UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTOS ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

ELIU CAMARGO HAHNER
WALLACE GRIZ AYRES

PROPOSTA DE UMA SOLUÇÃO DE ACESSO REMOTO SEGURO PARA EAD

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2015

ELIU CAMARGO HAHNER
WALLACE GRIZ AYRES

PROPOSTA DE UMA SOLUÇÃO DE ACESSO REMOTO SEGURO PARA EAD

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. MsC. Cristian C. S. Mendes

CURITIBA
2015

TERMO DE APROVAÇÃO

ELIU CAMARGO HAHNER
WALLACE GRIZ AYRES

PROPOSTA DE UMA SOLUÇÃO DE ACESSO REMOTO SEGURO PARA EAD

Este trabalho de conclusão de curso foi apresentado no dia 22 de julho de 2015, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Ph.D. Augusto Foronda
UTFPR

_____
Prof. MsC. Lincoln Herbert Teixeira
UTFPR

_____
Prof. MsC. Christian C. S. Mendes
Orientador - UTFPR

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

RESUMO

HAHNER, Eliu Camargo; AYRES, Wallace Griz. Mídia com VPN pré-configurada. 2015. 27 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Devido ao aumento das tecnologias disponíveis no mercado e que está ocorrendo um investimento maciço das instituições de ensino, buscando atingir possíveis alunos que até então não poderiam ter acesso a cursos de capacitação em instituições renomadas, foi criada a modalidade de Ensino a Distância buscando suprir essas necessidades. Entretanto ainda existe uma resistência pois a segurança na rede ainda não é totalmente confiável. Nesse sentido esta pesquisa, visa apresentar uma solução para a realização de provas e atividades a longa distância, que garanta segurança e gerenciamento das mesmas, com um custo de implantação extremamente baixo e confiável. Dessa forma, utilizando métodos de VPN com mídia pré-configurada para realização de atividades fora da sala de aula, permitindo assim, que as instituições de ensino possam adotar cada vez mais esse meio de ensino.

Palavras chave: Ensino a Distância. Segurança. VPN. Mídia.

ABSTRACT

HAHNER, Eliu Camargo; AYRES, Wallace Griz. Mídia com VPN pré-configurada. 2015. 27 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Due to increased technology available in the market and what is happening a massive investment of educational institutions, seeking to reach prospective students who previously could not have access to training courses in renowned institutions, the modality of Education was created seeking Distance address these needs. However there is still a resistance for the network security is not fully reliable. In this sense, this research aims to present a solution for conducting tests and activities at long range, guaranteeing security and management thereof, with an extremely low cost and reliable deployment. Thus, using VPN methods with pre-configured to perform outside the classroom activities media, thus allowing educational institutions to adopt increasingly this means of education.

Keywords: Distance Learning. Safety. VPN. Media.

LISTA DE SIGLAS

EAD	Educação a Distância
GNU	Licença Pública Geral
MEC	Ministério da Educação
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
TIC's	Tecnologias da Informação e Comunicação
VPN	Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

Com a evolução do mundo moderno e as tecnologias mais avançadas, a comunicação imediata, a necessidade de estar em vários lugares ao mesmo tempo, a exigência de uma comunicação precisa, é indispensável em qualquer lugar ter acesso a tecnologia. Diante da necessidade de uma filial no Brasil estabelecer uma comunicação com sua central no Japão ou simplesmente, um aluno acessando a página de sua universidade para realizar uma atividade, não havendo um horário específico para essa ação, esses avanços tecnológicos podem ajudar as pessoas que não tem tempo para estudar ou concluir alguma formação.

Inserindo essa tecnologia aos estudos surge um dos assuntos bastante discutidos, que é a Educação a Distância (EAD). O foco dessas discussões de que uma aula não presencial tem menor importância ou credibilidade do que uma aula em sala de aula com um educador presente, possa ser superada. E por que essas aulas a distância perdem o seu espaço? Por vários fatores. Mas o principal é se o aluno ao mesmo tempo em que realiza uma atividade avaliativa, não está se aproveitando de sua máquina para pesquisar sobre ela.

Existem sim falhas no momento em que um possível aluno realiza uma prova em sua máquina, e ao mesmo tempo usa um recurso que pode estar afetando o seu desempenho ao invés de ajuda-lo, que é a consulta a internet durante a prova.

Entretanto a ideia da Educação a Distância não pode ser abandonada, pois algumas de suas principais características são vantagens de os alunos poderem assistir a aula de sua casa, *lan house*, trabalho, no celular, em algum deslocamento distante, entre outros. Podendo também realizar provas em horários mais tranquilos ou até mesmo poder assistir a aula quando lhe for conveniente.

Desta forma, apresenta-se uma possível solução baseada em software livre, para universidades ou outras empresas voltadas à área de educação. Uma solução que seja necessário menos receita para gastos com segurança, mas que ao mesmo tempo essa ferramenta seja segura para garantir a restrição do acesso a informações extras durante essa atividade.

