz
```

A execução do comando acima, resultou na criação de um diretório chamado openvpn-2.0.7, onde continha todo o código da aplicação.

b. Preparando os arquivos para compilação.

Como a maioria das aplicações baseadas em opensource, o OpenVPN vem acompanhado de um script que faz a validação das bibliotecas necessárias para sua compilação, sendo executado da seguinte forma:

```
[root@fedora4 openvpn-2.0.7]# ./configure
```

A execução do comando acima, deu início a uma série de testes e verificações necessárias para instalação do OpenVPN.

c. Compilação da aplicação

Após a preparação dos arquivos, para compilar a aplicação foi usado o comando “make”, que é uma ferramenta que lê os scripts criados pelo “configure” e passa os parâmetros necessários para o compilador gerar o arquivo binário necessário para rodar a aplicação.

```
[root@fedora4 openvpn-2.0.7]# make ; make install
```

O comando “make install”, usado após o “make”, é utilizado para que os arquivos gerados pelo comando “make” sejam colocados nos diretórios finais, onde eles serão executados.

7.2.2. Instalação do OpenVPN com gerenciador de software YUM

Como foi citado anteriormente, existem várias maneiras de se instalar o OpenVPN, uma outra maneira de se instalar o OpenVPN é por meio de pacotes pré compilados, que na distribuição Linux utilizado é o RPM.

No servidor definitivo foi utilizada uma outra abordagem de instalação, como em servidores é muito importante que haja sempre atualizações das aplicações, conforme elas são disponibilizadas pelos desenvolvedores, na distribuição Fedora 4 existe um sistema de instalação e atualizações dos programas, chamado YUM.

Seu modo de funcionamento é bem simples e para instalar o OpenVPN no servidor definitivo bastou executar o seguinte comando:

```
[root@ironman ~]# yum install openvpn
```

O YUM se encarrega de baixar os últimos pacotes da aplicação, bem como todas as dependências necessárias. Este tipo de ferramenta, comum nas distribuições de linux mais conhecidas, é uma ótima opção para se manter sistemas atualizados e com maior segurança contra bugs.

7.2.3. Instalação do OpenVPN em Windows

A instalação em ambiente Windows, para utilização pelos funcionários que estão em viagem ou em suas casas, se tornou ainda mais fácil devido a possibilidade do OpenVPN incorporar uma ferramenta que possibilita customizar a sua instalação em ambiente windows, conforme figura 20, sendo possível a pré-escolha das opções a serem instaladas, exigindo assim do usuário final apenas clicar nos botões de “Next” e “Finish”.

É possível, nestas customizações da instalação do OpenVPN, empacotar até os certificados e as configurações pré definidas para cada usuário, porém, isso exigiria um grande trabalho manual da área de TI. Será visto na seção “Distribuição

(Deployment)", a solução desenvolvida para automatizar a criação das configurações para todos os usuários individualmente, sem que o mesmo tenha a necessidade de editar algum arquivo.

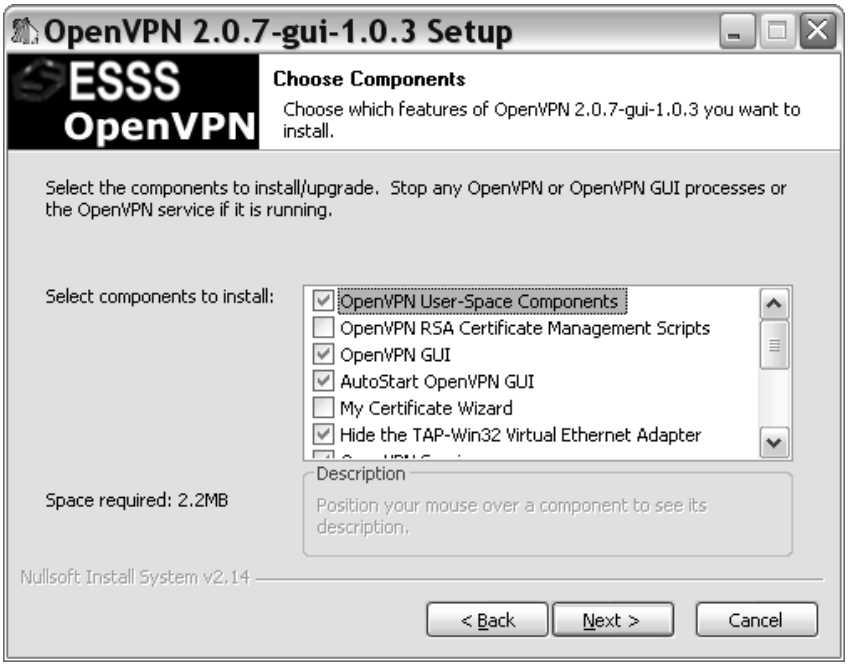


Figura 20 - Instalação do OpenVPN customizada para empresa ESSS

7.3. Configuração do OpenVPN

A configuração do servidor VPN é relativamente simples, bastando editar um arquivo texto com alguns parâmetros de configuração.

Por padrão, em sistema operacional linux, o arquivo de configuração do OpenVPN tem a extensão ".conf" não importando o seu nome, já que é possível ter várias instâncias de servidor VPN rodando na mesma máquina e trabalhando com configurações completamente diferentes, como foi utilizado na empresa ESSS para utilização de usuários em viagem e intercomunicação de escritórios.

Optou-se por esta separação entre o servidor VPN que iria atender as requisições de funcionários e o servidor que iria interconectar os escritórios da empresa, para haver uma distinção nos métodos de autenticação, já que para conectar servidores de forma automática não seria possível exigir uma senha de usuário toda vez que a conexão VPN fosse estabelecida.

Inicialmente para fazer esta separação foi necessário criar duas CAs (Autoridades Certificadoras), para que nenhum funcionário consiga se conectar na VPN que interconecta os escritórios apenas utilizando o certificado digital, sem usar seu login e senha.

Para gerenciar estas CAs foi utilizado um conjunto de ferramentas disponibilizados pelo OpenVPN, chamado EASY-RSA. Sua configuração e seu funcionamento serão descritos a seguir.

7.3.1. Configuração da CA para servidores

O primeiro passo foi a cópia do conjunto de ferramentas Easy-RSA para um diretório especifico:

```
[root@ironman ~]# cp -rp /usr/share/openvpn/easy-rsa/2.0/ \
/home/institucional/pki/easy-rsa-servers
```

Dentro do diretório /home/institucional/pki/easy-rsa-servers existe um arquivo chamado “vars” que deve ser configurado com os dados necessários para criação da CA. A seguir visualizaremos como ficou o arquivo e o que significa cada linha:

```
##################### arquivo vars#########################
export EASY_RSA="/home/institucional/pki/servers"
# Variavel EASY_RSA é a raiz de onde irão ficar os certificados
export KEY_CONFIG="$EASY_RSA/openssl.cnf"
#KEY_CONFIG é o arquivo de configuração do openssl, mais a frente será
#mostrado quais modificações devem ser feitas desse arquivo.
export KEY_DIR="$EASY_RSA/keys"
#KEY_DIR é o diretório que serão armazenados os certificados e também a #CRL,
que é onde ira ficar a lista de certificados revogados.
export KEY_SIZE=1024
#KEY_SIZE é o tamanho da chave de criptografia
export CA_EXPIRE=3650
#CA_EXPIRE é o tempo em que a CA ira expirar após a sua criação
export KEY_EXPIRE=365
#KEY_EXPIRE é o tempo que os certificados irão expirar após a sua criação,
#quando eles expiram eles devem ser revogados e colocados na CRL.
# as configurações abaixo são dados necessários para identificação da CA
export KEY_COUNTRY=BR
export KEY_PROVINCE=SC
export KEY_CITY=Florianopolis
export KEY_ORG="ESSS Ltda"
export KEY_EMAIL=fred@esss.com.br
```

Dentro do pacote de ferramentas de gerenciamento há um arquivo chamado openssl.cnf, que deve ser colocado dentro do diretório especificado com a variável EASY_RSA. Nele, o único parâmetro que foi modificado foi a variável “crl” que especifica o nome do arquivo que conterá a chave para revogação de outros certificados.

Após este procedimento foi dado início a CA, bastando executar um comando "source vars" para carregar as variáveis necessárias, executar o script "clean-all" para limpar do diretório de certificados e iniciar o índice de certificação. Depois executar um script do Easy-RSA chamado build-ca, como mostrado abaixo:

