Faculdade de Tecnologia de Americana
Curso Superior de Análise de Sistemas e Tecnologia da Informação – Segurança da Informação

Segurança em VPNs

Thomás Bellotto Corrêa da Silva

Americana, SP
2012

Faculdade de Tecnologia de Americana
Curso Superior de Análise de Sistemas e Tecnologia da Informação – Segurança da Informação

Segurança em VPNs

Thomás Bellotto Corrêa da Silva

thomas_thoti@hotmail.com

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular Curso Superior de Análise de Sistemas e Tecnologia da Informação com ênfase em Segurança da Informação, sob a orientação do Prof. Me. Alberto Martins Júnior.

Área: Segurança da Informação

Americana, SP
2012

BANCA EXAMINADORA

Prof. Me. Alberto Martins Júnior (Orientador)

Prof. Esp. Rogério Nunes de Freitas (Convidado)

Prof. Me. Clerivaldo José Roccia (Convidado)

AGRADECIMENTOS

Primeiramente agradeço à Deus por sempre acreditar em mim e iluminar meu caminho.

Agradeço aos meus pais, Wilson e Nereida, pela força, dedicação, apoio, amor e incentivo que não faltaram em nenhum momento. Ao meu irmão, Thiago, pelo apoio e companheirismo.

Agradeço ao meu orientador, Alberto Martins Júnior, pela paciência e dedicação, o qual me auxiliou no desenvolvimento deste trabalho.

Aos meus parentes e amigos que estavam presentes nessa longa jornada e me ajudaram muito durante a faculdade. Nunca irei esquecê-los.

DEDICATÓRIA

Dedico este trabalho principalmente aos meus pais, Wilson e Nereida, com amor e carinho.

Ao meu irmão, Thiago, pela força e dedicação.

Aos meus parentes e amigos pelo apoio e incentivo.

RESUMO

O conteúdo do presente trabalho descreve, baseado na revisão de literatura, sobre os conceitos e finalidades das VPNs - Redes Privadas Virtuais, tratando sobre os métodos de conexões que permitem ser feitos por meio da Internet. Além disso, foi abordado sobre os ataques que podem implicar na segurança das informações e os métodos para garantir segurança através da implantação de firewalls, protocolos de tunelamento, segurança AAA e protocolos de autenticação. Foi desenvolvido um projeto, o qual foi utilizado o OpenVPN para a realização do túnel entre duas redes corporativas diferentes. Foi usado também o Nessus, ferramenta responsável por mostrar as vulnerabilidades que podem estar presentes em um servidor VPN.

Palavras Chave: Redes Privadas Virtuais, Internet e Segurança das Informações.

ABSTRACT

The content of this paper describes based on a literature review on the concepts and objectives of VPNs - Virtual Private Networks, treating of the methods that allow connections to be made through the Internet. In addition, it was approached about the attacks that may involve the security of information and methods to ensure safety through the deployment of firewalls, tunneling protocols, security, AAA and authentication protocols. It was developed a project which was used to perform the OpenVPN tunnel between two different corporate networks. It was also used Nessus tool responsible for showing the vulnerabilities that may be present in a VPN server.

Keywords: Virtual Private Network, Internet and Information Security.

Sumário

Lista de Figuras

1. Introdução

A internet começou a dar os primeiros passos nos anos 50 pela ARPA (Defense Advanced Research Projects Agency ou Agência de Projetos de Pesquisa Avançada), onde sua principal função era para fins militares. Com a necessidade de ampliar a comunicação, a internet começa ser utilizada para interesses comerciais nos anos 90, onde o seu constante crescimento fez com que as redes de computadores sofressem transformações, os quais permitiam trocar informações em pequenas e grandes escalas.

Devido a esse crescimento, a segurança começa a ser um fator importante, pois atualmente muitas pessoas desfrutam de ferramentas que realizam transações por meio da internet, sejam elas para fins comerciais ou pessoais. Com o objetivo de garantir a transmissão das informações de modo seguro, foram criados mecanismos que, além de terem um papel importante para o gerenciamento seguro dessas redes, poderam garantir a confidencialidade das informações.

A partir disso, surgem as VPNs (Virtual Private Network ou Rede Privada Virtual), onde no começo ela funcionava através de uma linha dedicada acarretando em altos custos de implementação. Atualmente é utilizada uma infraestrutura pública (Internet) para realizar uma conexão entre o usuário remoto e a rede privada, fazendo com que muitas corporações pudessem trocar informações com integridade e confidencialidade estando elas fisicamente distantes, com baixo custo de implantação e ampla área de conectividade.

Com o uso das VPNs, as empresas conseguiram centralizar as bases de dados, para manter contato entre seus clientes e fornecedores. Porém surgem fatores de implicações com relação à segurança das informações, as quais estão vulneráveis a vários riscos, pois seus dados trafegam em um ambiente público, ou seja, a Internet.

Os recursos utilizados nas VPNs tornaram-se uma necessidade muito grande, os quais acarretam em estudo das ameaças que podem ocorrer, permitindo atender ao desenvolvimento de soluções seguras de acesso remoto VPN e a implantação de protocolos que possibilitem garantir a transmissão destas informações.

2. Justificativa

O tema deste trabalho foi escolhido por ser um assunto que vem representando um fator de grande importância para as organizações no que diz respeito à segurança no tráfego de informações. Atualmente várias empresas estão adaptando esse método, os quais os resultados apresentados até o possível momento são positivos.

As VPNs são ferramentas que proporcionam diversos recursos para as empresas, como, por exemplo: gerenciamento de endereços, autenticação dos usuários, criptografia dos dados, gerenciamento das chaves, suporte a múltiplos protocolos, confidencialidade e integridade. Devido a isso, houve reduções dos custos com linhas dedicadas e ampliação da área de conectividade.

Com a utilização das VPNs, foi possível conectar-se aos usuários remotos e as redes privadas da empresa possibilitando que clientes e fornecedores possam se comunicar, centralizar os dados da empresa e os funcionários não precisam estar fisicamente nas empresas para realizar suas atividades. Entretanto, o uso dessas conexões devem ser analisadas de tempos em tempos, pois podem ocorrer falhas durante o tráfego dos dados, acarretando em queda do desempenho e atrasos, comprometendo assim a qualidade destes serviços.

3. Objetivos

Este trabalho pretende mostrar os conceitos das Redes Privadas Virtuais, podendo conhecer como elas são implementadas nas organizações, os métodos de segurança que a envolvem e os tipos de ataques que podem ocorrer caso elas não estejam devidamente configuradas.

Outro objetivo será utilizar ferramentas que ajudaram na análise de segurança dos servidores, onde realizará um escaneamento na porta utilizada pela VPN, podendo exibir o nível de segurança que irá proporcionará na rede.

O estudo realizado neste trabalho de conclusão de curso tem como principal objetivo contribuir alertas e auxiliar as pessoas sobre como é avaliado a segurança das informações durante o tráfego e quais riscos podem ocorrer se medidas de segurança não forem tomadas.

4. Metodologia

A Metodologia escolhida para esse trabalho foi feita através de pesquisas em site, artigos científicos e livros tecnológicos que abordam sobre o assunto proposto que é do desenvolvimento de um experimento utilizando ferramentas para as VPNs.

Para isso, o trabalho foi divido em duas partes, sendo:

A primeira parte apresenta a revisão de literatura, onde foi possível entender sobre os conceitos das Redes Privadas Virtuais e abordar sobre possíveis falhas que podem ocorrer devido à falta de uma configuração adequada e métodos para garantir a segurança.

Já na segunda parte foi desenvolvido um experimento para a implementação das VPNs, os quais foram utilizados softwares livres, com o objetivo de analisar e demonstrar o seu funcionamento na plataforma Linux.

5. Revisão de Literatura

Neste capítulo serão apresentados os conceitos sobre as implantações das VPNs, formas de tunelamentos, modos de interconexão, riscos de ataques, protocolos de segurança, criptografia e uma demonstração de ferramentas que auxiliam na segurança das informações.

5.1 Tecnologia da Informação

Segundo Pacievitch (2009), a TIC (Tecnologia da Informação e Comunicação) pode ser definida como:

“Um conjunto de recursos tecnológicos, utilizados de forma integrada, com um objetivo comum.”

Conforme Alecrim (2011), antigamente com a utilização dos primeiros computadores, se tornou possível realizar tarefa de automatização para instituições de pesquisas, empresas e meios governamentais. Porém eles necessitavam ser alocadas em lugares grandes devido ao seu tamanho, mas com o avanço das tecnologias, foram se tornando cada vez menores e com processamento melhores. Através do surgimento e utilização da Internet, os computadores puderam trocar informações com outras estações, estando elas em diferentes lugares do mundo, nascendo o conceito da Tecnologia da Informação.

De acordo com Alecrim (2011), foi possível também identificar que a Tecnologia da Informação não faz uso apenas de recursos de hardware, podendo ser utilizada em conjunto com os softwares, possibilitando as operacionalizações de comunicações e processos através de meios virtuais, onde as informações que fazem parte de um patrimônio precisam ser utilizadas de maneira correta, tornando-as um diferencial.

5.2 Ataques de Segurança

Segundo Guimarães, Lins e Oliveira (2006), é necessário analisar as principais ameaças de segurança dentro de uma organização, a fim de não comprometer a integridade, a autenticidade e a privacidade das informações, tornando as redes mais confiáveis e seguras. As ameaças podem surgir a partir de dentro ou fora da rede da empresa.

Ainda de acordo com Guimarães, Lins e Oliveira (2006), os ataques podem ser de 6 tipos diferentes, podendo ser definidos da seguinte maneira:

a) Ataques de Interrupção

O ataque de interrupção mais conhecido é chamado de DoS (Denial of Service ou Negação de Serviço), o qual o principal objetivo dele é interromper os serviços oferecidos, ou seja, bloquear a disponibilidade das informações. Ele é responsável por enviar vários pedidos de requisições para um determinado serviço rodando em um servidor, fazendo com que não seja possível suprir toda a demanda das requisições, tornando o serviço indisponível. Esse ataque pode também destruir os componentes de hardware ou até mesmo a interrupção da rede.

b) Ataques de Interceptação

O ataque de interceptação é responsável por analisar e obter as informações que estão sendo transmitidas pela rede, ou seja, invadir a privacidade das informações. O man-in-the-midle é o principal ataque deste tipo, o qual seu objetivo é se passar por um usuário autenticado, obtendo cópias das informações não autorizadas. Uma maneira para realizar ataques de interceptação é fazer uso de ferramentas de Sniffer, onde o atacante pode capturar os dados e alterá-los através de possíveis falhas de segurança, como, por exemplo: falta de criptografia e senhas para o acesso.

c) Ataques de Modificação

O ataque de modificação é responsável por invadir a integridade das informações, onde o invasor se passa por um usuário autenticado, realizando cópias

das informações transmitidas, modificando-as e enviando-as posteriormente de volta a rede. Este mecanismo é chamado de Replay.

d) Ataques de Falsificação (Spoofing)

O ataque de falsificação é responsável por atacar a autenticidade das informações, com o objetivo de obter informações sigilosas. Uma técnica bastante conhecida é o IP Spoofing, onde o invasor se passa por um usuário autorizado através da troca do endereçamento IP do host, por exemplo: o endereço dele será o mesmo de um servidor Web.

5.3 Virtual Private Network (Redes Privadas Virtuais)

Segundo Tanenbaum (2003), uma possível definição para as VPNs seria:

> "As redes VPN são redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real".

Figura 1: Visão geral sobre as VPNs

Fonte: Cisco, 2007

Segundo Guimarães, Lins e Oliveira (2006), as VPN são consideradas um meio de comunicação protegido permitindo que usuários remotos consigam conectar-se a rede interna da organização que participam. Para isso, elas utilizam

canais públicos, por exemplo, a Internet, parecendo que estão diretamente conectadas a mesma. Elas também possibilitam conectar a diferentes redes privadas para a transmissão das informações.

Muitas empresas estão adaptando este tipo de recurso nas suas infraestruturas de redes para atender as demandas de conectividade entre seus clientes e funcionários, podendo realizar com eficiência, o aumento do nível de complexidade nas redes e suporte aos usuários.