1.1 TEMA

Com a evolução do mercado, hoje é necessário que tudo seja dinâmico e que se aproveite o máximo possível do tempo disponível, para trabalhar, estudar, etc. Todos almejam cada vez mais, altos cargos e melhores condições de vida, entretanto, para isso, é necessário que seja formado. Contudo as maiores barreiras para isso são os deslocamentos e o tempo, por isso foi criada a Educação a Distância (EAD), para amenizar essas dificuldades, mas com isso surgirão os novos desafios em relação a segurança desses estudos e a possibilidade de se aplicar uma atividade avaliativa a distância. (DAMASCENO, et all, 2010)

Nesse projeto o objetivo é uma nova alternativa para a EAD, podendo assim melhorar sua credibilidade, focando em uma maneira de “bloquear” os acessos na máquina de quem realizar a atividade e encaminhando as informações com segurança, direto para o servidor central.

1.2 PROBLEMA

Segundo o Ministério da Educação e Cultura, Educação a Distância (EAD) é uma “forma de ensino que possibilita autoaprendizagem, com medicação de recursos didáticos sistematicamente organizados, apresentados em diferentes suportes de informações, utilizados isoladamente ou combinados, e veiculados pelos diversos meios de comunicação”.

A Educação a Distância (EAD) possui algumas vantagens em relação a outro tipo de ensino, pois a pessoa pode escolher a hora de estudar, tanto quando iniciar seus estudos, impondo seu ritmo individual. Portanto as instituições formadoras têm que disponibilizar um bom suporte para os alunos.

Com o avanço da Educação a Distância (EAD), vários ambientes de aprendizagem virtuais foram criados cada um com características próprias, mas atuando sempre na mesma função, educar a distância. O ambiente virtual de

aprendizagem é um software baseado na internet que facilita a gestão de cursos no ambiente virtual. Existem diversos programas disponíveis no mercado de forma gratuita ou não. De acordo com Clark e Mayer (2007), estes ambientes virtuais, são elementos fundamentais na tarefa de ensino, porém necessitam de suporte pedagógico adequado em relação ao processo de aprendizagem.

O Ensino a Distância é uma ferramenta muito importante à educação e com avanços em telecomunicação através da internet, ele ganha cada vez mais espaço. O número de disciplinas e cursos disponíveis é maior a cada dia e uma das razões disso são os softwares com intuito de proteger seus usuários, facilitar na distribuição de material e comunicação entre todos os envolvidos no processo. (DAMASCENO, et all, 2010)

Portanto o resultado esperado de um programa de Educação a Distância é o desenvolvimento de um processo eficaz de aprendizagem, que possibilite ao estudante conquistar os objetivos almejados em relação a aprendizagem dos conteúdos.

Existem hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os antivírus, firewalls locais, filtros AntiSpam, fuzzers e analisadores de códigos. Mesmo com todas essas ferramentas de segurança, não se pode garantir quem está do outro lado do computador realizando as atividades, é realmente o aluno e o mesmo não está utilizando outros recursos para resolver a atividade ou avalição.

1.3 OBJETIVOS

1.3.1 Geral

Através da demonstração dos aspectos técnicos e de sua importância, apresentar uma solução para a realização de atividades de avaliações a longa distância, que garanta a segurança e o gerenciamento das mesmas, com um custo de implantação extremamente baixo e confiável.

1.3.2 Objetivos Específicos

- Discutir e apresentar um método de implementação de segurança.

- Descrever características, conceitos e a importância de métodos de segurança na rede.

- Demonstrar a configuração cliente/servidor em uma VPN, para o projeto de segurança.

- Simular um ambiente de rede, utilizando os CD-ROM com a mídia e a VPN.

1.4 JUSTIFICATIVA

Esse projeto foca na tecnologia para a EAD, pois é um recurso que no momento atual da humanidade não pode ser desperdiçado. A falta de tempo para poder ir as universidades, deslocamento ou apenas permitir chegar atrasado, são fatores que podem ser vencidos e realizar um aproveitamento melhor do tempo.

E uma das principais dificuldades que tendem a fragilizar a Educação a Distância é a falta de credibilidade no computador em que o aluno realiza suas atividades, podendo acessar vários recursos ao mesmo tempo em que seus conhecimentos estão sendo averiguados por uma atividade avaliativa.

É por isso que esse trabalho foca na melhoria dessas atividades, para que diminua o número de fraudes durante a realização das provas, podendo assim, ser um passo importante para a evolução da Educação a Distância e os estudantes possuírem essa opção de estudo diminuindo as dificuldades para uma graduação.

1.5 METODOLOGIA

A implantação do projeto será guiada por manuais, normas, guias e bibliografias de referências que tratam do tema, e também serão expostas informações oriundas de especialistas da área.

O projeto compreende as seguintes etapas: a primeira etapa, realizaremos uma contextualização sobre o tema segurança e mostraremos motivações que

levaram ao desenvolvimento do sistema para EAD, e em seguida desta pesquisa, iremos apresentar a importância, seus principais conceitos e as tecnologias utilizadas.

