UNIVERSIDADE DO SAGRADO CORAÇÃO

RAFAEL HENRIQUE DIAS

PROTOCOLO IPv6: INTEGRAÇÃO DO PROTROCOLO IPv6 COM O IPSEC

BAURU
2014

RAFAEL HENRIQUE DIAS

PROTOCOLO IPv6: INTEGRAÇÃO DO PROTROCOLO IPv6 COM O IPSEC

Trabalho de Conclusão de Curso Apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2014

Dias, Rafael Henrique.

D541p

Protocolo IPv6: Integração do Protocolo IPv6 com o IPSEC / Rafael Henrique Dias. -- 2014.

63 f. : il.

Orientador: Prof. Me. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. IPv4. 2. IPv6. 3. Internet. 4. Segurança. 5. IPsec. I. Martins, Henrique Pachioni. II. Título.

RAFAEL HENRIQUE DIAS

PROTOCOLO IPV6: INTEGRAÇÃO DO PROTROCOLO IPv6 COM O IPSEC

Trabalho de Conclusão de Curso Apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade do Sagrado Coração

Bauru, 09 de dezembro de 2014.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me dar saúde, e sabedoria para iniciar esse projeto.

Agradeço por ter os melhores pais do mundo, Vera e Osney, que sempre me deram amor, carinho e sábios conselhos, que contribuíram para minha formação pessoal, do meu caráter, e também ensinando sobre os verdadeiros valores da vida.

Agradeço-os por estarem presentes em minha vida, por me apoiarem, e darem todo o suporte nos meus estudos.

Agradeço minha família pela paciência e o respeito que tiveram comigo nas horas em que precisei de silêncio, e quando tive dificuldade em realizar alguma etapa no trabalho.

Não posso esquecer-me do apoio que tive da minha irmã Leila, do cunhado Alexandre e da minha linda sobrinha Maria Rosa, eles sempre me apoiaram nas minhas decisões, amo muito vocês.

Agradeço também minha avó Amélia, que está com 84 anos firme e forte, que me ajudou em todos os momentos. Amo-te vó.

Agradeço minha esposa Fernanda, pois ela sempre me incentivou e me apoiou nos momentos difíceis.

"- Fernanda você é a mulher da minha vida! Agradeço a Deus todos os dias por ter te conhecido."

Agradeço minha sogra, Maria Helena, por ser uma pessoa maravilhosa comigo, sempre me ajudando, incentivando e aconselhando.

Também agradeço meus amigos Deivide e João Paulo, pelo apoio mútuo, lembrarei-me dos momentos bons e ruins que passamos nesses anos, essas são amizades que levarei para o resto de minha vida.

E um agradecimento em especial aos meus mestres, professores dedicados que tive o privilégio de conviver: Elvio foi um dos meus primeiros professores da USC, excelente educador, me passou muito conhecimento e sou grato por tudo o que me ensinou, me ajudou e também pelos conselhos.

Patrick, obrigado por dividir sua sabedoria, agradeço pelo seu esforço, paciência que teve comigo, obrigado por explicar inúmeras vezes à mesma matéria, me incentivando a seguir em frente, e a estudar mais. Obrigado por tudo.

Henrique, meu professor e orientador, só tenho que lhe agradecer, pois foi você que me ajudou a realizar esse trabalho, me incentivou, respondeu meus e-mails de final de semana, de madrugada, me deu ideias, sugestões para a melhoria do projeto. Obrigado por ser um excelente professor e orientador, obrigado pela paciência. Você foi à base para a construção desse trabalho.

Um agradecimento especial para um uma pessoa que infelizmente me deixou em 2013, a minha segunda mãe, a minha Vó Rosa que sempre morou comigo.

Ela ajudou na minha criação quando pequeno, sempre fez o possível e o impossível para me agradar, nós éramos muito próximos, uma relação de muito amor e carinho. Sei que ela está pertinho de Deus olhando pela gente aqui.
Amo-te, a saudade só aumenta, e obrigado por tudo o que fez na minha vida.

“O motivo que convencerá a maioria das pessoas a comprar um computador para a casa será vinculando essa pessoa a uma rede nacional de comunicações. Somente estamos na etapa inicial do que será um avanço realmente notável para a maioria das pessoas, tão notável quanto o telefone”.

(Steve Jobs 1985)

RESUMO

Com o rápido aumento de usuários na internet deu-se o rápido esgotamento de endereços livres do protocolo de comunicação de internet o Internet Protocol versão 4 (IPv4), a solução para tanto, foi o desenvolvimento de um novo protocolo o Internet Protocol versão 6 (IPv6). Analisando falhas de segurança existentes na versão 4, e pensando na segurança dos dados transitados via internet, foi desenvolvido o Security Protocol (IPSEC), uma solução de segurança em nível de camada de rede para proteger todo o tráfego de rede. Este trabalho tem como objetivo demonstrar a utilização do protocolo IPv6 integrado com o IPSEC a fim de identificar sua segurança e desempenho, demonstrando se ouve ou não o aumento do tamanho dos pacotes que trafegam na rede, por conta das criptografias que acompanham os pacotes, e quanto esse aumento pode significar, e também se realmente os pacotes foram transmitidos com segurança até seu destinatário. Pode-se concluir que através dos testes realizados, e com a implementação do IPSEC junto ao protocolo IPv6, a segurança foi ativada em todos os modos de criptografia, assim garantindo a integridade e confidencialidade dos dados transmitidos, porém arquivos maiores que 500 MB geram um aumento no tempo de transferências, devido ao processo de criptografia, podendo ocasionar lentidões na rede.

Palavras-chave: IPv4. IPv6. Internet. Segurança. IPsec.

ABSTRACT

With the rapid increase of Internet users was given the rapid depletion of free addresses of Internet communication protocol Internet Protocol version 4 (IPv4), the solution to both, was the development of a new Protocol Internet Protocol version 6 (IPv6). Analyzing existing security holes in version 4, and thinking about the security of data carried over the Internet, we developed the Security Protocol (IPSec), a security solution for network layer level to protect all network traffic. This paper aims to demonstrate the use of integrated IPv6 protocol with the IPSEC to identify their safety and performance, demonstrating hear or not increasing the size of the packets traveling on the network, because of the encryption that accompany the packages, and as this increase could mean, and also really packets were transmitted safely to its destination. It can be concluded that through the tests, and with the implementation of IPSEC with the IPv6 protocol, security has been enabled on all encryption modes, thus ensuring the integrity and confidentiality of transmitted data, but files larger than 500 MB generate increase in time transfers due to the encryption process, which may cause delays in the network.

Keywords: IPv4. IPv6. Internet. Security. IPsec .

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AES Advanced Encryption Standard

AH Authentication Header

ARP Address Resolution Protocol

ATM Asynchronous Transfer Mode

BSD Berkeley Software Distribution

CAST Carlisle Adams and Stafford Tavares

CGA Cryptographically Generated Addresses

CIDR Classless Inter Domain Routing

DES Data Encryption Standard

DHCPv6 Dynamic Host Configuration Protocol version 6

DNS Domain Name System

ESP Encapsulating Security Payload

EUI-64 Extended Unique Identifier-64

FDDI Fiber Distributed Data Interface

FGV Fundação Getúlio Vargas

HMAC Hash-based Message Authentication Code

HTTP Hypertext Transfer Protocol

IANA Internet Assigned Numbers Authority

ICMPv6 Internet Control Message Protocol version 6

ICV Integrity Check Value

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IGMP Internet Group Management Protocol

IID Interface Identifier

IKE Internet Key Exchange

IP Internet Protocol

IPSEC IP Security Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

ISAKMP Internet Security Association

LAN Local Area Network

MAC Media Access Control

MD5 Message-Digest algorithm 5

MLD Multicast Listener Discovery

MTU Maximum Transmission Unit

NAT Network Address Translation

NIC Núcleo de Informação e Coordenação

NLA Next Level Aggregation

OSI Open Systems Interconnection

OAKLEY Key Management Protocol

PPP Point-to-point Protocol

RARP Reverse Address Resolution Protocol

RFC Request for Comments

RSVP Resource Reservation Protocol

SA Security Association

SAD Security Association Database

SHA Secure Hash Algorithm

SLA Site Level Aggregation

SPD Security Policy Database

SPI Security Parameter Index

SSH Secure Shell

SSL Secure Socket Layer

TCP/IP Transmission Control Protocol/Internet Protocol

TLA Top Level Aggregation

ULA Unique Local Address

URLs Uniform Resource Locators

UTFPR Universidade Tecnológica Federal do Paraná

VLSM Variable Length Subnet Mask

VoIP Voice Over IP

VPN Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

Um dos maiores projetos, senão o maior, já construído pela engenharia humana, foi a Internet, criada por pesquisadores no final da década de 60 (1966) nos Estados Unidos, durante a Guerra Fria entre EUA e URSS, havia um medo constante de que um ataque aos meios de comunicação do país culminasse na indisponibilidade dos serviços de telecomunicações. (TANEMBAUM, 2003).

Em 1969 foram instalados os primeiros quatro nós da rede em universidades que, naquela época, era denominada ARPANET. Somente em 1983, com mais de 500 hosts na rede, que surgiu a Internet propriamente dita com base estrutural que conhecemos atualmente, ou seja, baseada no protocolo IP. (TANEMBAUM, 2003).

Na década de 80, o resultado de diversas pesquisas realizadas em todo o mundo foi incorporado à rede mundial, o que contribuiu para o desenvolvimento de um novo padrão de protocolos conhecido como TCP/IP. (BRITO, 2013).

Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997. (IPv6.br)

A questão de segurança na Internet é discutida há décadas, e melhorias vêm sendo implementadas desde então.

Esse trabalho é um material de apoio para interessados em alternativas mais seguras para redes de computadores, na qual a comunicação é feita utilizando o protocolo IP. No momento a versão mais utilizada deste protocolo é o IPv4, que gradativamente está sendo substituído pelo IPv6.

Pensando em novos mecanismos de segurança o protocolo IP versão 6 foi criada para trabalhar em conjunto com o IPSEC. (BRITO, 2013).

O IPSEC pode ser muito útil, tanto em empresas quanto em qualquer ambiente que disponha de mais de um computador. Com o IPSEC é possível restringir determinadas informações sigilosas. O IPSEC pode ser útil também para a segurança de informações externas, pois ele atua diretamente na camada de rede, verificando todos os pacotes que entram e saem deste local. (BRITO, 2013).

1.1 OBJETIVOS

Nesse capítulo serão apresentados o objetivo geral, e os objetivos específicos.

1.1.1 Objetivo geral

Demonstrar como será feita à integração do protocolo IPV6 em conjunto com a solução de segurança IPSEC, a fim de documentar e testar sua performance.

1.1.2 Objetivos específicos

a) estudar o IPv6, e sua forma de integração com o IPSEC e seus cabeçalhos Authentication Header (AH) e Encapsulating Security Payload (ESP);
b) montar um cenário mostrando o funcionamento de uma rede IPv6 com IPSEC;
c) realizar testes de funcionamento do IPv6 em conjunto com IPSEC, nos modos AH e ESP, AH+ESP;
d) avaliar o desempenho do protocolo IPSEC em redes IPv6.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será apresentado o referencial teórico, para compreensão da transição gradual do protocolo IPv4 para o IPv6, assim como sua integração de segurança IPSEC com o IPv6.

2.1 PROTOCOLOS

Protocolo é um acordo de comunicação em que o ponto de envio de dados e o de recebimento estabelece regras de como a comunicação será realizada. (FARREL, 2005).

Basicamente, um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação. Como uma analogia, quando uma mulher é apresentada a um homem, ela pode estender a mão para ele que, por sua vez, pode apertá-la ou beijá-la, dependendo, por exemplo, do fato de ela ser uma advogada que esteja participando de uma reunião de negócios ou uma princesa europeia presente a um baile de gala. A violação do protocolo dificultará a comunicação, se não a tornar completamente impossível. (TANENBAUM, 2003).

Para melhor entender a funcionalidade de cada protocolo, dependendo do serviço que cada um presta, eles foram classificados em camadas distintas.

A função que cada conjunto de camadas com as atribuições que devem desempenhar em um sistema é chamado modelo de rede, juntando as camadas e os protocolos, denomina-se arquitetura de rede. (KUROSE; ROSS, 2006).

2.2 PROTOCOLO IPv4

O Internet Protocol (IP) é um protocolo utilizado para comunicação nas redes de computadores na Internet. Foi criado para que dois ou mais computadores pudessem se interligar. O endereço IP é formado por um campo de 32 bits, onde são identificados o host e a rede na qual host pertence. (FARREL, 2005).

Cada máquina de uma rede TCP/IP possui um endereço IP, tal como 200.252.155.9. O endereço IP, às vezes chamado de *dotted quad*, é composto por quatro números separados por ponto, cada qual na faixa de 0 a 255. (KUROSE, 2006).

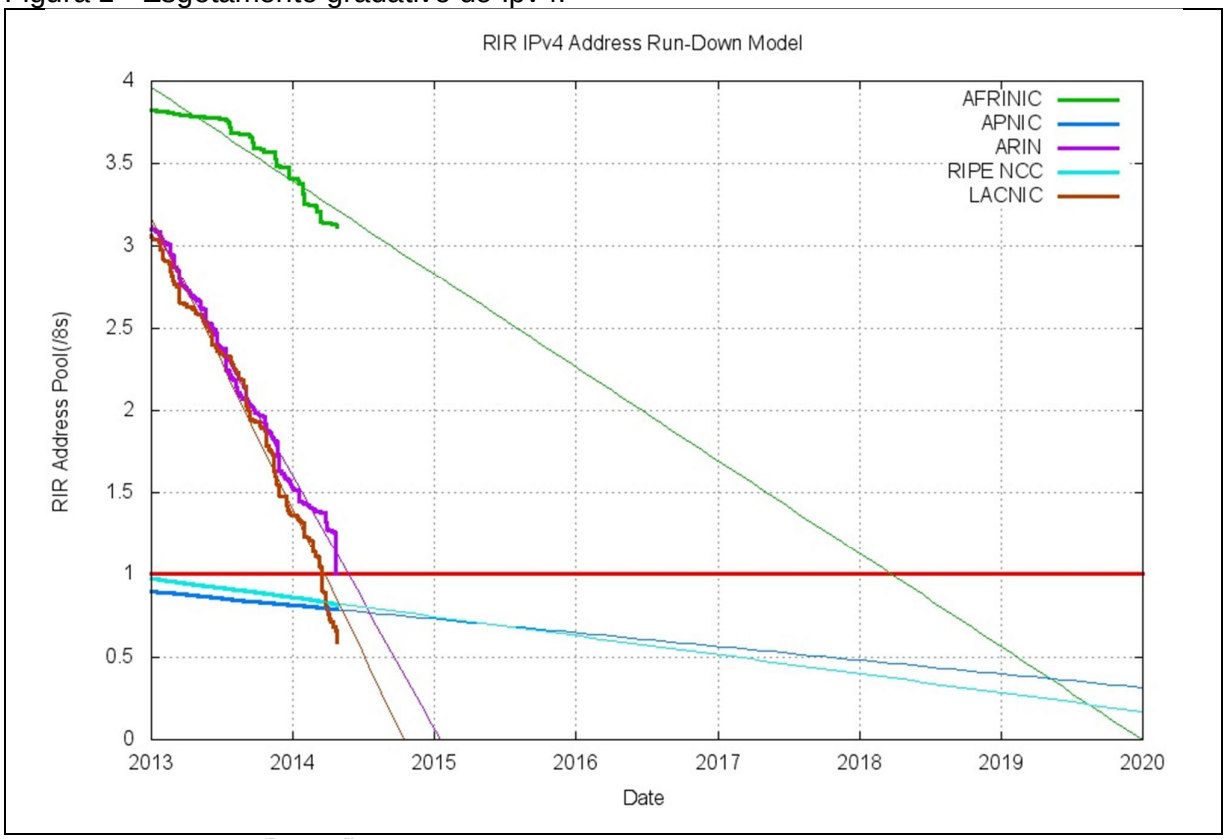
Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997. Diante desse cenário, a IETF (Internet Engineering Task Force) passa a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento, por esse motivo estão sendo utilizados alguns mecanismos, desde a década de 80, com a intencionalidade de se adiar o esgotamento dos endereços IPv4. (ROSS, 2006).

Alguns desses mecanismos são:

a) Network Address Translation (NAT): O NAT permite que com apenas um endereço válido na Internet, os computadores da rede interna tenham conexão com a Internet. Ele faz um mapeamento baseado no IP interno e na porta local do computador, gerando um número de 16 bits usando a tabela hash, posteriormente este número é utilizado no campo da porta de origem. O pacote que vai para a rede externa leva o IP do roteador e na porta de origem o número gerado pelo NAT, com isso o computador externo que receber o pacote sabe de onde ele veio, e envia a resposta novamente para o emissor;
b) Classless Inter Domain Routing (CIDR): Permite atribuir faixas de endereços de tamanhos variáveis, abolindo as classes de IP;
c) Variable Length Subnet Mask (VLSM): É um método que permite calcular sub redes, alocando somente os bits necessários da sub rede utilizando máscaras de tamanho variáveis. (ROSS, 2006).

No entanto, mesmo com todos esses mecanismos o esgotamento dos endereços IPv4 é inevitável. Segundo Antônio Moreiras, gerente de Projetos do Centro de Estudo e Pesquisas em Tecnologia de Redes, o esgotamento do protocolo IPv4 no Brasil deve ocorrer no primeiro semestre de 2014, já que os números de endereços de IPs disponíveis na versão quatro não são suficientes para atender a demanda atual da Internet, como mostra a figura 1, mostra o esgotamento do IPv4 no Brasil em meados de 2014 (representado pela linha marrom no gráfico), ocorrido oficialmente em 10 de Junho de 2014.

Figura 1 - Esgotamento gradativo do Ipv4.



Fonte: Esgotamento... ([2014?]).

O Registro Americano para Números da Internet é o Regional Internet Registry (ARIN), responsável pelas alocações de endereços para América do Norte, chegou ao último /8 IPv4 de seu estoque na última quarta-feira, 23 de abril 2014. Com isso, entraram em vigor regras mais restritas de alocação que implementam uma fila única de alocação e uma análise mais detalhada de todos os pedidos. Qualquer alocação maior que um /15 irá requerer aprovação da diretoria do ARIN. Esta é a última fase de alocação do ARIN.

No Registro de Endereços da Internet para a América Latina e o Caribe (LACNIC), as regras para as últimas alocações são um pouco diferentes, e a previsão para o esgotamento é para maio de 2014.

2.3 PROTOCOLO IPv6

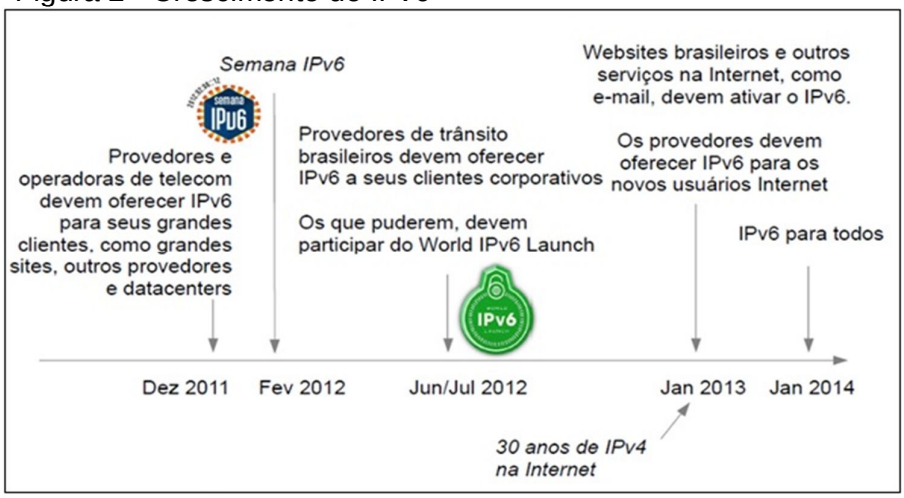
Esta versão do IP mantém a compatibilidade com a antiga versão (IPv4), uma vez que a transição está sendo feita gradativamente. A intenção do IPv6 é substituir

o IPv4, que suporta apenas cerca de 4 bilhões de endereços (4x109) , contra cerca de 3x1038 endereços da nova versão. (SANTOS, 2010).

A versão mais atual do IP, ou seja, a versão 6. Sua criação foi iniciada em 1994, por Scott Bradner e Allison Marken, após isto este protocolo já sofreu muitas mudanças e melhorias até os dias de hoje. (IPv6.BR, 2014).

Desde a criação do IPv6 foram feitas muitas modificações no protocolo, primeiramente foi testado em redes experimentais e após estar mais refinado, começou a ser utilizado em Provedores de Serviço, que passaram a utilizar o IPv6 em parte de suas redes. Empresas como Google, Facebook, Yahoo, Terra, IG já estão utilizam o IPv6. Provedores como a Global Crossing, da CTBC, e da Telefônica já fornecem trânsito IPv6 comercialmente no Brasil. A Figura 2 ilustra o crescimento do Ipv6 no setor comercial, a figura mostra o crescimento do IPv6 ao passar dos anos, e a adesão de provedores, operadoras, clientes até o ano de 2014.

Figura 2 - Crescimento do IPv6



Fonte: Esgotamento... ([2014?]).

Devido à importância desta nova versão do IP os governos tem apoiado esta implantação. (IPv6.BR, 2014).