De acordo com Tyson (2007), as vantagens que as redes privadas virtuais podem oferecer são:

- Ampliação da segurança
- Redução de custos
- Redução do tempo de locomoção
- Crescimento da produtividade
- Melhoramento das oportunidades de relacionamentos
- Suporte ao usuário remoto
- Ampliação da área de conectividade

Uma principal vantagem da utilização das Redes Privadas Virtuais, de acordo com Guimarães, Lins e Oliveira (2006), é que permitem o controle central das informações e suas devidas seguranças, o gerenciamento das redes e a conectividade entre as organizações.

Segundo Guimarães, Lins e Oliveira (2006), no começo as VPNs dependiam de circuitos virtuais permanentes ou de circuitos dedicados ponto-a-ponto, por exemplo: Frame-Relay, X.25 e ATM, os quais geravam custos elevados de implementação, podendo ser cada vez mais altos dependendo da ampliação das distâncias entre as organizações.

Devido a isso, de acordo com Guimarães, Lins e Oliveira (2006), as Redes Privadas baseadas na Internet, além de permitir baixo custo, utilizam mecanismos de criptografia, autenticação e protocolos de encapsulamento, que, por sua vez, fornecem integridade, privacidade e confidencialidade durante a transmissão dos dados.

Segundo Guimarães, Lins e Oliveira (2006), um fator relevante para adaptar as VPNs nas infraestruturas de redes das empresas é referente à sua área de

cobertura, os quais utilizando através da Internet, abrangem praticamente todo o mundo, facilitando a interligação com suas filias, clientes e fornecedores.

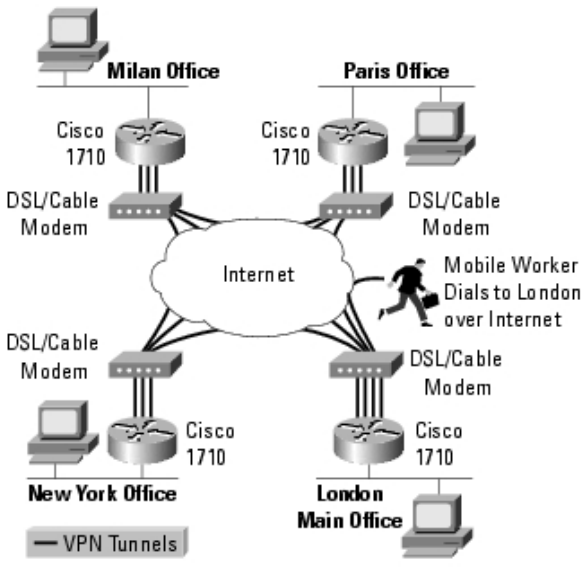
De acordo com o Santana, as conexões das VPNs utilizam a técnica de tunneling (tunelamento), onde os dados trafegam por uma rede pública roteada através de um “túnel privado” interligando uma conexão fim-a-fim, permitindo que as informações sejam transmitidas em uma mesma infraestrutura, porém em “túneis” distintos, fazendo uso de protocolos de segurança com o objetivo de evitar que as informações sejam roubadas ou fraudadas por um invasor.

5.4. Modos de Conexão

Os Modos de Conexões permitem definir de qual forma deverá ser realizada a conexão, onde, segundo Guimarães, Lins e Oliveira (2006), elas podem ser implementadas de três maneiras diferentes:

- **VPNs de Intranet (VPN LAN-to-LAN):** podem ser definida como uma conexão privada de uma organização ou instituições governamentais, proporcionando conectar suas respectivas matrizes, filiais ou a outras organizações, através das redes não-confiáveis.

Figura 2: Esquema da VPN Intranet

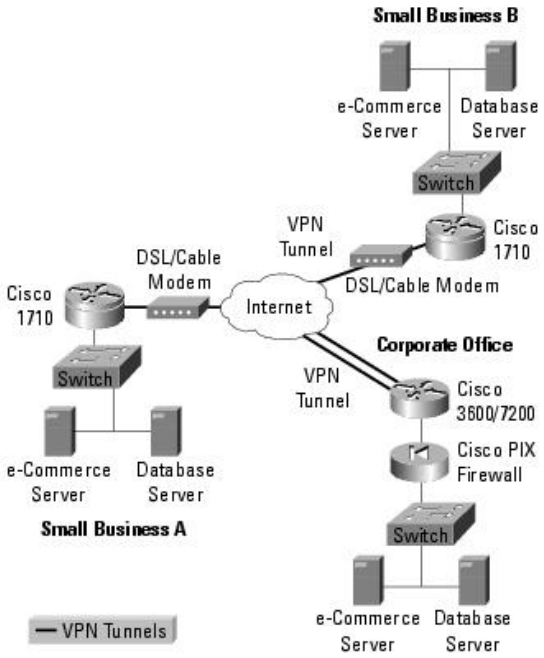


Fonte: Cisco

(http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a080088716.html)

- **VPNs de Extranet:** estabelece uma conexão entre uma organização e seus clientes, fornecedores, parceiros e representantes, podendo criar uma solução para melhorar o compartilhamento de informações de forma dinâmica e efetiva.

Figura 3: Esquema da VPN Extranet

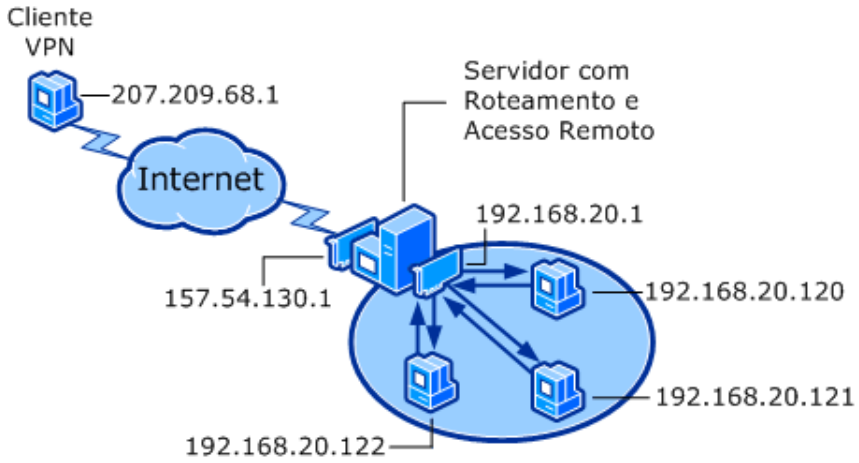


Fonte: Cisco

(http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a0080088716.html)

- **Acesso Remoto VPN:** este tipo de interconexão é utilizado para interligar a empresa aos funcionários fisicamente distantes da rede, havendo a necessidade de um software cliente de acesso remoto. Dois importantes requisitos a serem abordados são com relação ao QoS (Quality of Service ou Qualidade do Serviço), pois os usuários remotos estarão limitados à velocidade da banda e a realização da autenticação de modo rápido e eficiente, garantindo assim a autenticidade do usuário.

Figura 4: Esquema do Acesso Remoto via VPN



Fonte: Technet (http://technet.microsoft.com/pt-br/library/cc753870(v=ws.10).aspx)

5.5. Firewall

Segundo Tanenbaum (2003) os firewalls podem ser definidos da seguinte forma:

> "Os firewalls são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Este recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas."

Os firewalls são utilizados para fiscalizar todo o trafego de pacotes que entram e saem da rede das organizações. Neste capitulo serão abordados sobre os diferentes tipos de firewalls e suas devidas regras.

Segundo Guimarães, Lins e Oliveira (2006), os firewalls podem ser definidos em três tipos diferentes, como:

a) **Filtros de Pacotes Estáticos:** Os filtros de pacotes estáticos operam na camada de rede e analisam os pacotes que entram e sai da rede da empresa atuando para a defesa de profundidades. Sua velocidade é bem mais rápida comparado com os firewall com Estado e Proxy, permitindo agilizar o processo em caso de ataque ou sobrecarregamento do mesmo.

b) Firewalls com Estado: Os Firewalls com Estado são responsáveis por analisar o estado de uma conexão, onde são gravados em tabelas de estado e são interrompidos o tráfego dos pacotes caso não estejam presentes nestas tabelas. Eles também gravam os endereços de origem, destino e as portas que podem ser realizadas as conexões.

c) Firewalls Proxy: Os Firewalls Proxy além de possuir as mesmas funcionalidades dos firewalls citados anteriormente, eles utilizam serviços avançados, os quais permitem bloquear a comunicação direta entre hosts, podendo estes estarem internamente ou externamente a rede da organização. Deste modo, eles analisam detalhadamente todos os pacotes, a fim de evitar o tráfego de informações maliciosas.

5.6. Tunelamento em VPNs

Segundo Zanaroli, Lima e Rangel (2000), o tunelamento é o principal mecanismo para se criar uma conexão entre duas redes privadas distintas, os quais ela faz uso de técnicas de encapsulamento e de vários protocolos diferentes podendo estes ser classificados de dois tipos:

a) Protocolo que encapsula pacotes da camada 3 são responsáveis por transforma-los em quadros Point-to-Point Protocol. Para isso, utilizam-se os seguintes protocolos: o L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol) e o L2F (Layer 2 Fowarding).
b) Protocolo que encapsula pacotes IP é responsável por adicionar um cabeçalho antes de serem transmitidos na rede, onde o protocolo usado é o IPSec (Internet Protocol Security).

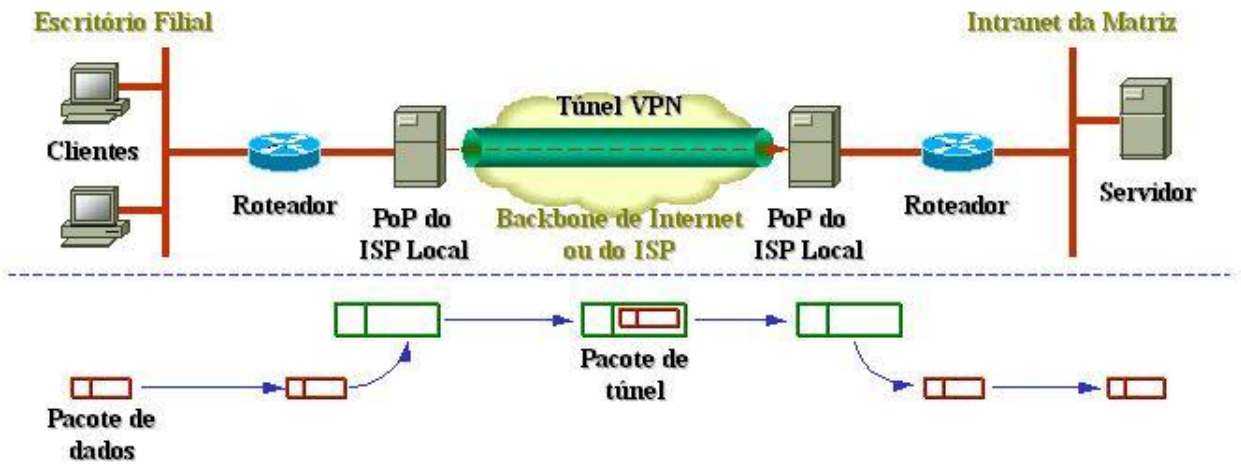
O objetivo de se utilizar túneis é criar um canal seguro sobre a rede pública, a fim de interconectar um usuário remoto a uma rede compartilhada de outros pontos remotos da VPN. Para isso, de acordo com Guimarães, Lins e Oliveira (2006), ela deverá funcionar da seguinte forma: o usuário remoto, primeiramente deverá estar autenticado no servidor VPN e precisará criptografar as informações. Após isso, será

necessário encapsular em pacotes IP, onde consistirá em acrescentar um cabeçalho IP, contendo o endereço de origem e destino.

Ainda segundo Guimarães, Lins e Oliveira (2006), o ponto de destino deverá remover o cabeçalho IP e desencapsular o pacote recebido, os quais são utilizadas técnicas de criptografia, evitando que usuários não autenticados possam acessar as informações.

