Universidade Federal Rural do Semi-Árido
Departamento de Ciências Exatas, Tecnológicas e Humanas
Bacharelado em Sistemas de Informação

EXPEDITO DANTAS BARBOSA NETO

Estudo de Redes Privadas Virtuais simuladas no software CISCO *Packet Tracer*

ANGICOS/RN
SETEMBRO/2018

EXPEDITO DANTAS BARBOSA NETO

Estudo de Redes Privadas Virtuais simuladas no software Cisco *Packet Tracer*

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação da Universidade Federal Rural do Semi-Árido, como requisito para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Leiva Casemiro Oliveira

ANGICOS/RN
SETEMBRO/2018

N469e Neto, Expedito Dantas Barbosa.
Estudo de Redes Privadas Virtuais simuladas no software Cisco Packet Tracer / Expedito Dantas Barbosa Neto. - 2018.
58 f. : il.

Orientador: Leiva Casemiro Oliveira.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Sistemas de Informação, 2018.

1. VPN. 2. SImulações. 3. Cenários. 4. CISCO. 5. Packet Tracer. I. Oliveira, Leiva Casemiro , orient. II. Título.

EXPEDITO DANTAS BARBOSA NETO

Estudo de redes virtuais privadas simuladas no software Cisco *Packet Tracer*

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação da Universidade Federal Rural do Semi-Árido, como requisito para obtenção do grau de Bacharel em Sistemas de Informação.

Defendida em: 12 / 09 / 2018.

BANCA EXAMINADORA

Leiva Casemiro Oliveira

Prof(a). Dr(a). Leiva Casemiro Oliveira (UFERSA)

Orientador e Presidente

Joêmia Laílane Gomes de Medeiros

Prof(a). Dr(a). Joemia Leilane Gomes de Medeiros (UFERSA)

Membro Examinador

Francisco de Assis P.V. de Arruda

Prof(a). Dr(a). Francisco de Assis Pereira Vasconcelos de Arruda (UFERSA)

Membro Examinador

Dedico este trabalho a Deus, pela força e perseverança dada a mim para continuar, e aos meus pais, Marlene Rodrigues Barbosa e Antônio Santos Barbosa, pelo amor e apoio incondicional.

AGRADECIMENTO

Agradeço a Deus pela força e motivação durante toda minha jornada acadêmica até aqui, pelo refúgio frente as adversidades que surgiam em meu caminho e por nunca me deixar abater. Onde por meio da fé me mostrou o caminho certo para alcançar meus objetivos e perseverar nos momentos adversos. A Deus, toda honra e toda glória.

A minha família, em especial, meus pais, Marlene Rodrigues e Antônio Santos, meus irmãos André Rodrigues e Francisco Adriano, minhas irmãs Samara Yasmim e Virginia Rodrigues, e minhas tias Marly Rodrigues, Irene Rodrigues e Azinete Rodrigues, que me apoiaram desde sempre e não mediram esforços para ajudar na realização dos meus objetivos e pelos cuidados prestados a mim quando mais precisei. Sou eternamente agradecido por tê-los em minha vida.

Agradeço a todos os professores que fizeram parte da minha trajetória na Universidade Federal Rural do Semi-Árido – UFERSA Campus Angicos. Pelo conhecimento, suporte e apoio passados a mim durante essa jornada de aprendizado. Cada um deles teve um papel fundamental na minha formação como estudante e como profissional, levarei na memória tudo de melhor que foi transferido a mim. A eles, toda gratidão e respeito.

A Leiva Casemiro pela orientação e paciência durante o desenvolvimento desta pesquisa e por tornar possível a realização deste projeto. Pelo apoio e incentivo dado a mim para seguir na área de redes de computadores. Sou infinitamente grato pelo apoio.

A Luana Dantas pelo suporte e esclarecimento dado a mim durante todo o período de realização desta pesquisa. Por sua paciência e compreensão, meu muito obrigado.

Aos amigos Felipe Ricardo, Juscimara Avelino e Júlio Cartier por caminharem junto comigo desde sempre e tornarem o percurso mais agradável, e por se transformarem em pessoas que levarei para toda minha vida. Agradeço por cada momento que compartilhamos.

A Lucian Santos, Rennan Fabrício, Danilo Ramos, Edmir José e Victor Michael pela amizade e companhia durantes as viagens diárias para Angicos, por tornarem mais agradável e mais feliz minhas noites na estrada. Muito obrigado pela amizade!

A todos meus amigos que sempre me apoiaram durante minha jornada acadêmica, Jordan Huan, Adriano Barreto, Alex Montenegro, João Marcos, Adriano Barreto, Jefferson de Paula, Adolfo Daniel, Wellington Leandro e Makson Borges.

A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.

(Arthur Schopenhauer)

RESUMO

Com o crescente desenvolvimento das redes corporativas e sua expansão geográfica, novas tecnologias se tornam necessárias para atender as novas demandas que surgem no mercado, e nesse contexto que surgem as Redes Privadas Virtuais (RVP, ou VPN, sigla em inglês para *Virtual Private Network*). Desta forma, este trabalho busca estudar os conceitos que englobam as VPNs, incluindo suas características, funcionamento, seus tipos e protocolos de segurança. Para compreender seus conceitos e funcionamentos sem que seja necessária nenhuma infraestrutura física, são feitas simulações de cenários que envolvem VPNs através do software de simulação de redes CISCO *Packet Tracer*.

Palavras-chave: VPN, simulações, cenários, CISCO *Packet Tracer*

ABSTRACT

With the increase of corporate networks and their geographic expansion, new technologies become necessary to meet the new demands that arise in the market and, in this context, appear the Virtual Private Networks (VPN). In this way, this project seeks to learn the concepts that involve the VPN, including its characteristics, operation, its types and security protocols. To understand their concepts and workings without the need for any physical infrastructure, scenario simulations involving VPNs are done through the CISCO Packet Tracer network simulation software.

Keywords: VPN, simulations, scenarios, CISCO Packet Tracer

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

VPN	Virtual Private Network
TCP	Transmission Control Protocol
IP	Internet Protocol
QoS	Quality of Service
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
IPsec	Internet Protocol Security
ISO	International Organization Standardization
OSI	Open System Interconnection
PPTP	Point-to-Point Tunneling Protocol
ISDN	Integrated Service Digital Network
Gateway	Dispositivo de rede intermediário destinado, geralmente, a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.
GNU	Sistema operacional livre do tipo Unix.
GRE	Generic Routing Encapsulation
PPP	Point-to-Point Protocol
ISP	Internet Service Provider
CCP	Compression Control Protocol
ECP	Encryption Control Protocol
DoS	Denial of Service
IETF	Internet Engineering Task Force
AH	Authentication Header
ESP	Encapsulation Security Payload
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
NAT	Network Address Translation
MPLS	Multiprotocol Label Switching

SUMÁRIO

1 INTRODUÇÃO

No atual cenário empresarial e coorporativo a internet possui um papel fundamental na comunicação entre os diversos segmentos de uma organização. As grandes empresas necessitam de uma infraestrutura capaz de atender suas demandas, sejam elas conectivas ou geográficas, já que muitas delas possuem filiais que funcionam longe de suas sedes, fugindo assim do alcance de uma rede privada local. Tanenbaum (2003) elucida que, para uma empresa que possuísse um segmento geograficamente distante conseguisse estabelecer uma rede privada, era necessário implementar quilômetros de linhas dedicadas de companhias telefônicas. Como seria financeiramente inviável ou insustentável manter uma rede física dedicada para a comunicação, surgiu o que se conhece como Redes Privadas Virtuais (RPV, ou VPN, sigla em inglês para *Virtual Private Network*), por meio da internet pública e utilizando o protocolo TCP/IP, garantem a comunicação entre os diversos setores fisicamente distantes de uma organização (KUROSE, 2010).

Para compreender o conceito de VPN, é necessário entender tudo aquilo que envolve sua implementação e gestão. Para que exista um serviço de qualidade quando for estabelecida, é necessário atentar para conceitos importantes no tráfego de informações na internet. Chin (2006) afirma que, acima de tudo, uma VPN deve garantir a segurança da informação transmitida satisfazendo os conceitos de confidencialidade, autenticidade e disponibilidade. Tal cuidado deve ser tomado devido ao tráfego ser estabelecido na rede pública da internet, deixando a informação quando não protegida a mercê de ataque por parte de terceiros – expondo os dados a terceiros que não possuem autorização para acessar aquela informação. A tecnologia VPN é capaz de se adequar aos mais diversos cenários e situações dentro de um ambiente coorporativo, tornando-a dessa forma, ideal para as características e particularidades da rede interna de cada organização, com uso de protocolos que asseguram o serviço e garantem a segurança da informação.

O presente trabalho apresenta os principais aspectos relacionados as Redes Privadas Virtuais. De forma teórica e prática conceitos como o tunelamento de uma VPN, seus protocolos de segurança e também seus principais tipos e cenários são apresentados. Do ponto de vista prático, os principais cenários em que se pode estabelecer/implementar uma VPN são simulados por meio do *Software* CISCO *Packet Tracer*, analisando parâmetros de estabelecimento e qualidade de serviço em uma VPN, investigando seus efeitos no funcionamento da rede.

1.1 JUSTIFICATIVA

O meio coorporativo é definido como a junção entre a matriz da organização, suas filiais, seus fornecedores e distribuidores, parceiros de negócio, clientes e usuários móveis, que por meio da comunicação entre todas essas partes interessadas se estabelece a infraestrutura fundamental de qualquer corporação moderna (NAKAMURA; GEUS, 2013). Com isso, as Redes Privadas Virtuais constituem um papel fundamental na viabilização dessa infraestrutura, tornando o processo de criação das corporações algo financeiramente viável. Quando implementada de acordo com um projeto bem estruturado da rede, a VPN garante também a segurança da informação que será transmitida nessa conexão além de melhorar a flexibilidade e escalabilidade com relação aos diversos usuários que farão uso da conexão (NAKAMURA; GEUS, 2013).

Por conta disso, se torna indispensável conhecer o funcionamento de uma VPN desde seus conceitos mais elementares até seus principais protocolos que garantem a segurança da informação transmitida, além das diversas formas em que se torna possível implementar uma VPN e seus parâmetros de qualidade.

Por meio da revisão de bibliografias e da simulação via *Software* dos principais cenários de uma VPN, este trabalho visa compreender o seu funcionamento e a forma em que se pode ser implementada. Dessa forma, a simulação é a forma mais eficiente e econômica de identificar falhas, garantir a segurança, testar a viabilidade e qualidade de uma VPN sem que seja comprometida nenhuma infraestrutura de rede real (NAKAMURA; GEUS, 2013).

1.2 ORGANIZAÇÃO DO TRABALHO

O conteúdo deste trabalho está subdividido em seções. Na introdução foram apresentados a contextualização, a justificativa e a organização do presente trabalho.

Seção 2 OBJETIVOS

A segunda seção trata dos principais objetivos desse trabalho, dividindo-os em objetivo geral e objetivos específicos.

Seção 3 REFERENCIAL TEÓRICO

Esta seção tem como objetivo descrever os conceitos relacionados a pesquisa de simular Redes Privadas Virtuais por meio do *Software* CISCO *Packet Tracer,* definindo conceitos como VPN, tunelamento, protocolos de segurança, tipos e cenários em que se pode implementar uma VPN. Esse capítulo também descreve simuladores, seus diversos tipos e as principais ferramentas existentes no mercado que podem atender os requisitos de trabalho.

Seção 4 METODOLOGIA

A seção quatro trata dos materiais e métodos utilizados para a construção deste trabalho. Onde os materiais estão relacionados ao que será utilizado e os métodos refere-se a metodologia utilizada para a construção deste trabalho.

Seção 5 RESULTADOS

Aqui são ilustrados os resultados obtidos por meio da simulação de determinados cenários em que se pode implementar uma VPN e o comportamento apresentado nos mesmos.

Seção 6 CONSIDERAÇÕES FINAIS

Esta seção trata das considerações finais acerca do trabalho proposto, onde os objetivos gerais e específicos foram atingidos, além de sugestões e formas de lidar com situações existentes na problemática do trabalho.

2 OBJETIVOS

A seguir são elencados os objetivos do trabalho.

2.1 OBJETIVO GERAL

O objetivo geral é simular diversos cenários em que se possa implementar uma VPN. Com isso, pretende-se aprender a como simular uma Rede Privada Virtual, demonstrar os benefícios obtidos com a VPN em redes coorporativas e nas mais diversas organizações que necessitem se comunicar e trocar informações de forma segura, mas que estejam fisicamente distantes.

2.2 OBJETIVOS ESPECIFICOS

Para consecução do objetivo principal, os seguintes objetivos específicos foram definidos:

- Realizar uma revisão bibliográfica sobre VPN: principais conceitos, tipos e cenários em que é possível implementá-la; conceito de tunelamento, seus protocolos de segurança e os principais sistemas disponíveis para simular os cenários escolhidos;
- Definir cenários e situações em que uma VPN pode ser implementada;
- Estudar e aprender a utilizar o *Software* CISCO *Packet Tracer,* para assim simular os cenários em que se aplicam uma VPN.

3 REFERENCIAL TEÓRICO

As Redes Privadas Virtuais garantem a comunicação segura de pequenas e grandes empresas que estão fisicamente distantes entre si, mas que necessitam de uma comunicação privada e segura para compartilhar informações. Por meio do tunelamento e dos protocolos de segurança, os diversos tipos de VPN garantem essa comunicação virtual e privada. A seguir serão apresentados os principais aspectos sobre a tecnologia de Redes Privadas Virtuais utilizados no presente trabalho.

3.1 REDES PRIVADAS VIRTUAIS

Uma Rede Privada Virtual (RVP ou VPN, sigla em inglês para *Virtual Private Network*) é uma rede virtual responsável pelo transporte de tráfego privado seguro na rede pública de internet utilizando o tunelamento e criptografia dos dados (MORAES, 2010).

Uma VPN permite que o usuário estabeleça uma conexão ponto-a-ponto por meio de um túnel que forma uma ligação entre sistemas finais, sejam eles uma rede coorporativa ou um sistema remoto, viabilizando ao usuário acesso a rede local privada da organização. A Figura 1 apresenta um esquema de uma VPN típica. O pacote original, antes de ser encaminhado por meio do túnel, tem anexado a si um cabeçalho adicional que possui um protocolo de segurança para garantir a autenticidade da informação quando for transmitida por meio do túnel virtual estabelecido na rede pública. Esse túnel pode ser estabelecido por meio de uma rede local (LAN, sigla em inglês para *Local Area Network*) em uma filial ou um *Home Office* a partir de um roteador extranet ou aplicativo de acesso remoto presente nesses ambientes e habilitados para conexão VPN. Esse mesmo túnel pode ser finalizado por um *Gateway* VPN em um roteador extranet de um ISP (sigla para *Internet Service Provider*, termo em inglês para referenciar o provedor de acesso à Internet).

