Instituto Superior de Tecnologias Avançadas

Projeto Global

Licenciatura em Informática

COMUNICAÇÕES SEGURAS

Realizado por: Ricardo Ascensão nº1764

Coordenador: Prof. Dr. Pedro Brandão

Orientador: Prof. Dr. Pedro Brandão

Ricardo Filipe Ascensão

Turma B 2013/2014

Lisboa,2013

Agradecimentos

Gostaria de agradecer a todos os que colaboraram de alguma forma na realização deste trabalho. Em especial, gostaria de agradecer aos meus colegas de turma pela ajuda que me deram a alcançar os objetivos propostos na realização deste trabalho.

Gostaria de agradecer também a minha namorada Alda Vaz, ao meu pai Luís Ascensão e ao meu primo Daniel Melo, pelo incentivo e ajuda na realização deste trabalho.

Resumo

Hoje em dia a utilização de VPNs tem-se tornado cada vez mais comum, pois a sua implementação e expansão é relativamente simples. A sua utilização possibilita por exemplo, a conexão de um utilizador à rede da sua empresa ou mesmo a ligação de várias filiais espalhadas por todo o mundo à sede, como se da mesma rede se tratasse. Esta tecnologia utiliza como suporte de interligação dos vários utilizadores a própria rede pública, bastando para tal alugar a um fornecedor de serviços de telecomunicações um acesso à Internet. Independentemente do tipo de acesso utilizado para obter ligação à Internet, a VPN é uma tecnologia segura que oferece privacidade aos seus utilizadores. Permite manter uma conexão bastante rápida, dependendo do tipo de acesso à Internet utilizado. Outra vantagem importante é a económica, quando comparada por exemplo com a utilização de circuitos dedicados. Neste trabalho serão demonstradas as vantagens de utilização de VPNs a nível de custos associados e segurança proporcionada pela sua utilização. O objetivo será a implementação de uma solução que irá permitir aos seus utilizadores estabelecerem ligações com a sede da empresa, utilizado VPNs com o intuito de garantir a segurança da mesma. O projeto abordará também três formas distintas dos utilizadores se ligarem remotamente à rede interna da empresa: A primeira utiliza dispositivos móveis com o sistema operativo Android e foi pensada para permitir que em qualquer momento o utilizador se possa ligar; A segunda forma utiliza dispositivos com o sistema operativo Windows e foi pensada para utilizadores que estejam fora da empresa – por exemplo em visita a um cliente – e necessitem aceder a informação da sede; A última forma utiliza um minicomputador com sistema operativo Linux e foi pensada para utilizadores que estejam em casa e necessitem se ligar à rede da sede, não necessitando de qualquer configuração do seu utilizador. Pela investigação efetuada a várias ofertas existentes no mercado, verificou-se que a solução apresentada é bastante versátil e abrangente, no que diz respeito às possíveis formas que os seus utilizadores poderão utilizar para se ligarem à rede da empresa, isto com baixo investimento em infraestruturas.

Palavras-Chave: VPN, Segurança, Internet, Conexão, Utilizadores, Linux.

Abstract

Nowadays the utilization of VPN has become more common, because its implementation and expansion is relatively simple. Its use enables for example, connecting a user to his company network or even connecting multiple branches spread all over the world to the headquarters, as if they were on the same network. This technology uses as support for interconnection of multiple users, the public network itself, by simply renting to a provider of telecommunications services an Internet access. Regardless the type of access used to get an Internet connection, the VPN is a safe technology that offers privacy to its users. It allows to maintaining a quick connection, depending of the type of Internet access used. Another important factor is the economic one, if compared for example with the use of dedicated circuits. In this study it will be demonstrated the benefits of using VPNs in terms of associated costs and the security provided by its use. The goal is to implement one solution that will enable their users to establish links with the company headquarters, using VPNs with the intent of ensuring safety. The project will also approach three distinct ways for the users to remotely connect to internal company network: The first one uses mobile devices with Android operating system and was thought out to allow at any time the user to connect to the company network; The second one uses devices with Windows operating system and has been thought for users who are outside the company – for example visiting a client – and needs to access information at headquarters; The last way uses a mini computer with Linux operating system and has been thought for users who are at home and need to connect to the headquarters' network, not requiring any configuration of its user. By the research performed from several offers on the market, it was verified that the presented solution is quite versatile and broadening, concerning the possible ways that the users may use to connect to the company's network, this with low investment in infrastructure.

Keywords: VPN, Security, Internet, Connection, Users, Linux.

Lista de abreviaturas

ACM - Association for Domputing Machinery

ADSL – Asymmetric Digital subscriber line

ARPA – Advanced Research Projects Agency

ARPANET - Advanced Research Projects Agency Network

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

IMP - Iinterface Message Processor

IP - Internet Protocol

IPSec - IP Security Protocol

LAN - Metropolitan Area Network

MAN – Metropolitan Area Network

MB – Mega Megabyte

Mhz – Mega Hertz

MPPE - Microsoft Point-to-Point Encryption

MTU -Maximum Transmission Unit

PPTP - Point-to-Point Tunneling Protocol

RAM - Random Access Memory

RFC - Request for Comments

SD - Secure Digital Card

SSL - Secure Socket Layer

VPNC - Virtual Private Network Consortium

VPNs - Virtual Private Nnetworks

WAN- Wide Area Network

Índice

Índice de figuras

Introdução

Atualmente as redes informáticas disponibilizam, para além da troca de informação, várias funcionalidades, levando a um crescente aumento do seu número de utilizadores, tanto a nível empresarial como particular.

Com o aumento de funcionalidades das redes informáticas, juntamente com as necessidades das empresas que possuem escritórios espalhados geograficamente por várias cidades ou mesmo países diferentes, verifica-se a existência de uma forte necessidade das empresas poderem trocar informação entre filiais ou parceiros de negócio e partilhar recursos de rede como impressoras, acesso a caixas de correio eletrónico, etc.

Na implementação destas funcionalidades nas redes informáticas, as empresas procuram um equilíbrio entre custos e segurança. O nível de custos deverá ser o mais baixo possível, e o nível de segurança deverá ser o mais alto possível, garantindo segurança na troca de informação mediante as necessidades e possibilidades das empresas.

Uma forma possível de implementação de várias funcionalidades, tendo em atenção otimização das duas questões referidas anteriormente, é a utilização de Rede Privada Virtual (VPNs - *Virtual Private Network*) VPNs. As VPNs têm a capacidade de interligar inúmeras redes privadas entre si ou utilizadores a uma determinada rede, com pouco investimento em infraestrutura, mesmo havendo necessidade de aumento do número de interligações por parte das empresas. Tal é conseguido utilizando como suporte de conexão à rede pública de comunicações – isto é, a Internet – quer seja um circuito dedicado[1], ADSL[2] ou qualquer outra tecnologia que permita ter acesso à Internet.

---

[1] Circuito dedicado – Circuito que é estabelecido fisicamente entre o emissor e o recetor, passando somente a informação do utilizador que o alugou ao operador de telecomunicações, não partilhando o mesmo com outros utilizadores (White, 2013).

[2] ADSL – asymmetric digital subscriber line – em português linha de assinante digital assimétrica – é uma das principais tecnologias utilizadas para fornecer serviços de comunicação de dados em alta velocidade, através de uma linha telefónica; é uma tecnologia assimétrica pois proporciona uma maior

De um modo geral a Internet não oferece segurança, pois qualquer utilizador tem acesso a ela, o que vulnerabiliza toda a informação que lá passa. No entanto, as VPNs têm características que permitem tornar a Internet segura.

Essencialmente as características de segurança e funcionamento das VPNs, baseiam-se na criação de um túnel virtual através da Internet, que irá ligar dois pontos por forma a estabelecer uma comunicação segura entre si. A segurança é garantida pois a informação que passa dentro deste túnel virtual é codificada ou seja, encriptada[3], impedindo que utilizadores não autorizados possam ter acesso a informação, permitindo deste modo comunicações privadas.

Com o presente trabalho pretende-se apresentar uma possível solução para atender às necessidades de utilizadores que necessitem de estabelecer comunicações de uma forma segura, com baixo investimento e de fácil utilização.

A solução consiste na implementação de VPNs, que utilizarão como suporte de configuração o sistema operativo Raspbian. Este, por sua vez, é baseado no sistema operativo Linux[4], que é de utilização livre, razão pela qual optou pelo seu uso. Este sistema operativo Raspbian será instalado num Raspberry Pi, que essencialmente é um minicomputador de baixo custo, razão da sua escolha.

A estrutura da solução utilizará o Raspberry Pi com função de servidor de VPNs, onde os utilizadores se ligam de forma segura. A sua localização será por exemplo na sede da empresa, para que o utilizador tenha acesso remoto a informação sigilosa, dispositivos de rede, caixas de correio eletrónico etc.

Para estabelecer a ligação com o servidor de VPNs, foram definidas três soluções possíveis. A primeira recorre a dispositivos que utilizem o sistema operativo

---

velocidade de transferência de informação para jusante (da Internet para o cliente) e menor velocidade para montante (do cliente para a Internet) (Tomsho, 2011).

[3] Criptografia – Palavra de origem Grega, significa escrita secreta. Usado o termo para se referir à ciência e à arte de transformar mensagens, para torná-las seguras e imune aos ataques. Criptografia significa que o remetente transforma a informação original numa outra forma e envia a mensagem resultante ao longo da rede. A descodificação inverte o processo para transformar mensagem de volta à sua forma original (Forouzan & Fegan, 2007).

[4] Linux – É um sistema operativo de livre utilização, desenvolvido pelo finlandês Linus Torvalds na universidade Helsinki, Finlândia, lançado a 5 de outubro de 1991.

