ANDRÉ LUIZ NASSERALA PIRES

USO DA TECNOLOGIA VPN NO GERENCIAMENTO A DISTANCIA DE EMPREENDIMENTOS DE ENGENHARIA

Dissertação apresentada ao Programa de Pós-graduação em Engenharia Civil da Universidade Federal Fluminense, como pré-requisito para obtenção do Grau de Mestre. Área de Concentração: Tecnologia da Construção.

Orientador: Prof. Dr. CARLOS ALBERTO PEREIRA SOARES

Niterói

2010

ANDRÉ LUIZ NASSERALA PIRES

USO DA TECNOLOGIA VPN NO GERENCIAMENTO A DISTANCIA DE EMPREENDIMENTOS DE ENGENHARIA

Dissertação apresentada ao Programa de Pós-graduação em Engenharia Civil da Universidade Federal Fluminense, como pré-requisito para obtenção do Grau de Mestre. Área de Concentração: Tecnologia da Construção.

Aprovada em 24 de fevereiro de 2010

BANCA EXAMINADORA

Prof. Carlos Alberto Pereira Soares, D.Sc.
Universidade Federal Fluminense

Prof. Orlando Celso Longo, D.Sc.
Universidade Federal Fluminense

Prof. Ricardo Bezerra Cavalcante Vieira
Universidade Federal do Estado do Rio de Janeiro

Niterói
2010

AGRADECIMENTOS

Gostaria de agradecer a todos os que colaboraram de alguma forma com a confecção deste trabalho. Em especial, gostaria de agradecer ao meu orientador, o Prof. Dr. Carlos Alberto Pereira Soares e a outros que me ajudaram de várias formas a alcançar os objetivos propostos.

Gostaria de agradecer também a minha esposa Camila Almeida de Souza, pela paciência e incentivo, e ao amigo Gilberto Angelucci, pela colaboração fundamental, aos meus pais Assis Dantas Pires e Nasserina Antonia Nasserala Pires, pelo dom da vida e ensinamentos que me tornaram o homem que sou hoje, Finalizando, aos meus filhos Luiz André e o que está em gestação.

“É preciso ter a coragem de seguir o seu coração e sua intuição, eles, de alguma maneira, já sabem o que você realmente deseja se tornar, todo o resto é secundário”, Steve Jobs.

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

SUMÁRIO

RESUMO

O presente trabalho procura mostrar a importância de se ter um controle preciso dos projetos executados pela ELETROBRÁS – Distribuição Acre, através da tecnologia VPN, bem como uma analise pós implantação dos sistemas. VPN é uma tecnologia que se liga à rede de computadores através da internet de forma a trabalhar como se estivesse presente na central de dados, com isso economiza tempo, gastos com movimentação de pessoal e equipamentos, assim como implantação de sistemas dedicados, que oneram os projetos. Vimos durante o processo que houve uma certa resistência por parte dos gestores e usuários do sistema por não conhecerem a fundo a tecnologia, apesar de ser um sistema confiável e seguro, uma novidade sempre é impactante, como por exemplo houve quem se sentisse desconfortável com os dados que eram apresentados, as duvidas foram sanadas após testes e analises, a mudança de confiança foi de “indiferente” para “satisfeito” ou “totalmente satisfeito” de acordo com pesquisa de satisfação entre os gestores e usuários.

Palavras-chave: VPN, projetos, confiável, impactante

ABSTRACT

This work shows the importance of having precise control of the projects executed by ELETROBRÁS - Distribution Acre, through the VPN technology and a post implementation review of systems. VPN is a technology that connects to the computer network via the Internet in order to work as if he were present in the data center, thus saving time spent on movement of personnel and equipment as well as deployment of dedicated systems, that tax projects. During the process there was some resistance from managers and users of the system by not knowing in depth the technology, despite being a reliable and safe, a novelty is always striking, for example some people feel uncomfortable with data that were presented, the doubts have been removed after testing and analysis, the change in confidence was "indifferent" to "satisfied" or "completely satisfied" according to a survey of satisfaction among managers and users.

Keywords: VPN, projects, confident, impactful

1 INTRODUÇÃO

1.1 APRESENTAÇÃO

O grande sucesso de um projeto está em seu gerenciamento, ou seja, está na rapidez e confiabilidade dos dados nele contidos. A confiabilidade é diretamente ligada ao gerente do projeto, assim como a exatidão dos dados, já a rapidez muitas vezes esbarra na distância física entre o projeto que está sendo executado e o acesso as ferramentas de TI usadas para essa finalidade. Até algum tempo atrás, a construção civil brasileira, tinha a gerência de suas obras feitas manualmente, atualmente, com a popularização da internet e a segurança de suas tecnologias, como uma Rede Privada Virtual (VPN, Virtual Private Network) houve uma aplicabilidade maior da transferência de dados através da Internet ou de outra rede pública, onde a informação trafega de uma forma criptografada através de um túnel, portanto os projetos em construção civil ficaram mais “próximos”, tornando possível o acesso as ferramentas de gerência em qualquer local.

Existem diversas técnicas quantitativas, bem como qualitativas, descritas em literatura especializada, com as quais se torna possível avaliar os riscos aos quais estará sujeito o empreendimento gerenciado. Assim sendo, é possível afirmar que gerenciamento remoto com uso de VPN pode ser uma alternativa a ser considerada no escopo de um projeto, garantindo sua eficiência.

Diante do cenário econômico brasileiro atual pressupõe-se que é primordial que a meta principal de uma construtora seja a preservação de seu lucro, que somente poderá ocorrer se a mesma executar seus empreendimentos cumprindo o prazo, mantendo o custo final dentro do intervalo inicialmente calculado, executando a obra com qualidade, obtendo assim a satisfação do cliente.

Assim sendo, para que as construtoras assegurem um adequado comportamento frente às condições do mercado, que se torna cada vez mais

competitivo, faz-se necessário o conhecimento prévio e preciso dos riscos existentes em um novo empreendimento imobiliário, através de mecanismo de análise de risco, assegurando ao mesmo tempo incremento de competitividade, lucratividade e qualidade.

É importante salientar que uma vez que os empreendimentos imobiliários de uma construtora podem ser de diversos tipos, tais como: loteamentos, construção de prédios comerciais, construção de condomínios, construção de casas residencial. Esta dissertação irá abordar apenas a gerência de projetos de um setor de engenharia numa empresa de distribuição de energia elétrica.

Como poderá ser observado ao longo do presente trabalho, o levantamento de dados ocorre praticamente durante todo o tempo da realização do mesmo. Desta forma, naturalmente conclui-se que o levantamento de dados é de vital importância para que o objetivo desta dissertação seja alcançado dentro de parâmetros que evidenciem a realidade de nossos dias. Assim sendo, todo o levantamento de dados foi executado dentro de cuidadosa atenção e com preocupação de coletar dados confiáveis e verdadeiros, visando obter uma amostra representativa da população amostrada.

A amostra considerada neste trabalho refere-se aos dados obtidos no setor de engenharia da ELETROBRÁS - Distribuição Acre, que é responsável pela distribuição de energia elétrica em todo o estado do Acre.

1.2 OBJETIVOS

a) Geral

Construir um modelo de gerenciamento remoto com VPN e avaliar as principais vantagens e desvantagens dele, bem como os benefícios trazidos com a utilização desse tipo de gerenciamento remoto para a empresa estudada.

b) Específicos

- Analisar a funcionalidade, principais aspectos, tipos de ligação e criptografia de dados de uma VPN;
- Mostrar os protocolos e softwares necessários para implantação;
- Levantar as melhorias trazidas para o gerenciamento das obras com o uso de VPN;

- Analisar o desempenho e produtividade do uso da tecnologia;

1.3 METODOLOGIA E ORGANIZAÇÃO DA PESQUISA

Com a finalidade de alcançar o objetivo proposto, este trabalho foi submetido ao cumprimento das etapas a seguir:

a) Pesquisa Bibliográfica;
b) Pesquisa de campo;
c) Análise dos dados encontrados;
d) Proposição de modelo de análise de risco.

Fez-se uso de algumas técnicas científicas de estudo, entre elas a observação, a experimentação, o raciocínio e a análise bibliográfica. Segundo Cury (1996, p. 85), a pesquisa bibliográfica refere-se a um levantamento de dados e uma reflexão sobre determinado tema; significa pesquisar o que está subentendido ou ainda algo que se encontra oculto, necessitando de um embasamento teórico para que possa aflorar.

No caso específico desta pesquisa, além de procurar saber sobre o tema proposto, é necessário analisar, ou ao menos procurar estabelecer critérios para análise de como a solução proposta funcionaria na ELETROBRÁS - Distribuição Acre, e que vantagens a empresa poderia agregar com a implantação da solução VPN.

Foi usado pesquisa de campo, através de visitas e esta pesquisa de campo, constitui-se basicamente de:

a) Elaboração de questionário inicial;
b) Aplicação do questionário;

Imediatamente após o término da pesquisa de campo, teve início a fase de análise dos dados encontrados, obedecendo aos seguintes passos:

a) Seleção dos resultados comparáveis e confiáveis dos demais resultados encontrados quando da aplicação dos questionários;
b) Tabulação dos resultados;
c) Análise dos resultados propriamente dita.

Com embasamento na pesquisa bibliográfica, elaborou-se uma proposição de modelo de análise do gerenciamento remoto de obras, assim como críticas,

sugestões e/ou recomendações de metodologias já utilizadas. Para propor o citado modelo fez-se necessário realizar pesquisa de campo junto à empresa, cuja metodologia será mais detalhadamente descrita no decorrer do trabalho.

1.4 JUSTIFICATIVA

A utilização de redes públicas tende para diversos usos, aqui realizaremos um estudo mais profundo no gerenciamento remoto de projetos, que vem a apresentar custos muito menores que os obtidos com a implantação de redes privadas, sendo este, justamente o grande estímulo para o uso de VPN's. Há uma tendência mundial de custos baixos nas empresas, nos seus empreendimentos, que necessitam de soluções cada vez mais rápidas e mais baratas, a utilização dessa rede, parece ser um caminho para interligar-se a outras redes, como no caso matriz e filial, a custos extremamente menores que os contratados exclusivamente por companhias de telecomunicação, por exemplo.

Para que esta abordagem se torne efetiva, a VPN deve prover um conjunto de funções que garantam: Confidencialidade, Integridade e Autenticidade, para ligar de forma confiável os pontos desejados e garantir que os engenheiros possam fazer a gerência remota de suas obras com sucesso.

1.5 RELEVÂNCIA DO ESTUDO

Num mercado onde quem domina mais tecnologia esta um passo à frente das demais empresas e, sabendo que a Internet está tão presente em nossas vidas, abordar um tema que traz economia às empresas com o auxilio da grande rede é o maior motivador para essa pesquisa. Não é necessário grandes investimentos para utilizá-la, a VPN é usada hoje em dia em pequenas, médias e grandes empresas e até mesmos nas residências, fazendo dessa tecnologia o futuro das interligações.

Este estudo pretende demonstrar as vantagens que as empresas terão em usar a rede virtual, assim como apontar que não é difícil a empresa se adaptar a tal tecnologia. Pretendemos também elaborar esquemas de utilização da tecnologia VPN, com base em estudos bibliográficos e de campo, que gerem um modelo de redução de custos.

O resultado do estudo gerado servirá de base para outras empresas, seja de construção civil ou não e o ganho que a sociedade terá será considerável, já que, o modelo proposto poderá ser utilizado em outro ambiente, inclusive doméstico.

1.6 ESTRUTURA DO TRABALHO

A presente dissertação é composta de corpo principal da mesma contendo 6 (seis) capítulos, 1 (um) apêndice e 1 (um) anexo.

No corrente capítulo faz-se a apresentação do trabalho, cita-se a relevância da abordagem do tema para a construção civil, são relacionados os objetivos desta dissertação, caracteriza-se a metodologia utilizada na elaboração da mesma e finaliza-se apresentando a estruturação do trabalho.

2 GERENCIAMENTO REMOTO DE PROJETOS

Definimos neste capitulo as principais características dos projetos e da gestão remota dos mesmos de forma a situar o leitor e elucidar alguns termos e definições de maneira a tornar mais fácil a compreensão do restante do trabalho.

2.1 PROJETO

2.1.1 Definição e características

LEWIS (2000) define o projeto como: um *trabalho único que possui início e fim claramente definidos, um escopo de trabalho especificado, um orçamento e um nível de performance a ser atingido*. O autor considera que, um trabalho é considerado um projeto, quando este tem mais de uma tarefa associada, ou seja, trabalhos por si só não são considerados projetos caso não sejam uma junção de vários outros trabalhos. GOODPASTURE (2000) segue o mesmo raciocínio, definindo projeto como *o conjunto de tarefas únicas, interdependentes e não repetitivas, planejadas e executadas de forma a produzir algum resultado*. NICHOLAS (1990), por sua vez, diz que projeto pode ser definido em termos de propósito, estrutura organizacional, complexidade, interesse e ciclo de vida:

1. Um projeto envolve uma finalidade, produto ou resultado único e definível, geralmente especificado em termos de requerimentos de custo, prazo e performance;
2. Os projetos “cortam” as linhas funcionais da organização, já que para sua execução são necessárias habilidades, competências e talentos de múltiplos profissionais de diferentes funções. A complexidade do projeto muitas vezes surge dessa necessidade de times multifuncionais;

3. Todo projeto é único no sentido que gera algo diferente em algum ponto do que já foi feito anteriormente. Mesmo em projetos de “rotina”, como a construção de uma subestação de energia, variáveis como o terreno, o acesso e leis de zoneamento certamente irão variar de uma construção para outra, tornando o projeto de cada construção único. Desta forma, um projeto é essencialmente diferente das atividades normais de produção de uma empresa, na medida que essas atividades são geralmente repetitivas e contínuas enquanto um projeto é, como definido, temporário e único;
4. Dado que um projeto é diferente do que já foi feito anteriormente, a incerteza e o risco são inerentes a ele, portanto, passível de um acompanhamento próximo de todas as suas etapas;
5. Projetos são empreendimentos temporários, ou seja, possuem início e fim definidos. O fim é alcançado quando os objetivos do mesmo são atingidos, quando se torna claro que esses objetivos nunca serão alcançados ou quando a necessidade de que os objetivos sejam atingidos não mais existir;
6. Finalmente, o projeto é um processo de trabalho para atingir uma meta. Durante esse processo, existem fases distintas. O conjunto dessas fases é chamado de ciclo de vida do projeto, e de vital importância um gerenciamento eficaz e rápido.

Um projeto pode ser dividido em sub-tarefas a serem executadas, segundo MEREDITH & MANTEL (1985), para que se alcance o fim desejado. Devido a sua complexidade é importante uma coordenação cuidadosa, com acompanhamento e controle, quanto a duração, precedência, custos e desempenho. Um projeto nunca é isolado, geralmente precisa ser coordenado com outros projetos sendo executados concomitantemente. Com isso, os autores, dizem que assim como entidades orgânicas, os projetos possuem um ciclo de vida. De um começo vagaroso, o nível de atividade vai se desenvolvendo até um pico, começando então a declinar e, finalmente, terminar. O *Project Management Institute* (PMI, 2000), resume essas definições:

- Projeto é algo temporário e realizado progressivamente para que se crie um produto ou serviço;

- Como os projetos são temporários, possuem um início e um término definidos, nem sempre curtos;
- A elaboração progressiva do resultado do projeto precisa ser cuidadosamente coordenada com o processo de definição de escopo, assim como um acompanhamento próximo, principalmente por equipes de engenharia responsáveis tanto pela elaboração como também pela execução do mesmo.

2.1.2 Fatores críticos, sucesso e fracasso de projetos

Qualquer que seja o projeto, desde o planejamento de construções até mesmo o acompanhamento das mesmas, existem certos pontos que devem ser observados para que o término seja eficaz.

Um dos pontos se refere a finalidade, priorizar as razões e entender os riscos também fazem parte do sucesso do projeto. Quando chegamos ao gerenciamento do projeto propriamente dito, chegamos a um impasse, essa eficiência somente se dará caso o acompanhamento seja o mais próximo possível, o que nos leva a questão que nem sempre é possível aproximar todo o aparato tecnológico da obra, portanto o gerenciamento remoto se torna necessário.

Quanto ao fracasso, CRAWFORD (2001) diz que gerenciar um projeto sem uma metodologia que possa apoiá-lo, terá grandes problemas para manter o projeto sob controle. As empresas investem alto em tecnologia de controle, mobilizar essa tecnologia para onde os projetos estão sendo executados, seria inviável, visto que há outros projetos que ocorrem ao mesmo tempo em outros lugares.

Normalmente o gerente de projeto irá até o local da execução do projeto, obtém os dados necessários e retornar até a base de dados e ali faz o lançamento dos processos já concluídos e ajustes necessários. O projeto assim tem um atraso na exatidão das informações, visto que o tempo que do deslocamento muitas vezes não é curto o suficiente.

Outra solução que poderia ser eficiente, seria a instalação de pontos de rede em cada projeto fazendo assim o gerente ter acesso imediato ao centro de dados, levando a um processo mais rápido nessa gerência, tornando a analise do projeto mais confiável, nesse ponto temos uma bifurcação na solução de rede mais recomendada, que seria a dedicada, mais cara ou a Rede Privada Virtual (VPN),

com a mesma eficácia que a dedicada, mas com um custo muito menor, como veremos mais adiante.

Quando gestores de projetos conseguem atingir o sucesso nestas condições, muitas vezes é fruto de um esforço individual e não de algo que a empresa pode com certeza reproduzir e institucionalizar. Há razões pelas quais um projeto pode falhar que não seja a distância, ou logística dos equipamentos necessários e incluem:

- Gestores de projetos que não têm uma visão corporativa de planejamento, controle, habilidades e ferramentas para o gerenciamento de projetos muitas vezes não conseguem visualizar o contexto no qual seus projetos estão inseridos, não conseguindo priorizar os recursos de acordo com as necessidades corporativas;
- Planos de recuperação dificilmente podem ser implantados a tempo em projetos que não são ativamente acompanhados e gerenciados durante sua execução;
- Falha no treinamento dos gestores de projetos: muitas organizações simplesmente promovem técnicos competentes para o cargo de gestor quando, na realidade, deveriam possibilitar entendimento e desenvolvimento das habilidades necessárias no gerenciamento de projetos, antes da promoção;
- Falta de apoio da alta administração para os gestores de projetos. Existe (ROBERT & FURLONGER apud CRAWFORD, 2001) uma alta correlação entre a falta de um patrocínio e apoio formal da alta administração e a falha em projetos;
- As organizações muitas vezes não possuem um único responsável pelo gerenciamento de projetos, desta forma, não existe um “culpado” na alta administração para as falhas em gerenciamento de projetos.

Como veremos mais adiante, a gestão de projetos tem como objetivo garantir o sucesso do mesmo, realizando as tarefas necessárias para esse sucesso e evitando as armadilhas que podem levar ao fracasso, e esse gerenciamento podendo ser feito mesmo a distância com precisão e em curto espaço de tempo nos leva a acreditar que as chances de conclusão do mesmo em tempo hábil se tornam promissoras.

2.2 GESTÃO DE PROJETOS

Apesar de as pessoas estarem rotineiramente envolvidas em projetos desde os primórdios da civilização, a natureza destes projetos mudou (NICHOLAS, 1990). Os projetos modernos envolvem grande complexidade técnica e requerem uma alta diversidade de habilidades e como dito na introdução, temos que diminuir os custos e manter a eficiência e credibilidade. Para lidar com esta nova e complexa natureza das atividades ligadas aos projetos modernos e com a incerteza inerente a essa complexidade, novas formas de gestão se desenvolveram. A moderna administração ou gestão de projetos é uma delas bem como a aplicação de tecnologias que evitem o desperdício, principalmente da parte de cálculos efetuados pela equipe de engenharia, mesmo com a aplicação de técnicas cada vez mais sofisticadas ou mesmo programas de alta precisão, o acompanhamento pessoal de um projeto continua sendo primordial para sua conclusão.

A gestão de projetos provê a empresa de ferramentas poderosas que melhoram a habilidade da organização para planejar, organizar, executar e controlar as atividades de maneira a conseguir atingir os resultados esperados dentro do prazo e custo previstos, mesmo em projetos de grande complexidade (MEREDITH & MANTEL, 1985). Gerenciamento de Projetos pode ser definido também como sendo a aplicação de conhecimentos, habilidades, ferramentas e técnicas nas atividades do projeto de forma a atingir os resultados necessários. LEWIS (2000) coloca que o gerenciamento de projetos consiste no planejamento, programação e controle das atividades que precisam ser executadas para que os objetivos do projeto sejam atingidos. FRAME (1995) diz que a gestão de projetos também está baseada em muitos dos princípios da administração geral, por isso, também envolve negociação, solução de problemas, política, comunicação, liderança e estudo de estrutura organizacional. Gerir um projeto a distância diminui consideravelmente o uso da estrutura logística da empresa, desafogando assim setores que ficariam livres para outras atividades ou mesmo realizarem outros projetos.

O *Project Management Institute* (PMI, 2000), novamente, consolida as definições dos autores dizendo que a gestão de projetos consiste em decisões que são tomadas ao longo de toda a vida do projeto, estabelecendo tarefas de planejamento, organização, execução e controle e está estruturada basicamente sobre quatro variáveis principais: escopo, prazo, custo e risco. RAD & RAGHAVAN

(2000), acentuam a importância dos processos no gerenciamento de projetos dizendo que, no passado, o foco da gestão de projetos estava em alocar pessoal competente para assegurar o sucesso do projeto e, apesar dessa abordagem ser necessária, o pensamento atual diz que procedimentos, processos, políticas e ferramentas mais formalizadas são vitais para o planejamento e gerenciamento dos projetos. NICHOLAS (1990) complementa dizendo que as soluções para problemas impostos por demandas que mudam rapidamente e por tecnologias complexas precisam ser de alguma forma complexas ou adaptativas às novas condições. Como resposta a essas demandas, novas abordagens de gerenciamento surgiram adotando a abordagem sistêmica ou por processo. O tempo atualmente é o principal inimigo do gerenciamento de projetos, saber lidar com todas as variáveis e executar todo o processo em um curto espaço de tempo, assim como a um custo menor é a grande objetivo que temos que alcançar, mais adiante veremos que um aproveitamento de algo que lidamos praticamente todos os dias, e que será a arma para isso: a internet, mais precisamente o tunelamento.

A tabela 1 ilustra os cinco grupos, com seus principais subprocessos. É importante notar que cada subprocesso pode ser dividido novamente nos cinco principais grupos de subprocessos até chegarmos ao nível de atividade. Os processos em negrito são considerados pelo PMI (2000) como sendo processos principais e os demais como processos de apoio.