Com relação ao endereçamento dos hosts remotos, as Redes Privadas podem proporcionar independência na rede compartilhada, pois caso deseja-se reutilizar o mesmo endereço privado dentro das várias VPNs, não ocorrerão conflitos na rede.

Figura 5: Visão Geral do Tunelamento



Fonte: Abusar.org (http://www.abusar.org.br/vpn/vpnport.htm)

Segundo Guimarães, Lins e Oliveira (2006), os tipos de tunelamento podem ser definidos da seguinte forma:

Tunelamento Voluntário – ocorre quando um computador ou servidor utiliza um software cliente de tunelamento para realizar uma conexão, através da Internet, com o Servidor VPN, onde ela irá fazer parte de uma das extremidades do túnel e funcionará como cliente do túnel.

Tunelamento Compulsório – o computador do cliente não realizará a conexão com o servidor remoto, pois é necessário existir um Servidor de Autenticação para acesso à rede. Além disso, o cliente não precisa utilizar quaisquer softwares cliente VPN para estabelecer uma conexão do túnel.

5.7. Protocolos de Tunelamento

Neste capítulo serão apresentados os protocolos de tunelamento utilizados para implementações nas redes privadas das organizações, descrevendo suas funcionalidades específicas.

5.7.1. Protocolo PPTP (Point-to-Point Tunneling Protocol)

Segundo o NORTHCUTT (2002), o protocolo PPTP pode ser definido como:

> "O protocolo PPTP ou Point-to-Point Tunneling Protocol, é um protocolo da camada 2 que foi desenvolvido por um consórcio de empresas de Tecnologia da Informação, incluindo a US Robotic (parte da 3Com), Microsoft, Ascend Communication (parte da Lucent) e ECL Telematic, mas, foi amplamente popularizado através das implementações realizadas pela Microsoft."

De acordo com Guimarães, Lins e Oliveira (2006), um dos principais propósitos do protocolo PPTP foi procurar atender os fornecedores de hardware, de Servidores de Acesso Remoto e aos interesses da Microsoft, facilitando a comunicação entre os usuários remotos com a rede privada de uma organização.

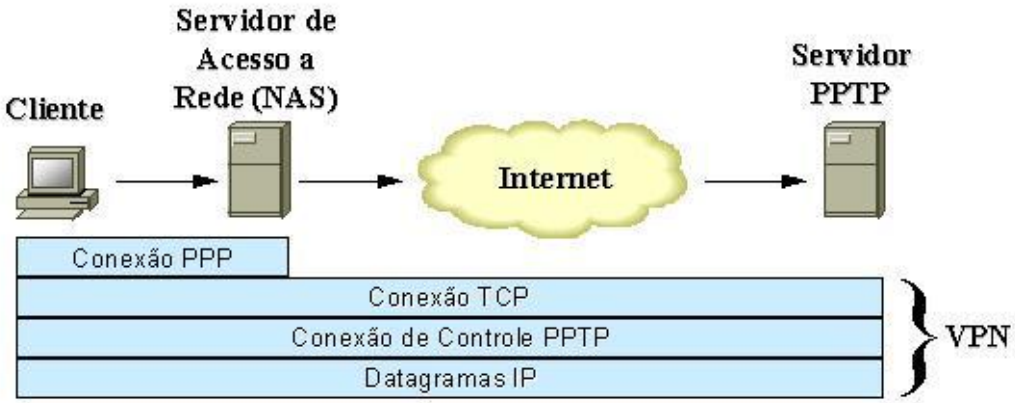
Segundo Zanaroli, Lima e Rangel (2000), o PPTP se baseia no protocolo PPP (Point-to-Point Protocol) permitindo realizar uma conexão para o acesso remoto através do tunelamento entre o cliente PPTP e o Gateway PPTP, onde os pacotes são encapsulados pelo protocolo GRE (Generic Routing Encapsulation ou Encapsulamento Genérico de Roteamento), tornando possível interagir protocolos diferentes, como, por exemplo: o IPX e NetBEUI.

Ainda segundo com Zanaroli, Lima e Rangel (2000), os mecanismos de autenticação utilizados pelo protocolo PPTP foi estruturado com base nos protocolos: PPP, CHAP e PAP. Porém ele possui algumas desvantagens, por exemplo: o seu processo de criptografia proporciona uma fraca proteção dos pacotes e não permite a utilização de autenticação através de token.

De acordo com Zanaroli, Lima e Rangel (2000), o processo de conexão do protocolo PPTP é realizado da seguinte forma:

- O cliente realiza uma conexão com o servidor NAS (Network Access Server ou Acesso à Rede), onde ele pode trocar informações via Internet.
- Feita a conexão com o servidor NAS, é realizada uma segunda conexão chamada dial-up, os quais as informações são transmitidas, em formato de datagramas IP, através do túnel interligando o cliente PPTP ao servidor PPTP.

Figura 6: Esquema utilizado pelo protocolo PPTP



Fonte: Abusar.org (http://www.abusar.org.br/vpn/vpnport.htm)

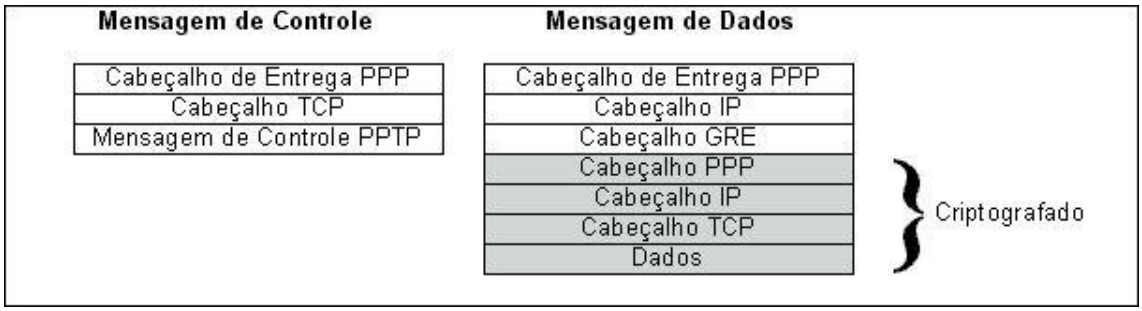
Segundo Zanaroli, Lima e Rangel (2000), existem três processos para realizar uma conexão segura utilizando o protocolo PPTP, onde podem ser definidas como:

- **Conexão e Comunicação PPP:** neste processo o PPP é utilizado para realizar uma conexão entre o cliente ao servidor NAS, através de uma linha telefônica ou serviço de ISDN (Integrated Services Digital Network). O PPP é utilizado para realizar uma conexão, criptografar informações e autenticar usuários.
- **Conexão de Controle PPTP:** este processo é chamado de túnel PPTP, pois é realizada uma conexão pelo PPP, onde o PPTP estabelecerá um controle sobre a conexão entre o cliente e o servidor PPTP, através do protocolo TCP.
- **Tunelamento de Dados PPTP:** neste processo o protocolo PPTP será responsável por enviar ao servidor PPTP os datagramas IP utilizando o túnel, onde apresenta os pacotes PPP criptografados. No servidor, os datagramas

serão desmanchados e os pacotes PPP descriptografados, a fim de serem enviados a rede privada da organização.

Segundo Zanaroli, Lima e Rangel (2000), os datagramas PPTP podem ser definidos de dois tipos: Datagramas de Mensagens de Controle (enviados através de datagramas TCP) e Datagramas de Mensagens de Dados (enviados através de datagramas IP).

Figura 7: Esquema do datagrama do protocolo PPTP



Fonte: Abusar.org (http://www.abusar.org.br/vpn/vpnport.htm)

5.7.2. Protocolo L2F (Layer Two Forwading)

Segundo Zanaroli, Lima e Rangel (2000), o protocolo L2F foi desenvolvido pela Cisco Systems, o qual atua na camada de enlace (camada 2) e possui o mesmo objetivo do protocolo PPTP em realizar o tráfego das informações entre os usuários remotos e a organização através dos túneis. Porém, uma diferença entre eles é que o protocolo L2F utiliza um tunelamento independente do IP, possibilitando trabalhar diretamente com outros recursos, por exemplo: Frame Relay e ATM.

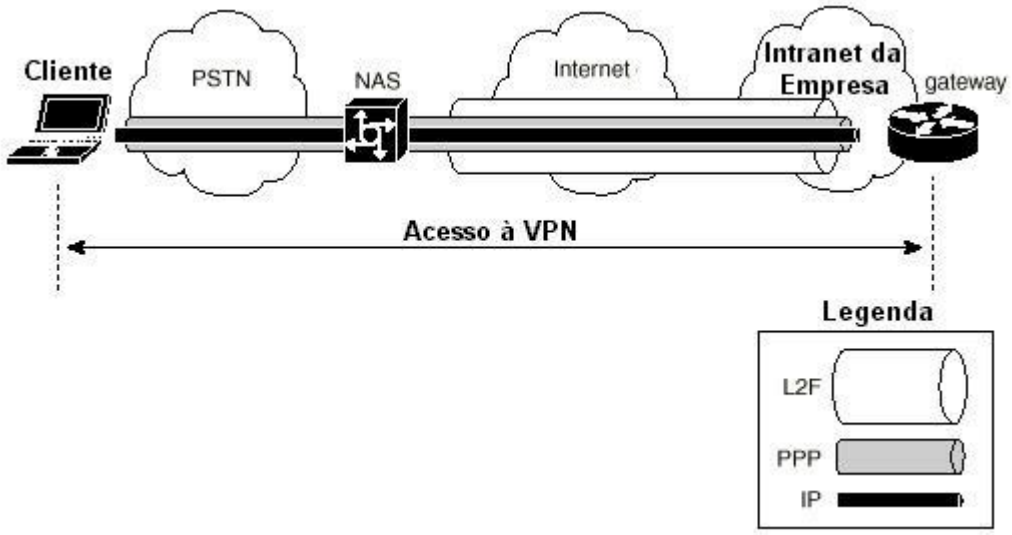
Outra diferença, de acordo com Zanaroli, Lima e Rangel (2000), é que o L2F permite realizar várias conexões nos túneis. Entretanto, semelhante ao protocolo PPTP, este protocolo possibilita interagir com protocolos diferentes do IP, como o IPX e o NetBEUI e o método utilizado para autenticação dos usuários remotos pode incluir suporte para autenticações como TACACS e RADIUS.

Segundo Zanaroli, Lima e Rangel (2000), o processo de conexão é realizado seguinte forma: o usuário conectará ao servidor NAS através de uma conexão PPP. Logo depois, o servidor NAS criará um túnel com o servidor VPN utilizando o

protocolo L2F, o qual este servidor autenticará o usuário usando um sistema triplo de autenticação via protocolo CHAP (Challenge Handshake Authentication Protocol) permitindo a conexão entre o usuário e a rede corporativa.

Segundo Fagundes (2007), a desvantagem de utilizar o protocolo L2F é que ele não proporciona uma criptografia e o encapsulamento das informações.

Figura 8: Esquema de conexão do protocolo L2F



Fonte: Abusar.org (http://www.abusar.org.br/vpn/vpnport.htm)

5.7.3. Protocolo L2TP (Layer 2 Tunneling Protocol)

Segundo Fagundes (2007), o protocolo L2TP (Protocolo de Tunelamento da Camada 2) foi desenvolvido pela IETF (Internet Engineering Task Force), com o objetivo de criar um padrão para os protocolos de tunelamento, buscando combinar as funcionalidades dos protocolos PPTP e L2F. O L2TP realiza conexões semelhantes ao PPTP, o qual utiliza o protocolo PPP e ele é independente do protocolo IP para a transmissão das informações, semelhante ao protocolo L2F.