Android[5]. A segunda a dispositivos que utilizem o sistema operativo Windows[6]. A terceira, utiliza um Raspberry Pi, onde será configurado o cliente VPN. Esta última, ao contrário das duas primeiras, não necessita de nenhuma configuração por parte do utilizador, pois só terá que ligar o seu computador ao Raspberry Pi que tem o cliente VPN instalado, e fornecer-lhe acesso à Internet. A ligação é estabelecida automaticamente entre o cliente VPN e o servidor de VPNs, estabelecendo o acesso remoto à rede da empresa.

A segurança na utilização das VPNs, será garantida pela implementação do protocolo de comunicação, protocolo de túnel tonto-a-ponto (PPTP - *point-to-point tunneling protocol*), em conjunto com o protocolo de encriptação, encriptação ponto-a-ponto microsoft (MPPE - *microsoft point-to-point encryption*). Os critérios utilizados na escolha destes dois protocolos foram a forma simples de configuração e o facto de serem protocolos específicos para ligações ponto-a-ponto.

O estudo realizado para chegar à solução apresentada neste projeto tem por base a pesquisa de possíveis alternativas para chegar ao objetivo final pretendido, sempre com o intuito de apresentar uma solução de baixo custo para pequenas empresas e fácil utilização.

O trabalho será estruturado com os seguintes capítulos, o *Estado da Arte* onde serão salientados temas atuais e significativos para o projeto desenvolvido, no seguinte capítulo *Contextualização* são demostradas solução de VPNs de vários fabricantes existentes no mercado, seguido do capítulo *Solução desenvolvida no âmbito do projeto* onde é demostrado a solução desenvolvida no projeto e as suas funcionalidades, por último o capítulo *Implementação da solução desenvolvida no âmbito do projeto* onde são demostrados todos os passos necessários para configurar o servidor de VPNs, o cliente VPN, VPN em Android e Windows.

---

[5] Android – Sistema operativo do Google baseado em Linux e utilizado em dispositivos móveis www.Android.com.

[6] Windows – Sistema operativo da Microsoft www.microsoft.com.

I. Estado da arte

Neste capítulo será abordado três temas principais, o primeiro será a Internet, seguido da tecnologia VPN e por último a segurança nas comunicações.

Relativamente ao tema Internet é descrita a sua definição, dando a conhecer como é constituída, descrevendo os tipos de redes privadas que a formam. É descrito e sua evolução desde o seu início em 1960 ate aos dias de hoje, referindo o seu surgimento devido á necessidade de interligação das várias organizações de pesquise pelo departamento de defesa Norte-americano, e como foi realizado a sua interligação.

É mostrado com a Internet revolucionou a vida diária dos seus utilizados, tanto a nível de lazer como profissional. Exemplo disso é o acesso a uma quantidade enorme de informação e funcionalidades possíveis de utilizar, como o pagamento de contas, envio de correio eletrónico, etc.

No tema VPN são descritas as razões que levaram as empresas a realizar o seu tráfego de dados através da Internet, como por exemplo a redução de custos, a diversidade de funcionalidades de rede passíveis de utilizar ou o elevado desempenho permitido na troca da informação. É mostrada a alternativa à utilização de VPNs, descrevendo as vantagens e desvantagem da sua utilização relativamente a circuitos dedicados, referindo-se questões como segurança e custos associados.

É descrito o funcionamento das VPNs, referindo como são estabelecidas as comunicações entre dois pontos e como é garantida a segurança nas comunicações. São também referidos três tipos de implementação de VPNs, nomeadamente VPNs aplicadas à intranet, à extranet e a acessos remotos.

No tema Segurança nas Comunicações são descritos os cinco serviços de segurança – autenticação, controle de acesso, confidencialidade, integridade e não-repúdio – que no seu conjunto garantem a segurança na transferência de dados através da Internet.

Nos últimos três séculos verificaram-se grandes evoluções tecnológicas, como referido por Tanenbaum e Wetherall "Cada um dos três seculos anteriores foi dominado por uma única tecnologia. O Século XVIII foi a época dos grandes sistemas mecânicos que acompanharam a Revolução Industrial. O Século XIX foi a era das máquinas a vapor. As principais conquistas tecnológicas do Século XX deram-se no

campo da aquisição, do processamento e da distribuição de informação" Tanenbaum & Wetherall, 2010,p.1.

Como referido por Torres "As redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante de si " Torres, 2001,p.5.

Com o crescimento das empresas e o aparecimento de filiais, surge a necessidade de interligação das suas redes com a rede da sede, para troca de informação entre si (White, 2013).

Como referido por Torres "Na Internet então, essa troca de informações armazenadas remotamente é levada ao extremo, acedemos a dados armazenados nos locais mais remotos e na maioria das vezes, o local onde os dados estão fisicamente armazenados não tem a menor importância" Torres, 2001,p.5.

1.1. Internet

A Internet pode ser descrita tal como feita por Forouzan e Fegan.

> Uma rede é um grupo de dispositivos de comunicação interligados, como computadores e impressoras. Uma internet (observe a letra minúscula i) é duas ou mais redes poderem comunicar entre si. A internet mais notável é chamada de Internet (letra I maiúscula), uma colaboração de mais de centenas de milhares de redes interligadas. Os particulares, bem como várias organizações, agências governamentais, escolas, centros de pesquisa, empresas e bibliotecas em mais de 100 países usar a Internet. Milhões de pessoas são utilizadores. No entanto, este sistema de comunicação extraordinário só passou a existir em 1969. (Forouzan & Fegan, 2007, p19).

Os estudos que levaram ao surgimento da Internet iniciaram-se na década de 1960, com a necessidade da agência de projetos de pesquisa avançada do departamento de defesa Norte-americano (ARPA – *advanced research projects agency*) em encontrar uma forma de ligar as suas organizações de pesquisa (Tanenbaum & Wetherall, 2010; Forouzan & Fegan, 2007). A ideia seria interligar os computadores das várias organizações que até então eram dispositivos independentes, pois eram incapazes de comunicarem entre si, permitindo assim a partilha de

informação e redução de custos e eliminado a duplicação de esforços (Forouzan & Fegan, 2007; Douglas, 2009).

Passados sete anos, em 1967, a associação de máquinas de computação (ACM - *association for computing machinery*) reuniu-se com a ARPA para apresentar a sua ideia de estabelecer a interligação das várias organizações de pesquisa, com a criação de uma rede computadores interligados denominada de ARPANET (*advanced research projects agency network*). A ideia seria que cada computador independentemente do fabricante fosse ligado a um computador central, chamado de interface processador de mensagens (IMP - *interface message processor*). Os IMPs, por sua vez, seriam ligados entre si através de linhas telefónicas. Estes teriam que conseguir comunicar com outros IMPs e com os computadores ligados a estes, estabelecendo assim a interligação das organizações (Forouzan & Fegan, 2007).

Em 1969, nasceu a primeira grande rede de comunicações, a ARPANET, nos Estado Unidos da América (Wong & Yeung, 2009). O responsável pelo seu desenvolvimento foi Lawrence Roberts com a cooperação de estudantes da Universidade de Snowbird, no Utah (Anttalainen, 2003; Wong & Yeung, 2009). Inicialmente, esta rede era constituída por quatro IMPs separados geograficamente. O primeiro localizado na Universidade da Califórnia em Los Angeles, o segundo localizado na Universidade da Califórnia em Santa Barbara, terceiro localizado no Instituto de Pesquisa de Stanford e o quarto localizado na Universidade de Utah (Forouzan & Fegan, 2007). Em Setembro de 1972, já interligava 34 locais, tal como se pode verificar na Figura 1 (Anttalainen, 2003; Wong & Yeung, 2009).

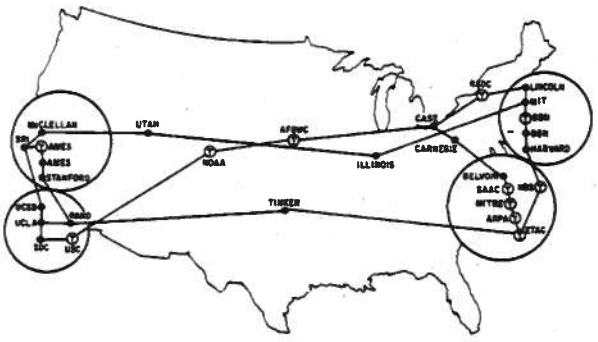

Figura 1 – ARPANET (Adaptado de Wong & Yeung, 2009)

Nos dias de hoje a Internet cresceu em larga escala, sendo composta por inúmeras redes, interligadas por dispositivos e estações de comutação de fornecedores de comunicações. É difícil fazer uma representação exata da Internet, pois esta está constantemente em mudança, com novas redes a serem criadas ou ampliadas e outras a serem extintas (Wong & Yeung, 2009).

Relativamente às redes de comunicações, essencialmente existem três tipos e distinguem-se entre si de acordo com o tamanho da área geográfica que ocupam. São elas a rede de área local (LAN - *local area network*), a rede de área metropolitana (MAN - *metropolitan area network*) e as redes de área alargada (WAN - *wide area network*) (Tanenbaum & Wetherall, 2010; Serpanos & Wolf, 2011).

As redes denominadas de locais são redes utilizadas para interligar utilizadores numa área geográfica relativamente pequena, que poderá ir desde a interligação de diferentes salas ou pisos no mesmo edifício, a uma área que poderá ir até pouco mais que uns quilómetros (Serpanos & Wolf, 2011; Tanenbaum & Wetherall, 2010).

As redes denominadas metropolitanas são, por sua vez, utilizadas para interligar utilizadores numa área geográfica maior do que as redes locais. Permitem a interligação de vários escritórios espalhados por uma cidade, podendo ser consideradas uma espécie de interligação de várias redes locais (Serpanos & Wolf, 2011; Tanenbaum & Wetherall, 2010).

As redes alargadas são redes geograficamente distribuídas, utilizadas para interligar utilizadores numa área geográfica maior do que as redes metropolitanas. Permitem a interligação de vários escritórios espalhados por um país ou continente, podendo-se considerar que são a interligação de várias redes locais e metropolitanas (Serpanos & Wolf, 2011; Tanenbaum & Wetherall, 2010).