Tabela 1 Processos de Gerenciamento

Grupos / Área	Iniciação	Planejamento	Execução	Controle	Fechamento
Integração		• Elaboração do Plano do Projeto	• Execução do Plano do Projeto	• Controle de Mudanças	
Escopo	• **Iniciação do Projeto**	• **Planejamento do Escopo** • **Definição do Escopo**		• **Verificação do Escopo** • **Contr. de Mud. De Escopo**	
Prazo		• **Definição de atividades** • **Sequenciamento de Atividades** • **Estimativa de duração de atividades** • **Elaboração do cronograma**		• **Controle do Cronograma (reprogramações)**	
Custo		• **Planejamento dos recursos** • **Elaboração do orçamento**		• **Controle dos custos**	
Qualidade		• Planejamento da Qualidade	• Quality Assurance	• Controle da Qualidade	
Recursos Humanos		• Planejamento Organizacional • Recrutamento	• Desenvolvimento do Time do Projeto		
Comunicação		• Planej. da comunicação	• Distribuição da informação	• Relatório de desempenho	• Fechamento administrativo
Risco		• **Planejamento do gerenc. do risco** • **Identificação dos riscos** • **Análise qualitativa e quantitativa dos riscos** • **Planejamento das respostas ao risco**		• **Monitoramento e controle dos riscos**	
Suprimento		• Planej. dos suprimentos • Planej. das solicitações	• Solicitações • Seleção de fornecedores • Administração de contratos		• Fechamento dos contratos

(Fonte: RAD & RAGHAVAN 2000)

Os processos de iniciação definem restrições, pré-requisitos e outras informações para o início dos processos de planejamento e execução. Durante os processos de iniciação, todas as informações relevantes para o planejamento devem ser levantadas, analisadas e relacionadas.

Os processos de planejamento definem e refinam os objetivos do processo principal, além de confeccionar o plano de trabalho para alcançar esses objetivos. Utilizam como base as informações coletadas e compiladas pelos processos de iniciação, trabalhando essas mesmas informações de maneira a planejar o trabalho a ser executado durante os processos de execução.

Os processos de execução coordenam pessoas e outros recursos para encaminhar a execução do projeto. Esses processos seguem o plano produzido

pelos processos de planejamento e têm como resultado o próprio resultado do projeto ou parte dele.

Os processos de controle asseguram que os objetivos do projeto serão alcançados e que o plano do projeto seja seguido ou então atualizado. Os processos de controle também mensuram os processos de execução.

Os processos de fechamento formalizam o término do projeto ou processo principal.

Em todas as fases é possível utilizar-se de toda a estrutura tecnológica da empresa, mesmo sem precisar movimentar seu centro de processamento de dados até a obra.

As interações entre esses processos são ilustradas nas Figuras 1, 2 e 3, de autoria do PMI (2000).

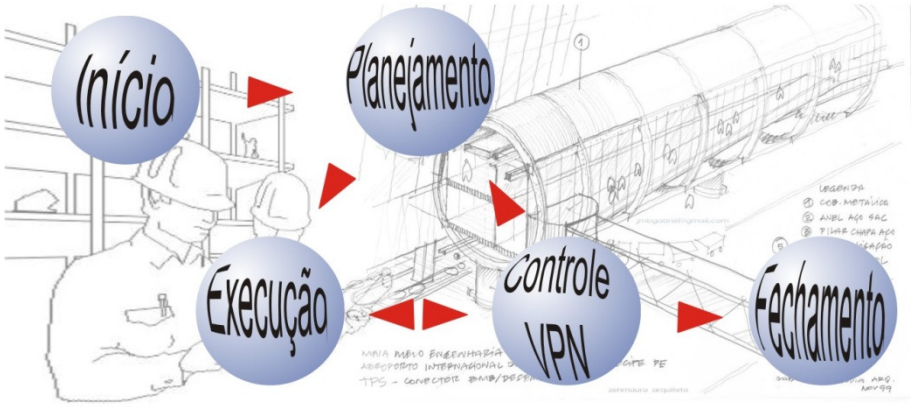

Figura 1 Fluxo dos Grupos de Processos

(Fonte: Autor)

Assim, os processos de iniciação geram resultados para os de planejamento, que geram resultados para os de execução, que passam pelos de controle, que alimentam novamente o planejamento e a execução e, finalmente, alimentam os processos de fechamento. Este fluxo é aplicável tanto ao projeto como um todo como a partes do projeto, desta forma, cada fase de um projeto pode ter seus processos enquadrados nos cinco grupos e o relacionamento entre eles será o mesmo da figura acima.

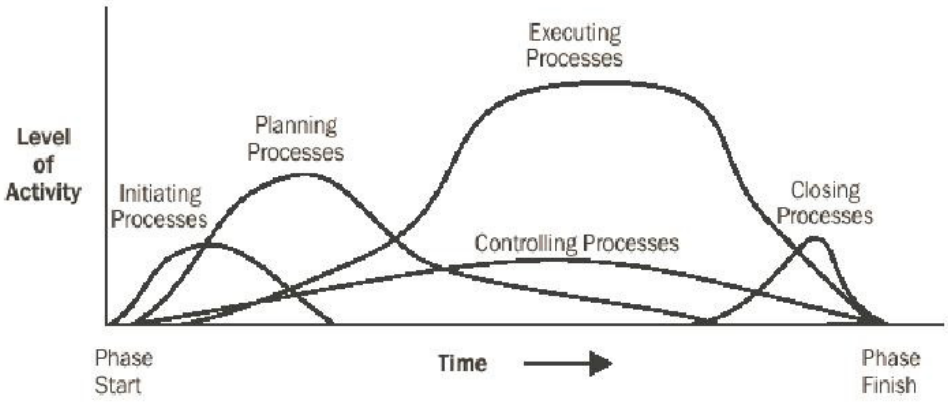

Figura 2 Distribuição do nível de atividade dos processos

(Fonte: RAD & RAGHAVAN 2000)

A figura 2 mostra o nível de atividades dos processos em função do tempo. Assim, no início dos projetos os processos de iniciação consomem a maioria dos recursos. Com o decorrer do tempo, os processos de planejamento começam a consumir mais recursos, seguidos dos processos de execução e, finalmente, dos processos de fechamento.

Os processos de controle têm uma atuação mais uniforme durante todo o ciclo de vida do projeto, portanto, com maior necessidade de utilização de dados precisos inclusive de outros setores da empresa, quanto menor o tempo de atualização desses dados, mais precisos serão os resultados obtidos.

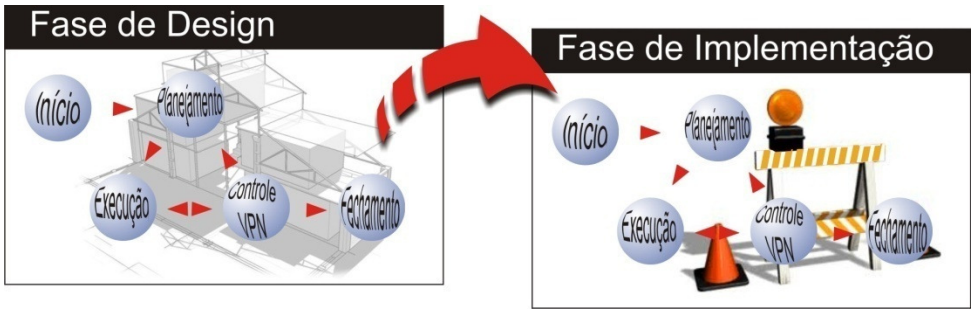

Figura 3 Relação entre os processos das fases

(Fonte: Autor)

A figura 3 acima ilustra a aplicação da figura 1 em todas as fases do projeto. Conforme dito antes, cada fase pode ter seus processos divididos nos cinco grupos e o relacionamento entre eles se dará de acordo com a Figura 1.

2.3 PROJETO VPN COMO MEIO DE IMPLEMENTAÇÃO DE ESTRATÉGIAS DE NEGÓCIO

GONSALEZ & RODRIGUES (2002) dizem que a implementação de estratégias de negócios envolvem:

- Mudanças nos parâmetros da operação dos processos atuais da empresa;
- Implementação de novas competências, tecnologias ou processos;
- Tem natureza tangível ou natureza intangível.

Estas ações de implementação sempre podem ser traduzidas em projetos e administradas como tal, com prazo, escopo, produtos e qualidade definidos. A figura a seguir ilustra a transformação de uma necessidade em ações estratégicas e sua implementação como projetos:

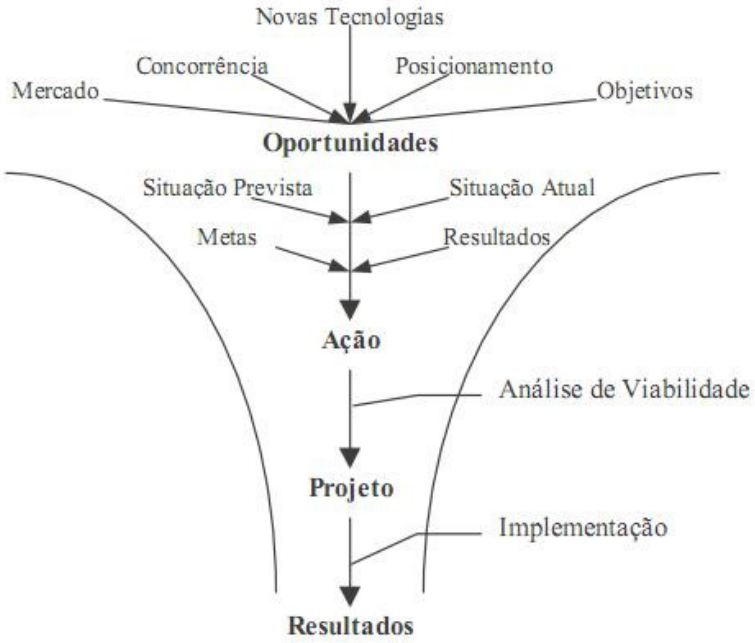

Figura 4 Transformação de Necessidades em Projetos

(Fonte: LEWIS 2000)

O projeto para implementação de uma ou mais estratégias organizacionais tem sempre por objetivo levar a empresa de um posicionamento atual para um outro posicionamento mais vantajoso no futuro, como é no caso que estudamos, A ELETROBRÁS – Distribuição Acre, vê a necessidade futura, baseada no crescimento da demanda energética no presente, e planeja a construção de

subestações para uso futuro, ou mesmo a implantação de novas tecnologias, como há um crescimento significativo nessa demanda, a necessidade de implantação dos projetos se faz urgente. Isto leva ao que os autores denominaram necessidade de ciclo de vida ampliado dos projetos para a evolução contínua da empresa. A figura a seguir ilustra esse ciclo:

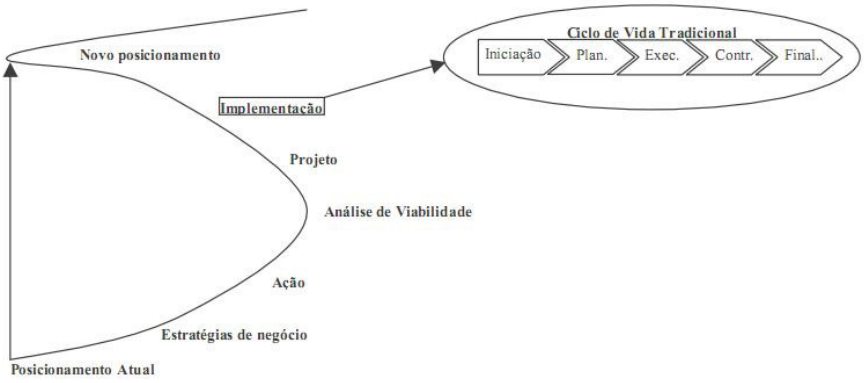

Figura 5 Ciclo de Vida Estendido dos Projetos

(Fonte: LEWIS 2000)

O ciclo de elaboração de estratégias, ação, análise de viabilidade, projeto e implementação é repetido para cada novo projeto de mudança organizacional, o que, se analisado como um todo, isso acarreta um aumento expressivo da complexidade do gerenciamento destes projetos, pois este gerenciamento irá envolver:

- Projetos em diferentes níveis de “maturidade ou diferentes fases de “evoluções”;
- Projetos que partem de vários ângulos de “posicionamento” da empresa: infra-estrutura, organização, tecnologia, etc.;
- Projetos diferentes que disputam os mesmos recursos;
- Projetos diferentes que facilitam ou dificultam a implementação de outros;
- Projetos que contribuem de forma diferente para os objetivos do negócio.

Este aumento de complexidade e de alcance do gerenciamento de projetos leva a um controle mais formal e centralizado para permitir uma transformação da empresa atual na organização do futuro de maneira orquestrada, ordenada e administrada e não caótica. A figura abaixo ilustra esse fato:

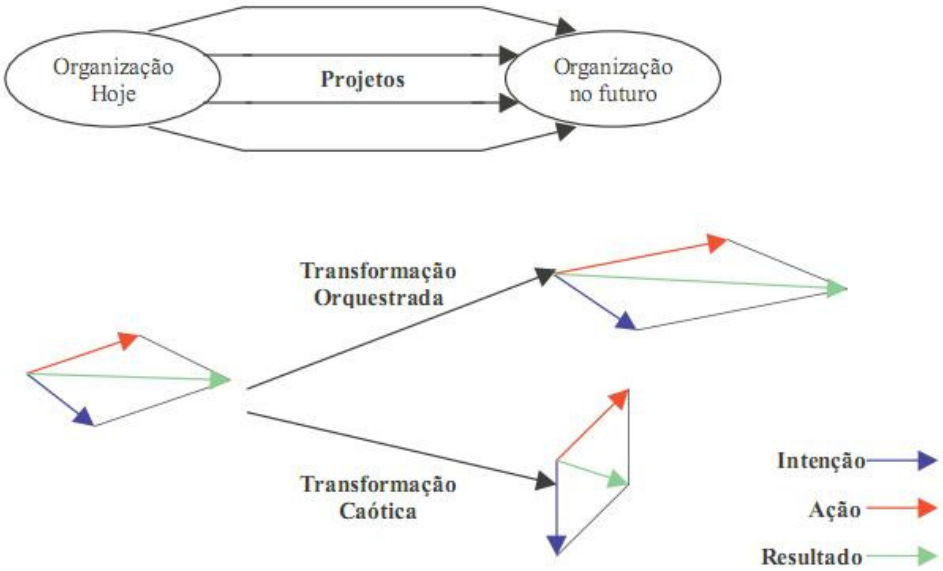

Figura 6 Transformações Orquestradas x Transformações Caóticas

(Fonte: LEWIS 2000)

Assim, fica evidente que é necessário uma coordenação entre os diversos projetos de iniciativas estratégicas da empresa de forma a tornar a ação mais próxima possível da intenção, obtendo os melhores resultados. Para isso, é necessário promover:

- O alinhamento entre as iniciativas;
- O alinhamento das iniciativas com a estratégia da empresa;
- Resultados obtidos próximos aos esperados;
- Reconhecimento da dinâmica da mudança.

O TDE (Técnico Departamento de Engenharia) precisa estar presente no controle desses projetos, a presença física muitas vezes é inviável, visto que os projetos, como vimos anteriormente ocorrem simultaneamente, a implantação de um planejamento e controle a distância é economicamente viável e necessário para a organização dessas iniciativas estratégicas.

3 TECNOLOGIA VPN

A finalidade deste capítulo é fazer um breve resumo e um histórico da tecnologia VPN, mostrando suas vantagens e desvantagens em relação às tecnologias existentes no mercado atual.

3.1 HISTÓRICO

Há alguns anos as corporações estabeleciam suas redes privativas, assumindo funções de responsabilidade das companhias telefônicas, mas estas não se moviam na velocidade desejada pelo mercado e não ofereciam os recursos nem as tarifas que as empresas buscavam. No Brasil havia o monopólio, e somente no governo de Fernando Collor de Melo é que as redes corporativas tornaram-se realidade. As empresas foram montando suas redes, criando infra-estruturas e direcionando recursos para atividades não afins, fugindo das altas tarifas de telecomunicações. Muitas delas investiram em link por satélite, que são adequados para telefonia, porém inadequados para Internet principalmente quando se quer usar telefonia IP (tipo de telefonia baseado no protocolo IP). Nos EUA também ocorreu fenômeno semelhante, mas no final dos anos 90 muitas das empresas americanas já estavam terceirizando suas redes, e claro voltando para os link's terrestres.

Segundo Ortiz (2002, p. 19), nascia a nova geração de VPN's, que teve como objetivo básico reduzir os custos de telecomunicações permitindo que corporações usassem a Internet como meio de comunicação, substituindo suas atuais redes corporativas que utilizam canais dedicados de dados, ISDN[1] ou Frame Relay[2].

---

[1] ISDN (*Integrated Services Digital Network*) é um serviço disponível em centrais telefônicas digitais, que permite acesso à internet, baseado na troca digital de dados, onde são transmitidos pacotes por multiplexagem sobre condutores de "par-trançado".

[2] [2] Frame Relay é uma tecnologia baseada em pacotes, ideal para tráfego de redes IP. Para cada largura de banda escolhida, existem diferentes taxas de CIR (CIR - *Committed Information Rate*), que são a garantia da taxa mínima de transferência de dados.

3.2 DEFINIÇÃO DE REDE VIRTUAL PRIVADA – VPN

Redes Virtuais Privadas é uma nova tecnologia que atualmente é muito trabalhada em projetos comerciais, assim como também é assunto pesquisado em universidades.

São muitas as definições dada à VPN, mas conforme Torres(2001, p. 531), pode-se definir uma VPN como uma rede privada simulada, ou seja, os link's dedicados existentes em uma rede privada normal são simulados. Além disso, em uma VPN, o acesso e a troca de dados só é permitido às pessoas que façam parte de uma mesma comunidade de interesse.

Quem faz o papel do link dedicado é o túnel, o qual usa a infra-estrutura de uma rede pública já existente, como a Internet, por exemplo.

Os pacotes são transmitidos através de uma técnica denominada tunelamento. Esta tecnologia possibilita que o tráfego de diversas fontes distintas viaje via diferentes túneis, sobre a mesma infra-estrutura, permitindo com isso, um diferenciamento das informações. Possibilitando, entre outras coisas, a garantia de prioridade para determinados túneis. Que por exemplo, contenham informações vitais para a empresa.

3.3 VANTAGENS DE SE UTILIZAR UMA VPN

As VPN's permitem estender as redes corporativas de uma empresa a pontos distantes da mesma, como outros escritórios, filiais, parceiros e até mesmo uma residência. Porém, ao invés de se utilizar um grande número de linhas dedicadas para a interconexão entre seus diversos pontos, o que onera muito o custo da rede (aluguel de linhas dedicadas, manutenção de diversos links para cada conexão, manutenção de equipamentos para diferentes conexões, uso de vários roteadores, monitoramento de tráfego nas portas de acesso remoto, grande número de portas, etc), uma VPN aproveita os serviços das redes baseadas no protocolo TCP/IP, espalhadas mundialmente, inclusive a Internet, ou até mesmo os provedores de serviços baseados em backbones privados, os quais apesar de limitados em alcance, poderão oferecer um melhor desempenho de serviço que a Internet, em detrimento do aumento de custos. Fazendo-se então, uma mistura de serviços prestados pela Internet e serviços prestados por IP's e backbones privados, uma

corporação poderá tirar vantagens sobre o desempenho do serviço e a redução dos custos.

Conforme Torres (2001, p. 530) outra grande vantagem das VPN's é que elas podem permitir acesso a qualquer lugar onde a Internet estiver presente. E como a Internet está presente em praticamente todos os lugares do mundo, conexões potenciais de VPN's poderão ser facilmente estabelecidas. Assim, no lugar de chamadas à longa distância, os usuários desta rede poderão, por exemplo, fazer ligações via Internet local, cuja tarifação é bem menor.

Entre as diversas vantagens que uma rede virtual oferece, pode-se destacar três principais:

3.3.1 Redução de custos

Trabalhando com VPN não há mais a necessidade de se manter onerosos link's dedicados entre os pontos da rede (filiais de uma empresa por exemplo), além também da economia observada no treinamento dos usuários e na aquisição e equipamentos. Enquanto redes tradicionais são baseadas em diversos links dedicados E1 (2 Mbps), acarretando altos custos mensais fixos, custos de instalação e utilização de diversos equipamentos. Para usuários remotos, devem ser mantidos equipamentos provedores de acesso e alugadas diversas linhas da companhia telefônica local. Enquanto isso, as VPN's ao invés de utilizar link's dedicados simulam essa comunicação ponto a ponto através da técnica de tunelamento.

3.3.2 Conexões seguras

A segurança nas conexões é garantida por diversos mecanismos implementados pelo protocolo utilizado na rede virtual privada, sendo o principal a criptografia de dados. A maior preocupação de uma ligação VPN está relacionada com privacidade, autenticidade e integridade dos dados que trafegam na rede.

3.3.3 Acesso de qualquer rede pública

Com apenas um software de acesso remoto o usuário tem acesso à rede virtual privada. Hoje em dia com a Internet, tem-se acesso de praticamente todo o mundo.

O quadro 1 a seguir, apresenta um comparativo entre as vantagens e desvantagens de uma VPN em relação as tecnologias tradicionais:

Tabela 2 Rede Tradicional x VPN

Rede Tradicional (Desvantagens)	**VPN (Vantagens)**
Taxa de Instalação	Custo mensal variável
Custo mensal fixo	Acesso remoto por provedor de Internet
Tarifas por Km	Interconexões via provedor de Internet
Taxa de manutenção	Manutenção feita via provedor de Internet
Vários equipamentos	Suporte de usuários remotos

(Fonte: Clube do Hardware)

3.4 TIPOS DE VPN

Existem vários tipos de implementação de VPN's. Cada uma tem suas especificações próprias, assim como características que devem ser levadas em conta na hora da implementação.

Entre os tipos de VPN, destacam-se três principais:

1 - Intranet VPN;

2 - Extranet VPN;

3 - Acesso Remoto VPN;

3.4.1 Intranet VPN

Conforme (ORTIZ 2002, p 32), em uma Intranet VPN, que pode, por exemplo, facilitar a comunicação entre departamentos de uma empresa, um dos quesitos básicos a considerar é a necessidade de uma criptografia rápida, para não sobrecarregar a rede (que tem de ser rápida).

Conforme (TORRES 2001, p 532), outro requisito essencial é a confiabilidade que garanta a prioridade de aplicações críticas, como por exemplo, sistemas financeiros, banco de dados. E por último, é importante a facilidade de gerenciamento, já que numa rede interna, tem-se constantes mudanças de usuários, seus direitos, etc.

A Figura 7 ilustra uma Intranet VPN e ilustra também a utilização de um *firewall*.

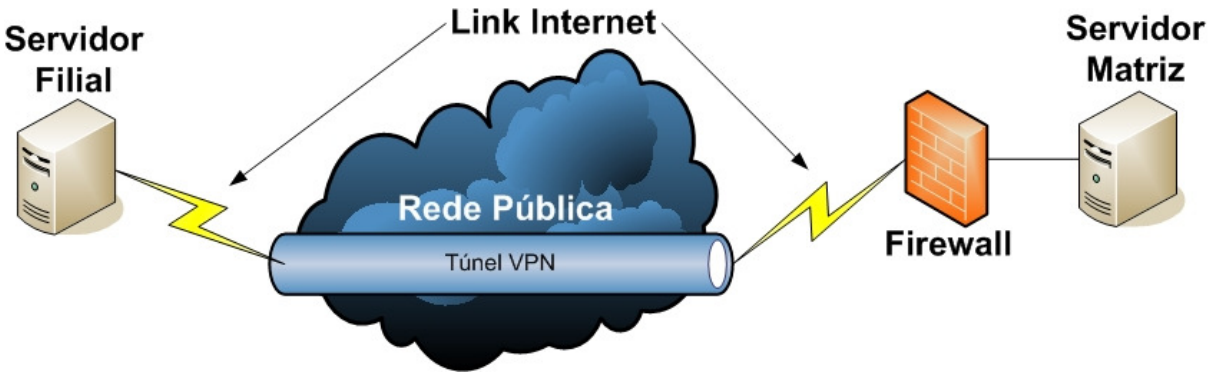

Figura 7 Exemplo de Intranet VPN

(Fonte: Autor)

3.4.2 Acesso Remoto VPN

Conforme (TORRES 2001, p 534), uma VPN de acesso remoto conecta uma empresa a seus empregados que estejam distante fisicamente da rede. Neste caso torna-se necessário um software cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS (*Quality of Service*), isto porque, geralmente quando se acessa remotamente de um laptop, estamos limitado à velocidade do modem. Outro item não menos importante é uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E por último, um fator importante, é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos conectados ao sistema, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação por exemplo, estejam centralizadas num único lugar. A Figura 8 ilustra um acesso remoto via VPN.