Na segunda parte do projeto, será apresentada as configurações aplicadas na mídia e no servidor, suas funções e maneiras de implantação. Esse estudo será guiado por apostilas, livros de estudo, que oferece grande quantidade de informações teóricas e detalhes da solução.

Em sua terceira parte, realizaremos uma simulação que demonstrará na prática o funcionamento do sistema e os principais atributos necessários para a implantação dessa tecnologia.

A última etapa visa vincular o conhecimento obtido nas simulações ao conhecimento teórico, para demonstrar os reais benefícios desta tecnologia.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 EAD

De acordo com o MEC (Ministério da Educação), a EAD é a modalidade de educacional onde ato de ensinar se dá em lugar e tempo diferentes do ato aprender, ou seja, na EAD o aluno está separado fisicamente de seu professor e dos seus colegas e faz uso de meios de comunicação e da tecnologia para interagir com o professor e com os seus colegas. A validade entre o curso EAD e o curso Presencial é a mesma, entretanto a instituição deverá ser bem selecionada dentro das universidades regulamentadas pelo MEC.

A vantagem desse modelo de curso é que proporciona uma flexibilidade de horários, o que nos dias atuais, é um ponto crucial. Muitas pessoas têm o desejo de fazer um curso de graduação ou de dar continuidade a sua formação, mas não consegue conciliar o horário de sua jornada de trabalho com os horários rígidos e locais dos cursos presenciais. Nos cursos EAD você pode definir a hora e local do seu estudo.

A mesma vem sendo considerada uma forma alternativa para ampliar horizontes no que diz respeito à formação profissional e científica. Através de uma proposta educativa enriquecedora, com o uso crítico das TIC's (Tecnologias da Informação e Comunicação), assegura a interatividade entre estudantes e professores. Flexibilizando o acesso à educação, a EAD tem contribuído para a democratização das oportunidades educacionais e para o desenvolvimento sociocultural e científico do país (DAMASCENO, 2010).

A utilização das TIC's na educação, e principalmente na EAD, deve estar ligada aos interesses coletivos e contribuir na busca de uma sociedade humana e emancipatória. Nela, os estudantes reconstroem o conhecimento através de suas experiências.

Nesse modelo de ensino o papel do estudante é importante, uma vez que é ele quem estabelece seus horários de estudo, organiza sua agenda e é sujeito ativo no processo de interatividade, colaboração e autonomia necessários a essa modalidade de educação.

Para o professor, a EAD é um espaço de mudanças, de um novo paradigma de ensino e de aprendizagem. Ele deve assegurar o acompanhamento contínuo e a motivação do estudante, que são peças importantes para o êxito do processo de ensino e aprendizagem nesta nova metodologia.

Segundo DAMASCENO (2010), a Educação a Distância é uma estratégia educativa baseada na aplicação da tecnologia na aprendizagem, sem limitação de lugar, tempo, ocupação ou idade dos estudantes. Implica novos papéis, novas atitudes e novos enfoques metodológicos para estudantes e professores.

O uso das TIC's em processos educativos, normalmente, é mais explicitado quando se refere a programas de EAD devido às necessidades inerentes a essa modalidade educativa, ou seja, de mediações pedagógicas que possibilitem estratégias de ensino/aprendizagem não-presenciais.

De acordo com DAMASCENO (2010), o mesmo processo de incorporação da informática também se repete no desenvolvimento dos programas de EAD. Para compreendermos essa transposição, precisamos rever a relação da tecnologia educacional com os processos educativos. Inicialmente, precisamos ter clareza de que o próprio discurso pedagógico consiste em uma tecnologia educacional que desloca o discurso da ação educativa, da prática de um determinado contexto e o reloca de acordo com seus princípios e reordenamentos. Neste processo de deslocamentos, o discurso original passa de uma prática real para uma prática virtual.

Da mesma forma como o discurso pedagógico, enquanto tecnologia educacional, que age reformulando as práticas educativas, temos as TIC's reorganizando as relações pedagógicas e reformulando as práticas educativas. E, no caso das tecnologias de informação e comunicação, perdemos o propósito da ação, perdemos a conexão com o sujeito da aprendizagem e, na maioria das vezes, passamos a ter a tecnologia/informática como um fim em si mesma.

2.2 VPN

VPN (*Virtual Private Network*) ou Rede Privada é aquela em que sua configuração, ao contrário das redes públicas, só pode ser utilizada ou aproveitada por uma empresa, grupo de pessoas ou dispositivos autorizados.

Os motivos para se utilizar uma rede privada:

- Segurança, garantir a integridade e a confidencialidade das comunicações;
- Qualidade de serviço, melhor performance;
- Não existe uma rede pública para fornecer o serviço.

