MARCOS EDUARDO MUNIZ GODINHO

UMA ARQUITETURA DE IMPLEMENTAÇÃO DE REDES VIRTUAIS PRIVADAS SOBRE A ESTRUTURA DA UNIVERSIDADE DO CONTESTADO-UnC

Florianópolis – SC
2002

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MARCOS EDUARDO MUNIZ GODINHO

UMA ARQUITETURA DE IMPLEMENTAÇÃO DE REDES VIRTUAIS PRIVADAS SOBRE A ESTRUTURA DA UNIVERSIDADE DO CONTESTADO-UnC

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

VITÓRIO BRUNO MAZZOLA

Florianópolis, Maio de 2002.

UMA ARQUITETURA DE IMPLEMENTAÇÃO DE REDES VIRTUAIS PRIVADAS SOBRE A ESTRUTURA DA UNIVERSIDADE DO CONTESTADO-UnC

MARCOS EDUARDO MUNIZ GODINHO

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Fernando Álvaro Ostuni Gauthier, D. Sc.
Coordenador do Curso

Banca Examinadora:

_____

Prof. Vitório Bruno Mazzola, Dr.
Orientador

_____

Prof. João Bosco Mangueira Sobral, Dr.

_____

Prof. Roberto Willrich, Dr.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ATM - Asynchronous Transfer Mode

BGP - Border gateway Protocol

CE - Customer Edge

CPE - Customer Provider Edge

DES - Data Encryption Standard

DNS - Domain Name System

ESP - Encapsulated Security Payload

GRE - Generic Routing Encapsulation

HMAC - Hashed Message Autentication Code

HTTP - Hyper Text Transfer Protocol

IETF - Internet Engineering Task Force

IKE - Internet Key Exchange

IP - Internet Protocol Version 4

IPV6 - Internet Protocol Version 6

IPSec - Internet Protocol Security

ISP - Internet Service Provider

L2TP - Layer Two Tunnelling Protocol

LAN - Local Area Network

LSP - Label Switching Path

LSR - Label Switching Router

MAC - Media Access Control

MPLS - Multi Protocol Label Switching

MPOA - Multi Protocol Over ATM

NAS - Network Access Server

NAT - Network Address Translation

PE - Provider Edge

PKI - Public Key Infraestructure

POP - Point of Presence

PPP - Point to Point Protocol

PPTP - Point to Point Tunnelling Protocol

PSTN - Public Switched Telephone Network

QoS - Quality of Service

SHA - Security Hashing Algorithm

SLA - Service Level Agreement

SLIP - Serial Line Internet Protocol

SPI - Security Parameters Index

SSL - Secure Socket Layer

VoIP - Voice Over Internet Protocol

UnC - Universidade do Contestado

VPN - Virtual Private Network

WAN - Wide Area Network

RESUMO

Este trabalho apresenta a proposta de um modelo para implementação de VPNs sobre a estrutura geograficamente distribuída da Universidade do Contestado – UnC.

A pesquisa realizada verifica os tipos de VPN, os protocolos de comunicação existentes, as características e sub-características de cada um para à partir deste levantamento definir qual tipo utilizar. O foco da pesquisa é a ligação de cinco campi universitários à Reitoria da Universidade do Contestado para a alimentação de um datawarehouse utilizando redes virtuais privadas.

O modelo leva em consideração a realidade da instituição, os equipamentos já existentes e a relação da solução escolhida perante outras possíveis soluções.

ABSTRACT

This study proposes a sample for the development of VPNs (Virtual Private Network) on the geographically distributed structure of the “Universidade do Contestado”– UnC.

This research checks the types of VPN, the existing protocols of communication, the traits and sub-traits of each VPN so that from this checking on, it is possible to define what type to use. The purpose of this research is connecting five University Campi to the Headquarters of the University in Caçador, utilizing a Virtual Private Network to feed a datawarehouse.

This model takes into consideration the reality of the institution, the existing equipments and the relation of the chosen solution to other possible solutions.

1. INTRODUÇÃO

A cada dia as corporações buscam melhores alternativas de comunicação entre suas unidades. O fator custo é determinante para viabilizar um projeto para interligação de filiais e parceiros e as soluções para redes de longa distância através de linhas dedicadas e circuitos Frame Relay além de caros não proporcionam flexibilidade para a criação de novos links de parcerias.

A expansão da rede interna da empresa além de suas fronteiras físicas é uma estratégia para criar novas oportunidades de negócio e integrar clientes, parceiros, filiais e funcionários que, fora da empresa precisam acessar dados ou informações com segurança.

O acesso a computadores remotos exige investimento em equipamentos como modems, servidores e muitas vezes incidem em tarifas de ligações à distância. Redes Privadas Corporativas baseadas em WANs tradicionais utilizavam circuitos de linhas dedicadas alugadas partindo de cada site para um ponto corporativo comum. Os preços destes circuitos eram calculados de acordo com a distância, aumentando consideravelmente o custo para localidades geograficamente dispersas. Mesmo com esta desvantagem, estas redes proporcionavam altíssimos níveis de segurança e de desempenho. Além do custo, estas WANs tradicionais apresentavam outros problemas: necessitavam de pessoal técnico especializado, equipamentos específicos para WAN, gerenciamento próprio da rede e os custos internacionais eram extremamente altos.

Buscando uma alternativa viável para solucionar grande parte destes problemas surgiu a idéia de utilizar a estrutura de uma rede pública, como a Internet, como uma opção às linhas privativas para implementar redes corporativas.

As VPNs (Virtual Private Networks), surgiram como alternativa para eliminar links dedicados de longa distância que podem ser “substituídos” pela Internet ou por uma estrutura similar. Este conceito está mudando a maneira pela qual as empresas operacionalizam as suas transações. Através da criptografia de pacotes de dados que são

enviados e decodificados quando alcançam o destino, possibilitam a utilização da Internet de forma segura incorporando criptografia entre as extremidades de uma conexão.

Desta forma, o resultado imediato da utilização desta tecnologia é a redução substancial de custos, tanto em ligações interurbanas ou internacionais quanto de infraestrutura, tendo em vista que a Internet está presente em quase todos os países, bem como a segurança das conexões entre as partes envolvidas.

Esta tecnologia pode vir a auxiliar sobremaneira as empresas que necessitam interligar suas filiais e parceiros, bem como os usuários que precisam utilizar recursos de sua rede interna.

Através do exposto, evidencia-se o tema central desta dissertação: a proposta de um modelo para implantação de Redes Virtuais Privadas sobre a estrutura Geograficamente Distribuída da Universidade do Contestado.

1.1 JUSTIFICATIVAS

A presente pesquisa fundamenta-se pelos seguintes motivos:

- O estudo da tecnologia é fundamental para desenvolver com clareza o modelo com a finalidade de garantir a qualidade da solução entre outras possíveis soluções ;

- Buscar opções que possam auxiliar na solução dos problemas apresentados;

- Permitir a análise das soluções nos aspectos financeiro e qualitativo e seus fatores de influência;

- Estudar e analisar como as tecnologias estão sendo utilizadas no mercado; possíveis soluções a que se propõem e como interagem.

1.2 OBJETIVOS

O objetivo deste trabalho é propor um modelo para implantação de redes Virtuais Privadas sobre a estrutura geograficamente distribuída da Universidade do Contestado – UnC.

Mais especificamente, pretende-se:

- Aprofundar o conhecimento através do estudo das Redes Virtuais privadas;

- Pesquisar os diversos tipos de VPNs, protocolos de comunicação e como se relacionam;

- Apresentar um modelo para implantação de Redes Virtuais Privadas sobre a Estrutura Geograficamente distribuída da Universidade do Contestado.

1.3 METODOLOGIA DE TRABALHO

O trabalho seguirá as seguintes etapas de estudo :

- Analisar os Tipos de VPNs, buscando através de suas características mensurar os aspectos relevantes a cada uma delas;

- Estudar e aprofundar conceitos relativos a protocolos de Tunelamento, para uma correta escolha do tipo de protocolo a utilizar no desenvolvimento do modelo.

- Pesquisar as soluções existentes no mercado e propor o modelo para implementação de Redes Virtuais Privadas sobre a Estrutura da Universidade do Contestado.

1.4 ESTRUTURA DO TRABALHO

Esta dissertação está assim dividida:

Capitulo 1: Contém a introdução, justificativa, objetivos, metodologia e estrutura do trabalho.

Capitulo2: Serão abordados conceitos sobre redes Virtuais Privadas; considerações para implementação de VPNs sobre o Backbone Internet/Intranet; tecnologias para implementação de VPN´s e tipos de VPNs. O Objetivo deste capítulo é evidenciar a importância das redes Virtuais Privadas, bem como os tipos disponíveis e as tecnologias para implementação.

Capítulo 3: Aborda o conceito de tunelamento, analisando os tipos de túneis e de protocolos, dando uma visão geral sobre o funcionamento e a estrutura de cada um.

Capítulo 4: Apresenta a arquitetura IPSEC, abordando conceitos de protocolos, gerenciamento de chaves e associações de segurança.

Capítulo 5: Faz a apresentação da Estrutura da Universidade do contestado; descrição de equipamentos; análise dos tipos de VPNs e protocolos a serem utilizados e apresenta a Topologia de rede para implementação.

2. VPN – VIRTUAL PRIVATE NETWORKS

Este capítulo trata dos conceitos acerca das VPNs, fundamentos sobre a implementação sobre um Backbone internet ou IP privado e tipos de VPNs.

Fica clara a importância do levantamento destes dados, já que à partir destes conceitos começa a ser delineado o processo de escolha de qual modelo empregar. Há a necessidade de fazer uma avaliação dos tipos de VPN, que possibilitarão um conhecimento das características e subcaracterísticas de cada um para dar início à proposta de um modelo para implementação de VPNs sobre a estrutura da UnC.

O texto que segue descreverá resumidamente os conceitos sobre VPNs e seus tipos, com a proposta de assegurar qualidade e confiabilidade da conexão entre as partes envolvidas.

2.1 Definição

A socialização da Internet possibilitou às pessoas e organizações uma nova forma de comunicação e acesso à informação. As organizações têm a Internet como um novo meio de apresentar seus produtos ou serviços e realizar transações de negócio. As Redes Privadas Virtuais ou VPN surgem como uma mudança na maneira pela qual organizações podem realizar as suas transações pela Internet, possibilitando reduzir custos utilizando um ambiente de comunicação seguro.

O termo VPN tem sido abordado de uma maneira geral e muitas vezes imprudente. Para um melhor esclarecimento, faz-se necessário o desmembramento e descrição de cada componente do termo conforme proposto por ZANAROLI (2000):

- **Rede:** conjunto de dois ou mais dispositivos, que podem estar localizados em áreas geograficamente distintas e que se comunicam entre si, enviando e recebendo dados, podendo compartilhar recursos.

- **Privada:** a comunicação entre dois ou mais dispositivos da rede estabelecida de forma a garantir que outros dispositivos, os quais não fazem parte desta não tem acesso à informações.

- **Virtual:** por ser uma rede construída logicamente e que não depende da estrutura física da rede utilizada. A comunicação é estabelecida de forma privada sobre uma infraestrutura compartilhada por vários usuários.

Com base no que foi descrito, podemos analisar algumas definições. Segundo FRASER (2001), "VPN (Virtual Private Network) é uma rede empresarial que utiliza uma infraestrutura pública ou compartilhada, como a Internet e estabelece conexões privadas e seguras sobre uma rede não confiável, com usuários geograficamente dispersos, clientes e parceiros de negócio".

GLEESON (2000) define VPN como "uma emulação de uma rede privativa de longa distância usando redes IP, tais como, a Internet, que é uma rede pública, ou backbones IP privados. As VPN podem ser vistas como redes virtuais operando sobre redes reais (IP, ATM, Frame Relay, etc)".

FERGUSON (1998) especifica VPN como "uma rede privada construída sobre uma infraestrutura de rede pública como a Internet global".

As Redes virtuais Privadas permitem interligar redes corporativas de uma instituição, sejam escritórios, fliliais ou parceiros de negócio utilizando os serviços das redes IP como a Internet ou provedores de serviços baseados em IP Backbones privados. Esta interligação tem a aparência de uma conexão dedicada, com a diferença de estar sendo implementada sobre uma rede compartilhada. A técnica de Tunneling ou

Tunelamento possibilita que os pacotes trafeguem sobre uma rede pública através de túneis virtuais que simulam uma conexão ponto a ponto.

A motivação principal para a utilização das VPNs foi o elevado custo fixo dos sistemas de comunicação. O fator custo é altamente considerável sob o ponto de vista econômico na escolha entre VPNs e linhas dedicadas, principalmente nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. As VPNs permitem estender a rede corporativa de uma empresa a inúmeros pontos, eliminando assim a necessidade da contratação de um grande número de linhas dedicadas, minimizando o custo da rede e permitindo acesso a qualquer lugar em que a Internet esteja presente.

Outro fator seria que um número maior de redes virtuais executadas em uma única estrutura física comum de comunicação tem um custo muito menor do que um número equivalente de conexões privadas.

Redes Virtuais Privadas possuem plataformas independentes e qualquer computador configurado para uma rede IP, poderá ser incorporado à VPN sem que nenhuma modificação seja necessária. O único procedimento será a instalação de um software para acesso remoto. Portanto possuem uma boa escalabilidade.

As VPNs Garantem a integridade dos serviços de comunicação e a privacidade que são a base para construção de ambientes seguros, mantendo-os separados de outros usuários que compartilham a mesma infraestrutura. Muitas corporações tem a necessidade de possibilitar a alguns usuários conexões seguras à rede e estão buscando atender a esta demanda pela conectividade remota. Por outro lado, devem suportar o crescimento relativo à conectividade dos escritórios da empresa. Muitas organizações crescem através de novas aquisições ou fusões e a habilidade de integrar infraestruturas independentes pode ser um ponto crítico entre o sucesso e o fracasso na relação de negócios.

VPNs são soluções para estes problemas, oferecendo condições para fornecer acesso remoto imediato e redução de custos na interligação de escritórios, beneficiando-se de uma infraestrutura de rede existente e dos serviços dos ISPs (Provedores de Serviço Internet) e NSPs (Provedores de serviço de rede), oferecendo redução de custos, escalabilidade, flexibilidade, gerenciamento e segurança.