Para os utilizadores finais terem acesso a Internet terão que alugar o serviço a um operador de comunicações. Havendo operadores de serviços internacionais, nacionais, regionais e por último locais, podendo afirmar-se que a Internet nos dias de hoje já não é gerida por governos, mas sim por empresas privadas (Forouzan & Fegan, 2007).

A Internet é um sistema de comunicação que permite aos seus utilizadores aceder a uma grande quantidade de informação. Este facto revolucionou em muitos aspetos a vida diária das pessoas, alterando a maneira como os seus utilizadores trabalham,

fazem negócios ou como despendem o seu tempo de lazer (Douglas, 2009; Forouzan & Fegan, 2007). Exemplo disso é a utilização de correio eletrónico na realização de um negócio, o pagamento de faturas como a eletricidade, efetuar uma reserva de um hotel, a comparação dos preços na compra de um carro, a visualização de um filme ou leitura de um jornal (Forouzan & Fegan, 2007).

Com o aparecimento da Internet e o aumento do seu número de utilizadores, levou ao desenvolvimento de aplicações que utilizam a Internet como suporte de partilha de recursos entre utilizadores, sendo uma das mais importantes as VPNs (Anttalainen, 2003).

1.2. VPN

Com o surgimento das VPNs muitas empresas optaram por passar a realizar o seu trafego de dados pela Internet, mas sem prescindirem da segurança das redes privadas (Douglas, 2009).

As VPNs são redes virtuais sobrepostas à Internet, mas que permitem aos seus utilizadores terem a mesma segurança oferecida pelas redes privadas e funcionalidades como trocar informação entre filiais ou parceiros de negócio, partilhar recursos de rede como impressoras, aceder a caixas de correio eletrónico, etc.. Esta tecnologia oferece às empresas a possibilidade de terem um melhor desempenho, permitindo uma maior rapidez e redução de custos na troca de informação entre departamentos ou filiais separadas geograficamente, bem como com parceiros de negócio (Tanenbaum & Wetherall, 2010; Douglas, 2009).

Como alternativa às VPNs existe a possibilidade de aluguer de circuitos dedicados, com um E1[7] ou E3[8], mas os seus custos são elevados se tivermos em conta o dinheiro que os operadores de comunicações cobram pelo seu aluguer, comparativamente a uma ligação à Internet (Scott, Wolfe, & Erwin, 1999; Tanenbaum & Wetherall).

A vantagem na utilização dos circuitos dedicados que formam as redes privadas é a questão da forte segurança que oferece aos seus utilizadores, pois o meio

[7] Linha E1 – Circuito dedicado com uma largura de banda de 2048Mbps (Douglas, 2009).

[8] Linha E3 – Circuito dedicado com uma largura de banda de 34,368Mbps (Douglas, 2009).

físico não é partilhado com outros utilizadores ao contrário de um acesso à Internet que suporta as VPNs (Scott, Wolfe, & Erwin, 1999). Se um intruso tentar aceder a informação que passa no circuito dedicado terá que aceder fisicamente ao mesmo (Tanenbaum & Wetherall, 2010).

A tecnologia VPN foi desenvolvida tendo como objetivo garantir segurança e redução de custos na interligação de dois pontos que se encontram separados geograficamente (Douglas, 2009). Combina o melhor das duas formas possíveis de troca de informação (Douglas, 2009; White, 2013), pois utiliza como suporte a Internet, que é comparativamente mais barata em relação ao aluguer de circuitos dedicados, e com a aplicação de serviços de segurança garante a troca de informação de forma segura, como se um circuito dedicado se tratasse, não permitindo o acesso a mesma por entidades não autorizadas (Douglas, 2009; Davies & Lewis, 2004; White, 2013).

Na figura dois são mostradas as duas formas de troca de informação referidas anteriormente, circuitos dedicados e VPNs.

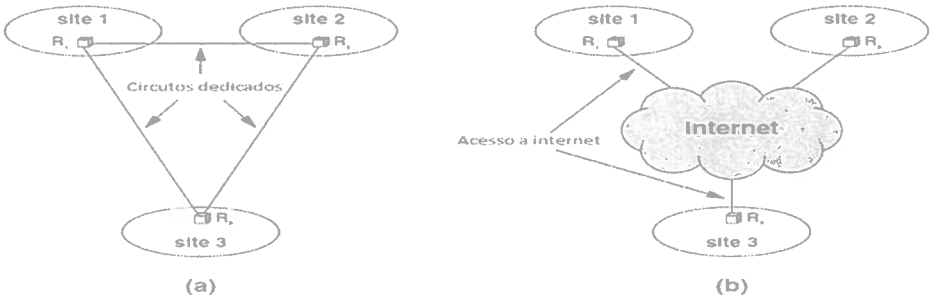

Figura 2 - Circuitos dedicados (a), e acesso a internet (b) (Adaptado de Douglas, 2009)

As VPNs tornam um computador remoto parte de uma rede privada, ou a união de várias redes fisicamente distintas numa só rede, como se da mesma rede se tratasse (Douglas, 2009; Davies & Lewis, 2004).

Tipicamente existem vários tipos de implementação de VPNs, distinguindo-se entre si em função da utilização e necessidades dos seus utilizadores. Neste contexto, destacam-se três variantes – VPNs aplicadas à intranet, VPNs aplicadas à extranet e VPNs aplicadas a acessos remotos (Davies & Lewis, 2004).

A primeira variante, VPNs aplicadas à intranet é aplicada aquando da interligação de utilizadores que se encontram dentro da mesma rede. Esta interligação poderá ser por exemplo com outros departamentos ou filiais da mesma impressa, facilitando assim a gestão de permissões de acesso dos vários utilizadores na rede (Davies & Lewis, 2004).

A segunda variante, que diz respeito a VPNs aplicadas à extranet, é por sua vez usada no acesso à rede interna da empresa por clientes, parceiros de negócios, fornecedores, etc, fomentando a interação entre estes intervenientes e tendo como objetivo facilitar a troca de informação (Davies & Lewis, 2004).

Por fim, a terceira variante, as VPNs aplicadas a acessos remotos, que são usadas por utilizadores móveis quando se ligam à rede da empresa a partir de vários locais geograficamente distintos, como por exemplo casa, hotéis, etc., bastando para tal ter acesso à Internet, a partir de um qualquer fornecedor de comunicações (Davies & Lewis, 2004).

Essencialmente quando uma VPN é estabelecida entre dois pontos, é criado um circuito virtual encriptado, através da Internet por forma a estabelecer comunicação entre eles, unindo desta forma os dois pontos na mesma rede (Davies & Lewis, 2004; Tanenbaum & Wetherall, 2010). O túnel virtual criado pelas VPN é uma forma de representação do caminho que os dados encriptados fazem entre dois pontos, utilizando uma infraestrutura de suporte intermédia não segura (Tanenbaum & Wetherall, 2010), tal como ilustrado na figura três.

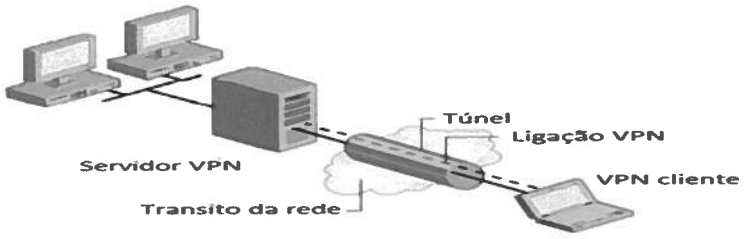

Figura 3 - Ligação VPN, (Adaptado de Davies & Lewis, 2004)

A informação ao ser enviada de forma encriptada sugere a ideia da existência de um túnel, em que só quem tenha acesso ao túnel terá também acesso à informação que passa no seu interior (White, 2013; Davies & Lewis, 2004; Ross, 2009).

1.3. Segurança nas comunicações

A utilização da Internet não é uma forma segura para tráfego de dados pois o meio físico é partilhado por inúmeros utilizadores passíveis de aceder à informação, colocando em risco a sua segurança (White, 2013).

A segurança pode ser descrita tal como feita por Stallings.

> X.800 define um serviço de segurança como um serviço prestado que garante adequada segurança dos sistemas ou de transferências de dados. Talvez uma definição mais clara é encontrada na RFC 2828, que fornece a seguinte definição: É um serviço de processamento ou de comunicação que é fornecido por um sistema para dar um tipo específico de proteção aos recursos do sistema; Serviços de segurança implementam políticas de segurança e são implementadas por meio de mecanismos de segurança (Stallings, 2005, p16).

Por forma a garantir uma bom nível de segurança nas comunicações, realizadas através da Internet com o uso de VPNs, são tidos em consideração cinco serviços de segurança. Estes são autenticação, controle de acesso, confidencialidade, integridade e não-repúdio (Stallings, 2005; Wong & Yeung, 2009).

No que diz respeito ao serviço de autenticação, este garante que a comunicação é autêntica e quando é recebida uma mensagem, a sua função é assegurar ao recetor que quem enviou a mensagem é quem afirma ser (Stallings, 2005). O controlo de acesso efetua a prevenção e limitação de acesso a recursos não autorizados, como acesso a rede privada ou aplicações. Este serviço controla quem pode ter acesso a determinado recurso, em que condições o acesso pode ocorrer e o que é permitido fazer ao utilizador que esteja a aceder ao recurso (Stallings, 2005). Quanto a confidencialidade, esta efetua a proteção do conteúdo de dados transmitidos entre dois utilizadores, restringindo o acesso à informação e garantindo que só utilizadores autorizados conseguem visualizar a informação (Stallings, 2007). A integridade garante que os dados recebidos são exatamente os dados enviados por uma entidade autorizada, ou seja, não contêm nenhuma modificação, inserção, exclusão ou repetição (Stallings, 2007). Por fim, o não-repúdio impede o emissor ou o recetor de negar uma mensagem transmitida. Quando uma mensagem é enviada, o recetor pode provar que o suposto remetente de fato enviou a mensagem, da mesma

forma quando uma mensagem é recebida, o remetente pode provar que o alegado recetor efetivamente recebeu a mensagem (Stallings, 2007).

