UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
XXII CURSO DE ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

JEFFERSON LEANDRO FERREIRA

ESTUDO DE CASO DE SOLUÇÕES EM VPN IPSEC COM SERVIDORES USANDO SOFTWARE LIVRE

CURITIBA – PR
2013

JEFFERSON LEANDRO FERREIRA

ESTUDO DE CASO DE SOLUÇÕES EM VPN IPSEC COM SERVIDORES USANDO SOFTWARE LIVRE

Monografia de Especialização apresentada ao Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de “Especialista em Teleinformática e Redes de Computadores”
Orientador: Prof. Dr. Kleber Nabas

CURITIBA – PR
2013

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TERMO DE APROVAÇÃO

ESTUDO DE CASO DE SOLUÇÕES EM VPN IPSEC COM SERVIDORES USANDO SOFTWARE LIVRE

por

JEFFERSON LEANDRO FERREIRA

Esta monografia foi apresentada às 14:00h do dia 26 de FEVEREIRO de 2014 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 8,5 (OITO INTEIROS E CINCO DÉCIMOS)

Prof. Dr. Kleber Nabas
(UTFPR)

Prof. Dr. Walter Godoy Júnior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

AGRADECIMENTOS

A paciência e colaboração dos meus amigos, docentes e família.

RESUMO

FERREIRA, Jefferson Leandro. **Estudo de caso de Soluções de VPN IPsec com servidores usando Software Livre.** 2014. 77f. Programa de Pós Graduação em Teleinformática e Redes de Computadores, Universidade Tecnológica Federal do Paraná. Curitiba, 2014

Este estudo mostra dois casos de VPN IPsec interligando primeiro dois escritórios de uma empresa, e segundo interligando esta mesma empresa a um fornecedor. Os casos apresentados foram uma alternativa viável instalação, tornando os custos para a empresa baixos, requerendo um conhecimento não muito profundo em equipamentos de rede como roteadores, por exemplo. A primeira VPN implantada com o firewall monowall substituiu uma VPN oferecida por uma operadora, a um custo quatro vezes mais barato, usando circuitos de banda larga ADSLs. A segunda VPN exigia mais recursos devido a complexidade técnica, porém, o firewall pfSense atendeu todos os requisitos como roteador, e pôde ser usado para estabelecer a comunicação com o parceiro através de VPN, conectando o pfSense com roteadores Cisco.

PalavrasChave: VPN, IPsec, pfSense, monowall, lan-to-lan

ABSTRACT

FERREIRA, Jefferson Leandro. **Case Study Solutions IPsec VPN servers using Free Software.** 2014. 77f. Graduate Program in Teleinformatics and Computer Networks, Federal Technological University of Paraná. Curitiba, 2014

This study shows two cases of IPsec VPN interconnecting first, two offices of a company, and second connecting this same company to a supplier. The cases presented were a viable alternative installation, making the costs low, and not requiring a deep knowledge of network equipment such as routers, for example. The first VPN was deployed with Monowall and replaced a VPN, a four times cheaper cost using broadband ADSLs circuits. The second VPN required more resources due to technical complexity, however, the pfSense firewall has met all the requirements as a router, and could be used to estabilished a communication with the partner across the VPN, connecting pfSense and Cisco routers.

Keywords: VPN, IPsec, pfSense, monowall, lan-to-lan

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica fez o mundo sair da Era Industrial para a Era da Informação exatamente pela necessidade da informação estar disponível o mais rápido possível e de forma descentralizada. A tecnologia adicionou ao modelo de produção industrial maneiras precisas de obter dados e previsões sobre a produção em tempo real, envolvendo os mais diferentes dados, como matéria prima, clientes, fornecedores, demandas, concorrentes entre outros.

Ocorre que em muitas grandes empresas, diga-se na maioria delas, as informações de produção podem ser até descentralizadas, mas em algum momento essas informações precisam estar disponíveis para executivos e tomadores de decisões em vários locais ao mesmo tempo, e é nesse ponto que a tecnologia faz o seu papel, seja em empresas do ramo tecnológico ou não.

1.1 Estruturas de Rede

Rede local é uma estrutura de comunicação organizada dentro de um ambiente, seja ambiente industrial ou comercial ou residencial. Essa estrutura é composta de vários dispositivos, tais como computadores, cabos, concentradores, cada um executando uma função diferente com o objetivo de manter a comunicação e o armazenamento de dados centralizado, ou não.

As primeiras redes de computadores tinham seu modelo de processamento centralizado, sendo feito por terminais chamados de “terminais burros”, acessando um computador central. Esses terminais não tinham nenhum poder de processamento, ficando este todo para o computador central. A comunicação entre os terminais e computador central era feita por acesso serial, e, mesmo usando uma comunicação mais simples, comparada a que usamos nos dias de hoje, é claro, a comunicação serial era feita em cima de um protocolo. Ainda no modelo antigo, para sistemas de grande porte para as primeiras redes,quando havia a necessidade de grande numero de terminais, estes eram conectados a controladoras de comunicação e, esta controlava o acesso ao computador central. O modelo inicial descrito acima era plausível, haja vista o alto custo de componentes, armazenamento e processamento.

Nos anos 80, o modelo sofreu modificações com o advento do computador pessoal, o PC. O PC evoluiu em hardware e software até os anos 90, e é claro não deixou de evoluir, mas no início dos anos 90, houve uma mudança grande nos padrões de redes de computadores, de duas formas. A primeira trouxe parte do processamento para as estações de usuários, que já não tinha mais um terminal sem processamento e sem armazenamento. O usuário final tinha espaço para guardar arquivos pessoais como planilhas, documentos textos, imagens, e também poder processar cálculos que antes dependiam de um computador central. A outra forma de mudança é uma continuidade da primeira, que, tendo toda a capacidade de processamento e armazenamento local, houve uma necessidade de compartilhamento de arquivos com outros usuários. E junto com essa necessidade houve uma evolução dos sistemas operacionais de rede que proporcionaram compartilhamento e organização de redes locais formadas por computadores pessoais e dispositivos periféricos.

Desta forma podemos conceituar as Redes Locais de Computadores como um grupo de computadores interligados entre si através de uma rede física (par trançado, fibra óptica ou conexão sem fio) através de um protocolo comum, em um ambiente variando em algumas dezenas de metros. As redes locais ainda podem ser classificadas em corporativas e domésticas.

1.1.1 Interconexão de Redes Locais

Novamente a evolução dos negócios e da tecnologia levou a expansão de escritórios, e com ela a necessidade de troca de informações entre uma sede e uma (ou várias) filial, havendo a necessidade de interconexão de redes locais.

Na tecnologia de redes locais existe uma ligação muito forte entre telecomunicações e informática. A informática diz respeito aos aplicativos e dados, e as telecomunicações ao transporte destes dados.

Até o começo dos anos 90, essa ligação era ainda mais forte, pois não havia ainda uma difusão maciça do protocolo Ethernet. Havia muita comunicação serial e protocolos de comunicação sobre serial, inclusive o TCP/IP.

Devido ao avanço tecnológico e a popularização do PC, o protocolo Ethernet e os sistemas operacionais para a plataforma x86 provocaram um avanço devido a facilidade no estabelecimento de redes locais. Sistemas

Operacionais como Windows 3.11, Windows NT, Novell Netware, tornaram o compartilhamento de arquivos e controle de usuários uma tarefa bem mais simples se comparada ao que era feito no acesso de Mainframes. Os protocolos mais usados para o funcionamento dessas redes locais eram o IPX/SPX para as redes de servidores Netware com estações Windowse TCP/IP para servidores Windows NT com estações Windows 3.11 ou Windows 9X. Aqui uma ressalva, o TCP/IP poderia ser usado em redes Novell normalmente assim como o IPX para as redes Windows, no entanto devido a padronização do TCP/IP para o acesso a Internet o mercado optou por adotar o TCP/IP como padrão.

Localmente, as redes locais usavam os sistemas operacionais descritos anteriormente para controle lógico. Fisicamente as redes locais eram inicialmente interconectadas por cabos coaxiais, que mais tarde foram migradas para a tecnologia de par trançado, tecnologia que permanece forte até hoje, porém é claro, com atualizações.

Mas em uma rede corporativa, mesmo no início, já começou com a necessidade de comunicação entre uma rede e outra. Nesse ponto entrou as interconexões que tornaram as redes locais (LANs) em redes metropolitanas (MANs) ou redes de longa distância (WANs). Para essas interconexões que poderiam variar entre alguns quilômetros e algumas centenas de quilômetros, ou até mesmo milhares de quilômetros, os meios usados para implementar eram também os mais variados, podendo ser usados par metálico, fibra óptica, enlace de rádio ou enlace de satélite.

Igualmente aos protocolos de redes locais, muitos protocolos de redes de longa distância foram implementados, podemos citar o X.25, Frame Relay, ATM, PPPoE, e todos com diferentes características e particularidades, mas especificamente cada um destes protocolos, estava associado à um hardware de camada física, ficando o protocolo de enlace ligado à um hardware para que houvesse tal implementação.

1.1.2 Redes Locais

As redes locais, geralmente chamadas de LANs (Local Area Network) são redes privadas dentro de um edifício ou condomínio com no máximo alguns quilômetros de tamanho (TANEMBAUM 2003). Sua atividade é ampla,

podendo ser usada para conectar computadores pessoais, dispositivos móveis, impressoras e muitos outros dispositivos. Em uma indústria, por exemplo, são conectados leitores de informações de produção,dados capturados por robôs e muitas outras informações que possam ser disponibilizadas por algum dispositivo via rede local. Devido a facilidade de conectividade entre os dispositivos da rede local, esta geralmente opera em alta velocidade. Atualmente ainda temos redes operando em 100Mbits/s mas pode-se dize que o padrão está em 1GBit/s.

1.1.3 Redes Metropolitanas

Redes Metropolitanas (MANs – MetropolitanArea Network) são redes de distâncias maiores que as LANs que normalmente compreendem alguns quilômetros.As redes de distribuição de banda larga das operadoras ou as redes de distribuição de sinais de televisão por operadoras de TV a cabo são exemplos de MANs. Essas redes operam em uma velocidade um pouco mais baixa que uma rede local, mas a um custo menor que uma rede de longa distância WAN.

1.1.4 Redes de Longa Distância

Redes de Longa Distância (WANs – WideArea Network) são redes geograficamente muito grandes, ou um apanhado de LANs ou MANs interligadas entre si formando uma grande rede. Normalmente, mesmo fazendo parte de uma grande rede, alguns serviços apenas são compartilhados a longa distância, com o objetivo de aperfeiçoar o tráfego, já que enlaces de grandes distâncias geralmente são caros, e também com o objetivo de priorizar os serviços mais importantes. Assim, serviços de autenticação e compartilhamento de arquivos ficam restritos a uma rede local, e serviços como um servidor de intranet corporativo ou qualquer serviço específico relativo ao negócio é priorizado para acesso entre os mais diferentes locais abrangidos pela WAN.

Algumas considerações sobre LANs, MANs e WANs devem ser feitas para equalizar o entendimento. Dentro de uma Rede Local (LAN), podemos ter vários segmentos de rede, lógicos ou físicos, porém é mais possível encontrar

vários segmentos lógicos (sub-redes) dentro de um mesmo segmento físico, por exemplo, um cabeamento de rede ligado a um ou vários switches, ligados a um roteador que pode prover rota para um ou várias redes.

Quando temos uma rede metropolitana ou uma rede de longa distância, o que geralmente acontece é uma interligação de redes locais através de roteadores com regras definidas para que as redes possam ter acesso entre si. A interligação dessas redes pode usar diversas tecnologias, geralmente providas por operadoras públicas de telecomunicações, que oferecem circuitos específicos dependendo da demanda que se tenha para tal serviço. Esses serviços podem ser produtos prontos para serem comercializados ou até mesmo projetos especificamente estudados para que não haja problemas na transmissão de dados entre uma rede e outra. A evolução na capacidade de armazenamento e transmissão de dados inseriu um contexto de serviço que já não é tão simples contratar um serviço de um enlace de dados de uma operadora. É preciso especificar que tipo de serviço será trafegado, que poderá ser voz, vídeo, dados, deverá ser especificado também latência, velocidade, redundância. Estas são apenas algumas das características ao se contratar um serviço de uma operadora de telecomunicações para interligação de redes. De acordo com a qualidade do serviço poderão existir diferentes equipamentos de redes envolvidos, como modems, roteadores e o meio, que pode ser par metálico, satélite ou fibra óptica.

Circuitos para enlaces de alto desempenho e alta prioridade normalmente não são únicos, a redundância deve ser uma das características principais em um projeto de enlace de dados. Para garantir a redundância são contratados enlaces de diferentes operadoras usando diferentes rotas. Em circuitos de fibra óptica, por exemplo, usa-se a topologia em anel, pois o rompimento de um ponto da fibra não coloca em risco o fornecimento do serviço.

1.2 Sistemas Operacionais e Protocolos de Rede.

1.2.1 O Modelo OSI

Com o objetivo de estabelecer a comunicação entre equipamentos de rede, computadores ou qualquer outro equipamento, estes devem estabelecer

sua comunicação usando um mesmo protocolo.Nos anos iniciais de redes havia muita desorganização, muitas empresas desenvolviam seus próprios padrões tornando muito difícil a interconexão entre padrões. Para tentar resolver esses problemas a*InternationalOrganizationStandardization* (ISO) criou um modelo para ajudar os fabricantes de hardware de rede a criar uma padronização. Então em 1984 o modelo OSI, *Open System Interconnection* se tornou um modelo bem definido de especificações feitas para manter a compatibilidade entre várias tecnologias.

O modelo OSI é uma referência na descrição de comunicação de rede, mas é claro é um modelo teórico e não é o único modelo, mas é o mais usado. O modelo OSI define sete camadas, cada uma com uma funcionalidade específica, e cada camada está associado um protocolo específico.

A comunicação de rede envolve várias camadas e vários protocolos. Uma lista de protocolos usados por um sistema, usando um protocolo por camada, é chamada de pilha de protocolo.

1.2.2 Camadas do Modelo OSI

Camada 7 – Aplicação: Camada responsável por fazer a interface de comunicação para o usuário entre a rede e a aplicação. Contém uma variedade de protocolos que são freqüentemente usados por usuários, tais como HTTP, FTP, SMTP e SSH por exemplo.

Camada 6 – Apresentação: A camada de apresentação define um padrão em como os dados são representados. A camada 6 também define criptografia como serviço da mesma camada.

Camada 5 – Sessão: Camada que define como começar, controlar e terminar uma comunicação. Essa comunicação é chamada sessão. Nesta camada encontra-se os protocolos NFS e RPC, por exemplo, e normalmente é controlada pelo sistema operacional.

Camada 4 – Transporte: A camada de transporte garante um gerenciamento virtual de circuitos entre a comunicação de dois dispositivos de rede, e contém uma série de protocolos relativos à comunicação entre dois computadores, ou seja, controle de fluxo. Por exemplo, pode conter protocolos que sejam responsáveis por ordenar pacotes que por ventura cheguem desordenados em uma das pontas da comunicação. Exemplos de protocolos de camada 4, são o TCP, UDP e o SPX.

Camada 3 – Rede: Endereçamento lógico e determinação de como os pacotes são roteados entre origem e destino são definidos nesta camada, por isso a associação entre roteamento e camada 3. Entre os protocolos relativos a esta camada encontramos o IP e o IPX.

Camada 2 – Camada de Enlace: Camada onde as especificações dizem respeito a qual meio os dados serão transmitidos, já que os protocolos dessa camada estão associados a diferentes hardwares. Os protocolos normalmente usados nessa camada são: ATM, Frame Relay, HDLC, PPP entre outros.

Camada 1 – Camada Física: Camada que especifica conectores, pinos, corrente elétrica, modulação, de luz e de sinal. Especificações de comprimento de cabo e padronizações como RJ45, V.35, V.24 EIA/TIA-232, também são descritas nesta camada.

1.2.3 O Modelo TCP/IP

O modelo de referência TCP/IP foi desenvolvido pelo Departamento de Defesa Americano (DoD – US DepartmentofDefense), com o objetivo de ser um sistema capaz de manter a comunicação em uma rede de computadores sob qualquer condição, até mesmo uma guerra nuclear, pensamento este devido a Guerra Fria. Este modelo deu origem e é o núcleo da estrutura atual da Internet.

O modelo TCP/IP consiste em quatro camadas: Aplicação, Transporte, Internet e Rede.

Mesmo tendo nomes semelhantes em algumas camadas, se compararmos com o modelo OSI, as camadas tem funções diferentes.

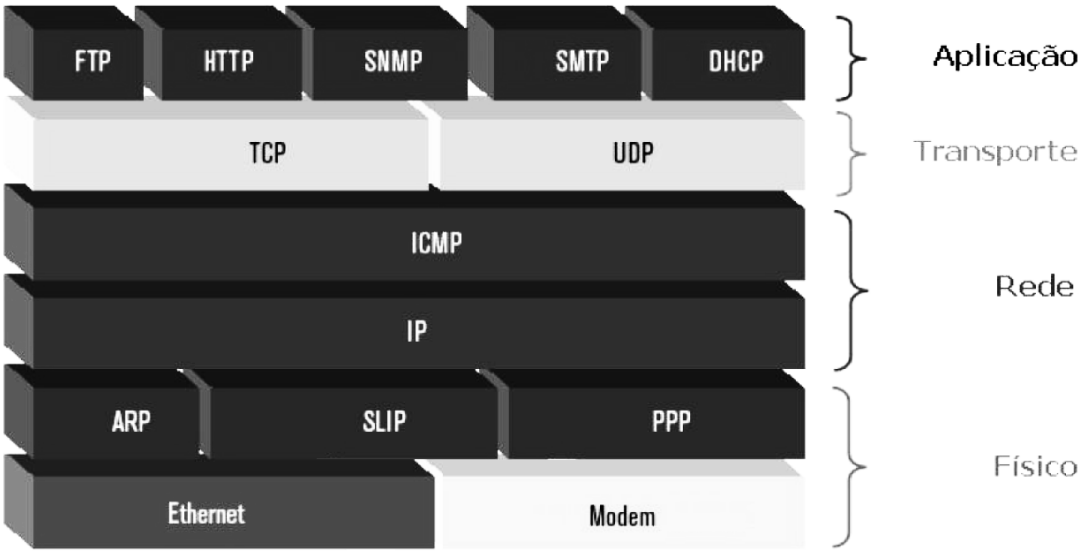

Figura 1 - Modelo TCP/IP

1.2.4 Modelo OSI versus Modelo TCP/IP

O modelo de referência OSI é um modelo teórico e útil para compreender os processos de comunicação entre computadores. No entanto na prática o modelo TCP/IP é usado na prática em toda a Internet, além de ser o protocolo mais popular utilizado atualmente. De forma que podemos tornar mais clara as semelhanças e diferenças destes modelos, que são amplamente utilizados para entender o funcionamento de um protocolo de rede.

Semelhanças:

Ambos os modelos são modelos em camadas e tem o benefício de modelar a informação por camada.

Ambos os modelos tem camada de Aplicação, mesmo incluindo diferentes serviços.

Ambos os modelos tem camada de transporte e rede, que tem funcionalidades semelhantes.

Na prática os dois modelos funcionam com um cabeçalho para cada camada, e os dados de cada camada sendo encapsulados na camada imediatamente inferior, até atingir a camada física, onde é transmitido para o meio.

Diferenças: Além das diferenças no número de camadas, sete para o modelo OSI e quatro para o modelo TCP/IP, a camada de enlace e rede do modelo OSI é combinada em uma única camada no modelo TCP/IP.

O protocolo TCP/IP parece mais simples devido ao número menor de camadas, no entanto em uma comunicação TCP/IP é possível identificar todas as camadas do modelo OSI.

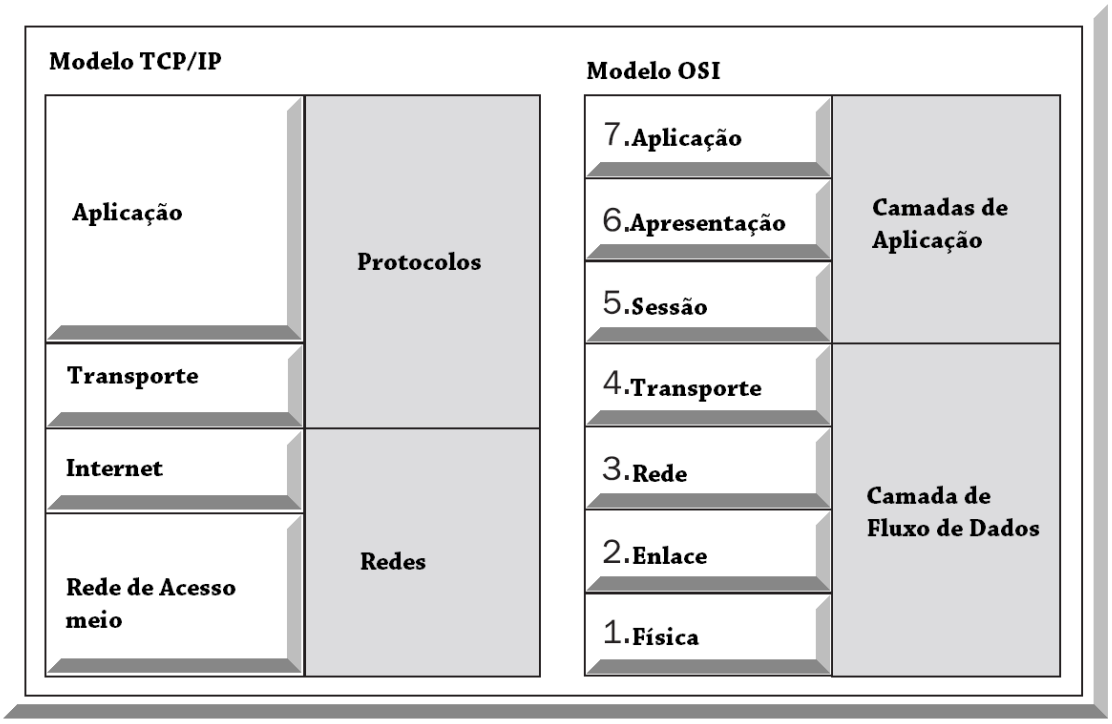

Figura 2 - Comparação do Modelo OSI e TCP/IP
Fonte: GHEORGHE, 2006

1.2.5 Sistemas Operacionais de Rede

Redes de computadores podem conter quaisquer elementos que contenham algum tipo de protocolo padronizado para que estes estabeleçam comunicação de forma ordenada e inteligível, elementos que podem ser hardwares com tarefas específicas, computadores pessoais, computadores servidores, supercomputadores e dispositivos móveis, como tablets e telefones celulares. O exemplo mais comum de utilização de um protocolo com essa característica é o uso do TCP/IP por estes dispositivos citados.