```
[root@ironman easy-rsa-servers]# source vars
[root@ironman easy-rsa-servers]# ./clean-all
[root@ironman easy-rsa-servers]# ./build-ca
```

Este comando criará a estrutura inicial da CA, com sua chave publica e privada, que serão usadas para assinar outros certificados.

Para aumentar a segurança durante a autenticação das VPN, será usado uma chave **Diffie-Hellman** e para isso é necessário também criá-la no Easy-RSA, utilizando o comando a seguir:

```
[root@ironman easy-rsa-servers]# ./build-dh
```

Feitos os procedimentos citados, já é possível criar e assinar certificados digitais com a CA para servidores e o próximo passo é a criação dos certificados do servidor principal.

Para criar os certificados e já assiná-los pela CA é utilizado o comando "pkitool", como mostrado abaixo:

```
[root@ironman easy-rsa-servers]# ./pkitool --server servers
```

O parametro "--server" é usado na criação de certificados dos servidores de VPN, pois isso marca os certificados para serem rodados apenas em servidores.

7.3.2. Configuração da CA para usuários

O procedimento para criação da CA responsável pelo controle de certificados de funcionários foi semelhante ao anterior, as únicas configurações que divergiram foram o diretório base dos certificados, que foi o /home/institucional/pki/certificates e o diretório da aplicação Easy-RSA, que foi o /home/institucional/pki/easy-rsa-users.

7.3.3. Configuração dos servidores

Após a instalação do OpenVPN e a criação da CA chegou o momento de configurar o arquivo de define o modo de funcionamento da VPN, o arquivo

server_clients.conf, que no caso deste servidor para funcionários, ficou da seguinte forma:

```
##################Configuração VPN Users###################
dev tap1
server 10.2.0.0 255.255.255.0
proto tcp-server
daemon
push "route 10.0.0.0 255.255.255.0"
push "route 10.1.0.0 255.255.255.248"
push "dhcp-option DNS 10.0.0.1"
push "dhcp-option WINS 10.0.0.1"
push "dhcp-option WINS 10.0.2.1"
push "dhcp-option NBT 2"
tls-server
dh /home/institucional/pki/certificates/keys/dh1024.pem
ca /home/institucional/pki/certificates/keys/ca.crt
cert /home/institucional/pki/certificates/keys/clients.crt
key /home/institucional/pki/certificates/keys/clients.key
crl-verify /home/institucional/pki/certificates/keys/crl.pem
ifconfig-pool-persist ipp.txt
reneg-sec 300
verb 5
client-to-client
keepalive 10 60
status openvpnstaus-clients.log 10
status-version 2
log-append /var/log/openvpn-clients.log
comp-lzo
tun-mtu-extra 32
persist-tun
persist-key
client-config-dir /etc/openvpn/ccd/
tmp-dir /tmp
auth-user-pass-verify /etc/openvpn/ldapauth.sh via-env
```

A descrição de cada parâmetro utilizado nesta configuração será mostrada a seguir:

Comando	Descrição
Dev	Parâmetro que especifica qual interface será utilizada para criação do tunelamento. Foi utilizada a forma fixa especificando a interface tap1, porém, poderia ter sido utilizada a forma dinâmica deixando apenas tap e o servidor se encarregava de enumerar as interfaces.
Server	Determina a classe de IPs que será distribuída pela VPN a seus clientes. A máscara de sub-rede delimita o tamanho da rede que estará disponível.
Proto	Determina o protocolo a ser utilizado pela comunicação entre

	o cliente e o servidor. Esta opção pode ser tanto TCP quanto UDP.
Daemon	Define que o servidor irá rodar em segundo plano, como a maioria das aplicações de serviços em linux.
Push	Executa uma ação no cliente, as duas primeiras linhas destas instruções foram para indicar nos clientes as rotas da rede ESSS e as rotas das VPN fixas entre os escritórios. As quatro linhas seguintes são de passagem de parâmetro para o DHCP do cliente, informado a ele qual o servidor DNS, os Servidores WINS e que esta rede trafega também protocolo NetBIOS do windows.
Tls-server	Este parâmetro indica que deverá ser estabelecida uma negociação de autenticação TLS em conjunto com a chave Diffie Hellman.
Dh	Indica onde está localizada a chave Diffie Hellman.
Ca	Indica onde está localizada a chave pública da Autoridade certificadora.
Cert	Indica onde está localizado o arquivo da chave pública criada para o servidor.
Key	Indica onde está localizada a chave privada criada para o servidor.
Crl-verify	Indica onde está localizado o arquivo que faz o controle dos certificados digitais revogados pela CA.
ifconfig-pool-persist	Define um arquivo que vai ser gravado o login e o IP de cada usuário que se conectar a VPN. Esta configuração não vai ser muito utilizada, pois mais à frente será visto que cada usuário terá um IP fixo.
Reneg-sec	Faz a renegociação da chave de criptografia do canal seguro estabelecido.
Verb	Indica o nível de detalhamento deve ser gravado no log.
Client-to-client	Este parâmetro permite que clientes possam se conectar entre si com a rota pelo servidor.
Keepalive	Faz o servidor efetuar uma espécie de ping no cliente sendo o primeiro número a cadencia de pings e o segundo número o tempo de timeout.
Status	Grava informações de status de conexões no servidor, sendo o primeiro parâmetro o arquivo a ser gravado e o segundo o tempo em que deve ser regravada a informação.
Status-version	Indica que o formato do arquivo de status gravado devera ser compatível com a versão 2 do OpenVPN.
Log-append	Informação de onde será gravado o log do OpenVPN.
Comp-lzo	Habilita compactação de informação utilizando a biblioteca lzo, otimizando assim a transferência de informações entre o túnel da VPN.
Tun-mtu-extra	Especifica quantos bytes a interface retorna a mais do que o MTU (Maximum Transmission Units), ou seja, a máxima quantidade de bytes que podem ser transmitidos sem haver fragmentação de pacotes. Este valor de 32 é padrão para interfaces TAP.

Persist-tun	Mantém a interface ativa durante o restart do processo do servidor, geralmente utilizado modificar alguma configuração.
Persist-key	Mantém o mesmo certificado quando o servidor é reiniciado com SIGHUP.
Client-config-dir	Especifica um diretório onde estarão as configurações individuais de cada usuário. São nestas configurações individuais que será passado o IP fixo de cada um, bem como a informação de domínio de procura das máquinas, dependendo do escritório em que a pessoa está lotada.
Tmp-dir	Indica onde é o diretório de informações temporárias.
Auth-user-pass-verify	Este parâmetro indica qual o script que fará a validação dos usuários e senhas. Como a empresa dispõe de um servidor LDAP, os usuários serão validados a partir desta base. O script ldapauth.sh será descrito nas considerações sobre a implementação.

Tabela 4 - Lista de parâmetros da configuração dos Gateways VPN

A configuração do serviço de VPN para servidores das filiais, com o arquivo **server_servers.conf** ficou da seguinte forma:

```
##################Configuração de Servers ###################
dev tap0
server 10.1.0.0 255.255.255.248
port 2402
proto tcp-server
daemon
route-gateway 10.1.0.2
route 10.0.2.0 255.255.255.0
push "route 10.0.0.0 255.255.255.0"
push "route 10.2.0.0 255.255.255.0"
tls-server
dh /home/institucional/pki/servers/keys/dh1024.pem
ca /home/institucional/pki/servers/keys/ca.crt
cert /home/institucional/pki/servers/keys/servers.crt
key /home/institucional/pki/servers/keys/servers.key
reneg-sec 600
tun-mtu-extra 32
ifconfig-pool-persist ipp2.txt
crl-verify /home/institucional/pki/servers/keys/crl.pem
verb 5
keepalive 10 60
status openvpnstaus-servers.log 10
status-version 2
client-config-dir /etc/openvpn/ccd/
log-append openvpn-servers.log
comp-lzo
persist-tun
persist-key
```

A configuração do serviço VPN para funcionários e para o serviço VPN para conexão de servidores, é basicamente a mesma, porém neste segundo não existe o parâmetro para utilizar um script de verificação de usuário e senha, no caso este não é necessitado, pois haveria certo problema em todas as vezes que o serviço de VPN fosse estabelecido houvesse a necessidade de se digitar usuário e senha em um servidor.

7.3.4. Configuração dos servidores nas filiais

A configuração dos servidores nas filiais, que na prática são clientes de VPN só que localizados em gateways ou servidores de terminal remoto e não acessíveis para qualquer funcionário, ficou como mostrada abaixo:

```
####################Configuração VPN Filiais #############
remote vpn.esss.com.br
daemon
port 2402
proto tcp-client
resolv-retry infinite
dev tap0
client
tls-client
ca ca.crt
cert firewall-sp.crt
key firewall-sp.key
reneg-sec 60
verb 1
status openvpnstaus.log 10
status-version 2
log-append openvpn.log
keepalive 10 60
persist-key
persist-tun
tun-mtu-extra 32
comp-lzo
```

Será descrito apenas os parâmetros não citados na configuração dos servidores.

Comando	Descrição
Remote	Este parâmetro indica qual o endereço do servidor, pode ser colocado na forma de IP ou hostname.
Resolv-retry	Este parâmetro especifica por quantos segundos o OpenVPN tem que fazer a tentativa de reconexão após a perda. Especificando

	infinite ele irá sempre tentar se conectar ao servidor.
Client	Indica ao OpenVPN que ele é um cliente de um servidor multi-client.
Tls-client	Faz o OpenVPN assumir a posição de cliente TLS durante o estabelecimento da conexão.

Tabela 5 - Tabela de parâmetros diferenciais da configuração das filiais

É possível notar que existem poucas diferenças entre a configuração de um cliente de VPN ou um servidor, basicamente a diferença está em parâmetros que especificam quem vai originar a conexão e quem vai ficar "ouvindo" uma porta a espera de conexão.

7.3.5. Configuração dos funcionários para acesso a VPN

A configuração do OpenVPN para clientes, é criada de forma automática, através da ferramenta VPN Configurator, que será vista adiante. O arquivo de configuração gerado, pode ser visualizado abaixo:

```
###############Configuração para funcionários###############
client
dev tap
proto tcp-client
remote vpn.esss.com.br
port 1194
resolv-retry infinite
redirect-gateway def1
auth-user-pass
persist-key
persist-tun
ns-cert-type server
ca ca.crt
cert fred.crt
key fred.key
tls-client
comp-lzo
verb 3
```

Existem alguns parâmetros diferentes nas configurações do OpenVPN para funcionários em relação aos parâmetros dos clientes VPN das filiais, a descrição de cada um deles é mostrada abaixo:

Comando	Descrição
Redirect-gateway	É usado para forçar a rota default da máquina do funcionário a passar por dentro da VPN, fazendo com que pareça que a máquina esteja dentro da empresa. Esta é opcional, podendo

	não ser selecionada, como será visto no próximo sub-capitulo.
Auth-user-pass	Como no servidor para conexões funcionários é exigida autenticação com usuário e senha, além do certificado, este parâmetro serve para apresentar um prompt ao usuário solicitando login e senha.
Ns-cert-type	Como foi descrito no item referente a criação de CA para servidores usando o parâmetro –server. A configuração dos usuários com a utilização do parâmetro ns-cert-type força ao usuário a conectar-se apenas ao servidor que tem certificado digital de servidor e assinado pela mesma CA.

Tabela 6 - Tabela de descrição de parâmetros da configuração de funcionários

7.4. Distribuição (Deployment)

Para que os funcionários possam acessar a VPN da empresa ESSS alguns pré-requisitos são necessários:

- OpenVPN instalado na máquina que vai se conectar a VPN.
- Arquivo de configuração do OpenVPN com os parâmetros necessários.
- Certificado digital do funcionário (Chave pública e chave Privada).
- Chave pública da CA responsável pela validação dos certificados dos funcionários.

Para que estes pré-requisitos sejam disponibilizados de uma forma fácil e segura aos funcionários, alguns módulos tiveram que ser desenvolvidos dentro da intranet da empresa, que é uma área onde são oferecidos alguns serviços e que requerem a autenticação prévia do usuário.

7.4.1. Download OpenVPN

Com intuito de ter uma área comum para os usuários baixarem a aplicação necessária para a VPN, foi criada esta área onde estará disponível a versão mais atual e já customizada para a empresa. Na figura 21 é mostrada a interface de download do OpenVPN.

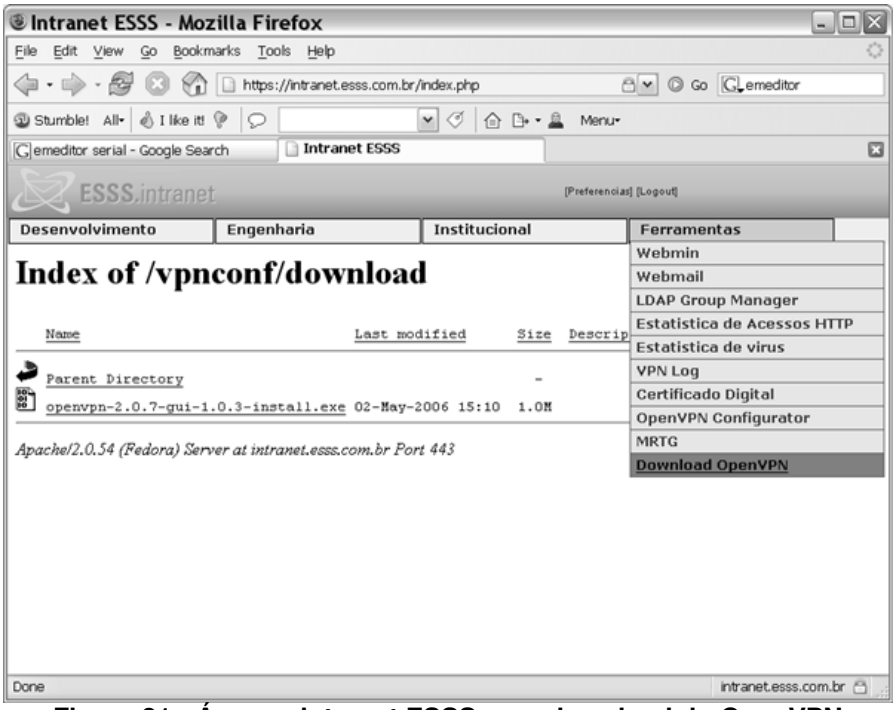


Figura 21 - Área na intranet ESSS para download do OpenVPN

7.4.2. VPN Configurator

O objetivo deste módulo é disponibilizar para o usuário uma forma mais simples possível para que ele possa obter o arquivo de configuração do OpenVPN.

Este módulo, além de já especificar diretamente como deve se chamar o arquivo do certificado digital do usuário no arquivo de configuração, também possibilita algumas customizações que dependem do lugar onde a pessoa está acessando a internet. Por exemplo, o usuário pode estar dentro de uma empresa que só permita acesso a internet via proxy. Portanto ele pode gerar uma configuração do OpenVPN que use este proxy.

Uma outra opção que pode ser customizada é a de ser direcionada a rota padrão da máquina pela VPN ou não, desta forma se o usuário optar por apenas conectar a VPN para acessar uma máquina interna e seu tráfego de internet continuar passando pelo local onde ele está. Ele escolhe esta opção antes de baixar a configuração. A figura 22 demonstra a interface apresentada ao usuário.

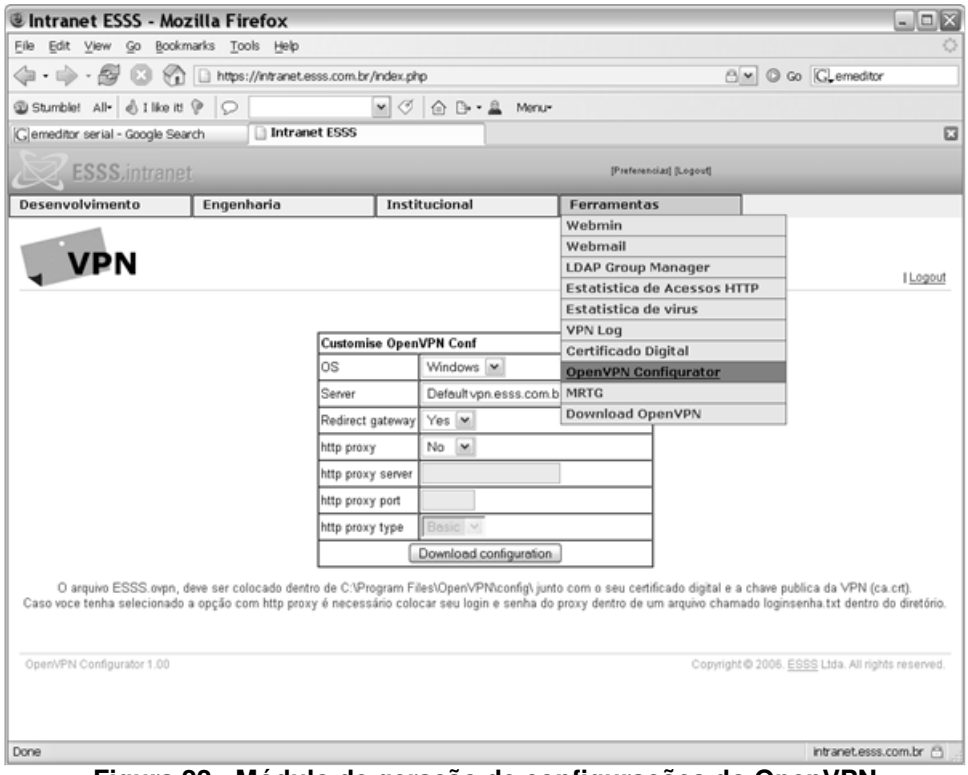


Figura 22 - Módulo de geração de configurações do OpenVPN

7.4.3. Certificado Digital

O certificado digital é constituído de dois arquivos: as chaves pública e privada. A chave pública pode ser visualizada por qualquer um, já a chave privada tem que ser de posse exclusiva de seu dono.

Este módulo foi desenvolvido para que apenas o próprio usuário possa baixar seu certificado, além disso, a intranet utiliza o servidor HTTPS impossibilitando que alguém possa se apropriar da chave privada durante sua transferência. A figura 23 apresenta a interface de download do certificado digital.

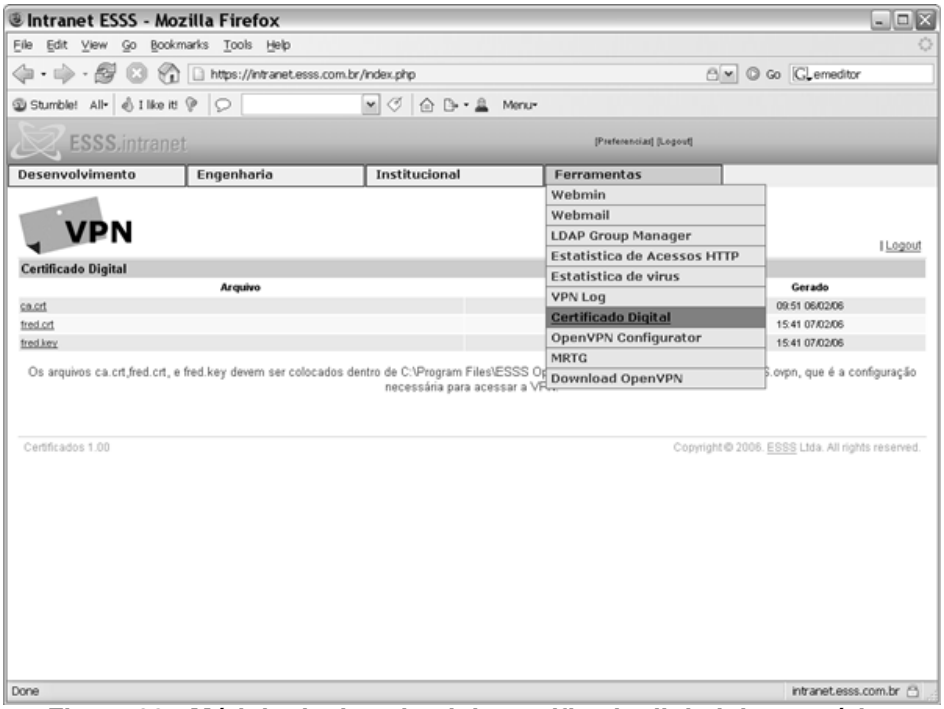


Figura 23 - Módulo de download do certificado digital dos usuários

7.5. Considerações sobre a implementação

Para a implementação da VPN, na empresa ESSS, alguns aspectos tiveram que ser considerados no planejamento.

7.5.1. Firewall

Para implementação da VPN na ESSS foi necessário escolher seu posicionamento em relação ao Firewall da empresa. Como a ESSS possuía um firewall implementado em Linux, optou-se por posicionar a VPN junto ao firewall. Com este tipo de posicionamento é possível implementar regras específicas de acesso para cada usuário da VPN.

Para esta implementação funcionar foi necessário fazer algumas modificações nas regras do firewall. São elas:

- Permitir o tráfego das interfaces tap0 e tap1 para a rede interna da empresa;
- Permitir conexão das duas portas dos serviços de VPN, porém a conexão na porta que é referente à VPN que interliga as filiais à matriz é permitida apenas de IPs específicos;

- Permitir que clientes conectados pela VPN pudessem acessar a internet, sendo o IP de saída mascarado pelo gateway da ESSS.

7.5.2. Autenticação dos usuários

Durante o planejamento da implementação da VPN optou-se por fazer uma autenticação de dois fatores conhecida como “dual-factor”, que é um método que combina dois elementos: O que o usuário sabe e o que o usuário possui.

No caso “o que o usuário sabe” é o seu login e sua senha e “o que o usuário possui”, é um certificado digital gerado individualmente para cada funcionário.

Para que o usuário não tenha que ficar memorizando várias senhas para cada serviço disponibilizado pela empresa em sua intranet, aproveitou-se a flexibilidade do OpenVPN em aceitar um script de validação de usuário e desenvolveu-se um script para validar o usuário diretamente na base de dados LDAP, na qual os usuários da empresa são cadastrados. O Script de validação é mostrado seguir:

```
#!/bin/sh
if [ "$common_name" = "$username" ]
then
        ldapwhoami -x -h 127.0.0.1 -D
uid=$username,ou=Users,ou=ESSS,dc=esss,dc=com,dc=br -w $password
else
        echo -e "\n####Certificate and login
ERROR####\nLogin:$username\nCertificate:$common_name\n"
        exit 1;
fi

if [ $? -eq 0 ]; then
   echo "LDAP auth OK"
   exit 0;
else
   echo "LDAP auth ERROR"
   exit 1;
fi
```

O Script funciona da seguinte maneira:

Primeiro ele verifica se o login que está conectando é o mesmo do certificado digital, se não for ele já apresenta uma mensagem de erro e finaliza o script com valor 1, que para o OpenVPN quer dizer erro de validação do usuário. Caso o login

seja o mesmo do certificado digital, ele “chama” um cliente de LDAP para linha de comando que testa se a senha fornecida pelo usuário é válida.

Caso haja erro na senha, ele retorna uma mensagem de erro e finaliza o script com 1. Se a senha for válida, o script é finalizado com 0 e uma mensagem de aprovação é criada no log.

A vantagem de se utilizar LDAP na VPN é manter uma equivalência de login e senha com os serviços já utilizados pelos usuários.

7.5.3. Servidor de DNS

Cada funcionário tem um número de IP da VPN fixo, para que seja mais fácil identificar o usuário ou conectar a máquina sem ter que decorar Ips. Para tanto, foi configurado no servidor de DNS da empresa uma zona destinada à classe de IP utilizada pela VPN.

O subdomínio interno usado para a classe de IP da VPN é vpn.esss.com.br, ficando os hosts dos usuários como mostrado a seguir:

```
[root@ironman ~]# arp -a | grep vpn
fred.vpn.esss.com.br (10.2.0.17) at 00:FF:8E:4D:D5:E8 [ether] on tap1
igor.vpn.esss.com.br (10.2.0.12) at 00:FF:BD:9B:88:B2 [ether] on tap1
```

7.6. Resumo do Capítulo

Neste capítulo foi descrito todo o processo de implantação da VPN na empresa ESSS com suas três, instalação, configuração e distribuição.

Também foi descrito alguns itens que tiveram que ser considerados para a implantação na empresa, como configuração de DNS, dupla autenticação do usuário e o posicionamento da VPN junto ao firewall devido a um legado já existente.

8. Análises e resultados

Para analisar o tráfego pela VPN e também as conexões dos usuários foram utilizadas algumas ferramentas de monitoramento, criados alguns scripts e desenvolvido um sistema on-line de relatório que extrai dados de um banco de dados. Vejamos agora todos estes procedimentos.

8.1. Análise de tráfego das VPNs

Para análise de tráfego entre as interfaces de VPN foi utilizado uma ferramenta bastante conhecida na área de gerência de redes de computadores, MRTG (Multi Router Traffic Grapher) [MRT 06].

Na empresa já era utilizado o MRTG para monitoramento de tráfego de internet e sua instalação no sistema operacional usado, foi semelhante a instalação do OpenVPN.