1.4. Conclusão

Atualmente a Internet é constituída pela união de inúmeras redes privadas. Para um utilizador poder ter acesso a Internet e a todas as suas capacidades, basta que alugue a um operador de comunicações um acesso.

A Internet é um sistema de comunicações que revolucionou em muitos aspetos a vida diária dos seus utilizadores, alterando a sua forma de trabalhar, fazer negócios ou mesmo como despendem o seu tempo de lazer. Possibilitam o acesso a uma grande quantidade de informação e comodidades, tais como a utilização de correio eletrónico na realização de um negócio, o pagamento de faturas como a eletricidade, realização de uma reserva de um hotel, a comparação dos preços na compra de um carro, a visualização de um filme ou leitura de um jornal.

Com o aumento de utilizadores da Internet, houve também um aumento de aplicações a serem desenvolvidas para partilha de recursos entre utilizadores, sendo um exemplo disto as VPNs. O fato das VPNs possibilitarem a mesma segurança e funcionalidades oferecidas nas redes privadas, levou a um incremento do número de empreses que adotaram esta tecnologia, que lhes possibilita terem um melhor desempenho, uma maior rapidez e uma redução de custos na troca de informação entre departamentos ou filiais separadas geograficamente, bem como com parceiros de negócio.

Como alternativa às VPNs, existe a possibilidade de utilizar circuitos dedicados, que permitem uma forte proteção aos seus utilizadores na troca informação, pois o meio físico não é partilhado com outros utilizadores, ao contrário do que acontece com as VPNs. A sua desvantagem relativamente as VPNs são os seus custos associados, que são comparativamente elevados.

Por outro lado as VPNs foram desenvolvidas tendo como objetivo a redução de custo e a garantia de segurança aos seus utilizadores na troca de informação em infraestruturas de suporte intermédias partilhadas por outros utilizadores, tradicionalmente não seguras. Segundo Douglas e White as VPNs combinam o

melhor das duas formas possíveis de troca de informação, pois utilizam como suporte a Internet que é – comparativamente à utilização de circuitos dedicados – mais barata, e com a aplicação de serviços de segurança garante a troca de informação de forma segura entre os seus utilizadores, como se um circuito dedicado se tratasse. As VPNs tornam um computador remoto parte de uma rede privada, ou a união de várias redes distintas numa só rede, possibilitando vários tipos de implementação de VPNs mediante as necessidades dos seus utilizadores.

II. Contextualização

Nos dias de hoje existem no mercado inúmeras soluções de VPNs à disposição, cada uma com diferentes funcionalidades, mediante as necessidades dos seus utilizadores.

Relativamente aos fabricantes de soluções de VPNs tais como D-Link, Juniter, Citrix, Cisco, Fortinet e Check Point, estes apostam cada vez mais nesta tecnologia, garantindo segurança aos seus clientes na sua utilização.

Devido ao grande potencial da tecnologia VPN, em 1999, foi fundado o consórcio de rede privada virtual (VPNC - *virtual private network consortium*) é a associação de comércio internacional para os fabricantes no mercado de VPNs. Os seus principais objetivos são a promoção dos produtos dos seus membros para a imprensa e para os potenciais clientes, o aumento da interoperabilidade entre os seus membros para ajudá-los a servir melhor os potenciais clientes, e servir como fórum para os fabricantes de VPNs em todo o mundo e ajuda a imprensa e potenciais clientes a compreender a tecnologias VPN e as sua normas[9].

2.1. Diferentes fabricantes de VPNs existentes no mercado

A diversidade de oferta de fabricantes que será apresentada de seguida mostra algumas soluções existentes no mercado, sendo a razão da sua escolha o facto de serem utilizadas pela empresa onde trabalha o autor deste documento.

2.1.1. Solução do fabricante D-Link

A D-Link é um fornecedor de dispositivos de segurança informática, como tal lançou o programa VPN Client Software para complementar a nível de segurança e funções a sua solução de Firewall NetDefend. A sua solução VPN Client Software é uma forma fácil, segura e económica de utilizar o protocolo de segurança cliente IP [10]

[9] Extraído de http://www.vpnc.org/

[10] Protocolo de internet (IP - Internet Protocol) é a forma de identificar um dispositivo como por exemplo um computador ou uma impressora, numa rede privada ou Internet. Todos os dispositivos

Sec[11], para estabelecer comunicações encriptadas entre o utilizador remoto e sede da empresa. Para a sua utilização basta o utilizador ter o programa VPN Client Software instalado no seu computador, por forma a poder estabelecer uma ligação VPN cliente com a *gateways*[12] IPSec da D-Link localizado na sede da empresa, sendo este uma solução *firewall*[13] NetDefend da D-Link.

Adicionalmente a solução VPN Client Software da D-Link é certificada pela VPNC por forma a garantir que a compatibilidade com equipamentos firewall de outros fabricantes (D-Link, 2013).

2.1.2. Solução do fabricante Citrix

A solução apresentada pela Citrix como nome NetScaler Gateway é uma solução de segurança com a função de estabelecer ligações seguras. Permite aos seus administradores controlar minuciosamente os dados na rede, enquanto permite aos utilizadores estabelecerem acessos remotos à rede privada de qualquer lugar.

A Citrix disponibiliza aos administradores da rede a aplicação SmartAccess, que lhes permite a gestão e controlo dos acessos remotos à rede e limitação de funcionalidades baseadas na identificação do utilizador e no seu equipamento terminal. Proporcionam assim uma melhor segurança e proteção dos dados como exemplificado no seguinte cenário: Um utilizador poderá ter acesso completo, isto é, permissão de leitura, de guardar localmente, de efetuar alterações num conjunto de

---

ligados à Internet possuem um IP único, que é utilizado pelos mesmos para serem identificados e poderem comunicar na Internet (Douglas, 2009).

[11] IPSec ou Segurança IP – É um conjunto de protocolos de segurança projetados pelo grupo de trabalho de engenharia de Internet (IETF - Internet Engineering Task Force) para garantir segurança na troca de informação encriptando-a, permitindo autenticação e confidencialidade (Forouzan & Fegan, 2007).

[12] Ponto de Ligação (Gateway) – Dispositivo com a funcionalidade de interligar redes incompatíveis, efetuado a tradução da informação dos diferentes protocolos de comunicação (Dean, 2010).

[13] Parede de Fogo (Firewall) – É um dispositivo de segurança utilizado para proteger os computadores de uma empresa e a sua rede contra ataques vindo da Internet. A Parede de Fogo localiza-se sempre entre a rede do utilizador e o acesso à Internet, obrigando que toda a informação que entre ou saia da rede do cliente passa pela Parede de Fogo (Dean, 2010).

arquivos quando está a utilizar o seu próprio computador de trabalho, mas, por outro lado, se o acesso ao mesmo conjunto de arquivos for realizado a partir de um dispositivo desconhecido ou de um dispositivo móvel, então o utilizador ficará restrito somente à leitura dos mesmos arquivos.

A solução NetScaler Gateway permite um grande desempenho e escalabilidade, pois possibilita ter até 10.000 acessos remotos estabelecidos em simultâneo na mesma NetScaler Gateway. A este nível, a Citrix disponibiliza equipamentos físicos e virtuais que permitem aos administradores a máxima flexibilidade na escolha das opções de implantação dos acessos remotos, de modo a que possam optar pelos que melhor cumpram os requisitos da empresa para um acesso seguro. A Citrix disponibiliza três versões diferentes para os seus clientes mediante as suas necessidades: A primeira versão é a Standard, aconselhada para clientes que necessitem até 500 utilizadores remotos ligados simultaneamente; A segunda versão é a Advanced, aconselhada para clientes que necessitem até 500 utilizadores remotos ligados simultaneamente, mas já inclui a aplicação SmartAccess[14] e o suporte para dispositivos móveis; Por último a versão Advanced, aconselhada para clientes que necessitem de mais que 500 utilizadores remotos ligados simultaneamente e que inclui a aplicação SmartAccess, suporte para dispositivos móveis e recuperação automática de falhas (Citrix, 2013).

2.1.3. Solução do fabricante Fortinet

A solução disponibilizada pela Fortinet, denominada FortiGate, permite às empresas estabelecer comunicações seguras e privacidade de dados, entre redes privadas e entre dispositivos, com a utilização dos protocolos de VPN IPSec e SSL.[15]

---

[14] Permite aos administradores de rede o controle de acesso, definindo políticas de segurança com base na identidade do usuário, localização e configuração do dispositivo terminal (Citrix, 2013).

[15] Protocolo de camada de sockets segura (SSL - Secure Socket Layer) – Tecnologia originalmente desenvolvido pela Netscape Communications, que usa criptografia para fornecer autenticidade e confidencialidade. Usada em ligações na Internet para fornecer segurança aos seus utilizadores na troca de informação entre emissor e recetor (Stallings, Cryptography and Network Security Principles and Practices, 2005).

A plataforma FortiGate é totalmente integrada com outros recursos de segurança como antivírus, prevenção de intrusão, filtros de correio eletrónico e Web, que podem ser aplicados a todos os dados que passam no túnel VPN.

A sua implementação é simples e flexível, utiliza os protocolos IPSec ou SSL nos acessos remotos criados na solução FortiGate, tornando as comunicações encriptadas entre o utilizador remoto e a rede privada, podendo os dois protocolos ser utlizados simultaneamente na mesma solução FortiGate.

As soluções VPN FortiGate são dimensionadas para satisfazer os requisitos de desempenho dos seus clientes independentemente do seu tamanho, que poderá ir desde uma ligação a um escritório, filiais, grandes empresas até mesmo operadores de comunicações.