Desde o início dos anos 80, quando o TCP/IP se tornou um padrão de comunicação da ARPANET, a rede de pesquisa avançada do governo americano, este protocolo não parou de crescer.

Nos anos 90, com a propagação massiva dos computadores pessoais, alguns padrões diferentes surgiram em redes corporativas, diferentes do TCP/IP. Em redes Novell, usando o sistema operacional Netware, o protocolo padrão era o IPX/SPX, e em algumas redes Microsoft Windows usando o protocolo NetBIOS/NetBeui. A Novell tinha o domínio das redes utilizando o Netware, podendo ser utilizada em redes de grande porte. Ao contrário, as redes Microsoft com NetBios eram estritamente para um número limitado de computadores, 255 especificamente.

Com a popularização da Internet no início dos anos 90, ocorrendo no Brasil em 1995, o uso do protocolo TCP/IP, padronizado para a Internet, começou a se expandir. Para alguns sistemas operacionais havia a necessidade de uma instalação adicional do protocolo, e para outros, no caso do Windows 95, que na época foi realmente uma revolução para o usuário final, o protocolo já era nativo.

Tratando-se do lado de servidores, a popularização do TCP/IP também foi muito forte, fazendo com que a Novell de forma tardia usasse também o protocolo, porém, em determinado momento acabou perdendo espaço para o Microsoft Windows NT, que já tinha de forma nativa o protocolo TCP/IP.

Paralelamente a isso, alguns sistemas operacionais nasciam e outros ficavam mais fortes ainda. Em 1991 nascia o kernel do Linux, desenvolvido por Linus Torvalds, que rapidamente se expandiu. Outro sistema operacional que ajudou a expandir e ao mesmo tempo acompanhou o crescimento da Internet foi o Unix. Já usado por grandes corporações desde os anos 80, quando houve a necessidade de configurar um *gateway* Internet, muitas empresas já estavam prontas. Mas devido ao amadorismo do começo da Internet, as preocupações com segurança não eram lembradas, e quem tinha um pouco mais de conhecimento nos sistemas operacionais usados, explorava falhas de configurações que muitas vezes deixavam expostas redes inteiras para a Internet.

Muitos provedores utilizaram sistemas operacionais Unix, como o freeBSD e o openBSD, como servidores principais, devido a ser um sistema operacional livre para o uso comercial sem custo algum.

Após 20 anos, a Internet se tornou o maior espetáculo da Terra, o custo do armazenamento diminuiu, as operadoras conseguem oferecer circuitos de

alta velocidade, as redes de telefonia celular cresceram, e o custo do hardware diminuiu. Na era dos telefones inteligentes, uma comparaçãosimples nos mostra que alguns telefones atuais têmprocessadores tão velozes quanto ao que usávamos em um computador pessoal há alguns anos atrás, e ainda executando o mesmo *kernel* de um sistema operacional que usamos em um computador desktop.

Quando falamos em sistemas operacionais de redes não devemos nos limitar somente aos sistemas operacionais como Unix, Linux e Windows. Uma análise mais específica nos mostra que devemos lembrar-nos dos equipamentos que compõem uma rede,o que nos remete a Switches e Roteadores, que geralmente dotados de sistemas operacionais muito estáveis e bem conhecidos do mundo da tecnologia.

Os sistemas operacionais embutidos nos equipamentos têm tarefas semelhantes aos sistemas operacionais de um computador pessoal, pois são responsáveis pelo processo de inicialização e operação do equipamento. Algumas vantagens os equipamentos com sistemas operacionais chamados de “embarcados” levam em relação a um computador pessoal, ou até mesmo um servidor: estes sistemas executam um número limitado de tarefas, e são instalados em uma memória de acesso rápido com um hardware otimizado, diferente de um computador pessoal ou servidor que geralmente usam discos magnéticos, que são muito mais lentos se comparado a memórias rápidas. Uma das marcas de roteadores mais usados na Internet e em redes corporativas é a Cisco, cujo sistema operacional instalado nos na maioria dos roteadores e switches é o IOS, *Internetworking Operating System*. Outros fabricantes como Juniper, Nortel e outros possuem seus próprios sistemas operacionais para seus equipamentos.

De maneira geral, todos os sistemas operacionais têmum módulo de núcleo dotado de um software de rede, que incorpora um ou mais protocolos de rede para comunicação de dados de aplicativos que residem em um servidor.

Como citado anteriormente, o protocolo mais usado em redes locais é o TCP/IP, mas ele não é o único, podemos ter o TCP/IPpara a plataforma Intel, como o SNA para os Mainframes que não tem o TCP/IP de forma nativa.

1.2.5.1 Sistema Operacional FreeBSD

O sistema operacional freeBSD é um tipo de sistema operacional UNIX baseado no UNIX 4.4BSD liberado pelo *Computer System ResearchGroup*(CSRG) da Universidade da Califórnia em Berkeley. Resumidamente, a Universidade da Califórnia teve incentivo da AT&T e o departamento de defesa dos Estados Unidos para desenvolvimento e avanço no sistema operacional Unix. Começando desde a versão 3BSD, passando pela 4.2BSD, 4.3BSD, 4.3BSD-Reno, 4.4BSD até a 4.4BSD-Lite.

Após a versão 4.4BSD,devido uma ação judicial movida pela AT&T, o código teve que ser reescrito, um trabalho que demorou 3 anos para ser finalizado, até resultar na versão 4.4BSD-Lite. Alguns softwares do freeBSD foram baseados em versões anteriores a 4.4BSD, como a 4.3BSD-Reno, esta deu origem ao projeto 386/BSD, mantido por Bill Jolitz.Mas, devido ao longo tempo para o desenvolvimento de algumas correções, dois grupos se formaram, o netBSD e o freeBSD (DIBONA, 1999).

Anterior a ação judicial, os Unixes BSD eram chamados de BSD UNIX, mas, com a remoção do código AT&T, teve que ser chamado somente de BSD (freeBSD DOCS).

O freeBSD é um sistema operacional desenvolvido usando o modelo Open Source e desenvolvido por uma comunidade de contribuintes tecnicamente compromissados espalhados ao redor do mundo. Diferente do sistema operacional Linux, o sistema o freeBSD é mantido como um todo, e não apenas o núcleo (*kernel*), além de existir um repositório central do código, com o código inteiro, além das versões anteriores.

O freeBSD é um sistema operacional de grande porte com um extenso pacotes de softwares aplicativos e softwares servidores, o que o tornam pronto para ser usado nos mais diferentes propósitos: servidor de serviços Internet, educação e pesquisa, plataforma de desenvolvimento de software, estação de trabalho entre outros.

Mais adiante, nosso trabalho descreverá algumas soluções de conectividade VPN com softwares baseados em freeBSD. Devido a um núcleo compacto, e a possibilidade de poder redistribuir o freeBSD, alguns sistemas como o monowall e o pfsense – dois *firewalls* baseados em freeBSD – usam essa vantagem para construir sistemas com funções específicas e

administração mais facilitada. O objeto de nosso estudo, que será explicado em capítulos posteriores, está baseado nesses dois sistemas.

1.2.5.2 Licença BSD

A licença BSD é um tipo de licença Open Source, uma das mais conhecidas. A outra é GNU General PublicLicense (GPL). O freeBSD é distribuído sob a licença BSD 2-Clause “Simplified” ou Licença freeBSD. Embora sejam as licenças mais conhecidas elas são aplicadas de forma diferente. A licença BSD requer que os trabalhos derivados tenham o reconhecimento dos autores enquanto que a GNU requer que os trabalhos derivados sejam licenciados sob a mesma licença, a GPL.

Como mencionado antes, os projetos de VPN ipSecqueserão mostrados mais tardes neste trabalho, são baseados no monowall e no pfsense. Ambos são softwares baseados no freeBSD, livres e customizados para serem usados como *firewall* e/ou roteadores. O monowall foi concebido para ser usado em sistemas embarcados e o pfsense concebido para instalação completa usando todos os recursos de um PC.

1.2.5.3 Firewall monowall

O monowall é um completo pacote de software embarcado. Inclui a facilidade de uso, e praticamente todas as outras características de outros *firewalls* comerciais. É baseado no núcleo do freeBSD, sendo toda configuração feita por interface gráfica PHP, com alguns outros recursos. Toda a configuração do sistema é armazenada em um arquivo XML. Além de ser, é claro, um tipo de UNIX.

Segundo o autor, Manuel Kasper, para se ter um *firewall* robusto e ao mesmo tempo leve, para ser executado em várias plataformas embarcadas, algumas características o monowall não tem e nem irá ter. Alguns controles como: Proxy Server, detecção de intrusão, inspeção de pacotes em camada 3 deverão ser executados em outro servidor (MONOWALL HANDBOOK).

1.2.5.4 Firewall pfSense

O pfSense é uma distribuição do freeBSD customizado para ser usado como *firewall* e roteador. Seus idealizadores, Chris Buechler e Scott Ullrich, iniciaram o projeto em 2004. Chris, que inicialmente contribuiu para o projeto do monowall, percebeu a necessidade de um *firewall* com as boas características de administração e configuração como o monowall, pudesse ir além de um hardware limitador e sistemas embarcados, então deu início ao projeto pfSense. Com uma administração feita através de uma interface web, o pfSense não exige conhecimento em freeBSD de seus usuários, já que toda a configuração pode ser feita pela interface gráfica.

Além das características básicas de *firewall* e roteamento semelhantes a do monowall, o pfSense inclui outros recursos que exigem mais hardware, sendo assim um sistema *firewall* completo com recursos avançados como servidor Proxy, servidor de acesso remoto (VPNs móveis), inspeção de pacotes, detecção de intrusão, entre outros. Mesmo com várias possibilidades o pfSense disponibiliza três tipos de instaladores , uma versão para memória flash ou “livecd” que pode ser executada a partir de um CD ou pen-drive, uma versão chamada nanoBSD, para ser executada em dispositivos com memória flash de forma embarcada, e a versão completa para instalação em disco rígido.

1.2.5.4.1 – Modelos de instalação pfSense

Como o pfSense é dotado de vários softwares, as possibilidades de aplicação são muitas. Sendo possível em qualquer tipo e tamanho de ambiente.

Firewall de borda –Desde um simples servidor de acesso de uma rede local a Internet, ou até mesmo o gerenciamento de regras de publicação de servidores.

Roteador – o pfsense como roteador pode estar ou não na mesma instalação que o *firewall* de borda. Em uma das aplicações, como roteador, pode ser para conectar redes parceiras, que nem sempre acontece pelo principal link Internet.

Servidor VPN –o servidor de VPN pode também estar em um *firewall* de borda, ou não. Isto depende muito de como está projetada a estrutura e complexidade da rede. Muitas vezes um *firewall* de borda é muito mais crítico de fazer alterações que um servidor de VPN, podendo tornar a configuração e a administração de outros serviços

Outras possíveis aplicações são como servidor DNS, servidor DHCP, aplicação de monitoração e gerenciamento de rede.

1.3 Criptografia

A criptografia é uma coleção de técnicas matemáticas com o objetivo de proteger informações em um processo de alterar dados de maneira a tornar esses dados indecifráveis para qualquer um que tenha acesso, a não ser aquele que conheça o método de decifrar, que pode ser o mesmo autor ou somente o destinatário, se o mesmo tiver meios para tal.

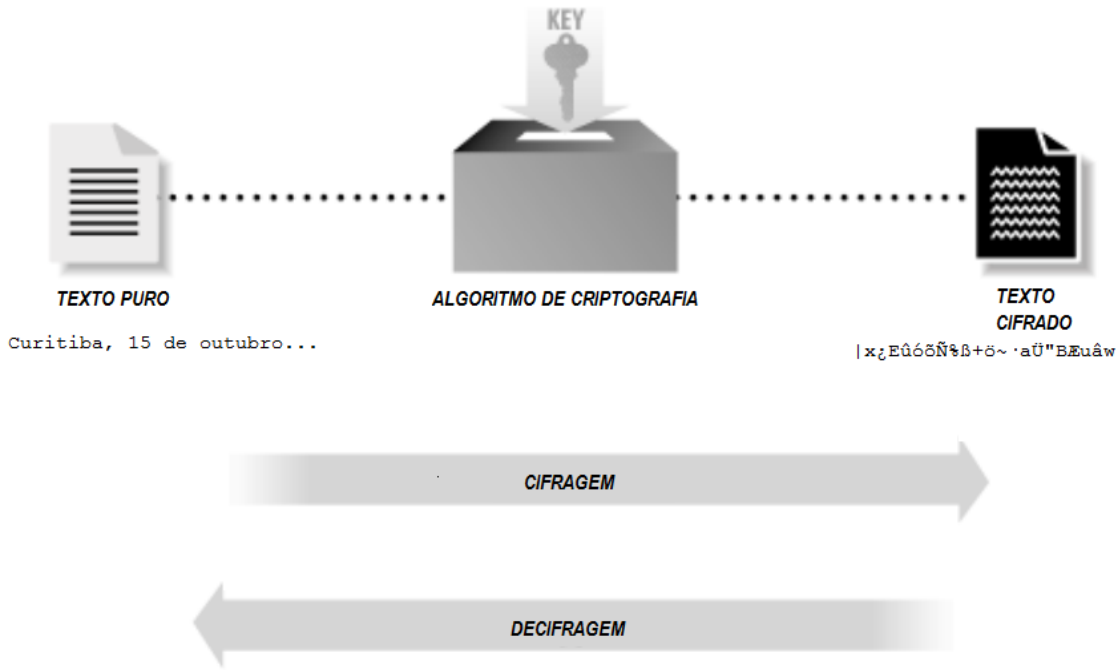

Figura 3 – Criptografia e Descriptografia
Fonte: GARFINKEL, 2003

A entrada para um algoritmo de criptografia é chamada de texto puro, enquanto que a saída é chamada de texto criptografado ou cifrado. Uma rotina de criptografia usa complexos métodos matemáticos para alterar os dados de uma maneira que o processo para reverter é trabalhoso e caro.

A criptografia é usada largamente hoje em tecnologia, mas seja na história, na política e em aplicações militares, sempre foi usada com o objetivo de proteger dados para que estes não caíssem facilmente em mãos inimigas.Sua origem remonta a idade antiga no Egito, Grécia e Roma.

A maioria dos sistemas de criptografia era baseada em duas técnicas, a substituição e a transposição. A substituição é baseada no princípio de repor cada letra da mensagem que se deseja transmitir por outra, através de um esquema pré-definido. A transposição consiste em embaralhar os caracteres na mensagem. Uma transposição consiste em escrever a mensagem em uma tabela linha a linha e então ler a mesma coluna a coluna.

Basicamente existem dois tipos de algoritmos de criptografia: o Algoritmo de Chave Simétrica e o Algoritmo de chave Assimétrica.

Os algoritmos de chave Simétrica, a mesma chave usada para criptografar uma mensagem é a mesma usada para descriptografar. Algoritmos de chave Simétrica muitas vezes são chamados de algoritmos de chave Secreta ou algoritmos de Chave Privada, o que pode criar confusão dos os algoritmos de chave Pública que não tem relação com os algoritmos de chave simétrica.

Os algoritmos de chave Assimétrica usam uma chave para criptografar a mensagem e outra chave usada para descriptografar.Uma particularidade importante dos algoritmos de chave assimétrica é o sistema de chave pública. A chave de criptografia é chamada chave pública,porque não há necessidade de manter segredo da chave ou da mensagem gerada pela chave pública. A chave de descriptografia, essa é chamada de Chave Privada, ou Chave Secreta.

1.3.1 Algoritmos de Chave Pública

O primeiro estudo sobre algoritmos de chave pública foi publicado em 1975 na Universidade de Stanford por WhitfieldDiffie e Martin Hellmann. Estes dois pesquisadores escreveram sobre a existência de uma técnica de

criptografia onde uma chave (chave pública) poderia ser usada para criptografar e outra chave (a chave privada) usada para descriptografar. Chaves sem relação uma com a outra. (GARFINKEL, 2003).

Resumidamente a lista a seguir descreve os sistemas de chave pública, mais utilizados. (GARFINKEL, 2003).

- Troca de chaves Diffie-Hellman: Um sistema de troca de chaves de criptografia entre as partes ativas em um meio público de comunicação. Não necessariamente um método de criptografia. Consiste em, as duas acordam alguns valores numéricos, e então cada parte cria uma chave. Transformações matemáticas destas chaves são trocadas. Cada parte então calcula uma terceira chave de sessão que não é facilmente derivada mesmo que atacantes conheçam os valores trocados.

- DAS/DSS: O padrão de assinatura digital (Digital Signature Standard - DSS) foi desenvolvido pela Agencia Nacional de Segurança dos Estados Unidos (NSA). É baseado no Algoritmo de Assinatura Digital (*Digital SignatureAlgorithm* – DSA). Enquanto o DAS permite chaves de qualquer tamanho, somente chaves de 512 e 1024 bits são permitidas no DSS. Ainda, o DSS pode ser usado somente para assinaturas digitais enquanto o DSA tem a possibilidade de usar algumas implementações para encriptação.

- RSA:Sistema de criptografia de chave publica desenvolvido em 1977 no MassachussetInstituteof Technology (MIT)por Adi Shamir, Leonard Adlemane Ronald Rivest. O RSA pode ser usado para criptografia de informação e como base para um sistema de assinatura digital. Não há limite para o tamanho da chave, estando diretamente ligado a aplicação/implementação.

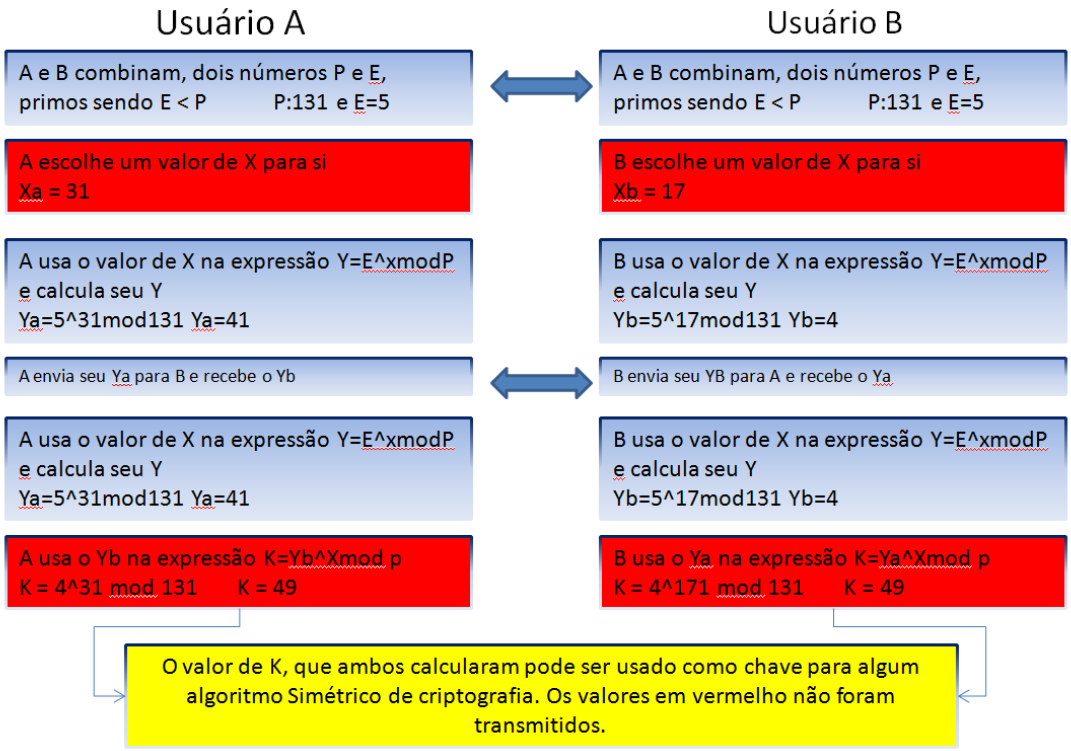

Figura 4– Esquema Diffie-Helmann

Fonte: VIVAOLINUX

1.3.2 Funções de Resumo de Mensagem (MessageDigest)

Funções de resumo de mensagem aplicadas a um arquivo, pequeno ou grande, criam um resumo geralmente entre 128 e 256 bits de tamanho (GARFINKEL, 2003). Essa transformação é feita usando um algoritmo de hash, ou seja, o resultado da aplicação de um algoritmo de hash em um arquivo cria uma identidade do mesmo. Pode-se fazer uma analogia à impressão digital do arquivo.