Além do tunelamento, a criptografia possui papel fundamental em uma VPN, pois é por meio dos mecanismos de criptografia que se garante a segurança da informação transmitida por meio do tunelamento.

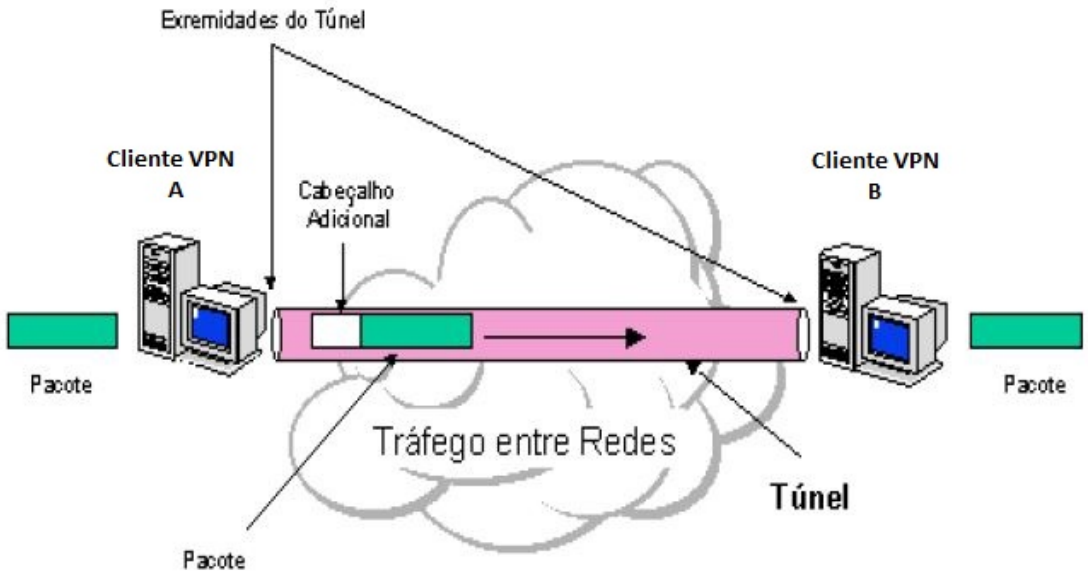

Figura 1: Transmissão de um pacote por meio de uma VPN entre dois clientes remotos sob a internet pública.
Fonte: Adaptado de CHIN (1998).

A depender do cenário no qual a VPN será empregada, níveis e estratégias de segurança distintas são necessários, e assim, diferentes algoritmos/mecanismos são empregados. Para túneis/VPNs estabelecidos por meio de acesso remoto via Software-Cliente e também por meio de um servidor VPN, os algoritmos Layer 2 Tunneling Procotol (L2TP) e o Point-to-Point Tunneling Protocol (PPTP) utilizam apenas a denominada autenticação PPP. O PPP é um protocolo da camada de enlace que trabalha sobre um enlace ponto a ponto. Detalhes sobe o protocolo PPP e sobre os demais protocolos presentes em uma VPN são apresentados na sessão 3.3 PROTOCOLOS DE SEGURANÇA. Dessa forma, o PPP visa garantir que somente pessoas autorizadas sejam capazes de fazer uso daquela conexão e ter acesso às informações disponíveis. Como a autenticação por meio do protocolo PPP não é suficiente, túneis/VPNs estabelecidos por meio de Software-Cliente, servidores VPN e *Gateway* também utilizam o protocolo IP Security (IPSec) para garantir a integridade e sigilo de pacotes além de prover melhores mecanismos de autenticação para o túnel.

Como seria financeiramente inviável ou insustentável manter uma rede física dedicada para a comunicação, as VPNs garantem a comunicação entre os diversos setores e filiais da empresa. Segundo Scrimger (2002), é possível multiplicar a quantidade de terminais conectados à rede sem que sejam necessários gastos extras com infraestrutura, pois com o estabelecimento de uma VPN os terminais conectados a uma rede privada passariam a ter as mesmas configurações da rede a que se desejar conectar e com isso passaria a fazer parte da mesma infraestrutura.

Para assegurar o correto funcionamento de uma VPN e garantir o compartilhamento de soluções, é necessário estabelecer o pleno funcionamento dos recursos considerados fundamentais. Os principais recursos são (CHIN, 1998) a **autenticação do usuário** - que se refere à validação da identificação submetida pelo usuário, tornando restrito o acesso somente a pessoas autorizadas, sendo necessários mecanismos de auditoria que assegurem a veracidade dessas informações; o **gerenciamento de endereços** - para garantir o sigilo do endereço de rede utilizado durante o compartilhamento de recursos fazendo uso de endereços fictícios para o tráfego externo; a **criptografia de dados** - uma vez que os dados devem trafegar na rede pública de forma criptografada para assegurar a autenticidade e integridade da informação; e o **suporte a múltiplos protocolos** - a fim de garantir o funcionamento em diversos tipos de infraestruturas e cenários de VPN.

3.2 TUNELAMENTO

Como mencionando anteriormente, os dados em uma VPN trafegam na rede pública por meio de um túnel lógico. O tunelamento é o estabelecimento de uma ponte (túnel) entre as duas partes da conexão para que a informação seja transmitida de forma privada e segura por meio de uma rede pública (MORAES, 2010). Na Figura 2, é ilustrado o conceito de tunelamento. Como mostra a figura, as informações que são transmitidas do Cliente VPN para o Servidor VPN atravessam um túnel virtual estabelecido sob a infraestrutura pública da internet, ficando encapsulado dentro do mesmo. Dessa forma, deixa as informações contidas dentro de cada pacote impossíveis de serem compreendidas caso seja interceptada por terceiros que não estejam autorizados. Com essa característica, os dados trafegados por meio de uma VPN se tornam seguros.

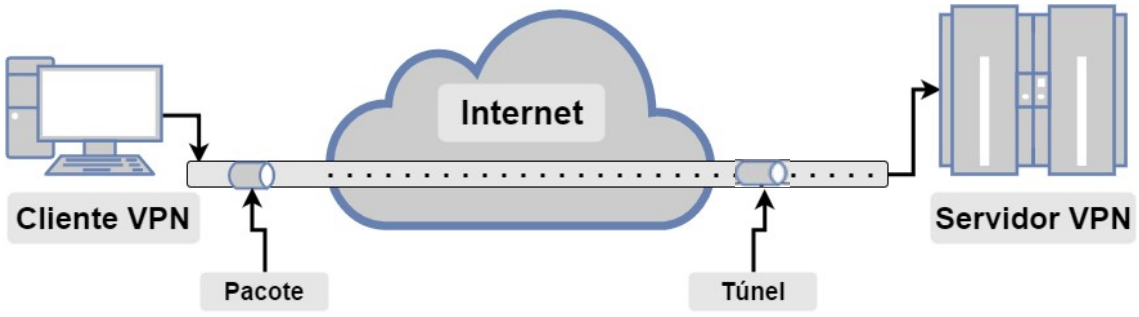

Figura 2: Tunelamento entre um cliente remoto e um servidor VPN na internet, conectando-se a rede local privada da organização.
Fonte: Autoria própria (2016).

Durante o estabelecimento da VPN, é na fase de tunelamento que os dados transportados são encapsulados (VELLOSO, 2011). Nessa fase são adicionados cabeçalhos contendo informações que vão desde o roteamento na rede pública até o desencapsulamento no usuário final.

Atrelado ao conceito de tunelamento, tem-se os conceitos de criptografia. A criptografia que tem como objetivo garantir a integridade, autenticidade e confidencialidade das conexões virtuais. Dessa forma é possível garantir a segurança dos dados transportados, valendo-se de diversos protocolos de segurança existentes, que são discutidos na sessão 3.3 PROTOCOLOS DE SEGURANÇA.

Para garantir essa autenticidade, a informação é certificada nas extremidades do túnel afim de assegurar que a mesma veio de usuários válidos. Estes algoritmos, em geral, adicionam um cabeçalho extra ao pacote conferindo sigilo aos dados dentro do túnel. A Figura 3 ilustra o conceito e encapsulamento. Na primeira parte (1) o cliente VPN adiciona um cabeçalho extra ao pacote original de forma a criptografar o mesmo antes de encaminhá-lo ao túnel; na segunda parte (2), o pacote já está encriptado e sendo transmitido de forma segura dentro do túnel; na terceira parte (3), o pacote é decriptado pelo servidor VPN após verificar-se que o mesmo se trata do pacote encaminhado pelo cliente VPN (NAKAMURA; GEUS 2013).

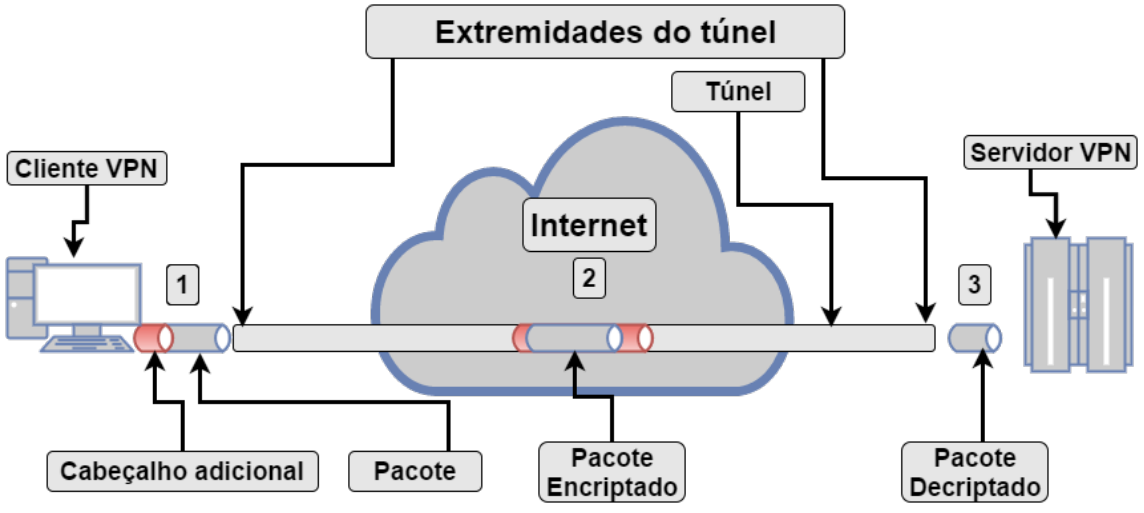

Figura 3: Encapsulamento e desencapsulamento de um pacote em um túnel VPN. Na primeira parte, o cliente VPN adiciona ao pacote original um cabeçalho responsável por realizar a encriptação. Na segunda parte, o pacote já encriptado é transmitido de forma segura dentro do túnel. Na terceira e última parte, o servidor VPN, após verificar a autenticidade do pacote, é responsável por decriptar e extrair o conteúdo original.
Fonte: Autoria própria (2016).

A seguir, apresentam-se os principais protocolos de segurança relacionados às Redes Privadas Virtuais, apresentando seu funcionamento e suas principais características.

3.3 PROTOCOLOS DE SEGURANÇA

Para que se torne possível aplicar os conceitos de tunelamento e criptografia, são necessários protocolos que viabilizem essa conexão e garantam a segurança da VPN (SANTANA, 2010). Segundo Moraes (2010), dentre as várias maneiras existentes para implementar uma VPN, em cada uma delas se faz uso de diferentes protocolos que se encontram em diferentes camadas do modelo OSI (sigla para *Open System Interconnection*, termo em inglês para referenciar o modelo de rede de computador dividido em camadas de funções).

Dentro da camada 2 ou de enlace temos os protocolos L2TP (*Layer 2 Tunneling Protocol*) e PPTP (*Point-to-point Tunneling Protocol*). Na camada 3 ou de rede, temos o protocolo IPsec (*Internet Protocol Security*). O tunelamento na camada de enlace possui inicialização bidirecional do túnel, fazendo com que os protocolos da camada 2 sejam mais empregados em conexões nas quais o custo esteja relacionado com sua utilização. Possuem desvantagens relacionadas a confiabilidade, padronização incompleta e escalabilidade (NAKAMURA; GEUS, 2013). Os protocolos de rede ou do nível 3 da camada OSI, por sua vez, garantem a escalabilidade além de vantagens de segurança e confiabilidade. Todavia, possui desvantagem ao que se refere ao número de fabricantes que implementam essa tecnologia e a sua complexidade de desenvolvimento (NAKAMURA; GEUS, 2013).

As principais características e funcionalidades dos principais protocolos de segurança utilizados em uma VPN serão apresentadas a seguir.

3.3.1 *Point-to-Point Tunneling Protocol* (PPTP)

O protocolo PPTP teve seu desenvolvimento concebido em 1999 pela união de algumas empresas, entre elas a Microsoft, 3Com, ECI Telematics, US Robotics e Ascend, sendo elas pertencentes a um grupo chamado PPTP Forum e foi um dos primeiros protocolos a surgir para o uso em Redes Privadas Virtuais (REZENDE; GEUS, 2002).

Seu principal objetivo era dividir as funções do acesso remoto para que a empresa e seus funcionários pudessem fazer uso da infraestrutura pública da internet para empregar uma conexão segura entre redes privadas e seus clientes remotos (REZENDE; GEUS, 2002).

Tal protocolo é originário do PPP, que é bastante utilizado para acesso remoto na internet em enlaces do tipo ponto-a-ponto, em que ambos os lados da conexão podem ajustar quesitos como o endereço IP e tamanho dos pacotes a serem transmitidos, além de um modelo de autenticação por parte do cliente para garantir a autenticidade e confiabilidade da conexão (KUROSE, 2010).

O protocolo PPP ainda se caracteriza por um mecanismo de enquadramento multiprotocolo, habilitando-o a ser utilizado em modems, linhas seriais e em outras camadas físicas da rede, além de ser capaz de detectar erros e compactar cabeçalhos. Ao que diz respeito a negociação de informações durante a conexão, o PPP é capaz de negociar o tamanho máximo da carga útil para quadros de dados, habilitar a autenticação e escolha do protocolo a ser utilizado, além de também habilitar o monitoramento da qualidade do enlace durante a conexão (TANENBAUM, 2010).

A conexão no PPTP utiliza o PPP para discar a um servidor de acesso ISP por meio de uma linha telefônica ou ISDN (sigla para *Integrated Service Digital Network*, termo em inglês que referencia o conjunto de padrões de comunicação para transmissão digital simultânea de voz, vídeo, dados e outros serviços de rede sobre a rede pública de telefonia) garantindo a transferência de pacotes ao cliente. Logo após, é estabelecida uma nova conexão sob a mesma conexão PPP já existente, provendo o mecanismo para o túnel na rede local da corporação, viabilizando o acesso remoto.

