

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

ALEXANDRE DE SABOYA PEREIRA

IMPLEMENTAÇÃO DE UMA REDE VIRTUAL PRIVADA – VPN- NA FEDERAÇÃO
DAS INDÚSTRIAS DO RIO GRANDE DO NORTE – FIERN

NATAL/RN
2009

ALEXANDRE DE SABOYA PEREIRA

IMPLEMENTAÇÃO DE UMA REDE VIRTUAL PRIVADA – VPN- NA FEDERAÇÃO
DAS INDÚSTRIAS DO ESTADO DO RIO GRANDE DO NORTE – FIERN

Monografia apresentada ao curso Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte – FARN. Como requisito obrigatório para obtenção do título de Especialista em Redes de Computadores.

Orientador: Dr. Aluizio Ferreira da Rocha Neto

Natal / RN
2009

RESUMO

Esta trabalho é referente a um estudo de caso sobre utilização de redes virtuais privadas – VPN – na Federação das Indústrias do Rio Grande do Norte. Nele, será mostrado algumas tecnologias existentes para interligar redes de computadores bem como um estudo de viabilidade entre a tecnologia em uso atualmente na Federação das Indústrias do Rio Grande do Norte (“Frane-Relay”) e um estudo de viabilidade de implementação de VPN utilizando o software OpenVPN. Além do estudo em si está incluído um pequeno exemplo da configuração mínima para se interligar uma unidade operacional ao prédio da casa da indústria, sede do Sistema FIERN.

ABSTRACT

This work is related to a case study on the use of virtual private networks - VPN - the Federation of Industries of Rio Grande do Norte. In it will be shown some existing technologies to interconnect computer networks and a feasibility study of technology in use today at the Federation of Industries of Rio Grande do Norte (Frane-Relay ") and a feasibility study of implementing a VPN using OpenVPN software. Besides the study itself is included a small example of minimal configuration to connect a facility to house building industry, head offices of the FIERN.

Sumário

1 INTRODUÇÃO	6
1.1 PROBLEMA DA PESQUISA	7
1.2 OBJETIVOS	
1.2.1 objetivos gerais	8
1.2.2 objetivos específicos.....	8
1.3 JUSTIFICATIVA	9
2 REFERENCIAL TEÓRICO	10
2.1 REDE INTERNA (INTRANET).....	10
2.2 MODELO OSI.....	10
2.3 ADSL	11
2.4 FRAME-RELAY	11
2.5 VIRTUAL PRIVATE NETWORK (VPN)	11
2.5.1 point to point tunneling protocol (pptp)	12
2.5.2 layer two forwarding (l2f)	13
2.5.3 layer two tunneling protocol (l2tp).....	14
2.5.4 ip security protocol (ipsec)	15
2.6 SOFTWARE LIVRE	18
2.7 FIREWALL NETFILTER/IPTABLES	19
2.8 NETWORK ADDRESS TRANSLATION - NAT	20
3 METODOLOGIA.....	21
4 DESENVOLVIMENTO	22
4.1 LEVANTAMENTO DOS CUSTOS.....	22
4.1.1 custos atuais.....	22
4.1.2 custos adsl.....	23
4.2 INSTALAÇÃO E CONFIGURAÇÃO DA VPN	24
4.2.1. instalação dos pacotes	24
4.2.2. geração de chaves estáticas	24
4.2.3. arquivos de configuração	26
4.2.4. políticas de firewall	28
5. CONSIDERAÇÕES FINAIS.....	29
6. REFERÊNCIAS.....	30

1 INTRODUÇÃO

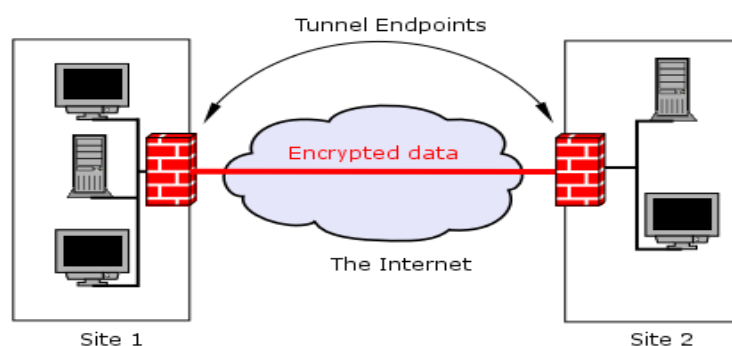
Cada vez mais as instituições, sejam pequenas ou grandes, buscam unificar seus sistemas, mantê-los atualizados em tempo real e principalmente disponibilizar informações dos seus sistemas de informática para todos os seus colaboradores.

A algum tempo uma rede de computadores deixou de ser um escritório que compartilhava recursos de rede, tais como pastas compartilhadas, sistemas, periféricos diversos e passou a necessitar destes recursos em qualquer local e a qualquer momento. Muitos destes recursos ainda ficam disponíveis apenas na Intranet local, devido a poucos recursos de rede, fatores de segurança, alto custo cobrado pelas operadoras para interligar os escritórios remotos ou simplesmente o desconhecimento das novas tecnologias.

Por outro lado, questões de segurança e confidencialidade das informações impossibilitam que máquinas e servidores sejam ligados diretamente à Rede Mundial de Computadores – Internet, sem uma preocupação maior com a segurança da informação.