O resumo de mensagem é também chamado de função de hash de uma via, porque produz valores difíceis de reverter, resistentes a ataques e efetivamente únicos.

Alguns exemplos das funções mais usadas de resumo de mensagem:

MD5 – *MessageDigest* #5, resumo de mensagem número 5. É uma modificação do MD4, que torna o modelo mais seguro. O MD4 por sua vez foi uma alternativa ao MD2.
O MD5 é amplamente usado e produz um resumo de mensagem de 128 bits.

SHA-1 – Uma revisão do SHA (*The SecureHashAlgorithm*), o algoritmo seguro de hash, o SHA1 produz um resumo de mensagem de 160 bits, da mesma forma que o SHA, porém incorporando mais segurança.

SHA-2 – O SHA2 é um conjunto de algoritmos de *hash* desenvolvidos pela Agência de Segurança Nacional dos Estados Unidos, a NSA, e engloba as seguintes funcções: SHA-224, SHA-256, SHA-384 e a SHA-512. Com mudanças significativas em relação ao SHA-1, essas funções produzem resumos de mensagens de 224, 256, 386 e 512 bits respectivamente.

SHA-3 – O SHA-3, também chamado de Keccak, é um algoritmo de *hash* criado por Bertoni, Peeters e Assche, sem a intenção de substituir o SHA-2, mas para complementar o seu uso. Recentemente o SHA-3 foi escolhido pelo NIST (NationalInstituteof Security and Technology) dos Estados Unidos, através de uma competição exclusiva sobre algoritmos de *hash.* O NIST continua procurando sempre novas alternativas nesses algoritmos, pois já existiram ataques significantes nas funções MD5 e SHA
Um exemplo de *hash* SHA-3:

SHA3 512(XXII Teleinfo) =
6ebb2eda18252ebcaae41e2108e0961719a8708dc8a84bdd49613b8ebf844a36
348461f1632e578ee7f4e78b5059b0799b87e49aa47428885322d54e42ebc5da

1.3.2.1 Colisão em funções hash

Resumo de mensagem geralmente não é usado para o processo de criptografia e descriptografia, e sim para gerar uma assinatura digital, um código de mensagem de autenticação (MAC – *MessageAuthenticationCode*), e chaves de criptografia a partir de palavras-passe.
Um exemplo do uso do resumo de mensagem abaixo:

MD5(XXII Teleinfo) = 6728d06b675fa7b340ca7c944424beac
MD5(XXII Teleinfo.)= 488b15e0e8c82350b0acfbae0fa6aa4c
MD5(XXII Teleinfo!)= 889f31da14731873715aa71fc36651be

Podemos notar que mudando apenas um caractere da mensagem, o resultado do hash MD5 é totalmente diferente, isso porque cada mensagem tem sua própria impressão digital e a mesma mensagem deve produzir sempre essa impressão digital.
Quando uma mensagem ou arquivo são transmitidos por qualquer meio, o resumo de mensagem pode ser útil para verificar se a mensagem foi alterada no meio do caminho, pois caso a mensagem ou o arquivo chegue ao seu destino e produza um resumo diferente, tem-se a certeza de que a mensagem foi alterada.

Segundo (GARFINKEL, 2003), para quaisquer dois arquivos, existe de fato infinitas chances de que os mesmos produzam o mesmo código MD5. Isto porque existem 128 bits independentes no resumo MD5, essa chance brutal é igual a 1 em 2^128. Como 2 elevado ao expoente 128 é um número muito grande, é extraordinariamente improvável que dos arquivos criados por um ser humano com conteúdos diferentes, produzam o mesmo código MD5.

Na teoria, dois diferentes arquivos podem produzir um mesmo resumo de mensagem. Isso é chamado de Colisão. Para que um resumo de mensagem seja seguro, deve ser computacionalmente inviável encontrar ou produzir colisão.

1.3.3 HMAC – Códigos de Mensagem baseados em hash

Um código de mensagem baseado em hash é uma técnica para verificar a integridade de uma mensagem transmitida entre duas partes que compartilham uma chave. Sua especificação está descrita na RFC 2104. Pode ser usada em combinação com qualquer função de hash de criptografia como MD5 e SHA-1, por exemplo. Quando usado dessa maneira o algoritmo pode ser denominado HMAC-MD5 ou HMAC-SHA-1. O tamanho da criptografia HMAC depende diretamente do tamanho da criptografia gerada pela função hash e no tamanho e qualidade da chave.

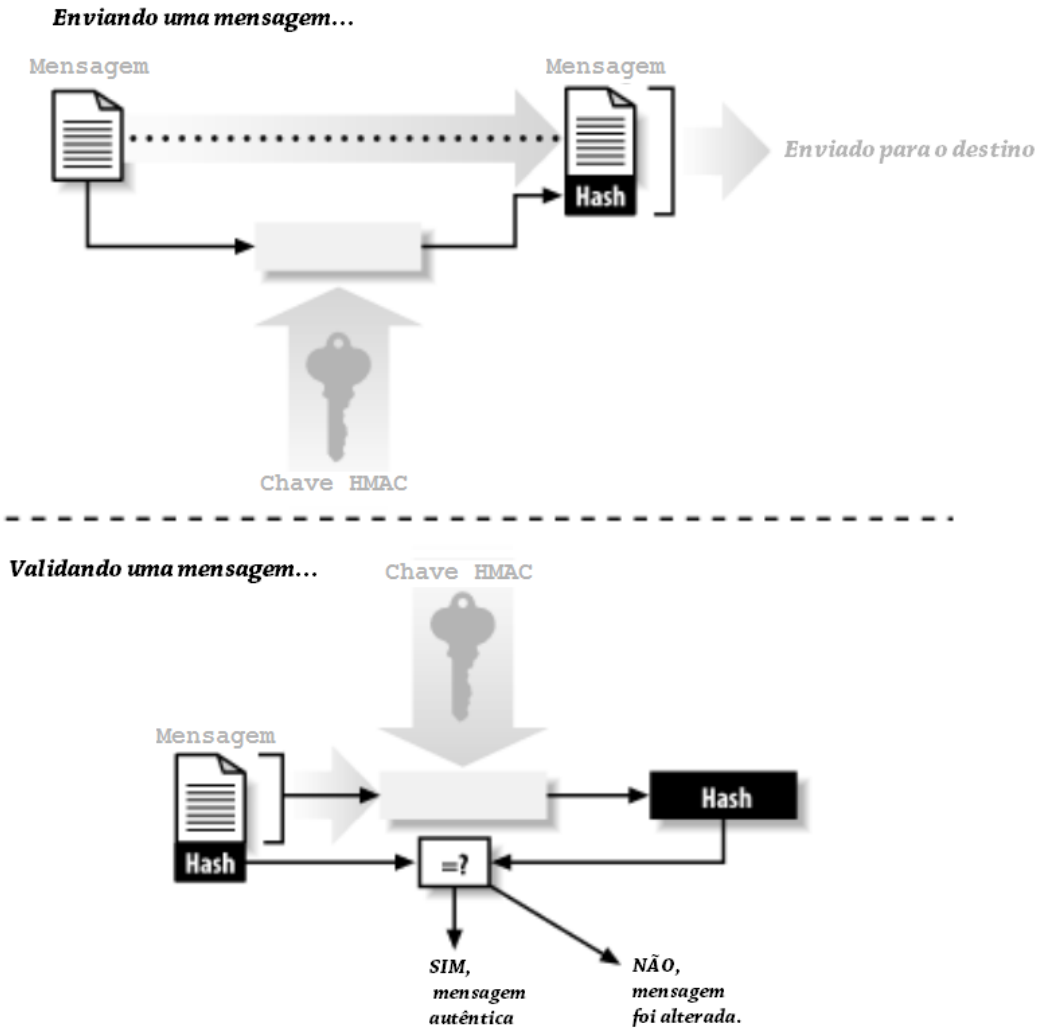

Figura 5 - Usando HMAC para verificar a autenticidade e Integridade de uma mensagem

Fonte: GARFINKEL, 2003

1.3.4 Algoritmos de Chave Simétrica

Algoritmos de chave Simétrica assim são chamados, pois a mesma chave usada na criptografia também é usada na descriptografia. Esses algoritmos são usados na maioria das vezes para criptografar a maior parte dos dados ou de um fluxo de dado. São algoritmos de alta velocidade e força.

A segurança desses algoritmos de chave simétrica reside em, uma vez os dados sendo criptografados com uma chave, não é fácil e rápido descriptografar sem a mesma chave. Podem ser divididos em duas categorias: bloco e fluxo. Os algoritmos de bloco criptografam um bloco de dados (alguns bytes) de uma vez, enquanto os algoritmos de fluxo criptografam byte a byte ou até mesmo bit a bit. (GARFINKEL, 2003)

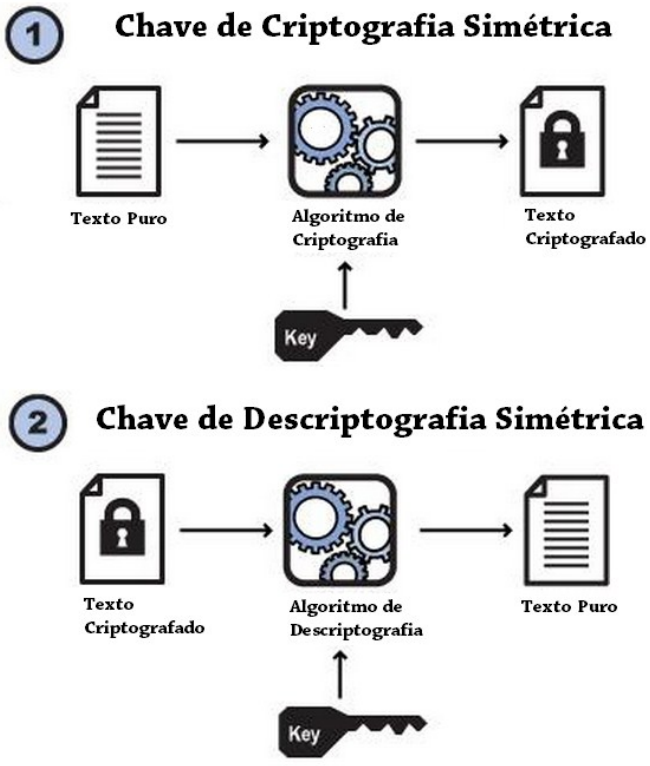

Figura 6– Chave Simétrica

1.3.4.1 Exemplos de Algoritmos de Chave Simétrica

DES – *Data Encryption Standard*, é um algoritmo que influenciou o desenvolvimento do mundo da criptografia moderna. Adotado como padrão pelo governo americano em 1977, o DES é um bloco que usa uma chave de bloco de 56 bits e tem muitos modos de operação, dependendo exatamente de qual a finalidade que está empregado. É um algoritmo forte, porém sua curta chave impõe limite ao seu uso. Em 1998 uma máquina com o propósito especial de quebrar o DES usando força bruta foi desenvolvida pela Eletronic Frontier Foundation. Com o custo de US$250.000,00 em uma demonstração foi capaz de encontrar a chave de uma mensagem criptografada em 22 horas e 15 minutos.

3DES ou TDEA – Triple DES ou *Triple Data EncryptionAlgorithm* - O TDEA é uma implementação que usa o DES gerando chaves por três vezes. Sendo a chave do DES viável computacionalmente, o TDEA torna o algoritmo muito forte. O TDEA consiste na operação de criptografar um bloco de dados de 64 bits, em seguida descriptografar e novamente criptografar, gerando assim uma chave de 168 bits. No algoritmo DES a chave é de 56 bits. As outras opções de chaves são 112 bits – usando duas chaves iguais, e a opção de 56 bits onde se usa as três chaves iguais. Neste último caso, por questão de compatibilidade, o TDEA fica a mesma coisa que o DES.É possível dizer que o TDEA (3DES) é o uso do DES em cascata por três vezes. O TDEA evita a vulnerabilidade do DES.

Blowfish – Um algoritmo criado por Bruce Schneier, o Blowfish foi criado para ser uma alternativa ao DES. É um algoritmo rápido e compacto que permite criar chaves de tamanho variável, acima de 448 bits. É otimizado para execução em processadores de 32 ou 64 bits. Ataques ao Blowfish já foram detectados e recomenda-se cuidados no uso. Os algoritmos sucessores são: Twofish e Threefish.

AES – *AdvancedEncryption Standard* - É um método de criptografia de bloco rápido e compacto que usa chaves de 128, 192 ou 256 bits de tamanho. Desenvolvido por Joan DaemeneVincentRijmen, o padrão AES é adotado como padrão pelo governo americano. Tem um desempenho muito bom podendo ser executado em cartões de 8 bits e até em computadores de alta performance. (WIKIPEDIA – AES)

MARS, IDEA RC3, RC4, RC5 e Serpent são outros exemplos de algoritmos simétricos de criptografia.

1.4 Redes Privadas Virtuais

Muito antes da Internet, grandes empresas sempre usaram enlaces de dados para comunicação entre matriz e filiais. Nos anos 80 e boa parte dos anos 90, esses enlaces eram estabelecidos, com circuitos oferecidos por operadoras de telecomunicações de acordo com a necessidade da comunicação. Após o advento da Internet e o barateamento de enlaces que colocam as empresas diretamente na Internet, houve naturalmente uma migração de boa parte da comunicação usando a Internet.

Necessariamente, mais cedo ou mais tarde, as empresas passaram pela necessidade de estarem plugadas na internet, seja para comunicação de correio eletrônico, seja para publicar um servidor web ou até mesmo para prover serviços, e para tudo isso houve necessidade de investimentos em infra-estrutura de comunicação Internet. Nos anos 90, provedores se encarregavam dessa tarefa, para pessoas físicas e pequenas e médias empresas. No entanto a figura do provedor de acesso à internet mudou na década seguinte, fazendo com que as empresas investissem em sua própria estrutura de Internet e servidores internos, deixando pouca coisa para provedores de internet especificamente. É claro, nos últimos anos, a estrutura de muitas empresas estão voltando para provedores, mas estes diferentes de antes, são provedores de serviços, criando o que podemos hoje chamar de Computação em Nuvem. Neste modelo, as empresas hospedam servidores de aplicação fora de suas estruturas, tornando menor o custo de manter uma infra-estrutura, além é claro de passar toda a administração a uma empresa que tem a expertise no assunto, podendo a empresa dar foco específico no próprio negócio.

Porém mesmo com toda a mudança, empresas continuam com a necessidade de interconexão com filiais, fornecedores ou parceiros de negócios, e, com a computação em nuvem, necessitam também de conexão segura com os provedores de serviços. Ainda que as operadoras continuem a oferecer enlaces ponto-a-ponto para comunicação de dados,estabelecer uma comunicação usando esses enlaces torna a comunicação muito cara, embora tenha a vantagem de ser uma comunicação de alta confiabilidade. E, a menos que a necessidade não seja um canal de baixa latência, com garantias extremamente altas, existe a alternativa de fazer uma conexão via Internet

usando uma Rede Virtual Privada.Esta pode diluir o custo do investimento em enlaces Internet de alta velocidade, utilizando o mesmo para estabelecer vários enlaces virtuais de forma segura e de simples administração.

Transmitir dados por uma Rede Virtual Privada (VPN, *virtual private network*)significa transmitir dados de forma segura e privada através de uma infra-estrutura insegura e compartilhada. Uma VPN torna a transmissão segura encapsulando, criptografando ou encapsulando e criptografando os dados. É uma maneira de simular uma rede privada sobre uma rede pública, tal como a Internet. É chamada virtual, pois depende do uso de uma conexão virtual criada entre dois pontos para efetivar a comunicação.

1.4.1 Características de uma VPN

Uma VPN efetivamente tem a tarefa de tornar seguro e garantir a privacidade da comunicação entre das redes. Para garantir isso existem alguns objetivos a serem atingidos:

- Confidencialidade dos dados: Proteger o conteúdo da mensagem de ser interpretada por fonte não autenticada e não autorizada.
- Integridade dos dados: Garantir que a integridade dos dados não tenha sido violada ou alterada em trânsito entre a fonte e o destino.
- Autenticação da mensagem: Garantir que a mensagem foi enviada por uma fonte autêntica e que a mensagem foi enviada para destinos autênticos.
- Irretratabilidade ou não-repúdio: não poderá ser possível ao emissor negar a autoria e origem da mensagem.

Em uma VPN com a capacidade de Confidencialidade de Dados, garante que somente origem e destino conhecidos são capazes de interpretar o conteúdo da mensagem original. O protocolo IPsec é efetivo para criptografar os dados usando o protocolo de encapsulamento de Segurança, o ESP (*encapsulatingsecurityprotocol*), descrito pela RFC 1827. A utilização do ESP transforma texto puro em dados criptografados, ou texto cifrado. Somente

mensagens ESP transformadas são enviadas através de sua própria representação, ficando a mensagem original mantida em confidencialidade.

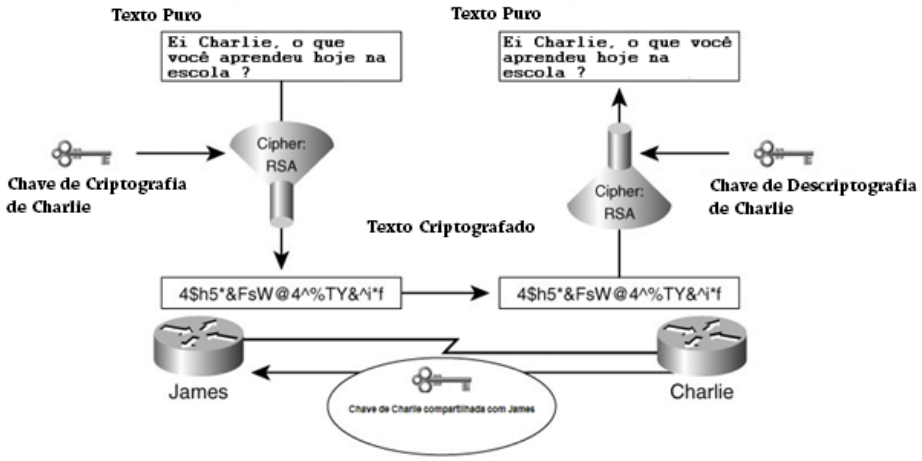

Figura 7– Confidencialidade e Autenticidade em comunicação Criptografada
Fonte: CARMOUCHE, 2006

1.4.2 IPSec – Internet Protocol Security (Protocolo de Segurança Internet)

IPSec, como definido na RFC 2401, provê a funcionalidade de garantir a autenticidade, integridade e a confidencialidade de dados na camada de rede conforme o modelo OSI. O IPSec é um conjunto de protocolos que define um padrão para os quatro elementos necessários na definição de uma rede privada virtual (VPN) de forma robusta:

- Protocolos de Segurança
- Mecanismo de troca de chaves
- Algoritmos de troca de chave segura e criptografia
- Definições de Associações Seguras (AS) e manutenção

O IPSec é um conjunto de protocolos que provê segurança para o IP (internet protocol). Inicialmente desenvolvido para o protocolo internet versão 6 (ipv6) como padrão, acabou sendo “portado” para o ipv4. Foi criado com a intenção de manter uma rede segura sem alterações nas aplicações acima. Atua na camada Internet, considerando o modelo TCP/IP, enquanto que alguns outros protocolos como SSL, TSL, SSH operam em camadas superiores do mesmo modelo.

Devido ao amplo uso do protocolo TCP/IP algumas vulnerabilidades são corrigidas, juntamente com a evolução e atualização, e desta forma o IPSec acabou sendo um padrão a mais de segurança para o protocolo, e fez isso de uma forma transparente para a aplicações existentes e futuras, pois mesmo com a implementação do IPSec, não há necessidade de mudança nas aplicações.

O órgão mantenedor do IPsec é o IETF (*Internet EngineeringTask Force* – Força Tarefa de Engenharia Internet), que tem como objetivo manter documentações, boas práticas e apresentar padrões para que desenvolvedores tenham como base ao desenvolver novos programas. A documentação do IETF para o IPSec define basicamente três bases para a segurança do protocolo IP: algoritmos de criptografia, algoritmos de autenticação e por último gerenciamento de chaves.