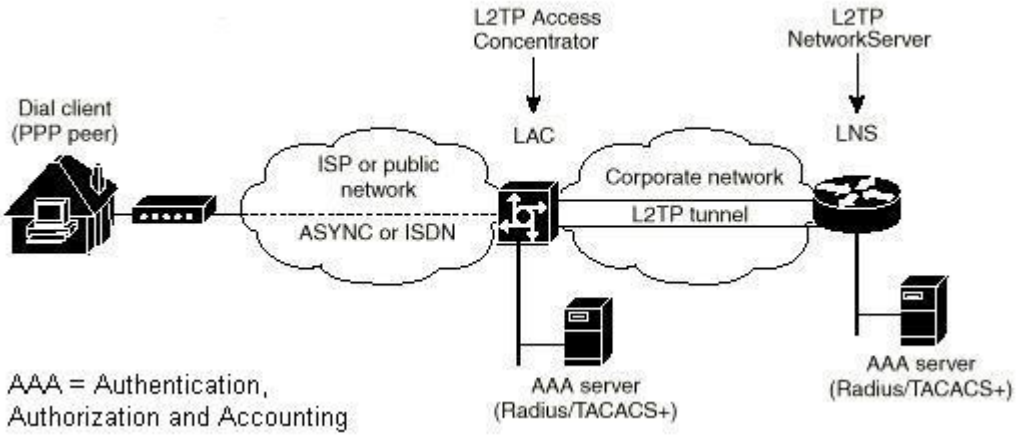
Segundo Guimarães, Lins e Oliveira (2006), o L2TP permite trabalhar com protocolos roteados, por exemplo: o IP, Appletalk e IPX e utilizar diferentes meios para o transporte das informações, como: ATM, X.25, Frame Relay e SO-NET.

Ainda de acordo com Guimarães, Lins e Oliveira (2006), este protocolo possibilita utilizar dois modos de tunelamento diferentes:

- **Tunelamento Voluntário:** a conexão é iniciada a partir do cliente remoto, permitindo que possa ser realizada uma conexão em qualquer provedor de acesso.
- **Tunelamento Compulsório:** é estabelecida uma conexão automaticamente, onde o provedor de acesso deve estar pré-configurado com as informações do túnel e dos usuários autenticados.

Com relação ao modo de conexão utilizado pelo protocolo L2TP, de acordo com Guimarães, Lins e Oliveira (2006), é feita da seguinte forma: o LAC ou Concentrador de Acesso L2TP que está alocado em um servidor NAS, realiza troca de mensagens PPP com o Servidor de Rede L2TP (LNS), a fim de estabelecer o tunelamento para a comunicação. Então o L2TP transmite as informações utilizando o protocolo UDP para a manutenção do túnel VPN, através da porta 1701, até a rede local da organização. Com isso, são transmitidos sequência de quadros L2TP, os quais são aprovados pelo NAS, encapsulados e transmitidos para o túnel. Ao chegarem ao destinatário, esses quadros devem ser desencapsulados, podendo fazer a leitura das informações.

Figura 9: Esquema de conexão do protocolo L2TP



Fonte: Abusar.org (http://www.abusar.org.br/vpn/vpnport.htm)

Com base no IPSec, o protocolo L2TP utiliza as funcionalidades para a criptografia e gerência das chaves para suporte ao NAT (Network Address Translation).

Segundo Fagundes (2007), os dados são encapsulados para a transmissão, onde recebe os seguintes parâmetros são Informação, Cabeçalho L2TP e Cabeçalho IP.

Figura 10: Visão do Encapsulamento L2TP

Fonte: Fagundes (2007)

5.7.4. Protocolo IPSec

O IPSec (IP Security Protocol ou Protocolo de Segurança IP) vem sendo aprimorado pela IETF, onde ele garante a segurança no uso de recurso do IPv6 e características do IPv4.

Segundo Guimarães, Lins e Oliveira (2006), ele atua na camada de rede (camada 3) do modelo OSI permitindo garantir a segurança nas outras camadas e pela utilização de recursos, como: controle de acesso, autenticidade, proteção contra replays, integridade, confidencialidade e controle no tráfego de informações.

Segundo Tanenbaum (2003) o IPSec pode ser destacado também que:

> "O IPSec é o padrão que não está vinculado a protocolos de criptografia específicos, portanto a sua estrutura sobrevive mesmo a violações em algoritmos de criptografia, pois, caso esta situação ocorra, basta alterar o algoritmo utilizado pelo IPSec."

De acordo com Fagundes (2007), o IPSec permite trabalhar com dois modos diferentes:

- **Modo Transporte:** é o modo nativo do protocolo IPSec, onde não existe a necessidade de um equipamento para a segurança, sendo feita a transmissão dos dados de host para host.

Figura 11: Encapsulamento IPSec no modo transporte

Fonte: Fagundes (2007)

- **Modo Túnel:** este modo é responsável por realizar o encapsulamento IPSec entre dois gateway, pois quando a transmissão é feita entre dois hosts, os dados não possuem suporte ao IPSec. Desta forma, o pacote original que será transmitido recebe um cabeçalho IPSec através do gateway e enviará até o outro gateway, onde este fará o desencapsulamento e leitura dos dados.

Figura 12: Encapsulamento IPSec no modo túnel

Fonte: Fagundes (2007)

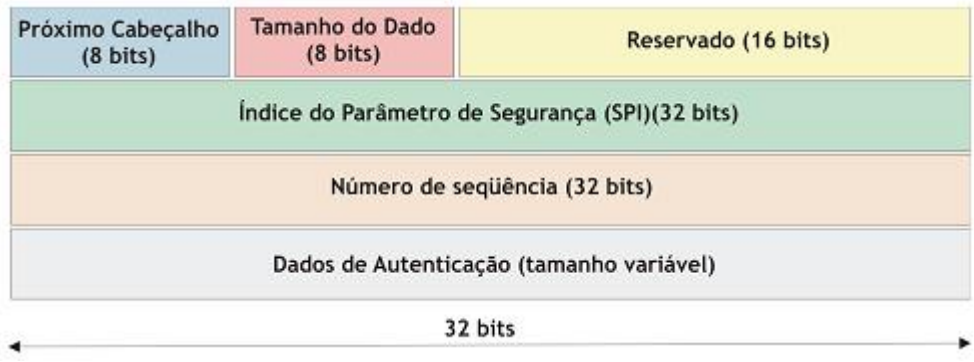
5.7.4.1. AH (IP Authentication Header)

Segundo Guimarães, Lins e Oliveira (2006), este protocolo oferece a garantia da autenticidade e proteção contra ataques do tipo spoofing e replays. Ele é responsável também por garantir a integridade, ou seja, evita que os dados não sejam modificados durante a transmissão, o qual é possível através da autenticação do usuário feita a partir de um sistema ou dispositivo de rede.

De acordo com Silva (2003), é possível destacar que:

> Embora a autenticação aconteça no pacote IP, nem todos os campos podem ser autenticados, porque alguns campos do cabeçalho serão alterados no decorrer da transmissão. Esses campos são considerados mutantes, ou variáveis, sendo ele: Tipo do Serviço, Offset Flags, Tempo de Vida do Pacote e Checksum.

Figura 13: Cabeçalho AH



Fonte: Fagundes (2007)

De acordo com Guimarães, Lins e Oliveira (2006), o AH utiliza um algoritmo hash, podendo ser: MD5 (Message Digest 5) e SHA1 ou SHA2 (Secure Hash Algoritm). Estes geram um valor único, os quais podem ser chamados de valor hash ou código de autenticação, com o objetivo de dificultar que outra mensagem utilize esse mesmo valor. Desta forma, o valor gerado é adicionado ao cabeçalho AH, permitindo que o receptor consiga realizar um novo cálculo, onde este o valor resultante deverá ser igual ao valor do hash calculada pelo emissor.

5.7.4.2. ESP (IP Encapsulating Security Payload)

Segundo Guimarães, Lins e Oliveira (2006), o protocolo ESP (Encapsulamento Seguro de Dados) tem como objetivo garantir a confidencialidade utilizando mecanismos de criptografia, autenticação, integridade e prevenção de ataques do tipo replay. Semelhante ao AH, ele utiliza um algoritmo para a criptografia dos dados (payload), onde é configurado através de uma SA (Security Association).

Figura 14: Estrutura do ESP

Fonte: Fagundes (2007)

5.7.4.3. SA (Security Association ou Associações de Segurança)

Segundo Fagundes (2007), a SA possui informações importantes que são necessárias, como: algoritmo de criptografia, função hash, chaves secretas porta de comunicação, entre outros; com o objetivo de realizar as conexões entre hosts que utilizam o protocolo IPSec.

Ainda de acordo com Fagundes (2007), ela utiliza três parâmetros para iniciar a identificação, os quais são: endereço IP, protocolo de segurança (ESP ou AH) e o índice SPI.

5.7.4.4. Bancos de Dados de Segurança

Segundo Guimarães, Lins e Oliveira (2006), são utilizados dois bancos de dados pelo protocolo IPSec, o SPD (Security Policy Database ou Banco de Dados de Políticas de Segurança), e o SAD (Security Association Database ou Banco de Dados de Associação de Segurança), onde estão associados com a SA.

De acordo com Fagundes (2007), além de o SPD utilizar políticas de segurança para o tráfego IP, os pacotes são submetidos a regras, onde o cumprimento de uma delas pode acarretar em uma ação prévia pelo administrador, como: negação dos dados, aceitação do pacote e aplicação do IPSec ou não. Os pacotes que entram e saem da rede são tratados de modo independente, onde as

interfaces de rede utilizam as políticas e o processamento deles possui uma direção específica.

Segundo Guimarães, Lins e Oliveira (2006), as informações que o SAD contém são:

- Endereço IP de origem e destino da SA;
- Modo de tunelamento operado pelo SA, podendo ser do modo túnel ou modo transporte;
- Algoritmo e a chave de autenticação;
- Algoritmo e a chave de criptografia;
- Protocolo de Segurança utilizado na SA, os quais podem ser o ESP ou o AH;
- Tempo de vida das chaves de criptografia;
- Tempo de vida das chaves de autenticação;
- Tempo de vida da SA;
- Sequencial do pacote IP dentro da SA;
- Identificação de cada SA dentro do SAD feito pelos SPIs.

5.7.5. Gerenciamento de Chaves

Segundo Fagundes (2007), o gerenciamento das chaves pode ser utilizado de maneira manual ou automática. O principal protocolo que realiza de forma automática o gerenciamento de chaves é conhecido como IKE (Internet Key Exchange), o qual associado com o protocolo ISAKMP (Internet Security Association and Key Management Protocol) tornou possível definir o mecanismo para a distribuição de chaves e com o OAKLEY, protocolo para definir a determinação das chaves.

Segundo Silva (2003), com relação ao protocolo ISAKMP é possível destacar que:

> “O ISAKMP define como duas entidades instituirão um canal de comunicação seguro entre elas, fazendo com que os participantes se autentiquem entre eles, trocando informações de chaves e negociando serviços de segurança. Entretanto, não especifica como a autenticação

> é feita ou quais as chaves serão geradas, ou seja, é definido um caminho seguro.”

Segundo Guimarães, Lins e Oliveira (2006), são necessários mecanismos para que o protocolo ISAKMP possa definir a troca de chaves e o procedimento para a autenticação, onde o protocolo OAKLEY fará o atendimento desses requerimentos.

Segundo Fagundes (2007), a criação do túnel pode ser realizada em duas fases, o qual será feita pelo protocolo IKE integrado com o ISAKMP:

A fase 1 é realizado um processo de segurança pelo ISAKMP, onde é estabelecida a conexão para a troca de informações, como: parâmetros de chaves e valores randômicos, a fim de evitar ataques do tipo replay. Desta forma, as informações passarão por métodos de autenticações, os quais podem ser:

- **Segredo Compartilhado:** é criada uma chave, onde ela será submetida a um processo de hash, com o objetivo de garantir a autenticidade durante a transmissão das informações.
- **Assinatura Digital:** os certificados digitais armazenam as assinaturas digitais, os quais estes contêm todas as assinaturas dos usuários, permitindo assim realizar a autenticação do mesmo.
- **Criptografia de chaves públicas:** são as chaves criptográficas utilizadas pelas entidades.

Ainda de acordo com Fagundes (2007), a fase 2 ou também conhecida como Modo Rápido, utiliza um canal seguro realizado na fase 1 garantindo a segurança dos dados, onde estes serão negociados pelas SA IPSec e transmitidos para cada SADs para cada nó ao final desta negociação. É possível utilizar uma alternativa, com o objetivo de aumentar a segurança, o qual é chamado de Perfect Forward Secrecy (PFS). Ela permite que a uma nova chave será baseada no algoritmo Diffie-Hellman, podendo acarretar na queda do desempenho.

