UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

DESCRIÇÃO E ANÁLISE ESTATÍSTICA DE PROTOCOLOS DE REDES VIRTUAIS PRIVADAS UTILIZANDO DIFERENTES ABORDAGENS

TRABALHO DE CONCLUSÃO DE CURSO

Guilherme Prestes da Silva

Santa Maria, RS, Brasil
2013

DESCRIÇÃO E ANÁLISE ESTATÍSTICA DE PROTOCOLOS DE REDES VIRTUAIS PRIVADAS UTILIZANDO DIFERENTES ABORDAGENS

Guilherme Prestes da Silva

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores do Colégio Técnico Industrial de Santa Maria, da Universidade Federal de Santa Maria (UFSM,RS), como requisito parcial para obtenção de grau de Tecnólogo em Redes de Computadores.

Orientador: Prof. Ms. Rogério Correa Turchetti

Santa Maria, RS, Brasil

2013

UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Conclusão de Curso

DESCRIÇÃO E ANÁLISE ESTATISTICA DE PROTOCOLOS DE REDES VIRTUAIS PRIVADAS UTILIZANDO DIFERENTES ABORDAGENS

elaborado por
Guilherme Prestes da Silva

como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA:

Rogério Corrêa Turchetti
(Presidente/Orientador)

Ms. Walter Priesnitz Filho (UFSM)

Pós-Dr. Viviane Cátia Köhler (UFSM)

Santa Maria, 22 de Julho 2013.

DEDICATÓRIA

Aos meus pais, Claudio Prestes da Silva e Rosângela Maria Prestes da Silva, pelos esforços imensuráveis durante suas vidas, pela compreensão, afeto, respeito e amor e, sobretudo, ao verem-me atingir este nível de graduação, realizarem um objetivo tão sonhado.

Ao meu irmão, Maurício Prestes da Silva, que desde sua adolescência incentivou-me, mesmo que indiretamente, a gostar e entender as “coisas” da computação.

AGRADECIMENTOS

Rogério Correa Turchetti, orientador deste trabalho de conclusão, por entender que a vida nem sempre nos rega com momentos felizes e que, portanto, precisamos dar um passo mais curto e esperarmos o momento certo. Pela dedicação e atenção que sempre esteve disposto a dar-me nas correções deste trabalho.

Cristiélle Pontes Machado, por entender que um futuro melhor passa necessariamente pelos esforços do presente, por fins de semana distantes e pela priorização dos estudos. Pelo carinho, afeto, amor e respeito que você sempre esteve disposta a dar-me em todas as ocasiões.

Humberto Boeira Poetini, fiel e incansável amigo, presente desde as primeiras provas de cálculo até as últimas linhas deste trabalho. Companheiro de chimarrão e ouvinte atento às conspirações, dilemas e aspirações deste amigo; o braço que muitas vezes sustentou-me da ausência da família e a mão que, sempre estendida, jamais negou-me um mate e uma ajuda.

Carla Juliana Biesdorf, por mostrar-me o curso de Redes de Computadores e convencer-me de que era possível. Por todas as horas que esteve ao lado para sustentar, ouvir e motivar-me a seguir nesta empreitada. Ainda, por há mais de 10 anos atrás ir comigo a Santa Maria desbravar o mundo.

Walter Priesnitz Filho, coordenador do curso, pelo excelente trabalho, pelo esforço em fazer as coisas serem melhores, mas principalmente por estar presente, disponível e entender que o caminho da vida é tortuoso e implacável.

Divar e Clécio Lopes, os “padrinhos” de minha graduação, atentos ao meu bem-estar em Santa Maria e também por comporem o alicerçe emocional que tanto eu quanto minha família necessitamos nos últimos anos.

Aos demais professores, colegas e funcionários do Colégio Técnico Industrial de Santa Maria.

RESUMO

Trabalho de Conclusão de Curso
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

DESCRIÇÃO E ANÁLISE ESTATÍSTICA DE PROTOCOLOS DE REDES VIRTUAIS PRIVADAS UTILIZANDO DIFERENTES ABORDAGENS

AUTOR: GUILHERME PRESTES DA SILVA
ORIENTADOR: ROGÉRIO CORREA TURCHETTI
Data e Local da Defesa: Santa Maria, 22 de Julho de 2013.

As redes de computadores e suas inúmeras aplicações caminham conjuntamente com as demais áreas do conhecimento, especialmente nos últimos vinte anos, em busca de soluções que proporcionem à sociedade ferramentas, aplicações, padrões e facilidades na comunicação de dados. O avanço contínuo e acelerado das tecnologias e suas inserções igualmente dinâmicas no cotidiano das pessoas e organizações traz à luz do debate e da pesquisa a segurança na troca das informações. Utilizando-se como base as estatísticas descritiva e probabilística buscou-se descobrir diferentes características de transmissão de dados utilizando-se redes virtuais privadas, afim de se obter dados suficientes para uma análise real e conclusiva desses protocolos. O conhecimento de diferentes modelos estatísticos aliados à uma intensa pesquisa teórica dos protocolos de redes virtuais privadas, permitiram a execução e realização deste trabalho. A análise dos resultados revela as diferentes características e aplicações que estes protocolos se aplicam, podendo, este trabalho, auxiliar na escolha de soluções em redes virtuais privadas.

Palavras-chave: redes de computadores, comunicação de dados, redes virtuais privadas.

ABSTRACT

Graduation Conclusion Work
Technology in Computer Networs Graduation Course
Universidade Federal de Santa Maria

DESCRIPTION AND STATISTICAL ANALYSIS OF PROTOCOLS OF VIRTUAL PRIVATE NETWORKS USING DIFFERENT APPROACHES

AUTHOR: GUILHERME PRESTES DA SILVA
ADVISER: ROGÉRIO CORREA TURCHETTI
Defense Place and Date: Santa Maria, July, 22nd 2013.

Computer network and its several applications evaluate together with other knowledge areas, specially in the last twenty years, seeking solutions which give tools, applications, patterns and easiness on data communication to society. Continuous and fast development of technologies and their equally dinamic insertion on people's daily life and companies brings to the light of debate and research the safety on changing information. Using as basis either descriptive or probabilistic statistic this work has sought to find out different characteristics of data transmission using virtual private network, to collect enough data to a real and conclusive analysis of these protocols. The knowledge of different statistical models coupled with an intense theoretical research of virtual private networks protocols allowed the implementation and execution of this work. Analysis of the results reveal the different features and applications that these protocols applied themselves, allowing this work to help choosing solutions in virtual private networks.

Keywords: computer network, data communication, virtual private network

ÍNDICE DE ILUSTRAÇÕES

LISTA DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

VPN	Virtual Private Network / Rede Privada Virtual
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
PPP	Point-to-Point Protocol / Protocolo Ponto-a-Ponto
PPTP	Point-to-Point Tunneling Protocol / Protocolo de Tunelamento Ponto-a-Ponto
L2F	Layer Two Forwarding / Encaminhador da camada dois
L2TP	Layer Two Tunelling Protocol / Protocolo de Tunelamento da camada dois
IPSec	Internet Protocol Security / Segurança do Protocolo de Internet
SSTP	Security Socket Tunneling Protocol / Protocolo de Tunelamento de Segurança de Soquetes
RFC	Request for Comments / Pedido para comentários
LCP	Link Control Protocol / Protocolo De Controle de Enlace
NCP	Network Control Protocol / Protocolo De Controle de Rede
OSI	Open Systems Interconnection / Interconexão de Sistemas Abertos
TCP	Transmission Control Protocol / Protocolo de Controle de Transmissão
UDP	User Datagram Protocol / Protocolo de Datagramas
PPPD	Point-to-Point Protocol Daemon / Servidor do Protocolo Ponto-a-Ponto
ISP	Internet Service Provider / Provedor de Acesso à Internet
ATM	Assynchronous Transfer Mode / Modo de Transferência Assíncrona
PAP	Password Authentication Protocol / Protocolo de Autenticação de Senha
CHAP	Challenge Handshake Authentication Protocol / Protocolo de Autenticação de Handshake de Desafio
ETD	Equipamento Terminal de Dados
DES	Data Encryption Standard / Padrão de Criptografia de Dados
IKE	Internet Key Exchange Protocol / Protocolo de Troca de Chaves de Internet
ISAKMP	Internet Security Association and Key Management Protocol / Protocolo de Gerenciamento de Chaves e Associação de Segurança
PFS	Perfect Forward Secrecy / Sigilo Avançado Perfeito
SSL	Security Socket Layer / Protocolo de Camada de Sockets Segura
HTTP	Hyper Text Transfer Protocol – Protocolo de Transferência de Hipertextos
FTP	File Transfer Protocol / Protocolo de Transferência de Arquivos
SMTP	Single Mail Transfer Protocol / Protocolo de transferência de correio simples
HTTPS	Hyper Text Transfer Protocol Secure – Segurança do Protocolo de Transferência de Hipertextos
EAP – TLS	Extensible Authentication Protocol – Transport Layer Security / Protocolo de Autenticação Extensa – Segurança da Camada de Transportes
Ipv6	Internet Protocol version 6 / Protocolo de Internet versão 6
DMZ	Demilitarized Zone / Zona Desmilitarizada
RAM	Read Acess Memory / Memória de Acesso à leitura
NTP	Network Time Protocol / Protocolo de Tempo da Rede

LISTA DE ANEXOS E APÊNDICES

SUMÁRIO

1 INTRODUÇÃO

"As inovações tecnológicas pós revolução industrial, especialmente dadas pelo maior conhecimento da administração geral, viram em Henry Ford primeiramente, mas especialmente pós Segunda Guerra Mundial, a necessidade da troca de informações e, tão importante quanto, a inovação tecnológica rápida e segura" (VASCONCELLOS, 1972, p. 34).

Como resultado da evolução surge, a partir da década de 1990 com mais força, a internet, uma rede virtual capaz de conectar qualquer computador autônomo, em qualquer lugar. Fez-se necessário, pois, que a coleta, transporte, processamento e armazenamento de informações fossem dadas de maneira segura e confiável. Empresas e suas filiais espalhadas pelo mundo todo demandam convergência de dados, rapidez e confiabilidade no movimento da informação, por exemplo.

Segundo dados do *CERT*[1]*,* casos de atividades maliciosas, negação de serviço, invasões, comprometimento de servidores e fraudes registraram 399.515 incidentes em 2011, sendo este último responsável por 34,65% dos incidentes no período Abril – Junho de 2012. De maneira análoga, em *Leading Statistics Portal*[2], o número médio de dias para "resolver" um ataque cibernético contra companhias americanas em 2011 chegou a 42*,* enquanto que os danos financeiros às companhias chegaram, em 30% dos ataques bem-sucedidos, a 200.000 – 300.000 dólares por ataque*.*

Geralmente há uma relação inversa de proporcionalidade entre tráfego de dados *versus* segurança da informação. Diversas são as ferramentas geradoras de criptografias, certificações digitais, chaves simétricas e assimétricas, e quanto mais *bits* precisarem ser inseridos/retirados em um cabeçalho de pacote de dados, maior o processamento e, consequentemente, menor a otimização do canal de comunicação. Para tanto, protocolos de redes privadas virtuais devem buscar a melhor relação entre confiabilidade na entrega dos pacotes e velocidade da informação.

Para tanto, protocolos de redes privadas virtuais devem buscar a melhor relação entre confiabilidade na entrega dos pacotes e velocidade da informação. Isso justifica-se através dos diversos trabalhos que tratam este assunto, como *Kosta, Dalal e Jha* (2010), *Gendorf* (2006) e *Peña e Evans* (2000).

1 *www.cert.br*
2 *www.statista.com*

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Analisar os diferentes protocolos de redes privadas virtuais, desenvolvendo cenários específicos de troca de informações, afim de buscar dados estatísticos que promovam uma comparação entre as diferentes soluções.

1.1.2 Objetivos Específicos

- Promover a troca de dados entre dois equipamentos terminais, implementando redes privadas virtuais;
- Coletar dados estatísticos suficientes nos diversos cenários;
- Analisar os dados obtidos e compará-los de acordo com critérios pré-definidos;
- Elaborar um estudo sobre diferentes protocolos de comunicação para uso de VPNs;
- Buscar o protocolo que mais se adapta nos diversos cenários considerando o objetivo de sua aplicação.

2 METODOLOGIA

As comunicações de dados entre dois ou mais equipamentos terminais, com ou sem um nó central, constituem a base para sustentar o maçico tráfego de informações do mundo globalizado. Utilizar as diferentes topologias e os mais diversos *hardware* afim de alcançar êxito nas comunicações torna qualquer experimento científico necessário para simular e confrontar resultados adquiridos em um ambiente restrito e controlado com aqueles que ocorrem nas comunicações reais.

Torna-se assim mais simples buscar pequenas características, falhas, erros e análises dos dados, conhecer melhor os equipamentos e finalmente atingir um cenário eficiente e o mais verossímil possível, corroborando ou não com os objetivos do projeto.

Na busca por uma comunicação ao mesmo tempo simples e confiável buscou-se a montagem de um cenário com dois equipamentos terminais de dados e um dispositivo centralizador (o qual é o responsável pelo início, manutenção e finalização da sessão da rede privada virtual). Os diferentes protocolos de tunelamento e as respectivas criptografias, a definição de ferramentas de captura e análise dos dados para que a parte estatística seja a mais precisa possível, constituem igualmente processos vitais para que as soluções propostas atingam a máxima fidelidade.

A análise estatística, neste trabalho, é puramente uma ferramenta necessária para traduzir números e dados em gráficos e TABELAS que auxiliem em um entendimento profundo de desempenho de VPNs. Bem como a configuração das redes privadas virtuais, *scripts,* arquivos de configuração e demais elementos necessários para o estabelecimento do canal de comunicação não são elementos tratados como fundamentais para o êxito do trabalho. Tanto a estatística quanto a configuração das redes são suportes para alcançar-se dados suficientes para uma análise.

Os protocolos avaliados neste trabalho são: PPTP, L2TP com IPSec e OpenVPN, e para cada uma destas abordagens o estabelecimento de canais de comunicação com tráfego de dados de 128, 256, 512 e 1024 *bytes*. Para cada um destes cenários foram efetuadas três coletas de 600 pacotes – 1 pacote por segundo – e extraída a média aritmética dos tempos de transmissão dos pacotes de mesma ordem numérica em cada comunicação. Dessa forma, diminiu-se a chance de que dados distorcidos ou erros no canal possam revelar um comportamento não condizente com a realidade do experimento.

3 PROTOCOLOS PARA A IMPLEMENTAÇÃO DE UMA VPN

Para a implementação de uma VPN existem diferentes protocolos de tunelamento disponíveis. Segundo *Filho* (2006, p. 51) os principais protocolos de encapsulamento de pacotes são: PPP, PPTP, L2F, L2TP, *IP Security* (IPSec), SSTP e OpenVPN.

3.1 POINT-TO-POINT PROTOCOL (PPP)

O protocolo PPP, desenvolvido e padronizado pela RFC 1548[3] (1993), não é propriamente um protocolo capaz de estabelecer uma VPN. A internet, desde sua origem, necessita de protocolos capazes de gerar uma comunicação fim-a-fim com algum nível de controle, capazes de, por exemplo, manter um enlace entre dois roteadores ou entre um modem doméstico e um provedor de serviços de internet. Para tanto, este protocolo dispõe de quatro características básicas e essenciais para que uma rede virtual privada possa ser estabelecida:

- enquadramento de pacotes e detecção de erros;
- campo de controle de 8 bits, conforme FIGURA 1;
- LCP, do inglês *link control protocol*, capaz de estabelecer, manter e finalizar conexões e
- NCP, do inglês *network control protocol,* responsável por negociar as opções da camada de rede.

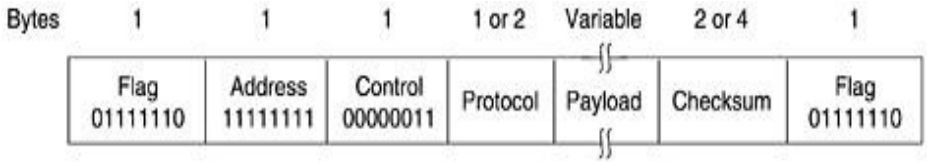


Figura 1 – quadro PPP padrão

Só é possível estabelecer uma VPN caso haja um protocolo do tipo PPP em estado de execução, já que protocolos VPN propriamente ditos são responsáveis por encapsular pacotes, encapsulados ou não por outros protocolos. Conforme será visto nos próximos capítulos, protocolos como o PPTP, L2F e L2TP sobre o PPP criarão túneis em nível de enlace (camada 2 do modelo OSI).

3 http://www.ietf.org/rfc/rfc1548.txt

3.2 POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

Um dos primeiros protocolos de tunelamento que surgiram, o PPTP (RFC 2637[4], 1999) veio incorporado ao Windows NT 4.0 (1995), e fora desenvolvido por um aglomerado de empresas para facilitar o acesso remoto de computadores a uma rede privada. Ao encapsular pacotes PPP, as funcionalidades deste protocolo são agregadas fazendo um túnel até o destino, permitindo assim uma flexibilização do PPTP para lidar com diferentes protocolos.