Antes de enviar o datagrama, o PPTP cifra e encapsula o mesmo por meio do protocolo PPP, que por sua vez encapsula o mesmo pacote em um pacote GRE (*Generic Routing Encapsulation)*, que é um protocolo de tunelamento desenvolvido pela CISCO em parceria com a Juniper que serve para estabelecer o túnel, mas que não garante a segurança do mesmo, contendo em seu cabeçalho o endereço final (REZENDE e GEUS, 2002). A Figura 4 apresenta o datagrama do protocolo PPTP com uso do PPP e do GRE.

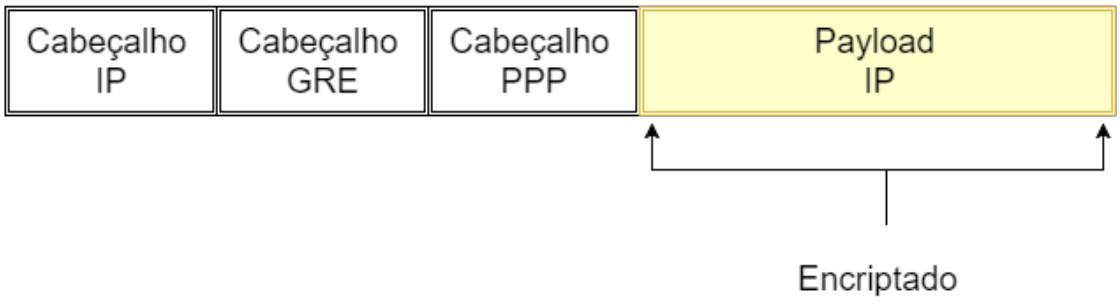

Figura 4: Datagrama IP encapsulado por meio do protocolo PPTP valendo-se do protocolo PPP e do Protocolo GRE. O protocolo GRE garante o estabelecimento do túnel e o protocolo PPP garante a segurança desse mesmo túnel.

Fonte: Adaptado de REZENDE; GEUS (2012)

Apesar da massiva utilização do protocolo PPTP, este possui uma grande desvantagem de segurança com relação aos demais. O seu procedimento de negociação de parâmetros antes de garantir a segurança no tráfego entre os sistemas finais, permite a um atacante modificar esses mesmos parâmetros e obter informações que comprometam a confiabilidade, autenticidade e integridade da conexão. Essas informações vão desde o endereço IP dos sistemas finais até o *Hash* (termo em inglês para o valor sumarizado obtido após o escrutínio de um conjunto de dados) contendo o nome de usuário e senha.

Ao utilizar o PPTP, a técnica de tunelamento é iniciada pelo usuário em seu sistema operacional por meio de uma aplicação que disponibilize o estabelecimento de uma conexão VPN. Dessa forma, o PPTP torna-se mais adequado para conexões entre clientes remotos que podem ser iniciadas de qualquer lugar por meio de um terminal e *Software* habilitados a estabelecer tal conexão, como ilustra a Figura 5.

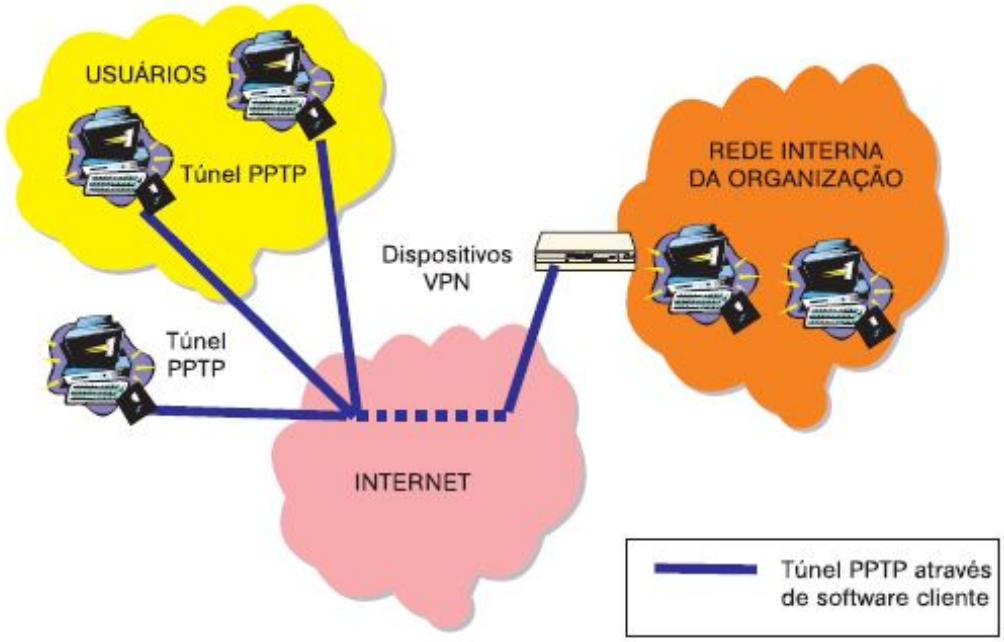

Figura 5: Aplicação do protocolo PPTP por meio de uma conexão VPN do tipo *Software*-Cliente onde a geração do protocolo é feita no sistema operacional do usuário, por meio de um *Software* habilitado a estabelecer tais conexões.

Fonte: NAKAMURA e GEUS et al (2013).

3.3.2 *Layer Two Tunneling Protocol* (L2TP)

Criado pela CISCO Systems, o L2TP surgiu como uma alternativa para o PPTP e assim como o precedente, o L2TP utiliza o PPP para prover acesso *Dial-Up* (termo em inglês para referenciar a forma de acesso à internet que usa a rede pública de telefonia para estabelecer conexão com o ISP) e assim dar início ao procedimento de tunelamento (REZENDE; GEUS, 2002).

Esse protocolo, por meio do ISP, troca mensagens PPP com os usuários remotos e requisições com o servidor L2TP para poder estabelecer o túnel. Após estabelecido o tunelamento, os dados são transmitidos entre as extremidades da conexão ponto-a-ponto. Os datagramas transmitidos pelo usuário são aceitos em um concentrador, encapsulados em pacotes do tipo L2TP e encaminhados pelo túnel para o sistema final, onde no *Gateway* de destino, esses mesmos datagramas são desencapsulados e enviados de forma original para a porta de acesso do sistema final (CELESTINO, 2005).

Diferente do PPTP, o L2TP inicia o tunelamento no *Gateway* do provedor ISP e não por meio de software no sistema operacional do usuário, como ilustra a Figura 6.

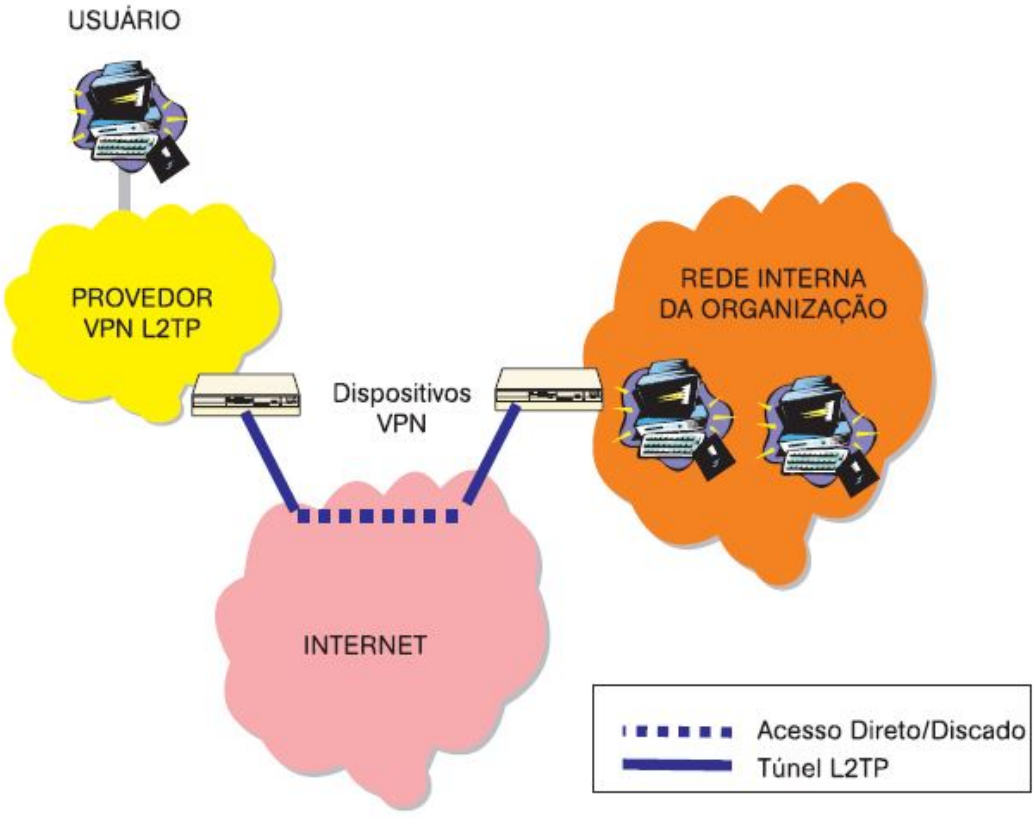

Figura 6: Aplicação do protocolo L2TP por meio de uma conexão VPN estabelecida somente no *Gateway* do roteador do ISP.

Fonte: NAKAMURA e GEUS et al (2013).

Com relação à segurança, o L2TP por encapsular seus pacotes por meio do protocolo PPP, pode também fazer uso dos mecanismos de autenticação do PPP bem como utilizar os mecanismos descritos pelo Protocolo de Controle de Cifragem (PCCi ou ECP, sigla em inglês para *Encryption Control Protocol*), que é um protocolo que tem como objetivo permitir a encriptação e decriptação dos pacotes pelos algoritmos de criptografia nas extremidades do túnel e pelo Protocolo de Controle de Compressão (PCCo ou CCP, sigla em inglês para *Compression Control Protocol*) que é um protocolo responsável por garantir a compressão e descompressão dos dados nas extremidades do túnel, além de também sinalizar falhas no processo de compressão/descompressão dos pacotes, ambos utilizados pelo PPP (REZENDE; GEUS, 2002).

Os ataques nos quais o túnel tende a ficar exposto podem ser capazes de extrair informações como a identidade do usuário, modificar e sequestrar pacotes, sequestrar o túnel L2TP ou a conexão PPP, ataques de negação de serviço (*Denial of Service* - DoS), interrupção de negociação e enfraquecimento do processo de autenticação PPP (NAKAMURA; GEUS, 2013). Para assegurar a conexão e evitar problemas de segurança, o uso do protocolo L2TP deve sempre ser mesclado com o de outro protocolo capaz de suprir as suas carências relacionadas à segurança do túnel.

Desse modo, tanto o L2TP quanto o PPTP precisam de outro protocolo para assegurar o sigilo, autenticidade e a integridade dos pontos conectados e que realizam a troca de informação por meio do acesso remoto. Esse protocolo é o IPsec e será apresentado a seguir.

3.3.3 *IP Security* (IPsec)

Definido pelo IETF (*Internet Engineering Task Force*) como um padrão que tem como principal propósito oferecer mecanismos contra o monitoramento e controle de tráfego não autorizado em uma rede, o IPsec é baseado em três funcionalidades essenciais: o cabeçalho de autenticação (*Authentication Header* - AH), o cabeçalho de encapsulamento (*Encapsulation Security Payload* - ESP) e o protocolo de negociação e troca de chaves (*Internet Key Exchange* - IKE) (REZENDE; GEUS, 2002).

O AH é um cabeçalho que é acrescido ao pacote IP, contendo informações sobre a autenticação da mensagem, que deve ser verificado pelo receptor da mensagem; além disso tem como objetivo assegurar a origem dos pacotes e garantir a autenticidade dos mesmos, podendo também proteger contra os ataques de *Spoofing*, onde o IP de origem é oculto de

forma a mascarar endereços de IP falsos. Já o ESP garante o sigilo dos dados que são transmitidos pela rede pública por meio do encapsulamento e encriptação dos pacotes, assegurando que o conteúdo daquele pacote só possa ser lido pelo seu destinatário.

Segundo Rezende e Geus (2002), a principal diferença entre o AH e o ESP está relacionado a abrangência do serviço, em que o AH protege todos os campos do cabeçalho IP antecessores ao encapsulamento ESP, enquanto esse segundo alcança apenas o seu próprio cabeçalho e os dados do pacote. Outra diferença relevante entre o AH e o ESP é que o AH garante a autenticidade e integridade do pacote, mas não garante o sigilo do mesmo, diferente do ESP que garante a autenticidade, integridade e também o sigilo do pacote (KUROSE, 2010).

Uma outra característica essencial do IPsec é a associação de segurança (*Security Association* - SA), técnica pela qual são definidos e negociados atributos relacionados à segurança. Os atributos a serem compartilhados são algoritmos a serem utilizados, chaves de criptografia e vida útil das mesmas, informações sobre o fluxo de dados, tempo de duração, além de informações que devem ser compartilhadas entre as partes atuantes (NAKAMURA; GEUS, 2013).

A associação de segurança pode ser estabelecida de forma estática ou dinâmica. Na forma estática os parâmetros são inseridos de forma manual nas duas extremidades do túnel. Quando a associação de segurança é estabelecida de forma dinâmica, os parâmetros são negociados por meio do mecanismo de troca de chaves sem que haja intervenção externa (REZENDE; GEUS, 2002). Rezende e Geus (2002) afirmam que a escalabilidade do IPsec está relacionada a implementação eficaz de associações de segurança, quando são estabelecidas pela conexão ou por usuários a fim de fornecer mais segurança.

Já com relação as trocas de chave, é por meio do IKE que as mesmas são trocadas de forma segura entre as organizações. O IKE faz uso de outro protocolo que serve como base para criar as associações de segurança, denominado ISAKMP (*Internet Security Association Key and Management Protocol).* O protocolo ISAKMP tem como principal objetivo gerenciar as políticas de troca de chaves e criar uma estrutura homogênea para a geração de chaves, garantindo a compatibilidade das mesmas. Fazendo uso do ISAKMP para a criação das SAs que serão utilizadas pelos protocolos AH ou ESP, é criado um canal seguro e bidirecional onde nesse canal estão contidos as chaves de segurança e os algoritmos de criptografia que serão utilizados nas negociações (MENDONÇA, 2009).