2.2 Considerações para implementações de uma VPN sobre o Backbone Internet

Dois fatores de fundamental importância devem ser levados em consideração quando da implementação de uma VPN sobre o backbone Internet: desempenho e segurança. Os protocolos TCP (Transmission Control Protocol) , o IP (Internet Protocol) e a própria Internet não foram projetados com base nestes requisitos, sendo que, nos primórdios da Internet as aplicações existentes e o número de usuários não exigiam fortes medidas de segurança e desempenho. Porém, se as VPNs são apresentadas como soluções alternativas para as linhas dedicadas e outros enlaces de WAN, novas tecnologias capazes de proporcionar segurança e desempenho foram acrescentadas à Internet, possibilitando a criação de um meio seguro de comunicação.

2.2.1 Compatibilidade

Para a utilização do Backbone internet, faz-se necessário que a VPN seja compatível com o protocolo IP (na camada 3 do modelo de referência OSI), e que utilize endereços IP oficiais. A maioria das organizações prefere utilizar endereços IP privados à adquirir uma faixa de endereços IP oficiais. Através da convenção RFC (Request For Comment) 1597, foram definidos três grupos de endereços para utilização em redes privadas, que são bloqueados por roteadores na Internet.

Para tornar estas redes privadas compatíveis com a Internet, existem três opções:

- Converter em Endereços Internet;

- Instalar Gateways IP especiais;

- Empregar técnicas de tunelamento.

2.2.1.1 Endereços IP

Os endereços IP oficiais são fornecidos pela InterNIC, organização que controla sua utilização. Como a grande maioria das organizações utiliza endereços IP privados, uma solução econômica e inteligente é atribuir endereços IP oficiais para servidores e clientes da rede virtual privada. Nesta solução, os servidores VPN são configurados com um endereço IP permanente, enquanto que os clientes podem utilizar temporariamente endereços oficiais disponíveis. Quando uma conexão VPN é iniciada, através do DHCP (Dynamic Host Configuration Protocol) ou NAT(Network Adress Translation), os clientes recebem temporariamente um endereço IP oficial, que é automaticamente desvinculado do cliente quando a conexão for encerrada.

2.2.1.2 Gateways IP

Gateway IP é um elemento de rede que opera traduzindo o tráfego de um protocolo qualquer para IP e vice-versa. A aplicação do Gateway pode funcionar em um servidor que possua um protocolo qualquer, em um servidor separado ou um dispositivo dedicado. Podem ser usados sem a necessidade de nenhuma modificação para VPNs baseadas em Internet.

2.2.1.3 Tunelamento

Tunelamento é a melhor opção para tornar redes privadas compatíveis com a Internet. A técnica de tunelamento funciona da seguinte forma: numa conexão entre dois pontos, o ponto de origem encapsula os pacotes de outros protocolos em pacotes IP para transmissão via Internet. O processo de encapsulamento consiste em adicionar um cabeçalho IP padrão e o pacote original ser tratado como área de dados. O ponto de destino remove o cabeçalho IP. No capítulo 2 este conceito será abordado com maiores detalhes.

2.2.2 Segurança

A segurança é a primeira preocupação de uma empresa interessada em utilizar VPNs baseadas em Internet. As redes privadas corporativas garantem privacidade e muitas empresas podem considerar que a utilização da internet não fornece padrões de segurança para a criação de uma rede privada. A maior preocupação é quanto à interceptação de dados confidenciais em trânsito na internet. Uma VPN deve ser capaz de validar usuários através de senhas para proteger os recursos contra acessos não autorizados e utilizar criptografia para proteger os dados em trânsito. Deve prover fácil administração e ser transparente aos usuários.

2.3 Tecnologias para implementação de VPNs

Existem quatro componentes básicos para implementação de VPNs baseadas na Internet: A própria Internet, gateways seguros, servidores com políticas de segurança e certificados de autenticidade.

A Internet provê a infraestrutura para sustentação de uma VPN e os gateways seguros (que podem ser roteadores, firewalls, hardwares específicos e outros), são colocados entre a rede privada da corporação e a Internet para impedir a entrada de intrusos e são capazes de fornecer o tunelamento e criptografia necessários antes da transmissão dos dados através da rede pública.

Os roteadores necessitam examinar e processar cada pacote que deixa a LAN, pode-se incluir a criptografia nos pacotes no próprio roteador.

Firewalls também processam todo o tráfego IP, baseado em filtros definidos nos mesmos e por este motivo não são aconselhados para tunelamento de grandes redes com grande volume de tráfego.

A utilização de hardware específico para implementar tarefas de tunelamento, criptografia e autenticação é outra solução. Estes dispositivos operam como pontes, implementando a criptografia e são geralmente colocados entre o roteador e e os links de WANs. O ponto principal desta solução é que várias funções estão implementadas em um único dispositivo.

VPNs providas através de software são capazes de criar túneis entre pares de gateways seguros ou entre um cliente remoto e um gateway seguro. Apesar de apresentar custo baixo não é aconselhável sua utilização para redes que apresentam um grande volume de tráfego. Sua vantagem, além do baixo custo é que esta implementação pode ser efetuada em servidores já existentes e seus clientes.

A política de segurança dos servidores é outro aspecto importante na implementação de VPNs. Um servidor seguro deve manter a lista de controle de acesso e outras informações relacionadas aos usuários, que serão utilizados pelos gateways para a determinação do tráfego autorizado.

Os certificados de autenticidade são necessários para verificar as chaves trocadas entre sites ou usuários remotos.

2.4 Tipos de VPNs

Existem vários tipos de VPNs e dependendo dos requisitos funcionais, vários métodos de construção de cada tipo estão disponíveis. Ao analisar o tipo de VPN a ser aplicado, devem ser analisadas considerações sobre qual o tipo de problema a ser solucionado, qual o risco em relação à segurança fornecida de cada implementação e fatores sobre a escalabilidade e a complexidade envolvida para implementação e manutenção da VPN. De acordo com as camadas do modelo TCP/IP, as VPNs podem ser classificadas nos seguintes tipos:

2.4.1 VPN da camada de rede (Network Layer VPN)

Esta camada refere-se ao sistema de roteamento IP (o encaminhamento da informação de um ponto para outro da rede). Segundo FERGUSON (1998), existem dois modelos de VPN que merecem destaque:

PEER VPN: É o modelo em que a definição da rota na camada de rede para entrega dos pacotes é feita “hop-by-hop”, onde cada nó intermediário é um par do próximo nó hop. Ex: redes roteadas.

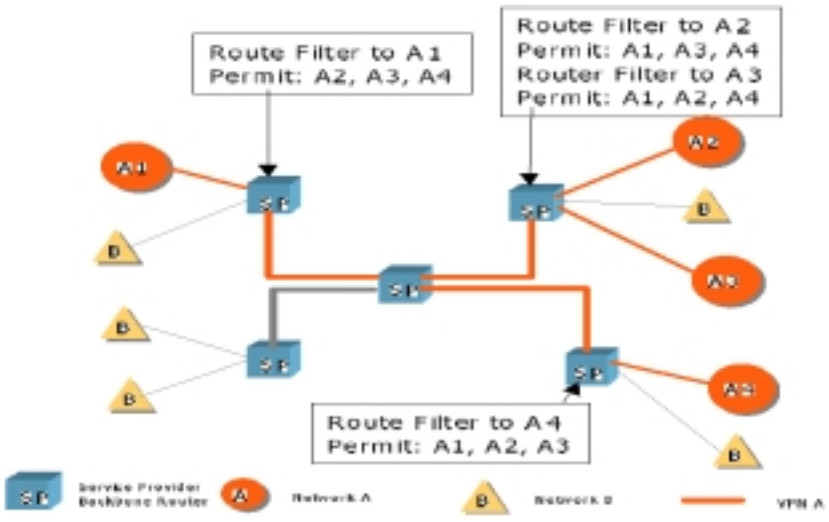
OVERLAY VPN: A camada de enlace intermediária é usada como “cut-through” (atalho) para outro nó de borda da rede. Ex: ATM, Frame Relay.

2.4.1.1 Controlled Route Leaking

Conhecido também como “route filtering”, onde a propagação das rotas é feita de maneira controlada. Apenas alguns pontos específicos de uma rede recebem rotas de outras redes que pertencem a uma mesma comunidade de interesse. O roteador de uma VPN estabelece uma relação de roteamento com o roteador da rede do provedor de serviços VPN. Apenas um subconjunto de redes forma a VPN. As rotas associadas a este conjunto são filtradas de forma que não sejam anunciadas para outro conjunto de rede não autorizado. Além disso, as rotas não-VPN não são anunciadas para as redes pertencentes a VPN.

Por exemplo, as informações de roteamento de um site na rede A só são transmitidas para os outros sites da mesma rede. Os sites fora da rede A não têm nenhum conhecimento explícito sobre ela, embora pertençam a mesma infraestrutura. Este exemplo é ilustrado abaixo:

Figura 1 - Implementação de VPN através de filtros



Fonte: **FERGUSON,** Paul; **HUSTON**, Geoff. **What Is a VPN?**. **Cisco Systems, Abril, 1998.**

A privacidade dos serviços é garantida por qualquer host de VPN ser incapaz de responder a pacotes que contém endereço de origem que não estejam relacionados à mesma comunidade de interesse. A dificuldade de implementação deste tipo de VPN está na configuração correta de filtros, especialmente em grandes redes causando um elevado overhead operacional.

2.4.1.2 Tunneling

Atualmente, a transmissão segura entre redes privadas na Internet se faz possível através do uso de tecnologias baseadas em túneis IP (IP tunnel).

Os túneis IP são soluções combinadas de software e hardware, e oferecem serviços como: troca segura de informações entre redes privadas e indivíduos através da Internet pela utilização de recursos de criptografia, verificação de integridade dos dados transmitidos, autenticação e controle de acesso a usuários. Este método de construção de VPNs permite que a informação seja transferida com segurança, usando uma rede pública, como se os computadores estivessem na mesma rede física.

Quando uma corporação opta por utilizar VPNs sobre uma estrutura como a Internet, podem ocorrer problemas de performance e atrasos na transmissão de dados, sobre os quais a corporação não tem nenhum controle.

Mesmo com a vantagem da redução de custos, quando se constrói uma WAN corporativa utilizando a Internet como meio de transporte o fator segurança deve ser observado com atenção. As transmissões da empresa não estarão mais restritas a um link dedicado privado. Os dados farão a maior parte do trajeto através de um caminho de roteadores e hosts desconhecidos pela corporação, e praticamente inseguro. Por este motivo, o uso da criptografia nas VPNs é fundamental.

Quando a informação é encriptada no lado emissor, uma chave é necessária para decriptá-la no lado receptor. Os dispositivos que implementam a VPN em cada lado da conexão (Firewalls ou servidores de túneis dedicados) gerenciam esta troca de chaves de forma automática e transparente. Fornecer acesso para usuários remotos à rede através de VPNs é uma tarefa um pouco mais complexa, pois há a necessidade de existir algum mecanismo para autenticar o usuário e uma forma de negociar a troca de chaves. Algoritmos de chaves públicas e assinaturas digitais são utilizados para este fim.

O processo de tunelamento é simples. Num primeiro momento o cliente é autenticado pelo servidor túnel ao tentar estabelecer a conexão. A informação é encapsulada em pacotes TCP/IP e enviada pela rede em um formato de dados ilegíveis (criptografados). Uma vez que os pacotes chegam em seu destino, serão reconstituídos e decodificados para um formato legível (descriptografados). A criptografia se faz necessária para garantir a segurança.

Existe outro método de construção de VPNs onde a transmissão da informação é processada em “túneis” criptografados” através do tunelamento GRE (Generic Routing Encapsulation) entre um roteador origem e destino. Outros protocolos router-to-router ou host-to-host conhecidos, como o L2TP e o PPTP serão descritos no capítulo 2.

Quanto a arquitetura o conceito de VPN tem como base a idéia de uma coleção de túneis, estabelecida ao longo de uma rede pública. Cada site de conexão com a rede é configurado como um link físico, o qual usa o endereçamento e roteamento à partir da estrutura de rede existente. Cada ponto final de uma conexão túnel é ligado logicamente a outro ponto remoto da mesma VPN. O roteamento da VPN é isolado do roteamento normal feito para a rede pública. As VPNs podem usar o mesmo espaço de endereçamento privado em múltiplas VPNs sem nenhum impacto, o que fornece uma considerável independência de hosts.

O túnel pode encapsular famílias diferentes de protocolos, sendo possível para as VPNs que usam a tecnologia de ‘tunelamento’ simular grande parte das funcionalidades de uma rede privada dedicada.

Figura 2 – Transmissão de pacotes pelo túnel

Fonte: CHIN, **Liou Kuo:** Rede Privada Virtual**. News Generation, Volume 2, Número 8. RNP 1998.**

2.4.2 VPN da camada de enlace (Link-Layer VPNs)

Este modelo funcional é o mais parecido com o das redes privadas convencionais. O Modelo utiliza os sistemas de transmissão e a plataforma de rede para a conectividade da camada física e de enlace.

2.4.2.1 Conexões Virtuais ATM e Frame Relay

Uma rede privada convencional utiliza uma combinação de circuitos dedicados de uma operadora de telecomunicações aliado a uma infraestrutura de comunicação privada adicional com a finalidade de construir redes independentes. Geralmente usa a infraestrutura privada para dar suporte às VPNs. Quando esta rede privada estende-se para além das fronteiras da empresa, os circuitos dedicados são, tipicamente, fornecidos por uma grande infraestrutura pública de comunicação. Faz-se necessário então a utilização de algum método de multiplexação (divisão por tempo ou por frequência) para criar circuitos dedicados. A característica essencial deste tipo de circuitos é a sincronização do clock, assim o emissor e receptor enviam os dados de acordo com a taxa de clock que é estabelecida pela capacidade dos circuitos dedicados.

Segundo SOUZA (2000), “A VPN de enlace empenha-se em manter os elementos críticos da funcionalidade de uma rede privada independentes, ao mesmo tempo em que requer um menor investimento ao utilizar a infraestrutura de redes públicas. Assim, um conjunto de VPNs pode compartilhar a mesma infraestrutura de conectividade, sem que tenham visibilidade ou conhecimento umas das outras. Geralmente, essas redes operam no nível 3 da camada de rede e a infraestrutura consiste de rede Frame Relay ou ATM”.

A principal diferença entre a arquitetura de circuitos virtuais e circuitos dedicados é que não existe a necessidade da sincronização do clock ser compartilhado entre o emissor e receptor, nem a necessidade de ser assinalado um caminho dedicado para transmissão. O emissor não tem um conhecimento prévio da capacidade disponível dos circuitos virtuais, e essa capacidade pode variar de acordo com a demanda total requisitada por outras transmissões simultâneas e pela própria atividade dos switches. Entretanto, o emissor e receptor podem usar um clock adaptado, no qual o emissor ajusta a taxa de transmissão em consonância com os requerimentos da aplicação e da sinalização recebida do receptor ou da rede.