O protocolo IPSecestabelece canais de comunicação seguro entre dois pontos de rede usando o modo Transporte e o modo Túnel.Esses modos geralmente são chamados de IPSec SA, ou Associações Seguras IPSec. As associações seguras IPsec são unidirecionais, então para cada canal seguro de comunicação, existirão duas associações seguras, uma em cada sentido de comunicação. Dois protocolos de segurança são usados para garantira confidencialidade, integridade e autenticação do cabeçalho IP na camada de rede, são eles o ESP (*Encapsulating Security Payload*) e o AH (*Authentication Header*)

Modo Transporte - protege criptografando somente porção de dados, o payload, a cada pacote. É usado em comunicações onde é necessária proteger a comunicação deum host para outro, uma VPN tradicional. Descrito pela RFC 2401, que define que as associações seguras de IPSec neste modo usam o protocolo ESP (Encapsulating Security Payload), mantendo a confidencialidade apenas para protocolos acima do protocolo IP. (IPSEC HOWTO)

Modo Túnel - O modo túnel criptografa o cabeçalho e o payload, se tornando assim mais seguro, pois protege a identidade original de origem e destino. Neste modo o datagrama IP é criptografado por inteiro, sendo necessário o seu encapsulamento, agora como payload, em outro datagrama IP. Usado pra criar

um túnel através de um meio público, como a Internet por exemplo. (IPSEC HOWTO)

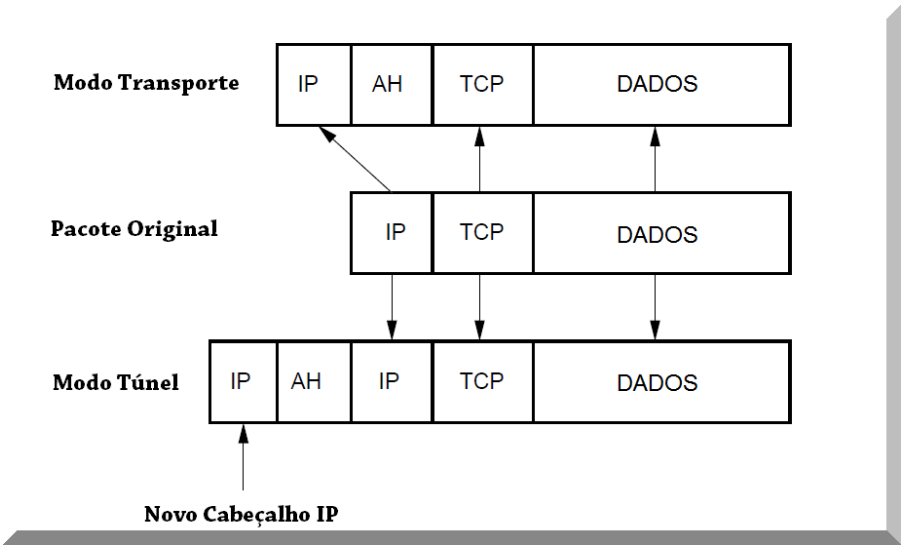

Figura 8– Cabeçalhos nosmodos Transporte e Túnel

Fonte: IPSEC HOWTO

1.4.3 ESP (Encapsulating Security Payload)

A Internet, ou interconexões de redes mesmo que privadas que precisam ser roteadas para uma rede WAN, baseia-se na transformação de pacotes de dados de uma LAN para uma WAN, vice e versa sucessivamente. O IPSec trabalha da mesma forma, porém gerenciando pacotes de dados criptografados usando o protocolo ESP.

O ESP é responsável confidencialidade usando os protocolos de criptografia de chave simétrica DES, 3-DES ou AES. Os pacotes ESP são marcados com um valor de 32 bits chamado SPI (securityparametersindex) usado para identificar uma associação de segurança. O SPI faz com que o dispositivo usado para criptografar e descriptografar, saiba exatamente a qual associação de segurança pertence o pacote ESP. A seqüência numérica gerada no SPI é incremental a cada pacote.

A confidencialidade é verificada com a criptografia e a integridade usando HMAC. Após a criptografia do pacote e após calcular o HMAC, o cabeçalho ESP é gerado e adicionado ao pacote.

1.4.4 AH (Authentication Header)

O cabeçalho de autenticação, AH, é uma escolha para usa o IPSec na possibilidade de não haver necessidade de confidencialidade. O AH pode ser usado com o ESP em modo túnel ou, somente o AH, como autenticador.

A atuação do cabeçalho de autenticação AH, consiste em proteger a informação do cabeçalho IP, enquanto que o ESP protege os dados (o payload).

A configuração do AH pode ser feita em modo túnel e modo transporte. No modo túnel o cabeçalho final do pacote IP é montado com base no cabeçalho IP original, provendo autenticidade e integridade ao cabeçalho IP e os dados (payload), do pacote original. Como o AH protege o cabeçalho IP atuando em partes que não podem ser modificadas, como o valor do endereço IP contido no cabeçalho IP, o protocolo AH não permite NAT. A tradução de endereços feita pelo NAT substitui o endereço original no cabeçalho IP, por um endereço diferente. Porém se houver troca de endereço, o HMAC (hash calculado com o endereço original), não será mais válido. Uma extensão do protocolo IPSec, o NAT-Transversal, permite maneiras de implementar o NAT com IPSec.

1.4.5 IPsec SA – Associações de Segurança do protocolo IPsec

Para que seja estabelecidas comunicações seguras entre dois pontos usando o protocolo IPsec, os pontos precisam negociar vários parâmetros para fechar um túnel. Cada associação única requer uma negociação para cada direção do túnel e para cada protocolo usado (AH, ESP ou uma combinação destes).

Os parâmetros necessários para configurar um túnel efetivamente são:

Modo: Transporte ou Túnel. Podem ser usadas as transformações ESP e AH.

Transformação: Protocolo IPsec de encapsulamento e criptografia. Inclui a especificação de transformação AH, ESP ou ambos. Inclui também o mecanismo de criptografia de chave simétrica, DES, 3-DES ou AES.

Peer: Define a extremidade de cada túnel, é onde as associações seguras (SA) são negociadas.

Tráfego Combinado: Esse ponto é extremamente importante, pois define o acesso entre hosts, ou entre hosts e sub-redes, ou entre sub-redes. A definição tem que ser a mesma nas duas extremidades, caso contrário haverá falha na negociação as associações.
MTU do caminho:Os extremos do túnel precisam concordar e garantir o MTU no tráfego pelo túnel.
SPI: Valor único de 32 bits usado para identificar cada pacote transformado à qualpacote original pertence.

1.4.6 ISAKMPe IKE

Complementando a segurança do pacote IPsec, a comunicação segura entre dois hosts deve, além do encapsulamento ESP e do cabeçalho de autenticação (AH), ser capaz de negociar chaves enquanto a comunicação acontece, além de decidir qual os algoritmos de autenticação e criptografia serão usados.O mecanismo capaz de gerenciar as políticas de segurança, autenticação dos peers e controlar as trocas de chaves é o ISAKMP (Internet Security Associationand Key Management Protocol).(CARMOUCHE, 2006).

As principais rotinas definidas no ISAKMP são (CARMOUCHE, 2006):
Procedimentos de autenticação das extremidades
Negociação das Associações de Segurança, manutenção e timeout
Geração da chave de criptografia e técnicas de troca (Diffie-hellman)
Técnicas de redução de ataques (antireply, DoS)

1.4.6.1 O protocolo IKE

O protocolo IKE (Internet Key Exchange) é o responsável pela autenticação dos peers e pela troca de chave simétrica. O protocolo cria as associações de segurança e propaga o SAD (o banco de dados de associações seguras). O protocolo IKE usa o serviço udp/500 para comunicação e depende de um processo de usuário para sua inicialização, não sendo nativo do sistema operacional, seja Unix, Linux ou Windows.

O IKE trabalha em duas fases de comunicação, a primeira estabelece uma associação ISAKMP (ISAKMP SA), e a segunda fase, a associação

ISAKMP é usada para negociar e configurar as associações IPSec. (IPSEC HOWTO)

A autenticação dos peers na fase 1, pode ser feita pro chave pré-compartilhada (PSK – pre-sharedkey), chaves RSA e certificados X.509. Há também suporte para Kerberos. Ainda, a fase 1, pode ser definida em modo Principal (MainMode) ou modo Agressivo (AgressiveMode). Os dois modos autenticam os peers e configuram associações ISAKMP, porém o modo agressivo usa a metade de mensagens para atingir o objetivo, mas é mais vulnerável a ataques do tipo man-in-the-middle se usado com chaves pré-compartilhada.

Na fase 2 o protocolo IKE faz as associações de segurança e negocia a segurança das associações baseado na associação ISAKMP previamente efetuada. A associação ISAKMP define autenticação que protege contra um ataque man-in-the-middle.

Geralmente dois peers negociam uma única associação ISAKMP, que é usada para negociar várias, no mínimo duas, associações unidirecionais IPsec.

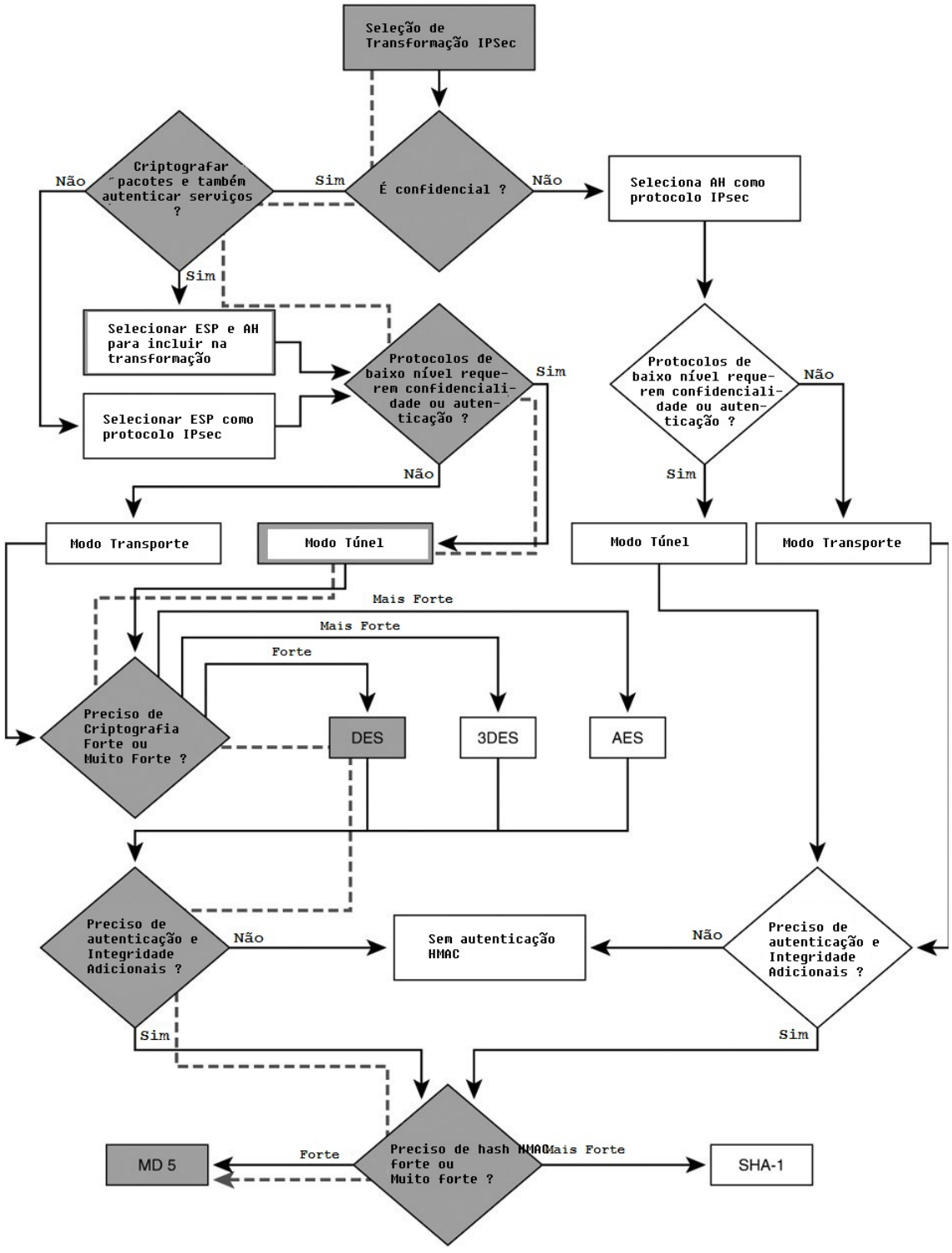

Figura 9– Arvore de decisão para transformações IPSec

Fonte: CARMOUCHE, 2006

2 VPNs LAN TO LAN – ESTUDOS DE CASOS

Os estudos mostrados a seguir são situações reais, cuja demanda se mostrou urgente e com pouco recurso para implantação, porém de uma necessidade e importância alta para a empresa a qual foi aplicada. As VPNsIPsec mostradas a seguir, e suas respectivas configurações poderiam ser de possível implementação usando sistemas operacionais Unix, Linux ou até mesmo Windows, ou ainda ser configuradas com roteadores (Cisco, HP, etc) com a funcionalidade IPSec disponível. Porém como veremos na evolução dos casos, os softwares usados foram inicialmente o monowall e o posteriormente o pfSense. Mesmo com um núcleo do sistema operacional freeBSD, esses dois sistemas dispõem de uma ferramenta gráfica de configuração (GUI – GraphicalUser Interface), baseada em PHP, que torna mais fácil a aplicação de conceitos, aqui no caso do IPSec,sema necessidade de conhecimento no sistema operacional.

Esses dois softwares têm um mesmo princípio, porém com objetivos diferentes. O monowall tem o propósito de trabalhar como roteador apenas. Já o pfSense além de poder fazer a mesma tarefa de roteador, disponibiliza pacotes de aplicativos para análise de rede, Proxy, entre outros. Porém, como citei a pouco, é necessário que o conceito básico do que está se propondo a fazer esteja claro, seja para a configuração de um simples roteador ou de um roteador, com VPN, Proxy e outros serviços.

2.1 Interconexão de Redes Locais para acesso remoto e backup remoto

Inicialmente nesse primeiro caso existia um cenário de uma VPN existente, oferecida por uma operadora. Era uma VPN do tipo MPLS com velocidade de 1Mbps. O funcionamento desse serviço era bom, porém o problema era o custo elevado, algo em torno de R$1500,00. A existência da VPN se fazia necessário, porém poderia ser com baixa prioridade no uso diário, ou seja, não havia necessidade de ter um custo alto, garantias de serviços, para pouco uso.

Minha sugestão inicialmente foi montar uma VPN usando enlaces ADSL, devido a ter um custo baixo. No entanto foi necessário verificar a disponibilidade de fornecimento do circuito de ADSL nas duas pontas. Após

essa confirmação, a segunda necessidade é que os dois ADSLsque seriam usados necessitariam obrigatoriamente ter endereço IP fixo.

Reunindo todos os custos dos circuitos ADSLs, custo mensal, mais custo do endereço IP fixo, cheguei a um valor de aproximadamente R$400,00, um valor bem abaixo dos R$1500,00 na VPN oferecida pela operadora.

Uma comparação inicial pode-se logo perceber que a solução seria bem mais simples do que a já instalada pela operadora, já que a solução instalada contava com roteadores Cisco e modems fornecidos pela operadora. Já a solução pretendida teria apenas um modem adsl em cada site, e o mecanismo para fechar a VPN.

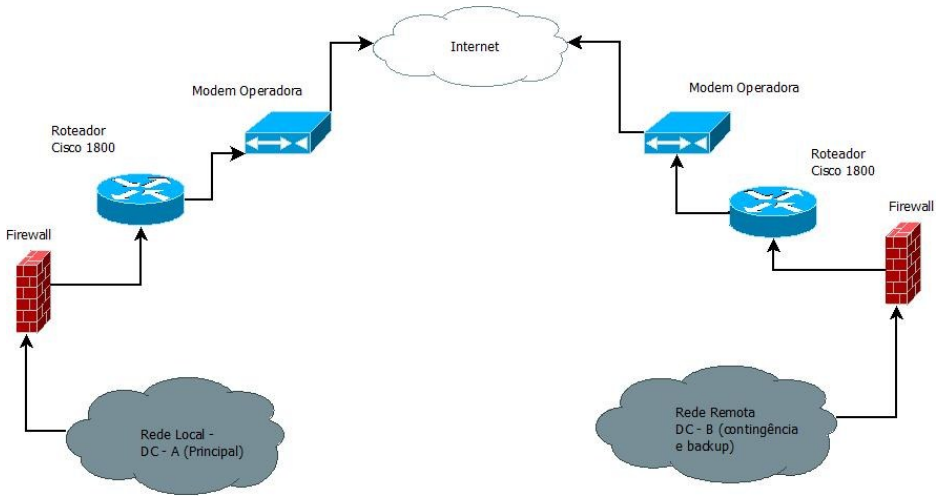

Figura 10– Panorama Inicial, estrutura para a VPN oferecida pela Operadora

Fonte: O Autor

O passo seguinte foi definir como configurar uma VPN usando o ADSL, já que na solução anterior, toda a configuração da VPN estava no roteador Cisco. Inicialmente a solução desejada foi uma VPN IPsec, utilizando modo túnel, pois assim a rede A poderia se comunicar sem restrições com a rede B e vice e versa.

As possibilidades de configuração de uma rede IPSec são inúmeras. A primeira possibilidade, seria que a empresa em questão (vamos chamá-la de ZXC), adquirisse roteadores com capacidade de configurar IPSec, mas, devido a custos, essa hipótese foi descartada. A segunda possibilidade foi usar servidores Linux ou Unix, com o pacote de software ipsec para tal configuração. Nesse caso, houve duas avaliações iniciais, o pacote

StrongSwan e o pacote ipsec-tools, ambos disponíveis para as principais distribuições de Linux e Unix (freeBSD e openBSD). Avaliando o tempo de deploy (instalação e configuração) dessas ferramentas, poderíamos ter atrasos, e uma necessidade de estudo mais aprofundada, além da ferramenta e dos sistemas operacionais escolhidos. Como já havia um projeto em paralelo em andamento com o monowall, acabeilevando-o em consideração, e este acabou sento a terceira possibilidade. Inicialmente os pontos positivos agradaram, principalmente devido à facilidade dedeploy.

O monowall é um sistema que embora baseado em Unix, acaba sendo um sistema muito compacto, podendo consumir um espaço de 12 Mbytes. É um *firewall* feito para ser usado de forma embarcada com hardwares simples, porém nada impede de usá-lo em um PC ou máquina Virtual. No nosso estudo de caso a instalação do monowall foi feita como máquina virtual em ambiente VMWareESXi 4.1. Como mencionado acima, a necessidade de uma alternativa era urgente, e nesse caso, uma instalação em configuração como máquina virtual ganhou-se muito tempo, pois o ambiente de nuvem (o ESXi) já estava montado em com plano de capacidade para suportar algum crescimento.

2.1.1 Instalação e Configuração

Inicialmente vamos definir as nomenclaturas usadas neste item:

- Rede local da empresa ZXC, 192.168.X.0/24, chamada de OCMainOffice
- Rede remota da empresa ZXC, 192.168.Y.0/24, chamada de OCASOffice

A configuração inicial foi a instalação do ambiente monowall, que pode serfeita de algumas maneiras, como sugeridas pelo website do projeto (m0n0.ch/wall) e mesmo nas opções de instalação do site há uma opção de efetuar o download de uma imagem VMWare, porém como eu já tinha um CD criado a partir de uma imagem, usei-o para fazer a instalação no VMWare.

Pouco recurso de máquina virtualfoireservado, já que o monowall necessita de pouco espaço em disco e pouca memória. A instalação é muito simples, basta criar uma máquina virtual, reservar os recursos, e antes de

iniciar a máquina virtual, há a necessidade de mapear qual dispositivo de CD que será usado para fazer a leitura do software de instalação (figura 12)

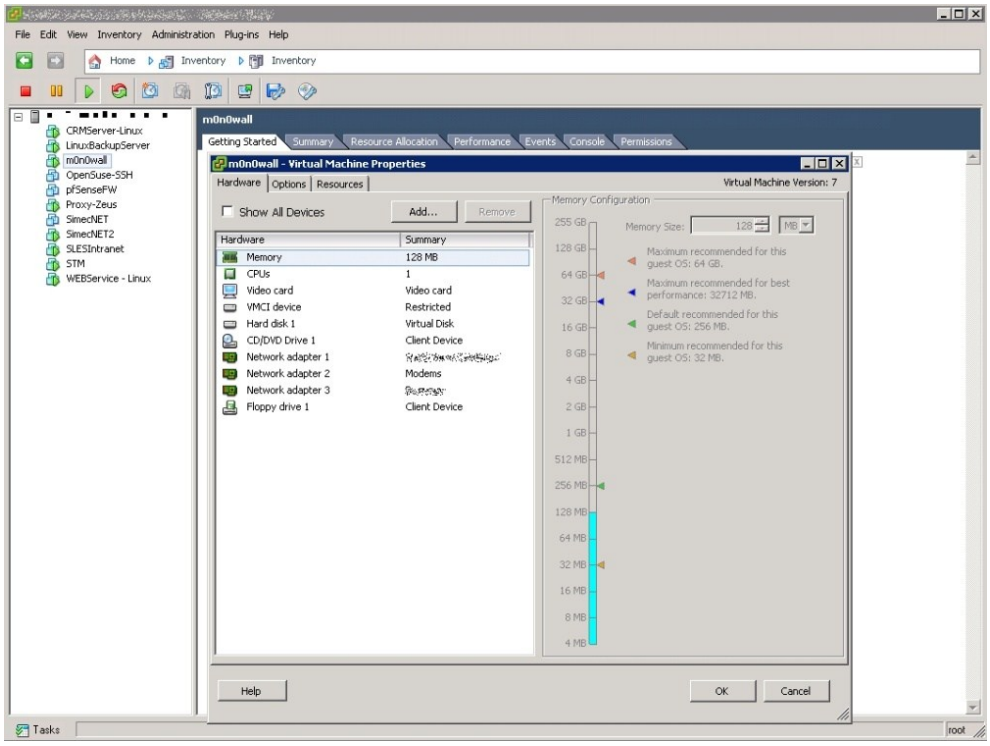

Figura 11– Recursos da máquina virtual destinada ao monowall

Fonte: O Autor

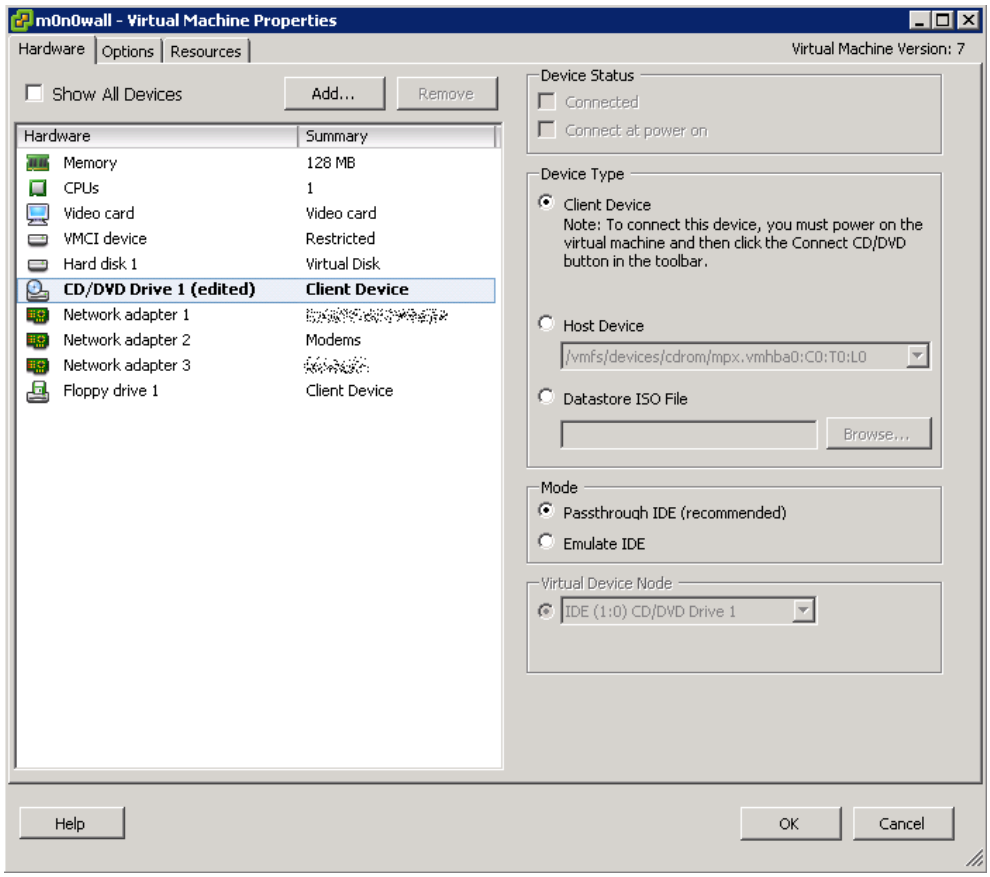

Figura 12– Configuração da Unidade de Leitura de CD

Fonte: O Autor

Após a instalação, é necessário configurar a interface de rede para acesso a interface web de configuração do sistema. O monowall disponibiliza um menu de opções na console, porém são opções bem simples como definir qual interface de rede será a WAN e LAN por exemplo, definição de endereço IP e reset da senha da interface web.

