METODOLOGIA DE PROJETO E IMPLEMENTAÇÃO DE REDE VPN (VIRTUAL PRIVATE NETWORK) SOBRE A INTERNET VOLTADA A INTEGRAÇÃO DAS INSTITUIÇÕES DE ENSINO SUPERIOR (IES)

Raimundo Viégas Junior[1], Luiz Affonso H. G. de Oliveira[2]

Resumo *— Este trabalho apresenta uma metodologia de projeto para Rede Privada Virtual (VPN) com o objetivo de estender a Intranet da UFPA (Universidade Federal do Pará) até os campis do interior e/ou a casa dos docentes e administradores, utilizando os serviços públicos da Internet. Nessa solução os dados trafegam através de túneis criptografados entre os diversos pontos da rede. Esta solução permitiu uma grande redução de custos com o aluguel de links privados de comunicação de dados. A metodologia, que pode ser reutilizada em outras instituições, sistematiza as etapas da implantação da VPN, em um conjunto de passos; baseada em informações estratégicas, administrativas e técnicas, garantindo a qualidade do projeto e minimizando os riscos de segurança.*

Índice de Termos – Metodologia de Projeto, Rede Privada Virtual, VPN.

INTRODUÇÃO

O grande desenvolvimento tecnológico experimentado nas áreas da informática e das telecomunicações tem ampliado de forma sem precedentes a quantidade de informações disponibilizadas ao pessoal das instituições de ensino. O sistema decisório em todos os níveis da administração é enriquecido na medida em que pessoas, executando tarefas em diferentes setores dessas instituições, podem acessar os mesmos dados de forma compartilhada, integrando as ações e aumentando a confiabilidade das informações geradas. Uma forma de acessar dados e sistemas de qualquer local e a qualquer hora é utilizando serviços que operam sobre a Internet. Em decorrência disto, o desenvolvimento de uma metodologia de projeto e implementação de VPN sobre a Internet, necessariamente contribui para uma maior flexibilidade e disponibilidade dos serviços on-line providos pelas IES aos seus usuários de intranet e ao seu público de internet. A vantagem de uma VPN é possibilidade de reutilização sobre a *Web*, de sistemas cliente-servidor originalmente desenvolvidos para ambientes de intranet. Além da reutilização de software uma VPN contribui para redução de custos com comunicações, pois possibilita a execução de sistemas que exigem links dedicados sobre a infra-estrutura pública da Internet [5].

CARACTERÍSTICAS DE VPNS

Rede Privada Virtual ou VPN (*Virtual Private Network*) é a implementação segura de uma rede de longa distância, utilizando a infra-estrutura existente privada ou pública, para trafegar dados através de um túnel de criptografia entre todos os pontos autorizados da rede [6]. Os dados são criptografados de tal maneira que usuários autorizados conseguem ter acesso às informações na sua forma original. Para que as VPNs possam usar o *backbone* da Internet é vital que elas sejam compatíveis com o protocolo Internet (IP), utilizando endereços IP oficiais [3].

Apesar da redução de custos com comunicação e simplificação da administração da rede é preciso muita atenção com a segurança quando se constrói uma rede VPN sobre a Internet. Na VPN os sistemas da instituição não estão mais restritos a um link dedicado privado, em vez disso, os dados e sistemas trafegam a maior parte do tempo numa rede pública, sujeita a ataques. Por este motivo, o uso da criptografia nas VPNs é fundamental. O tema segurança é a primeira preocupação no projeto de uma VPN. Acostumadas com a privacidade garantida pelas redes proprietárias, muitas IES podem considerar a Internet bastante aberta para a criação de uma rede privada. Mas tomando-se as devidas precauções, a Internet pública pode ser tornar tão privada como a rede de telefonia comutada.

A disponibilidade é um fator que abrange o tempo de funcionamento da rede e seu desempenho. Existem redes privadas que asseguram determinados níveis de serviço quanto a esse parâmetro. Diferente destas redes privadas, a Internet atualmente não possui tal garantia de serviços. A expansão da Internet ocorre de forma desenfreada e descontrolada sem o benefício de uma organização que supervisiona o seu crescimento. Por outro lado, a Internet possui redundância e elasticidade muito mais robustas do que uma típica rede privada [7]. Esta robustez permite evitar catástrofes em larga escala, deixando os problemas de serviços isolados em suas localidades de origem. Portanto, é razoável dizer que a Internet oferece confiabilidade suficiente para a grande maioria de aplicações educacionais, em termos de disponibilidade.