A gestão da solução é centralizada no programa FortiManager, onde é fornecido ao cliente a capacidade de gestão e implementação das VPNs, podendo mesmo gerir milhares de soluções FortiGate a partir de um único FortiManager (Fortinet, 2013).

2.1.4. Solução do fabricante Check Point IPSec VPN Software Blade

A solução da Check Point, VPN IPSec Software Blade proporciona uma conectividade segura às redes empresariais para utilizadores remotos, móveis, filiais e parceiros de negócios. O programa Blade integra controle de acesso, autenticação e encriptação para garantir a segurança nas ligações à rede através da Internet.

A solução possui uma gestão centralizada dos acessos VPN, remotos e ponto-a-ponto. A segurança IPSec das VPNs é reforçada contra ataques permitindo que as políticas de segurança sejam aplicadas com diferentes graus, com base no nível de encriptação aplicado.

É uma solução flexível pois permite a criação de VPNs mediante as necessidades específicas do seu utilizador, permitindo vários modos de acessos remotos, oferecendo um conjunto abrangente de opções de configuração do cliente VPN, tal com descrito na figura quatro.

Característica	Detalhe
Métodos de autenticação	Palavra-chave, RADIUS, TACACS, X.509, SecurID
Certificado de autorização	Certificado de autorização integrado X.509
Comunidades VPN	Configura automaticamente ligações *site* a *site* à medida que os objectos são criados
Suporte à topologia	Estrela e *mesh*
VPN baseada em *routing*	Utiliza túneis de interfaces virtuais
Injecção de rotas na VPN	Mecanismo de injecção de rotas (RIM)
Modos de VPN *site* a *site*	Baseados em domínios, baseados em rotas
VPN direccional	Execução entre e dentro do comunidade
Troca de chaves IKE (Fase 1)	AES-256, 3DES, DES, CAST
Integridade de dados IKE (Fase 1)	MD5, SHA1
Encriptação de dados IPSec (Fase 2)	3DES, AES-128, AES-256, DES, CAST, DES-40CP, CAST-40, NULL
Integridade de dados IPSec (Fase 2)	MD5, SHA1
Grupos *Diffie-Hellman* IKE (Fase 1) e IPSec (Fase 2)	Grupo 1 (768 *bit*), Grupo 2 (1024 *bit*), Grupo 5 (1536 *bit*), Grupo 14 (2048 *bit*)
Opções IKE (Fase 1)	*Aggressive Mode*
Opções IPSec (Fase 2)	*Perfect Forward Secrecy*, compressão IP
Suporte a dispositivos móveis	Suporte de L2TP no iPhone, *SecureClient Mobile* para o *Windows Mobile*
Clientes de VPN IPSec variados	*Check Point Endpoint Security, SecureClient, SecuRemote*

Figura 4 - Configuração do cliente VPN

(Adaptado de www.checkpoint.com/products/ipsec-vpn-software-blade/index.html)

Esta solução simplifica a criação e gestão de VPNs complexas. O SmartDashboard[16] permite aos administradores definir Gateways participantes e a sua configuração em minutos independente da topologia da rede.

A nível de segurança IPSec é bastante avançada, permitindo que utilizadores locais, remotos e parceiros de negócios estabeleçam ligações seguras, onde as políticas de segurança podem ser aplicadas a todo o tráfego encriptado ou a parte do tráfego.

Sendo que cada empresa possui necessidades específicas de acessos remotos, a solução disponibiliza um vasto conjunto de escolhas de clientes VPN, que permitem projetar uma solução que satisfaça as suas necessidades específicas.

Fornece diferentes modos de abordar os problemas de conectividade enfrentados pelos utilizadores remotos: O primeiro modo, denominado Escritório, permite aos utilizadores parecer que estão "no escritório" ao se conectarem remotamente; O

[16] SmartDashboard é um programa de interface de gestão de políticas de segurança da marca Check Point - http://www.checkpoint.com/products/smartcenter/smartcenter_management.html

segundo modo, denominado Visitante, permite aos funcionários enquanto trabalham numa localização remota e onde o acesso à Internet possa ser restritivo na sua utilização, como por exemplo num hotel ou num cliente, acederem a recursos na empresa ou acederem a totalmente à Internet através da empresa. Por último, o modo Hub permite uma rigorosa inspeção centralizada de todo o tráfego de cliente, o que elimina a necessidade de implementar funções de segurança nos vários escritórios, fornecendo aos funcionários comunicações seguras cliente para cliente (Checkpoint, 2013).

III. Solução desenvolvida no âmbito do projeto

Neste capítulo será demonstrado o objetivo e funcionalidades da solução desenvolvida no projeto. O objetivo do projeto é demonstrar uma possível solução de baixo custo para pequenas empresas que pretendam possuir uma forma segura dos funcionários e colaboradores se ligarem remotamente à rede da empresa, para que possam aceder aos recursos disponíveis e à informação armazenada.

O projeto consiste na configuração e implementação de ligações entre o utilizador e o servidor de VPNs localizado na empresa, utilizado VPNs para garantir a segurança das comunicações.

Como se pode visualizar na figura cinco, onde é mostrado o diagrama da solução, verifica-se que a solução permite efetuar três formas destintas de ligação ao servidor de VPNs.

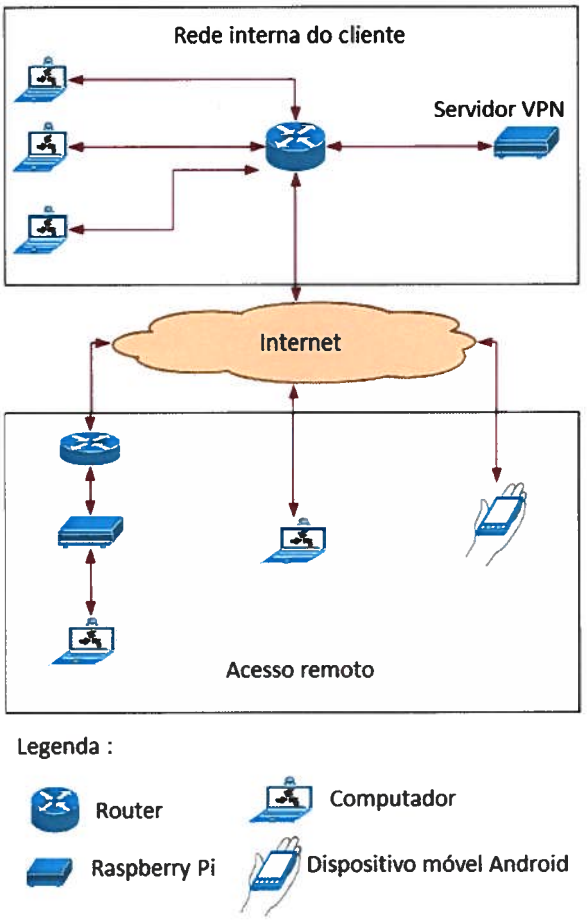

Figura 5 - Diagrama da solução

3.1. Solução

O ponto central da solução será o servidor de VPNs, pois será onde todas as ligações entre os utilizadores e a sede da empresa são estabelecidas. A sua localização será na sede da empresa, ligado ao router do cliente para permitir a ligação à Internet.

Para implementar o servidor de VPNs foi utilizado um Raspberry Pi (será feita a sua apresentação mais abaixo) cuja configuração foi realizada de forma a garantir que só utilizadores com permissão conseguem estabelecer uma ligação a este. As permissões foram garantidas previamente, com a atribuição de um nome de utilizador e palavra passe a cada utilizador.

A segurança nas comunicações é garantida com a utilização do protocolo MPPE sobre PPTP. O protocolo PPTP estabelece a ligação ponto-a-ponto entre o servidor de VPNs e o utilizador e o protocolo MPPE é um protocolo concebido para encriptar informação em ligações ponto-a-ponto normas RFC3078 e RFC3079.

A escolha das três formas de ligação ao servidor de VPNs tem o objetivo de dar aos utilizadores diferentes possibilidades de se ligarem remotamente à sede da empresa. A primeira forma demonstrada baseia-se no uso de dispositivos que utilizem o sistema operativo Android, com o intuito de estabelecer uma ligação que será suportada por uma rede móvel. A segunda forma demonstrada basear-se-á no uso de computadores que utilizem o sistema operativo Windows, com o intuito de permitir uma ligação suportada na rede fixa. Na última forma demonstrada, o cliente VPN é uma solução que tal como o servidor de VPNs foi implantado num Raspberry Pi. Mas esta solução não necessita de qualquer configuração por parte do utilizador, bastando que o mesmo ligue o seu computador ao cliente VPN e que este lhe forneça acesso à Internet. A VPN é estabelecida automaticamente entre o servidor de VPNs e o cliente VPN, pois este último foi configurado previamente com as permissões de acesso do utilizador em questão.

3.2. Minicomputador Raspberry Pi

Um ponto importante na implementação do projeto é o Raspberry Pi, pois a solução é suportada em grande parte por este equipamento, razão pela qual será feito uma breve apresentação das suas características e capacidades.

O minicomputador utilizado no projeto é o Raspberry Pi modelo B, pois é o mais comum e de fácil aquisição, tendo sido desenvolvido em Inglaterra pela fundação Raspberry Pi e colocado à venda ao público em fevereiro de 2012.

É um computador de pequenas dimensões quando comparado com os computadores de secretaria, tendo o tamanho de 85,60 mm × 53,98 mm. Possui vários interfaces de ligação, tal como se pode ver na figura sete, onde são mostrados quais e a sua localização.

