FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da informação

Yu Chwen Wang

Protocolo de Segurança (IPsec):

Implantação e comparativo nos protocolos IPv4 e IPv6

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da informação

Yu Chwen Wang

Protocolo de Segurança (IPsec):

Implantação e comparativo nos protocolos IPv4 e IPv6

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Rogério Nunes de Freitas
Área de concentração: Segurança da Informação

Americana, SP

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

W218p WANG, Yu Chwen

Protocolo de segurança (IPsec): implantação e comparativo nos protocolos IPv4 e IPv6./ Yu Chwen Wang. – Americana: 2017.

99f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp.Rogério Nunes de Freitas.

1. Segurança em sistemas de informação 2. Redes de computadores I. FREITAS, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Yu Chwen Wang

Protocolo de Segurança (IPsec):

Implantação e comparativo nos protocolos IPv4 e IPv6

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana 26 de junho de 2017.

Banca Examinadora:

ROGÉRIO NUNES DE FREITAS (Presidente)
Especialista
Faculdade de Tecnologia Americana

ALBERTO MARTINS JUNIOR (Membro)
Mestre
Faculdade de Tecnologia Americana

BENEDITO APARECIDO CRUZ (Membro)
Graduado
Faculdade de Tecnologia Americana

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus por me conceder essa grande oportunidade de crescimento pessoal e a chance de obter essa conquista importante na vida.

Agradeço o apoio da minha família, que estiveram sempre ao meu lado, atuando como pilares me sustentando todos os momentos.

Agradeço pela paciência e apoio, do meu orientador Rogério Nunes Freitas, que me auxiliou e acompanhou passo a passo durante o desenvolvimento desse trabalho, e através do seu conhecimento me mostrando o melhor caminho com ideias e sugestões para concluir essa última etapa importante da minha vida acadêmica.

Agradeço a todos os professores que caminharam junto comigo nessa jornada, construindo me com conhecimentos valiosos, para a minha formação durante o progresso acadêmico.

Aos meus colegas de sala, que batalhamos juntos nessa caminhada, grata pelo apoio e ajuda durante esses anos.

O meu agradecimento a todos que me ajudaram durante esses anos na vida acadêmica, para a minha formação e crescimento pessoal.

DEDICATÓRIA

A Deus que me concedeu força para vencer os obstáculos e proporcionou a oportunidade de obter conquistas importante na minha vida.

RESUMO

A evolução da tecnologia, contribuiu para o aumento de dispositivos conectados na rede que oferecem serviços aos usuários, além de agilizar os processos do dia a dia, também vem trazendo ilimitados benefícios, mas com o aumento da necessidade de dispositivos às redes, o protocolo IP da versão mais usada atualmente (IPv4), não está mais conseguindo atender a essa demanda, ou seja, está ocorrendo a falta de endereços para conectar os dispositivos. Dessa forma, foi desenvolvido uma versão otimizada o IPv6, sucessora do IPv4, que está sendo implantada aos poucos na rede atual. Esse trabalho tem como objetivo, apresentar estudo das versões de protocolos IPv4 e IPv6, e o protocolo de segurança IPsec, pois, atualmente a maioria das transações importantes são feitas pela rede, assim, a segurança na transferência de dados torna-se um elemento importante em relação à essa questão, no entanto, nesse projeto foi feito a comparação do protocolo IPsec, integrado no IPv4 e em IPv6, mostrando como ele atua em cada um em relação à questão crítica de segurança de transmissão de dados pela rede, e foi desenvolvido uma aplicação prática, implantando cenários simulado usando ferramentas: GNS3, VirtualBox e Wireshark. Por fim, foi proposto os resultados e observações obtidos sobre o desempenho de cada um dos protocolos.

Palavras chave: IPsec, IPv4, IPv6.

ABSTRACT

The evolution of technology has contributed to the increase of connected devices in the network that offer services to users, in addition to streamlining day-to-day processes, it has also brought unlimited benefits, but with the increasing need of devices to networks, IP protocol of the most used version (IPv4), is no longer able to meet this demand, that is, there is a lack of addresses to connect the devices. In this way, an optimized version was developed IPv6, successor to IPv4, which is being gradually implemented in the current network. This work aims to present a study of the versions of IPv4 and IPv6 protocols, and the IPsec security protocol, since currently most of the important transactions are done by the network, thus, the security in the data transfer becomes an important element In relation to this issue, however, in this project the IPsec protocol, integrated in IPv4 and IPv6, was compared, showing how it acts in each one in relation to the critical issue of data transmission security over the network, and was developed A practical application, deploying simulated scenarios using tools: GNS3, VirtualBox and Wireshark. Finally, the results and observations obtained on the performance of each of the protocols were proposed.

Keywords: IPsec, IPv4, IPv6.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3DES	*Triple Data Encryption Standard*
AES	*Advanced Encryption Standard*
AFRINIC	*African Network Information Centre*
AH	*Authentication Header*
ANS	*Advanced Network and Services*
APNIC	*Asia-Pacific Network Information Centre*
ARIN	*American Registry for Internet Numbers*
ARPANET	*Advanced Research Projects Agency Network*
AS	*Security Association*
Bit	*Binary digit*
BGP	*Border Gateway Protocol*
Bytes	*Binary Term*
CAST	*Carlisle Adams and Stafford Tavares*
Cert.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CID	confidencialidade, integridade e disponibilidade
CIDR	*Classless Inter Domain Routing*
CSNET	*Computer Science Network*
DARPA	*Defense Advanced Research Project Agency*
DAS	*Digital Signature Algorithm*
DDoS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denial of Service*

ECC	*Elliptic curve cryptography*
EIGRP	*Enhanced IGRP*
ESP	*Encapsulated Security Payload*
Gb	*Gigabyte*
GNS3	*Graphical Network Simulator3*
IANA	*Internet Assigned Numbers Authority*
IBM	*International Business Machines*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICMP	*Internet Control Message Protocol*
IDEA	*International Data Encryption Algorithm*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
IGRP	*Interior Gateway Protocol*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPsec	*IP Security Protocolo*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISAKMP	*Internet Security Association and Key Management Protocol*
LACNIC	*Latin American and Caribbean Internet Addresses Registry*
LAN	*Local Area Network*
MAC	*Media Access Control*
Mb	*Megabyte*

MCI	*Microwave Communications, Inc.*
MILNET	*Military Network*
MLD	*Multicast Listener Discovery*
NAT	*Network Address Translation*
NCP	*Network Control Protocol*
NSF	*National Science Foundation*
OSI	*Open System Interconnection*
OSPF	*Open Shortest Path First*
OTP	*One-time pad*
PDU	*Protocol Data Unit*
QoS	*Quality of Service*
RC4	*Rivest Cipher 4*
RC5	*Rivest Cipher 5*
RFCs	*Requests for Comments*
RIP	*Routing Information Protocol*
RIPE NCC	*Réseaux IP Européens Network Coordination Centre*
RSA	algoritmo é referente as primeiras letras dos criadores *Rivest, Shamir e Adleman*
SPI	*Security Parameter Index*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
UDP	*User Datagram Protocol*
ULA	*Unique-Local Address*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
www	*World Wide Web*

1. INTRODUÇÃO

A Internet disponibiliza várias ferramentas e funções que facilita e ajuda a vida das pessoas, dessa forma, incorporando e tornando-se parte do cotidiano do indivíduo, tais como, efetuar pesquisas, compras e vendas online, acessar conta bancária através da Internet, realizar a comunicação instantânea.

Conforme Cert.br (2012), “A Internet já está presente no cotidiano de grande parte da população e, provavelmente para estas pessoas, seria muito difícil imaginar como seria a vida sem poder usufruir das diversas facilidades e oportunidades trazidas por esta tecnologia. ”

Com o passar dos anos a Internet está em constante aperfeiçoamento com intuito de oferecer serviços mais aprimorados para atender as necessidades dos usuários e aumentando também as suas funcionalidades.

Apesar da Internet apresentar grande quantidade de recursos que beneficia as pessoas, ela também traz riscos, uma vez que, o pacote trafegado na rede possuir informações valiosas para empresa ou para o usuário, e esses dados podem ser interceptado por indivíduos mal-intencionados, ocorrendo o uso inadequada dessas informações.

Com a popularização da Internet que contribuiu na troca maciça de informações, a questão de segurança é um dos temas mais questionados, para isso foram propostas várias soluções e ferramentas para atender a segurança da rede, e nesse trabalho foi utilizado uma delas, o protocolo de segurança IPsec, mostrando como ele atua diante do cenário de tráfego de pacote na rede, de forma segura até o destino aplicando as funções de autenticação e criptografia, na rede IPv4 e IPv6.

O objetivo geral desse trabalho é avaliar o desempenho do protocolo IPsec, aplicada no tráfego dos pacotes da rede, mostrando os benefícios que traz em relação à questão de segurança.

O objetivo específico é a implementação de equipamentos de redes através de emulação onde foram configurados o protocolo IPsec, e em seguida foram

realizados testes e análises de desempenho para manter um tráfego seguro na rede analisada.

A metodologia usada para a realização desse trabalho foi baseada nas fontes de pesquisa de sites e livros referentes ao assunto. O trabalho foi estruturado em cinco capítulos, que está organizada da seguinte forma:

O primeiro capítulo mostra a visão geral do projeto.

O segundo capítulo apresenta os principais temas que serão necessários para o entendimento do trabalho, conceituando a evolução da Internet, riscos que a internet traz, o papel da segurança da informação.

No terceiro capítulo é apresentado o protocolo IP, dos modelos OSI e TCP/IP, e uma breve descrição dos protocolos da versão quatro (IPv4) e da versão seis (IPv6).

No quarto capítulo foi explicado o protocolo de segurança IPsec, mostrando suas funcionalidades, e como ele atua para garantir a segurança dos pacotes durante o tráfego.

No quinto capítulo foi apresentado os cenários simulado do estudo de caso feito, onde é mostrado os resultados e discussões, análises de dados obtidos, usando o protocolo IPsec.

Por fim, a conclusão apresenta a contribuição do trabalho feito e as propostas futuras.

2. INTERNET

A Internet está em constante expansão e na sociedade atual ela está presente em quase todas os lugares, oferecendo recursos que auxiliam no cotidiano das pessoas, tornando assim um elemento fundamental, tanto na parte acadêmica, domiciliar ou empresarial. Muitos dos processos funcionam de forma eficiente graças a Internet como exemplo: disponibiliza variedades de fontes de pesquisas, comunicação instantâneo, transição de arquivos empresariais, compras online entre outros.

> "À medida que a rede se tornava mais popular, a quantidade de conteúdo só aumentava e os serviços oferecidos ficavam cada vez mais complexos, com o lançamento de sites de pesquisas (buscadores), comércio eletrônico (*e-commerce*), bancos online (*bankline*), serviços públicos governamentais (*e-governament*), entre várias outros. Toda a comodidade proporcionada por esses serviços online somente repercutiu no crescimento desenfreado da rede com quantidades cada vez mais expressivas de usuários" (BRITO, 2013, p. 22).

2.1 Definição da rede Internet

Conforme definido pelo Kurose e Ross (2013), a Internet é uma rede pública mundial de computadores, onde diversos equipamentos são interconectados em todo mundo, possibilitando o acesso e a transferência de informações.

A Internet não é apenas uma rede, e sim, uma grande rede composta por diversas redes distintas, com variedades de equipamento interligado e através de um conjunto de protocolos, no qual, permitem se comunicarem entre si para a troca de informações. Como mostrado na Figura 1, é possível perceber que nos pontos onde a localização da luz é mais intensa, significa que o número de usuários da Internet é maior.

Outra definição feita pelo Tanenbaum (2011, p.53), "A Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços em comum [...] "

Figura 1 - Conexão realizada através da rede Internet

Fonte: BBC (2016)[1]

2.2 Evolução da Internet

No mundo atual com a Internet tudo se tornou mais fácil, mas nos primórdios da sua criação até atualidade, passou-se por vários processos de modificações e aprimoramentos com a finalidade de propor um recurso que possa atender melhor essa vasta gama de transições de dados e disponibilizar funcionalidades mais satisfatórios para os dias de hoje. Em seguida será apresentada uma breve história do desenvolvimento da rede Internet, mostrando as suas principais etapas de evolução com o passar do tempo.

Origem - A criação da rede mundial pelos Estados Unidos deu se origem na Guerra Fria, era usada para fins militares, para proteger as informações sigilosas, pois na época os sistemas eram centralizados, no entanto, caso aconteça algum ataque, acarretaria a perda total da informação. Com base nisso foi realizado vários

[1] Disponível em: <http://www.bbc.com/mundo/noticias-america-latina-37167144>. Acesso em: 15 fev. 2017.

estudos nas universidades e centros de pesquisa, com intuito de desenvolver uma rede distribuída com capacidade de tolerar essa vulnerabilidade.

De acordo com Tanenbaum (2011, p. 54):

> "A história começa no final da década de 1950. No auge da Guerra Fria, o departamento de Defesa dos Estados Unidos queria uma rede de controle e comando capaz de sobreviver a uma guerra nuclear [...] centrais de comutação telefônica, cada uma das quais conectada a milhares de telefones. Por sua vez, essas centrais de comutação estavam conectadas a centrai de comutação de nível mais alto (centrais interurbanas), formando uma hierarquia nacional apenas com uma pequena redundância. A vulnerabilidade do sistema era o fato de que a destruição de algumas centrais interurbanas importantes poderia fragmentar o sistema em muitas ilhas isoladas".

Década de 1960 a 1970 – Conforme Brito (2013, p. 19), "com o financiamento da DARPA – *Defense Advanced Research Project Agency* (Departamento de Defesa dos Estados Unidos), os especialistas de universidades e centros de pesquisas criaram uma rede experimental chamada de ARPANET, o objetivo inicial era fazer a interligação de algumas instituições de pesquisas".

Segundo Kurose e Ross (2013), para obter a comunicação entre os diferentes equipamentos das instituições, foi criado o primeiro protocolo o NCP- *Network Control Protocol* (Protocolo de Controle de Rede)**,** no qual, atua como um idioma em comum que mantem a comunicação entre as máquinas da rede. Nessa mesma época foi desenvolvimento um dos primeiros programas, o e-mail.

Década de 1970 a 1980 - O progresso das pesquisas propôs o aumento da criação de novas redes que resultou no crescimento das interligações de equipamentos, e consequentemente, o protocolo NCP não conseguiu mais suportar esse grande tráfego e começou a apresentar problemas, então era necessário a substituição pelo novo protocolo padrão TCP/IP - *Transmission Control Protocol / Internet Protocol* (Protocolo de Controle de Transmissão / Protocolo de Internet), pois, com a expansão da rede, o ponto mais importante foi direcionado para o transferência de dados entre equipamentos afim de manter a comunicação, e o TCP/IP foi criado para esse fim, e é usados até os dias de hoje.

> "[...] os protocolos da ARPANET não eram adequados para a execução em redes múltiplas. Essa observação levou a mais pesquisas sobre protocolos, culminando com a invenção dos protocolos TCP/IP (Cerf e Kahn, 1974). O TCP/IP foi criado especificamente para manipular a comunicação sobre inter-redes, algo que se tornou mais importante à medida que um número maior de redes era conectado à ARPANET" (TANENBAUM, 2011, p.58).

Nesse período surgiu o termo *internetting*, que era aplicada no projeto para a interligação de redes distintas, onde computadores de redes diferentes conseguiam se comunicar, e posteriormente, deu a origem ao nome dessa grande rede, que chamamos hoje de Internet.

De acordo com Kleina (2011), "[...] cientistas tentavam conectar três redes diferentes em um processo descrito em inglês como *interneting*. O termo foi abreviado e, aos poucos, imortalizado como sinônimo de toda a rede".

Década de 1980 a 1990 – Segundo Forouzan (2008), a ARPANET foi divido em dois grupos, a rede MILNET, que era usado pelos militares e ARPANET, usado pelos pesquisadores.

A rede chamada CSNET, foi criado pelo NSF - *National Science Foundation* (Fundação Nacional da Ciência) com o propósito de disponibilizar uma rede aberta para o acesso dos cientistas das universidades, na troca de informações sobre determinadas pesquisas, pois nem todos os campus universitários tinham acesso a ARPANET, eram autorizadas apenas para os que tinham vínculo com Departamento de Defesa de Estados Unidos.

> "[...] a NFS (*National Science Foundation*) percebeu o enorme impacto que a ARRPANET estava causando nas pesquisas universitárias nos Estados Unidos, permitindo que cientistas de todo o país compartilhassem dados e trabalhassem juntos em projetos de pesquisa. No entanto, para entrar na ARPANET, uma universidade precisava ter um contrato de pesquisa com o Departamento de Defesa dos Estados Unidos, privilégio que muitos não tinham" (TANENBAUM, 2011, p. 58).

Kurose e Ross (2013), relatam posteriormente foi desenvolvido pela NSF uma rede sucessora da ARPANET o NSFNET que conectava centros de supercomputadores do país inteiro, e interligava as redes regionais.

Década de 1990 – Conforme Forouzan (2008, p.3) "Em 1990, a ARPANET foi oficialmente aposentada e substituída pela NSFNET ".

A rede NSFNET conectou vários campus universitário, bibliotecas e centros de pesquisas do país inteiro, e estava em contínuo crescimento, mas logo percebeu que não conseguiria mais sustentar essa grande escala de tráfego, e o governo não pretendia continuar financiando essa rede, então foi concedido para três empresas (IBM, MCI e Merit) que formaram o ANS – *Advanced Network and Services*, criaram um link com velocidade mais elevada, que passou a ser chamado de ANSNET.

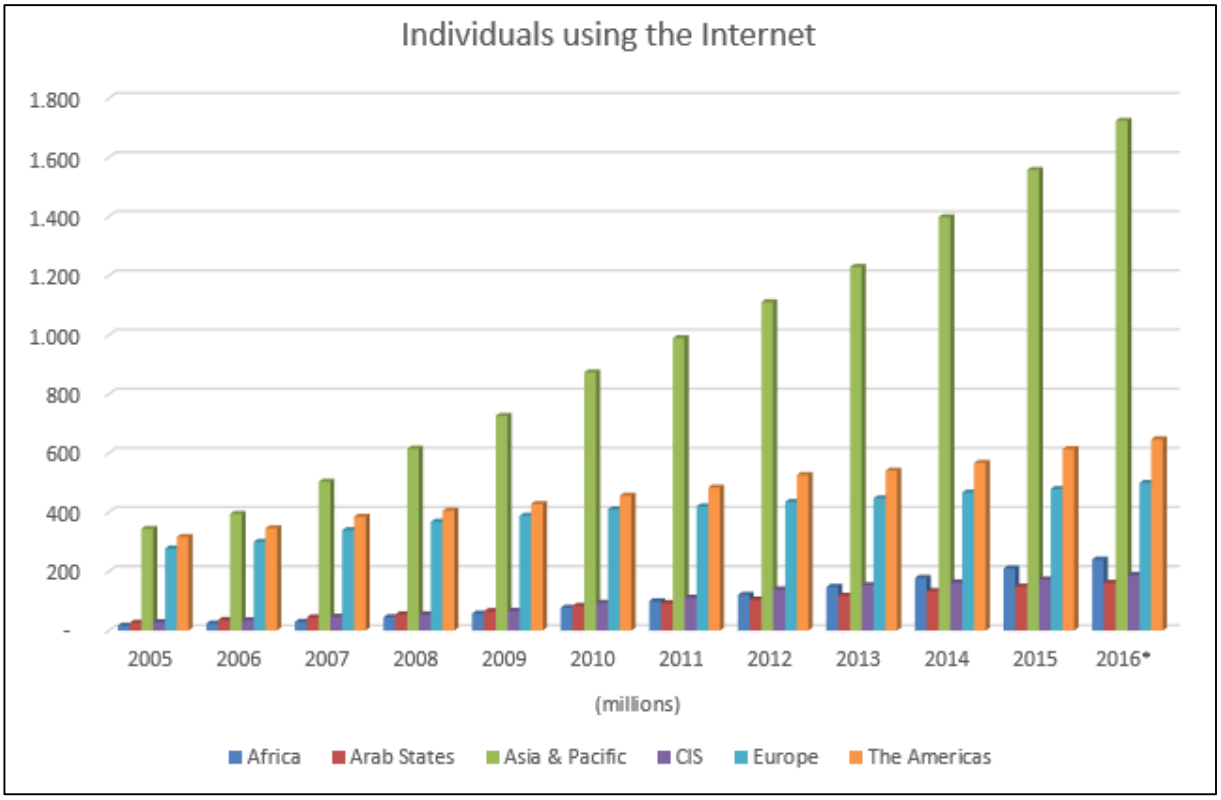
> "[...] o governo norte-americano decidiu que a NSFNET não era capaz de suportar o tráfego rapidamente crescente da Internet. Três empresas (IBM, Merit e MCI) preencheram essa lacuna formando uma organização sem fins lucrativos central de alta velocidade, chamado de ANSNET" (FOROUZAN, 2008, p.3).

Segundo Kurose e Ross (2013), nos meados da década de 90 a Internet, foi-se tornando comercial com o surgimento de empresas provedores de serviço de Internet, e através do *World Wide Web (www)* que foi implantado nessa mesma época, tornou-se possível a disponibilização de diversas informações nas páginas dos navegadores, como texto e figura. Também ocorreu a criação de novas aplicações e serviços, que levou a disseminação do uso da Internet nas empresas e para milhares de pessoas, aumentando o número de usuários pelo mundo inteiro.

Conforme Forouzan (2008, p.6), "Estão sendo desenvolvidas novas tecnologias que aumentam a capacidade das redes e fornecerão mais largura de banda aos usuários da Internet". Até os dias de hoje a rede Internet, está em constante evolução, todo instante está surgindo novas ferramentas e serviços, e junto dele, os equipamentos também estão em contínuo processo de inovação, onde leva essas tecnologias até os usuários.

No começo, o principal objetivo da rede mundial era a eliminação dos problemas geográficos, mas com o passar do tempo vem oferecendo inúmeros benefícios nas atividades cotidianas dos usuários, e agilizando no funcionamento de diversos processos das empresas, assim, aos poucos foi-se incorporando na vida dos indivíduos e tornando-se um elemento essencial para o progresso da sociedade moderna. A Figura 2 mostra o aumento de usuários em milhões na rede Internet desde ano 2005 a 2016 na *Africa* (África), *Arab States* (Estados árabes), *Asia & Pacific* (Ásia & Pacífico), CIS-*Commonwealth of Independent States* (Comunidade dos Estados Independentes), *Europe* (Europa) e *The Americas* (Américas).

Figura 2 - Crescimento de usuário de Internet no mundo em milhões por ano



Fonte: Adaptado de ITU - *Committed to connecting the world* (2017) [1]

[1] Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em: 17 fev. 2017.

3. PROTOCOLO IP

O elemento principal que compõe a Internet é o protocolo, ele é responsável em estabelecer a troca de informações entre as entidades envolvidas (transmissão / recepção), para que a comunicação ocorra é necessário estar dentro das regras propostos pelo protocolo. Segundo Kurose e Ross (2013, p. 7), “Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento”.

Dois modelos de arquiteturas de rede serão apresentados a seguir:

3.1 Modelo OSI

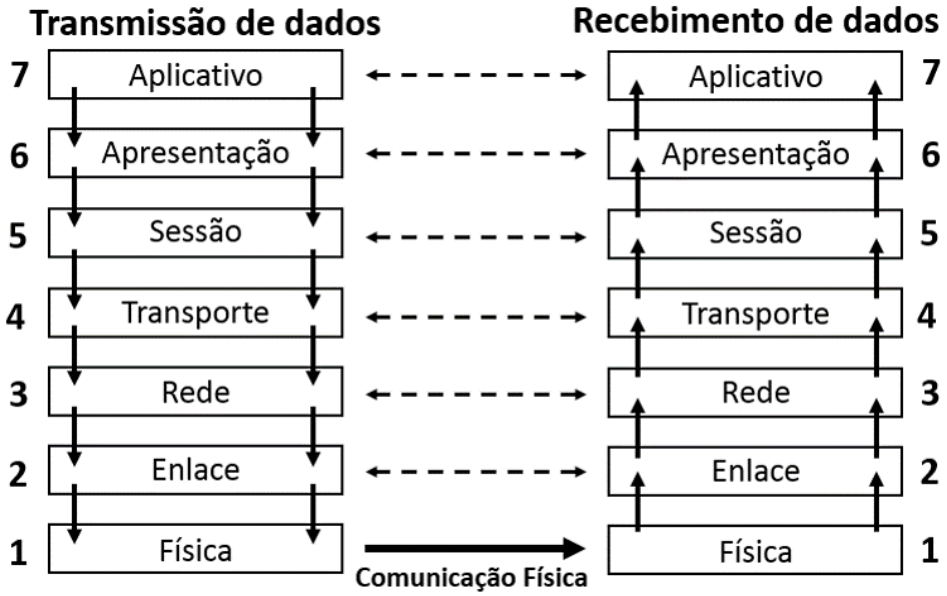
O modelo de referência OSI - *Open System Interconnection* (Interconexão de Sistemas Abertas), é criado pelo ISO - *International Standards Organization* (Organização Internacional de Padrões), com objetivo de padronizar os protocolos em forma de camadas, mas não foi totalmente implantada, no entanto, serve somente como um modelo para estudos, e é válido até os dias de hoje, pois expõe aspectos importantes de cada camada, mostrando a possibilidade de comunicação entre redes distintas.

De acordo com Tanembaum (2011, p.40), “esse modelo se baseia em uma proposta desenvolvida pelo ISO (*International Standards Organization)* como um primeiro passo a direção à padronização internacional dos protocolos empregados nas diversas camadas”.

Esse modelo é composto por sete camadas, no qual, trabalham em conjunto. Cada camada possui a sua própria função que é responsável em uma parte na transmissão das informações. A Figura 3, mostra o percurso da informação quando é enviada.

Conforme Forouzan (2008, p. 18), “o modelo OSI é composto de sete camadas ordenadas: física (camada 1), enlace de dados (camada 2), rede (camada 3), transporte (camada 4), sessão (camada 5), apresentação (camada 6) e aplicativo (camada 7) ”.

Figura 3 - Modelo OSI



Fonte: Elaborado pelo autor

A seguir são apresentadas as funções de atuação de cada camada, no modelo OSI.