O Projeto de Lei 2126/ 2011, referente ao Marco Civil da Internet no Brasil, sancionado no dia 24 de Abril de 2014, entrará em vigor no final de Junho desse mesmo ano. Dentre essas regulamentações governamentais, o Art. 2º no seu parágrafo V, se refere à segurança e funcionalidade da rede por meio de medidas técnicas compatíveis com os padrões internacionais, mostra um Estado vigilante e atual com as questões virtuais, ressaltando a importância da segurança cibernética,

no tópico 2.4 será abordado o IPSEC (Protocolo de segurança na internet) em consonância com o IPv6, que são ou se tornarão fundamentais para o cumprimento eficiente desse Projeto, no qual internautas e provedores encontraram um respaldo legal.(Poder Executivo, PL-2126/2011).

2.3.1 Comparativo entre os protocolos IPv4 x IPv6

A versão Ipv6 possui aprimoramentos se comparados com a anterior, tais como (Ipv6.br,2014):

- A nova versão do protocolo possui seu espaço de endereçamento de 128 bits, antes era composto somente de 32 bits;
- Faz a atribuição automática dos IPs em uma rede;
- Os cabeçalhos foram remodelados, para que o processo dos roteadores seja simplificado e de uma forma mais segura, também foram criados cabeçalhos de extensão, que podem guardar informações adicionais;
- Suporte a qualidade de serviço (QoS): Aplicações de áudio e vídeo passam a estabelecer conexões apropriadas tendo em conta as suas exigências em termos de qualidade de serviço;
- Várias extensões no IPv6 permitem as opções de segurança como encriptação, autenticação, integridade e confidencialidade dos dados.

Para implementação do Ipv6, foram analisadas as limitações do IPv4, a criação da RFC 1755 (PEREZ, 1995), que resume os requisitos para o IPv6, fizeram as devidas aprimorações.

2.3.2 Endereçamento

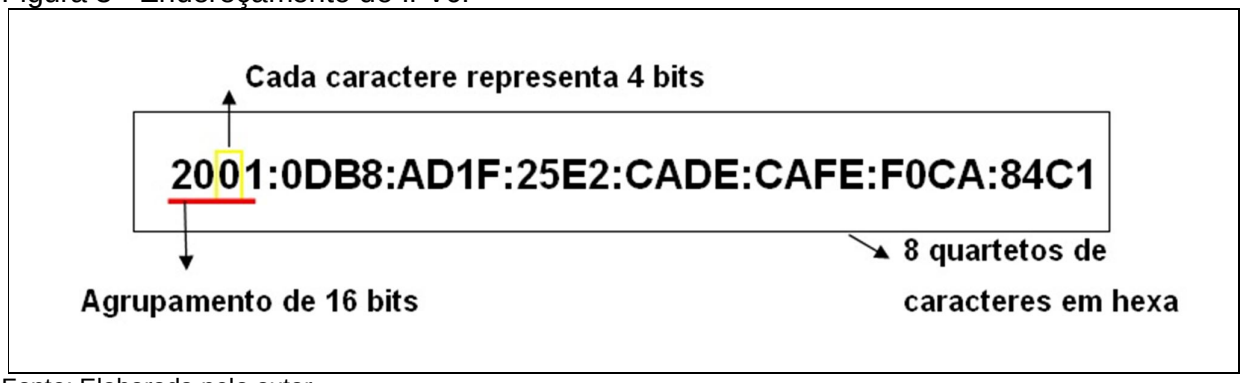
O IPv4 faz agrupamento de 8 em 8 bits, cada um representando um número de 0 a 255, por exemplo “206.44.30.230”, porém esta nomenclatura seria inviável para o IPv6, pois se teria 16 octetos, e os endereços ficariam muito extensos, por

exemplo “232.234.12.43.45.65.132.54.45.43.232.121.45.154.34.78” (FARREL, 2005).

O IPv6 dispõe de endereços de 128 bits, que permite um endereçamento flexível e um roteamento em blocos de grande escala. Nestes endereços a segurança é padronizada, sendo a camada de rede a responsável por isto.

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por”:”, escritos com dígitos hexadecimais (0-F), conforme ilustra figura 3:

Figura 3 - Endereçamento do IPv6.



Fonte: Elaborada pelo autor

Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos.

Além disso, 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 ":”.

Por exemplo, o endereço **2001:0DB8:0000:0000:130F:0000:0000:140B** pode ser escrito como **2001:DB8:0:0:130F::140B** ou **2001:DB8::130F:0:0:140B**. (BRITO, 2013)

Neste exemplo acima é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço. Se o endereço acima fosse escrito como **2001:DB8::130F::140B**, não seria possível determinar se ele corresponde a **2001:DB8:0:0:130F:0:0:140B**, a **2001:DB8:0:0:0:130F:0:140B** ou **2001:DB8:0:130F:0:0:0:140B**.

Esta abreviação pode ser feita também no fim ou no início do endereço, como ocorre em **2001:DB8:0:54:0:0:0:0** que pode ser escrito da forma **2001:DB8:0:54::** (BRITO, 2013).

2.3.2.1 Prefixos

Outra representação importante é a dos prefixos de rede. Em endereços IPv6 ela continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR.

Esta notação é representada da forma “endereço-IPv6/tamanho do prefixo”, onde “tamanho do prefixo” é um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreendem o prefixo. O exemplo de prefixo de sub rede apresentado na figura 4 indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub rede.

Figura 4 – Prefixo.

Fonte: Endereçamento... ([2014?]).

Esta representação também possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub rede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

Com relação à representação dos endereços IPv6 em URLs (Uniform Resource Locators), estes agora passam a ser representados entre colchetes. Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL. (BRITO, 2013).

Observe os exemplos a seguir, mostram diferentes formas de se usar o endereço IPv6 na barra de endereço.

http://**[2001:12ff:0:4::22]**/index.html
http://[2001:12ff:0:4::22**]:8080**

2.3.2.2 Endereçamento do IPv6

Há três tipos de endereços definidos no IPv6:

a) Unicast
b) Anycast
c) Multicast

2.3.2.2.1 Unicast

Os endereços unicast são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada, etc., e sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4. Este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface. (RICCI, 2007)

Tipos de Endereços Unicast:

a) Global Unicast: é o endereço unicast que será globalmente utilizado na Internet. Seu novo formato possui sete campos: o prefixo de 3 bits (001), um identificador TLA (Top-Level Aggregation), um campo RES reservado, um identificador NLA (Next-Level Aggregation), um identificador SLA (Site-Level Aggregation) e o identificador da interface, Similar aos endereços públicos do IPv4, o Global Unicast é Globalmente roteável e acessível na Internet;
b) Link Local: Faixa de Endereçamento FE80::/10: Deve ser utilizado apenas localmente, ou pode ser usado apenas no enlace específico onde à interface está conectada. Os roteadores não devem encaminhar para outros enlaces, pacotes que possuam como origem

ou destino um endereço link-local; É atribuído automaticamente (autoconfiguração stateless), usando o prefixo FE80::/64. (RICCI, 2007);

c) Unique-Local (ULA – Unique Local Address): Faixa de Endereçamento: FC00::/7, seguido de um ID global único de 40 bits gerado randomicamente. Utilizado apenas na comunicação dentro de um enlace ou entre um conjunto limitado de enlaces. Não deve ser roteável na Internet.

A diferença entre o ULA e o Link Local, é que o link local é atribuído automaticamente através da autoconfiguração stateless podendo ser utilizado somente por um enlace. (RICCI, 2007).

2.3.2.2.2 Anycast

Um endereço IPv6 anycast é utilizado para identificar um grupo de interfaces, porém, com a propriedade de que um pacote enviado a um endereço anycast é encaminhado apenas à interface do grupo mais próxima da origem do pacote.

Os endereços anycast são atribuídos a partir da faixa de endereços unicast e não há diferenças sintáticas entre eles. (Portanto, um endereço unicast atribuído a mais de uma interface transforma-se em um endereço anycast, devendo-se neste caso, configurar explicitamente os nós para que saibam que lhes foi atribuído um endereço anycast). (FARREL, 2005).

Este esquema de endereçamento pode ser utilizado para descobrir serviços na rede, como servidores DNS e proxies HTTP, garantindo a redundância desses serviços. Também pode-se utilizar para fazer balanceamento de carga em situações onde múltiplos hosts ou roteadores provem o mesmo serviço, para localizar roteadores que forneçam acesso a uma determinada sub rede ou para localizar os Agentes de Origem em redes com suporte a mobilidade IPv6.

Todos os roteadores devem ter suporte ao endereço anycast Subnet-Router. Este tipo de endereço é formado pelo prefixo da sub-rede e pelo IID preenchido com zeros (ex.: 2001:db8:cafe:dad0::/64). Um pacote enviado para o endereço Subnet-Router será entregue para o roteador mais próximo da origem dentro da mesma

sub-rede. Também foi definido um endereço anycast para ser utilizada no suporte a mobilidade IPv6. (FARREL, 2005).

2.3.2.2.3 Multicast

Endereços multicast são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo. Os pacotes enviados para esses endereços são entregues a todos as interfaces que compõe o grupo.

No IPv4, o suporte a multicast é opcional, já que foi introduzido apenas como uma extensão ao protocolo. Entretanto, no IPv6 é requerido que todos os nós suportem multicast, visto que muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço. (ALLEN, 1999).

Seu funcionamento é similar ao do broadcast, dado que um único pacote é enviado a vários hosts, diferenciando-se apenas pelo fato de que no broadcast o pacote é enviado a todos os hosts da rede, sem exceção, enquanto que no multicast apenas um grupo de hosts receberá esse pacote.

Deste modo, a possibilidade de transportar apenas uma cópia dos dados a todos os elementos do grupo, a partir de uma árvore de distribuição, pode reduzir a utilização de recurso de uma rede, bem como otimizar a entrega de dados aos hosts receptores. Aplicações como videoconferência, distribuição de vídeo sob demanda, atualizações de softwares e jogos on-line, são exemplos de serviços que vêm ganhando notoriedade e podem utilizar as vantagens apresentadas pelo multicast.

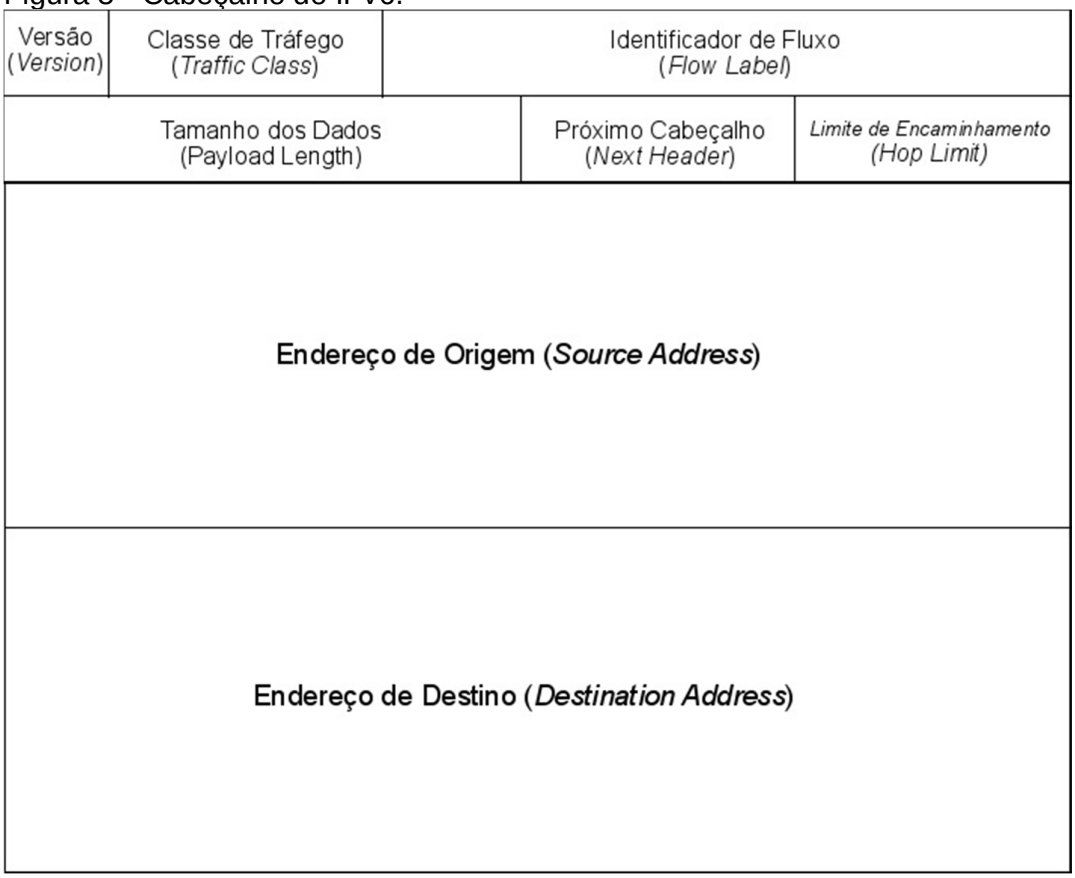
Os endereços multicast não devem ser utilizados como endereço de origem de um pacote. Esses endereços derivam do bloco FF00::/8, onde o prefixo FF, que identifica um endereço multicast, é precedido por quatro bits, que representam quatro flags, e um valor de quatro bits que define o escopo do grupo multicast. Os 112 bits restantes são utilizados para identificar o grupo multicast. (ALLEN, 1999).

2.3.3 Cabeçalhos do IPv6

Campos do Cabeçalho IPv6 (TANENBAUM, 2003), foram melhorados em relação ao Cabeçalho IPv4, como mostra a Figura 5 :

- Versão: Este campo possui 4 bits e identifica a versão do protocolo IP utilizado, sendo valorizado com 6, se estiver na versão IPv6;
- Classe de Tráfego: Este campo possui 8 bits onde os pacotes são identificados através da prioridade ou classe de serviços;
- Identificador de Fluxo: Este campo possui 20 bits e faz a diferenciação dos pacotes do mesmo fluxo de rede, permitindo que o roteador identifique o tipo de fluxo de cada pacote, sem verificar sua aplicação;
- Tamanho dos Dados: Este campo possui 16 bits, identifica o tamanho dos dados em bytes, enviados junto ao cabeçalho IPv6. Os cabeçalhos de extensão estão inclusos também neste cálculo;
- Próximo Cabeçalho: Este campo possui 8 bits e identifica o cabeçalho que segue ao cabeçalho IPv6, este campo não contém apenas valores referentes a outros protocolos, mas também indica os valores dos cabeçalhos de extensão;
- Limite de Encaminhamento: Este campo possui 8 bits onde sua função é indicar o número máximo de roteadores que o pacote IPv6 pode passar antes de ser descartado;
- Endereço de Origem: Este campo possui 128 bits e indica o endereço de origem do pacote;
- Endereço de Destino: Este campo possui 128 bits e indica o endereço de destino do pacote.

Figura 5 - Cabeçalho do IPv6.



Fonte: Cabeçalho ([2014?]).

Algumas mudanças foram realizadas no formato do cabeçalho base do IPv6 de modo a torná-lo mais simples. O número de campos foi reduzido para apenas oito e o tamanho foi fixado de 40 Bytes. Além disso, ele ficou mais flexível e eficiente com a adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários. (SOUSA, 2009).

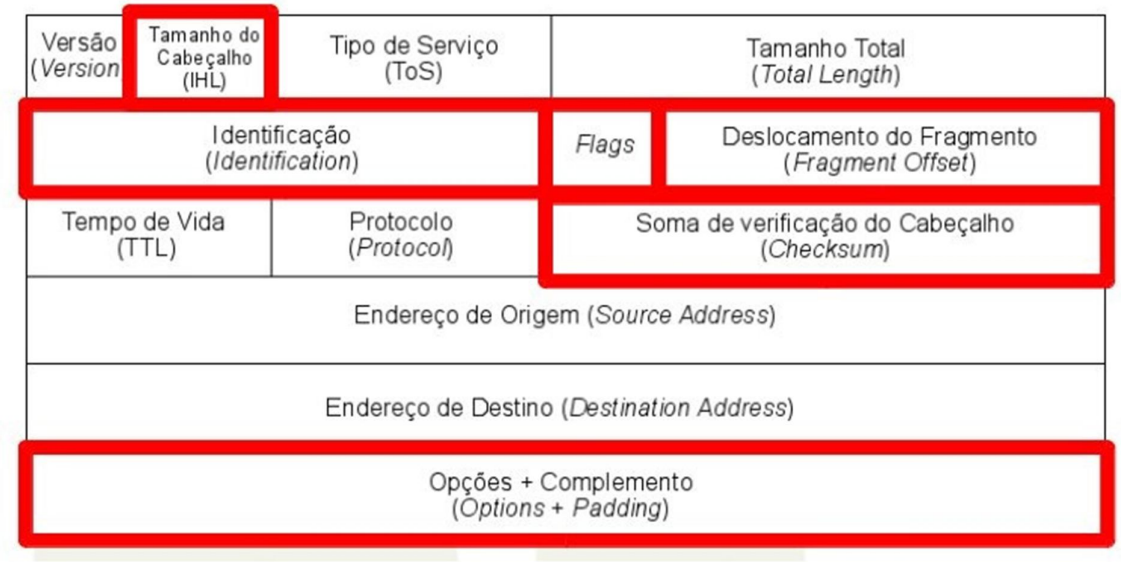
Tais alterações permitiram que, mesmo com um espaço de endereçamento quatro vezes maior que o do IPv4, o tamanho total do cabeçalho IPv6 fosse apenas duas vezes.

Dentre essas mudanças, destaca-se a remoção de seis dos campos existentes cabeçalho IPv4, como resultado tanto da inutilização de suas funções quanto de sua reimplantação com o uso de cabeçalhos de extensão. A figura 6 identifica esses campos.

A primeira remoção foi a do campo “Tamanho do Cabeçalho” que se tornou desnecessário uma vez que seu valor foi fixado. A seguir, os campos “Identificação”, “Flags”, “Deslocamento do Fragmento” e “Opções e Complementos” passaram a ter

suas informações indicadas em cabeçalhos de extensão apropriados. Por fim, o campo ”Soma de Verificação” foi descartado com o objetivo de deixar o protocolo mais eficiente já que outras validações são realizadas pelos protocolos das camadas superiores da rede. (SOUSA, 2009).

Figura 6 - Alterações no IPv4.



Fonte: Cabeçalho ([2014?]).

Outra alteração realizada com o intuito de agilizar o processamento foi a renomeação e reposicionamento de quatro campos, conforme a figura 7, mostra as alterações dos nomes dos cabeçalhos entre IPv4 e IPv6:

Figura 7 - Alteração entre os protocolos

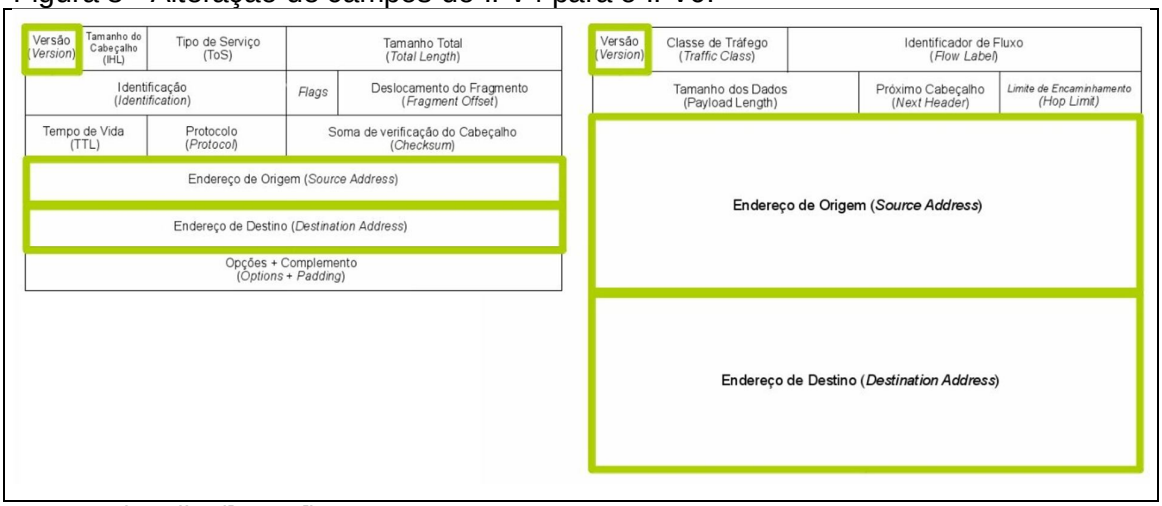
IPv4	IPv6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho dos Dados
Tempo de Vida (TTL)	Limite de encaminhamento
Protocolo	Próximo Cabeçalho

Fonte: Cabeçalho ([2014?]).

Além disso, o campo “Identificador de Fluxo” foi adicionado para possibilitar o funcionamento de um mecanismo extra de suporte a QoS (Quality of Service). Mais detalhes sobre este campo e mecanismo serão apresentados nas próximas seções.

Por fim, os campos “Versão”, “Endereço de Origem” e “Endereço de Destino” foram mantidos e apenas tiveram seus tamanhos alterados conforme ilustra a Figura 8.

Figura 8 - Alteração de campos do IPv4 para o IPv6.

