Análise de desempenho da VPN em redes corporativas

VPN performance analysis on corporate networks

Camila Santos Faustino de Andrade
Redes de Computadores pela Fatec Bauru
camila.andrade2@fatec.sp.gov.br
Anderson Francisco Talon
Redes de Computadores pela Fatec Bauru
anderson.talon@fatec.sp.gov.br

RESUMO: O seguinte trabalho visa mostrar a eficiência da *virtual private network* (VPN) em redes corporativas, mostrando sua eficácia em prevenir a perda e/ou extravio de dados. A VPN utiliza um conceito conhecido como um túnel virtual (tunelamento) e criptografia de dados ponta a ponta entre um par de nós que estão distantes fisicamente ou geograficamente, sendo assim, muitas vezes é necessário a realização de um acesso remoto. O acesso permite que um usuário autorizado acesse informações de sua corporação que são consideradas privadas. Conclui-se então que após observados os pontos acima será feita a análise com base em dois artigos com foco em VPN, segurança e seus protocolos, buscando comprovar através de estudos e experimentos a eficácia da VPN em uma rede corporativa e seu funcionamento através da análise dos protocolos mais utilizados em sua arquitetura.

Palavras-chave: servidores. acesso remoto. segurança da informação.

ABSTRACT: *The following work aims to show the efficiency of the virtual private network (VPN) in corporate networks, showing its effectiveness in preventing data loss. VPN uses a concept known as a virtual tunnel (tunneling) and end-to-end data encryption between a pair of nodes that are physically or geographically distant, so remote access is often required. Access allows an authorized user to access information about your corporation that is considered private.* It is concluded then after observing the above points, the analysis will be made based on two articles focusing on VPN, security and its protocols, seeking to prove through studies and experiments the effectiveness of VPN in a corporate network and its operation through the analysis of the most used protocols in its architecture.

Keywords: servers. remote access. information security.

1 INTRODUÇÃO

Para Marsic (2013) uma rede é uma série de dispositivos (conhecidos também como nós) conectados por links de comunicação que são construídos utilizando diferentes meios físicos. Um nó pode ser um computador, telefone, ou qualquer outro dispositivo capaz de enviar e receber mensagens. O meio de comunicação é o caminho físico pelo qual cada mensagem viaja do remetente para o

destinatário, por exemplo o meio utiliza fibra ótica, cabos ou ondas através do ar.

A comunicação entre matriz, filiais, fornecedores, distribuidores, parceiros de negócio, clientes e usuário móveis formam uma malha de comunicação em um ambiente corporativo, uma infraestrutura importante para qualquer organização. Há um crescimento da necessidade de acesso remoto, por isso é um aspecto importante e deve ser considerado na política de segurança de redes corporativas (NAKAMURA; GEUS).

Segundo Peterson e Davie (2013) o termo VPN é utilizado em demasia e as definições variam, mas intuitivamente podemos definir uma VPN considerando primeiro a ideia de uma rede privada. As corporações com muitas sedes montam redes privadas alugando linhas de transmissão das companhias telefônicas e usando essas linhas para interconectar as sedes.

O foco principal deste trabalho é realizar uma análise teórica sobre a performance da VPN, em ambientes corporativos. A análise será realizada através de dois artigos que evidenciam a VPN como uma aplicação que realiza a transmissão de dados com pouca ou nenhuma perda, dependendo da sua configuração e infraestrutura em um acesso remoto.

O artigo **Análise de segurança do acesso remoto VPN** (NAKAMURA; GEUS; 2000) demonstra que a VPN é eficaz quando falamos de proteção de dados, entretanto a aplicação apresenta algumas brechas de segurança, quando utilizada em situações como gateway, ou quando os ataques ocorrem através do sistema operacional, aplicativos ou serviços. O artigo **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA; 2019) tem como propósito demonstrar quais são os protocolos utilizados quando falamos da arquitetura de software da VPN, e demostra quais são os mais seguros quando falamos de criptografia de dados.