A grande vantagem de uma rede WAN pública que oferece circuitos virtuais é a sua flexibilidade. A maioria dos usuários dos serviços Frame Relay, aderiram a esta tecnologia pelo fator custo. Além de ser mais barato os usuários podem negociar níveis de serviços (SLA – Service Level Agreement) para garantir uma taxa na entrega de frames. A tecnologia usada na camada 2 não é baseada na sincronização do clock onde o fluxo de cada novo serviço é aceito ou rejeitado de acordo com a capacidade de atender totalmente a demanda dos recursos solicitados, ao contrário, cada serviço adicional é aceito pela rede e processado na base da lei do “melhor esforço”. A flexibilidade fornecida pelos PVC’s permitem a construção de VPNs em uma rede Frame Relay. O mesmo mecanismo pode ser usado em redes ATM. Em ambos os casos, a qualidade de serviço vai depender da tecnologia e engenharia adequada utilizada na rede, pois não existe uma garantia da qualidade de serviço como um atributo da tecnologia Frame Relay ou ATM.

2.4.2.2 MPOA (Multi Protocol Over ATM)

Redes Virtuais Privadas podem ser construídas através do protocolo MPOA. O protocolo em questão utiliza o encapsulamento descrito no RFC1483 da IETF. Tem um processo parecido com o mecanismo “cut-through”; switches da camada 2 são utilizados para tornar possível que todos os pontos de saída sejam visíveis como simples hops distantes entre si. Os roteadores da borda determinam o caminho de transmissão numa rede ATM. Quando é tomada a decisão de como alcançar a rede, o roteador repassa o pacote para uma Conexão Virtual (VC) designada para um roteador egress em particular.

Esta tecnologia tem uma certa aplicabilidade em um ambiente ATM homogêneo, porém oferece poucos benefícios ao provedor de serviço VPN analisando o vasto ambiente de VPN que engloba outras tecnologias da camada de enlace . A principal vantagem do MPOA é que utiliza circuitos dinâmicos ao invés de modelos estáticos. O ambiente objetiva controlar a criação dinâmica de VC’s ATM edge-to-edge, reduzindo o overhead operacional. Requer, porém, uma disponibilidade uniforme da tecnologia ATM.

Foi introduzido o modelo “peer” de VPNs que permitem aos nós de saída (egress) manter tabelas de roteamento separadas, uma para cada VPN, permitindo que decisões de roteamento sejam feitas em cada nó para cada VPN existente. A desvantagem é que cada saída deve executar um processo de roteamento e manter uma base de informações (RIB-Routing Information Base) para cada comunidade VPN de interesse.

É importante observar que o conceito “virtual router” requer uma forma de marcar os pacotes (packet labeling), através do cabeçalho ou de algum mecanismo de encapsulamento para que o switch possa associá-los com a tabela de roteamento VPN correta.

2.4.2.3 MPLS (Multi Protocol Label Switching)

Talvez seja um dos modelos que melhor atende aos requisitos de escalabilidade, usando labels VPN em ambientes de roteamento distintos, do mesmo modo que labels de pacotes são necessários para ativar a correta tabela VPN de roteamento.

A arquitetura MPLS é baseada no uso de 'label switching'. A arquitetura é híbrida e busca combinar duas abordagens VPN distintas: a utilização de estruturas de roteamento da camada de rede e comutação por pacotes e a utilização dos circuitos da camada de enlace e comutação por fluxo. O MPLS requer um protocolo baseado nas funcionalidades de roteamento nas saídas intermediárias e opera tornando a infra-estrutura de transporte inter-switch visível ao roteamento.

No caso do protocolo IP sobre ATM, cada link ATM aparece como um link IP, adicionado aos switches ATM a funcionalidade de roteamento IP. O roteamento IP é utilizado para selecionar caminhos através da rede, que são marcados com uma seqüência de labels, podendo ser vistos como indicadores do caminho de entrega definidos localmente.

Pacotes que entram no ambiente MPLS são assinalados com um label local e a interface outbound baseia-se na decisão de entrega local. O label local é atachado ao pacote via um mecanismo simples de encapsulamento. No próximo switch MPLS, a decisão de entrega do pacote será tomada de acordo com o label do mesmo, que irá determinar a próxima interface hop e o label correspondente ao pacote de saída, usando uma tabela local indexada pelo label. Assim, o label aplicado a um pacote que entra no ambiente MPLS determina a seleção do roteador de saída.

Segundo (FERGUSON,1998) as VPNs MPLS têm três componentes chaves:

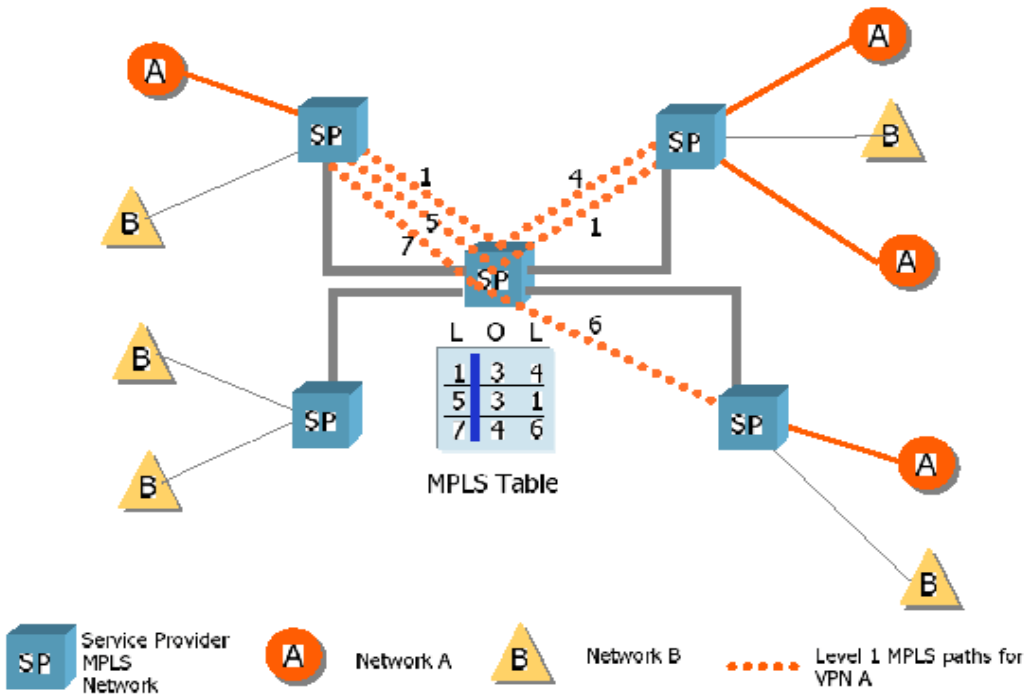
1) Distribuição obrigatória das informações de roteamento como uma maneira de formar as VPNs e controlar interconectividade entre elas;

2) Utilização de VPN ID’s e a concatenação destes identificadores com o endereço IP para tornar único os endereços que são repetidos;

3) Utilização do label switching (MPLS) para oferecer um caminho de envio ao longo das rotas construídas nos passos 1 e 2.

A figura a seguir exibe uma estrutura MPLS. A tabela ilustrada indica como os circuitos virtuais MPLS são construídos:

Figura 3 – Estrutura MPLS



Fonte: FERGUSON, **Paul;** HUSTON**, Geoff.** What Is a VPN?**.**

Cisco Systems, Abril, 1998.

2.4.2.4 Criptografia a nível de enlace (Link-Layer Encryption)

As tecnologias de criptografia disponíveis são extremamente efetivas em oferecer dois requisitos básicos para conectividade das VPNs: segmentação e virtualidade. Elas podem ser usadas em quase todas as camadas da pilha de protocolos. Por si só, não existe um padrão da indústria para a criptografia da camada de enlace. Todas as soluções oferecidas são, geralmente, proprietárias de cada fornecedor, requerendo hardware especiais de criptografia.

A criptografia na camada de link evita a complexidade da implementação de esquemas criptográficos nas camadas mais altas do modelo, mas por outro lado, pode-se tornar economicamente inviável, dependendo da solução adotada.

2.4.3 VPN da Camada de Transporte e Aplicação

Embora as VPNs possam ser implementadas nas camadas de transporte e aplicação, esta não é uma solução muito comum. O método mais conhecido para fornecer esta virtualidade é através da utilização dos serviços de criptografia nestas camadas. Como exemplo destes serviços, temos as transações criptografadas de e-mail ou o serviço de transferência autenticada de zonas DNS entre servidores (DNSSec – Domain Name System Security).

2.4.4 Considerações sobre o MPLS

O MPLS está se destacando mundialmente e deverá ascender à partir do fim do ano de 2002 como uma ferramenta para as operadoras que pretendem oferecer uma melhor qualidade nos serviços IP para usuários corporativos. Este protocolo está sendo

padronizado por seu respectivo fórum que até o final do ano pretende concluir a parte de interoperabilidade entre os fabricantes.

O MPLS é uma tecnologia de transporte de dados que vem a profissionalizar o IP, permitindo grande avanço na área de serviços, especialmente os de VPN e voz sobre IP, pela qualidade e segurança que oferece. Este protocolo acrescenta rótulos (chamados de labels) em cada pacote e faz o roteamento das informações de acordo com a categoria de serviços, tornando as redes IP previsíveis e gerenciáveis.

As aplicações de redes virtuais privadas IP são as maiores beneficiadas por este protocolo, que oferece grandes vantagens em relação aos circuitos ATM, Frame Relay e outros. O MPLS viabiliza as VPNs de maneira econômica, dispensando as tradicionais ligações ponto-a-ponto para a conectividade. Como o núcleo já está preparado, o acesso se dá através de um roteador multisserviço, levando em consideração que o maior impacto do MPLS está no incremento do outsourcing, com uma maior procura das operadoras por parte das empresas para resolver problemas de conexão.

Outra vantagem do MPLS está na possibilidade de controle do tráfego dentro da rede, que poderá ser otimizado de acordo com as aplicações e o fluxo de dados previsto nos SLAs e, portanto, segurança na garantia de QoS. O MPLS identifica por onde passa o maior volume de tráfego e indica como desviá-lo para otimizar a topologia e prestar um melhor serviço ao cliente. De acordo com Roosevelt Ferreira, consultor técnico da Nortel Networks, o MPLS permite, por exemplo, enviar o tráfego de São Paulo para Belo Horizonte via Rio de Janeiro, o que não é possível no roteamento IP normal, que seleciona sempre o caminho mais curto.

Atualmente, a grande maioria dos usuários VPN do Brasil trabalham com uma estrutura baseada em Frame Relay ou ATM. Nessa modalidade a operadora não identifica em sua rede o que está passando, mas com o MPLS é possível tratar o tráfego do cliente, oferecendo serviços adicionais. Este protocolo oferece a possibilidade de estabelecer classes de serviços diferenciadas por meio de mecanismos que controlam as filas dos pacotes nos roteadores, indicando as prioridades.

O MPLS não prioriza o protocolo de nível 2 que deverá utilizar. Ele pode rodar sobre ATM, Frame Relay, Gigabit, Ethernet e outros. Alguns fabricantesestão introduzindo em sua linha de switches ATM o roteamento MPLS. Outros fabricantes estão adaptando os roteadores tradicionais para fazerem o switching MPLS. A vantagem do roteamento MPLS em switches ATM está na diminuição do delay da rede, já que os fabricantes de roteadores devem incorporar novo hardware para não deixar o trabalho todo para o software.

A idéia de oferecer um switch que seja ao mesmo tempo um roteador puro IP, MPLS e ATM, viabiliza diferentes tipos de serviços na mesma plataforma. Isso torna o MPLS um protocolo bastante promissor, já que garante conexões seguras e com qualidade no núcleo da rede viabilizando, portanto o serviço de voz sobre IP na nova rede pública e até o serviço de celular de terceira geração.

O futuro aponta para a transmissão de voz diretamente sobre o MPLS sem passar pelo IP. Já existe um padrão, o VoMPLS, que está sendo estudado pelo fórum. Também foi desenvolvida uma extensão deste protocolo, o G-MPLS (Generalizer MPLS), cuja idéia é consolidar desde a camada 1 até as camadas 4 e 5 do modelo OSI.

2.5 Conclusões

Este capítulo apresentou conceitos importantes com a finalidade de auxiliar no desenvolvimento do modelo para implementação de VPNs sobre a estrutura da UnC. Num primeiro momento, utilizar uma infraestrutura pública de comunicação como a Internet para trafegar dados corporativos com segurança parece ser uma idéia um tanto confusa.

Quando se pensa em confiabilidade de uma conexão, é fácil imaginar padrões de comparação, provavelmente ligados à confiabilidade e qualidade de um serviço que uma

empresa ofereça ou alguma característica física da própria conexão. Quando se trata de Internet, como podemos definir confiabilidade e segurança?

A Internet é uma alternativa para as conexões privadas ou por linha discada. Na Internet, não se paga pela distância de comunicação, nem pelo volume de tráfego transportado. Basta uma ligação de curta distância a um provedor local. Esta ligação pode ser por linha discada ou por linha dedicada. A grande vantagem da Internet é permitir o acesso a qualquer outro ponto de sua rede através de uma ligação única. Não é necessário manter uma infra-estrutura de comunicação complexa para comunicar-se através dela. Basta um modem ou um roteador. Entretanto, Redes Virtuais Privadas se fazem necessárias para permitir uma comunicação segura através da rede. As VPNs não são exclusividade da Internet. Elas podem ser criadas também no interior de redes locais.

Redes Virtuais Privadas são constituídas para garantir a integridade dos serviços de comunicação e a privacidade construindo um ambiente seguro de comunicação sobre uma infraestrutura pública como a Internet, possibilitando isolar o tráfego de outros usuários que compartilham a mesma infraestrutura através da criptografia e autenticação.

Observamos que existem vários tipos de VPN e que podem ser aplicados sobre as diversas camadas do modelo OSI. No caso da UnC, podemos utilizar dois tipos de VPNs: VPNs da camada de enlace (utilizando MPLS) e VPNs da camada de rede (através do tunelamento) que deverão ser analisados posteriormente.

A análise dos tipos de VPNs é importante porque ajuda a definir melhor qual modelo aplicar. Dentre os itens a serem analisados alguns merecem maior destaque: nível de segurança, Qos, facilidade de implementação e custo.

3. TUNELAMENTO

Como todas as novas tecnologias, as VPNs passam a contar com um importante impulso: a padronização de protocolos que permitem a interoperabilidade entre os produtos. No caso das redes virtuais, o IPsec, voltado para a incorporação de recursos de encriptação dos dados já é adotado por diversos fabricantes que incorporaram em suas linhas destinadas ao negócio Internet.