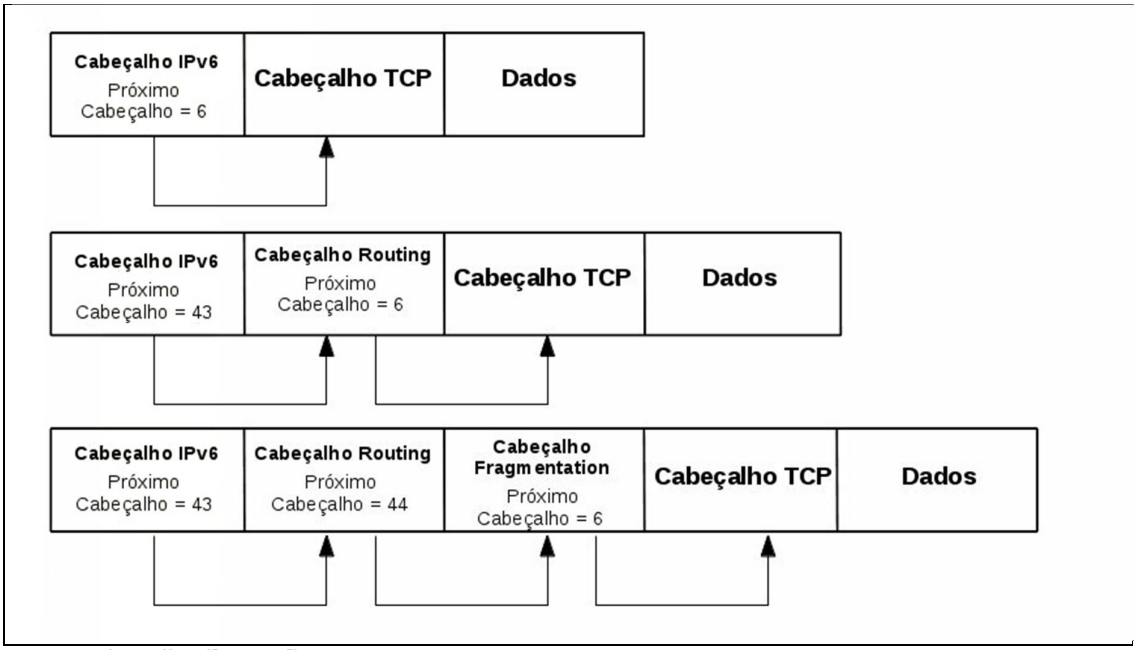


Fonte: Cabeçalho ([2014?]).

2.3.3.1 Cabeçalhos de Extensão

Diferente do IPv4, que inclui no cabeçalho base todas as informações opcionais, o IPv6 trata essas informações através de cabeçalhos de extensão. Estes localizam-se entre o cabeçalho base e o cabeçalho da camada de imediatamente acima e, não possuem quantidade ou tamanho fixo. Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão adicionados em série formando uma “cadeia de cabeçalhos”. A Figura 9 exemplifica essa situação.

Figura 9 - Cabeçalho de extensão IPv6.



Fonte: Cabeçalho ([2014?]).

As especificações do IPv6 definem seis cabeçalhos de extensão:

a) hop-by-Hop Options (Opções de Salto-a-Salto);
b) destination Options (Opções de Destino);
c) routing (Rota de Origem);
d) fragmentation (Fragmentação);
e) authentication Header (Autenticação);
f) encapsulating Security Payload (Encapsulamento seguro).

A criação dos cabeçalhos de extensão do IPv6 teve a finalidade de aumentar a velocidade de processamento nos roteadores, visto que o único que deve ser processado em cada roteador é o Hop-by-Hop, enquanto que os demais são tratados apenas pelo nó de destino. Além disso, novos cabeçalhos podem ser definidos no protocolo sem a necessidade alterações no cabeçalho base. (SANTOS, 2010).

Considerando a linha de pesquisa desse trabalho, cujo foco é a segurança, serão explicados apenas os cabeçalhos Authentication Header e Encapsulating Security Payload:

- Authentication Header: Identificado pelo valor 51 no campo Próximo Cabeçalho, é utilizado pelo IPSec para que os pacotes tenham autenticação e garantia de integridade dos dados.
- Encapsulating Security Payload: Identificado pelo valor 52 no campo Próximo Cabeçalho, é utilizado pelo IPSec para que os pacotes tenham integridade e confidencialidade dos dados. (SANTOS, 2010).

A Figura 10 demonstra as diferenças entre os cabeçalhos do protocolo IPv4 e o IPv6:

Figura 10 - Diferenças e equivalências entre o cabeçalho IPv4 e IPv6.

Campos do Cabeçalho IPv4	**Campos do Cabeçalho IPv6**
Version	Mesmo campo, porém informa versão diferente.
IHL – Internet Header Length	Campo removido no IPv6. O IPv6 não inclui o IHL porque o seu cabeçalho básico é sempre de tamanho fixo, 40 bytes. Cada cabeçalho de extensão também possui tamanho fixo ou seu tamanho é indicado.
TOS – Type of Service	Substituído pelo campo Traffic Class – Classe de Tráfego.
Total Length	Substituído pelo campo Payload Length, que apenas indica o tamanho do payload.
Identification Fragmentation Flags Fragment Offset	Campos removidos no IPv6. Informações de fragmentação estão contidos no cabeçalho de extensão correspondente a fragmentação.
TTL – Time to Live	Substituído pelo campo Hop Limit.
Protocol	Substituído pelo campo Next Header
Header Checksum	Campo removido no IPv6. A detecção de erros é feita para todo o pacote e é executado pela camada de link.
Source Address	Mesmo campo, porém com tamanho maior, 128 bits.
Destination Address	Mesmo campo, porém com o tamanho de 128 bits.
Options	Campo removido no IPv6. Este campo foi substituído pelos cabeçalhos de extensão.

Fonte: Davies (2004).

2.4 IPSEC

O quesito segurança sempre foi muito discutido e analisado, desde a criação do IPv6 , mecanismos de segurança passam a fazer parte do protocolo IPv6, sendo que qualquer par de dispositivos de uma conexão fim-a-fim possam se manter

seguros, com métodos que visam garantir a segurança dos dados que trafegam pela rede.

Com a utilização cada vez maior da Internet para meios comerciais e transações que envolvem compras, vendas transferências de informações importantes ou valores em dinheiro é cada vez mais necessário que a rede tenha segurança. Para isto utilizam-se métodos para ajudar nesta proteção, tais como, firewalls, antivírus, segurança no acesso a web com Secure Socket Layer (SSL - RFC 2246. (DIERKS; ALLEN,1999).

A melhor alternativa para a segurança em nível de aplicação é fornecida na camada de rede, onde todo o conteúdo dos pacotes IP, e mesmo os próprios cabeçalhos IP, são protegidos. Essa solução apresenta muitas vantagens. Ela está disponível para todo o tráfego IP entre qualquer par de lados e, portanto, é útil para proteger dados de aplicações e também pode ser usada para proteger trocas de roteamento e sinalização. O IPSEC é à base da segurança em nível de rede. Ele é usado para autenticar o emissor das mensagens, para verificar se os dados da mensagem não foram adulterados e para ocultar informações de olhos não autorizados. (FARREL, 2005).

Em suma, o IPSEC é uma especificação de segurança que está incorporado ao IPv6, utilizando os cabeçalhos de extensão AH e ESP para seu funcionamento.
No IPSEC a criptografia e autenticação de pacotes são feitas na camada de rede, fornecendo assim uma solução de segurança fim-a-fim, garantindo a integridade, confidencialidade e autenticidade dos dados.

No IPv6 o seu suporte é obrigatório, já com seus principais elementos integrado, facilitando sua utilização .No IPv4 ele foi adaptado para funcionar, sendo opcional a sua utilização.

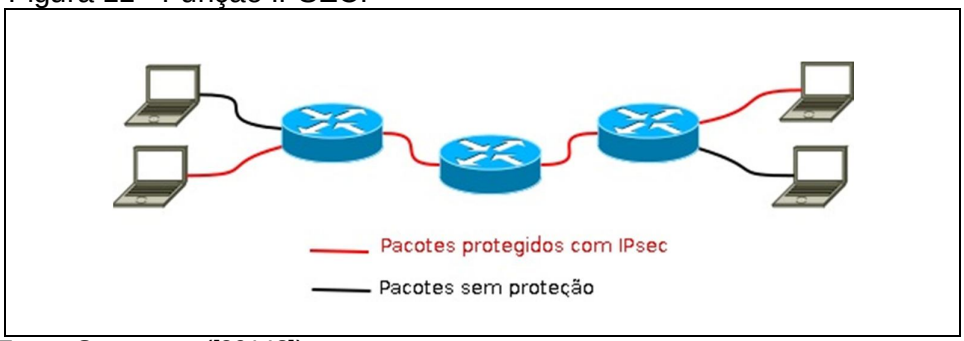
2.4.1 Arquitetura de segurança do IPSEC

A arquitetura do IPSEC foi originalmente especificada na RFC2401 em 1998 e posteriormente atualizada pela RFC4301 em 2005. (SILVA, 2005).

Existem duas formas distintas de utilização do IPSEC, em Modo Transporte ou
Modo Túnel.

Modo de transporte: No modo transporte, o emissor e receptor da comunicação segura necessitam de suporte ao IPSEC, conforme a Figura 11.

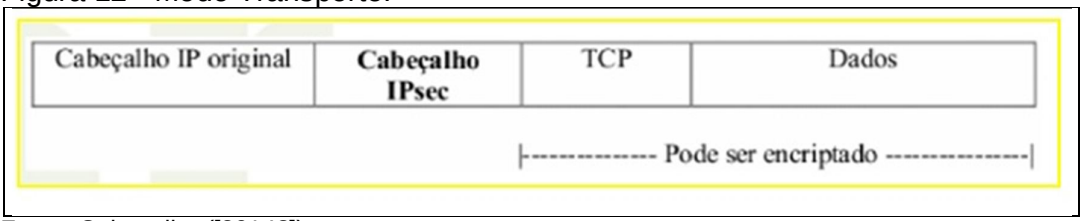
Figura 11 - Função IPSEC.



Fonte: Segurança ([2014?]).

Neste modo o cabeçalho IP mantém-se original, protegendo apenas os cabeçalhos superiores, pois o cabeçalho IPSEC é adicionado imediatamente após o Cabeçalho IP, e antes dos cabeçalhos dos protocolos das camadas superiores, conforme Figura 12:

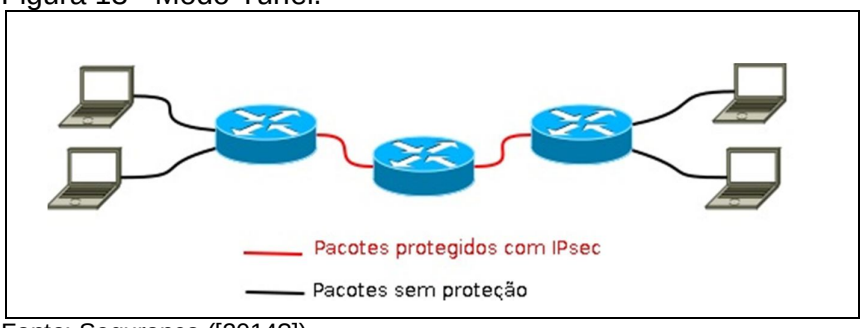
Figura 12 - Modo Transporte.



Fonte: Cabeçalho ([2014?]).

Modo de tunelamento: No Modo Túnel (conhecido por Virtual Private Network - VPN) é protegido o pacote IP inteiro, onde todo o pacote é encapsulado dentro de outro pacote IP, após isto é criado um cabeçalho IP externo, que fica visível, tornando possível a ligação entre o dispositivo emissor com o receptor do túnel. Ao invés de configurar todos os dispositivos para utilizar IPSEC, esta configuração é feita somente nos roteadores de borda que encapsulam o pacote original, ao chegar ao roteador de borda do destino o pacote é descapsulado, como mostra a Figura 13.

Figura 13 - Modo Túnel.



Fonte: Segurança ([2014?]).

2.4.2 Especificação de segurança

- Autenticidade: Garante a prova da identidade dos objetos, ou seja, fazer com que usuários ou sistema provem que são realmente quem alegam ser. (RICCI, 2007).
- Confidencialidade: Processo que objetiva manter dados escondidos de pessoas não autorizadas. (RICCI, 2007). Quando o modo ESP do IPSEC é utilizado está se garantindo a confidencialidade na transmissão de dados.
- Integridade: Consiste no processo de garantir que dados transmitidos não tenham sido alterados durante sua transmissão de um ponto A até um ponto B. (RICCI, 2007).

  O modo AH garante a autenticidade e integridade.

2.4.3 Associação de segurança

A crescente capacidade do IPSEC está relacionada ao estabelecimento dinâmico de SAs (associações de segurança) que devem ser definidas por conexão ou, no máximo, por usuário, para prover maior segurança.

Uma associação de segurança (SA) é uma comunicação segura, protegida com IPSEC, entre duas máquinas. Para que duas entidades consigam enviar e receber pacotes utilizando o IPSEC é necessário o estabelecimento de SA, que determinam os algoritmos a redes usados, as chaves de criptografia e o tempo de vida das mesmas, entre outros parâmetros, definindo a política de segurança (SPD) e regras para envio e recebimento de pacotes IP. (SILVA, 2005).

Formas de SA:

a) estática: os parâmetros são inseridos manualmente no ponto de origem e destino da comunicação;
b) dinâmica: os parâmetros são gerenciados por protocolos como o IKE, não necessita da manipulação do administrador.

2.4.4 Gerenciamento de chaves

Como os serviços de segurança IPSEC compartilham chaves secretas que são utilizadas para autenticação, integridade e criptografia, as especificações IPSEC definem um conjunto separado de mecanismos para o gerenciamento de chaves, com suporte para distribuição automática ou manual das chaves. Para distribuição manual e automática das chaves foram especificados procedimentos baseados em chaves públicas, sendo possível utilizar Internet Security Association e Key Management Protocol (ISAKMP/OAKLEY). O ISAKMP define o método de distribuição de chave e o OAKLEY define como as chaves serão determinadas (SILVA, 2005). Ou seja, O protocolo IKE trabalha em duas fases:

a) **Fase 1**: a autenticidade dos dispositivos é verificada, através de uma série de mensagens trocadas, e uma chave ISAKMP SA (Internet Security Association Key Management Security Association) é gerada
b) **Fase 2**: a partir da ISAKMP SA as chaves para o AH e ESP para esta comunicação são geradas e o IPSEC começa a ser utilizado.

Descrito na RFC 2409, o Internet Key Exchange consiste no padrão criado pela IETF responsável por especificar uma metodologia segura para a troca de chaves entre duas pontas, visando fazer com que essas se autentiquem entre si e entrem em acordo quando ao meio utilizado para assegurar dados transmitidos, ou seja, este protocolo é utilizado entre junto a duas pontas IPSec para que essas estabeleçam uma relação de confiança entre si antes de transmitirem dados confidenciais (RICCI, 2007).

2.4.5 Frameworks de Segurança do IPSEC (AH e ESP)

Os Frameworks são estruturas de suporte definidas em que outro projeto de software pode ser organizado e desenvolvido. Um framework pode incluir programas de suporte, bibliotecas de código, linguagens de script e outros softwares para auxiliar no desenvolvimento e unir diferentes componentes de um projeto de software.

Os Frameworks de segurança utilizam recursos independentes para realizar suas funções. O IPSEC suporta alguns algoritmos pré-definidos, que podem ser alterados ao longo do tempo, de acordo com a sua maturação e necessidades. Hoje a lista de algoritmos disponíveis, não necessariamente implementados por todos os fornecedores de IPSec, inclui:

a) Criptografia: o Data Encryption Standard (DES): É um algoritmo matemático para criptografar e descriptografar informações em código binário. Usa uma chave de 64 bits mínima, da qual 56 bits estão disponíveis para definir a chave propriamente dita, e 8 bits são usados para fornecer detecção de erro na chave. (FARREL, 2005);
b) 3-DES: O Triplo DES, sigla para Triple Data Encryption Standard é um padrão de criptografia baseado no algoritmo de criptografia DES desenvolvido pela IBM em 1974 e adotado como padrão em 1977. 3-DES usa 3 chaves de 64 bits (o tamanho máximo da chave é de 192 bits, embora o comprimento atual seja de 56 bits). Os dados são encriptados com a primeira chave, decrepitado com a segunda chave e finalmente encriptados novamente com a terceira chave. Isto faz do 3-DES ser mais lento que o DES original, mas oferece maior segurança. Em vez de 3 chaves, podem ser utilizadas apenas 2, fazendo-se K1 =K3. (TANENBAUM, 2003);
c) AES: O AES é basicamente uma cifra de substituição mono alfabética que utiliza caracteres grandes (128 bits para AES). Sempre que o mesmo bloco de texto simples chega ao front end, o mesmo bloco de texto cifrado sai pelo back end. Se codificar o texto simples abcdefgh 100 vezes com a mesma chave DES, você obterá o mesmo texto cifrado 100 vezes. Um intruso pode explorar essa propriedade para ajudar a subverter a cifra. (TANENBAUM, 2003);
d) Autenticação:

- HMAC: Mecanismo de autenticação mensagem utilizando funções criptográficas hash. HMAC pode ser usado com qualquer função hash, por exemplo, MD5, SHA-1, em combinação com uma chave secreta compartilhada. A força de criptografia HMAC depende das propriedades do subjacente função hash (KRAWCZYK; BELLARE; CANETTI, 1997).
- SHA1, 2 e 3: Utiliza uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. As versões 2 e 3 tiveram melhoramentos na segurança (TANENBAUM, 2003).
- MD5: Produz um código de autenticação de 16 bytes (a síntese de mensagem) a partir dos dados de qualquer tamanho com ou sem uma chave de qualquer tamanho. Sem uma chave, o MD5 pode ser usado para detectar mudanças acidentais nos dados. Ele pode ser aplicado mensagens individuais, estruturas de dados ou arquivos inteiros (FARREL, 2005).

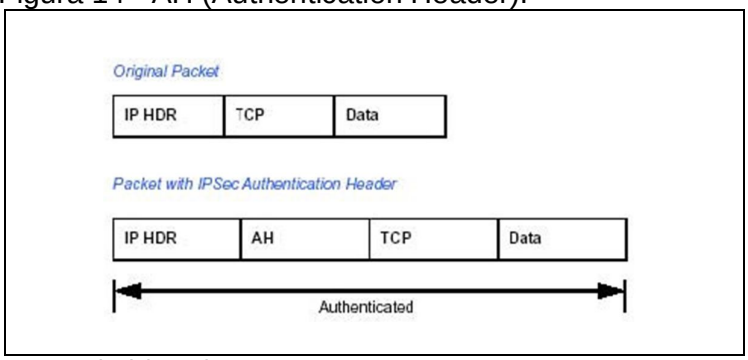
2.4.5.1 AH (Authentication Header)

Faz com que haja a autenticação da origem do pacote, evitando que pacotes sejam reenviados, e fornecendo a integridade dos dados de todo o pacote, garantindo assim que a origem e o destino e os dados não foram alterados durante o seu tráfego na Internet.

Apesar de garantir a integridade do pacote, ele não garante a confidencialidade dos dados, ou seja, não possui recurso de criptografia, então caso ele seja capturado ao longo da transmissão, os dados do pacote poderão ser capturados e visualizados indevidamente.

Para seu funcionamento, o cabeçalho AH é adicionado após os cabeçalhos Hop-by-Hop, Routing e Fragmentation. Pode ser utilizado com o modo de operação Transporte ou Túnel, como ilustrado na Figura 14.

Figura 14 - AH (Authentication Header).



Fonte: Ricci (2007).

O Cabeçalho AH contém seis campos (SILVA, 2005):

a) Próximo Cabeçalho (IP HDR): Contém o identificador do protocolo do protocolo do próximo cabeçalho. É o mesmo valor atribuído ao campo
b) Protocolo no cabeçalho IP original.
c) Tamanho do Dado: Comprimento do cabeçalho de autenticação e não o comprimento do dado, como pode ser confundido com o nome do campo.
d) Reservado: 16 bits reservados para extensão do protocolo.
e) SPI (Security Parameter Index): Este índice, em conjunto com o protocolo AH e o endereço fonte, indica unicamente uma SA para um determinado pacote.
f) Número de Sequência: Contador que identifica os pacotes pertencentes a uma determinada SA.
g) Dados de Autenticação: Campo de comprimento variável que contém ICV (Integrity Check Value) para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela SA.

Nem todos os campos podem ser autenticados, mesmo a autenticação acontecendo no pacote IP, pois existem alguns campos variáveis ou mutantes do cabeçalho que serão alterados no decorrer da transmissão. O mecanismo de autenticação é feito utilizando a função hash, utilizando a chave negociada durante o processo de estabelecimento da SA. (BRITO, 2013).

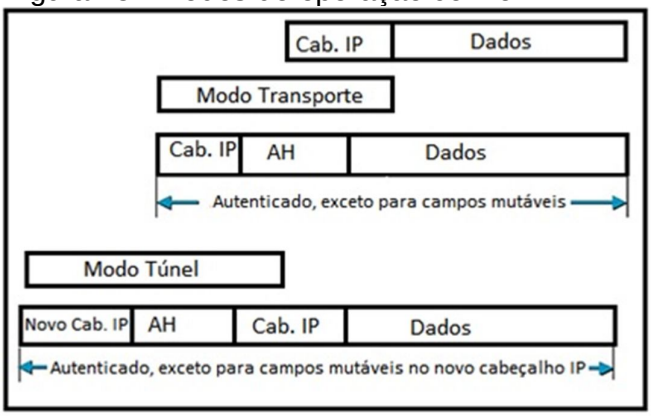
2.4.5.1.1 Authentication Header (AH) em Modo de operação Transporte

Com este modo de operação, o endereço IP de origem é mantido e autenticado, não podendo ser modificado por um roteador. Não permite a tradução de endereços NAT.