Empresas como a “Oi” no nosso estado, permitem a ligação entre uma cidade e outra através de sua rede, utilizando por exemplo a tecnologia “Frame-Relay”.

Este trabalho visa mostrar uma alternativa à utilização desta infraestrutura das operadoras, passando a utilizar a infraestrutura da própria Internet, viabilizando a comunicação entre a sede da empresa e sua unidade remota sediada em um local distante.



Veja o exemplo na figura abaixo.

Figura 1:

Fonte: <http://www.rnp.br/newsgen/9811/vpn.html>

1.1 PROBLEMA DE PESQUISA

Atualmente a Federação das Indústrias do Rio Grande do Norte - FIERN , composto pelo Serviço Social da Industria – SESI, Serviço Nacional de Aprendizagem Industrial – SENAI e pelo Instituto Euvaldo Lodi – IEL, possui diversas unidades espalhadas pela capital e interior do Rio Grande do Norte. Algumas destas unidades estão ligadas diretamente ao prédio da Casa da Indústria (CI) como as Unidades do SESI/SENAI-Mossoró, já outras como o SESI-Assú e SESI-Macau, não estão ligadas ao prédio da CI.

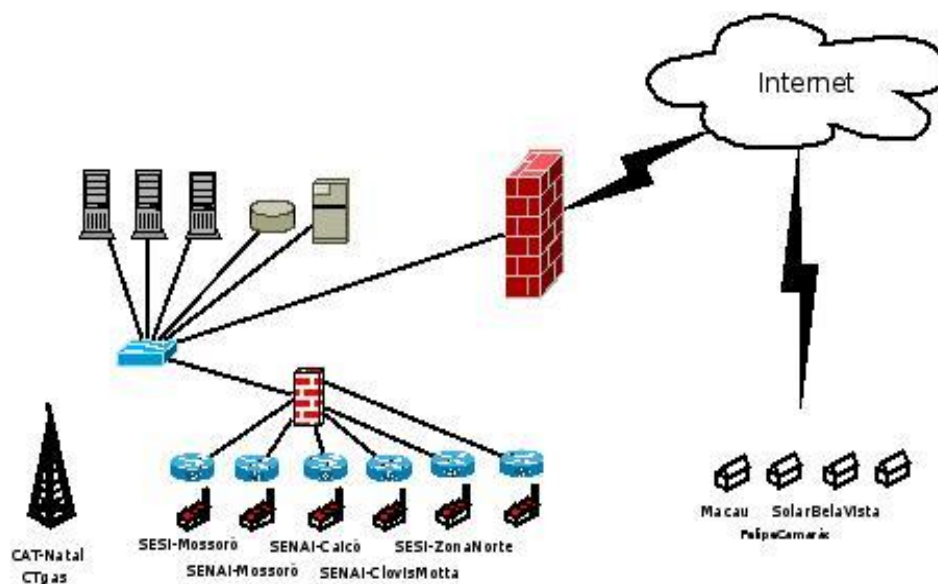


Figura 2 – Situação atual.

Fonte: Do autor (2009)

Estas unidades compartilham, não apenas os sistemas administrativos, mais principalmente o link de Internet.

Neste sentido existem três grandes problemas a serem levantados. Em primeiro lugar o alto custo cobrado pelas empresas prestadoras de serviços de dados na utilização de um link “frame-relay”, a impossibilidade de utilização deste link em alguns municípios do RN e principalmente, a exposição da rede interna a laboratórios de informática disponíveis em algumas escolas do SENAI.

Devemos também citar um possível problema que necessitará de um estudo mais aprofundado, a qualidade do acesso à Internet em algumas cidades do interior do estado.

1.2 OBJETIVOS

1.2.1 Objetivos gerais

Especificar um novo canal de comunicação seguro entre a Casa da Indústria e suas Unidades Operacionais na capital e no interior do estado.

1.2.2 Objetivos específicos

Interligar todas unidades operacionais da FIERN ao prédio central da CI, permitindo assim o uso de todas as ferramentas, disponíveis atualmente apenas aos funcionários lotados na CI e unidades que possuem ligação via “frame-relay”, melhorando a comunicação interna bem como manter os sistemas de informação atualizados em tempo real.

1.3 JUSTIFICATIVA

Minimizar os custos atuais de algumas unidades devido ao elevado preço cobrado pela operadora “Oi” para manutenção do link frame-relay, além de melhorar a capacidade de transmissão de dados destas unidades que atualmente estão limitados à 512K (256 In 256 Out).

Outro aspecto importante é a atualização dos sistemas informatizados que sofrem diversos atrasos devido a inexistência de uma ligação entre todas as Unidades Operacionais, gerando atrasos por exemplo na contabilidade, financeiro, setor pessoal, etc.

Além disso, se faz necessário expor a rede interna para a utilização de alguns sistemas (utilizando técnicas de NAT), o que torna a rede bastante insegura se houver alguma falha no software ou até mesmo no protocolo específico.

2 REFERENCIAL TEÓRICO

2.1 Rede interna (intranet)

Ambiente interno da instituição, nele estão “rodando” os principais serviços da empresa como servidores de aplicações, de autenticação, de compartilhamento de arquivos entre outros.

2.2 O MODELO OSI

Modelo desenvolvido pela ISO (International Standards Organization) como primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas (DAY; ZIMMERMANN, 1983) .

O Modelo OSI, também conhecido como Modelo de referência OSI é um modelo de sete camadas, a transmissão dos dados consiste no encapsulamento dos mesmo e o repasse às camadas inferiores até ultima camada, responsável pela transmissão dos pacotes. Na outra extremidade o processo se repete, completando assim a comunicação.