Segundo Nakamura e Geus (2011) a privacidade da comunicação é de suma importância para as organizações, o que faz com que as VPN's se tornem também importante em caso de "parcionamento" de uma rede compartilhada. Assim a VPN garante a integridade dos dados enviados na conexão fechada, isolando os dados de outras conexões presentes no meio compartilhado.

2 FUNDAMENTAÇÃO TEÓRICA

Este artigo teve o intuito de comprovar a eficácia da VPN em uma rede corporativa, sendo assim foi feita a comparação de dois artigos que tinham como base o estudo da *virtual private network* (VPN) e seus protocolos. O **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA, 2019), teve como base de estudo a análise dos principais protocolos utilizados na *virtual private network* (VPN) e o artigo **Análise de segurança do acesso remoto VPN** (NAKAMURA; GEUS, 2000) teve como base o estudo da VPN e sua implantação em ambientes corporativos.

No artigo **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA, 2019), podemos notar que foram analisados cinco protocolos sendo eles: PPTP, L2F, L2FP, IPSec, SSL. Para obter um resultado satisfatório na análise houve

um estudo aprofundado, visando a assimilação do funcionamento de cada um dos protocolos descritos, podendo então através disto examinar o ponto alto e o ponto baixo de cada protocolo assim como suas características distintas e similares para somente então observar qual protocolo teria um melhor desempenho na elaboração de uma *virtual private network* (VPN).

O artigo **Análise de segurança do acesso remoto VPN** (NAKAMURA; GEUS 2000) tem a intenção de comprovar a eficiência da VPN, em uma rede corporativa mostrando então seu comportamento quando implantada neste meio, ele demonstra os principais pontos da VPN que vão desde sua configuração inicial até quando utilizada como gateway, executa também a análise da VPN em alguns ambientes que aumentam o risco de invasão da rede e simulam algumas situações a qual o usuário poderia expor a rede.

Ambos os artigos comprovam a grande efetividade da VPN em uma rede corporativa com algumas ressalvas sendo estas: risco a que o usuário expõe a rede, os protocolos corretos devem ser implementados, sendo tais protocolos o IPSec ou SSL, a configuração deve ser realizada de forma correta com a utilização de uma chave assimétrica não abrindo supostas brechas para invasão.

2.1 O estudo dos protocolos

2.1.1 PPTP (Point-to-Point Tunneling Protocol)

O protocolo foi criado através de um fórum de empresas e tem como objetivo facilitar o acesso a computadores remotos de uma rede privada através da internet ou em outra rede baseada em IP. Podemos observar pela descrição do protocolo que ele atua na base dos acessos remotos como conhecemos hoje, este foi um dos primeiros protocolos a serem criados para este fim.

Este protocolo está incorporado no Windows e pode ser analisado a partir do Windows NT e em clientes Windows 95 através uma instalação sendo então um dos primeiros protocolos com a função VPN, possibilitando que as funcionalidades realizem um túnel através do acesso remoto. Este protocolo agrega as funções de um outro protocolo conhecido o PPP (*point-to-point*). O protocolo se baseia nos seguintes meios de autenticação do PPP sendo eles os protocolos CHAP (SIMPSON; 1996), MS-CHAP (ZORN; 2000) e o PAP (LLOYD; SMIPSON ;1992), sendo este último considerado um protocolo inseguro.

Para uma conexão PPP existir é necessário a seguinte arquitetura: cliente remoto, internet, rede local. Para que ocorra um bom funcionamento é necessário que cada um dos processos se satisfaça. O cliente PPTP utiliza o PPP para se conectar à rede *Internet Service Provider (ISP*), nesta fase o protocolo PPP é utilizado para realizar uma conexão e criptografar os dados, após a conexão estabelecida, cria-se uma conexão de controle desde o cliente até o servidor pela rede internet, através desta conexão todos os parâmetros são estabelecidos entre as extremidades do túnel, a conexão utilizada é o protocolo TCP/IP sendo conhecido como PPTP.