2.4.5.1.2 Authentication Header (AH) em Modo de operação Túnel

Com este modo de operação, os endereços IP do gateway e a fonte serão autenticados, não permitindo esconder o endereço IP da rede local. Não permite a tradução de endereços NAT, conforme Figura 15.

Figura 15 - Modos de operação com o AH.



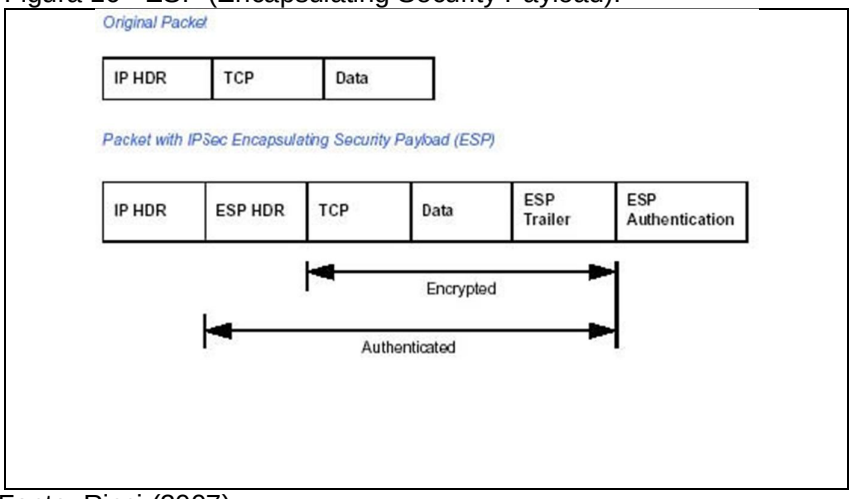
Fonte: Manson (2011).

2.4.5.2 ESP (Encapsulating Security Payload)

É um cabeçalho que garante a autenticação, confidencialidade e integridade dos pacotes, evita que os pacotes sejam reenviados, podendo criptografar os dados.

Assim os dados trafegados pela Internet não foram alterados, além de tornar estes ilegíveis através da utilização de criptografia. Está localizado entre o cabeçalho IP e o resto do datagrama. Assim, os campos de dados são alterados após a criptografia dos mesmos. Cada pacote deve conter informações necessárias para estabelecer o sincronismo da criptografia, permitindo que a de criptografia ocorra na entidade de destino. Uma situação possível de acontecer é não utilizar nenhum algoritmo de criptografia, neste caso o protocolo ESP só oferecerá o serviço de autenticação. Pode ser utilizado com o modo de operação Transporte ou Túnel.

Figura 16 - ESP (Encapsulating Security Payload).



Fonte: Ricci (2007).

Assim como no protocolo AH, alguns campos são inseridos no pacote IP para adicionar os serviços necessários. Os campos estão contidos no Cabeçalho ESP, outros no final do pacote e outros campos no segmento de autenticação, como mostrado na Figura 16.

Como se pode perceber o pacote resultante será maior do que o original, Este acréscimo é um ponto a ser analisado, uma vez que o tamanho máximo do pacote normalmente PE de 1.500 bytes (MTU – Maximun Transmition Unit). Este tamanho pode não ser suficiente para comportar o pacote resultante, o que irá acarretar em sua fragmentação. Neste caso, todo o processo acontece somente no pacote não fragmentado, ou seja, caso o pacote original não comporte os bytes adicionais, este deve ser fragmentado antes do processamento, e cabe ao gateway que irá receber o pacote de criptografar as informações e remontá-lo antes de deixá-lo continuar dentro da rede destino. (SILVA, 2005).

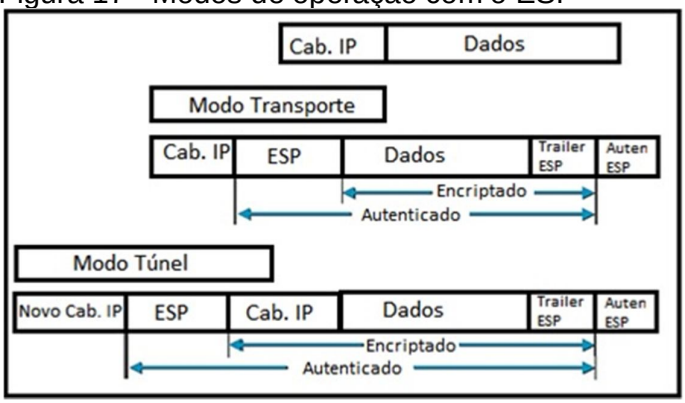
2.4.5.2.1 ESP em Modo de Operação Transporte

Com este modo de operação, o endereço IP de origem não é autenticado. Apenas os dados são autenticados. O roteamento de pacotes é possível, permitindo a tradução de endereços NAT.

2.4.5.2.2 ESP em Modo de Operação Túnel

Com este modo de operação, o endereço IP de origem é criptografado com os dados. Apenas o destino pode conhecê-lo. Como no modo de transporte, o novo cabeçalho IP não é autenticado, o que permite a tradução endereços NAT. Podemos utilizar os cabeçalhos AH e ESP de forma paralela, como mostra a Figura 17. (MANSON, 2011).

Figura 17 - Modos de operação com o ESP



Fonte: Manson (2011).

3 METODOLOGIA

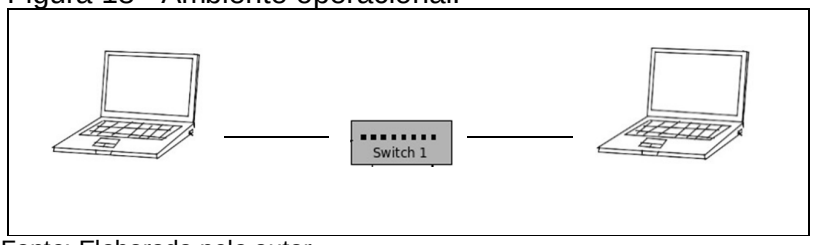
A metodologia adotada para a realização deste trabalho, reflete as etapas utilizadas para configurar um ambiente operacional de testes, para a implementação de IPv6 integrado com o IPSEC.

3.1 HARDWARE

Para o desenvolvimento desse trabalho, foi montado um cenário composto por dois notebooks Dell Inspiron 14r Core I3, 4 GB de memória RAM, com placa de rede 100 Mbps, essa configuração de hardware foi pensada para a instalação de um programa para virtualizar sistemas operacionais, pois com o programa de virtualização iniciado se divide o processador e a memória RAM entre a máquina física e a máquina virtual, com isso, esse hardware suportou o programa de virtualização muito bem, sem nenhuma lentidão que pudesse interferir nos testes. Os dois notebooks utilizam o sistema operacional Windows 7 Ultimate 64 bits.

Foi utilizado um Switch Netgear 8 portas 100MBs para a comunicação entre as máquinas, como mostra a Figura 18.

Figura 18 - Ambiente operacional.



Fonte: Elaborada pelo autor.

3.2 SOFTWARE

O software de virtualização utilizado foi o Oracle VM VirtualBox 4.3, e o sistema operacional virtualizado utilizado foi Linux Ubuntu 14.04 32 bits, no Linux foram instalados diversos pacotes e programas para realização dos testes, descritos abaixo.

a) O Pacote IPsec: Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPsec) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja o mesmo da origem) e autenticidade das informações ou prevenção de identity spoofing (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet.
b) Wireshark: É um software para análise de pacotes que recebe contribuições de especialistas em rede de todo o mundo. Ele foi usado para analisar os pacotes sem criptografia, com criptografia ESP, AH e ESP/AH, e também foi usado para medir o tamanho dos pacotes.
c) Open Secure Shell (SSH): Esse pacote foi utilizado nos testes de desempenho, onde possui um comando chamado SCP que possibilita a cópia de arquivos de uma máquina para outra, para a transferência de arquivos em IPv6, foi usado Colchetes ([ ]) em torno do IPv6.

3.3 MÉTODO

Na primeira etapa foi realizado um estudo teórico sobre o protocolo IPv6, verificando o seu funcionamento e formas de realizar a sua configuração. Em um segundo momento foi estudado as formas de segurança do IPSEC.

Depois de realizados os estudos, foram analisadas as ferramentas para realização da configuração do IPSEC. Logo em seguida sucederam os testes de configuração do IPv6 e do IPSEC, seguidos de testes de desempenho do funcionamento do IPSEC em conjunto com o IPv6.

3.3.1 Configuração do IPv6

Fase 1 - No computador 1 foi utilizado o IP ff:1111::f1 e no computador 2 foi utilizado o IP ff:1111::f2, devido sua facilidade para testes laboratoriais, utilizando

uma rede privada, conforme demonstrado na Figura 19, sendo o eth0 a placa de rede utilizada a qual foi adicionado o IPv6 nas duas máquinas.

Figura 19 – Comando para visualizar o IP configurado em cada máquina.

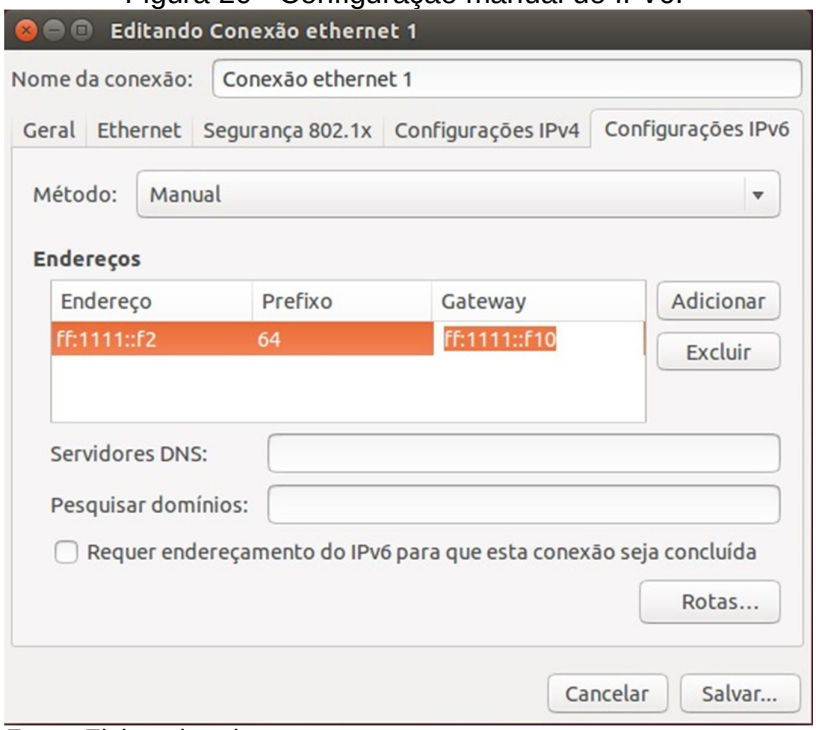
```
ifconfig # no computador 1

ifconfig # no computador 2
```

Fonte: Elaborada pelo autor.

A rede em IPv6 foi configurado de forma manualmente no Linux Ubuntu, editando suas propriedades de redes, conforme a figura 20.

Figura 20 - Configuração manual do IPv6.

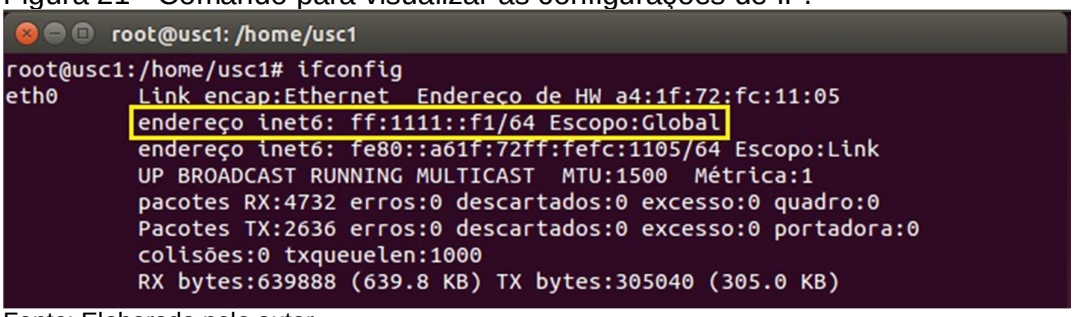


Fonte: Elaborada pelo autor.

Esse modo de configuração do IP garante que mesmo que os computadores sejam desligados as configurações se mantenham a mesmas, evitando ter que refaze-las.

Para visualizar as configurações de IP, foi digitado o comando da figura 19 no terminal do Linux, conforme demonstrado Figura 21.

Figura 21 - Comando para visualizar as configurações de IP.

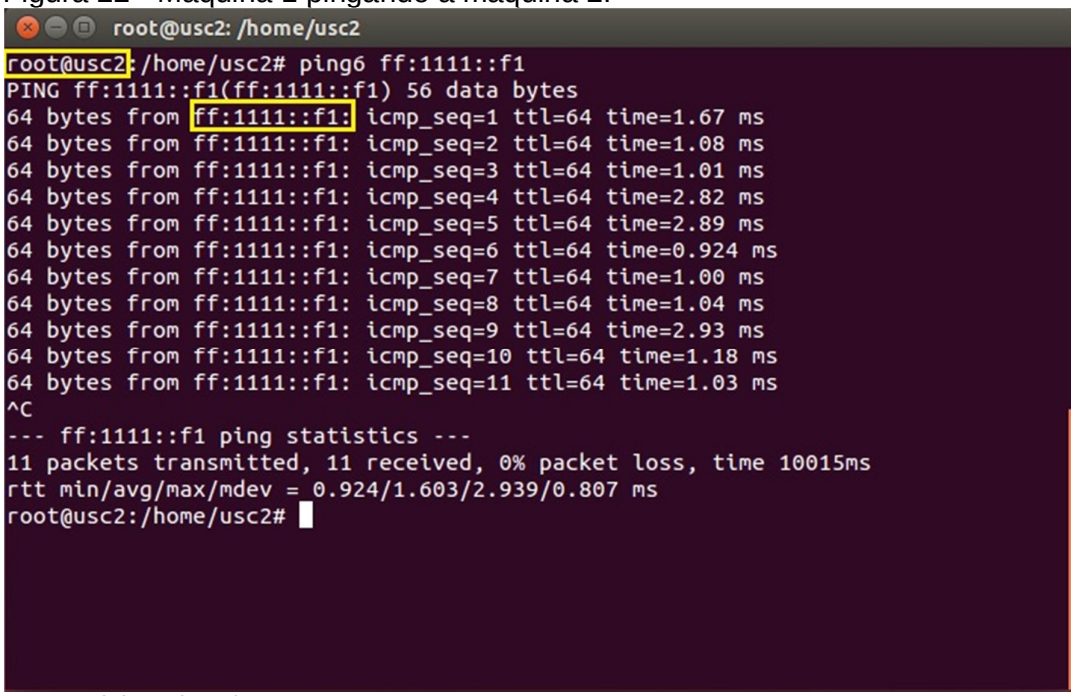


Fonte: Elaborada pelo autor.

Fase 2 - Comunicação entre as máquinas.

O comando “ping6” foi usado para verificar a comunicação entre as maquinas, conforme Figura 22.

Figura 22 - Máquina 1 pingando a máquina 2.



Fonte: Elaborada pelo autor.

Fase 3 - Após a conclusão das fases 1 e 2, foi realizado a instalação do pacote de segurança IPSEC, esse pacote fornece filtragem de tráfego, que é necessário para negociar à segurança dos pacotes. Conforme a Figura 23.

.

Figura 23 - Instalando IPSE.

```
# apt-get install ipsec-tools
```

Fonte: Elaborada pelo autor.

3.3.2 Configuração do ipsec-tools

Após a instalação do pacote IPSEC, foi necessário editar suas configurações, no arquivo que se encontra no diretório /etc/ipsec-tools.conf, nele é possível realizar as configurações de criptografia (Sem Criptografia, ESP, AH e AH+ESP).
Para verificar a configuração em que se encontra o IPSEC, foi utilizado o comando da Figura 24, em todos os modos (AH, ESP e AH+ESP).

Figura 24 - Comando para verificar o status das configurações do IPSEC.

```
# setkey –PD
```

Fonte: Elaborada pelo autor.

3.3.2.1 Modo ESP (Modo Transporte):

Todos os passos a seguir foram realizados nas duas máquinas, utilizando o usuário root (máquina 1 e máquina 2):

É necessário gerar as chaves de criptografia para cada máquina, no terminal conforme ilustrado na Figura 25.

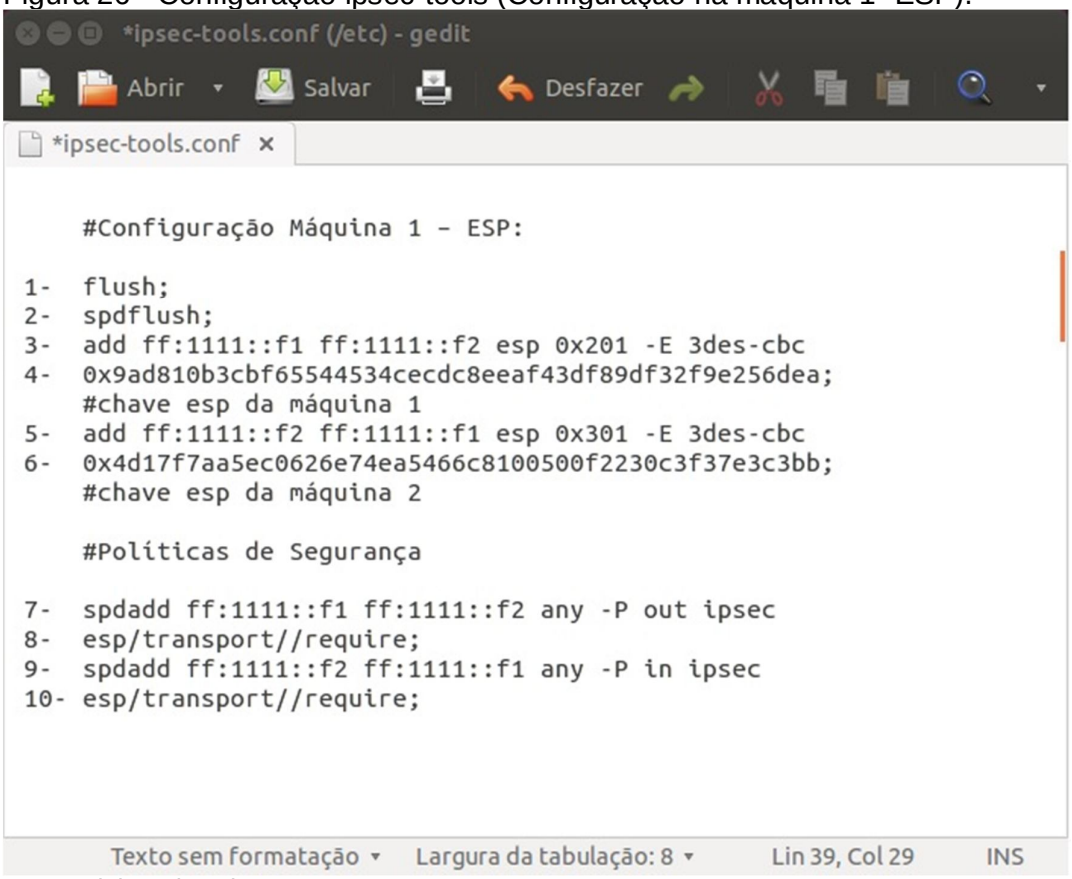
Figura 25 - Gerar chave ESP.

```
# dd if =/dev/random count=24 bs=1 | xxd –ps
```

Fonte: Elaborada pelo autor.

Cada chave será única, para cada máquina, sendo necessária a inclusão no arquivo ipsec-tools*.conf*, sendo prescrita a inclusão do termo “0x” no início da chave, indicando que é uma chave em hexadecimal, como mostra a Figura 26.

Figura 26 - Configuração ipsec-tools (Configuração na máquina 1- ESP).



Fonte: Elaborada pelo autor.