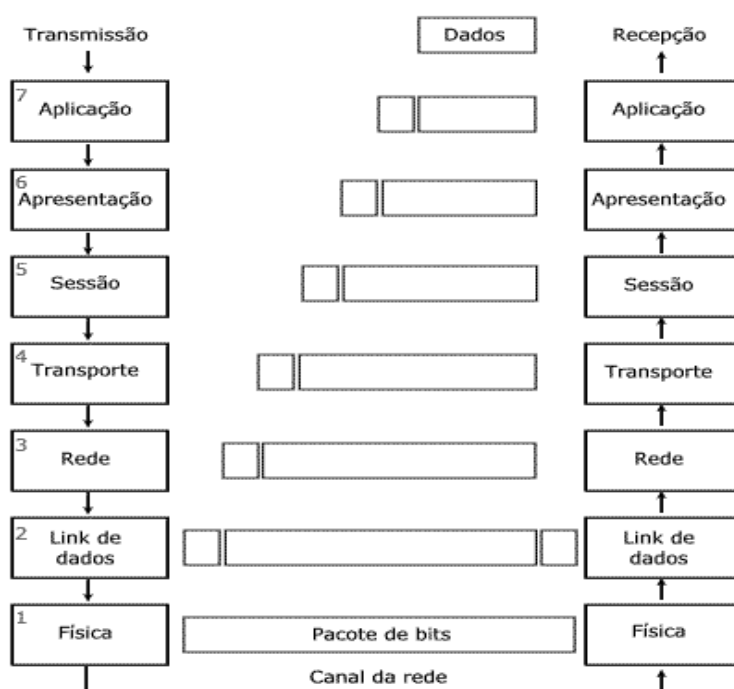


Figura 3: Modelo OSI

Fonte: http://dicitel.blogspot.com/2008_11_01_archive.html

2.3 ADSL

Tecnologia em alta atualmente devido a sua utilização relativamente simples. Pelo fato de utilizar a mesma estrutura física dos telefones, tornou-se muito prático e barato a sua utilização em muitas organizações.

2.4 FRAME-RELAY

Semelhante a uma VPN, porém utiliza a estrutura física da operadora contratada, nesta estrutura são criados circuitos virtuais, agindo como uma linha privada.

“Tipicamente as redes frame-relay são redes públicas, podendo ser alugadas de uma empresa que oferece redes públicas para conectar duas redes de uma organização.” (TORRES, 2001, p.158)

2.5 VIRTUAL PRIVATE NETWORK - VPN

VPNs podem ser criadas utilizando frame-relay e outras tecnologias, porém o mais comum é criar estas redes virtuais diretamente sobre a Internet.

“São redes sobrepostas às redes públicas com a maioria das propriedades das redes privadas.” (TANEMBAUM, 2003, p.123).

O princípio básico consiste na criação de um túnel entre estas redes. Este tunelamento pode ocorrer nas camadas 2 ou 3, respectivamente Enlace e Rede do modelo OSI.

Com o passar do tempo, alguns protocolos se destacaram nesta tarefa, são eles, por ordem de surgimento:

- PPTP – Point to Point Tunneling Protocol;
- L2F – Layer Two Forwarding;
- L2TP – Layer Two Tunneling Protocol;
- IPSec – IP Security Protocol.

Os três primeiros são utilizados para soluções “Client-to-Lan” e trabalham na camada 2 do Modelo OSI, já o IPSec, um protocolo da camada 3, é utilizado em soluções Lan-to-Lan.

2.5.1 PPTP - – Point to Point Tunneling Protocol

O PPTP (Point-to-Point Protocol- Protocolo de Tunelamento Ponto-a-Ponto) é um protocolo da camada dois do TCP/IP, ou camada de enlace. Foi um dos primeiros protocolos de VPN que surgiram e tinha como objetivo facilitar o acesso de computadores remotos a uma rede privada. Baseado nos protocolos de autenticação do PPP como CHAP , MS-CHAP e PAP.

Os elementos que compõem uma conexão por tunelamento PPTP são: o cliente PPTP, o servidor de acesso à rede e o servidor PPTP.

Primeiramente, o protocolo PPTP utiliza o PPP para estabelecer a conexão entre o cliente PPTP e o servidor de acesso à rede (NAS). Os quadros encapsulados pelo cabeçalho PPP ganham um cabeçalho GRE (Generic Routing Encapsulation) para o transporte dos dados. Após, ocorre a criação de uma conexão de controle entre o cliente PPTP e o servidor PPTP, através da utilização do protocolo TCP , por essa conexão são estabelecidos os parâmetros de configuração da conexão entre os extremos do túnel, possibilitando a criação de uma VPN.