Após, os pacotes de dados são criptografados e encapsulados como um cabeçalho PPP, o quadro PPP resultante é depois encapsulado como um cabeçalho *GRE,* após isso o quadro é finalmente encapsulado com um cabeçalho IP que contém o endereço de origem e destino.

2.1.2 L2F (Layer Two Forwarding)

Este protocolo foi desenvolvido pela empresa Cisco, conhecido também como L2F. Este protocolo utiliza o PPP para autenticação de usuários remotos, e pode incluir suporte para autenticação via RADIUS, TACACS, TACACS+. Ele inclui dois níveis de autenticação sendo um no *ISP* antes de estabelecer o túnel e outro quando é realizada a conexão com gateway, diferente do PPTP, o L2F possuí tunelamento independente do IP sendo capaz de trabalhar com outros meios como por exemplo: *ATM* e *Frame Relay*. O L2F sempre presume que a rede privada do cliente estará atrás de um gateway podendo ser um roteador ou um firewall (VALENCIA ET AL, 1998)

A aplicação funciona da seguinte forma, primeiro é necessário que o usuário estabeleça uma conexão PPP com o servidor de acesso à rede (NAS) do ISP, após realizada a conexão, o NAS estabelece um túnel L2F com o gateway e então ocorre a autenticação pelo gateway como o nome de usuário e senha e estabelecida a conexão PPP ou *serial line* IP (SLIP). Esta autenticação é realizada quando uma sessão VPN-L2F é estabelecida. O cliente, o NAS e o gateway da internet utilizam um sistema triplo de autenticação via CHAP.

2.1.3 L2FP (Layer Two Tunneling Protocol)

Um padrão para protocolos tipo tunelamento reuniu as melhores características de dois protocolos existem para criar o L2FP, sendo eles PPTP e o antecessor L2F. Este protocolo possuí flexibilidade e a escalabilidade do protocolo IP que foi junto com a privacidade do *Frame Relay ou ATM*, permitindo desta forma que os serviços de redes sejam encaminhados nas terminações do túnel.

O L2TP (TOWNSLEY ET AL; 1999) realiza o encapsulamento de pacotes do tipo PPP, podendo então fazer uso dos mecanismos de autenticação PPP, também provê suporte para autenticação do túnel, permitindo que ambas as extremidades sejam autenticadas. Desta forma o protocolo em questão foi criado para atuar em dois modos de tunelamento, sendo eles:

- Voluntário: Iniciado pelo computador, sendo mais flexível, trânsito que pode discar para qualquer outro provedor de acesso já que o provedor de acesso não participa da criação dos túneis, este pode percorrer vários servidores sem necessitar de uma configuração específica.
- Compulsório: Neste modo é criado automaticamente e iniciado pelo servidor de acesso a rede sob a conexão discada. Por isso é necessário que o servidor de acesso à rede seja pré-configurado para que seja possível saber a terminação de cada túnel baseado nas informações de autenticação do usuário.

O funcionamento se baseia em um concentrador de acessos L2TP localizado no *ISP*, troca de mensagens PPP com o servidor de rede L2TP para criação dos túneis. Então o L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão, após isso os quadros encaminhados pelos usuários são aceitos pelo *ISP*, encapsulados em pacotes L2TP e encaminhados pelo túnel, então no gateway de destino os quadros L2TP são desencapsulados e os pacotes originais são processados pela interface apropriada.

2.1.4 IPsec

O IPsec foi criado para suprir a carência de segurança existente na época do protocolo IP, sendo responsável por sua criação o Grupo de Trabalho de Segurança IP do IEFT, criando assim uma alternativa para a nova geração de IPv4 e IPv6. De acordo com (VPN: Protocolos e Segurança / Borges; Fagundes; Cunha ;2019) este conjunto de protocolos fornece principalmente serviços de integridade, autenticação, controle de acesso, e confidencialidade permitindo interoperabilidade com protocolos de camadas superiores como TCP, UDP, ICMP, etc.