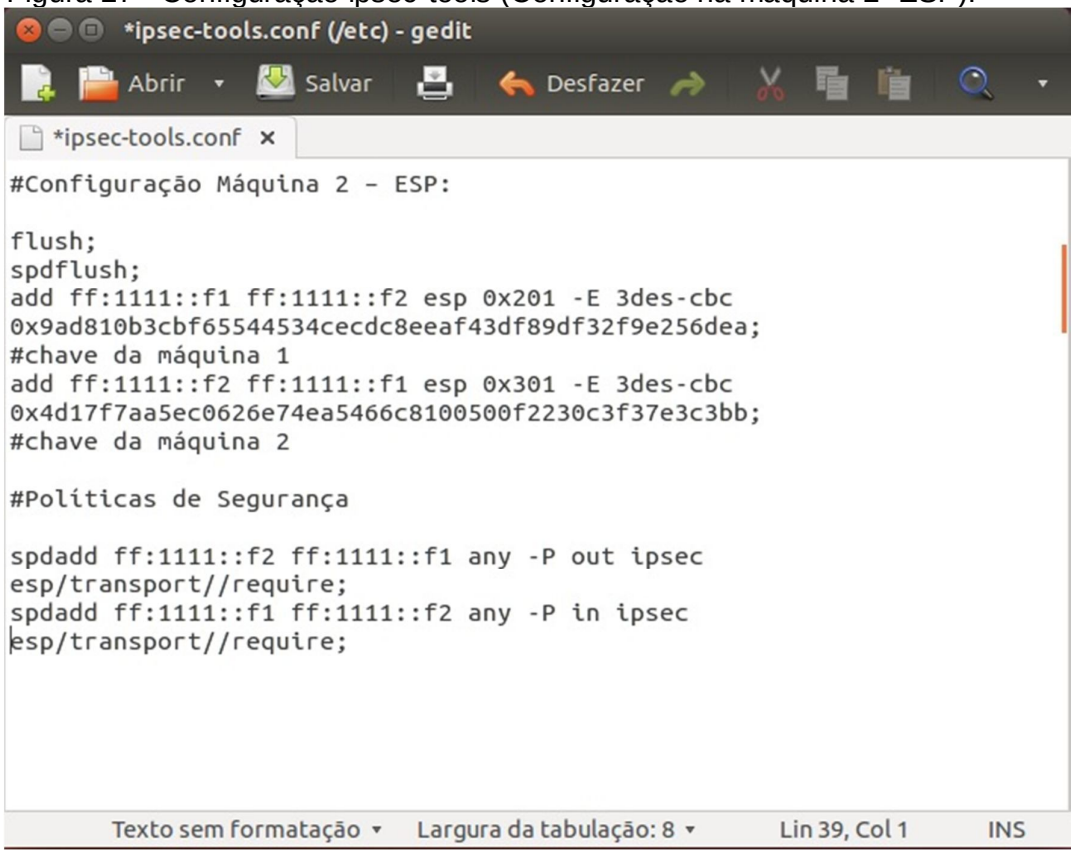
Conforme a Figura 26 é possível visualizar nas linhas 1 e 2 a diretiva responsável por limpar o banco das políticas de segurança, o comando “spdflush” remove toda e qualquer entrada previamente criada. Já na linha 3 são adicionados os dois endereços IPv6 da máquina 1 e 2 que realizaram a conexão através de IPSEC, na linha 4 foi incluída a chave da máquina 1 gerada conforme a figura 26. Nas linhas 5 e 6 foi feito o mesmo procedimento mas com as informações da máquina 2.

Nas linhas 7 e 9, a diretiva “spdadd” é responsável por adicionar uma entrada para o banco de políticas de segurança. O comando “spdadd” primeiramente libera a saída (out) de qualquer protocolo (*any*) originado por este IP e com destino a um determinado IP. Posteriormente este aplica uma política IPSEC que determina a utilização do protocolo ESP para proteção da conexão. Nas linhas 8 e 10, como último parâmetro é determinado que a associação de segurança entre as pontas é obrigatória (*require*) para que seja autorizada a troca de dados entre elas. Vale ressaltar que o segundo comando “spdadd” libera o retorno da saída liberada no

primeiro comando “spdadd”, ou seja, primeiramente libera a entrada (in) de qualquer protocolo (*any*) originado pelo IP ff:1111::f1 com destino ao IP ff:1111::f2 e posteriormente, aplica as mesmas políticas definidas para a saída dos pacotes (*out*).

Conforme apresentado na Figura 27 é possível visualizar a configuração da máquina 2, com cabeçalho ESP.

Figura 27 - Configuração ipsec-tools (Configuração na máquina 2- ESP).



Fonte: Elaborada pelo autor.

Para verificação de erros no arquivo ipsec-tools.conf é necessário a utilização do comando conforme representado na Figura 28.

Figura 28 - Comando para verificação de erros do configurador do IPSEC.

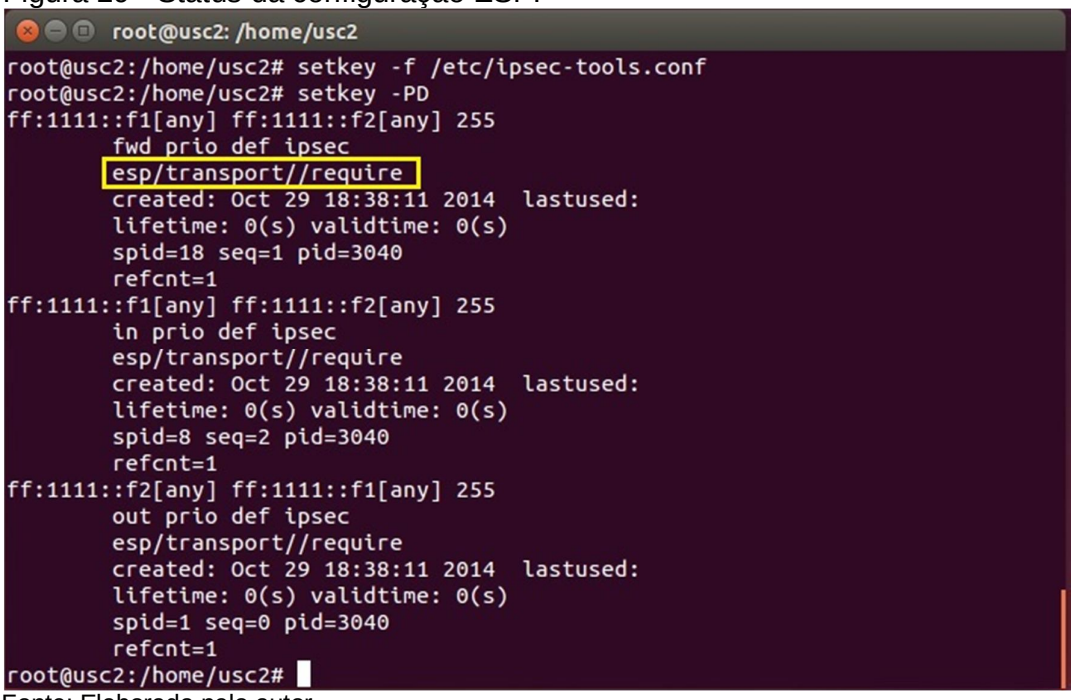
```
# setkey –f /etc/ipsec-tools.conf
```

Fonte: Elaborada pelo autor.

O comando da Figura 24 foi usado para mostrar em qual configuração o IPSEC se encontra.

A Figura 29 mostra a configuração do IPSEC, configurado em modo ESP.

Figura 29 - Status da configuração ESP.



Fonte: Elaborada pelo autor.

Depois de realizada as devidas configurações do IPSEC, o serviço foi inicializado com o comando apresentado na Figura 30.

Figura 30 - Comando para iniciar serviço setkey.

```
# /etc/init.d/setkey start
```

Fonte: Elaborada pelo autor.

3.3.2.2 Modo AH (Modo Transporte):

Todos os passos a seguir foram realizados nas duas máquinas (máquina 1 e máquina 2).

Foi necessário gerar as chaves de criptografia para cada modo, no terminal foi digitado o comando, como mostra a Figura 31.

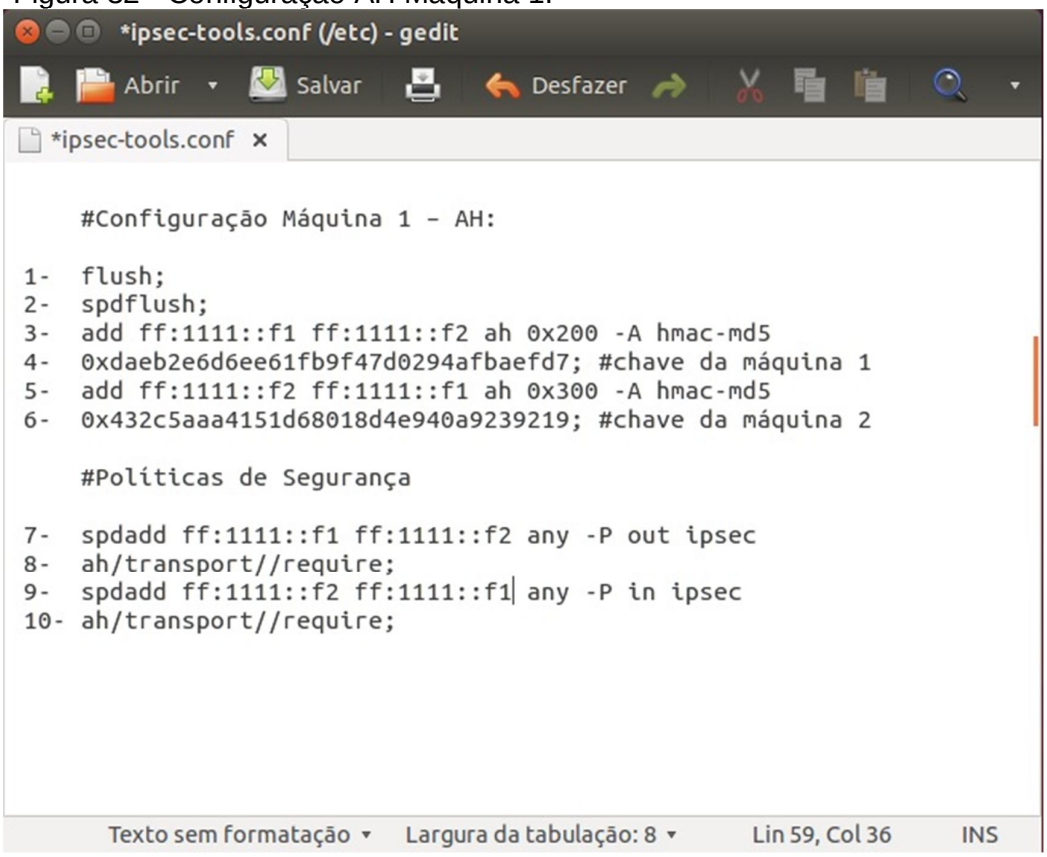
Figura 31 - Gerar chave AH.

```
# dd if=/dev/random count=16 bs=1| xxd –ps
```

Fonte: Elaborada pelo autor.

Conforme a Figura 32, o arquivo ipsec-tools.conf da máquina 1 se encontra configurado em modo AH.

Figura 32 - Configuração AH Máquina 1.



Fonte: Elaborada pelo autor.

Conforme a Figura 32, é possível visualizar nas linhas 1 e 2 a diretiva responsável por limpar o banco das políticas de segurança, o comando “spdflush” remove toda e qualquer entrada previamente criada. Na linha 3 é adicionados os dois endereços IPv6 da máquina 1 e 2 que farão a conexão através de IPSEC, na linha 4 é incluída a chave da máquina 1 gerada conforme a Figura 34. Nas linhas 5 e 6 é feito o mesmo procedimento mas as informações da máquina 2.

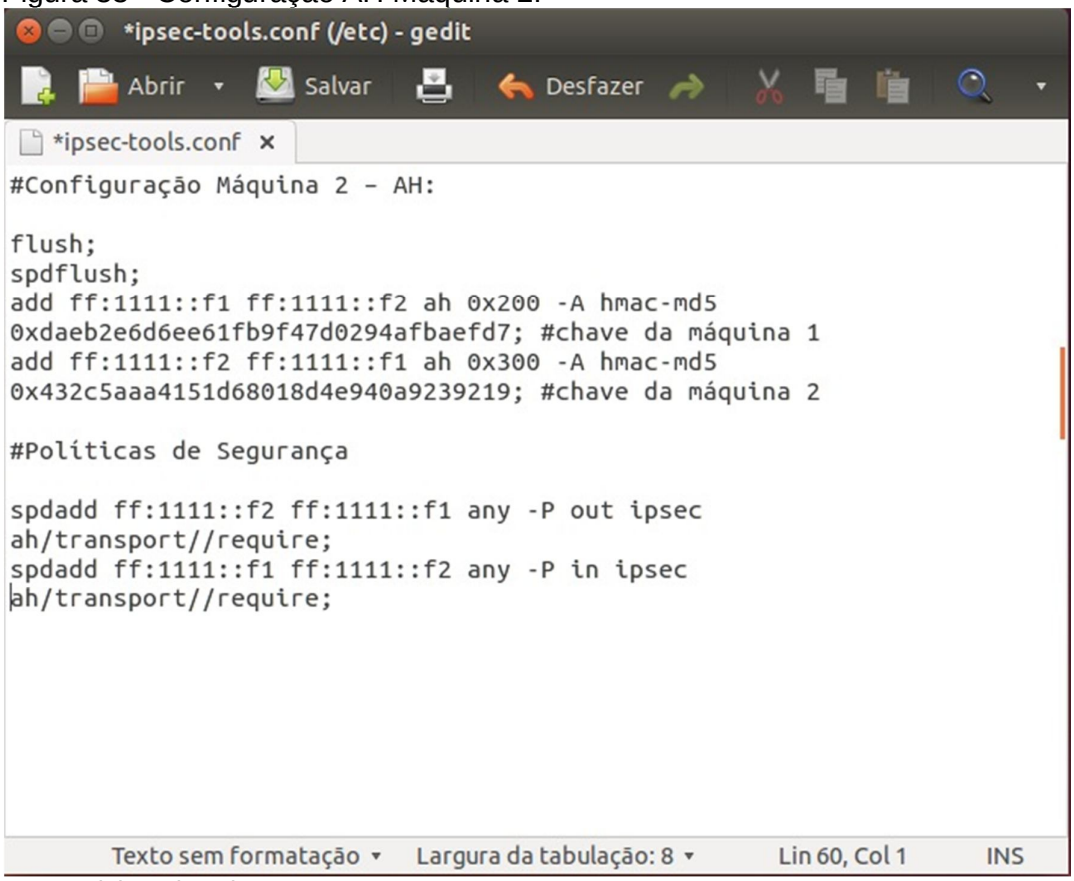
Nas linhas 7 e 9 da figura 32, a diretiva “spdadd” é responsável pro adicionar uma entrada para o banco de políticas de segurança. O comando “spdadd”

primeiramente libera a saída (out) de qualquer protocolo (*any*) originado por este IP e com destino a um determinado IP. Posteriormente este aplica uma política IPSEC que determina a utilização do protocolo AH para proteção da conexão. Nas linhas 8 e 10, como último parâmetro é determinado que a associação de segurança entre as pontas é obrigatória (require) para que seja autorizada a troca de dados entre elas.

Vale ressaltar que o segundo comando “spdadd” libera o retorno da saída liberada no primeiro comando “spdadd”, ou seja, primeiramente libera a entrada (in) de qualquer protocolo (any) originado pelo IP ff:1111::f1 com destino ao IP ff:1111::f2 e, posteriormente, aplica as mesmas políticas definidas para a saída dos pacotes (*out*).

Conforme apresentado na Figura 33 é possível visualizar a configuração da máquina 2, com cabeçalho AH.

Figura 33 - Configuração AH Máquina 2.



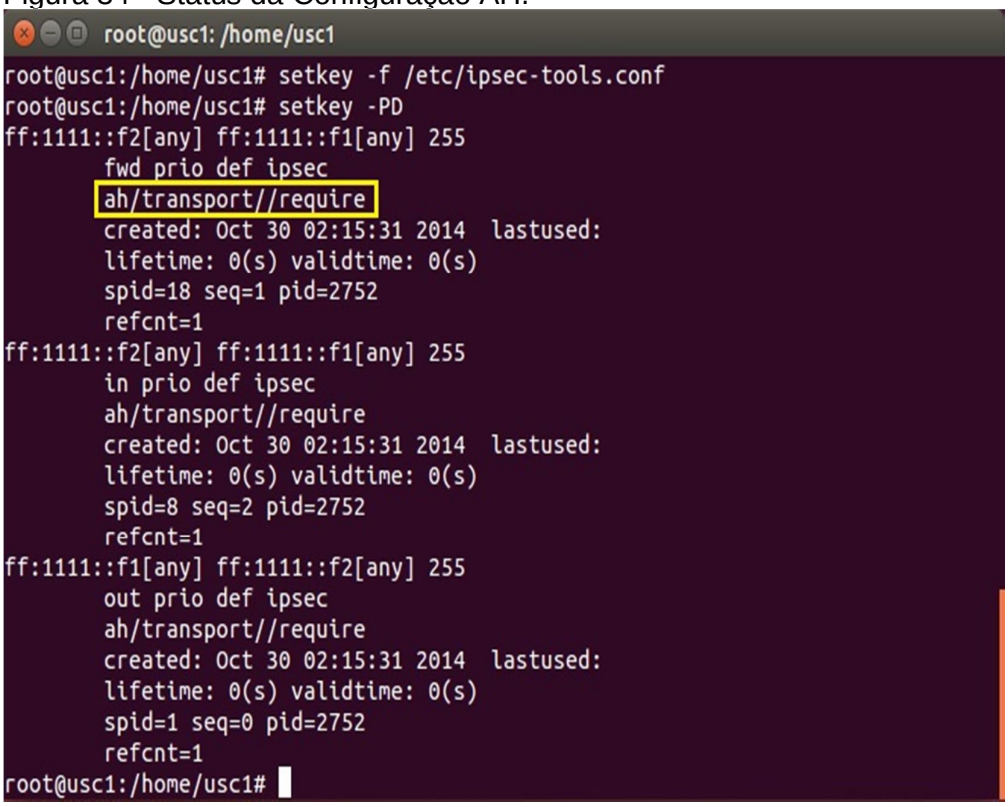
Fonte: Elaborada pelo autor.

A diferença da configuração entre o AH e o ESP, estão no tipo das chaves geradas e no parâmetro da linha 3 e 5. As políticas de segurança também são alteradas, de AH para ESP.

O comando da Figura 24 foi usado para mostrar em qual configuração o IPSEC se encontra.

A Figura 37 mostra a configuração do IPSEC, configurado no modo AH.

Figura 34 - Status da Configuração AH.



Fonte: Elaborada pelo autor.

Depois de realizada as devidas configurações do IPSEC, o serviço foi inicializado com o comando apresentado na figura 30.

3.3.2.3 Modo ESP/AH (Modo Transporte)

As configurações seguintes foram realizadas em duas fases em ambas as máquinas.

Gerando chave ESP e AH:

Gerando chave ESP:

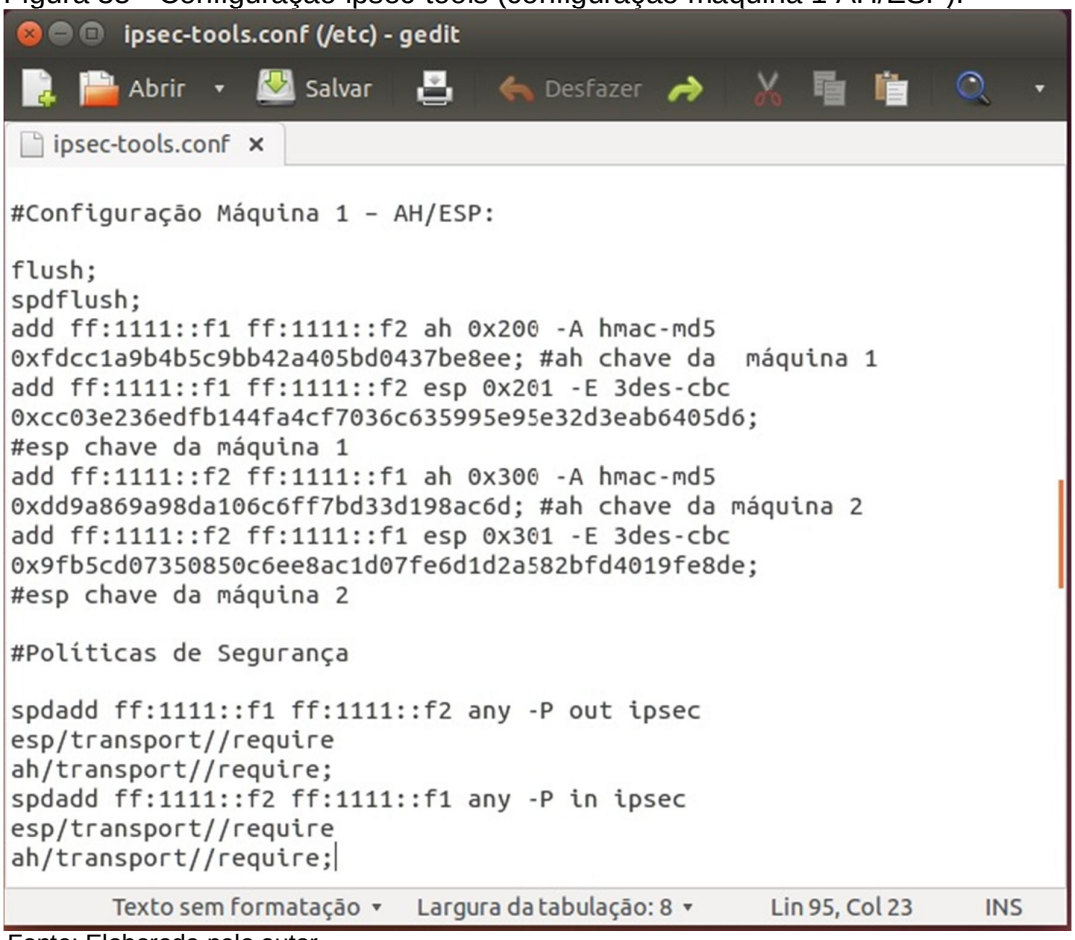
No terminal do Linux, foi digitado o comando conforme Figura 25.

Gerando chave AH:

Também foi gerada a chave AH do mesmo modo que a chave ESP acima, porém foi usado o comando da Figura 31.