Permite, portanto, a transferência segura de dados de um computador remoto para um servidor privado ao criar uma conexão VPN em todas as redes de dados baseadas em IP. Diferentemente do protocolo L2TP, este permite que um usuário remoto tenha a possibilidade de escolher o destino do túnel. O PPTP encapsula os quadros PPP em datagramas IP para transmissão pela rede, utilizando uma conexão TCP para o gerenciamento de encapsulamento, conforme mostra a FIGURA 2.

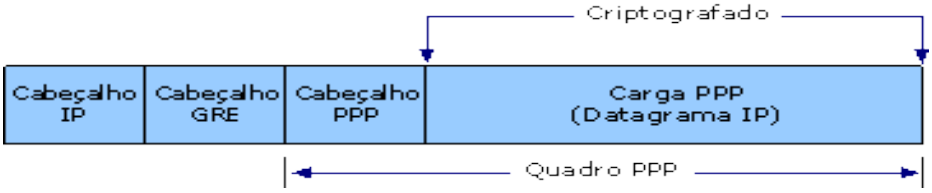


Figura 2: estrutura de um pacote PPTP

Para que uma conexão PPTP seja estabelecida deve-se ter disponíveis um cliente e um servidor PPPD[5]. De acordo com *Borges, Fagundes e Cunha* (2010, p. 3), o cliente PPTP utiliza o PPP para se conectar ao ISP. Nesta etapa o PPP é utilizado para estabelecer a conexão e criptografar os dados. Utilizando a conexão estabelecida pelo PPP, cria-se uma conexão de controle desde o cliente até o servidor PPTP através da Internet. O esquema final, portanto, é mostrado na FIGURA 3.

4 http://www.ietf.org/rfc/rfc2637.txt
5 Do inglês *Point-to-Point Daemon*

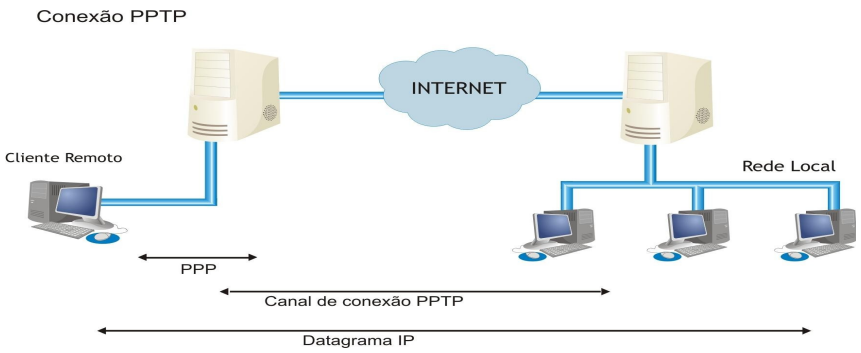


Figura 3: tunelamento PPT

3.3 LAYER TWO FORWARDING

Definido pela RFC 2341[6], este protocolo de tunelamento – desenvolvido pela *Cisco Systems* – diferencia-se por não depender do IP, trabalhando assim diretamente com outros protocolos. Esta característica trouxe uma interessante inovação aos processos de tunelamento e criação de redes virtuais privadas. Segundo *Borges, Fagundes e Cunha* (2010, p. 4) o L2F é capaz de trabalhar com diferentes tecnologias, como redes *ATM* e *Frame Relay* - e também permite mais de uma conexão ao mesmo tempo.

Conforme a FIGURA 4 mostra, este protocolo exige duas autenticações distintas: a primeira delas ao conectar-se cliente - ISP e a segunda ao conectar-se ao ISP – *gateway* passando pela Internet. Nota-se, ainda que, ao não utilizar-se do protocolo IP, um canal direto é gerado entre cliente – ISP – servidor de tunel – gateway.

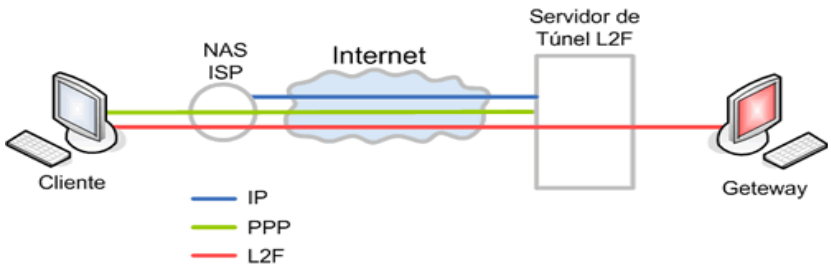


Figura 4: Tunelamento L2F

Mais especificamente, a criação do túnel inicia com o usuário remoto requisitando ao ISP uma conexão PPP. Após o servidor de acesso à rede permitir a conexão, o enlace

6 http://www.ietf.org/rfc/rfc2341.txt

PPP estabelece-se. Utilizando os protocolos PAP[7] e CHAP[8] como meios de autenticação de usuários, um túnel é criado na outra ponta da conexão através de um pedido de comunicação VPN. Desta forma, pacotes PPP podem trafegar normalmente pelo túnel L2F.

Comparativamente, este protocolo pode ser considerado uma melhoria do PPTP, ao permitir que novas tecnologias possam ser utilizadas (não somente IP). Porém, como veremos a seguir, além de uma solução proprietária, este protocolo logo foi sucedido pelo L2TP, por não possuir criptografia e encapsulamento de dados.

3.4 LAYER TWO TUNNELING PROTOCOL (L2TP)

Originalmente definido pela RFC 2661[9], é um protocolo de encapsulamento bastante robusto que repassa o usuário para outros nós da rede, e não necessariamente a ponta final do túnel. Pode-se, portanto, ter-se um túnel L2TP entre um ETD[10] e um roteador, ou entre roteadores. Permite, ainda, que o tráfego IP seja criptografado e enviado através de canais de comunicação tais como *IP, X25, Frame Relay ou ATM.* Este protocolo já permite a criptografia dos datagramas, e assim como os demais protocolos vistos, encapsula pacotes PPP.

Em uma análise geral, o L2TF apresenta-se com aquilo que de melhor extraiu-se do PPP e do PPTP, além de ter sido desenvolvido para operar em dois modos de tunelamento:

1. voluntário: é iniciado pelo cliente remoto, tornando-se assim flexível para usuários móveis;
2. compulsório: criado automaticamente e iniciado/autenticado pelo servidor de acesso à rede (que deve estar pré-configurado).

Utilizando a criptografia DES[11] antes dos dados serem enviados, utiliza pacotes UDP para manter o túnel através de mensagens de manutenção enviadas constantemente entre as duas terminações. Já para fins de autenticação, assim como no

7 Do inglês *password authentication protocol*
8 Do inglês *challenge handshake authentication protocol*
9 http://www.ietf.org/rfc/rfc2661.txt
10 Equipamento Terminal de Dados
11 Do inglês *Data Encryption Standard*

PPTP, utiliza protocolos PAP e CHAP.

3.5 IP SECURITY

A RFC 4301[12] de 2005 especifica e normatiza um conjunto de protocolos afim de garantir segurança, integridade, autenticação, controle de acesso e confidencialidade ao IP. Segundo *Martins* (2000, p. 8), este conjunto de protocolos pode trabalhar de dois modos distintos:

1. modo transporte: é o modo tradicional da imensa maioria das comunicações pela rede. A transmissão dos dados acontece de forma direta e
2. modo túnel: utilizado em gateways que encapsulam os pacotes originais em um novo pacote criptografado IPSec. É sobre este modo de funcionamento que detalharemos túneis IPSec.

Implementando um túnel na camada de rede (IP – camada 3 do modelo OSI), não utiliza como os protocolos antecessores, pacotes PPP. Portanto, fornece autenticação em nível da rede, verificação da integridade de dados, transmissão com criptografia e chaves fortes de 128 bits e um alto grau de segurança na transmissão das informações.

No modo túnel é fornecido ao pacote IP original uma proteção de modo que este pacote seja tratado como o *payload* de um novo pacote (datagrama IPSec). Deste modo pode ser usado para enviar dados encriptados através de um túnel, o que permite enviar dados independentemente da infraestrutura utilizada, não dependendo de configurações prévias nos terminais do túnel. Também acaba por proteger o pacote IP original de ataques, visto que um atacante não tem como descobrir a origem e destino de um pacote, apenas a origem e destino do túnel.

Constituindo o datagrama IPSec, conforme FIGURA 5, são adicionados dois cabeçalhos:

- AH (*autenthication header)*: garante a autenticidade do pacote, não permitindo então que este seja alterado. Previne ataques do tipo *replay*[13]*, spoofing*[14] *e connection hijacking*[15]*.*

12 http://www.ietf.org/rfc/rfc4301.txt
13 Ocorre quando um um atacante copia mensagens em uma comunicação de dados e retransmite estas mensagens para uma das partes.
14 Situação na qual uma pessoa ou programa mascara-se como outra, assim falsificando dados.
15 Situação na qual um atacante intercepta uma comunicação legítima de dados, controlando o tráfego entre os *hosts.*

- ESP (*encapsulation security payload)*: garante que somente destinatários autorizados tenham acesso ao conteúdo do pacote. Previne ataques do tipo *replay,* particionamento de pacotes cifrados e *sniffer*[16].

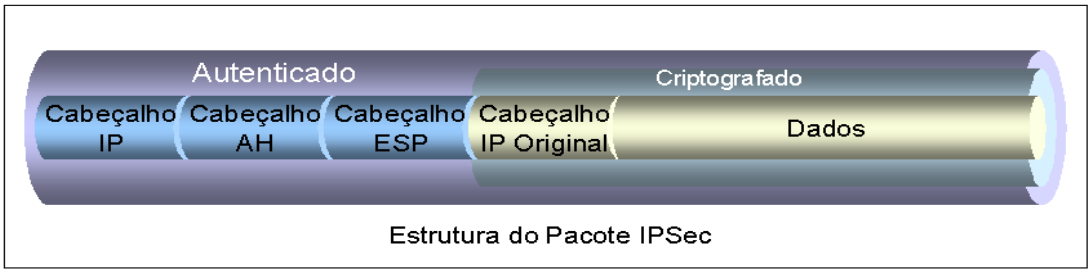


Figura 5: pacote IPSec

Em relação ao gerenciamento das chaves, utiliza o protocolo IKE[17], o qual combina o ISAKMP[18] para definir quais chaves serão determinadas. Ainda pode-se usar o PFS[19], aumentando ainda mais a segurança, visto que esta possibilidade permite que a chave seja gerada a partir do algoritmo de *Diffie-Hellman* (Whitfield, Diffie e Hellman, Martin, 1976), porém apresentando diminuição na performance.

3.6 SECURITY SOCKET TUNNELING PROTOCOL (SSTP) E OPENVPN

Soluções proprietárias, totalmente protegidas, como o protocolo SSTP (RFC 6301[20]), quase sempre encontram semelhantes aplicações, ou por vezes melhores, em código aberto. OpenVPN, assim como SSTP, também faz uso da tecnologia SSL - desenvolvido pela *Netscape Communications* para garantir a segurança entre aplicações cliente/servidor evitando influências externas e falsificação dos dados. Ao ser padronizado recebeu o nome de *Transport Layer Security* (TSL) 1.0 e é o mesmo que o SSL 3.0. O SSL atua entre as camadas de Transporte e Aplicação (TCP), podendo rodar sobre outros protocolos como o HTTP, Telnet, *File Transfer Protocol* (FTP), *Single Message Transfer Protocol* (SMTP) e outros de forma transparente - e funciona em Mac OS, Windows, Linux

16 Quando um atacante analisa dados em uma comunicação, assim aproveitando-se para obter senhas e/ou informações confidenciais.
17 Do inglês *Internet Key Exchange*
18 Do inglês *Internet Security Association and Key Management Protocol*
19 Do inglês *Perfect Forward Secrecy*
20 http://www.ietf.org/rfc/rfc6301.txt

e alguns telefones IP.

Opera em ambas camadas 2 e 3 e tem recursos extras de transporte de quadros Ethernet, IPX e NETBIOS. Pode, ainda, lidar com múltiplos canais gerenciáveis através de uma configuração Telnet, bem como para ligar dois roteadores interligados através de um canal sem-fio (wireless) não-confiável. O protocolo pode acomodar uma larga escala de configurações incluindo acesso remoto, segurança em redes sem fio, soluções em escala de empresa de acesso remoto com balanceamento de carga, controles de acesso refinados e túneis para sub-redes IP.

Outras características deste protocolo são: utiliza encriptação, autenticação e certificação OpenSSL, bem como cifragem, tamanho de chave e uso de chaves simétricas ou assimétricas, configuração de VPNs tanto com IP fixo como IP dinâmico, e autenticação apenas de VPNs. Os pacotes de rede são selecionados unicamente por conta do seu IP de destino. E eles são apenas re-encapsulados sem qualquer manipulação. Assim, o OpenVPN não precisa interferir no processamento da terceira camada, e portanto não precisa ter qualquer módulo implementado dentro do kernel.

O protocolo fornece um mecanismo para encapsular o tráfego PPP através do canal SSL do protocolo HTTPS. O uso do PPP possibilita o suporte a métodos de autenticação fortes, como o EAP-TLS. O uso de HTTPS significa que o tráfego irá passar através da porta TCP 443, usada comumente para acesso à Web. SSL (Secure Sockets Layer) oferece segurança de nível de transporte com recursos aprimorados de negociação de chaves, criptografia e verificação de integridade.

4 SOLUÇÕES EM VPN – MODELOS DE INTERCONEXÃO

De posse das análises bibliográficas dos protocolos para implementação de VPNs, cabe agora definir as soluções existentes, como os modelos de interconexão (tipos de túneis e arquiteturas de conexão) e as topologias. Obviamente que questões como redundância e tolerância a falhas devem sempre ser levadas em consideração ao se implementar tunelamentos em escala corporativa, porém o escopo deste trabalho é analisar critérios relativos aos protocolos de tunelamento.

Segundo Castro (2004, p. 73), *“as soluções para redundância e tolerância a falhas*

em uma rede corporativa são proprietárias, ocasionando na maioria das vezes falta de interoperabilidade, além de manter a empresa amarrada a um determinado fabricante e ainda o custo elevado dos equipamentos." De posse dessas informações, é salutar definir soluções que atendam a critérios como usabilidade, instalação, documentação, atualização e performance e desempenho.

Várias são as formas de conectar dispositivos, *gateways* ou redes com VPN. Como alguns exemplos, pode-se citar um usuário remoto acessando a rede de sua empresa, ou mesmo servidores de banco de dados de um banco atualizando sua base de dados, ou ainda um *gateway* que atende a requisições para autenticação de usuários. Modelos de interconexão, portanto, podem se diferenciar minimamente de acordo com aplicabilidade. Porém, de qualquer maneira, o tipo do túnel que é o responsável por realizar tais conexões deve ser muito bem definido.

4.1 HOST-TO-HOST

Consiste na mais simples implementação de uma VPN, onde em uma ponta do túnel encontra-se um cliente e na outra, o servidor (FIGURA 6). Como exemplos práticos deste uso se pode citar três: a sincronização de dados entre servidores de matriz e filiais de uma empresa; o uso do IPv6 sobre IPSec estabelecendo um canal seguro e o uso do SSL através do *web browser* para acesso ao servidor web dentro de uma DMZ[21].

Figura 6: VPN host to host

21 Do Inglês *Demilitarized Zone*

4.2 HOST-TO-NETWORK

Tipo de tunelamento entre um *host* e um dispositivo como um *gateway* (*switch* ou roteador), configurado para a VPN. Os dispositivos que estão abaixo do *gateway* - e que formam uma LAN[22] - tem uma comunicação transparente com o *host* VPN externo, pois recebem os pacotes já descriptografados pelo *gateway*, bem como os pacotes com origem na LAN só serão autenticados e criptografados se forem destinados para a “nuvem”.

4.3 NETWORK TO NETWORK

Neste tipo de implementação, duas ou mais LANs distintas (redes com IPs diferentes) podem fazer-se transparentes aos dispositivos nelas presentes. Conforme a FIGURA 7, em ambas terminações do túnel encontra-se um *gateway*, responsável por autenticar e criptografar/descriptografar os pacotes. Desta maneira, dispositivos pertencentes a LANs diferentes tem a troca de dados efetuada de maneira transparente, como se entre eles houvesse apenas um roteador.