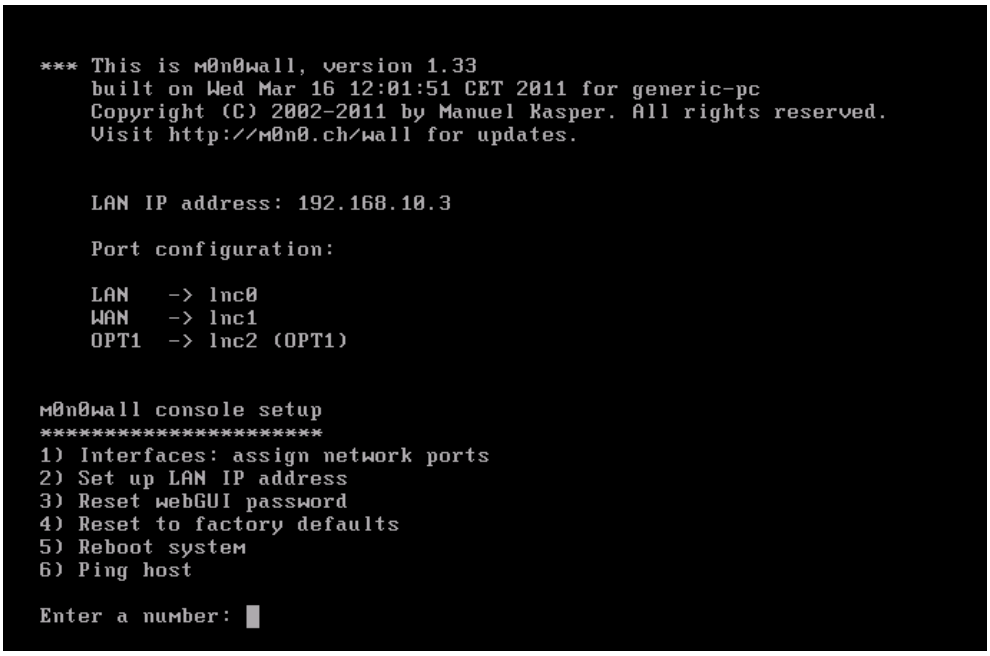

Figura 13– Menu de opções na console do monowall

Fonte: O Autor

A configuração necessária para o estabelecimento da VPN IPsec exige duas interfaces de rede, uma LAN e outra para WAN. Uma vez definida e configurada a interface LAN todas as configurações passam a serem feitas pela interface web.

O cenário inicial proposto era o proposto na figura 13:

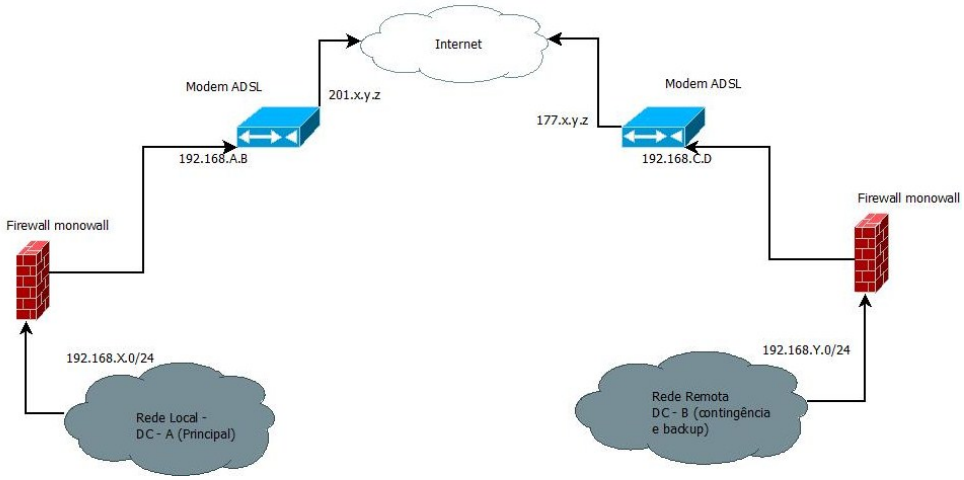

Figura 14 - Cenário Inicial proposto para a VPN IPsec

Fonte: O Autor

O cenário acima, apesar de simples, tem a necessidade de traduções de endereço (NAT) nas duas redes, local e remota, pois o *firewall* responsável pela VPN está antes do modem ADSL, e ainda, a porta WAN do *firewall*monowall, não é exatamente o endereço IP público oferecido pela operadora. Ficando a configuração necessária da seguinte maneira:

DC-A
192.168.X.24/0 -> Nat -> 192.168.A.B/24 -> Nat -> IP WAN modem

DC-B
IP WAM Modem ->nat -> 192.168.C.D/24 ->nat -> 192.168.Y.0/24

Porém com o andamento do projeto, houve uma necessidade de configuração adicional dos modems, nas duas pontas. A configuração em questão trata-se de um regra de entrada para duas portas UDP usadas para o IPsec, que são as portas 500 e 4500 do protocolo UDP, usadas para definir as associações seguras (SAs) e troca de chaves no protocolo IKE. A porta 500/udp sempre é usada, e a 4500/udp quando o protocolo NAT-T (NAT transversal) é usado.

A configuração da rede local, DC-A, foi feita em modem ADSL da marca speedTouch, fornecido pela operadora. A configuração consistiu em definir as portas (500 e 4500) do serviço e o protocolo (TCP ou UDP) usado. No modem speedTouch uma vez feito isso, aponta-se para o dispositivo interno, no caso o monowall, para receber essas conexões.

Figura 15 - Definição do protocolo IKE no modem speedTouch

Fonte: O Autor

Figura 16– Atribuição do Serviço ao host de destino, o monowall

Fonte: O Autor

A próxima configuração seria fazer a mesma liberação no modem na outra ponta, no DC-B, para posteriormente configurar o monowall. Porém nesse caso em uma breve análise do modem, percebi que o modelo de modem instalado no DC-B, já tinha a implementação do protocolo IPsec embutida. Nesse caso, usar o IPsec provido pelo modem resultaria em mais uma economia: uma máquina a menos no meio do caminho, pois deveria fechar a VPN não mais entre dois servidores monowall, mas sim entre um monowall e um modem.O modem em questão é um D-LINK modelo DSL-2730B. O procedimento então prosseguiu com a configuração do IPsec, e o próximo passo foi verificar se seria possível configurar as características IPsec desejadas de forma compatível nas duas pontas.

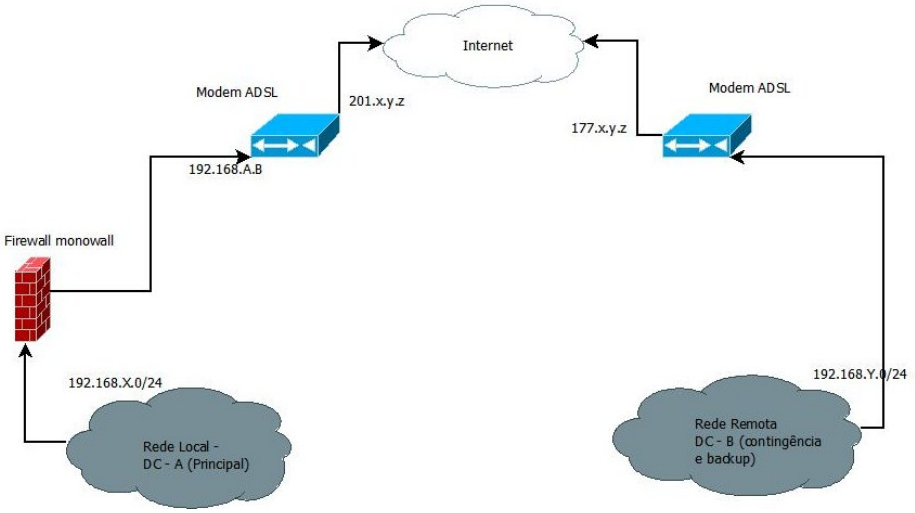

Figura 17– Cenário da rede sem o firewall monowall no DC-B

Fonte: O Autor

A definição da VPN IPsec ficou da seguinte maneira:

VPN Modo Túnel	
Rede local	192.168.X.0/24
Rede Remota	192.168.Y.0/24
Gateway Remoto:	177.x.y.z
Gateway Local	201.x.y.z
Fase 1:	
Modo de Autenticação	PSK – (Chave compartilhada)
Chave	teste123
Modo de trocachave	IKE
PFS	Enable
Identificadores (Peers)	201.x.y.z e 177.x.y.z
Modo Negociação	Main
Algoritmo de Criptografia	3DES
Algotimo de hash	SHA1
Diffie-Hellmann grupo	5
Lifetime:	1800 segundos
Fase 2	
Protocolo	ESP
Algoritmo de Criptografia	3DES
Algoritmo de Hash	SHA1
PFS Key	5
Lifetime	1800 segundos

Tabela 1 – Definição VPN monowall e D-Link

Com base nos dados acima, o passo seguinte foi a configuração do monowall e do modem D-LINK para estabelecer a VPN.

2.1.1.1 - Configuração IPsecmonowall

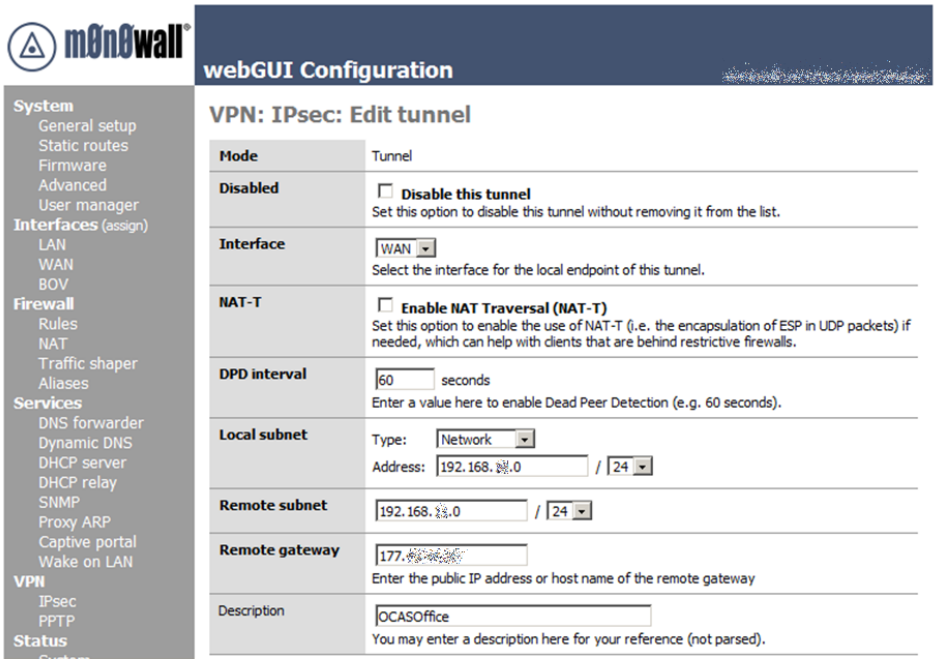

Figura 18– Configuração VPN

Fonte: O Autor

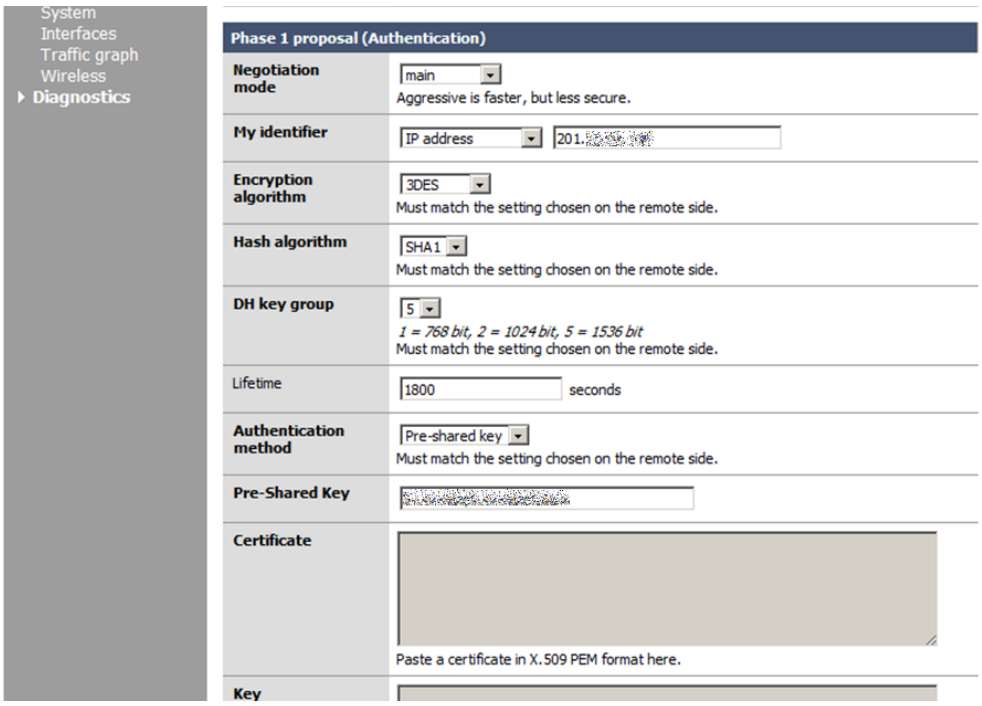

Figura 19– Configuração VPN fase 1

Fonte: O Autor

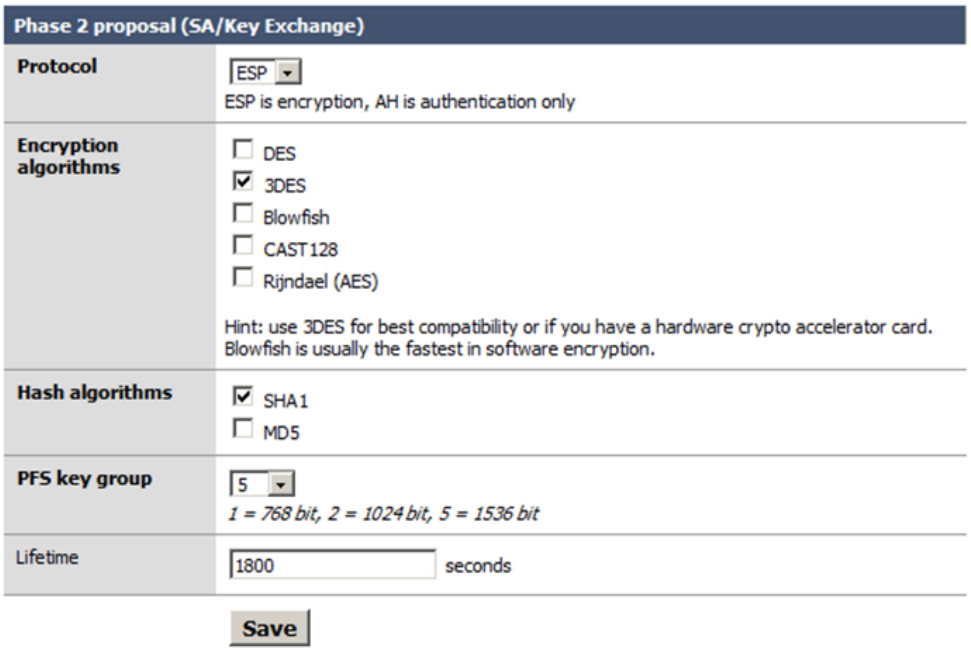

Figura 20 – Configuração VPN fase 2

Fonte: O Autor

2.1.2 Configuração IPsec modem D-LINK

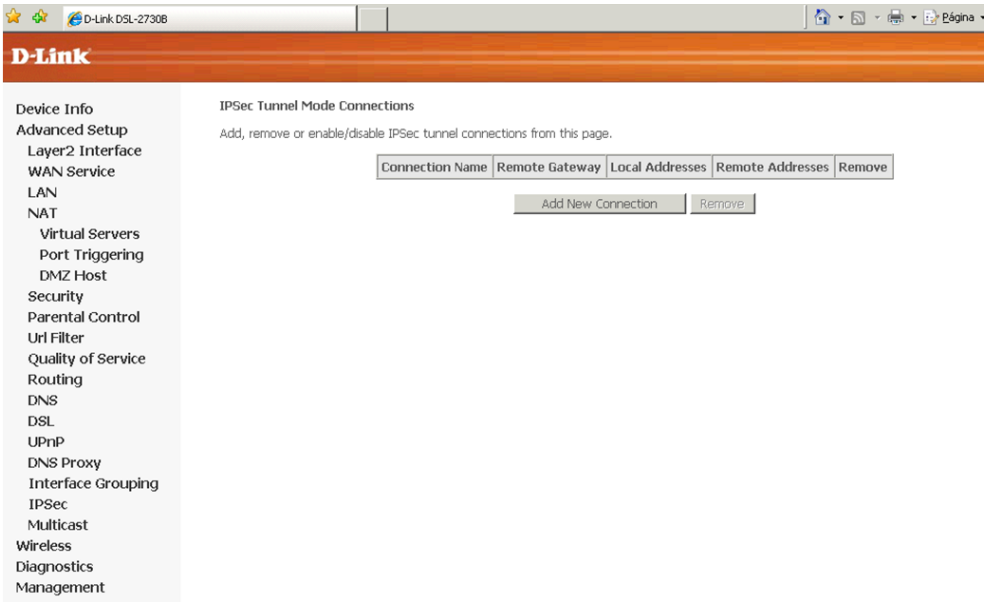

Figura 21- Definindo uma nova VPN no modem D-LINK

Fonte: O Autor

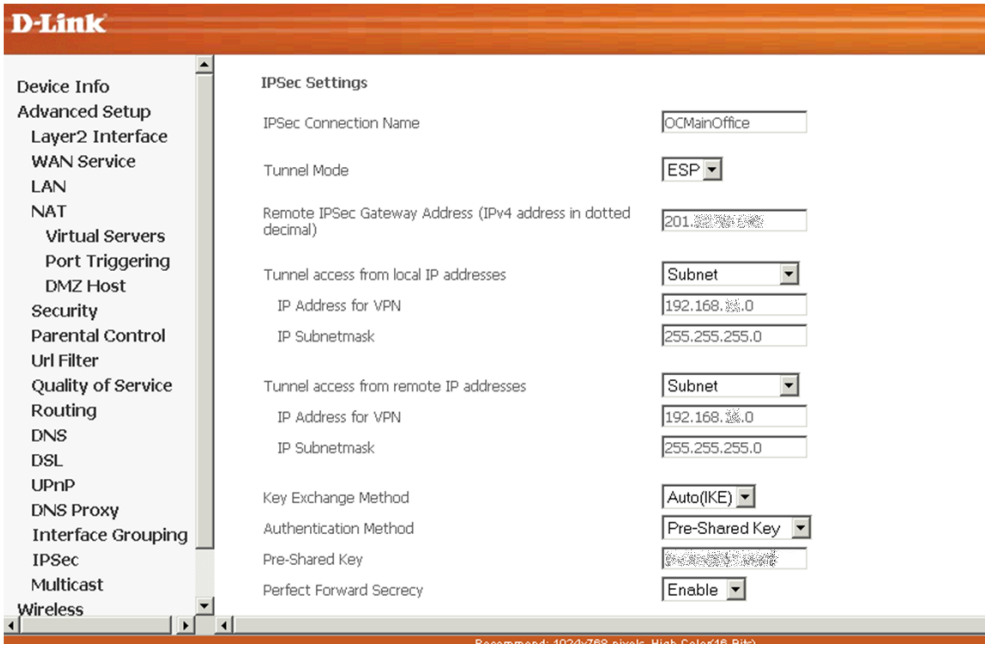

Figura 22– Configuração dos padrões da VPN, rede local, rede remota

Fonte: O Autor

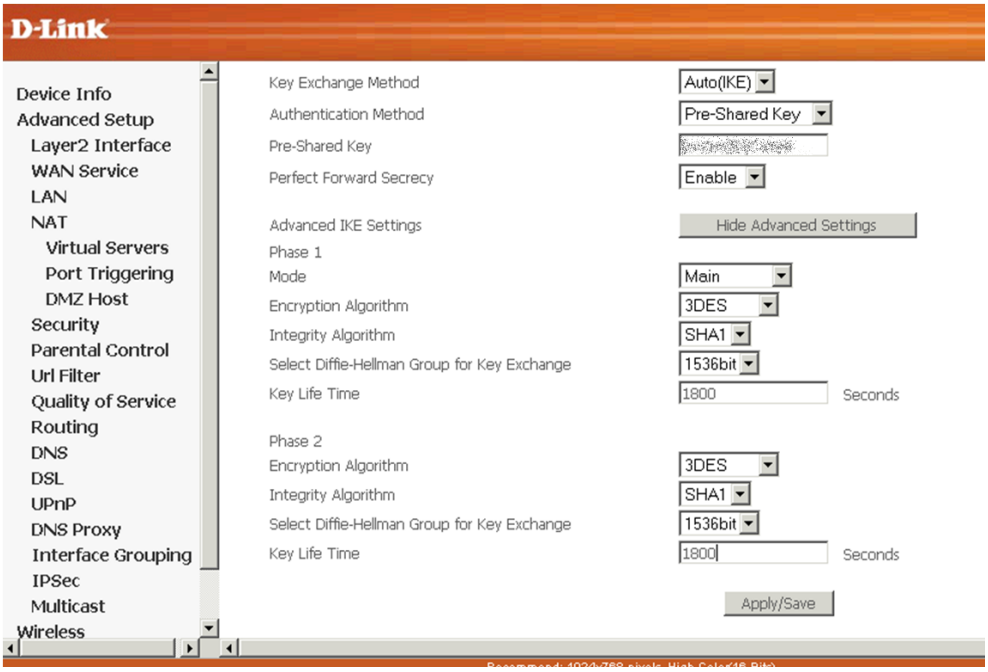

Figura 23– Configuração da fase 1 e fase 2 da VPN IPsec.