Camada física (1): Situado no nível mais baixo, é responsável pelo processo de deslocamento de *bits* de uma máquina para a outra máquina através de um meio físico (*hardware*). Nessa camada é definido toda estrutura para a movimentação dos

bits, como os componentes físicos serão conectados, velocidade e modo de transmissão, a interface (elétrica, mecânica, óptica e funcional), codificação (transformado em sinais) e sincronização de *bits.*

> "A camada física coordena as funções exigidas para transportar um fluxo de bits por um meio físico. Ela lida com as especificações mecânicas e elétricas das interfaces e do meio de transmissão. Define, também, os procedimentos e funções que os dispositivos físicos e interfaces precisam executar para que a transmissão ocorra" (FOROUZAN, 2008, p. 21).

Camada de enlace de dados (2): A principal função dessa camada é a detecção e correção de erro na transmissão de dados da camada física para camadas superiores, ele divide os dados em inúmeros quadros (*frames*) que é incluído o cabeçalho do remetente / receptor (MAC) e em seguida são enviados de forma ordenada, fazendo o controle do fluxo, onde, gerencia a quantidade e a velocidade desses *frames*, regulando o tráfego.

> "A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruto em uma linha que pareça livre de erros de transmissão não detectados para a camada de rede. Para executar essa tarefa, a camada de enlace de dados faz com que o transmissor divida os dados de entrada em quadros de dados (que, em geral, tem algumas centenas ou alguns milhares de *bytes*), e transmita os quadros sequencialmente" (TANENBAUM, 2011, p. 42).

Camada de rede (3): A camada de rede é responsável pelo endereçamento dos dispositivos e faz o controle da rota dos pacotes, selecionando melhores caminhos para o tráfego de dados da origem até destino, em situações de congestionamento ou falha, ele procura por caminhos alternativos para levar até o receptor, dessa forma, estabelece a interligação entre as redes desde o começo até a finalização da transferência.

Segundo Macêdo (2012):

> "[...] o endereço físico (MAC) da camada de Enlace (2) e converte para endereço lógico (IP). Quando a camada de Rede (3) recebe a unidade de dados da camada de Enlace (2), chamado de "quadro", transforma em sua própria PDU com esse endereço lógico, que será utilizado pelos roteadores para encontrar os melhores caminhos de dados".

Camada de transporte (4): Essa etapa é realizada a associação entre os pacotes que pertence a mesma mensagem, fazendo com que os dados cheguem inteira e

em sequência ao destinatário. Conforme Forouzan (2008, p. 24), “[..] garante que a mensagem chegue intacta e em ordem, supervisionando o controle de erros e o controle de fluxo em nível de origem para o destino”. Nessa camada também é feito o controle de fluxo e controle de erro, verificando se ocorreu algum dano ou perda, para realizar a transmissão novamente dos pacotes.

Camada de sessão (5): Na camada sessão, estabelece o diálogo e sincronização entre ambas as partes durante a comunicação.

Conforme Macêdo (2012), “[...] sendo esta responsável por iniciar, gerenciar e finalizar as conexões entre os hosts, e por se preocupar com a sincronização entre eles, para que a sessão aberta entre eles mantenha-se funcionando. ”

Camada de apresentação (6): Encarregado de realizar a tradução das informações de uma máquina para a outra máquina, uma vez que as máquinas que se comunicam têm codificações diferenciadas, então em uma ponta (origem) a camada de apresentação traduz em formato em que possa entender, essa tradução também é feita em outra ponta (destino).

A camada 6 faz a criptografia das informações e compactação das informações trafegadas, garantindo a confidencialidade e redução do tamanho dos pacotes.

> “Ela pode ser considerada o tradutor da rede. Pode converter dados de um formato usado pela camada de aplicativo ou aplicação em um formato comum na estação de envio e, em seguida, converter esse formato comum em um formato conhecido pela camada de aplicativo na estação de recepção” (SILVEIRA, 2016).

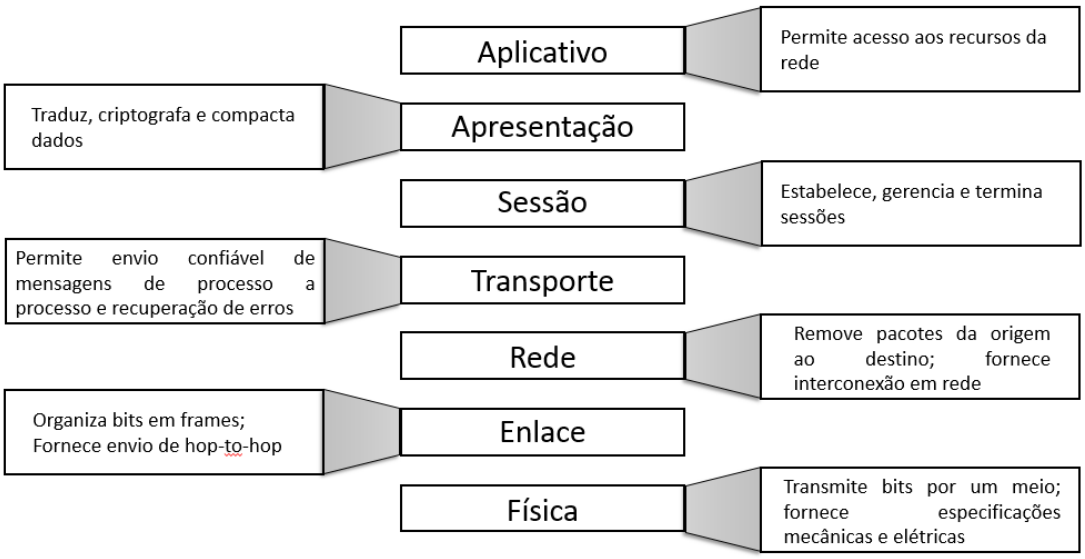
Camada de aplicativo (7): Camada que possui contato com o usuário, onde localiza um conjunto de protocolos usados para transferência de dados.

Para Tanenbaum (2011, p. 44), “A camada de aplicação contém uma série de protocolos comumente necessário para os usuários ”.

Outra definição feita pelo Forouzan (2008, p. 28), “A camada de aplicativo permite ao usuário, seja humano ou software, acessar a rede. Ela fornece interfaces do usuário e suporte para serviços [...] ”.

Como apresentado na Figura 4 um breve resumo das funções de cada camada.

Figura 4 - Resumo do modelo OSI



onte: Adaptado de Forouzan (2008, p. 29)

Essas camadas são divididas em três grupos, onde as camadas 1, 2 e 3 (física, enlace e rede), atuam como transferência de dados por meio físico, as camadas 5, 6 e 7 (sessão, apresentação e aplicativo), levam serviços ou informações até o usuário, a camada 4 (transporte) faz a interligação entre o meio físico e meio digital.

> “As sete camadas podem ser consideradas como pertencentes a três subgrupos. As camadas 1, 2 e 3 – física, enlace de dados e rede – são as de suporte de rede; elas lidam com os aspectos físicos de movimentação de dados de um dispositivo ao outro (como as especificações elétricas, conexões físicas, endereçamento físico, sincronização de transporte e confiabilidade). As camadas 5, 6 e 7 – sessão, apresentação e aplicativo – podem ser considerados como suporte ao usuário; elas permitem a operação conjunta entre sistemas de *software* não-relacionadas. A camada 4, de transporte, une os dois subgrupos [...]” (FOROUZAN, 2008, p.20).

3.2 Modelo TCP/IP

O protocolo TCP/IP é usado nos dias de hoje para a transferência de dados pela rede, como citado anteriormente, foi desenvolvida nova arquitetura para substituir o antigo protocolo (NCP), pois com o aumento do uso da Internet, O NCP, não estava conseguindo suportar a grande escala de usuário, então era necessário a substituição pelos protocolos modelo TCP/IP, que tornou padrão, na utilização para transferência de informações pela rede.

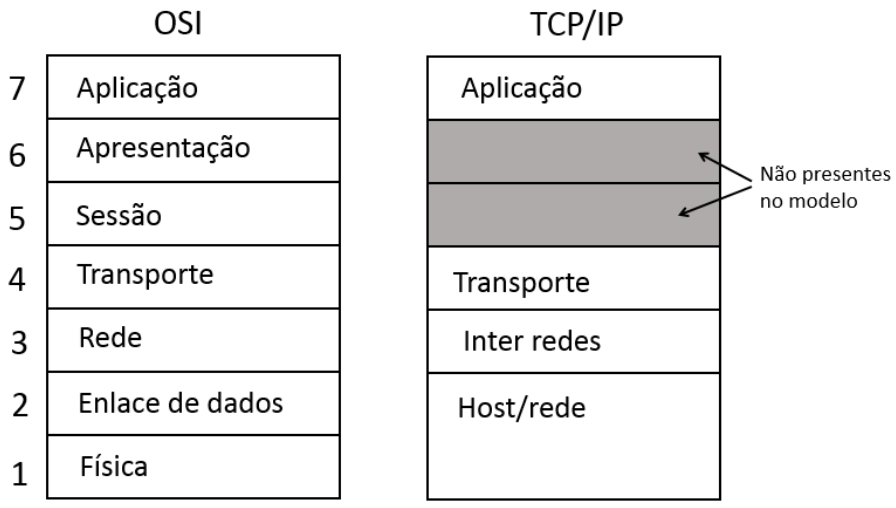
Segundo Tanenbaum (2011, p.44):

> “Pouco a pouco, centenas de universidades e repartições públicas foram conectadas, usando linha telefônica dedicada. Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência. Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto, desde o início. Mais tarde, essa arquitetura ficou conhecida como Modelo de Referência TCP/IP [...]”

O TCP/IP é formado por camadas: host/rede, Inter redes, transporte e aplicação, em que as funções são referentes aos do modelo OSI, mas trabalham de forma independente, ou seja, cada camada serve serviços as camadas superiores, mas uma camada não influencia na atividade da outra camada. A Figura 5, mostra a comparação do modelo TCP/IP em relação ao modelo OSI.

De acordo com Forouzan (2008, p.30), “[...] as camadas do conjunto de protocolos TCP/IP contêm protocolos relativamente independentes que podem ser misturados e combinados de acordo com as necessidades do sistema”.

Figura 5 - Comparação entre modelo OSI e modelo TCP/IP



Fonte: Adaptado de Tanenbaum (2011, p. 46)

3.3 Endereço IP

O endereço IP- *Internet Protocol*, é uma forma padrão para estabelecer a comunicação entre duas ou mais rede, todos os dispositivos, para se conectarem na Internet é fundamental possuir um endereço IP. Conforme Brito (2013, p. 25), “ [...]

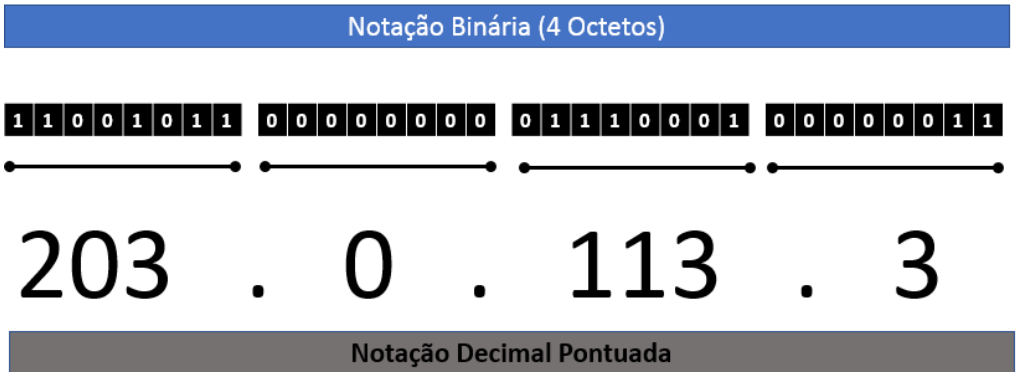
uma vez que toda nova máquina conectada na Internet necessitava de um endereço IP. ”

3.3.1 Protocolo versão quatro (IPv4)

IPv4 é a verão mais utilizada atualmente, é constituído por 32 bits de comprimento, divididos em quatro blocos de 8 bits (octeto), que são escritos no formato decimal, dentro da faixa 0 a 255 e são separados através de pontos, utilizados para identificar a rede e o *host* que pertence a determinada rede. Conforme mostrado na Figura 6, exemplo de endereço IPv4.

Segundo IBM [s.d], “32 bits de comprimento (4 *bytes*). O endereço é composto por uma rede e uma parte do sistema central, que depende da classe do endereço [...] O formato de texto do endereço de IPv4 é nnn.nnn.nnn.nnn, em que 0<=*nnn*<=255, e cada *n* é um algarismo decimal ”.

Figura 6 - Exemplo de endereço IPv4



Fonte: Adaptado de Brito (2013, p. 24)

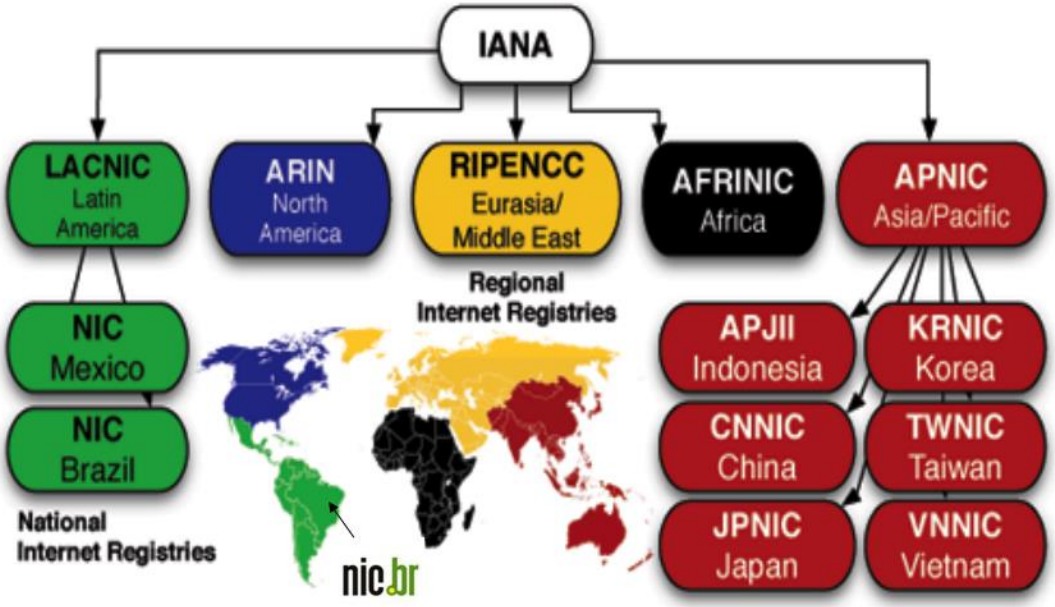
O protocolo versão 4 possui aproximadamente 4.3 bilhões de endereços, mas com o crescimento dos dispositivos e o aumento no uso do endereço IP que levou o esgotamento desses, ou seja, não possui mais endereços o suficiente para atender a demanda dessa grande escala de objetos conectados pela rede.

> “Com os 32 bits do IPv4, era possível endereçar 2^{32} nós, o equivalente a 4.294.967.296 (aproximadamente 4 bilhões e 300 milhões) de endereços únicos. Esse número parecia absurdamente alto para a finalidade inicial, e ninguém podia imaginar que esses endereços um dia esgotar-se-iam [...]” (BRITO, 2013, p. 24).

A Figura 7, mostra as autoridades regionais responsáveis pela distribuição de endereços IP, coordenado pela ICANN - *Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Atribuição de Nomes e Números), órgão global responsável pelo gerenciamento de nome de domínio e endereços na Internet, que assumiu o trabalho da IANA - *Internet Assigned Numbers Authority* (Autoridade para Atribuição de Números da Internet).

Conforme Forouzan (2008, p. 13), "[...] a ICANN (*Internet Corporation for Assigned Names and Numbers*), uma empresa privada sem fins lucrativos, gerenciada por uma junta internacional, assumiu as operações da IANA ".

Figura 7 - Autoridades regionais no gerenciamento de endereços na Internet

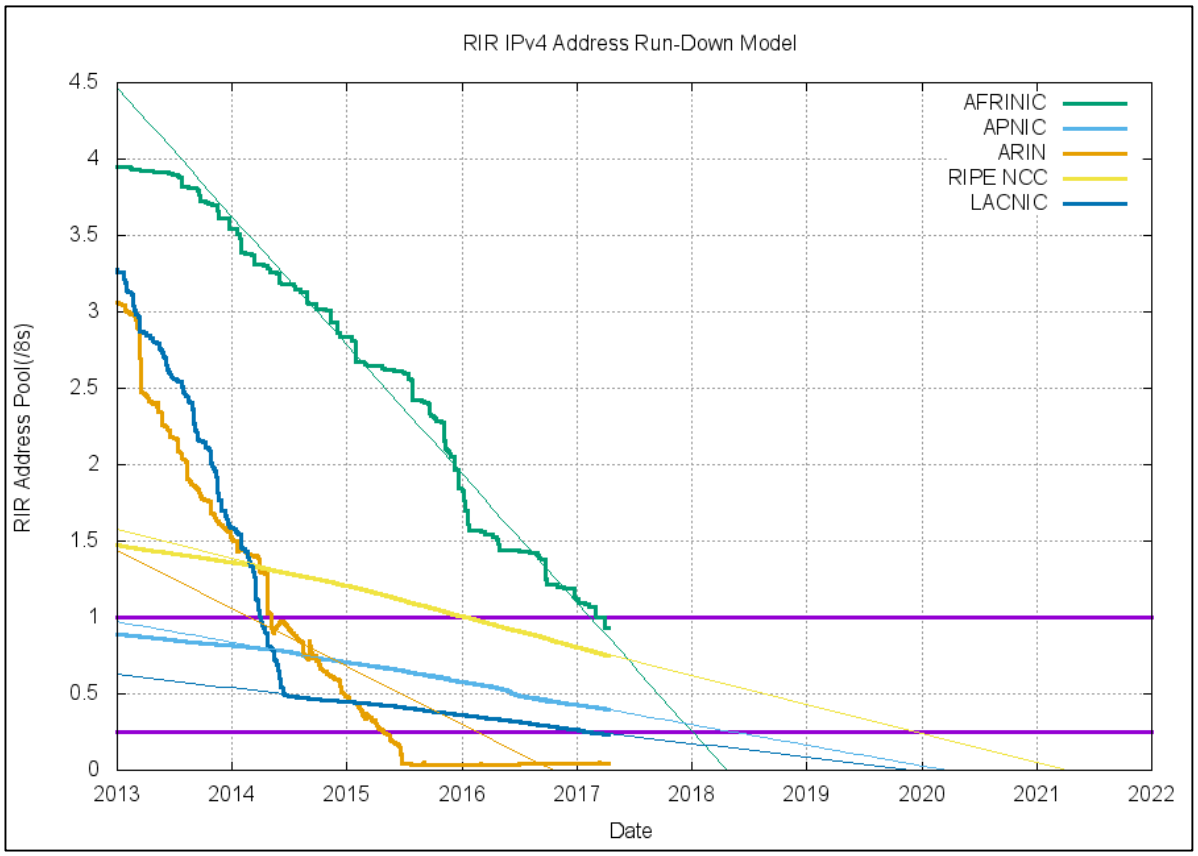


Fonte: Comitê Gestor da Internet no Brasil (2013) [1]

[1] Disponível em: <http://www.cgi.br/media/pdfs/apresentacoes/ipv6apresentacaoCGI_RI19032013.pdf>. Acesso em: 20 fev. 2017.

Conforme o gráfico da Figura 8, mostra o esgotamento do IPv4, de cada autoridade regional, AFRINIC (ÁFRICA), APNIC (Ásia e Pacífico), ARIN (América do Norte), RIPE NCC (Europa) e LACNIC (América Latina e Caribe).

Figura 8 - Esgotamento de IPv4



Fonte: Portal IPv6 - LACNIC [s.d][1]

[1] Disponível em: <http://www.cgi.br/media/pdfs/apresentacoes/ipv6apresentacaoCGI_RI19032013.pdf>. Acesso em: 20 fev. 2017.

O esgotamento de IPv4 foi previsto em 1990, a partir disso, a entidade IETF - *Internet Engineering Task Force*, iniciou o estudo e o desenvolvimento da nova versão de protocolo, e durante esse tempo foram propostos mecanismos com o intuito de adiar o esgotamento dos endereços IPv4.

De acordo com Kurose e Ross (2013, p. 270), “ No começo da década de 1990, a IETF iniciou um esforço para desenvolver o sucessor do protocolo IPv4. Uma motivação primária para esse esforço foi o entendimento de que o espaço de endereços IP de 32 bits estava começando a escassear [...] ”.

Para Brito (2013), os três principais métodos usados para adiar o processo de esgotamento do IPv4 foram: CIDR, DHCP e NAT.

- CIDR - *Classless Inter Domain Routing* (Roteamento Interdomínio sem Classes)

Conforme IPv6.br (2012), “[...] o CIDR tem como ideia básica o fim do uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado a real necessidade de cada rede”, o endereçamento IPv4 é dividido em três classe: A (8 bits), B (16 bits), C (24 bits), para endereçar redes de pequeno, médio e grande porte, mas através dessa forma de atribuição estava causando muito desperdiço de endereços, e em relação ao problema de esgotamento de IP, foi proposta a medida de CIDR, onde, possibilita a distribuição de endereços em faixas com tamanhos variáveis.

- DHCP - *Dynamic Host Configuration Protocol* (Protocolo de configuração dinâmica de host)

O DHCP, faz atribuição de endereço IP automático, em que, atua de maneira temporária no usuário conectado, quando esse se desconecta da rede, o IP é devolvido para o reservatório, dessa forma, não é necessário que cada dispositivo tenha seu próprio endereço IP.

Segundo Kurose e Ross (2013, p.266), “Toda vez que um hospedeiro se conecta à rede, o servidor DHCP designa a ele um endereço arbitrário do seu

reservatório corrente de endereços disponíveis; toda vez que um hospedeiro sair, o endereço é devolvido ao reservatório ”.

- NAT - *Network Address Translation* (Tradução de endereços de rede)

O NAT tem como função, o compartilhamento de um ou alguns endereços IP entre os *hosts* para que possam se conectar na rede externa, em relação a conexão da rede interna é atribuído para cada host endereço privado para possibilitar a troca de dados apenas no ambiente interno.

> “[...] foram reservadas algumas faixas de endereços dentro de cada uma das classes padrões para uso apenas local, sem comunicação com a Internet. Esses endereços são 10 /8 (de 10.0.0.0 até 10.255.255.255), 172.16 /12 (de 176.16.0.0 até 172.31.255.255) e 192.168 /16 (de 192.168.0.0 até 192.168.255.255). Essa também foi uma medida para fins de economizar os endereços IPv4 roteáveis na Internet, pois, em razão desses endereços privados, uma empresa não precisava mais de um endereço público roteável na Internet para cada um dos seus hosts internos. ” (BRITO, 2013, p. 32).

3.3.2 Protocolo versão seis (IPv6)

Quando foi acionada a alerta de que o protocolo IPv4 estava se esgotando, a entidade IETF, iniciou as pesquisas para a criação da nova versão de IP o IPv6, ele é compatível com o seu antecessor IPv4, mas teve algumas mudanças, e melhoramento em vários aspectos.

> “Para atender a essa necessidade de maior espaço para endereços IP, um novo protocolo IP, o IPv6, foi desenvolvido. Os projetistas do IPv6 também aproveitaram essa oportunidade para ajustar e ampliar outros aspectos do IPv4 com base na experiência operacional acumulada sobre esse protocolo. ” (KUROSE; ROSS, 2013, p.2008).

Alguns novos aspectos e mudanças principais entre IPv4 comparado com seu sucessor o IPv6, pode ser observado na Tabela 1 criado com base no BCA Telecom. [1]

[1] Disponível em: < http://www.consultoriastelecom.com.br/artigo-46-diferencas-entre-ipv4-e-ipv6>. Acesso em: 23 fev. 2017.

Tabela 1 - Comparação de IPv6 e IPv4

	IPv4	**IPv6**
Endereço	32 bits (4 bytes)	128 bits (16 bytes)
Tamanho do pacote	Suporta 576 bytes, fragmentação opcional	Suporta 1280 bytes, sem fragmentação
Fragmentação do pacote	Feito pelo *router*	Feito pelo *host*
Cabeçalho do pacote	Não contém *QoS – Quality of Service* (Qualidade de serviço)	Contém campo que manuseia *QoS*

Registro DNS - Domain Name System (Sistema de Nomes de Domínios)	Registro (A), para mapear os nomes de hosts	Registro (AAAA), para mapear os nomes de hosts
Configuração do endereço	DHCP ou manualmente	Automático
Resolução IP para MAC	Usa, Broadcast ARP	Usa, Multicast Neighbor Solicitation
Gestão de grupos de sub-rede local	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Broadcast	Utiliza	Não utiliza
Multcast	Possui	Possui
IPsec	Opcional	Obrigatorio

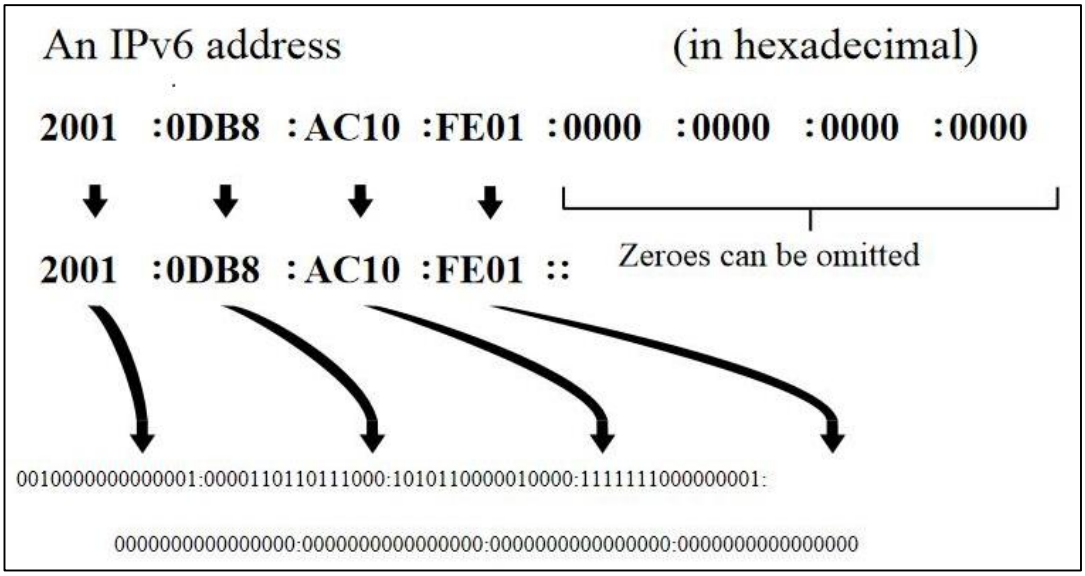
Fonte: Elaborado pelo próprio autor

O endereço IPv6 possui 128 bits de comprimento, é dividido em oito grupos de 16 bits (oito quartetos), e são escritos no formato hexadecimal, os dígitos podem ser escritos no formato maiúscula ou minúscula, pois a apresentação será o mesmo, ou seja, válido, nessa versão cada bloco é separado através de dois pontos. A Figura 9, mostra um exemplo de endereço IPv6, em formato binário comparado com o formato hexadecimal.