2.1.5 SSL (Secure Socket Layer)

Este protocolo foi criado pela empresa Netscape Communications, para garantir a segurança entre aplicações do tipo cliente/servidor, evitando desta forma influências externas e falsificações de dados e “escutas”. Quando foi padronizado o protocolo recebeu o nome inicial de Transport Layer Security, o TSL.

Este atua entre as camadas de transporte do TCP e aplicação, podendo rodar também sobre outros protocolos como: Telnet, FTP e SMTP, além de outros.

A outra extremidade da conexão realizada a função oposta e junta os fragmentos as invés de “separá-las” e entrega a mensagem completa para os protocolos posteriores.

2.2 Gateway

Para Shinder (2003, p.231), um gateway é um sistema que conecta dois ou mais seguimentos da mesma rede por meio de duas ou mais interfaces. Os motivos para essa configuração são normalmente situações como usuários dial-up que não precisam de conexões dedicadas ou seguimentos da mesma rede que são divididos por algum obstáculo físico no qual um link de saída adicional para internet não é necessário ou não é desejado**.**

2.3 Modem

Segundo Jennings (1986), um modem é um tipo de dispositivo que converte vários sinais digitais em analógicos e vice-versa. As organizações padrões utilizam a abreviação genérica de DCE (Data Circuit Terminating Equipament) para descrever um computador terminal ou qualquer dispositivo conectado em um modem. O modem tem duas interfaces sendo elas: DCE para uma interface de circuito (linha) analógico e uma DCE para DTE (Multi Wire Digital Interface)

As organizações se referem a cada fio (condutor) no Multi Wire Digital Interface como um “interchanged circuit”. Circuitos intercambio são usados para uma mistura de transferência de dados, e para fins de controles e contagens.

2.4 Certificados digitais

Para Afshar (2015), o certificado digital é um documento eletrônico que fornece informação para comprovar a identidade de uma entidade. Ela liga a identidade de uma entidade a uma chave pública. Certificado digital contém algumas informações padrões, como por exemplo o nome da entidade que detém o certificado, chave pública, período válido e a assinatura digital da certificadora autorizada. Desta forma podemos nos atentar aos principais e mais conhecidos tipos de certificados, sendo eles: pessoal, organizacional, de servidores, desenvolvimento e governamental. Neste trabalho o certificado abordado foi o do tipo organizacional.

3 MATERIAIS E MÉTODO

O trabalho consiste na análise de dois artigos que validam a eficiência da VPN em ambientes corporativos, e demonstra suas falhas em situações distintas apresentando também seu comportamento no instante do acesso remoto e abordando os tipos de protocolos de criptografia que são utilizados na arquitetura de software da aplicação.

O artigo **Análise de segurança do acesso remoto VPN** (NAKAMURA, GEUS; 2000), demonstra que a VPN é uma ferramenta eficaz para manter a rede segura, contanto não deve ser utilizada em todos os cenários. O artigo apresenta duas situações onde a VPN pode abrir uma brecha ainda maior para que se ocorra ataques na rede, sendo eles: quando utilizada como gateway e quando temos um modem trabalhando em conjunto com a VPN. Como ponto positivo podemos concluir que a VPN é um ótimo investimento já que através dela é possível diminuir a infraestrutura e assim enxugar os gastos de forma considerável. Um ponto alto do artigo é quando ele detalha o funcionamento da VPN do momento de sua instalação, até o seu funcionamento, onde nesta parte observamos a importância da chave simétrica em sua instalação.

Podemos observar que a VPN se torna ainda mais segura quando atua juntamente com o firewall, minimizando consideravelmente o risco de ataques bem sucedidos na rede, é importante destacar que o artigo deixa claro que a VPN é importante porém é necessário uma política de segurança alinhada e atual e que a mesma seja seguida pelo usuário que é o elo fraco quando falamos de segurança da informação. Não foram realizados testes neste artigo, desta forma concluímos que os autores focaram em demonstrar o funcionamento da VPN em uma rede corporativa não específica demonstrando assim seu comportamento em cenários não práticos, comprovando com prós e contras sua eficiência, os autores não focaram em demonstrar o comportamento da VPN quando a mesma está sob ataque.