Fonte: O Autor

2.1.3 Testes

Após a configuração do monowall e dos modems o passo seguinte foram os testes, que foram efetuados com sucesso, e resultados dentro do esperado.

No item logs do monowall pode-se verificar as associações seguras (SAs) dos túneis estabelecidos.

Jul 11 16:53:42	racoon: INFO: respond new phase 1 negotiation: 192.168.[illegible].108[500]<=>177.[illegible][500]
Jul 11 16:53:42	racoon: INFO: begin Identity Protection mode.
Jul 11 16:53:42	racoon: INFO: received Vendor ID: DPD
Jul 11 16:53:43	racoon: INFO: ISAKMP-SA established 192.168.[illegible].108[500]-177.[illegible][500] spi:8677622eea5ca60e:c3e17089bd6824a9
Jul 11 16:53:45	racoon: INFO: respond new phase 2 negotiation: 192.168.[illegible].108[500]<=>177.[illegible][500]
Jul 11 16:53:45	racoon: INFO: IPsec-SA established: ESP/Tunnel 177.[illegible][0]->192.168.[illegible].108[0] spi=249490758(0xedeed46)
Jul 11 16:53:45	racoon: INFO: IPsec-SA established: ESP/Tunnel 192.168.[illegible].108[500]->177.[illegible][500] spi=16520440(0xfc14f8)

Figura 24– Log do daemonracoon, responsável pelo IPsec no monowall

Fonte: O Autor

Ainda na figura 22 é possível perceber que as Associações Seguras (SAs) não estão sendo fechadas pelos peers, e sim por um peer, o 177.x.y.z e um IP inválido depois do peer 201.x.y.z., isso é devido ao redirecionamento de portas explicado anteriormente, pois a interface WAN do monowall, não está com IP publico, e sim com IP privado, antes do modem.

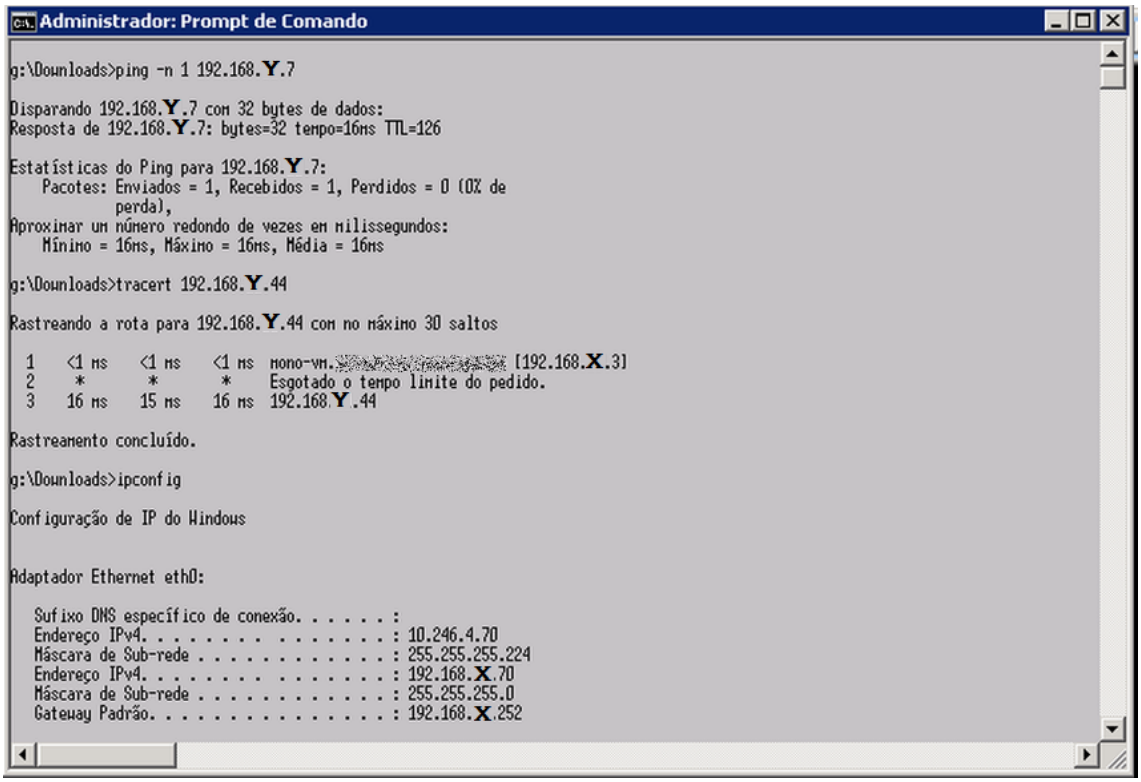

Figura 25– Testes de acesso a rede remota

Fonte: O Autor

Na figura 25, alguns testes simples para mostrar o acesso a rede remota 192.168.Y.0/24 a partir da rede 192.168.X.0/24.

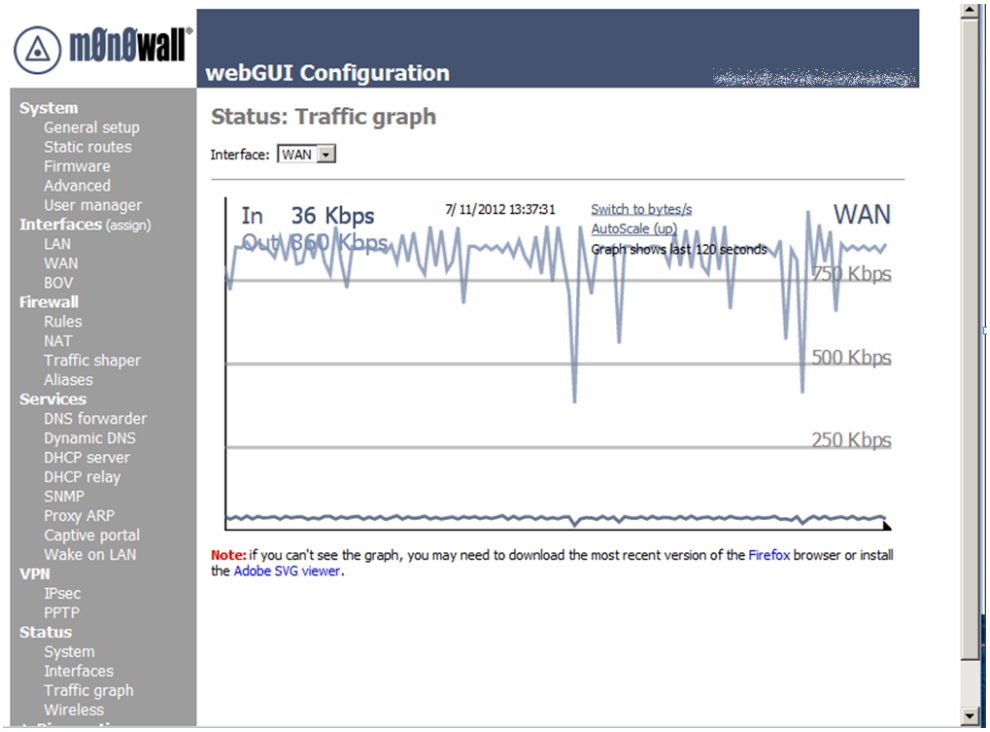

Figura 26– Velocidade medida em Kbps no uso da VPN

Fonte: O Autor

2.1.4 Conclusão

A solução proposta se mostrou muito instável, estando em produção a mais de um ano, com algumas indisponibilidades devido a problemas no fornecimento de banda larga por parte da operadora. A facilidade de implementação da solução também foi outro ponto positivo.

Como os requisitos para essa VPN era apenas uma interligação de uma rede com outra, a solução de fechar VPN entre o servidor monowall e um modem atendeu perfeitamente. Caso fosse necessário a VPN entre dois servidores monowall, a solução também seria assertiva.

2.2 Interconexão de Redes para acesso a serviços de fornecedores

Os casos a seguir de VPNsIPsec, foram um pouco mais complexos já logo no início. No caso anterior, item 2.1, todas as definições foram feitas com base no que já tínhamos instalado no caso as redes, e nos equipamentos que tínhamos disponíveis, o servidor monowall e o modem D-LINK. Um dos problemas enfrentados pela empresa ZXC na comunicação com fornecedores, foi que, as regras definidas para as VPNs eram passadas por eles, os fornecedores, já que a infraestrutura já estava definida na ponta deles, pois os mesmos já atendiam outros parceiros como a empresa ZXC. E logo no início do estudo para instalar o software para fechar a VPN uma regra deixou bem clara a impossibilidade de a VPN ser atendida pelo monowall. Basicamente havia a necessidade de que a rede local de ZXC tivesse conectividade para várias redes ou vários hosts ao mesmo tempo, e o monowall permite apenas uma rede (ou sub-rede) para outra rede(ou sub-rede), tornando impossível atender a necessidade imposta.

Com algumas conversas e troca de informações com um colega que estava procurando uma solução de Proxy e Firewall integrados, mencionei o uso do monowall, porém acrescentei que não disponibilizava de *firewall*, e foi quando ele mencionou o pfSense, que além de todos os componentes de *firewall* do monowall, tinha a possibilidade de ter softwares de Proxy, além de outras aplicações. Acabamos entrando num projeto paralelo para a configuração de um Proxy com o pfSense, e até este momento eu não tinha achado uma solução para o problema de conectividade com os fornecedores da empresa ZXC para fechar a VPN com as regras necessárias, já que dispunha apenas do monowall. Então analisando a documentação do pfSense, verifiquei que a configuração do IPsec atendia prontamente a minha necessidade, com a possibilidade de vários túneis na VPN IPsec. Imediatamente comecei a testar o pfsense, e estudar a melhor possibilidade para colocá-lo em produção.

A configuração de uma VPN lan-to-lan descrita neste item 1.6.2, como citei a pouco, parte de uma configuração imposta pelo fornecedor de serviços, deixando poucas opções de mudanças no que diz respeito ao padrão da

configuração dos túneis. A configuração principal da VPN IPsec no pfSense tem o site remoto configurado em roteadores Cisco ASA. A configuração dos roteadores Cisco não foi compartilhada pelo fornecedor, somente os padrões necessários para fechar os túneis.

2.2.1 Configuração pfSense

Com o pfSense o objetivo foi fechar duas VPNs com dois fornecedores diferentes. A mesma rede local precisaria acessar diferentes serviços, nos dois fornecedores. Selecionei um PC de boa características de hardware para fazer o deploy do pfSense. Como inicialmente já havia testado o pfSense como máquina virtual algumas características já eram conhecidas.

A instalação do pfSense pode ser obtida através do website do projeto, http://www.pfsense.org clicando no item Downloads. Uma explicação das versões disponíveis para download está no link Info / Versions que explica basicamente os três tipos de downloads disponíveis do pfSense, que são:

- Versão Live CD – Instalador
- Versão USB
- Versão NanoBSD para hardwares específicos ou embarcados.

A versão mais recomendada para o propósito de *firewall* e gateway IPsec em um PC é a primeira, a versão Live CD. Nessa versão logo na inicialização há uma opção de execução a partir do CD ou a instalação em disco rígido.

A escolha do hardware, além de ser um bom hardware, teve a necessidade inicial de três interfaces de rede, LAN, WAN e DMZ. A interface LAN para gerenciamento e acesso pela rede local, a Interface WAN para o endereço IP externo na Internet e a interface DMZ para uma sub-rede destinada a servidores.

Após a instalação do pfSense, há a necessidade de atribuir um endereço IP para uma interface, normalmente a WAN, e em seguida a interface LAN, isso para poder disponibilizar o acesso a interface de gerenciamento do pfsense. Essa atribuição é feita na opção 1 e 2 da console de acesso do pfSense (figura 25).

Figura 27- Console de acesso e configuração pfSense

Fonte: O Autor

Uma vez configurado os endereços de WAN e LAN, podemos acessar a interface de gerenciamento WEB do pfSense. Nesta interface é feita toda a configuração do pfSense, inclusive as configurações de interfaces disponíveis na console. Para acesso a Interface WEB basta apontar o browser para http://<endereçoIP> da interface LAN do pfSense. Após passar o login e password inicial, a tela principal será a tela de Dashboard, que é um painel configurável de monitoração do pfSense (figura 26).

Durante as configurações básicas são necessários alguns cuidados de segurança essenciais antes de colocar o pfSense em produção, e antes de conectar o cabo de rede na Interface WAN, é preciso configurar a administração somente para a interface LAN e trocar a senha inicial para uma senha forte. O pfSense não é instalado com nenhuma regra de roteamento e *firewall* por padrão, a não ser a regra de anti-lockout para evitar a perda de acesso a interface, que é uma regra de *firewall* permitindo acesso a interface LAN nas portas 80 e 443 do protocolo TCP.

2.2.2 Configuração dos túneis IPsec

Inicialmente a configuração dos túneis IPsec foi passada pelo fornecedor, e novamente volto a mencionar que é uma configuração imposta a empresa que fará a configuração de acesso, pois devido a conectividade com muitos outros parceiros, várias sub-redes são definidas, uma para cada

parceiro, então a necessidade de se adequar a configuração solicitada por eles. A documentação do fornecedor, que chamaremos de BVC foi passada a empresa ZXC logo após a assinatura de um contrato de confidencialidade assinado pelos representantes legais de ambas as partes.

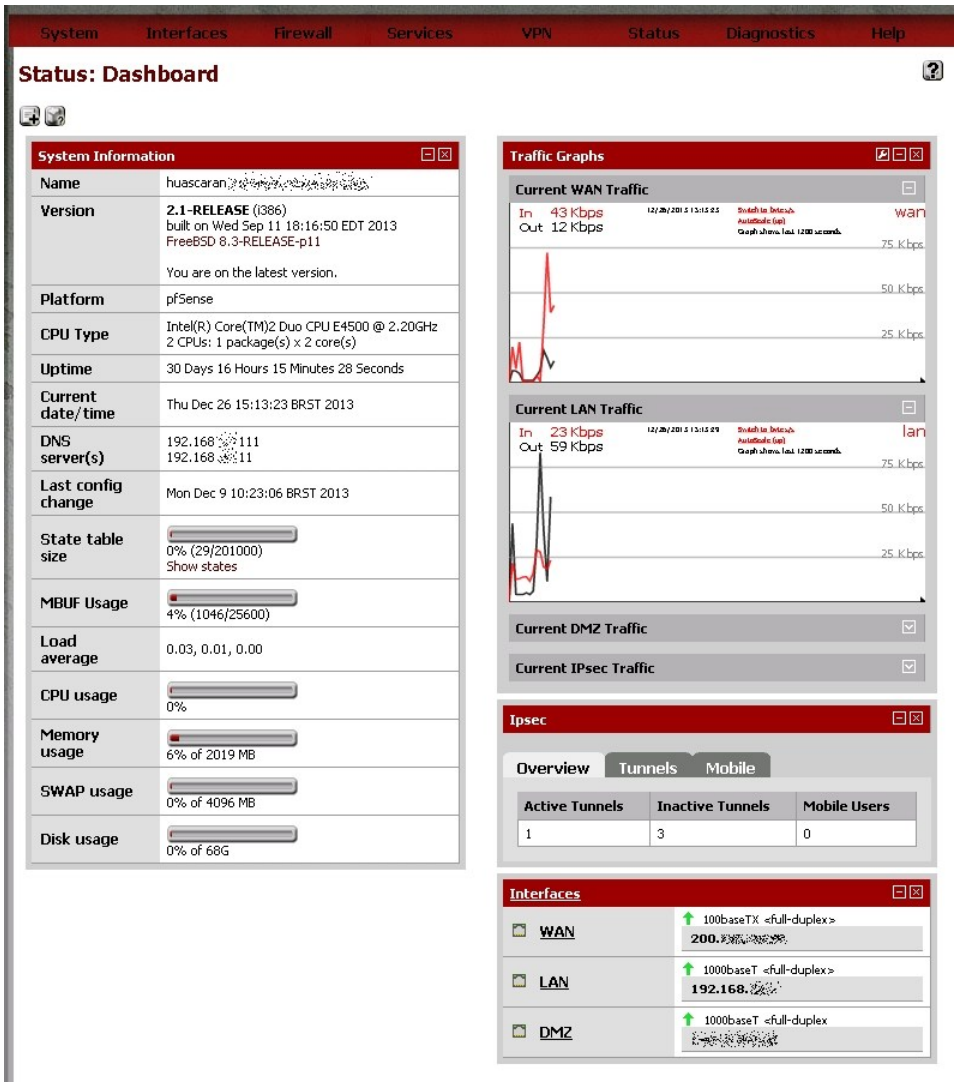

Figura 28 – Dashboard, pfSense

Fonte: O Autor

A configuração para os túneis IPsec enviada à empresa ZXC pelo fornecedor BVC está na tabela 2.

VPN Modo Túnel	
Túneis	
ISAKMP udp/500	200.Z.Y.Z <-> 200.I.J.K
ISAKMP udp/500	200.I.J.K <-> 200.Z.Y.Z
ISAKMP ESP 50	200.Z.Y.Z <-> 200.I.J.K
ISAKMP ESP 50	200.I.J.K <-> 200.Z.Y.Z
Serviços http-https-ftp-1445/tcp	10.x.y.z/27 <-> 200.a.b.c/24
	10.x.y.z/27 <-> 200.a.b.d/24
	10.x.y.z/27 <-> 177.a.b.c/24
	10.x.y.z/27 <->177.a.b.d/24
Fase 1:	
Modo de Autenticação	PSK (chave compartilhada)
Chave	exemplo123
Modo de trocachave	IKE
PFS	Enable
Modo Negociação	Main
Algoritmo de Criptografia	3DES
Algotimo de hash	SHA1
Diffie-Hellmann grupo	2
Lifetime:	86400 segundos
Fase 2	
Protocolo	ESP
Algoritmo de Criptografia	3DES
Algoritmo de Hash	SHA1, hmac
PFS Key	2
Lifetime	4608000 kilobytes/3600 segundos

Tabela 2 – Configuração necessária para estabelecer os túneis IPsec entre a empresa ZXC e BVC

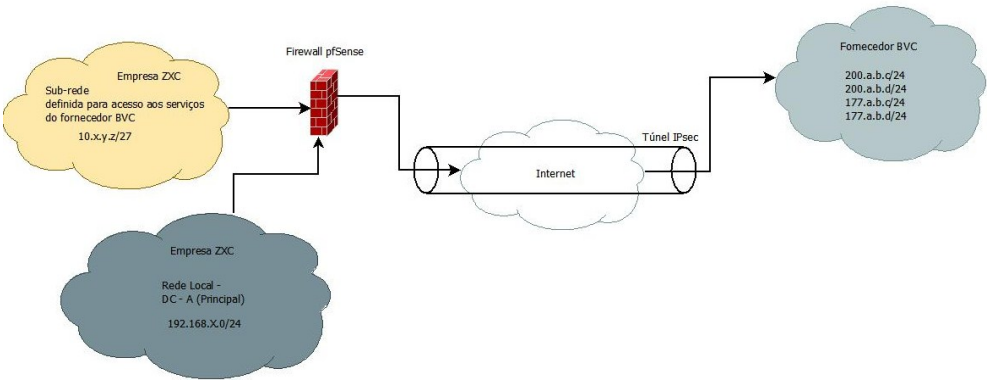

Figura 29– Esquema da VPN IPsec para acesso às redes da empresa BVC

Fonte: O Autor

Com base nas informações da tabela 2, o próximo passo foi realmente configurar o pfSense. No menu principal, VPN / IPsec, inicialmente foi feita a configuração para uma VPN IPsec fase1, e após a fase1 configurada, pode-se configurar as outras fases 2.