De acordo com IBM [s.d]:

> "O número de endereços de IPv6 é 10^{28} (79 228 162 514 264 337 593 543 950 336) vezes superior ao número de endereços de IPv4. O formato de texto do endereço de IPv6 é: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx em que cada x é um algarismo hexadecimal que representa 4 bits. Os zeros à esquerda podem ser omitidos. Os dois pontos duplos (::) podem ser utilizados se estiverem no formato de texto de um endereço, para designar qualquer número de 0 bits. "

Figura 9 - Endereço IPv6



Fonte: DLTec (2013)[1]

[1] Disponível em: <http://www.dltec.com.br/blog/redes/resumo-dos-enderecos-ipv6-para-quem-esta-estudando-para-ceriticacao/>. Acesso em: 25 fev. 2017.

Conforme Brito (2013, p.51):

> “O IPv6 possui 128 bits, o que permite o endereçamento de 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) de nós públicos na Internet. Esse número equivale a 79 trilhões de trilhões de vezes a quantidade atual de 4 bilhões e 294 milhões e 967 mil e 296 endereços IPv4. ”

O IPv6 em comparação ao IPv4, teve um aumento vultoso na capacidade de endereçamento, como mostrado na Figura 10, um exemplo de comparação de um copo de água (IPv4), com um rio (IPv6).

Figura 10 - Comparação de IPv4 e IPv6

Fonte: InfoWester (2011) [1]

[1] Disponível em: < https://www.infowester.com/ip.php>. Acesso em: 27 fev. 2017.

Os dígitos zero no endereço IPv6 podem ser abreviados, e essa abreviação pode ser feita em duas formas, nas quais contribuem para facilitar a manipulação desses endereços extensos.

Regra 1 – A abreviação, pode ser feita eliminando os zeros presente à esquerda de um quarteto. Exemplo: B8 equivale a 00B8, ou seja, as duas formas apresentada é válido, mas quando é 0000, o quarteto de zero poderá ser apresentado apenas por um 0.

Regra 2 – Outra forma aplicada quando o endereço apresentar uma sequência de zeros, esses podem ser eliminados substituindo por "**::**". Exemplo: 2001: 0DB8:0000:0000:0000:0000:0000:00B1, quando os zeros são retirados, o endereço se encontra dessa forma 2001:DB8::B1, pode perceber que tornou mais fácil na visualização do endereço.

Segundo IPv6.br (2012), "[...] regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por "::" ".

Os endereços IPv6 é apresentado em três tipos de categorias: *unicast, multcast e anycast.* De acordo com Kurose e Ross (2013, p.271), "Além dos endereços *multicast* e *unicast*, o IPv6 introduziu um novo tipo de endereço, denominado endereço *anycast* [...] ".

Conforme Brito (2013), as definições de cada categoria de endereços, são assim especificadas:

***Unicast* –** O pacote é enviado apenas para uma única interface, essa forma de comunicação pertence às seguintes categorias:

- *Link-local:* São autoconfigurados, apenas são usados para comunicação local, os pacotes não devem ser encaminhados para os outros enlaces.
- *Unique-Local Address* (ULA): Endereços privados, são utilizados localmente, ou seja, apenas utilizada na parte interna da empresa, essa opção é usada

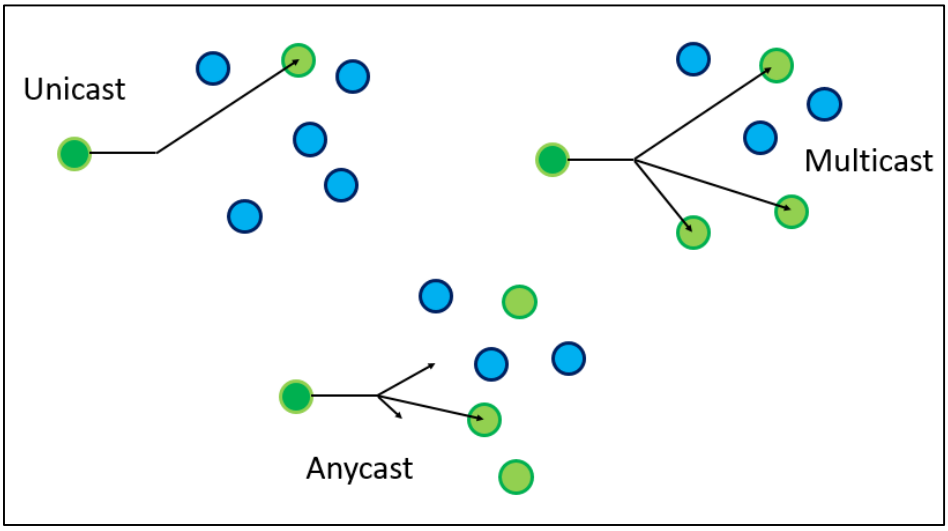
por instituições que não desejam atribuir endereços públicos em determinadas máquinas, para rotearem na Internet.

- *Global unicast:* É roteado globalmente e permite utilizar a Internet.

Multcast – O pacote é enviado para todas os enlaces que fazem parte do grupo, não pode ser utilizado na origem de uma comunicação, pois esse representa um grupo, e contém vários nós, então é apenas utilizado como destino.

Anycast – Esse modelo surgiu no IPv6, atua de forma que, quando um pacote é enviado, apenas é direcionada para a interface do grupo que está mais próximo da origem que enviou o pacote. A Figura 11, mostra de forma ilustrada cada tipo de endereçamento.

Figura 11 - Tipos de comunicação de rede no IPv6



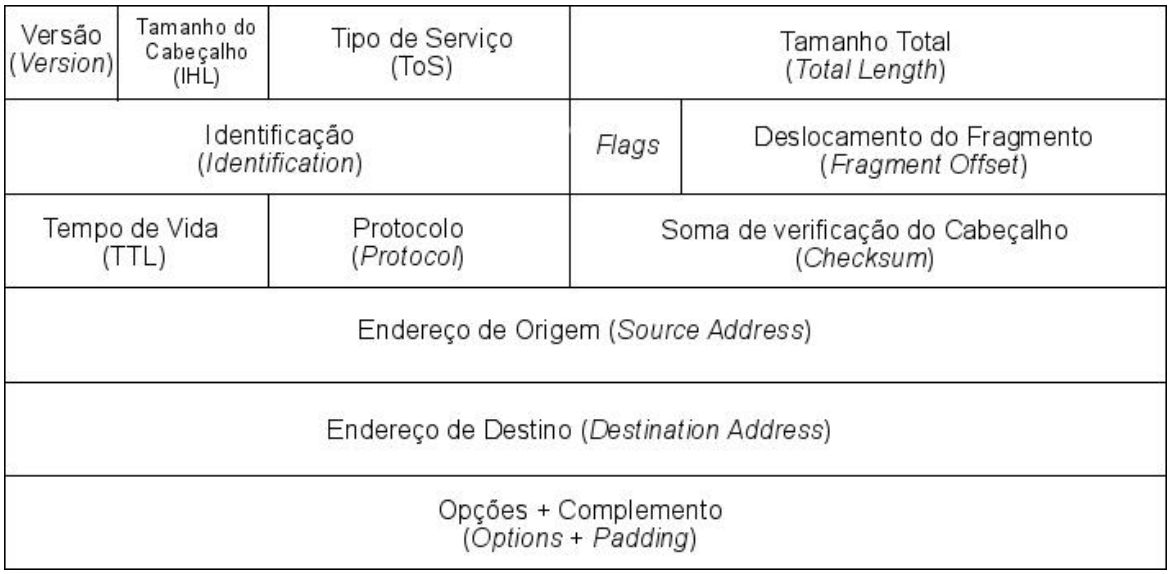
Fonte: Brito (2013, p. 58)

3.3.3 Cabeçalho do protocolo IPv4 e IPv6

Na nova versão de IP (IPv6), uma das mudanças que mais se destacou foi a estrutura do cabeçalho, onde muitos elementos foram otimizados. A comparação entre os cabeçalhos das duas versões (IPv4 e IPv6), será mostrado a seguir.

Conforme IPv6.br (2012), o tamanho do cabeçalho de IPv4 que varia de 20 a 60 *bytes*, ele é composto por 12 campos fixos. A Figura 12, apresenta o modelo do cabeçalho IPv4.

Figura 12 - Cabeçalho IPv4



Fonte: IPv6.br (2012)[1]

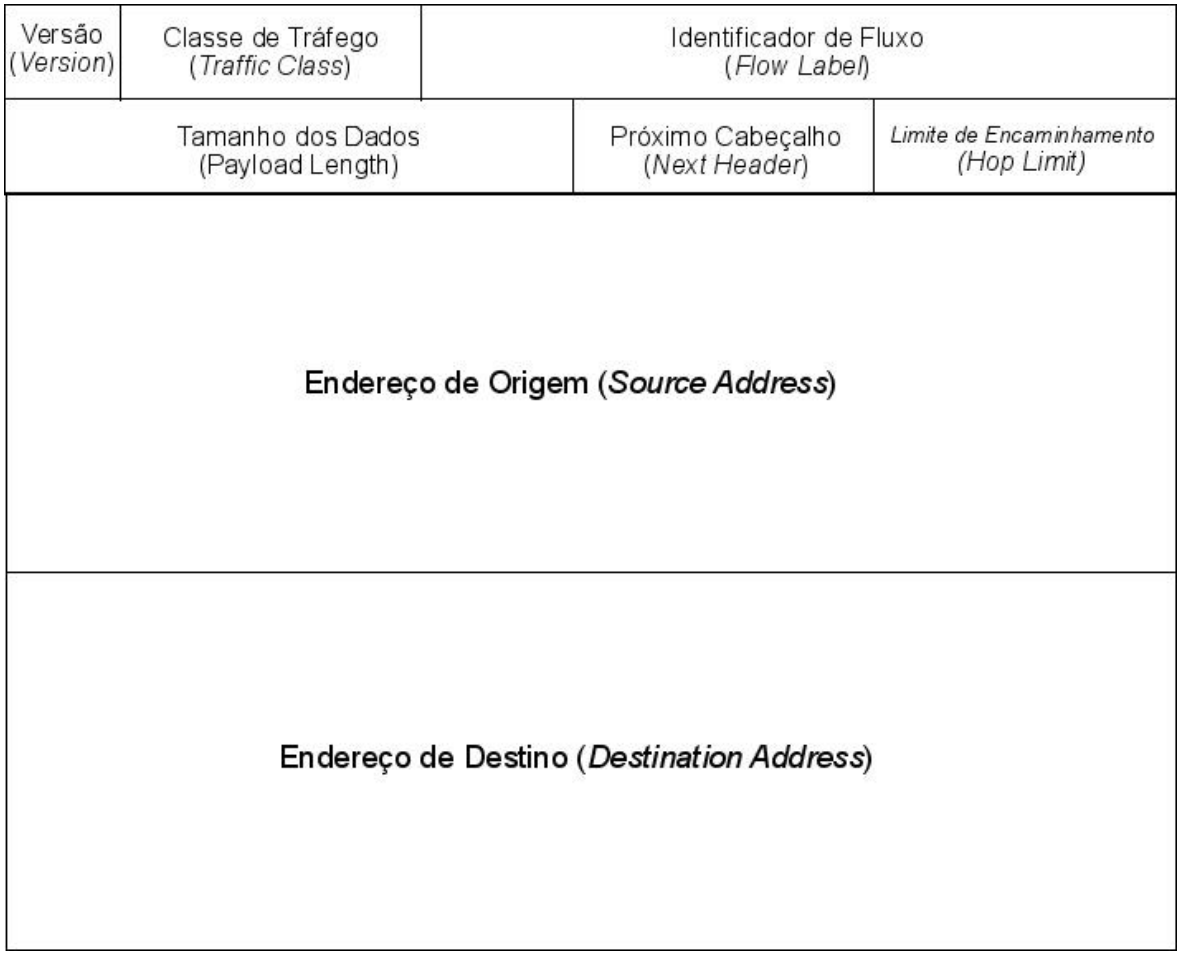
[1] Disponível em: <http://ipv6.br/post/cabecalho/>. Acesso em: 3 mar. 2017.

De acordo com Kurose e Ross (2013), os elementos contidos no cabeçalho IPv4, mostrado acima são:

- Versão: número da versão do protocolo IP, no caso é 4.
- Tamanho do cabeçalho: varia de 20 a 60 bytes.
- Tipo de serviço: realiza a diferenciação dos datagramas de IP, verificando os tipos de serviços que será aplicada em relação a alguns datagramas que necessitam de alta vazão, baixo atraso, confiabilidade, entre outros.
- Tamanho total: o comprimento do datagrama, ou seja, o tamanho do cabeçalho junto com os dados.
- Identificação, *flags* e deslocamento de fragmentação: fragmentação dos pacotes.
- Tempo de vida: quando o pacote ultrapassa do seu tempo de envio é descartado, para evitar a circulação permanente pela rede.
- Protocolo: identifica para qual protocolo (TCP, UDP, ICMP) o pacote deve ser direcionado.
- Soma de verificação do cabeçalho: faz a verificação e auxilia o roteador a detectar erros de bits de um pacote recebido.
- Endereço de origem / endereço de destino: é adicionado o IP de origem e de destino.
- Opções: pouco usado, campo para incluir outros tipos de serviço, em proporção a isso em que o cabeçalho varia de 60 a 20 bytes.

Segundo Brito (2013), o cabeçalho do IPv6 foi aprimorado, possuindo apenas 8 campos, com tamanho fixo de 40 bytes, dessa forma, os pacotes não serão mais necessários ser analisado pelo roteador, assim contribuirá no melhoramento do seu desempenho. Pode ser observado na Figura 13, o modelo do cabeçalho IPv6.

Figura 13 - Cabeçalho IPv6



Fonte: IPv6.br (2012)[1]

[1] Disponível em: <http://ipv6.br/post/cabecalho/>. Acesso em: 3 mar. 2017.

Segundo Kurose e Ross (2013), os elementos presentes no cabeçalho IPv6, mostrado acima são:

- Versão: número da versão IP, no caso é 6.
- Classe de tráfego: contém a mesma função do campo “tipo de serviço”, do cabeçalho IPv4.
- Identificador do fluxo: identificar o fluxo do pacote da mesma comunicação, para aplicar tratamentos específicos, nesse campo atua também o serviço de suporte a *QoS.*
- Tamanho dos dados: tamanho do cabeçalho junto com os dados enviados, é adicionado também o cabeçalho de extensão (será explicado no próximo sessão).
- Próximo cabeçalho: realiza a análise do pacote, identificando para qual protocolo que esse será entregue.
- Limites de encaminhamento: limite de salto, ou seja, quando atingir o número máximo de vezes que passou pelo roteador, o pacote é descartado.
- Endereço de origem / endereço de destino: é adicionado o IP de origem e de destino.

3.3.4 Cabeçalho de extensão

Conforme IPv6.br (2012), os serviços opcionais no cabeçalho IPv6 são tratados como cabeçalho de extensão que é localizado entre cabeçalho base e cabeçalho de camada de transporte, não tem um tamanho fixo, pois são adicionados de acordo a necessidade. Em situações de quando existir vários cabeçalhos de extensão no mesmo pacote, esses são inseridos de forma ordenada no formato de cadeia como mostrado na Figura 14.

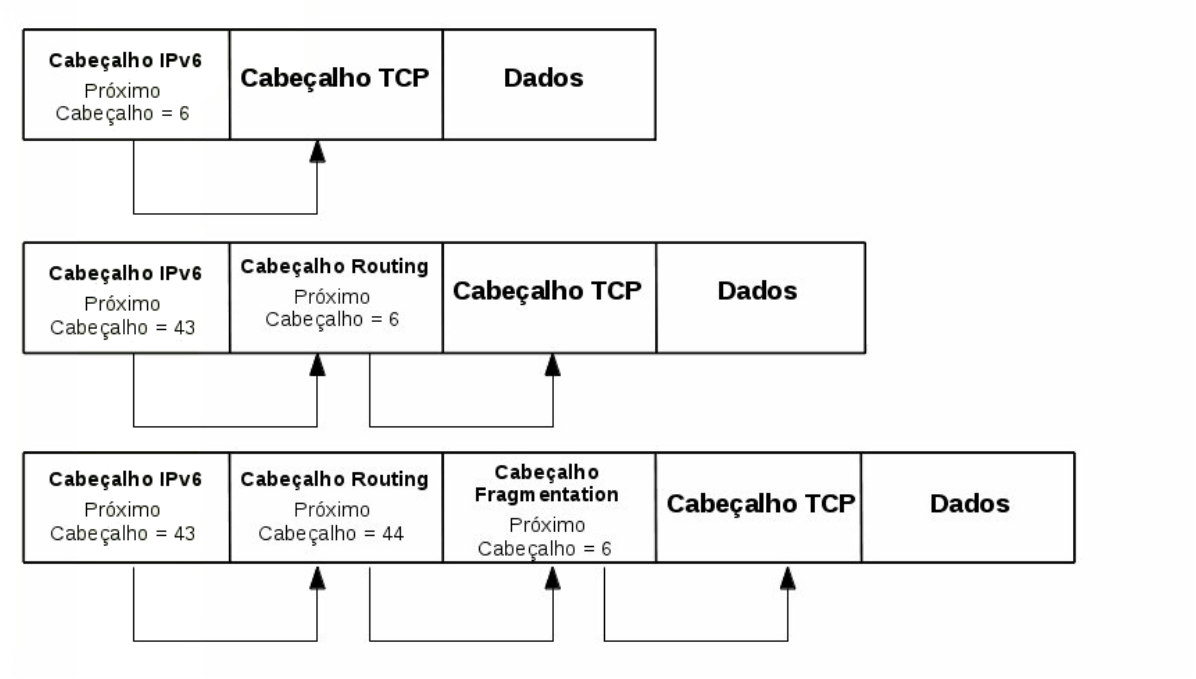


Figura 14 - Cadeia de cabeçalhos

Fonte: IPv6.br (2012)[1]

[1] Disponível em: <http://ipv6.br/post/cabecalho/>. Acesso em: 5 mar. 2017.

De acordo com Forouzan (2008), os seis tipos de extensões. São expostos com mais detalhe abaixo:

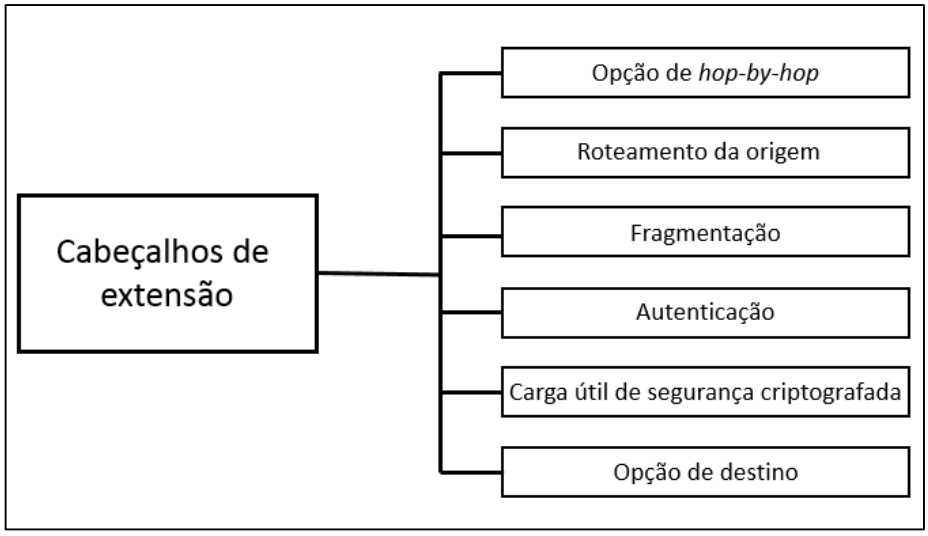
- Opção de *hop-by-hop* – no caminho é analisado pelos roteadores, essa extensão é usada quando a origem precisa passar alguma mensagem para os roteadores, informando de algum serviço que necessita ser prestado por eles.
- Roteamento de origem – analisado pelo destinatário, usado para suporte de mecanismo móvel.
- Fragmentação – utilizado para verificação dos pacotes que precisam ser fragmentados pela origem.
- Autenticação – essa extensão garante a integridade dos dados recebidos pelo destinatário, assegurando que as informações foram omitidas pelo remetente e não foram modificados.
- Carga útil de segurança criptografada – define o tipo de criptografia, usado para prover confidencialidade.
- Opção de destino – permitir apenas o receptor tenha acesso às informações, os roteadores não terão permissão de acessar a esses dados.

Essas opções de cabeçalhos de extensão devem ser inseridas de forma ordenada, assim, quando o roteador, no momento de processar não necessite passar por todos eles a procura do cabeçalho que deverá ser tratado primeiro. A ordem definida é ilustrada na Figura 15.

Segundo IPv6.br (2012):

> “Primeiramente, estes cabeçalhos devem ser enviados segundo uma determinada ordem com o intuito de evitar que os nós intermediários tenham que processar toda a cadeia de cabeçalhos para decidir quais eles deverão tratar. Assim, os cabeçalhos importantes para todos os nós envolvidos no roteamento devem ser colocados em antes daqueles que são relevantes apenas para o destinatário final. ”

Figura 15 - Cabeçalhos de extensão



Fonte:

Adaptado de Forouzan (2006, p.703)

4. SEGURANÇA DA INFORMAÇÃO

Na era da informação mudanças não param, novas tecnologias e novos métodos são criados a cada momento, segundo Menezes (2003), “A convergência digital cria novos aparelhos, novas formas de comunicação e novas plataformas de produção de dados, fazendo surgir novos canais a partir da hibridação de formas de comunicação, antes isoladas”. Mas além dos benefícios abundantes que a tecnologia traz, o fator maléfico também está em constante evolução, e a proteção da informação está sendo cada vez mais necessária e indispensável.

A informação é considerada como um ativo de alta relevância para a continuidade dos processos e dependendo do seu grau de importância pode trazer impacto para o usuário ou para a empresa, caso aconteça algum evento inesperado, como, dano, roubo ou perda da informação. A questão da redução do número de risco até o mínimo possível, é tratada pela Segurança da Informação.

> “Segurança da informação é o conjunto de orientação, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o

> recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada. Segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos da informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas" (FONTE, 2006).

A Segurança da Informação é um conjunto de métodos tomados para minimizar os riscos e as vulnerabilidades, assegurando a proteção da informação contra os ataques

Tanenbaum (2011, p. 767) define a Segurança da Informação como:

> "A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que elas não estão autorizadas a usar. Ela também lida com meios para saber se uma mensagem supostamente verdadeira é um trote."

As ferramentas e técnicas tem como função a preservação do valor da informação, introduzindo obstáculos, evitando que o agente mal-intencionado alcance o objetivo desejado.

De acordo com Kurose e Ross (2013), segurança não é apenas assegurar com que a informação seja intacta, mas também, detectar ataques e falhas da rede e propor soluções para esses casos.

Campos (2007), a elaboração de estratégias e ações em relação à proteção da informação, está baseada nos três pilares (CID - confidencialidade, integridade e disponibilidade), como mostrado na Figura 16, os elementos fundamentais para sustentar a Segurança da Informação.

Figura 16 - Três principais pilares da Segurança da Informação

Fonte: Deb Solutions TI (2015)[1]

[1] Disponível em: <http://debsolutionsti.com/iso-27000/iso-27000/>. Acesso em: 3 mar. 2017.

- Confidencialidade

Segundo Kurose e Ross (2013, p. 513), “Somente o remetente e o destinatário pretendidos devem poder entender o conteúdo da mensagem transmitida”, ou seja, apenas as pessoas autorizadas podem ter acesso às informações.

De acordo com Microsoft TechNet (2012), a confidencialidade preserva a informação para o acesso apenas por pessoas que tenham permissão, evitando o acesso de pessoas não autorizados.

- Integridade

Integridade para Microsoft TechNet (2012), “É a garantia de que apenas a informação permanecerá sem alteração indevida por pessoa não autorizadas”.

Conforme Kurose e Ross (2013), Integridade é assegurar que a informação seja verdadeira, originada pelo remetente legítimo, e não sofreu nenhuma modificação indevido no caminho até o receptor.

- Disponibilidade

Segundo Kurose e Ross (2013), a disponibilidade é garantir que a informação ou algum recurso do sistema esteja sempre disponível para os usuários legítimos quando solicitados.

4.1 Mecanismos de segurança

Para assegurar que os elementos fundamentais para a Segurança da Informação sejam atendidos, foram desenvolvidas ferramentas e técnicas com o propósito de proteger e tratar as ameaças e ataques ocorridos na rede, esses métodos atuam como um escudo, quando trabalham em conjuntos, fortalece ainda mais a segurança.

Existem vários tipos de ferramentas que oferecem suporte à segurança da informação, conforme Cert.br (2012), “[...] mecanismos de segurança que, quando

corretamente configurados e utilizados, podem auxiliá-lo a se proteger dos riscos envolvendo o uso da Internet. ”, em seguida será apresentado algumas delas.