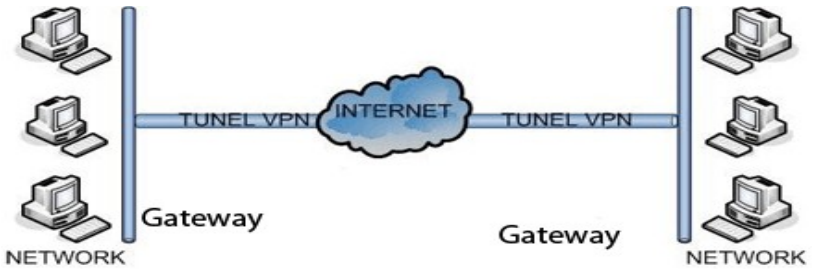


Figura 7: VPN network-to-network

5 AMBIENTE DE TESTES

Segundo Tannenbaum (2003, p. 54), *“as questões referentes ao desempenho são muito importantes nas redes de computadores. Quando centenas de milhares de computadores estão interconectados, são comuns interações complexas que trazem*

22 Do inglês *Large Area Network*

conseqüências imprevistas. Com freqüência, essa complexidade resulta em um fraco desempenho, cujas razões todos desconhecem."

Conforme mencionado anteriormente, em se tratando de desempenho de redes privadas virtuais, parte-se da ideia que quanto mais simples e direta a comunicação dos dados, maiores serão as chances de obterem-se resultados confiáveis. Com a finalidade de realizar os experimentos em um ambiente confinado, ou seja, que não houvesse muitas distorções para a comunicação dos experimentos, como em geral ocorre em uma comunicação via internet, optou-se por utilizar um ambiente, para todos os casos de testes, como descrito a seguir: a rede é composta por um servidor centralizador que fornece acesso e autenticação ao túnel para dois computadores clientes, os quais conectam-se fisicamente via cabo de rede através da interface ethernet até um *switch* logicamente na rede interna, conforme FIGURA 8.

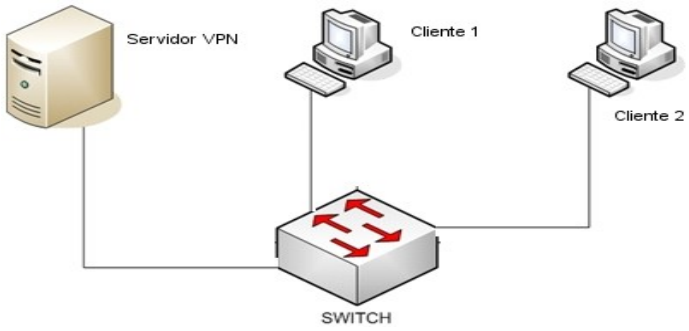


Figura 8: cenário implementado para a realização de todos os casos de testes

Os dispositivos do cenário possuem as seguintes configurações:

- 3 microcomputadores (Servidor VPN, Cliente 1 e Cliente 2) Intel core i3, 3 MB de memória cache, clock de 1,7 GHz, 512MB de memória RAM, DDR3, 1,33 MHz, interface de rede 10/100 mbps; Sistema Operacional Linux Ubuntu 32 bits versão 12.04;
- 1 switch 3com modelo 4210 10/100 mbps e
- cabos de rede categoria 5E.

Objetivando a criação de fluxo de dados e a verificação do seu comportamento, como também a possibilidade de realizar análises estatísticas posteriormente, os seguintes softwares foram adotados:

- *Wireshark*: analisador de protocolos de rede em tempo-real, permite visualizar o tráfego de pacotes nas diferentes interfaces de rede. É considerado programa-padrão para a maioria das aplicações, em ambientes empresarial, industrial e educacional;
- *Rude & Crude:* ferramenta de geração de tráfego de pacotes entre dois terminais de dados, *Rude* é responsável por gerar o tráfego de datagramas e *Crude* tem como função receber estes pacotes e gerar arquivos de *log* e histórico, de acordo com métricas e critérios previamente estabelecidos. Dentre as métricas, pode-se citar vazão, *throughput e* relação pacotes transmitidos-recebidos;
- *NTP: P*rotocolo para sincronização dos relógios dos computadores, define uma maneira para um grupo de computadores conversar entre si e acertar seus relógios, baseados em alguma fonte precisa de tempo, como os relógios atômicos que definem a Hora Oficial Brasileira. Através da consulta de vários outros computadores para saber a hora certa, distinguem-se aqueles que estão corretos dos que estão enganados;
- TOP: provê uma visão dinâmica em tempo real dos processos em um sistema operacional. Mostra informações do sistema bem como lista processos e threads, e a partir da captura de dados como uso do processador, uso de memória, tempo de execução e espera de processos é possível obter dados estatísticos confiáveis.

6 OBTENÇÃO DOS DADOS

De posse do conhecimento necessário dos protocolos, soluções, *hardware* e ferramentas para a melhor avaliação de desempenho das diferentes VPNs, o próximo passo é o estabelecimento do canal de comunicação.

6.1 VPN COM PPTP

A configuração do servidor PPTP, responsável por estabelecer, manter e finalizar uma sessão VPN cliente-servidor encontra-se discriminada no APÊNDICE A. Já o cliente,

para requisitar uma sessão deve configurar sua conexão PPTP através das configurações

de rede, incluíndo o IP do servidor, nome de usuário e senha.

Estabelecidas as sessões, o tráfego de pacotes com o uso da ferramenta *Rude & Crude* deve ser gerado (conforme capítulo 2), bem como a instalação do servidor NTP no servidor VPN deve estar ativa. O APÊNDICE B traz as configurações de ambas ferramentas.

Conforme descrito no capítulo 2, foram efetuadas três coletas subsequentes de 600 pacotes cada:

- coleta 1: 535 pacotes recebidos, 65 pacotes perdidos;
- coleta 2: 541 pacotes recebidos, 59 pacotes perdidos;
- coleta 3: 549 pacotes recebidos, 51 pacotes perdidos.

Após o cálculo das médias aritméticas dos tempos de mesmo número de ordem, e descartando-se tempos com número de ordem superior ao número de pacotes da coleta com menores valores de pacotes recebidos, obteve-se os dados estatísticos de tempo de transmissão descritos na TABELA 1.

Tabela 1: estatística PPTP 128 Bytes

classes	10
amplitude	0,23s
max	2,82s
min	0,55s
média arit	0,86s
mediana	0,76s
moda	0,74s
desvio med	0,19s
variancia	0,10s
desvio pad	0,31s

A distribuição de frequências dos 535 pacotes transmitidos com sucesso, bem como suas probabilidades por classe, pode ser visualizada na TABELA 2.

Tabela 2: distribuição de frequências PPTP 128 Bytes

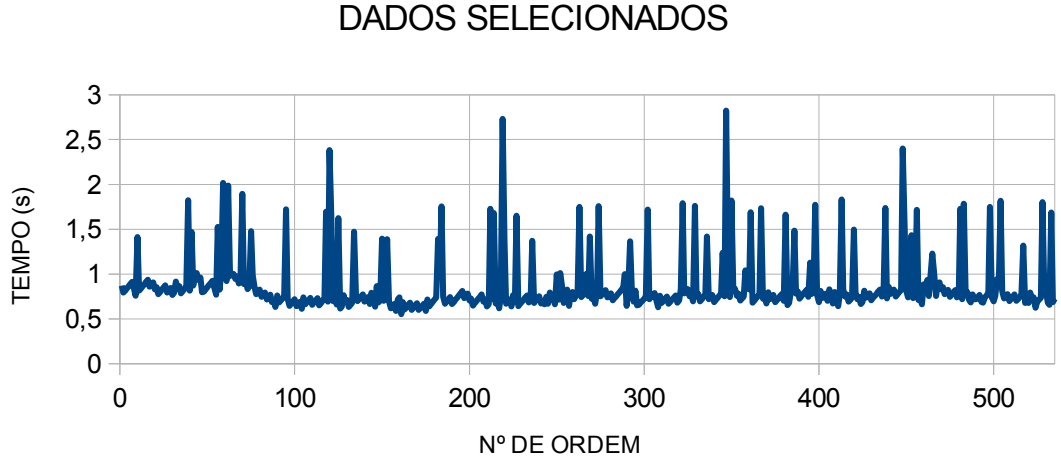
Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência Relativa	Frequência RelativaAcumulada
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	466	466	87,10	87,10
3	1,0 |--- 1,5	1,25	32	498	5,98	93,08
4	1,5 |--- 2,0	1,75	32	530	5,98	99,07
5	2,0 |--- 2,5	2,25	3	533	0,56	99,63
6	2,5 |--- 3,0	2,75	2	535	0,37	100,00

Conforme mostra a TABELA 1, a amplitude das classes deve ser de 0,23s. Este resultado é obtido a partir dos 535 pacotes deste cenário de teste específico. Como este trabalho busca comparar diferentes protocolos em diferentes cenários, optou-se por utilizar amplitudes de 0,5s. Neste cenário, percebe-se nenhuma necessidade dos tempos de respostas a partir da classe 7, o que não irá se verificar em outros cenários, onde tempos de respostas maiores utilizarão classes mais elevadas.

Já a TABELA 2 traz uma série de análises de acordo com as classes: a maioria dos tempos de resposta encontra-se na classe 2 – entre 0,5s e 1s – e somando-se as classes 3 e 4 verifica-se 10% de dados. Logo, tempos de resposta entre 0,5s e 2s contemplam 99,07% do total de pacotes (conforme coluna de frequência relativa acumulada).

Este resultado pode ser melhor visualizado através da ILUSTRAÇÃO 1, que relaciona a distribuição dos tempos de transmissão pelo seu número de ordem. Percebe-se que poucos pacotes excedem o tempo de 1s, ao passo que nenhum deles é menor que 0,5s.

Ilustração 1: tempos de resposta PPTP 128 Bytes



Em termos comparativos, e utilizando-se sempre a mesma metodologia e mesmo cenário de testes, as ILUSTRAÇÕES 2, 3, 4 e 5 trazem uma análise da frequência dos tempos de resposta pelas classes para, respectivamente, pacotes de 128B, 256B, 512B e 1024 bytes.

Ilustração 2: ocorrências por classe PPTP 128 Bytes

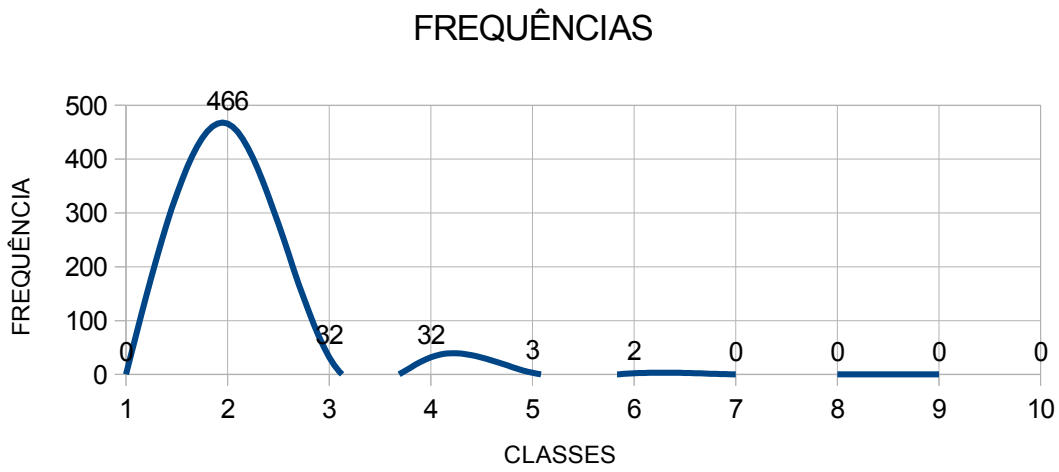


Ilustração 3: ocorrências por classe PPTP 256 Bytes

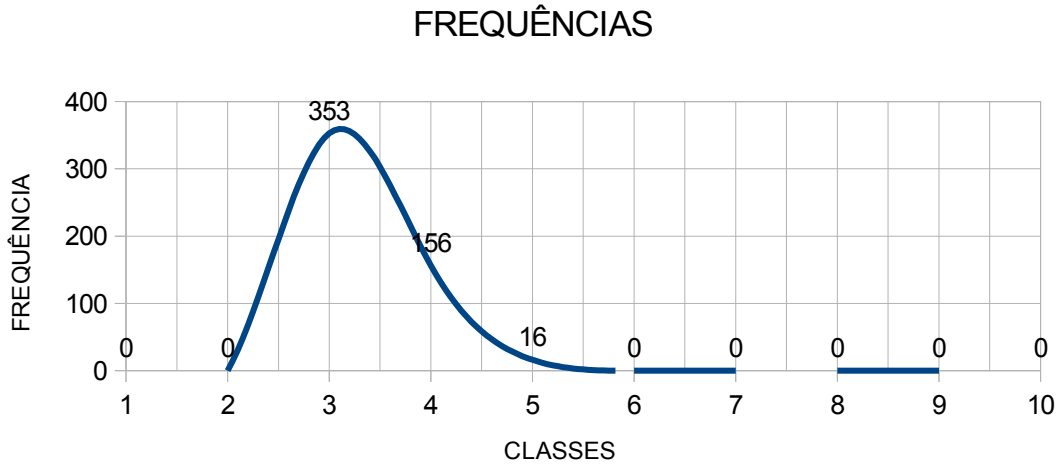


Ilustração 4: ocorrências por classe PPTP 512 Bytes

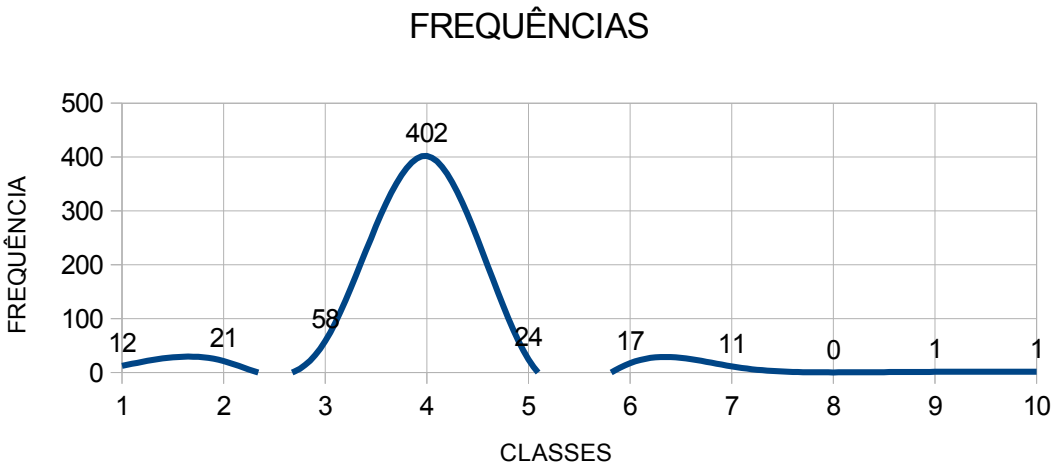
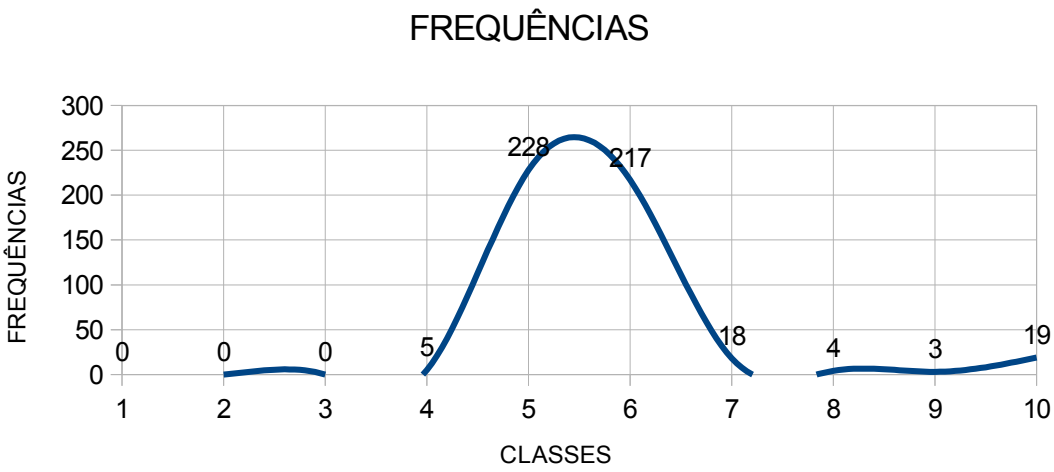


Ilustração 5: ocorrências por classe PPTP 1024 Bytes



A partir das ILUSTRAÇÕES 2, 3, 4 e 5 – que diferenciam-se apenas pelo tamanho dos pacotes -, verifica-se que enquanto 466 pacotes de 128 *bytes* tem entre 0,5s e 1s (classe 2), para pacotes de 256 *bytes*, 353 pacotes encontram-se na classe 3, e, respectivamente, para pacotes de tamanho 512 *bytes* e 1024 *bytes*, 402 pacotes na classe 4 e 445 nas classes 5 e 6. Percebe-se, assim, que em transmissões utilizando-se uma rede privada virtual com protocolo PPTP, o tempo de resposta de uma transmissão aumenta à medida que o tamanho do pacote também aumenta.