Existem dois modos de implementação do IPsec: o modo transporte e o modo túnel. O modo transporte, que também é o modo nativo do IPsec, tem seus cabeçalhos de segurança

inseridos após o cabeçalho IP, onde além de seu cabeçalho original e sua carga, são anexados o cabeçalho do IPsec contendo o protocolo AH e/ou ESP que garantem a autenticação dos dados. Nesse caso, o cabeçalho IP original não sofre alterações, mantendo, por exemplo, seus endereços de origem e de destino. A Figura 7 ilustra o cabeçalho IPsec no modo transporte. Esse modo de utilização do IPsec é comumente utilizado para conexões do tipo Cliente-para-Cliente entre dois sistemas finais (REZENDE; GEUS 2002).

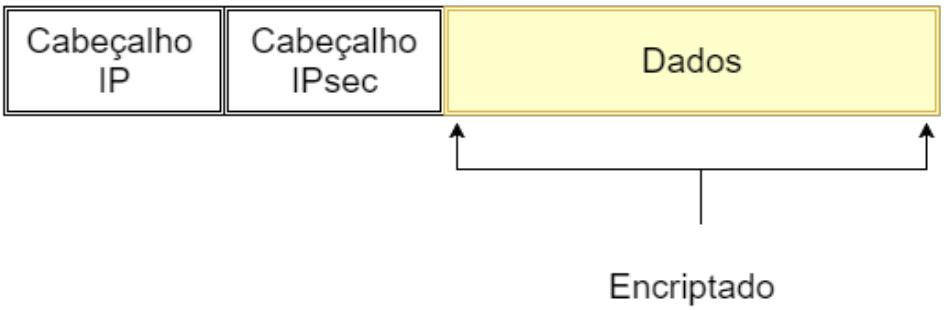

Figura 7: Codificação do protocolo IPsec no modo transporte. O cabeçalho do IPsec é inserido após o cabeçalho IP inalterado e os dados do pacote são encriptados pelo IPsec, que fornecem além da criptografia, a autenticação. Fonte: Adaptado de MENDONÇA (2009).

Já no modo túnel, o pacote IP é totalmente encapsulado e são acrescidos a ele: um novo cabeçalho IP - que é utilizado para o roteamento do pacote na rede pública por meio de um NAT (*Network Address Translation*) e o cabeçalho IPsec - que implementa o protocolo AH e/ou ESP para garantir a autenticidade e segurança do pacote. Verificada a autenticidade do pacote, o cabeçalho IPsec é removido e o pacote original é reconstruído e decodificado no destino. A Figura 8 ilustra o cabeçalho IPsec no modo túnel. Na figura podemos ver a adição de um novo cabeçalho e do cabeçalho IPsec ao pacote original. Nesse modo, o *Gateway* é tratado como um roteador de borda, onde o *Gateway* local envia o pacote protegido com IPsec pelo túnel até o *Gateway* remoto ou de destino, que após receber o pacote o decodifica transmite ao cliente remoto a informação desencapsulada, ou seja, o pacote original. (REZENDE; GEUS 2002).

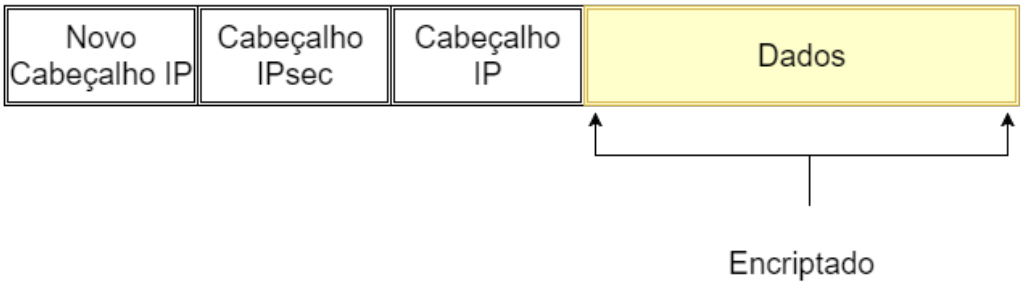

Figura 8: Codificação do protocolo IPsec no modo túnel, onde é acrescido um novo cabeçalho IP que é utilizado para o roteamento do pacote na rede pública fazendo o uso de um NAT para garantir a integridade dos endereços

de origem e destino, além do cabeçalho IPsec contendo o protocolo AH e/ou ESP que garantem a autenticidade e integridade dos dados transmitidos.

Fonte: Adaptado de MENDONÇA (2009).

A Figura 9 ilustra as etapas de como é estabelecida uma VPN por meio do IPsec. Na primeira etapa o *Gateway* verifica se o *Host* (máquina hospedeira) está apto a criar um túnel virtual. Se houver confirmação por parte do *Host*, dar-se início ao segundo passo no qual *Gateway* negocia a associação de segurança. Por último, o *Host* se comunica por meio do túnel estabelecido.

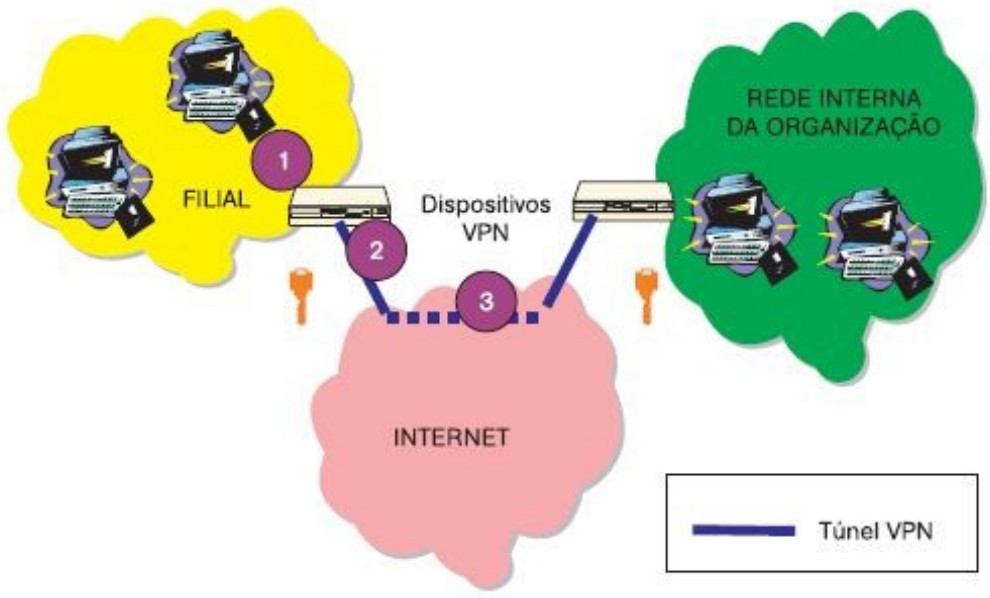

Figura 9: Estabelecimento de uma conexão segura entre dois *Gateways* utilizando IPsec.
Fonte: NAKAMURA e GEUS et al (2013).

3.4 TIPOS/CENÁRIOS DE VPN

Existem diversos tipos/cenários de VPN capazes de garantir a comunicação e a troca de informação de forma segura. Os principais tipos de VPN são: Cliente-para-Cliente, Cliente-para-*Gateway* e *Gateway*-para-*Gateway*.

O modo Cliente-para-Cliente é considerada uma das formas mais simples de se implementar uma VPN. Nesse modo, é estabelecido um canal seguro entre duas máquinas por meio da internet que simula um circuito físico dedicado ou linha privada, não precisam necessariamente estar incluídos em uma rede da corporação, ou seja, pode ser um usuário que precise administrar um sistema remotamente (MARTINS, 2000). Para ilustrar o

funcionamento de uma VPN do tipo cliente-para-cliente, é exibido um computador que se conecta à rede pública e em seguida a um computador remoto, ver Figura 11.

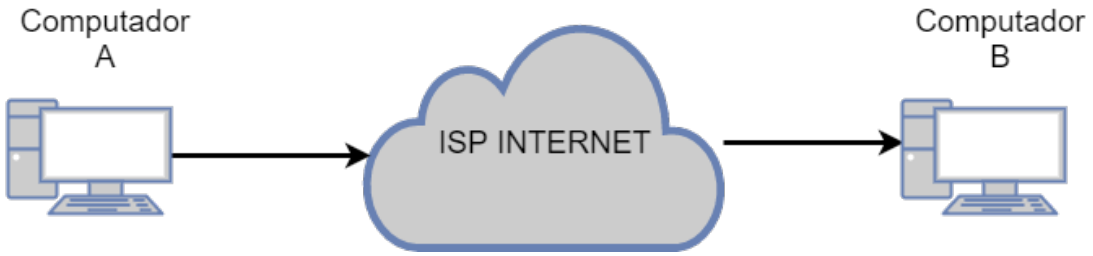

Figura 10: VPN do tipo Cliente-para-Cliente, onde nesse exemplo, dois computadores se comunicam por meio de um circuito físico simulado.
Fonte: Autoria Própria (2016)

No modo Cliente-para-*Gateway*, a VPN permite que um *Host* móvel se comunique a uma rede coorporativa por meio da internet, onde esse *host* móvel é um sistema final que possui um *software* de acesso remoto habilitado a estabelecer uma conexão VPN com a rede privada da organização. Normalmente, esses sistemas finais fazem parte de um *Home Office*, permitindo que em muitos casos os funcionários da organização possam se conectar aos servidores da empresa de onde estiverem. Para garantir a qualidade dessa conexão, é necessária uma largura de banda e enlace bons suficientes de forma a viabilizar a conexão e acesso remoto. Como é ilustrado na Figura 11, diversos sistemas finais podem acessar a rede privada, desde que possuam um *Software* habilitado para conexão VPN (MARTINS, 2000).

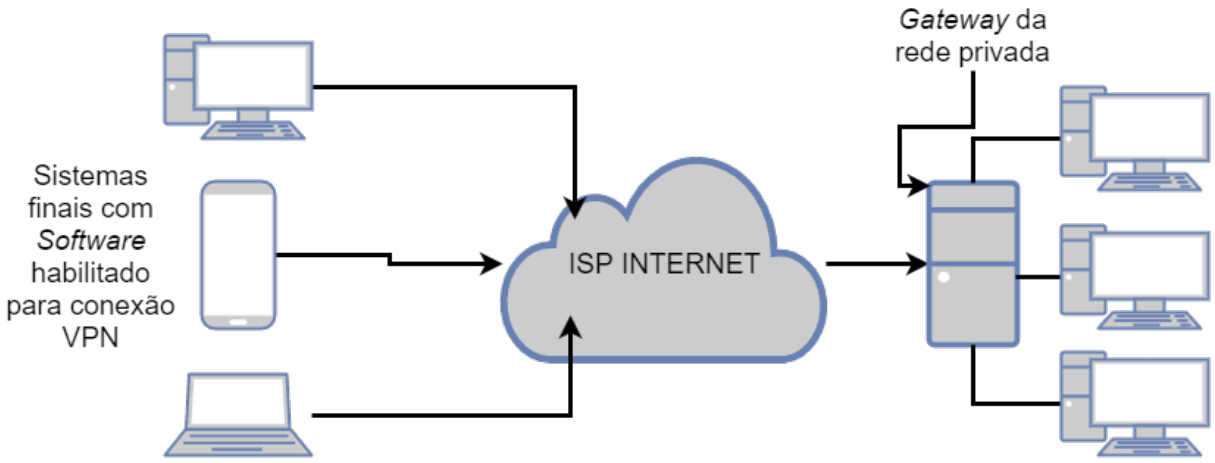

Figura 11: Conexão VPN do tipo Cliente-para-*Gateway* da organização, onde um sistema final que possua um Software habilitado para a conexão VPN e autorizado dentro da rede da organização é capaz de se conectar a mesma.
Fonte: Autoria Própria (2016)

Por último se tem o modo *Gateway*-para-*Gateway*, onde existe um *Gateway* nas extremidades do túnel responsável por enviar e receber os pacotes encapsulados dentro do

túnel, além de verificar a origem dos pacotes e garantir a autenticidade dos mesmos por meio dos protocolos de segurança já citados. Nesse tipo de VPN, redes fisicamente distantes podem se comunicar por meio de uma VPN. Por exemplo, empresas que possuam filiais em outras cidades podem estabelecer uma VPN entre suas duas redes de forma a permitir a troca de informações. É possível ver na figura 12 uma rede privada A (que pode ser a sede de uma organização) se comunicando com outra rede B (pode ser a filial dessa mesma organização, mas que pode estar distante fisicamente) (MARTINS, 2000).

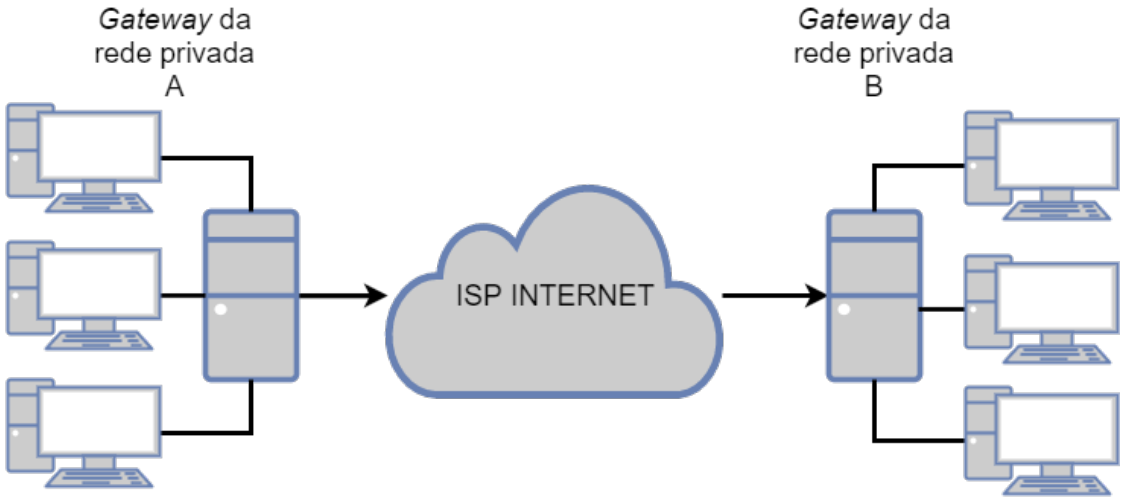

Figura 12: Conexão VPN do tipo *Gateway*-para-*Gateway*, onde duas redes fisicamente separas se comunicam e trocam informações por meio do estabelecimento de uma VPN. O *Gateway* da rede A ao transmitir o pacote por meio do túnel espera que o *Gateway* da rede B verifique a origem do pacote, desencapsule o mesmo e o transmita o pacote original ao seu sistema de destino.
Fonte: Autoria Própria (2016)

Esses diversos tipos de VPN garantem a economia da organização com relação a infraestrutura de rede e segurança da informação, pois quando um desses modelos de VPN é aplicado de forma correta e com os protocolos corretos, é possível obter uma qualidade de serviço com relação a disponibilidade do serviço oferecido e assegurar o pleno funcionamento do tráfego de informação necessário a realização das atividades da empresa (VALENTE, 2010).