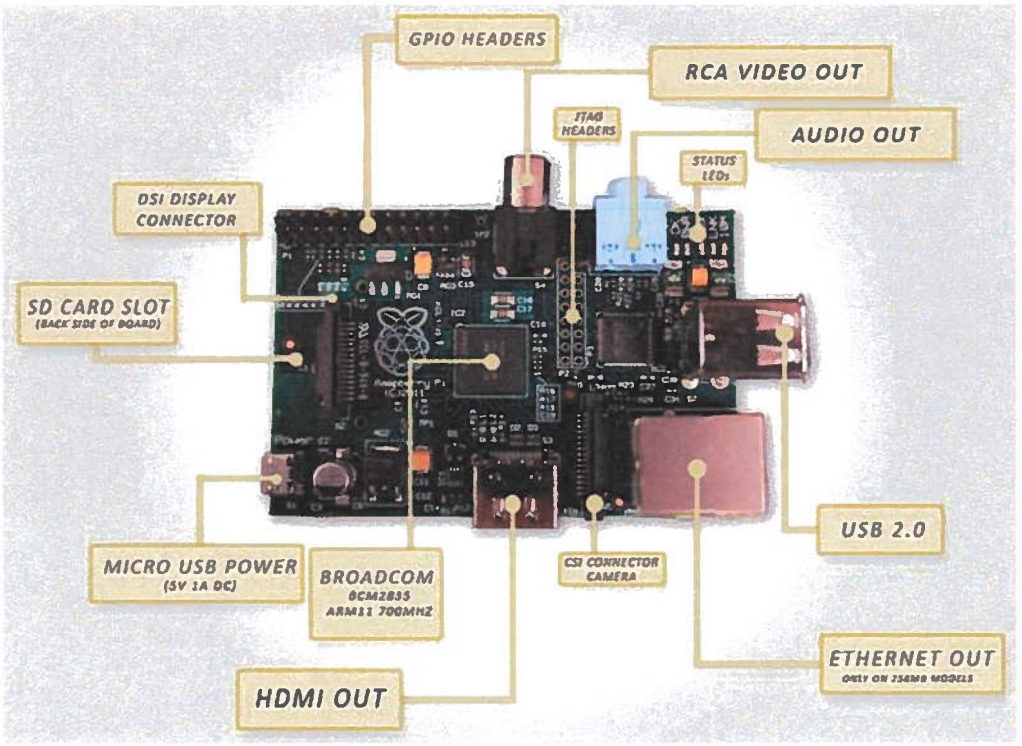

Figura 6 - Raspberry Pi (Adaptado de Schmidt, 2012)

O Raspberry Pi modelo B possui um processador[17] de 32 bits ARM1176JZF-s de 700Mhz, 512 Mb de memória RAM[18], utiliza um cartão SD como disco rígido[19], o processador gráfico[20] está integrado e dispõe de 256 Mb de memória, e é alimentado por 5 volts (Schmidt, 2012; Horan, 2013).

O sistema operativo utilizado é o Raspbian, que é uma otimização da distribuição Debian de Linux para o Raspberry Pi. Este é um sistema operativo de livre utilização e que dispõe de um repositório com mais de 35.000 aplicações de fácil instalação no Raspberry Pi.

---

[17] Processador - É o cérebro do computador e o responsável por todo o processamento. Também conhecido por CPU – central processing unit em português unidade central de processamento (Torres, 2001).

[18] Memória de acesso aleatório (RAM - *random access aemory*) - É a memória pelo processador para inicializar os programas. Sendo que o conteúdo da memória RAM é apagado cada vez que desligamos o computador, os programas e a informação são armazenados num sistema de memória secundário como por exemplo num disco rígido (Torres, 2001).

[19] Disco Rígido - É onde os programas e arquivos são armazenados. Ao executar um programa ou carregar arquivo, os mesmos são transferidos para a memória RAM para serem carregados pelo processador (Torres, 2001).

[20] Processador gráfico - É o processador responsável por converter sinais gerados pelo computador em sinais compreendidos pelo monitor de vídeo (Torres, 2001).

IV. Implementação da solução desenvolvida no âmbito do projeto

Neste capítulo serão demonstrados todos os passos necessários para a configuração do servidor de VPNs e das três formas de acesso VPNs abordadas anteriormente.

No caso do servidor de VPNs e cliente VPN a configuração é mostrada por linhas de comandos, ao passo que nas formas de acesso VPN de dispositivos Android e Windows a configuração será demonstrada por meio de imagens e legendas.

4.1. Configuração do servidor de VPNs

O sistema operativo utilizado e previamente instalado é o Raspbian. Por forma a manter este sistema operativo e restantes aplicações atualizadas, é recomendado começar por efetuar uma atualização. Para o efeito, basta executar os seguintes comandos:

```
$sudo apt-get update
$sudo apt-get upgrade
```

Para editar os ficheiros de configuração será necessário recorrer a um editor de texto. Neste trabalho será usado o Nano, no entanto poderá ser usado qualquer outro editor (ex: Vi). A instalação do Nano é feita através da seguinte instrução:

```
$sudo apt-get install nano
```

Para configurar a rede do servidor de VPNs, é preciso editar o ficheiro "/etc/network/interfaces":

```
$sudo nano /etc/network/interfaces
```

Este ficheiro permite efetuar a configuração da rede do servidor. O conteúdo deste ficheiro, no que diz respeito à configuração do interface "eth0", deve ser alterado para:

```
iface eth0 inet static
address 192.168.1.200
netmask 255.255.255.0
gateway 192.168.1.1
```

.

De maneira a suportar MPPE no servidor de VPNs, o modulo "ppp-compress-18", tem de ser carregado:

```
$sudo modprobe ppp-compress-18
```

O serviço responsável por o funcionamento da VPN PPTP, é o pptpd, que deve ser instalado da seguinte forma:

```
$sudo apt-get install pptpd
```

Depois de instalado, é necessário efetuar a sua configuração, editando o ficheiro "pptpd.conf", onde deve ser configurando o IP local e os IPs que serão atribuídos aos clientes VPN:

```
$ sudo nano /etc/pptpd.conf

localip 192.168.0.1
remoteip 192.168.1.234-238
```

O IP local será o 192.168.0.1, e os IPs atribuídos aos clientes poderão ser desde o 192.168.1.234 até ao 192.168.1.238. É ainda necessário configurar o endereço do servidor DNS.

O sistema de nomes de domínios (DNS - Domain Name Service) efetua a conversão de endereços de computadores (IPs) em nomes simbólicos legíveis por humanos Computer Networks and Internets - 5th Edition.

Estas configurações devem ser feitas no ficheiro "pptpd-options":

$sudo nano /etc/ppp/pptpd-options

ms-dns 192.168.1.1
nobsdcomp
noipx
mtu 1490
mru 1490

No passo seguinte será editado o ficheiro "chap-secrets", para configurar credenciais de acesso á VPN. Só os utilizadores presentes neste ficheiro é que terão acesso á VPN, para além do nome de utilizador têm de ser introduzidas as respetivas palavra-passe:

$ sudo nano /etc/ppp/chap-secrets

A configuração é efetuada da seguinte forma:

$username[TAB]*[TAB]password[TAB]*
$client<tab>server<tab>secret<tab>IPaddresses
$ricardo * raspberry *

O utilizador (cliente) "ricardo" pode ligar-se a qualquer "*" servidor, com a palavra-passe "raspberry" a partir de qualquer "*" IP.

Depois de efetuada esta configuração, é preciso reinicializar o serviço pptpd para que este assuma as alterações, com o seguinte comando:

$sudo service pptpd restart

Para poder ter acesso a rede interna da empresa, é preciso ativar o reencaminhamento IP, editando o ficheiro "sysctl.conf":

$sudo nano /etc/sysctl.conf

Procurar a linha #net.ipv4.ip_forward=1, retirar o cardinal (#) que serve para comentar a instrução.

Para aplicar as alterações deve ser executado o seguinte comando:

$sudo sysctl -p

Para finalizar e de maneira a garantir que todas as alterações são assumidas, é recomendado reinicializar o servidor com o seguinte comando:

$sudo reboot

De maneira a garantir o acesso á VPN a partir da Internet, é necessário reencaminhar a porta TCP 1723 do router para o Raspberry Pi. Esta porta servirá para inicializar e gerir o túnel virtual da VPN.

Se o acesso em questão tiver IP dinâmico, atribuído por o operador de comunicações via DHCP[21], devera criar um domínio que estará sempre atualizado com o IP atual do acesso. Existem diversos serviços gratuitos que conseguem garantir esta atualização, normalmente são designados por "dynDNS" ou Dynamic DNS que provem do inglês Dynamic Domain Name Server, ou seja Servidor de domínios de nome dinâmico.

[21] Protocolo de configuração dinâmica de hospedeiro (DHCP Dynamic Host Configuration Protocol), permite atribuir dinamicamente a um dispositivo de rede um endereço IP ou DNS, a partir de um do servidor de DHCP (Douglas, 2009).

4.2. Configuração do cliente VPN utilizando um Raspberry Pi.

O objetivo da solução cliente VPN é permitir que um ou mais dispositivos possam aceder á VPN sem configurações no próprio dispositivo. O Raspberry Pi deverá ter dois interfaces de rede, um será o responsável por estabelecer a ligação com o servidor de VPNs e o segundo interface disponibilizar a VPN ao cliente.

É recomendado começar-se por atualizar o sistema operativo, do Raspberry Pi que será utilizado como cliente VPN da mesma forma que foi feito para o servidor:

$sudo apt-get update
$sudo apt-get upgrade

Instalar o editor de texto Nano:

```
$sudo apt-get install nano
```

Instalar a aplicação "pptp-linux" que é o "cliente" da VPN:

$sudo apt-get install pptp-linux

De seguida será configurado o interface Ethernet1. Quando toda a configuração estiver concluída, este interface irá permitir a ligação direta á VPN sem que seja necessária qualquer configuração adicional nos terminais aqui ligados. Como tal o servidor de DHCP, deverá correr neste interface para atribuir automaticamente IPs aos dispositivos. Os endereços IP são atribuídos à medida que os dispositivos efetuam o pedido de ligação a rede. Se qualquer dispositivo se desligar da rede, o endereço IP ficará livre para ser atribuído a um outro dispositivo.

