CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE JAHU

CURSO SUPERIOR DE TECNOLOGIA DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

GABRIEL AULER BARRIENTOS

JHONNY PEREIRA DA SILVA

SEGURANÇA DE REDES: UMA SOLUÇÃO COM BAIXO CUSTO

JAHU

DEZEMBRO/2013

GABRIEL AULER BARRIENTOS
JHONNY PEREIRA DA SILVA

SEGURANÇA DE REDES: UMA SOLUÇÃO COM BAIXO CUSTO

Trabalho de conclusão de graduação apresentado à Faculdade de Tecnologia de Jahu, como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Orientador: Prof. Everton Aparecido Ribeiro de Carvalho

JAHU
DEZEMBRO/2013

“O sucesso é ir de fracasso em fracasso sem perder entusiasmo.”

Winston Churchill

AGRADECIMENTOS

Eu, Gabriel, agradeço a toda minha família pelo incentivo e apoio que me motivaram na caminhada de estudos.

Agradeço aos professores que ao longo dos anos se dedicaram a transmitir parte do seu conhecimento, com paciência e empenho.

E a todos os colegas da Fatec Jahu com quem convivi durante este período de graduação, em momentos bons e ruins, muito obrigado.

Eu, Jhonny, agradeço primeiramente a Deus que me permitiu chegar até aqui. Agradeço também a meu pai, Joaquim, minha mãe ,Ana, e minha namorada, Marina, obrigado pelo apoio, incentivo, amor e confiança que me ajudaram a seguir até o fim desta graduação.

Agradeço também a todos os professores que, durante esses anos, repassaram com paciência e sabedoria seus conhecimentos.

E a todos os amigos e colegas do curso de Gestão em T.I., muito obrigado pela amizade e companheirismo durante estes anos de graduação.

Por fim, agradeço a todas as pessoas que de algum modo colaboraram para o desenvolvimento deste trabalho.

RESUMO

Este trabalho apresenta uma proposta de solução em segurança de rede com baixo custo. Possibilita a conexão de redes locais a redes públicas ou a outras redes locais por meio de redes públicas. Além disso, apresenta uma proposta de comunicação de filiais, parceiros e usuários remotos com a matriz da organização, a um baixo custo, devido ao uso de *Softwares Open Sources*. A ideia surge da necessidade das organizações em manter conexões seguras com suas filiais e usuários remotos. É possível prover esta segurança de redes, tanto externas, como internas, a um baixo custo, por meio da VPN. Uma VPN é uma rede virtual que opera sobre uma infra-estrutura de rede já existente como a *internet*, e *Softwares Open Source* como o Linux.

Palavras Chave: Segurança de Rede; VPN; *Open Source*; Linux.

ABSTRACT

This paper proposes a low cost network security solution Enables connecting local networks or the public to other LANs via public networks. Furthermore, this paper presents a communication proposal for branch offices, partners and remote users with the mother organization, at a low cost due to use of Open Software Sources. The idea of this project arises from the need to maintain secure connections to branch offices and remote users to their organizations. It is possible to provide this network security, both external as internal, at low cost through the VPN. A VPN is a virtual network that operates on an infrastructure of existing network such as the Internet and Open Source Software such as Linux.

Key Words: Network Security; VPN; Open Source; Linux.

LISTA DE FIGURAS

LISTA DE TABELAS

GLOSSÁRIO

Antispam: programa que filtra as mensagens recebidas afim de não permitir que e-mails indesejáveis cheguem a sua caixa de entrada.

Assembly: é uma notação legível por humanos para o código de máquina que uma arquitetura de computador específica usa, utilizada para programar dispositivos computacionais.

Bug: Erros durante execução do programa.

C : Linguagem de programação.

Desktop: microcomputador de mesa.

Download significa transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local.

Early-adopters: usuários que estudam e tem conhecimento avançados sobre determinada tecnologia.

Executável: Um programa executável ou arquivo executável, em informática, é um arquivo em que seu conteúdo deve ser interpretado como um programa por um computador.

Firewall : nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede.

Gateway: sistema que faz a ponte entre dois sistemas incompatíveis, como a ligação entre o correio eletrônico interno de uma empresa e o *e-mail* da *Internet*.

Hardware: é a parte física de um computador, é formado pelos componentes eletrônicos.

Internet: rede mundial de computadores, ou conjunto de redes mundial.

Pacote: conjunto de dados que transita pela rede.

Porta: o termo usado para denominar um canal físico de entrada ou de um dispositivo. É um endereço para o qual os pacotes são enviados.

Proxy: um servidor proxy é um tipo de servidor que atua nas requisições dos seus clientes executando os pedidos de conexão a outros servidores.

Road Warriors: usuário remote que acessa a rede local mas não está na rede local.

Software: sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. São programas de computadores que permitem ao usuário executar uma série de tarefas especificas em diversas areas.

Software open source ou *software* livre: programa que tem seu código fonte aberto, podendo ser alterado.

LISTA DE SIGLAS

DHCP - *Dynamic Host Configuration Protocol*; protocolo de configuração dinâmica de hosts.

DNS - *Domain Name System*

GNU - *General Public License*

ISP - *Internet Service Provider*

NAT - *Network Address Translation*

VPN- *Virtual Private Network*

SUMÁRIO

1. INTRODUÇÃO

Atualmente, nas organizações de pequeno, médio ou grande porte, há um grande fluxo de informações sendo enviadas e recebidas utilizando a estrutura de rede disponível. Estas informações podem ter caráter confidencial e possuir grande relevância para a gestão estratégica da organização. Para garantir a segurança destas informações é necessário o uso de algumas ferramentas de segurança da informação.

Essas informações confidenciais podem sofrer "ataques" internos e externos, podendo resultar no comprometimento de sua integridade e causando grandes danos a uma empresa.

Os "ataques" possuem diferentes origens: podem ser provocados por um usuário com permissões indevidas, o que possibilita o acesso a programas e/ou arquivos sigilosos, podendo "vazar" informações internas com a finalidade de prejudicar a organização, ou mesmo por engano. Além disso, os ataques podem ser originados por meio de *softwares* mal intencionados que passam pelos computadores, roteadores e *softwares* de defesa muitas vezes desatualizados, com configurações de segurança falhas, ou não configuradas de forma correta. Essas falhas possibilitam a abertura da rede para um invasor e gera o risco de comprometimento da segurança de toda a rede.

Segundo Ali Ghorbani,Wei Lu,Mahbod Tavallaee (2009)

> Ataques a redes são definidos como atividades maliciosas para romper, rejeitar, degradar ou destruir informação e serviços nos computadores da rede. O ataque a rede é executado através do fluxo de dados na rede e tem intenção de comprometer a integridade, confidencialidade ou validade do sistema de rede.

Frequentemente, os problemas de segurança de rede etsão ligados ao sigilo e à identidade. O sigilo consiste na disponibilidade de determinada informação para determinado usuário ou computador. A identidade trata-se da verificação da autenticidade do usuário ou computador. Uma máquina, ao enviar um pacote à outra máquina da mesma rede ou para uma rede externa, envia também um identificador de origem, e é com esta informação que a máquina de destino saberá a origem do pacote, que pode conter dados confidenciais, e fornecerá, ou não, dependendo do privilegio, as informações requeridas, ou aceitará o pacote enviado se a maquina de origem for identificada como de origem segura.

De toda a necessidade de segurança de informação em adendo ao fluxo de informações cada vez maior e a busca por melhores serviços e redução nos gastos de maneira geral, surge a necessidade de uma solução que viabilize a segurança da informação e possa ser implantada mesmo em organizações que dispõem de poucos recursos financeiros.

1.1 Objetivos

Este trabalho tem como objetivo prover um serviço de segurança de rede que possa garantir a comunicação segura entre redes internas e externas, além da integridade das informações, e que seja financeiramente acessível a qualquer organização, independente do porte. Para atingir este objetivo, serão utilizadas ferramentas e *Softwares Open Source*[1] que reduzem, de maneira significativa, o custo na implantação de uma solução em segurança de rede.

1.2 Justificativa

A utilização de S*oftwares Open Source* como o Linux, garante, além do baixo custo, uma alta confiabilidade na segurança de informações. Ao efetuar o *download* de um *Software Open Source*, dependendo da licença para uso oferecida, o usuário adquire o direito de utilizá-lo para qualquer propósito, podendo, inclusive, modificá-lo e redistribuí-lo. Com isso, muitos usuários incrementam o *software* com funcionalidades extras e podem, ainda, efetuar reparos de possíveis *bugs*, já que o sistema possui código aberto.

O Linux é um sistema operacional gratuito e com baixo custo de implantação que tem um papel importante na área de segurança de redes: pode ser utilizado com vários propósitos, desde estações para clientes até robustos servidores de rede. Além disso, pode ser utilizado como *firewall* em uma rede de computadores, auxiliando a segurança dos dados trafegados.

A VPN[2] (*Virtual Private Network*) é um recurso utilizado para suprir essa necessidade de segurança com baixo custo, e a cada dia é mais aceita no mercado da Tecnologia da Informação. Por conseguinte, a VPN é amplamente utilizada na transmissão segura de dados entre redes. Ela pode fazer com que um meio inseguro, como uma rede pública como a *Internet*, torne-se um meio de comunicação seguro, por onde possam trafegar dados sem o risco de serem capturados por terceiros.

Expansões em empresas ocasionam a necessidade de se criar um ambiente seguro de troca de informações entre a matriz, as filiais e seus respectivos vendedores.

Essa necessidade de comunicação e segurança pode ser suprida com o uso da VPN. Este uso tem como benefícios, além do baixo, ou nenhum custo de implantação, segurança, baixo custo de *hardware* para manter vários usuários conectados (graças à utilização de uma infra-estrutura de rede já existente, como a *Internet*), inexistência de custos adicionais além de

[1] S*oftwares Open Source* são programas de código aberto, nos quais os usuários possuem autonomia para alterações e adaptações.

[2] Tradução: Rede Virtual Privada

um contrato com alguma ISP [3](*Internet Service Provider*), ou a aquisição de um *link* privativo que resultaria a necessidade da criação de uma infra-estrutura entre as empresas a um custo mais elevado.

1.3 Metodologia

O projeto foi desenvolvido e testado na empresa Sandra Regina Munhoz ME, localizada na Rua Cônego Anselmo Valwenkens nº 183b.

Para o desenvolvimento e os testes foram utilizadas duas máquinas com configurações diferentes, e *internet* de provedores diferentes.