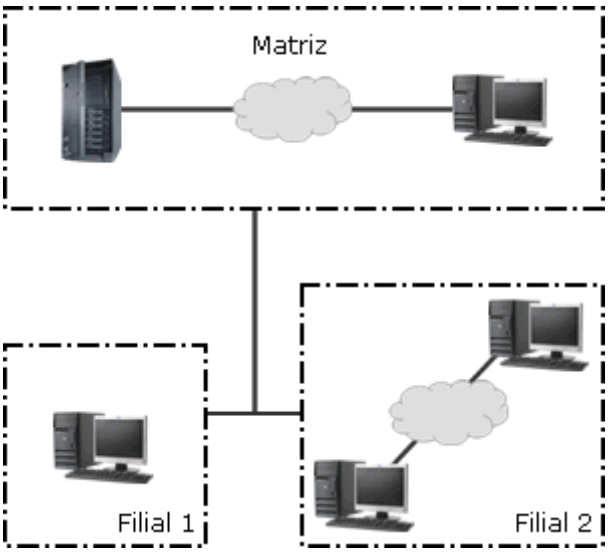

Figura 1 – Empresa com sede e filiais.
Fonte: TUDE, 2007.

Os principais tipos de VPN's são:

- VPN formada por circuitos virtuais;

- VPN utilizando a Internet;

- VPN/IP oferecida por um provedor com backbone IP.

Nesse projeto será utilizada a VPN sobre na internet.

2.2.1 VPN: Internet

O conceito de se utilizar uma VPN na Internet é para o foco na segurança, com a passagem de dados através da Internet que é uma rede pública e não segura. Ao implantar uma VPN utilizando a Internet a qualidade de serviço será a da operadora que fornece o serviço, uma vez que o usuário não tem como exercer controle da mesma. (TUDE, 2007).

O mecanismo utilizado para aumentar a segurança é conhecido como tunelamento (*Tunneling*), que consiste no encapsulamento de um protocolo em outro protocolo.

		IP Cabeçalho Original	Dados
IP Novo Cabeçalho	Cabeçalho do outro protocolo	IP Cabeçalho Original	Dados

Figura 2 – Processo de encapsulamento de um pacote IP.
Fonte: TUDE, 2007.

O **IPSec** (IP *Security*) é um conjunto de protocolos definido pelo IETF (*Internet Engineering Task Force*) para prover segurança nas comunicações em redes IP. Essa forma permite autenticação, integridade e confidencialidade a nível do pacote de dados pela adição de dois cabeçalhos. Esses cabeçalhos permitem a integridade e a confidencialidade, AH (cabeçalho de autenticação) e o ESP (*Payload* de encapsulamento de segurança). Ambos utilizam protocolos de gerenciamento de chaves de criptografia padrões da Internet.

As principais desvantagens na utilização do IPsec são o *overhead* adicional imposto ao pacote de dados e o fato dele só oferecer suporte a redes IP o que impede a autenticação de usuários com acesso remoto.

O **PPTP** (*Point-to-Point Tunneling Protocol*), é uma extensão do protocolo PPP (*Point-to-Point Protocol*) utilizado em acesso discado na Internet. É um protocolo proprietário desenvolvido por um grupo liderado pela Microsoft, que possibilita a autenticação de usuários remotos e suporta criptografia (TUDE, 2007).

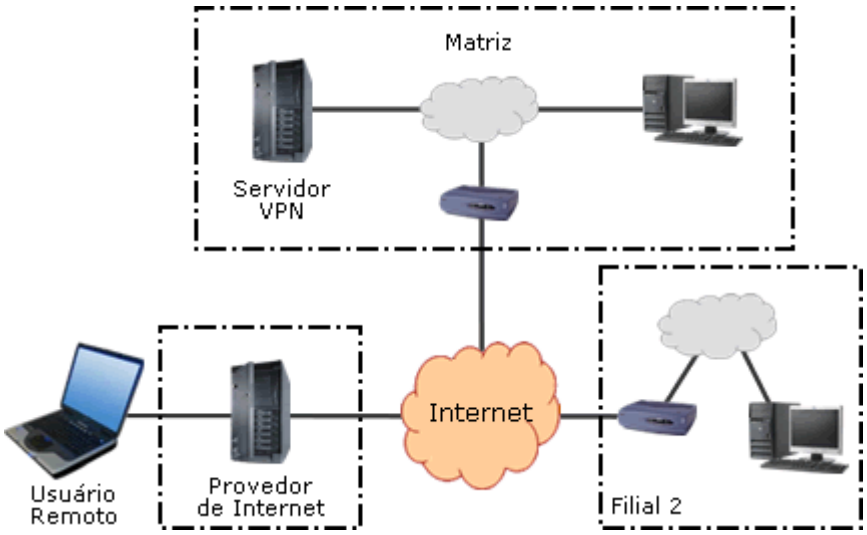

Figura 3 – Representa uma arquitetura de Matriz e filiais na internet.
Fonte: TUDE, 2007.

2.3 REDE CLIENTE/SERVIDOR

Segundo Morimoto (2002), a rede cliente/servidor é mais difícil de montar e configurar e também tem um custo mais elevado por exigir um bom poder de processamento. Essa rede concentra todos os recursos em um ou mais servidores, como arquivos, impressoras, serviços de fax e acesso à internet, etc. Tudo será controlado pelos servidores.