Com o propósito de evitar erros no planejamento e implementação, a simulação de diversos cenários de uma VPN permite que sejam testadas todas as funcionalidades da rede e garante um panorama de como a mesma funcionaria na realidade (DIAS FILHO, 2011). Erros cometidos não comprometem a rede simulada, pois é possível reiniciar o processo e simular novamente o cenário desejado quantas vezes se achar necessário, economizando dessa forma, recursos que seriam desperdiçados se a rede tivesse que sofrer mudanças depois de implementada.

3.5 SIMULADORES

Com o propósito de evitar erros no planejamento e implementação, a simulação de diversos cenários de uma VPN permite que sejam averiguadas as funcionalidades requeridas pela rede, prevendo seu comportamento antes da implementação.

3.5.1 Modelos de simulação

Existem diversos modelos que tem como objetivo avaliar e medir o desempenho de uma rede simulada, sendo que os mesmos servem para garantir a qualidade e coerência dos cenários em estudo, garantindo a qualidade do processo de simulação. Dentre os principais modelos contidos nos simuladores, destacam-se:

1. O MODELO COM CENÁRIOS REAIS: Esse modelo faz uso de uma infraestrutura real para simular os diversos cenários desejados. Possui um grande custo, demanda muito tempo para instalar e adaptar os equipamentos a cada cenário desejado e necessita de técnicas para coletar e analisar os dados obtidos por meio da simulação; por outro lado, oferece uma visão ampla e realística do que se deseja.
2. MODELOS ANALÍTICOS: Faz uso de modelos estatísticos e matemáticos para analisar os cenários simulados das diversas formas possíveis, garantindo um alto grau de confiança nos dados obtidos. Tem como desvantagem a necessidade de pessoal específico para adaptar as diversas variáveis e analisar os dados obtidos.
3. MODELOS COMPUTACIONAIS: Os modelos computacionais funcionam por meio de softwares específicos que simulam os diversos cenários possíveis, garantindo uma previsão do funcionamento daquilo que se deseja simular. Sua principal vantagem é seu baixo custo de implementação, que dispensa a necessidade de grandes gastos com infraestrutura. Por outro lado, é necessário que exista um treinamento por parte do usuário para que se use os recursos de forma correta, sem que sejam gerados dados inconsistentes.

Na Tabela 1 são ilustrados os três principais modelos de simuladores, expondo suas principais vantagens e desvantagens.

Tabela 1: Os três principais modelos de simuladores, com suas vantagens e desvantagens.
Fonte: Autoria Própria (2016).

	Vantagens	**Desvantagens**
Modelos com cenários reais	Ampla visão da rede simulada.	Alto custo, implementação demorada.
Modelo analítico	Resultados com alto grau de confiança.	Conhecimento técnico necessário para análise dos dados.
Modelo computacional	Baixo custo, fácil implementação.	Necessário treinamento para utilizar o *Software*.

3.5.2 Principais *Softwares* para simulação

Para o trabalho em questão, será usado a simulação com base no modelo computacional. Para tanto faz-se necessário conhecer as principais ferramentas capazes de atender as necessidades em questão e simular uma VPN em diversos cenários possíveis.

A seguir serão apresentadas as principais ferramentas disponíveis para a simulação de redes, e em especifico, Redes Privadas Virtuais.

OPNET

O OPNET trata-se de simulador largamente utilizado dentro do âmbito coorporativo e acadêmico, com o propósito de simular diversas situações relacionadas a redes de computadores. Trata-se de um simulador orientando a eventos, onde os códigos são executados a medida em que algum evento especifico ocorre. O OPNET é baseado em três níveis hierárquicos de implementação: rede, nó e processo. Nesse simulador, existem editores para cada um desses níveis hierárquicos (PEREIRA, 2004).

O editor de rede ou de projeto tem como objetivo fornecer um espaço para a distribuição dentro do cenário imaginado, interligação e conexão das partes envolvidas na simulação e configuração de cada uma dessas partes dentro daquilo que se deseja simular.

Já o editor de nó serve para modelar o funcionamento interno de um nó (PEREIRA, 2004). Essa modelagem funciona de acordo com a distribuição e conexão dos elementos existentes dentro da rede simulada.

Por fim, o editor de processo é a implementação por meio de variáveis e linhas de código da configuração e transição de estados por meio do caminho seguido por um pacote simulado.

CISCO PACKET TRACER

Trata-se de um programa de simulação desenvolvido pela CISCO *Systems* voltado para estudantes e profissionais das áreas de telecomunicação e redes de computadores, onde por meio de sua interface e ferramentas é possível simular comportamentos em diversos tipos de cenários (RUSSO, 2012).

A ferramenta foi construída para atender demandas relacionadas a escalabilidade dentro das simulações que envolvem o hardware de rede ou periférico conectado à mesma rede (FREZZO, BEHRENS e MISLEVY, 2009). Por meio do CISCO Packet Tracer é possível visualizar, simular, criar, avaliar e contar com recursos de colaboração que auxiliam o ensino e também validam modelos propostos para teste. É possível simular o funcionamento de diversos protocolos tanto para as Redes Locais (LAN) como também para as Redes de Longa Distância (WLAN), com suporte para *Switches,* roteadores, terminais, ISPs, e diversas outras partes de uma infraestrutura de redes, além do suporte para a simulação em um ambiente cooperativo e multiusuário.

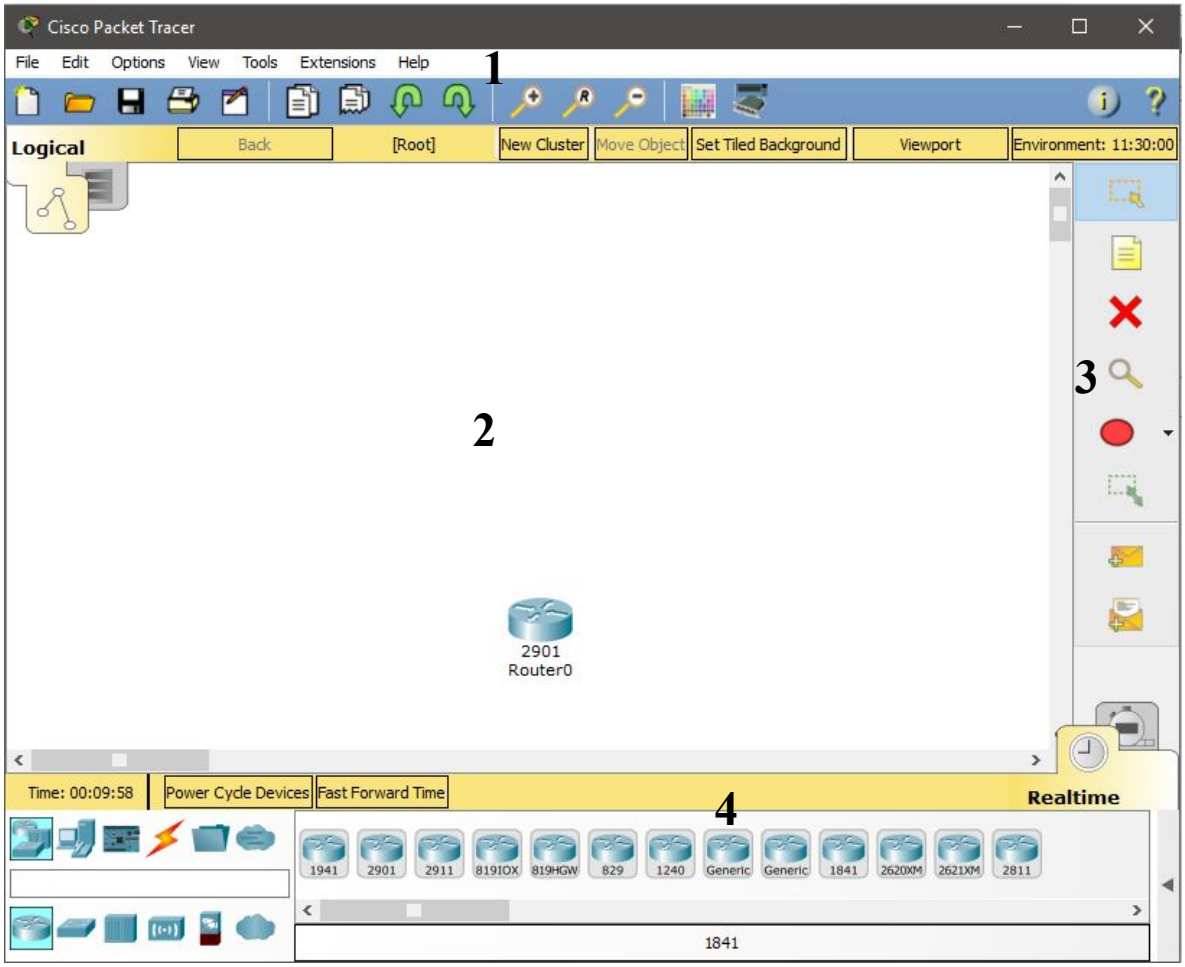

Figura 13: Interface do *Software* de simulação CISCO *Packet Tracer*, onde são exibidos suas ferramentas e ambiente de trabalho. (1) Na parte superior estão as opções de salvar, copiar, colar, paleta de cores e outras ferramentas básicas; (2) A tela em branco é o espaço utilizado para criar os diagramas de rede e modelar o cenário a ser simulado; (3) Opções de seleção, caixa de texto e redimensionar imagem também são opções disponíveis no sistema. (4) Ícones que representam o hardware a ser simulado, de forma a garantir a fidelidade da simulação.

O Packet Tracer é uma ferramenta fechada e com isso é impossível fazer modificações em sua estrutura, ficando responsável por isso seu desenvolvedor que frequentemente lança novas versões do sistema. A interface intuitiva e de fácil compreensão facilita o processo de modelagem dos cenários de rede, assegurando maior fidelidade a ideia proposta. A aplicação ainda suporta um interpretador para que a configuração dos hardwares seja feita via linha de comando. A Figura 13 apresenta uma imagem da interface do CISCO *Packet Tracer* e descrição de algumas de suas ferramentas que vão desde paletas de cores simples até ícones que representam o hardware de rede a ser simulado; contador de tempo para o tempo gasto no ambiente de simulação, caixa de seleção, caixa de texto e redimensionar objeto; ícones que representam alguns dos hardwares de rede da CISCO e simulação em tempo real.

GNS3

É um *Software* gratuito sob licença da GNU que fornece ao usuário um ambiente capaz de construir topologias e criar cenários onde se possam realizar simulações de rede de acordo com o que o usuário deseje simular.

O GNS3 possui diversos emuladores de sistemas operacionais para que se possam criar topologias e cenários sem que o usuário fique limitado a um único tipo de sistema ou fabricante fornecedora de *Hardware* de rede. Além de componentes intermediários da rede (como roteadores, *Switches* e etc), no GNS3 também é possível realizar a emulação de sistemas operacionais para o usuário final como Linux e Windows (SOUZA; SILVA; SOUZA, 2016).

Segundo Souza, Silva e Souza (2016), sua principal característica é a capacidade de integração da topologia simulada com um dispositivo real para ambientes de produção que é inserido na rede por meio de um serviço de nuvem emulado pelo próprio *Software*. Uma desvantagem desse *Software* é a ausência de um modo de análise de pacotes próprio, sendo necessário a utilização de softwares de terceiros para análise do tráfego.

Por mim, também possui uma vasta quantidade de material para estudo e uma comunidade ativa que dá suporte de forma colaborativa ao sistema. Possui também treinamentos oferecidos pelos desenvolvedores para quem desejar obter certificação na plataforma GNS3.

4 METODOLOGIA

A seguir são apresentados os materiais e métodos utilizados para o desenvolvimento deste trabalho.

4.1 MATERIAL

Para a simulação dos cenários descritos neste trabalho, será utilizado o *Software* CISCO *Packert Tracer* versão 6.0.1.0011 que será responsável pela construção dos modelos a serem simulados e especificação das configurações relacionadas a rede.

4.2 MÉTODOS

Após o estudo e revisão da literatura sobre os principais aspectos envolvendo a os conceitos de VPN, sobre as técnicas de tunelamento, os principais protocolos de segurança, dos tipos e cenários de implementação de uma VPN e utilização do *Software* CISCO *Packet Tracer* (CPT), dar-se início a implantação de uma VPN por meio do CPT.

As simulações serão realizadas para os três diferentes protocolos de segurança PPTP, L2TP e IPSec, os quais categorizam os diferentes cenários que uma VPN pode ser implementada. Para cada protocolo, as etapas de criação de topologia, de tabela de endereços, de configuração do protocolo e da geração de tráfego na rede simulada VPN com os protocolos estudados serão apresentados.

A análise dos dados simulados será utilizada para validar a corretude dos parâmetros de configuração e implementação da VPN.

5 RESULTADOS

Os resultados das simulações das Redes Privadas Virtuais no *Software* CISCO *Packet Tracer* seguindo os métodos propostos em diferentes cenários através dos três protocolos de segurança elencados no trabalho, são apresentados nessa seção.

5.1 SIMULAÇÃO VPN COM PROTOCOLO IPSEC.

A simulação a seguir irá demonstrar o funcionamento de uma VPN operando com o protocolo IPsec. Neste cenário, será criado um túnel entre o *Roteador1* e o *Roteador3* via *Roteador2*, ou seja, o *Roteador2* funcionará como o túnel necessário para o estabelecimento da conexão. Os próximos tópicos descrevem todas as etapas, desde a topologia até a configuração dos periféricos, para a simulação do cenário de uma VPN implementada através do protocolo IPSec.

a) Topologia

A topologia apresentada na Figura 15 ilustra como estão distribuídos os equipamentos para estabelecer a VPN neste cenário. Para a construção da VPN serão necessários: três roteadores Cisco 1941, três Switchs Cisco Catalyst 2460 de 24 portas e três computadores genéricos para o teste de envio e recebimento de pacotes. As conexões entre os computadores e Switchs são do tipo LAN, dos Switchs até os roteadores também são do tipo LAN, e para simular a comunicação e garantir a troca de dados entre os roteadores são usadas conexões seriais do tipo DCE (*Data Communications Equipment*). A Fig. 14 ilustra a distribuição do cenário e sua topologia.

b) Tabela de endereços

A Tabela 2 de endereços ilustra as configurações básicas sobre os equipamentos do cenário e informa dados sobre tais dispositivos, suas interfaces e endereços de IP, máscara de rede, *Gateway* e portas do *Switch*. As conexões do tipo DCE possuem uma máscara 255.255.255.254 para que apenas os dois roteadores que vão estabelecer o túnel VPN possam se conectar à rede, evitando que mais dispositivos tenham acesso.