PROTOCOLOS DE SUPORTE A VPNS

Os protocolos de tunelamento são responsáveis pela abertura e gerenciamento de sessões de túneis em VPNs [4]. Estes protocolos definidos pelo modelo *OSI/ISO (Open Systems*

[1] Raimundo Viégas Junior, Universidade Federal do Pará, Campus Guamá, Rua Augusto Correa 01, 66075-110, Belém, PA, Brasil, rviegas@ufpa.br
[2] Luiz Affonso H. G. de Oliveira, Universidade Federal do Rio Grande do Norte, Campus Lagoa Nova, 59072-970, Natal, RN, Brasil, affonso@dca.ufrn.br

Interconnection / International Standards Organization) [1] são divididos em dois grupos:

- Protocolos de camada de enlace PPP (*Point to Point Protocol*) sobre IP (*Internet Protocol*): transportam informações da Camada de rede, utilizando quadros como unidade de troca; os pacotes são "encapsulados" em quadros PPP [7] [8] [9];
- Protocolos de rede (IP sobre IP): "encapsulam" pacotes IP com cabeçalhos deste mesmo protocolo antes de enviá-los [10].

O túnel VPN utilizado na Camada dois (Enlace) é similar a uma sessão, onde as duas extremidades negociam a configuração dos parâmetros para estabelecimento do endereçamento, criptografia e parâmetros de compressão do túnel [6]. A gerência é realizada através de protocolos específicos de manutenção do túnel. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de Camada três (Rede) é análoga, porém não existe a fase de manutenção do túnel [5]. Para as técnicas de tunelamento VPN sobre Internet atualmente em uso, quatro protocolos se destacaram, em ordem de surgimento:

- PPTP - *Point to Point Tunneling Protocol* [7];
- L2F - *Layer 2 Forwarding* [8];
- L2TP - *Layer 2 Tunneling Protocol* [9] e
- IPSec - *IP Security Protocol* [10].

Cada protocolo tem suas vantagens e desvantagem, mas sempre quando possível utilizaremos padrões abertos recomendados pelo *Internet Engineering Task Force* (IETF).

VISÃO GERAL DA METODOLOGIA

A metodologia proposta para o projeto e implementação de VPN, utilizando a Internet, é baseada em três etapas [12]:

- 1° Etapa – Levantamento das Informações da IES
- 2° Etapa – Projeto lógico da VPN
- 3° Etapa – Modelo de Implementação da VPN

1ª ETAPA DA METODOLOGIA

Levantamento das Informações da IES: Nesta etapa faz-se o levantamento das macros informações, incluindo-se as atuais características da rede de computadores, desde análise do projeto físico (elementos ativos e passivos) e lógico (topologia, sistema operacional e serviços de rede) que compõem o ambiente de informática da instituição, até a necessidade de comunicação. Nesta fase objetiva-se a integração do ambiente educacional, pois isto é de fundamental importância para o sucesso da implantação do projeto.

Objetivo principal da implantação do projeto: Levantar com os grupos de usuários o que a instituição espera com a nova rede de comunicações, como será utilizada e como aumentará a produtividade. Por exemplo: reduzir custos com telecomunicações, oferecer acesso remoto aos professores e administradores a aplicações e dados pertencente a IES.

Integração Institucional: Levantar a necessidade de integração dos campis à sede da instituição, levando-se em conta as linhas de pesquisa desenvolvidas, que podem ter desde atuação, nacional ou internacional. Neste quesito é importante também levantar os maiores parceiros da instituição, e se estes necessitam integrar-se à rede da IES.

Estrutura Administrativa: Neste quesito o projetista deve obter informações e entender como funciona a estrutura operacional levantando como está organizada a instituição, tais como, Departamentos, Centros de Pesquisa, Pró-Reitorias e como a integração da rede educacional vai impactar na tomada de decisões dos administradores.

Grupos de Usuários: Identificar os maiores grupos de usuários da rede institucional e quais suas atuais e futuras necessidade de comunicação (serviços de rede) verificando também a possibilidade de implantação de uma Intranet caso ainda não exista com a finalidade de aumentar a produtividade dos professores e técnicos da IES.