Todos os sistemas operacionais necessitam de tempo para configurar os servidores, assim como permissões de acesso aos recursos, senhas, entre outros. Com isso, uma vez que tudo estiver funcionando você terá uma rede muito mais robusta e confiável.

Torres (2001) diz que o servidor nada mais é que um computador que gera recursos para os demais computadores da rede, pode ficar sobrecarregado com a utilização de várias tarefas e fornecendo para os demais computadores para rede, assim tornando baixo o desempenho da rede. Com o servidor dedicado, que é um servidor para executar somente uma tarefa, por exemplo, somente um servidor de arquivos, ele consegue responder rapidamente os pedidos recebidos dos demais computadores da rede assim não compromete o desempenho e oferece um melhor desempenho para executar uma determinada tarefa.

A administração e configuração da rede cliente/servidor é centralizada, isso melhora a organização e segurança da rede e possibilita a execução de programas cliente/servidor, como, por exemplo, um banco de dados que pode ser modificado por vários usuários ao mesmo tempo. Assim Torres (2001), resume a rede cliente/servidor: usada normalmente em redes com mais de 10 computadores ou redes pequenas que necessitem de um alto grau de segurança; custo maior que o de redes ponto-a-ponto; maior desempenho do que redes ponto-a-ponto; implementação necessita de especialistas; alta segurança; manutenção e configuração da rede realizada pelo administrador de rede e de forma centralizada; possibilidade de uso de aplicações de cliente/servidor.

3 DESENVOLVIMENTO

Após as pesquisas realizadas sobre os materiais de rede, aplicações e hardware chegou-se ao cenário ideal.

Para os sistemas operacionais foram utilizados para servidor e máquina cliente, *Debian* e *Xubuntu* respectivamente, para criação da VPN foi escolhido o OpenVPN, para a criação da mídia foram utilizados os aplicativos *Remaster* e *squashfs-tools*. Todos os aplicativos foram escolhidos devido a facilidade de utilização e por serem softwares livres geridos pela licença GNU Linux.

O *Xubuntu* para a máquina cliente foi escolhido devido à baixa utilização de hardware necessária, isso se deve à interface gráfica Xfce conhecidamente mais leve que outras interfaces do mercado.

O hardware do servidor de testes as especificações foram 1Gb de ram, processador Intel Dual Core 1.3Ghz e devido as máquinas clientes serem dos mais diversos tipos foi utilizado como configuração mínima da mesma um netbook com 1Gb de ram e processador Atom 1.6Ghz.

3.1 OpenVPN

Segundo Tanenbaum (2003) as redes privadas possuem um ótimo desempenho e muito bem referenciadas no quesito segurança, entretanto, o custo de manutenção é muito alto. Com o surgimento da Internet, muitas empresas trocaram o uso das redes privadas das concessionárias de telefonia pelo uso da internet para trafegar seus dados. Essa mudança diminuiu muito o custo da manutenção, entretanto, era necessário manter o mesmo padrão de segurança das redes privadas.

A OpenVPN é um software livre que permite a criação de redes virtuais do tipo PPTP ou Cliente/Servidor. Ela é capaz de estabelecer conexões diretas entre computadores mesmo que estes sejam protegidos por Firewalls, sem a necessidade de reconfiguração de rede. Foi criado por James Yonan e está sob licença GNU General Public License (Licença Pública Geral).

Quando utilizado em Cliente/servidor ele permite que o cliente utilize a autenticação pública com certificados digitais, fazendo isto através de assinaturas

digitais e certificados de autoridade. Contém muitos recursos de controle de segurança, todo pacote do OpenVPN consiste em apenas um binário tanto para conexões do lado do cliente quanto para conexões do lado do servidor, com isso encontra mais alguns arquivos e chaves dependendo do tipo e método de autenticação utilizado.

3.2 CRIAÇÃO DA MÍDIA

Para a criação da mídia, inicialmente foi criado vários cenários dentro de máquinas virtuais, até definir um considerado adequado para o projeto final. Esses testes incluíam principalmente a facilidade para utilizar o sistema operacional, além de suas respostas para os vários *hardwares* disponíveis no mercado.

Após definido a escolha do sistema, foi aplicada as configurações para que no momento do boot inicia-se a conexão com o servidor. Com todas as configurações e cenários imaginados, criamos a mídia salvando o sistema operacional criado na máquina virtual no USB, CD-ROM, DVD, etc. Para esse processo é utilizado o programa *Remaster*, um programa que cria um *backup* do seu sistema operacional podendo salvar em qualquer mídia selecionada.