O artigo **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA, 2019), busca uma indicação dos protocolos utilizados na conexão VPN e as vantagens e desvantagens de cada um, a análise será realizada em cima dos seguintes protocolos: PPTP, L2F, L2TP, IPsec e SSL.

Nos atentemos para o seu foco principal nos protocolos que compõe a VPN, e explica, desde sua criação até a sua forma de funcionamento. Os autores explicam de forma breve os tipos de VPN e os ambientes, sendo eles três e através de um estudo em cima de cada protocolo chegando a dois que foram

considerados seguros, estes não demonstraram instabilidade como podemos observar com os demais, sendo: IPsec e SSL. Foram abordadas as características destes protocolos e podemos observar que os dois utilizam certificados digitais, sendo o IPsec mais estável que o SSL. Não foram realizados testes práticos neste artigo, foi realizado um profundo estudo acerca dos protocolos disponíveis no mercado e após análise foi comprovado que dois protocolos atendiam a demanda da VPN, sem apresentar tantos erros.

Porém, existe uma possibilidade de falha nos protocolos. Ambos os artigos concordam que a VPN é uma excelente ferramenta, desde que aja em conjunto com um firewall e uma política de segurança.

4 RESULTADOS E DISCUSSÕES

Após analises realizadas podemos observar que ambos os artigos concordam que com o fato da VPN ser um meio de garantir a seguridade na transmissão de dados, entretanto ambos os artigos concordam que as falhas podem ocorrer na implantação dos protocolo, na implantação da aplicação, esta falha pode ser de cunho humano ou um problema na configuração de um protocolo no sistema escolhido, temos como ponto alto em ambos os artigos o protocolo IPsec, este protocolo é tido como um dos mais eficientes quando falamos de criptografia e autenticação de cliente/servidor.

O artigo **Análise segurança acesso remoto VPN** (NAKAMURA; GEUS; 2000) aborda a VPN como um ótimo meio para contenção de gastos já que não se faz necessário uma estrutura de grande porte para que ocorra a sua implantação.

A Tabela 1 destaca os pontos dos protocolos SSL e IPsec.

Tabela 1. SSL e IPsec.

SSL	IPSec
Usa tokens ou certificados digitais	Usa tokens ou certificados digitais
Forte, mas variável pois depende do browser	Forte e constante, definido na implementação
Complexidade de implementação moderada	Complexidade de implementação alta
Escalabilidade alta	Escalabilidade muito alta
Segurança total moderada, pois pode ser usada para criar regras	Segurança total alta, pois define cada dispositivo e implementações

Entretanto existe o questionamento sobre a eficiência da VPN, quando os autores de **Análise de segurança em acesso remoto VPN** (NAKAMURA; GEUS; 2000) citam que "*A efetividade da segurança porém é colocada sob questionamento, uma vez que o backbone da comunicação é uma rede pública, e o que está em jogo são as informações e os recursos da organização.".*

Já o artigo **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA; 2019) afirmam que os protocolos PPTP, L2F, L2FP, são protocolos falhos ou deficientes que podem ser utilizados na conexão VPN, eles demonstrar sua ineficácia através dos pontos presentes na Tabela 2.

Tabela 2. PPTP, L2F e L2FP.