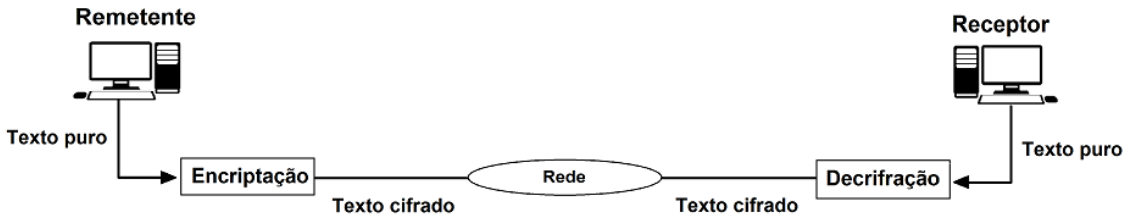
Criptografia - São técnicas que modificam as mensagens do remetente para o formato de cifras, tornando incompreensível, apenas o receptor consegue restaurar esses dados para o formato legível, tem como finalidade proteger as informações contra acessos indevidos.

> “Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário, é claro, deve estar habilitado a recuperar os dados originais a partir dos dados interceptado” (KUROSE; ROSS, 2006, p.516).

Outra definição feita por Forouzan (2008, p. 727), “ [...] a palavra criptografia significa ‘escrita secreta’. Entretanto, atualmente o termo se refere à ciência e à arte de transformar mensagens para torná-las seguras e imunes a ataques ”.

Mostrado na Figura 17, o processo de transformação das mensagens legíveis (texto claro), para mensagens cifradas, é chamado de encriptação, onde é usado o método de algoritmo e chaves, em que, exerce o papel de criptografar e descriptografar (quando o remetente faz a restauração do texto para o formato original).

Figura 17 - Componentes da criptografia



Fonte: Adaptado de Forouzan (2008, p. 727)

A divisão dos algoritmos de chaves para encriptação é feita da seguinte forma, segundo Forouzan (2008, p. 728):

> “Podemos dividir todos os algoritmos de encriptação do mundo em dois grupos: algoritmos de encriptação de chave simétrica (às vezes chamada

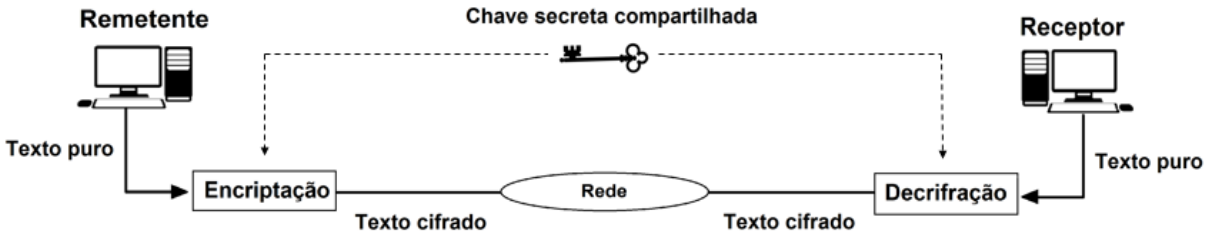
> de chave secreta) e algoritmos de encriptação de chave assimétrica (frequentemente chamada de chave pública) ”.

- Chaves simétricas: A chave é compartilhada entre o remetente e o receptor, ou seja, a chave usada pelas ambas as partes são iguais, na codificação e descodificação das informações.

De acordo com Cert.br (2012), chave simétrica pode também ser chamada de chave secreta, esse método é utilizado para assegurar a confidencialidade dos dados trafegados na rede. Exemplos de alguns algoritmos onde são usados na chave simétrica: 3DES - *Triple Data Encryption Standard* (*Triplo* DES), AES - *Advanced Encryption Standard* (Padrão avançado de criptografia), *Blowfish*, RC4 - *Rivest Cipher 4* (Cifrador de Rivest) e OTP - *One-time pad* (Chave de uso único).

De acordo com Forouzan (2008, p. 728), “ Na criptografia de chave simétrica, a mesma chave é usada pelo remetente (para encriptação) e pelo receptor (para decifração). A chave é compartilhada”. Como mostrado na Figura 18.

Figura 18 - Criptografia de chave simétrica



Fonte: Adaptado de Forouzan (2008, p. 729)

- Chaves assimétricas: Duas chaves criptográficas distintas, uma chave pública é distribuída publicamente, e uma chave privada, apenas o proprietário possui para decifrar a mensagem. Como mostrado na Figura 19.

Segundo Cert.br (2012), existe duas chaves diferentes na criptografia assimétrica, cada um tem suas próprias funções, quando uma é usada para cifrar apenas a outra correspondente consegue decifrar. Alguns exemplos de algoritmos

assimétrica usados: RSA (sigla do algoritmo é referente as primeiras letras dos criadores Rivest, Shamir e Adleman), Diffie-Hellman (o nome originou dos nomes dos desenvolvedores do algoritmo o Whitfield Diffie e Martin Hellman), ECC - *Elliptic curve cryptography* (Criptografía de curvas elípticas) e DAS - *Digital Signature Algorithm* (Padrão de assinatura digital).

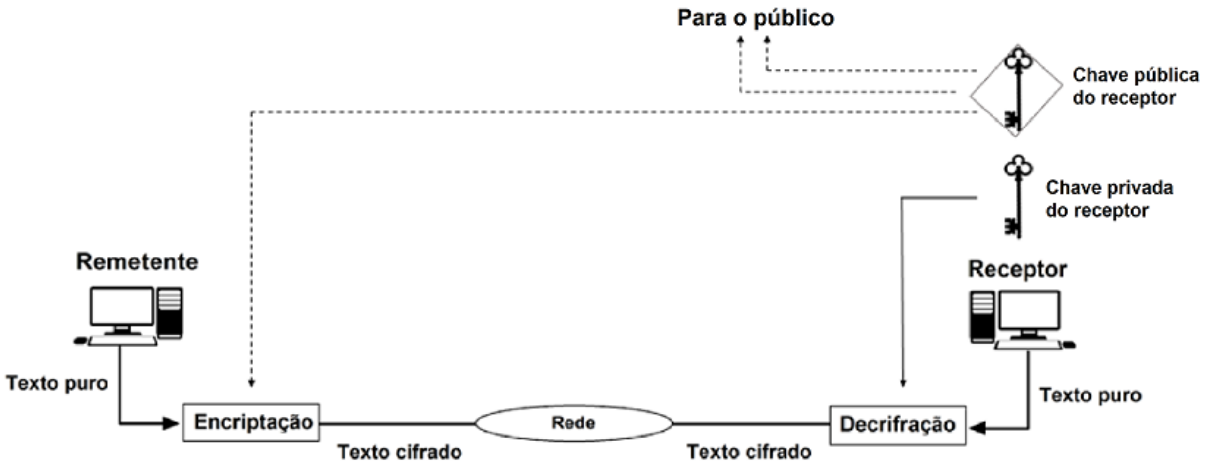


Figura 19 - Criptografia de chave pública

Fonte: Adaptado de Forouzan (2008, p. 733)

Exemplo do uso da chave assimétrica: Pessoa 1 deseja mandar uma mensagem de forma segura para pessoa 2. A pessoa 1 usa a chave pública da pessoa 2 para criptografar a mensagem e somente com a chave privada da pessoa 2 (apenas pessoa 2 possui essa chave) a mensagem será descriptografada.

> “Na encriptação/decifração de chaves pública, a chave pública usada para encriptação é diferente da chave privada usada para decifração. A chave pública fica disponível ao público; a chave privada fica disponível somente a uma pessoa” (FOROUZAN, 2008, p. 732).

***Firewalls* -** Também chamado de “parede de fogo”, atua como uma barreira de defesa entre a rede interna e a rede externa, como mostrado na Figura 20. Firewall funciona através de um conjunto de regras (configuração personalizada) realizando a filtragem do tráfego, fazendo análise de conteúdo, bloqueando as operações indesejáveis, e apenas permitindo a entrada e a execução dos pacotes aprovados.

De acordo com Kurose e Ross (2013, p. 541), “Um *firewall* é uma combinação de *hardware* e *software* que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros”.

Figura 20 - *Firewall*

Fonte: Chipset [s.d][1]

[1] Disponível em: <http://www.chipsetsuporte.com.br/?page_id=143>. Acesso em: 13 mar. 2017.

Ferramenta *antimalwares* - *Software* que detecta a presença de agentes maliciosos e realiza a remoção antes que esses provoquem danos ao sistema. A Figura 21, apresenta alguns dos programas *antimalwares.*

Conforme Cert.br (2012), “Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas deste tipo”.

Figura 21 - Algumas ferramentas *antimalwares*

Fonte: Coisas Digitais (2014)[1]

[1] Disponível em: < http://coisasdigitais.blogs.sapo.pt//como-escolher-o-melhor-antivirus/>. Acesso em: 15 mar. 2017

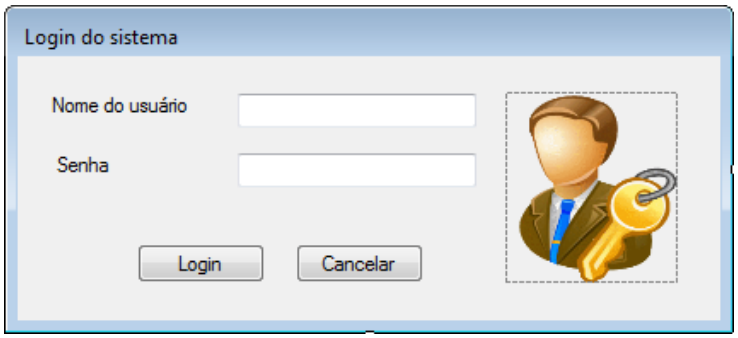
Ferramentas de detecção de ataques – Método usado para identificar ataques, alertando o acontecimento ao administrador do sistema que posteriormente irá propor soluções adequadas para esses fatos.

Conforme Snort [s.d], “o IDS - *Intrusion Detection System* (Sistema de detecção de intrusos) é um sistema de configurações e regras que tem como objetivo gerar alertas quando detectar pacotes que possam fazer parte de um possível ataque”.

Autenticação – Antes de ocorrer alguma comunicação entre ambas as partes, esse mecanismo faz a confirmação de identidade, assegurando que é o usuário legítimo que está realizando a troca de mensagens ou o acesso das informações. Exemplo deste mecanismo é apresentado na Figura 22 *(login* e senha).

Segundo Kurose e Ross (2013, p. 252), “O protocolo de autenticação estabelece primeiramente as identidades das partes de maneira satisfatória para ambas; somente após a autenticação, as partes se lançam à tarefa que têm em mãos”.

Figura 22 - Autenticação do usuário através do *login* e senha



Fonte: Pimenta (2012)[1]

[1] Disponível em: <http://www.lucianopimenta.com/post.aspx?id=195>. Acesso em: 15 mar. 2017

A Figura 23, mostra um tipo de sistema de autenticação, a biometria, onde apenas o proprietário do aparelho ou o usuário que tenha permissão possa ter o acesso.

Figura 23 - Sistema de biometria

Fonte: MeioBit (2015)[1]

[1] Disponível em: <http://meiobit.com/322861/sonavation-tecnologia-sensores-biometricos-gorilla-glass/>. Acesso em: 15 mar. 2017

IPsec – É um protocolo de segurança, que trabalha com um conjunto de técnicas fornecendo tráfego seguro de pacotes de dados pela rede. IPsec é o elemento principal para abordagem desse projeto e será tratado com mais detalhes nos próximos capítulos.

Lembrando que nos itens anteriores foram citados como exemplo apenas alguns tipos de mecanismo de segurança, e atualmente nas redes implantadas, encontra-se outras de ferramentas de segurança que atendem à essas ocorrências maléficas, as quais serão apesentadas a seguir.

4.2 Principais riscos e ataques pela rede

As redes atuais são mais eficientes, devido a modificações e aprimoramentos sofridos durante longo tempo. Nesse mesmo percurso foram surgindo diferentes tipos de ataques e ameaças pela rede. A execução dessas atividades ilegais para quebrar o sistema de segurança da informação tem intenções variadas, podendo-se citar alguns exemplos como, o atacante apenas deseja mostrar do que é capaz de fazer (invadir o sistema e expor os dados roubados, fazer com que o sistema fique fora do ar, impedindo o acesso), por questões comerciais (invadir sistemas do concorrente para danificar a imagem da empresa ou roubar ideias de projetos), por motivos financeiros (lucrar por determinadas informações obtidas). Em todas as circunstâncias, se as informações importantes caírem em mãos erradas, pode-se trazer grandes prejuízos para o proprietário desses dados.

Segundo Nakamura e Geus (2007), quanto mais a tecnologia evolui, mais as vulnerabilidades aumentam, e apenas com uma falha de informação presente, pode trazer consequências graves para o negócio da organização, como a perda financeira.

Na rede ocorre incontáveis transferências de dados todos os dias, e nessas transições informações valiosas podem trazer lucro e benefício para as pessoas mal-intencionadas. Isso leva algumas pessoas a planejarem armadilhas e técnicas para obterem essas preciosas informações.

De acordo com Cisco [s.d]:

> “A industrialização da invasão está criando uma geração de lucros da economia criminosa mais rápida, eficaz e eficiente a partir dos ataques a nossa infraestrutura de TI. A troca organizada de explorações é próspera e lucrativa, e o mercado aberto ajuda a impulsionar a mudança da exploração para roubo, transtorno e destruição”.

Conforme Stallings (2008), os ataques são divididos em duas formas. São eles:

- Ataques passivos: é quando o atacante consegue capturar e monitorar as informações trafegados pela rede, geralmente são difíceis de serem detectados, pois os dados não sofrem alterações, trafegam como tivessem normal, nesse caso o emissor e o receptor não percebem que há vazamento das informações.
- Ataques ativos: os conteúdos da informação são modificados pelo atacante, caso esse tipo de ataque aconteça, poderá ocorrer danos significativos para a instituição.

A seguir será apresentado os principais riscos e ataques que acontecem na rede:

Mapeamento (*Scanner* de portas) – É uma técnica que realiza a coleta das informações da rede, e através desses dados que os ataques são elaborados, pois quanto mais o atacante adquirir conhecimento do seu alvo, mais chance de ter sucesso nas invasões, e diminuindo a probabilidade de ser descoberto.

> “[...] Antes de atacar uma rede, os invasores gostariam de saber os endereços IP das máquinas pertencentes à rede, quais sistemas operacionais elas utilizam e os serviços que esses sistemas oferecem. Com essas informações, os ataques podem ter um foco mais concentrado e a probabilidade de causar alarme é menor” (KUROSE; ROSS, 2013, p. 546).

Segundo Cert.br (2012, p. 18), “[...] é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados”.

Falsificação de IP (*Spoofing*) – Um método em que o atacante passa a ser o componente intermediário entre o remetente e o destinatário, trabalhando de forma idêntica ao elemento legítimo, mas modificando o endereço IP das máquinas. Assim

quando uma mensagem é enviada pode ser interceptada pelo atacante e mandando como resposta mensagens alteradas para o destinatário, ou fazer o redirecionamento para ambiente falso criado pelo atacante. Exemplo de consequência: digitação de senha na página falsa.

De acordo com G1 (2010), "[...] um ataque em que o hacker fica entre a conexão do usuário com o site legítimo que ele quer acessar. Com isso, ele consegue alterar ou ler as informações que o usuário envia".

Negação de Serviço – É chamado também de ataque *DoS* (*Denial of Service),* essa técnica consiste em mandar várias solicitações ao mesmo tempo através de endereços falsos, causando sobrecarga e paralização no funcionamento do sistema.

> "[...] um ataque *DoS* torna impossível a utilização de uma rede, de um hospedeiro ou de qualquer outro componente da infraestrutura da rede pelos usuários legítimos. Em geral, um ataque *DoS* funciona pela criação de uma quantidade tão grande de trabalho na infraestrutura sob ataque que o trabalho legítimo não pode ser realizado" (KUROSE; ROSS, 2013, p. 548).

O congestionamento na rede é causado através do envio de grande quantidade de pacotes fragmentados incompletos, fazendo com que as requisições fiquem em aberto, aguardando para serem completadas. Dessa maneira, cada vez que entram novas solicitações elas vão se acumulando até chegar um ponto em que o sistema não consegue aguentar mais, consequentemente provocando o travamento.

Outra maneira de implementar esse ataque é usando máquinas infectadas pelos *malwares* (será explicado no próximo tópico), o atacante tem o controle dessas máquinas sem a conhecimento do proprietário, por meio de um programa mestre, onde manda instruções e faz a ordenação de ataque, esse meio é chamado de *DDoS - Distributed Denial of Service* (Ataque de negação de serviço distribuído).

Segundo Cert.br (2012), o principal objetivo desse ataque é deixar o sistema alvo indisponível para os usuários legítimos que necessitam, sem a intenção de invadir e coletar informações, apenas esgotar os recursos oferecidos pelos sistemas.

Códigos maliciosos (vírus e *malwares*) – São programas que infiltram nos sistemas e executam ações que podem comprometer a segurança da informação, o objetivo que leva a criação e a disseminação desses códigos pelas pessoas mal-

intencionados tem como intenção, capturar informações, por propósitos financeiros, mostrar suas habilidades, acessar máquina remotamente sem a percepção do dono, entre outros.

Ainda de acordo com Cert.br (2012) “[...] são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador [...]”. Os números de códigos maliciosos não param de crescer, novos tipos surgem a todo momento, com habilidades diferentes, afetando o desempenho da rede e trazendo danos aos usuários.

Força bruta – Ataque feito através de sucessivas tentativas para descobrir o *login* e a senha do usuário.

Conforme Cert.br (2012), “Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário”. Quando o atacante conseguir o acesso da conta, poderá realizar atividades como, instalação de código malicioso em outros locais através dessa conta, remover ou alterar as informações contidos. Os dados poderão ser usados para a execução de ações ilegais, troca de senha, impedindo que o usuário legítimo da conta tenha acesso, arruinando assim a reputação desse usuário, entre outros.

Analisador de pacotes (*Sniffer*) – Programa que consegue ver todos os pacotes de dados que trafegam pela rede, pode ser usado de modo legítimo e também de modo malicioso.

> “Um analisador de pacote (*packet sniffer*) é um programa que funciona em um dispositivo acoplado à rede e que recebe passivamente todos os quadros de camada de enlace que passam por sua interface de rede. Em ambiente *broadcast* como uma LAN Ethernet, isso significa que o analisador de pacotes recebe todos os quadros que estão sendo transmitidos de ou para todos os hospedeiros da LAN” (KUROSE; ROSS, 2013, p.547).

De acordo com Cert.br (2012), a diferença entre os dois modos de uso (modo legítimo e malicioso) é, a forma legítima, o administrador usa para gerenciamento da rede (detecção de problemas, monitoramento do desempenho da rede), e a forma maliciosa, é usado pelo atacante para capturar informações sensíveis (número de cartão de crédito, senhas, informações sigilosas).

Na época atual a informação é um negócio que gera lucro, e em todos os tipos de ambientes onde há benefício, existe risco. Foi mencionado anteriormente apenas alguns tipos de ataque, com o intuito de mostrar os danos que podem causar. A importância da Segurança da Informação, em relação a questão da proteção dos dados, que já foi exposto no subcapítulo anterior. A seguir será apresentado o protocolo IPsec, na qual, é o foco principal desse trabalho.

4.3 Protocolo IPsec

Segundo IPv6.br (2015, p. 217), " Destinado principalmente a interligar redes de pesquisa acadêmicas, o projeto original do IPv4 não apresentava nenhuma grande preocupação com questões relacionadas à segurança das informações transmitidas". A princípio o IPv4 foi criado apenas com o intuito de conectar as instituições, mas com o decorrer do tempo a rede teve um constante crescimento, e várias transações importantes passaram a ser feitos através da Internet, e com o surgimento de ameaças, a segurança tornou-se um elemento indispensável, portanto, no protocolo da nova versão (IPv6) o suporte IPsec já vem embutido, ou seja, é obrigatório, mas para sua utilização, deverá ser habilitado, já no IPv4, o IPsec não é nativo.

De acordo com Teleco [s.d]:

> "Em oposição à crença de muitos administradores de rede, o IPSec é relativamente antigo, sendo desenvolvido para ser utilizado com a arquitetura IPv4. Sua arquitetura não proprietária [19] possibilitou o avanço desta solução e sua utilização em larga escala. Com isso, o significativo ganho trazido por esta ferramenta foi tamanho, que sua utilização em ambientes IPv6 se tornou obrigatória. "

Conforme Brito (2013), o IPsec – *IP Security Protocolo* (Protocolo de segurança), é um protocolo criado para proteger os pacotes trafegados pela rede na camada IP, oferecendo serviço de segurança principalmente na camada de rede, mas também protege as camadas superiores, trazendo segurança fim-a-fim. Esses métodos de segurança operam nos dispositivos: *host, firewall*, roteador, e entre outras possibilidades.

Para Forouzan (2008), a principal função do IPsec é oferecer mecanismos de segurança como criptografia, autenticação, compactação, onde são aplicadas nos pacotes de dados, antes de serem enviados pela rede, dessa forma, protegendo os conteúdos trafegados, o IPsec trabalha de forma transparente ao usuário, garantindo a autenticidade, integridade e confidencialidade.

Segundo Stallings (2008, p. 349), “O IPsec oferece a capacidade de proteger a comunicação por uma LAN, por WAN privadas e públicas e pela Internet”. Esse elemento além de trazer vários benefícios, também traz consigo a redução de custo devido a possibilidade de criação de redes privadas através da Internet.

Conforme IBM [s.d], os serviços de segurança que o IPsec oferece, são as seguintes:

- Autenticação da origem de dados - Verifica se cada datagrama (pacote de dado) teve origem no suposto remetente.
- Integridade dos dados - Verifica se o conteúdo de um datagrama foi alterado durante a circulação, quer seja deliberadamente, quer seja devido a erros aleatórios.
- Confidencialidade de dados - Oculta o conteúdo de uma mensagem, normalmente através de codificação.
- Proteção de repetição - Assegura que o elemento estranho não consegue interceptar um datagrama e repeti-lo mais tarde.
- Gestão automática de chaves criptográficas e associações de segurança - Assegura que a sua política de VPN pode ser implementada em toda a rede com pouca ou nenhuma configuração manual.

4.3.1 Documentos IPsec

O RFCs - *Requests for Comments*, são documentos cujo padrão é mantido pela IETF, e refere-se a vários aspectos na área de redes de computadores.

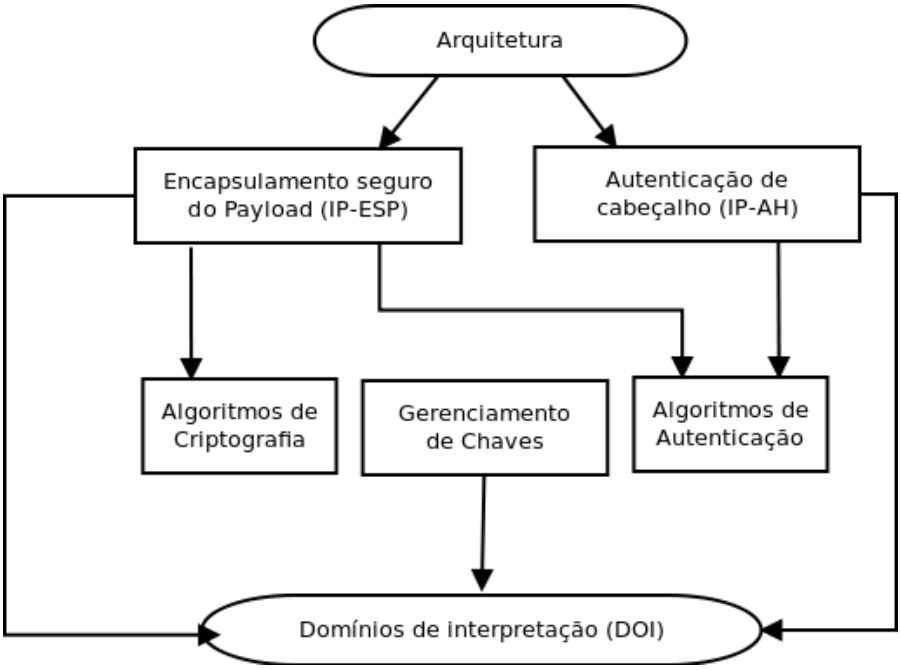
Segundo Reis (2015), “Os RFCs (*Request for Comments*) são publicações que documentam os padrões, serviços e protocolos oficiais da Internet, sendo mantidos pelo IETF-*Internet Engineering Task Force*, comunidade internacional aberta que desenvolve as especificações que se tornam padrões da Internet. ”

O IPsec é retratado nos seguintes documentos, conforme Stallings (2008, p. 351):

- RFC 2401: Uma visão geral de uma arquitetura de segurança.
- RFC 2402: Descrição de uma extensão de autenticação de pacote para IPv4 e IPv6.
- RFC 2406: Descrição de uma extensão de criptografia de pacote para IPv4 e IPv6.
- RFC 2408: Especificação das capacidades de gerenciamento de chaves.

Além desses citados acima, também foram publicados outros documentos adicionais, dentro desses quatro RFCs o que mais se destaca é o RFC 2401, ele retrata a arquitetura geral do IPsec, como mostra na Figura 24.

Figura 24 - Arquitetura IPsec



Fonte: DevelSitemas [s.d][1]

[1] Disponível em: <http://www.develsistemas.com.br/ipsec-protocolo-de-seguranca-para-redes-ip/>. Acesso em: 17 abr. 2017

A seguir será mostrado cada item da arquitetura, de acordo com Stallings (2008):

- Arquitetura: conceito geral do IPsec.
- Encapsulamento de segurança do *payload* (ESP): questões dos pacotes relacionados ao uso de ESP, para criptografar e opcionalmente as questões de autenticação.
- Autenticação do cabeçalho (AH): questões relacionados ao uso de AH nos pacotes para autenticação.
- Algoritmo de criptografia: documentos que descreve como diversos algoritmo de criptografia são usados no ESP.
- Algoritmo de autenticação: documentos que descreve como diversos algoritmo de criptografia são usados na AH e a autenticação no ESP.
- Gerenciamento de chaves: documentos que descreve formas de gerenciamento de chaves.
- Domínio de interpretação (DOI): faz com que os documentos se relacionam entre si, contém parâmetro como tempo de vida da chave e identificadores de algoritmos aprovados de criptografia e autenticação.