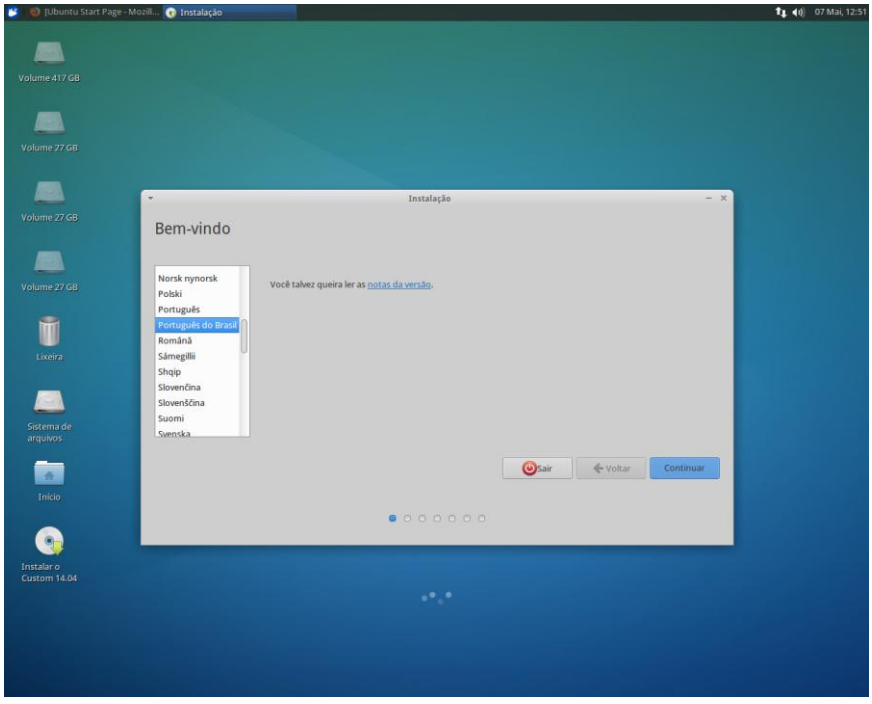

Figura 4 – Tela de Instalação do Remaster.
Fonte: Própria

Adicionalmente foi verificado que utilizando o *Remaster* o tempo de criação de mídias é muito elevado, aproximadamente 8 horas por isso utilizado a ferramenta *squashfs-tools* que possibilita a troca dos arquivos do *filesystem*, que em consequência possibilitou a troca apenas do arquivo de configuração, da chave e do certificado do OpenVPN podendo ser automatizado via *ShellScript.*

3.3 TESTES

Inicialmente os testes básicos foram ponto-a-ponto entre dois notebooks utilizando Linux *Debian*, e a configuração padrão da OpenVPN, que foi administrada em matéria na UTFPR.

Gerar chave de criptografia
cd /usr/local
openvpn --genkey --secret chaveserver
Copiar a chave gerada em um servidor para o outro
scp /usr/local/chaveserver root@ip_válido_de_rede:/tmp
Obs: Será solicitada a senha do usuário no servidor para o qual você está enviado o arquivo
ls -la /tmp/chaveclient
Copiar a chave para o /usr/local
cp /tmp/chavecliente /usr/local
Servidor 1
openvpn --dev tun0 --remote ip_válido_de_rede --ifconfig 10.0.0.1 255.255.255.0 --secret /usr/local/chavecliente --verb 3 --comp-lzo
Servidor 2
openvpn --dev tun0 --remote ip_válido_de_rede --ifconfig ipv-servidor1 ipv-servidor2 --secret /usr/local/nomedachave --verb 3 --comp-lzo
route add 10.0.0.1 mask 255.255.255.0 10.0.0.2

Configurações administradas pela UTFPR, Matéria de Rede Longas Distâncias.

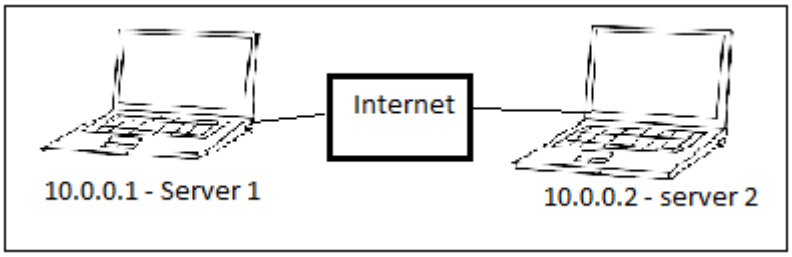

Figura 5 – Teste OpenVPN ponto-a-ponto.
Fonte: Própria

Após os testes para ponto-a-ponto, no caso atendendo apenas um cliente, foi iniciado o processo para múltiplos clientes, várias chaves acessando ao mesmo tempo o servidor. Alterando as configurações de cada Mídia utilizando a ferramenta *squashfs-tools*, devido às limitações por falta de recursos, o teste máximo de acessos obtidos foi o de 4 clientes ao mesmo tempo.