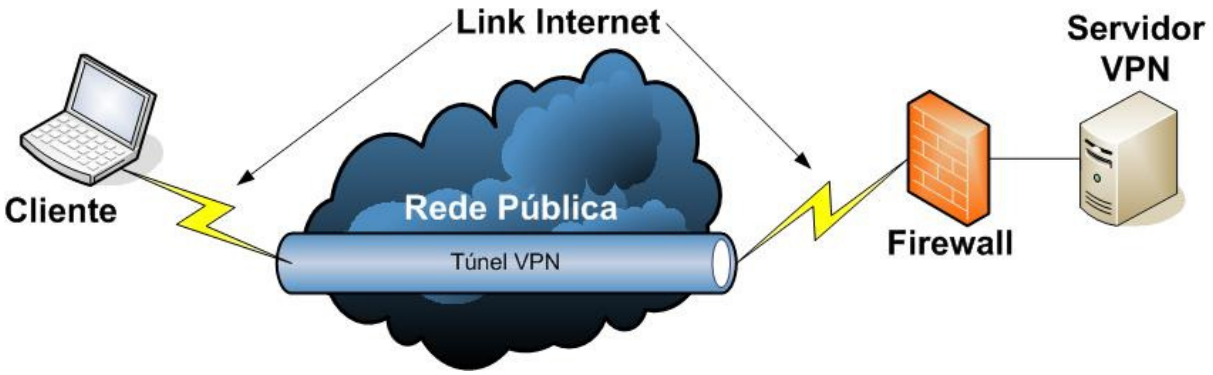

Figura 8 Exemplo de Acesso Remoto VPN

(Fonte: Autor)

3.4.3 Extranet VPN

Conforme (ORTIZ 2002, p 35), extranet VPN's são implementadas para conectar uma empresa à seus sócios, fornecedores, clientes, etc. Para isso é necessário uma solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Outro ponto muito importante a se considerar é o controle de tráfego, o que minimiza os efeitos dos gargalos existentes em possíveis nós entre as redes, e ainda garante uma resposta rápida e suave para aplicações críticas. A Figura 9 ilustra uma Extranet VPN.

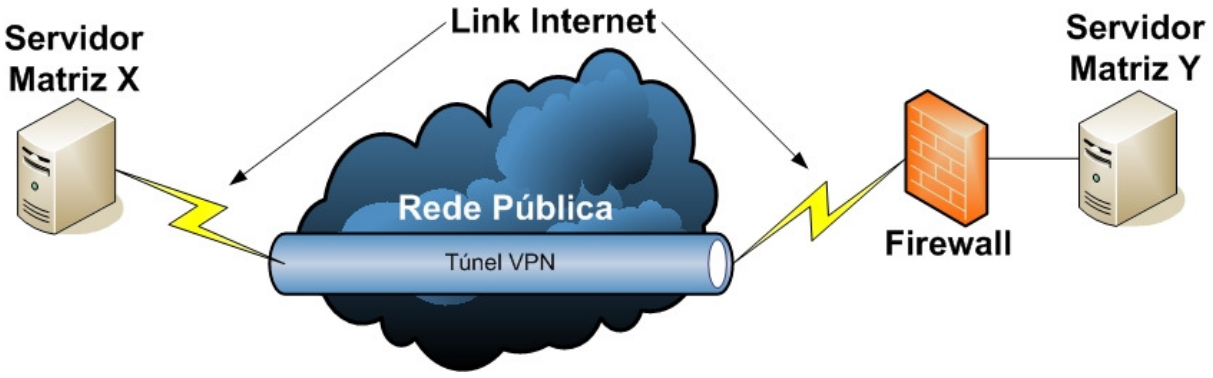

Figura 9 Exemplo de Extranet VPN

(Fonte: Autor)

3.5 SEGURANÇA

Segundo (CLUBE, 2006), a segurança de dados hoje em dia ainda é muito fraca na Internet, e até mesmo em redes privadas, onde se tem um maior nível de segurança é necessário uma certa preocupação no que diz respeito a esse assunto. As VPN's têm como principal característica a garantia de segurança dos dados. Para isso aconteça é necessário dar prioridade a três fatores:

- Controle de Acesso;
- Autenticação;
- Criptografia;

3.5.1 Controle de Acesso

Segundo (CLUBE, 2006), o controle de acesso basicamente dita os direitos de cada usuário na rede. Ele faz o controle e "log" de todos os acessos dos usuários na rede. Através desse controle é possível saber o que cada usuário está fazendo e fez em determinado momento, e também controlar os direitos de cada um.

3.5.2 Autenticação

Segundo (CLUBE, 2006) permite a entrada do usuário na rede virtual privada. Isto é feito geralmente através de uma senha. Porém, já se implementa em algumas redes uma autenticação denominada "dois fatores". Além de uma senha o usuário precisa ter algo em seu poder, como por exemplo, um cartão magnético. Isso reduz a probabilidade de uma pessoa ter sucesso ao tentar se passar por outra pessoa.

Além disso, a autenticação dos usuários permite ao sistema enxergar se a origem dos dados faz parte da comunidade que pode exercer acesso à rede. A autenticação dos usuários permite ao sistema enxergar se a origem dos dados faz parte da comunidade que pode exercer acesso à rede, como por exemplo, a utilização de um laptop, que pode ser um funcionário ou um invasor, por exemplo.

3.5.3 Criptografia

Conforme (ORTIZ 2002, p 54), a idéia da criptografia é embaralhar os dados e associar a esses dados uma chave. Apenas quem possuir essa chave poderá desembaralhar esses dados. Com isso garante-se a privacidade dos dados, ou seja, garante-se que ninguém conseguirá entender os dados que trafegam protegidos, assim como também se garante a integridade dos dados, ou seja, que ninguém irá alterar as informações contidas no pacote.

Cada protocolo implementa esses três fatores de varias formas. Para isso o capitulo seguinte mostrará as características de cada protocolo.

3.6 FUNCIONAMENTO DE UMA VPN

Agora é importante explicar o funcionamento, e os componentes de uma VPN, desde seus elementos até os protocolos utilizados.

3.6.1 Principais Elementos de uma VPN

Para que se possa entender o funcionamento de uma VPN, é muito importante conhecer os elementos que fazem parte dessa rede virtual. Para implementar uma rede virtual privada, será necessário conhecer o conceito de alguns elementos que a compõe:

Servidor VPN;

Cliente VPN;

Túnel;

Conexão VPN;

Protocolos de Tunelamento;

Dados Tunelados;

Rede Pública;

Para que se possa visualizar melhor alguns elementos de uma VPN, a Figura 10 ilustra uma VPN e seus principais elementos.

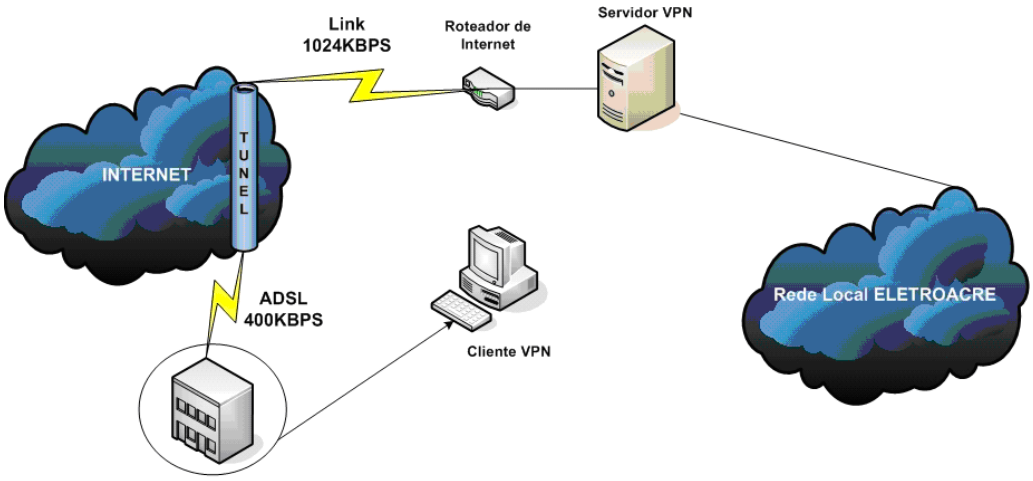

Figura 10 Elementos de uma VPN

(Fonte: Autor)

- Servidor VPN: Conforme (ORTIZ 2002, p 39), o servidor VPN é responsável por aceitar conexões de clientes VPN. Também é responsabilidade do Servidor VPN, autenticar e prover as conexões da rede virtual a seus clientes;
- Cliente VPN: O cliente VPN é aquele que faz a solicitação ao servidor VPN para conexão à rede virtual. Esse cliente pode ser um computador ou até mesmo um roteador;
- Túnel: Conforme (ORTIZ 2002, p 39), túnel é o caminho por onde trafegam os dados de uma VPN. Nesse túnel acontece o encapsulamento dos dados que serão transmitidos;
- Conexão VPN: É na conexão VPN que os dados da rede interna são criptografados para seguirem até seu destino. Do outro lado da conexão, por sua vez, os dados são descriptografados;
- Protocolos de Tunelamento: São responsáveis pelo gerenciamento e encapsulamento dos túneis criados por meio da rede pública. Também são considerados como padrões de comunicação da VPN. Será visto detalhadamente cada um dos mais freqüentes protocolos usados na implementação de uma VPN, juntamente com suas características;
- Dados Tunelados: Os dados tunelados são os dados que percorrem a rede publica através do túnel de uma rede virtual privada;

- Rede Pública: É utilizada pela VPN para efetuar suas conexões. Ela pode ser uma rede privada de uma empresa que vende os serviços de concessão ou mais provavelmente a Internet;

3.6.2 Tipos de VPN

Como foi visto anteriormente existem três tipos de implantação de uma rede virtual privada, que são: Intranet VPN, Extranet VPN e Acesso Remoto VPN.

3.6.3 Propriedades de uma Conexão VPN

Conforme (TORRES 201, p 536), quando o cliente se conecta por meio de uma VPN ao seu servidor central, tudo acontece de forma rápida e transparente, porem por trás desta ação existe uma série de processos ocorrendo, para que a conexão permaneça estável e com o mínimo de segurança necessária para o trafego das informações.

Existem quatro propriedades que envolvem as conexões e o envio de informações dentro de uma rede virtual.

3.6.3.1 Encapsulamento

Conforme (TORRES 2001, p 539) O encapsulamento dos dados numa rede virtual privada é feito por meio de um cabeçalho que permite que os dados trafeguem com segurança na rede pública.

3.6.3.2 Tunelamento

Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPN’s incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e decriptografado, retornando ao seu formato original. Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

Conforme (ORTIZ 2002, p 39), o protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

3.6.3.3 Autenticação

Conforme (ORTIZ 2002, p 37), numa rede virtual privada existem dois tipos de autenticação, que podem ser de usuários ou de integridade de dados. A autenticação de usuário é feita para que se possa saber se o usuário que deseja se conectar, tem realmente permissão para acessar a rede, e a autenticação da integridade de dados serve para verificar se os dados que chegam do outro lado do túnel não foram alterados nesse caminho.

A Autenticação é importante para garantir que o originador dos dados que trafeguem na VPN seja, realmente, quem diz ser. Um usuário deve ser identificado no seu ponto de acesso à VPN, de forma que, somente o tráfego de usuários autenticados transite pela rede. Tal ponto de acesso fica responsável por rejeitar as conexões que não sejam adequadamente identificadas. Para realizar o processo de autenticação, podem ser utilizados sistemas de identificação/senha, senhas geradas dinamicamente, autenticação por RADIUS (*Remote Authentication Dial-In User Service*) ou um código duplo.

A definição exata do grau de liberdade que cada usuário tem dentro do sistema, tendo como conseqüência o controle dos acessos permitidos, é mais uma necessidade que justifica a importância da autenticação, pois é a partir da garantia da identificação precisa do usuário que poderá ser selecionado o perfil de acesso permitido para ele.

3.6.3.4 Criptografia dos Dados

A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma seqüência de bits (chave) como padrão a ser utilizado na criptografia. Conforme (ORTIZ 2002, p 35), partindo dos dados que serão transmitidos, o objetivo é criar uma seqüência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso da chave.

São chamadas de Chave Simétrica e de Chave Assimétrica as tecnologias utilizadas para criptografar dados:

- Chave Simétrica ou Chave Privada: Conforme (CLUBE, 2006) é a técnica de criptografia onde é utilizada a mesma chave para criptografar e descriptografar os dados. Sendo assim, a manutenção da chave em segredo é fundamental para a eficiência do processo.
- Chave Assimétrica ou Chave Pública: Conforme (CLUBE, 2006) é a técnica de criptografia onde as chaves utilizadas para criptografar e descriptografar são diferentes, sendo, no entanto relacionadas. A chave utilizada para criptografar os dados é formada por duas partes, sendo uma pública e outra privada, da mesma forma que a chave utilizada para descriptografar.

3.6.4 Protocolos de Tunelamento

Conforme (GABRIELA, 2006), tunelamento é o encapsulamento ponto-a-ponto das transmissões dentro de 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 (*Quality of Service*), direcionado e priorizando o tráfico de dados para destinos específicos.

Ainda conforme (GABRIELA, 2006), as VPN's são, geralmente redes dinâmicas, ou seja, as conexões são formadas de acordo com as necessidades das

corporações. Assim, ao contrário das linhas dedicadas utilizadas por uma estrutura de rede privada tradicional, as VPN's não mantêm links permanentes entre dois pontos da rede da corporação, pelo contrário, quando uma conexão se faz necessária entre dois pontos desta corporação, ela é criada e quando a mesma não for mais necessária, ela será desativada, fazendo com que a banda esteja disponível para outros usuários.

Os túneis podem consistir de dois tipos de pontos finais: um computador individual ou uma LAN com um gateway seguro, que poderá ser um roteador ou um firewall. Porém, somente duas combinações desse pontos finais, são consideradas nos projetos de VPN's. No primeiro caso, tunelamento LAN-to-LAN, um gateway de segurança em cada ponto servirá de interface entre o túnel e a LAN privada. Desta forma, usuários de ambas as LANs poderão utilizar o túnel transparentemente para conseguir uma comunicação entre eles.

Um segundo caso, tunelamento Client-to-LAN, é aquele utilizado por usuários remotos que desejam acessar a LAN corporativa. O cliente, ou seja, o usuário remoto, inicia o tunelamento em seu ponto, para a troca de tráfego com a rede corporativa. A ferramenta para esta comunicação é um software instalado em seu computador, que permite transpor o gateway que protege a LAN de destino.

A Figura 11 é uma ilustração genérica do processo de tunelamento.

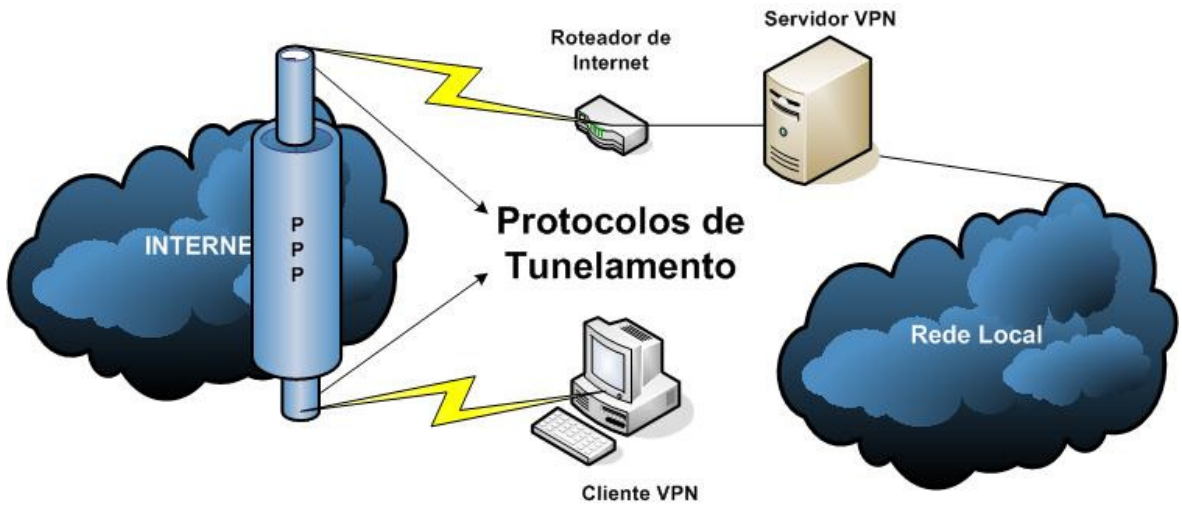

Figura 11 Processo de Tunelamento

(Fonte: Autor)

Agora veremos quais são os principais protocolos de tunelamento, juntamente com suas características e utilização, fazendo ainda um comparativo entre eles para o melhor entendimento.

3.6.4.1 O Protocolo GRE

Conforme (GABRIELA, 2006) túneis GRE (*Generic Routing Encapsulation*) são geralmente configurados entre roteadores fonte e roteadores destino (pacotes ponto-a-ponto). Os pacotes designados para serem enviados através do túnel (já encapsulados com um cabeçalho de um protocolo como, por exemplo, o IP) são encapsulados por um novo cabeçalho (cabeçalho GRE) e colocados no túnel com o endereço de destino do final do túnel. Ao chegar a este final, os pacotes são desencapsulados (retira-se o cabeçalho GRE) e continuarão seu caminho para o destino determinado pelo cabeçalho original.

A Figura 12 ilustra o funcionamento do protocolo GRE.

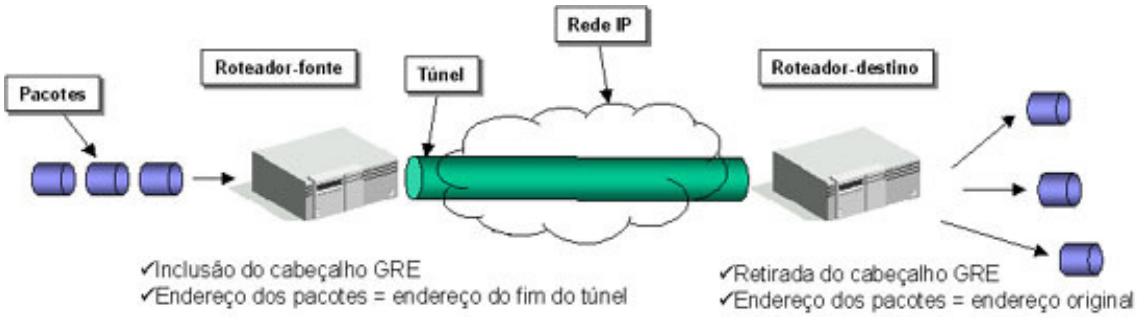

Figura 12 Protocolo GRE

(Fonte: Gabriela 2006)

Desvantagens:

- Os túneis GRE são, geralmente, configurados manualmente, o que requer um esforço grande no gerenciamento e manutenção de acordo com a quantidade de túneis: toda vez que o final de um túnel mudar, ele deverá ser manualmente configurado;
- Embora a quantidade de processamento requerida para encapsular um pacote GRE pareça pequena, existe uma relação direta entre o número de túneis a serem configurados e o processamento requerido para o encapsulamento dos pacotes GRE: quanto maior a quantidade de túneis, maior será o processamento requerido para o encapsulamento

- Uma grande quantidade de túneis poderá afetar a eficiência da rede;

3.6.4.2 O Protocolo PPTP

Conforme (TORRES 2001, p 540) o PPTP (*Point-To-Point Tunneling Protocol*), faz parte do pacote do Windows NT Server e Workstation. Um PC rodando este protocolo pode utilizar o mesmo para conectar com segurança a uma rede privada como um cliente de acesso remoto utilizando um rede de dados pública, como a Internet.

A principal característica no uso do PPTP é o suporte aVPN's. Dentro desta características, podemos considerar o uso através das Redes de Telefônica Pública Comutada (RTPCs). Utilizando o PPTP, uma grande empresa poderá reduzir os seus custos com comunicação remota, inclusive com usuários móveis, visto que o mesmo provê uma comunicação segura e codificada, seja através de RTPCs ou pela Internet.

3.6.4.2.1 Uma Conexão PPTP Padrão

Conforme (TORRES 2001, p 541) geralmente três computadores estão envolvidos nesta conexão:

- Um cliente PPTP;
- Um Servidor de Acesso a Rede;
- Um Servidor PPTP

O servidor de acesso à rede é opcional, porém, em uma conexão normal, eles estão presentes. Uma típica conexão PPTP começa com um PC remoto ou usuário móvel que será o cliente PPTP. Este cliente PPTP necessita ter acesso à rede privada de sua empresa utilizando a Internet através de um provedor local. Os clientes que estiverem utilizando um servidor Windows NT ou Workstation usarão a rede Dial-Up e o PPP para se conectar ao provedor de acesso local. Uma vez conectado, o cliente encontra-se habilitado para trocar informações em cima da Internet. O Servidor de Acesso a Rede utiliza o protocolo TCP/IP para manipulação de todo o tráfego.

Depois que o cliente efetuou a conexão PPP inicial ao provedor de acesso, uma segunda Rede Dial-Up, é ativada é efetua uma chamada através da conexão

PPP existente. Os dados enviados nesta segunda conexão, que contém dados PPP, são chamados de PPP encapsulado. É esta segunda chamada que cria a conexão, formando a Rede Virtual Privada junto a um servidor PPTP nas instalações da empresa remota. Este processo como vimos, é chamado de tunelamento.

O tunelamento é o processo de troca de dados de um computador para a rede privada, em cima de outra rede. Esta outra rede não tem acesso aos dados tunelados da conexão, porém esta rede transmite os pacotes do computador remoto para outro intermediário que neste caso seria o servidor PPTP. Este servidor PPTP está conectado, tanto na rede privada da empresa como na outra rede, que neste caso pode ser a Internet. Ambos, o cliente PPTP é o servidor PPTP utilizam este túnel para transmitir pacotes com segurança a um computador que encontra-se na rede interna da empresa.

Quando um servidor PPTP recebe um pacote da rede pública (Internet), envia-o para o computador de destino da rede interna. O servidor PPTP processa os pacotes PPTP obtendo o nome do computador de destino, que está dentro da rede interna ou a informação de endereço que encontram-se encapsuladas no pacote PPP.

O pacote PPP que está encapsulado poderá conter informações de múltiplos protocolos, tal como o TCP/IP, IPX/SPX, ou NetBEUI. O Servidor PPTP é configurado para se comunicar com a rede privada utilizando os protocolos da rede interna e externa.

