

REDES DE COMPUTADORES COM ÊNFASE EM VPN¹

Eduardo Augusto G. de O. Daleffe²

Renato Arnaut Amadio³

Júlio Cesar Gavilan⁴

RESUMO

A tendência da utilização da tecnologia computacional nas comunicações teve uma profunda influência na forma como os sistemas computacionais são organizados. O conceito da computação no qual se restringe a uma sala com um macro computador onde os usuários levam suas tarefas para processamento, hoje, está completamente defasado. Com a ascensão da Tecnologia, hoje, torna-se indispensável a utilização em grandes empresas, adquirindo maquinário próprio ou terceirizando-o. Conseqüentemente o Macro Computador foi substituído por um grande número de computadores, denominando-se “Cluster”, o nome dado a um sistema que relaciona dois ou mais computadores para que estes trabalhem de maneira conjunta no intuito de processar uma tarefa. Estas máquinas dividem entre si as atividades de processamento e executam este trabalho de maneira simultânea. O conjunto de protocolos de comunicação denominado TCP/IP domina o mercado de interconexão de redes de computadores. Ele é referenciado como um modelo de protocolos de interconexão de redes de computadores, sendo um padrão de facto, ou seja, um padrão adotado pelas empresas no mercado. Com base nisto e juntamente a necessidade de comunicar de forma eficiente e segura, surgiu a tecnologia VPN. A VPN usa a rede pública, ou seja, a internet, para transportar os arquivos. Uma outra forma seria criando uma rede privada física, que poderia, sim, garantir privacidade, segurança e integridade, mas que também não é segura em sua totalidade. O custo para implementação de uma rede privada física pode não ser tão alto para pequenas

¹ Artigo apresentado para conclusão de graduação em Sistemas de Informações da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço - EDUVALE

² Acadêmico do curso de Sistema de Informação da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE: xgutierrez7@gmail.com

³ Professor Especialista da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE: renatoamadio@uol.com.br

⁴ Físico Computacional pela Universidade de São Paulo, Mestre em Ciências da Computação pela Universidade Federal de Santa Catarina, Professor da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE: jcgavilan@gmail.com

distâncias, porém se torna impraticável quando se trata de organizações que possuem polos espalhados pelo mundo e precisam trocar informações constantemente. Com isso, utilizando o método de pesquisa bibliográfica, onde obtemos através de revistas, livros e artigos, entende-se que a VPN se adequa para um conjunto de situações e é isto que a torna, retornando a fala, o modelo de interligação mais seguro e eficiente na relação custo-benefício.

Palavras-chave - Redes de computadores, Empresas de grande porte, VPN

ABSTRACT

The trend in the use of computer technology in communications has had a profound influence on the way in which computer systems are organized. The concept of computing in which it is restricted to a room with a macro computer where users take their tasks for processing, today, is completely out of date. With the rise of Technology, today, it is essential to use it in large companies, purchasing their own machinery or outsourcing it. Consequently, the Macro Computer has been replaced by a large number of computers, called "Cluster", the name given to a system that relates two or more computers so that they work together in order to process a task. These machines divide the processing activities among themselves and perform this work simultaneously. The set of communication protocols called TCP / IP dominates the market for the interconnection of computer networks. It is referred to as a model of computer network interconnection protocols, being a de facto standard, that is, a standard adopted by companies in the market. Based on this and together the need to communicate efficiently and safely, VPN technology emerged. The VPN uses the public network, that is, the internet, to transport files. Another way would be to create a physical private network, which could, indeed, guarantee privacy, security and integrity, but which is also not completely secure. The cost to implement a physical private network may not be so high for short distances, but it becomes impractical when it comes to organizations that have hubs around the world and need to exchange information constantly. With this, using the bibliographic search method, where we obtain through magazines, books and articles, it is understood that VPN is suitable for a set of situations and this is what makes it, returning speech, the most secure interconnection model and cost-effective.