Grupo Gestor: Identificar os responsáveis na IES pelo projeto de VPN, verificando a quem compete aceitar ou rejeitar o modelo de implantação proposto. Discutindo com os administradores responsáveis de como o projeto deve integrar a instituição e quais os seus impactos globais, desde adoção de políticas de segurança a treinamento dos usuários para a utilização dos novos serviços disponíveis.

Topologia Física: Levantar qual é a topologia física e lógica adotada na rede da IES. Geralmente a topologia física é do tipo estrela, apesar de ainda existirem IES operando com topologia do tipo barramento ou anel.

Infra-estrutura Elétrica: Levantar como está implementada a infra-estrutura de distribuição de energia elétrica para os computadores. Analisando-se também a existência de um sistema de fornecimento emergencial de energia, tais como: geradores e no-breaks departamentais ou individuais.

Infra-estrutura Lógica: Levantar como está implementada a infra-estrutura física de cabeamento lógico da rede. Basicamente há dois modelos de cabeamento lógico existente. O estruturado; caracteriza-se pela utilização de um tipo de cabo lógico (categoria 5 ou superiores) para tráfego de voz (telefônico) e dados. O não-estruturado permite apenas o tráfego de dados, pois existe um cabeamento telefônico especifico para voz [11]. Identificar também quais os elementos ativos que compõem a rede, que podem ser: *hubs*, *switches* e roteadores e como estão interconectados, se via cabo ou ondas de rádio, analisando se estes elementos ativos estão com a capacidade satisfatória para suportar os serviços de redes atuais.

Esquema Físico da Rede: Levantar a existência de um mapa da rede, que inclui a localização dos segmentos e

dispositivos de conexão, descrevendo todas as características físicas das instalações e equipamentos que compõem a rede, tais como, tecnologia utilizada nos enlace, provedor de serviços de telecomunicações, localização dos hubs, switches, roteadores, servidores, mainframes e estações de gerência da rede.

Topologia Lógica: Verificar qual a topologia lógica da rede adotada se barramento ou anel, pois ela indica os segmentos de rede na Camada dois e três do modelo *OSI/ISO*, pontos de interconexão e qual o alcance da rede [1].

Protocolo e Endereçamento da Rede: Levantar qual é o protocolo de rede e qual a classe de endereçamento utilizada, preferencialmente o protocolo TCP/IP, pois este indica a atribuição de endereços de camada de rede e de recursos disponíveis [1].

Sistema Operacional de Rede e Estações de Trabalho: Levantar qual o sistema operacional utilizado nos servidores e estações de trabalho, pois não obrigatoriamente há uma hegemonia no uso de um único programa, visto que há necessidades especificas que cada *software* se propõe a suprir em determinados setores da IES.

Serviços de Rede: Levantar quais são os serviços de redes atualmente disponíveis aos usuários Institucionais, tais como, correio eletrônico, comando remoto, transferência de arquivos e acesso a Internet ou a Intranet da instituição.

Gerência de Redes: Levantar qual a estratégia de gerenciamento utilizada na rede institucional, que pode ser classificada em centralizada ou distribuída, e se esta estratégia utiliza algum tipo de protocolo específico tal como o SNMP (*Single Network Manangement Protocol*) [2] para o gerenciamento da rede da instituição.

Segurança de Redes: Levantar se existe algum sistema de segurança de dados implantado na Instituição que necessite de políticas específicas que deverão ser implantadas no uso da VPN Institucional.

2ª ETAPA DA METODOLOGIA

Projeto Lógico da VPN: De posse de todas as informações levantadas na etapa anterior defini-se qual a topologia a ser adotada pela solução VPN e os requisitos de projeto, bem como a configuração lógica da rede e as facilidades de gerência, desempenho e segurança. Os módulos nesta etapa são tratados de forma independente e podem ser desenvolvidos simultaneamente no projeto, de modo a suportar e atender as necessidades levantadas.

Abrangência do Projeto VPN

Na rede da instituição, alguns princípios como privacidade, integridade dos dados, autenticidade e confidencialidade devem ser consideradas e cautelosamente implementadas. A VPN pode ser implantada com relação à abrangência de três formas distintas, são elas; Intranet, Extranet e VPN interna [5]. A seguir descrevem-se estas três formas.

Intranet: a VPN em uma Intranet pode ser criada entre a sede da organização e um campi remoto. Deste modo, ela só é usada dentro da rede da organização e é acessada apenas por usuários autenticados tais como; administradores, técnicos e professores, que podem utilizar conexões dedicadas do tipo LAN (*Local Area Network*) para LAN ou discadas do tipo Cliente para LAN [6].