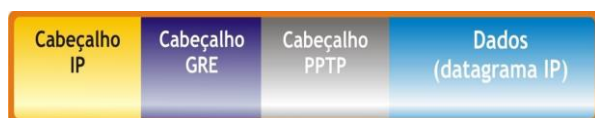


Figura 4: Cabeçalho PPTP
<http://www.guiadohardware.net>

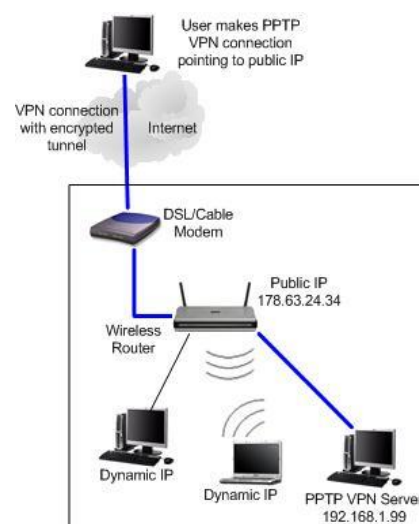


Figura 5: Exemplo PPTP

Fonte: <http://www.guiadohardware.net>

As grandes desvantagens do tunelamento PPTP são a fraca criptografia durante o estabelecimento da conexão e as transmissões de mensagens no canal de controle serem realizadas sem nenhuma autenticação e proteção à integridade.

O PPTP não necessita de uma estrutura de certificados para a autenticação dos seus usuários, é multi-plataforma e pode ser utilizado atrás de um NAT (Network Address Translator,) sem prejuízo a autenticação de usuários.

2.5.2 L2F - Layer Two Forwarding

Desenvolvido pela empresa CISCO, surgiu nos primeiros estágios da tecnologia VPN. Possui tunelamento independente do IP, sendo capaz de trabalhar diretamente com outros meios como ATM e Frame -Relay. Sempre assume que a rede privada estará atrás de um gateway.

O L2F utiliza o PPP para autenticação de usuários remotos mas também pode incluir suporte para autenticação via RADIUS, TACACS e TACACS+.

Existem dois níveis de autenticação de usuário: um no ISP antes de estabelecer o túnel e outro quando se estabelece a conexão com o gateway. Primeiro o usuário estabelece uma conexão PPP com o servidor de acesso a rede (NAS) do ISP, então o NAS estabelece um túnel L2F com o gateway. Finalmente o gateway autentica o nome do usuário e a senha e estabelece a conexão PPP ou Serial Line. A autenticação é feita quando uma sessão VPN-L2F é estabelecida, o cliente, o NAS e o gateway da Internet usam um sistema triplo de autenticação via CHAP.

A grande **desvantagem** do L2F, é não definir criptografia e encapsulamento de dados.

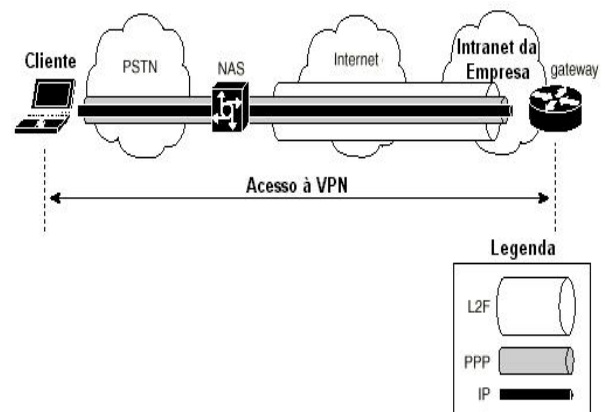


Figura 6: Exemplo L2F

Fonte: <http://www.guiadohardware.net/>

2.5.3 L2TP - Layer Two Tunneling Protocol

Protocolo para Tunelamento na Camada de Enlace, L2TP é uma extensão do PPP, unindo características de outros dois protocolos proprietários: o L2F da Cisco e o PPTP da Microsoft. É um padrão da IETF (Internet Engineering Task Force), que conta com a participação da Cisco e do PPTP fórum, entre outros líderes de mercado.

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

Vantagens oferecidas pelo L2TP:

- a) Transporte de protocolos não IP, como o IPX (Novell) e o SNA;
- b) Mecanismo simples de tunelamento para implementar funcionalidades de LAN e IP de forma transparente, possibilitando serviços de VPN IP de forma bastante simples;
- c) Simplifica a interação entre as redes do cliente e do provedor;
- d) Fácil configuração para o cliente.

Pacotes recebidos na interface Int1 serão redirecionados para R4. As redes R3 e R4 não veem a rede que entre seus roteadores;

O mesmo método é utilizado para interfaces Ethernet: qualquer pacote recebido da LAN1 por R1 na interface E1 será encapsulado pelo L2TP e enviado pelo túnel Tu2 até a interface E2 de R2, ao que será transmitido para a LAN2.



Figura 7: Funcionamento do L2TP

Fonte: <http://www.guiadohardware.net>

O protocolo L2TP pode ser dividido em duas partes: uma responsável por iniciar a conexão e outra responsável pelo tunelamento dos quadros da camada 2.

2.5.4 IPSec - IPSec – IP Security Protocol

IPSec não é o mecanismo de encriptação ou autenticação, mas sim o que vem gerenciar estes. Em poucas palavras, é um conjunto de diversas ferramentas, compondo

um sistema de padrões abertos que visa a garantir uma comunicação segura em redes IP. Baseado em padrões desenvolvidos pela IETF (Internet Engineering Task Force, organização que desenvolve os padrões da Internet), o IPSec busca garantir confidencialidade, integridade e autenticidade nas comunicações de dados em uma rede IP pública.