Conforme apresentado na Figura 35 é possível visualizar a configuração da máquina 1, com cabeçalho AH/ESP.

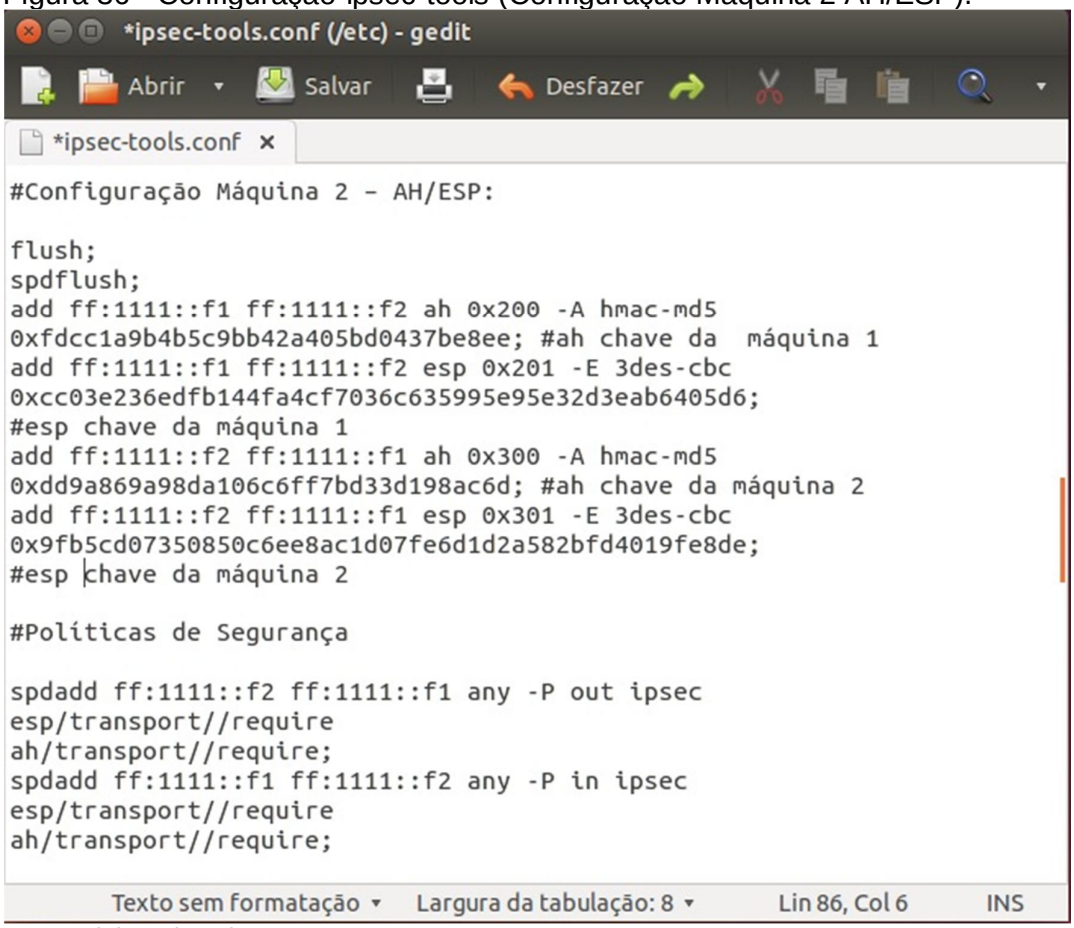
Figura 35 - Configuração ipsec-tools (configuração máquina 1 AH/ESP).



Fonte: Elaborada pelo autor.

Conforme apresentado na Figura 36 é possível visualizar a configuração da máquina 2, com cabeçalho AH/ESP.

Figura 36 - Configuração-ipsec-tools (Configuração Máquina 2 AH/ESP).

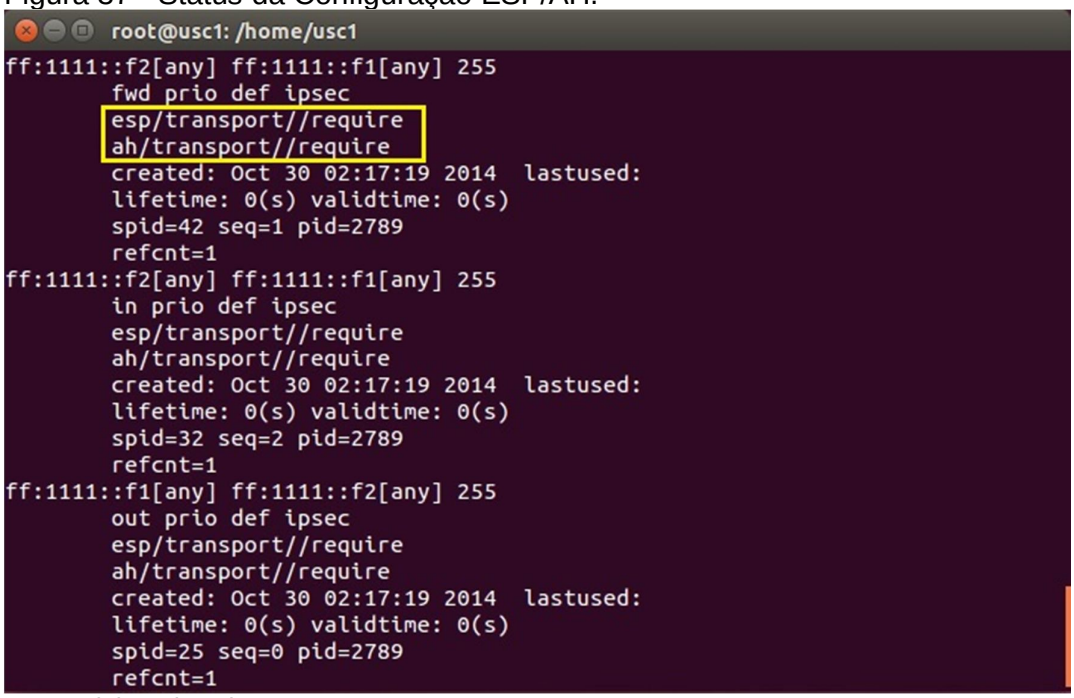


Fonte: Elaborada pelo autor.

O comando da Figura 24 foi usado para mostrar em qual configuração o IPSEC se encontra.

A Figura 37 mostra a configuração em que o IPSEC se encontra, nesse caso foi configurado com as criptografias AH/ESP.

Figura 37 - Status da Configuração ESP/AH.



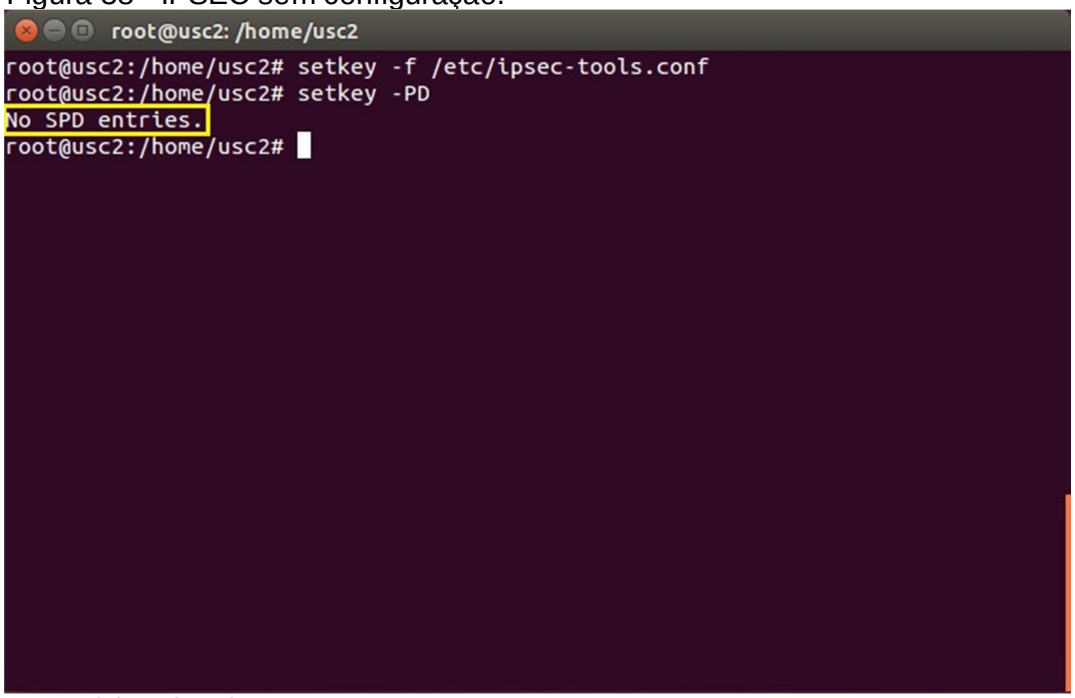
Fonte: Elaborada pelo autor.

Depois de realizada as devidas configurações do IPSEC, o serviço foi inicializado com o comando apresentado na Figura 30.

3.3.2.4 Sem Criptografia

Foram realizados testes sem criptografia alguma, para tanto, também foi utilizado o comando da Figura 24 para verificar se não existe criptografia alguma configurada conforme demonstrado na Figura 38.

Figura 38 - IPSEC sem configuração.



Fonte: Elaborada pelo autor.

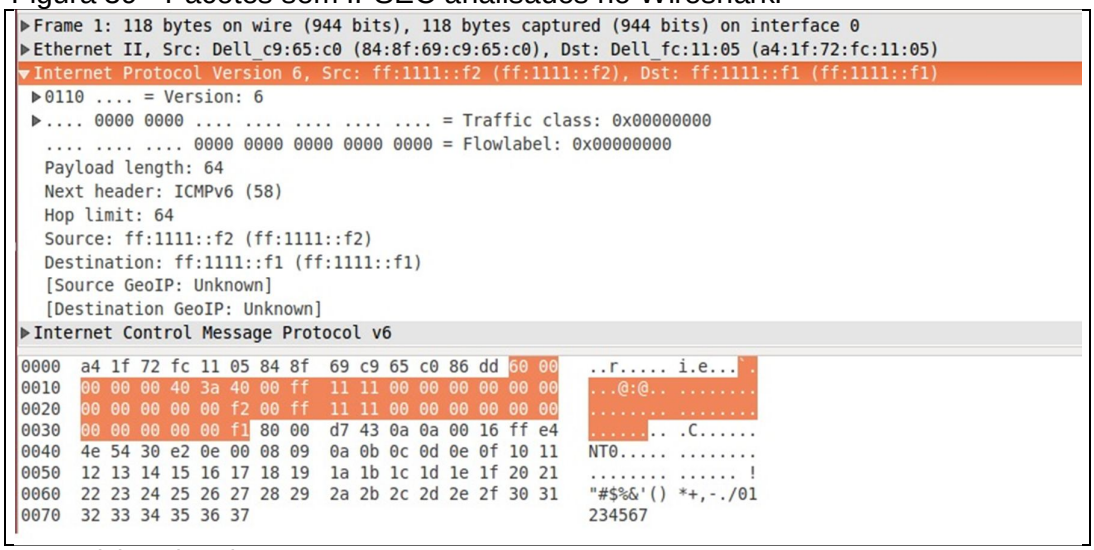
3.3.3 Verificação de envio de pacotes analisado via Wireshark.

O software Wireshark foi uado para analisar os pacotes, sem criptografia, e com criptografias (ESP – AH – ESP mais AH).

3.3.3.1 Sem IPSEC

Na Figura 39 pode se observar pacotes sendo analisados sem IPsec, , dentro do Campo “Internet Protocol Version 6,” não consta nenhum tipo de criptografia ativa, apenas a versão do protocolo, e também os IPs de origem e destino dos pacotes.

Figura 39 - Pacotes sem IPSEC analisados no Wireshark.



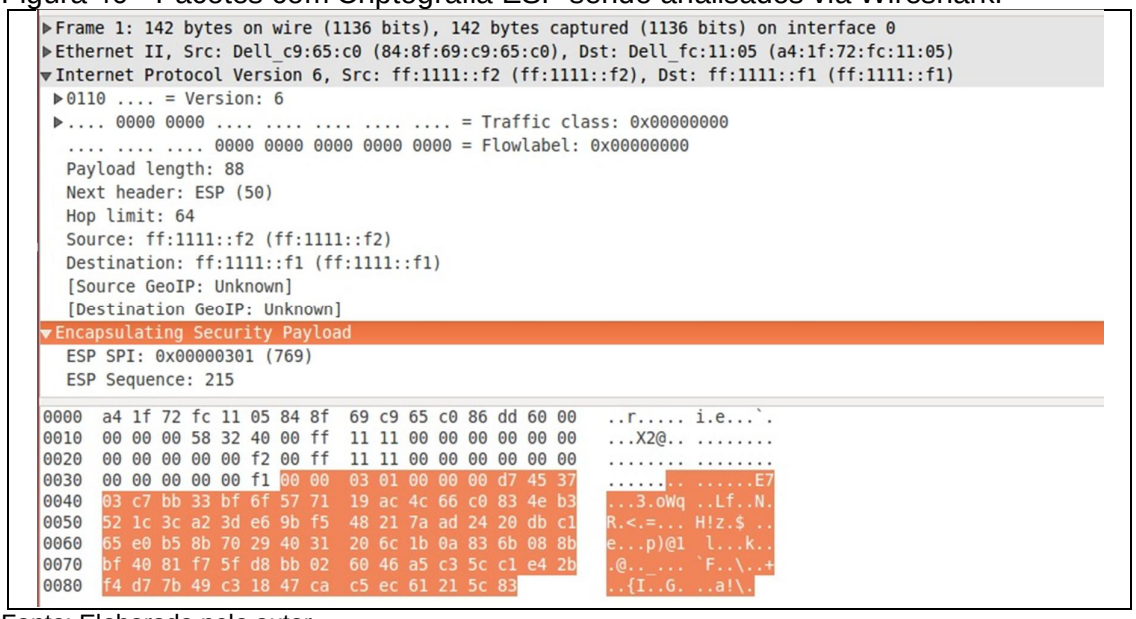
Fonte: Elaborada pelo autor.

3.3.3.2 ESP (Encapsulating Security Payload)

Na Figura 40 observa se pacotes analisados com criptografia ESP. Visualiza-se o cabeçalho ESP adicionado após o cabeçalho IP, sendo que o cabeçalho IP ficou mais próximo do cabeçalho ESP.

Conforme mostrado anteriormente na Figura 12, o cabeçalho IP mantém-se original, protegendo apenas os cabeçalhos superiores, pois o cabeçalho IPSEC é adicionado imediatamente após o Cabeçalho IP, e antes dos cabeçalhos dos protocolos das camadas superiores.

Figura 40 - Pacotes com Criptografia ESP sendo analisados via Wireshark.



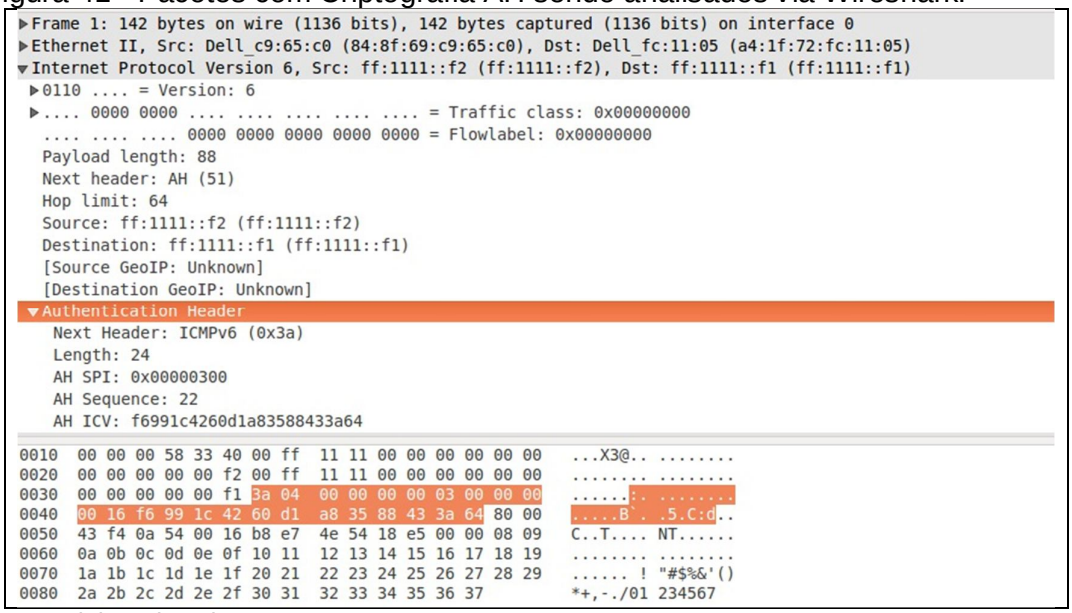
Fonte: Elaborada pelo autor.

3.3.3.3 AH (Authentication Header)

Como é possível verificar na Figura 41, o cabeçalho AH foi adicionado dentro do cabeçalho IP.

Conforme mostrado anteriormente na Figura 12, o cabeçalho IP mantém-se original, protegendo apenas os cabeçalhos superiores, pois o cabeçalho IPSEC é adicionado imediatamente após o Cabeçalho IP e antes dos cabeçalhos dos protocolos das camadas superiores.

Figura 41 - Pacotes com Criptografia AH sendo analisados via Wireshark.

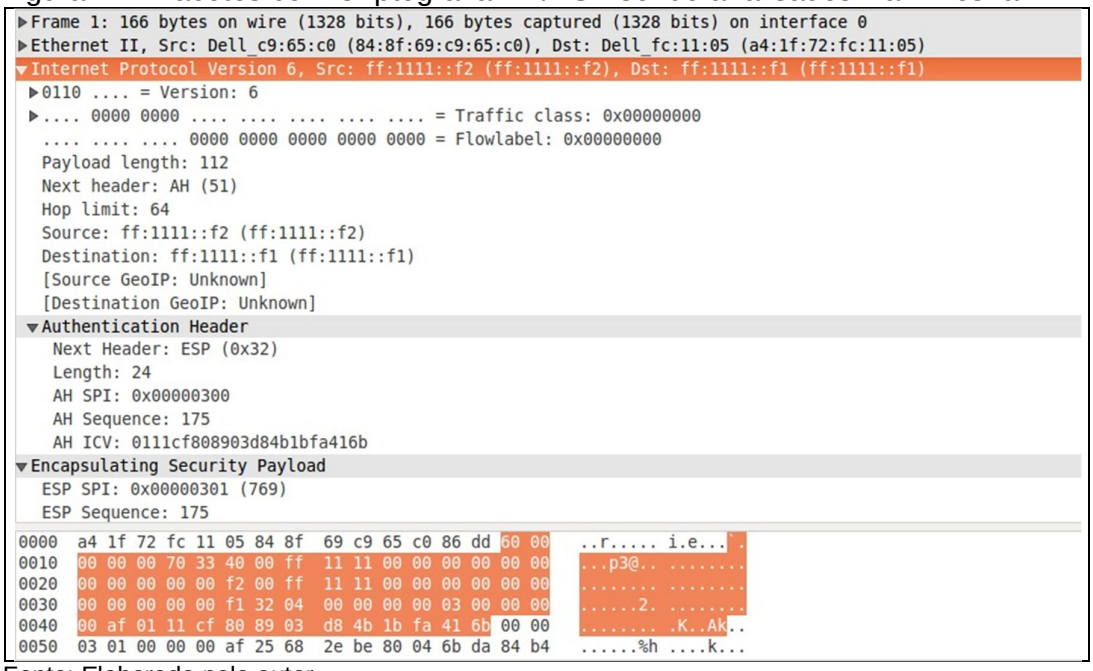


Fonte: Elaborada pelo autor.

3.3.3.4 ESP/AH

Na Figura 42 pode-se visualizar os dois cabeçalhos em conjunto, o cabeçalho AH que foi adicionado dentro do cabeçalho IP. O cabeçalho ESP foi adicionado após o cabeçalho IP, e como próximo cabeçalho o ESP.

Figura 42 - Pacotes com Criptografia AH/ESP sendo analisados via Wireshark



Fonte: Elaborada pelo autor.

4 RESULTADOS

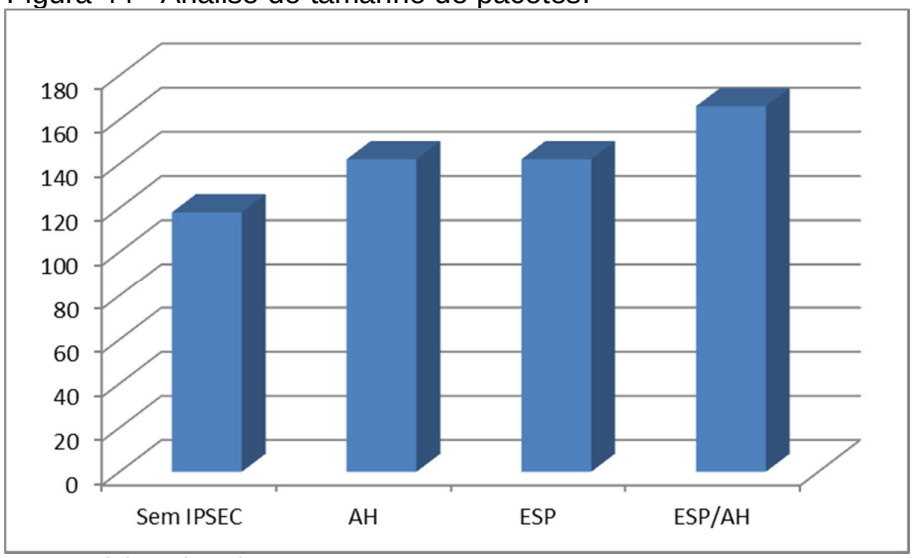
Foram realizados testes com arquivos de tamanhos crescentes, até perceber-se houve alteração no tempo de transmissão dos arquivos, conforme a Figura 43, na primeira coluna, pode-se visualizar o tamanho dos pacotes que foram transferidos, após isto está descrito qual cabeçalho (Sem IPSEC, AH, ESP, ESP/AH), também foi adicionado qual foi o tempo de transferência de cada arquivo. O tempo de transferência foi colocado em segundos na Figura 43.