```
[root@ironman ~]# yum install mrtg
```

O MRTG para mostrar gráficos de tráfego nas interfaces, utiliza o protocolo SNMP. Para isso foi necessário instalar também o pacote net-snmp que é um agente snmp para linux.

```
[root@fedora4 ~]# yum install net-snmp
```

Os arquivos de configuração do MRTG que monitoram o tráfego do servidor VPN ficaram da seguinte forma:

Configuração para monitoramento da interface TAP0, o arquivo v**pn-servers.cfg**.

```
### Global Config Options
EnableIPv6: no
WorkDir: /home/www/intranet/mrtg
Options[_]: bits,growright
Target[localhost_tap0]: \tap0:public@localhost:
SetEnv[localhost_tap0]: MRTG_INT_IP="10.1.0.1" MRTG_INT_DESCR="tap0"
```

```
MaxBytes[localhost_tap0]: 256000
Title[localhost_tap0]: 10.1.0.1 -- Link Externo
PageTop[localhost_tap0]: <H1>10.1.0.1 -- VPN-SERVERS</H1>
 <TABLE>
  <TR><TD>System:</TD>     <TD>ironman vpn-servers</TD></TR>
  <TR><TD>Maintainer:</TD> <TD>Frederico Gendorf
&lt;fred@esss.com.br&gt;</TD></TR>
  <TR><TD>Description:</TD><TD>tap0  </TD></TR>
  <TR><TD>ifType:</TD>     <TD>tapernetCsmacd (6)</TD></TR>
  <TR><TD>ifName:</TD>     <TD></TD></TR>
  <TR><TD>Max Speed:</TD>  <TD>2 Mbits/s</TD></TR>
  <TR><TD>Ip:</TD>         <TD>10.1.0.1 (fln.esss.com.br)</TD></TR>
 </TABLE>
```

A configuração da interface TAP1 é semelhante a TAP0.

```
### Global Config Options
EnableIPv6: no
WorkDir: /home/www/intranet/mrtg
Options[_]: bits,growright
Target[localhost_tap1]: \tap1:public@localhost:
SetEnv[localhost_tap1]: MRTG_INT_IP="10.2.0.1" MRTG_INT_DESCR="tap1"
MaxBytes[localhost_tap1]: 1250000
Title[localhost_tap1]: 10.2.0.1 -- Link Externo
PageTop[localhost_tap1]: <H1>10.2.0.1 -- VPN-Clients</H1>
 <TABLE>
  <TR><TD>System:</TD>     <TD>ironman vpn-clients</TD></TR>
  <TR><TD>Maintainer:</TD> <TD>Frederico Gendorf
&lt;fred@esss.com.br&gt;</TD></TR>
  <TR><TD>Description:</TD><TD>tap1  </TD></TR>
  <TR><TD>ifType:</TD>     <TD>tapernetCsmacd (6)</TD></TR>
  <TR><TD>ifName:</TD>     <TD></TD></TR>
  <TR><TD>Max Speed:</TD>  <TD>10.0 Mbits/s</TD></TR>
  <TR><TD>Ip:</TD>         <TD>10.2.0.1 (fln.esss.com.br)</TD></TR>
 </TABLE>
```

Estas duas configurações são executadas de cinco em cinco minutos, gerando gráficos que podem ser visualizados nas figuras 24 e 25.

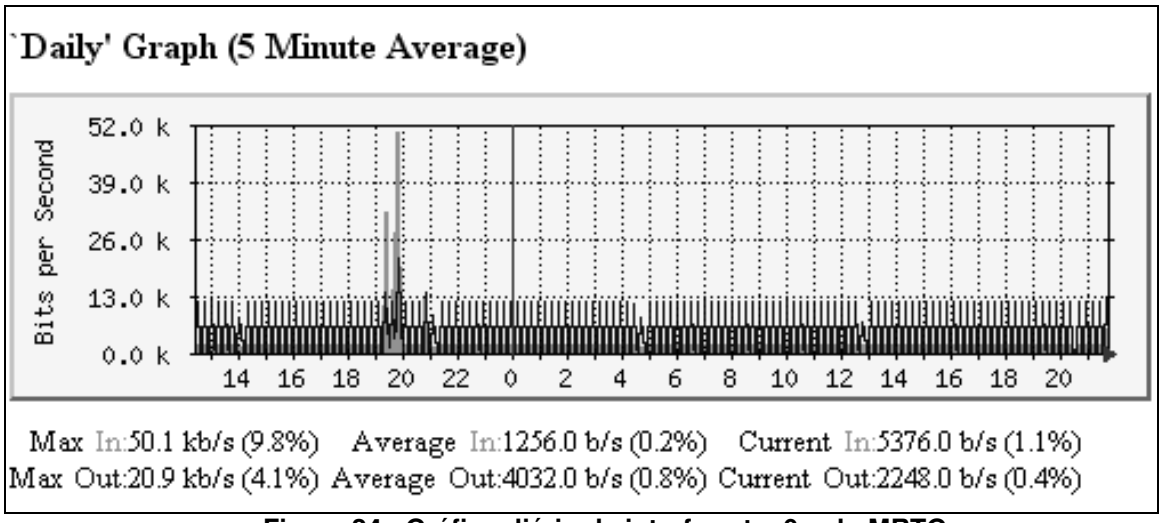


Figura 24 - Gráfico diário da interface tap0 pelo MRTG.

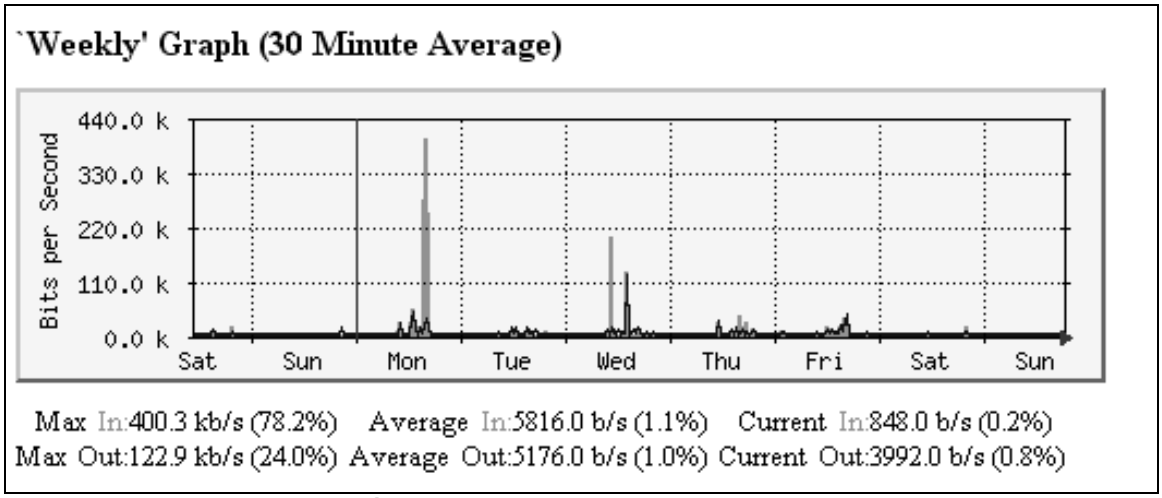


Figura 25 - Gráfico semanal da interface tap0 plotado pelo MRTG.

8.2. Análise de conexões de usuários

Utilizando também a ferramenta MRTG, foi montado gráfico de conexão de usuários, conforme configuração abaixo:

```
WorkDir: /home/www/intranet/mrtg
MaxBytes[openvpn]: 1250000
Target[openvpn]: `/usr/sbin/vpn-mrtginfo`
Options[openvpn]: gauge, growright
Title[openvpn]: OpenVPN
PageTop[openvpn]: <H1>OpenVPN Statistics</H1>
WithPeak[openvpn]: dwmy
YLegend[openvpn]: No. of Users
ShortLegend[openvpn]: Users
LegendI[openvpn]:  Incoming:
LegendO[openvpn]:  Outgoing:
```

É possível notar que esta configuração não utiliza SNMP e sim um script, que em conjunto com outro, capturam dos dados do OpenVPN e geram um resultado no formato do MRTG.

O primeiro script, que pode ser visto abaixo, é feito em PHP e filtra dos dados do arquivo de status da VPN e retorna os usuários conectados e algumas informações sobre o status das conexões.