Keyword - Computer networks, Large companies, VPN

2. INTRODUÇÃO

A Importância da Internet e a utilização da mesma por grandes empresas já se tornou algo indiscutível quando se é falado no âmbito de concorrência, otimizando resultados e encurtando distâncias, a internet torna possível a ramificação de uma empresa em um amplo território como por exemplo, diferentes estados.

Diante disso, surge a pergunta deste presente artigo, como se apresenta a aplicação da tecnologia VPN nas empresas de grande porte?

O objetivo geral deste artigo é apresentar a utilização da Tecnologia de Rede: VPN dentro de uma empresa de grande porte, afim de proporcionar uma comunicação de rede flexível e segura entre suas filiais.

Para tanto o artigo foi estruturado em três tópicos principais sendo:

- 1º Tópico - Dados, Redes e Topologia
nesta etapa conhecemos os conceitos, possibilidades e aplicações das Redes.
- 2º Tópico - Padrões e Protocolos, Tipos de Redes e Firewall
nestes colocamos em discussão formas de utilizações das Redes .
- 3º Tópico – aqui temos os estudos sobre a plataforma Mikrotik e a utilização da tecnologia da VPN na mesma.

Desta forma este artigo pretende contribuir para o entendimento da utilização da tecnologia VPN aplicada em grandes empresas de forma segura, eficiente e econômica em seu processo de expansão territorial.

2. DADOS E REDES

2.1. O que são dados.

Com a ascensão da utilização da tecnologia de redes, tornou-se comum no mercado, para muitas empresas e usuários domésticos tornou-se indispensável a utilização da mesma, no entanto, muitos não conhecem um fator primordial, que é a segurança. Os dados e recursos da rede são valiosos, e caso utilizado de maneira

maliciosa pode causar grandes estragos, por isso devem ser protegidos (TANENBAUM,1997).

2.2. Surgimento das Redes

Segundo Tanenbaum (2011), a rede de computadores surgiu na década de 60, na qual as redes telefônicas estavam em seu auge, dominando a maior parte do mundo. Já em 1970 os números de pequenas redes estavam crescendo cada vez mais, sendo apresentado por Robert Metcalfe os princípios de uma rede local, uma ETHERNET que tardiamente originariam LANs de curta distância.

Pinheiro (2003), cita que na década de 1970 houve um movimento para padronizar as redes, contando com diferentes fabricantes, dando direção à construção de protocolos abertos que poderiam se adaptar e gerar várias soluções. No início, as redes eram pequenas, possuindo poucos computadores, sendo usadas em 1964, nos EUA, pelas companhias aéreas.

Segundo Comer (2015), A DARPA começou a trabalhar em direção a uma tecnologia de interconexão de redes em meados da década de 1970. Nessa época, a DARPA era conhecida como a principal agência financiadora de pesquisa de redes de comutação de pacotes, uma delas a ARPANET.

2.2.1. O que são redes de computadores

Segundo Tanenbaum (2011), a tendência da utilização da tecnologia computacional nas comunicações teve uma profunda influência na forma como os sistemas computacionais são organizados. O conceito da computação no qual se restringe a uma sala com um macro computador onde os usuários levam suas tarefas para processamento, hoje, está completamente defasado. Com a ascensão da Tecnologia, hoje, torna-se indispensável a utilização em grandes empresas, adquirindo maquinário próprio ou terceirizando-o. Consequentemente o Macro Computador foi substituído por um grande número de computadores, denominando-se “CLUSTER”, o nome dado a um sistema que relaciona dois ou mais computadores para que estes trabalhem de maneira conjunta no intuito de processar

uma tarefa. Estas máquinas dividem entre si as atividades de processamento e executam este trabalho de maneira simultânea.

Comer (2015), cita que na atualidade, o conjunto de protocolos de comunicação denominado TCP/IP domina o mercado de interconexão de redes de computadores. Ele é referenciado como um modelo de protocolos de interconexão de redes de computadores, sendo um padrão de facto, ou seja, um padrão adotado pelas empresas no mercado.