4.3.2 Subprotocolos AH e ESP

O IPsec é composto por dois principais subprotocolos, o protocolo *AH - Authentication Header* e *ESP - Encapsulated Security Payload*, esses métodos asseguram com que o datagrama seja enviado de forma segura até o destinatário com os dados intactos.

Conforme Stallings (2008), a função principal do protocolo *AH - Authentication Header* (Autenticação de cabeçalho) é, ele realizar a autenticação da fonte, a integridade dos pacotes trafegados, garantindo que os dados foram emitidos pelo emissor legitimo e não falsificado, também proteger as informações contra acesso não autorizado, para isso ambas as partes que se comunicam compartilham uma chave secreta. O protocolo AH não garante a confidencialidade, já no protocolo *ESP - Encapsulated Security Payload* (Segurança de encapsulamento de carga útil), que provê serviços de autenticação e integridade, é adicionado mais um elemento de segurança que garante a confidencialidade das informações e por esse motivo, o

ESP é mais utilizado. No ESP é apresentado variedades de algoritmos de criptografia que são usados, dentre eles: 3DES, RC5, IDEA, CAST e *Blowfish.*

Os algoritmos são mostrados com mais detalhes conforme, Fernando (2007):

- 3DES – Pode ser utilizado na forma de 2 ou 3 chaves, onde cada um possui 56 bits mais 8 bits que são reservados para a verificação de paridade, os dados são criptografados da seguinte forma, encriptados com a 1º chave, decriptados com a 2º chave e encriprados novamente com a 3º chave, no processo de criptografia os blocos de 64 bits percorrem por 48 operações.
- RC5 – *Rivest Cipher 5* (Cifrador de Rivest 5): Usa chave que pode chegar até 2048 bit, a criptografia é operada em blocos de 32 bits, 64 bits ou 128 bits.
- IDEA – *International Data Encryption Algorithm* (Algoritmo Internacional de Criptografia de Dados): Usa chave de 128 bits, para cifrar blocos de 64 bits, o processo é semelhante do DES.
- CAST – *Carlisle Adams and Stafford Tavares* (nomes dos criadores do algoritmo) – Usa chave com tamanho variável entre 40 a 128 bits, a cifragem é feita em blocos de 64 bits, esse algoritmo possui uma versão mais forte o CAT 256, que opera em blocos de 128 bits, usando chave variável entre 128 bits, 192 bits, 224 bits e 256 bits.
- *Blowfish* – chave variável entre 32 a 448 bits, opera em blocos de 64 bits.

Esses dois protocolos empenham o controle do fluxo dos pacotes, a distribuição de chaves de criptografia e o controle de acesso.

4.3.3 Funcionamento IPsec

O IPsec permite que a entidade (as partes em que manterão a comunicação) escolha os mecanismos de segurança que serão usados. Segundo Stallings (2008, p. 352), “O IPSec oferece serviços de segurança na camada de IP permitindo que um sistema selecione protocolos de segurança exigidos, determine o(s) algoritmo(s) a ser(em) usado(s) para o(s) serviço(s) e coloque no lugar quaisquer chaves criptográficas[...] ”

4.3.3.1 SA – *Security Association* (Associação de Segurança)

Kurose e Ross (2013, p. 558), “ [...] antes de enviar datagramas seguros de um a outro, os hospedeiros de origem e de destino fazem uma apresentação mútua e criam uma ligação lógica de camada de rede. Esse canal lógico é denominado acordo de segurança (*security association – SA*) [...]”.

Conforme Forouzan (2008), o IPsec transforma a conexão não orientada em conexão orientada, criando um canal lógico entre a origem e o destino da comunicação, chamado de conexão SA – *Security Association* (Associação de Segurança). Ele determina o tipo de algoritmo que será usado, a chave de criptografia e o seu tempo de vida, o tipo de ligação em SA é no modo simplex (unidirecional), isto é, conexão entre a origem e o destino. Caso necessite de troca segura bidirecional, então serão feitas duas associações, ou seja, terá duas conexões SA, no SA é determinada o tipo de algoritmo que será usado, chave de criptografia e o seu tempo de vida. A conexão SA é determinada em três elementos:

- Tipo de protocolo de segurança: AH e ESP;
- IP de destino da conexão;
- SPI – *Security Parameter Index* (Índice de Parâmetro de Segurança) de 32 bits, transportado no cabeçalho AH ou ESP, para identificar a conexão.

4.3.3.2 Modo transporte e modo túnel

O IPsec foi projetado para operar em dois modos, em modo transporte, protege a conexão entre ambas partes (emissor e receptor), e modo túnel, é através de configuração de roteadores, onde protege todo o canal do tráfego de dados.

A seguir será mostrado com mais detalhes cada tipo de operação, de acordo com Brito (2013):

Modo Transporte – o cabeçalho IPsec é localizado depois do cabeçalho IP, protege apenas os protocolos das camadas superiores, nesse modo apenas os dados são criptografados, o cabeçalho é inalterado. Esse tipo é mais usado na comunicação ponta a ponta.

- ESP no modo transporte: apenas os dados são criptografados e opcionalmente os autentica.
- AH no modo transporte: autentica e partes de cabeçalho de IP, que são selecionadas.

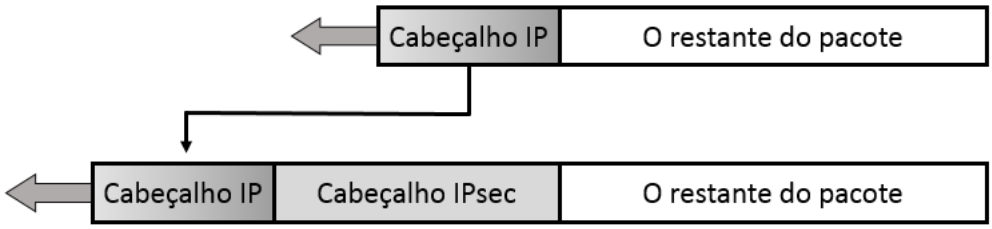
Modo Túnel – o cabeçalho IPsec é localizado na frente do cabeçalho IP, protege todo o pacote IP, nesse modo o pacote inteiro é criptografado, incluído dados e cabeçalho, entretanto, para rotear pela rede é necessário reencapsular o pacote e atribuindo um novo cabeçalho, o cabeçalho túnel, que é localizado na frente do cabeçalho IPsec, nesse tipo de operação é estabelecido o VPN - *Virtual private network* (Rede privada virtual) para trafegar os dados.

- ESP no modo túnel: todo pacote interno incluindo cabeçalho IP interno é criptografado e autenticado (opcional).
- AH no modo túnel: Todo pacote interno e uma parte do cabeçalho externo é autenticado.

No IPv6 os protocolos AH e ESP são apresentados no cabeçalho de extensão.

A Figura 25 mostra a localização do cabeçalho IPsec do modo transporte.

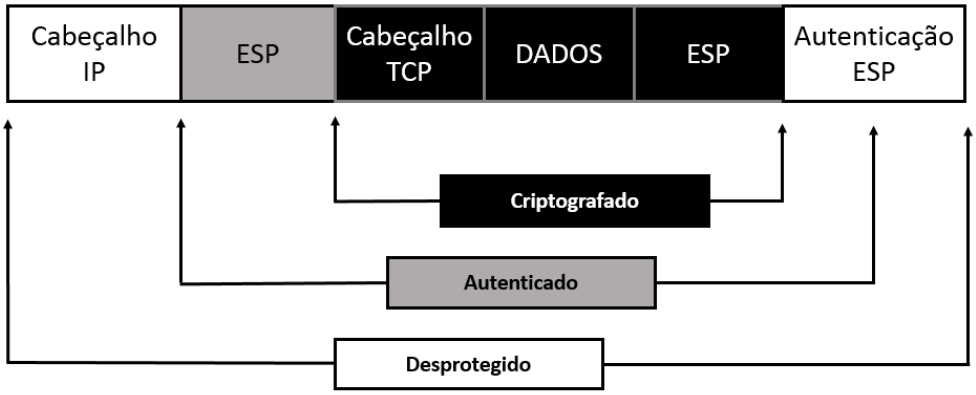
Figura 25 - Modo transporte



Fonte: Adaptado de Forouzan (2008, p. 755)

O modo transporte é mostrado com mais de detalhe na Figura 26.

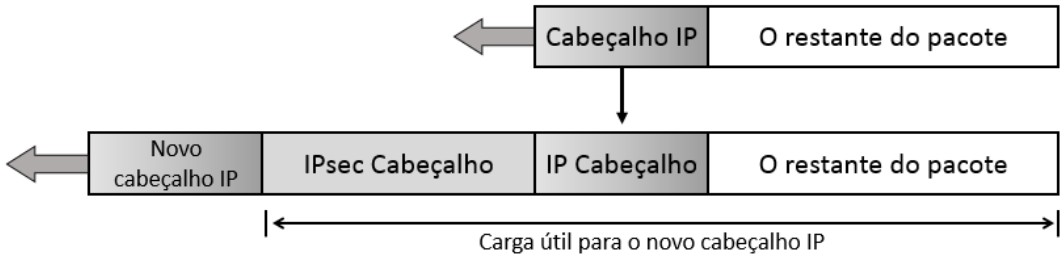
Figura 26 - Elementos do modo transporte



Fonte: Fonte: Adaptado de Brito (2013, p. 161)

A Figura 27, apresenta a localização do Cabeçalho IPsec no modo túnel, onde um novo cabeçalho IP é adicionado na frente do cabeçalho IPsec, e esse localizado na frente do cabeçalho IP original do pacote.

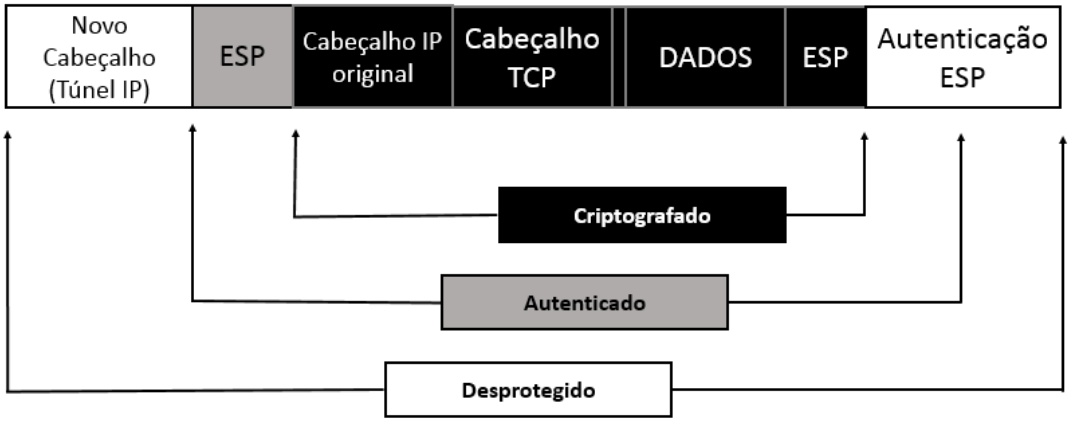
Figura 27 - Modo túnel



Fonte: Adaptado de Forouzan (2008, p. 755)

A Figura 28 identifica a posição do cabeçalho modo túnel e como é formada.

Figura 28 - Elementos do modo túnel



Font

e: Adaptado de Brito (2013, p. 161)

Conforme Stallings (2008), os pacotes que trafegam no modo transporte atua da seguinte forma:

1. Na origem, antes dos pacotes serem despachados pela rede, os dados constituídos no ESP mais o segmento inteiro da camada de transporte são criptografados, assim o texto (mensagem original) é transformado em texto cifrado para a transmissão, e a autenticação é adicionada caso seja usado.
2. O pacote é roteado para o destino, os roteadores intermediários verificam e processam o cabeçalho IP e cabeçalhos de extensão em texto legível, não necessitando verificar os textos cifrados.
3. O destino faz a verificação e processa o cabeçalho IP, e cabeçalhos de extensão se os tiver. Em seguida com base no SPI do cabeçalho ESP, o destinatário descriptografa o restante do pacote para texto legível.

Os pacotes que trafegam no modo túnel na comunicação de um *host* interno com um *host* externo atua da seguinte forma:

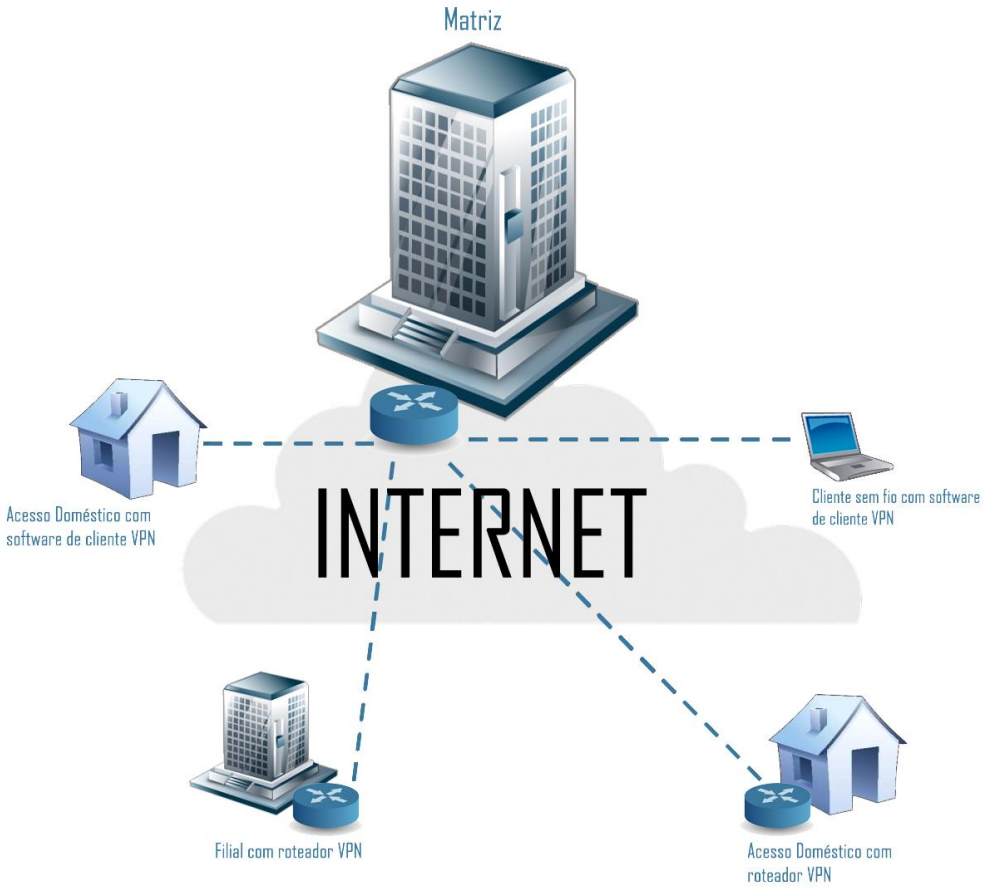
1. A origem prepara um pacote interno com o endereço de destino (endereço de destino de um *host* interno da outra ponta de comunicação), o pacote é fixado com um cabeçalho ESP, e os dados contidos são criptografados. Se possuir dados de autenticação esses serão adicionados. Em seguida o bloco é encapsulado, com um novo cabeçalho de destino (cabeçalho de *firewall* de destino), dessa forma o pacote IP torna-se externo.
2. O pacote é roteado para o *firewall* destino, os roteadores intermediários verificam e processam o cabeçalho IP e cabeçalhos de extensão externos. Neste caso não será necessário examinar o conteúdo cifrado.
3. O *firewall* verifica e processa o cabeçalho IP e cabeçalho de extensão externo em seguida com base no SPI no cabeçalho ESP, o destino descriptografa o pacote IP interno em texto claro, esse pacote então é trafegado na rede interna.
4. O pacote é roteado na rede interna até chegar ao destinatário.

4.3.3.3 VPN

VPN – *Virtual Private Networks* (Rede privada virtual), realiza a comunicação entre as entidades através de tunelamento combinado com certas tecnologias que garantem que a informação seja enviada de forma sigilosa e segura, através de um canal público a Internet. VPN é bastante utilizado pelas empresas, para se conectarem com as filiais, clientes, fornecedores, funcionários que trabalham remotamente, entre outras, ele apresenta um custo mais acessível em relação a *links* dedicados. A Figura 29, elucida a utilização da VPN pelas entidades.

> “A Rede Privada Virtual possui a grande vantagem de ser bem mais barata que os links dedicados. Além disso, a Internet está presente em todo o mundo com pontos de acesso espalhados por todos os lugares. As redes VPN são muito utilizadas pelas grandes empresas, especialmente nas companhias em que funcionários trabalham remotamente, seja nas ruas ou no sistema home office, para se conectar à estrutura interna mesmo estando longe. Usuários comuns também aproveitam a tecnologia das redes VPN para construírem redes privadas virtuais” (CIPOLI, 2016).

Figura 29 - Utilização da VPN

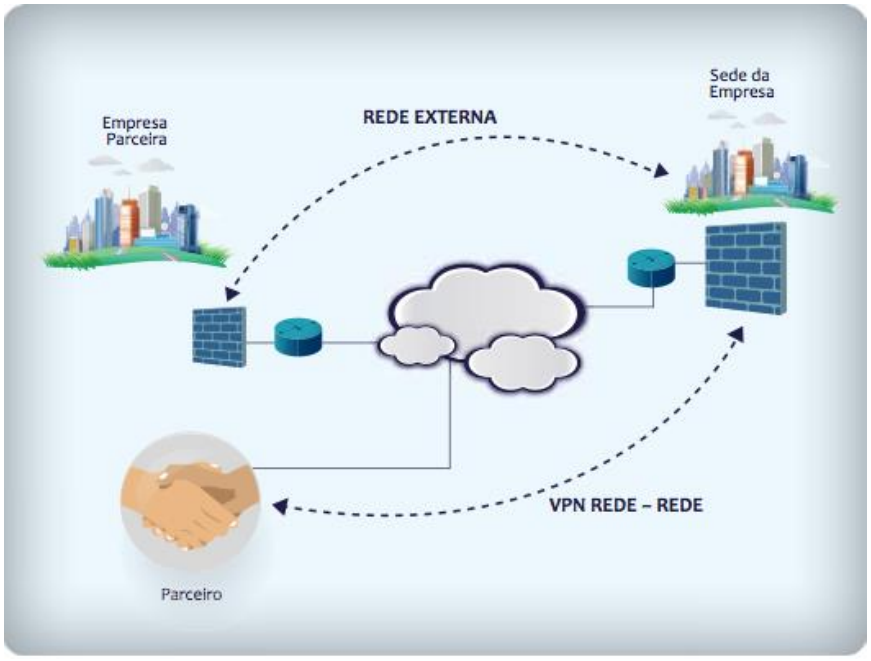


Fonte: UFRJ (2013)[1]

[1] Disponível em: <https://www.gta.ufrj.br/grad/13_1/vpn_ipsec/VPN_Capitulo2.html#2_1>. Acesso em: 20 abr. 2017.

Segundo Garrett (2015), “VPN como uma forma de criar pontes de ligação entre diferentes dispositivos via Internet, mantendo os dados de comunicação trocados entre eles codificados e mais seguros, já que sua interceptação se torna mais difícil. ” A VPN é conexão por tunelamento, onde os dados antes de serem enviados são criptografados e encapsulados dentro de outro pacote que contém um novo cabeçalho, na qual, mostra o caminho que leva até o destino, passando através da rede pública, quando chega no destino, ou seja, fim do túnel, esse pacote é examinado e em seguida é desencapsulado, e enviado para o destinatário final. A Figura 30, apresenta a conexão VPN, entre duas instituições.

Figura 30 - Conexão VPN



Fonte: MACEDO [s.d][1]

[1] Disponível em: <http://www.diegomacedo.com.br/tag/vpn?print=print-page>. Acesso em: 20 abr. 2017.

O ponto mais importante da VPN é a segurança, pois com a criptografia de dados garante-se a confidencialidade, visto que, através do tunelamento impede-se que os dados sejam acessados por usuários não autorizados, e também não sejam modificados.

> "[...] por meio da criptografia nas informações e nas comunicações entre hosts da rede privada é possível aumentar consideravelmente a confidencialidade dos dados que trafegam pela rede. Por meio do sistema de tunelamento, os dados podem ser enviados sem que outros usuários tenham acesso, e mesmo que os tenham, ainda os receberão criptografados" (CIPOLI, 2016).

O VPN vem embutido no IPsec, conforme Tanenbaum (2011), o IPsec foi arquitetado para estabelecer o tunelamento, fornecendo autenticação e criptografia, dessa forma, obtendo o controle de integridade, sigilo e imunidade à análise de tráfego.

Um dos pontos negativos que o VPN traz é, dependência da velocidade da conexão da Internet, na qual, poderá afetar no tempo de transmissão dos pacotes, e posteriormente influenciará na qualidade do serviço, portanto antes de implementar o VPN é preciso de planejamentos para ter controle sobre isso.

4.3.3.4 Gerenciamento de chaves

O gerenciamento de chaves no IPsec, define e distribui a chave secreta que serão utilizados durante a comunicação, existem dois tipos de suporte no gerenciamento como apresentado abaixo, segundo Stallings (2008):

- Manual: É feito a configuração manualmente em cada sistema com suas próprias chaves e as chaves de outros sistemas, que manterá a comunicação. Esse tipo é e aplicado nos ambientes pequenos.
- Automatizado: O sistema gera chaves sob demanda, em ambientes grandes, dessa forma, agiliza os processos.

O protocolo responsável pelo gerenciamento de chaves é o IKE - *Internet Key Exchange*, que é uma combinação de ISAKMP – *Internet Security Association and Key Management Protocol* (Protocolo de gerenciamento de chaves e de associação de segurança na Internet, e Oakley (Protocolo de determinação de chave).

Conforme a CISCO (2008), o ISAKMP, define o formato dos pacotes para negociar e estabelecer a associação de segurança, ele atua como parte do SA. As duas entidades se autenticam, na qual, é determinado como será feito a autenticação dos dados e geração das chaves, que serão compartilhadas entre si durante a comunicação, ou seja, o ISAKMP determina o método de como as chaves serão distribuídos entre duas entidades.

Oakley é o protocolo que faz a determinação de troca de chaves baseado no algoritmo Diffie-Hellman, esse algoritmo funciona da seguinte forma, segundo Forouzan (2008):

> "[...]o protocolo de *Diffie-Hellman* (DH), inventado por Diffie-Hellman, fornece uma chave de sessão para ser usada uma vez por dois participantes. Os dois participantes usam a chave de sessão para troca de dados, sem precisarem lembrar-se dela ou armazená-la para uso futuro. "

Para Stalling (2008), o algoritmo Diffie-Hellman, cria as chaves secretas apenas quando é necessário, essas chaves não precisam ser armazenadas por muito tempo, a troca de chave não exige infraestrutura pré-determinada, apenas precisa seguir os parâmetros globais que foram definidos, o Oakley também oferece segurança adicional.

5. ESTUDO DE CASO

Para realização desse trabalho, na implantação do ambiente de teste, foram utilizados os *softwares* GNS3, VirtualBox e Wireshark, onde, foram criados 4 cenários:

1. IPv4 sem aplicação do IPsec
2. IPv4 com aplicação do IPsec
3. IPv6 sem IPsec
4. IPV6 com IPsec

No GNS3 foram montados os cenários com 2 roteadores, 2 *switches* e 2 computadores, em que os dois computadores, estabelecem a comunicação. Essas duas máquinas são criadas no VirtualBox, sendo uma máquina cliente e uma máquina servidor, e em seguida com a ferramenta Wireshark, foram feitas as capturas de pacotes.

A seguir será feita uma breve apresentação das ferramentas utilizadas para o ambiente de teste.

5.1 GNS3

O Software GNS3 (*Graphical Network Simulator*), é uma ferramenta simulador de redes com interface gráfica, foi escolhido esse componente para a realização do teste, pois ele possui a integração com o VirtualBox. Dessa forma, podendo criar ambiente de teste muito próximo do real. Outro aspecto que levou a utilização do GNS3, que, é uma das ferramentas mais utilizadas para o treinamento de certificações, além de fácil manipulação, ele possibilita criação de vários tipos de topologias complexas. Nesse projeto foi utilizado o GNS3 da versão 1.5.3.

5.2 VirtualBox

VirtualBox é uma ferramenta de emulação que permite a criação de máquinas com plataformas Windows e Linux, essa máquina virtualizada, apresenta desempenho como se estivesse gerenciando uma máquina real.

No VirtualBox, foram criadas máquinas com sistema operacional Linux Ubuntu, foram instalados um servidor e uma máquina usuário, para testes. A escolha dessa plataforma, foi devido à facilidade de trabalhar em conjunto com a ferramenta GNS3. Para a realização desse projeto foi utilizado VirtualBox da versão 4.3.26.

As máquinas virtuais foram criadas com as seguintes características.

Linux Ubuntu Server versão 16.10:

- Ubuntu (64 bits)
- Memória (RAM) – 512 Mb
- Disco rígido – 8 Gb

Linux Ubuntu versão 16.10:

- Ubuntu (64 bits)
- Memória (RAM) – 512 Mb
- Disco rígido – 10 Gb

5.3 Wireshark

Wireshark é um programa analisador de pacotes. Ele verifica e monitora a entrada e saída de pacotes de uma máquina, exerce a captura de pacotes trafegados na rede em tempo real, é uma ferramenta que é bastante usada pelos administradores de rede, para detectar problemas ou conexões suspeitas, auxilia também no desenvolvimento de aplicativos, entre outros. Foi escolhido pois é uma ferramenta de fácil manuseio e bem recomendado pelos profissionais de informática. O programa Wireshark da versão 2.2.6 é utilizada para esse trabalho.

5.4 Cenários simulados

A seguir será apresentada a configuração prática dos cenários simulado.

5.4.1 IPv4 sem IPsec

A Figura 31 mostra o cenário montado do protocolo IPv4 sem IPsec.