O IPSec implementa encriptação e autenticação na camada de rede, fornecendo uma solução de segurança fim-a-fim. Pode ser implementado nos roteadores ou no sistema operacional dos terminais, assim os aplicativos não precisam de alterações para poder utilizar comunicações seguras. Como os pacotes encriptados têm o mesmo formato de pacotes IP comuns, eles podem ser roteados sem problemas em qualquer rede IP, e sem qualquer alteração nos equipamentos de rede intermediários. Os únicos dispositivos de rede que precisam ser alterados são os do início e fim das comunicações IPSec, reduzindo assim os custos de implementação e gerenciamento. A figura abaixo mostra onde a encriptação atua nas diferentes camadas.

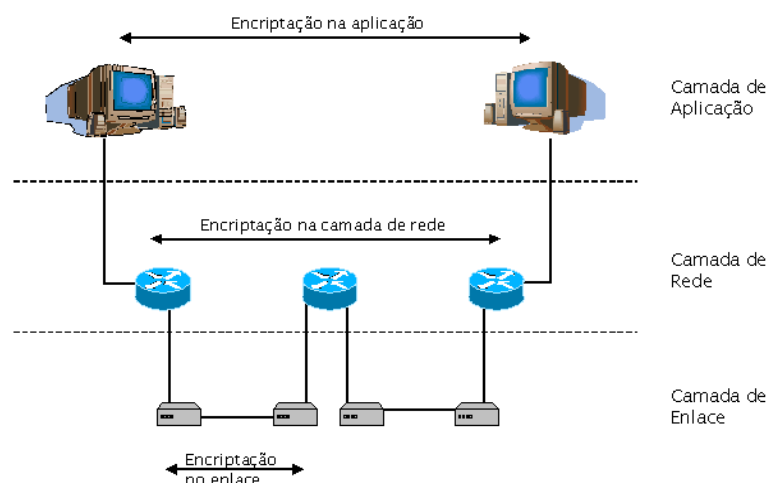


Figura 8: Exemplo IPSec

Fonte: <http://www.guiadohardware.net>

IPSec combina diversas tecnologias diferentes de segurança em um sistema completo que provê confidencialidade, integridade e autenticidade, empregando atualmente:

- mecanismo de troca de chaves de Diffie-Hellman;
- criptografia de chave pública para assinar as trocas de chave de Diffie-Hellman, garantindo assim a identidade das duas partes e evitando ataques do tipo man-in-the-middle (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação);

- algoritmos de encriptação para grandes volumes de dados, como o DES (Data Encryption Standard);
- algoritmos para cálculo de hash (resto de uma divisão, de tamanho fixo) com utilização de chaves, com o HMAC, combinado com os algoritmos de hash tradicionais como o MD5 ou SHA, autenticando os pacotes;
- certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

Na realidade, além das tecnologias mencionadas anteriormente, o IPSec também se refere a diversos outros protocolos visando proteger datagramas IP. Estes padrões são:

- Protocolo de Segurança IP, que define que informações adicionar ao pacote IP para permitir o controle da confidencialidade, autenticidade e integridade, assim como a forma em que os dados devem ser encriptados;
- Internet Key Exchange (IKE), que negocia Associações de Segurança (Security Association, SA) entre duas entidades e realiza a troca de chaves. O uso da IKE não é obrigatório, mas a configuração manual de Associações de Segurança é difícil e trabalhosa, torna-se impossível para comunicações seguras em larga escala.

Pacotes IPSec: É definido um novo conjunto de cabeçalhos a serem adicionados em datagramas IP. Os novos cabeçalhos são colocados após o cabeçalho IP e antes do cabeçalho da camada superior (como o dos protocolos de transporte TCP ou UDP). Estes novos cabeçalhos é que fornecem mecanismos para proteção das informações (payload) do pacote IP:

- Authentication Header (AH): este cabeçalho, ao ser adicionado a um datagrama IP, garante a integridade e autenticidade dos dados, incluindo os campos do cabeçalho original que não são alterados entre a origem e o destino; no entanto, não fornece confidencialidade. É utilizada uma função hash com chave, ao invés de assinatura digital, pois o mecanismo de assinatura digital é bem mais lento e poderia reduzir a capacidade da rede.
- Encapsulating Security Payload (ESP): este cabeçalho protege a confidencialidade, integridade e autenticidade da informação. Se o ESP for usado para validar a integridade, ele não inclui os campos invariantes do cabeçalho IP.

AH e ESP podem ser usados separadamente ou em conjunto, mas para a maioria das aplicações apenas um deles é suficiente. Para os dois cabçalhos, o IPSec não especifica quais algoritmos de segurança devem ser utilizados, mas dá uma relação dos possíveis algoritmos, todos padronizados e bastante difundidos. Inicialmente, quase todas as implementações

trabalham com MD5 (da RSA Data Security) e o Secure Hash Algorithm (SHA, do governo dos EUA) para integridade e autenticação. O DES é o algoritmo mais comumente usado para a encriptação dos dados, apesar de muitos outros estarem disponíveis, de acordo com as RFCs, como o IDEA, Blowfish e o RC4.



Figura 9: Cabeçalho Original / IPSec

Fonte: <http://www.guiadohardware.net>

2.6 SOFTWARE LIVRE

A Free Software Foundation (FSF, Fundação para o Software Livre) é uma organização sem fins lucrativos, fundada em 1985 por Richard Stallman e que se dedica à eliminação de restrições sobre a cópia, redistribuição, entendimento e modificação de programas de computadores – bandeiras do movimento do software livre, em essência. Faz isso promovendo o desenvolvimento e o uso de software livre em todas as áreas da computação mas, particularmente, ajudando a desenvolver o sistema operacional GNU e suas ferramentas.