5.7.6. Protocolos SSL/TLS

De acordo com Fagundes (2007), o protocolo SSL tem como finalidade proporcionar a segurança entre cliente/servidor, podendo evitar quaisquer problemas, como: interceptação de informações. Ele está presente na camada de Transporte e na de Aplicação, o qual permite trabalhar com outros tipos de protocolos, como: HTTP, FTP, Telnet, entre outros. O SSL recebeu o nome de TLS (Transport Layer Security) devido à padronização do mesmo.

Figura 15: Estrutura das camadas do Protocolo SSL/TLS

Fonte: Fagundes (2007)

Segundo Fagundes (2007), o protocolo SSL/TLS pode ser dividido em duas camadas: Handshake e Record, podendo ser descritas da seguinte forma:

a) SSL Handshake

Este protocolo tem como função autenticar os clientes, servidores e fornecer parâmetros para auxiliar no funcionamento do SSL Record. Desta forma, as mensagens de Handshake utilizam um mecanismo de segurança chamado MAC (Message Authetication Code). Ele possui duas fases, onde a primeira consiste em realizar a escolha das chaves para o cliente e o servidor, a autenticação do servidor e a substituição da chave mestra. Na segunda fase é realizada a autenticação do cliente, podendo está não ser necessária. O SSL Handshake faz uso de outros protocolos, como: Change Cipher Spec Protocol e o Alert Protocol, os quais estes auxiliarão para a segurança dos dados.

Figura 16: Estrutura da mensagem do protocolo SSL Handshake

Fonte: Fagundes (2007)

b) Change Cipher Spec Protocol

Ele é responsável por realizar a substituição dos algoritmos de criptografia, onde consiste em uma variável a fim de indicar o método criptografia que será necessário utilizar, podendo ser feita tanto pelo cliente como pelo servidor.

c) Alert Protocol

O Alert Protocol é responsável por monitorar os erros que ocorrerem durante a transmissão do SSL, onde será enviada para a próxima extremidade da conexão mensagens contendo alertas para os erros encontrados. Se ocorrerem muitos erros, a conexão é suspendida.

d) SSL Record

Este protocolo, após o receber os dados do protocolo SSL Handshake, será responsável por fragmentá-los em tamanhos fixos adicionando um código MAC utilizando funções de hash, como: MD5 ou SHA-1, onde os dados são criptografados e transmitidos para o receptor.

5.8. Segurança AAA

Segundo Guimarães, Lins e Oliveira (2006), a segurança AAA (Authentication, Authorization e Accounting) funciona com base em uma arquitetura modular, permitindo auxiliar assim na administração das VPNs. Eles podem ser descritos da seguinte forma:

- **Authentication:** mecanismo responsável por autenticar um usuário, a fim de que este prove que é realmente quem diz ser, onde algumas técnicas

utilizadas para a autenticação é através de senhas, desafios (pergunta/resposta), biometria, entre outros.

- **Authorization:** este mecanismos tem como principal objetivo definir quais recursos cada usuário poderá ter acesso e que direitos ele terá, como: leitura, escrita e execução.
- **Accounting:** já este mecanismo permite monitorar as atividades realizadas pelos usuários, ou seja, quais documentos ele acessou ou quais aplicações foram utilizadas pelo mesmo, a fim de manter um controle seguro sobre a rede e prevenir contra intrusões.

5.9. Protocolos de Autenticação

Segundo Tanenbaum (2003), os protocolos de autenticação são responsáveis por autenticarem os dois nós de uma conexão, onde eles utilizam protocolos complexos e criptografia, a fim de realizar uma conexão VPN. Com isso, se tornou possível identificar se um usuário é realmente quem diz ser. Neste capítulo serão descritos alguns protocolos de autenticação existentes, como:

5.9.1. PAP (Password Authetication Protocol)

Segundo Guimarães, Lins e Oliveira (2006), o protocolo PAP realiza uma conexão utilizando o protocolo PPP e logo depois a senha é transmitida em um formato string para um servidor NAS (Network Authentication Service ou Serviço de Autenticação da Rede), onde por fim ela passa por um processo de checagem das informações, com o objetivo de liberar o acesso à rede caso elas estiverem corretas.

Porém o protocolo PAP possui algumas fragilidades, de acordo com Guimarães, Lins e Oliveira (2006), como:

- Não existe um processo de criptografia durante o envio do login (nome do usuário) e da senha para o servidor NAS;
- Autenticação é realizada apenas no início da conexão;
- Não oferece suporte contra ataques de reprodução ou tentativas de erros.

5.9.2. CHAP (Challenge Handshake Authentication Protocol)

De acordo com Guimarães, Lins e Oliveira (2006), o protocolo CHAP é muito utilizado em plataformas Linux e o método de conexão é realizado através do protocolo PPP, semelhante ao protocolo PAP. Entretanto o processo de autenticação do CHAP é relativamente mais complexo, pois a senha não é transmitida durante a comunicação, mas utilizada com o objetivo de gerar uma string hash a partir do desafio enviado pelo servidor.

Neste contexto, segundo TechNet (2005), Guimarães, Lins e Oliveira (2006), o processo de autenticação poderá ser realizado da seguinte forma: O Servidor de Autenticação enviará um desafio ao cliente remoto, onde este deverá calcular a valor hash (algoritmo MD5) do desafio para responder e reenviar a resposta ao servidor. Então o servidor deverá verificar esta resposta a partir do valor do hash esperado, onde ele utilizará a senha do usuário para decifrar a mensagem, podendo autorizá-lo ou não.

De acordo com Guimarães, Lins e Oliveira (2006), este processo pode repetir em determinados intervalos de tempo, sendo necessário realizar todos esses processos novamente.

5.9.3. EAP (Extensible Authentication Protocol)

Segundo Guimarães, Lins e Oliveira (2006), o EAP é um protocolo de autenticação, o qual utiliza vários mecanismos de autenticação, comparados com os protocolos PAP e CHAP. O EAP permite utilizar vários tipos de autenticação, os quais somente irão funcionar após o estabelecimento de uma conexão.

Ainda de acordo Guimarães, Lins e Oliveira (2006), eles podem ser:

- **MD5 Challenge:** especifica que através da função hash MD5 permite gerar os desafios e respostas.
- **One-Time Password:** para cada seção é criada somente uma senha.
- **Generic Token Card:** para cada seção é criada uma combinação numérica

aleatória.

5.9.4. RADIUS

Segundo Guimarães, Lins e Oliveira (2006), o RADIUS (Remote Authentication Dial-in User Service ou Serviço de Autenticação Remota de Usuários Dial-in) utiliza uma arquitetura cliente/servidor, o qual ele adiciona um servidor de acesso remoto, com o objetivo de realizar a autenticação e autorização dos usuários, a contabilização e monitoração dos recursos que serão utilizados pelos usuários.

Segundo a TechNet (2005), para a implantação do protocolo RADIUS existe dois componentes:

- **Cliente RADIUS:** é geralmente um servidor NAS ou um servidor VPN, o qual é responsável por enviar as credenciais e informações contendo os parâmetros de ligações em um formato de mensagem RADIUS até chegarem ao servidor RADIUS. Os clientes podem enviar aos servidores RADIUS mensagens de gestão das contas RADIUS.
- **Servidor RADIUS:** é responsável por autenticar e permitir o acesso um cliente RADIUS, devolvendo uma resposta em formato de mensagem RADIUS.

Segundo Wenstrom (2002) o protocolo RADIUS suporta recursos de um Servidor de Segurança, os quais podem ser:

- Fornecer suporte AAA para os usuários remotos;
- Utiliza o protocolo UDP (porta 1812), a fim de comunicar o servidor NAS e o Servidor de Segurança;
- Possui serviços de autenticação e autorização, permitindo autenticar um cliente e enviar informações de configurações do servidor a eles;
- Utiliza o hash MD5 para criptografar as senhas dos usuários;
- Permite utilizar a autenticação através de perguntas/respostas PAP e CHAP;
- As transações efetuadas pelo cliente e o servidor de segurança são autenticadas através do segredo compartilhado.

5.9.5. TACACS+

Segundo Guimarães, Lins e Oliveira (2006), o TACACS+ (Terminal Access Controller Access-Control System Plus) é um protocolo responsável por controlar de modo centralizado os usuários que procuram ter acesso através do servidor NAS e é um aplicativo AAA (Authentication, Authorization, and Accounting) para os servidores de segurança. O TACACS+ apresenta muitas semelhanças com o RADIUS, entretanto podem ser destacadas algumas diferenças, como:

- O TACACS+ além de oferecer suporte ao AAA, ele separa-os de forma individual, facilitando para o acesso administrativo;
- O protocolo de transporte utilizado pelo TACACS+ é o TCP, enquanto o RADIUS utiliza o protocolo UDP;
- O TACACS+ utiliza autenticação através de perguntas/resposta, onde ela é bidirecional, ou seja, a pergunta pode partir do servidor TACACS+ para o cliente e vice-versa;
- O TACACS+ criptografa todos os pacotes, garantindo a integridade deles, onde o RADIUS apenas criptografa a senha do usuário.

5.9.6. Kerberos

Segundo Guimarães, Lins e Oliveira (2006), o protocolo de autenticação Kerberos desenvolvido pela MIT (Massachusstes Institute of Technology), tem como principal objetivo prover um forte esquema de autenticação entre as estações cliente/servidor, o qual ele utiliza o algoritmo de criptografia 3-DES garantindo a autenticidade.

Entretanto, ainda segundo Guimarães, Lins e Oliveira (2006), o protocolo Kerberos necessita de outra entidade validadora, conhecida como KDC (Key Distribution Center ou Centro de Distribuição de Chaves), o qual é responsável por verificar de forma segura os usuários e os serviços, onde eles são armazenados em uma base de dados.

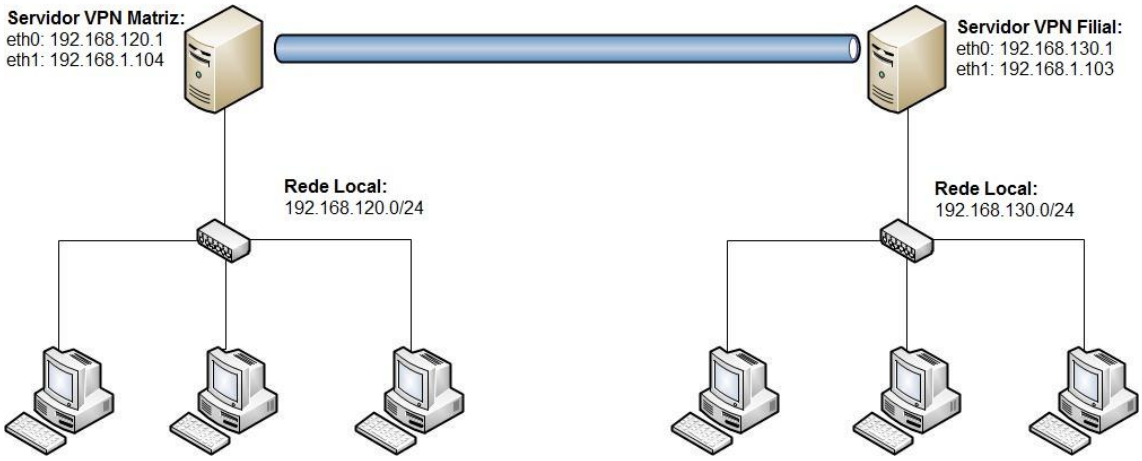
Outra característica do KDC, de acordo com Guimarães, Lins e Oliveira (2006), é que ele realiza verificações dos seus usuários e serviços, a fim de verificar se eles são quem dizem ser e o que afirmam ser. Para isso, o KDC utiliza bilhetes, onde são trocados de tempos em tempos e são armazenados em caches de credenciais, possibilitando serem utilizados substituindo o mecanismo de autenticação padrão (login/senha).