Os primeiros passos de redes de computadores e da internet, podem ser traçados desde o início da década de 1960, quando a rede telefônica era a rede dominante no mundo inteiro (KUROSE,2010 p.45)

3. PADRÕES, PROTOCOLOS, TIPOS DE REDES E FIREWALL

3.1. Tipos de Redes

Para Deitel (2005), atualmente quando o assunto é redes, em sua grande maioria estamos nos referindo a duas principais categorias, sendo elas as redes locais denominadas (Lans) e as redes de longa distância denominadas (Wans).

As redes de dados que cobrem grandes distancias geográficas (por exemplo, A América Latina) são diferentes daquelas que cobrem curtas distancias (uma casa, por exemplo). Para ajudar a caracterizar as diferenças entre elas, as tecnologias da troca de pacotes normalmente são divididas em duas categorias: redes de longa distância (WANs) e redes locais (LANs), sendo que ambas não possuem definições formais. Em vez disso, os fornecedores aplicam os termos de forma livre para ajudar os clientes a diferenciar as tecnologias. (COMER, 2015)

3.1.2. Redes locais Lans

Segundo Kurose (2010), LAN é uma rede de computadores concentrada em uma área específica, não muito abrangente, tal como um prédio ou uma residência ou até mesmo uma sala, quando um usuário acessa a Internet, esse acesso é quase sempre por meio de uma LAN. A velocidade de transmissão, na maioria das LANs por ser uma curta distância, é geralmente muito alta. Atualmente no mercado é

possível encontrar a venda dispositivos entre 100 mbps a 10 gbps, onde sua grande maioria é de 1gbps.

Segundo Comer (2015) Tecnologias de LAN fornecem as conexões de mais alta velocidade e capacidade entre os computadores, contudo deixam de poder cobrir longas distâncias. Por exemplo, uma LAN comum cobre uma pequena área, como um único prédio, casa ou uma sala, e opera normalmente entre 100 Mbps e 10 Gbps. Também oferecendo atrasos (latências) Como as tecnologias de LAN cobrem curtas distancias, elas oferecem menores atrasos que a WAN. O atraso através de uma LAN pode ser tão curto quanto alguns décimos de milissegundos ou tão longo como 10 milissegundos.

3.2.2. Redes Wans

Tecnologias WAN, às vezes chamadas *long haul networks* (redes de transporte a longa distância), fornecem comunicação a longas distâncias. A maioria das tecnologias de WAN não limita o leque de distância; uma WAN pode permitir que as extremidades de uma comunicação sejam distanciadas arbitrariamente. Por exemplo, uma WAN pode cobrir um continente ou ainda unir computadores através de um oceano. Normalmente, as WANs operam em velocidades mais baixas que as LANs, e possuem muito mais atraso entre as conexões. As velocidades típicas para uma WAN variam de 100 Mbps (milhões de bits por segundo) até 10 Gbps (bilhões de bits por segundo). Os atrasos através de uma WAN podem variar de alguns milissegundos até várias dezenas de segundos." (COMER, 2015).

Lunard (2007), cita que, as redes Wans tem como principal finalidade ligar diferentes locais, até mesmo cidades e Países e normalmente utilizam o modelo cliente-Servidor.

Wans consistem em muitas Lans e conectam muitos computadores a grandes distancias, a maior das Wans é de longe, a internet. Wans em geral empregam uma topologia em malha, funcionam a velocidades mais baixas e suas taxas de erro são mais altas por que tem de interagir com várias Lans e Wans que muitas vezes são heterogenias. (DEITEL,2005, p 490).

3.3. Padrão de Rede

Segundo Morimoto (2010), os padrões de rede definem com detalhes a forma como os dados são organizados e transmitidos, permitindo que produtos de diversos fabricantes se comuniquem perfeitamente. Os mesmos são desenvolvidos pelo IEEE (Institute of Electrical and Electronics Engineers), que atualmente é uma das maiores organizações profissionais sem fins lucrativos.