Comparando-se a probabilidade acumulada de um pacote estar em uma determinada classe, fica ainda mais evidente que o tamanho do pacote influencia uma transmissão PPTP: as ILUSTRAÇÕES 6, 7, 8 e 9 mostram que:

- para tamanho 128 *bytes*, a partir da classe 3 (tempos de resposta > 1,5s), espera-se que apenas 6,92% dos pacotes encontrem-se nesta região;
- para 256 *bytes*, tempos maiores que 1,5s representam 32,76% dos pacotes;
- para 512 *bytes*, tempos maiores que 1,5s representam 85,33% dos pacotes e para 1024 *bytes*, não haverá ocorrências menores que 1,5s.

Ilustração 6: frequência relativa acumulada PPTP 128 *Bytes*

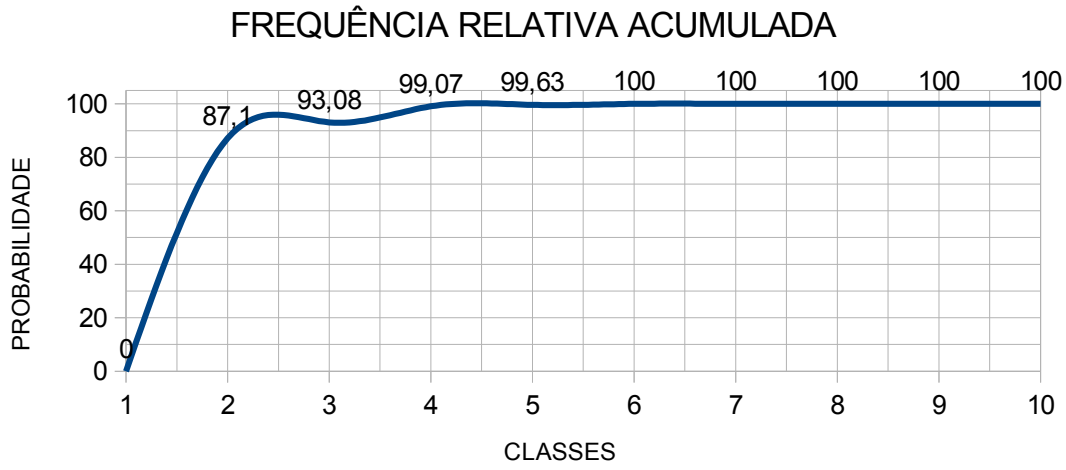


Ilustração 7: frequência relativa acumulada PPTP 256 *Bytes*

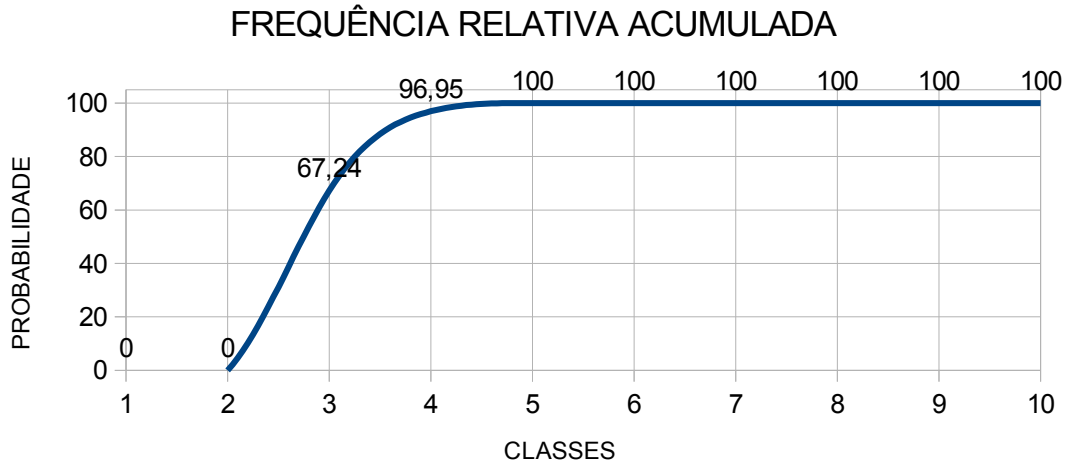


Ilustração 8: frequência relativa acumulada PPTP 512 *Bytes*

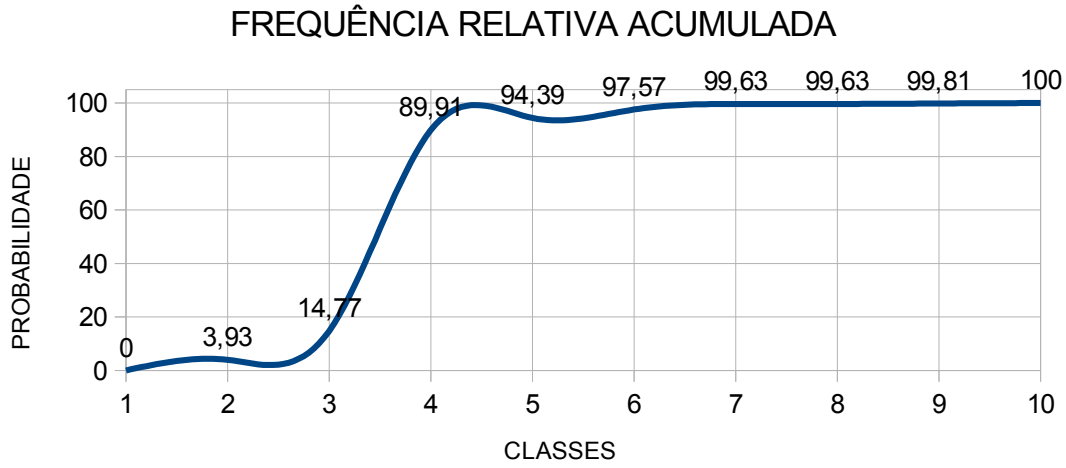
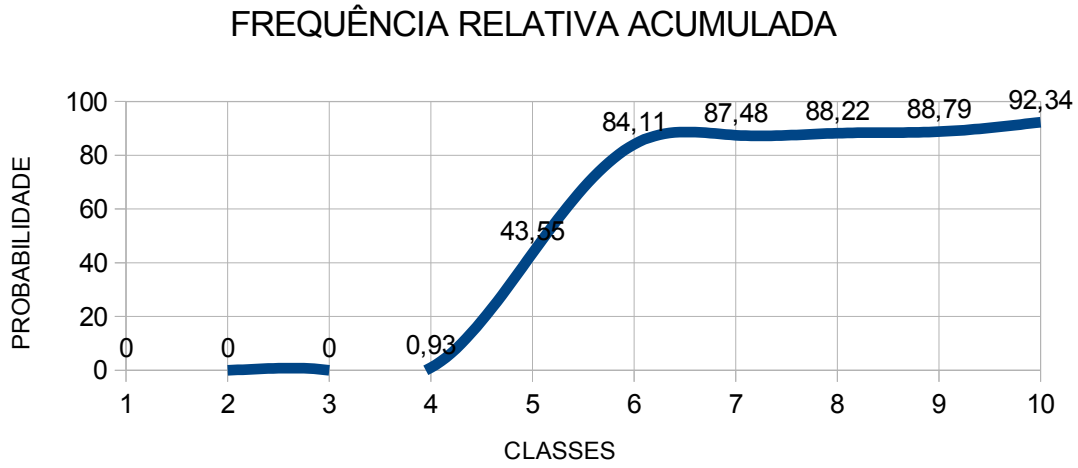


Ilustração 9: frequência relativa acumulada PPTP 1024 *Bytes*



O ANEXO 1 traz outras ilustrações e tabelas referentes aos quatro cenários implementados para o protocolo PPTP (128 *Bytes*, 256 *Bytes*, 512 *Bytes* e 1024 *Bytes*). Diversas análises podem ser feitas a partir destas informações:

- 128 bytes – 0,86s
- 256 bytes – 1,46s
- 512 bytes – 1,66s
- 1024 bytes – 2,84s

Verifica-se, portanto, que o aumento médio dos tempos de resposta não é linear em relação ao tamanho dos pacotes: enquanto um pacote de 1024 *Bytes* é oito vezes maior que um de 128 *Bytes*, o tempo médio de resposta é pouco maior que três vezes.

A TABELA 3 traz uma análise de dados utilizando-se a ferramenta *Wireshark,* a qual possibilita utilizar métricas como *throughput,* tamanho total da transmissão, bem como a hierarquia dos protocolos utilizados na transmissão quando analisada a interface de rede *PPP0.*

Tabela 3: captura de dados na *interface* PPP0

	PPP0			
	128	256	512	1024
Pacotes Rude & Crude	535	525	547	527
Pacotes Wireshark	2475	2481	2496	2507
Relação R&C – Wireshark (%)	21,34	21,16	21,91	21,02
Tamanho Total da Transmissão R&C	72760	134400	284440	543864
Tamanho Total da Transmissão Wireshark	313300	573566	867096	1437724
Pacotes / segundo R&C	0,89	0,88	0,91	0,88
Pacotes / segundo Wireshark	2,45	2,79	2,98	2,26
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	180,08	197,8	314,06	540,09
Bytes / segundo R&C	121,27	224,04	474,19	907,09
Bytes / segundo Wireshark	442,11	552,28	935,75	1223,64
HIERARQUIA DE PROTOCOLOS %				
ICMP	49,05	48,45	47,8	47,39
UDP – DNS	48,84	51,51	49,84	51,62
UDP – DADOS	0,07	0,04	0,04	0,04
TCP	2,04	-	2,32	0,95
Total	100	100	100	100

A partir da TABELA 3 infere-se que a relação de pacotes gerados pelo Rude & Crude e os pacotes que trafegam pela interface *PPP0* é constante (~21%). Este fato explica-se pois para cada pacote ICMP gerado pelo Rude & Crude há a confirmação do recebimento do pacote (*echo request, echo reply).* Há, ainda, o fato de que para todos os casos ocorrem requisições do tipo *DNS* tanto no envio do pacote quanto no envio da confirmação de recebimento deste pacote. Sendo assim, para cada pacote gerado há duas requisições de nome de domínio.

A vazão dos pacotes permanece constante independentemente do tamanho do mesmo (~0,9 pacotes/segundo no Rude & Crude e ~2,5 pacotes/segundo na PPP0). Outro fato interessante é em relação ao tamanho médio dos pacotes: enquanto os pacotes originais gerados pelo Rude & Crude tem apenas 8 *Bytes* de inserção de cabeçalho pelo protocolo TCP (portanto com tamanhos de 136 *Bytes*, 264 *Bytes*, 520 *Bytes* e 1032 *Bytes*), quando estes pacotes trafegam pela interface *PPP0* há a inserção de adicionais 36 *Bytes* no cabeçalho (conforme visto nos capítulos 3.1 e 3.2). Logo, a

relação pacote gerado *versus* pacote transmitido é dada por:

- 128 *Bytes* + 8 *Bytes* TCP + 36 *Bytes* PPP / PPTP = pacote ICMP tamanho 172 *Bytes*;
- 256 *Bytes* + 8 *Bytes* TCP + 36 *Bytes* PPP / PPTP = pacote ICMP tamanho 300 *Bytes*;
- 512 *Bytes* + 8 *Bytes* TCP + 36 *Bytes* PPP / PPTP = pacote ICMP tamanho 556 *Bytes*;
- 1024 *Bytes* + 8 *Bytes* TCP + 36 *Bytes* PPP / PPTP = pacote ICMP tamanho 1068 *Bytes*;

Em relação aos pacotes do tipo *DNS*, o tamanho deste é sempre de 89 *Bytes* independente do tamanho do pacote original.

Já analisando-se o tráfego de pacotes na interface *eth0 (*Tabela 4), infere-se que a relação entre os pacotes gerados pelo *Rude & Crude* e os pacotes que trafegam nesta interface é de aproximadamente 13% em todos os casos. Este número é menor que a mesma relação na interface *PPP0* pois os pacotes já chegam encapsulados na *eth0* e também pois a requisição DNS já está completa. A justificativa para que a quantidade de pacotes que trafegam pela *interface* seja aproximadamente 7 vezes maior que a quantidade de pacote gerados (~4000 na *eth0* e ~500 no *Rude & Crude*) é que, para cada pacote original trafegam na *eth0* a seguinte sequência de dados comprimidos:

- 1 pacote de 207 *Bytes* PPP Compressed (dados comprimidos);
- 1 pacote de 128 *Bytes* PPP Compressed (dados comprimidos);
- 1 pacote de 46 *Bytes* Encapsulated PPP (PPP encapsulado);
- 1 pacote de 128 *Bytes* PPP Compressed (dados comprimidos);
- 1 pacote de 161 *Bytes* PPP Compressed (dados comprimidos);
- 1 pacote de 211 *Bytes* PPP Compressed (dados comprimidos);
- 1 pacote de 46 *Bytes* Encapsulated PPP (PPP encapsulado).

Logo, para cada pacote original há a criação de 7 novos pacotes.

Tabela 4: captura de dados na *interface eth*0

	ETH0			
	128	256	512	1024
Pacotes Rude & Crude	535	525	547	527
Pacotes Wireshark	4183	3912	3943	3997
Relação R&C – Wireshark (%)	12,78%	13,42%	13,87%	13,18%
Tamanho Total da Transmissão R&C	72760	134400	284440	543864,00
Tamanho Total da Transmissão Wireshark	919792	852088	1150708	1731276
Pacotes / segundo R&C	0,89	0,88	0,91	0,88
Pacotes / segundo Wireshark	4,85	4,43	4,73	4,58
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	186,45	184,37	258,37	399,69
Bytes / segundo R&C	121,27	224,04	474,19	907,09
Bytes / segundo Wireshark	905,74	818,32	1223,28	1883,44
HIERARQUIA DE PROTOCOLOS %				
GRE – PPP	87,4	87,45	88,7	87,63
TCP – PPTP	1,15	1,15	1,09	1,08
UDP – DNS	1,79	2,4	2,1	1,73
ICMPv6	8,37	8,05	6,97	8,78
ARP	1,29	0,95	1,14	0,78
Total	100	100	100	100

6.2 VPN COM L2TP/IPSEC

A configuração do servidor L2TP/IPSec, responsável por estabelecer, manter e finalizar uma sessão VPN cliente-servidor encontra-se discriminada no APÊNDICE C. Já o cliente, para requisitar uma sessão deve configurar sua conexão L2TP através das configurações de rede, incluíndo o IP do servidor, nome de usuário e senha.

Estabelecidas as sessões, o tráfego de pacotes com o uso da ferramenta Rude & Crude deve ser gerado (conforme CAPÍTULO 2), bem como a instalação do servidor NTP no servidor VPN deve estar ativa. O APÊNDICE B traz as configurações de ambas ferramentas.

Conforme descrito no CAPÍTULO 2, foram efetuadas três coletas subsequentes de 600 pacotes cada para cada um dos cenários (transmissões de 128 *Bytes*, 256 *Bytes*, 512 *Bytes* e 1024 *Bytes*), sendo para a comunicação de 128 *Bytes* de tamanho de pacotes:

- coleta 1: 589 pacotes recebidos, 11 pacotes perdidos;
- coleta 2: 577 pacotes recebidos, 23 pacotes perdidos;
- coleta 3: 579 pacotes recebidos, 21 pacotes perdidos.

Após o cálculo das médias aritméticas dos tempos de mesmo número de ordem, e

descartando-se tempos com número de ordem superior ao número de pacotes da coleta com menores valores de pacotes recebidos, obteve-se os dados estatísticos de tempo de transmissão descritos na TABELA 5.

Tabela 5: estatística L2TP 128 *Bytes*

classes	10
amplitude	0,17s
max	2,33s
min	0,6s
média arit	0,7s
mediana	0,67s
moda	0,67s
desvio med	0,06s
variancia	0,02s
desvio pad	0,15s

A partir da Tabela 5 infere-se que a distribuição dos dados é assimétrica positiva (MACHADO, 2010), pois média aritmética > mediana >= média. Esta característica mantem-se até para 1024 *Bytes* (sendo neste tamanho mais evidente a distribuição assimétrica positiva), conforme TABELAS 6, 7 e 8. De fato, a TABELA 8 traz tempos mais elevados em todas as categorias, característica que será melhor analisada com a visualização dos pacotes com a ferramenta Wireshark.

Visualmente as características de assimetria evidenciam-se ao se analisar as Ilustrações 10, 11, 12 e 13, mostrando, ainda, que para qualquer tamanho de pacote a maioria dos tempos médios de transmissão mantiveram-se na classe 2 (entre 0,5s e 1s), característica bastante divergente se comparada ao protocolo analisado na seção 6.1.