Um dos UTM utilizou-se de uma conexão banda larga Vivo Speedy 2 que foi nomeado como SpeedyFW, com a seguinte configuração: Processador Pentium 3, 512 MB SDRAM, HD 80 GB, placa de rede adicional Realtek RTL 8139C. O outro UTM utilizou uma conexão de 10 megas da NET empresas, que foi nomeado como NetFW, com a seguinte configuração: Processador Pentium Dual Core, 2GB DDR2, HD 300 GB, placa de rede adicional Realtek RTL 8139C. Cada UTM ficou com um *switch* da marca TP-LINK e um computador ligados a eles com a função de servidor.

Um computadores foi configurado com o Windows Server 2008 com a função de Terminal Server, e outro com o Ubuntu Server 13.10 com a função de Samba Server.

Os usuários remotos fizeram uso de outra conexão para efetuar o acesso como *road warriors*, conexões estas feitas a partir das casas dos desenvolvedores do projeto.

O Endian foi instalado nos dois computadores em sua versão estável 2.5, por meio de um disco de *boot*, previamente gravado. Durante a instalação do Endian é realizada a configuração inicial, onde é necessário que cada computador tenha uma faixa de IP diferente do outro para que ocorra comunicação

O computador NetFW foi configurado com o IP 192.168.1.254, e o computador SpeedyFW foi configurado com o IP 192.168.2.254, como visto, em faixas diferentes de IP. Foram digitadas senhas para os usuários root em cada uma das máquinas, e, após elas reiniciarem, as máquinas carregaram os processos para as configurações do *firewall*.

As configurações foram feitas por meio de um terceiro computador com o Linux usando a distribuição Ubuntu 13.04 e o navegador Mozilla Firefox. No navegador foram

[3] Em português: Provedor de Serviço de *Internet*

digitados os endereços de IP dos respectivos UTM utilizando a porta 10443, https://192.168.1.254:10443 e https://192.168.2.254:10443.

Na configuração inicial foram configuradas a senha para o admin e o tipo de rede que os UTM utilizariam, no caso: GREEN (rede local) e RED (*internet*).

O SpeedyFW foi configurado com uma conexão PPPoE, utilizando-se de um usuário senha. No NetFW a conexão RED foi configurada como DHCP, que recebe um IP dinâmico de um provedor de IPS.

Após essas configurações os processos dos UTMs são reiniciados, e já iniciam as redes locais para suas respectivas faixas de IPs.

Por conseguinte foram configurados os dynDNS para cada máquina. O *site* dynDNS dispõe um serviço de resolução de nomes para conexões com IPs dinâmicos: um foi configurado como speedyfw.dyndns.org, e o outro como netfw.dyndns.org. Em seguida foram configuradas as VPNs, para assim se obter a comunicação entre os servidores e clientes externos.

Os clientes externos foram configurados com o cliente gratuito openVPN 2.3.0 localizado em http://openvpn.net/index.php/download.html. Depois de instalado é usado um arquivo de configuração para fazer a comunicação com os Endians. O cliente OpenVPN no Endian gera um certificado, que deve ser disponibilizado para todos os clientes que se conectarão às respectivas redes.

Ao iniciar o processo de conexão, o Endian solicitará o nome de usuário e a senha para cada um dos usuários configurados no servidor, e conferirá a certificação exigida.

Após a conexão com os UTMs, os clientes adquirem um IP dentro da faixa dos UTM, e possuem acesso aos recursos disponibilizados dentro daquela rede. Os recursos disponibilizados podem ser compartilhamento e acesso a serviços nos servidores, recursos estes que podem ser controlados pelo *firewall* da VPN, aumentando a segurança de acesso aos dados por usuários distintos.

Os UTMs foram configurados como site-2-site, ou, como uma empresa ligada a outra empresa, assim os computadores e dispositivos dentro das redes obtiveram comunicação entre ambas as redes: os computadores ligados ao UTM NetFW obtiveram acesso ao *Terminal Server* dentro do SpeedyFW, como se fizessem parte da mesma rede. O *Terminal Server*, por

sua vez, obteve acesso ao Sambaserver configurado dentro da rede controlada pelo UTM NetFW.

A transferência de arquivos teve um limitante que é a banda disponível para transferência, mas o acesso ao *Terminal Server* foi satisfatório. A segurança a ataques externos obteve aumento significativo devido ao fato do fechamento de todas as portas de acesso externo.

2. SEGURANÇA DE REDES

A segurança de uma rede é um nível de garantia de funcionamento para que o conjunto das máquinas interligadas da rede funcionem de maneira otimizada e que os usuários tenham apenas os privilégios que lhes foram concedidos.

A segurança de rede possui objetivo de proteger a usabilidade, confiabilidade, integridade e segurança da uma rede e dados. Uma segurança de rede eficaz tem como alvo uma variedade de ameaças e as impede de entrar ou difundir na rede.

De acordo com o material disponibilizado na página http://en.kioskea.net/contents/606-protection-introduction-to-network-security (acesso em 03/01/2014), há alguns cuidados gerais para garantir a segurança de uma rede:

- Manter-se informado;
- Conhecer o sistema de exploração;
- Reduzir o acesso à rede (*firewall*);
- Reduzir o número de pontos de entrada (portas);
- Definir uma política de segurança interna (senha, lançamento de realizáveis);
- Utilizar utilitários de segurança;

2.1 Ataques e vulnerabilidades

Em segurança de computadores, uma vulnerabilidade é uma fraqueza que permite que um atacante reduza a garantia da informação de um sistema.

Para Anderson (2012), vulnerabilidade é a intersecção de três elementos: a suscetibilidade do sistema ou falha, o acesso do invasor pela a falha, e a posse de técnica e pelo menos uma ferramenta aplicável que pode se conectar a uma fraqueza do sistema por parte do invasor. Neste quadro, a vulnerabilidade é também conhecida como a superfície de ataque.

Segundo Anderson (2010), muitos ataques envolvem combinações de vulnerabilidades e quebra de senha, como exemplificado abaixo:

1 . Estouro de pilha no ataque o programa BIND, usado por muitos Unix e Linux hospedeiros de DNS , que dão acesso imediato à conta;

2 . Programas CGI vulneráveis em servidores Web, muitas vezes vindos do próprio fornecedor . Falhas de programas CGI são meios comuns de assumir e desfigurar servidores.

3 . Um bug no Internet Information Server (IIS), o software de servidor Web da Microsoft, que permitiu acesso imediato a uma conta de administrador no servidor.

4 . Ataques à NFS e seus equivalentes no Windows e nos Sistemas operacionais NT e Macintosh. Estes mecanismos são usados para compartilhar arquivos em uma rede local.

5 . Palpites de nomes de usuários e senhas, especialmente onde a raiz ou administrador senha é fraca, ou em que um sistema é fornecido com senhas padrão que as pessoas não se preocupam em mudar.

6 . Os protocolos IMAP e POP , que permitem o acesso remoto a *e-mail*, mas são muitas vezes mal configurados para permitir o acesso de intrusos .

7 . Autenticação fraca no protocolo SNMP, usado por administradores de rede para gerenciar todos os tipos de dispositivos conectados à rede.

2.1.1 Tipos comuns de ataques às redes

Sem medidas de segurança e de controle no lugar a rede pode ser submetida a um ataque. Os ataques podem ser passivos, quando a informação é monitorada , ou ativos , quando a informação é alterada com a intenção de danificar ou destruir os dados ou a própria rede.

Alguns dos principais tipos de ataques:

- Espionagem

Em geral as comunicações de rede trafegam em um formato inseguro chamado "texto puro", que permite a um invasor, que tenha obtido acesso a caminhos de dados em sua rede, "escutar" ou interpretar (ler) o tráfego de informações. A capacidade de um espião para monitorar a rede é geralmente o maior problema de segurança que os administradores enfrentam em uma empresa: sem serviços de criptografia, os dados podem ser lidos por outras pessoas.

- Modificação de dados

Depois de ler os dados, o próximo passo lógico é alterá-los. Um intruso pode modificar os dados no pacote sem o conhecimento do emissor ou receptor.

- Falsificação de identidade (falsificação de endereço IP)

A maioria das redes e sistemas operacionais usa o endereço IP de um computador para identificar uma entidade válida.. Um invasor também pode usar programas especiais para a construção de pacotes IP que parecem se originar de endereços válidos dentro da intranet corporativa.

- Ataques baseados em senha

A maioria dos sistemas operacionais possui controle de acesso baseado em senha. Isto significa que os direitos de acesso a um computador e recursos de rede são determinados pelo nome de usuário e sua senha.

Quando um atacante encontra uma conta de usuário válida, o atacante tem os mesmos direitos que o usuário real. Portanto, se o usuário tem direitos de administrador, o atacante também pode criar contas de acesso posterior em um momento posterior.

- Ataque *Sniffer*

S*niffer* é um aplicativo ou dispositivo que pode monitorar a troca de dados de rede, capturar pacotes e ler . Se os pacotes não são criptografados, um sniffer oferece uma visão completa dos dados dentro do pacote.

- Ataque de camada de aplicação

O ataque de camada de aplicação tem como alvo os servidores de aplicativos, que acontece deliberadamente causando uma falha no sistema operacional do servidor ou aplicações. Isso resulta no ganho do atacante de capacidade de contornar os controles de acesso normais.

2.2 Criptografia

Formada a partir dos termos gregos *kryptos* (escondido, oculto) e *graphé* (grafia, escrita) a criptografia é a ciência que possibilita a comunicação mais segura entre dois agentes, em um canal aberto, convertendo informação legível enviada por um agente, em algo sem sentido, com a capacidade de ser recuperada ao estado original pelo outro agente.