Disponível: http://pt.wikipedia.org/wiki/Free_Software_Foundation .
Acesso em 05 Ago 2009.

A FSF considera um software livre quando atende os usuários destas quatro formas:

- A liberdade para executar o programa, para qualquer propósito (liberdade nº 0);
- A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades (liberdade nº 1). Acesso ao código-fonte é um pré-requisito para esta liberdade;
- A liberdade de redistribuir, inclusive vender, cópias de modo que você possa ajudar ao seu próximo (liberdade nº 2);
- A liberdade de modificar o programa, e liberar estas modificações, de modo que toda a comunidade se beneficie (liberdade nº 3). Acesso ao código-fonte é um pré-requisito para esta liberdade;

2.7 FIREWALL NETFILTER/IPTABLES

O sistema de processamento de pacotes do kernel GNU/LINUX é denominado “*netfilter*”, o *iptables* é o comando para sua utilização. É um código de firewall das versões 2.4 do kernel, que substituiu o *ipchains* (presente nas séries 2.2 do kernel). Foi incluído à partir da série 2.4 em 1999.

O *iptables* opera na camada 3 do Modelo OSI, abaixo algumas de suas principais características:

- Especificação de portas/endereço de origem/destino ;
- Suporte a protocolos TCP/UDP/ICMP ;
- Suporte a interfaces de origem/destino de pacotes ;
- Permite um número ilimitado de regras por chain ;
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados;
- Suporte a módulos externos para expansão das funcionalidades padrões oferecidos pelo código de firewall;
- Suporte completo a roteamento de pacotes, tratadas em uma área diferente de tráfegos padrões;
- Permite especificar exceções para as regras ou parte das regras;
- Permite enviar alertas personalizados ao syslog sobre o tráfego aceito/bloqueado;
- Redirecionamento de portas e masquerading;
- Suporte a SNAT e DNAT (modificação do endereço de origem/destino das máquinas para um único IP ou fixa de IP's);
- Contagem de pacotes que atravessaram uma interface/regra ;
- Limitação de passagem de pacotes/conferência de regra (muito útil para criar proteções contra, syn flood, ping flood, DoS, etc).

2.8 NETWORK ADDRESS TRANSLATION - NAT

Em redes de computadores, NAT, também conhecido como masquerading é uma modificação de endereços e/ou portas de pacotes que percorrem a rede. A técnica consiste em rescrever os endereços IP de um pacote que passa por um roteador ou firewall “mascarando

este IP/porta. O SNAT (tradução de endereço de origem) e o DNAT (tradução de endereço de destino) são exemplos desta técnica.

3 METODOLOGIA

As ferramentas utilizadas para interligar estas redes serão todas livres, dos servidores aos softwares. Por ser uma distribuição bastante robusta, a escolhida foi a Debian. O software que gerenciará será o OpenVpn, um dos mais populares e seguros quando o assunto é VPN.

Estes servidores serão responsáveis, não apenas pela ligação “entre-redes”, mas principalmente pelo Firewall e outras ferramentas necessárias ao funcionamento seguro e eficaz da VPN.

Inicialmente será feito um levantamento dos custos atuais, das condições dos links de Internet na capital e principalmente no interior do estado. Em seguida os primeiros testes nas unidades menores e que não possuem qualquer ligação com a CI.

O passo seguinte será a instalação nas unidades maiores, como o SENAI-Mossoró, afim de averiguarmos a capacidade e principalmente a estabilidade da VPN, por fim a instalação em todas as demais unidades.

4 DESENVOLVIMENTO

4.1 LEVANTAMENTO DOS CUSTOS

4.1.1 CUSTOS ATUAIS

Atualmente a FIERN tem um custo mensal com a interligação de suas unidades estimado em R\$ 10.000,000 (dez mil reais). Alguns links como o do SENAI Santa Cruz, com custo mensal de aproximadamente R\$ 800,00 (oitocentos reais), possui um link de 256K com apenas 128K garantido. Este link está disponível para toda a Unidade, atualmente com 15 funcionários mais um laboratório de informática com 16 computadores.

Além disso, nem todas as Unidades estão interligadas ao prédio da Casa da Indústria, a Unidade do Sesi-Assú e do Sesi-Solar Bela Vista, sequer possuem esta interligação.

Abaixo, quadro demonstrativo das unidades existentes com custos e velocidades dos links, além das outras que sequer possuem esta interligação.

Unidade	Interligado à CI	Velocidade (Kbps) / CID(Kbps)	Valor
SESI Zona Norte	SIM	256/128	1.200,00
SESI CAT-Natal	SIM	Via Link Rádio CTGás	0,00
SESI Solar Bela Vista	NÃO	---	0,00
SENAI Clóvis Motta	SIM	256/128	1.200,00
SENAI Construção Civil	NÃO	----	0,00
SENAI Sta Cruz	SIM	256/128	1.300,00
SENAI Caicó	SIM	256/128	1.400,00
SESI Mossoró	SIM	512/256	1.600,00
SENAI Mossoró	SIM	512/256	1.600,00
IEL Mossoró	NÃO	---	
SESI Assú	NÃO	---	
SESI Macau	NÃO	---	
Ligação Unidades x CI		2048/2048	2.800,00
TOTAL			11.100,00

CID = Velocidade mínima garantida pela “Oi”.

Quadro 1: Custos atuais

Fonte: Do autor, 2009.