O PPTP encapsulado, encripta e comprime os pacotes PPP e o transmite através de datragrama IP para a Internet, onde chegam até o servidor PPTP. O servidor PPTP desmonta o datagrama IP em um pacote PPP e então decodifica o pacote que contém o protocolo utilizado na rede interna da empresa. Como mencionado anteriormente, os protocolos que são suportados pelo PPTP é o TCP/IP, IPX/SPX é o NetBEUI.

3.6.4.2.2 Clientes PPTP

Um computador que utiliza o protocolo PPTP poderá conectar-se a um servidor PPTP de duas formas diferente:

Utilizando um servidor de acesso através de um provedor que aceite conexões PPP entrantes;

Utilizando uma conexão física TCP/IP (LAN) para conectar a um servidor PPTP.

Para acessar um servidor PPTP através de um provedor de acesso, os clientes PPTP deverão ter o MODEM e o dispositivo VPN devidamente configurados. A primeira conexão com o provedor de acesso e feito através do protocolo PPP. A Segunda conexão é uma conexão VPN que utiliza o PPTP. Todos são efetuados através do MODEM conectando-se ao provedor de acesso. A Segunda conexão requer a primeira porque o túnel entre os dispositivos VPN são estabelecidos utilizando o MODEM e a conexão PPP para a Internet.

A exceção nestes dois processos da conexão que está utilizando o PPTP é a criação de uma Rede Virtual Privada para os computadores que encontram-se fisicamente conectados a uma LAN. Neste caso o cliente encontra-se conectado e utilizando apenas uma conexão PPP e o dispositivo VPN que cria a conexão para um servidor PPTP na LAN remota.

Os pacotes PPTP de um cliente PPTP remoto e clientes PPTP de uma LAN local são processados de forma diferente. Um pacote PPTP de um cliente remoto é transmitido através da interface física de telecomunicação (normalmente um MODEM), enquanto o pacote PPTP de um cliente em uma LAN é colocado no adaptador de rede.

3.6.4.2.3 Arquitetura PPTP

Tipicamente, o estabelecimento de uma conexão segura utilizando o PPTP envolve três processos e cada qual requer o sucesso do anterior. Segue abaixo a explicação destes três processos e como eles trabalham:

Comunicação e Conexão PPP: Um cliente PPTP utiliza o PPP para conectar-se a um provedor de acesso utilizando uma linha telefônica padrão ou RDSI. Esta conexão utiliza o protocolo PPP para estabelecer a conexão e codificar os pacotes de dados.

Controle da Conexão PPTP: Utilizando a conexão para a Internet e estabelecido o protocolo PPP, o protocolo PPTP cria uma conexão de controle (cliente) para um servidor PPTP na Internet. Esta conexão utiliza o TCP para estabelecer a comunicação e é chamada de Túnel PPTP.

Tunelamento do Dados PPTP: O protocolo PPTP cria datagramas de IP que contém pacotes PPP codificados que são enviados para o Túnel PPTP e

consequentemente ao servidor PPTP. O servidor PPTP desmonta os datagramas IP e decodifica os pacotes PPP. Neste processo também é decodificado o destino do pacote, isto é, qual o destino do mesmo na rede privada.

3.6.4.3 O Protocolo PPP

Não entraremos a fundo no protocolo PPP *(point to point protocol*), mas apenas no necessário para o entendimento do ambiente PPTP. O PPP é um protocolo de acesso remoto utilizado pelo PPTP para enviar dados TCP/IP através de redes. O PPP encapsula em seu quadro os protocolos IP, IPX e pacotes NetBEUI criando uma conexão ponto-a-ponto para transmissão e recepção entre computadores.

A maioria das sessões PPTP é inicializada por um cliente que disca para um servidor do provedor de acesso e o protocolo PPP é utilizado para criar uma conexão dial-up entre o cliente é a rede do servidor de acesso e executa as seguintes funções:

- Estabelece e termina a conexão física. O protocolo PPP utiliza uma sequência definida para estabelecer e manter a conexão entre os computadores distantes;
- Autentica os usuários. Os clientes PPTP são autenticados utilizando o PPP. Para autenticação o protocolo PPP utiliza texto não codificado, codificado e MS CHAP;
- Cria datagramas PPP que contém IPX codificado, NetBEUI, ou pacotes TCP/IP;

3.6.4.3.1 Controle da Conexão PPP

Conforme [CLUBE] o protocolo PPTP especifica uma série de mensagens que são utilizadas para o controle da sessão. Estas mensagens são enviadas entre um cliente PPTP e um servidor PPTP. As mensagens de controle estabelecem e estabilizam o túnel PPTP. O Quadro 2 mostra uma lista de mensagens de controle primárias que estabelecem e estabilizam a sessão PPTP.

Tabela 3 Mensagens Primarias do PPTP

Tipo de mensagem	Propósito
PPTP_START_SESSION_REQUEST	Inicio de sessão
PPTP_START_SESSION_REPLY	Resposta para o pedido de inicio de sessão
PPTP_ECHO_REQUEST	Manter sessão
PPTP_ECHO_REPLY	Resposta para manter pedido de sessão
PPTP_WAN_ERROR_NOTIFY	Relatar erro na conexão PPP
PPTP_SET_LINK_INFO	Configura conexão PPTP Cliente/Servidor
PPTP_STOP_SESSION_REQUEST	Finalizar sessão
PPTP_STOP_SESSION_REPLY	Resposta para o pedido de término de sessão

(Fonte: Autor)

As mensagens de controle são enviadas dentro de pacotes de controle de um datagrama TCP. Uma conexão TCP é habilitada entre o cliente e o servidor PPTP. Este caminho e utilizado para enviar e receber mensagens de controle. O datagrama contém um cabeçalho PPP, cabeçalho TCP, Mensagem de Controle PPTP e informações de preenchimento.

Cabeçalho PPP de chegada

Cabeçalho IP

Mensagem de Controle PPTP

Preenchimento

3.6.4.3.2 Transmissão de Dados PPTP

Depois que o Túnel PPTP estiver criado, os dados do usuário são transmitidos entre o cliente PPTP e o servidor. Os dados é enviado através de datagramas IP, contendo pacotes PPP. O datagrama IP criado utiliza uma versão

modificada, isto é, um protocolo genérico de roteamento encapsulado (GRE - *Generic Routing Encapsulation*). Segue abaixo a estrutura do datagrama IP:

Cabeçalho PPP de chegada

Cabeçalho IP

Cabeçalho GRE

Cabeçalho PPP

Cabeçalho IP

Cabeçalho TCP

Dados

Observando com atenção a construção do pacote, podemos ver como os cabeçalhos transmitidos pela Internet podem ser desprezados. O cabeçalho PPP de chegada provê a informação necessária para que o datragrama atravesse a Internet. O cabeçalho GRE é utilizado para encapsular o pacote PPP dentro do datagrama IP. O pacote PPP é criado pelo RAS (Serviço de Acesso Remoto). O pacote PPP é codificado e se for interceptado, não terá como ser interpretado.

3.6.4.3.3 - Compreensão da Segurança do PPTP

O PPTP utiliza uma autenticação rígida e encriptação como segurança e está disponível para o RAS rodando sobre o Windows NT Server 4.0. O PPTP pode proteger o servidor PPTP e a rede privada ignorando todos os pacotes não PPTP. Apesar desta segurança, é fácil de configurar um firewall para permitir que o os pacotes PPTP tenham acesso a rede privada.

Inicialmente, uma conexão requer que você seja autenticado pela rede do Provedor de Acesso. Se a autenticação é requisitada, a mesma fica devidamente

registrada no LOG do provedor e não é relacionado com a autenticação do Windows NT. Um servidor PPTP é um gateway na sua rede e como tal requer um logon baseado no padrão do Windows NT. Todos os clientes PPTP têm que prover um nome de usuário e uma senha. O logon efetuado de forma remota através de um servidor Windows NT Server ou Workstation é tão seguro, como um PC se autenticando numa LAN (teoricamente). A autenticação de clientes PPTP remotos é estabelecida utilizando o mesmo método de autenticação PPP de clientes RAS que discam diretamente para um servidor NT. Por este motivo há o suporte através do MS-CHAP (*Microsoft Challenge Handshake Authentication Protocol*), que utiliza o método MD4, e anteriormente, também, utilizado pelo Lan Manager.

Depois da autenticação, todo o acesso a LAN privada continua utilizando as estruturas de segurança baseadas no NT. Havendo acesso a compartilhamentos (*Drivers* NTFS) ou para outros recursos da rede, será requerido as permissões formais, da mesma forma que se você tivesse conectado diretamente a LAN.

Para encriptar os dados, o PPTP utiliza o RAS através do processo "*shared-secret".* A referência ao "*shared-secret*" é porque ambas as pontas da conexão compartilham a chave de encriptação. Por baixo da imprementação do RAS da Microsoft, o segredo do compartilhamento é a senha do usuário (outros métodos incluem encriptação de chave pública). O PPTP utiliza a encriptação do PPP e esquemas de compressão. O CCP (*Compression Control Protocol* em português Protocolo de Controle de Compressão) é utilizado para negociar a encriptação usada. O nome do usuário e senha para a autenticação no servidor, é provida pelo cliente. Uma chave de encriptação é gerada utilizado o HASH da senha que é armazenado no cliente e no servidor. A chave de sessão é baseada na senha do cliente e é utilizado o padrão RSA e RC4, para criar a chave de 40-bit (No Canadá e EUA já encontra-se disponível a de 128-bit). Esta chave é então utilizada para codificar todos os dados transferidos entre o cliente e o servidor PPTP. Os dados do pacote PPP é codificado. O pacote PPP que contém o bloco de dados codificados é colocado em um datagrama IP para roteamento.

A segurança da rede contra intruso poderá ser melhorada habilitando o filtro PPTP no servidor. Quando o filtro PPTP é habilitado, o servidor PPTP na rede privada aceita e envia somente pacotes PPTP. Isto previne contra todos os demais pacotes entrantes na rede. O trafégo PPTP utiliza a porta 1723.

3.6.4.4 O Protocolo L2F

Conforme [ORTIZ] foi um dos primeiros protocolos utilizado por VPN's. Como o PPTP, o L2F foi projetado como um protocolo de tunelamento entre usuários remotos e corporações. Uma grande diferença entre o PPTP e o L2F, é o fato do mesmo não depender de IP e, por isso, é capaz de trabalhar diretamente com outros meios como FRAME RELAY ou ATM.

Este protocolo utiliza conexões PPP para a autentificação de usuários remotos, mas também inclui suporte para TACACS+ e RADIUS para uma autentificação desde o inicio da conexão. Na verdade, a autentificação é feita em dois níveis: primeiro, quando a conexão é solicitada pelo usuário ao provedor de acesso; depois, quando o túnel se forma, o gateway da corporação também irá requerer uma autentificação.

A grande vantagem desse protocolo é que os túneis podem suportar mais de uma conexão, o que não é possível no protocolo PPTP. Além disso, o L2F também permite tratar de outros pacotes diferentes de IP, como o IPX e o NetBEUI por ser um protocolo baseado na camada 2 do modelo OSI.

3.6.4.5 O Protocolo L2TP

Este protocolo foi criado pela IETF (*Internet Engennering Task Force*) para resolver as falhas do PPTP e do L2F. Na verdade, utiliza os mesmo conceitos do L2F e assim como este, foi desenvolvido para transportar pacotes por diferentes meios, como X.25, frame-relay e ATM e também é capaz de tratar de outros pacotes diferentes de IP, como o IPX e o NetBEUI (protocolo baseado na camada 2 do modelo OSI) .

O L2TP é porém, um modelo de tunelamento "compulsório", ou seja, criado pelo provedor de acesso, não permitindo ao usuário qualquer participação na formação do túnel (o tunelamento é iniciado pelo provedor de acesso). Neste modelo, o usuário disca para o provedor de acesso á rede e, de acordo com o perfil configurado para o usuário e ainda, em caso de autentificação positiva, um túnel L2TP é estabelecido dinamicamente para um ponto pré-determinado, onde a conexão PPP é encerrada.

3.6.4.6 PPTP x L2TP

Apesar de parecidos, ambos os protocolos, L2TP ou PPTP, diferenciam-se quanto suas aplicações, ou melhor, a escolha do protocolo a ser utilizado é baseado na determinação da posse do controle sobre o túnel: controlado pelo usuário ou pelo provedor de acesso.

No protocolo PPTP, o usuário remoto tem a possibilidade de escolher o final do túnel, destino dos pacotes. Uma grande vantagem desta característica é que, quando os destinos mudam com muita freqüência, nenhuma modificação (configuração) nos equipamentos por onde o túnel passa se torna necessária. Além disso, os túneis PPTP são transparentes aos provedores de acesso e nenhuma outra ação, além de prover serviço de acesso á rede, se faz necessária. Usuários com perfis diferenciados em relação aos locais de acesso – diferentes cidades, estados e países – se utilizam deste protocolo com mais freqüência pelo fato de se tornar desnecessária a intermediação do provedor no estabelecimento do túnel. Somente é necessário saber o número local para o acesso e o sistema do usuário, seu laptop, realizará o resto.

A desvantagem do protocolo L2TP é que, como o controle está na mão do provedor, o mesmo esta fornecendo um serviço extra que poderá ser cobrado.

A Figura 10 mostra um comparativo do funcionamento do protocolo PPTP e L2TP.

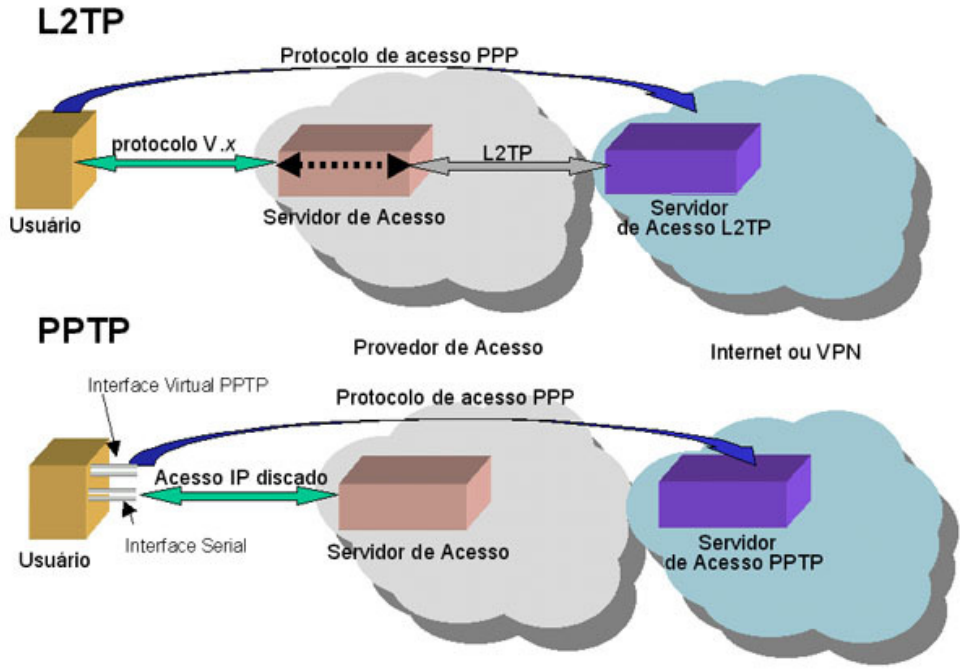

Figura 13 PPTP x L2TP

(Fonte: Gabriela 2006)

3.6.4.7 O Protocolo IPSec

PPTP, L2F e L2TP não incluem criptografia ou processamento para tratar chaves criptográficas, o que é bastante recomendado para garantir a segurança dos pacotes. Por isso, surgiu um dos mais importantes protocolos, criado para garantir a segurança da próxima geração de pacotes IP(IPv6) e que, no momento, vem sendo utilizado com protocolos IPv4.

O IPSec permite ao usuário, ou ao gateway de segurança que está agindo em seu favor, autentificar ou criptografar cada pacote IP, ou ainda, fazer os dois processos simultaneamente. Assim, separando os processos de autentificação e de criptografia, surgiram dois diferentes métodos para a utilização do IPSec, chamados de modos: no modo transporte, somente o segmento da camada de transporte de um pacote IP é autentificado ou criptografado; a outra abordagem, autentificação e criptografia de todo o pacote IP, é chamada de modo túnel. Enquanto que no modo transporte o IPSec tem provado ser eficiente para várias situações, no modo túnel ele é capaz de prover uma proteção maior contra certos ataques e monitoração de tráfico que podem ocorrer na Internet.

Conforme (GABRIELA 2006) o IPSec é baseado em várias tecnologias de criptografias padronizadas para proverem confiabilidade, integridade de dados e confiabilidade. Por exemplo, o IPSec utiliza:

Diffie-Hellman-Key-exchanges para entregar chaves criptográficas entre as partes na rede pública;

Public-key-criptography para sinalizar trocas do tipo *Diffie-Hellman* e garantir a identificação das duas partes, evitando assim, ataques de intrusos no meio do caminho;

3.6.5 DES e outros algorítmos para criptografar dados

Algorítimos para a autentificação de pacotes que utilizam "*hashing functions*".

3.6.6 Certificados digitais para validar chaves públicas

Existe duas maneiras para lidar com a troca de chaves e gerenciamento numa arquitetura IPSec: chaveamento manual (*manual keying*) e Internet Key Exchange (IKE) para gerenciamento automático de chaves. Enquanto o chaveamento manual pode ser usado em VPN's com um número pequeno de sites, o IKE deve ser obrigatoriamente em VPN's que suportam um grande número de sites e usuários remotos.

O IPSec tem sido considerado a melhor evolução para ambientes IP por incluir fortes modelos de segurança - criptografia , autentificação e troca de chaves - mas não foi desenvolvido para suportar outros tipos de pacotes além do IP. No caso de pacotes multiprotocolos, devem ser usados PPTP ou L2TP que suportam outros tipos de pacotes.

4 METODOLOGIA DA PESQUISA

Descreveremos agora a metodologia da pesquisa empregada no trabalho. A pesquisa foi classificada conforme as formas existentes identificadas durante o processo de revisão bibliográfica. A seguir foi definido o método científico a ser utilizado, e definidos alguns conceitos e esclarecimentos a ser considerados em pesquisas experimentais. Finalizando, relatadas as etapas da metodologia da pesquisa utilizada, ou seja, a etapa de pesquisa e análise, constando de revisão bibliográfica e pesquisa de campo e a de desenvolvimento do trabalho.

4.1 OBJETIVOS

O principal objetivo da pesquisa é o de descobrir respostas para questionamentos e alcançar os objetivos propostos. Realizando-se a pesquisa quando: se tem um questionamento, não existem informações para esclarecê-lo ou seja necessário a percepção dos sujeitos da pesquisa quanto a aplicação de uma ferramenta. Uma pesquisa deve estar fundamentada e metodologicamente construída no intuito solucionar ou esclarecer um determinado problema, pois de sua formulação dependerá todo o processo de desenvolvimento da pesquisa.

Este estudo foi desenvolvido através de pesquisa de campo utilizando uma abordagem qualitativa com tabulação dos dados e definição de escores para as respostas, facilitaram o entendimento das percepções dos atores através de análises estatísticas. Utilizou-se o viés interpretativo para preparar o questionário que foi construído com base nas entrevistas.

Esta abordagem tornou possível estudar os dados pela análise e comparação, buscando abrir o campo de possibilidades para que sejam encontradas respostas consistentes às perguntas que nortearam essa pesquisa. A escolha encontra suporte em Alves-Mazzotti (1999) quando destaca que as pesquisas qualitativas admitem mais de um instrumento de pesquisa e análise.

Para possibilitar fazer a inferência sobre determinado subconjunto do universo a ser pesquisado, os dados foram organizados em colunas e linhas. Esta tabela e denominada como *tabela de contingência* ou de *dupla entra*da permite estudar a relação entre duas variáveis qualitativas.

As pesquisas de campo ficaram concentradas na definição da satisfação dos usuários bem como a relação desses com os novos métodos tecnológicos apresentados, além disso, perguntou-se a sensação vivida antes e após a implantação do sistema.

O pesquisador atua como professor de graduação e pós-graduação em IES públicas e privadas desde 2004 e leciona as disciplinas de Redes de Computadores, Gerencia de Redes, Comunicação de Dados e Gerencia de Projetos de TIC no curso de Bacharelado em Sistemas de Informação da Universidade Federal do Acre. Lecionou Administração e Gerencia de Redes para curso de pós-graduação em Administração e Gerencia de Redes da União Educacional do Norte - UNINORTE. Prestou serviço de consultoria na área de redes de computadores na Eletrobrás Distribuição Acre, Sebrae/AC e Companhia de Habitação do Acre- COHAB/AC.

A pesquisa foi desenvolvida, segundo a metodologia a seguir:

4.2 PESQUISA BIBLIOGRÁFICA

Iniciou-se pela pesquisa bibliográfica, que constou de levantamento bibliográfico sobre a literatura publicada em livros, periódicos, dissertações, teses etc, publicadas ou disponibilizadas na Internet, que sejam pertinentes ao tema da dissertação.

A pesquisa foi exploratória e visou proporcionar um primeiro contato com o assunto a ser estudado, ou seja, seu objetivo foi proporcionar maior familiaridade com o assunto, com vistas a torná-lo mais explícito.

A pesquisa bibliográfica recorreu ao uso de livros e artigos, para dar fundamentação teórica ao trabalho que Vergara (1998, p.48) define como um:

> [...] estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, redes eletrônicas, isto é, material acessível ao público em geral. Fornece instrumental analítico para qualquer outro tipo de pesquisa, mas também pode esgotar-se em si mesma. O material publicado pode ser fonte primária ou secundária.

Resumidamente, direcionou-se a revisão bibliográfica para que fossem atingidos os seguintes objetivos:

- Aquisição de informações sobre a situação atual do tema pesquisado;
- Conhecimento das publicações já existentes;
- Verificação de opiniões semelhantes e diferentes, como também quanto aos aspectos relacionadas ao tema.

A pesquisa bibliográfica serviu de base para a compreensão e desenvolvimento da fundamentação teórica do trabalho.

4.3 PESQUISA DE CAMPO

O trabalho utilizou pesquisa de campo que constou de entrevistas com utilizadores e gestores de projetos do Departamento de Engenharia da ELETROBRAS – Distribuição Acre no município de Rio Branco – Acre, onde são centralizadas todas as ações de construção e acompanhamento de obras efetuadas pela empresa

Nas entrevistas foram utilizadas perguntas conforme Anexo 1, com a intenção de mapear tanto a satisfação com a nova tecnologia, como também traçar um comparativo entre as duas formas de gerenciamento, a saber: presencial e remota.

Como sujeitos da pesquisa foram considerados os engenheiros e gestores de projetos bem como demais profissionais que atuam em gestão dos projetos de construção e planejamentos de novas subestações de distribuição de energia elétrica.

Ao se escolher uma empresa que atua na área de distribuição de energia, se tem uma dimensão mais exata do montante que se economizará com tempo e gastos na gestão dos projetos. Estes dados justificam a seleção da empresa

4.4 PROCEDIMENTOS E INSTRUMENTAL DE COLETA E ANÁLISE DOS DADOS

A pesquisa de campo utilizou de entrevista individual dos gestores para coleta de dados que foram organizados através de um processo contínuo que identificou o graus de satisfação, a opinião de cada manipulador do sistema sobre a diferença entre a nova tecnologia e o método de manipulação anterior assim como uma avaliação de cada um sobre a economia de gastos para levar a cabo o projeto.