Protocolos		
PPTP	L2F	L2FP
Processo de negociação realizado de forma fraca	Não define criptografia	Não possui processos para gerenciamento de chaves criptográficas
Processo de negociação realizado de forma fraca	Não define encapsulamento de dados	Não é recomendado o uso deste tipo de protocolo em uma rede insegura como a internet
Não existe negociação no período de negociação dos parâmetros da conexão		Deve ser combinado com outro protocolo que corrijam as vulnerabilidades acima

Sabemos que um dos principais motivos para a implantação da VPN no meio corporativo é para que se tenha ou se mantenha a segurança na transmissão de dados entre cliente/servidor. Ambos os artigos comentam brevemente sobre os diversos tipos de *VPN's* que existem sendo elas: host-to-host, host-gateway, gateway-gateway. A Tabela 3 **apresenta** o papel de cada topologia da VPN.

Tabela 3. Tipos de arquitetura da VPN

Host-to-Host	Comunicação entre dois microcomputadores separados remotamente podendo ou não estarem em uma mesma rede.
Host-Gateway	Comunicação entre um microcomputador e uma rede específica.
Gateway-Gateway	Comunicação entre duas redes de uma mesma companhia.

Para o artigo **Análise de segurança em acesso remoto VPN** (NAKAMURA; GEUS; 2000) um ponto importante a ser observado é quando abordamos o tópico certificado digital e chave assimétrica, estes possibilitam a captura do arquivo de configuração da VPN, podendo ocasionar em uma VPN ineficaz dando a possibilidade de se executar o roteamento de pacotes.

O artigo **VPN: Protocolos e Segurança** (BORGES; FAGUNDES; CUNHA; 2019) foca nos principais protocolos utilizados nas VPN's, e retrata especificamente 5 protocolos que são utilizados na tecnologia ou que ajudaram em sua implementação, como já citamos os autores relatam sobre a efetividade dos seguintes protocolos PPTP, L2F, L2TP, IPSec, SSL.

Porém ambos os trabalhos têm em comum a especificação do protocolo IPsec, como um tipo de autenticação de extrema confiabilidade quando se trata da tecnologia *VPN's.* O protocolo IPSec tem como principal funcionalidade o serviço de integridade, autenticação de controle de acesso e confidencialidade, permitindo interoperabilidade com alguns protocolos de camadas superiores.

5 CONCLUSÕES

O seguinte trabalho buscou comprovar a eficiência da VPN em uma rede corporativa com base em estudos sobre VPN's, segurança e os seus protocolos. Após a análise dos artigos conseguimos comprovar que a VPN é uma aplicação para proteção da rede prevenindo invasões e possíveis perda de dados, desde que utilizada com outra ferramenta para complemento como por exemplo um firewall. Devemos deixar claro que como toda e qualquer ferramenta a VPN está exposta a erros e falhas, que podem ser de via humana, como por exemplo, um erro na implementação da aplicação ou erro na configuração da chave assimétrica.

5.1 TRABALHOS FUTUROS

Para trabalhos futuros, a execução de testes práticos seriam necessários, como por exemplo: montar um ambiente cliente/servidor e executar a implantação de uma VPN, com testagem de chaves assimétricas e assim submeter a rede ataques para verificar o seu comportamento.

REFERÊNCIAS

BORGES F, FAGUNDES B.A, CUNHA G.N. VPN: Protocolos e Segurança

Larry L. Peterson e Bruce S. Davie; Redes de computadores: uma abordagem de sistemas /tradução de Multinet Produtos - Rio de Janeiro: Elsevier, 2013

Jennings F; Pratical data communications: modems, networks and protocol, Blackwell Scientific Publications, 1986

MARSIC, I. Computer network performance and quality of service; New Jersey: Rutgers University, 2013

NAKAMURA, E.T, E GEUS P.L. Análise de segurança do acesso remoto VPN

NAKAMURA, E.T, E.; GEUS, P.L. Segurança de redes de computadores: Em ambientes corporativos 3. ed. São Paulo: Novatec, 2011.

Reshma. A. Digital Certificates (Public Key Infrastructure) Indiana State University ,2015.

Shimonski, R. J, Shinder L.D, Shinder T.W, Henmi A.C; The Best Damn Firewall Book Period, p.231, Rockland, MA: Syngress Publishing, Inc, 2003.