Tabela 6: estatística L2TP 256 *Bytes*

classes	10
amplitude	0,19s
max	2,57s
min	0,65s
média arit	0,74s
mediana	0,72s
moda	0,7s
desvio med	0,19s
variancia	0,02s
desvio pad	0,16s

Tabela 7: estatística L2TP 512 *Bytes*

classes	10
amplitude	0,24s
max	3,08s
min	0,69s
média arit	0,81s
mediana	0,79s
moda	0,78s
desvio med	0,06s
variancia	0,03s
desvio pad	0,18s

Tabela 8: estatística L2TP 1024 *Bytes*

classes	10
amplitude	0,23s
max	3,04s
min	0,71s
média arit	0,94s
mediana	0,84s
moda	0,82s
desvio med	0,17s
variancia	0,08s
desvio pad	0,28s

Ilustração 10 – ocorrências por classe L2TP 128 *bytes*

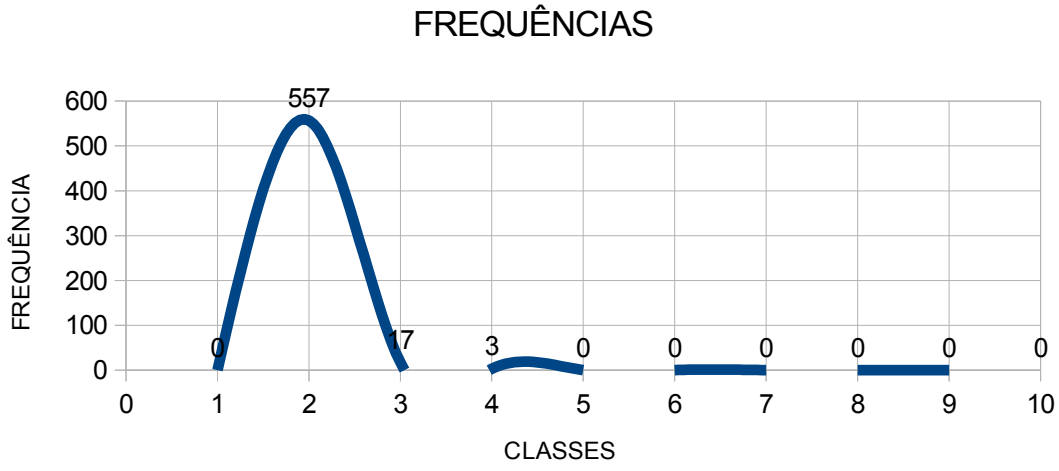


Ilustração 11 – ocorrências por classe L2TP 256 *Bytes*

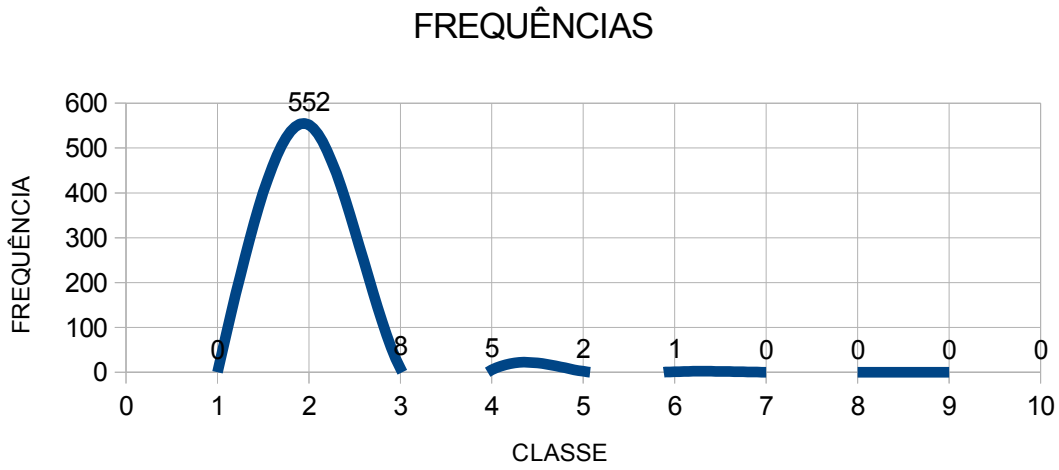


Ilustração 12 – ocorrências por classe L2TP 512 *Bytes*

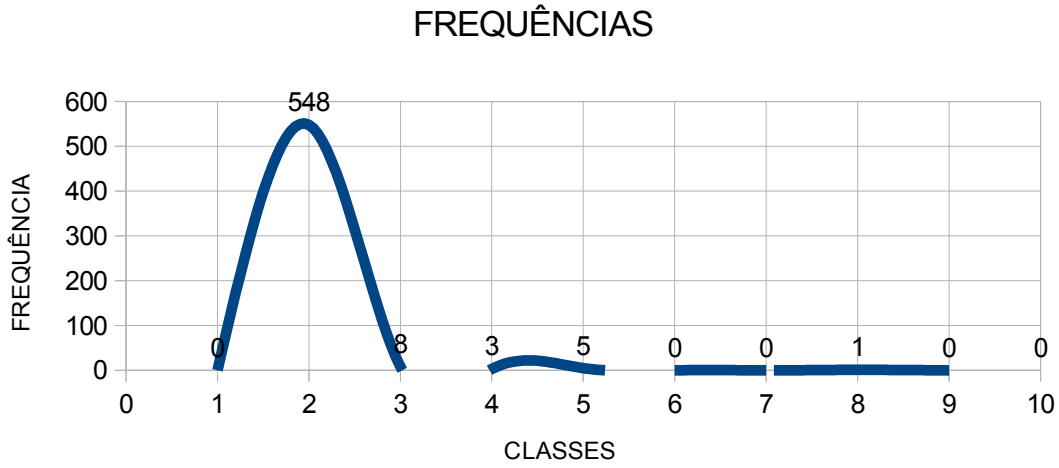
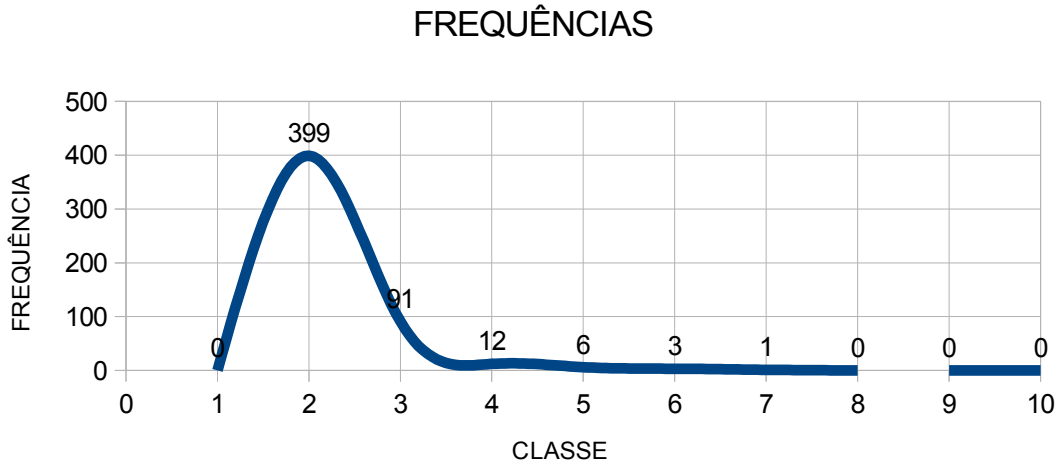


Ilustração 13 – ocorrências por classe L2TP 1024 *Bytes*



A comunicação VPN com o protocolo L2TP mostrou-se mais eficiente do que a com o protocolo PPTP para pacotes maiores em relação ao tempo de transmissão. Em relação à análise da frequência relativa acumulada percebe-se através das Tabelas 9, 10, 11 e 12 que pelo menos 95% dos pacotes terão tempos máximos entre 0,5s e 1s, enquanto que para o protocolo analisado na seção 6.1 este índice só é alcançado a partir da classe 3 (1,0s à1,5s) para pacotes de 128 *Bytes* e 256 *Bytes* e classe 4 (1,5s e 2,0s) para pacotes maiores.

Tabela 9 - distribuição de frequências L2TP 128 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência relativa	Frequência relativa acumulada
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	557	557	96,53	96,53
3	1,0 |--- 1,5	1,25	17	574	2,95	99,48
4	1,5 |--- 2,0	1,75	3	577	0,52	100,00

Tabela 10 - distribuição de frequências L2TP 256 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência relativa	Frequência relativa acumulada
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	552	552	97,18	97,18
3	1,0 |--- 1,5	1,25	8	560	1,41	98,59
4	1,5 |--- 2,0	1,75	5	565	0,88	99,47
5	2,0 |--- 2,5	2,25	2	567	0,35	99,82
6	2,5 |--- 3,0	2,75	1	568	0,18	100,00

Tabela 11 - distribuição de frequências L2TP 512 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência relativa	Frequência relativa acumulada
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	548	548	96,99	96,99
3	1,0 |--- 1,5	1,25	8	556	1,42	98,41
4	1,5 |--- 2,0	1,75	3	559	0,53	98,94
5	2,0 |--- 2,5	2,25	5	564	0,88	99,82
6	2,5 |--- 3,0	2,75	0	564	0,00	99,82
7	3,0 |--- 3,5	3,25	0	564	0,00	99,82
8	3,5 |--- 4,0	3,75	1	565	0,18	100,00

Tabela 12 - distribuição de frequências L2TP 1024 Bytes

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência relativa	Frequência relativa acumulada
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	399	399	77,93	77,93
3	1,0 |--- 1,5	1,25	91	490	17,77	95,70
4	1,5 |--- 2,0	1,75	12	502	2,34	98,05
5	2,0 |--- 2,5	2,25	6	508	1,17	99,22
6	2,5 |--- 3,0	2,75	3	511	0,59	99,80
7	3,0 |--- 3,5	3,25	1	512	0,20	100,00

Analisando-se o tráfego de pacotes através da interface *PPP0* (TABELA 13), outra característica que mostra uma otimização do túnel por parte do protocolo L2TP em relação ao PPTP é a relação de pacotes gerados entre *Rude & Crude* e os pacotes que trafegam pela interface *PPP0*: enquanto naquele protocolo a relação é de ~20%, neste ela varia entre 33% - 45%.

Tabela 13 - tráfego de canal *interface PPP0*

	PPP0			
	128	256	512	1024
Pacotes Rude & Crude	577	568	565	512
Pacotes Wireshark	1713	1246	1255	1232
Relação R&C – Wireshark (%)	33,68	45,58	45,01	41,55
Tamanho Total da Transmissão R&C	78472	149952	293800	528384
Tamanho Total da Transmissão Wireshark	401536B	396580B	696268B	1246356B
Pacotes / segundo R&C	0,94	0,90	0,93	0,68
Pacotes / segundo Wireshark	2,8	1,68	2,06	1,64
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	202,03B	286,9	522,63	979,41
Bytes / segundo R&C	128,85	239,25	482,49	705,45
Bytes / segundo Wireshark	565,808	480,52	1077,2	1609,24
HIERARQUIA DE PROTOCOLOS %				
ICMP	95,41	96,23	94,82	94,16
UDP – DNS	1,81	3,21	2,71	5,11
UDP – DADOS	0,12	0,16	-	0,08
TCP	2,66	0,4	2,47	0,65
Total	100	100	100	100

Esta diferença de relações e consequentemente otimização do túnel encontra justificativa no CAPÍTULO 3.4: enquanto que um tunelamento PPTP emite uma requisição de nome de domínio a cada 3 ou 4 segundos em média, o túnel L2TP também utiliza pacotes UDP para manter o túnel através de mensagens de manutenção, porém a cada 20 segundos aproximadamente.

Implica, ainda, que apesar de um túnel L2TP com IPSec prover maior segurança dos dados, este utiliza menos pacotes do que o tunelamento PPTP:

• Tamanho total da transmissão *Wireshark*: 1246356B (TABELA 13);

• Tamanho total da transmissão *Wireshark*: 1437724B (TABELA 3).

Analisando-se o tráfego de pacotes através da interface *eth0* (TABELA 14), a otimização do canal torna-se ainda mais evidente quando comparada com a mesma interface do protocolo PPTP. Para cada pacote gerado pela ferramenta *Rude & Crude*, os seguintes pacotes, em média, trafegam pela interface *eth0*:

• 1 pacote tipo UDP-IPSEC-ESP com 374 *Bytes*;

- 1 pacote tipo UDP-IPSEC-ESP com 374 *Bytes*;
- 1 pacote tipo UDP-DNS com 87 *Bytes;*
- 1 pacote tipo UDP-IPSEC-ESP com 102 *Bytes*;
- 1 pacote tipo UDP-ICMP com 86 *Bytes*.

Tabela 14 - tráfego de canal *interface* eth*0*

	ETH0			
	128	256	512	1024
Pacotes Rude & Crude	577	568	565	512
Pacotes Wireshark	2766	2762	2011	1867
Relação R&C – Wireshark (%)	20,86%	20,56%	28,09%	27,42%
Tamanho Total da Transmissão R&C	78472	149952	293800,00	528384,00
Tamanho Total da Transmissão Wireshark	662514B	693847B	848464	1402000B
Pacotes / segundo R&C	0,94	0,9	0,93	0,68
Pacotes / segundo Wireshark	4,55	4,32	3,28	3,03
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	206,13B	217,86B	388,18	717,2
Bytes / segundo R&C	128,85	239,25	482,49	705,45
Bytes / segundo Wireshark	939,57	942,66	1275,99	2179,28
HIERARQUIA DE PROTOCOLOS %				
UDP – IPSEC – ESP	76,12	77,48	77,42	75,87
UDP – DNS	6,97	5,87	9,7	8,21
UDP – ICMP	10,21	9,14	7,49	7,02
UDP – IGMP	1,8	1,02	1,54	0,99
UDP – DADOS	0,25	-	0,25	0,32
ARP	0,4	0,21	0,39	0,74
Ipv6	4,25	6,28	3,21	6,85
NetBios Datagram Service	-	-	0,1	0,11
Total	100	100	100	100

O ANEXO 2 traz outras ilustrações e tabelas que complementam a análise do tunelamento L2TP / IPSec.

6.3 VPN COM OPENVPN

A configuração do servidor OPENVPN, responsável por estabelecer, manter e finalizar uma sessão VPN cliente-servidor encontra-se discriminada no APÊNDICE D. A geração das chaves critpográficas pode ser encontrada no APÊNDICE E. Já o cliente para requisitar uma sessão deve configurar sua conexão OPENVPN conforme APÊNDICE F.

Estabelecidas as sessões, o tráfego de pacotes com o uso da ferramenta *Rude & Crude* deve ser gerado (conforme CAPÍTULO 2), bem como a instalação do servidor NTP

no servidor VPN deve estar ativa. O APÊNDICE B traz as configurações de ambas ferramentas.

Conforme descrito no CAPÍTULO 2, foram efetuadas três coletas subsequentes de 600 pacotes cada para cada um dos cenários (transmissões de 128 *Bytes*, 256 *Bytes*, 512 *Bytes* e 1024 *Bytes*), sendo para a comunicação de 128 *Bytes* de tamanho de pacotes:

- coleta 1: 574 pacotes recebidos, 26 pacotes perdidos;
- coleta 2: 563 pacotes recebidos, 37 pacotes perdidos;
- coleta 3: 551 pacotes recebidos, 49 pacotes perdidos.

Após o cálculo das médias aritméticas dos tempos de mesmo número de ordem, e descartando-se tempos com número de ordem superior ao número de pacotes da coleta com menores valores de pacotes recebidos, obteve-se os dados estatísticos de tempo de transmissão descritos na TABELA 15.

Tabela 15 – estatística descritiva

OPENVPN 128 *Bytes*

classes	10
amplitude	0,5s
max	5,99s
min	1,0s
média arit	1,36s
mediana	1,06s
moda	1,01s
desvio med	0,39s
variancia	0,27s
desvio pad	0,52s

De maneira análoga ao tunelamento L2TP com IPSec, mostra-se evidente que as distribuições de frequência para pacotes de tamanho 128 *Bytes* (TABELA 16), 256 *Bytes* (TABELA 17), 512 *Bytes* (TABELA 18) e 1024 *Bytes* (TABELA 19) apresentam comportamento assimétrico positivo, com especial destaque para os pacotes de tamanho maior, que apresentaram média aritmética de 1,8s, mediana de 1,51s e moda de 1,01s.