Segundo Comer (2015) a *Xerox Palo Alto Research Center* (PARC) no início da década de 1970, desenvolveu uma tecnologia LAN de comutação de pacotes chamada Ethernet e em 1978 juntamente com a *Intel Corporation* e a *Digital Equipment Corporation* padronizaram a Ethernet, logo depois o IEEE lançou uma versão compatível do padrão denominando-se padrão 802.3.

3.3.1. Padrão 802.3

A Ethernet é a tecnologia LAN mais popular em nosso cotidiano, é utilizado pela maioria das redes corporativas e pessoais, as versões atuais da Ethernet são conhecidas como Gigabit Ethernet e 10 Gigabit Ethernet, respectivamente transferindo dados a 1Gbps e 10Gbps, (COMER, 2015).

3.4. Firewalls

É um modelo adaptado de segurança medieval, na era medieval cavava-se fossos profundos em torno dos castelos com o intuito de forçar a passagem, passando por uma única ponte, onde teriam maior controle do fluxo de pessoas, seja na revista ou na defesa do castelo. (TANENBAUM,2011)

Nas redes pode –se usar o mesmo artifício uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou entrada da empresa é feito através de uma ponte levadiça eletrônica (firewall). (TANENBAUM,2011, p.825).

Segundo Tanenbaum (2011), o Firewall atua como um filtro de pacotes. Ele inspeciona todo e qualquer pacote que esteja no fluxo da rede. Os pacotes que atenderem a algum critério descrito nas regras formuladas pelo administrador da rede serão remetidos a ação descrita na regra, seja ela de *accept*, *reject*, *drop*, etc... Segundo Kurose (2010), o Firewall é nada mais que uma combinação de hardware e rede lógica que isola a rede local de uma organização da rede externa (Internet/WAN), criando um filtro no fluxo de dados e caso o pacote seja malicioso é bloqueado, caso permitido passa normalmente, todo administrador de rede controla o acesso entre o mundo externo e os recursos da rede que administra, gerenciando o fluxo de tráfego.

O Firewall em si é imune a invasões, contudo, deve ser instalado/configurado corretamente para que não crie uma falsa sensação de segurança, que acaba se tornando pior do que não ter nenhum Firewall. (KUROSE 2010).

3.5. Topologias

A topologia de rede descreve o modo como todos os dispositivos estão ligados entre si e a forma como se desenvolve a troca de informação entre eles. A topologia garante a redução de custo e o aumento da eficiência do sistema por meio da combinação de recursos. A mais utilizada é a topologia estrela, caracterizada por um elemento central que gerencia o fluxo de dados da rede. (LUNARDI,2007).

Segundo Maia (2011), as redes ponto a ponto possuem uma conexão dedicada ligando dois dispositivos, ou seja, não existe compartilhamento físico do canal de comunicação, apenas lógico, já nas redes multiponto o canal de comunicação é compartilhado por todos os dispositivos de rede.

3.5.1. Anéis

É uma rede em formato circular, representando um anel, consiste em estações conectadas através de um caminho fechado. Eles se comunicam diretamente com o computador central (LUNARDI, 2007)

Segundo Maia (2011), na topologia em anel, os dispositivos compartilham o mesmo canal de comunicação, a vantagem dessa topologia é a semelhança com topologia em barra e é usada em redes locais e em redes metropolitanas, contudo, como a topologia anel é compartilhada por várias estações, se faz necessário um protocolo de controle de acesso ao meio, chamado FDDI.

3.5.2. Árvore

A topologia em árvore, também conhecida como hierárquica, é uma série de barras interconectadas. Geralmente existe uma barra central em que outras conexões menores se conectam. (LUNARDI, 2007).