Existem diversos protocolos disponíveis para a construção de VPNs e que ao mesmo tempo garantem a segurança e privacidade da conexão. Mas, a grande dúvida aparece: qual protocolo escolher? 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 desejamos obter.

Durante muito tempo as empresas de telecomunicações têm construído VPNs que aparecem transparentes para o usuário, mas fisicamente elas compartilham um backbone com outros clientes. VPNS têm sido construídas sobre as tecnologias X.25, Frame Relay e ATM. Com o objetivo de manter a privacidade em um ambiente público, a VPN usa o controle de acesso e a criptografia. Os usuários têm disponível uma diversidade de protocolos que garantem a segurança dos dados. Estes protocolos oferecem a vantagem da transferência de informação através de “túneis” . Os principais a serem citados são: PPTP, L2F, L2TP, IPSec.

O que diferem estes protocolos são os objetivos para os quais as VPNs foram inicialmente utilizadas. Para alguns, elas vieram substituir os servidores de acesso remoto, passando as conexões a serem feitas através de um provedor local de serviços Internet. Para outros, as VPNs estabeleceram os chamados "túneis seguros" para o tráfego entre LANs protegidas. Os protocolos refletem essa dualidade: PPTP, L2F e L2TP são voltados para VPNs dial-up, enquanto o IPSec focaliza em soluções LAN-to-LAN. A seleção, portanto, deverá se basear no tipo de VPN que se deseja implementar (dial-up, LAN-to-LAN ou uma combinação das duas).

Este capítulo se propõe a investigar, ou seja, a estudar os diversos tipos de Túneis e Protocolos, bem como suas diferenças, necessidades, vantagens e desvantagens de forma a deduzir o melhor protocolo a utilizar neste projeto.

3.1 Definição

O tráfego de dados transmitidos pelo TCP/IP através da Internet está sujeito a vários problemas de segurança. Atualmente, a transmissão segura entre redes privadas na Internet é possível através do uso de tecnologias baseadas em túneis IP.

Segundo SOUZA (2000) “Tunelamento é o encapsulamento ponto-a–ponto das transmissões dentro dos pacotes IP”. O tunelamento permite:

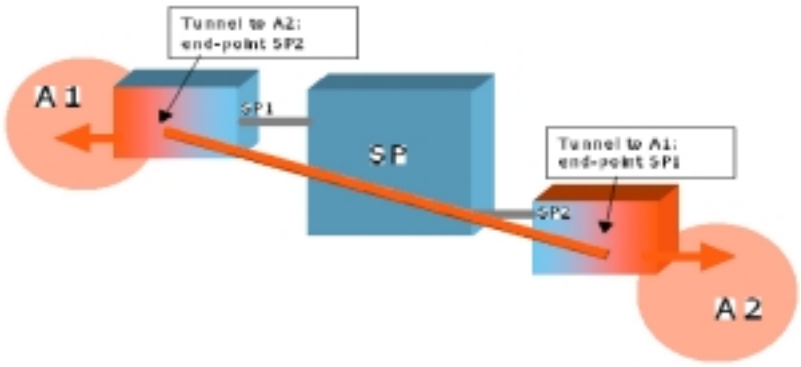
- tráfego de dados de várias fontes para diversos destinos em uma mesma infra-estrutura;
- tráfego de diferentes protocolos em uma mesma infra-estrutura;
- garantia de QoS, direcionando e priorizando o tráfego de dados para destinos específicos.

3.2 Tipos de Túneis

O mecanismo mais comumente utilizado é o tunelamento GRE (Generic Routing Encapsulation) entre roteadores ou entre hosts que executam protocolos de tunelamento como L2TP e o PPTP. Túneis GRE são configurados entre um roteador origem (ingress) e o roteador destino (egress). Os pacotes a serem transmitidos pelo túnel são encapsulados com um novo header do protocolo GRE e colocados no túnel com o

endereço de destino do túnel end-point (o próximo hop). Quando o pacote chegar no túnel end-point, o cabeçalho GRE é retirado e o pacote continua a ser transmitido até o destino, de acordo com o cabeçalho IP original.

Figura 4 - Tunelamento GRE



Fonte: FERGUSON, **Paul;** HUSTON**, Geoff.** What Is a VPN?**. Cisco Systems, Abril, 1998.**

Na maioria das vezes o túnel GRE é ponto-a-ponto, existindo um único endereço fonte associado com somente um túnel endpoint, mas existem algumas implementações que permitem a configuração “point-to-multipoint”, onde o endereço de origem está associado com vários destinos. Desde que o túnel GRE deve ser configurado manualmente, existe uma relação direta entre a quantidade de túneis que devem ser configuradas e o trabalho administrativo necessário para configuração e manutenção dos mesmos, bem como o overhead causado pelo encapsulamento de cabeçalho GRE. Segundo SOUZA (2000), “Como o túnel ainda mantém um pequeno percentual de vulnerabilidade (a privacidade não é absoluta), a segurança da rede ainda é um assunto que merece preocupação”. Pacotes com o formato GRE podem, por exemplo, ser injetados na VPN por terceiros. Para garantir um alto nível de integridade e privacidade na VPN, é necessário configurar filtros de entrada no roteador (ingress) que devem estar alinhados com a estrutura túnel estabelecida.

3.2.1 Virtual Private Dial Networks (VPDN's)

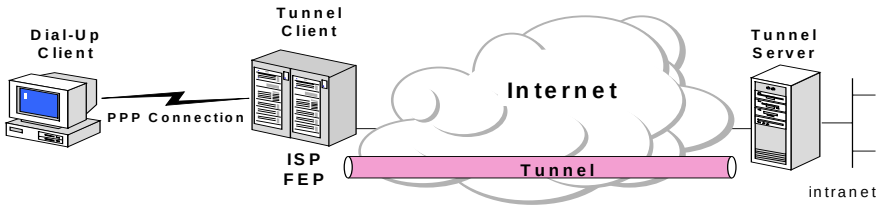
Existem diversas tecnologias proprietárias e padrões abertos disponíveis para a construção de VPNs discadas. Os métodos de implementação mais populares baseiam-se no túnel PPTP e L2TP.

Segundo CHIN (1998), a conexão túnel pode ser inicializada por um cliente ou por um NAS (Nerwork Access Server ou Dial Access Server), tendo como características os seguintes tipos:

- Túnel voluntário - criado a partir de um pedido do usuário. Um usuário ou cliente pode emitir um pedido de VPN para configurar e criar um *túnel voluntário.* Neste caso, o computador do usuário representa o túnel end-point, fazendo também o papel do cliente túnel. Uma conexão é estabelecida para cada cliente. Ex: PPTP.

- Túnel compulsório - O túnel é criado sem que o usuário inicie alguma ação. O cliente não precisa mais fazer a conexão com outro ponto da rede ou com outra rede. Neste cenário, tudo que ele precisa é estabelecer a ligação dial-up com o provedor (NAS). Baseado no perfil do cliente e na sua correta autenticação, o túnel compulsório é dinamicamente estabelecido entre o NAS e um end-point, onde a sessão PPP do cliente é finalizada. O servidor de acesso remoto VPN, localizado entre o computador do usuário e o servidor túnel, é responsável pela configuração e criação do túnel, desempenhando a função de túnel end-point e cliente. Ex: L2TP.

Figura 5 - Túnel compulsório



Fonte: CHIN, **Liou Kuo:** Rede Privada Virtual**. News Generation, Volume 2, Número 8. RNP 1998.**

O túnel compulsório pode ser classificado em:

- Estático: Todas as chamadas são transmitidas via túnel para um mesmo servidor.
- Realm: As chamadas são transmitidas em túneis criados de acordo com o domínio do usuário. Ex: ufsc.br
- User: As chamadas são transmitidas em túneis criados baseados no userID. Ex: godinho@ufsc.br

3.3 Protocolos

Os Protocolos de Tunelamento são responsáveis pela abertura e gerenciamento de sessões de túneis em VPNs. Segundo ZANAROLLI (2000), estes protocolos podem ser divididos em dois grupos:

- **Protocolos de camada 2 (PPP sobre IP):** transportam protocolos de camada 3, utilizando quadros como unidade de troca. Os pacotes são encapsulados em quadros PPP;
- **Protocolos de camada 3 (IP sobre IP):** encapsulam pacotes IP com cabeçalhos deste mesmo protocolo antes de enviá-los .

Os túneis orientados à camada 2 (enlace) são similares a uma sessão onde as extremidades do túnel negociam a configuração dos parâmetros para estabelecimento do mesmo (endereçamento, criptografia, parâmetros de compressão, etc.). A gerência do túnel é realizada através de protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada 3 (rede) a fase de manutenção do túnel não existe.

Para técnicas de tunelamento VPN Internet, quatro protocolos se destacaram, em ordem de surgimento:

- PPTP - Point to Point Tunneling Protocol;
- L2F - Layer Two Forwading;
- L2TP - Layer Two Tunneling Protocol;
- IPsec - IP Security Protocol.

O PPTP, o L2F e o L2TP são protocolos de camada 2 e têm sido utilizados para soluções Client-to-Lan; O IPsec é um protocolo de camada 3 mais enfocado em soluções LAN-to-LAN.

3.3.1 PPTP (Point-to-Point Tunneling Protocol)

A Microsoft (junto com a 3Com, Ascend Communications, ECI Telematics e U.S. Robotics) tem sua solução para a criação de um canal seguro de comunicação em redes Windows NT/2000, Windows 95/98 e servidores de acesso remoto. A solução Microsoft é baseada no protocolo chamado PPTP , que oferece serviços de autenticação e criptografia.

Protocolo de encapsulamento Ponto a Ponto (PPTP) é uma tecnologia de rede que permite usar a Internet como sua própria rede privada virtual e segura. O PPTP é integrado ao servidor RAS (Remote Access Server) que faz parte do Windows NT Server. Com o PPTP, os usuários podem discar para um provedor de serviços de Internet (ISP) local ou conectar-se diretamente à Internet, e acessar sua rede com a mesma facilidade e segurança como se estivessem em suas próprias mesas de trabalho.

A tecnologia PPTP oferece vantagens significativas:

- Custos de transmissão mais baixos pela conexão via Internet, em vez de uma chamada de longa distância ou do uso de uma linha telefônica do tipo "0800";

- Custos de hardware mais baixo ao permitir a localização centralizada de placas de ISDN ou modems;

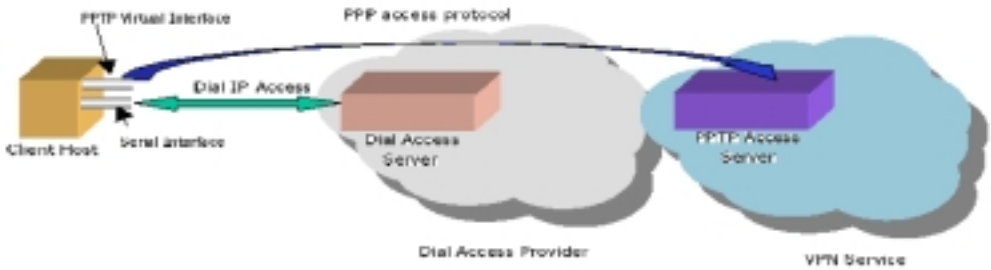
- Menor sobrecarga administrativa por meio da criptografia de dados e da compatibilidade com todos os protocolos de rede (como IP, IPX e NetBEUI);

- Suportado pelo Windows NT Workstation e Windows 95;

- Rede fácil e flexível. Pode-se transferir PPTP para o PC do cliente remoto ou nos pontos locais de presença do provedor de serviços de Internet.

Este padrão vem tornando-se cada vez mais popular em função de estar incluído no sistema operacional da maioria dos computadores pessoais existentes no mundo. Inserido na categoria de túnel voluntário, o PPTP permite o estabelecimento de túneis point-to-point individuais (para localizar servidores PPTP) a partir de computadores desktop. Não há nenhuma participação de servidores NAS na negociação PPTP e no estabelecimento do túnel. Neste cenário, o cliente estabelece uma ligação dial-up com o NAS, entretanto, a sessão PPP encerra-se no NAS, de acordo com o modelo PPP tradicional. A sessão PPTP subsequente é estabelecida entre o cliente (end-system) e um PPTP server que o cliente deseja acessar.

Figura 6 - Acesso dial-up PPTP



Fonte: FERGUSON, **Paul;** HUSTON**, Geoff.** What Is a VPN?**. Cisco Systems, Abril, 1998.**

O usuário PPTP tem a vantagem de poder escolher o término do túnel PPTP depois da negociação PPP ter sido inicializada. Este fato é importante para o caso do tunnel end-point mudar com freqüência. Outra vantagem significativa é que o túnel PPTP é transparente para o provedor de serviço e nenhuma configuração é necessária entre o operador NAS e a VPN de acesso dial up. Neste caso, o provedor não é responsável pelo servidor PPTP. Ele, simplesmente, repassa o tráfego PPTP da mesma maneira que processa o tráfego IP. O túnel PPTP pode se estender por vários provedores sem a necessidade de configurações explícitas. Entretanto, existe o lado econômico e as VPNs trazem uma nova oportunidade de negócio para os provedores de serviço caracterizando-se por ser mais uma fonte de renda, onde os clientes seriam cobrados de acordo com seus privilégios. Porém, do lado cliente esta é uma solução onde ele só tem a ganhar, ficando independente dos provedores. Ele só precisa ter uma conectividade a nível do protocolo IP, não precisando pagar caro por uma inscrição ao provedor. A maioria das aplicações da VPN PPTP é destinada aos usuários que deslocam-se constantemente. Eles precisam, apenas, fazer uma conexão local com uma rede pública de dados (Internet) e a partir daí, criar um túnel privado do sistema cliente até o ponto remoto desejado.

O PPTP fornece um método consistente para encapsular o tráfego da camada de rede e fazer a transmissão remota entre clientes Windows e servidores. Este protocolo não especifica um esquema de criptografia particular. Normalmente, utiliza o protocolo MPPE (Microsoft Point-to-Point Encryption) para este fim, o qual adiciona privacidade

dos dados ao Microsoft Dial-Up Networking. Uma versão de 40 bits é distribuída com o PPTP do Windows 95 e Windows NT, já possuindo uma versão de 128 bits. O MPPE criptografa pacotes IP na estação cliente antes de serem transmitidos pelo túnel PPTP. Quando o cliente faz a negociação PPP com o terminador túnel, inicia-se a sessão criptografada. O MPPE utiliza o MS-CHAP para fazer a autenticação do usuário.