4.5 LIMITAÇÕES DA PESQUISA

A pesquisa limitou-se a avaliar a facilitação no tocante ao sistema de VPN, assim como a opinião sobre a adaptação dos gestores com a nova tecnologia, visto que não houve modificação estrutural quanto ao sistema empregado, mas sim uma nova estratégia. Um dos fatores limitantes da pesquisa foi o desconhecimento dos meios que levam o sistema a funcionar, cabendo aos gestores e usuários dos sistemas apenas a manipulação do sistema e não a implantação da tecnologia.

5 ESTUDO DE CASO

Os resultados da pesquisa procuram retratar as análises e as interpretações dos dados realizados à luz dos pressupostos subjacentes às teorias de autores reconhecidos e já mencionados anteriormente. Para uma melhor compreensão das informações levantadas nesta pesquisa, as análises estão apresentadas em tópicos que refletem os momentos distintos que compõem a análise de um processo de gerenciamento da pós-implantação da tecnologia VPN.

5.1 ELABORAÇÃO DE QUESTIONÁRIO PARA ANÁLISE DOS RESULTADOS

Para servir de base no estudo feito, foi elaborado questionário simples de poucas questões, de modo que seu preenchimento fosse feito de forma rápida e fácil. Nele foram abordados 7 temas:

1. Índice de satisfação do usuário;
2. Relevância da tecnologia em relação ao gerenciamento de projetos;
3. A aplicabilidade de VPN em outras empresas;
4. O tempo gasto com o acompanhamento do projeto usando VPN;
5. Os gastos financeiros com o projeto;
6. A facilidade de adaptação com a VPN pelo setor;
7. Dificuldade ou desconfiança no sistema.

Para o tema 1, foi solicitado notas de 0 a 5 com relação ao assunto tratado. Para o tema 2, também foi solicitado notas entre 0 e 5. Já para os temas 3, 4, 5, 6 e 7 foi pedido que os entrevistados respondessem “sim” ou “não” a respeito da aplicabilidade da VPN em outras empresas de mesmo ramo, o tempo gasto com o

acompanhamento do projeto, gastos financeiros com o projeto, facilidade de adaptação com a VPN pelo setor e dificuldade ou desconfiança no sistema.

O conjunto das pessoas entrevistadas foi de 11(onze) pessoas, levando em conta que o corpo do TDE (setor de engenharia), é de aproximadamente 120 pessoas, chegamos a ter um percentual de entrevistado próximo a 10% do total geral de funcionários da área.

5.2 ANALISE DOS RESULTADOS

5.2.1 Tema 1, Nível de Satisfação

Nessa fase, a pesquisa identificou os índices de satisfação da empresa pesquisada com a implantação e uso da VPN. Em uma escala variando de 0 (totalmente insatisfeito) até 5 (totalmente satisfeito), a percepção do nível de satisfação das empresas pode ser verificada pelo Gráfico 1.

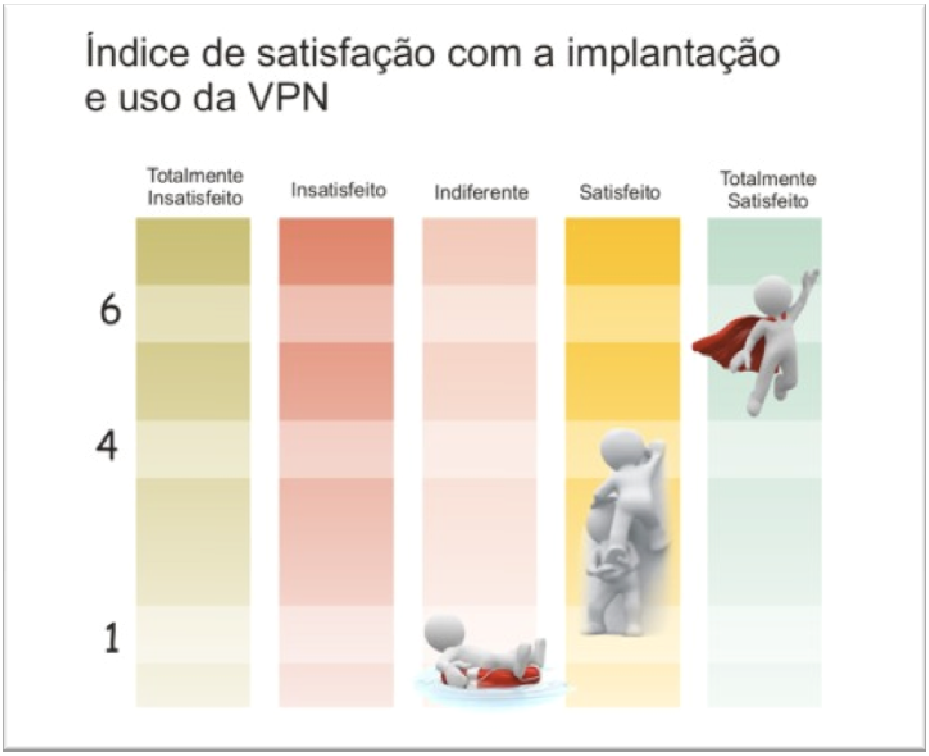

Gráfico 1 Índice de satisfação com a implantação e uso da VPN

(Fonte: Autor)

Conforme verificado no gráfico anterior o nível de satisfação num universo de 11 pessoas que atuam diretamente no sistema é bastante elevado, representando

mais de 50% dos usuários da VPN. O gráfico 2 abaixo mostra em valores percentuais o nível de satisfação da equipe com a utilização da VPN.

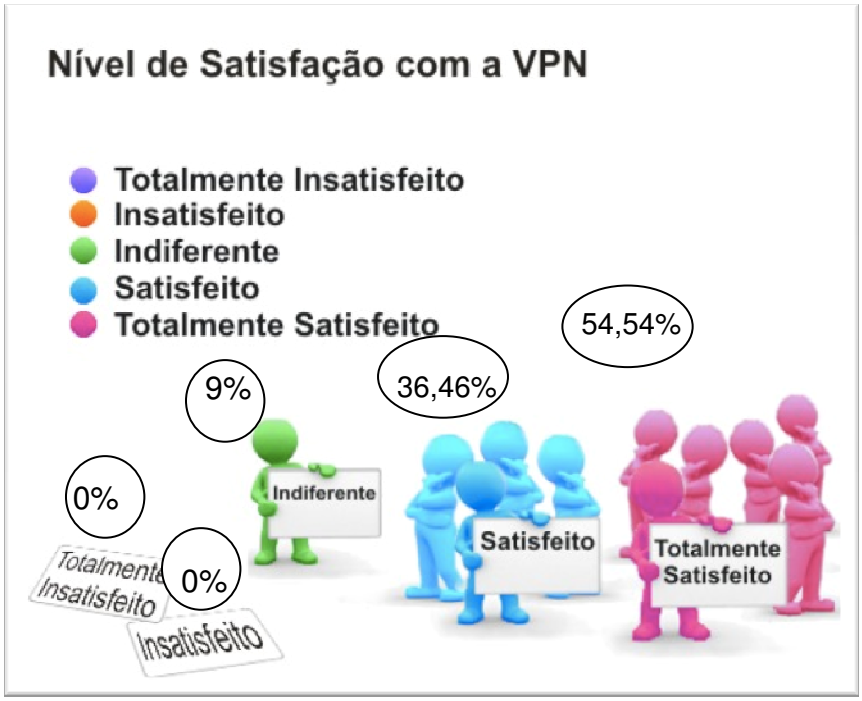

Gráfico 2 Índice de satisfação em percentuais

(Fonte: Autor)

Os níveis “Totalmente Insatisfeito” e “Insatisfeito” representam juntos 0%, reforçando mais uma vez que a ferramenta implantada é de muita valia para as atividades exercidas pelo setor pesquisado, e que mais utilidades, alem dos acesso remotos aos sistemas, trarão mais facilidades, como por exemplo, acesso ao servidor de arquivo da empresa, visto que, nele se encontram todos os arquivos do AutoCAD do setor e que as vezes é necessário acesa-los remotamente para verificações.

5.2.2 Tema 2, Relevância para Gerenciamento de Projetos

Nesse ponto foi analisado quão importante é o uso de VPN, para tal foi solicitado que o entrevistado desse nota 0 (para totalmente irrelevante) e 5 (para totalmente relevante), os resultados alcançados refletem a primeira questão tratada e reafirma que VPN, pode ser sim, um grande aliado a gerencia de empreendimentos e/ou projetos de engenharia. Conforme gráfico abaixo temos essa relação de relevância representada:

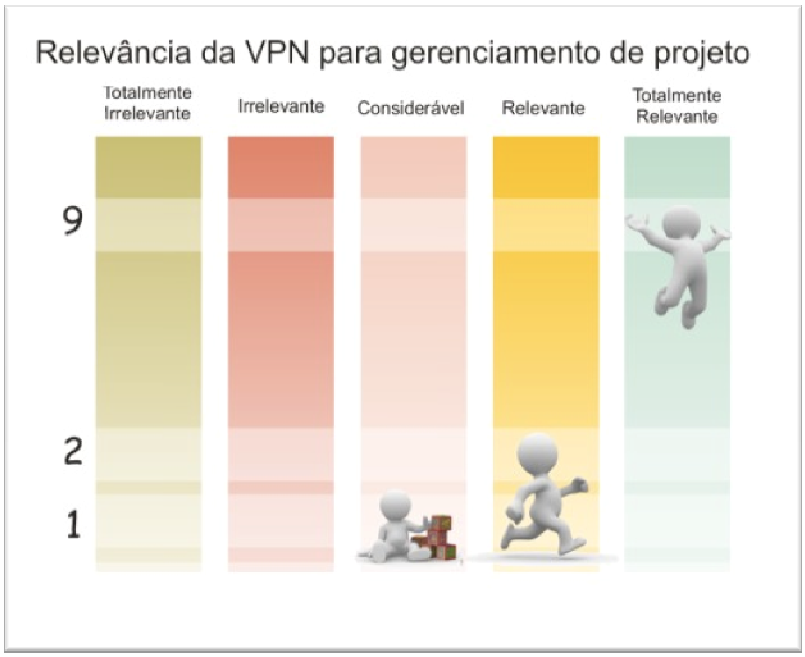

Gráfico 3 Relevância da VPN para gerenciamento de projeto

(Fonte: Autor)

Levando em conta os valores percentuais vemos 0% para os indicadores “Totalmente Irrelevante” e “Irrelevante” juntos e apenas 9% tem a tecnologia como “Considerável”, temos que 91% que é a soma dos que julgam “Relevante” e “Totalmente Relevante”, reafirmando a importância do uso de VPN no acesso remoto e conseqüentemente no gerenciamento de empreendimentos de forma remota. O gráfico abaixo exprime em percentuais o que foi tratado nesse tema.

Gráfico 4 Valores Percentuais da Relevância de VPN

5.2.3 Tema 3, A aplicabilidade de VPN em outras empresas

Para esse tema foi tratado simplesmente se “sim”, ou seja, é aplicável a outras empresas e/ou situações que envolva o gerenciamento de empreendimentos remotamente e “não”, ou seja, não é aplicável.

Temos que apenas 2 dos 11 entrevistados julgaram que a tecnologia VPN não pode ser aplicada em outras empresas, para justificar esse numero levo em conta uma das dificuldades encontradas que é cultura de uso, ou seja, a pessoa não usa porque não é do seu dia a dia trabalhar com computador, muito menos com acesso remoto. Mesmo assim o valor 9 é bastante amplo no conjunto estudado e de forma definitiva reflete o sucesso da pesquisa. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema:

Gráfico 5 Aplicabilidade da VPN

(Fonte: Autor)

Finalizando temos os valores percentuais, que demonstram uma maioria esmagadora, ou seja, 82% julgaram que é possível utilizar VPN em outras empresas e em outras atividades dentro da construção civil. Apenas 18% julgaram que não é, mas como dito anteriormente isso é irrelevante dentro do contexto e precisamente de natureza cultural. O gráfico a seguir mostra de forma clara e objetiva esses valores percentuais que fecham este tema do questionário confirmando o resultado esperado:

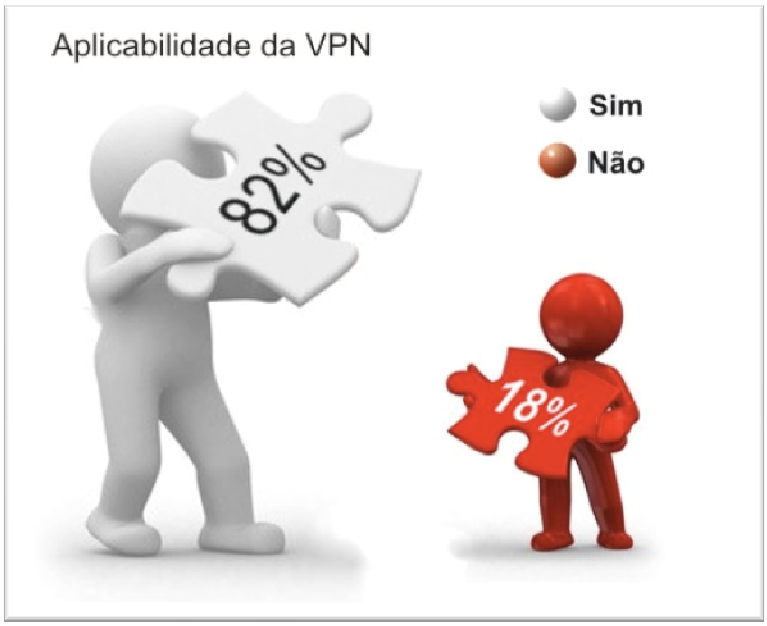

Gráfico 6 Aplicabilidade da VPN em percentuais

(Fonte: Autor)

5.2.4 Tema 4, O tempo gasto com o acompanhamento do projeto usando VPN

Para esse tema foi perguntado se a implantação da VPN diminuiu o tempo gasto com o acompanhamento do projeto. Foi solicitado ao entrevistado que respondesse “sim” em caso de diminuição do tempo gasto com o acompanhamento do projeto ou “não” para definir que a tecnologia não auxilia na redução de tempo de acompanhamento.

Obtivemos no resultado que apenas 2 dos 11 entrevistados julgaram que a tecnologia VPN não reduziu o tempo gasto, enquanto 9 dos 11 entrevistados julgaram que a tecnologia VPN ajudou a reduzir o tempo gasto com o acompanhamento do projeto. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema:

Gráfico 7 Quanto a redução do tempo

(Fonte: Autor)

Em termos percentuais obtemos os mesmos resultados do tema anterior, onde temos 82% dos entrevistados aprovando a redução de tempo e apenas 18% julgando a ineficácia da solução adotada. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema em valores percentuais:

Gráfico 8 Sentiram a diminuição dos gastos

(Fonte: Autor)

5.2.5 Tema 5, Os gastos financeiros com o projeto

Nesse tema foi questionado ao entrevistado se, na opinião dele, os gastos financeiros com o projeto podem diminuir de alguma forma. Obteve-se os seguintes resultados: 7 dos entrevistados julgaram que “sim”, pode-se reduzir gastos com uso dessa solução, contra 4 que optaram pelo “não”, julgando irrelevante a redução de custos gerada pela VPN.

Acredito que a VPN, assim como as videoconferências e VoIP, diminuem as distancias e reduzem as idas e vindas ao escritório para fazer lançamento de dados em sistemas como AutoCad e SGD(Solução proprietária da Eletrobrás Distribuição Acre) e assim, podem sim reduzir gastos de locomoção. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema:

Gráfico 9 Diminuição com gastos financeiros

(Fonte: Autor)

Em valores percentuais vemos que 63,64% dos entrevistados optaram pelo “sim” nesse tema e 36,36% optaram pelo “não”. Pode-se ver que temos, em dados percentuais, quase o dobro de “sim” em relação ao “não”, o gráfico abaixo mostra os valores mencionados e discutidos nesse tema em valores percentuais:

Gráfico 10 Percentual quanto a diminuição de gastos

(Fonte: Autor)

5.2.6 Tema 6, A facilidade de adaptação com a VPN pelo setor

Nesse tema foi abordada a facilidade de adaptação e uso da VPN, foi perguntado se a implantação da VPN foi de fácil adaptação ao setor. Nesse tema reflete-se o que foi abordado anteriormente: A cultura de uso de novas tecnologias, pois obtivemos 6 dos 11 julgando que “não”, ou seja, a VPN não é de fácil adaptação e uso, e 5 dos 11 respondendo “sim”.

Em todas as profissões a resistência a mudanças é fator vital e decisivo, e não seria diferente na engenharia civil, a cultura de uso do computador está até bem difundida nesse ramo, mas a utilização de novas tecnologias, diferente do Auto-Cad, por exemplo, dificulta a adaptação, mesmo assim deve-se levar em conta que um treinamento pode sanar essa carência. O gráfico a seguir mostra de forma clara e objetiva esses valores:

Gráfico 11 Facilidade de adaptação pelo setor

(Fonte: Autor)

Em termos percentuais, tem-se o primeiro revés em relação as hipóteses do trabalho, visto que, acreditava-se que a adaptação de uso não seria fator tão rejeitado como visto em números. Tem-se 54,55% analisando que foi difícil a adaptação a nova tecnologia e que 45,45% julgando que não foi difícil e que VPN é de fácil uso. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema em valores percentuais:

Gráfico 12 Percentual de facilidade na adaptação

(Fonte: Autor)

5.2.7 Tema 7, Dificuldade ou desconfiança no sistema

Nesse ultimo e derradeiro tema, foi perguntado ao entrevistado se ele sentiu dificuldade ou desconfiança no sistema. Novamente refletimos os resultados do tema anterior, onde obtivemos 6 dos 11 julgando que “sim”, ou seja, tem desconfiança ou dificuldades com VPN e 5 dos 11 respondendo “não”, que sentem-se confiantes e não tem dificuldades com ela. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema:

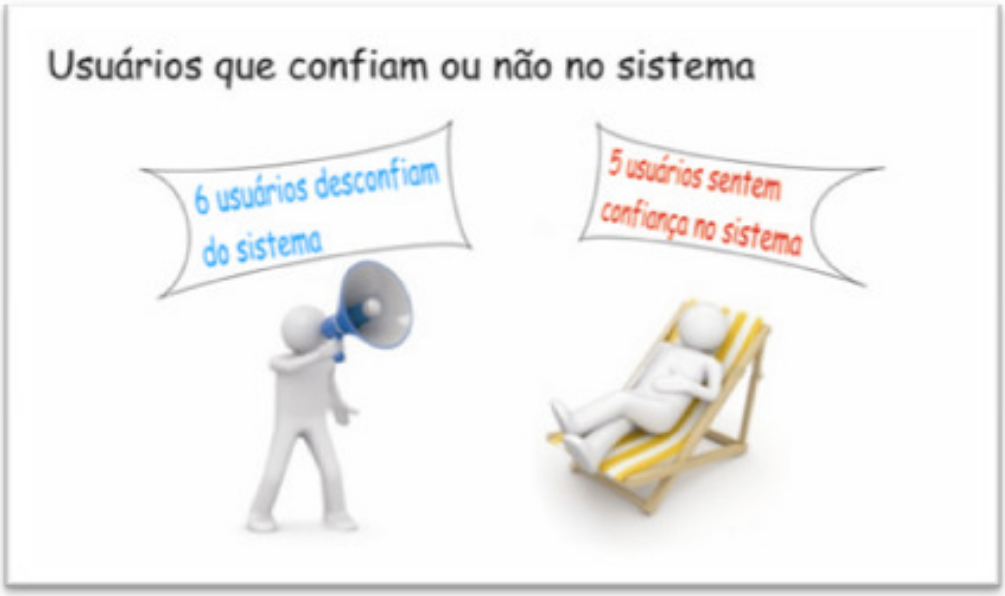

Gráfico 13 Confiança ou não no sistema VPN

Em valores percentuais obteve-se 54,55% julgam “sim”, que tem dificuldades ou desconfiança na tecnologia VPN e 45,45 “não”, ou seja, tem confiança no sistema. O gráfico abaixo mostra os valores mencionados e discutidos nesse tema em valores percentuais:

Gráfico 14 Percentual de credibilidade no sistema

5.3 RESUMO DOS DADOS TABULADOS

Para melhor visualização dos dados da pesquisa, tem-se a seguir um tabela com todos os dados do questionários formatados de forma a refletir o resultado final em valores percentuais.

Tabela 4 Resumo da Pesquisa

	Totalmente Insatisfeito	Insatisfeito	Indiferente	Satisfeito	Totalmente Satisfeito
Nível de satisfação com a implantação e uso da VPN	0,00%	0,00%	9,00%	36,46%	54,54%

	Totalmente Irrelevante	Irrelevante	Considerável	Relevante	Totalmente Relevante
Relevância da VPN para gerenciamento dos projetos	0,00%	0,00%	18,00%	9,00%	73,00%

	Sim	Não
Em sua opinião a tecnologia VPN é aplicável à empresa?	82,00%	18,00%
A implantação da VPN diminuiu o tempo gasto com o acompanhamento do projeto?	82,00%	18,00%
Em sua opinião, os gastos financeiros com o projeto diminuíram de alguma forma?	63,64%	36,36%
A implantação da VPN foi de fácil adaptação ao setor?	45,45%	54,55%
Você sentiu dificuldade ou desconfiança no sistema?	54,55%	45,45%

5.4 PRINCIPAIS VANTAGENS E DESVANTAGENS PERCEBIDAS PELA EMPRESA

5.4.1 Vantagens

Com relação as vantagens podemos elencar várias descritas pelos funcionários e as implícitas na pesquisa, mas certamente as principais são as descritas abaixo:

- Interligação de redes usando a Internet;
- Sempre disponível, onde quer que esteja desde que tenha acesso à Internet;
- Encriptação de Alto-Nivel, ou seja, proteção de dados;
- Baixo custo em relação a linhas dedicadas;
- Aceita múltiplas ligações em simultâneo;
- Redução de custos com locomoção;
- Agilidade no lançamento das informações;
- Análise de dados em tempo real.

5.4.2 Desvantagens

As desvantagens, levando-se em conta o lado técnico da ferramenta, estão sempre voltadas para limitações em conexões de Internet lentas que limitam a velocidade do acesso ao sistema. Com todo o impacto que cercou historicamente VPNs, os principais perigos, ou pontos fracos do modelo da VPN são facilmente esquecidos. Quatro pontos podem ser destacados neste aspecto:

- Requer um profundo conhecimento de segurança de rede pública para se adotar todas as devidas precauções na implementação de uma VPN.
- A disponibilidade e o desempenho da VPN de uma organização entre pontos geográficos diferentes envolvem fatores que estão fora do controle da organização. Como por exemplo: quando ha problema da operadora do serviço, ou algum problema físico no meio publico apresenta problema.

- Tecnologias de VPNs de diferentes fabricantes podem não trabalhar bem quando juntadas a novos padrões;
- VPNs precisam acomodar protocolos diferentes de IP e tecnologia de rede interna existente (conflito de IP);
- Necessidade de treinamento para quebra do paradigma cultural.