Figura 43 - Tabela de resultados das transferências de arquivos.

Tamanho dos arquivos	Sem IPSEC	AH	ESP	ESP/AH
60 MB	05	05	05	05
87 MB	08	08	08	08
518 MB	50	51	51	52
900 MB	78	79	79	81

Fonte: Elaborada pelo autor.

Figura 44 - Análise do tamanho de pacotes.



Fonte: Elaborada pelo autor.

Na Figura 44 pode-se visualizar, que com a utilização do IPSEC o tamanho do pacote aumenta, podendo tornar lenta uma rede que possui um grande número de máquinas, utilizando o comando ping entre as maquinas sem a configuração do IPSEC o tamanho do pacote é de 118 bytes, configurado com o cabeçalho AH e

com o cabeçalho ESP o tamanho do pacote passa a ser 142 bytes cada, e com o AH+ESP passa a ser 166 bytes.

4.1 DESEMPENHO

No primeiro teste foi enviado um arquivo com o tamanho de 60MB, sem que a configuração do IPSEC esteja ativa seu tempo de transmissão foi de 5 segundos, em seguida foi utilizado o mesmo arquivo com o cabeçalho AH ativo, o tempo de transmissão também foi de 5 segundos, no terceiro teste novamente o utilizando o mesmo arquivo, porém com o cabeçalho ESP ativo, e seu resultado também foi de 5 segundos e, por ultimo, foi transmitido com o cabeçalho AH+ESP obtendo o mesmo resultado,

Para o segundo teste foi aumentado o tamanho do arquivo para 87 MB obtendo 8 segundos sem acionamento da criptografia, 8 segundos para AH, 8 segundos para o modo ESP e, por fim, 8 segundos AH+ESP.

No terceiro teste foi utilizado um arquivo de 587 MB, sem criptografia o tempo foi de 50 segundos, no modo AH seu tempo foi de 51 segundos, em modo ESP, modo AH+ESP de 52 segundos.

E, por último, foi realizado a transferência do arquivo de 900 MB, sem a utilização do IPSEC, a sua marca foi de 78 segundos, com o modo AH 79 segundos, utilizando o modo ESP o tempo foi de 79 segundos, e por ultimo com o modo AH+ESP foi de 81 segundos.

Conclui-se que com esses testes arquivos de até aproximadamente 100 MB, não se encontra nenhum tipo de atraso na transferência de arquivos mesmo o pacote tendo passado pela criptografia ESP+AH, porém arquivos maiores de 500 MB que passam pela criptografia geram um atraso, podendo ocasionar lentidão em uma rede com muitos computadores.

5 CONCLUSÃO

O IPSEC garante que os dados sejam criptografados garantindo a segurança dos dados que navegam pela rede, protegendo-os, pois somente quem tem a chave de segurança pode ler esses dados.

Quando adicionado o cabeçalho AH o pacote aumenta cerca de 24 bytes do seu tamanho original, para que aja a autenticação no modo ESP os pacotes foram criptografados aumentando sua segurança, pois agora não é possível visualizar o conteúdo dos pacotes, e o seu tamanho também foi de 24 bytes.

Quando acionado os dois cabeçalhos em conjuntos (AH+ESP), ouve a autenticação e a criptografia, aumentando substancialmente sua segurança, e houve um aumento de 48 bytes nos pacotes transmitidos, ocasionando lentidão na rede pelo qual trafegam pois os pacotes necessitam ser autenticados, criptografados e para somente assim serem enviados, e na máquina que recebe necessita fazer o processo inverso receber, verificar a autenticidade dos pacotes e remover a criptografia.

Para arquivos de até 100MB, a utilização do IPSEC pode ser utilizada sem prejudicar o desempenho da rede não causando nenhum tipo de lentidão por conta da criptografia, e também foi possível demonstrar que o modo ESP tem um atraso um pouco maior que o modo AH, e com os dois modos ativados percebe-se que para arquivos grandes maiores que 500MB percebe-se um atraso pouco mais significativo na rede.

O IPSEC é uma importante ferramenta para administradores de rede, se devidamente configurada pode aumentar bastante a segurança da mesma, protegendo assim seus dados.

Recomendações para trabalhos futuros.

Para melhoria e aprofundamento do estudo sobre IPV6, estudar o IPSEC em conjunto com o protocolo versão 6 (IPv6), com o sistema de tunelamento,

Uso do protocolo IPv6 para computadores caseiros para melhoria e segurança do uso da internet para usuários finais.

REFERÊNCIAS

BRITO, H. O **Novo Protocolo da Internet**. São Paulo: Novatec, 2013.

CABEÇALHO. **Ipv6**, [2014?]. Disponível em: <http://ipv6.br/entenda/cabecalho/>. Acesso em: 10 abr. 2014.

ESGOTAMENTO.**Ipv6**, [2014?]. Disponível em: <http://ipv6.br/cronograma/>. Acesso em: 10 abr. 2014.

ENDEREÇANENTO.**Ipv6**, [2014?]. Disponível em: < http://ipv6.br/entenda/enderecamento/>. Acesso em: 10 abr. 2014.

SEGURANÇA.**Ipv6**, [2014?]. Disponível em: < ipv6.br/download/ipv6-seguranca-fisl13.pdf/>. Acesso em: 10 abr. 2014.

DAVIES, J. **Introduction to IP version 6**. Microsoft Corporation: 2004. **Technet**, 2002. Disponível em < http://technet.microsoft.com/en-us/library/cc783437%28v=ws.10%29.aspx> Acesso em: 12 abr. 2014.

DIERKS, T; ALLEN, C. The TLS Protocol. **Ietf**, 1999. Disponível em: <http://www.ietf.org/rfc/rfc2246.txt> Acesso em: 12 abr. 2014.

ESGOTAMENTO do IPv4 em nossa região (LACNIC**). Ipv6**, [2014?]. Disponível em: < http://ipv6.br/estatisticas/>. Acesso em: 12 abr. 2014.

FARREL, A. **A Internet e seus Protocolos: Uma análise Comparativa**. Rio de Janeiro: Elsevier, 2005.

KRAWCZYK, H; BELLARE, M; CANETTI, R. HMAC: Keyed-Hashing for Message Authentication. **Ietf**, 1997. Disponível em: <http://www.ietf.org/rfc/rfc2104.txt> Acesso em: 15 abr. 2014.

KENT, S; SEO, K. **Security Architecture for the Internet Protocol**. RFC 4301, IETF. 2005. Disponível em: < http://www.ietf.org/rfc/rfc4301.txt> Acesso em: 16 abr. 2014.

KUROSE, J. F.; ROSS Keith. W. **Redes de Computadores e a Internet:** uma abordagem top-down. São Paulo: Person Education, 2006.

PEREZ, M. ATM Signaling Support for IP over ATM. **Ietf**, 1995. Disponível em: < http://www.ietf.org/rfc/rfc1755.txt> Acesso em: 16 abr. 2014.

RICCI, B. **Rede Segura:** VPN Linux. Rio de Janeiro: Ciência Moderna, 2007.

SANTOS, R. dos et al. **Curso IPv6 Básico**. São Paulo: Érica, 2010.

SILVA, A. **Redes Frame Relay**, 2005.

SILVA, A. **Curso Básico de ATM**. 2004. Disponível em <http://www.rjunior.com.br/download/curso%20atm.pdf>.Acesso em: 15 abr. 2014

SOUSA, B. **Redes de Computadores Guia total**. São Paulo: Érica, 2009.

TANENBAUM, S. **Redes de computadores**. São Paulo: Campus, 2003.

Protocolo IPv6: Integração do Protrocolo IPv6 com o IPSEC

Rafael Henrqiue Dias, Henrique Pachioni Martins, Elvio Gilberto da Silva, Patrick Pedreira Silva

Centro de Ciências Exatas e Sociais Aplicadas
Universidade Sagrado Coração (USC) – Bauru, SP – Brasil

diassccp@gmail.com, henrique.martins@usc.br

Resumo. *Com o rápido aumento de usuários na internet deu-se o rápido esgotamento de endereços livres do protocolo de comunicação de internet o Internet Protocol versão 4 (IPv4), a solução para tanto, foi o desenvolvimento de um novo protocolo o Internet Protocol versão 6 (IPv6). Analisando falhas de segurança existentes na versão 4, e pensando na segurança dos dados transitados via internet, foi desenvolvido o Security Protocol (IPSEC), uma solução de segurança em nível de camada de rede para proteger todo o tráfego de rede. Este trabalho tem como objetivo demonstrar a utilização do protocolo IPv6 integrado com o IPSEC a fim de identificar sua segurança e desempenho, demonstrando se ouve ou não o aumento do tamanho dos pacotes que trafegam na rede, por conta das criptografias que acompanham os pacotes, e quanto esse aumento pode significar, e também se realmente os pacotes foram transmitidos com segurança até seu destinatário. Pode-se concluir que através dos testes realizados, e com a implementação do IPSEC junto ao protocolo IPv6, a segurança foi ativada em todos os modos de criptografia, assim garantindo a integridade e confidencialidade dos dados transmitidos, porém arquivos maiores que 500 MB geram um aumento no tempo de transferências, devido ao processo de criptografia, podendo ocasionar lentidões na rede.*

Abstract. *With the rapid increase of Internet users was given the rapid depletion of free addresses of Internet communication protocol Internet Protocol version 4 (IPv4), the solution to both, was the development of a new Protocol Internet Protocol version 6 (IPv6). Analyzing existing security holes in version 4, and thinking about the security of data carried over the Internet, we developed the Security Protocol (IPSec), a security solution for network layer level to protect all network traffic. This paper aims to demonstrate the use of integrated IPv6 protocol with the IPSEC to identify their safety and performance, demonstrating hear or not increasing the size of the packets traveling on the network, because of the encryption that accompany the packages, and as this increase could mean, and also really packets were transmitted safely to its destination. It can be concluded that through the tests, and with the implementation of IPSEC with the IPv6 protocol, security has been enabled on all encryption modes, thus ensuring the integrity and confidentiality of transmitted data, but files larger than 500 MB generate increase in time transfers due to the encryption process, which may cause delays in the network.*

1. Introdução

Um dos maiores projetos, senão o maior, já construído pela engenharia humana, foi a Internet, criada por pesquisadores no final da década de 60 (1966) nos Estados Unidos, durante a Guerra Fria entre EUA e URSS, havia um medo constante de que um ataque aos meios de comunicação do país culminasse na indisponibilidade dos serviços de telecomunicações. (TANEMBAUM, 2003).

Em 1969 foram instalados os primeiros quatro nós da rede em universidades que, naquela época, era denominada ARPANET. Somente em 1983, com mais de 500 hosts na rede, que surgiu a Internet propriamente dita com base estrutural que conhecemos atualmente, ou seja, baseada no protocolo IP. (TANEMBAUM, 2003).

Na década de 80, o resultado de diversas pesquisas realizadas em todo o mundo foi incorporado à rede mundial, o que contribuiu para o desenvolvimento de um novo padrão de protocolos conhecido como TCP/IP. (BRITO, 2013).

Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997. (IPv6.br).

A questão de segurança na Internet é discutida há décadas, e melhorias vêm sendo implementadas desde então.

Esse trabalho é um material de apoio para interessados em alternativas mais seguras para redes de computadores, na qual a comunicação é feita utilizando o protocolo IP. No momento a versão mais utilizada deste protocolo é o IPv4, que gradativamente está sendo substituído pelo IPv6.

Pensando em novos mecanismos de segurança o protocolo IP versão 6 foi criada para trabalhar em conjunto com o IPSEC. (BRITO, 2013).

O IPSEC pode ser muito útil, tanto em empresas quanto em qualquer ambiente que disponha de mais de um computador. Com o IPSEC é possível restringir determinadas informações sigilosas. O IPSEC pode ser útil também para a segurança de informações externas, pois ele atua diretamente na camada de rede, verificando todos os pacotes que entram e saem deste local. (BRITO, 2013)

2. Objetivos

Nesse capítulo serão apresentados o objetivo geral, e os objetivos específicos.

2.1. Objetivo Geral

O objetivo desse projeto é demonstrar como será feita a integração do protocolo IPV6 em conjunto com a solução de segurança IPSEC, a fim de documentar e testar sua performance.

2.2. Objetivos Específicos

- Estudar o IPv6, e sua forma de integração com o IPSEC e seus cabeçalhos Authentication Header (AH) e Encapsulating Security Payload (ESP);

- Montar um cenário mostrando o funcionamento de uma rede IPv6 com IPSEC;
- Realizar testes de funcionamento do IPv6 em conjunto com IPSEC, nos modos AH e ESP, AH+ESP;
- Avaliar o desempenho do protocolo IPSEC em redes IPv6.

3. Revisão de Literatura

Neste capítulo será apresentado o referencial teórico, para compreensão da transição gradual do protocolo IPv4 para o IPv6, assim como sua integração de segurança IPSEC com o IPv6.

3.1 Protocolos

Protocolo é um acordo de comunicação em que o ponto de envio de dados e o de recebimento estabelece regras de como a comunicação será realizada. (FARREL, 2005).

Basicamente, um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação. Como uma analogia, quando uma mulher é apresentada a um homem, ela pode estender a mão para ele que, por sua vez, pode apertá-la ou beijá-la, dependendo, por exemplo, do fato de ela ser uma advogada que esteja participando de uma reunião de negócios ou uma princesa europeia presente a um baile de gala. A violação do protocolo dificultará a comunicação, se não a tornar completamente impossível. (TANENBAUM, 2003).

Para melhor entender a funcionalidade de cada protocolo, dependendo do serviço que cada um presta, eles foram classificados em camadas distintas.

A função que cada conjunto de camadas com as atribuições que devem desempenhar em um sistema é chamado modelo de rede, juntando as camadas e os protocolos, denomina-se arquitetura de rede. (KUROSE; ROSS, 2006).

3.2 Protocolo IPv4

O Internet Protocol (IP) é um protocolo utilizado para comunicação nas redes de computadores na Internet. Foi criado para que dois ou mais computadores pudessem se interligar. O endereço IP é formado por um campo de 32 bits, onde são identificados o host e a rede na qual host pertence. (FARREL, 2005).

Cada máquina de uma rede TCP/IP possui um endereço IP, tal como 200.252.155.9. O endereço IP, às vezes chamado de *dotted quad*, é composto por quatro números separados por ponto, cada qual na faixa de 0 a 255. (KUROSE, 2006).

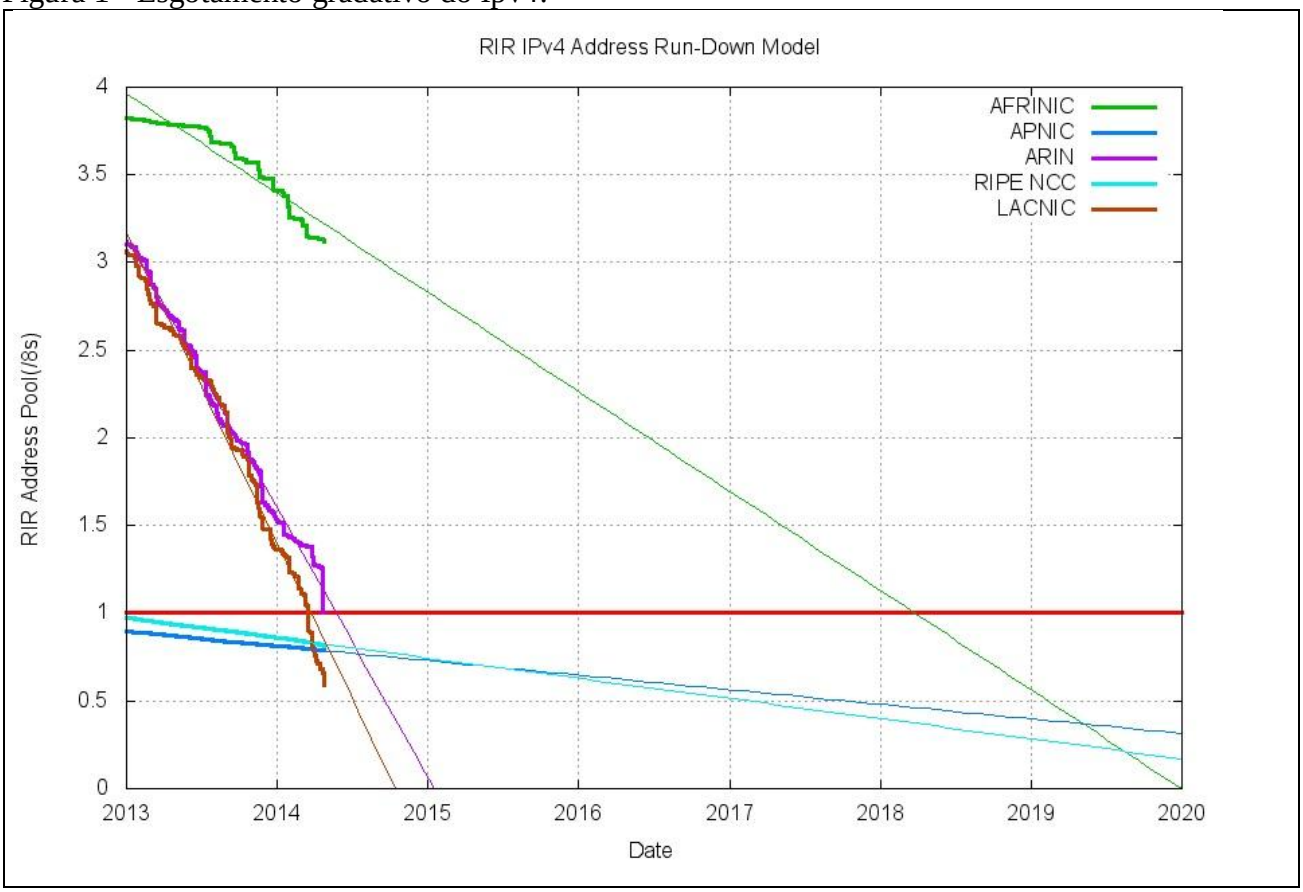
Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997. Diante desse cenário, a IETF (Internet Engineering Task Force) passa a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento, por esse motivo estão sendo utilizados alguns mecanismos, desde a década de 80, com a intencionalidade de se adiar o esgotamento dos endereços IPv4. (ROSS, 2006).

Alguns desses mecanismos são:

- Network Address Translation (NAT): O NAT permite que com apenas um endereço válido na Internet, os computadores da rede interna tenham conexão com a Internet. Ele faz um mapeamento baseado no IP interno e na porta local do computador, gerando um número de 16 bits usando a tabela hash, posteriormente este número é utilizado no campo da porta de origem. O pacote que vai para a rede externa leva o IP do roteador e na porta de origem o número gerado pelo NAT, com isso o computador externo que receber o pacote sabe de onde ele veio, e envia a resposta novamente para o emissor;
- Classless Inter Domain Routing (CIDR): Permite atribuir faixas de endereços de tamanhos variáveis, abolindo as classes de IP;
- Variable Length Subnet Mask (VLSM): É um método que permite calcular sub redes, alocando somente os bits necessários da sub rede utilizando máscaras de tamanho variáveis. (ROSS, 2006).

No entanto, mesmo com todos esses mecanismos o esgotamento dos endereços IPv4 é inevitável. Segundo Antônio Moreiras, gerente de Projetos do Centro de Estudo e Pesquisas em Tecnologia de Redes, o esgotamento do protocolo IPv4 no Brasil deve ocorrer no primeiro semestre de 2014, já que os números de endereços de IPs disponíveis na versão quatro não são suficientes para atender a demanda atual da Internet, como mostra a Figura 1, mostra o esgotamento do IPv4 no Brasil em meados de 2014 (representado pela linha marrom no gráfico), ocorrido oficialmente em 10 de Junho de 2014.

Figura 1 - Esgotamento gradativo do Ipv4.



Fonte: NIC.br/2014.

O ARIN (Registro Americano para Números da Internet é o Regional Internet Registry), responsável pelas alocações de endereços para América do Norte, chegou ao último /8 IPv4 de seu estoque na última quarta-feira, 23 de abril 2014. Com isso, entraram em vigor regras mais restritas de alocação que implementam uma fila única de alocação e uma análise mais detalhada de todos os pedidos. Qualquer alocação maior que um /15 irá requerer aprovação da diretoria do ARIN. Esta é a última fase de alocação do ARIN.
No LACNIC (Registro de Endereços da Internet para a América Latina e o Caribe) as regras para as últimas alocações são um pouco diferentes, e a previsão para o esgotamento é para maio de 2014.