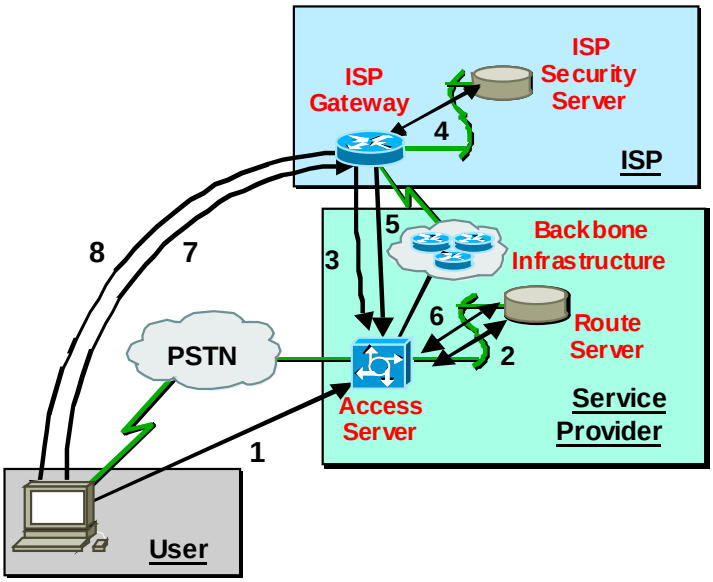
3.3.2 L2F (Layer 2 Forwarding)

Protocolo desenvolvido pela CISCO. Permite que clientes remotos façam a conexão e autenticação na rede da corporação através de um ISP ou NSP. Opera na camada 2, podendo multiplexar varias sessões do usuário em um único túnel L2F. A especificação do L2F aceita a criação do túnel tanto com conexões PPP como conexões SLIP. Ele utiliza o protocolo UDP para criação do canal de controle e sinalização da conexão. Foi um protocolo desenvolvido para configurar roteadores a serem implementados nas VPNs dos provedores de serviço, permitindo que estes mantenham o controle dos usuários. Caracteriza-se pela criação do túnel compulsório.

Quando um cliente faz uma conexão PPP com um NAS para a partir daí inicializar um túnel L2F com um servidor ou um ISP, são seguidos os passos descritos abaixo:

1) Usuário remoto inicia uma conexão PPP. O NAS aceita a chamada.
2) NAS identifica o usuário remoto.
3) NAS inicia o túnel L2F com o ISP solicitado.
4) ISP Gateway autentica o usuário remoto, aceitando ou rejeitando o estabelecimento do túnel.
5) ISP Gateway confirma a chamada e o túnel L2F.
6) NAS registra um log de concordância e de tráfego (opcional).
7) ISP Gateway negocia com o usuário remoto a conexão PPP. IP pode ser assinalado pelo ISP Gateway.
8) End-to-end túnel entre o usuário remoto e o ISP Gateway é criado.

Figura 7 – Túnel L2F

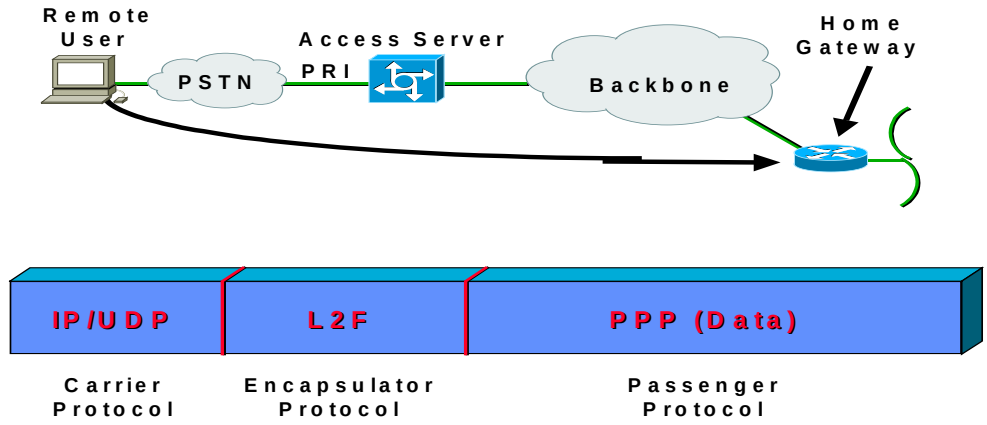


Fonte: SOUZA, **Karina Carneiro Campelo de**: Redes Privadas Virtuais**.**
UFPE, 2000

O objetivo do tunelamento de protocolo em nível 2 é o de transportar protocolos de nível 3 como AppleTalk, IP e IPX na Internet. Para conseguir isto, os projetistas do L2F utilizaram o protocolo de nível 2 PPP, o qual foi projetado para transportar diferentes protocolos de nível 3 em canais seriais. Nesse esquema, os pacotes de nível 3 são encapsulados em pacotes PPP, os quais são encapsulados em pacotes IP para serem transportados via Internet.

Uma vantagem é que o L2F não requer dos ISPs a tarefa de configuração dos endereçamentos e preocupação com o processo de autenticação. O L2F é um componente do Cisco's Internetwork Operating System (IOS), assim ele tem suporte em todos os devices de acesso e de conectividade de rede da CISCO.

Figura 8 – Formato do pacote L2F



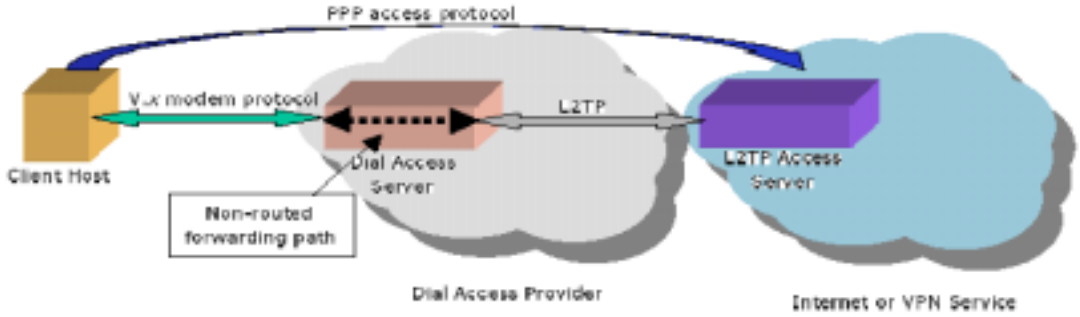
Fonte: SOUZA, **Karina Carneiro Campelo de**: Redes Privadas Virtuais**. UFPE, 2000**

3.3.3 L2TP (Layer 2 Tunneling Protocol**)**

Este protocolo nasceu da convergência técnica da especificação dos protocolos L2F e PPTP, ambos operam na camada 2. O L2TP oferece as melhores funções e características destes dois protocolos, além de benefícios adicionais como o túnel multiponto, o qual permite que um único cliente inicialize várias VPNs. Na prática um cliente remoto pode criar simultaneamente uma conexão para acessar uma aplicação de banco de dados da corporação e outra para acessar a intranet.

Enquadra-se na categoria de túnel compulsório. O provedor de serviço controla o local onde a sessão PPP irá terminar. Isto é importante para o caso em que o provedor, para quem o usuário está ligando (normalmente é disponibilizado um pool de modems), deve conduzir a sessão PPP de usuário para outra rede de maneira transparente. O usuário tem a nítida impressão de estar conectando-se diretamente à rede a qual pertence o servidor que ele deseja acessar.

Figura 9 - acesso dial-up L2TP



Fonte: FERGUSON, **Paul;** HUSTON**, Geoff.** What Is a VPN?**. Cisco Systems, Abril, 1998.**

Redes de grande porte podem terceirizar para provedores a disponibilização e manutenção das diversas portas de modem, que por sua vez irão transmitir o tráfego gerado pelos clientes para a rede a ser acessada. A maior motivação para esta configuração encontra-se na estrutura hierárquica existente para redes PSTN.

Existem implementações do L2TP que seguem o modelo de túnel voluntário, permitindo que o cliente inicialize o túnel. Não existe nada especificado no protocolo L2F que impeça a criação do túnel voluntário, assim como, o PPTP também tem sido usado, na especificação de alguns fabricantes, para a implementação do túnel compulsório.

O L2TP suporta qualquer protocolo roteado como o IP, IPX, Appletalk e qualquer tecnologia de backbone WAN (ATM, X.25, Frame Relay, SONET). Uma vantagem para sua implementação é o uso que é feito do PPTP, o qual por ser uma extensão do PPP, é um protocolo que já está incluído nas funcionalidades de acesso remoto do Windows 95/98/NT.

O L2TP e PPTP oferecem características adicionais que não estão disponíveis nos protocolos túnel da camada 3:

- Permite que a empresa escolha entre assumir o gerenciamento das funções de autorização do usuário, permissão de acesso e endereçamento da rede ou transferir estas responsabilidades para o NSP. Através dos pacotes PPP recebidos pelo túnel, os servidores da empresa têm acesso às informações sobre os usuários remotos, necessárias para a realização destas tarefas;

- Suporte a tecnologia do tunnel switch, o qual permite a facilidade de finalizar um túnel e inicializar outro com um subsequente terminador túnel. Ele estende a conexão PPP para um posterior end-point;

- Permite a aplicação de políticas de acesso no firewall e nos servidores internos. Como os terminadores túnel no firewall recebem pacotes PPP que possuem informações dos usuários, eles podem aplicar políticas de segurança específicas para o tráfego de diferentes fontes de origem. Como o tunnel switch inicializa um novo túnel na camada 2 com os servidores internos, podem ser criados níveis adicionais de controle de acesso.

- O endereço IP do pacote PPP é transparente para o endereço IP do Túnel.

- O PPTP, L2F e L2TP podem transportar múltiplos protocolos. Eles funcionam tanto em conexões LAN-LAN como em conexões discadas, abrangendo as aplicações mais comuns de VPN.

3.3.4 IPSec (IP Security Protocol)

A cada dia aumentam as exigências dos usuários por qualidade de serviços e segurança. Novas aplicações como audio e vídeo precisam trafegar na rede com uma certa prioridade. Para garantir o fluxo das informações e as novas exigências, algumas empresas, sob controle do IETF, especificaram o IPSec, considerado o padrão de segurança da VPN baseada no protocolo IP.

O IETF ("Internet Engineering Task Force") já publicou vários RFCs abrangendo parte do protocolo IPSec . Um aspecto interessante a ser comentado é que se o IPv6 vier a substituir o IPv4, o IPSec irá se tornar automaticamente o padrão de VPN da Internet já que ele está integrado às especificações do IPv6.

A especificação define um conjunto de protocolos que dá suporte aos requisitos de segurança exigidos por uma VPN IP, sendo considerado o padrão emergente de segurança na VPN. Como é uma função da camada 3, ele não pode fornecer serviços para outros protocolos da mesma camada, como o IPX e SNA. O IPSec oferece os meios necessários para garantir a confidencialidade, integridade e autenticidade dos pacotes IPs transmitidos e recebidos. Ele trabalha com uma variedade de esquemas padronizados e processos de negociação de criptografia, bem como, com vários sistemas de segurança (assinatura digital, certificado digital, infra-estrutura de chave pública). O padrão IPSec especificado pelo comitê do IETF, consiste em um conjunto de protocolos no nível IP que negociam os métodos de criptografia e assinatura digital a serem usados entre duas estações IP .

O IPSec encapsula o pacote IP original dentro de um novo pacote IP adequado aos cabeçalhos de autenticação e segurança, os quais contêm informações que serão usadas pelo destino no processo de negociação da segurança para autenticar e descriptografar o dado inserido no pacote. A autenticação e privacidade implementadas no IPSec é garantida através de cabeçalhos adicionais que seguem o cabeçalho principal de um pacote IP. O header adicional para a autenticação do tráfego IP é chamado de Authentication Header (AH) enquanto que o header para privacidade é chamado Encapsulating Security Payload (ESP) que define a criptografia para a parte de dados do IP.

O primeiro pacote IP dispara a negociação de segurança realizada entre o ponto de origem e o destino para estabelecimento do esquema de autenticação, criptografia e gerência de chaves. O protocolo padrão que realiza esta negociação é o ISAKMP/Oakley. Neste momento, as duas máquinas envolvidas no processo

estabelecem o método de autenticação e algoritmo de segurança a ser utilizado e geram uma chave compartilhada para a subsequente operação de criptografia dos dados. O IPSec Tunnel utiliza o método de segurança negociado para encapsular e criptografar os pacotes IPs e fazer uma transferência segura por uma rede privada ou pública. Os dados criptografados são encapsulados novamente com um cabeçalho IP no formato de texto plano. Quando o device finalizador do túnel IPSec receber o pacote, este último cabeçalho será descartado para em seguida fazer a descriptografia do seu conteúdo, recuperando o pacote IP original.

O IPSec foi desenhado para suportar múltiplos protocolos de encriptação, uma característica que permitirá aos seus usuários escolher o nível de segurança desejado. No próximo capítulo será descrita a arquitetura IPSEC.

3.4 Conclusões

O PPTP foi no início o protocolo de VPN mais popular. Atualmente ele perde espaço para outros protocolos como o L2TP e o IPsec. O L2TP implementa mecanismos de segurança, como autenticação e controle de integridade das mensagens transmitidas, mas não implementa criptografia. O princípio do L2TP consiste em encapsular pacotes PPP em datagramas UDP. Essa característica permite multiplexar várias conexões de VPN com um único endereço IP nas extremidades, variando o número das portas. Por esta razão, o protocolo L2TP é muito usado na implementação de VPN por roteadores.

O L2TP, não possui suporte a criptografia, e depende de outros protocolos para realizá-lo. O Internet Protocol Security (IPSEC) é uma extensão de segurança para o protocolo IP. Pode ser utilizado conjuntamente com o L2TP para prover criptografia. Ele suporta mecanismos de autenticação, tunelamento e criptografia através de cabeçalhos adicionais incluídos nos pacotes IP. Ao contrário do L2TP, o IPsec foi desenvolvidos exclusivamente para o protolo IP. O tunelamento do IPsec é de IP para IP, não suportando diretamente outros protocolos. Para transportar outros protocolos o IPsec deve ser combinado com o L2TP.

IPsec implementa autenticação e criptografia utilizando algoritmos por chaves como o DES. O IPsec define mecanismos para aplicar a criptografia mas não para gerenciar as chaves. O mecanismo que gerencia a distribuição de chaves é denominado ISAKMP (Internet Security Association and Key Management Protocol), é desenvolvido na forma de uma aplicação externa ao protocolo de rede. O Ipsec, propriamente dito, se comporta como um driver de placa de rede, que realiza mecanismos de criptografia e decriptogafia logo abaixo da camada IP .