```
#!/usr/bin/php -q
<?

exec("grep \"^CLIENT_LIST\" /etc/openvpn/openvpnstaus-{$argv[1]}.log
",$res);
for($x=0;sizeof($res)>$x;++$x){
        $dados = split(',',$res[$x]);
        $login = $dados[1];
        $remote = $dados[2];
        $local = $dados[3];
        $send = $dados[4];
        $received = $dados[5];
        $since = $dados[7];
        if(($login!="UNDEF")&&($local!="")){
                echo "$login,$remote,$local,$since,".time().",$send,$received\n";
        }
}
?>
```

O uso deste script tem como parâmetro o argumento que identifica qual servidor de VPN obter-se-á as informações. Abaixo podemos observar um exemplo do resultado da execução do referido script:

```
[root@ironman mrtg]# vpn clients
fred,200.xxx.xxx.34:1583,10.2.0.17,1148255866,1148259818,1178038,535142

[root@ironman mrtg]# vpn servers
firewall-sp,200.xxx.xxx.53:36781,10.1.0.2,11480492,11482598,897272,124313
```

O segundo script, feito em bash, filtra ainda mais as informações deste primeiro script e coloca as informações no formato aceito pelo MRTG.

```
#!/bin/bash
USERS=`/usr/bin/vpn clients | wc -l`
echo $USERS
```

```
echo $USERS
echo `uptime | cut -b 0-20`
echo vpn-clients
```

A execução deste script retorna o seguinte resultado, que é usado pelo MRTG para plotar um gráfico de conexão de usuários:

```
[root@ironman mrtg]# /usr/sbin/vpn-mrtginfo
2
2
22:10:55 up 24 days
vpn-clients
```

O gráfico que o MRTG gera a partir destes valores é mostrado pelas figuras 26 e 27.

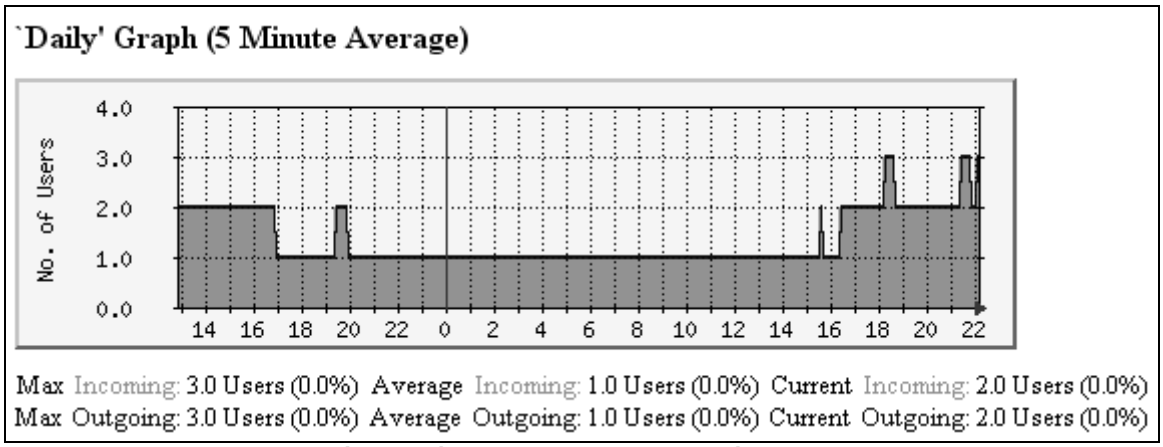


Figura 26 - Gráfico diário de conexão de usuários plotado pelo MRTG.

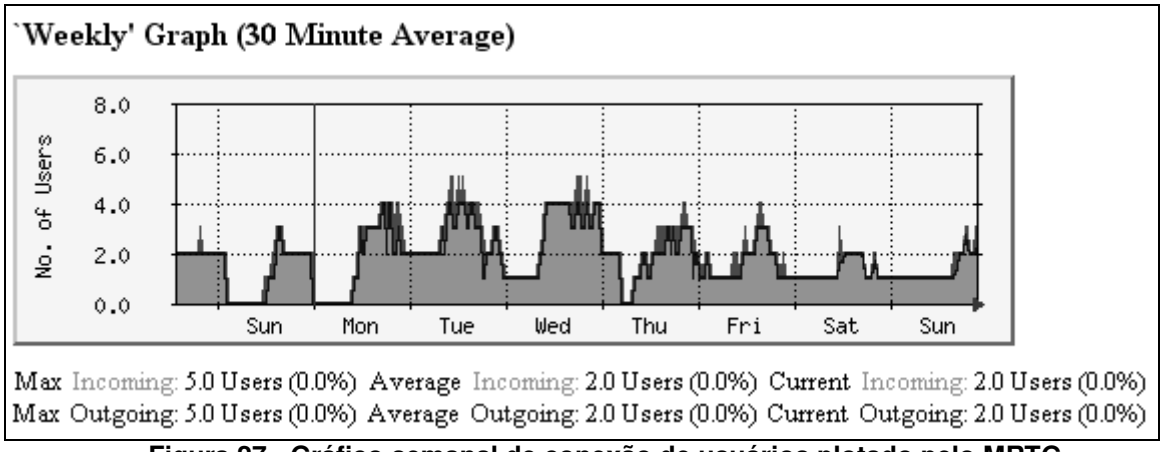


Figura 27 - Gráfico semanal de conexão de usuários plotado pelo MRTG.

Além do gráfico de conexões de usuários, que utiliza o MRTG, foi desenvolvido uma aplicação, em PHP, em conjunto com banco de dados MySQL para poder fazer um melhor acompanhamento das conexões dos usuários. A figura 28 mostra a interface de acompanhamento dos usuários on-line.

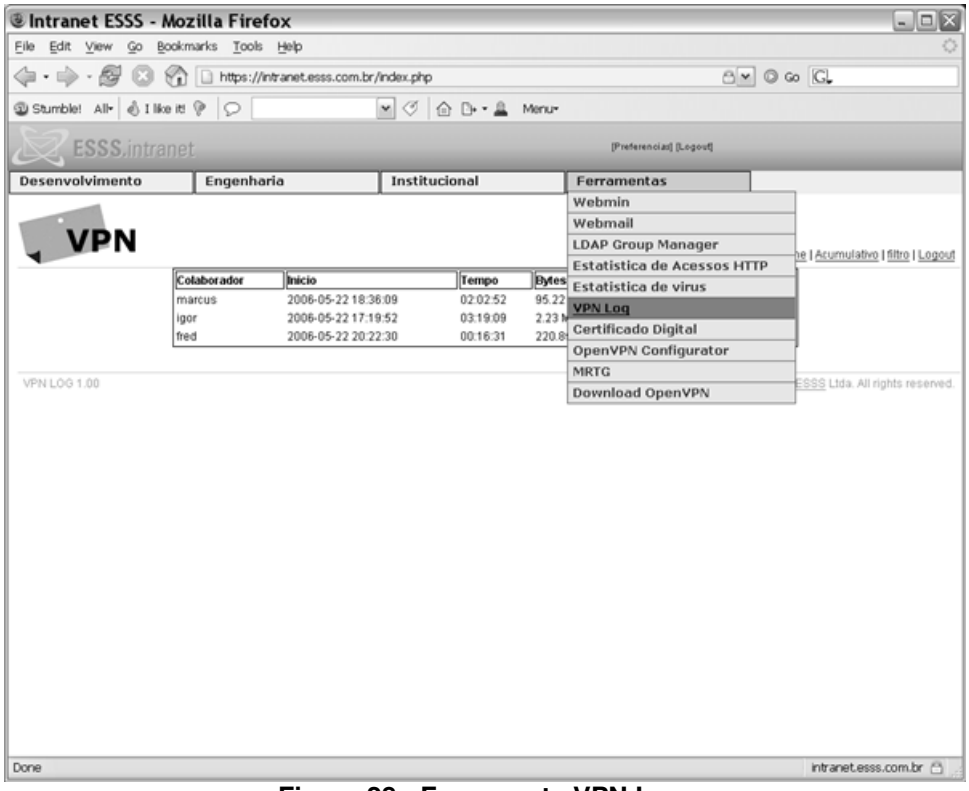


Figura 28 - Ferramenta VPN Log.

Apelidado de **VPN Log**, esta ferramenta funciona da seguinte maneira:

Uma rotina é executada pela crontab com o arquivo cronvpn.php de um em um minuto, faz a filtragem dos dados do arquivo de status do servidor VPN de funcionários e o insere em um banco de dados. Os dados são guardados em uma tabela no banco de dados com os seguintes campos:

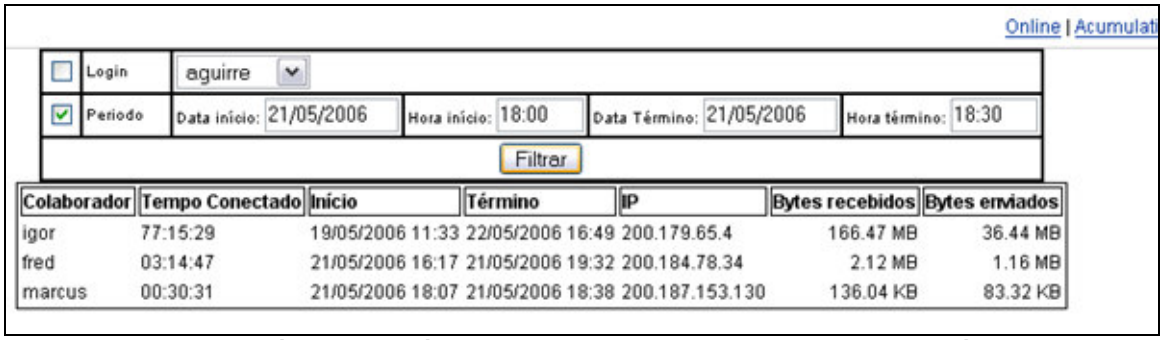
Campo	Descrição
idVpnConnection	Campo de identificação
loginVpnConnection	login do usuário conectado a VPN
remoteIpVpnConnection	IP da conexão remota
localIpVpnConnection	IP local sendo usado pelo usuário
sendVpnConnection	Quantidade de dados enviados em bytes
receivedVpnConnection	Quantidade de dados recebidos em bytes
sinceVpnConnection	Início da conexão
endVpnConnection	Término da conexão

Tabela 7 - Campos do banco de dados do VPN Log

Com estes dados é possível gerar um relatório de número e duração das conexões e transferência de dados, de extrema importância para auditoria da utilização da VPN e de sua estabilidade.

Com a aplicação de filtros, por período, é possível casar os dados visualizados no MRTG com o VPN Log. Por exemplo:

Observando o gráfico da figura 26, se desejarmos saber quem esteve conectado no horário das 18:00 às 18:30 horas, de um determinado dia, basta digitar os valores no campo especifico e filtrar a informação, conforme pode ser visto na figura 29.



Colaborador	Tempo Conectado	Início	Término	IP	Bytes recebidos	Bytes enviados
igor	77:15:29	19/05/2006 11:33	22/05/2006 16:49	200.179.65.4	166.47 MB	36.44 MB
fred	03:14:47	21/05/2006 16:17	21/05/2006 19:32	200.184.78.34	2.12 MB	1.16 MB
marcus	00:30:31	21/05/2006 18:07	21/05/2006 18:38	200.187.153.130	136.04 KB	83.32 KB

Figura 29 - Relatório por período para casar informações visuais do gráfico do MRTG.

Existe também a opção de relatório acumulativo, em que podemos verificar a utilização da VPN durante determinado período. No caso específico está sendo mostrado na figura 30, a utilização da VPN, nos quatro últimos meses, tempo este que a VPN está em operação.

Nº de Conexões	Colaborador	Tempo Conectado	Ultima informação	Bytes recebidos	Bytes enviados
3	aguirre	00:12:47	19/05/2006 11:32	70.38 KB	67.57 KB
3	claudio	00:08:07	05/04/2006 20:25	882.68 KB	253.14 KB
321	coi	199:33:23	30/04/2006 21:43	876.10 MB	151.46 MB
20	contessi	16:04:39	15/05/2006 21:10	280.92 MB	46.47 MB
208	damiani	358:16:21	22/05/2006 19:06	1.07 GB	157.96 MB
31	emilio	63:02:12	18/05/2006 22:00	378.93 MB	356.95 MB
23	fabiane	47:39:44	19/05/2006 17:21	143.82 MB	61.11 MB
11	fernando	02:09:02	19/05/2006 02:02	12.07 MB	6.05 MB
6	ferraz	00:49:01	18/05/2006 22:34	221.19 KB	178.24 KB
13	filipe	03:14:44	06/04/2006 22:46	25.74 MB	8.46 MB
92	fred	46:32:12	22/05/2006 21:12	191.18 MB	52.56 MB
37	gustavo	07:38:42	16/05/2006 21:32	39.49 MB	14.45 MB
32	hoff	72:31:57	10/05/2006 04:21	402.35 MB	303.77 MB
267	igor	1293:01:38	22/05/2006 21:12	2.39 GB	799.12 MB
82	kasper	229:51:47	09/03/2006 23:15	74.54 MB	64.10 MB
13	liliane	01:35:19	17/05/2006 17:13	31.84 MB	5.64 MB
391	marcus	128:47:14	22/05/2006 21:12	219.67 MB	66.99 MB
37	nicolas	10:43:14	22/05/2006 20:38	74.75 MB	25.64 MB
9	rafael	15:30:09	14/02/2006 11:27	8.29 MB	10.92 MB
58	regis	42:14:43	22/05/2006 01:16	422.59 MB	100.29 MB
249	ricardo	217:08:33	22/05/2006 13:56	4.38 GB	851.42 MB
7	sergio	04:05:12	02/05/2006 19:03	6.88 MB	6.41 MB
7	tasca	20:27:06	16/05/2006 10:03	1.19 GB	102.21 MB

Figura 30 - Relatório acumulativo que mostra o uso intenso da VPN desde a sua implantação.

8.3. Resumo do Capítulo

Neste capítulo foram apresentadas as ferramentas utilizadas para monitoramento da VPN, tanto na parte de conexões quanto na parte de tráfego pelos usuários.

Foi mostrada também a ferramenta desenvolvida para melhor acompanhamento de utilização da VPN, podendo ser gerado relatórios de períodos e bytes transferidos.

9. Conclusões

Este trabalho se propôs a mostrar a implementação de uma VPN em ambiente cooperativo utilizando a ferramenta OpenVPN, detalhando aspectos de suas configurações, além de analisar a segurança da mesma e sua utilização.

As VPNs cada vez mais são pesquisadas e incorporadas às organizações, sejam privadas ou governamentais, em diversos sistemas e ambientes computacionais. Os principais motivos desta crescente procura estão relacionados à segurança e economia no tráfego das informações.

Esta segurança é obtida principalmente através da utilização de algoritmos de criptografia e protocolos específicos, que geram grandes obstáculos aos invasores.

Algumas das funções de segurança garantidas por uma VPN são a integridade e a confidencialidade das informações transmitidas, assim como a autenticação e o controle de acesso dos gateways, permitindo maior garantia às empresas que adotam esta solução.

Algumas das ferramentas abordadas neste trabalho foram o PoPToP e o OpenSWAN, que se mostraram boas alternativas de implementação, porém não alcançaram alguns critérios pré estabelecidos durante o planejamento da VPN. Por sua vez, o OpenVPN mostrou-se mais completo em relação a estes, possuindo características mais expressivas no intuito de proteger o tráfego das redes interligadas.

É importante destacar que nem o OpenVPN nem uma outra ferramenta de VPN isoladamente conseguem garantir a segurança entre redes. É essencial que um planejamento cuidadoso seja feito, envolvendo políticas rígidas de segurança, permitindo que haja proteção física e lógica dos servidores.

Foi possível também observar, analisando o relatório acumulativo da ferramenta de análise de log desenvolvida, que o uso da VPN desde a sua implementação definitiva foi bastante intenso por alguns usuários, provando que seu objetivo de implementação foi atingido.

9.1 Contribuições

Analisando os tópicos abordados e relacionando-os com os resultados obtidos, pôde-se concluir que este trabalho, através de ampla pesquisa bibliográfica utilizada, contribuiu academicamente para conceituar os principais aspectos de

segurança utilizados em VPNs, além de analisar diversas características das Redes Privadas Virtuais, assim como seus elementos, topologias e principais protocolos.

Outra contribuição, esta de caráter prático, foi a implementação de uma VPN utilizando o OpenVPN que é uma ferramenta para disponibilizar VPNs baseado no protocolo SSL/TLS, interligando a empresa ESSS a suas filiais e possibilitando a conexão de funcionários em viagem à rede interna da empresa.