Segundo Guimarães, Lins e Oliveira (2006), o Kerberos permite ser utilizado em autenticar sessões PPP, logins em Servidores NAS, acesso a serviços FTP, entre outros.

6. Estudo de Caso: Configuração e Verificação de segurança da VPN

O estudo de caso foi implementado em um ambiente Linux (Debian 6) utilizando a estrutura Gateway-Gateway, onde a aplicação escolhida faz uso de chaves públicas com base no SSL/TLS e RSA, representado na figura 16:

Figura 17: Cenário do Estudo de Caso



Fonte: Próprio autor (2012)

Esta demonstração tem como objetivo conectar duas redes diferentes de uma mesma empresa, onde neste caso o servidor VPN Matriz ficou instalado na matriz e o servidor VPN Filial ficou na filial, possibilitando que a troca de informações seja feita de forma rápida e eficiente. As interfaces de rede dos servidores foram definidas da seguinte forma:

Matriz

- eth0: 192.168.120.1
- eth1: 192.168.1.104
- Rede local: 192.168.120.0/24

Filial

- eth0: 192.168.130.1
- eth1: 192.168.1.103
- Rede local: 192.168.130.0/24

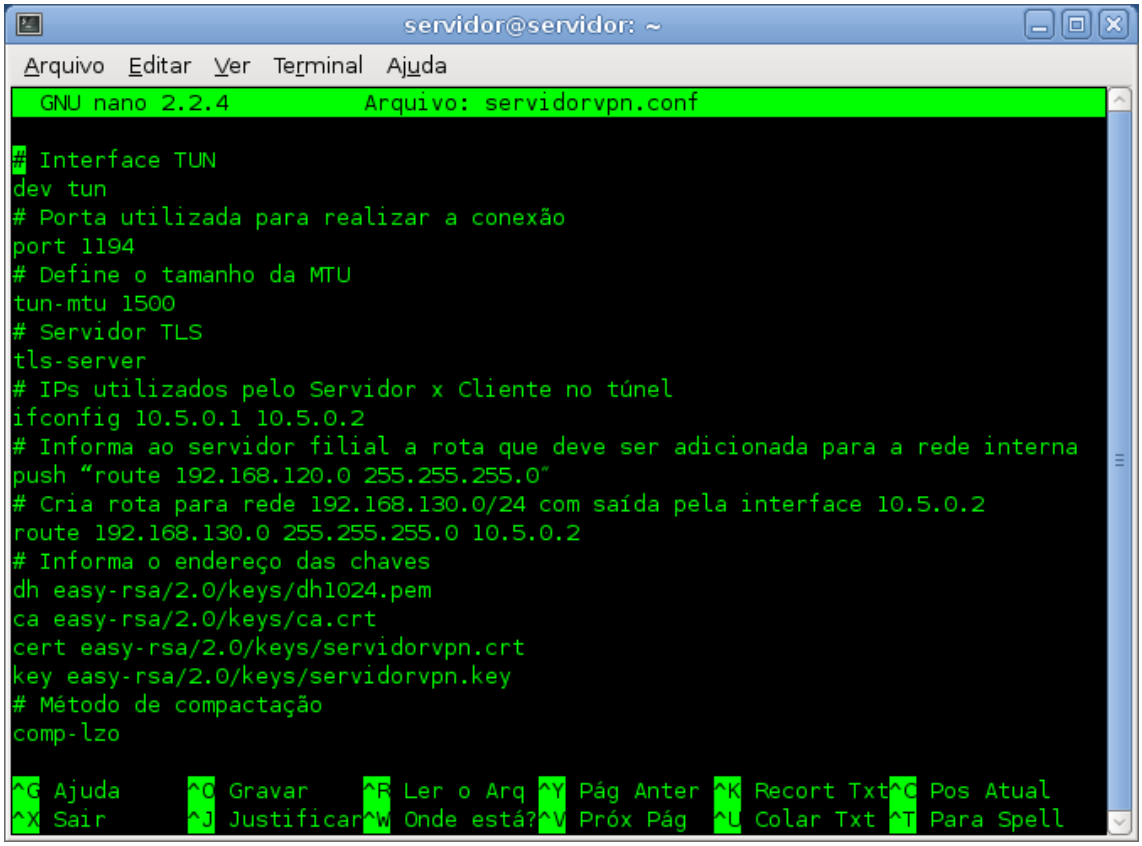
6.1. OpenVPN

Para a implementação foi utilizado uma ferramenta chamada OpenVPN, o qual permite ser instalado em vários plataformas, como: Windows, Linux, FreeBSD, MacOS X e Solaris. Com o objetivo de proporcionar mais segurança, ele utiliza o OpenSSL, mecanismo responsável por realizar criptografia durante a transmissão, podendo ser enviados utilizando o protocolo TCP ou UDP. O OpenVPN oferece suporte para a biblioteca LZO, responsável por realizar recursos de compactação das informações que serão enviadas.

6.1.1. Scripts de Configuração do OpenVPN

Os scripts são responsáveis pela inicialização da conexão VPN, onde estão armazenados dentro do diretório /etc/openvpn. No servidor da matriz, o script servidorvpn.conf (nome do script) foi definido da seguinte forma:

Figura 18: Script de configuração no Servidor VPN Matriz



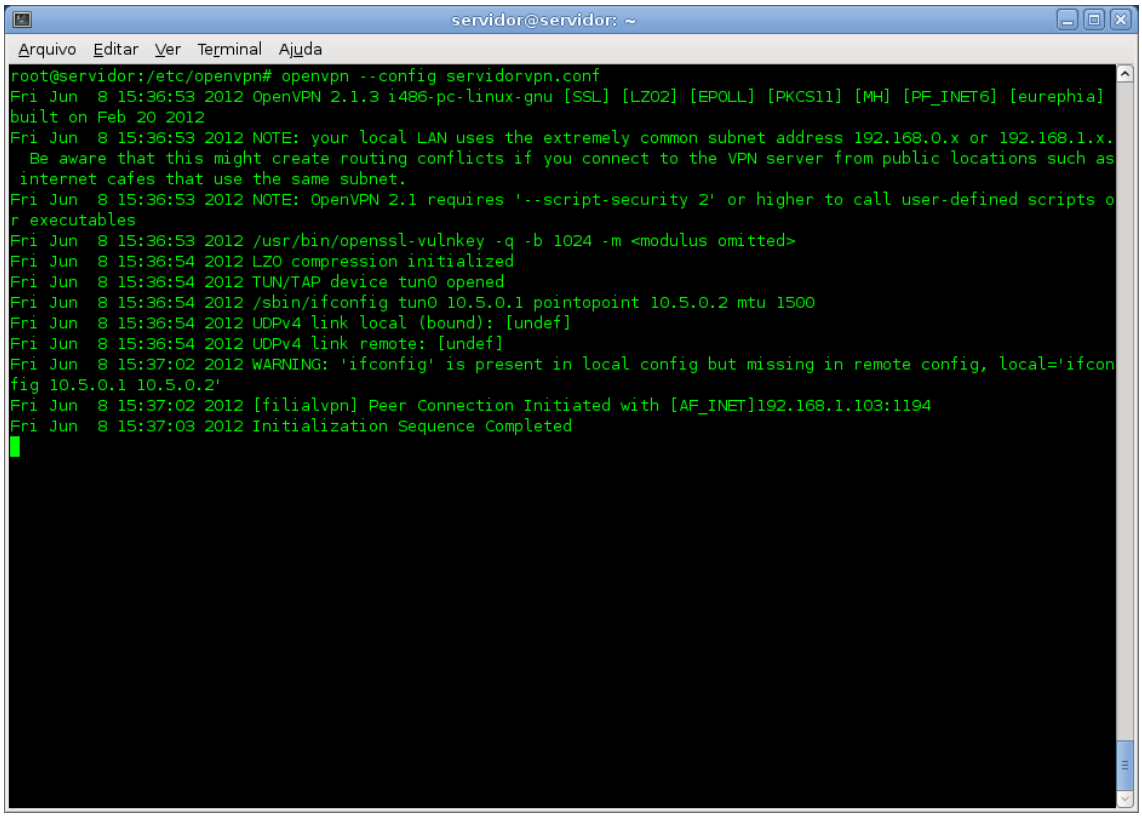
Fonte: Próprio autor (2012)

Após a definição do script é necessário inicializá-lo utilizando o seguinte comando:

 # openvpn - -config servidorvpn.conf

Desta forma, o servidor ficará aguardando para receber a conexão do servidor VPN na filial, onde feito isso o Servidor VPN Matriz irá exibir a seguinte mensagem ilustrada na figura 18, informando que a conexão foi completada e iniciada:

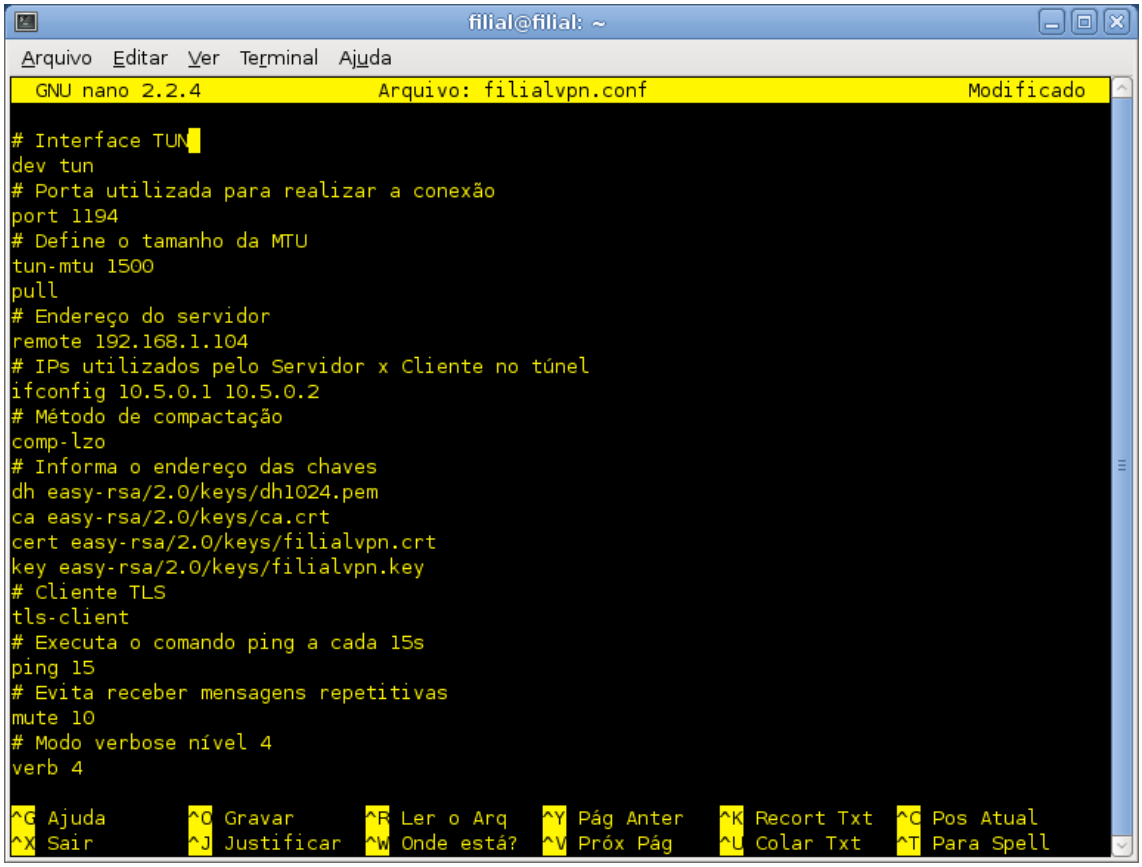
Figura 19: Script do Servidor VPN Matriz inicializado



Fonte: Próprio autor (2012)

Após a realização de todo o processo de configuração do Servidor VPN Matriz, é preciso realizar os mesmos procedimentos no Servidor VPN Filial. Para isso, foi criado um arquivo chamado filialvpn.conf, onde foi definido os seguintes scripts:

Figura 20: Script de configuração no Servidor VPN Filial



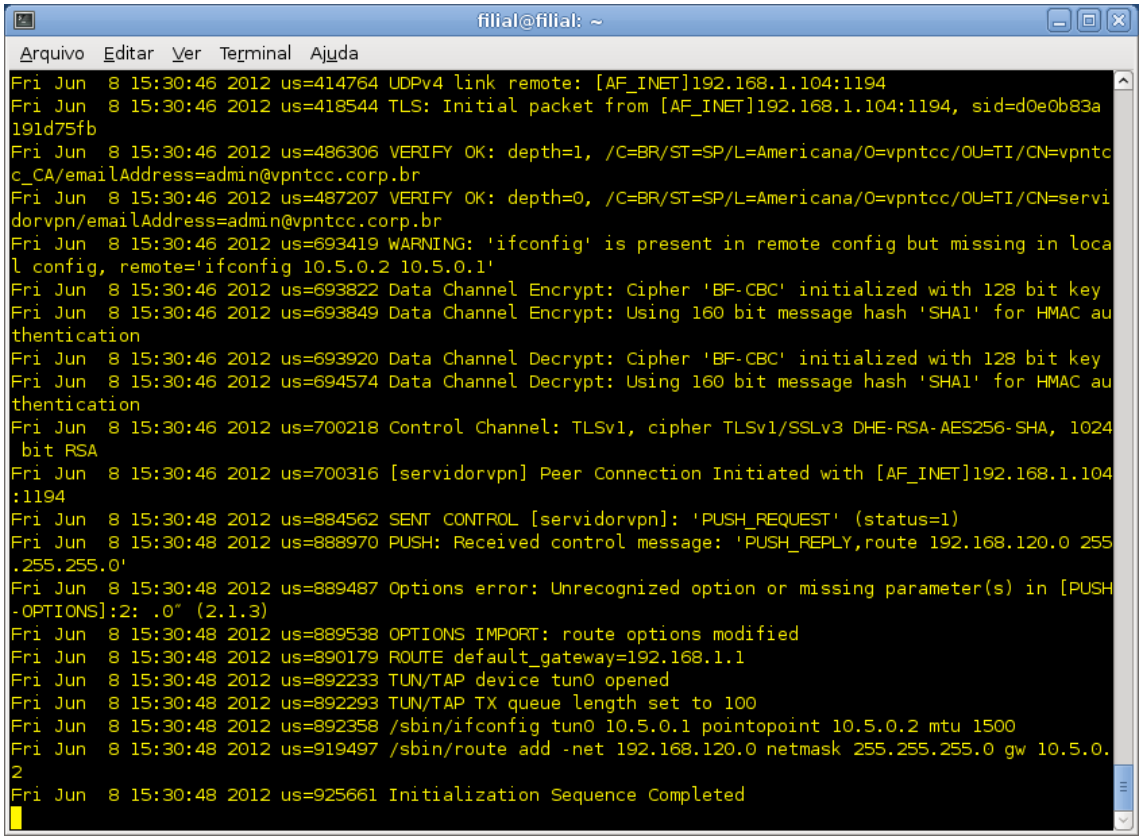
Fonte: Próprio autor (2012)

Com o script do servidor VPN da filial definidos será necessário utilizar o comando abaixo para inicia-lo:

 # openvpn - -config filialvpn.conf

Sendo assim, o servidor realizará a conexão com o Servidor VPN Matriz, onde será completada e inicializada exibindo as seguintes mensagens:

Figura 21: Script do Servidor VPN Filial inicializado

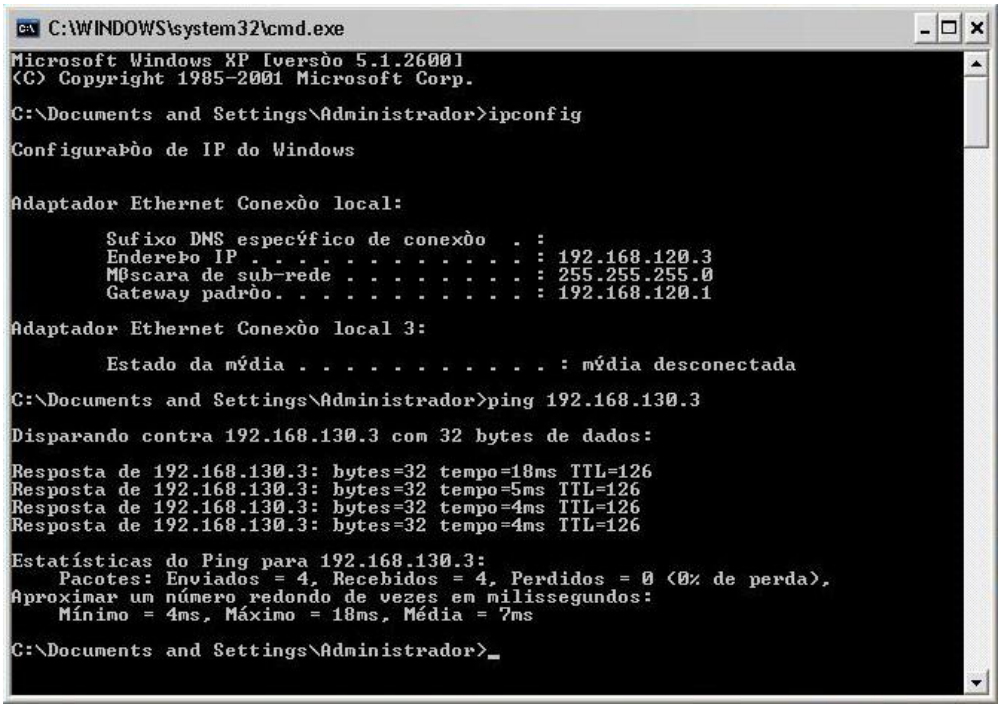


Fonte: Próprio autor (2012)

Com o objetivo de verificar se a conexão foi realmente estabelecida, foi preciso realizar testes nas máquinas clientes, onde uma delas está situada na matriz e a outra na filial, sendo possível obter os seguintes resultados:

Cliente-matriz:

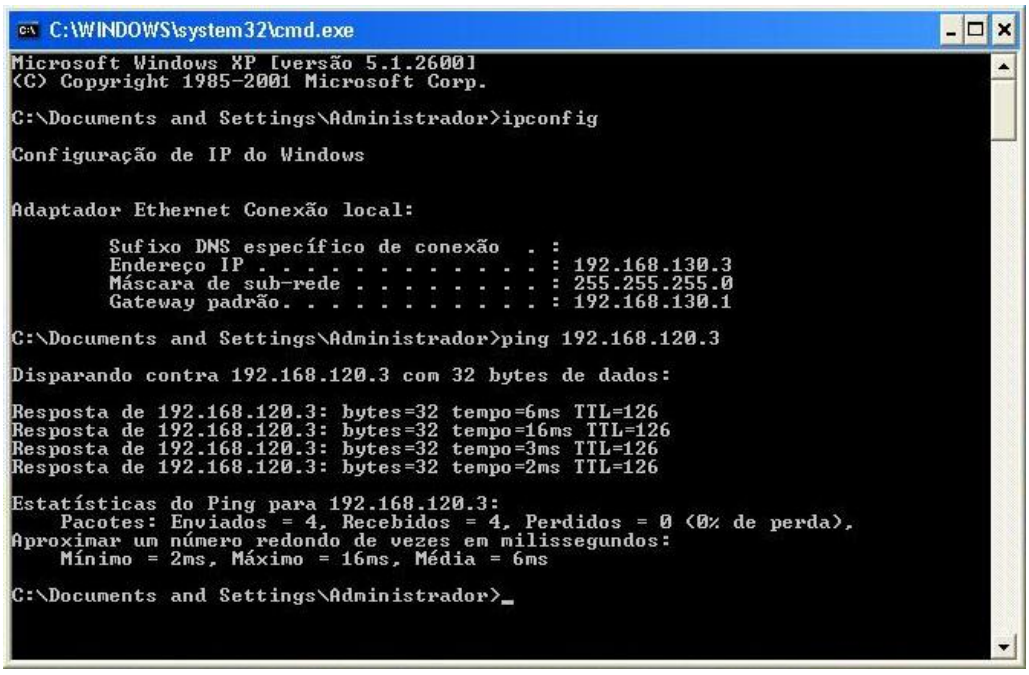
Figura 22: Teste de ping realizado no cliente-matriz



Fonte: Próprio autor (2012)

Cliente-filial:

Figura 23: Teste de ping realizado no cliente-filial



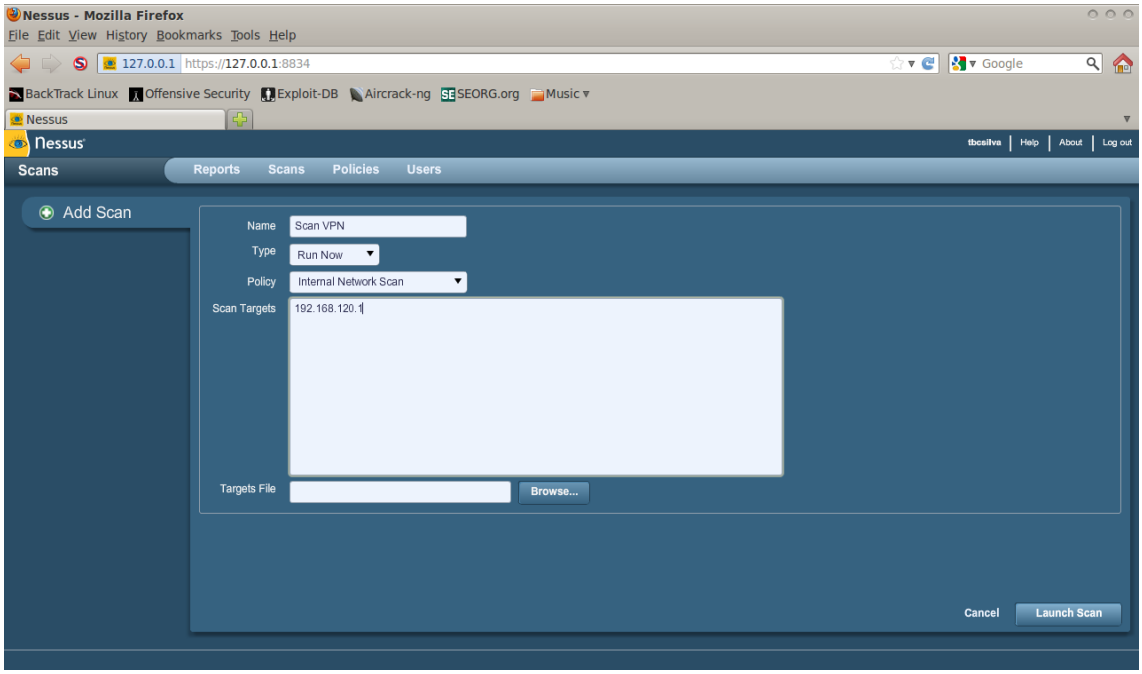
Fonte: Próprio autor (2012)

6.2. Nessus

Com o objetivo de garantir a segurança nos servidores VPN, foi utilizada outra ferramenta, chamada Nessus, onde é responsável por descobrir e corrigir vulnerabilidades existentes. Desta forma, ele realiza um escaneamento de todas as portas do servidor, o qual exibirá uma lista contendo as portas escaneadas e o nível de segurança de cada uma delas. Para isso, o Nessus foi instalado na plataforma Linux (Backtrack 5), o qual o escaneamento foi feito da seguinte forma:

Primeiramente, foi necessário definir no campo “Name” o nome do escaneamento, a fim de facilitar a procura dele no futuro. Com relação ao Type (Modelo) foi deixado como padrão, onde será executado logo depois de completar o preenchimento das regras e a Policy (Política) foi definida para realizar o escaneamento apenas na rede interna da empresa. Por fim no campo Scan Targets (Alvo) é o local que são definidos os IPs que serão escaneados, onde foi colocado o IP do Servidor VPN Matriz.