4. ARQUITETURA IPSEC (IP Security Protocol)

Com a difusão da Internet comercial, Intranets, Extranets e aplicações Business to Business a utilização de VPNs e dos protocolos de rede que vem a oferecer maior segurança na comunicação tornaram-se uma opção interessante e peças estratégicas para implementar estes conceitos. Em função de termos muitos fabricantes oferecendo sua própria solução para VPNs em um mercado que por si só é heterogêneo há a necessidade de padronização do protocolo a ser utilizado.

O IPSEC (IP Secure) é um padrão de comunicação que se sobressaiu dentre outros, pois oferece a estrutura de segurança mais completa para VPNs. O IPSEC oferece conexão LAN-to-LAN e cliente-LAN. Além de ser um padrão aberto IETF que está sendo adotado por todos os fabricantes de equipamentos de redes e desenvolvedores de sistemas tornando-se o padrão de fato.

A plataforma IPSEC foi desenvolvida para prover serviços de segurança de alta qualidade, baseados em criptografia para o nível IP e/ou para as camadas superiores. O conjunto de serviços oferecidos inclui controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e criptografia.

Estes serviços são implementados através da utilização conjunta de protocolos de segurança de tráfego de dados, de autenticação de cabeçalho (AH – Autentication Header), de encapsulamento seguro do payload ou conteúdo dos dados (ESP – Encapsulating Security Payload) e de procedimentos e protocolos de gerência de chaves. Por definição o IPSEC possui uma arquitetura aberta no sentido de possibilitar a inclusão de outros algoritmos de autenticação e criptografia.

Pretende-se com este capítulo abordar conceitos do funcionamento da arquitetura IPSEC, identificar suas vantagens e a relevância deste protocolo para o modelo a ser proposto.

4.1 Protocolos AH e ESP

Os Protocolos AH (Authentication Header) e ESP (Encapsulating Security Payload) fazem parte da arquitetura básica IPSec e, por questões de garantia de interoperabilidade, estes protocolos estabelecem que todas as implementações IPSec suportam alguns algoritmos pré-definidos. Para autenticação de cabeçalho, os algoritimos obrigatórios são os seguintes:

- HMAC-MD5, RFC 2403 – **The Use of HMAC-MD5 within ESP and AH**;

- HMAC-SHA-1, RFC 2404 – **The Use of HMAC-SHA-1 within ESP and AH;**

para o encapsulamento seguro do payload, além dos algoritmos citados acima, outros algoritmos são:

- DES-CBC, RFC 2405 – **ESP DES-CBC Cipher Algorithm With Explicit IV**;

- **Null Authentication Algorithm**;

- **Null Encryption Algorithm.**

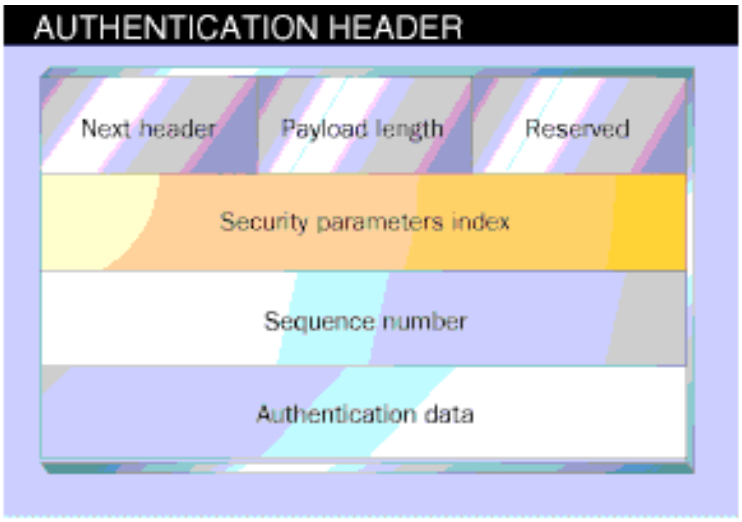
O protocolo AH tem as seguintes propriedades:

- Garante a integridade dos dados e autenticação;

- Define a autenticação para o tráfego IP (Verifica a autenticidade de um pacote IP).

Além disso, garante que o pacote não foi alterado durante a transmissão e quando utilizado, o header AH segue imediatamente o header IP.

Figura 10 – Formato do Header AH



O primeiro campo identifica o header do próximo campo; este é composto por 8 bits que informam qual o protocolo de nível mais alto (ex: UDP, TCP, ESP) que segue o AH. O “payload lenght” é um valor de 8 bits que indica o comprimento do campo de dados autenticado. A área reservada de 16 bits não é utilizada, sendo setada com zero.

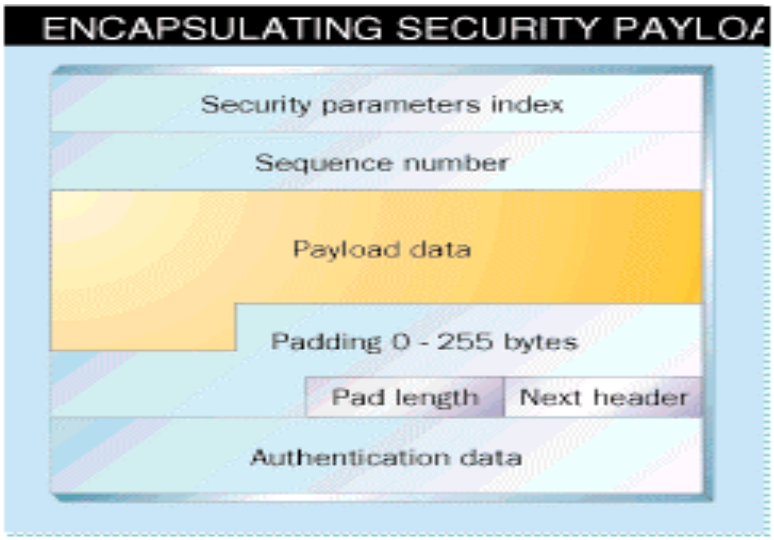
O Security Parameters Index (SPI) é um número de 32 bits que diz ao receptor quais protocolos de segurança que estão sendo utilizados. Esta informação inclui os algoritmos e chaves aplicados pelo device de origem.

O Sequence number informa quantos pacotes com os mesmos parâmetros configurados serão enviados. Este número trabalha como um contador, sendo incrementado cada vez que um pacote com o mesmo SPI é entregue para o mesmo endereço. No fim do AH está o dado autenticado, ou seja, uma assinatura digital para o pacote.

As propriedades do protocolo ESP (Encapsulation Security Payload) são as seguintes:

- Garante a privacidade (criptografia) e integridade.
- Define a criptografia para a parte de dados do pacote IP (payload)

Figura 11 – Formato do Header ESP



O ESP utiliza chave simétrica ou secreta e algoritmos de criptografia como o DES para criptografar o payload. O método default é o 56-bit DES e est protocolo é composto de várias partes. A primeira é o header de controle que contem o SPI e o número seqüencial que têm o mesmo propósito definido do header AH. Eles não são criptografados, mas são autenticados. As partes seguintes do ESP são criptografadas durante a transmissão.

O “payload data” pode ser de qualquer tamanho, sujeito ao limite normal do pacote IP. O Esp também contém de 0 a 255 bytes de padding, que garantem que o dado estará no tamanho correto para um determinado algoritmo de criptografia.

4.2 Gerenciamento de Chaves no IPSec

O gerenciamento de chaves pelo IPSec é feito pelo protocolo IKE(Internet Key Management), o qual é uma combinação do ISAKMP (Internet Security Association and Key Management Protocol) e o protocolo de Oakley . O primeiro é utilizado como moldura para prover os serviços de autenticação e permuta de chaves. O segundo descreve os vários modos de troca de chaves de criptografia. O IKE opera em duas fases. Na primeira, dois pares estabelecem um canal seguro para realizar as operações do ISAKMP. Na segunda, os dois pares negociam as autenticações de segurança (AS) de propósito geral.

O protocolo de Oakley provê três modos para a troca de informações de chaves e estabelecimento das AS ISAKMP. O modo principal (main mode) faz a fase um de troca do ISAKMP para estabelecimento de um canal seguro. O modo agressivo (agressive mode) é outra forma de realizar a fase um de troca. Este segundo modo é mais simples e rápido do que o modo principal, porém, não protege as identidades dos nós envolvidos na negociação, porque há a transmissão das identidades antes do estabelecimento de um canal seguro de comunicação. O modo rápido (quick mode) faz a segunda fase de troca negociando uma AS para comunicação do grupo em geral. O IKE possui ainda um outro modo, chamado Novo Grupo (New Group Mode), o qual não se ajusta à fase um ou dois. Ele segue a fase um de negociação e é utilizado para prover um mecanismo que define grupos privados para troca do tipo Diffie-Hellman.

4.3 Associação de Segurança

O conceito de Associação de Segurança – AS (Security Association – AS) é uma das partes fundamentais do IPSec. Segundo ZANAROLI (2000) “*uma associação de segurança é uma conexão que viabiliza o tráfego de serviços seguros*”. A segurança dos

serviços é garantida pela utilização dos protocolos de segurança. No caso da utilização conjunta dos dois protocolos, mais de uma AS deve ser definida.

Uma AS é identificada unicamente por três parâmetros:

- **SPI (Security Parameter Index)**: Número que identifica uma AS, sendo definido durante a negociação que antecede o estabelecimento da mesma. Todos os membros de uma associação de segurança devem conhecer o SPI correspondente e utiliza-lo durante a comunicação;

- **Endereço IP de Destino**: pode ser unicast, broadcast ou multicast. Porém, para o gerenciamento de AS, o IPSec assume um endereço destino unicast, estendendo as definições para o caso de broadcast e multicast;

- **Identificador de Protocolo:** é o número 51 para o AH e o número 50 para o ESP.

Uma AS pode ser estabelecida de duas maneiras diferentes: transporte ou túnel.

No modo transporte uma associação de Segurança é estabelecida entre dois hosts. Com o IPv4, o cabeçalho do protocolo de segurança é inserido entre o cabeçalho IP e os cabeçalhos dos protocolos de mais alto nível, como TCP ou UDP. Por outro lado, no IPv6, o cabeçalho do protocolo de segurança é inserido após o cabeçalho básico IPv6 e dos cabeçalhos de extensão end-to-end, e antes dos protocolos de mais alto nível.

No caso do ESP, uma AS em modo transporte provê serviços de segurança somente para os protocolos de mais alto nível, não incluindo o cabeçalho IP ou os cabeçalhos de extensão que precedem o ESP. No entanto, o AH estende a proteção a estes cabeçalhos. Isto se deve ao fato do ESP cifrar os dados que o sucedem no pacote, além de autenticar apenas a porção ESP do mesmo, enquanto o AH autentica o pacote todo.

Uma AS em modo túnel é aplicada a um túnel IP. Quando, pelo menos um dos membros de uma AS for um gateway de segurança, ou seja, implementa IPSec, então a AS deverá ser estabelecida em modo túnel.

Em uma AS no modo túnel, o chamado cabeçalho IP externo especifica o destino no contexto do IPSec, e o cabeçalho IP interno especifica o destino real do pacote IP. Neste caso, os cabeçalhos dos protocolos de segurança são inseridos depois do cabeçalho IP externo e antes do cabeçalho IP interno. Assim, de modo análogo às considerações feitas para o modo transporte, em modo túnel, o AH provê segurança para o cabeçalho IP externo, e conseqüentemente para os protocolos de mais alto nível, assim como para o pacote IP "tunelado". Vale ressaltar que quando o ESP é utilizado em modo túnel, apenas a segurança do pacote IP tunelado é assegurada.

O ponto chave para o IPSec tornar-se o protocolo padrão das VPNs é sua interoperabilidade. Por não especificar um método proprietário de autenticação e criptografia, ele trabalha com vários sistemas já padronizados no mercado. Além disso, o IPSec pode trabalhar em conjunto com outros protocolos de VPN. O L2TP pode fazer as funções de receber o pacote a ser transmitido, inicializar o túnel e transmitir o pacote encapsulado para o destino final; enquanto que o IPSec executaria as funções de negociação da criptografia e autenticação.

4.4 Conclusões

Com a explosão do e-commerce e o e-business surgiu o o IPSEC, que corresponde a um esforço de padronização da segurança na Internet. O IPSEC já é suportado nos Sistemas Operacionais mais atuais, como Windows 2000, e Linux.

De acordo com STALLINGS (2000), o IPSEC provê capacidade para garantir a segurança nas comunicações entre redes, tornando-o atraente para várias aplicações. As VPNs tem sido utilizadas para conectividade entre parceiros de negócios (extranet),

acesso remoto seguro, criação de sub-redes virtuais entre matrizes e filiais e o fortalecimento do comérico eletrônico em geral.

Segundo FERGUSSON (1998) O IPSEC possui como vantagem a sua flexibilidade quanto ao uso, pois pode residir em servidores, clientes móveis ou gateways seguros. Caso seja necessário estabelecer a identidade de toda e qualquer conexão, pode-se instalar o IPSEC em todos os computadores.

Um dos principais benefícios é que o IPSEC fica abaixo da camada de transporte (TCP, UDP), tornando-se totalmente transparente para as aplicações que dá suporte, sem exigir nenhuma mudança no software dos servidores, se o IPSEC for implementado em um firewall ou roteador. Cabe citar que, sendo implementado em um firewall ou roteador, o nível de segurança que pode ser obtido é extremamente alto, sem contar que tudo isso fica totalmente transparente para os usuários finais.

IPsec implementa autenticação e criptografia utilizando algoritmos por chaves como o DES. O IPsec define mecanismos para aplicar a criptografia mas não para gerenciar as chaves. O mecanismo que gerencia a distribuição de chaves é denominado ISAKMP (Internet Security Association and Key Management Protocol), é desenvolvido na forma de uma aplicação externa ao protocolo de rede. Segundo JAMHOUR (2000), o IPSEC, se comporta como um driver de placa de rede, que realiza mecanismos de criptografia e decriptogafia logo abaixo da camada IP .

O IETF ("Internet Engineering Task Force") já publicou vários RFCs abrangendo parte do protocolo IPSec . Um aspecto interessante a ser comentado é que se o IPv6 vier a substituir o IPv4, o IPSec irá se tornar automaticamente o padrão de VPN da Internet já que ele está integrado às especificações do IPv6.

Pela facilidade de implementação e por ter sido adotado pela maioria dos fabricantes de equipamentos seria um protocolo interessante a ser utilizado para implementar VPNs na Universidade do Contestado.