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN 200.[redacted]	main	3DES	SHA1	VPN[redacted]

Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods
tunnel	10.[redacted]/27	200.[redacted]/24	ESP	3DES	SHA1
tunnel	10.[redacted]/27	200.[redacted]/24	ESP	3DES	SHA1
tunnel	10.[redacted]/27	177.[redacted]0/24	ESP	3DES	SHA1
tunnel	10.[redacted]/27	177.[redacted]0/24	ESP	3DES	SHA1

Figura 30– Painel de configuração VPN IPsecpfSense

Fonte: O Autor

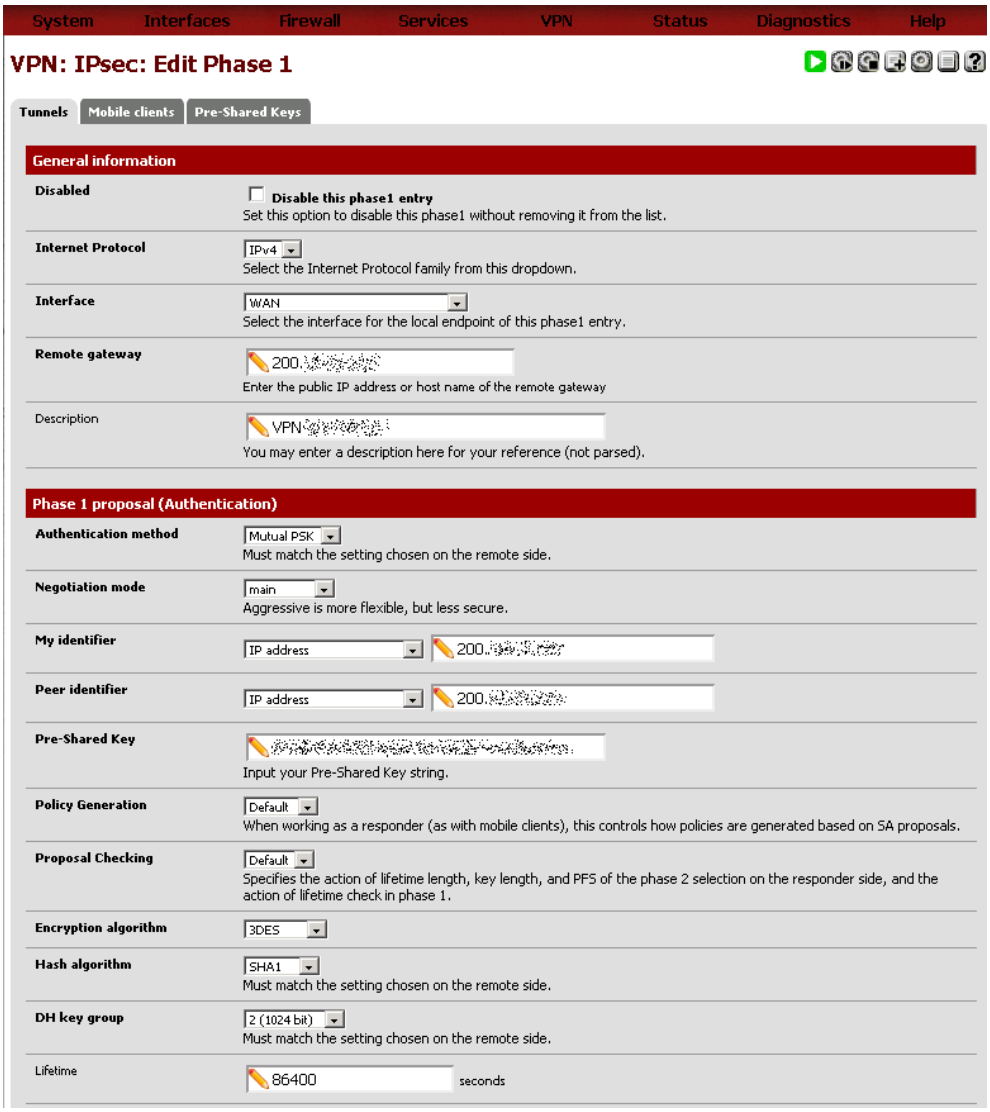

Figura 31– Configuração da VPN IPsec fase1

Fonte: O Autor

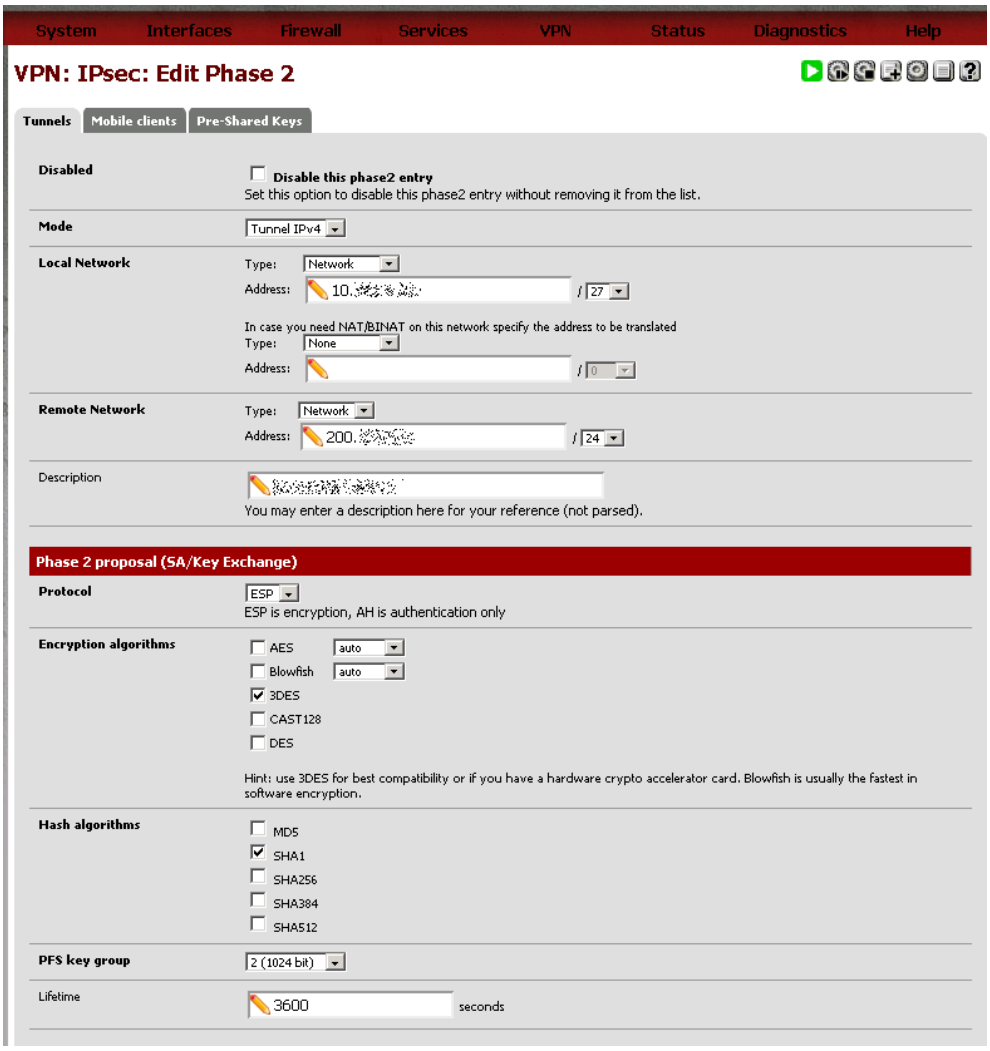

Figura 32– Configuração da VPN IPsec fase2

Fonte: O Autor

Na figura 29 está a configuração da VPN fase 1, e na figura 30, está um exemplo de configuração de um dos túneis fase 2 configurados, ao todo foram 4 como mostrado na figura 28. A configuração dos túneis fase 2 são as mesmas, somente alterando os endereços IPs de relacionamento.

Após a configuração foi necessário configurar na infraestrutura de rede a sub-rede proposta na documentação. Uma vez feita essa configuração, os testes puderam ser efetuados apontando rotas para as redes remotas do fornecedor BVC tendo como *gateway* para essas rotas, o servidor pfSense. É importante dizer que, caso o servidor pfSense não fosse o *gateway* principal da rede, como nesse caso da empresa ZXC, há a necessidade de configurar as

rotas no *gateway* principal, ou na estação que fará acesso as redes remotas pela VPN IPsec.

Neste ponto uma configuração específica foi feita para que o acesso pudesse acontecer. Na sub-rede proposta pelo fornecedor BVC, a rede 10.x.y.z/27, um endereço dessa rede foi configurado como endereço IP virtual no pfSense, figura 31 a 33. Esse endereço virtual, posteriormente foi configurado como *Gateway*da rede 10.x.y.z/27, figura 34. E na figura 35, foi adicionada uma rota estática para a rede através do *gateway* previamente cadastrado.

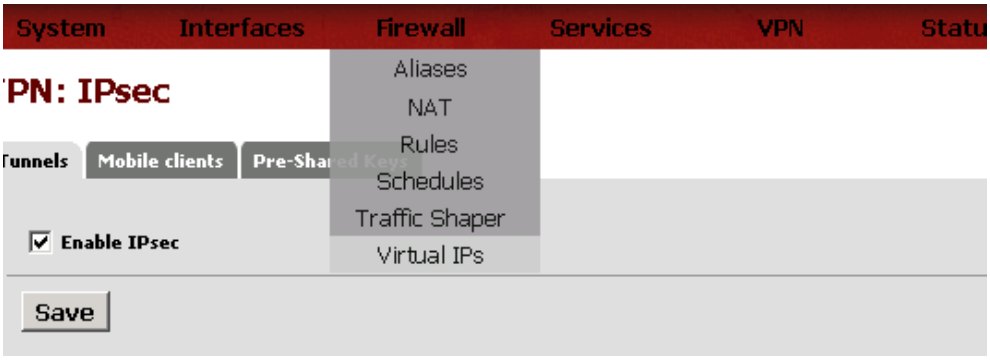

Figura 33– Menu de configuração de Endereço IP virtual

Fonte: O Autor

Figura 34 - Configuração de IP virtual, interface e máscara de rede

Fonte: O Autor

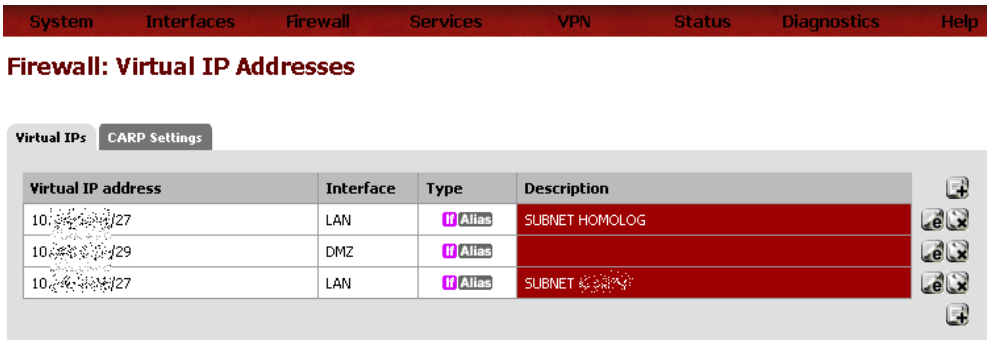

Figura 35– Lista de IPs Virtuais

Fonte: O Autor

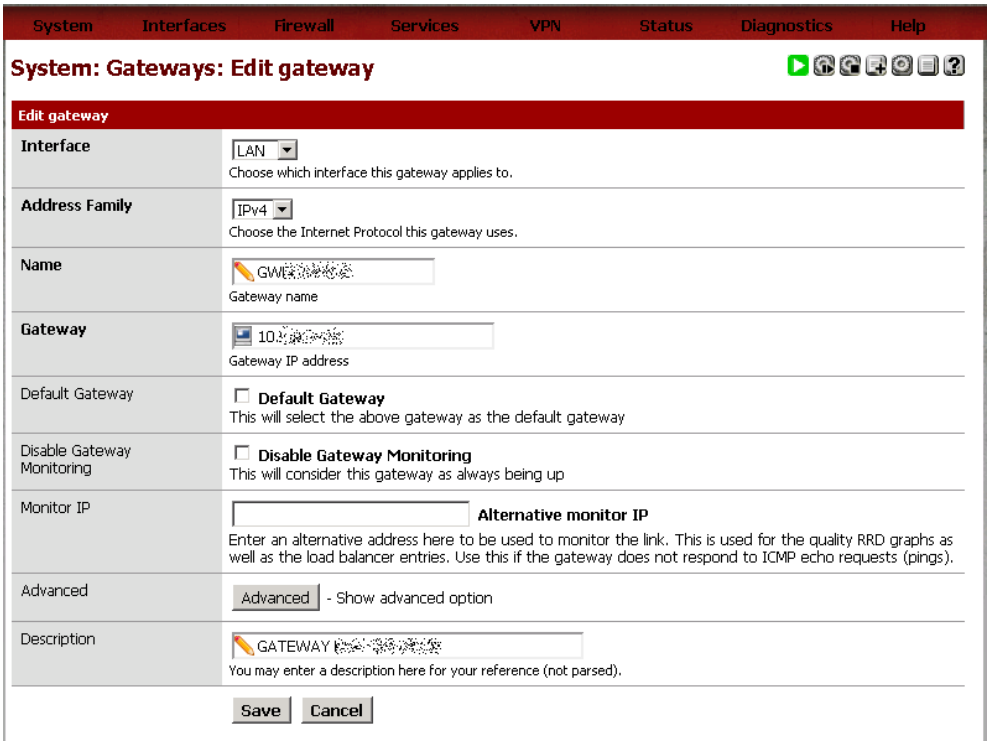

Figura 36 - Configuração do IP Virtual como gateway da sub-rede

Fonte: O Autor

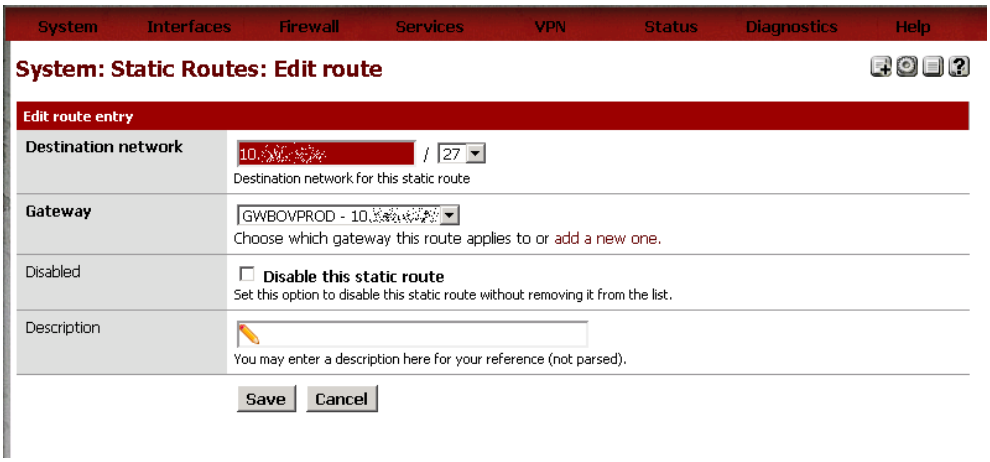

Figura 37 - Rota para a rede 10.x.y.z/27 através do gateway previamente cadastrado

Fonte: O Autor

Uma vez configurado o *gateway*, uma tentativa de acesso aos endereços da rede remota, faz com que o *daemon* da VPN IPsec procure fechar o túnel para estabelecer a comunicação. No entanto para que a conexão realmente seja estabelecida, é necessária uma regra de *firewall* permitindo o acesso a partir da rede 10.x.y.z/27 para as redes remotas listadas na tabela 2. Na figura 36 é mostrado o menu de acesso as regras de *Firewall*. Na figura 37, estão relacionadas as regras de acesso para a sub-rede ZXC acessar os serviços disponíveis no fornecedor BVC. Vale ressaltar que a relação de serviços disponíveis, foi disponibilizada em um documento específico. No *firewall* do fornecedor BVC essas regras também foram aplicadas.

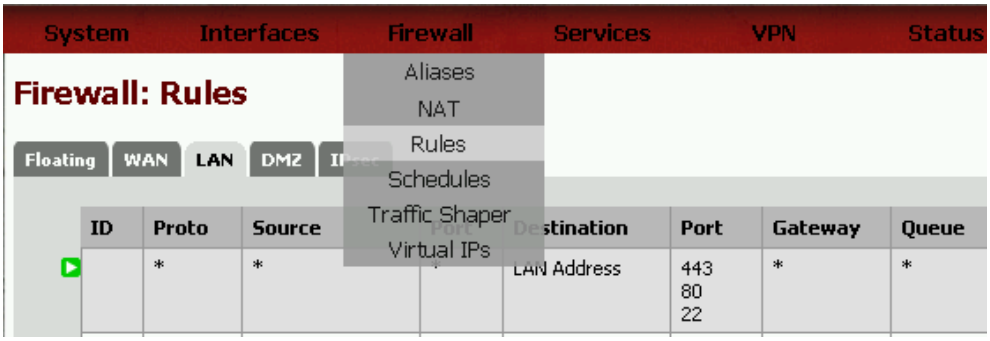

Figura 38– Regras de Firewall

Fonte: O Autor

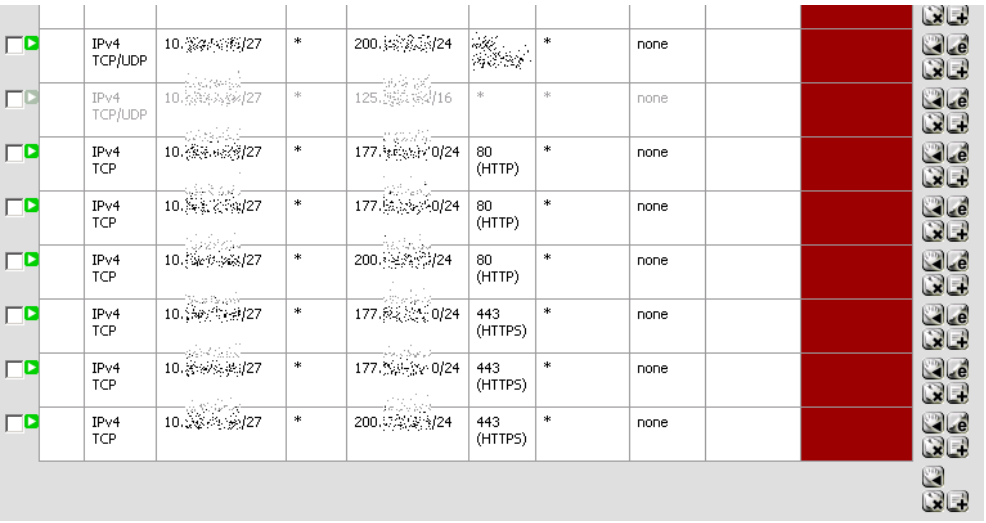

Figura 39 - Regras de Firewall, separadas por serviços

Fonte: O Autor

2.2.3 Testes

Após as configurações feitas, o próximo passo foi começar os testes. Com uma estação de usuário já configurada para acesso com o endereço IP da sub-rede, o teste inicial foi fazer um acesso a um dos serviços relacionados na documentação. Na opção do menu principal do pfSense em Status / IPsec pode-se obter informações de como está o funcionamento da VPN. Nesta opção são mostradas as Associações Seguras (SAD – Security AssociationDatabase), que é uma relação de todas as associações seguras estabelecidas entre os roteadores, no nosso casoopfSense e o Cisco. Também são mostradas as Políticas de Segurança através do SPD (Security PolicyDatabase), que define como o tráfego será protegido e qual o protocolo será usado, neste o ESP. Na figura 38, a VPN está pronta, porém sem nenhum acesso, pois na coluna Status o símbolo em amarelo indica que não há nenhuma comunicação.

O estabelecimento do túnel para a comunicação entre as redes, pode ser feita de maneira forçada pelo Administrador no próprio pfSense, ou sob demanda pelo usuário ao acessar qualquer serviço que procure a rede remota. A figura 39 mostra um túnel fechado na coluna status, e na figura 40, de Associações Seguras, mostra duas associações, uma em cada sentido de

comunicação, com bytes enviados e bytes recebidos. Neste caso, há uma comunicação em andamento. De fato, clicando-se em Logs, pode-se verificar o log do *daemon*racoon (figura 42), onde é mostrada a negociação da fase 2 da VPN IPsec e os SPIs, que são os identificadores da política de segurança aplicada as associações seguras.