Tabela 16 – estatística descritiva

OPENVPN 256 *Bytes*

classes	10
amplitude	0,8s
max	9,0s
min	1,0s
média arit	1,57s
mediana	1,23s
moda	1,03s
desvio med	0,57s
variancia	0,74s
desvio pad	0,86s

Tabela 17 – estatística descritiva

OPENVPN 512 *Bytes*

classes	10
amplitude	0,36s
max	4,61s
min	1,0s
média arit	1,46s
mediana	1,07s
moda	1,03s
desvio med	0,51s
variancia	0,46s
desvio pad	0,68s

Tabela 18 – estatística descritiva

OPENVPN 1024 *Bytes*

classes	10
amplitude	0,65s
max	7,47s
min	1,0s
média arit	1,8s
mediana	1,51s
moda	1,01s
desvio med	0,73s
variancia	0,99s
desvio pad	0,99s

Analisando-se os gráficos de dados brutos para pacotes de tamanho 128 *Bytes* (ILUSTRAÇÃO 14), 256 *Bytes* (ILUSTRAÇÃO 15), 512 *Bytes* (ILUSTRAÇÃO 16) e 1024 *Bytes* (ILUSTRAÇÃO 17) percebe-se um maior desvio médio dos dados, ou seja, um determinado pacote registra um tempo muito diferente do seu antecessor e do seu

sucessor. Tanto o túnel PPTP quanto o L2TP não apresentaram mesmo comportamento, tendo assim um desvio médio menor do que o túnel OPENVPN (TABELA 19). Isto demonstra que o túnel OPENVPN é menos estável e torna-se mais imprevisível para se determinar o tempo de chegada de um pacote. Esta análise prova que, conforme APÊNDICE E e APÊNDICE F, tanto o servidor OPENVPN quanto o cliente foram configurados para utilizar conexão TCP na porta 22222. Neste caso, ao se utilizar o TCP o desempenho da VPN possivelmente é pior do que se utilizada uma porta UDP. Isso ocorre porque em um túnel UDP os pacotes são transmitidos diretamente, o que garante o melhor desempenho.

Tabela 19 - comparação dos desvios médios

	DESVIO MÉDIO		
	PPTP	L2TP	OPENVPN
128B	0,19s	0,06s	0,39s
256B	0,16s	0,19s	0,57s
512B	0,26s	0,06s	0,51s
1024B	0,61s	0,17s	0,73s

Ilustração 14 - distribuição dos tempos de transmissão OPENVPN 128 B*ytes*

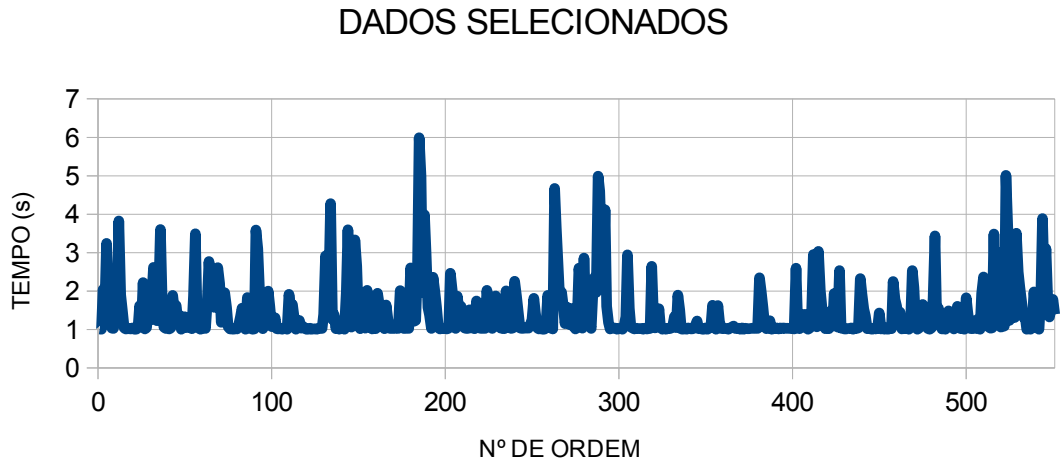


Ilustração 15 - distribuição dos tempos de transmissão OPENVPN 256 B*ytes*

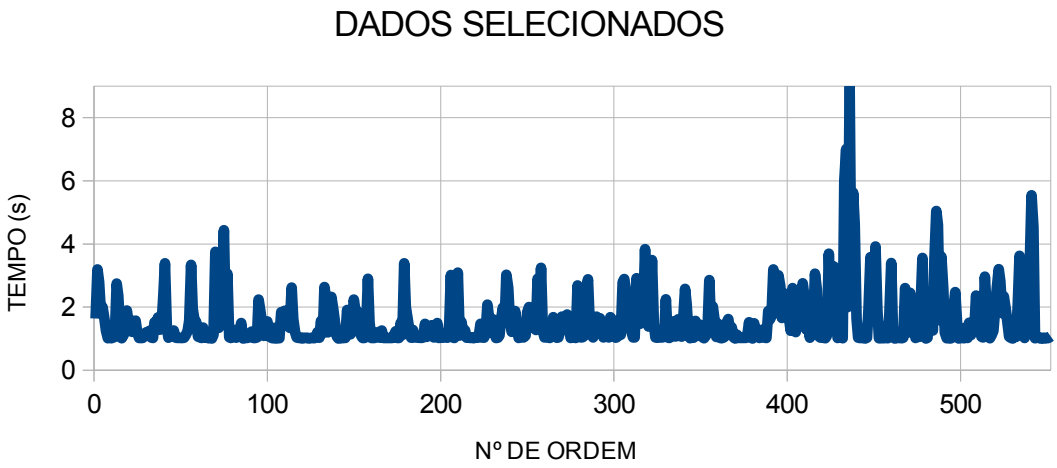


Ilustração 16 - distribuição dos tempos de transmissão OPENVPN 512 B*ytes*

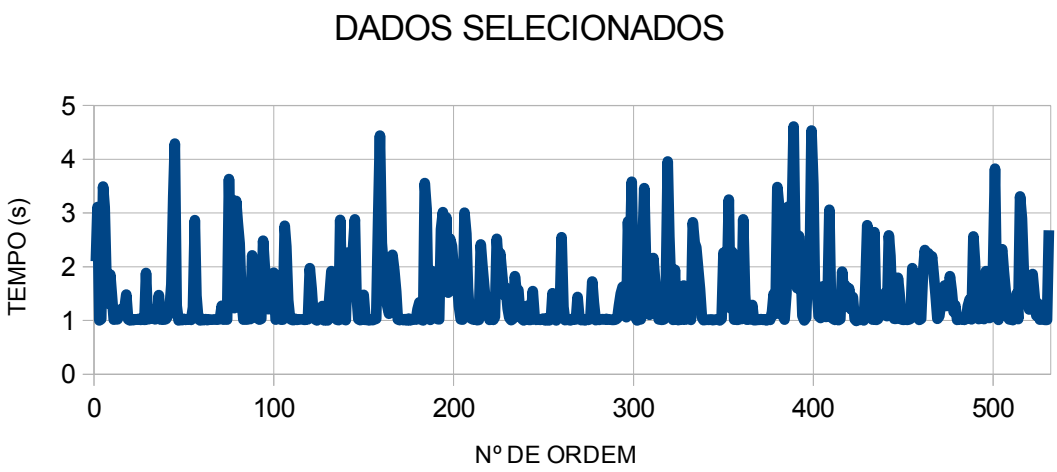
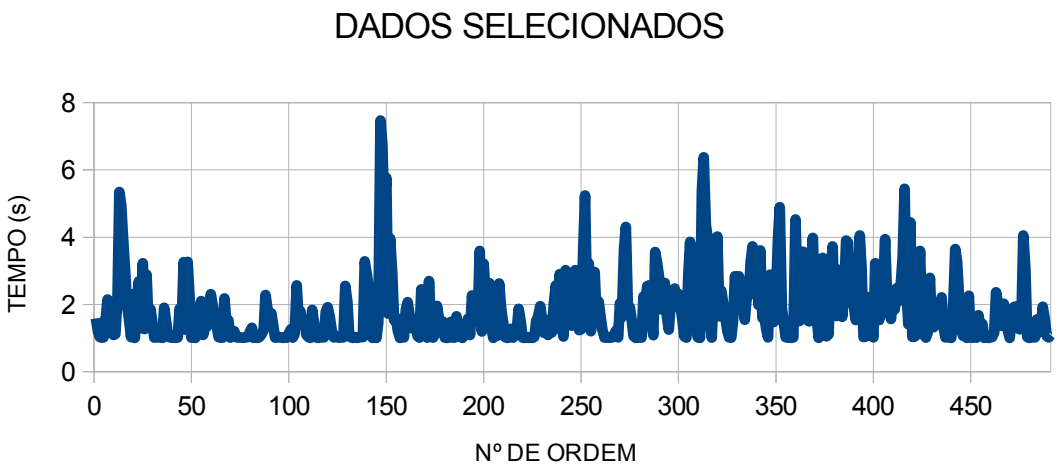


Ilustração 17 - distribuição dos tempos de transmissão OPENVPN 1024 B*ytes*



Em relação a frequência relativa acumulada, mais uma vez torna-se evidente que, entre os três protocolos analisados neste trabalho, o OPENVPN é o protocolo com maior latência e, portanto, ao exigir maior segurança no tráfego das informações, perde-se em tempo de resposta de entrega de pacote. As ILUSTRAÇÕES 18, 19, 20 e 21 mostram que:

- nenhum pacote chegará no destino antes de 1 segundo;
- para que um pacote chegue ao destino em até 1,5s, a probabilidade é de 49,29% para tamanho de 1024B;
- 13,25% dos pacotes chegarão, no melhor cenário, após 2s do envio.

Ilustração 18 - probabilidade por classes OPENVPN 128 *Bytes*

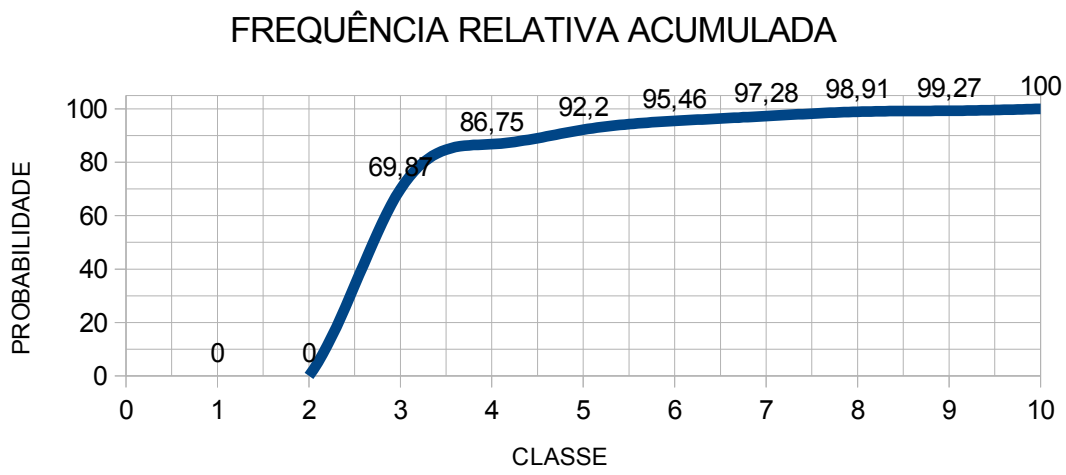


Ilustração 19 - probabilidade por classes OPENVPN 256 *Bytes*

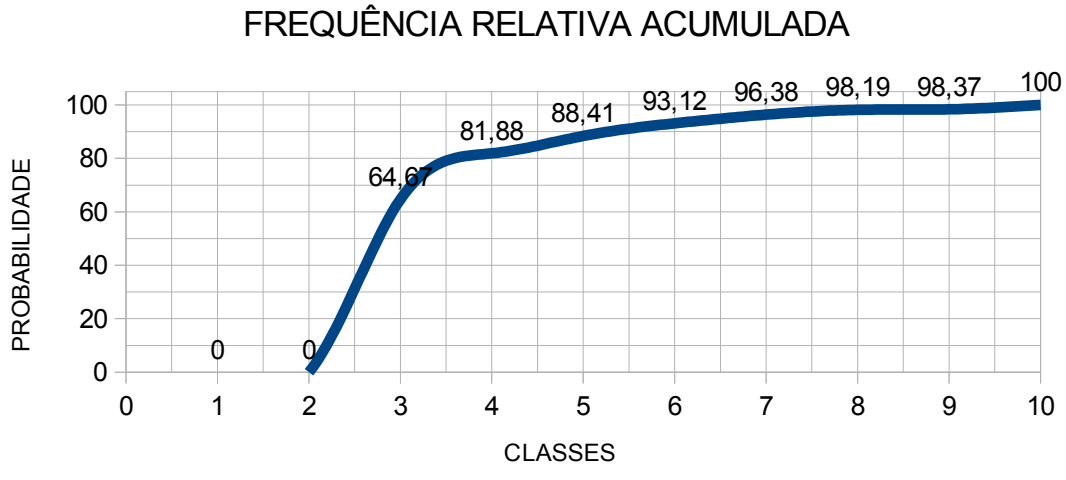


Ilustração 20 - probabilidade por classes OPENVPN 512 *Bytes*

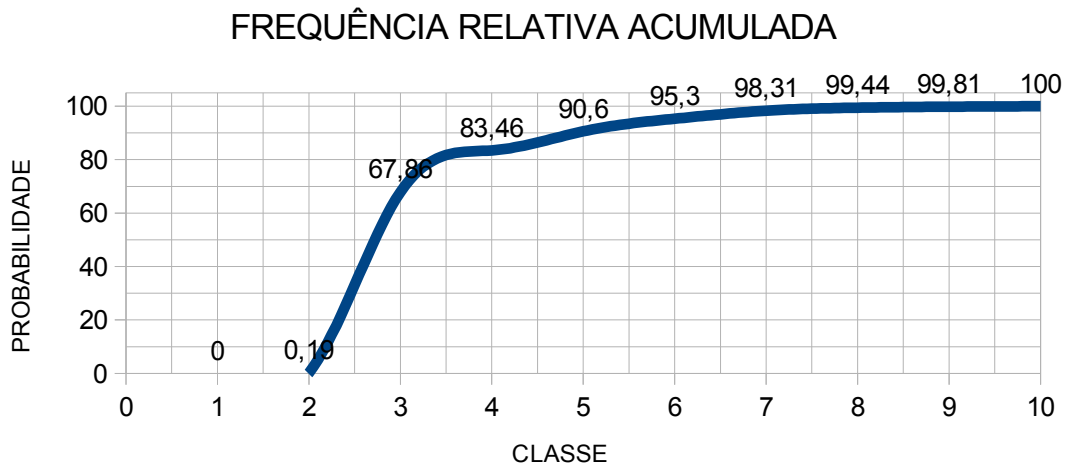
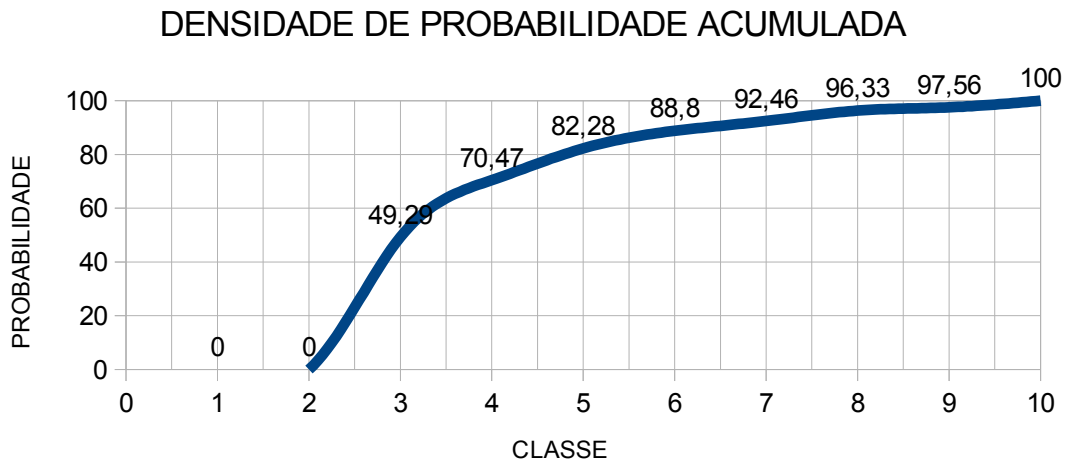


Ilustração 21 - probabilidade por classes OPENVPN 1024 *Bytes*



Analisando-se o tráfego de pacotes através da interface *tun1* (TABELA 20) e a relação entre os pacotes gerados pela ferramenta *Rude & Crude* e os pacotes que passam por esta i*nterface*, percebe-se que este tipo de túnel é o que gera menos pacotes em relação aos pacotes originais. Por conseguinte, o tamanho total da transmissão aferido na interface *tun1*, por exemplo, com pacotes de 1024 *Bytes*, é de 923264 *Bytes*, ao passo que para o mesmo tamanho de pacote, no tunelamento L2TP é de 1246356 *Bytes* e no PPTP é de 1437724 *Bytes*, uma diferença de 55,72% de tráfego de dados entre OPENVPN e PPTP.

Ainda, percebe-se que em média 90% da transmissão original é de pacotes do tipo

ICMP e, assim como no tunelamento L2TP, a manutenção do canal é feita com muito menos frequência que no PPTP (através de pacotes DNS, aproximadamente 5% do total de pacotes gerados).