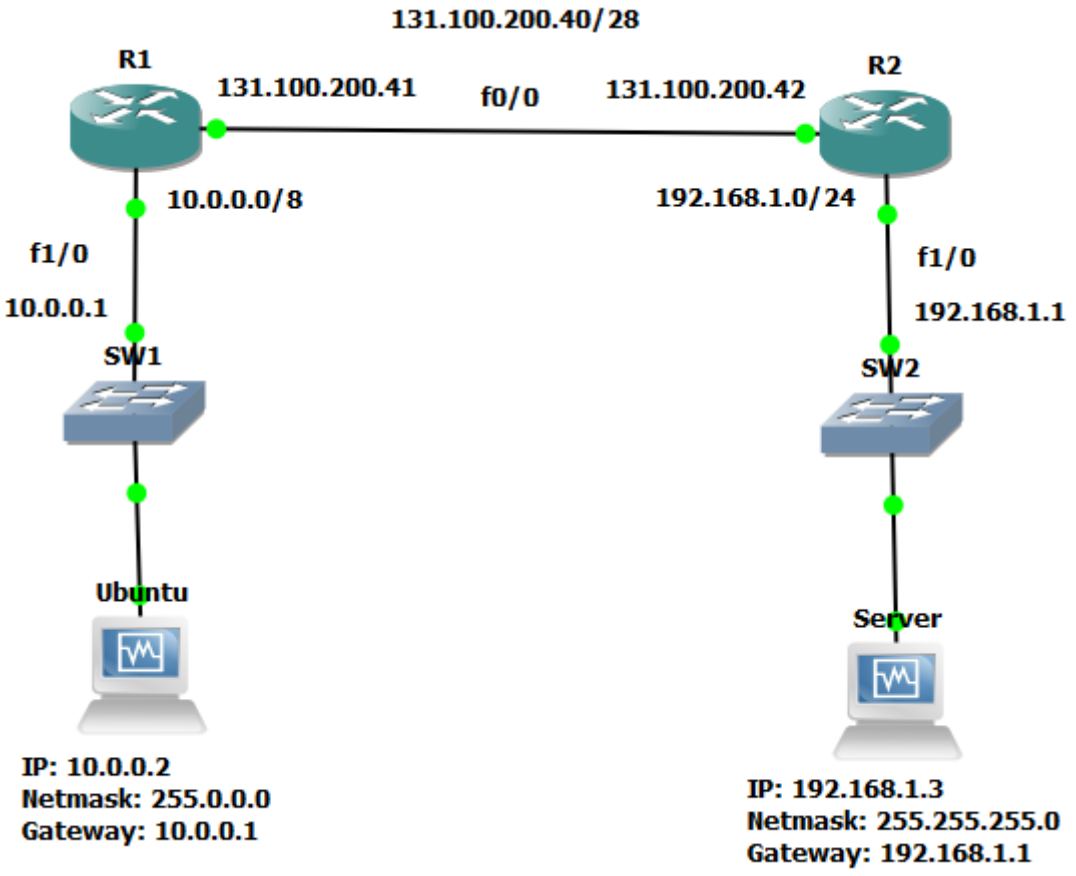


Figura 31 - Cenário IPv4 sem IPsec

Fonte: Elaborado pelo autor

Etapa 01 – A Figura 32 apresenta a configuração das interfaces 0/0 e 1/0 do roteador 1(R1).

Figura 32 - Configuração das interfaces

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 131.100.200.41 255.255.255.240
R1(config-if)#no shutdown
*May 24 07:50:09.799: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 24 07:50:10.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config-if)#exit
R1(config)#interface fastEthernet 1/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
*May 24 07:50:52.671: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*May 24 07:50:53.671: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up
R1(config-if)#exit
```

Fonte: Elaborado pelo autor

No roteador 2 (R2), são aplicados os mesmos comandos para a configuração das interfaces, apenas modificando o campo do endereço, nesse caso, no R2 ficará da seguinte forma:

F0/0 – IP: 131.100.200.42

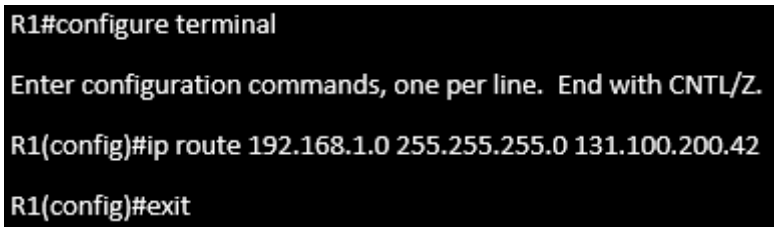
Máscara: 255.255.255.240

F1/0 – IP: 192.168.1.1

Máscara: 255.255.255.0

Etapa 02 – A Figura 33, mostra como foi feito a determinação das rotas no roteador 1 (R1), com o comando: *#ip route* “IP do destino” “máscara do destino” “IP do próximo salto”.

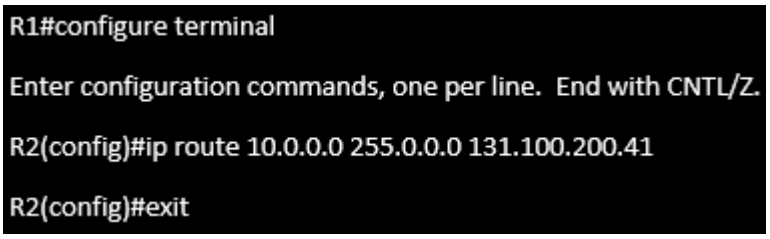
Figura 33 - Determinação da rota no R1



Fonte: Elaborado pelo autor

A Figura 34, apresenta a determinação da rota no roteador 2.

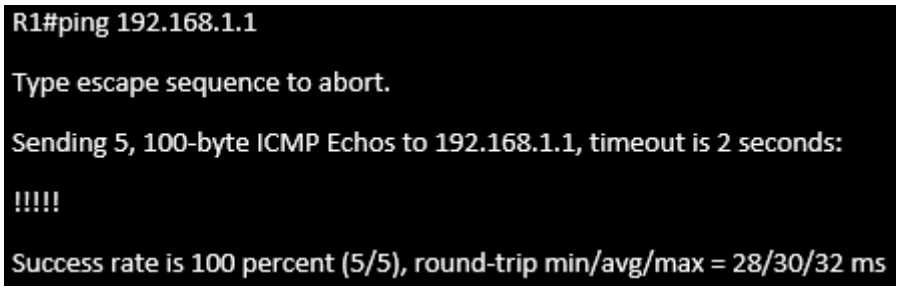
Figura 34 - Determinação da rota no R2



Fonte: Elaborado pelo autor

Etapa 03 – Com o comando: *#ping* “ip de destino”, mostrado na Figura 35, verifica a comunicação entre as interfaces.

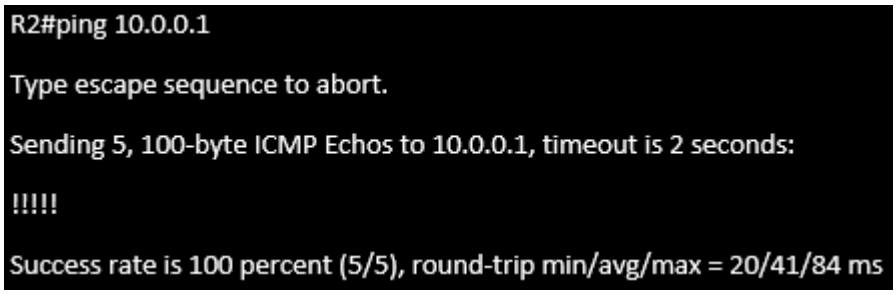
Figura 35 - Comunicação entre a interface do R1 com R2



Fonte: Elaborado pelo autor

A Figura 36, mostra a comunicação sucedida entre as interfaces do R2 com as interfaces do R1, caso, ocorrer algum erro na comunicação os sinal de “! ! ! ! !” serão “. . . . .”.

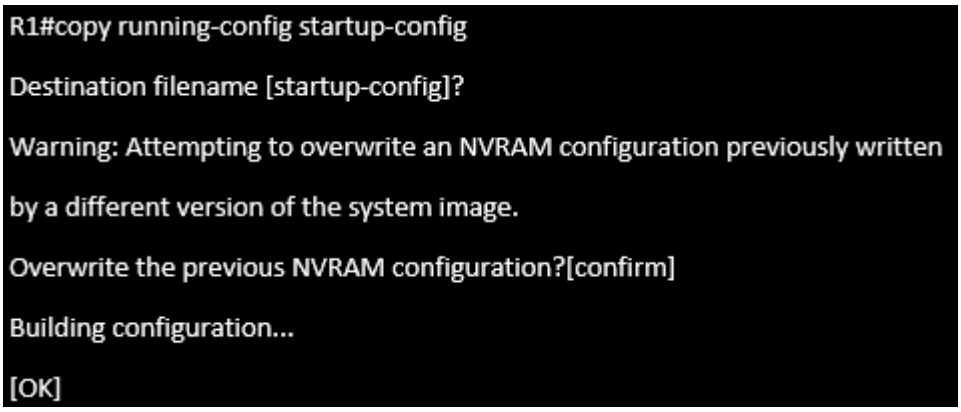
Figura 36 - Comunicação entre a interface do R2 com R1



Fonte: Elaborado pelo autor

Etapa 04 – O comando mostrado na Figura 37 foi aplicado o comando: *#copy running-config startup-config*, para salvar as configurações realizadas, com o objetivo de não precisar realizar toda a configuração novamente quando o cenário é fechado, e aberto posteriormente.

Figura 37 - Comando para salvar as configurações realizadas



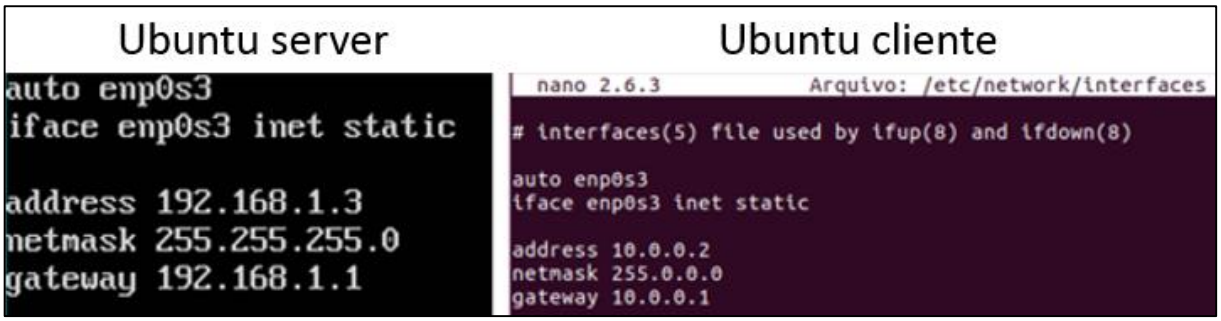
Fonte: Elaborado pelo autor

Etapa 05 – As duas máquinas criados no VirtualBox foram interligados no cenário e configurados da seguinte forma:

- Ubuntu cliente: IP 10.0.0.2, máscara 255.0.0.0 e *gateway* 10.0.0.1
- Ubuntu server: IP 192.168.1.3, máscara 255.255.255.0 e *gateway* 192.168.1.1

Foi definido o endereço IP estático através do arquivo # */etc/network/interfaces*, como retratado na Figura 38.

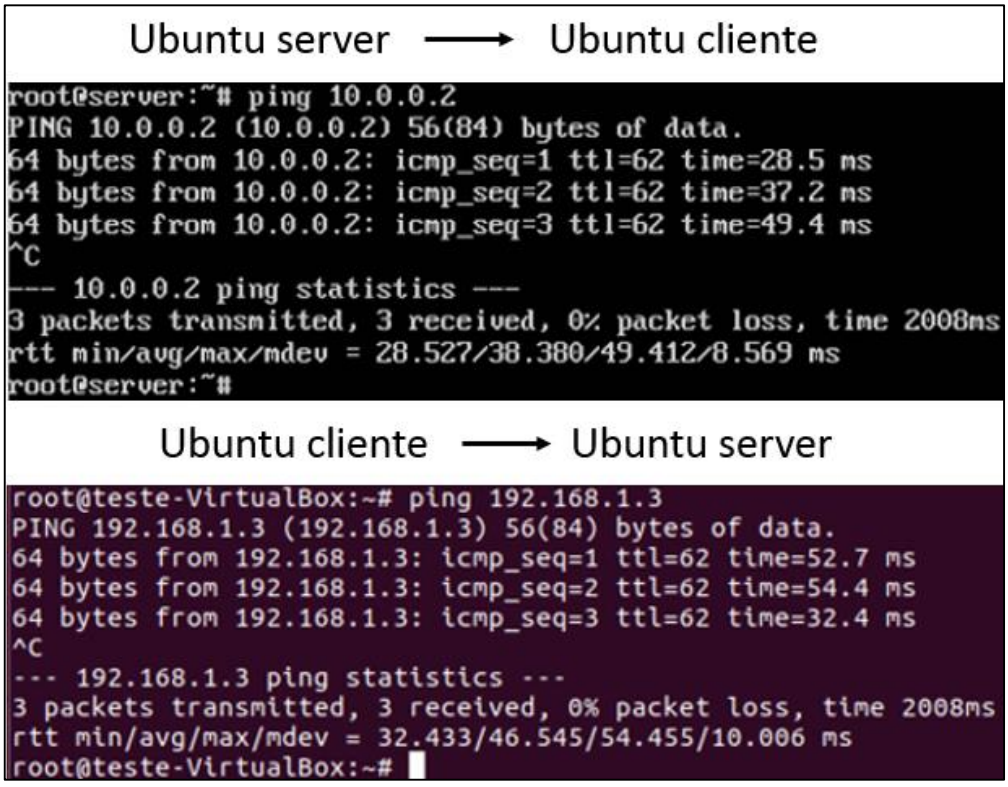
Figura 38 - Configuração IP estático nas máquinas Ubuntu server e Ubuntu cliente



Fonte: Elaborado pelo autor

Etapa 06 – Verificação da comunicação entre as máquinas, como mostrado na Figura 39.

Figura 39 - Comunicação entre as máquinas Ubuntu e Server

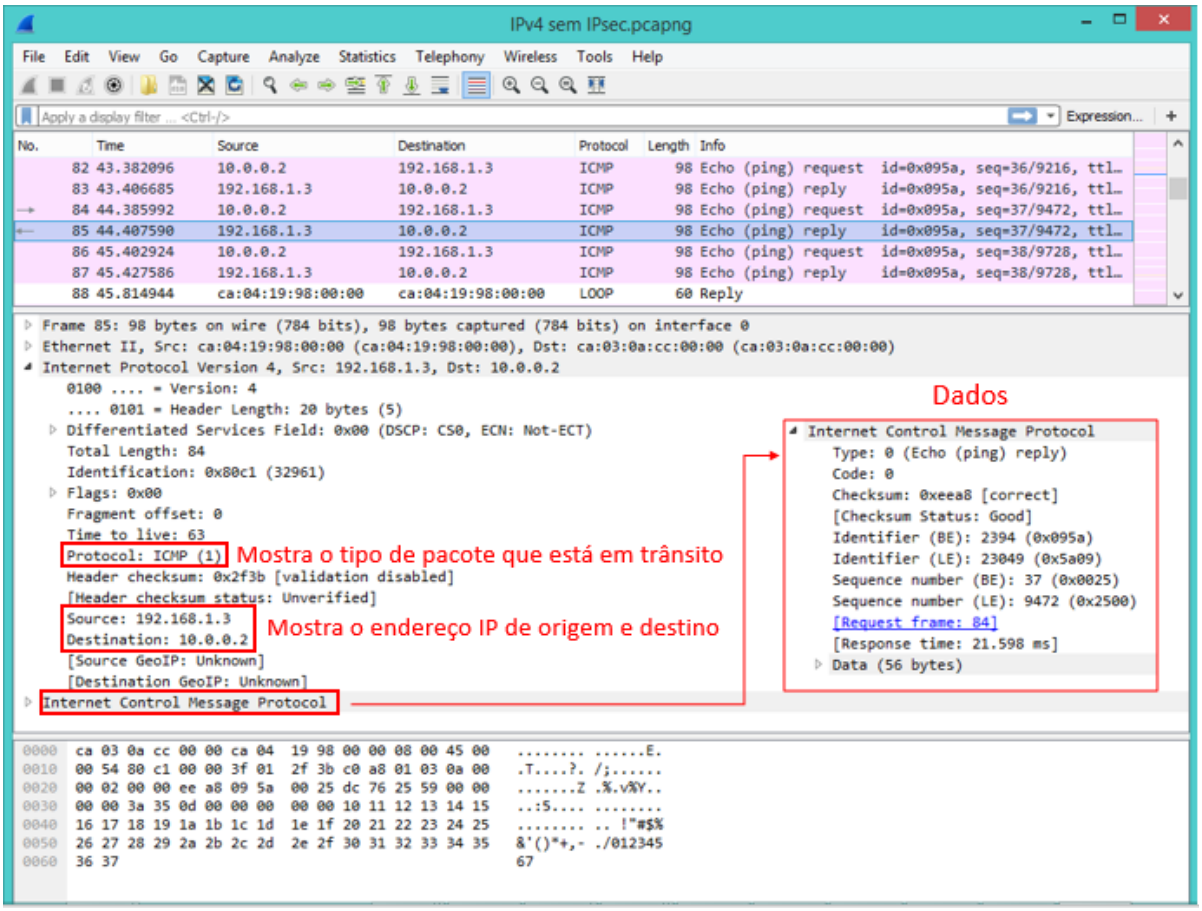


Fonte: Elaborado pelo autor

Etapa 07 – Através do programa Wireshark, foi realizado a captura de pacotes, como exposto na Figura 40.

No cenário IPv4 sem o uso do IPsec foi feito a captura de pacotes enviados da máquina Ubuntu cliente para Ubuntu server ou vice-versa.

Figura 40 - Captura de pacotes do cenário IPv4 sem IPsec através do Wireshark

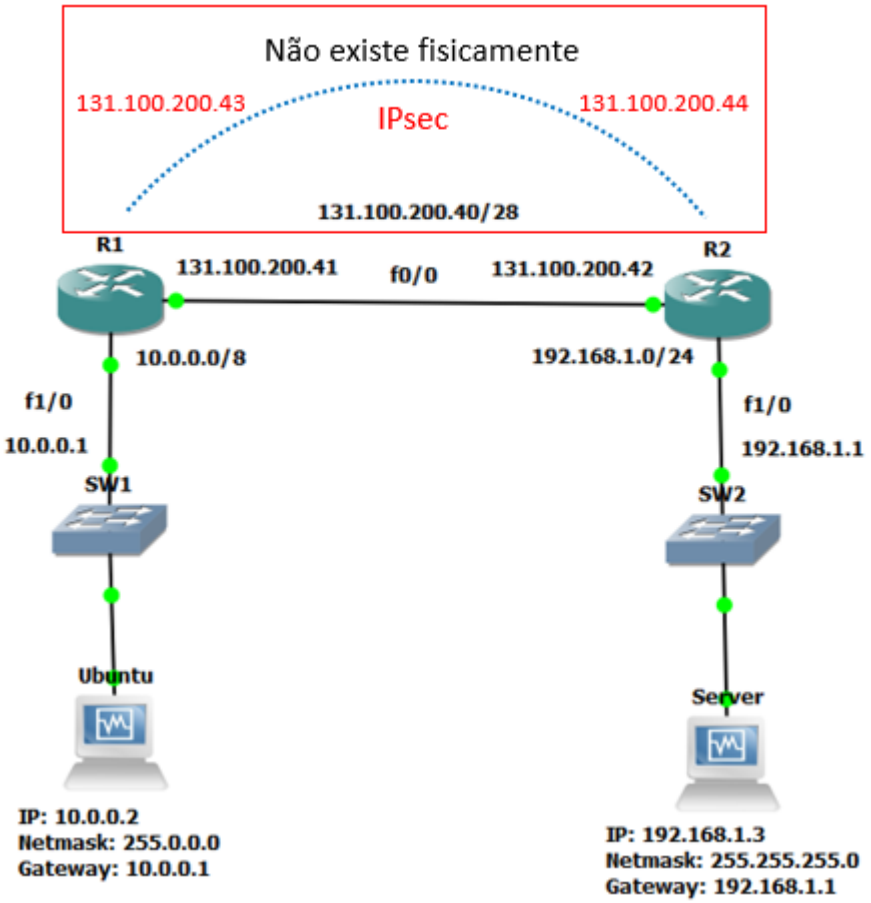


Fonte: Elaborado pelo autor

5.4.2 IPv4 com IPsec

A Figura 41 mostra o cenário do protocolo IPv4 com IPsec configurado.

Figura 41 - IPv4 com IPsec



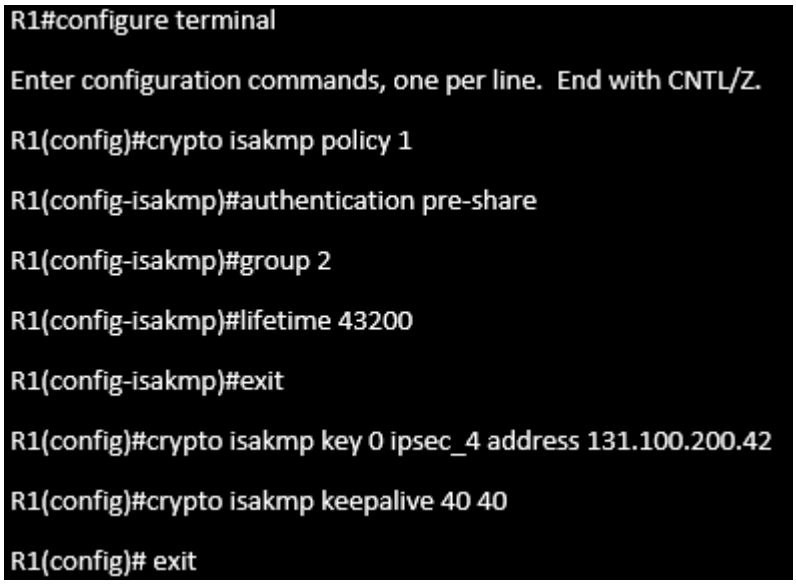
Fonte: Elaborado pelo autor

Antes de realizar a configuração do IPsec é necessário realizar todas as etapas feitos no cenário IPv4 sem IPsec.

Etapa 01 – A Figura 42 apresenta a definição dos parâmetros:

- Política ISAKMP;
- Algoritmo de criptografia;
- Método de autenticação;
- Grupo para a troca de chaves;
- Tempo de vida SA;
- Chave ISAKMP;
- Intervalo de repetição caso ocorrer algum erro com o pacote.

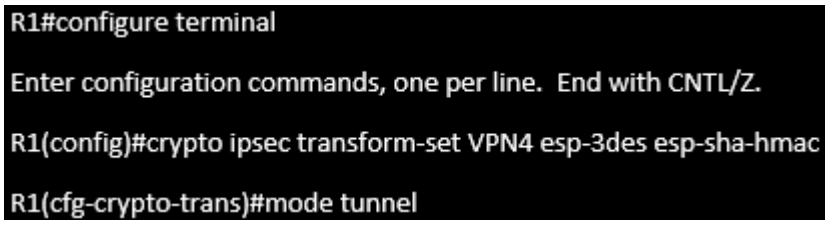
Figura 42 - Definição dos parâmetros na configuração do IPsec



Fonte: elaborado pelo autor

Etapa 02 – Durante a associação entre os roteadores foi definido o conjunto de criptografia e método de autenticação, onde o mesmo parâmetro será aplicado nos roteadores que mantiveram a comunicação, protegendo dessa forma o fluxo de dados que passaram entre ambas as partes. Os comandos aplicados são apresentados na Figura 43.

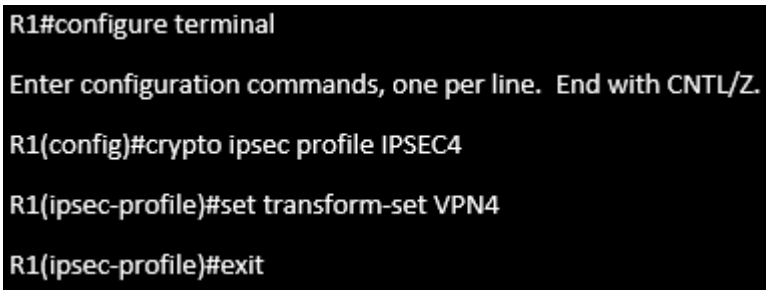
Figura 43 - Transformação IPsec



Fonte: Elaborado pelo autor

Etapa 03 – Criação do perfil IPsec e vinculando com a transformação IPsec, mostrado na Figura 44.

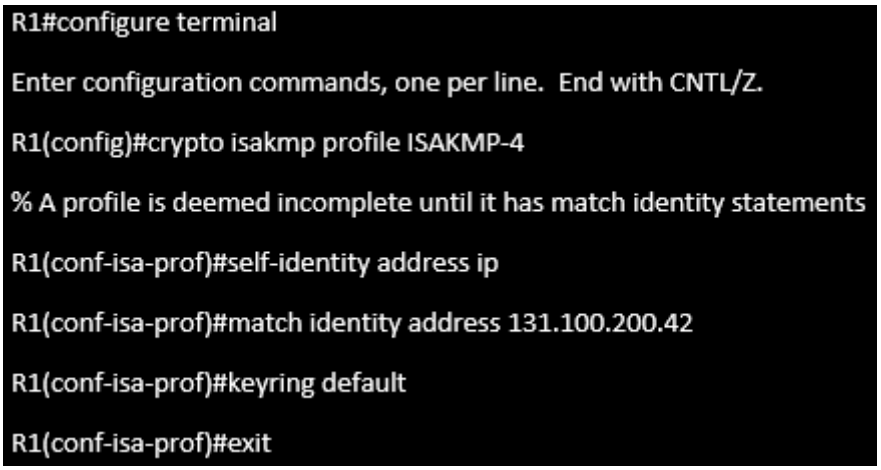
Figura 44 - Perfil IPsec



Fonte: Elaborado pelo autor

Etapa 04 – A Figura 45 mostra os comandos para a criação do perfil ISAKMP, em que realiza a identificação e verificação da identidade do componente que manterá a comunicação.

Figura 45 - Criação do perfil ISAKMP



Fonte: Elaborado pelo autor

No roteador 2 (R2), o campo de endereço foi aplicado 131.100.200.41.

Etapa 05 – Nessa etapa foi feito as seguintes configurações, como mostrado na Figura 46.

- Criação do túnel;
- Atribuição do IP para o túnel;
- Mostrar o início do túnel, ou seja, a origem onde os pacotes de dados são gerados;
- Mostrar o destino onde os pacotes de dados chegaram;
- Habilitar o modo túnel do IPsec no protocolo IPv4;

- Identificação do perfil IPsec (criado anteriormente) que será aplicado.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface tunnel 1
*May 24 12:01:56.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
R1(config-if)#ip address 131.100.200.43 255.255.255.240
R1(config-if)#tunnel source 131.100.200.41
R1(config-if)#tunnel destination 131.100.200.42
*May 24 12:07:37.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
state to up
R1(config-if)#tunnel mode ipsec ipv4
*May 24 12:08:04.875: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
state to down
R1(config-if)#tunnel protection ipsec profile IPSEC4
*May 24 12:08:54.563: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figura 46 - Configuração do túnel

Fonte: Elaborado pelo autor

No R2, foi atribuído o endereço 131.100.200.44 com máscara 255.255.255.240, para o túnel criado.

Etapa 06 – Determinação da rota, com o comando mostrado na Figura 47.

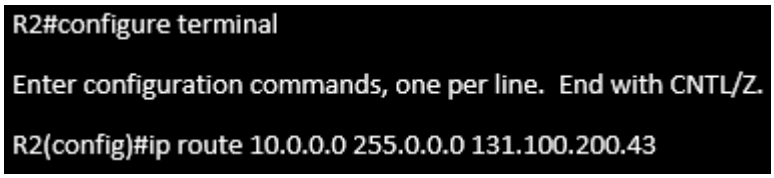
Figura 47 - Determinação da rota túnel no R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 192.168.1.0 255.255.255.0 131.100.200.44
```

Fonte: Elaborado pelo autor

Essa rota não poderá ser enxergada fisicamente, pois é uma rota criada para que os pacotes trafeguem sobre o túnel. A Figura 48 mostra o comando para traçar a rota no R2.