9.2 Trabalhos Futuros

Ficam como sugestões de trabalhos futuros, a partir da elaboração deste estudo, os seguintes temas:

- Relacionamento entre domínios Windows via VPN;
- Desenvolvimento de intranets distribuída com uso de VPN;
- Implantação de QoS em servidores VPN;
- Centralização de informações e aumento de segurança na prestação de serviços ASP (Application Server Provider).

Referências

[ALE 04] ALECRIM, Emerson. **Firewall: conceitos e tipos** - http://www.infowester.com/firewall.php Publicado em 11/04/2004, acesso em 03/2006

[ASS 04] ASSIS, João Mário de. **Implementando VPN em Linux;** Universidade Federal de Lavras, Setembro de 2004

[CAS 05] CASSETARI, Luiz Antonio Vieira Filho. **HowTo oficial do OpenVPN** http://www.altoriopreto.com.br/artigos_3rd/artigo_vpn.php , Acesso em Outubro de 2005.

[COM 99] COMER, Douglas E. / Stevens, David L. **Interligação em Rede com TCP/IP** - Volume II - projeto, implementação e estrutura. Editora Campus 1999

[DER 95] DERFLER JUNIOR, Frank J**. Guia de Conectividade**: terceira edição americana. Rio de Janeiro: Campus, 1995.

[GAL 03] GALLO, Michael A. / Hancock, William M. **Comunicação Entre Computadores e Tecnologias de Rede.** Primeira edição – Editora Thomson Pioneira, 2003

[HOS 04] HOSNER, Charlie. **OpenVPN and the SSL VPN Revolution** - SANS Institute 2004

[JOA 03] ASSIS, João Mário de. **Implementando VPN em Linux** Monografia de Pós-Graduação apresentada ao Departamento de Ciência da computação da Universidade Federal de Lavras como parte das exigências do Curso ARL- Administração em Redes Linux. Lavras/Minas Gerais 2003

[LES 00] LESSMANN, Marcelo. **CONSIDERAÇÕES SOBRE A IMPLANTAÇÃO DE INTRANETS EM PEQUENAS E MÉDIAS EMPRESAS.** Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina como requisito parcial para obtenção do título de Mestre em Engenharia de Produção. UFSC dezembro de 2000

[MRT 06] MRTG - Tobi Oetiker's MRTG - The Multi Router Traffic Grapher
Disponível em <http://oss.oetiker.ch/mrtg/> acesso em 02/2006

[NAK 02] NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. **Segurança de Redes em ambientes Cooperativos**. 3° Edição, Editora Futura, 2002.

[OPE 06] OPENVPN - **An Open Source SSL VPN Solution by James Yonan** – http://www.openvpn.net Acessado Outubro de 2005

[ORE 05] O'REILLY **Network: Deploying a VPN with PKI** - http://www.oreillynet.com/pub/a/security/2004/10/21/vpns_and_pki.html . Acessado 03/2006

[PIN 01] PINCOVSCY, João Alberto. **Uma estratégia para projetos de redes de computadores. -** Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina como requisito parcial para obtenção do título de Mestre em Engenharia de Produção, 2001

[RAP 03] RAPOPORT, Eduardo. **VPN - Virtual Private Network**, disponível em http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/index.html, Julho de 2003. Acesso em 02/2006.

[RFC 2246] RFC2246 **The TLS Protocol**. Disponível em <http://www.ietf.org/rfc/rfc2246.txt>

[RFC 2401] RFC2401 **Security Architecture for the Internet Protocol.** Disponível em <http://www.ietf.org/rfc/rfc2401.txt>

[RFC 2459] RFC2459 **Internet X.509 Public Key Infrastructure.** Certificate and CRL Profile. Disponível em <http://www.ietf.org/rfc/rfc2459.txt>

[RFC 2661] RFC2661 **Layer Two Tunneling Protocol "L2TP"** Disponível em <http://www.ietf.org/rfc/rfc2661.txt>

[RFC 4279] RFC4279 **Pre-Shared Key Ciphersuites for Transport Layer Security (TLS).** Disponível em <http://www.ietf.org/rfc/rfc4279.txt>

[RIB 01] RIBAS, Júlio César da Costa; DIAS Roberto Alexandre – **Fundamentos de TCP/IP** CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE SANTA CATARINA, GERÊNCIA DE TECNOLOGIA DE INFORMAÇÕES, Junho de 2001

[ROS 00] ROSSI, Marco Antonio G.; FRANZIN, Oswaldo. **VPN - Virtual Private Network.** GPr Sistemas/ASP Systems - Agosto/2000

[SAR 03] SARLO, Lino, da Silva. “**Virtual Private Network**”. Aprenda a construir rede privadas virtuais em plataformas linux e windows, Editora Novatec 2003

[SEC 06] SecurityFocus **Site de referencia em informações de segurança na internet.** Disponível em <http://www.securityfocus.com>. Acesso em: 05/2006

[SOA 97] SOARES, Luiz Fernando Gomes et al. **Redes de Computadores**: das LANs, MANs e WANs às Redes ATM. Rio de Janeiro: Campus, 1997.

[TAN 97] TANENBAUM, Andrew C. **Redes de Computadores** 3ª Edição. Ed. Campus, Rio de Janeiro de 1997

[UFS 06] UFSC. **SISTEMA RAS**. Sistema de acesso remoto da redeUFSC. Disponível em <http://www.ras.ufsc.br/>. Acesso em 05/2006

[VMW 06] VMWare Workstation 5.0. **Powerful Virtual Machine Software for the Technical Professional.** Disponível para avaliação em: <http://www.vmware.com/products/ws/>. Acesso 02/2006

Glossário

Backbone	Conjunto de roteadores que formam o “core”, onde os dados de várias redes trafegam de uma LAN para outra.
DMZ	De-militized Zone, Sub-rede localizada entre a rede interna e a rede externa.
DoS	Denial of Service ou Negação de Serviço. Ataque que explora a vulnerabilidade de um determinado servidor não poder distinguir requisições falsas das legítimas, explorada por meio da solicitação falsa em massa de um serviço específico, saturando o servidor e evitando que o mesmo responda a requisições legítimas.
Gateway	Porta de comunicação ou computador que faz a ligação entre duas redes distintas
Host	Computador conectado a uma rede.
ISO	International Standards Organization – uma sociedade multinacional responsável pela formulação, elaboração e manutenção de padrões tecnológicos no âmbito mundial.
ISO/OSI	Maneira padronizada de conceber a comunicação por computador com base no Modelo de Referência. Proposto em 1983 pela ISO, este modelo é importante porque pode ser usado para comparar diferentes tecnologias da rede.
Plug-and-Play	Ligar e usar, padrão de hardware que possibilita a instalação simples de novos hardwares, através do reconhecimento e configuração automática.
RAS	Remote Access Server, responsável por aceitar e gerenciar as conexões Dial-Up, provendo acesso à rede.
Roteador	Dispositivo de rede que direciona os pacotes para seus endereços de destino. Roteadores inteligentes são computadores capazes de bloquear pacotes com base na origem ou no destino, funcionado assim com um firewall de filtragem de pacotes.

Sniffer	Software analisador de pacotes de rede, com objetivo de coletar informações alheias
SSL	Security Socket Layer, protocolo que visa segurança no nível de aplicação.
TCP/IP	Transmission Control Protocol/Internet Protocol - Pilha de protocolos de rede da Internet
TI	Tecnologia da Informação, Expressão usada para descrever profissionais, setores, empresas etc. ligadas à área de informática.
UDP	User Datagram Protocol, protocolo que permite o envio de banco de dados através da Internet (pouco confiável, pois não garante a entrega)
VPN	Uma **Rede Privada Virtual** (**Virtual Private Network** - **VPN**) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.