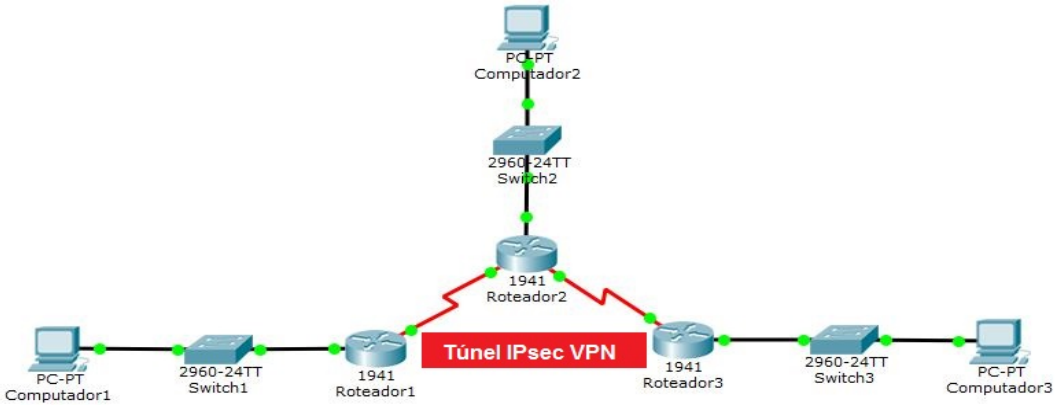

Figura 14: Topologia da VPN *Site-to-Site*(ou *Gateway-to-Gateway)*, com a distribuição e identificação dos equipamentos. Também é possível identificar as conexões estabelecidas, onda as ligações em cor preta são do tipo LAN e as conexões vermelhas do tipo Serial DCE.

Tabela 2: Tabela com os endereços dos dispositivos utilizados na simulação e demais informações como a descrição das interfaces em que estão conectados os dispositivos e o número da porta no Switch em que o equipamento está conectado.

Dispositivo	**Interface**	**Endereço IP**	**Máscara de rede**	***Gateway***	**Porta do *Switch***
Roteador 1	G 0/0	192.168.1.1	255.255.255.0	-	Switch 1 F0/1
	S 0/0/0 (DCE)	10.1.1.2	255.255.255.252	-	-
Roteador 2	G 0/0	192.168.2.1	255.255.255.0	-	Switch 2 F0/2
	S 0/0/0	10.1.1.1	255.255.255.252	-	-
	S 0/0/1 (DCE)	10.2.2.1	255.255.255.252	-	-
Roteador 3	G 0/0	192.168.3.1	255.255.255.0	-	Switch 3 F0/5
	S 0/0/1	10.2.2.2	255.255.255.252	-	-
Computador 1	Inespecífica	192.168.1.3	255.255.255.0	192.168.1.1	Switch 1 F0/2
Computador 2	Inespecífica	192.168.2.3	255.255.255.0	192.168.2.1	Switch 2 F0/1
Computador 3	Inespecífica	192.168.3.3	255.255.255.0	192.168.3.1	Switch 3 F0/18

c) Parâmetros IPsec no Roteador1

O primeiro passo para configurar o IPsec no Roteador1 é verificar se o pacote de tecnologias de segurança está habilitado. Para isso, é necessário usar o comando *show version* dentro da CLI (*Comand Line Interface*) e verificar se a licença do pacote de segurança está

presente. Caso não esteja, utiliza-se o comando abaixo para ativar o pacote de tecnologia que tornará o roteador habilitado para reconhecer os protocolos de segurança necessários para configurar a VPN.

licence boot module c1900 technology-package securityk9

Em seguida, faz-se necessário configurar a lista de controle de acesso para que o tráfego LAN entre o Roteador1 e o Roteador3 seja permitido. Essa lista de acesso serve para identificar e selecionar qual tráfego deve passar dentro daquela rede através da interface ou porta (SIMULATION EXAMS, 2017). Ao configurar a lista de acesso, quando um pacote entre o Roteador1 e Roteador3 trafegar na rede, o protocolo IPsec será implementado e os dados serão criptografados. O comando *acces-list* utiliza um número para que seja possível identificar a lista de acesso no roteador para que não exista conflito entre listas de acesso configuradas posteriormente; nesse exemplo o número que identifica a lista de acesso é 110. É passado como parâmetro os endereços de rede dos roteadores com sua máscara inversa para que seja possível saber quantos bits de rede serão combinados para permitir o tráfego de pacotes somente de endereços de origem 192.168.1.0 e endereço de destino 192.168.3.0.

access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Depois de adicionado os endereços LAN na lista de acesso do Roteador1, é necessário configurar a política de criptografia ISAKMP para que seja possível realizar a troca de chaves de segurança entre os roteadores. Esse processo é dividido em duas fases, na primeira fase apenas o método de criptografia e de troca de chaves é configurado. O primeiro comando, *crypta isakmp policy 10,* ativa o protocolo ISAKMP no roteador e especifica uma prioridade de valor 10, identificando o protocolo de segurança para o caso de que outros túneis sejam estabelecidos com o mesmo protocolo; em seguida é definido o protocolo de criptografia, com uma chave AES de 256bits pré-compartilhada e com um grupo 5 que define o método de troca de chaves segundo o protocolo DH (Diffie-Hellman), sendo que quanto maior for o tamanho da chave AES e seu grupo de troca de chaves, maior será o tempo gasto para processar o pacote, tanto na origem quanto no destino. Para infraestruturas que possuam equipamentos e conexões com alta disponibilidade, poder de processamento e grande largura de banda, chaves do tipo AES e grupos DH maiores que 5 garantem maior segurança no

processo de troca de chaves, deixando a conexão VPN mais segura. O último comando define qual a chave e o endereço do Roteador 2.

A seguir os comandos necessários para configuração da primeira fase:

crypta isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 10.2.2.2

A segunda fase do processo de criação e compartilhamento de chave ISAKMP consiste na criação do mapa de criptografia *VPN-MAP* que interligará todos os parâmetros da primeira fase do ISAKMP através do comando *crypto map*, que é responsável por mapear os parâmetros de troca de chaves para que as informações criadas na origem sejam compatíveis com as informações de troca de chaves (tamanho da chave, tipo de segurança, vida útil e registros do processo de troca de chaves) no destino, além de descrever o processo de VPN dentro do roteador com o comando *description*. Também nessa fase é definido o par de destino, ou seja, em que outra parte será estabelecido o túnel para troca de chaves e estabelecimento da VPN; nesse caso, o comando *peer* define o destino 10.2.2.2, que se refere ao *Roteador3*. Ainda nessa fase, através do comando *set transform-set*, é possível definir o parâmetro *VPN-SET* como um conjunto de atributos que serão compartilhadas entre a origem e destino para estabelecimento da VPN; é por meio desse processo que é dito que tanto a origem, quanto o destino, utilizaram as mesmas diretivas de segurança para estabelecimento do tráfego. O *match address 110* mapeia o processo VPN com a lista de acesso, permitindo que o tráfego a ser gerado pela VPN seja autorizado tanto na origem quanto no destino. É possível visualizar a seguir os comandos para implementação da segunda etapa do ISAKMP:

crypto map VPN-MAP 10 ipsec-isakmp
description Conexao VPN para o roteador3
set peer 10.2.2.2
set transform-set VPN-SET
match address 110
exit

Antes de passar para as configurações no Roteador3, deve-se mapear a interface serial para que a comunicação entre os roteadores seja habilitada para a VPN e especificar que o mapeamento dos parâmetros necessários ao estabelecimento do IPsec está contido no mapa de criptografia *VPN-MAP*. Essa configuração é ilustrada no conjunto de comandos abaixo:

interface 0/0/0
crypto map VPN-MAP

d) Parâmetros IPsec no Roteador3

Com o Roteador1 já configurado para o túnel VPN, com o protocolo IPsec habilitado e o protocolo de troca de chaves ISAKMP definido e ativo, deve-se configurar o Roteador3 para que o tráfego proveniente do Roteador1 seja reconhecido e tenha um destino, ou seja, deve-se habilitar a outra extremidade do túnel.

Assim como no Roteador1, o primeiro passo é ativar o pacote que contém as tecnologias de segurança que permitem a configuração do túnel e habilitar o protocolo IPsec. O processo é idêntico ao feito no Roteador1, quando através da CLI é fornecida a instrução ao roteador para ativar o recurso:

licence boot module c1900 technology-package securityk9

Em seguida, faz-se necessário configurar o protocolo de troca de chaves ISAKMP. A primeira fase do processo de configuração é a mesma do Roteador1, com exceção que no destino, é necessário especificar que a autenticação da VPN será feita de forma pré-compartilhada, ou seja, o estabelecimento da associação de segurança será do tipo estático. Outra informação é a definição da chave de segurança, que por ser uma associação de segurança do tipo estática, deve ser inserida manualmente por meio do comando *crypto isakmp key* e ainda possui como parâmetro o endereço em que se está definindo a chave; nesse caso, o Roteador 3. Comando ilustrados abaixo:

crypto isakmp policy 10
encryption aes 256
authentication pre-share

group 5
exit
crypto isakmp key vpnpa55 address 10.2.2.2

Da mesma forma que foi feito no Roteador1, na segunda fase do processo de criação e compartilhamento de chave ISAKMP, será criado um mapa entre os roteadores que ligará todos os parâmetros necessários para o protocolo IPsec criptografar os dados. Com exceção de que nessa fase, especificamos uma combinação de algoritmos e protocolos de segurança adicionais que são usados para proteger as chaves com o comando *crypto ipsec transform-set*, onde o *esp*-aes especifica que o cabeçalho IPsec ESP fará uso de um algoritmo de cifragem do tipo AES (que já foi definido como de 256 bits) e uma função de *hash* criptográfica do tipo SHA e um código de autenticação de mensagens do tipo HMAC, que servirá para autenticar tanto o endereço de MAC na origem quanto no destino. O processo é feito através dos comandos ilustrados abaixo:

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description vpn connection r1
set peer 10.1.1.2
set transform-set VPN-SET
match address 110
exit

Para finalizar a configuração do túnel e criptografia do Roteador3, deve-se mapear a interface serial por onde será trafegada a informação e ativar o já configurado mapa da VPN, com os comandos listados abaixo:

interface s0/0/1
crypto map VPN-MAP

5.1.1 Gerando tráfego na rede simulada VPN com IPSec

Para verificar se o túnel IPsec foi estabelecido e a conexão foi criptografada corretamente, deve-se simular uma troca de pacotes entre os computadores utilizados no cenário e depois analisar se os pacotes enviados foram recebidos e criptografados.

O primeiro passo para realizar esse teste é realizando um comando *ping* entre o Computador1 e o Computador3 que possuem respectivamente os endereços de IP 192.168.1.3 e 192.168.3.3.

A cada comando *ping* são enviados quatro pacotes para o endereço de destino. A Figura 15 ilustra a execução do comando *ping*. No exemplo ilustrado, o comando *ping* foi executado duas vezes, então espera-se que o Computador3 tenha recebido 6 pacotes. A ferramenta de simulação disponibiliza o terminal para execução do comando. Na imagem da Fig. 15 é possível observa que todos os pacotes foram enviados de forma correta até o destino.

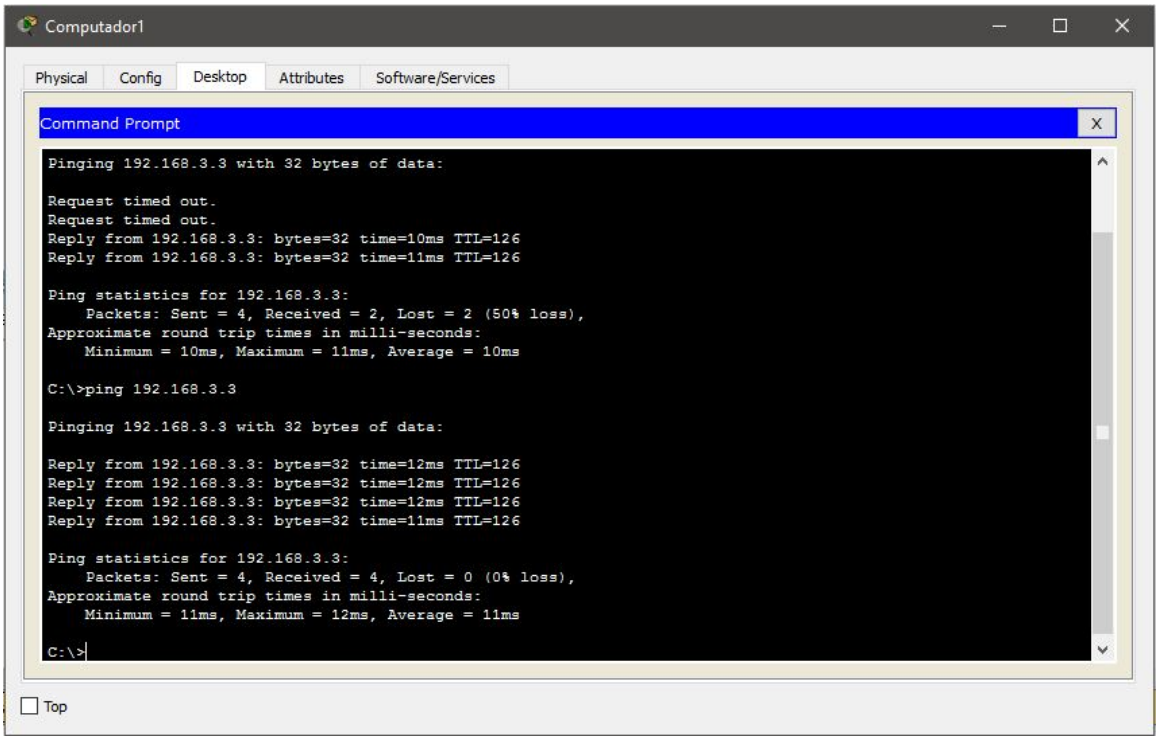

Figura 15: Execução do comando ping partido do Computador1 para o Computador3. O comando foi executado duas vezes, ou seja, 6 pacotes foram enviados até o destino final.

Após o envio dos pacotes, deve-se verificar se os pacotes foram enviados dentro do túnel VPN e se foram criptografados pelo protocolo IPsec. Para isso, utiliza-se o comando *show crypto ipsec sa*, que vai buscar as informações referentes a associação de segurança do protocolo IPsec. O comando é executado no Roteador3, que é por onde os pacotes passaram antes de chegar ao destino final. A imagem da Figura 16 ilustra o *log* (relatório) de registro gerado pelo comando, que especifica quantos pacotes chegaram ao destino, quantos pacotes

foram criptografados, quantos não foram criptografados e outras informações referentes ao tunelamento e criptografia da VPN. Como apresentado no relatório, todos os pacotes foram encapsulados e encriptados corretamente, atestando a correta implementação da VPN.