Para Terada a Criptografia pode ser definida como

> a ciência que estuda a transformação de dados de maneira a torná-los incompreensíveis sem o conhecimento apropriado para a sua tradução, tornando os conteúdos secretos, evitando riscos internos e externos que venham a ocorrer durante o trajeto dos dados enviados, que são convertidos em um código que só poderão ser traduzidos por quem possuir a "chave" secreta, enquanto que a Criptoanálise executa o processo inverso, sendo a ciência que estuda a decifração, tornando o código compreensível. (TERADA, 2000, p.16)

Para Morimoto a criptografia

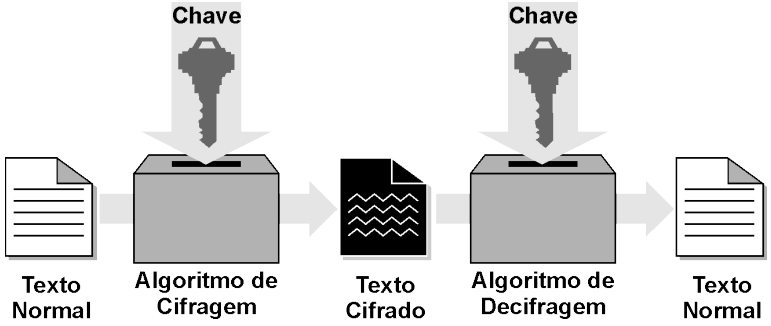
> consiste em cifrar um arquivo ou mensagem usando um conjunto de cálculos. O arquivo cifrado (ou encriptado) torna-se incompreensível até que seja desencriptado. Os cálculos usados para encriptar ou desencriptar o arquivo são chamados de chaves. Apenas alguém que tenha a chave poderá ler o arquivo criptografado. (Disponível em http://www.hardware.com.br/termos/criptografia, acesso em 05/01/2013)

Com objetivo de ocultar informações não autorizadas e garantir privacidade, a criptografia transforma informação inteligível em ilegível.

2.2.1 Chaves

Segundo TRINTA e MACÊDO (1998), chaves de criptografia são como senhas de acesso a computadores ou a caixas eletrônicos. Com a senha correta, o acesso do usuário é permitido, mas, se a senha é incorreta ou o usuário não a possui, o acesso é negado. Para a criptografia, o uso de chaves está relacionado com o acesso ou não à informação cifrada. Para decifrar as mensagens é necessário que o usuário utilize a chave correta, como é possivel visualizar na figura 1, onde o texto cifrado retorna a sua forma original com o uso da chave para decifrar a mensagem enviada.

Figura 1 – Cifragem e decifragem de uma mensagem



Fonte: TRINTA e MACÊDO, 1998, disponível em http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm.

Assim como as senhas de acesso, as chaves na criptografia possuem diferentes tamanhos, e seu grau de segurança também está relacionado com sua extensão

> na criptografia moderna, as chaves são longas seqüências de bits. Visto que um bit pode ter apenas dois valores, 0 ou 1, uma chave de três dígitos oferecerá $2^3 = 8$ possíveis valores para a chave. Sendo assim, quanto maior for o tamanho da chave, maior será o grau de confidencialidade da mensagem (TRINTA e MACÊDO, 1998, disponível em http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm).

2.2.2 Tipos de criptografia

Segundo Yoshida (2001) existem dois principais tipos de criptografia: a simétrica e a assimétrica.

Na criptografia simétrica, o algoritmo e a chave são iguais, ou seja, a mesma chave que é utilizada para encriptar a mensagem também é utilizada para desencriptar.

Na criptografia assimétrica são utilizadas duas chaves relacionadas: uma pública para encriptar e outra privada, para desencriptar. Dessa forma, uma mensagem criptografada com uma chave pública só poderá ser desencriptografada com a chave privada correta.

3. FERRAMENTAS UTILIZADAS NO DESENVOLVIMENTO DO PROJETO

3.1 *SOFTWARE* LIVRE

A ideia do *Software* Livre é de Richard Stallman, e consiste em um movimento de combate à tendência de desenvolvedores e empresas de *software* de não distribuírem o código livre para uso, estudo, cópia e distribuição, somente os executáveis.

> Por "software livre" devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários. Grosso modo, os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software. Com essas liberdades, os usuários (tanto individualmente quanto coletivamente) controlam o programa e o que ele faz por eles. Quando os usuários não controlam o programa, o programa controla os usuários. O desenvolvedor controla o programa e, por meio dele, controla os usuários. Esse programa não-livre e "proprietário" é, portanto, um instrumento de poder injusto. (Disponível em http://www.gnu.org/philosophy /free-sw.pt-br.html, acesso em 02/12)

De acordo com as informações disponibilizadas na página http://www.gnu.org/, um *software* é livre se respeita quatro liberdades:

- A liberdade de executar o programa, para qualquer propósito (liberdade 0);
- A liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades (liberdade 1). Para tanto, acesso ao código-fonte é um pré-requisito;
- A liberdade de redistribuir cópias de modo que você possa ajudar ao próximo (liberdade 2);
- A liberdade de distribuir cópias de suas versões modificadas a outros (liberdade 3). Desta forma, você pode dar a toda comunidade a chance de beneficiar de suas mudanças. Para tanto, acesso ao código-fonte é um pré-requisito.

3.1.1 Linux

Em 1991, Linus Torvald iniciou um projeto pessoal como um *hobby*, que ficou conhecido como *Linux Kernel*. Esse projeto teve como base para desenvolvimento outro sistema chamado *Minix* (Mini-Unix), desenvolvido por Andrew S. Tenenbaum, que foi baseado no UNIX. O nome Linux surgiu, portanto, do nome do idealizador Linus e o X em homenagem ao Unix.

Em 1992 Linus lançou o *Kernel* do Linux sob a GNU (*General Public License*), disponibilizando, dessa forma, a garantia do *software* livre para o usuário final usar, estudar,

alterar, copiar e distribuir gratuitamente.

Acredita-se que o sucesso do Linux foi decorrente da decisão de compartilhamento tomada por Linus, que garantiu que os programadores pudessem contribuir para o *Kernel* do Linux e que tivessem certeza de que seu trabalho continuaria livre e ajudaria a todos os usuários, afastando o Linux de empresas de *software* que o usariam em benefício próprio.

O Linux continua em desenvolvimento constante pela comunidade *Open Source* usando linguagens de programação C e *Assembly*, e pode ser encontrado em distribuições gratuitas em versões tanto para servidores quanto para *desktop*.

O *Kernel* do Linux foi altamente portado, e, atualmente, pode ser usado em vários tipos de arquiteturas de *hardware*. Ele está presente desde celulares até os mais rápidos supercomputadores do mundo.

3.2 VPN

A sigla VPN, como já supracitado, significa *Virtual Private Network*, em português, Redes Privadas Virtuais, onde: Rede corresponde às redes de computadores; Privada corresponde à forma como os dados trafegam (neste caso os dados podem ser criptografados , garantindo a privacidade das informações) e virtual por não fazerem, necessariamente, parte do mesmo meio físico (FAGUNDES, 2007).

Historicamente, quando uma empresa necessita de comunicação com uma filial, ela investe em um *link* privativo, que a oferece segurança e disponibilidade todo o tempo. Entretanto, ainda que bastante seguro, este meio de comunicação pode sofrer vários problemas externos e defeitos, já que utiliza apenas uma via de comunicação, e esta via está sujeita a problemas técnicos.

Em contrapartida, a solução VPN utiliza qualquer infra-estrutura de comunicação pública disponível para efetuar a comunicação entre filiais e vendedores (*road warriors*), por exemplo. Um exemplo de serviço de VPN gratuito é gratuito é o *OPEN*vpn, que pode ser executado nos mais variados dispositivos e sistemas operacionais, e é altamente seguro, no anexo2 a descrição do openVPN.

Segundo Chin (2010), uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elas eliminam a necessidade de *links* dedicados de longa distância, substituindo-os pela *Internet*.

Segundo Gilbert Held VPN pode ser definida como uma rota temporaria fisica

formada sobre uma estrutura de rede publica e existem quatro principais desvantagens da VPN:

- Exige a compreensão dos métodos necessários para assegurar a transmissão através de uma rede pública
- Pode exigir configuração personalizada além do uso de assistente.
- Obtenção de alcançar uma qualidade e capacidade de serviço Desempenho depende de fatores externos da organização
- Interoperabilidade total entre produtos de diferentes fornecedores podem ser difíceis de alcançar, devido à complexidade de algumas normas relacionadas com VPN

Segundo Roger Sutton (2002), uma rede privada

> é aquela que é dedicada a um grupo de usuários e é mantida escondida . Portanto, uma rede privada virtual atua como dedicada a um grupo de usuários e está escondida de todos os outros enquanto opera através de uma rede pública. A rede pública é a internet (ou outra rede baseada em IP), o que é notório por ser na zona de recreio do atacante , o ponto importante é que a rede está oculta para os forasteiros.

Ainda sob os termos de Sutton (2002), o conceito de VPNs é o de um nó que pode aderir à rede para uma função desejada a qualquer momento. Por se colocar os dados dentro de um pacote de IP, as informações permanecem escondidas, encapsulando o pacote inteiro, e é colocado em um novo pacote IP. Este novo pacote IP é enviado ao destino de entrada e transmitido através da rede pública.

As informações que estão encapsuladas são retiradas na chegada ao ponto de destino e encaminhadas para o seu verdadeiro endereço na rede privada. Este processo é chamado de *Link* de Túnel.

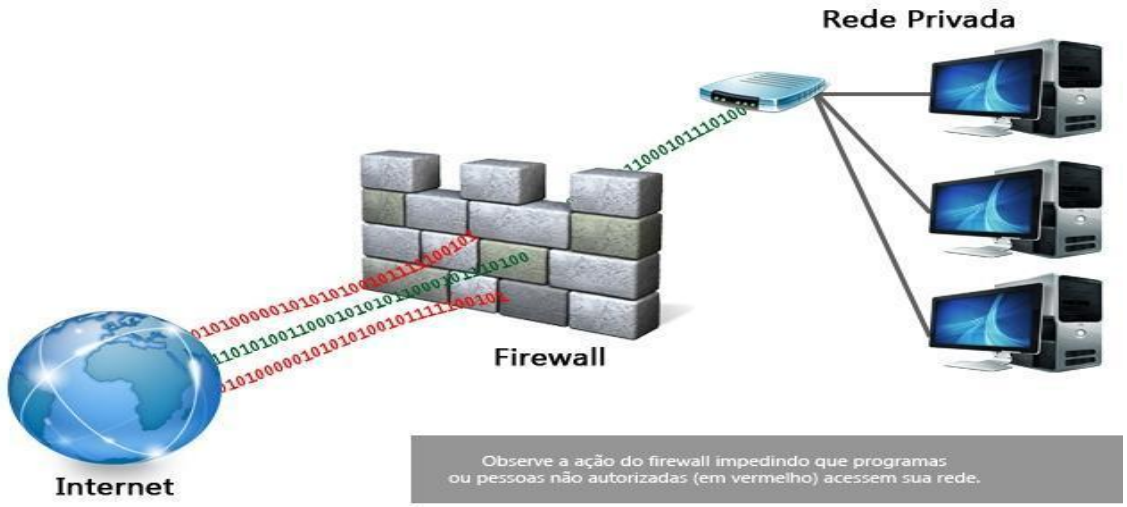
As LANs[4] (*Local Area Network*) podem, por exemplo, por meio de *links* dedicados ou discados, conectarem-se a algum provedor de acesso local e interligarem-se a outras LANs, possibilitando o fluxo de dados através da *Internet*. No entanto, uma VPN depende da rede pública (*Internet*) para realização de suas conexões.