4.1.2 Custos ADSL

Atualmente nem todas as localidades que a FIERN está presente dispõem de infraestrutura ADSL de empresas oficiais, nestas unidades será necessário um estudo maior sobre a viabilidade de interligar todos os sistemas internos disponíveis na CI, a princípio, apenas os sistemas mais “leves” seriam disponibilizados através da VPN. De qualquer maneira, a estrutura já estaria montada e quando fosse possível um link aceitável (mínimo 1G) outros sistemas ficariam disponíveis, no primeiro momento, apenas os sistemas específicos de cada unidade seriam disponibilizados, a saber:

- SESI: Sistemas de Saúde / Lazer (Cliente x Servidor);
- SENAI: Sistemas da Escola (Cliente x Servidor);
- IEL: Sistema de acompanhamento ao estágio (Sistema Web).

Unidade	Velocidade ADSL Velox (Kbps)	Valor
SESI Zona Norte	1024	189,00
SESI CAT-Natal	Via Link Rádio CTGás	0,00
SESI Solar Bela Vista	1024	189,00
SENAI Clóvis Motta	1024	189,00
SENAI Construção Civil	600	120,00
SENAI Sta Cruz	1024	189,00
SENAI Caicó	1024	189,00
SESI Mossoró	1024	189,00
SENAI Mossoró	1024	189,00
IEL Mossoró	1024	189,00
SESI Assú	600	189,00
SESI Macau	600	189,00
		2.010,00

Quadro 2: Custos ADSL.

Fonte: Do autor, 2009.

4.2 INSTALAÇÃO E CONFIGURAÇÃO DA VPN

Neste ponto iniciamos a configuração da VPN tanto na matriz como na filial. A segurança ficará a cargo da troca de chaves estáticas, pois contempla uma abordagem segura e

rápida. A rede interna possui autenticação própria, existe um firewall entre as duas redes gerenciando o tráfego no túnel VPN, não sendo necessário nenhuma outra medida adicional de segurança, visando principalmente a agilidade da troca de informações entre redes.

4.2.1 Instalação dos pacotes

- `aptitude install openvpn openvpn-blacklist openssl`

4.2.2 Geração de chaves estáticas

Esta chave será a responsável por manter a conexão segura, possui 2048 bits e deverá ser copiada para `/etc/openvpn/chaves/“unidade”.key` na matriz e `/etc/openvpn/chaves/“filial”.key` na filial remota.

- `openvpn --genkey --secret /etc/openvpn/chaves/“unidade”.key`

Como medida de segurança adicional, mudaremos suas permissões através do comando `chmod`, permitindo assim que apenas o super usuário tenha acesso a chave.

- `chmod 600 /etc/openvpn/chaves/“unidade”.key`

Exemplo de arquivo de chave:

```
-----BEGIN OpenVPN Static key-----
b7a8b51a2bddc57d662f5986a2b6a961
5baafcc3a39988d3cb6dd80baf1295c0
ae2bbe8b35f8022396fe25443831e61d
c36180f76fdre2334e9b7967fa1282b9b
ca25415a340802d834b912fd535f96a7
8ec47843c12wsah4c90188a90305d405
avg559044ae858a8e1a442923ef7b944b
```

```
b9a353f3cbd8f08ab819894b264d2e94
3618dafe4d5d2c0943ed781511ab41ad
983098160b757f384101e7136dbb7564
347278a8ac83d2a3c723a0f343d6758d
181710e43e7d39e1c4be3770695b5470
dbff1c35361092a56b66fa917cd908d6
898f7c8663ca54422432ce4e0678e626
466d96598c4bd92420ad2294e61de3b0
0abf0c696d6d5779835e6fd4386av1139
-----END OpenVPN Static key V1-----
```

Quadro 3: Chave 2048 bits
Fonte: Do autor, 2009.

4.2.3 Arquivos de configuração

Matriz Casa da Indústria.

Arquivo: /etc/openvpn/"unidade".conf

```
# cria túnel
dev tun0
# definir IPs "local -> remoto"
ifconfig 172.16.1.1 172.16.1.2
# definir chave a utilizar
secret /etc/openvpn/chaves/"unidade".key
# criar rotas (Rota para a Unidade Remota – Rede + Máscara)
route 192.5.5.0 255.255.255.0
# criar logs
#verb 1 => # verb [1..11] maior numero, maiores informações logadas
verb 3
log-append /var/log/openvpn/"unidade".log
```

```
# tamanho do pacote (mtu) = 1500 = tamanho do ethernet - necessário ao windows
tun-mtu 1500

# tamanho extra aos mtu 1500 (necessário ao windows)
tun-mtu-extra 32

# necessário ao windows - pacote 1450
mssfix 1450

# habilitar compactação de dados
comp-lzo
```

Quadro 4: Arquivo de configuração matriz.

Fonte: Do autor, 2009.

Filial remota.

Arquivo: /etc/openvpn/"matriz".conf

```
# cria tunel
dev tun0

# define endereço servidor – Matriz
remote 200.164.229.147

# definir IPs "local -> remoto"
ifconfig 172.16.1.2 172.16.1.1

# definir chave a utilizar
secret /etc/openvpn/chaves/"matriz".key

# criar rotas (Rotas para a Matriz – Rede + máscara)
route 10.134.24.0 255.255.252.0

# criar logs
log-append /var/log/openvpn/fiern.log

# tamanho do pacote (mtu) = 1500 = tamanho do ethernet - necessário ao windows
tun-mtu 1500
```

```
# tamanho extra aos mtu 1500 (necessário ao windows)
tun-mtu-extra 32
# necessário ao windows - pacote 1450
mssfix 1450
# habilitar compactação de dados
comp-lzo
```

Quadro 5: Arquivo de configuração filial..