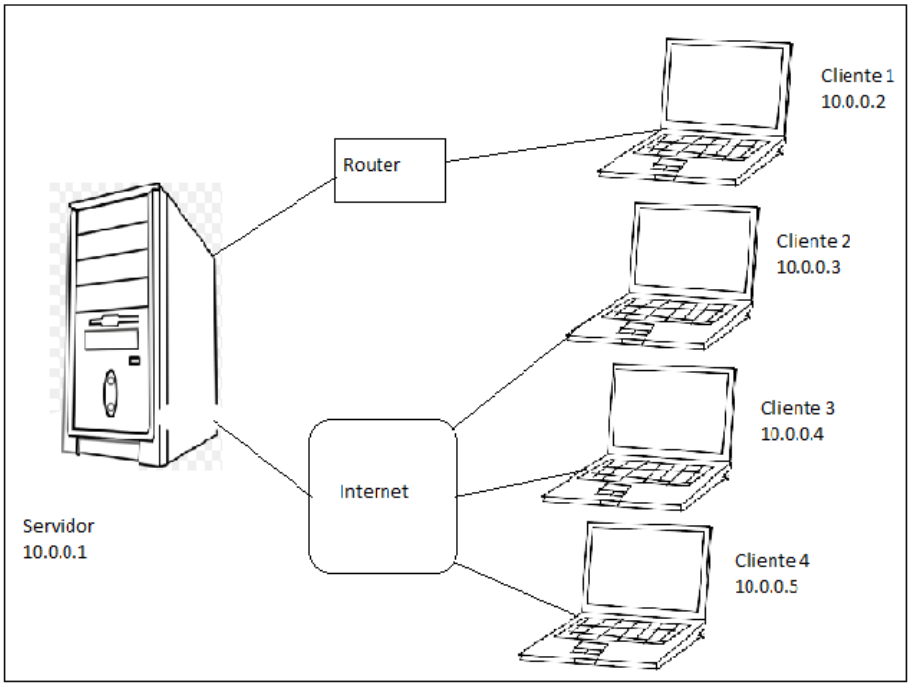

Figura 6 – Teste com Múltiplos clientes.
Fonte: Própria

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

O resultado do projeto foi considerado satisfatório, porque atende aos objetivos propostos e foi possível associar várias configurações, que foram aplicadas tanto no servidor, quanto para o cliente. Na sequência serão demonstrados os passos necessários para se chegar ao resultado almejado, demonstrando todos os recursos utilizados para o bom funcionamento do servidor.

Para o servidor foi utilizado o **debian-8.0.0-i386** por ser um sistema operacional mais leve e por ser mais fácil a edição e programação apenas do necessário, podendo instalar apenas programas padrões como openvpn, ssh, etc.

Abaixo segue a configuração aplicada para o *firewall,* criada especificamente para os recursos que utilizamos:

```
iptables -P INPUT  DROP
iptables -A INPUT -p icmp -i eth1 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -i eth1 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 80  -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 8080 -j ACCEPT
iptables -A INPUT -p tcp -i tap0 --dport 8080 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 443  -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 23 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 7000 -j ACCEPT
iptables -A INPUT -p udp -i eth1 --dport 7000 -j ACCEPT
iptables -A INPUT -p tcp -i eth1 --dport 1194 -j ACCEPT
iptables -A INPUT -p udp -i eth1 --dport 1194 -j ACCEPT
```

Configurações disponíveis no manual do *iptables* (*man iptables*).

Com as aplicações do firewall pode ser controlado todos os dados transferidos dentro do servidor, ele também é responsável pela prevenção do vazamento de informações e também bloqueando os acessos de software que possam prejudicar o mesmo.

Foi utilizado esse recurso pois é mais recomendado para redes de pequeno e médio porte, se for bem configurado, um firewall trabalhando com filtragem de pacotes é capaz de analisar informações sobre a conexão e o conteúdo presente na transferência de dados. Para uma rede maior como uma universidade será necessário um cuidado maior com o firewall, sendo recomendado utilizar o Firewall

por hardware quando há mais de um computador em uma mesma rede, pois, as máquinas estão ligadas em um mesmo roteador, que gerencia as conexões e também executa a função de Firewall.

Para a VPN foi instalado o *openvpn* e criado a pasta */etc/openvpn*. Toda configuração deverá ficar nesta pasta. Antes deve ser criado todos os certificados necessários, esses certificados serão usados tanto pelo servidor como pelo cliente, de forma que após a verificação destes certificados é que a conexão será estabelecida.

Foi criado uma VPN server para vários clientes, pois assim poderá ser usado por qualquer um que necessite acessar a rede interna, mas está fisicamente em outro local, como por exemplo algum aluno que deve acessar o sistema para realizar atividades, ou mesmo o professor que quer ter acesso a rede interna quando está viajando.