Figura 48 - Determinação da rota túnel no R2



Fonte Elaborado pelo autor

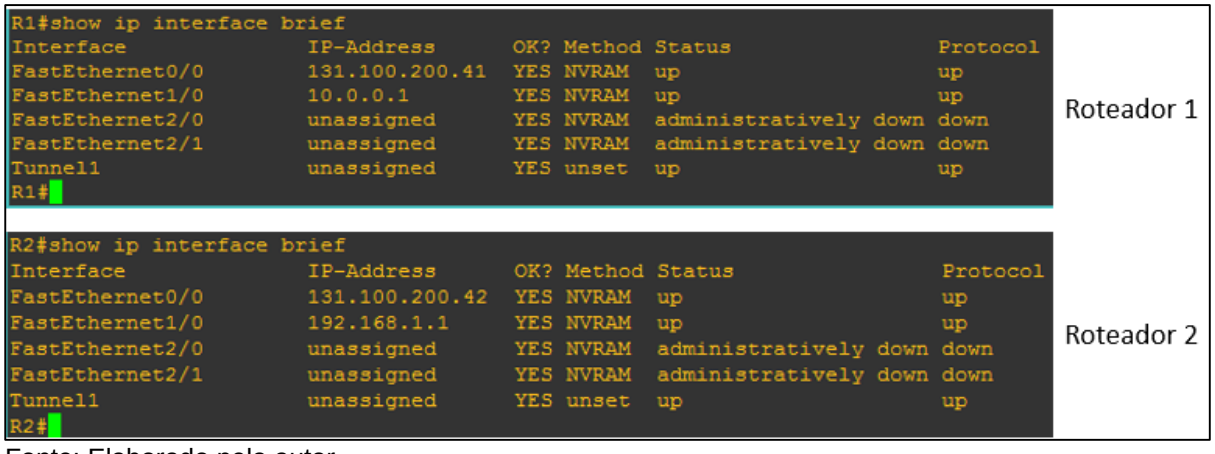
Com o comando: *#show crypto ipsec sa*, é possível visualizar o tráfego de pacotes, como:

- Quantidade de pacote que passaram pelo túnel;
- Número de pacotes que foram encriptados;
- Pacotes que apresentaram erro no envio;
- IP do início e fim do túnel.

No roteador 2 será aplicado os mesmos comandos para a configuração do IPsec.

A Figura 49 apresenta o comando: # *show ip interface brief*, na qual, pode ser visualizado as interfaces e os seus respectivos endereços.

Figura 49 - Visualização das interfaces



Fonte: Elaborado pelo autor

A Figura 50 mostra a aplicação do comando: *#show crypto ipsec sa*, antes do envio de pacote.

```
R1#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 131.100.200.41

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 131.100.200.42 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 131.100.200.41, remote crypto endpt.: 131.100.200.42
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x51A3B03A(1369681978)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xDE10BC96(3725638806)
 --More--
```

Figura 50 - Visualização em detalhe antes dos pacotes serem enviados

Fonte: Elaborado pelo autor

A Figura 51 mostra a aplicação do comando: *#show crypto ipsec sa*, depois do envio de pacote.

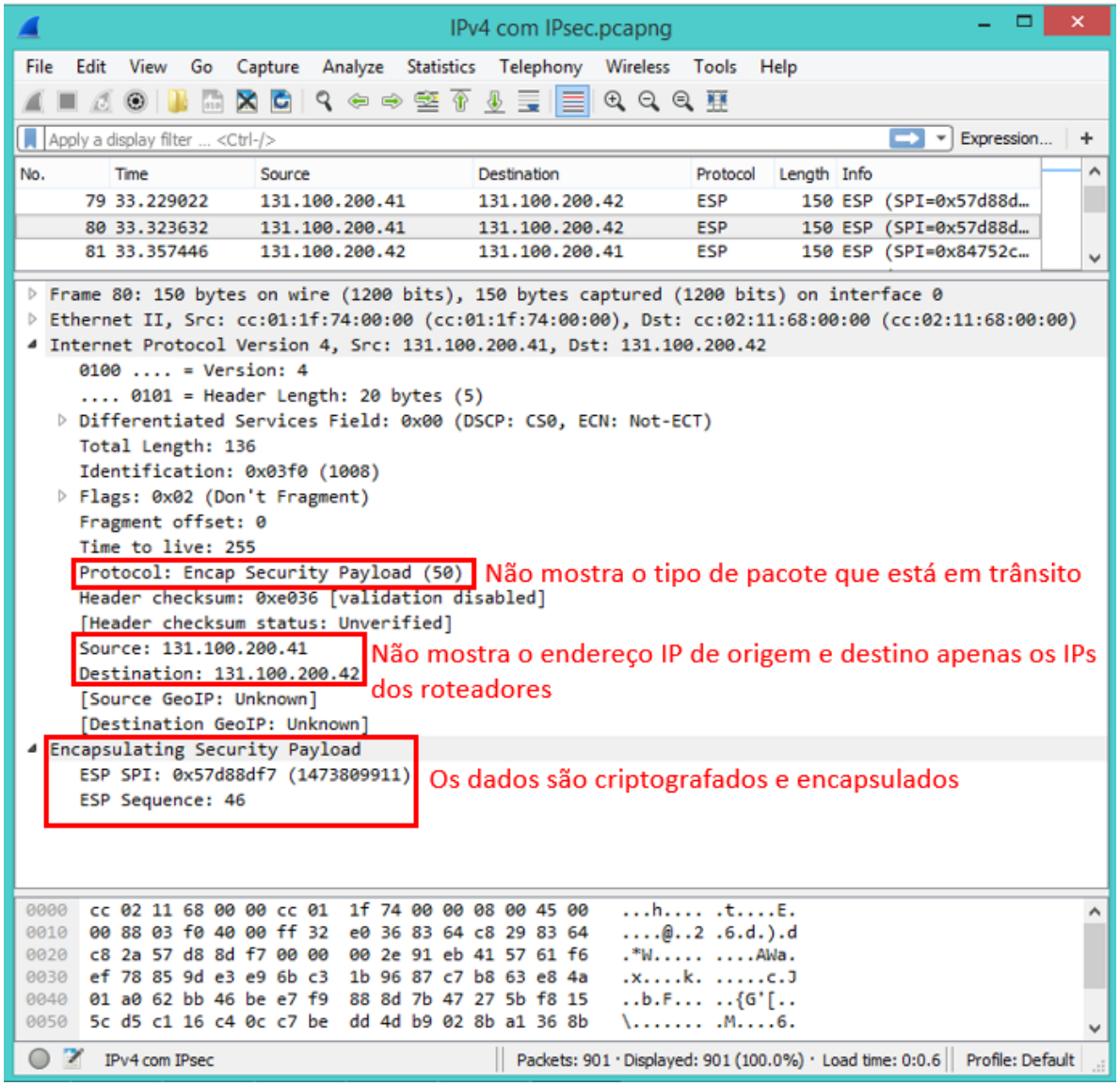
Figura 51 - Visualização em detalhe depois dos pacotes serem enviados.

```
R1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: IPSEC4, local addr 131.100.200.41

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 131.100.200.42 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 11, #recv errors 0

     local crypto endpt.: 131.100.200.41, remote crypto endpt.: 131.100.200.42
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x57D88DF7(1473809911)

     inbound esp sas:
      spi: 0x84752CC5(2222271685)
        transform: esp-3des esp-sha-hmac ,
 --More--
```

Fonte: Elaborado pelo autor

Etapa 07 – A Figura 52 mostra o cenário IPv4 com IPsec, onde foi feito a captura de pacotes enviados da máquina Ubuntu server para Ubuntu cliente ou vice-versa.

Figura 52 - Captura de pacotes do cenário IPv4 com IPsec através do Wireshark

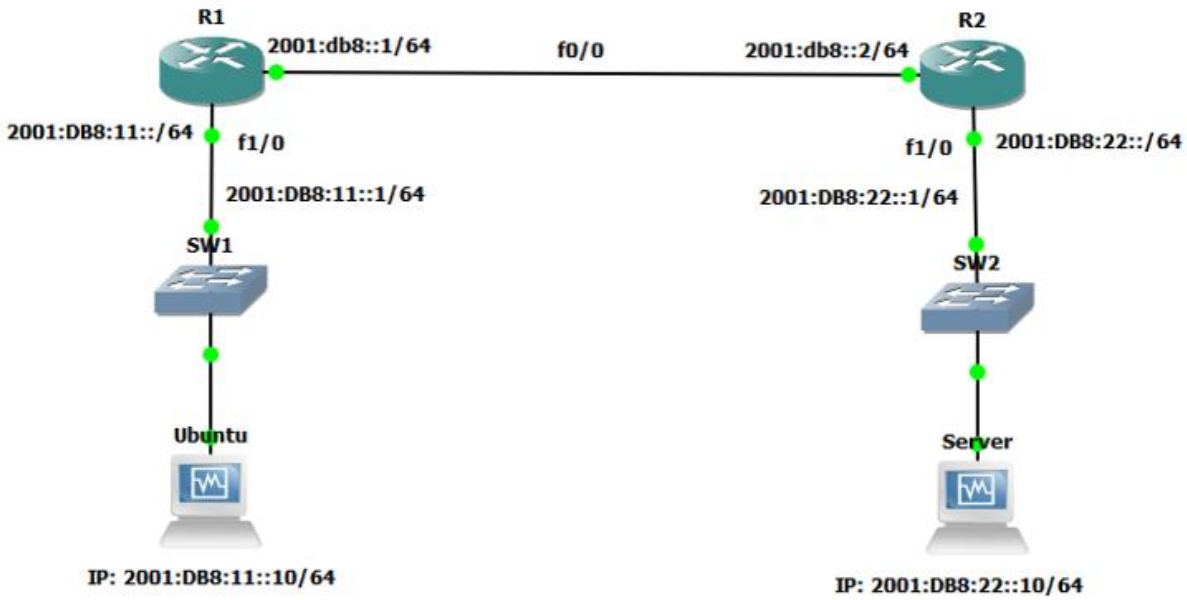


Fonte: Elaborado pelo autor

5.4.3 IPv6 sem IPsec

A Figura 53 mostra o cenário montado do protocolo IPv6 sem IPsec.

Figura 53 - Cenário IPv6 sem IPsec



Fonte: Elaborado pelo autor

Etapa 01 – A Figura 54 apresenta a configuração das interfaces 0/0 e 1/0 do roteador 1 (R1).

Figura 54 - Configuração das interfaces do cenário IPv6 sem IPsec

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:db8::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
*May 29 18:07:16.183: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 29 18:07:17.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config)#interface fastEthernet 1/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:db8:11::1/64
R1(config-if)#no shutdown
*May 29 18:08:10.251: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*May 29 18:08:11.251: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
```

Fonte: Elaborado pelo autor

No roteador 2 (R2) é aplicado os mesmos comandos para a configuração das interfaces, apenas modificando o campo do endereço IP, nesse caso, no R2 ficará da seguinte forma:

F0/0 – IP: 2001:db8::2/64

F1/0 – IP: 2001:db8:22::1/64

Etapa 02 – A Figura 55 mostra a determinação das rotas no roteador 1 (R1).

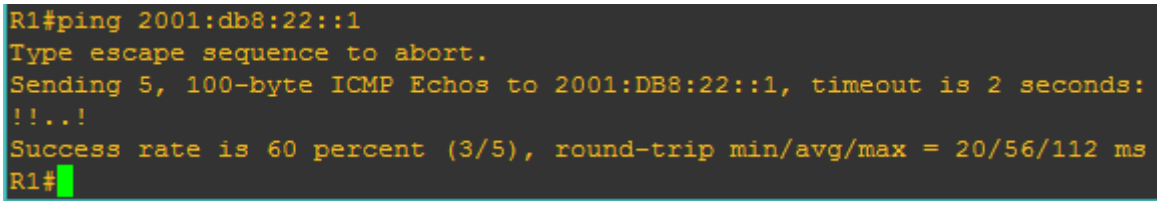
Figura 55 - Determinação da rota no R1 do cenário IPv6

Fonte: Elaborado pelo autor

A determinação da rota no roteador 2, ficará da seguinte forma R2(config)#*ipv6 route 2001:db8:11::/64 2001:db8::1.*

Etapa 03 – Com o comando: *#ping* “ip de destino”, mostrado na Figura 56, verifica a comunicação entre as interfaces.

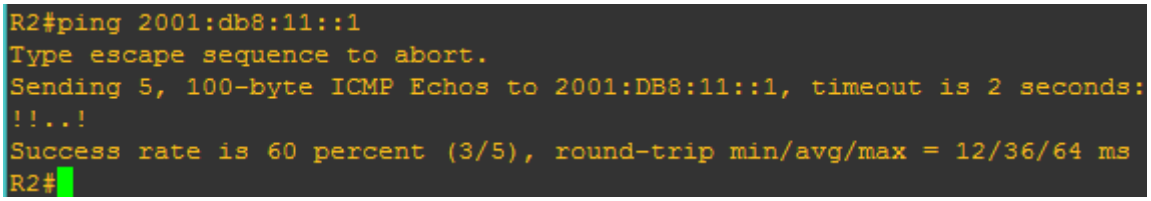
Figura 56 - Comunicação entre a interface do R1 com R2 do cenário IPv6



Fonte: Elaborado pelo autor

A Figura 57 mostra a comunicação sucedida entre as interfaces do R2 com as interfaces do R1, caso, ocorrer algum erro na comunicação os sinal de “! ” serão “. ”.

Figura 57 - Comunicação entre a interface do R2 com R1 do cenário IPv6



Fonte: Elaborado pelo autor

Etapa 04 – O comando mostrado na Figura 58 foi aplicado para salvar as configurações realizadas.

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

Figura 58 - Comando para salvar as configurações

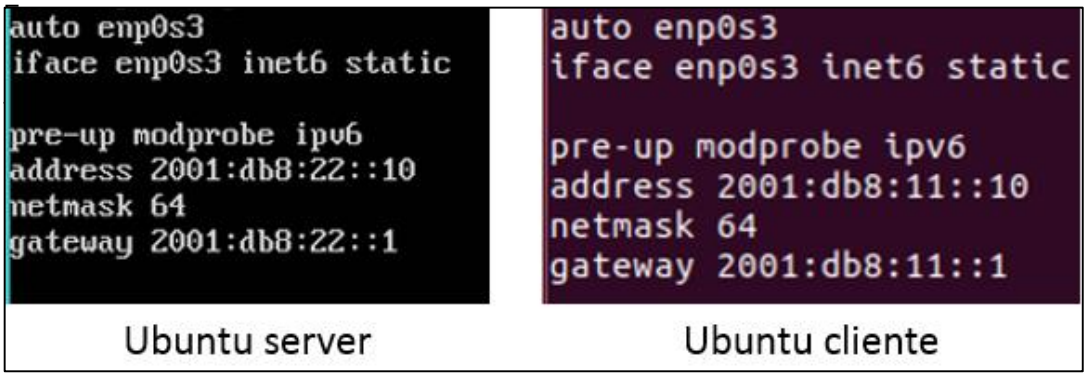
Fonte: Elaborado pelo autor

Etapa 05 – As duas máquinas criados no VirtualBox foram interligados no cenário e configurados da seguinte forma:

- Ubuntu: IP 2001:db8:11::10/64 e *gateway* 2001:db8:11::1
- Server: IP 2001:db8:22::10/64 e *gateway* 2001:db8:22::1

Foi definido o endereço IPv6 estático através do *arquivo #/etc/network/interfaces,* como retratado na Figura 59.

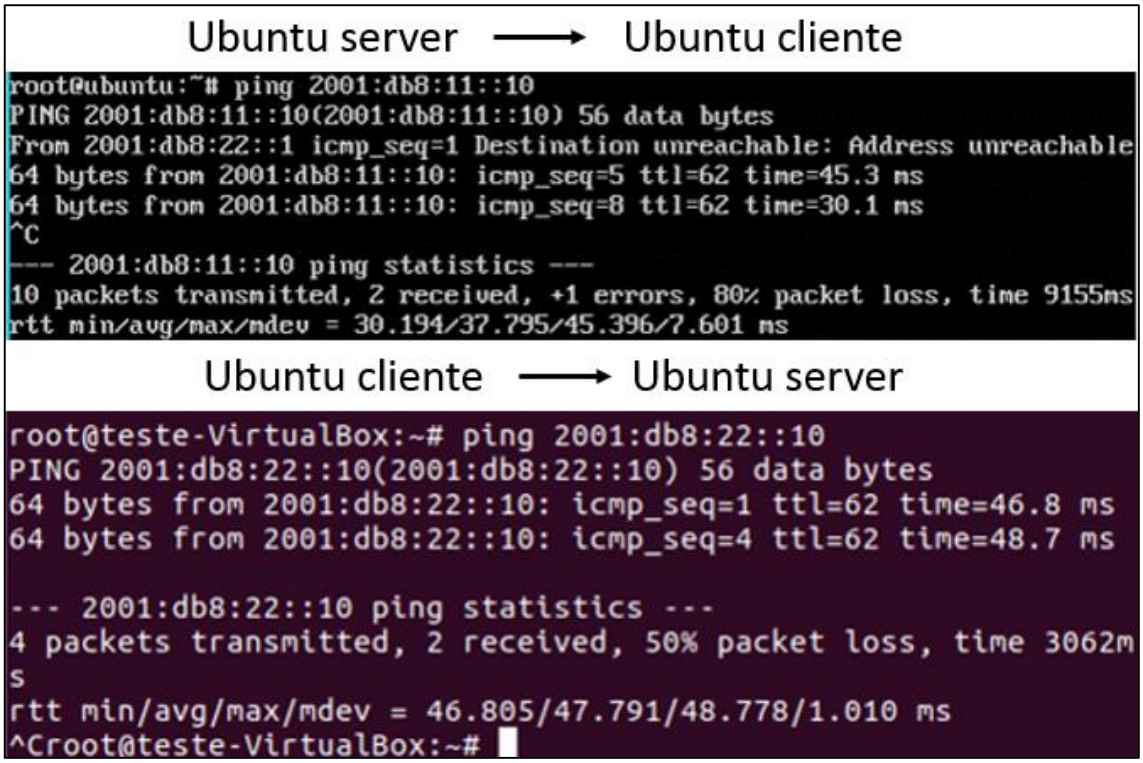
Figura 59 - Configuração IPv6 estático nas máquinas Server e Ubuntu



a
do pelo autor

Etapa 06 – Verificação da comunicação entre as máquinas, como mostrado na Figura 60.

Figura 60 - Comunicação entre as máquinas Ubuntu cliente e Ubuntu server

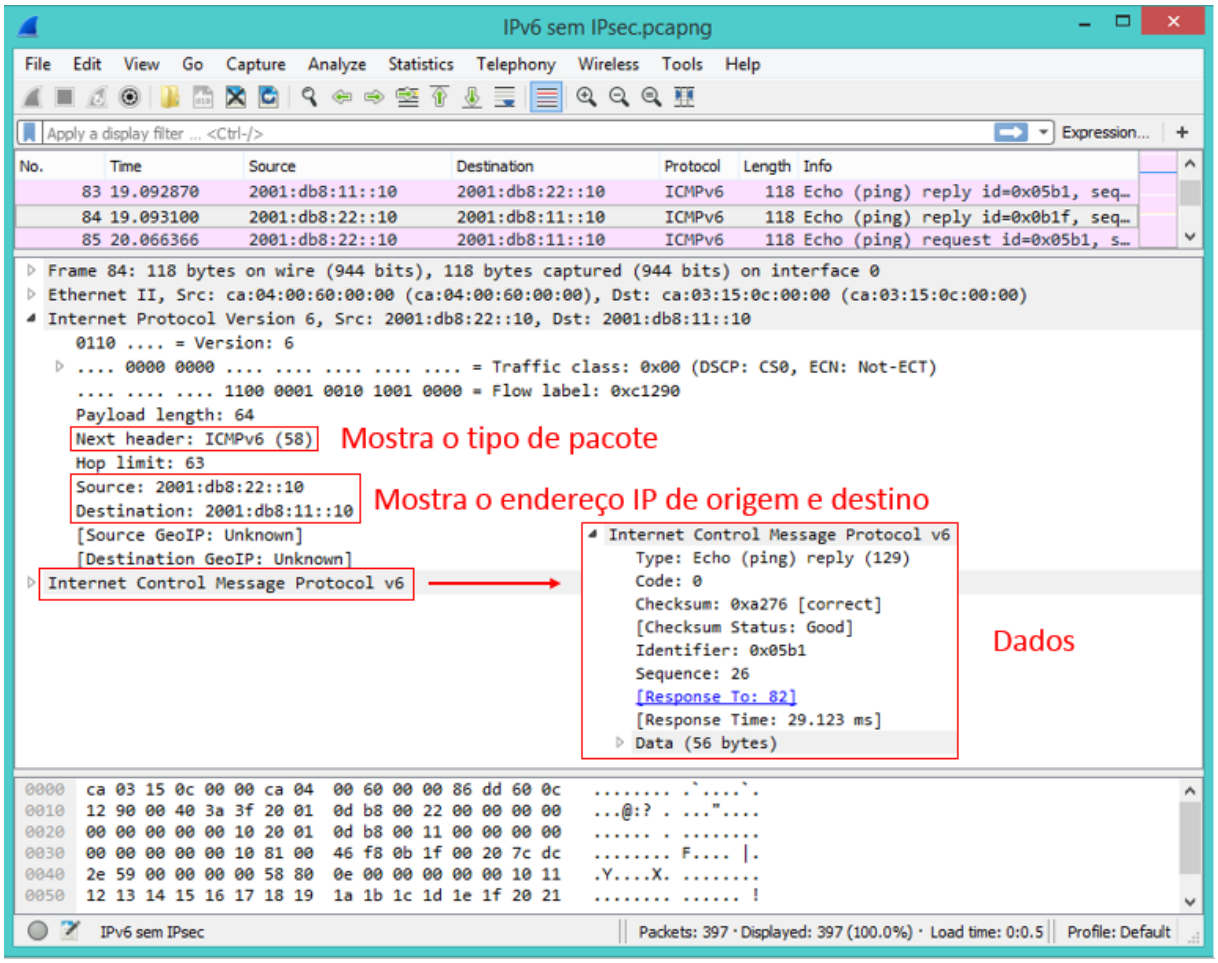


Fonte: Elaborado pelo autor

Etapa 07 – Com programa Wireshark, foi feito a captura de pacotes, como apresentado na Figura 61.

No cenário IPv6 sem o uso do IPsec foi feito a captura de pacotes enviados da máquina Ubuntu cliente para Ubuntu server ou vice-versa.

Figura 61 - Captura de pacotes do cenário IPv6 sem IPsec

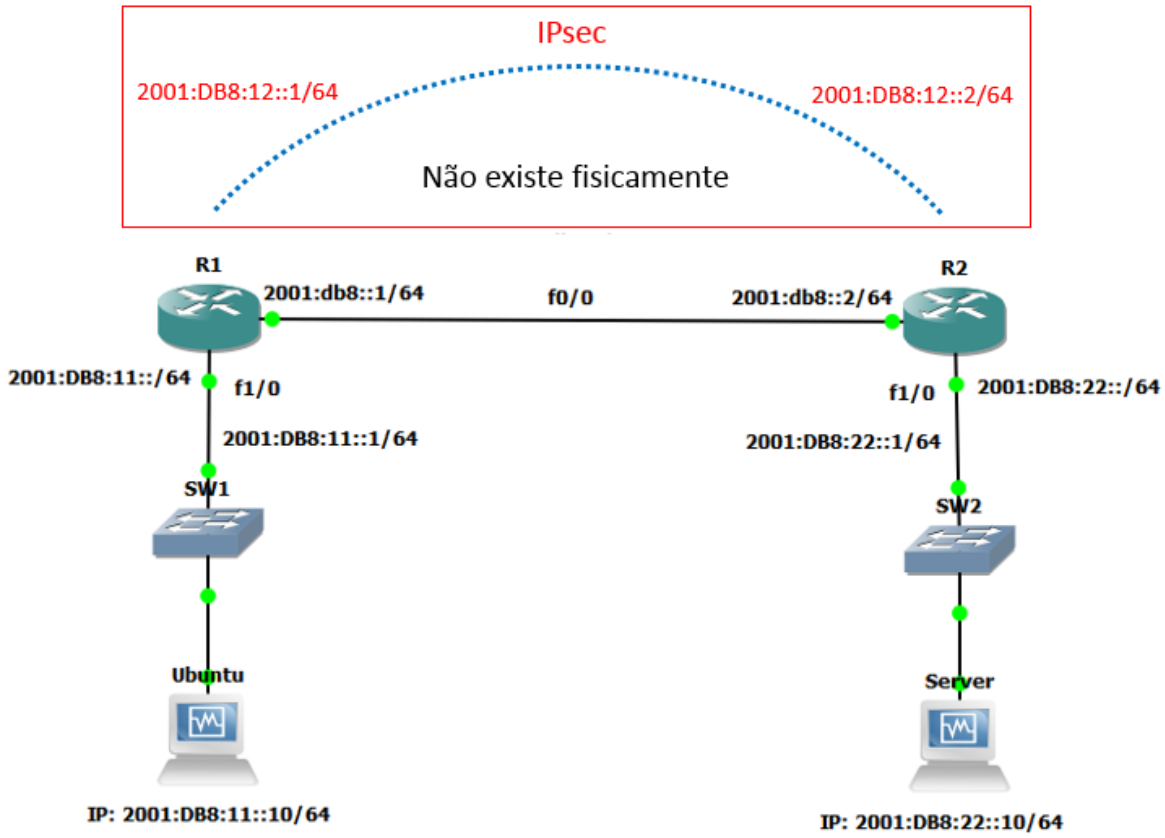


Fonte: Elaborado pelo autor

5.4.4 IPv6 com IPsec

A Figura 62 mostra o cenário do protocolo IPv6 com IPsec configurado.

Figura 62 - IPv6 com IPsec



Fonte: Elaborado pelo autor

Antes de realizar a configuração do IPsec é necessário realizar todas as etapas feitos no cenário IPv6 sem IPsec.

Etapa 01 – A Figura 63 apresenta a definição do tipo de chave e tipo de autenticação ISAKMP que será usado.

Figura 63 - Definição de autenticação ISAKMP

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto keyring keyring1
R1(conf-keyring)#pre-shared-key address ipv6 2001:db8::2/128 key teste
R1(conf-keyring)#exit
R1(config)#crypto isakmp key teste address ipv6 2001:db8::2/128
```