Tabela 20 - tráfego de pacotes na interface *tun1*

	tun1			
	128	256	512	1024
Pacotes Rude & Crude	551	552	532	491
Pacotes Wireshark	845	1009	1004	903
Relação R&C – Wireshark (%)	65,20%	54,70%	52,98%	54,37%
Tamanho Total da Transmissão R&C	74936	145728	276640	506712
Tamanho Total da Transmissão Wireshark	154380	308536	496048	923264
Pacotes / segundo R&C	0,92	0,92	0,89	0,82
Pacotes / segundo Wireshark	1,43	1,67	1,69	1,51
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	150,36	273,52	461,76	990,13
Bytes / segundo R&C	124,89	242,88	461,07	844,52
Bytes / segundo Wireshark	257,3	458,96	826,75	1538,77
HIERARQUIA DE PROTOCOLOS %				
ICMP	93,25	95,04	83,07	93,69
UDP – DNS	6,63	4,96	4,68	6,31
UDP – DADOS	-	-	-	-
TCP	0,12	-	12,25	-
Total	100	100	100	100

Já na interface *eth0*, conforme TABELA 21, o tráfego total de pacotes também é menor se comparado aos demais tunelamentos, provocados principalmente pelo maior número de pacotes transmitidos por segundo.

Tabela 21 - tráfego de pacotes na interface *eth0*

	ETH0			
	128	256	512	1024
Pacotes Rude & Crude	551	552	532	491
Pacotes Wireshark	3016	3155	3091	3071
Relação R&C – Wireshark (%)	18,26%	17,49%	17,21%	15,98%
Tamanho Total da Transmissão R&C	74936	145728	276640	506712
Tamanho Total da Transmissão Wireshark	575686	735824	755787	753066
Pacotes / segundo R&C	0,92	0,92	0,89	0,82
Pacotes / segundo Wireshark	5,03	5,26	5,15	5,12
Tamanho médio do pacote R&C	136	264	520	1032
Tamanho médio do pacote Wireshark	157,07	199,41	210,7	211,38
Bytes / segundo R&C	124,89	242,88	461,07	844,52
Bytes / segundo Wireshark	959,48	1226,37	1259,65	1255,11
HIERARQUIA DE PROTOCOLOS %				
TCP – SSL	63,06	62,22	64,64	64,8
UDP – DNS	29,21	31,22	29,6	29,14
Ipv6 – UDP – ICMP	6,27	6,5	5,69	5,96
ARP	0,23	0,06	0,07	0,1
Outros	1,23	-	-	-
Total	100	100	100	100

Para cada pacote ICMP gerado na origem trafegam pela interface eth0 os seguintes pacotes, em sequência contínua:

- pacote do tipo TCP – tamanho 66 bytes;
- pacote do tipo SSL – tamanho 281 bytes;
- pacote do tipo SSL – tamanho 137 bytes;
- pacote do tipo TCP – tamanho 66 bytes;
- pacote do tipo TCP – tamanho 66 bytes;
- pacote do tipo SSL – tamanho 281 bytes;
- pacote do tipo SSL – tamanho 281 bytes;
- pacote do tipo TCP – tamanho 66 bytes;
- pacote do tipo DNS – tamanho 87 bytes;
- pacote do tipo DNS – tamanho 124 bytes.

Em média, a quantidade de pacotes encapsulados do tipo SSL representam 63% do tráfego gerado. Em comparação com os demais pacotes encapsulados nos demais tunelamentos, tem-se que para o túnel PPTP ~87% e no túnel L2TP ~76% dos pacotes são encapsulados. A maior segurança e utilização de chaves criptográficas maiores influem significativamente na quantidade de tais pacotes.

7 ANÁLISE COMPARATIVA

Afim de atender os objetivos deste trabalho e analisar os diferentes protocolos de redes privadas virtuais, desenvolvendo cenários específicos de troca de informações, no intuito de buscar dados estatísticos que promovam uma comparação entre as diferentes soluções, torna-se salutar desenvolver tabelas e ilustrações para que se possa contemplar o maior número de comparações possíveis entre os protocolos.

A TABELA 22 promove a comparação entre as médias aritméticas dos tempos de transmissão dos pacotes em relação ao seu tamanho e túnel.

Tabela 22 - médias aritméticas - tempos de transmissão

	MÉDIA ARITMÉTICA			
	128 Bytes	256 Bytes	512 Bytes	1024 Bytes
PPTP	0,86s	1,46s	1,66s	2,84s
L2TP	0,70s	0,74s	0,81s	0,94s
OPENVPN	1,36s	1,57s	1,46s	1,80s

Conforme discutido na SEÇÃO 6.2, a necessidade de uma manutenção mais robusta do canal (maior número de pacotes UDP) faz com que o túnel PPTP apresente médias aritméticas maiores em comparação ao L2TP, mesmo este tendo criptografia, ao contrário daquele que não apresenta chaves e senhas. Como é de se esperar, o tunelamento que apresenta maior robustez na segurança (OPENVPN) apresenta tempos de transmissão mais elevados.

A TABELA 23 traz a comparação entre as classes de tempo que mais tiveram pacotes nos diferentes cenários. É possível verificar diferentes comportamentos em todos os protocolos: enquanto que no tunelamento PPTP a classe variou de acordo com o tamanho do pacote transmitido, nos demais túneis tal fato não ocorreu. Porém, verifica-se que em todos os três tipos de túneis, para pacotes de tamanho 1024 *Bytes*, ocorre uma redução no número absoluto de pacotes nas respectivas classes. Conclui-se, pois, que para pacotes deste tamanho os tempos de transmissão são difusos, não apresentando um padrão específico, como por exemplo na transmissão PPTP 1024 *Bytes*, há 228 pacotes na classe 5 e 217 pacotes na classe imediatamente superior.

Em relação a probabilidade de um pacote estar em determinada classe de tempo, a TABELA 24 traz valores que corroboram a análise do parágrafo anterior e serve como parâmetros de previsibilidade de tunelamentos de mesmo tipo e mesmo cenário. Mais uma vez percebe-se que para os maiores tamanhos de pacote a probabilidade decai.

Tabela 23 - pacotes por classe

	MAIOR NÚMERO DE PACOTES				
	CLASSE 1	CLASSE 2	CLASSE 3	CLASSE 4	CLASSE 5
PPTP 128B	-	466	-	-	-
PPTP 256B	-	-	353	-	-
PPTP 512B	-	-	-	402	-
PPTP 1024B	-	-	-	-	228
L2TP 128B	-	557	-	-	-
L2TP 256B	-	552	-	-	-
L2TP 512B	-	548	-	-	-
L2TP 1024B	-	399	-	-	-
OPENVPN 128B	-	-	385	-	-
OPENVPN 256B	-	-	357		-
OPENVPN 512B	-	-	360	-	-
OPENVPN 1024B	-	-	242	-	-

Tabela 24 - probabilidades por classe

	MAIORES PROBABILIDADES POR CLASSE				
	CLASSE 1	CLASSE 2	CLASSE 3	CLASSE 4	CLASSE 5
PPTP 128B	-	87,10%	-	-	-
PPTP 256B	-	-	67,24%	-	-
PPTP 512B	-	-	-	75,14%	-
PPTP 1024B	-	-	-	-	42,62%
L2TP 128B	-	96,53%	-	-	-
L2TP 256B	-	97,18%	-	-	-
L2TP 512B	-	96,99%	-	-	-
L2TP 1024B	-	77,93%	-	-	-
OPENVPN 128B	-	-	69,87%	-	-
OPENVPN 256B	-	-	64,67%		-
OPENVPN 512B	-	-	67,67%	-	-
OPENVPN 1024B	-	-	49,29%	-	-

A otimização do canal de comunicação (túnel) em relação ao número de pacotes criptografados que trafegam pela interface *eth0*, conforme a TABELA 25, mostra que à medida que o número de mecanismos de segurança, como chaves criptográficas e senhas aumenta, diminui-se o percentual de pacotes criptografados. Este fenômeno é natural pois para garantir uma segurança elevada, é necessária a utilização de outros pacotes e protocolos para tal fim. Enquanto um túnel PPTP não utiliza criptografia, este utiliza maior percentual do canal de comunicação para trafegar seus pacotes encapsulados, comportamento diverso aos outros dois túneis analisados neste trabalho.

Tabela 25 - otimização do canal

% PACOTES ENCAPSULADOS NO CANAL				
	128B	256B	512B	1024B
PPTP	87,40%	87,45%	88,70%	87,63%
L2TP	76,12%	77,48%	77,42%	75,87%
OPENVPN	63,06%	62,22%	64,64%	64,80%

8 UTILIZAÇÃO DO PROCESSADOR

Foi observado o comportamento do uso do processador no servidor, visto que este é o responsável por manter a conexão VPN ativa e gerenciar o tráfego destes pacotes. Os testes foram executados para todos os cenários discriminados no CAPÍTULO 6, utilizando a ferramenta *TOP*, gerenciador de processos do Ubuntu. De maneira semelhante à metodologia adotada para os demais cenários, foram capturados 600 dados de ocupação

do processador (um por segundo), sendo os seguintes resultados obtidos:

- sem a implementação de qualquer VPN, em média, o processador manteve-se 1,10% do tempo ocupado com processos do usuário e 0,71% do tempo ocupado com processos do sistema.

A TABELA 26 ilustra os demais resultados para testes com as VPNs.

Tabela 26 - utilização do processador

USO DO PROCESSADOR (%)				
	128B	256B	512B	1024B
PPTP processos do usuário	1,49%	1,40%	1,08%	1,25%
PPTP processos do usuário	1,04%	1,09%	1,23%	1,21%
L2TP processos do usuário	1,38%	1,25%	1,17%	1,02%
L2TP processos do usuário	1,10%	1,14%	1,11%	1,49%
OPENVPN processos do usuário	1,25%	1,31%	1,38%	1,30%
OPENVPN processos do usuário	1,16%	1,40%	1,44%	1,32%

De posse destas informações, verifica-se que independe a escolha do tipo de tunelamento em se tratando do uso de processador, pois a variação dos valores é baixa, e mesmo que se encontre, por exemplo, uma diferença de cerca de 30% no uso do processador em processos do usuário entre L2TP 1024 *bytes* e OPENVPN de mesmo tamanho e processo, ainda o processador permanece ocioso por cerca de 98,7% do tempo, trabalhando apenas 1,3% para o tunelamento.

9 CONCLUSÃO

A troca de informações pessoais e confidenciais através da Internet exige que o canal de comunicação seja intransponível por qualquer parte não autorizada. As redes privadas virtuais, apresentadas neste trabalho, trazem consigo uma série de configurações, arranjos, chaves criptográficas e senhas que tem sido utilizadas com êxito nas mais diferentes aplicações que necessitam segurança dos dados.

Este trabalho buscou analisar protocolos de redes privadas virtuais afim de encontrar pontos fortes e fraquezas de tais redes e trazer estes resultados de maneira direta ao leitor. O objetivo é fazer com que o leitor possa aplicar os resultados apresentados neste trabalho no seu contexto de desenvolvimento.

Observou-se que para o protocolo PPTP o tamanho do pacote influencia de maneira acentuada no tempo de transmisssão, necessitando-se, portanto, avaliar previamente à comunicação dos dados, os tipos de pacotes e seus respectivos tamanhos. Já para o tunelamento estabelecido com o protocolo L2TP, os tempos de transmissão pouco diferem do que para o tunelamento com OPENVPN – para todos os cenários de teste destes protocolos os tempos de transmissão mantiveram-se na classe 2. Sendo assim, em se tratando de transmissões de dados com alta necessidade de segurança das informações, é salutar utilizar-se tunelamento com o protocolo OPENVPN.

Trabalhos futuros podem trazer análises comparativas com outros protocolos de VPNs, ou inclusive os mesmos porém com cenários mais complexos - inclusão de firewalls, por exemplo, utilização de redes sem fio – ou o mesmo cenário, porém testando-se a vazão com pacotes maiores ou mais pacotes/segundo.

Este trabalho complementa a formação acadêmica ao unir diversos conhecimentos adquiridos durante o curso e também pela necessidade de complementar ou buscar outros conhecimentos. O resultado deste esforço é gratificante, transformando o calouro que inicia um curso superior em um profissional preparado para os novos desafios que batem à porta.

REFERÊNCIAS

VASCONCELLOS, EDUARDO PINHEIRO G. de. **Contribuições ao estudo da estrutura administrativa.** 1972. 163f. Tese (Doutorado em Administração) – Faculdade de Economia e Administração, Universidade de São Paulo, São Paulo, 1972.

KOSTA, Y. P. DALAL, Upena. JHA, Rakesh. In **Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN).** Artigo Científico. 2010 *International Conference on Recent Trends in Information. I*EEE Computer Society. 2010.

PEÑA, JAVIER. EVANS, JOSEPH. In **Performance Evaluation of Software Virtual Private Networks (VPN).** Artigo Científico. *IEEE International Conference. I*EEE Computer Society. 2000.

FILHO, LUIS RODRIGUES DA SILVA. **Estudo Comparativo entre VPN IP e VPN IP MPLS.** Monografia. Centro de Ciências Tecnológicas. Curso de Informática. Universidade de Fortaleza. Fortaleza. 2006.

BORGES, FÁBIO. FAGUNDES, BRUNO ALVES. CUNHA, GERSON NUNES DA. **VPN – Protocolos e Segurança.** Artigo Científico. Laboratório Nacional de Computação Científica. Rio de Janeiro – RJ.

MARTINS, DÊNER LIMA FERNANDES. **Redes Privadas Virtuais com IPSec.** Trabalho de Extensão. Faculdade de Ciência da Computação. Universidade de Brasília. Brasília. 2000.

CASTRO, ROBLEDO DE ANDRADE. **Uma análise de soluções VPN em redes corporativas de alta capilaridade.** Dissertação (Mestrado Profissional). Universidade Estadual de Campinas, Campinas, São Paulo. 2004.

TANENBAUM, Andrew S. **Redes de Computadores.** 4a Ed., Editora Campus (Elsevier). São Paulo. 2003.

MACHADO, R. **Estatística**. Santa Maria: UFSM, 2010. Notas de Aula.

APÊNDICE

APÊNDICE A – configuração do servidor PPTP

sudo apt-get install pptpd
sudo nano /etc/pptpd.conf
localip xxx.xxx.xxx.xxx
remoteip xxx.xxx.xxx.xxx - xxx
sudo nano /etc/ppp/pptpd-options
ms-dns 8.8.8.8
ms-dns 8.8.4.4
sudo nano /etc/ppp/chap-secrets
client
server secret
IP addresses
username * myPassword *
/etc/init.d/pptpd restart
sudo nano /etc/sysctl.conf
net.ipv4.ip_forward=1
sudo sysctl -p
sudo nano /etc/rc.local
iptabless -t nat -A POSTROUTING -s xxx.xxx.xxx.xxx/24 -o eth0 -j MASQUERADE
iptables -A FORWARD -p tcp --syn -s xxx.xxx.xxx.xxx/24 -j TCPMSS --set-mss 1356

APÊNDICE B – configuração RUDE & C RUDE E SERVIDOR NTP

NTP

sudo apt-get install ntp
service ntp start

Rude & Crude (arquivo script_rude.cfg)

START NOW 0000 0010 ON 3001 ip_destino:10001 CONSTANT 1 128 600000 0010 OFF

APÊNDICE C – CONFIGURAÇÃO DO SERVIDOR L2TP

```
sudo apt-get install xl2tpd openswan ppp
sudo nano /etc/ipsec.conf
config setup
nat_traversal=yes
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:!
10.152.2.0/24
oe=off
protostack=netkey
conn L2TP-PSK-NAT
rightsubnet=vhost:%priv
also=L2TP-PSK-noNAT
conn L2TP-PSK-noNAT
authby=secret
pfs=no
auto=add
keyingtries=3
rekey=no
dpddelay=30
dpdtimeout=120
dpdaction=clea
ikelifetime=8h
keylife=1h
type=transport
left=x.x.x.x
forceencaps=yes
sudo nano /etc/ipsec.secrets
x.x.x.x %any: PSK "password"
sudo ipsec verify
sudo nano /etc/init.d/ipsec.vpn
case "$1" in
start(
echo "Iniciando IPSec"
iptables -t nat -A POSTROUTING -o eth0 -s x.x.x.x/24 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
for each in /proc/sys/net/ipv4/conf/*
do
echo 0 > $each/accept_redirects
echo 0 > $each/send_redirects
done
/etc/init.d/ipsec start
/etc/init.d/xl2tpd start
;;
stop)
echo "Terminando VPN"
iptables --tabela nat --flush
echo 0 > /proc/sys/net/ipv4/ip_forward
/etc/init.d/ipsec stop
/etc/init.d/xl2tpd stop
;;
restart)
```

```
echo "Reiniciando VPN"
iptables -t nat -A POSTROUTING -o eth0 -s 10.152.2.0/24 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
for each in /proc/sys/net/ipv4/conf/*
do
echo 0 > $each/accept_redirects
echo 0 > $each/send_redirects
done
/etc/init.d/ipsec restart
/etc/init.d/xl2tpd restart;;
*)
echo "Usage: /etc/init.d/ipsec.vpn {start|stop|restart}"
exit 1
;;
esac
sudo chmod 755 ipsec.vpn
sudo nano /etc/xl2tpd/xl2tpd.conf
[global]
ipsec saref = no
[lns default]
ip range = 10.152.2.2-10.152.2.254
local ip = x.x.x.x
require chap = yes
refuse pap = yes
require authentication = yes
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
sudo nano /etc/xl2tpd/l2tp-secrets
* * password
sudo nano /etc/ppp/options.xl2tpd
refuse-mschap-v2
refuse-mschap
ms-dns 8.8.8.8
ms-dns 8.8.4.4
asyncmap 0
auth
crtscts
idle 1800
mtu 1200
mru 1200
lock
hide-password
local
name l2tpd
proxyarp
proxyarp
lcp-echo-failure 4
sudo nano /etc/ppp/chap-secrets
user1 l2tpd password *
user2 l2tpd password *
sudo nano /etc/sysctl.conf
```

net.ipv4.ip_forward=1
sudo nano /etc/sysctl.conf
sysctl -p
sudo /etc/init.d/ipsec.vpn restart
sudo /etc/init.d/xl2tpd restart