A sua configuração do interface é feita da mesma forma que descrito no servidor de VPNs:

$sudo nano /etc/network/interfaces

```
iface eth1 inet static
address 192.168.2.1
netmask 255.255.255.0
```

O servidor DHCP, deve ser instalado da seguinte forma:

```
$sudo apt-get install isc-dhcp-server
```

Depois de instalado, é preciso efetuar a sua configuração, editando o ficheiro "dhcpd.conf":

```
$sudo nano/etc/dhcp/dhcpd.conf
```

```
option domain-name-servers 8.8.8.8, 8.8.4.4;
option domain-name "ra-vpnclient";
subnet 192.168.2.0 netmask 255.255.255.0
{
range 192.168.2.2 192.168.2.254;
option routers 192.168.2.1;
}
```

Depois de configurado o servidor DHCP dever-se-á reinicializar o mesmo recorrendo ao comando:

```
$sudo service isc-dhcp-server stop/start
```

No passo seguinte será configurada a rede sem fios no cliente VPN que será a ligação à Internet utilizada para estabelecer a VPN. A configuração é feita editando o ficheiro "interfaces" com o seguinte comando:

```
$sudo nano /etc/network/interfaces
```

Efetuar a configuração da rede sem fios da forma demonstrado em baixo:

```
auto wlan0
iface wlan0 inet dhcp
wpa-ssid "RAAP"
wpa-psk "x12345"
```

Passo seguinte será criar a VPN cliente, usando a ferramenta "pptpsetup" da seguinte forma:

```
$sudo pptpsetup
```

Passando os seguintes parametros:

```
--create ricardovpn
--server ricardovpn.myftp.biz
--username ricardo
--password raspberry
--start
```

O passo seguinte será ligar estabelecer a ligação à VPN, com o seguinte comando:

```
$sudo pon ricardovpn
```

Para que a ligação à VPN seja efetuada de forma automática, quando o Raspberry Pi é ligado, terá que se efetuar a seguinte configuração:

```
$sudo nano /etc/network/interfaces
```

```
auto tunnel
iface tunnel inet ppp
provider ricardovpn
```

Para desligar manualmente a VPN, pode ser usado o seguinte comando:

```
$sudo poff ricardovpn
```

O interface PPP0 deverá desaparecer da lista de interfaces:

$Ifconfig

De seguida editar o ficheiro "sysctl.conf", para ativar o reencaminhamento do trafego IP:

$sudo nano /etc/sysctl.conf

net.ipv4.ip_forward=1

Para assumir as alterações é preciso reinicializar a rede da seguinte forma:

$sudo service network restart

O passo seguinte configura o IP forwarding e postrouting, nas tabelas IP "iptables" (Firewall), tal como demonstrada em baixo:
$sudo iptables --table nat --append POSTROUTING --out-interface ppp0 –j ASQUERADE

$sudo iptables --append FORWARD --in-interface eth1 -j ACCEPT

Deverá ser instalada a aplicação "iptables-persistent" para tornar esta configuração persistente:

$sudo apt-get install iptables-persistent

No passo seguinte é acrescentada a rota, que vai encaminhar todo o tráfego para a VPN:

$sudo route add -net 0.0.0.0/0 ppp0

De seguida confirmar se a rota foi criada, com o comando seguinte:

$route -n

Para acrescentar a rota, sempre que a VPN sobe, deve ser editado o ficheiro "ricardovpn", da seguinte forma:

$sudo nano /etc/ppp/ip-up.d/ricardovpn

#!/bin/sh/sbin/route add -net 0.0.0.0/0 dev ppp0

4.3. Configuração do cliente VPN utilizando o sistema operativo Windows 7

Neste subcapítulo serão demonstrados os passos necessários para configurar a VPN no Windows. A demonstração foi feita no Windows 7 mas a configuração no Windows 8 e Vista é idêntica.

Começar por abrir o "Network and Sharing Center".

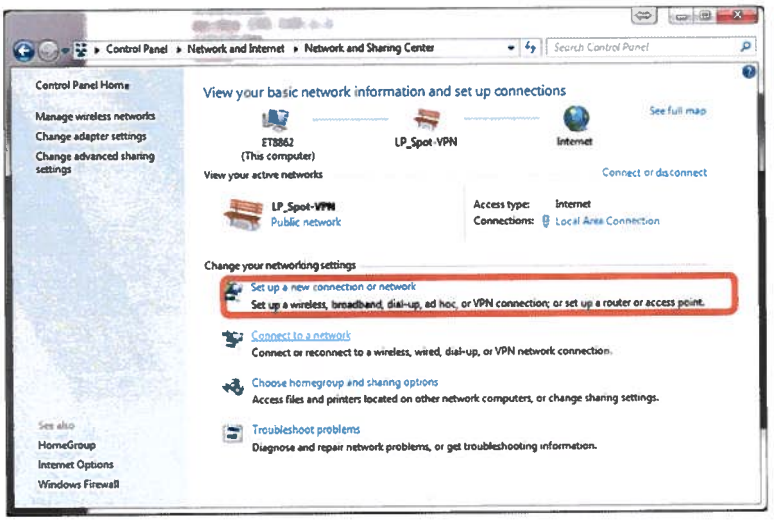

Figura 7 – Network and Sharing Center

Já no Network and Sharing Center, escolher a opção "Setup a new connection or Network".

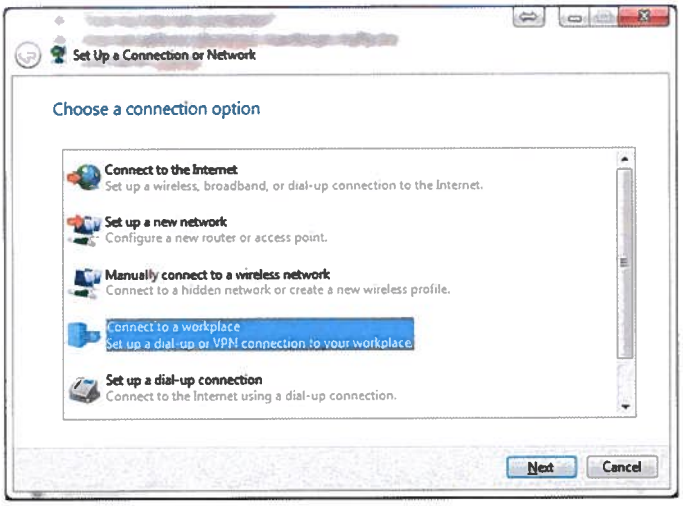

Figura 8 - Connect to a workplace

De seguida escolher a opção "Connect to a workplace", e fazer next.

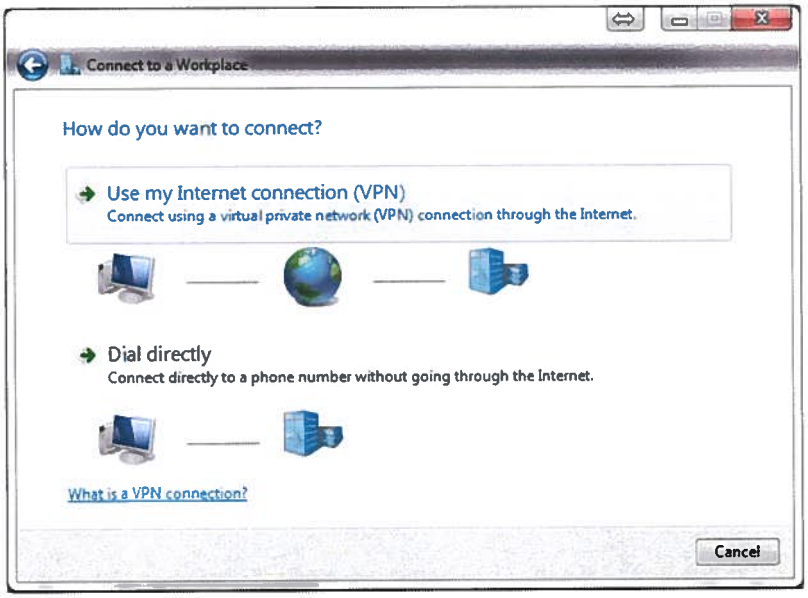

Figura 9 - Seleção da opção workplace

Escolher a opção "Use my Internet connection (VPN)".

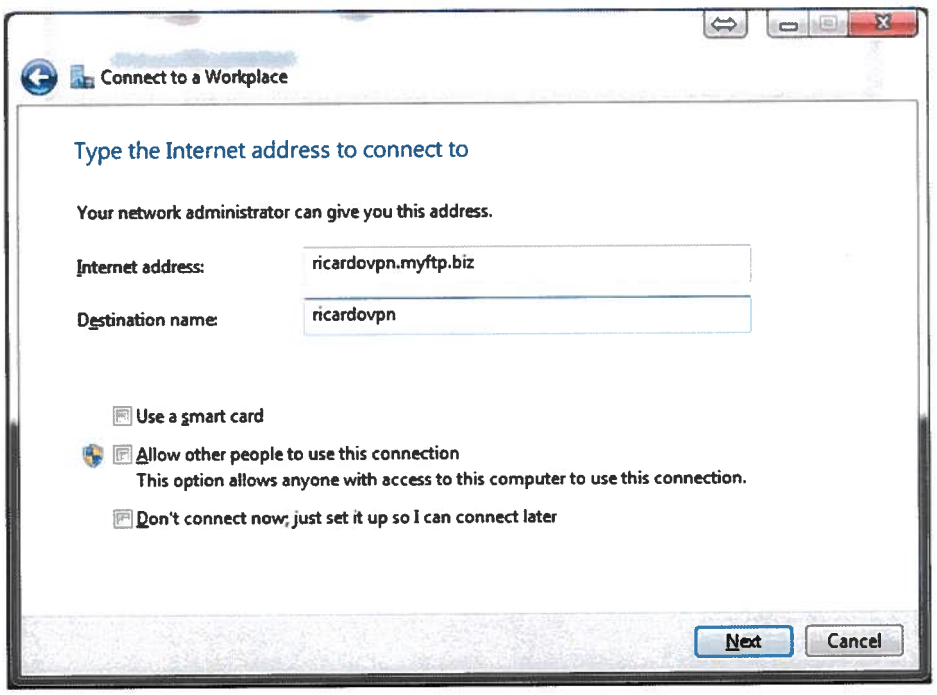

Figura 10 - Configuração da opção workplace

Neste passo deverá preencher os campos Internet address e Destination name como mostrado na figura em cima, e por fim fazer "Next".