Extranet: Uma VPN em uma Extranet pode ser criada entre uma organização educacional e seus parceiros ou provedores. A Extranet permitirá o acesso a VPN usando o protocolo HTTP (*Hipertext Transfer Protocol*) ou utilizando algum outro serviço e protocolo ajustado pelos usuários envolvidos [2]. Este processo é muito utilizado hoje em dia nas aplicações comerciais.

VPN Interna: Uma VPN interna pode e deve ser usada para dar maior segurança para a organização, na comunicação das estações com os servidores [6], prevenindo-se de possíveis ataques de usuários mal intencionados. Toda comunicação interna que venha a ser considerada crítica em termo de segurança pode trafegar por um túnel VPN na rede da instituição.

Topologias de VPN

Há muitos tipos de topologias de VPN que poderão se adequar às necessidades da instituição ou se adaptar a uma configuração de rede já existente. Estas topologias podem ser definidas basicamente como: Cliente para LAN e LAN para LAN.

Cliente para LAN: A arquitetura de VPN baseada em cliente para LAN surge quando um usuário remoto que pode ser um administrador, professor ou técnico tenta estabelecer uma conexão com sua instituição. Isto implica na criação de um túnel com o servidor interno. Este túnel poderá vir da Internet ou de uma linha discada. Para que se consiga a comunicação com o servidor interno é necessário primeiro passar pelo servidor de acesso, que poderá ser um: roteador, *firewall*, *blackbox,* ou servidores de autenticação *stand–alone* que lhe garantirá o acesso requisitado, sendo que o cliente opcionalmente pode ter também instalado um software de criptografia compatível com o do*firewall* [3].

VPN LAN para LAN: Este tipo de topologia VPN é utilizado quando é necessário interligar redes locais (LAN) separadas geograficamente [5]. As Lans poderão estar operando em diferentes plataformas como, por exemplo, um *firewall* utilizando o sistema operacional GNU/Linux de um lado e um *firewall* Windows NT, do outro. Eles estarão

rodando *software* de VPN diferentes, mas têm que estar usando o mesmo protocolo de tunelamento, algoritmo de criptografia e estarem configurados para detectar automaticamente quando houver algum tipo de tráfego para a rede VPN.

Arquitetura VPN

Existem muitos tipos de arquiteturas de VPN que poderão se adequar às necessidades da instituição, abaixo são descritos as principais:

VPN Baseada em *Firewall*: VPN baseada em *firewall* é a forma mais comum de implementar uma VPN, geralmente as soluções comerciais de implementação de VPN se baseiam nesta modalidade [3]. As instituições, pelo simples fato de já possuírem um *firewall*, optam por esta implementação, decidindo apenas qual protocolo de tunelamento utilizar (L2F, PPTP, L2TP e IPSec). Um caso particular típico é o *firewall* VPN com NAT (*Network Adrress Translation*), que se baseia no processo de mudar o endereço IP da organização para um endereço IP público [6].

VPN Baseada em Dispositivos *Black-Box*: Consiste em um dispositivo contendo software de criptografia e hardware integrado para criar um túnel VPN. Este normalmente está localizado atrás de um *firewall* [5]. Quando o pacote chega no *firewall* ele é examinado, ou seja, o *firewall* verifica se este pacote tem permissão para entrar ou não na rede, pois o *firewall* contém uma série de regras e políticas de segurança implementadas de acordo com os critérios definidos pelo administrador da rede da IES. Acontece que os pacotes vindos de um túnel VPN estão criptografados, tornando o *firewall* incapaz de examiná-lo. É neste ponto que deverá existir alguma regra implementada para que estes pacotes que estão criptografados sejam passados para o dispositivo VPN, que só assim poderá autenticá-los, descriptografá-los e enviá-los para seu destino.

VPN Baseada em Roteadores: Os roteadores devem examinar e processar cada pacote que deixa a LAN, por isto, este tipo de VPN possui um custo relativamente alto devido ao investimento em roteadores. Atualmente existem dois tipos de VPN baseadas em roteadores. O primeiro se baseia em um *software* que é adicionado ao roteador para garantir que o processo de criptografia ocorra. O segundo consiste em um dispositivo que é inserido no roteador permitindo um maior número de rotas ou ainda a implementação de um algoritmo de criptografia [4].