5. PROPOSTA PARA IMPLEMENTAÇÃO DE VPNs NA UnC

A necessidade da Reitoria da Universidade do Contestado consolidar informações acadêmicas e administrativas dentro do menor espaço de tempo possível é um ponto de fundamental importância para a área administrativa da instituição.

Através do grupo que gerencia os setores de tecnologia da informação da Universidade, composto pelos administradores destes mais o analista de suporte da Reitoria, foi proposta a adoção de um sistema único para gerenciar os dados acadêmicos dos cinco campi. O sistema seria composto de um banco de dados local (em cada campus) e um datawarehouse na reitoria, consolidando as informações de todos os campi e apresentando uma visão da Universidade como um todo.

A utilização de VPNs na Universidade do Contestado teria inicialmente como foco principal a criação de caminhos seguros para a passagem dos dados do sistema acadêmico dos campi até a Reitoria, consolidando esta informação com segurança. Num segundo momento, poderia-se utilizar Voz sobre IP através desta VPN para redução dos custos de comunicação entre as unidades. Este é um projeto piloto de integração que possibilitará avaliar a possibilidade de integrar toda a estrutura da UnC através de uma rede Wireless com segurança, interligando várias RMAVs, as quais já estão em fase de consolidação. O fator custo é outro indicador positivo para a utilização de VPNs, pois a contratação de LPs para fazer a interligação dos campi com a reitoria não seria justificável sendo que a instituição possui equipamentos que fazem este procedimento a custo zero, dependendo apenas da configuração.

Para que isto seja possível, o responsável pela implementação de uma VPN corporativa deverá escolher o tipo de protocolo e equipamentos a serem utilizados, levando em consideração alguns requisitos funcionais.

A confidencialidade, transparência e baixo custo, juntamente com a possibilidade de utilização de hardware já existente na instituição justificam a adoção das VPNs para a interligação da instituição.

Neste capítulo apresentarei uma análise destes requisitos de acordo com a realidade da instituição para a correta escolha do protocolo a utilizar no modelo e à partir desta definir qual arquitetura utilizar para a implementação de VPNs na estrutura da UnC.

5.1 Universidade do Contestado – UnC – Um estudo de Caso

A Universidade do Contestado – UnC é uma Universidade multicampi composta de cinco campi universitários e a Reitoria, sendo que os campi ficam localizados nas cidades de Caçador, Canoinhas, Concórdia, Curitibanos e Mafra. A Reitoria tem sede na cidade de Caçador.

A UnC adquiriu recentemente um sistema de gestão acadêmica, o qual funciona sobre a plataforma Windows, utilizando o banco de dados Microsoft SQL Server. Cada campi tem o seu banco de dados local e o objetivo é alimentar o datawarehouse da Reitoria pelo menos uma vez ao dia.

A principal motivação para a implementação de VPNs nesta estrutura é financeira pois links dedicados são caros, principalmente quando as distâncias são grandes. As VPNs possibilitam a utilização de uma rede pública como uma rede privada, e serão a base para a interligação da instituição, reduzindo os custos de comunicação interna e externa, expandindo a infraestrutura da rede corporativa, contribuindo também para a modificação de alguns conceitos de desenvolvimento de sistemas. O baixo custo da Internet é uma das principais vantagens em comparação às WANS tradicionais.

Além da interligação dos campi universitários a VPN pode futuramente ser utilizada para a disponibilização de uma extranet, possibilitando aos parceiros acesso a aplicações internas e dados , também pode ser utilizada para tráfego de voz sobre IP, com segurança, reduzindo os custos mensais de telecomunicações.

A interligação da Universidade através de redes virtuais privadas está prevista para 2003, após a implantação do software em todos os campi e a instalação do Datawarehouse na Reitoria.

5.1.1 Possibilidades de Implementação

Através do levantamento do hardware existente nos Campi, e tendo como base o equipamento que a instituição possui, existem duas possibilidades de ligação destes sites: VPNs com arquitetura IPSec implementada sobre roteadores ou firewalls.

5.1.1.1 VPNs com IPSec utilizando Roteadores

A utilização de um Roteador para a configuração de VPNs é interessante já que todo o tráfego internet passa obrigatoriamente por ele e o mesmo trata cada pacote que deixa a LAN.

De posse da especificação do hardware existente nos campi, verificamos que todos possuem roteadores CISCO com as seguintes características:

- Campus Caçador: possui um roteador CISCO 2600;
- Campus Curitibanos: possui um roteador CISCO 1700;

- Campus Concórdia: possui um roteador CISCO 2600;

- Campus Canoinhas: possui um roteador CISCO 2600;

- Campus Mafra: possui um roteador CISCO 2600;

- A reitoria está ligada ao Campus Caçador.

- IPSec: um padrão aberto que fornece o confidencialidade, integridade e autenticação entre os pontos de ligação. Fornece serviços de segurança na camada do IP; usa IKE para assegurar a negociação dos protocolos e dos algoritmos baseados na política local, e gerar as chaves do criptografia e de autenticação a serem utilizadas. Pode ser usado para proteger um ou mais conjuntos de dados entre um par de hosts, entre um par de gateways seguros, ou entre um gateway seguro e um host.

- IKE: Uma combinação do ISAKMP (Internet Security Association and Key Management Protocol) e o protocolo de Oakley . O primeiro é utilizado como moldura para prover os serviços de autenticação e permuta de chaves. O segundo descreve os vários modos de troca de chaves de criptografia. Quando o IKE for utilizado com outros protocolos, sua negociação inicial é com o protocolo IPSEC. Provê autenticação para os pontos IPSec, negocia as associações de segurança e estabelece as chaves IPSec.

- DES: Data Encription Standard é utilizada para criptografar pacotes de dados. O IOS Cisco implementa como padrão o DES-CBC 56 bit. Implementa também criptografia 3DES (168 bit) , dependendo da versão do software e da plataforma específica. 3DES é uma forma extremamente segura de criptografia que permite que informações confidenciais sejam transmitidas sobre redes públicas.

- AH: Authentication Header. Um protocolo de segurança que provê autenticação de dados.

- ESP: Encapsulating |Securit Payload. Um protocolo de segurança que prove serviço de privacidade de dados e uma opcional autenticação de dados. Os dados são encapsulados para serem protegidos.

5.1.1.2 VPNs com IPSec utilizando Firewalls

Um Firewall, assim como o roteador, examina e processa todo o tráfego IP, baseado em filtros e políticas de segurança configurados nele. Em função do volume de processamento realizado em um firewall, o mesmo não é aconselhado para tunelamento de grandes redes ou de redes com um grande volume de tráfego. A combinação de tunelamento e criptografia aplicada a um firewall é voltada para redes pequenas, com pouco tráfego.

No caso da UnC, poderíamos inicialmente utilizar Firewalls para implementar VPNs, mas a curto prazo esta solução deveria ser revista em função de novos serviços serem implementados na VPN. Portanto, pensando numa solução que venha a atender as necessidades da instituição a médio e curto prazo, a VPN será implementada em roteadores.

5.2 Análise dos protocolos de tunelamento

Conforme estudo realizado no capítulo 2, citei os diversos protocolos de tunelamento, os quais trabalham sobre as diferentes camadas do modelo de referência OSI. Conforme RODGERS (2000), existe um conjunto de características desejáveis para um mecanismo de tunelamento de redes virtuais privadas, que incluem o seguinte:

- ✓ Multiplexação: para casos em que múltiplas conexões (túneis) VPN são necessários para um mesmo end-point.

- ✓ Protocolos de Sinalização: O estabelecimento de um túnel pode ser alcançado de duas maneiras: por uma operação de gerenciamento ou por um protocolo de sinalização, o qual suporta a criação de túneis dinâmicos. A utilização de protocolos de sinalização é essencial para a resolução de problemas em muitos cenários, como uma alternativa à imposição de uma sobrecarga administrativa. O protocolo de sinalização pretende simplificar sobremaneira o processo de configuração necessário toda a vez que uma VPN interliga vários domínios administrativos.

- ✓ Segurança de dados: Um protocolo de tunelamento deve prover suporte para vários requisitos de segurança, incluindo autenticação e criptografia. Se túneis são estabelecidos dinamicamente, são necessários para autenticar o requisitante para o estabelecimento do mesmo.

- ✓ Transporte de Múltiplos Protocolos: Muitas VPN´s necessitam transmitir vários protocolos entre sites, então o protocolo de tunelamento deve facilitar o transporte deste tráfego através desta característica.

- ✓ Seqüência de Quadros: a habilidade de ordenar pacotes numa stream de dados pode ser necessária para suportar operações mais detalhadas sobre protocolos VPN ou aplicações. Do mesmo modo, o processo deve exigir que o mecanismo de tunelamento suporte uma ordenação dos campos.

- ✓ Manutenção do Túnel: É necessário para Túneis end-points, com o intuito de monitorar túneis já estabelecidos assegurando que a conectividade não será perdida. Isto pode ser alcançado com a checagem periódica da banda de entrada (in-band), ou através do uso de alguns mecanismos out-of band para detectar a perda da conectividade.

- ✓ Suporte para grandes MTUs (Maximum Transmittable Unit): Se a MTU do túnel é maior que a MTU de um ou mais pontos através do caminho do túnel, fragmentação pode ser necessária dentro do mesmo, a qual pode criar obstrução no túnel. Preferivelmente, o protocolo de tunelamento deve prover fragmentação e serviços de reunião no fim do túnel, para que o tráfego possa fluir facilmente através dele.

- ✓ QoS/ Gerenciamento de tráfego: Clientes VPN exigem um comportamento específico para a rede, como latência assegurada, largura de banda e perda de velocidade. A garantia de entrega (QoS) geralmente é de responsabilidade dos pontos VPN e dos backbones (infraestrutura) de rede.

Com base nos requisitos acima, analisamos a tabela à seguir:

Tabela 1- Características dos protocolos de tunelamento.

Requisitos/ Características	**PROTOCOLOS DE TUNELAMENTO**				
	L2TP	GRE	IP/IP	IPSEC	MPLS
MULTIPLEXAÇÃO	✓	~	X	✓	X
SINALIZAÇÃO	✓	✓	X	✓	~
SEGURANÇA DE DADOS	X	X	X	✓	~
TRANSPORTE DE MULTIPLOS PROTOCOL OS	✓	✓	X	~	✓
SEQUENCIA DE QUADROS	✓	✓	X	~	X
MANUTENÇÃO DO TÚNEL	✓	~	~	~	~
SUPORTE DE GRANDES MTUs	X	X	X	X	X
QOS/GERENCIAMENTO DE TRÁFEGO	X	X	X	X	✓

LEGENDA
✓ Suporta
X Não suporta
~ Suportado através de extensões

Fonte: RODGERS, **Chris;** HUNT, **Ray:** Virtual Private Networks – Strong Security at What Cost? **2001.**

De acordo com a tabela acima podemos definir qual (ou quais) protocolo será utilizado para a implementação de VPNs sobre a estrutura da UnC. O primeiro requisito é que haja a possibilidade de multiplexação, ou seja, a ligação devários túneis num mesmo destino (5 campus ligados na reitoria). Sendo assim, dois protocolos de tunelamento atendem a este requisito. São eles o L2TP e o IPSEC.

O segundo e o mais importante requisito é a segurança de dados (criptografia, autenticação). Como o L2TP não atende ao requisito de segurança, o IPSEC deverá ser utilizado. Os cinco campi da UnC utilizam o protocolo TCP/IP e o IPSec é uma extensão de segurança para este protocolo. Caso houvesse a necessidade de transporte de outro protocolo, como o IPX da Novell, o IPSec poderia ser utilizado em conjunto com o L2TP para executar esta tarefa, já que o L2TP possui a característica de transportar múltiplos protocolos.

5.3 Proposta de um modelo para implementação de VPNs sobre a estrutura da UnC

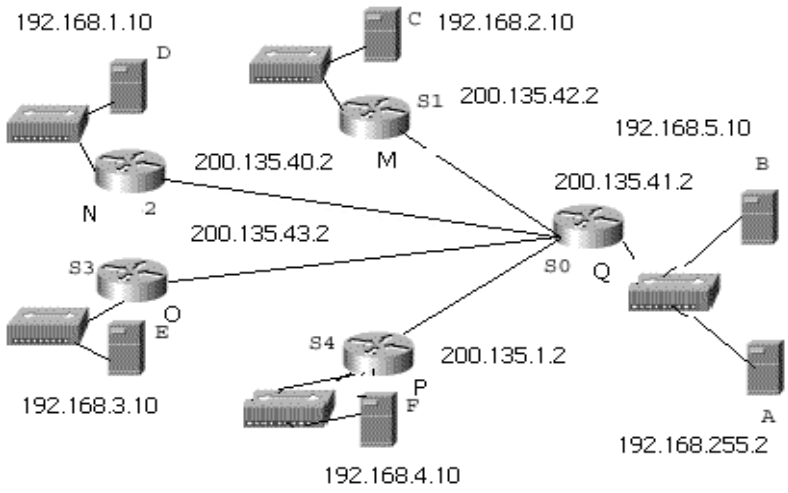
Através da utilização do protocolo IPsec, objetiva-se prover túneis seguros entre os campi e a reitoria. A configuração feita nos roteadores definirá quais pacotes serão criptografados e quais passarão de forma normal entre os pontos. Os túneis são conjuntos de associações de segurança que serão estabelecidas entre dois pontos através do IPSec. A associação de segurança definirá quais protocolos e algoritmos serão aplicados sobre os pacotes e também especifica a chave que será utilizada entre os dois pontos. A Associação de segurança é unidirecional e é estabelecida pelo protocolo de segurança (AH ou ESP).

Nos roteadores Cisco podemos especificar qual tráfego será protegido entre dois pontos IPSec configurando listas de acesso e aplicando estas listas a interfaces através de conjutos de crypto maps.

Um Crypto Map pode conter múltiplas entradas cada uma com uma lista de acesso diferente.

Para exemplificar uma ligação de um Campus à Reitoria, deveremos ter uma lista de acesso que conterá o endereço de origem e destino para a ligação. Através da figura 14, faremos a ligação do host D até o Host A.

Fig. 12 - Proposta de VPN utilizando Roteadores CISCO



Primeiramente, deveremos configurar as associações de segurança para através do IKE no Roteador do Campus Caçador para todos os pontos.

Exemplo: Políticas IKE definida para os pontos:

Crypto isakmp policy 4

Authentication pre-share

Em seguida, devemos especificar as chaves compartilhadas para os diferentes pontos:

Crypto isakmp key xxxxxx1111 address 200.135.42.2
Crypto isakmp key xxxxxx1111 address 200.135.40.2
Crypto isakmp key xxxxxx1111 address 200.135.43.2
Crypto isakmp key xxxxxx1111 address 200.135.1.2

Através da configuração acima especificamos que utilizaremos o IKE para estabelecer o gerenciamento das chaves.