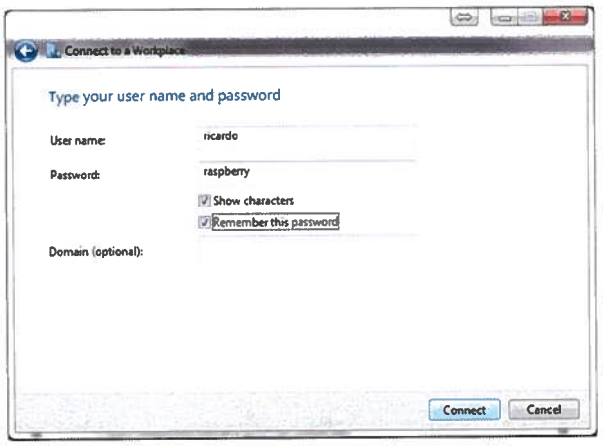

Figura 11 - Configuração de permissões do utilizador

Por último, preencher os campos Username e Password com os dados configurados anteriormente no servidor, tal como mostrado na figura em cima e carregar na opção "Connect". A VPN fica desta forma configurada, e para estabelecer a ligação basta carregar duas vezes no icon.

4.4. Configuração do cliente VPN no sistema operativo Android

Neste subcapítulo será demostrada a configuração da VPN em Android. Começar-se-á por entrar nas definições do sistema operativo.

Figura 12 - Configuração de definições

Selecionar a opção de "Mais definições".

Figura 13 - Escolha de opção VPN

Selecionar a opção "VPN".

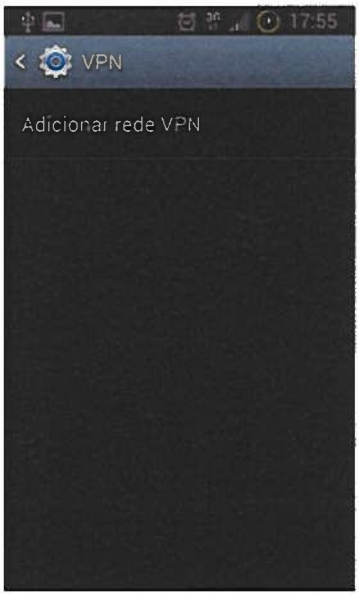

Figura 14 - Adicionar VPN

Escolha-se a opção "Adicionar rede VPN".

Figura 15 - Configuração da VPN

Neste ecrã deveram ser preenchidos os dados do servidor como mostrado na figura 16. Deverá também selecionar-se a opção "Encriptação PPP (MPPE)" e carregar em "Guardar".

Figura 16 - Selecionar a VPN

Após guardar as configurações a ligação pode ser estabelecida carregado na VPN que foi acabada de criar, neste caso denominada por "Ricardo VPN".

Figura 17 - Permissões de acesso

Por último, preencher os campos Nome de utilizador e Palavra passe. E a ligação será estabelecida.

Conclusão

Este trabalho teve como objetivo demostrar uma possível solução de baixo custo na implementação de VPNs. Foi utilizado para tal o sistema operativo Linux na sua configuração, e encontram-se descritos detalhadamente os vários passos necessários para a sua implementação, bem como funcionalidades e diversidade de plataformas possíveis na utilização da solução.

Pôde-se constatar que a VPN é uma tecnologia em crescimento, sendo comercializada por inúmeros fabricantes por todo o mundo. É utilizada tanto por organizações privadas como por instituições públicas. Os principais motivos do aumento da sua procura são o seu reduzido custo de instalação e utilização (que permite uma poupança significativa de investimentos em infraestrutura), a mobilidade que possibilita aos seus utilizadores, a evolução da velocidade de acessos à Internet graças à banda larga e, por último, a importante questão da segurança que é garantida à informação privada dos seus utilizadores, estabelecida através da aplicação de criptografia aos dados do utilizador, juntamente com a utilização de serviços de segurança tais como autenticação, controle de acesso, confidencialidade, integridade e não-repúdio, dificultando o acesso a informação por utilizadores não autorizados, permitindo maior confiança por parte das empresas que adotam esta tecnologia.

A utilização do sistema operacional Linux e Raspeberry Pi como suporte na configuração de VPNs mostrou ser uma solução atrativa para pequenas empresas que dispõem de reduzidos recursos financeiros para investir em segurança das suas comunicações ou soluções proprietárias.

Os resultados alcançados com este trabalho foram positivos, tanto a nível funcional como económico. A nível funcional os objetivos foram alcançados, sendo possível estabelecer VPNs utilizado três sistemas operativos diferentes, sendo eles Android, Windows e Linux. A nível económico foi possível implementar a solução VPN com baixo investimento como pretendido inicialmente, contribuindo para tal a utilização de programas de livre utilização, sendo o único investimento a aquisição de um Raspberry Pi por forma a suportar o sistema operativo Linux.

Com este trabalho conclui-se que uma solução VPN é uma forma segura e econômica de se estabelecer uma ligação a uma rede privada através de um meio

público, como a Internet. Optou-se por utilizar Linux por ser um programa de livre utilização, ser de fácil instalação e utilizar protocolo PPTP que foi desenvolvido para transferências de informação ponto-a-ponto de forma segura pela Internet.

No trabalho que o autor deste trabalho desempenha profissionalmente, inúmeras questões são levantadas sobre a redundância existente nas redes de telecomunicações, havendo a noção de que todos os serviços dos clientes devem ser garantidos à mínima falha de comunicações, sendo esta uma questão recorrente todos os dias. Como sugestão para um trabalho futuramente proposto, fica a sugestão de implementação de uma VPN como redundância do circuito principal de uma empresa.

Referências bibliográficas

Ross, J. (2009). *Network Know How.* San Francisco: No starch press.

Anttalainen, T. (2003). *Introduction to Telecommunications Network Engineering.* Londen: Artech House.

Checkpoint. (20 de 10 de 2013). Check Point IPSec VPN Software Blade. Obtido de Checkpoint: http://www.checkpoint.com/products/softwareblades/ipsec-virtual-private-network.html

Citrix. (20 de 10 de 2013). NetScaler Gateway. Obtido de Citrix: http://www.citrix.com/products/netscaler-gateway/overview.html

Davies, J., & Lewis, E. (2004). *Deploying Virtual Private Networks With Microsoft Windows Server 2003.* Washington: Microsoft Press.

Dean, T. (2010). *Network Guide to Networks.* Boston: Course Technology, Cengage Learning.

D-Link. (24 de 12 de 2013). VPN Remote Access Software. Obtido de D-Link: http://www.dlink.com/us/en/business-solutions/security/utm-firewalls/ds-601-vpn-remote-access-software-1-user-license

Douglas, C. (2009). *Computer Networks and Internets.* New Jersey: Pearson Education Ltd.

Feilner, M. (2006). *Open VPN.* Birmingham: Packt.

Forouzan, B., & Fegan, S. (2007). *Data Communications and Networking.* New York: Higher Education.

Fortinet. (22 de 10 de 2013). Soluções Virtual Private Network (VPN) - IPsec & SSL . Obtido de Fortinet: http://www.fortinet.com/solutions/vpn.html

Guichard, J., Pepelnjak, I., & Apcar, J. (2003). *Cisco Press - MPLS and VPN Architectures.* New York: Cisco Press.

Horan, B. (2013). *Practical Raspberry Pi.* New York: Apress.

Johnson, T., Weinstein, K., Nolan, H., & Miller, H. (2007). *NetworkSec.* Indianapolis: Wiley.

Lowe, D. (2003). *Networking For Dummies.* Indianapolis: Wiley.

Membrey, P., & Hows, D. (2013). *Learn Raspberrry Pi with Linux.* New York: Apress.

Rhodes, B., & Goerzen, J. (2010). *Foundations of Python Network Programming Second Edition.* New York: Apress.

Richardson, M., & Wallace, S. (2013). *Getting Started with Raspberry Pi.* Cambridge: O'Reilly.

Schmidt, M. (2012). *Raspberry Pi A Quick Start Guide.* Washington: Copyright.

Scott, C. (1999). *Virtual Private Networks.* Cambridge: O'Reilly.

Scott, C., Wolfe, P., & Erwin, M. (1999). *Virtual Private Networks.* Cambridge: O'Reilly.

Serpanos, D., & Wolf, T. (2011). *Architecture Of Network Systems.* Boston: Elsevier.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices.* New Jersey: Prentice Hall.

Stallings, W. (2007). *Data and computer communications.* New Jersey: Pearson.

Tanenbaum, A., & Wetherall, A. (2010). *COMPUTER NETWORKS - FIFTH EDITION.* New Jersey: Pearson.

Tomsho, G. (2011). *Guide to Networking Essentials.* Stamford: Course Technology.

Torres, G. (2001). *Redes de Computadores.* Rio de Janeiro: Axé brasil editora ltda.

White, C. (2013). *Data Communications and Computer Networks - A Business User's Approach.* Stamford: Course Technology.

Wiley, J. (2012). *Raspberry Pi User Guide.* Indianapolis: Wiley.

Wong, A., & Yeung, A. (2009). *Network Infrastructure Security.* Neu Isenburg: Springer.