Softwares de VPN: São programas instalados em estações de trabalho que disponibilizam a criação e administração de túneis, tanto entre um par de *gateways* de segurança quanto entre um cliente remoto para o *gateway* de segurança [5]. Estes softwares de sistemas VPN são em geral, uma boa escolha de baixo custo para sistemas relativamente pequenos e que não exijam um processamento de tráfego intenso.

Gerenciamento, Desempenho e Segurança em VPNs

Há três componentes principais quanto à segurança de uma VPN baseada na Internet: provedor Internet, *gateways* VPN e servidores de segurança [2], descritos abaixo:

- **Provedor Internet**: Levantar qual será a empresa de telecomunicações ou provedor de acesso a Internet que deverá prover a infra-estrutura de comunicação básica para a implementação da VPN.
- ***Gateways* VPN**: Levantar se dentro da IES existe a utilização de produto exclusivo de um único fornecedor de solução de redes, pois a adição de suporte a criptografia nestes produtos reduz os custos da VPN. Por outro lado, por exemplo, acrescentar tarefas de criptografia a um equipamento que já funciona como roteador aumenta os riscos, ou seja, numa falha do roteador falha também a VPN.
- **Servidor de Segurança**: Este servidor mantém as listas de controle de acesso e outras informações referentes ao usuário que o *gateway* utiliza para determinar que tráfego é autorizado. Por exemplo, em alguns sistemas, o acesso pode ser controlado através de servidor de autenticação.

Também se deve considerar a integração do controle de outras funções relativas à rede, como reserva de recursos e controle de banda. A integração do controle de tráfego com autenticação e controle de acesso são implementadas conforme a política de gerenciamento de rede da instituição. As implementações de VPN utilizam os *gateways* de segurança VPN que têm a função de se situar entre as redes pública e privada, prevenindo acessos não autorizados.

3ª ETAPA DA METODOLOGIA

Modelo de Implementação da VPN: Nesta etapa revisa-se o levantamento de informações da IES e o refinamento do projeto lógico da VPN visando possíveis ajustes, definindo os protocolos de tunelamento a serem utilizados no projeto, a arquitetura VPN com suas particularidades, o nível de segurança do projeto e tipos de acesso ao sistema de comunicação, assim como o custo e o prazo para implementação da solução. Estabelecendo-se assim as seguintes ações: cronograma de implementação da VPN, definição do *hardware* e *software*, procedimento de teste e relatório técnico operacional da solução VPN.

Protocolos de Tunelamento VPN: Como já foi analisado, existem diversos protocolos disponíveis para a construção de VPNs e que ao mesmo tempo garantem a segurança da conexão, mas cada caso é uma situação diferente que precisa ser analisada para que as reais necessidades sejam especificadas. A aplicabilidade de cada protocolo depende do problema que está sendo apresentado e da solução que se deseja obter. Depende, também, do controle e de como é feita cada implementação destes protocolos. Os protocolos refletem essa dualidade: PPTP, L2F e L2TP são voltados para VPNs do tipo Cliente para LAN, enquanto o IPSec

focaliza em soluções LAN para LAN. A seleção, portanto, deverá se basear no tipo de VPN que se deseja implementar.

Definição do *hardware* e *software* VPN: Definido o tipo de solução VPN, seja LAN para LAN ou cliente para LAN, e o nível de segurança utilizando *gateways*, deve-se procurar no mercado uma solução de *hardware*, por exemplo, roteadores VPN. Por outro lado pode-se ter uma solução de *software*, uma das soluções que estão se difundido rapidamente é aquela implementada com *software* livre GNU/Linux que se baseia em um clone do conjunto de instruções do UNIX [2], mostrando-se atualmente de grande desempenho e baixo custo. Outra solução seria a compra de pacotes fechados que rodam em sistemas operacionais proprietários, porém estas soluções devem demandar custos consideráveis ao projeto, justamente por ser tratar de soluções proprietárias.

Cronograma de implantação da solução VPN: O cronograma de implantação da solução VPN deve ser exeqüível, tanto do ponto de vista técnico como operacional, visto que *hardware* e *software* VPN devem ser montados e configurados observando todas as premissas de desempenho e segurança. Porém, há o outro lado, o dos usuários que não devem ser negligenciados. Pois, caso não haja treinamento efetivo ministrado ao grupo, este ficará impossibilitado de tirar o máximo de vantagem da solução VPN.