6 CONSIDERAÇÕES FINAIS

6.1 CONCLUSÃO

Usar uma VPN permite que todos possam compartilhar arquivos e usar aplicativos com maior produtividade e gerenciamento, como se todos os computadores estivessem conectados à mesma rede local. Pode-se até mesmo imprimir em impressoras da rede remota, da mesma forma que faria com uma impressora local. Assim o resultado alcançado fica acima das expectativas, visto que, com o uso de VPN o departamento de engenharia da ELETROBRÁS - Distribuição Acre pode fazer uso de sistemas de ordem técnica, diretamente da obra, ou de qualquer lugar, podendo assim trabalhar na rede da empresa em viagens ou até mesmo em casa, por exemplo.

A maior dificuldade encontrada é de nível cultural, pois os engenheiros e colaboradores do setor não têm a cultura de uso de técnicas de acesso remoto, mas isso é irrelevante diante do resultado encontrado, pois o ganho de produtividade adquirido trouxe mais benefícios à empresa do que prejuízos, assim, um investimento mínimo em treinamento resolveria essa questão de maneira rápida e fácil.

O trabalho foi desenvolvido com objetivo de entender a tecnologia VPN e sua aplicabilidade no gerenciamento remoto de empreendimentos/projetos. Em linhas gerais, a pesquisa e a empresa estudada alcançaram seus objetivos iniciais que eram a comprovação da importância da VPN no gerenciamento remoto de empreendimentos e a atuação como gestor de recursos ligados ao gerenciamento de projetos. Como foi visto no estudo apresentado, efetivamente essa relevância aconteceu e a VPN acabou sendo efetivamente usada como ferramenta para acesso remoto. Porém, existe uma grande barreira a ser rompida que a cultura de uso, e a única maneira de reverter esse quadro e investimento em treinamento e

capacitações do corpo de engenheiros. Possivelmente num futuro próximo, com a inclusão digital crescendo de forma exponencial, teremos um cenário que facilite mais ainda a inclusão desse tipo de tecnologia no ramo da construção civil e traga todos os benefícios argumentos no decorrer da pesquisa.

O grau de confiabilidade do sistema mostrou-se extremamente alto, visto se trabalhar com dados modificados em temos reais. Por utilizar-se da internet como meio de comunicação entre os pontos mostrou-se eficaz visto este serviço estar disponível praticamente 24 horas

A redução de custos e prazos e tempo de trabalho foram sentidos no setor de engenharia, até mesmo a outros setores, apesar de não haver um estudo profundo desses custos como um todo, até mesmo a integração com as ferramentas de gerenciamento foi reduzida graças a não modificação do sistema de gerenciamento em si, apenas na maneira como se conecta a rede.

6.2 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Algumas importantes questões surgiram no decorrer deste estudo e que, por não serem objetivos deste trabalho, não foram aprofundadas. Como sugestão tem-se o estudo mais aprofundado, dentro do escopo do gerenciamento de empreendimentos, de acompanhamento via software especifico para gerencia de projeto, como é o caso do MS-Project sobre VPN, trabalhando em camadas cliente-servidor. No campo especifico das VPN o aprofundamento dos protocolos de tunelamento e também o estudo das técnicas de criptografias utilizadas em uma VPN, além de outros estudos de casos baseados em outros tipos de VPN, com configurações mais seguras, como por exemplo certificados digitais sobre IPSec.

Também vimos que não houve um estudo profundo sobre a real economia com o tempo gasto quando houve a implantação da VPN, bem como dos recursos financeiros específicos.

Temos também que analisar o motivo pelo qual houve resistência de alguns usuários na implantação do sistema, apesar de para o usuário não ter sido modificado os protocolos de acesso a rede.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. *O Método nas ciências naturais e sociais*: pesquisa quantitativa e qualitativa. 2. ed. São Paulo: Pioneira, 1999.

CLUBE, Rede Privada Virtual, pesquisado na Web em junho de 2009 no Site Clube do Hardware, Endereço: www.clubedohardware.com.br.

CURY, Antonio. *Organizações & Métodos: uma visão holística*. 7. ed. São Paulo: Atlas, 2000.

DAVISON, JONATHAN. *Livro Fundamentos de VoIP*. 2 ed. Rio de Janeiro: Cisco Press, 2008.

FIGUEIREDO, N.M.A. (Org.). *Método e Metodologia na Pesquisa Científica*. São Paulo: Difusão Editora, 2004.

GABRIELA, Ferraz Catramby, pesquisado na Web em julho de 2009 no site http://www.abusar.org/vpn/vpn2.htm

GIL, A. C. *Métodos e técnicas de pesquisa social*. 4 ed. São Paulo: Atlas, 1995, p.105-113.

GOODPASTURE, John C., The *Project Office: Finding Pearls and Avoiding Perils*. In: Proceedings of the Project Management Institute Annual Seminars & Symposium, Houston, Setembro de 2000.

JENNINGS, Roger*. Usando Windows NT Server 4/ Tradução Follow-Up Traduções e Assessoria de Informática*. Rio de Janeiro: Campus, 1997.

LEOPARDI, M. T. *Metodologia da Pesquisa na Saúde*. Santa Maria: Pallotti, 2001, p. 193-278.

LEWIS, James P. *The Project Manager´s Desk Reference*, 2. ed., Boston : MacGraw-Hill, 2000.

MINAYO, M.C.S. *Ciência, técnica e arte: O desafio da pesquisa social*. In: MINAYO, M. C.S. (org). *Pesquisa social: Teoria, método e criatividade*. 17 ed. Petrópolis, RJ: Vozes, p.9-29, 1994.

NICHOLAS, John M. *Managing Business and Engineering Projects: concepts and implementation*, Nova Jersey: Prentice-Hall, 1990

ORTIZ, Eduardo Bellincanta. *VPN Implementando Soluções com Windows 2000 Server*. São Paulo: Árica, 2002.

POLIT, D.F.; HUNGLER, B.P. *Fundamentos de Pesquisa de Enfermagem*. 3 ed. Porto Alegre: Artes Médicas, 1995.391 p.

SOUZA, Lindeberg Barros de. *TCP/IP Básico e Conectividade em Redes*. São Paulo: Árica, 2002.

TANENBAUM, Andrew S. *Redes de Computadores* 4º Edição. Rio de Janeiro: Campus 2008.

TORRES, Gabriel. *Redes de Computadores Curso Completo*. Rio de Janeiro: Axcel Books do Brasil, 2008.

VERGARA, Sylvia Constant. *Projetos e relatórios de pesquisa em administração*. 2. ed. São Paulo: Atlas, 1998.

APENDICE A

1 IMPLANTAÇÃO DA TECNOLOGIA VPN

Esse tutorial tem o objetivo de mostrar como se configura uma intranet VPN para interligar usuários remotos do departamento de engenharia aos sistemas e serviços disponíveis na rede da ELETROBRÁS - Distribuição Acre.

1.1 Escolha de Sistema Operacional e demais softwares

Para este caso foram escolhidos com sistema operacional do servidor VPN o Windows 2000 Server e como protocolo da VPN o PPTP, alem de se trabalhar com um firewall baseado em linux(CentOS 5.4 com kernel 2.6) e com Iptables 1.3.5. A escolha dos softwares citados deve-se a disponibilidade das licenças de uso disponíveis na ELETROBRÁS - Distribuição Acre, variações desses configurações podem funcionar perfeitamente.

1.2 Configurando o Firewall

Como geralmente um servidor VPN funciona atrás de um firewall3, ajustes de regras devem ser acertados antes de se configurar o serviço. Será necessário a filtragem de portas, alem de utilizar o protocolo GRE no firewall, basicamente as configurações são as seguintes:

[3] Firewall é o nome dado ao dispositivo da rede que tem por função regular o tráfego entre redes distintas, além de impedir a transmissão de dados nocivos ou não autorizado de uma rede a outra.

- Fazer a filtragem da porta 1723, que é utilizada pelo protocolo PPTP, redirecionando os pacotes direcionados a ela(NAT4) para um IP de rede local(IP do servidor VPN) na mesma porta;
- Habilitar o protocolo GRE, que é necessário para criação do túnel da VPN;

As regras ficarão assim:

```
Iptables -t nat -A PREROUTING -p tcp -s 0/0 --dport 1723 -j DNAT --to 172.16.0.20:1723
Iptables -t nat -A PREROUTING -p gre -s 0/0 -j DNAT --to 172.16.0.20
```

Observe que no exemplo acima o IP da rede local que será usado no servidor VPN é 172.16.0.20 e que essa regra aceita pacotes proveniente de qualquer origem(-s 0/0), que pode ser considerado como uma falha de segurança, pois, qualquer pessoa conectada a internet pode ficar tentando ingressar na VPN, para resolver esse problema tivemos que solicitar que nosso parceiro obtivesse um IP valido na internet, resolvendo de vez esse problema e deixando a regra assim:

```
Iptables -t nat -A PREROUTING -p tcp -s 200.252.165.140 --dport 1723 -j DNAT --to 172.16.0.20:1723
Iptables -t nat -A PREROUTING -p gre -s 200.252.165.140 -j DNAT --to 172.16.0.20
```

Assim o firewall somente aceitará os pacotes provenientes do IP 200.252.165.140, que é o IP do escritório de cobrança.

Também é importante fazer LOG do acesso da VPN no firewall para checar possíveis problemas e tentativas de invasão futuras, para fazer isso basta incluir a seguinte regra no firewall:

```
iptables -A INPUT -p tcp --dport 1723 -j LOG --log-prefix "VPN: "
iptables –A INPUT -p gre –j LOG –log-prefix “GRE: “
```

---

[4] NAT(Network Adress Translation) consiste numa série de tarefas que um roteador (ou equipamento equivalente) deve realizar para converter endereços IPs entre redes distintas.

1.3 CONFIGURANDO O SERVIDOR VPN

1.3.1 Configurando a Rede

Como foi informado anteriormente o IP local (que deve ser fixo) do servidor VPN nesse exemplo será 172.16.0.20, então devemos configurar a interface de rede para isso. Como mostra a figura 14 abaixo:

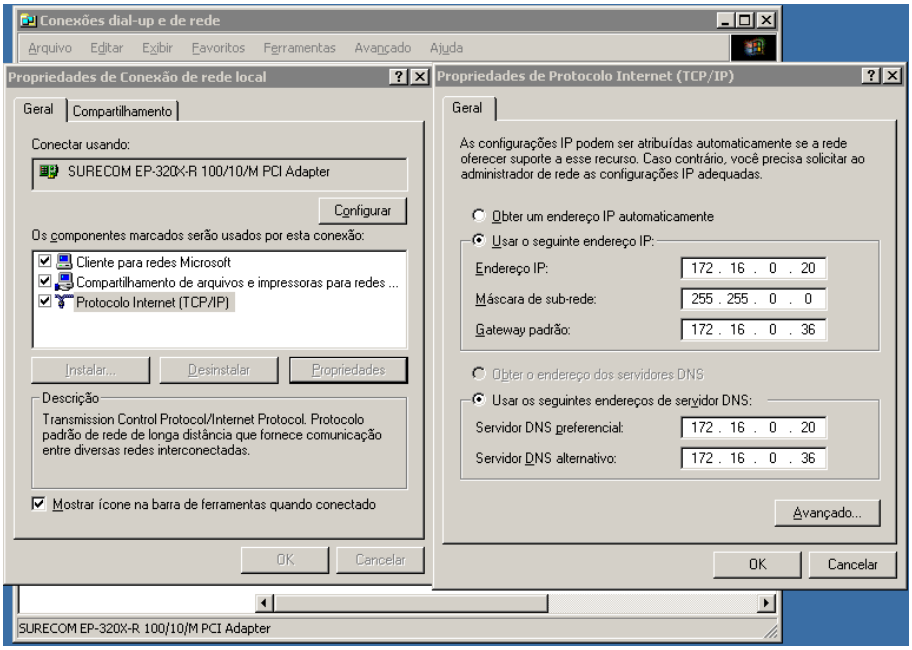

Figura 14 Propriedades da Conexão de Rede

1.3.2 Instalando o Servidor VPN

Para iniciar a instalação do servidor VPN, seguiremos os seguintes passos: Iniciar ► Configurações ► Painel de Controle;

Nessa tela acessaremos a opção “Adicionar ou Remover Programas” e dentro dela selecionar a opção “Adicionar ou Remover Componentes do Windows”. Conforme mostrado na figura 15 a seguir:

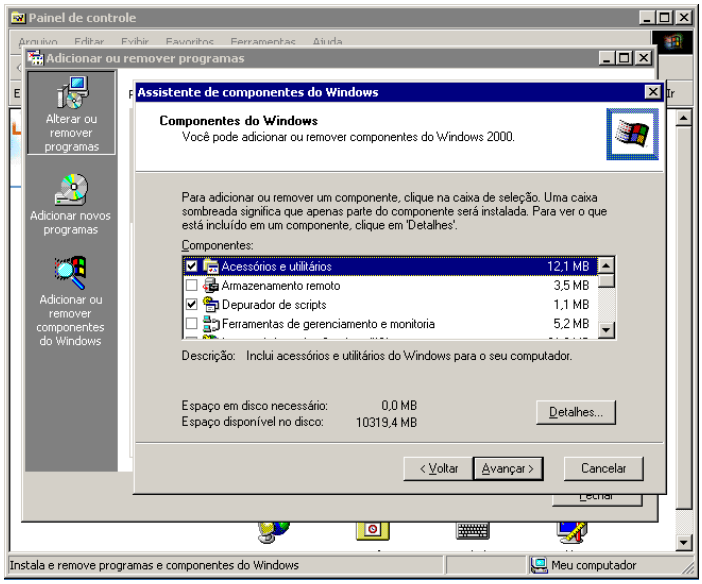

Figura 15 Componente do Windows

Será necessário a instalar o serviço IAS5 , que está disponível na opção “Serviços de rede” que por sua vez se encontra em “Assistente de componentes do Windows” como mostrado na figura 16 a seguir:

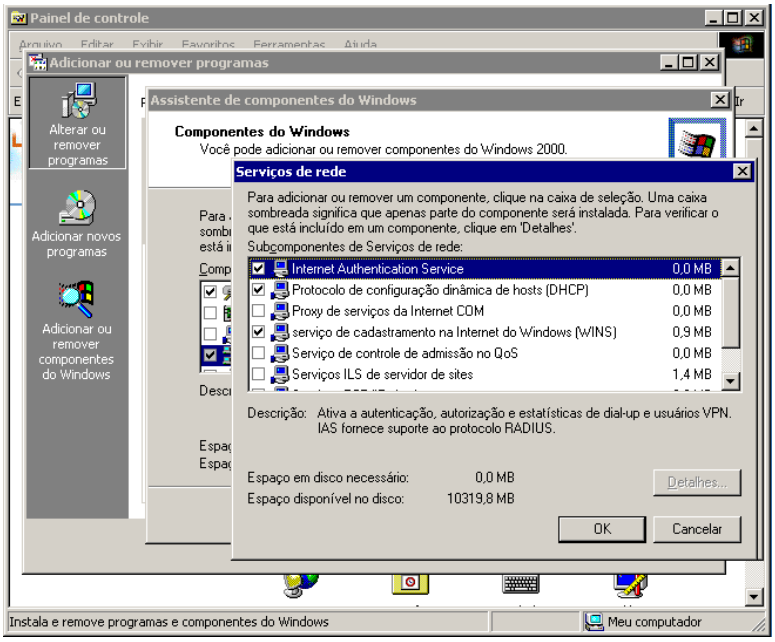

Figura 16 IAS

[5] IAS (Internet Authentication Service) é um serviço do Windows Server que deve ser instalado quando há a necessidade de trabalhar com autenticação pela internet de outro serviço

Após a o clique no botão “OK” o Windows retorna a tela anterior, em seguida clica-se em “Avançar”, e será terminada a instalação do IAS. Agora é necessário configurar o IAS entrando na tela:

Iniciar ► Programas ► Ferramentas Administrativas ► Internet Authentication Service.

Como é possível observar na figura 14, o console do IAS é formado por três componentes básicos:

- Clientes: Local onde devem ser cadastrados todos os clientes Radius6;
- Log de acesso remoto: Local onde pode-se configurar as características do arquivo de LOG deste serviço nesse componente;
- Diretivas de Acesso Remoto: Onde os critérios exigidos para os clientes VPN se conectem ao servidor são configurados;

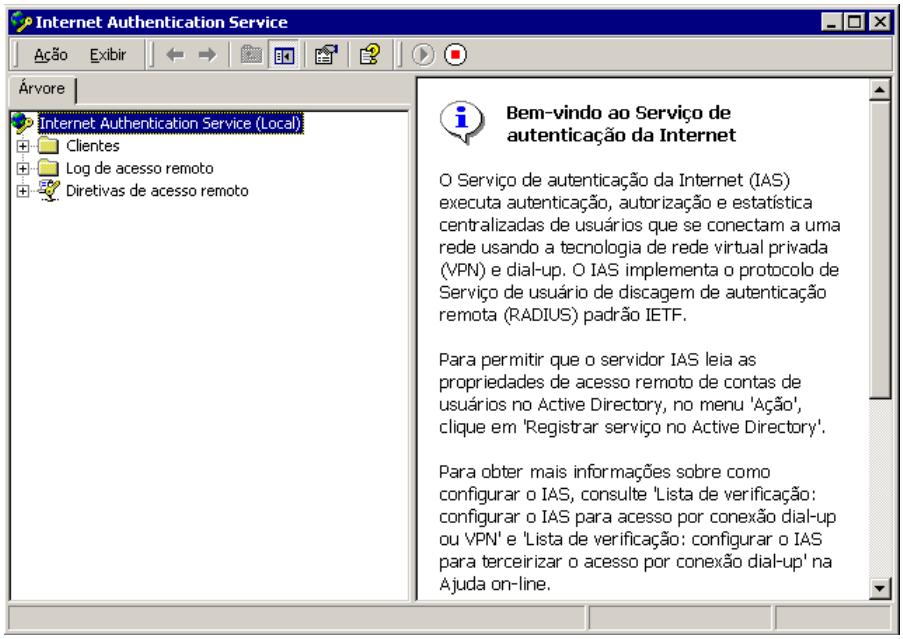

Figura 17 Configurar IAS

Agora para iniciar a configuração clicamos com o botão direito do mouse sobre “Clientes” e selecionamos a opção “Novo Cliente”, em seguida preenchemos os campos “Nome Amigável” com um nome que identifique de forma fácil o servidor RADIUS e o campo protocolo com “Radius”, como mostrado na figura 18 a seguir:

[6] RADIUS (Remote Authentication Dial In User Service) - Serviço de autenticação remota de usuários discados.

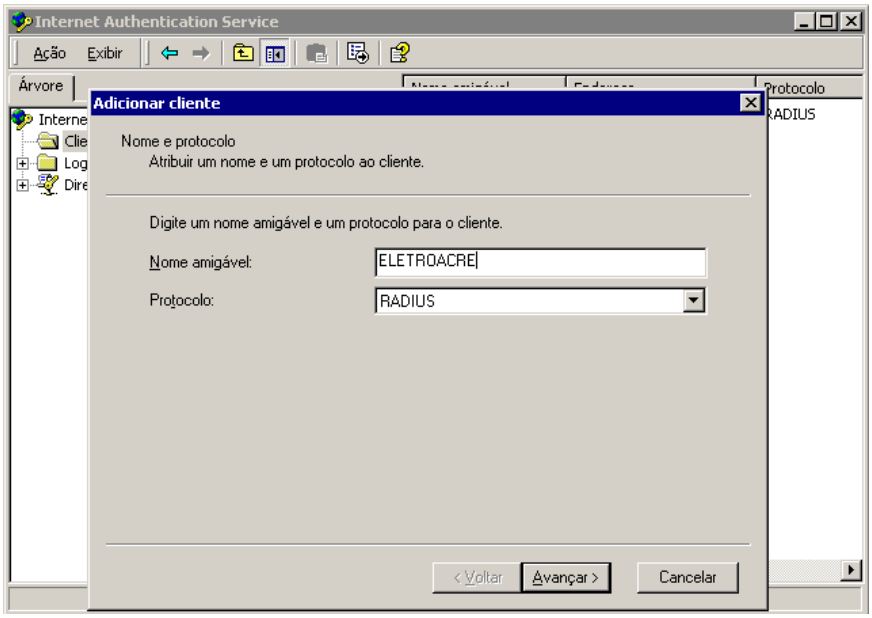

Figura 18 Configurando novo cliente Radius

Clicando em “Avançar”, outras configurações serão solicitadas, o endereço IP do servidor além do nome do fornecedor, que deve ser preenchido com Microsoft, e uma senha que será usada posteriormente na configuração do acesso remoto como mostrado na figura 19 a seguir:

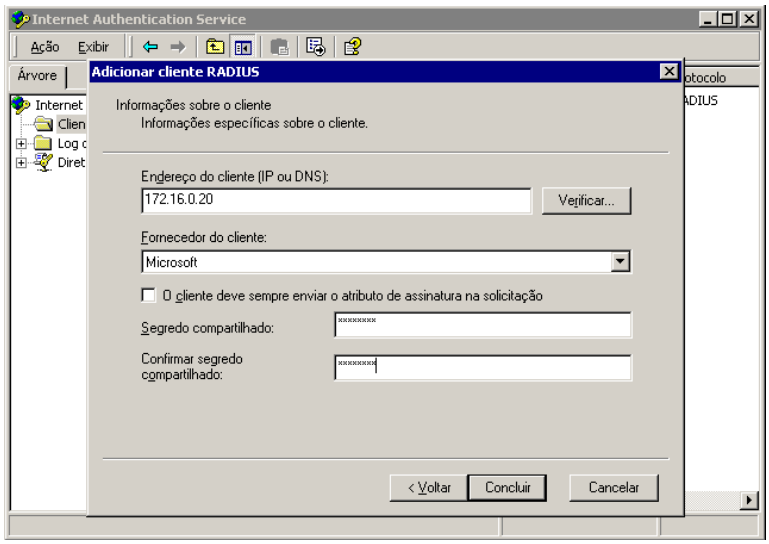

Figura 19 Configuração do Cliente

Após clicar em “Concluir”, deve-se observar que o cliente com nome “ELETROBRÁS - DISTRIBUIÇÃO ACRE” aparecerá na lista de clientes. Agora é

necessário registrar o serviço IAS no Active Directory7 e para fazer isso basta dar um clique com o botão direito do mouse sobre o item “Internet Authentication Service” e selecionar o item “Registrar serviço no Active Directory” como mostrado na figura 17 a seguir:

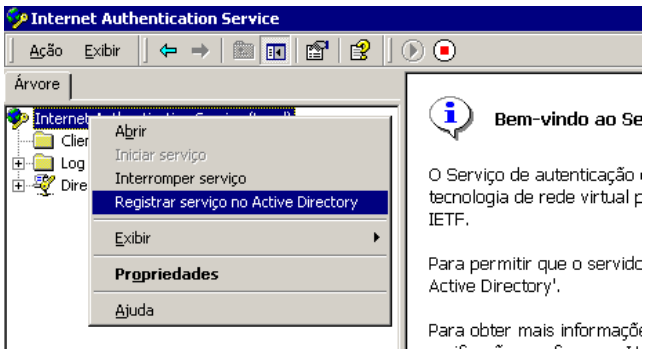

Figura 20 Registrando o IAS no Active Directory

Logo após isso duas confirmações aparecerão, a primeira fala que o cliente Radius está autorizado a discagem dos usuários e a segunda pede para confirma se o computador em que o IAS está rodando terá acesso as propriedades dos usuários, daí é so confirma “OK”. Logo após isso a implementação do IAS estará concluída e podemos passar para o próximo passo que é a implantação do serviço de VPN e para iniciar esta instalação seguiremos os seguintes passos:

Iniciar ► Programas ► Ferramentas Administrativas ► Roteamento e Acesso Remoto

Após isso aparecerá o console do de Roteamento e Acesso Remoto, para configurar esse serviço basta clicar com o botão direito do mouse sobre o item ELETROBRÁS - DISTRIBUIÇÃO ACRE(item do IAS criado anteriormente) e selecionar a opção ”Configurar e ativar roteamento e acesso remoto”, após isso será aberto o assistente para configuração do servidor e depois clicar em avançar, na tela seguinte selecionar a opção “Servidor Configurado Manualmente” e na tela seguinte clicar em concluir. Finalmente após isso o servidor pergunta se queremos iniciar imediatamente o serviço, clicamos em “Sim” e então o serviço deve está iniciado. Agora acessaremos as propriedades do servidor, clicando com o botão direito em cima do nome do servidor, no nosso caso o nome dele é EA-10, e acessando a

[7] Active Directory é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows.

opção “propriedades”, logo em seguida a aba IP, como mostrado na figura 21 a seguir:

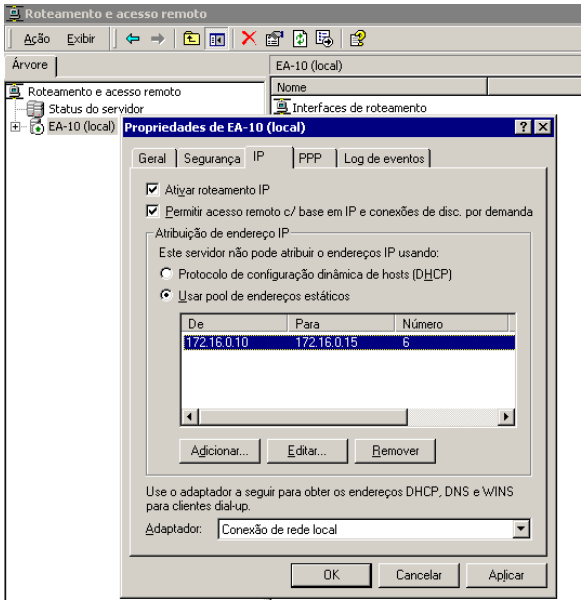

Figura 21 Propriedades do Servidor

Nessa tela devemos ativar as opções “Ativar roteamento IP” e “Permitir acesso remoto” alem de definir uma faixa de IP’s que serão distribuídos pela VPN as clientes que se conectarem, nesse exemplo a faixa é: 172.16.0.10-172.16.0.15, ou seja, 6 IP’s, também escolheremos o adaptador de rede, no nosso exemplo será o de rede local(definido anteriormente).