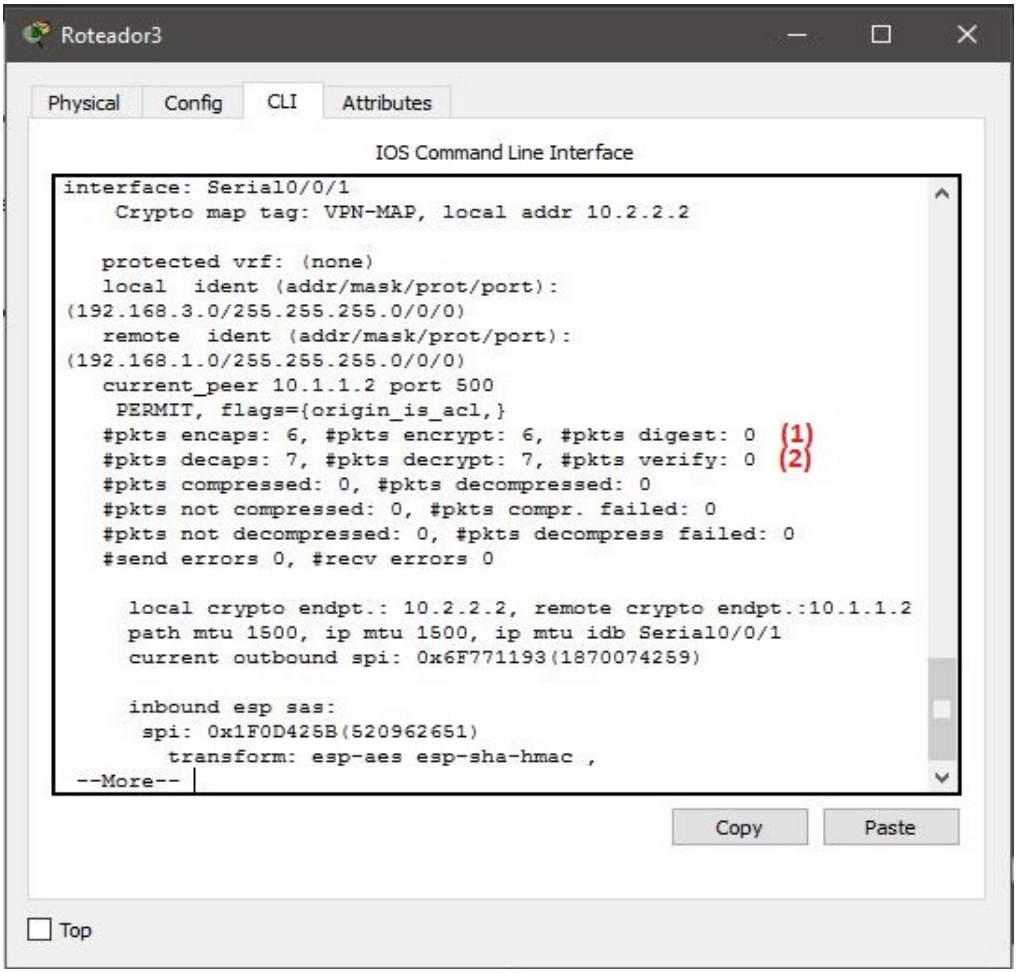

Figura 16: Log do túnel IPsec do Roteador3, que contém informações sobre os pacotes que trafegaram dentro do túnel IPsec. É possível identificar (1) quantos pacotes foram encapsulados e encriptados, (2) e quantos pacotes foram desencapsulados e decriptados.

5.2 SIMULAÇÃO VPN COM PROTOCOLO PPTP

A simulação a seguir irá demonstrar o funcionamento de uma VPN operando com o protocolo PPTP. Neste cenário, será necessário configurar o roteador CISCO para que ele autorize a conexão dos usuários remotos à rede interna, fornecendo também um endereço IP interno e acesso a todas as funcionalidades da rede permitidas ao usuário remoto.

Configurando o roteador CISCO para atuar como um servidor PPTP, o usuário remoto precisará apenas criar uma conexão Dial-Up a partir do seu sistema operacional de origem, o que garantirá a autenticidade da conexão. O suporte ao protocolo PPTP por parte dos roteadores CISCO se deu desde a versão 12.1 de seu sistema operacional.

a) Topologia

A topologia apresentada a seguir ilustra a distribuição dos equipamentos necessários a simulação, onde será feito o uso de um roteador Cisco 1941, um Switch CISCO Catalyst 2460 de 24 portas, um servidor de arquivos e computador genérico para a rede interna e um computador genérico para o acesso remoto externo. O Switch conectará o servidor de arquivos e o computador genérico da rede interna ao roteador Cisco 1941 através da LAN, sendo que o roteador também pertence a rede interna. Já o computador genérico externo, irá se conectar ao roteador Cisco 1941 através de uma conexão simulada do tipo serial DCE (*Data Communications Equipment*) por meio do túnel implementado pela VPN. A figura 17 ilustra a topologia acima descrita:

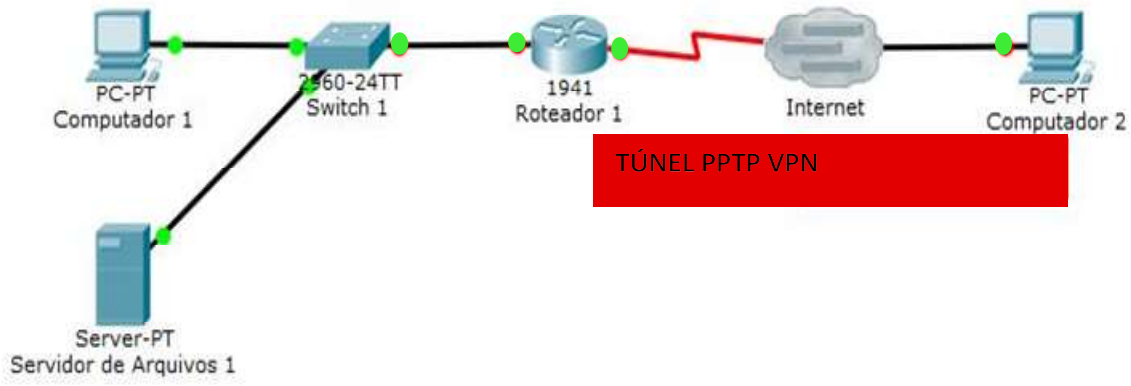

Figura 17: Topologia da VPN com o protocolo PPTP, com a distribuição e identificação dos equipamentos e sua nomenclatura. Nese cenário, o Computador 2 acessa remotamente a rede interna do Roteador 1 através da infraestrutura pública da internet, fazendo uso do protocolo PPTP

b) Tabela de endereços

A Tabela 3 de endereços ilustra as configurações básicas sobre os equipamentos do cenário e informa dados sobre tais dispositivos, suas interfaces e endereços de IP, máscara de rede, *Gateway* e portas do *Switch*.

Tabela 3: Tabela com as configurações de rede dos equipamentos utilizados na simulação, incluindo o endereço IP, Máscara de rede e *Gateway* de cada dispositivo. Neste cenário, o Computador 2 não possui uma conexão direta à rede pois sua conexão é remota, de forma que o mesmo não possui conexão a uma porta do Switch. O endereço IP atribuído ao Computador 2 está em uma faixa reservada para conexão remota, por isso existe o intervalo.

Dispositivo	**Interface**	**Endereço IP**	**Máscara de rede**	***Gateway***	**Porta do *Switch***
Roteador 1	G 0/0	192.168.0.1	255.255.255.0	-	Switch 1 F0/24
	S 0/0/0 (DCE)	200.2.2.2	255.255.255.0	-	-
Computador 1	Inespecífica	192.168.0.5	255.255.255.0	192.168.0.1	Switch 1 F0/1
Servidor de Arquivos	Inespecífica	192.168.0.6	255.255.255.0	192.168.0.1	Switch 1 F0/2
Computador 2	Inespecífica	192.168.0.20 ~ 192.168.0.25	255.255.255.0	192.168.0.1	-

c) Parâmetros PPTP Roteador 1

Para que o Roteador 1 aceite a conexão remota do tipo PPTP, é necessário configura-lo por meio da CLI, de forma que os parâmetros do acesso remoto sejam aceitos e a conexão estabelecida.

Habilitado o modo de execução autorizado no roteador com o comando *configure terminal,* habilita-se o modo de configuração de VPN com o comando *vpdn enable,* e define que a VPN a ser configurada pertence ao grupo 1, que servirá para identificar a conexão no caso de haver, no mesmo roteador, outra configuração VPN. O próximo passo é habilitar a conexão dial-up por meio do comando *R1(config-vpdn)# accept-dialin,* autorizando assim o roteador a aceitar as solicitações PPTP que forem encaminhadas. Em seguida o comando *R1(config-vpdn-acc-in)# protocol pptp* habilita o protocolo de segurança e autoriza o mesmo a nomear uma interface virtual para estabelecimento do túnel PPTP por meio do comando *R1(config-vpdn-acc-in)# virtual-template 1*. A sequência de comandos abaixo foi executada para configurar o Roteador 1:

R1# configure terminal
R1(config)# vpdn enable
R1(config)# vpdn-group 1
R1(config-vpdn)# accept-dialin

R1(config-vpdn-acc-in)# protocol pptp
R1(config-vpdn-acc-in)# virtual-template 1
R1(config-vpdn-acc-in)# exit

O próximo passo é conectar a interface virtual que já foi definida com o comando *interface virtual-template 1* a uma interface real, de forma a viabilizar a conexão remota PPTP a uma interface real da rede; isso é feito com o comando *ip unnumbered GigabitEthernet 0/0*, onde *ip unnumbered* define que um número de IP a ser atribuído será conectado a interface de rede *GigabitEthernet 0/0*. Para que os computadores que acessem remotamente consigam obter um endereço IP, faz-se necessário reservar um conjunto de endereços para serem atribuídos as máquinas que se conectarem remotamente a rede, esse conjunto de endereços é criado através do comando *R1(config-if) peer default ip address pool PPTP-Pool*. Feito o mapeamento da porta virtual com a porta de rede física, estabelecido o intervalo de endereços reservados para a conexão VPN, o próximo passo é especificar o tipo de criptografia a ser utilizada no túnel VPN, que no caso é feita com o protocolo PPP, utilizando o método de encriptação ponto-a-ponto, com uma chave de 128 bits com mecanismo de autenticação MS-CHAP e MS-CHAP-V2, que são algoritmos de criptografia existentes no protocolo PPP. Ver sequência de comandos abaixo:

R1(config)# interface virtual-template1
R1(config-if)# ip unnumbered GigabitEthernet 0/0
R1(config-if)# peer default ip address pool PPTP-Pool
R1(config-if)# ppp encrypt mppe 128
R1(config-if)# ppp authentication ms-chap ms-chap-v2

O comando *R1(config-if)# ppp encrypt mppe 128* define o tipo de criptografia que será utilizado na conexão remota. Para o cenário simulado, foi utilizado uma chave de 128bits. Já a autenticação é garantida com o protocolo MS-CHAP 2 (*Microsoft Challenge Handshake Authentication Protocol)* que se adequa ao protocolo PPTP, conforme descrito na seção 3.1 PROTOCOLOS DE SEGURANÇA.

Reservado o conjunto de endereços para a conexão remota, o próximo passo é especificar tais endereços dentro do Roteador 1, para que os mesmos sejam atribuídos aos dispositivos que ingressarem de forma remota a rede. Tal especificação é feita com a

especificação da reserva de endereços criada previamente e que nomeamos *PPTP-Pool* que atribui um intervalo de endereços para acesso remoto, conforme comando a seguir:

R1 (config) # ip pool local PPTP-Pool 192.168.0.20 192.168.0.25

A última etapa da configuração do Roteador 1 é a criação de um usuário e senha para garantir a autenticidade da conexão e evitar que acessos não credenciados sejam realizados.

R1 (config) # username usuario password abc@2018

Depois de configurado o Roteador 1 e criado o túnel VPN para estabelecimento da conexão remota, a próxima etapa é configurar no Computador 2 a VPN. Tal configuração fica a critério do sistema operacional utilizado para criar a conexão Dial-Up.

5.2.1 Gerando tráfego na rede simulada VPN com PPTP

Como forma de testar a conexão VPN e garantir que a comunicação foi estabelecida, é gerado um tráfego na rede através de uma troca de pacotes por meio do comando *ping* entre o roteador, que neste cenário é o servidor PPTP, e um computador que está fora da rede interna.

Para que o computador utilizado no cenário se comunique com a rede externa, deve-se estabelecer uma conexão DIAL-UP com o servidor PPTP. Essa conexão é feita por meio do sistema operacional, utilizando um nome de usuário e senha para garantir a autenticidade da conexão, como ilustra a Figura a 18.

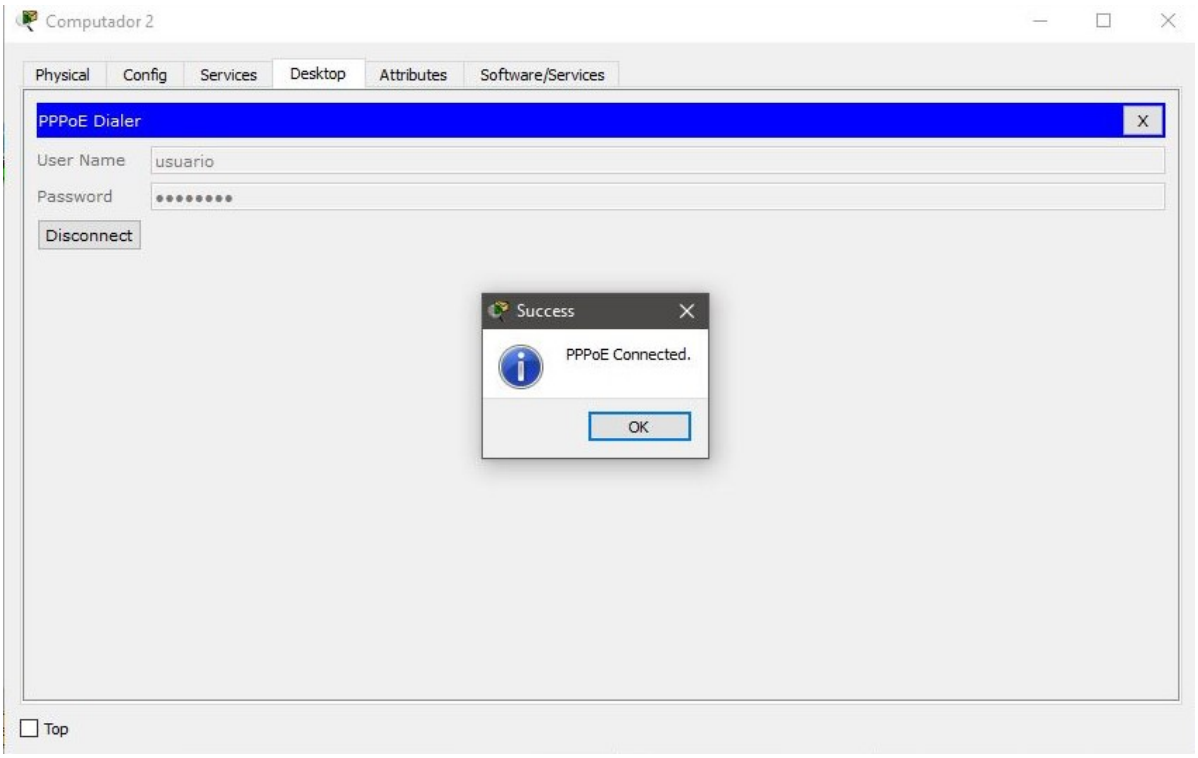

Figura 18: Estabelecimento da conexão DIAL-UP com o servidor PPTP. A conexão foi estabelecida por meio de usuário e senha que são autenticados pelo próprio roteador.