[4] Tradução: Rede Local

3.3 *FIREWALL*

Segundo Urubatan Neto (2004), um *firewall* é um *software* que tem a autonomia concedida pelo próprio sistema para controlar o tráfego existente entre o mesmo e outros *hosts*/redes. Em alguns casos, ele pode ser também uma combinação de *hardware* e *software* com a função de isolar a rede interna da *Internet*, permitindo que alguns pacotes passem e bloqueando outros como ilustrado na figura 2. Há mais de uma forma de funcionamento de um *firewall*, que varia de acordo com o sistema, aplicação ou desenvolvedor do programa.

Figura 2: *Firewall*



Fonte: http://toniinfo.com/firewall/

3.3.1 *Firewall* "filtro de pacotes"

A classe de *Firewall* "filtro de pacotes" é responsável por filtrar todo o tráfego direcionado ao próprio *host firewall* ou à rede que o mesmo isola, tal como todos os pacotes emitidos por ele ou por sua rede. Ocorre mediante a análise de regras previamente inseridas pelo administrador do mesmo (NETO, 2004). Esta é a classe de *Firewall* mais utilizada e a não utilização destes conceitos em uma rede permite a livre circulação de pacotes não confiáveis pela rede.

Para NETO (2004), o *firewall* "filtro de pacotes" é capaz de analisar cabeçalhos de pacotes enquanto trafegam pela rede. Por meio desta análise, que é o resultado de uma comparação complexa das regras previamente definidas, é decidido qual o destino do pacote, se será permitido seu tráfego livre de determinado pacote pela rede ou então se será bloqueada sua trajetória, ignorando o pacote por completo.

Existem três motivos para a implementação do *firewall* "filtro de pacotes" em uma rede, são eles:

a) Controle: Com regras bem definidas, é possível determinar tudo o que é enviado para a rede, o que circula pela rede e o que é enviado pela mesma;

b) Segurança: Uma rede é segura quando se tem controle sobre o que trafega por ela;

c) Vigilância: A partir das regras de segurança pacotes considerados suspeitos serão ignorados.

3.3.2 *Firewall* NAT

Um *Firewall* aplicado à classe NAT, a princípio, possui o objetivo de manipular a rota padrão de pacotes que atravessam o *karnel* do *host firewall* aplicando-lhes o que conhecemos por "tradução de endereçamento".

Manipular a rota lhes agrega diversas funcionalidades dentro do conceito de NAT, como por exemplo, manipular o endereço de origem (SNAT) e o destino dos pacotes (DNAT) dos pacotes, e realizar *masqueranding* sobre conexões PPP, entre outras potencialidades.

Para NETO (2004) o *firewall* NAT permite muito mais que a filtragem de pacotes, ele parte para outros aspectos que envolvem conceitos de roteamento de redes. É possível, por exemplo, que um *Firewall* NAT realize o trabalho de um *Proxy*.

Em uma conexão envolvendo uma rede local, a *internet* e um *firewall* NAT, o *firewall* NAT estabelece uma conexão entre as redes sem que elas efetuem comunicação direta, resultando no que é conhecido por SNAT. Isso é possível, pois o *Firewall* NAT altera o endereço de origem do pacote enviado pela rede local, passando a ser o endereço do H*ost Firewall* Nat o que ocorre também na operação inversa.

3.3.3 *Firewall* Híbrido

Segundo NETO (2004) "um *firewall* híbrido agrega a si tanto funções de filtragem de pacotes quanto de NAT. Trata-se, na verdade, da união de ambas as classes e não tão somente de uma classe isolada com propriedades próprias".

3.3.4 UTM

O conceito UTM [5](*Unified Threat Management*) surgiu por volta de 2004 como uma evolução *firewall*, visando a combinação de vários recursos de segurança de rede em apenas um dispositivo.

Segundo John Jacob, a aplicação UTM foi definida como produto que agrupa vários recursos de segurança. Para ser chamado UTM, a aplicação ou dispositivo precisa ter capacidade para realizar ao menos quatro funções, sendo elas: de *firewall*, detecção de intrusos e prevenção, e *gateway* antivírus. Além disso, o dispositivo também deve ter um sistema operacional e um processo de instalação que requer o mínimo de intervenção humana.

Podem ser, ainda, atribuídas outras funcionalidades à UTM, tais como gerenciamento de segurança e gestão de políticas de grupo ou usuário(s).

Segundo John R. Vacca (2012), Sistemas UTM são multicamadas e incorporam várias tecnologias de segurança da informação. Produtos UTM, ainda, fornecem serviços diversos como antivírus, VPN, serviços de *firewall* e *antispam*, além da prevenção contra ataques.

As vantagens de um sistema de UTM são sua facilidade de ser operado e configurado, e a agilidade da atualização de seus recursos de segurança, o que proporciona uma evolução rápida contra ameaças e atende à demanda por segurança.

UTM é um sistema que foi projetado para ser flexível, adaptável, e de fácil e rápido gerenciamento. Ele incorpora *firewall*, VPN, fonte confiável, IPs, antispan e antivírus, URL *filtreing* descriptografia SSL, e de auditoria / relatórios.

Um exemplo de um UTM *Open Source* é o *Endian*, que, além dos seus módulos de segurança padrão, inclui um módulo de VPN, por meio do *software Open source OPEN*vpn, que foi utilizado na elaboração deste protótipo.

3.4 Endian UTM

Baseado no sistema operacional Linux, distribuição IPCop, o Endian UTM possui várias funções de integração e segurança de redes. Criado sob o conceito de UTM, concentra em apenas um produto soluções como *firewall proxy* de *e-mails,proxy web*, antispam, antivírus, roteador, IDS (Intrusion Detection System) e servidor VPN.

[5] Tradução: Central Unificada de Gerenciamento de Ameaças

Desenvolvido pela empresa italiana Endian, o Endian UTM também pode ser encontrado na versão de hardware e software combinados, versão, por sua vez, comercial. A versão utilizada neste protótipo é a ferramenta Open Source.

A versão comercial da EDIANT UTM oferece algumas funcionalidades adicionais se comparada à *open source*:

- Suporte técnico;
- Opção pela utilização de antivírus de versões comerciais;
- Clientes VPN nativos para Microsoft Windows, MacOS e Linux;
- HotSpot, que é disponibilidade de controle especifico de pontos de acesso às redes sem fio.

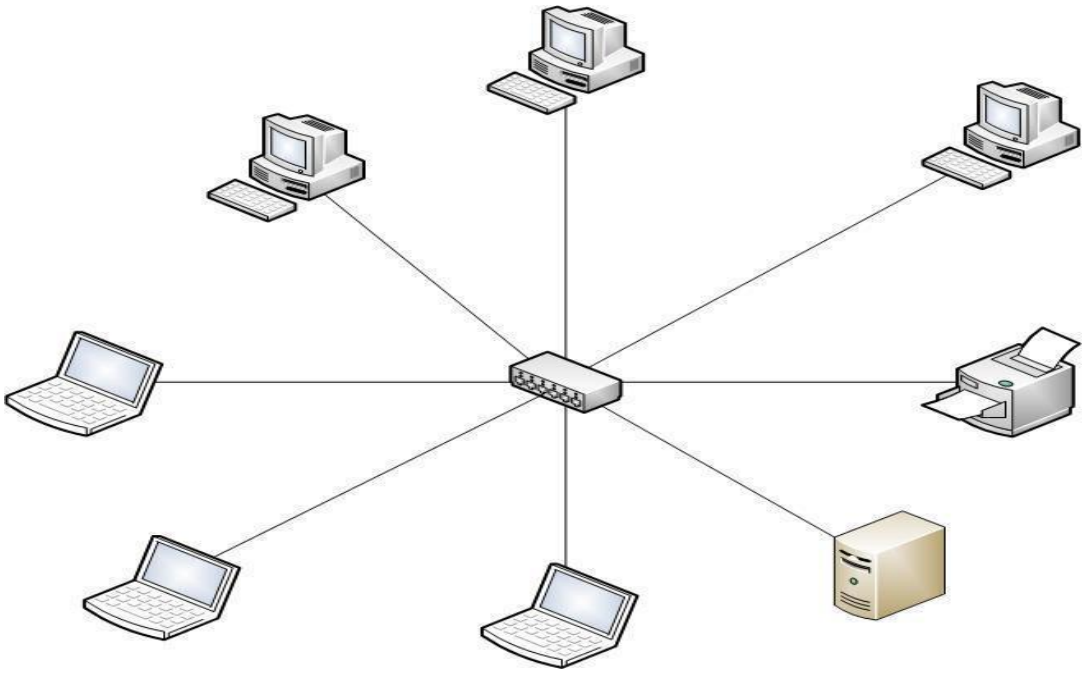
Para obter a versão *Open Source* do Endian UTM basta acessar a página http://www.endian.com/en/community/download/ e executar o *download*. Em sua versão de código aberto, voltado para desenvolvedores e e*arly-adopters*, para ambientes de computação não críticos ou uso privado, o apoio do Endian não está disponível, o suporte é fornecido somente pela Comunidade *Open Source* por de fóruns e listas de discussão. O Anexo 1 exibe todas as funcionalidades do Edian UTM distribuídas nas versões *open source* e comercial.

3.5 LAN - *Local Area Network*

Para Bradley Mitchell, uma rede local (LAN) define-se como a ligação em rede ou a capacidade de comunicação em um grupo de computadores próximos, como em escritórios, casas e escolas. A LAN é utilizada no compartilhamento de recursos como arquivos, impressoras, jogos ou outras aplicações.Em muitos casos a LAN se conecta a outras redes locais, com a Internet ou outra WAN.

Philip Miller e Michael Cummins (2000, p.4) definem LAN como um conjunto de dispositivos que estão interligados através de um meio de transporte comum para fins de troca de informações em uma mesma edificação, como visto na figura 3.