3.5.3. Estrela

A topologia estrela é caracterizada por um elemento central que gerencia o fluxo de dados na rede, estando ligado a todos os dispositivos na rede, por isso a designação estrela. A comunicação de um dispositivo de rede para outro deverá, obrigatoriamente, passar pelo ponto central tornando o processo muito mais eficaz, já que os dados nessa topologia não deverão, necessariamente, passar por todas as estações. Esta topologia somente será possível, caso esteja sendo utilizado um switch como concentrador (TANENBAUM,2003).

Segundo Maia (2011), a vantagem dessa topologia é a sua simplicidade e baixo custo, e sua desvantagem está na baixa disponibilidade, pois depende integralmente do dispositivo central (concentrador/switch) para o funcionamento da rede.

3.5.4. Barramentos

A topologia em barramento, também chamada de backbone, é, uma configuração linear, que conecta todos os computadores da rede em uma única linha ou cabo, ou seja, todos os pontos atuam da mesma maneira, algumas vezes

assumindo um papel ativo, outras assumindo um papel passivo, assim, criando o tráfego de informações (LUNARDI, 2007).

4 PLATAFORMA MIKROTIK E A UTILIZAÇÃO DA TECNOLOGIA VPN

4.1. Origens da Mikrotik

Mikrotik é uma empresa que trabalha com desenvolvimento de hardwares e softwares para gerenciamento de redes de computadores, fundada em 1995, em Riga, capital da Letônia. A empresa também possui um Sistema Operacional baseado em Linux, chamado Mikrotik RouterOS. Ele permite que qualquer plataforma x86 torne-se um poderoso roteador, com funções como VPN, Proxy, Hotspots, Controle de Banda, QoS, Firewall, dentre outras, que variam de acordo com o pacote de serviços adquirido. (ENTELCO, 2014)

O RouterOS possibilita a criação de ambientes de rede seguros, trabalhando com um firewall eficiente e concatenação de links. Além disso, o sistema conta com o suporte de protocolos de roteamento, entre eles BGP, RIP, OSPF, MPLS, entre outros. (ENTELCO, 2014).

Para aprender a utilizar, configurar e planejar uma rede utilizando a Plataforma Mikrotik. As Empresas de pequeno, médio e grande porte, primeiramente estão utilizando o RouterOS (Os da Mikrotik) para administrar, gerenciar e controlar suas operações dos dados via rede, assim como utilizado por operadoras de Telecom, provedores de acesso via rádio (WISP) e integradores de serviços em TI. (ENTELCO, 2014)

4.2. VPN

Em meados da década de 1990, a ascensão da Internet e o aumento da velocidade para conexões baratas de Internet pavimentou o caminho para novas tecnologias. Muitos desenvolvedores, administradores e gerentes descobriram que pode haver soluções melhores do que gastar rios de dinheiro, em linhas de acesso discadas e dedicadas.

A ideia era usar a Internet para comunicação entre filiais e ao mesmo tempo garantir segurança e sigilo dos dados transferidos. Resumindo: fornecendo conexões seguras entre filiais da empresa através de linhas de baixo custo usando a Internet. (FEILNER, 2006)

4.3. O que é VPN

- **Virtual**, porque não há conexão de rede direta real entre os dois (ou mais) parceiros de comunicação, mas apenas uma conexão virtual fornecida por VPN.
- **Software**, realizado normalmente em conexões públicas de Internet.
- **Privado**, pois apenas os membros da empresa conectados pelo Software VPN têm permissão para ler os dados transferidos.

4.3.1. Características Prático-Teóricas de VPN's

VPN's de Acesso Remoto: são Vpns que fazem conexão segura de usuários remotos. Dentro de VPN's com acesso remoto tem-se mais uma divisão de tipos que são: - Iniciadas pelo cliente: usuários remotos usam aplicações clientes para estabelecer um túnel seguro entre um ISP e empresa. - Iniciadas pelo NAS (Network Access Server): usuários ligam-se a um ISP-NAS e este estabelece um túnel seguro até a empresa e este ainda permiti múltiplas sessões de conexões de usuários. VPN's LAN-to-LAN: são Vpns com conexões seguras entre empresas matriz-filial (Intranet VPN's) ou pode ser uma (Extranet VPN) que é composta, por exemplo, por consumidores, fornecedores e um terceiro parceiro.