Estabelecida a conexão, o computador dois recebe um endereço de IP fornecido pelo servidor PPTP ao se conectar à nova rede. Esse *pool* de endereços garante que qualquer máquina autenticada que se conectar à rede interna receba um endereço de IP entre 192.168.0.20 até 192.168.0.25.

Agora que o Computador 2 já está conectado à rede interna e possui um endereço de IP, executa-se um comando *ping* para o endereço 192.168.0.1 que é o do servidor PPTP, para confirmar a comunicação entre as máquinas na rede interna com o Computador 2 que está na rede externa, como ilustra a Figura 19.

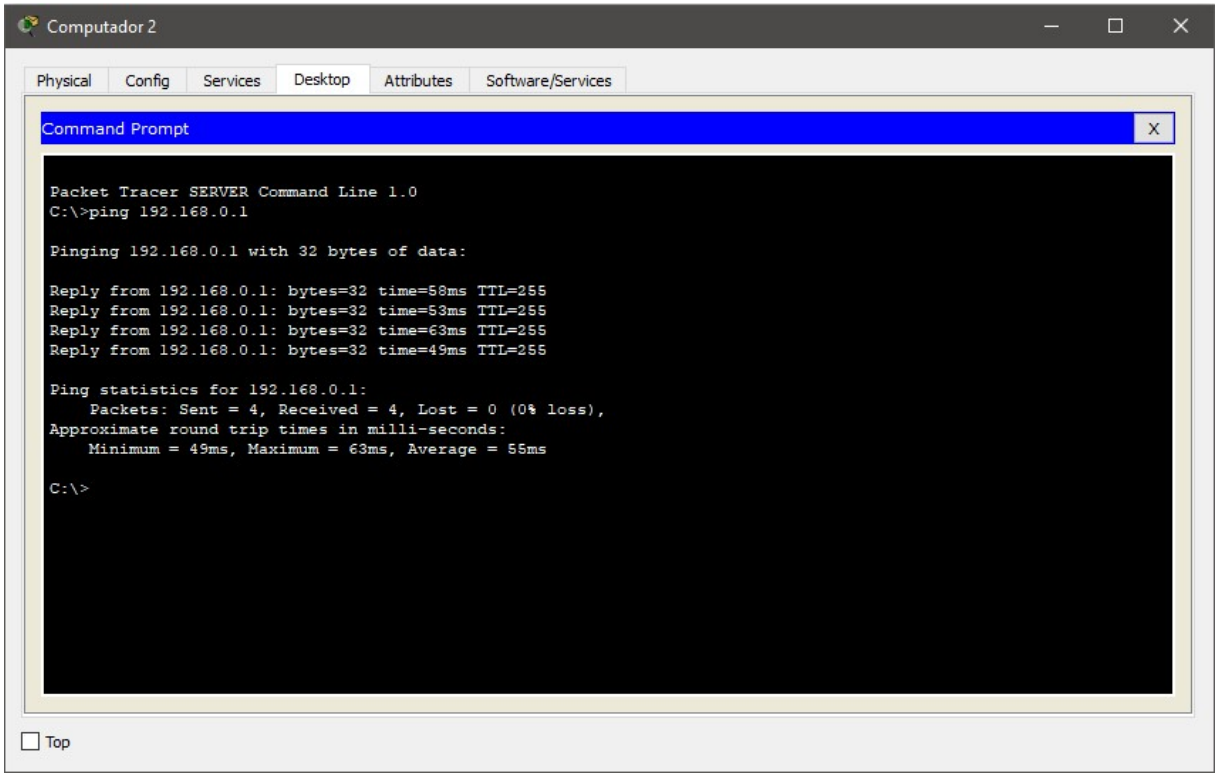

Figura 19: Captura de tela que mostra a execução do comando ping da estação para o servidor PPTP.

Confirmado a conexão e a troca de pacotes entre a rede interna e rede externa, o último quesito a ser verificado é se a VPN está criptografando a conexão PPTP. Essa informação é obtida no servidor PPTP através do comando *show running-config* o qual mostra as configurações do Roteador 1 e informa se os protocolos para estabelecimento da VPN e criptografia foram habilitados.

6 CONSIDERAÇÕES FINAIS

Com o presente trabalho foi possível, por meio da revisão de literatura, obter um panorama sobre o funcionamento de uma VPN, incluindo seus conceitos, características, definições e forma de operação. Também foi possível conhecer como funciona a técnica de tunelamento e os protocolos de segurança associados à implementação de uma Rede Privada Virtual, além de um entendimento sobre os principais tipos e cenários em que se pode implementar uma VPN, atingindo assim um dos objetivos centrais desta pesquisa.

Foi escolhido o CISCO *Packet Tracer* para a construção e simulação dos cenários; tal sistema foi escolhido devido sua grande utilização no meio acadêmico para pesquisa e teste em diversos segmentos da área de Redes de Computadores, além de se tratar de uma plataforma gratuita. Devido a uma boa usabilidade por parte do *Software* e a disponibilidade de material para estudo e consulta, o processo de simulação foi implementado com sucesso.

Também foi possível definir que a simulação dos cenários de implementação de uma VPN é a melhor e mais econômica forma de compreender os conceitos referentes ao tema central da pesquisa, pois não se faz necessário a construção de uma infraestrutura de redes para que seja possível realizar o estudo.

Entre as facilidades para construção deste trabalho, podemos citar a grande variedade de literatura específica referente ao tema da pesquisa, boa usabilidade e material de consulta para aprendizado do sistema CISCO *Packet Tracer* e posteriormente para a realização das simulações. As dificuldades encontradas para elaboração desta pesquisa concentram-se nas simulações, onde alguns equipamentos utilizados nos cenários virtuais não permitiam o uso de protocolos relacionados a VPN de forma separada, como foi o caso do protocolo L2TP, que só foi possível utilizar nos equipamentos CISCO em conjunto com o protocolo IPsec.

Dessa forma, este trabalho obteve sucesso em alcançar seus objetivos propostos ao desenvolver uma base teórica sobre o que engloba as Redes Privadas Virtuais e seu funcionamento, ao compreender a importância em usar simulações para abranger conceitos relacionados as redes de computadores e também o aprendizado obtido na utilização da ferramenta CISCO *Packet Tracer*.

6.1 TRABALHOS FUTUROS

Por ser tratar de uma temática bastante abrangente, as Redes Privadas Virtuais permitem diversos outros estudos e englobam vários setores na área de redes de computadores. Sua abrangência se dá pela necessidade de aprimorar as técnicas já existentes e explorar novas soluções para problemas que as soluções oferecidas não foram capazes de solucionar.

Com isso, a seguir apresenta-se algumas ideias com foco na simulação de vários cenários de possíveis pesquisas que podem ser realizadas:

1. A simulação de cenários em Redes Privadas Virtuais com a implementação de QOS, gerando um tráfego em que seja possível analisar o funcionamento de alguns dos parâmetros da qualidade de serviço e seu impacto no cenário simulado;
2. A simulação do funcionamento de uma VPN em um cenário com o protocolo de endereçamento MPLS, onde seja possível verificar o comportamento da VPN através da análise de tráfego e o roteamento dos pacotes;
3. O uso das Redes Privadas Virtuais em uma simulação envolvendo tráfego de serviços de voz e dados, como os serviços de voz sob IP (VoIP);
4. Um estudo sobre VPN em redes celulares (LTE);
5. A simulação de cenários VPN com utilização de servidores DNS nas redes compartilhadas e uma análise do seu funcionamento.

7 APÊNDICE

Configuração IPsec Roteador1:

R1> enable

R1# configure terminal

R1(config)# license boot module c2900 technology-package securityk9

R1(config)# end

R1# copy running-config startup-config

R1# reload

R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

R1(config)# crypto isakmp policy 10

R1(config-isakmp)# encryption aes

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 2

R1(config-isakmp)# exit

R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2

R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

R1(config)# crypto map VPN-MAP 10 ipsec-isakmp

R1(config-crypto-map)# description VPN connection to R3

R1(config-crypto-map)# set peer 10.2.2.2

R1(config-crypto-map)# set transform-set VPN-SET

R1(config-crypto-map)# match address 110

R1(config-crypto-map)# exit

R1(config)# interface S0/0/0

R1(config-if)# crypto map VPN-MAP

R1(config)# exit

R1# copy running-config startup-config

Configuração IPsec Roteador3:

R3> enable

R3# configure terminal

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

R3(config)# crypto isakmp policy 10

R3(config-isakmp)# encryption aes

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# group 2

R3(config-isakmp)# exit

R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2

R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

R3(config)# crypto map VPN-MAP 10 ipsec-isakmp

R3(config-crypto-map)# description VPN connection to R1

R3(config-crypto-map)# set peer 10.1.1.2

R3(config-crypto-map)# set transform-set VPN-SET

R3(config-crypto-map)# match address 110

R3(config-crypto-map)# exit

R3(config)# interface S0/0/1

R3(config-if)# crypto map VPN-MAP

R3(config)# exit

R3# copy running-config startup-config

Configuração PPTP Roteador1:

R1> enable

R1# configure terminal

R1(config)# vpdn enable

R1(config)# vpdn-group 1

R1(config-vpdn)# accept-dialin

R1(config-vpdn-acc-in)# protocol pptp

R1(config-vpdn-acc-in)# virtual-template 1

R1(config-vpdn-acc-in)# exit

R1(config)# interface virtual-template1

R1(config-if)# ip unnumbered GigabitEthernet 0/0

R1(config-if)# peer default ip address pool PPTP-Pool

R1(config-if)# ppp encrypt mppe 128

R1(config-if)# ppp authentication ms-chap ms-chap-v2

R1 (config) # ip pool local PPTP-Pool 192.168.0.20 192.168.0.25

R1 (config) # username usuario password abc@2018

R1(config)# exit

R1# copy running-config startup-config

8 REFERÊNCIAS

CELESTINO, Pedro. **Redes Privadas Virtuais.** 2005. 90 f. Dissertação (Mestrado) - Curso de Engenharia Mecânica, Universidade de Taubaté, Taubaté, 2005.

CHIN, Liou Kuo. **Rede Privada Virtual - VPN.** 1998. Rede Nacional de Ensino e Pesquisa (RNP). Disponível em: <http://memoria.rnp.br/newsgen/9811/vpn.html#inicio>. Acesso em: 29 fev. 2016.

DIAS FILHO, José Roberto Teixeira. **Simulação de redes de computadores com OPNET IT GURU® ACADEMIC EDITION.** 2011. Disponível em: <http://cict.inatel.br/nova2/docentes/lucianol/opnet/opnet_tutorial.pdf>. Acesso em: 20 dez. 2011.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down.** 5. ed. Cidade: São Paulo. Pearson Education do Brasil, 2010. 576 p

MARTINS, Dêner Lima Fernandes. **Redes privadas Virtuais com IPsec.** 2000. 13 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade de Brasilia, Distrito Federal, 2000. Disponível em: <http://cic.unb.br/docentes/pedro/trabs/vpn.pdf>. Acesso em: 02 mar. 2016.

MENDONÇA, Gabriel Guimarães. **Protocolos de Segurança IP - IPSec.** 2009. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/gabriel/index.html>. Acesso em: 14 maio 2016.

MORAES, Alexandre Fernandes de. **Segurança em Redes.** São Paulo: Érica, 2010.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em ambientes coorporativos.** 6. ed. São Paulo: Novatec, 2013.

PEREIRA, Tatiana Brito. **Uma estratégia de roteamento OSPF Adaptativo Baseado em Estimação de Banda.** 2004. 162 f. Dissertação (Mestrado) - Curso de Engenharia Eletrica, Universidade Estadual de Campinas, Campinas, 2004. Disponível em:

<http://unicamp.sibi.usp.br/handle/SBURI/83055?show=full>. Acesso em: 27 abr. 2016.

REZENDE, Edmar Roberto Santana de; GEUS, Paulo Lício de. **Análise de segurança dos protocolos utilizados para acesso remoto VPN em plataformas Windows.** 2002. Disponível em: <ftp://143.107.200.66/pub1/SSI/Anais_2002/An?lise de Seguran?a dos Protocolos Utilizados para Acesso Remoto VPN em Plataformas Windows.pdf>. Acesso em: 02 mar. 2016.

RUSSO, Rafael. **Cisco Packet Tracer – Simulação e comportamentos reais de uma Rede.** 2012. Disponível em: <http://escreveassim.com.br/2012/10/26/cisco-packet-tracer-simulacao-e-comportamentos-reais-de-uma-re>. Acesso em: 28 abr. 2016.

SANTANA, Edmar Roberto. **Segurança no Acesso Remoto VPN.** Disponível em: <http://www.las.ic.unicamp.br/paulo/teses/20040227-MSc-Edmar.Roberto.Santana.de.Rezende-Seguranca.no.acesso.remoto.VPN.pdf>. Acesso em: 05 jul. 2010.

SOUZA, Marcelo; SILVA, Joab; SOUZA, Whasley. Simuladores e Emuladores de Rede para o Projeto e Solução de Problemas em Ambiente de Produção. 2016. Disponível em: <http://rtic.com.br/index.php/rtic/article/view/76/75>. Acesso em: 12 jun. 2017.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003. 945 p.

VALENTE, Daniel. **Introdução a tecnologia VPLS (Virtual Private Lan Segment).** 2010. Disponível em: <http://blog.ccna.com.br/2010/11/01/introducao-a-tecnologia-vpls-virtual-private-lan-service/>. Acesso em: 01 mar. 2016.

VELLOSO, Fernando de Castro. **Informática: conceitos basicos.** 8. ed. Rio de Janeiro: Elsevier, 2011.