Figura 3: LAN



Fonte: o autor

Segundo Carlos E. Morimoto , LAN consiste em:

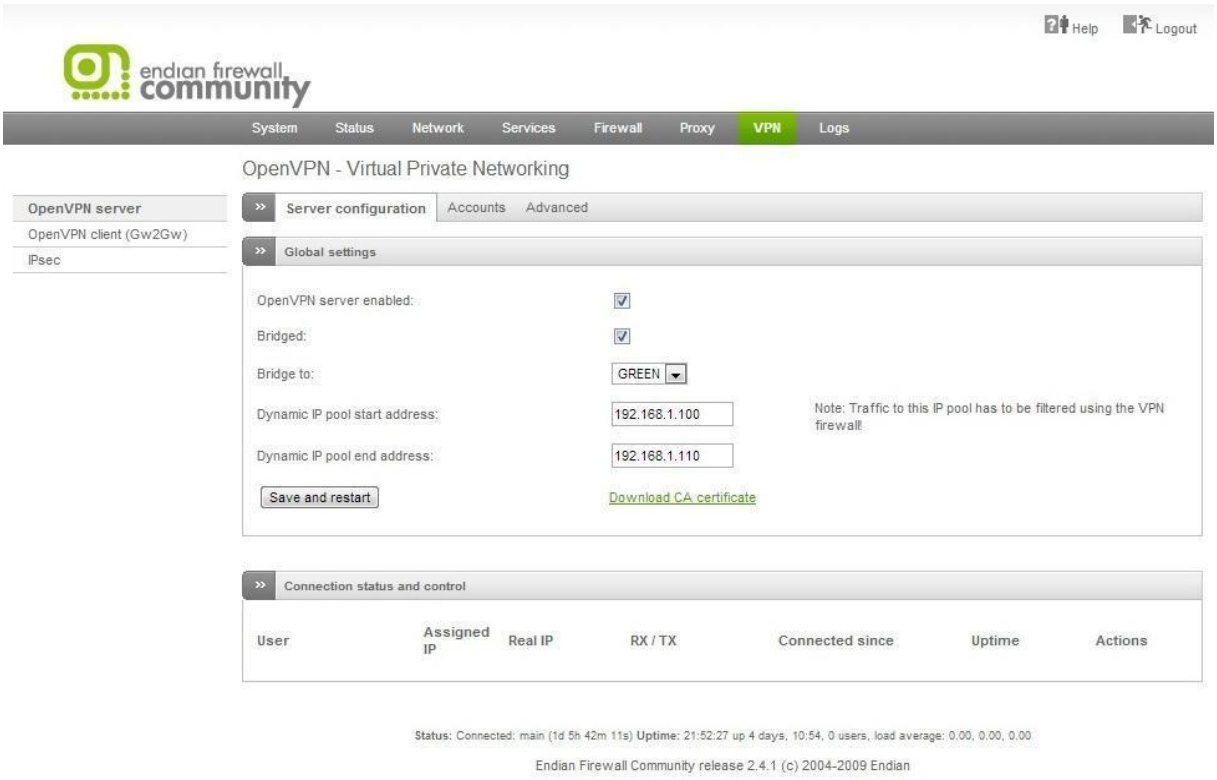
> Local Area Network, ou rede local. Qualquer rede de micros que englobe um pequeno espaço, uma sala, um andar ou mesmo um prédio. Como estas pequenas redes são de longe as mais numerosas atualmente é comum ver o termo LAN usado até mesmo como sinônimo de rede. (Disponível em http://www.hardware.com.br/termos/lan, acesso em 03/12)

4. CONFIGURAÇÃO E EXECUÇÃO

4.1 CLIENT-SITE

O servidor de VPN foi ativado e configurado para fazer uma *bridge* para a conexão local GREEN. Além disso, foi configurado o OPENvpn para trabalhar com o servidor DHCP da rede em uma faixa diferenciada para os usuários da VPN. A ação pode ser vista na figura 4:

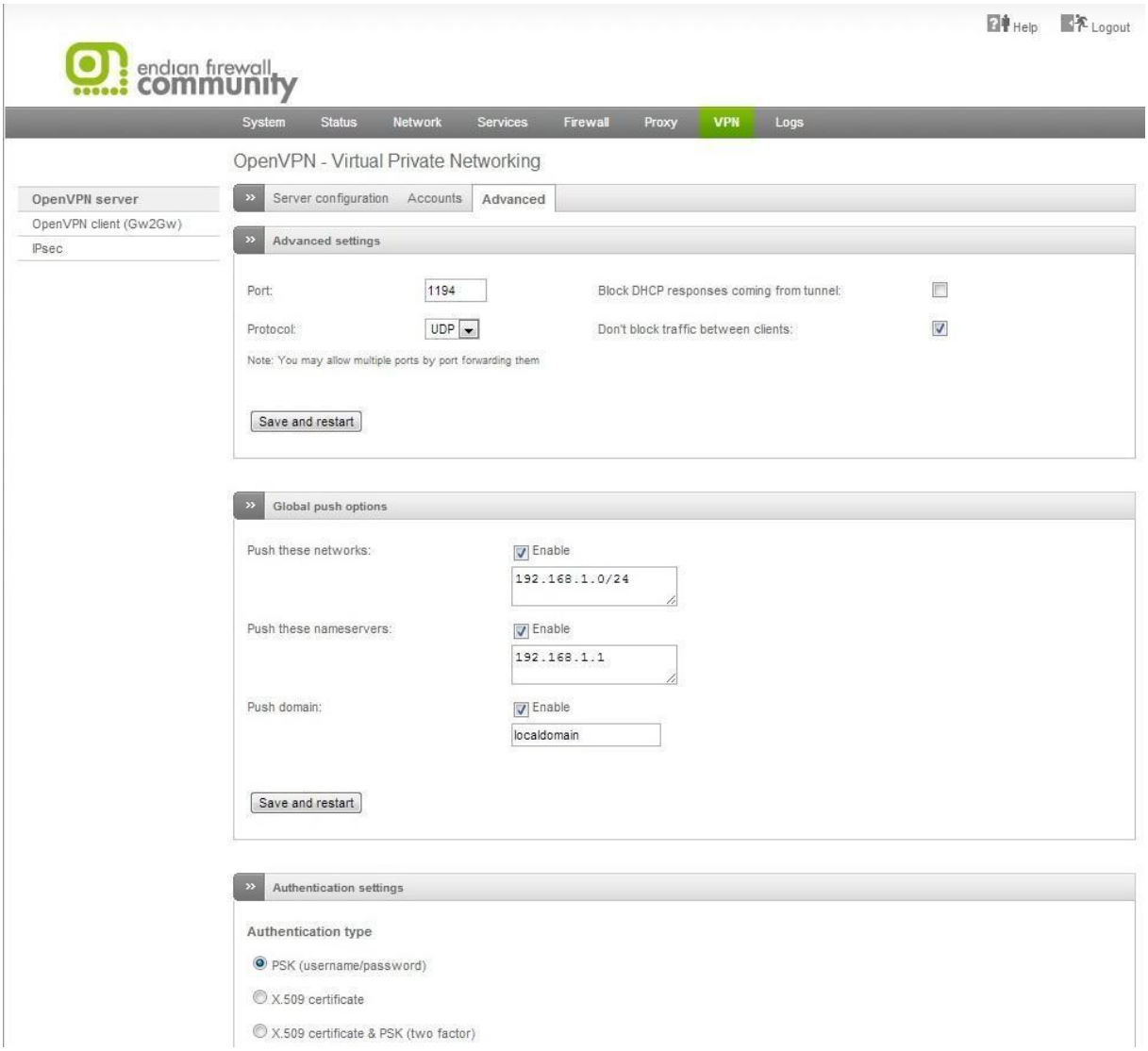
Figura 4: Configuração de Servidor



Fonte: o autor

Logo após, foi configurado para que as conexões fossem feitas por meio Porta UDP 1194, fazendo com que os clientes utilizem o *gateway* e o DNS do servidor local, como na figura 5:

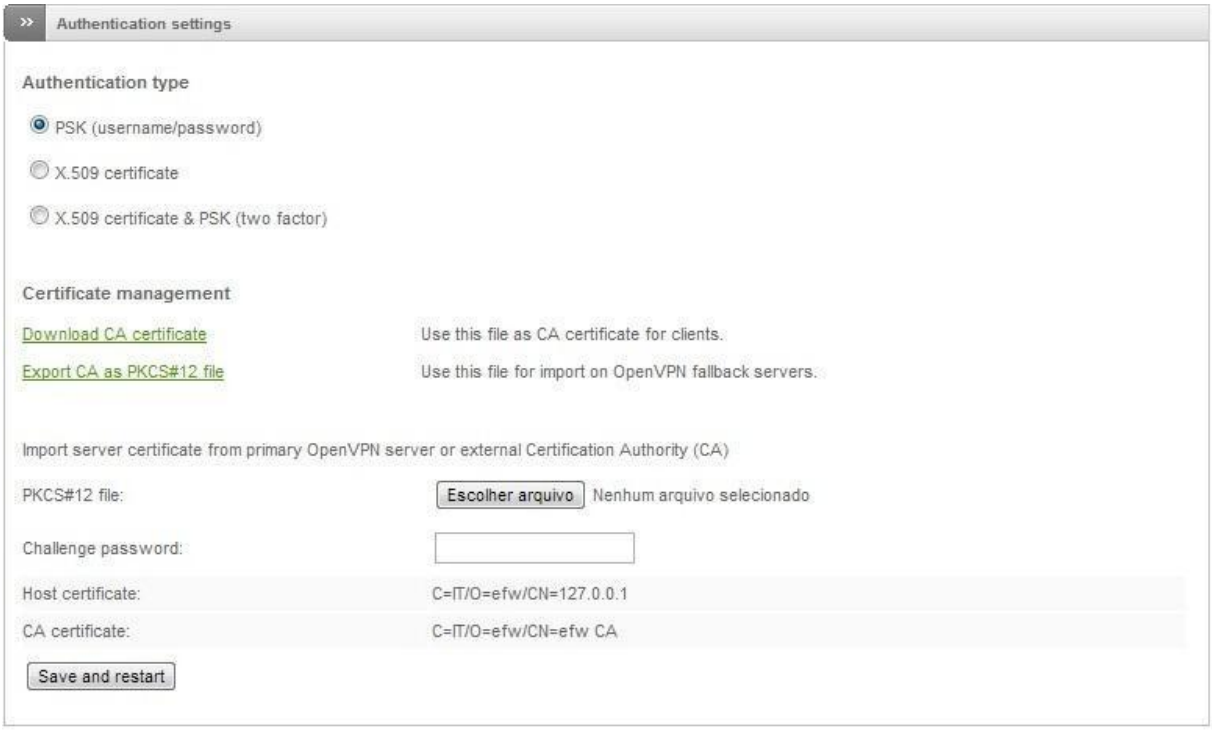
Figura 5: Configuração de porta



Fonte: o autor

A configuração de segurança foi realizada utilizando OPENvpn que gera um certificado para autenticação dos clientes no servidor, além do nome de usuário e senha. A ação pode ser verificada na figura 6:

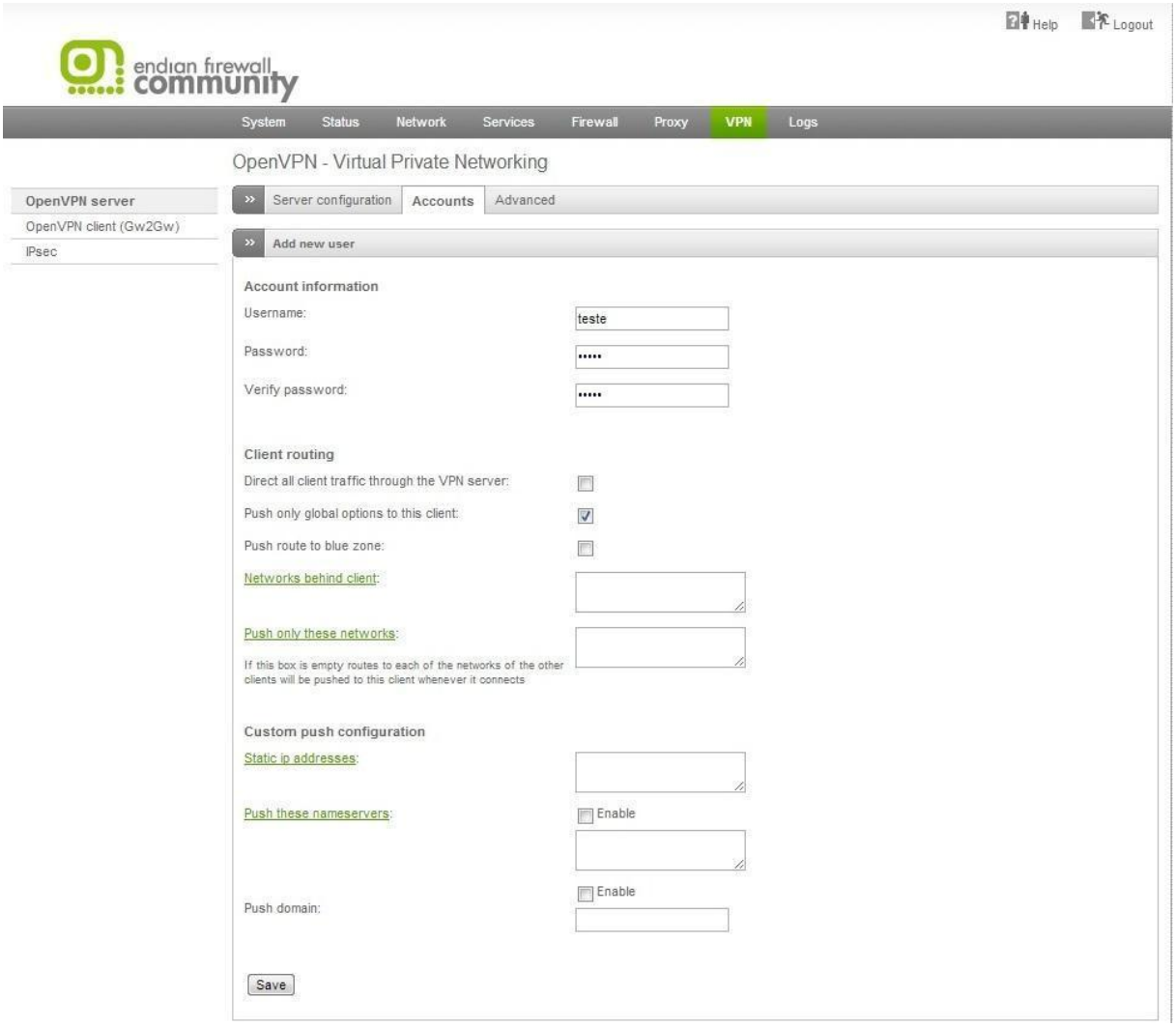
Figura 6: Configurações de autenticação



Fonte: o autor

Na criação dos usuários, foram configurados nome de usuário e senha, para que seja utilizada a rede global, e não uma configuração definida para cada usuário, como visto na figura 7:

Figura 7: Configuração de usuários

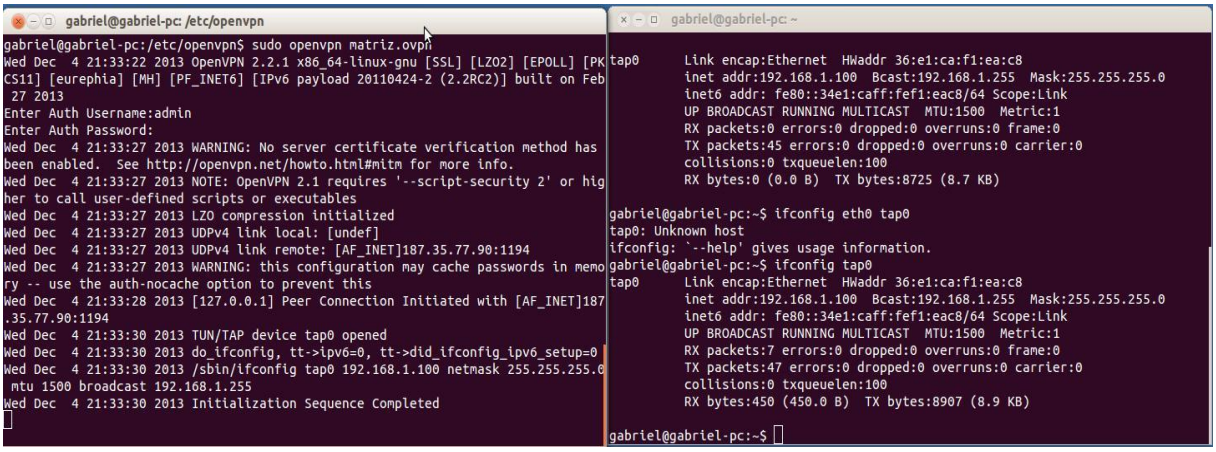


Fonte: o autor

Nos usuários remotos (*road warriors*) foram instalados clientes OPENvpn para Windows e Linux. Foi criada, também, uma pasta nos documentos dos usuários com o arquivo de configuração e certificado juntos. A conexão pode ser usada a partir da GUI do OPENvpn ou executando o arquivo .ovpn (clicando em cima do mesmo com o botão direito do *mouse*). Quando executado o arquivo, será solicitado o nome de usuário e senha, e, no arquivo de configuração, o OPENvpn verificará o certificado que está na mesma pasta.

A conexão segura é criada e o usuário recebe a faixa de IP do servidor, fazendo com que a conexão local não tenha problemas intervenientes e usando os serviços da rede da matriz. Essas informações podem ser verificadas na figura 8:

Figura 8: Conexão remota utilizando Linux

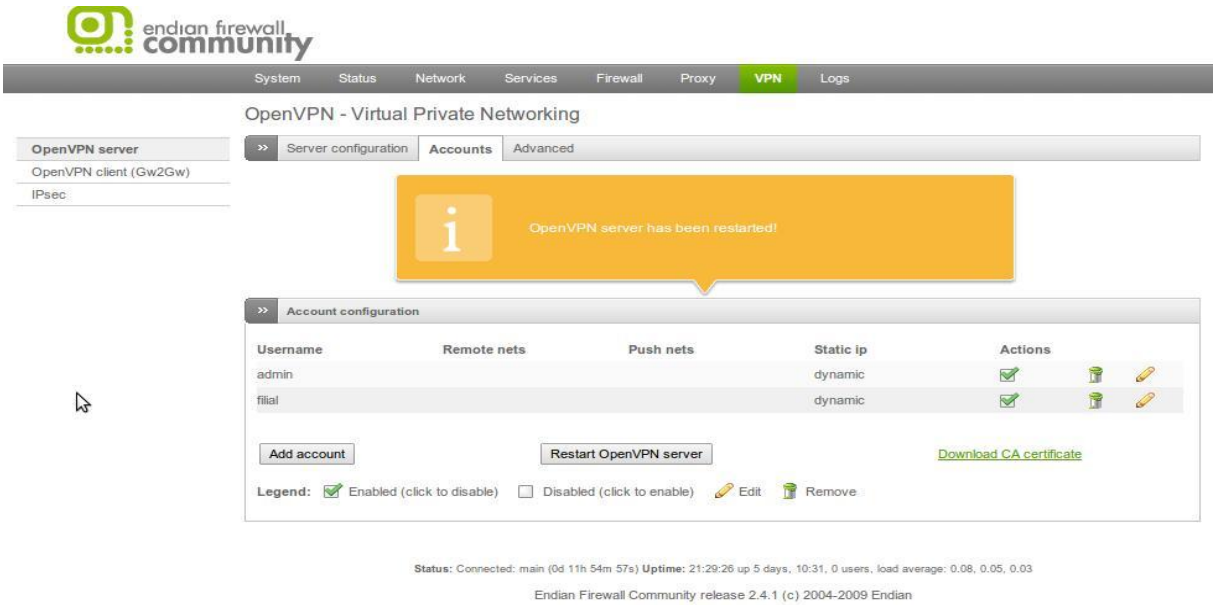


Fonte: o autor

4.2 SITE-TO-SITE

A comunicação Site-to-Site foi estabelecida utilizando o UTM da filial como cliente. Foi criado um usuário para essa VPN filial no servidor da matriz, e, da mesma forma, foram criados usuários para os *road warriors*; houve a importação do certificado para o UTM filial. O processo descrito pode ser verificado na figura 9:

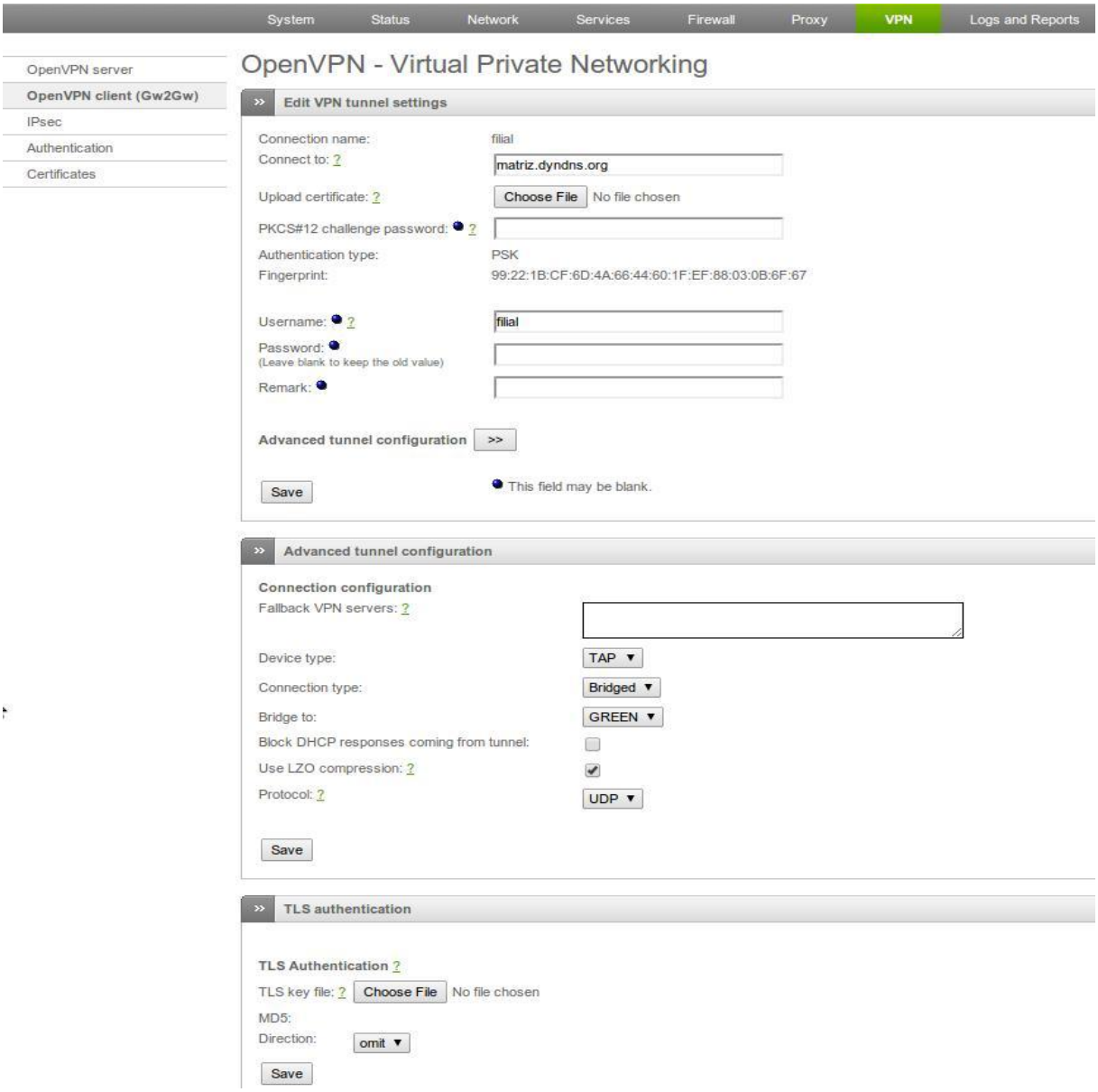
Figura 9: Usuários Criados Matriz



Fonte: o autor

Na filial foi feita a configuração do OPENvpn cliente gateway to gateway ou site-to-site (gw2gw), configurando um usuário para a conexão com a matriz**,** como visto na figura 10:

Figura 10: Configuração usuário-matriz



Fonte: o autor

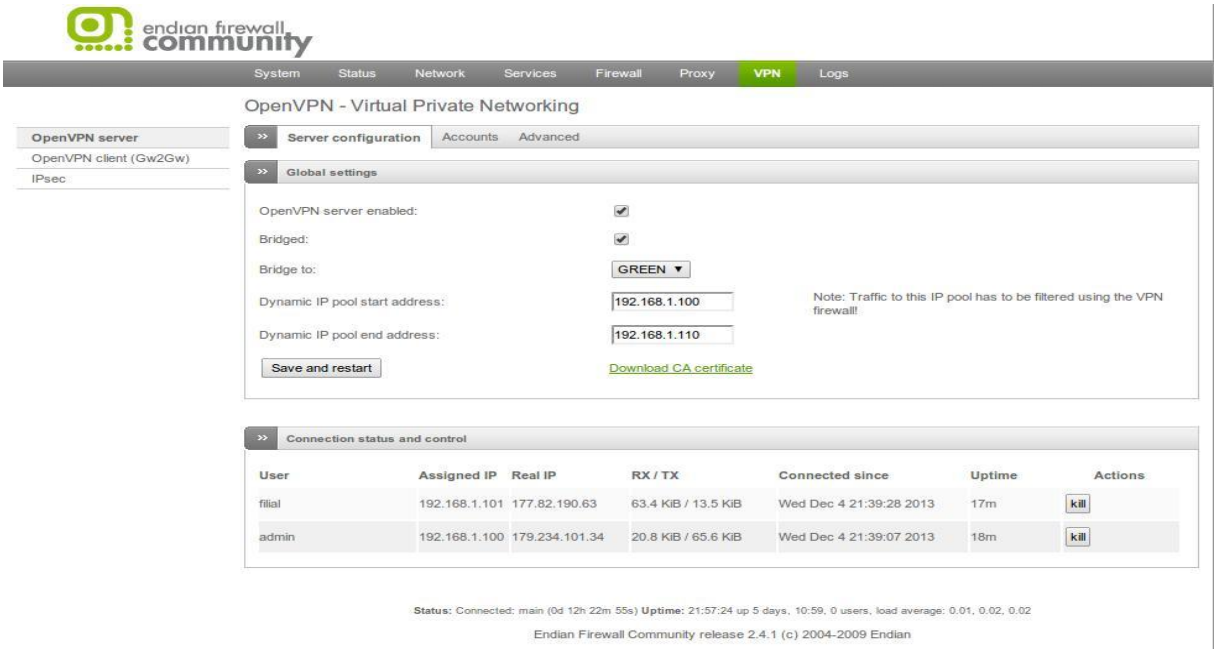
A conexão é estabelecida automaticamente após a criação do usuário**,** como pode ser visto na figura 11:

Figura 11: Conexão filial-matriz

Fonte: o autor

Conexão estabelecida tanto para o *Road warrior* quanto para a filial no servidor figura 12.

Figura 12: Conexão Estabelecida Server



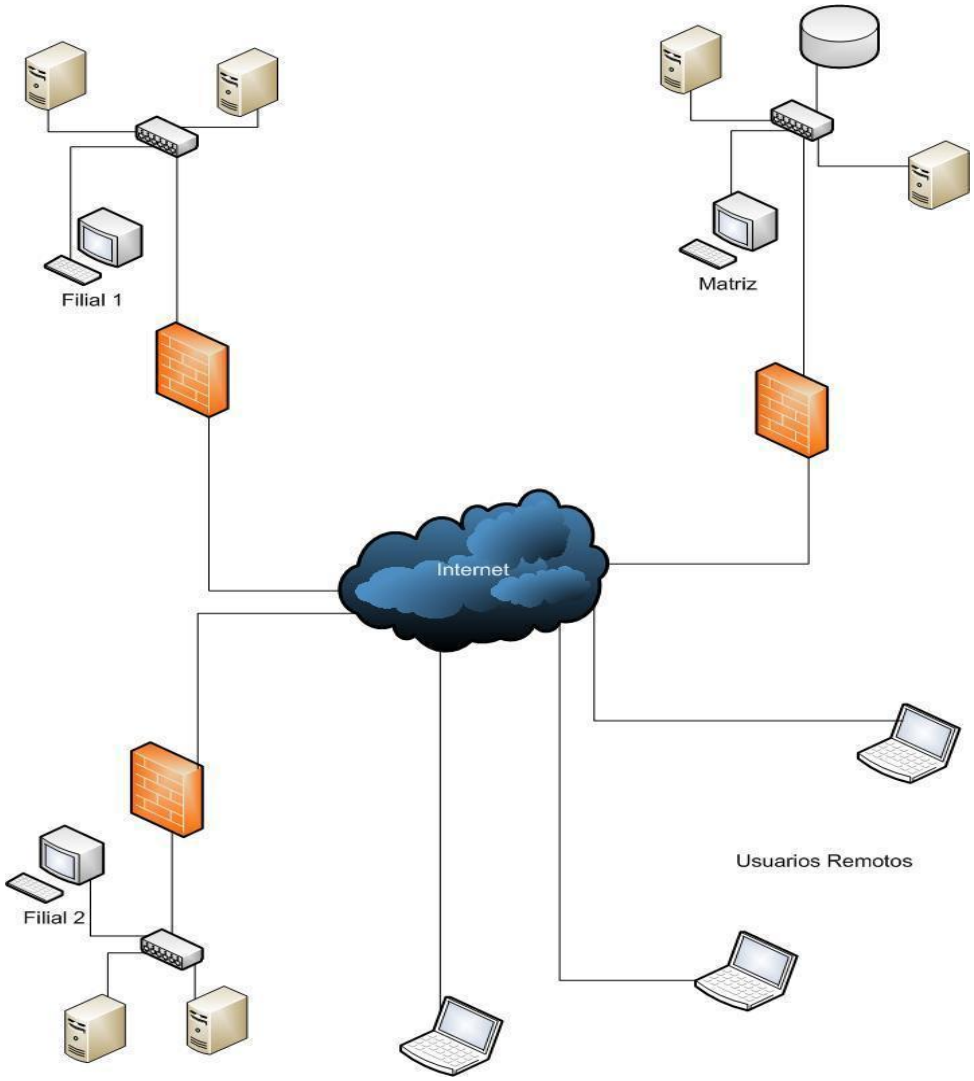
Fonte: o autor

Depois de estabelecida a conexão, os clientes, pela filial, possuem acesso aos arquivos e serviços dentro da matriz.

5. CONCLUSÃO

Utilizando as técnicas e ferramentas apresentadas neste artigo foi criada uma conexão VPN segura entre matrizes, filiais e usuários remotos (*road warriors*), que garantiu acesso aos dados das empresas com segurança e eficácia, como mostra a figura 13:

Figura 13: Protótipo do Projeto



Fonte: o autor

A VPN reduziu a zero os ataques às portas de serviços remotos, como *terminal server*, pois elas mesmas foram fechadas. A garantia do acesso aos dados internos foi assegurada pela VPN.O requisito de *hardware* para uso dessas aplicações é baixo. Para a comunicação entre uma matriz e filial foram usados computadores com as seguintes configurações:

- Processadores: Pentium Dual-Core e Pentium 3
- Memória RAM: 2GB DDR2 e 512 sdram
- Disco rígido de 300gb e 80 gb.
- A conexão dos usuários foi estabelecida por meio de *desktops* variados.