APÊNDICE D – CONFIGURAÇÃO DO SERVIDOR OPENVPN

```
sudo apt-get install openvpn bridge-utils
auto lo eth0
iface lo inet loopback
iface eth0 inet static
address xxx.xxx.xxx.xxx
netmask 255.255.255.0
gateway xxx.xxx.xxx.xxx
sudo nano /etc/network/interfaces
auto lo br0
iface lo inet loopback
iface br0 inet static
address xxx.xxx.xxx.xxx
netmask 255.255.255.0
gateway xxx.xxx.xxx.xxx
bridge_ports eth0
iface eth0 inet manual
up ip link set $IFACE up promisc on
down ip link set $IFACE down promisc off
sudo /etc/init.d/networking restart
sudo vi /etc/openvpn/easy-rsa/vars
export KEY_COUNTRY="BR"
export KEY_PROVINCE="RS"
export KEY_CITY="SM"
cd /etc/openvpn/easy-rsa/
sudo chown -R root:admin .
sudo chmod g+w .
source ./vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
sudo cp server.crt server.key ca.crt dh1024.pem ta.key
sudo vi /etc/openvpn/up.sh
#!/bin/sh
BR=$1
DEV=$2
MTU=$3
/sbin/ip link set "$DEV" up promisc on mtu "$MTU"
/sbin/brctl addif $BR $DEV
sudo vi /etc/openvpn/down.sh
#!/bin/sh
BR=$1
DEV=$2
/sbin/brctl delif $BR $DEV
/sbin/ip link set "$DEV" down
sudo chmod +x /etc/openvpn/up.sh /etc/openvpn/down.sh
sudo vi /etc/openvpn/server.conf
```

```
mode server
tls-server
local xxx.xxx.xxx.xxx
port 22222
proto tcp-server
dev tap0
up "/etc/openvpn/up.sh br0 tap0 1500"
down "/etc/openvpn/down.sh br0 tap0"
persist-key
persist-tun
ca ca.crtcert server.crt
key server.key
dh dh1024.pem
tls-auth ta.key
cipher BF-CBC
comp-lzo
ifconfig-pool-persist ipp.txt
user nobody
group nogroup
keepalive 10 120
status openvpn-status.log
verb 3
touch /usr/share/openssl-blacklist/blacklist.RSA-4096
sudo /etc/init.d/openvpn restart
```

APÊNDICE E – geração de certificados

```
cd /etc/openvpn/easy-rsa/
source ./vars
./pkitool cliente
```

APÊNDICE F – CONFIGURAÇÃO DO CLIENTE VPN

```
sudo vi /etc/openvpn/easy-rsa/
sudo vi cliente.conf
client
dev tap
remote <ip do servidor> 1194
nobind
resolv-retry infinite
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
tls-auth ta.key 1
cipher BF-CBC
comp-lzo
verb 3
proto tcp-client
port 22222
```

ANEXOS

ANEXO 1 – VPN COM PPTP

Tabela 27 - estatística descritiva
PPTP 256 *Bytes*

classes	10
amplitude	0,10s
max	2,15s
min	1,15s
média arit	1,46s
mediana	1,41s
moda	1,35s
desvio med	0,16s
variancia	0,04s

Tabela 28 - estatística descritiva
PPTP 512 *Bytes*

classes	10
amplitude	0,47s
max	4,86s
min	0,16s
média arit	1,66s
mediana	1,66s
moda	1,63s
desvio med	0,26s
variancia	0,23s
desvio pad	0,48s

Tabela 29 - estatística descritiva
PPTP 1024 *Bytes*

classes	10
amplitude	0,74s
max	9,31s
min	1,91s
média arit	2,84s
mediana	2,54s
moda	2,63s
desvio med	0,61s
variancia	1,04s
desvio pad	1,02s

T*abela 30*: distribuição de frequências PPTP 256 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência Relativa	Frequência Relativa Acumulada %
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	0	0	0,00	0,00
3	1,0 |--- 1,5	1,25	353	353	67,24	67,24
4	1,5 |--- 2,0	1,75	156	509	29,71	96,95
5	2,0 |--- 2,5	2,25	16	525	3,05	100,00

T*abela 31*: distribuição de frequências PPTP 512 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência Relativa	Frequência Relativa Acumulada %
1	0 |--- 0,5	0,25	12	12	2,24	0,00
2	0,5 |--- 1,0	0,75	21	33	3,93	3,93
3	1,0 |--- 1,5	1,25	58	91	10,84	14,77
4	1,5 |--- 2,0	1,75	402	493	75,14	89,91
5	2,0 |--- 2,5	2,25	24	517	4,49	94,39
6	2,5 |--- 3,0	2,75	17	534	3,18	97,57
7	3,0 |--- 3,5	3,25	11	545	2,06	99,63
8	3,5 |--- 4,0	3,75	0	545	0,00	99,63
9	4,0 |--- 4,5	4,25	1	546	0,19	99,81
10	4,5 |--- 5,0	4,75	1	547	0,19	100,00

T*abela 32*: distribuição de frequências PPTP 1024 *Bytes*

Número da Classe	Amplitude (s)	Ponto Médio	Frequência	Fac	Frequência Relativa	Frequência Relativa Acumulada %
1	0 |--- 0,5	0,25	0	0	0,00	0,00
2	0,5 |--- 1,0	0,75	0	0	0,00	0,00
3	1,0 |--- 1,5	1,25	0	0	0,00	0,00
4	1,5 |--- 2,0	1,75	5	5	0,93	0,93
5	2,0 |--- 2,5	2,25	236	241	44,11	45,05
6	2,5 |--- 3,0	2,75	225	466	42,06	87,10
7	3,0 |--- 3,5	3,25	23	489	4,30	91,40
8	3,5 |--- 4,0	3,75	11	500	2,06	93,46
9	4,0 |--- 4,5	4,25	9	509	1,68	95,14
10	4,5 |--- 5,0	4,75	26	535	4,86	100,00

Ilustração 22: distribuição dos tempos de transmissão PPTP 256 Bytes

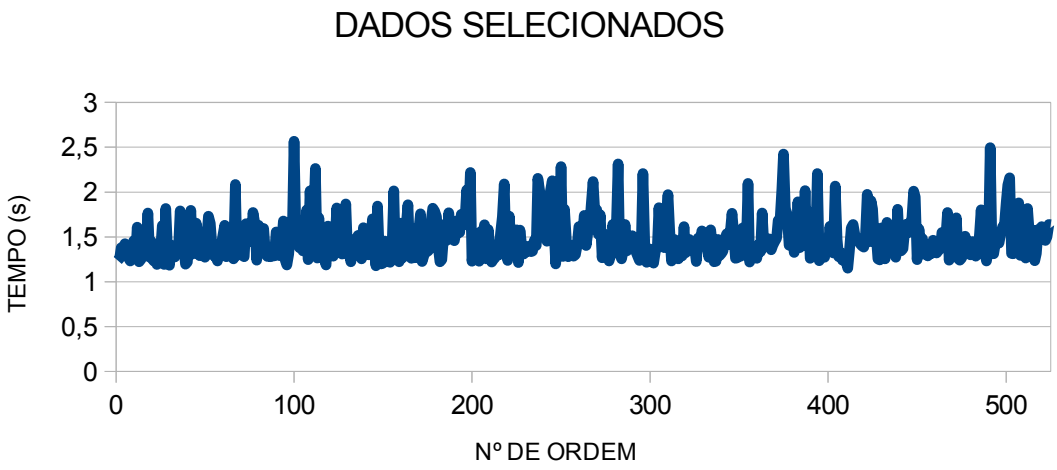


Ilustração 23: distribuição dos tempos de transmissão PPTP 512 Bytes

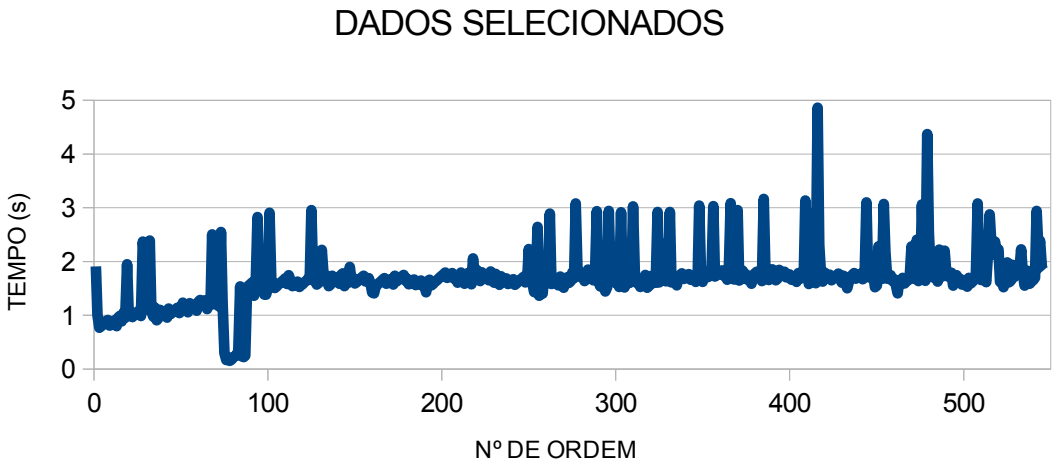
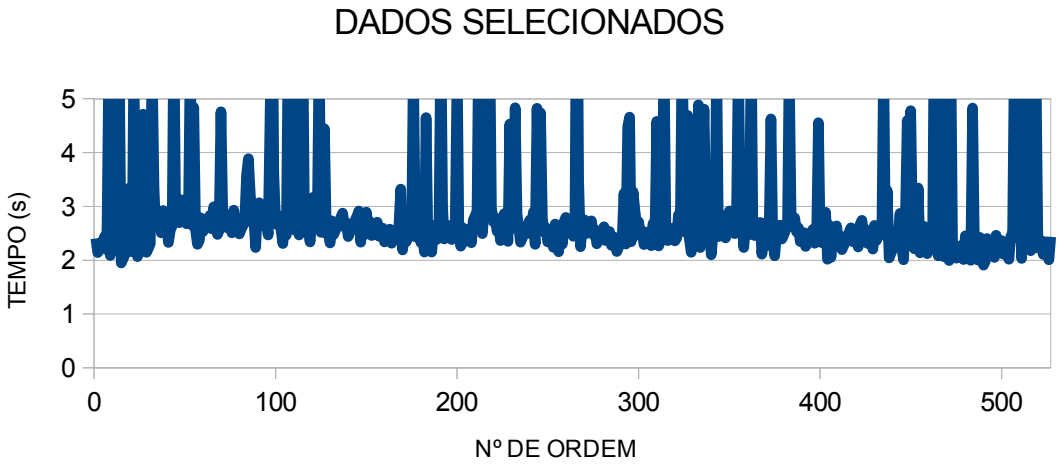


Ilustração 24: distribuição dos tempos de transmissão PPTP 1024 Bytes



ANEXO 2 – VPN COM L2TP / IPSEC

Il*ustração* 25: distribuição dos tempos de transmissão L2TP 128 B*ytes*

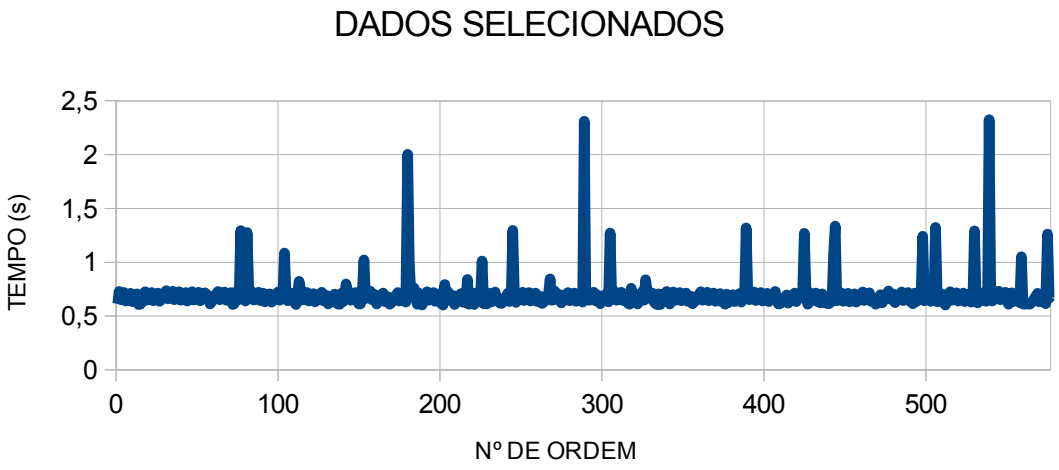


Ilustração 26: distribuição dos tempos de transmissão L2TP 256 Bytes

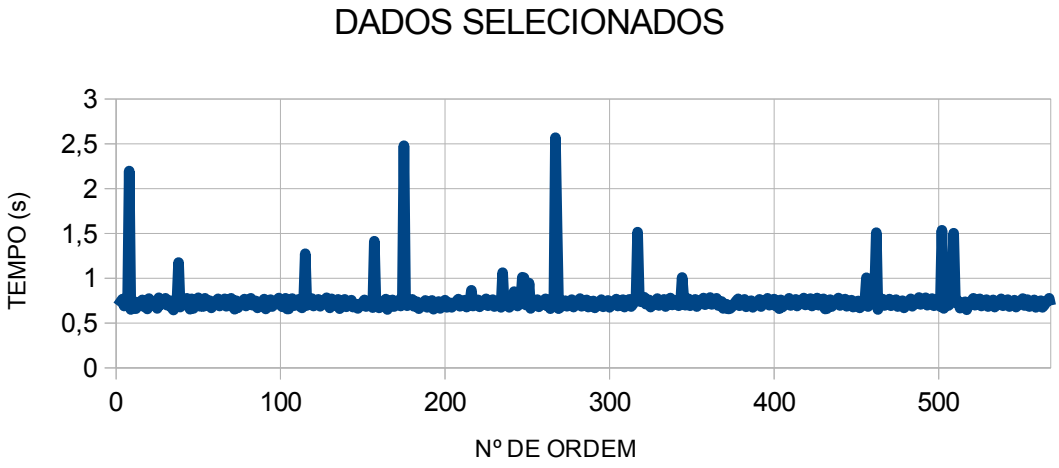


Ilustração 27: distribuição dos tempos de transmissão L2TP 512 Bytes

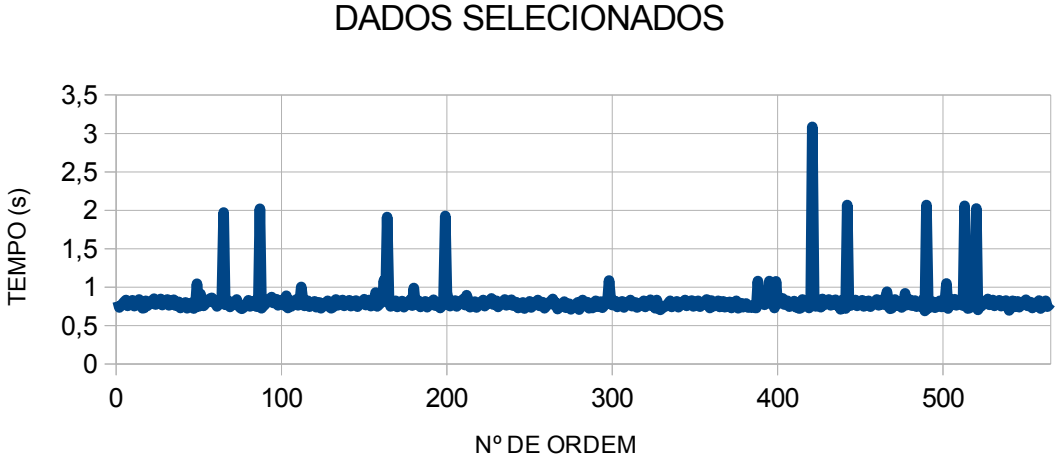


Ilustração 28: distribuição dos tempos de transmissão L2TP 1024 Bytes