Custo da Solução VPN: O custo dependerá do tipo de solução adotada (Cliente para LAN ou LAN para LAN), sua abrangência (Intranet, Extranet ou VPN interna), hardware e software para a implantação da solução, alem do custo de infra-estrutura física, desenvolvimento de programas, mão de obra (consultoria ou própria da instituição) e o provedor de telecomunicações que suportará o *link* com a Internet. O projetista deve decidir dentro destes fatores qual a melhor relação Custo X Benefício para a organização.

Procedimento de Teste da Solução VPN: Os testes da solução VPN são basicamente os teste de segurança, para uma arquitetura de rede deve cobrir os seguintes serviços: Autenticação, Controle de Acesso, Confidencialidade, Não-Repúdio e Auditoria [6].

Geração do Relatório Técnico da Solução VPN: De posse de todas as informações com relação aos fatores envolvidos na solução VPN é gerado um relatório técnico que é disponibilizado ao Grupo Gestor e Usuário, sobre como conduzir a implantação da solução VPN na IES para que haja qualidade, menor prazo e custo compensador.

CONSIDERAÇÕES FINAIS

A Universidade Federal do Pará opera uma das maiores redes Intranet do norte do país, interligando os principais municípios do estado do Pará, que é geograficamente extenso. Além disso, a cada ano, diversos novos núcleos da UFPA são criados para atender a demanda de cursos no interior do estado. Neste cenário hoje enfrentamos dois principais problemas: pouca disponibilidade dos *links* dedicados espalhados no interior do estado; e o alto valor dos custos dos *links* dedicados cobrados pelas operadoras de telecomunicações (pois a maioria dos links para o interior é via satélite).

Neste contexto, houve a necessidade de viabilizar a implantação de uma rede VPN visando atender inúmeros núcleos (ainda sem *link* de comunicação) e também como um serviço alternativo para os locais onde temos *link* com baixa disponibilidade. Na implantação da VPN seguiu-se a metodologia de projeto e implementação propostos neste trabalho. O sucesso da implantação do projeto esta ancorada na nossa real necessidade desse serviço aliado ao uso de ferramentas desenvolvidas e instaladas sobre plataforma de *hardware* aberto (*Personal Computer*) e *software* livre (Sistema Operacional GNU/Linux). A rede privada virtual institucional beneficia principalmente os Campis e núcleos do interior, mas também permite que um usuário remoto em qualquer lugar do mundo utilize os sistemas cliente-servidor como se estivesse em nossa rede Intranet.

REFERÊNCIAS

[1] Murhammer, Martin; Atakan , Orcun; Bretz, Stefan, Pugh, Larry; Susuki, Kazunari; Wood, David,"TCP/IP Tutorial e Técnico", *MAKRON Books*, 2000.

[2] Garfinkel, Simson; Spanfford, Gene, "Pratical UNIX and Internet, Security",*O'Reilly*, 1996.

[3] Dubrawsky, Ido, "Firewall Evolution – Deep Packet Inspection", *SecurityFocus*, 2003.

[4] Virtual Private Network Consortium, <http://www.vpnc.org/>,acesso em 05/11/2002

[5] Brown, Stevew, "Implementing Virtual Private Networks", *McGraw Hill*, 1999.

[6] Scott, Wolfe and Erwin, Chalie, Paul and Mike. "Virtual Private Networks", 2nd Edition, *O'Reilly*, 1998.

[7] PPTP Protocol, <http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/enus/intwork/inbe_vpn_naxe.asp>, acesso em 10/11/2002

[8] L2F Procol, <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm> , acesso em 15/11/2002

[9] L2TP Protocol, <http://search.ietf.org/internet-drafts/draft-ietf-l2tpext-ds-04.txt>, acesso em 15/11/2002

[10] IPSEC - Internet Protocol Security - Security Project at the TCM Laboratory, <http://www.tcm.hut.fi/Tutkimus/IPSEC/ipsec.html>, acesso em 10/11/2002.

[11] Carvalho, Tereza Cristina Melo de Brito, "Metodologia e Ferramentas de Projeto de Redes Locais", *USP,* 1995.

[12] Olíveira, Affonso G.H. and Viégas Jr, Raimundo, "Metodologia de Projeto e Implementação de Rede Privada Virtual Utilizando a Internet", *UFPA*, 2002.