REFERÊNCIAS

ANDERSON, Ross, J. **A Guide to Building Dependable Distributed Systems.** John Wiley & Sons**.** 2 ª Ed. 2010

ANDERSON, Ross, J. **Security Engineering**. Cram101. 2 ª Ed. 2012

Criptografia disponível em <http://www.hardware.com.br/termos/criptografia>. Acesso em 05/01/2014

CUMMINS, Michael ; MILLER, Philip. **LAN Technologies Explained.** Digital Press, 2000, p.4.

CHIN, Liou Kuo. **Rede Privada Virtual**. Disponível em: <http://www.rnp.br/newsgen/9811/vpn.html> Acesso em 25/11/2013

FAGUNDES, Bruno Alves. **Uma Implementação de VPN.** 2007. 76f. Monografia (Graduação em Tecnologia da Informação e Comunicação) – Instituto Superior de Tecnologiaem Ciências da Computação de Petrópolis, Petrópolis. Disponível em <http://www.lncc.br/~borges/doc/Uma%20Implementa%E7%E3o%20de%20VPN.TCC.pdf>. Acesso em 25/11/2013.

GHORBANI, Ali; LU,Wei; TAVALLAEE, Mahbod; **Network Intrusion Detection and Prevention: Concepts and Techniques.** Springer, 2009, p.1

Introdução à segurança de redes disponível em <http://en.kioskea.net/contents/606-protection-introduction-to-network-security>. Acesso em 03/01/2014

LEITE, Leonardo Alexandre Ferreira. **Resumo - Máquinas Virtuais.** Disponível em: <http://stoa.usp.br/leonardofl/files/1402/7860/virtualizacao_leonardo.pdf>. Acesso em 25/11/2013.

MACEDO, Rodrigo Cavalcante de; TRINTA, Fernando Antonio Mota. **Um Estudo sobre Criptografia e Assinatura Digital** disponível em < http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. 1998

MARKOFF, John**. BUSINESS TECHNOLOGY :One Man's Fight for Free Software.** Disponível em <http://www.nytimes.com/1989/01/11/business/business-technology-one-man-s-fight-for-free-software.html>. Acesso em 25/11/2013.

NETO, Urubatan. **Dominando Linux Firewall Iptables**. Rio de Janeiro: Editora Ciência moderna Ltda,2004, p. 11,12 e 13.

Open Source disponível em <http://www.gnu.org>. Acesso em 02/12/2013.

Open VPN disponível em <http://openvpn.net/index.php/manuals.html> Acesso em 02/12/2013

O que é GNU/Linux disponível em <http://www.vivaolinux.com.br/linux/>. Acesso em 23/11/2013.

O que é segurança de redes? Disponível em <http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html>. Acesso em 03/01/2014

O que é software livre? Disponível em <http://www.gnu.org/philosophy/free-sw.html>. Acesso em 25/11/2013.

SUTTON, Roger. **Secure Communication: Applications and Management**. John Wiley & Sons, 2002, p. 275 e 276.

TERADA, Routo. **Segurança de Dados: Criptografia em Redes de Computador**. Edgard Blucher, 2000

Tipos comuns de ataques a redes disponível em < http://technet.microsoft.com/en-us/library/cc959354.aspx>. Acesso em 05/01/2014

The rise of integrated security appliances disponível em < http://www.channelbusiness.in/index.php?Itemid=83&id=252&option=com_content&task=view> acesso em 02/12/2013.

VACCA, John R. **Computer and Information Security Handbook.** 2012.

VASQUES, Tamer Alan; SCHUBER, Rafael Priante**. Implementação de uma VPN em Linux utilizando o protocolo IPSec.** 2002. 72f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro Universitário do Estado do Pará – CESUPA, Belém.

YOSHIDA, Elias Yoshiaki. **Informação, Comunicação e a Sociedade do Conhecimento** disponível em < http://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/elias/>. 2001.

ANEXOS

ANEXO 1

Tabela 1: Funcionalidades do Endian UTM

Função	Características
Segurança de Rede	• *Firewall Stateful Packet* • Zona Desmilitarizada (DMZ) • Prevenção contra intrusos (Snort) • Vários IPs públicos • Várias Wan • Qualidade de Serviço e Gerenciamento de Banda • Suporte SNMP • VoIP support / SIP • SYN / ICMP proteção contra inundações • Suporte VLAN (IEEE 802.1Q trunking) • Proxy DNS / Routing • Rede de Monitoramento • Anti-spyware • Proteção contra phishing
Segurança Web	• HTTP e FTP proxies • Anti-vírus (100.000 + padrões) • Apoio Proxy Transparente • Análise de Conteúdo / Filtering • URL Blacklist • Autenticação: Local, RADIUS, LDAP, Active Directory • NTLM Single Sign-On • Grupo e usuário com base na web filtro de conteúdo

	• Políticas de acesso web do grupo e usuário com base • Controle de acesso com vários intervalos de tempo • Commtouch RPD (opcional) • Sophos Antivírus (opcional)
Segurança de e-mail	• SMTP e POP3 proxies • Anti-spam com Bayes, Padrão, e SPF • Heurística, apoio Branco-listas em preto-e • Anti-vírus (100.000 + padrões) • Apoio Proxy Transparente • Spam Auto-Learning • Transparente Redirecionamento (BCC) • Greylisting • Commtouch Antispam (opcional) • Sophos Antivírus (opcional)
Rede Privada Virtual IPsec	• Criptografia; 3DES, AES 128/256-bit, MD5, SHA1 • Diffie-Hellman (2, 5, 14, 15, 16,17,18) • Autenticação: Pre-Shared Key, chaves RSA • X.509-certificates IKEv1, L2TP DPD (Dead Peer Detection) • NAT-Taversal • Compressão • PFS (Perfect Forward Secrecy)

	• VPN Site / site • VPN Client / Site (guerreiro Road) • VPN Failover • Integrada Autoridade Certificadora **Verdadeira SSL / TLS VPN (OpenVPN)** • Criptografia; DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish • Autenticação: Pre-Shared Key, X.509-certificados, autoridade de certificação e local • Suporte para VPN através de HTTPS Proxy (OpenVPN) • PPTP • VPN client-to-Site (Road Wwarriors) • VPN Client para Microsoft Windows, Mac OS X e Linux • Logins multipe por usuário (opcional) • VPN Failover **Gerenciamento unificado VPN Usuário** • Os usuários podem ser criados com apenas alguns cliques, quer para OpenVPN, L2TP ou ambos.
	• Automatic WAN Failover Uplink • Monitoramento de WAN Uplinks • Tipos Uplink: Ethernet (Static /

WAN Failover	DHCP), PPPoE, ADSL, ISDN, PPTP SupportUMTS/GPRS/3G dongles USB
Autenticação de Usuário	• Diretório actice / NTLM • LDAP • RADIUS • Local
Hotspot	• Portal Captive • Apoio Wired / Wireless • Serviço RADIUS integrado • Logging Conexão • Por usuário e largura de banda global, limitando • Contas de usuário com base MAC-address • As contas de usuário de importação / exportação por CSV • Recuperação de usuário Senha • Configuração de rede do cliente automático (suporte para DHCP e IP estático) • Genérico JSON API para contabilidade externa e integração de terceiros • Instantâneo WLanTicket Shop (Endian SmartConnect) • Geração bilhete único clique (bilhete rápida) • Verificação de usuário E-mail para

	SmartConnect • Validação do usuário SMS e bilhética • Bilhetes Pre-/Post-paid e gratuitos • Bilhetes à base de tráfego • Validade do bilhete ajustável • MAC traking endereço para Hotspots gratuitos •
NAT	• Tráfego de entrada roteado • One-to-One NAT • Source NAT (SNAT) • IPsec NAT Traversal
Roteador	• Rotas estáticas • Roteamento baseado em Fonte • Roteamento baseado em Destino • Roteamento baseado em políticas (com base em interface, MAC, protocolo ou porta)
Bridging	• Firewall Stealth Mode • OSI camada 2 firewall de função • Spanning tree • Bridges ilimitadas • Interfaces ilimitadas por bridge

High Availability	• Hot Standby (ativo/passivo) • Sincronização de Dados / Configuração
Serviços Extra	• Notificação e manuseio de evento • NTP (Network Time Protocol) • Servidor DHCP • SNMP Servidor • DynDNS
Registros e relatórios	• Personalizável painel em tempo real • Vivo Log Viewer (baseado AJAX) • Detalhamento do Usuário Baseada Relatório Web Access (não em 4i, Mini) • Estatísticas Rede / Sistema / Desempenho • Configurações de log baseados em regras (regras de firewall) • Syslog: Local ou Remoto • OpenTSA timestamping confiável
Gerenciamento	• Fácil administração baseada na Web (SSL) • Remoto seguro SSH / SCP Acesso • Serial Console • Gerenciamento centralizado pelo Endian Network (SSL)
Atualizações e backup	• Atualizações centralizadas através da rede Endian • Agendada Backup automático

	• Os backups criptografados via e-mail • Instant Recovery / Backup para USB Stick (Endian Recuperação)

Fonte: http://www.endian.com/en/products/security-gateways-utm/features/#.UqkapvRDt8h

ANEXO 2 : Descrição OpenVPN

- OpenVPN é um VPN robusto e altamente flexível. OpenVPN suporta SSL / TLS segurança, ethernet bridge, TCP ou UDP transporte túnel através de proxys ou NAT, suporte para endereços IP dinâmicos e DHCP, escalabilidade para centenas ou milhares de usuários, e portabilidade para a maioria das principais plataformas de sistemas operacionais.
- OpenVPN está fortemente vinculado à biblioteca OpenSSL, e deriva muito de sua capacidade de criptografia a partir dele.
- OpenVPN suporta criptografia convencional, usando uma chave pré-compartilhada segredo (modo de chave estática) ou de segurança de chave pública (modo SSL / TLS) usando certificados de cliente e servidor. OpenVPN também suporta não-criptografados túneis TCP / UDP.
- OpenVPN é projetado para trabalhar com o TUN / TAP interface de rede virtual que existe na maioria das plataformas.
- No geral, OpenVPN tem como objetivo oferecer muitas das características-chave do IPSec, mas com uma pegada relativamente leve.

Disponível em <http://openvpn.net/index.php/manuals.html>