4.3.1. Utilizações de VPN

Segundo Feilner (2006), atualmente mais e mais empresas oferecem seus clientes ou parceiros de negócios um acesso protegido a dados relevantes para suas relações comerciais, como fórmulas de pedidos ou dados de estoque. Assim, temos três cenários típicos para soluções VPN nas empresas modernas:

- Intranet que abrange vários locais de uma empresa.

- Dial-up para trabalhadores domésticos (Home-Office) ou de campo com IP's Dinâmicos.

- Extranet para clientes ou parceiros de negócios.

Cada um desses cenários típicos requer considerações e configurações de segurança especiais. Os funcionários Home-Office precisarão de acesso diferente aos servidores da empresa do que os clientes e parceiros de negócios. Na verdade, o acesso de parceiros de negócios e clientes deve ser severamente restrito.

5. CONSIDERAÇÕES FINAIS

A rede de computadores surgiu na década de 60, na qual as redes telefônicas estavam em seu auge, dominando a maior parte do mundo. Atualmente quando o assunto é redes entendemos que as redes de dados cobrem grandes distancias geográficas, mas não estão presentes somente nas organizações, até em nossas residências é comum o compartilhamento de informações, compartilhar Internet com outros dispositivos, assistir filmes e conversar com amigos. A tendência da utilização da tecnologia computacional nas comunicações teve uma profunda influência na forma como os sistemas computacionais são organizados e com base nisto e juntamente com a necessidade de comunicar de forma eficiente e segura, surgiu a tecnologia VPN. Graças a esse avanço tecnológico hoje é possível Matriz e Filiais estarem em pontos territoriais extremos, porem manter sua comunicação com informações em tempo real, de forma segura, ágil e eficiente. Fazer essa análise da aplicação da tecnologia VPN nas empresas de grande porte, foi a proposta principal deste artigo e para isso utilizou-se o método de pesquisa bibliográfica em acervos de livros e artigos científicos com autores de renomado conceito dentro do tema abordado.

REFERÊNCIAS

- COMER, Douglas E. “**Interligação em Rede com TCP/IP**”, Volume I. 6ª Edição. São Paulo, Ed. Campus, 2015;
- DEITEL, Harvey. **Sistemas Operacionais** – Editora: São Paulo: Pearson Prentice Hall, 2010.
- Entelco - **Saiba como a MikroTik produz seus Hardwares** – Publicado em: 2 de abril de 2013, Disponível em: <http://www.entelco.com.br/blog/?tag=historia-mikrotik> acesso em 22 de Novembro de 2014.
- FEILNER, Markus. **OpenVPN Building and integrating virtual private Networks** – Olton, Packt Publishing Ltd, 2006
- KUROSE, James F. **Redes de computadores e a internet: uma abordagem top-down/**. São Paulo: Addison Wesley, 2010.
- LUNARDI, Marco Agisander - **Redes de Computadores - Prático e Didático** – Editora: Ciências Modernas, 2007.
- MAIA, Luiz Paulo- **Arquitetura de redes de computadores /**. – Rio de janeiro LTC, 2011.
- MORIMOTO, Carlos Eduardo. - **Redes, Guia Prático**. 2ª Ed. Porto Alegre: Sul Editores, 2010.
- PINHEIRO, José Maurício. **Guia completo de cabeamento de redes**. Rio de Janeiro: Campus, 2003
- TANENBAUM, Andrew S. - “**Redes de Computadores**”. Editora Campus. 3º Edição. Rio de Janeiro, 1997.
- TANENBAUM, Andrew S. e WETHERALL David **Redes de Computadores**, 4. ed. São Paulo: 2011.
- TANENBAUM, Andrew S. **Redes de Computadores**, 4. ed. São Paulo: Editora Campus, 2003.