Com as configurações abaixo padrão, definimos a porta pela qual será executada a VPN e a chave para certificação.

```
root@PC-TCC:~/Desktop# cat /etc/openvpn/servidor.conf
dev tap
port 1194
tls-server
mode server
ca ca.crt
cert servidor.crt
key servidor.key
dh dh1024.pem
duplicate-cn
ifconfig 10.0.0.1 255.255.255.0
ifconfig-pool 10.0.0.2 10.0.0.100 255.255.255.0
ping 10
ping-restart 120
push “ping 10"
push “ping-restart 120"
push “route 192.168.10.0 255.255.255.0 10.0.0.1"
push “dhcp-options DNS 10.0.0.1"
verb 5
log /var/log/openvpn.log
```

Configurações básicas obtidas no site http://www.stato.blog.br/

Para o cliente utilizamos o ***xubuntu-14.04.2-desktop-i386***, é um sistema operacional mais leve para realizar *boot* via mídia, devido a utilização de ambiente gráfico *Xfce* possibilitando a utilização em praticamente em qualquer máquina. A configuração padrão é prática e completa, sendo apenas necessário aplicar as configurações referentes a VPN.

Abaixo segue as configurações utilizadas no cliente referente a VPN, utilizando sua própria chave para acesso.

```
cat /etc/openvpn/cliente.conf
dev tap0
port 1194
tls-client
remote tcc.no-ip.org
ca ca.crt
key cliente1.key
cert cliente1.crt
pull
verb 5
```

Configurações básicas obtidas no site http://www.stato.blog.br/

Com a VPN fechada entre cliente e servidor, já está apto a prosseguir com as atividades necessárias nesse meio, tendo a rota do cliente direcionada para o servidor, e com o funcionamento do *firewall*, o cliente apenas pode e deverá acessar a página específica para a sua atividade.

Figura 7 – Acesso do cliente.
Fonte: Própria

5 CONSIDERAÇÔES FINAIS

Ao falar sobre o conceito de educação a distância se caminha lado a lado a internet e sistemas computacionais que necessitam ser cada vez mais interativos, eficientes e proporcionar as melhores ferramentas para a evolução do aprendizado dos estudantes.

No entanto, no que diz respeito a melhores ferramentas, a proposta desse trabalho é permitir que qualquer instituição de ensino, possa fornecer uma possibilidade de educação para as pessoas, mesmo sendo a distância, com a garantia de que quem esteja realizando as provas e atividades, seja realmente o aluno.

Diante desse objetivo e a necessidade da EAD é uma realidade, apresentamos um dispositivo que poderá conectar-se com o mundo em uma mídia própria e novas aplicações que poderão ser geradas, tornando a informação dentro da EAD algo mais confiável e com segurança, oferecendo ao estudante a flexibilização de horários para seus estudos.

Nesse trabalho, também foi explicado o passo a passo, para o melhor entendimento de todo o processo decorrido.

Através desse dispositivo, a instituição ou aluno poderá conectar-se com o mundo por meio de uma mídia própria, atendendo as necessidades da EAD nos dias atuais, podendo serem geradas novas aplicações.

A ideia central é incentivar a prática dessa forma de ensino, pois cada vez mais com as tecnologias em evolução, pode-se criar métodos mais seguros. Sendo que na maioria dos processos existentes, não são de segurança total, e com isso também não será extinta as salas de aula, pois o contato aluno professor ainda é algo necessário.

Contudo, as instituições que quiserem ingressar na educação a distância, poderão utilizar as orientações do nosso trabalho como base.

REFERÊNCIAS

CLARK, Ruth Colvin; MAYER, Richard E. ***e-Learning and the Science of Instruction:Proven Guidelines for Consumers*****:** and Designers of Multimedia Learning. New York: Pfeiffer, 2007. pp. 496

DAMASCENO, et all. Segurança e privacidade em meios de Ensino Online. Disponível em www.textolivre.pro.br/blog/UEADSL/2010-2artigosPDF/segurançaprovacidade.pdf Acessado em: 6 de agosto de 2014.

EAD. **Dificuldades e Limitações da Educação a Distância no Brasil.** Disponível em: www.kmbusiness.net/images/SEPROSUL_EAD%20DIFICULDADES.pdf. Acesso em 20 de agosto de 2014.

LFS. ***Linux From Scratch.*** Disponível em: www.linuxfromscratch.org/lfs/. Acessado em 21 de agosto de 2014.

MEC, **Regulamentação da EAD no Brasil**, Disponível em: portal.mec.gov.br/default.html acesso em: 15 de agosto de 2014.

MORIMOTO, C. E. **Redes – Guia Completo**. E-book. 2002. Disponível em: http://www.de9.ime.eb.br/~mpribeiro/redes/Redes.pdf Acessado em 21 de agosto de 2014.

STATO FILHO, André. **Linux Controle de Redes.** 1ª ed. Florianópolis: Editores Visuais Books, 2009.

TANENBAUM, Andrew S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003.

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

TUDE, Eduardo. VPN. **Redes Privadas Virtuais.** Disponível em: www.teleco.com.br/tutoriais/tutorialvpn/default.asp. Teleco, 2007. Acesso em 9 de agosto de 2014.

Acesso ao site: http://www.stato.blog.br/wordpress/?p=180. Acessado em 25 de fevereiro de 2015.

Acesso ao site:
http://linuxdicasesuporte.blogspot.com.br/p/remaster-gtk-ubuntu-e-derivados.html. Acessado em 25 de fevereiro de 2015.