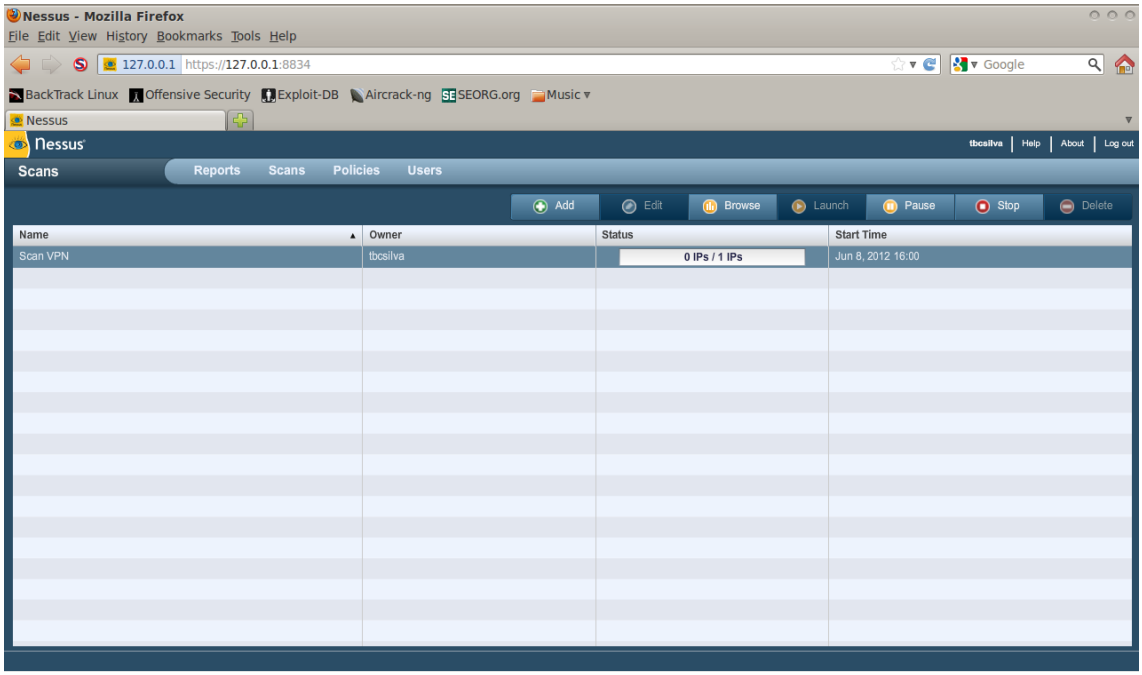
Figura 24: Definição das regras para o escaneamento do Nessus



Fonte: Próprio autor (2012)

Ao fim desse processo, o Nessus iniciará o escaneamento do servidor definido, o qual pode demorar um pouco devido ao alto tráfego na rede interna, podendo ser visualizado na figura abaixo:

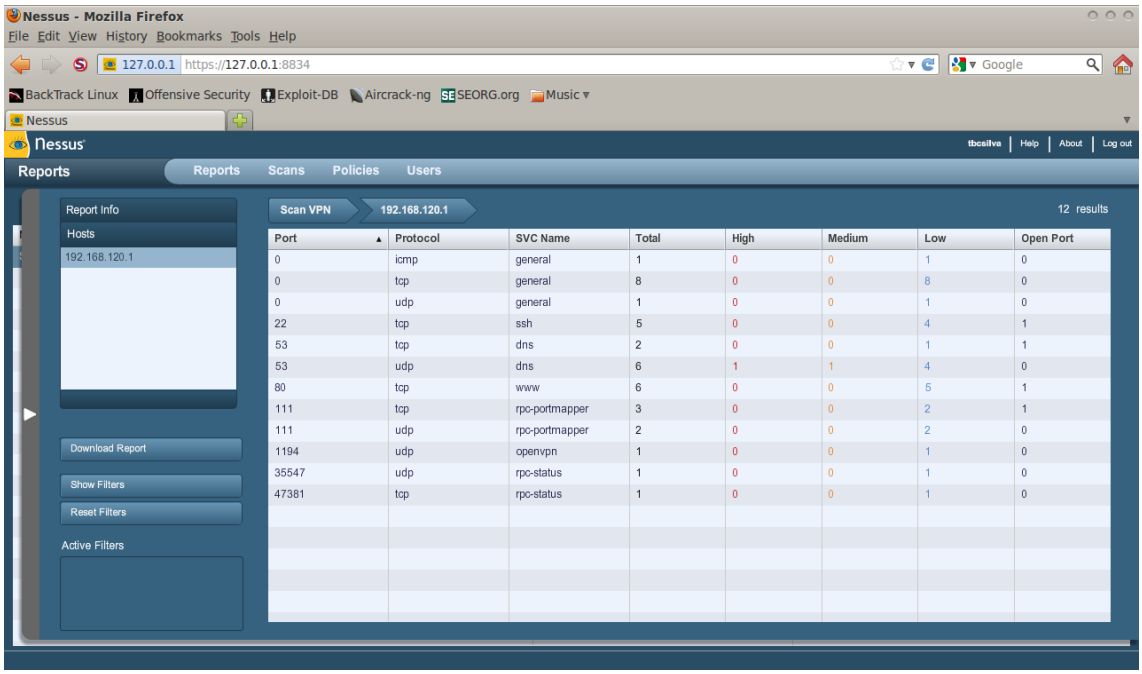
Figura 25: Escaneamento iniciado no Nessus



Fonte: Próprio autor (2012)

Após finalizar o escaneamento, o Nessus exibirá uma lista contendo todas as portas abertas no servidor e seus respectivos níveis de segurança.

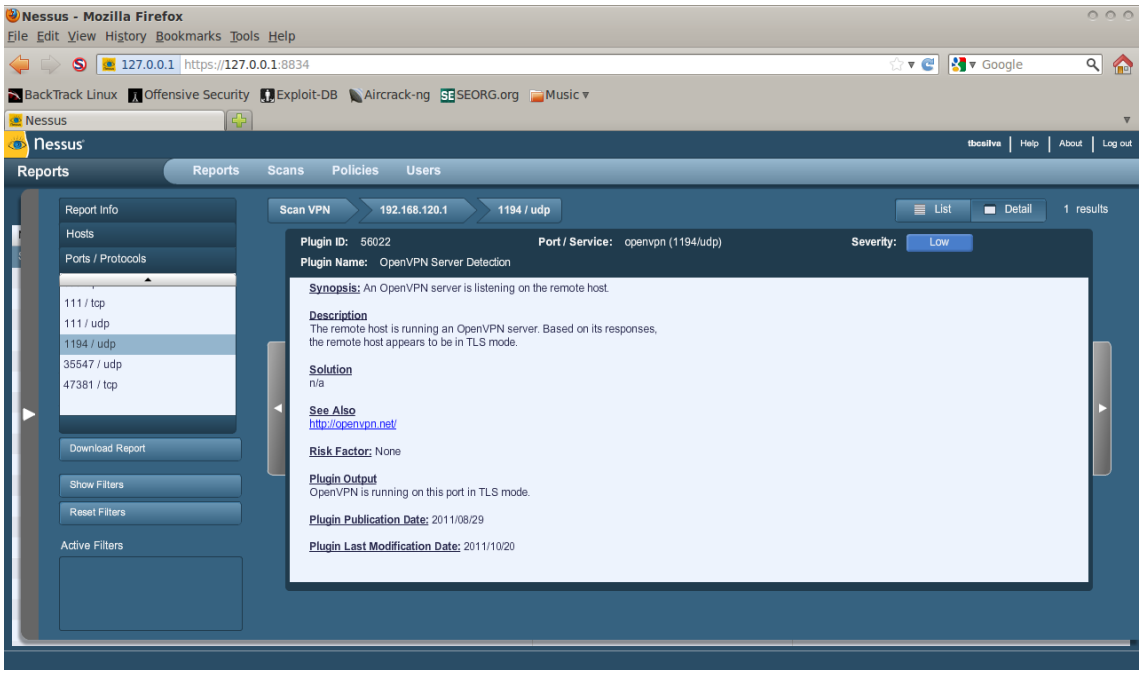
Figura 26: Lista das portas escaneadas



Fonte: Próprio autor (2012)

Desta forma é possível visualizar de forma detalhada a descrição do serviço utilizado, o risco, soluções, entre outras informações, o qual é exibida pela figura abaixo:

Figura 27: Detalhes da porta utilizado pelo OpenVPN



Fonte: Próprio autor (2012)

Com o Nessus é possível, de forma eficiente, resolver vários incidentes de invasão, garantindo mais segurança nos servidores.

7. Conclusão

As Redes Privadas Virtuais representam um avanço da tecnologia nos dias de hoje, o qual permitiu interligar de modo seguro diversas redes através da Internet, facilitando a comunicação e transmissão das informações. Além disso, elas permitiram eliminar as conexões realizadas por linhas dedicadas, os quais geravam muitos gastos para a sua implementação.

Pode-se dizer também que os inúmeros protocolos de tunelamento e protocolos de autenticação, além da utilização de firewalls, possibilitam realizar diferentes implementações nas estruturas de segurança de uma VPN, evitando que quaisquer tipos de ataques possam ocorrer, podendo causar vários danos para uma organização.

Por fim, o desenvolvimento do estudo de caso, permitiu analisar como é realizado uma conexão entre dois servidores VPN, através da criação dos scripts e certificados, onde foi possível também avaliar as suas vulnerabilidades, através de ferramentas específicas, os quais informam onde permite utilizar recursos para corrigi-los.

8. Referências Bibliográficas

ALECRIM, E., **O que é Tecnologia da Informação (TI)**, 2011. Disponível em: http://www.infowester.com/ti.php. Acessado em Abril de 2012.

CHIN, L. K., **Rede Privada Virtual – VPN**, 1998. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acessado em Fevereiro de 2012.

FAGUNDES, B. A., **Uma Implementação de VPN**, 2007. 76 f. Monografia de Graduação (Ciência da Computação) – Instituto Superior de Tecnologia em Ciência da Computação de Petrópolis, Rio de Janeiro.

GUIMARÃES, A. G., LINS, Rafael D., OLIVEIRA, R., Segurança com Redes Privadas Virtuais - VPNs. Rio de Janeiro: Brasport, 2006. 210 p.

NORTHCUTT, S., ZELTSER, L., WINTERS, S., FREDERICK, Karen K., RITCHEY, Ronald W. **Desvendando Segurança em Redes.** Ed. Campus, Rio de Janeiro-RJ, 2002.

PACIEVITCH, T., **Tecnologia da Informação e Comunicação**, 2009. Disponível em: http://www.infoescola.com/informatica/tecnologia-da-informacao-e-comunicacao. Acessado em Março de 2012.

SANTANA, A. V., **VNP: Uma análise de conectividade**, 1999. Disponível em: http://www1.serpro.gov.br/publicacoes/tematec/pubtem48.htm. Acessado em Março de 2012.

SILVA, Lino Sarlo. **VPN: Aprenda a construir redes privadas virtuais em plataformas Linux e Windows**, Ed. Novatec, São Paulo, SP, Brasil – 2003.

TANENBAUM, Andrew. **Computer Networks**. Fourth Edition. Prentice Hall. New Jersey, USA, 2003.

TechNet, **Protocolo CHAP (protocolo de autenticação de handshake de desafio)**, 2005. Disponível em: http://technet.microsoft.com/en-us/library/cc775567(v=ws.10).aspx. Acessado em Maio de 2012.

TechNet, **Protocolo RADIUS**, 2005. Disponível em: http://technet.microsoft.com/pt-

br/library/cc781821(v=ws.10).aspx. Acessado em Maio de 2012.

TYSON, J., **HowStuffWorks - Como funciona uma VPN**, 2007. Disponível em: http://informatica.hsw.uol.com.br/vpn.htm. Acessado em Fevereiro de 2012.

WENSTROM, Michael. **Managing Cisco Network Security**. Editora Alta Books, Rio de Janeiro, 2002.

ZANAROLI, Ana P., LIMA, M. B., RANGEL, R. A., **VPN – Virtual Private Networks**, 2000. Disponível em: http://www.abusar.org.br/vpn/vpnport.htm. Acessado em Março de 2012.