Fonte: Do autor, 2009.

4.2.4 Políticas de firewall

De forma didática criamos regras liberando TODO o tráfego dentro do túnel VPN, o ideal é liberar apenas para os IPs e portas específicas.

Outra observação importante é que, para cada VPN criada, deveremos utilizar um túnel e uma porta diferentes, além dos IPs ponto-a-ponto.

Matriz

```
eth0 # interface externa no firewall
porta 1194 # udp = porta padrão OpenVpn

# Destinando pacotes ao firewall
iptables -t nat -A PREROUTING -d 200.164.229.147 -p udp --dport 1194 -i eth0 -j DNAT
--to 10.134.25.254

# Liberando roteamento dentro do túnel
iptables -A INPUT -p udp --dport 1194 -i eth0 -j ACCEPT
iptables -A FORWARD -i tun0 -j ACCEPT
iptables -A FORWARD -o tun0 -j ACCEPT
iptables -A INPUT -i tun0 -j ACCEPT
iptables -A OUTPUT -o tun0 -j ACCEPT
```

Filial

```
iptables -A INPUT -p udp --dport 1194 -i eth0 -j ACCEPT
iptables -A FORWARD -i tun0 -j ACCEPT
iptables -A FORWARD -o tun0 -j ACCEPT
iptables -A INPUT -i tun0 -j ACCEPT
iptables -A OUTPUT -o tun0 -j ACCEPT
```

5 CONSIDERAÇÕES FINAIS

Importante ressaltar que o impacto financeiro na aquisição de um bem ou serviço para a empresa, é um dos pontos a serem observados, senão o primeiro, pois na conjuntura econômica atual as instituições se veem “forçadas” a sempre monitorar e diminuir seus gastos. Desta forma, os gastos expostos anteriormente a cerca da substituição da nova estrutura aqui proposta, estão relacionados especificadamente com os custos diretos.

O custo atual estimado em manter os links Frame-Relay gira em torno de R\$ 11.100,00 de mensalidades pagos à prestadora “Oi”, além destes, existe o custo dos equipamentos adicionais (por Unidade Operacional) tais como, roteadores (R\$ 1.500,00), *no-breaks* (R\$ 500,00) e salas com ar-condicionado ligadas 24h por dia.

Comparativamente com a nova estrutura proposta, este custo cai substancialmente: R\$ 2.000,00 de mensalidades dos links ADSL para TODAS as Unidades Operacionais, R\$ 500,00 preço médio de um computador *Pentium IV* que será o responsável pelo roteamento entre-redes, já disponível para todas as UO. Além da redução dos custos, estas máquinas funcionarão, não apenas como “túneis” VPN, mas principalmente, provendo segurança através de um *Proxy/Firewall*, limitando todo o acesso à Internet/VPN.

Portanto, o impacto na redução dos custos diretos em tempos de crise, da procura por alavancagem financeira e da redução dos gastos cada vez mais procurados pelas empresas, já é por si só uma questão que deve ser considerada em uma tomada de decisão para a mudança na estrutura atual, visando o custo-benefício sem deixar de focar as questões importantes como segurança, eficiência e eficácia.

Com a implantação da VPN existirá não apenas a redução dos valores financeiros, mas principalmente, o ganho na velocidade, na disponibilidade da informação, na agilidade dos processos, proporcionando uma maior qualidade de trabalho para todos os colaboradores do Sistema FIERN.

Além disso, será possível liberar acesso à rede interna para Diretores e Gerentes durante suas viagens à trabalho, permitindo que os mesmos resolvam suas pendências remotamente, novamente tornando o processo mais ágil e rápido, impactando nos chamados custos indiretos.

REFERÊNCIAS

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

DIÓGENES, Y. **Certificação Cisco CCNA 4.0**, 3. ed. Rio de Janeiro: Axcel Books, 2004

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

PURDY, G. N. **Linux Iptables, Guia de Bolso**, 1. ed. Rio de Janeiro: Altabooks, 2005

RIBEIRO, U. **Certificação Linux**, 1. ed. Rio de Janeiro: Axcel Books, 2004

RICCI, B. **Rede Segura: VPN Linux**, 1. ed. Rio de Janeiro: Ciência Moderna, 2007

MARCELO, A. **Open VPN**, 1. ed. Rio de Janeiro: Brasport, 2007

da SILVA, L. S. **Virtual Private Network – VPN**. 1. ed. São Paulo: Novatec, 2002

WIKIPEDIA, Disponível em <<http://www.wikipedia.org>>. Acesso em: 28 Jul. 2009.

OPENVPN, Disponível em <<http://www.openvpn.net>>. Acesso em: 28 Jul. 2009.

REDE NACIONAL DE PESQUISA, Disponível em <<http://www.rnp.br/newsgen/9811/vpn.html>>. Acesso em: 2 Ago. 2009.

IETF, Disponível em <<http://www.ietf.org/>> Acesso em: 2 de Ago. 2009.

NETFILTER, Disponível em <<http://www.netfilter.org/>> Acesso: em 22 de Out. 2009.

VOL, Disponível em <<http://www.vivaolinux.com.br/>> Acesso: em 22 de Out. 2009.