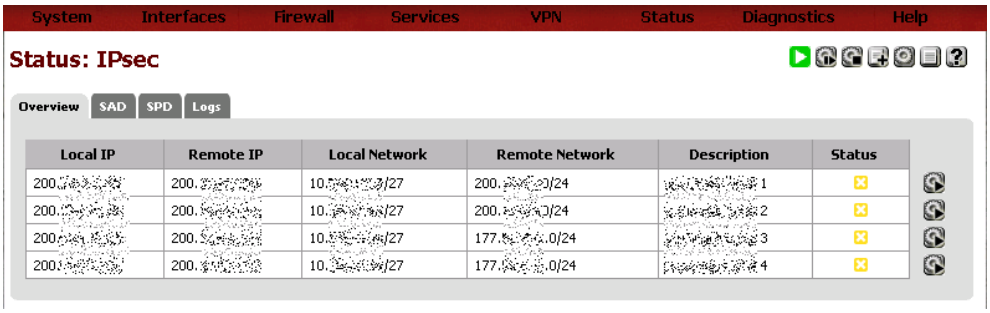

Figura 40 - VPN sem atividade

Fonte: O Autor

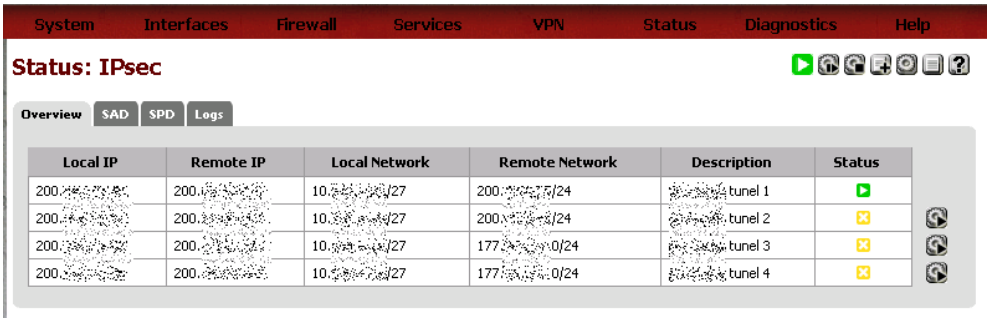

Figura 41– VPN em atividade

Fonte: O Autor

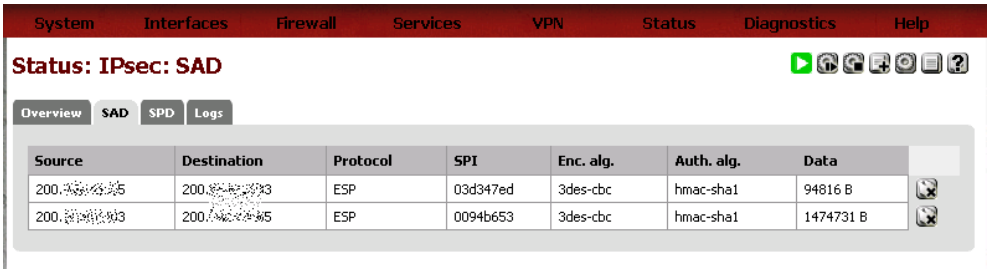

Figura 42– Associações Seguras

Fonte: O Autor

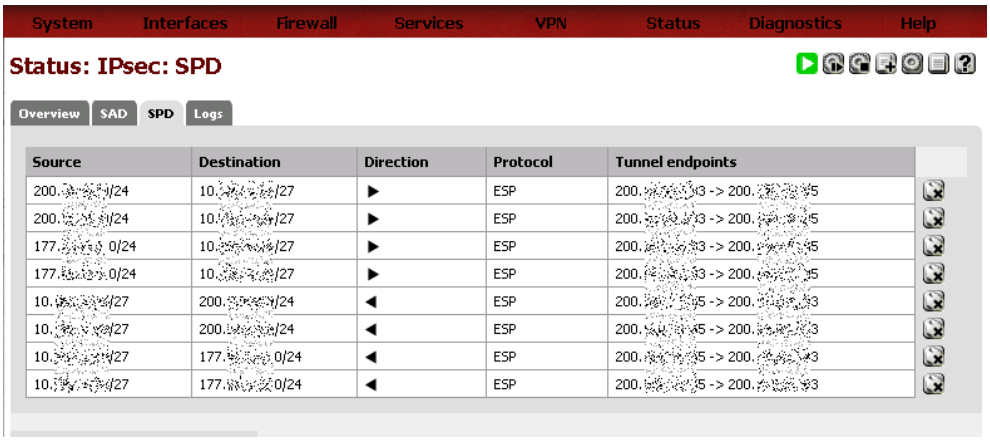

Figura 43– Políticas de Segurança

Fonte: O Autor

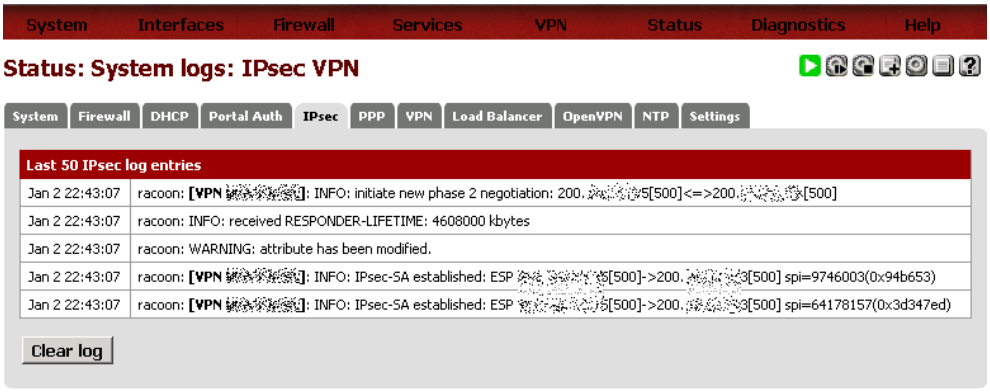

Figura 44– Logs do daemonIPsec (racoon)

Fonte: O Autor

Os primeiros acessos para testes efetuados foram os acessos a serviços http e https, que no início teve um tempo de resposta um pouco alto. O link utilizado nesse ambiente, embora compartilhado com outros serviços, dispõe de uma banda de 5Mbps, então o início houve alguma suspeita de incompatibilidade, porém os serviços testados funcionaram.

É importante salientar que todas as aplicações testadas na VPN IPsec já funcionavam perfeitamente através de um link dedicado com o fornecedor BVC, e a partir da validação dos acessos feitos pela VPN IPsec, estas aplicações foram migradas uma a uma. A migração dependeu principalmente na mudança dos cadastros dos hosts nos servidores DNSs internos da empresa ZXC. Uma vez os hosts apontando para as redes cujos destinos são

as redes remotas da VPN, automaticamente o tráfego foi direcionado para a VPN.

Um acesso a um sistema gerencial, uma aplicação de gerenciamento de conteúdo cujo servidor é DB2 se mostrou um problema inicialmente. Essa aplicação traz os dados em forma de relatórios para o usuário, e é acessada mediante credenciais já existentes. O sistema estava fazendo a validação de usuário, mas, em seguida congelava a tela. Através de analisadores de pacotes na estação e no servidor, de alguma maneira havia uma comunicação inicial, mas que em seguida parava.

A primeira suspeita era a fragmentação de pacotes, pois como os analistas da empresa BVC sugeriram, nos roteadores Cisco há a necessidade de configurar a fragmentação. No entanto, pela documentação do pfSense, a fragmentação é reconhecida e tratada por padrão, não havendo necessidade de tal configuração. O que poderia ser feito seria a mudança do valor do MTU. O valor do MTU, a unidade máxima de transferência é 1500 bytes, mas esse valor cai para conexões PPP ou VPN, por exemplo. Há uma maneira de descobrir o valor do MTU entre duas conexões usando o comando ping, porém no nosso caso isso não foi possível, pois o protocolo ICMP não foi liberado na regra de *firewall*. A alternativa foi alterar o MTU ate achar o MTU para o correto funcionamento da VPN.

O pfSense tem em sua configuração padrão um MTU de 1400 bytes para tráfego via VPN, caso seja necessário diminuir, há um item chamado de MSS (MaximumSegmentSize – tamanho máximo do segmento), que é uma propriedade do protocolo TCP, podendo ser alterado para qualquer valor de ajuste (figura 43). O valor do MSS pode ser alterado pelo menu system / Advanced / Miscellaneuos / Maximum MSS.

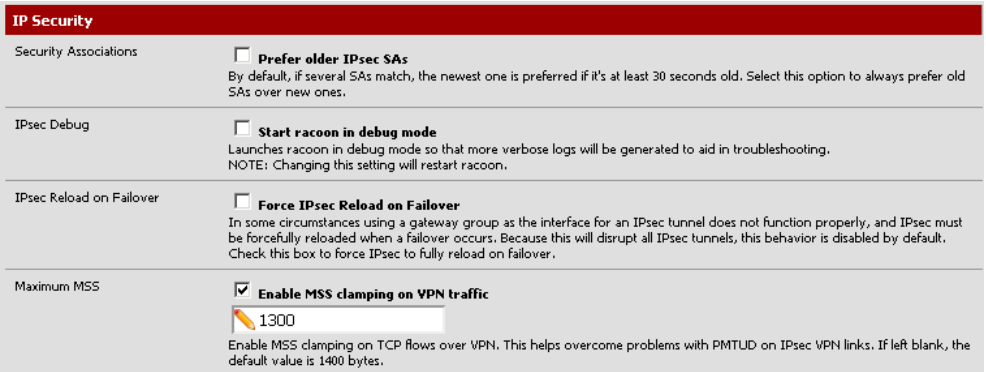

Figura 45– Alteração do tamanho do segmento via VPN

Fonte: O Autor

Após essa alteração, a resposta ao acessar os serviços http e https ficaram muito boas e o problema com a aplicação de acesso ao DB2 também foi resolvido.

Ainda com um uso pequeno, a VPN tem se mostrado estável e com boa resposta para os acessos e tráfego de dados de um modo geral. Uma amostra da taxa em bits por segundo pode ser verificada na figura 44. Também, pode-se verificar uma média no tempo de resposta como um todo na comunicação da VPN na figura 45. Após a migração dos serviços do antigo link para a VPN IPsec não houve reclamação por parte dos usuários, o que tornou a migração totalmente transparente.

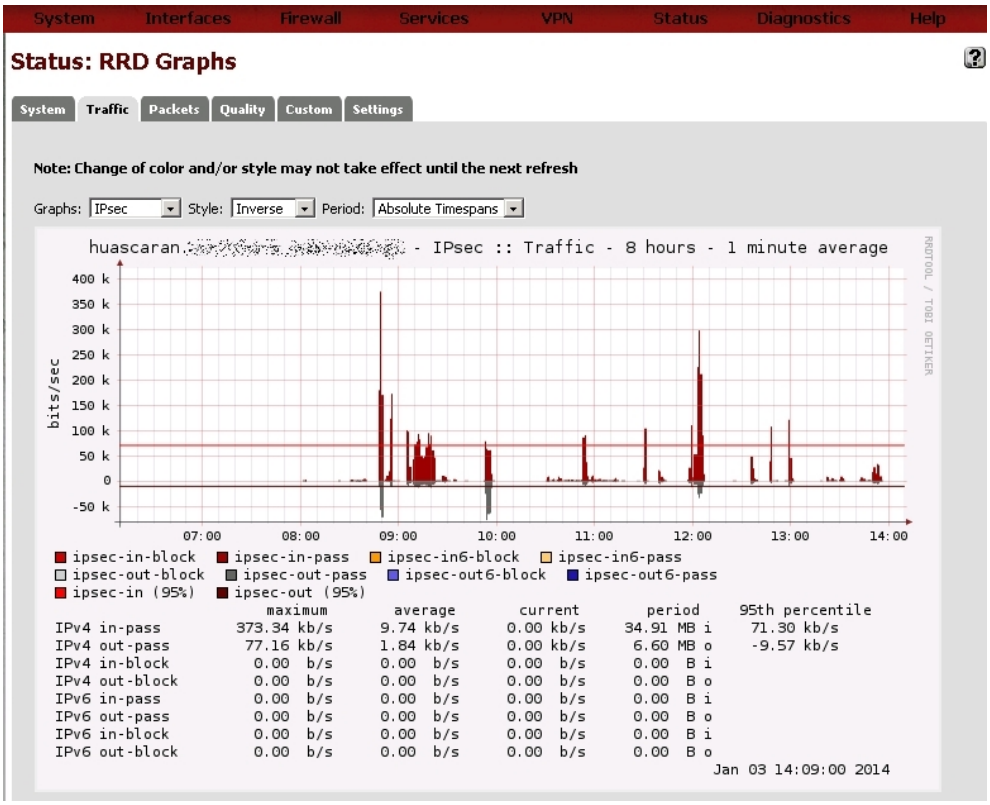

Figura 46– Velocidade em bits por segundo

Fonte: O Autor

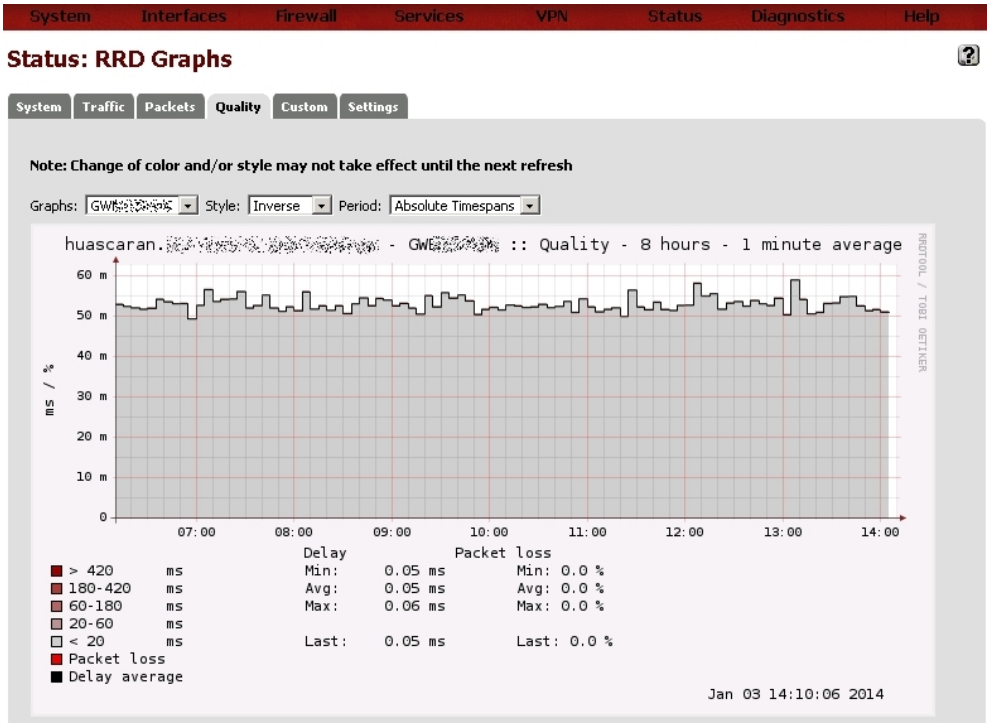

Figura 47– Tempo de resposta em milissegundos

Fonte: O Autor

3 CONCLUSÃO

As soluções de VPN IPsec mostradas neste trabalho surgiram como necessidade abrupta, e foram executadas com quase nenhum orçamento, e sobre isso as duas soluções apresentaram baixos custos se comparadas com outras soluções disponíveis no mercado, como soluções com roteadores ou fornecidas por operadoras. A primeira VPN estabelecida com o monowall reduziu os custos de comunicação entre dois sites de R$1800,00 para R$400,00 e, a segunda VPN estabelecida com o pfSense reduziu um custo de comunicação de R$7500,00 de um link interestadual, para um custo de R$800,00 por mês, já que o fornecedor BVC cobra uma taxa para estabelecer a VPN. O link de utilização para a VPN do pfSense, é um link utilizado também para outros fins, e nesse caso, o custo é diluído, não ficando exclusivo da VPN.

Além da economia, a facilidade de administração das soluções implantadas é inquestionável. Como citado neste documento, é necessário ter um conhecimento do que está se propondo a fazer, no entanto a administração dos servidores é bem menos complexa se compararmos a roteadores ou com um sistema operacional específico.

Com backups de configuração frequentes, é possível montar o mesmo ambiente em outro servidor, bastando restaurar o backup. É importante dizer que o servidor deve ter as mesmas características. No caso da VPN IPsec estabelecida com o pfSense, a empresa ZXC já tem outro servidor com as mesmas características pronto e com o backup restaurado, para caso haja uma falha de hardware no servidor principal.

As soluções apresentadas aqui não são exclusivas, e há muitas maneiras de estabelecer VPNsIPsec. Existem softwares livres, como é o nosso caso, mas também existem softwares proprietários, e cada um atende uma determinada situação, porém é preciso analisar caso a caso, pois não há porque ter custos com equipamentos ou softwares quando não há necessidade. Uma VPN lan-to-lan, como no primeiro caso, é um caso com requisitos simples, e o monowall foi uma solução rápida para atender esses requisitos. Soluções alternativas, com base nos softwares usados pela empresa ZXC, poderiam ser feitas com o Firewall Microsoft ForeFronte

o Endian Firewall (versão community). No caso do pfSense as regras exigidas pelo parceiro BVC eram de uma sub-rede acessando outras sub-redes, tornando um pouco mais complexo o cenário. Soluções alternativas poderiam ser executadas com roteadores, *daemons*IPsec sendo executados em servidores Unix ou Linux e um ultimo software proprietário que testamos por um período, o Green Bow VPN. Estas soluções conseguem adicionar vários túneis em uma mesma VPN, atendendo a necessidade inicial. Para atender essa necessidade foi testado o Endian Firewall, Mocrosoft ISA Server e o Microsoft ForeFront, porém, a necessidade de vários túneis de sub-redes para várias sub-redes e sub-redes para alguns hosts somente não foi atendida ou tornou-se muito complexa durante a configuração.

O pfSense tem grandes vantagens como *firewall*, pois utiliza um sistema operacional confiável e pode ter várias funções, como servidor Proxy, servidor DHCP, filtro de conteúdo, além de *firewall* o que torna um bom software para ser utilizado como *gateway* principal de uma rede, sem a necessidade de ter vários servidores. Se comparar com um servidor Linux, para ser executado com as mesmas funções do pfSense a mão de obra é grande, pois há a necessidade de configurar cada aplicativo separadamente, e aqui, muitas vezes são encontradas dificuldades em relação a versões dos pacotes disponíveis.

A empresa citada neste trabalho, a ZXC, conta com um parque de servidores e entre eles estão um servidor Microsoft ForeFront, um servidor Linux atuando como Servidor Proxy e Firewall em conjunto com o ForeFront, porém até a conclusão deste trabalho um projeto já está em andamento para a substituição dos servidores citados pelo pfSense, pois até agora este está atendendo todos os requisitos necessários como servidor, não só de *gateway* VPN IPsec, mas também como roteador e Proxy.

REFERÊNCIAS

TANEMBAUM, Andrew S**..Computer Networks 4th Edition**. Prentice Hall 2003

GHEORGHE, Lucian. **Linux Firewalls and QoS**.Birmingham: Packt Publishing 2006

GARFINKEL, Simson; SCHWARTZ, Alan; SPAFFORD, Gene.**PracticalUnix& Internet Security, 3rd Edition**.O'Reilly 2003

SCOTT, Charlie; WOLFE, Paul; ERWIN, Mike.**Virtual Private Networks, 2nd Edition**, O'Reilly 1999

CARMOUCHE, James Henry. **IPsec Virtual Private Network Fundamentals.** Cisco Press, 2006

DIBONA, Chris; OCKMAN, Sam.**OPEN SOURCES: Voices from the Open Source Revolution**. O'Reilly Media. 1999.Disponivel em: <http://oreilly.com/catalog/opensources/book/kirkmck.html/>, acesso em 15 de Nov. 2013.

FREEBSD DOCs: Disponível em: <http://www.freebsd.org/doc/en/articles/explaining-bsd/what-a-real-unix.html/>, acesso em 15 de Nov. de 2013.

PFSENSE.ORG: Disponível em: < http://www.pfsense.org/>, acesso em 03 de Jan. de 2014.

MONOWALL HANDBOOK: Disponível em: <doc.m0n0.ch/handbook-single/>, acesso em 20 de novembro de 2013.

WIKIPEDIA - AES: Disponível em: <http://en.wikipedia.org/wiki/Advanced_Encryption_Standard>, acesso em dez. 2013.

IPSEC HOWTO: Disponível em: <http://www.ipsec-howto.org/>, acesso em 05de janeiro de 2014.

VIVAOLINUX: Disponível em: <http://www.vivaolinux.com.br/artigo/Fundamentos-da-criptografia-assimetrica?pagina=4/>, acesso em 15 de dezembro de 2013.

RFC 1827: Disponível em: <http://www.rfc-editor.org/rfc/rfc1827.txt>, acesso em dezembro de 2013

RFC 2401: Disponível em: <http://www.rfc-editor.org/rfc/rfc2401.txt>, acesso em dezembro de 2013