O próximo passo será a configuração das portas de comunicação e definir o protocolo de tunelamento usado, nesse exemplo serão permitidas somente conexões por meio do protocolo PPTP. Para configurar as portas, observar a figura 22 a seguir, clique com o botão direito em “Portas” e selecione “Propriedades”.

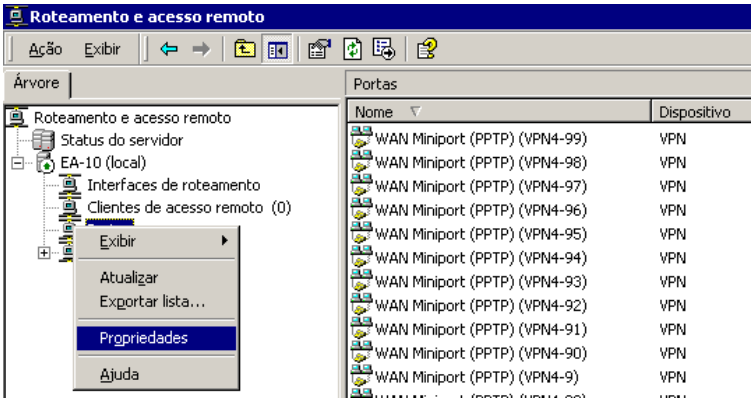

Figura 22 Portas

Desabilite todas as portas L2TP, pois não serão usadas nesse servidor, ou seja, sete como número de L2TP “0”, como mostrado na figura 23 abaixo, entre em configuração da porta PPTP:

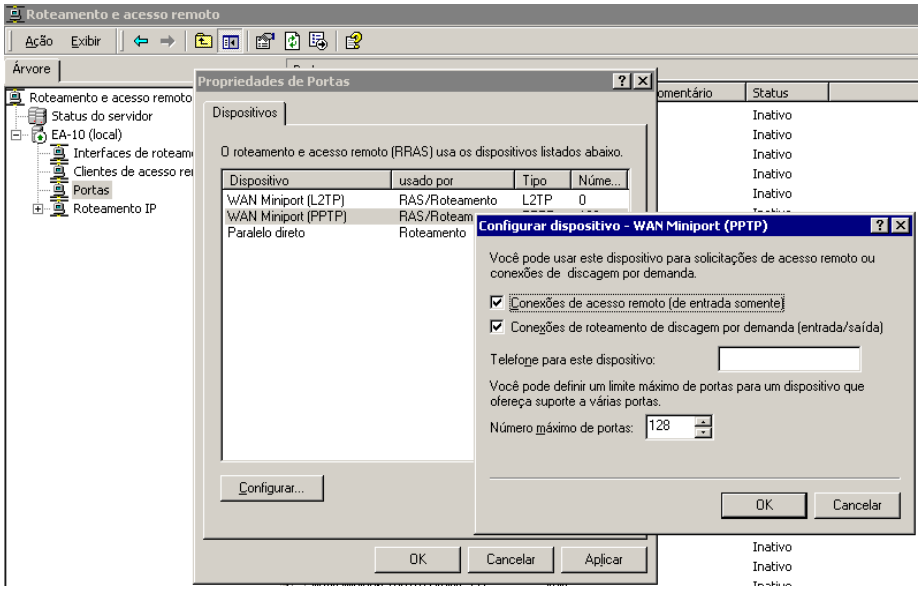

Figura 23 Propriedades da porta PPTP

Nessa tela você deve setar as opções “Conexões de acesso remoto(de entrada somente)” e “Conexões de roteamento de discagem por demanda(entrada/saída)” alem de setar o numero máximo de portas como 128. Com essa tarefa a configuração do serviço de IAS e roteamento e acesso remoto está concluída a VPN já esta funcional e no próximo item trataremos de questões de segurança da VPN.

1.4 CONFIGURANDO A SEGURANÇA E AUTENTICAÇÃO

Para implementar as configurações de segurança e autenticação, devemos acessar o console “Roteamento e acesso remoto”. Com o mesmo aberto clicamos com o botão direito sobre o servidor e em seguida em propriedades como mostra a figura 24 seguir:

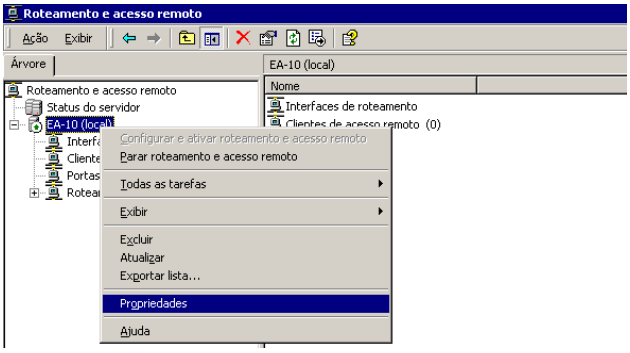

Figura 24 Acesso as propriedades do servidor

Para registrar os eventos ocorridos no servidor VPN, devemos acessar a aba "Log de eventos" do console "Propriedades de Server". Feito isso, selecionar a opção "Registrar o máximo de informações no log" e marcando também o item "Ativar o log do protocolo ponto a ponto (PPP), conforme figura 25. Para continuar, clicaremos no botão "OK".

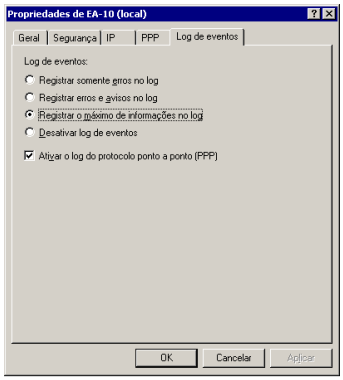

Figura 25 Log de Eventos

Para habilitar as configurações efetuadas, o assistente irá solicitar que reiniciemos o serviço de roteamento e acesso remoto. Para reiniciar o serviço, basta dicar no botão "Sim".

É muito importante verificar se os serviços de roteamento e acesso remoto foram reiniciados com sucesso. Observe que o ícone do servidor apresenta uma seta apontando para cima. Isto significa que o serviço está operante.

Agora devemos configurar o log no servidor Radius. Acessando o console do serviço IAS, conforme a figura 26. Selecionaremos a opção "Log de acesso remoto" e clicando com o botão direito sobre o item "Arquivo local. Feito isso, dique na opção "Propriedades" para configurar o log do sistema.

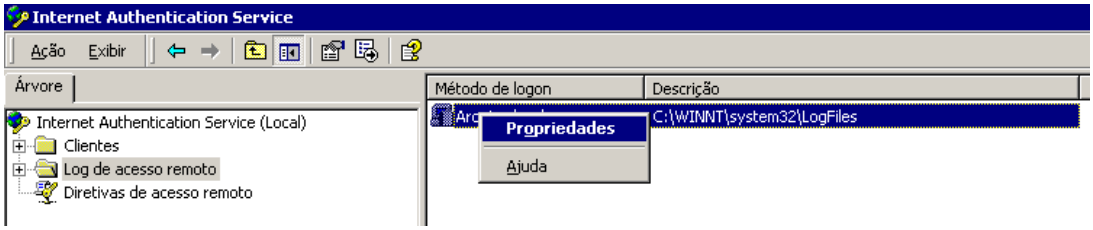

Figura 26 Log de acesso remoto

Para registrar as ocorrências desse servidor, devemos marcar as seguintes - opções: "Registrar solicitações de autenticação" e "Registrar status periódico". Se for necessário configurar o arquivo de log gerado, basta selecionar a aba "Arquivo Local", conforme figura 24. Dentro desta janela pode ser determinado se o arquivo de log será diário, semanal ou mensal. Podemos determinar também o tamanho físico desse arquivo e a sua localização.

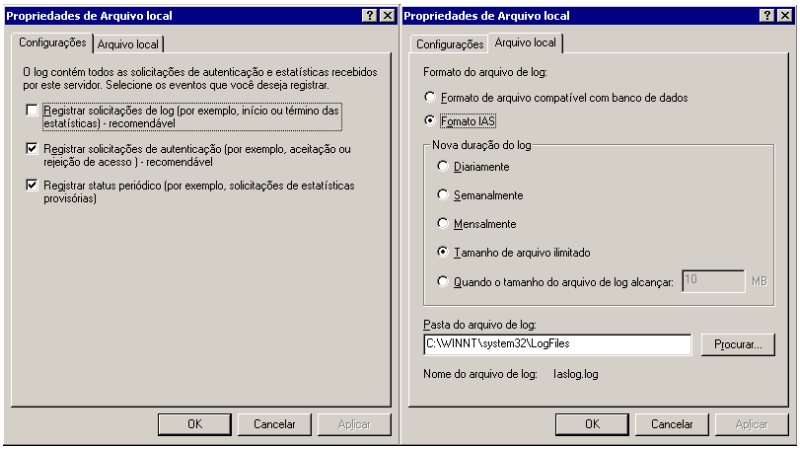

Figura 27 Propriedades de arquivo local

Agora vamos as diretivas de acesso remoto. Selecionando o item "Diretivas de acesso remoto" e clicando com o botão direito sobre a opção "Permite acesso se a permissão ... ". Clicamos sobre o item "Propriedades" para configurar as diretivas. Nesta janela devemos marcar a opção "Conceder permissão de acesso remoto". Desta forma, os usuários só se conectarão se os critérios exigidos nas diretivas forem atendidos. Observe a figura 28. Para adicionar critérios, devemos clicar no botão "Adicionar..,".

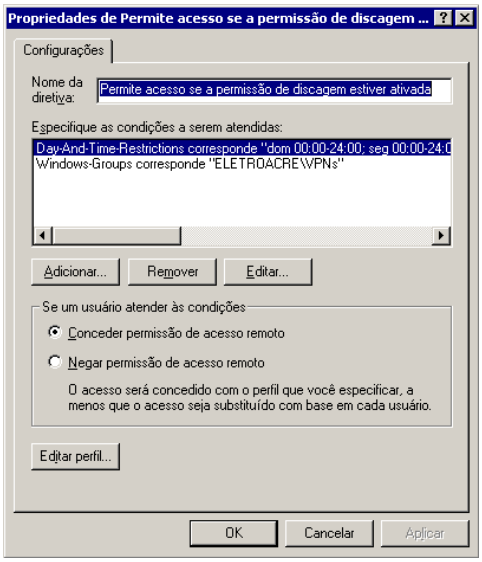

Figura 28 Diretivas de acesso remoto

Surgirá então uma lista de atributos que serão implementados como critérios exigidos para conexões. Neste exemplo, como pode ser visto na figura 29, devemos selecionar o atributo "Windows-Groups".

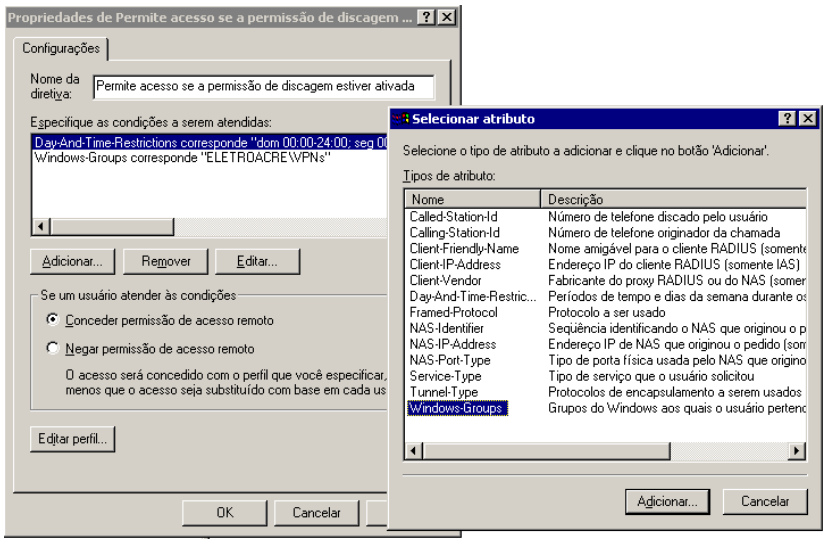

Figura 29 Atributos

Na próxima janela devemos incluir os grupos que terão acesso ao servidor VPN por meio de conexões remotas. Para continuar, dique no botão "Adicionar". A figura 30 que o console traz uma relação com todos os grupos existentes nesse servidor. Para este exemplo, escolhemos o grupo VPN, assim somente quem pertencer a esse grupo terá permissão de se conectar ao servidor VPN. Para incluir o grupo, basta selecioná-lo e clicar no botão "Adicionar". Dando continuidade, dique no botão "OK".

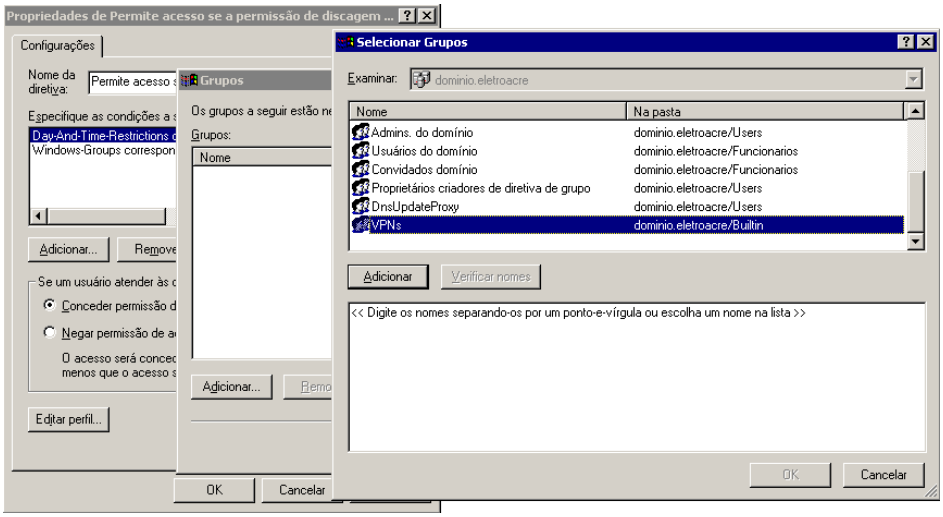

Figura 30 Selecionar grupos

Observe que na janela seguinte o grupo selecionado já está incluído. Para continuar, clique no botão "OK". Agora como exemplo vamos editar uma diretiva que já vem como padrão no Windows 2000 Server. Você deve selecionar a diretiva "Day-and-Time-Restrictions" e clicar sobre o botão "Editar".

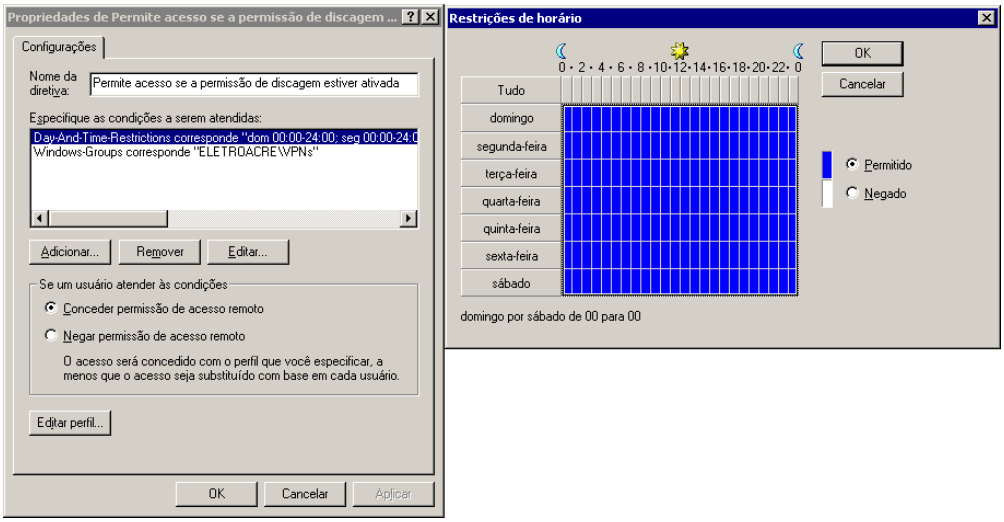

Figura 31 Diretivas de horários e acessos

Agora devemos configurar os dias e horários nos quais usuários do grupo VPN's podem acessar o servidor VPN. Veja na figura 31 que foi imposto um horário liberado, mas, conforme a necessidade esse horário pode ser restrito, por exemplo ao horário de funcionamento da empresa. Podemos configurar esses horários da maneira que achar melhor, porém fora dos horários especificados ninguém pode acessar o servidor. Para continuar, escolha os dias e horários e dique no botão "OK".

Observe que os critérios que foram selecionados estão aparecendo. Para editar o perfil desta diretiva de acesso remoto, devemos clicar no botão "Editar perfil". No console "Editar perfil de discagem" devemos configurar as formas de criptografia, os métodos de autenticação, filtros de pacotes ip, entre outras coisas.

Selecionando a aba "Restrições de discagem" observe que existem várias opções de restrições. Marque a opção "Desconectar se ocioso por:" e informe o tempo de 10 minutos, o que vai desconectar a conexão que não apresentar tráfego por 10 minutos. O administrador da rede também pode restringir a conexão pelo tipo de mídia utilizado pelo cliente. Marcando a opção "Restringir a mídia de discagem", serão habilitadas as mídias para escolha. Caso desejemos que somente usuários de ADSL tenham acesso a esse servidor, deve marcar a opção "ADSL-DMT" e assim sucessivamente para as demais mídias. Se o administrador preferir alterar o tipo de autenticação utilizado, basta clicar na aba "Autenticação" deste console. Veja na figura 32 os tipos de autenticação disponíveis para o Windows 2000 Server além da informações citas nesse parágrafo.

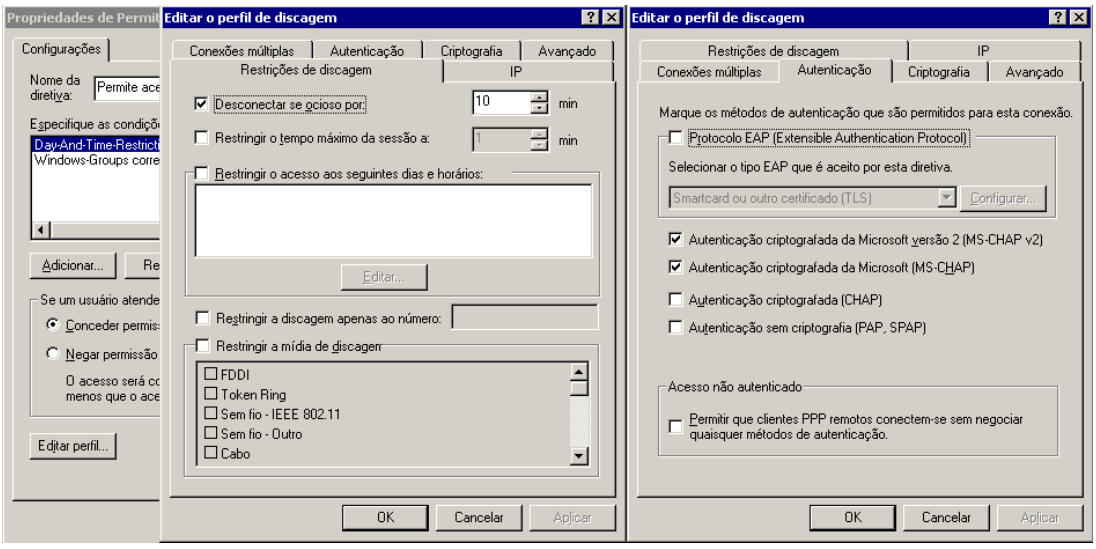

Figura 32 Perfis de discagem

Neste exemplo serão permitidas somente autenticações utilizando os métodos MS-CHAP e MS-CHAP v2. Para definir o nível de segurança das conexões VPN, dique na aba "Criptografia", conforme figura 30, observe que o administrador pode escolher entre quatro tipos de criptografja:

- Sem criptografia - Os membros deste perfil não podem se autenticar utilizando criptografia se esta opção for marcada;

- Básico - Com esta opção selecionada, os membros deste perfil podem utilizar criptografia de dados IPSec, DES 56 Bits e MPPE 40 bits;
- Forte - Utiliza os mesmos métodos de criptografia de dados da opção anterior. A diferença entre elas esta na criptografia MPPE de 56 bits implementada na opção "Forte";
- Mais forte - Trabalha com criptografia de dados IPSec, 3DES e MPPE de 128 bits;

Neste exemplo, selecionaremos as opções "Básico" e "Forte" para continuar. Se for necessário filtrar o tráfego de entrada e o de saída nos túneis de conexão VPN, selecione a aba "IP".