Fonte: elaborado pelo autor

Etapa 02 – A Figura 64 mostra a definição dos parâmetros:

- Política ISAKMP;
- Algoritmo de criptografia;
- Método de autenticação;
- Tempo de vida SA;
- Chave ISAKMP;

Figura 64 - Perfil IPsec

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
```

Fonte: Elaborado pelo autor

Etapa 03 – Durante a associação entre os roteadores foi definido o conjunto de criptografia e método de autenticação, onde o mesmo parâmetro será aplicado nos roteadores que mantiveram a comunicação, dessa forma protegendo o fluxo de dados que passaram entre ambas as partes, os comandos aplicados são apresentados na Figura 65.

Figura 65 - Criação do perfil ISAKMP e transformação IPsec

```
R1(config)#crypto ipsec transform-set 3des esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#exit
R1(config)#crypto ipsec profile profile0
R1(ipsec-profile)#set transform-set 3des
R1(ipsec-profile)#exit
```

Fonte: Elaborado pelo autor

Etapa 05 – Nessa etapa foi feito as seguintes configurações, como mostrado na Figura 66.

- Criação do túnel;
- Atribuição do IP para o túnel;
- Mostrar o início do túnel, ou seja, a origem onde os pacotes de dados são gerados;
- Mostrar o destino onde os pacotes de dados chegaram;
- Habilitar o modo túnel do IPsec no protocolo IPv6;
- Ligar o perfil IPsec (criado anteriormente) no túnel.

Figura 66 - Configuração do túnel no IPv6

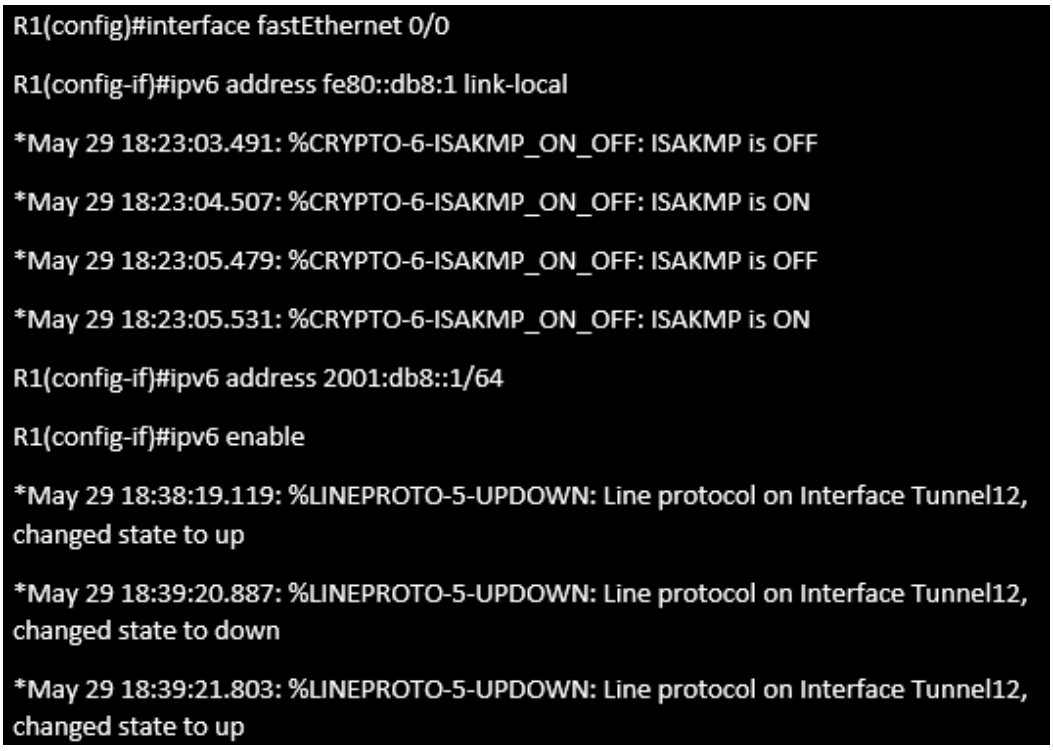
```
R1(config)#interface tunnel 12
*May 29 18:19:58.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel12, changed state to down
R1(config-if)#ipv6 address fe80::db8:12:1 link-local
R1(config-if)#ipv6 address 2001:db8:12::1/64
R1(config-if)#tunnel source 2001:db8::1
R1(config-if)#tunnel source f0/0
R1(config-if)#tunnel destination 2001:db8::2
R1(config-if)#tunnel protection ipsec profile profile0
*May 29 18:22:09.383: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
```

Fonte: Elaborado pelo autor

No R2, foi atribuído o endereço IPv6 2001:DB8:12::2/64, para o túnel criado.

Etapa 06 – Verificação das rotas, com o comando mostrado na Figura 67.

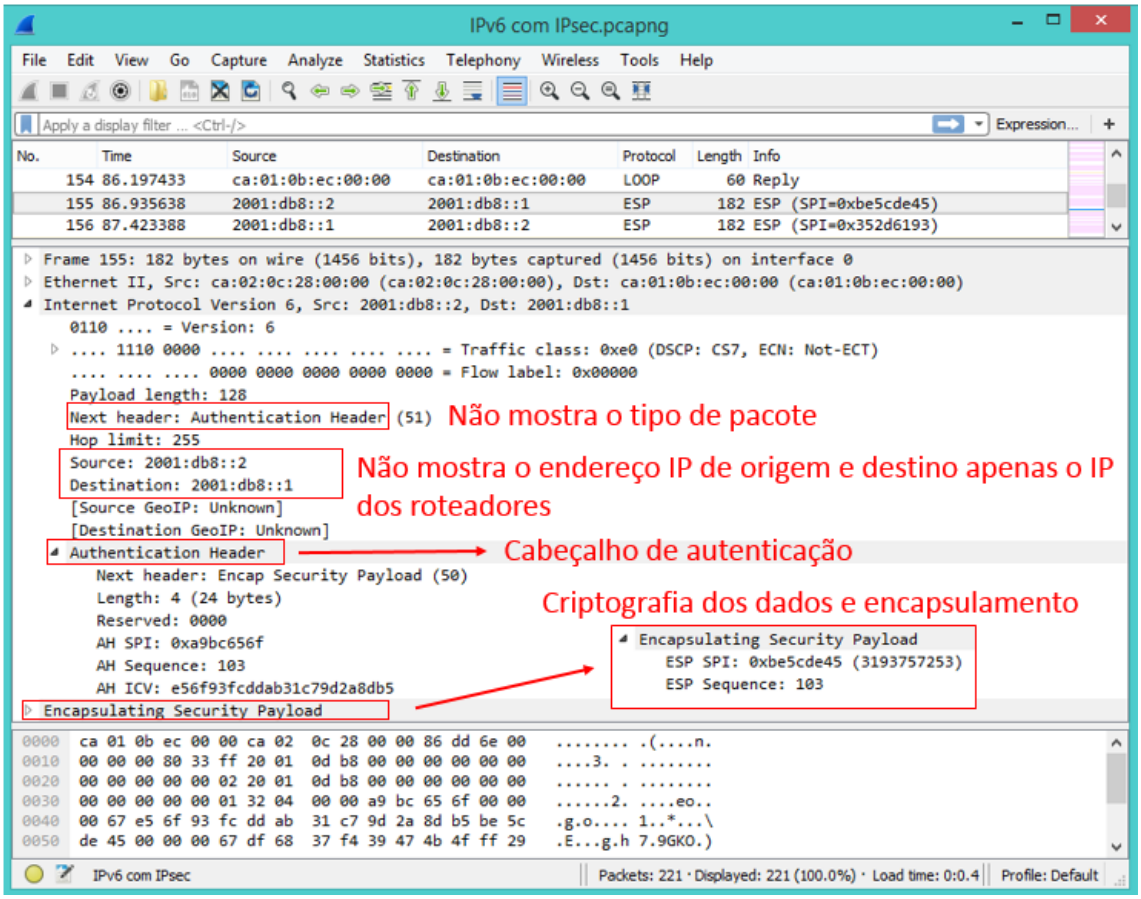
Figura 67 - Verificação das rotas



Fonte: Elaborado pelo autor

Etapa 07 – A Figura 68 mostra o cenário IPv6 com IPsec, onde foi feito a captura de pacotes enviados da máquina Ubuntu cliente para Ubuntu server ou vice-versa.

Figura 68 - Captura de pacotes do cenário IPv6 com IPsec através do Wireshark

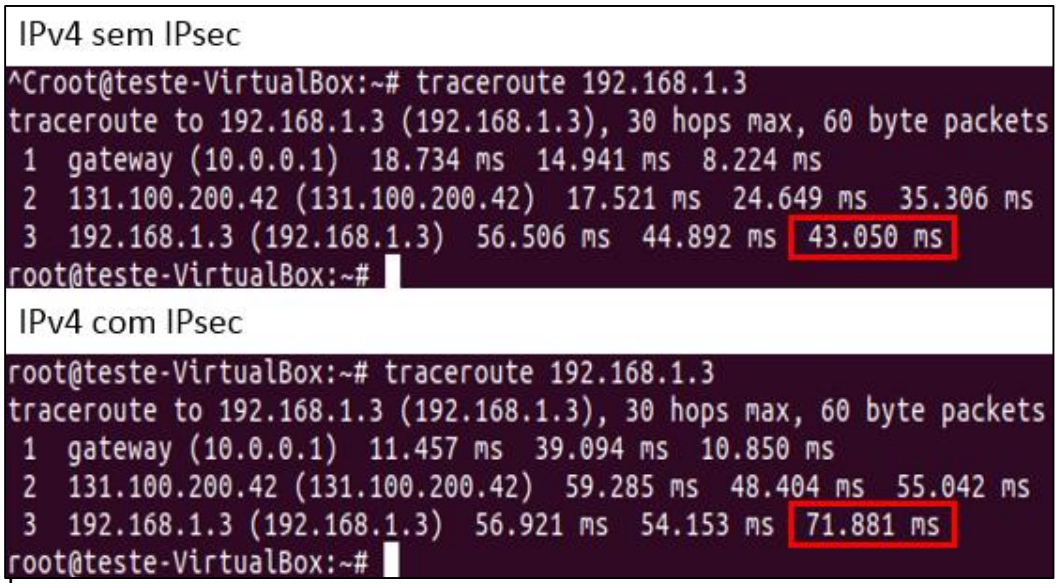


Fonte: Elaborado pelo autor

Através da ferramenta *traceroute* foi possível analisar a rota e o tempo dos pacotes enviados desde a origem até chegar ao destino, a seguir será apresentado a comparação do desempenho entre o IPv4 sem IPsec, IPv4 com IPsec, IPv6 sem IPsec e IPv6 com IPsec.

Na Figura 69 mostra o desempenho de IPv4 sem o uso do IPsec comparando com o IPv4 com IPsec aplicada.

Figura 69 - Comparação do IPv4 com e sem a aplicação do IPsec

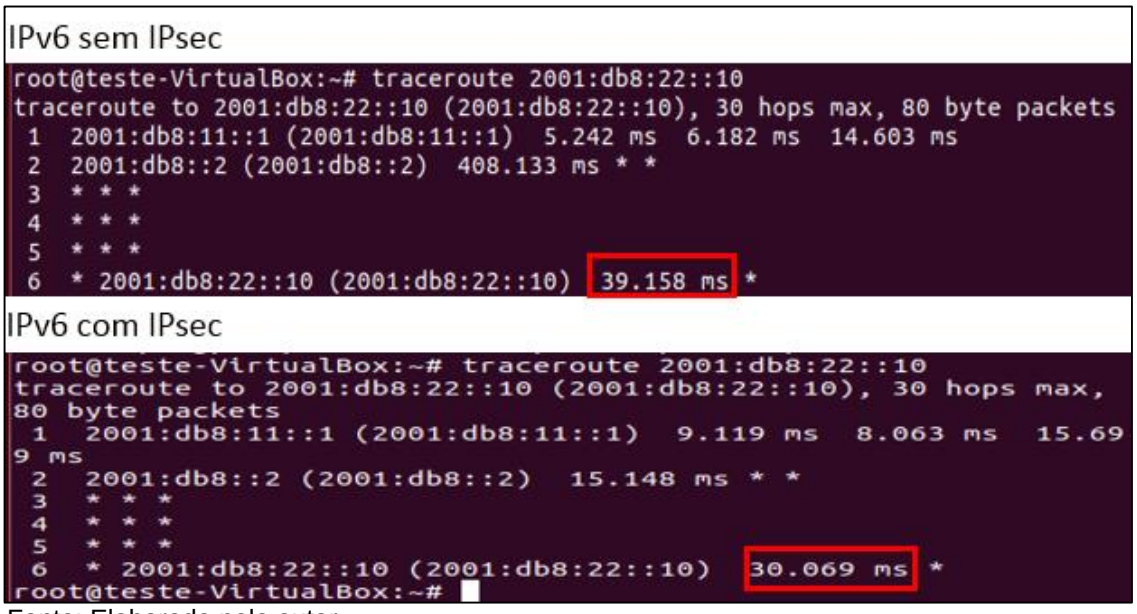


onte: Elaborado pelo autor

Pode-se observar que no IPv4 sem IPsec o tempo que levou para o pacote chegar até o destino é de 43.050 milissegundos, mais rápido que o IPv4 com IPsec, na qual levou 71.881 milissegundos para chegar ao destino.

A Figura 70 mostra o desempenho do tráfego de pacotes entre IPv6 sem IPsec e IPv6 com IPsec.

Figura 70 - Comparação do IPv6 com e sem a aplicação do IPsec



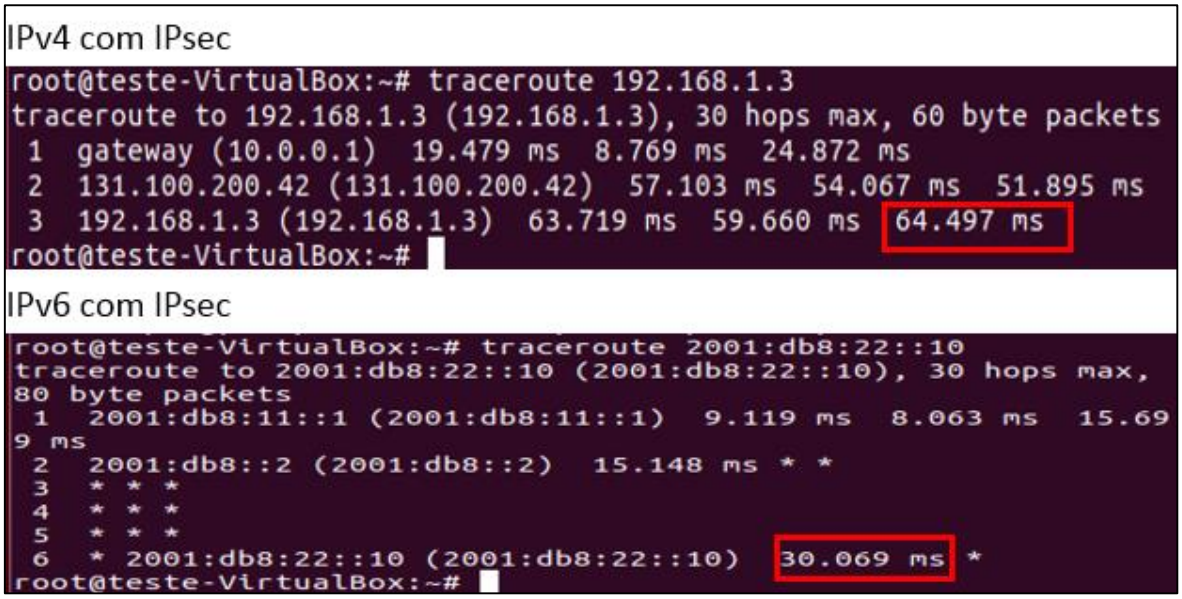
Fonte: Elaborado pelo autor

Como mostrado na figura acima a comparação do IPsec aplicado no IPv6 tem o desempenho próximo ou melhor do que IPv6 sem IPsec, pois no IPv6 como citado

nos capítulos anteriores o IPsec já vem embutido, necessita apenas ser habilitado, outro ponto positivo no IPv6, é o cabeçalho, na qual, possui um tamanho fixo, dessa forma quando os pacotes são despachados, não necessitam ser verificados pelos roteadores, assim, o envio dos dados torna-se mais rápido.

A comparação do desempenho entre o IPv4 e IPv6, onde ambas usam o IPsec, é mostrado na Figura 71.

Figura 71 - Comparação do desempenho do IPsec aplicado no IPv4 e no IPv6



Fonte: Elaborado pelo autor

A aplicação da ferramenta *traceroute* para a verificação do tempo do percurso que o pacote levou desde saída de origem até chegar o destino foi realizada várias vezes, com o intuito de analisar se ouve alguma diferença muito grande em relação ao tempo, mas como esperado a diferença de tempo são próximas, onde mostra que o desempenho do IPsec executado no IPv6 é muito melhor do que IPsec aplicado no IPv4.

6. CONSIDERAÇÕES FINAIS

O desenvolvimento desse trabalho teve como intuito apresentar o protocolo de segurança IPsec aplicado no IPv4 e no IPv6, fazendo comparativo entre ambas as versões de protocolo, analisando o desempenho em relação ao tráfego de pacotes de forma segura desde a origem até o destino, uma vez que a segurança de dados vem sendo uma questão de alta relevância no mundo digitalizado.

Os resultados adquiridos nos testes realizados são próximos aos esperados, demonstrando que o IPsec atua de forma mais eficiente no IPv6 do que no IPv4. Isto ocorre, pois, o IPsec já vem embutido no IPv6 desde a sua criação. Já no IPv4, o desempenho não é tão satisfatório, uma vez que o IPsec foi inserido posteriormente.

O IPsec traz benefícios, provendo forte segurança no tráfego de dados pela rede, trabalhando na camada de rede, onde atua de forma transparente ao usuário e aplicações. Dessa forma não será necessário nenhum tipo de treinamento ou modificação de software para o seu uso, além da redução de custo devido à possibilidade de criação de redes privadas através da Internet.

O mecanismo IPsec possibilita que os pacotes de dados trafeguem pela rede de forma segura, garantindo que apenas as pessoas autorizadas tenham acesso a essas informações. Mas isso não tira a necessidade da utilização de outros mecanismos de segurança para proteger as informações, pois o IPsec apenas atua uma parte na segurança de dados na comunicação entre duas entidades. Outros métodos também serão necessários para manter as informações seguras.

Para a realização desse trabalho foram utilizados vários conceitos como: conhecimento de redes de computadores, sistema operacional Linux, configuração de roteadores e máquinas para teste, entre outros.

Como sugestões para trabalhos futuros, poderiam ser realizados, estudos de desempenho dos protocolos de roteamento (RIP - *Routing Information Protocol*, OSPF - *Open Shortest Path First*, IGRP - *Interior Gateway Protocol*, EIGRP - *Enhanced IGRP*, BGP - *Border Gateway Protocol*), onde poderão ser realizados testes no ambiente virtual, mostrando o comportamento de cada protocolo e como atuam no IPv6.

REFERÊNCIAS

BRITO, Samuel Henrique Bucke. **IPv6:** o novo protocolo da internet. São Paulo: Novatec Editora Ltda, 2013.

CAMPOS, André. **Sistema de segurança da informação:** controlando os riscos. 2ª.ed. Florianópolis: Visual Books, 2007.

CANALTECH. **O que é VPN?**. Disponível em: <https://canaltech.com.br/o-que-e/internet/o-que-e-vpn-23748/>. Acesso em: 29 abr. 2017.

CERT.BR. **Cartilha de segurança para Internet:** ataques na Internet. Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em: 23 fev. 2017.

CERT.BR. **Cartilha de segurança para Internet:** códigos maliciosos (*Malware*). Disponível em: < https://cartilha.cert.br/malware/>. Acesso em: 1 mar. 2017

CERT.BR. **Cartilha de segurança para Internet:** criptografia. Disponível em: <https://cartilha.cert.br/criptografia/>. Acesso em: 9 mar. 2017.

CERT.BR. **Cartilha de segurança para Internet:** mecanismo de segurança. Disponível em: <https://cartilha.cert.br/mecanismos/>. Acesso em: 7 mar. 2017.

CERT.BR. **Cartilha de segurança para Internet:** segurança na internet. Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em: 21 mar. 2017.

CISCO. **Como lidar com a sequência de ataque completa:** antes, durante e depois de um ataque. Disponível em: <http://www.cisco.com/c/dam/r/pt/br/internet-of-everything-ioe/assets/pdfs/sec_bda_wp_cte_pte_etmg_pt-br_39724.pdf>. Acesso em: 21 mar. 2017.

CISCO. **Configurando e pesquisando defeitos a criptografia de camada de rede Cisco:** IPsec e ISAKMP - Parte 2. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2015/11/o-que-e-vpn-saiba-tudo-sobre-rede-virtual-privada.html>. Acesso em: 29 abr. 2017.

Equipe IPV6.br. **Laboratório de IPv6:** aprenda na prática usando emular de rede. São Paulo: Novatec Editora Ltda, 2015.

FERNANDO, Rubens. **Criptografia de Dados**: Parte 02 (Componentes, Algoritmos e Modelos). IMasters, 2007. Disponível em: <

https://imasters.com.br/artigo/6361/linguagens/criptografia-de-dados-parte-02-componentes-algoritmos-e-modelos/?trace=1519021197&source=single>. Acesso em: 28 abr. 2017.

FONTES, Edison Luiz Gonçalves. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

FOROUZAN, Behrouz. **Protocolo TCP/IP**. Trad. João Eduardo Nóbrega Tortello. 3ª. ed. São Paulo: McGraw-Hill, 2008.

IBM. **Comparação entre IPv4 e ipv6**. Disponível em: < https://www.ibm.com/support/knowledgecenter/pt/ssw_ibm_i_71/rzai2/rzai2compipv4ipv6.htm>. Acesso em: 10 abr. 2017.

IBM. **Protocolos IP security (IPSec)**. Disponível em: <https://www.ibm.com /support/knowledgecenter/pt/ssw_i5_54/rzaja/rzajaipsec.htm>. Acesso em: 18 abr. 2017.

IPV6.BR**. Ipv6.** Disponível em: < http://ipv6.br/post/introducao/>. Acesso em: 11 abr. 2017.

KLEINA, **Nilton. A história da internet:** pré-década de 60 até anos 80 [infográfico]. TecMundo, 2011. Disponível em: < https://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>Acesso em: 15 fev. 2017.

KUROSE, James.; ROSS, Keith. **Redes de computadores e a internet:** uma abordagem top-down. Trad. Arlete Simille Marques. 6ª. ed. São Paulo: Pearson Addison Wesley, 2013.

MENEZES, Eduardo Pimentel. **Novas Tecnologias:** repercussões no tempo e no espaço da educação a distância. Universidade Salgado de Oliveira, 2003. Disponível em: <http://www.abed.org.br/seminario2003/texto07.htm>. Acesso em: 22 mar. 2017.

MOZART, Vinicius. **Segurança da Informação (pilares de segurança).** Microsoft TechNet, 2012. Disponível em: <https://social.technet.microsoft.com/wiki/pt-br/contents/articles/14950.aspx>. Acesso em: 8 mar. 2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de rede em ambientes cooperativos**. São Paulo: Novatec Editora Ltda, 2007.

ROHR, Altieres. **Conheça os diferentes tipos de vulnerabilidades e ataques de hackers.** G1, 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/05/conheca-os-diferentes-tipos-de-vulnerabilidades-e-ataques-de-hackers.html>. Acesso em: 28 fev. 2017.

SILVEIRA, Debora Priscila. **O que é modelo OSI?.** Oficina da Net, 2016. Disponível em: <https://www.oficinadanet.com.br/post/15976-o-que-e-o-modelo-osi>. Acesso em: 06 abr. 2017.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. Trad. Daniel Vieira. 4ª. ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew. **Redes de computadores**. Trad. Vandenberg D. de Souza. 5ª. ed. Rio de Janeiro: Elsevier, 2011.

TECHTUDO. **O que é VPN?:** saiba tudo sobre a rede virtual privada. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2015/11/o-que-e-vpn-saiba-tudo-sobre-rede-virtual-privada.html>. Acesso em: 29 abr. 2017.