A configuração à seguir define o tipo de algoritmo de criptografia a ser utilizado nos pacotes e o tipo de autenticação:

Crypto ipsec transform-set encrypt-des esp-des

Em seguida, devemos configurar o ponto, os transform-sets e o tráfego criptografado para os pontos dos túneis.

Crypto map combined local-address serial0
Crypto map combined 20 ipsec-isakmp
Set peer 200.135.40.2
Set transform-set encrypt-des
Match address 105
Crypto map combined 30 ipsec-isakmp
Set peer 200.135.42.2
Set transform-set encrypt-des
Match address 106
Crypto map combined 40 ipsec-isakmp
Set peer 200.135.43.2
Set transform-set encrypt-des
Match address 107
Crypto map combined 50 ipsec-isakmp
Set peer 200.135.1.2
Set transform-set encrypt-des

Match address 108

Interface serial0

Ip address 200.135.41.2 255.255.255.?

No ip direct-broadcast

Ip nat outside

No ip route-cache

No ip mroute-cache

No fair-queue

No cpd enable

Crypto map combined

Interface FastEthernet0

Ip address 192.168.255.1 255.255.255.0

No ip direct-broadcast

Ip nat inside

No cdp enable

Após a criação dos crypto maps, ou seja, da especificação dos pontos/túneis que fazem parte da Rede Virtual Privada, definiremos o tráfego que passara pelo NAT:

Ip nat inside source route-map nonat interface serial0 overload

Finalizando a configuração, serão definidas as listas de controle de acesso para o tráfego que deverá passar ou não pelo túnel.

a) Tráfego criptografado passa pelo túnel:

Access-list 105 permit ip 192.168.255.0 0.0.0.255 192.168.1.0 0.0.0.255

Access-list 106 permit ip 192.168.255.0 0.0.0.255 192.168.2.0 0.0.0.255

Access-list 107 permit ip 192.168.255.0 0.0.0.255 192.168.3.0 0.0.0.255

Access-list 108 permit ip 192.168.255.0 0.0.0.255 192.168.4.0 0.0.0.255

Ou

Access-list 105 permit ip 192.168.255.2 255.255.255.0 192.168.1.10 255.255.255.0

Access-list 106 permit ip 192.168.255.2 255.255.255.0 192.168.2.10 255.255.255.0

Access-list 107 permit ip 192.168.255.2 255.255.255.0 192.168.3.10 255.255.255.0

Access-list 108 permit ip 192.168.255.2 255.255.255.0 192.168.4.10 255.255.255.0

b) Evita que o tráfego que utiliza NAT passe pelo túnel

Access-list 150 deny ip 192.168.255.0 0.0.0.255 192.168.1.0 0.0.0.255

Access-list 150 deny ip 192.168.255.0 0.0.0.255 192.168.2.0 0.0.0.255

Access-list 150 deny ip 192.168.255.0 0.0.0.255 192.168.3.0 0.0.0.255

Access-list 150 deny ip 192.168.255.0 0.0.0.255 192.168.4.0 0.0.0.255

Ou

Access-list 150 deny ip 192.168.255.2 255.255.255.0 192.168.1.10 255.255.255.0

Access-list 150 deny ip 192.168.255.2 255.255.255.0 192.168.2.10 255.255.255.0

Access-list 150 deny ip 192.168.255.2 255.255.255.0 192.168.3.10 255.255.255.0

Access-list 150 deny ip 192.168.255.2 255.255.255.0 192.168.4.10 255.255.255.0

c) Desvia o tráfego NAT do túnel.

Access-list 150 permit ip 192.168.255.0 0.0.0.255 Any

Ou

Access-list 150 deny ip 192.168.255.2 255.255.255.0 Any

d) Não faz NAT com o tráfego IPSec

Route-map nonat permit 10

Match ip address 150

Tomando como exemplo a o roteador de Canoinhas, a configuração do mesmo seria a seguinte:

Em todos os pontos, deve ser definida as políticas IKE:

Crypto isakmp policy 4

Authentication pre-share

Em seguida, devemos especificar as chaves compartilhadas para o acesso à Reitoria:

Crypto isakmp key xxxxxx1111 address 200.135.41.1

Caso necessário, pode-se estabelecer a troca de chaves para acesso aos outros campi:

Crypto isakmp key xxxxxx1111 address 200.135.40.2

Crypto isakmp key xxxxxx1111 address 200.135.43.2

Crypto isakmp key xxxxxx1111 address 200.135.1.2

A configuração a seguir define o tipo de algoritmo de criptografia a ser utilizado nos pacotes e o tipo de autenticação:

Crypto ipsec transform-set encrypt-des esp-des

Crypto ipsec transform-set to_reitoria esp-des

Em seguida , devemos configurar o ponto, os transform-sets e o tráfego criptografado para o túnel.

Crypto map combined local-address serial0

Crypto map combined 7 ipsec-isakmp

Set peer 200.135..41.2

Set transform-set encrypt-des

Match address 105

Interface serial 0

Ip address 200.135.42.2 255.255.255.?

No ip directed-broadcast

No ip route-cache

Ip nat outside

Crypto map combined

Interface FastEthernet0

Ip address 192.168.255.1 255.255.255.0

No ip direct-broadcast

Ip nat inside

No cdp enable

Após a criação dos crypto maps, ou seja, da especificação dos pontos/túneis que fazem parte da Rede Virtual Privada para ligação à Reitoria, definiremos o tráfego que passará pelo NAT:

Ip nat inside source route-map nonat interface serial0 overload

Finalizando a configuração, serão definidas as listas de controle de acesso para o tráfego que deverá passar ou não pelo túnel.

e) Tráfego criptografado passa pelo túnel:
Access-list 105 permit ip 192.168.2.0 0.0.0.255 192.168.255.0 0.0.0.255
Ou
Access-list 105 permit ip 192.168.2.10 255.255.255.0 192.168.255.2 255.255.255.0

f) Evita que o tráfego que utiliza NAT passe pelo túnel

Access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.255.0 0.0.0.255

Ou

Access-list 150 deny ip 192.168.2.10 255.255.255.0 192.168.255.10 255.255.255.0

g) Desvia o tráfego NAT do túnel.

Access-list 150 permit ip 192.168.2.0 0.0.0.255 Any

Ou

Access-list 150 deny ip 192.168.2.2 255.255.255.0 Any

h) Não faz NAT com o tráfego IPSec

Route-map nonat permit 10

Match ip address 150

O tráfego entre os servidores 192.168.2.10 e 192.168.255.2 ou entre as redes 192.168.2.0 e 192.168.255.0 está protegido entre os roteadores N S2 e Q S0.

6. CONCLUSÕES DO MODELO PROPOSTO

O modelo proposto para a interligação da instituição possibilitará o envio das informações de forma segura entre os campi e a Reitoria, efetivando estas para que o administrador possa investigá-las e utilizá-las para a tomada de decisões.

É uma solução viável nos aspectos financeiro e qualitativo perante outras possíveis soluções. Oferece uma considerável redução de custos pois não há a necessidade de adquirir e configurar linhas de dados e interfaces WAN para cada site.

É um modelo flexível, o qual pode ser adaptado para futuras aplicações de forma transparente ao usuário final. Possui fácil escalabilidade com o mínimo esforço. Não há a necessidade de um especialista técnico para cada site. Através de um conjunto de comandos um roteador extranet é configurado para conectividade VPN e Internet, podendo, de acordo com os objetivos futuros da instituição, criar conexões interistitucionais, para facilitar o relacionamento com parceiros em projetos específicos.

O modelo permite também o isolamento seletivo do canal de comunicação, aplicando criptografia transparente, utilizando algoritmos fortes como o DES.

As perspectivas futuras na área de VPNs são promissoras. Através do estudo realizado, ainda há a possibilidade de:

a) - Estudar a problemática e Implementar VPNs sobre o Protocolo IPV6;

b) - Aprofundar os conhecimentos sobre Wireless e VPNs sobre estas arquiteturas;

c) - Interligar as diversas RMAVs da Universidade do Contestado através de uma estrutura Wireless utilizando VPNs para tráfego corporativo;

RERÊNCIAS BIBLIOGRÁFICAS

ABELÉM, Jorge G.; **STANTON,** Michael A.; **RODRIGUEZ,** Noemi: **QoS Fim a Fim através da Combinação entre serviços integrados e serviços diferenciados.** PUC, Rio de Janeiro, 2001. Disponível em: http:// **www.inf.puc-rio.br/~abelem/mcc06_2001.pdf**. Acesso em: 12 fev. 2002.

ALTERSON, Gary: **Comparing BGP/MPLS and IPSec VPNs.** Sans Institute, 2002. Disponível em: **http://rr.sans.org/encryption/mpls2.php**. Acesso em: 12 jan. 2002.

BLAKELY, J.; **HOLLEY**, J.; **SOOTER,** M.: **Critical considerations for LAN-to-LAN Virtual Private Networks.** 2000. Disponível em: http://**198.11.21.25/capstoneTest/Students/ Papers/docs/prceed35124.pdf0.** Acesso em 10 ago. 2001.

BORT, Julie: **Tunneling for Dollars: Comparing IPSec and PPTP for extranet security.** Intranet Journal, 29 Abr. 2001. Santa Clara, Califórnia. Disponível em: **http://www.intranetjournal.com/foundation/tunneling.shtml**. Acesso em 25 jul. 2001.

CASTRO, Antonio Pires de; **RIOS**, Alexandre Theotonio T.; **FONSECA**, Nelson Luis S.: **Alocação de recursos para redes Virtuais Privadas em redes baseadas em Switchlets**. UNICAMP, 2001.

CHIN, Liou Kuo: **Rede Privada Virtual**. News Generation, Volume 2, número 8. RNP 1998. Disponível em: **www.rnp.br/newsgen/9811/vpn.shtml.** Acesso em 08 ago. 2001.

CISCO SYSTEM: A comparison between Ipsec and Multiprotocol Label

Switching Private Networks. Cisco, 2000. Disponível em: http://www.cisco.com/offer/sp/pdfs/vpn/SOLMK_WPfinal.pdf. Acesso em 28 dez. 2001.

CISCO SYSTEMS: **A Primer for Implementing a Cisco Virtual Private Network**. 1999. Disponível em: http://www.cisco.com/warp/public/cc/so/ neso/vpn/vpne/vpn21_rg.htm. Acesso em 13 ago. 2001.

CISCO SYSTEMS: **Configuring a Router IPSec Tunnel Private-to-Private network with NAT and a Static**. 2001. Disponível em: http://www.cisco.com/warp/public/707/static.html. Acesso em 15 abr. 2002.

CISCO SYSTEMS: How NAT Works. 1999. Disponível em http://www.cisco.com/warp/public/556/nat-cisco.shtml. Acesso em: 12 ago. 2001.

CISCO SYSTEMS: Intranet and Extranet Virtual Private Networking. 2001. Disponível em: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/ievpn_rg.html. Acesso em: 22 abr. 2002.

CISCO SYSTEMS: **IPSec Router-to-Router, Pre-shared, NAT Overload Between a Private and Public Network**. 2001. Disponível em: http://www.cisco.com/warp/public/707/overload_public.html. Acesso em 15 abr. 2002.

DAMASCENO, Sérgio: **A fonte que não seca**. Teletime, Rio de Janeiro, Ano 4, nº 38, Nov. 2001. Disponível em: http://www.teletime.com.br/revista/38/especial.htm. Acesso em: 08 jan.

2002.

ETHIER, Patrick: **ISAKMP and IPSec in the VPN environment.** 2000. Disponível em: **http://www.secureops.com/vpn/ipsecvpn.html**. Acesso em 15 abr. 2002.

FERGUSON, Paul; **HUSTON**, Geoff. **What Is a VPN?**. Cisco Systems, Abril, 1998. p.1 – 22. Disponível em: http:// **www.employees.org/~ferguson/vpn.pdf**. Acesso em: 06 set. 2001.

FRASER, Moye: **Understanding Virtual Private Networks (VPN)**. Sans Institute, Março.2001. Disponível em http://www.sans.org/infosecFAQ/encryption/undestanding_VPN.htm. Acesso em: 28 Jul. 2001.

HALPERN, Jason: **SAFE VPN – IPSec Virtual Private Networks in Depth.** Cisco System, 2001. Disponível em: **http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm**. Acesso em: 27 abr. 2002.

LAURENT, Ashley. **VPCom Firewall & VPN Gateway – Configuring the VPN** , 2000 p.1 – 18. Disponível em: **http://www.ashleylaurent.com**. Acesso em 04 ago. 2001.

LAURENT, Ashley. **VPCom Firewall & VPN Gateway – Configuration & Conceptual Overview**, 2000 p.1 – 12. Disponível em: **http://www.ashleylaurent.com**. Acesso em 04 ago. 2001.

RODGERS, Chris; **HUNT,** Ray: **Virtual Private Networks – Strong Security at What Cost?** 2001. Disponível em: http://www.cosc.canterbury.ac.nz/research/reports/ HonsReps/2001/hons_0109.pdf

Acesso em 04 jan. 2002

ROSSI, Marco Antônio G.; **FRANZIN,** Oswaldo: **VPN – Virtual Private Network – Rede Privada Virtual.** ASP Systems, Ago. 2000. Disponível em: http://www.gpr.com.br/cursos/vpn/vpn.html. Acesso em: 29 ago. 2001.

SILVA, Adailton; **CICILINI,** Renata: **Arquitetura IP Security – Parte 1.** News Generation, Volume 2, número 8. RNP 1998. Disponível em: http://www.rnp.br/newsgen/9907/ipsec3.shtml**.** Acesso em 08 ago. 2001.

SOUZA, Karina Carneiro Campelo de**: Redes Privadas Virtuais**. UFPE, 2000, p. 1-51.

SOLIS, Bertha; **TRAN,** Tam; **MUBENGA,** Anne; et al.: **Virtual Private Network.** 2001. Disponível em: http://ouray.cudenver.edu/~bjsolis/VPN.doc. Acesso em 20 abr. 2002.

ZANAROLI, Ana Paula Cossich Pereira; **LIMA**, Maria Beatriz Marques Fiúza; **RANGEL,** Rodrigo de Araújo Lima: **Virtual Private Networks**, 2000, Rio de Janeiro. Disponível em: http://www.cefet-rj.br/ensino/engenharia/redeslocais/trabalhos/0200/vpn/vpn.html