Para configurar o filtro de pacotes do cliente, clicamos no botão "Do cliente ... " para implementar o filtro. Conforme figura 33 a seguir.

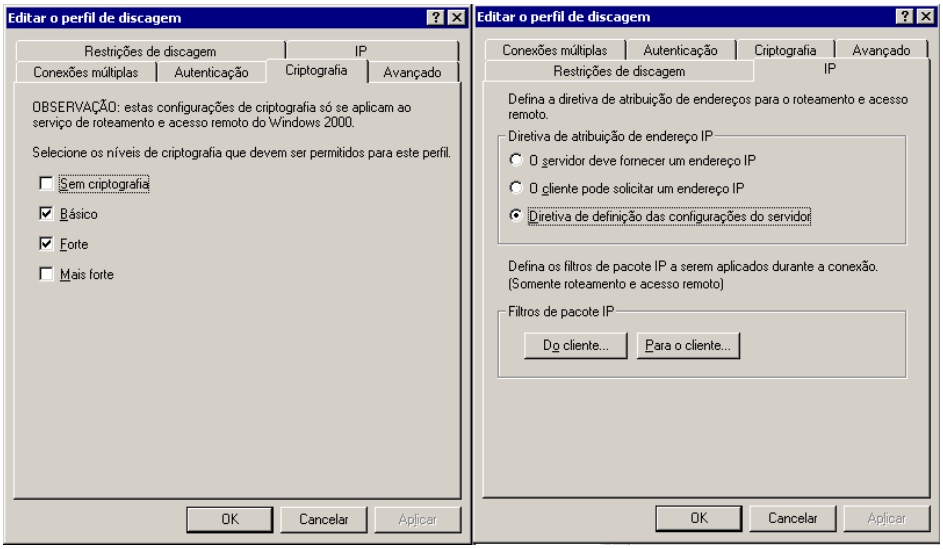

Figura 33 Editar o perfil de discagem – IP e Criptografia

Clicamos sobre o botão "Adicionar ..." para criar o filtro de pacotes para o cliente. Preenchemos os campos conforme figura 34. Desta forma todos os pacotes solicitados para o servidor serão verificados.

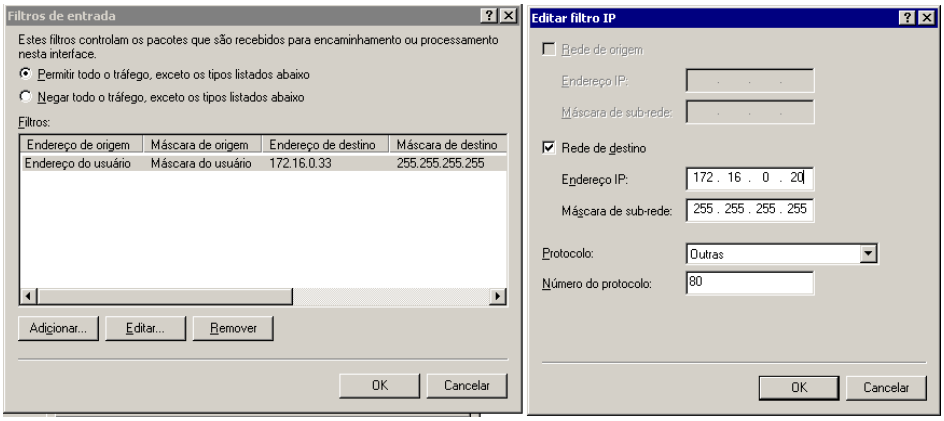

Figura 34 Filtro de IP

Neste exemplo serão filtradas as solicitações referentes às páginas de internet. Nenhum tráfego internet será aceito nas conexões. Se você preferir liberar o servidor VPN, não preencha estes campos. Nesse estudo de caso, a ELETROBRÁS - Distribuição Acre e o Escritório de Cobrança terão acesso a intranet da empresa; se implementarmos os filtros, ninguém terá acesso remoto a ela.

Chegou a hora de configurar o servidor VPN como cliente do servidor Radius. Desta forma implementaremos mais um nível de segurança à rede VPN.

Acessando o console "Roteamento e acesso remoto" para configurar o cliente Radius. Clicamos com o botão direito do mouse sobre o servidor e clicamos na opção "Propriedades".

No console "Propriedades de Server", abriremos a aba "Segurança". Devemos informar os métodos de autenticação escolhidos no servidor IAS. Os métodos de autenticação devem ser os mesmos no servidor IAS e no servidor VPN.

Selecionaremos, conforme a figura 32, os métodos de autenticação "MS-CHAP" e "MS CHAP v2". Lembrando que estes são os mesmos métodos utilizados nas configurações do servidor Radius. Para continuar as configurações, clicamos no botão "OK". Configuraremos o servidor VPN para autenticação Radius. Para isso, clicaremos na opção "Autenticação Radius" no item "Provedor de autenticação" conforme figura 32. Após escolher a autenticação Radius, clicaremos sobre o botão "Configurar" para informar o endereço e a senha do servidor Radius.

Clicamos no botão "Adicionar" para incluir um servidor Radius a esta configuração. Caso haja outros servidores de autenticação na rede, você devemos informá-los aqui.

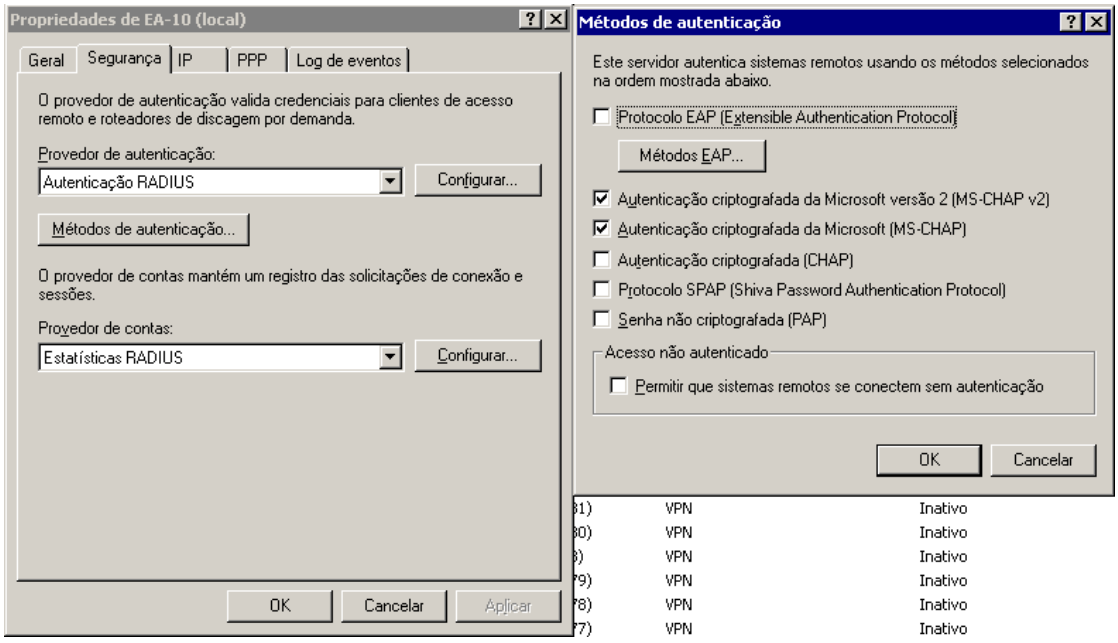

Figura 35 Métodos de Autenticação

Preencheremos os campos solicitados. No campo "Nome do servidor" informe o endereço IP fixo do seu servidor Radius.

Para configurar a senha desse cliente Radius, clique no botão "Alterar". Digitaremos a mesma senha que foi configurada no servidor Radius. Caso a senha informada no cliente não for a mesma do servidor, não haverá troca de informações entre eles. Informaremos a senha e clicaremos no botão "OK" para continuar a configuração. Após a definição da senha, clicamos no botão "OK" e o servidor Radius foi configurado no roteamento e acesso remoto do Windows 2000 Server.

O assistente de roteamento e acesso remoto vai informar que depois de configurada a autenticação Radius será necessária a reinicialização do serviço.

Depois de configurado com sucesso o provedor de autenticação como sendo a autenticação Radius, Devemos configurar o provedor de contas para fazer estatísticas do serviço Radius.

Selecionaremos a opção "Estatísticas Radius" no item "Provedor de contas" e dique no botão "Configurar. .. ". Veja a janela apresentada e observe que é a mesma tela da configuração feita para adicionar o servidor Radius.

Então sem maiores mistérios, clicaremos no botão "Adicionar ... " para continuar a configuração do provedor de contas.

Veremos uma janela que informa que o serviço está sendo reiniciado. Desta forma todas as configurações efetuadas estarão disponíveis após a volta do serviço.

Depois disso a tarefa estará pronta, verificamos se o serviço de roteamento e acesso remoto voltou ao ar.

Verificaremos se o ícone que representa o servidor está com uma seta verde apontando para cima. Estas foram as configurações necessárias para o estabelecimento de autenticações e estatísticas Radius. Observe que teremos que configurar os clientes que terão acesso remoto a esse computador. Entraremos no seguinte caminho:

Iniciar ► Programas ► Ferramentas administrativas ► Usuários e computadores do Active Directory.

Clicaremos o item "*Users*". Selecionaremos o usuário que pode acessar esse computador remotamente e clicando com o botão direito sobre ele, selecionaremos a opção "Propriedades". Conforme mostrado na figura 36 a seguir.

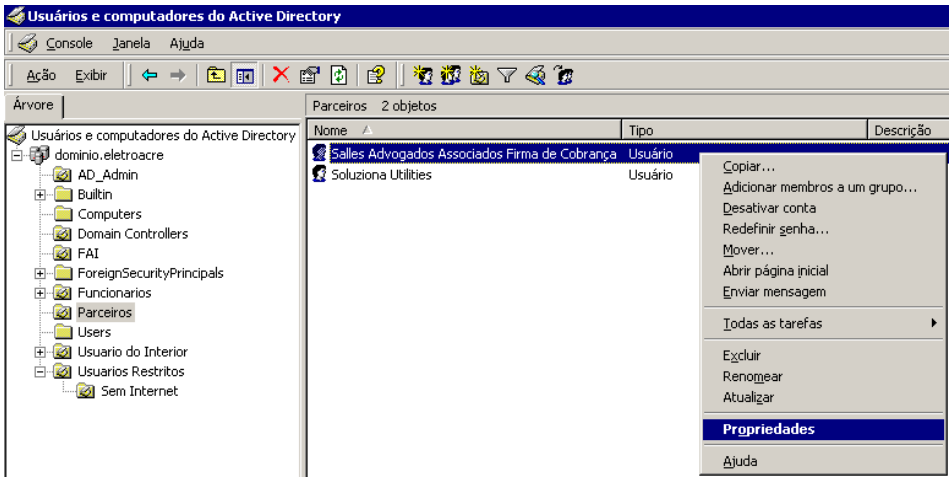

Figura 36 Usuários da VPN

Acessando a aba "Discagem" e clicando sobre a opção "Permitir acesso". Caso esta opção não esteja selecionada, o usuário não conseguirá se conectar ao servidor pelo acesso remoto.

Desta forma encerramos as configurações de segurança e autenticação deste exemplo. Mais uma vez, vale a pena frisar que para uma implementação deste porte possa ter sucesso, um estudo detalhado das necessidades da empresa deve ser feito antecipadamente. Devemos sempre procurar prever os problemas que possamos ter em um projeto deste tipo e analise a situação por partes para poder chegar à solução completa com sucesso.

1.5 CONFIGURANDO OS CLIENTES DE ACESSO

A partir do Windows 98SE, todos a Microsoft já disponibiliza um cliente VPN em seus sistemas operacionais. A configuração desses clientes é bastante simples e é o que falaremos agora. Nesse caso o sistema operacional usado é o Windows XP SP2 e para configurá-lo clicaremos em:

Iniciar ► Configurações ► Conexões de Rede

Na janela “Conexões de Rede”, clicaremos em “Criar nova conexão” e então deverá aparecer o assistente para novas conexões, conforme mostrado na figura 37 a seguir.

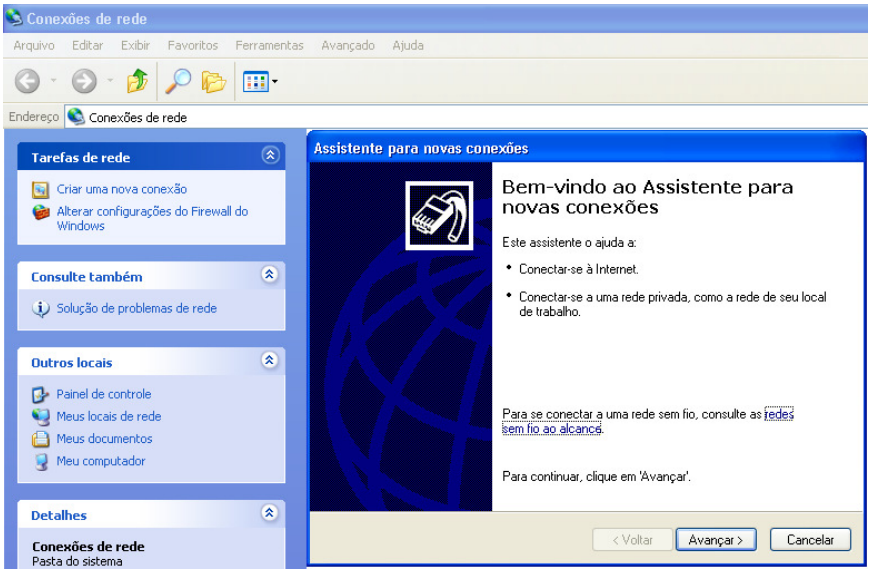

Figura 37 Conexões de rede

Clicaremos em avançar. Na tela posterior escolheremos a opção “Conectar-me a uma rede em meu local de trabalho” e na próxima tela será perguntado como desejamos nos conectar a essa rede, responderemos marcando a opção “Conexão VPN”, conforme mostrado na figura 35 a seguir.

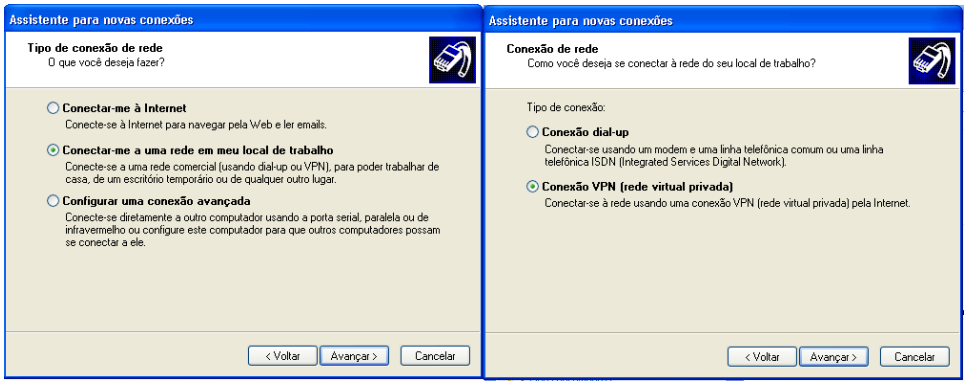

Figura 38 Assistente para novas conexões

Em seguida informaremos o nome da empresa que queremos nos conectar, esse nome pode ser dado a nossa escolha, mas o ideal é que o mesmo seja ELETROBRÁS - DISTRIBUIÇÃO ACRE. Na tela seguinte o assistente pergunta se queremos discar uma outra conexão antes, no nosso casso não faremos isso porque o escritório de cobrança possui link de Internet, conforme mostrado na figura 39 a seguir.

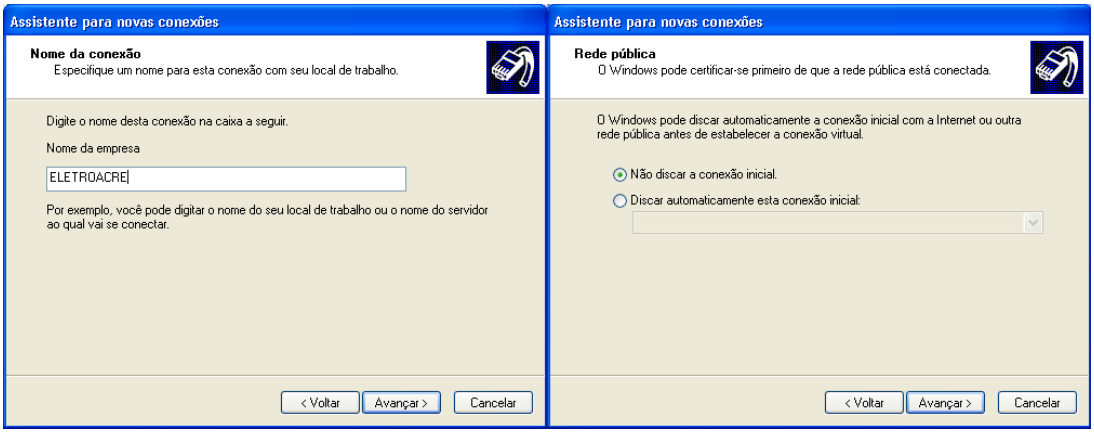

Figura 39 Finalizando o Assistente

Logo em seguida o assistente perguntará o endereço IP do servidor, no nosso caso o endereço IP do firewall da ELETROBRÁS - Distribuição Acre, que é 200.252.28.1 e por fim sugere que criemos um ícone na área de trabalho da conexão, conforme mostrado na figura 40 a seguir.

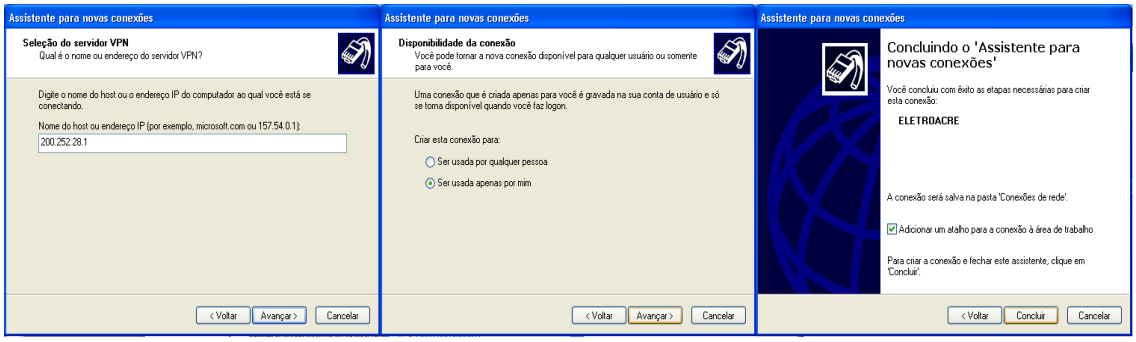

Figura 40 Passos finais

Ao fim do assistente a conexão aparece imediatamente na tela, e para otimizá-la faremos algumas modificações. Clicaremos em “Propriedades”, na orelha “Opções”, marcaremos a opção “incluir domínio de logon do windows”. Na orelha “Rede”, marcaremos o “Tipo da VPN” como “PPTP VPN”. Após isso veremos que foi incluído na tela de logon o campo “Domínio Windows”, faltando somente conectar na VPN, como mostrado na figura 41 a seguir.

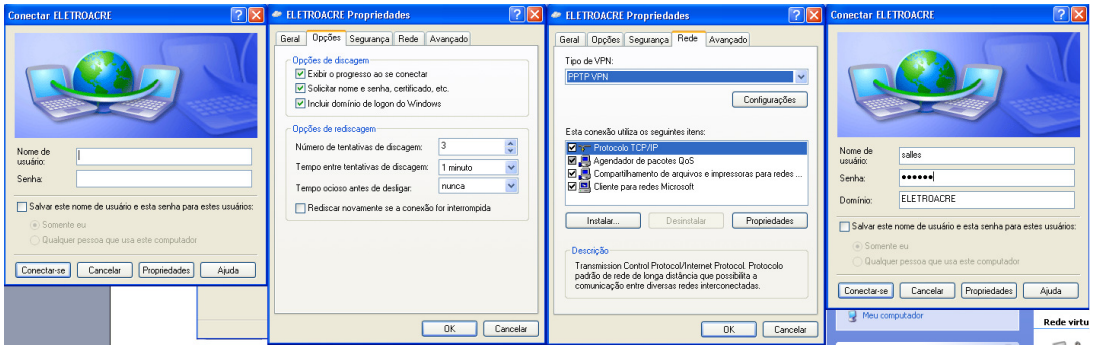

Figura 41 Conectando na VPN

Finalmente estaremos conectados a VPN da empresa com todos os cuidados tomados na implantação do servidor, que incluem criptografia, restrição de IP de origem, restrições de horários além de logar tudo que acontece na conexão, como mostra a figura 42 a seguir.

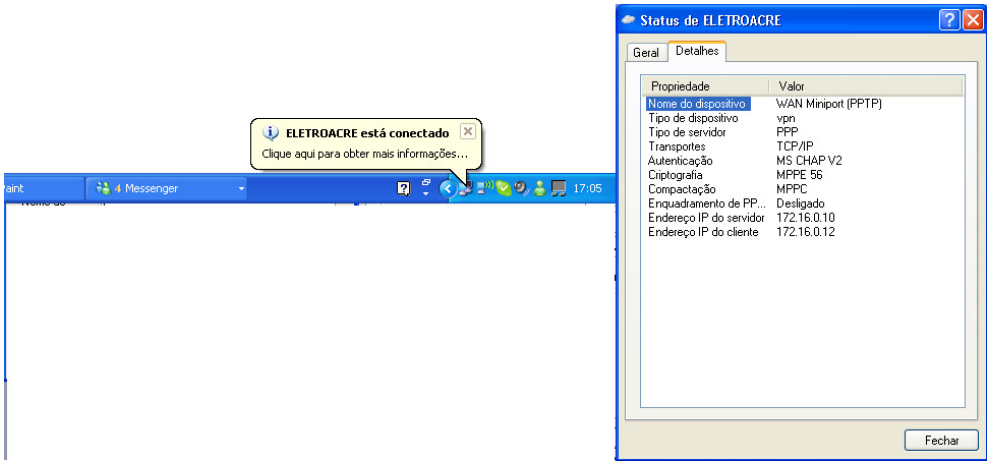

Figura 42 VPN conectada

ANEXO

Pesquisa do nível de satisfação dos usuários VPN

1. Qual o seu nível de satisfação com a implantação e uso da VPN?

Totalmente Insatisfeito	Insatisfeito	Indiferente	Satisfeito	Totalmente Satisfeito

2. Em sua opinião qual o nível de relevância da VPN para gerenciamento dos projetos desenvolvidos na Eletrobrás – Distribuição Acre?

Totalmente Irrelevante	Irrelevante	Considerável	Relevante	Totalmente Relevante

3. Em sua opinião a tecnologia VPN é aplicável à empresa?

Sim	Não

4. A implantação da VPN diminuiu o tempo gasto com o acompanhamento do projeto?

Sim	Não

5. Em sua opinião, os gastos financeiros com o projeto podem de alguma forma diminuir com o uso dessa tecnologia?

Sim	Não

6. A implantação da VPN foi de fácil adaptação ao setor?

Sim	Não

7. Você sentiu dificuldade ou desconfiança no sistema?

Sim	Não