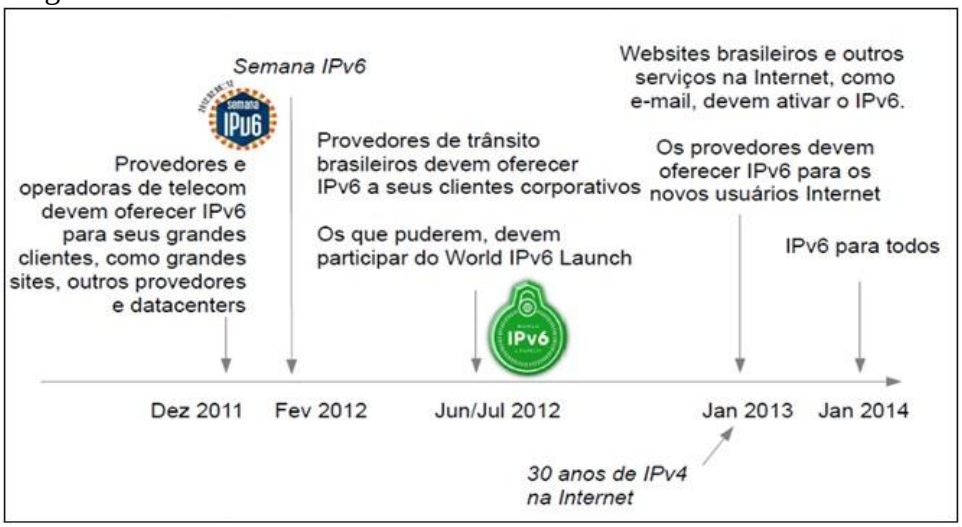
3.4 Protocolo IPv6

Esta versão do IP mantém a compatibilidade com a antiga versão (IPv4), uma vez que a transição está sendo feita gradativamente. A intenção do IPv6 é substituir o IPv4, que suporta apenas cerca de 4 bilhões de endereços (4x109) , contra cerca de 3x1038 endereços da nova versão. (SANTOS, 2010).

É a versão mais atual do IP, ou seja, a versão 6 . Sua criação foi iniciada em1994, por Scott Bradner e Allison Marken, após isto este protocolo já sofreu muitas mudanças e melhorias até os dias de hoje. (IPv6.BR, 2014).

Desde a criação do IPv6 foram feitas muitas modificações no protocolo, primeiramente foi testado em redes experimentais e após estar mais refinado, começou a ser utilizado em Provedores de Serviço, que passaram a utilizar o IPv6 em parte de suas redes. Empresas como Google, Facebook, Yahoo, Terra, IG já estão utilizando o IPv6, e provedores como a Global Crossing, da CTBC, e da Telefônica já fornecem trânsito IPv6 comercialmente no Brasil. A Figura 2 ilustra o crescimento do IPv6 no setor comercial.

Figura 2 - Crescimento do IPv6.



Fonte: nic.br (2014).

Devido à importância desta nova versão do IP os governos tem apoiado esta implantação. (IPv6.BR, 2014).

O Projeto de Lei 2126/ 2011, referente ao Marco Civil da Internet no Brasil,

sancionado no dia 24 de Abril de 2014, entrará em vigor no final de Junho desse mesmo ano. Dentre essas regulamentações governamentais, o Art. 2º no seu parágrafo V, se refere à segurança e funcionalidade da rede por meio de medidas técnicas compatíveis com os padrões internacionais, mostra um Estado vigilante e atual com as questões virtuais, ressaltando a importância da segurança cibernética, no tópico 2.4 será abordado o IPSEC (Protocolo de segurança na internet) em consonância com o IPv6, que são ou se tornarão fundamentais para o cumprimento eficiente desse Projeto, no qual internautas e provedores encontraram um respaldo legal.(Poder Executivo, PL-2126/2011).

3.4.1. Comparativo entre os protocolos IPv4 x IPv6

A versão IPv6 possui aprimoramentos se comparados com a anterior, tais como: (Ipv6.br,2014).

- A nova versão do protocolo possui seu espaço de endereçamento de 128 bits, antes era composto somente de 32 bits;
- Faz a atribuição automática dos IPs em uma rede;
- Os cabeçalhos foram remodelados, para que o processo dos roteadores seja simplificado e de uma forma mais segura, também foram criados cabeçalhos de extensão, que podem guardar informações adicionais;
- Suporte a qualidade de serviço (QoS): Aplicações de áudio e vídeo passam a estabelecer conexões apropriadas tendo em conta as suas exigências em termos de qualidade de serviço;
- Várias extensões no IPv6 permitem as opções de segurança como encriptação, autenticação, integridade e confidencialidade dos dados.

Para implementação do Ipv6, foram analisadas as limitações do IPv4, a criação da RFC 1755 (PEREZ, 1995), que resume os requisitos para o IPv6, fizeram as devidas aprimorações.

3.5. IPSEC

O quesito segurança sempre foi muito discutido e analisado, desde a criação do IPv6 , mecanismos de segurança passam a fazer parte do protocolo IPv6, sendo que qualquer par de dispositivos de uma conexão fim-a-fim possam se manter seguros, com métodos que visam garantir a segurança dos dados que trafegam pela rede.

Com a utilização cada vez maior da Internet para meios comerciais e transações que envolvem compras, vendas transferências de informações importantes ou valores em dinheiro é cada vez mais necessário que a rede tenha segurança. Para isto utilizam-se métodos para ajudar nesta proteção, tais como, firewalls, antivírus, segurança no acesso a web com Secure Socket Layer (SSL - RFC 2246 (DIERKS; ALLEN,1999).

A melhor alternativa para a segurança em nível de aplicação é fornecida na camada de rede, onde todo o conteúdo dos pacotes IP, e mesmo os próprios cabeçalhos IP, são protegidos. Essa solução apresenta muitas vantagens. Ela está disponível para todo o tráfego IP entre qualquer par de lados e, portanto, é útil para proteger dados de aplicações e também pode ser usada para proteger trocas de roteamento e sinalização. O IPSEC é à base da segurança em nível de rede. Ele é usado para autenticar o emissor das mensagens, para verificar se os dados da mensagem não foram adulterados e para ocultar informações de olhos não autorizados. (FARREL, 2005).

Em suma, o IPSEC é uma especificação de segurança que está incorporado ao IPv6, utilizando os cabeçalhos de extensão AH e ESP para seu funcionamento.

No IPSEC a criptografia e autenticação de pacotes são feitas na camada de rede, fornecendo assim uma solução de segurança fim-a-fim, garantindo a integridade, confidencialidade e autenticidade dos dados.

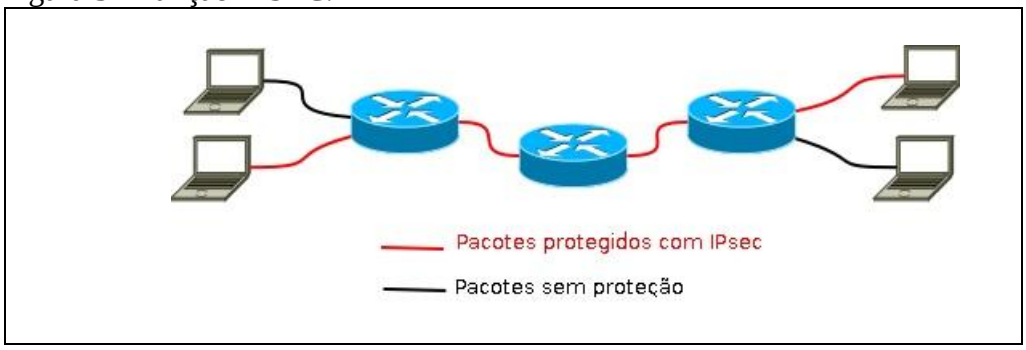
No IPv6 o seu suporte é obrigatório, já com seus principais elementos integrado, facilitando sua utilização. No IPv4 ele foi adaptado para funcionar, sendo opcional a sua utilização.

3.5.1. Arquitetura de segurança do IPSEC

A arquitetura do IPSEC foi originalmente especificada na RFC2401 em 1998 e posteriormente atualizada pela RFC4301 em 2005. (SILVA, 2005)
Existem duas formas distintas de utilização do IPSEC, em Modo Transporte ou Modo Túnel.

- **Modo de transporte:** No modo transporte, o emissor e receptor da comunicação segura necessitam de suporte ao IPSEC, conforme a Figura 3.

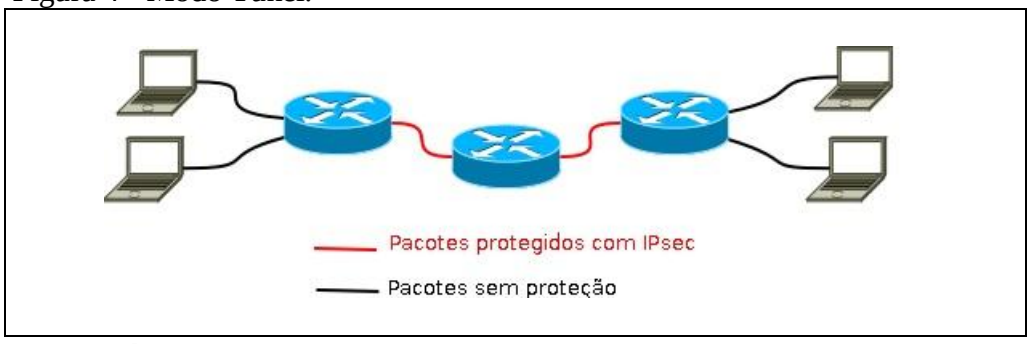
Figura 3 - Função IPSEC.



Fonte: nic.br (2014).

- **Modo de tunelamento:** No Modo Túnel (conhecido por Virtual Private Network - VPN) é protegido o pacote IP inteiro, onde todo o pacote é encapsulado dentro de outro pacote IP, após isto é criado um cabeçalho IP externo, que fica visível, tornando possível a ligação entre o dispositivo emissor com o receptor do túnel. Ao invés de configurar todos os dispositivos para utilizar IPSEC, esta configuração é feita somente nos roteadores de borda que encapsulam o pacote original, ao chegar ao roteador de borda do destino o pacote é descapsulado, como mostra a Figura 4:

Figura 4 - Modo Túnel.



Fonte: nic.br (2014).

3.6. Frameworks de Segurança do IPSEC (AH e ESP)

Os Frameworks são estruturas de suporte definidas em que outro projeto de software pode ser organizado e desenvolvido. Um framework pode incluir programas de suporte, bibliotecas de código, linguagens de script e outros softwares para auxiliar no desenvolvimento e unir diferentes componentes de um projeto de software.

3.6.1. AH (Authentication Header)

Faz com que haja a autenticação da origem do pacote, evitando que pacotes sejam reenviados, e fornecendo a integridade dos dados de todo o pacote, garantindo assim que a origem e o destino e os dados não foram alterados durante o seu tráfego na Internet (SILVA, 2005).

3.6.2. ESP (Encapsulating Security Payload)

É um cabeçalho que garante a autenticação, confidencialidade e integridade dos pacotes, evita que os pacotes sejam reenviados, podendo criptografar os dados.

Assim os dados trafegados pela Internet não foram alterados, além de tornar estes ilegíveis através da utilização de criptografia. Está localizado entre o cabeçalho IP e o resto do datagrama. Assim, os campos de dados são alterados após a criptografia dos mesmos. Cada pacote deve conter informações necessárias para estabelecer o sincronismo da criptografia, permitindo que a de criptografia ocorra na entidade de destino. Uma situação possível de acontecer é não utilizar nenhum algoritmo de criptografia, neste caso o protocolo ESP só oferecerá o serviço de autenticação. Pode ser utilizado com o modo de operação Transporte ou Túnel (SILVA, 2005).

4. Metodologia

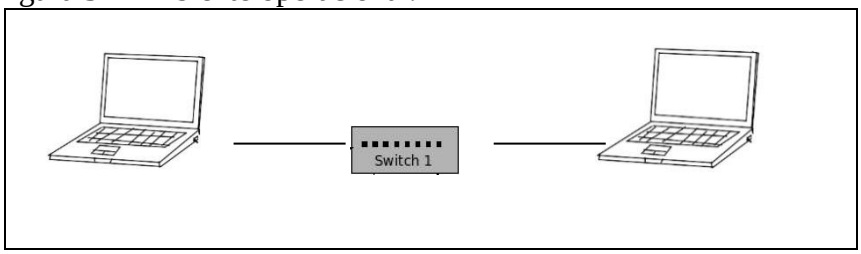
A metodologia adotada para a realização deste trabalho, reflete as etapas utilizadas para configurar um ambiente operacional de testes, para a implementação de IPv6 integrado com o IPSEC.

4.1 Hardware

Para o desenvolvimento desse trabalho, foi montado um cenário composto por dois notebooks Dell Inspiron 14r Core I3, 4 GB de memória RAM, com placa de rede 100 Mbps, essa configuração de hardware foi pensada para a instalação de um programa para virtualizar sistemas operacionais, pois com o programa de virtualização iniciado se divide o processador e a memória RAM entre a máquina física e a máquina virtual, com isso, esse hardware suportou o programa de virtualização muito bem, sem nenhuma lentidão que pudesse interferir nos testes. Os dois notebooks utilizam o sistema operacional Windows 7 Ultimate 64 bits.

Foi utilizado um Switch Netgear 8 portas 100MBs para a comunicação entre as máquinas, como mostra a Figura 5.

Figura 5 - Ambiente operacional.



Fonte: Elaborada pelo autor.

4.2. Software

O software de virtualização utilizado foi o Oracle VM VirtualBox 4.3, e o sistema operacional virtualizado utilizado foi Linux Ubuntu 14.04 32 bits, no Linux foram instalados diversos pacotes e programas para realização dos testes, descritos abaixo.

- O Pacote IPsec: Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPsec) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja o mesmo da origem) e autenticidade das informações ou prevenção de identity spoofing (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet.

- Wireshark: É um software para análise de pacotes que recebe contribuições de especialistas em rede de todo o mundo. Ele foi usado para analisar os pacotes sem criptografia, com criptografia ESP, AH e ESP/AH, e também foi usado para medir o tamanho dos pacotes.

- Open Secure Shell (SSH): Esse pacote foi utilizado nos testes de desempenho, onde possui um comando chamado SCP que possibilita a cópia de arquivos de uma máquina para outra, para a transferência de arquivos em IPv6, foi usado Colchetes ([ ]) em torno do IPv6.

-

4.3. Método

Na primeira etapa foi realizado o processo teórico sobre o protocolo IPv6, verificando o seu funcionamento e formas de realizar a sua configuração. Em um segundo momento foi estudado as formas de segurança do IPSEC.
Depois de realizados os estudos, foram analisadas as ferramentas para realização da configuração do IPSEC. Logo em seguida sucederam os testes de configuração do IPv6 e do IPSEC, seguidos de testes de desempenho do funcionamento do IPSEC em conjunto com o IPv6.

5. Resultados

Foram realizados testes com arquivos de tamanhos crescentes, até perceber-se

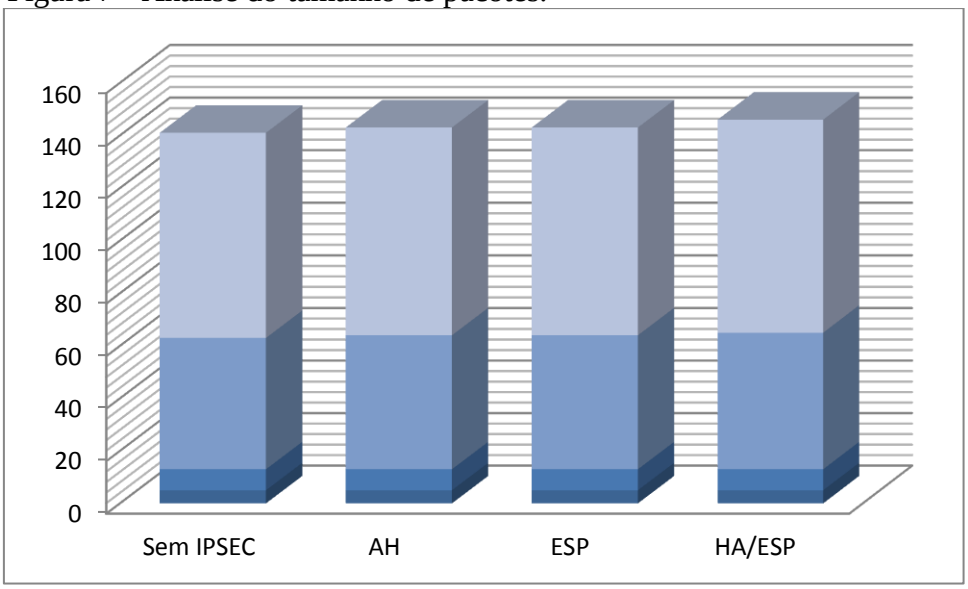
houve alteração no tempo de transmissão dos arquivos, conforme a Figura 6, na primeira coluna, pode-se visualizar o tamanho dos pacotes que foram transferidos, após isto está descrito qual cabeçalho (Sem IPSEC, AH, ESP, ESP/AH), também foi adicionado qual foi o tempo de transferência de cada arquivo. O tempo de transferência foi colocado em segundos na Figura 6.

Figura 6 - Tabela de resultados das transferências de arquivos.

Tamanho dos arquivos	Sem IPSEC	AH	ESP	ESP/AH
60 MB	05	05	05	05
87 MB	08	08	08	08
518 MB	50	51	51	52
900 MB	78	79	79	81

Fonte: Elaborada pelo autor.

Figura 7 - Análise do tamanho de pacotes.



Fonte: Elaborado pelo autor.

Na Figura 7 pode-se visualizar, que com o a utilização do IPSEC o tomanho do pacote aumenta, podendo tornar lenta uma rede que possui um grande número de máquinas, utilizando o comando “ping6” entre as maquinas sem a configuraçãodo IPSEC o tamanho do pacote é de 118 bytes, configurado com o cabeçalho AH e com o cabeçalho ESP o tamanho do pacote passa a ser 142 bytes, e com o AH+ESP passa a ser 166 bytes.

5.1. Desempenho

No primeiro teste foi enviado um arquivo com o tamanho de 60MB, sem que a configuração do IPSEC esteja ativa seu tempo de transmissão foi de 5 segundos, em seguida foi utilizado o mesmo arquivo com o cabeçalho AH ativo, o tempo de

transmissão também foi de 5 segundos, no terceiro teste novamente o utilizando o mesmo arquivo, porém com o cabeçalho ESP ativo, e seu resultado também foi de 5 segundos e, por ultimo, foi transmitido com o cabeçalho AH+ESP obtendo o mesmo resultado,

Para o segundo teste foi aumentado o tamanho do arquivo para 87 MB obtendo 8 segundos sem acionamento da criptografia, 8 segundos para AH, 8 segundos para o modo ESP e, por fim, 8 segundos AH+ESP.

No terceiro teste foi utilizado um arquivo de 587 MB, sem criptografia o tempo foi de 50 segundos, no modo AH seu tempo foi de 51 segundos, em modo ESP, modo AH+ESP de 52 segundos.

E, por último, foi realizado a transferência do arquivos de 900 MB, sem a utilização do IPSEC, a sua marca foi de 78 segundos, com o modo AH 79 segundos, utilizando o modo ESP o tempo foi de 79 segundos, e por ultimo com o modo AH+ESP foi de 81 segundos.

Conclui-se que com esses testes arquivos de até aproximadamente 100 MB, não se encontra nenhum tipo de atraso na transferência de arquivos mesmo o pacote tendo passado pela criptografia ESP+AH, porém arquivos maiores de 500 MB que passam pela criptografia geram um atraso, podendo ocasionar lentidão em uma rede com muitos computadores.

6. Considerações Finais

O IPSEC garante que os dados sejam criptografados garantindo a segurança dos dados que navegam pela rede, protegendo-os, pois somente quem tem a chave de segurança pode ler esses dados.

Quando adicionado o cabeçalho AH o pacote aumenta cerca de 24 bytes do seu tamanho original, para que aja a autenticação no modo ESP os pacotes foram criptografados aumentando sua segurança, pois agora não é possível visualizar o conteúdo dos pacotes, e o seu tamanho também foi de 24 bytes.

Quando acionado os dois cabeçalhos em conjuntos (AH+ESP), ouve a autenticação e a criptografia, aumentando substancialmente sua segurança, e houve um aumento de 48 bytes nos pacotes transmitidos, ocasionando lentidão na rede pelo qual trafegam pois os pacotes necessitam ser autenticados, criptografados e para somente assim serem enviados, e na máquina que recebe necessita fazer o processo inverso receber, verificar a autenticidade dos pacotes e remover a criptografia.

Para arquivos de até 100MB, a utilização do IPSEC pode ser utilizada sem prejudicar o desempenho da rede não causando nenhum tipo de lentidão por conta da criptografia, e também foi possível demonstrar que o modo ESP tem um atraso um pouco maior que o modo AH, e com os dois modos ativados percebe-se que para arquivos grandes maiores que 500MB percebe-se um atraso pouco mais significativo na rede.

O IPSEC é uma importante ferramenta para administradores de rede, se devidamente configurada pode aumentar bastante a segurança da mesma, protegendo assim seus dados.

7. Referências

BRITO, H. O **Novo Protocolo da Internet**. São Paulo: Novatec, 2013.
CABEÇALHO. **Ipv6**, [2014?]. Disponível em: <http://ipv6.br/entenda/cabecalho/>. Acesso em: 10 abr. 2014.

ESGOTAMENTO.**Ipv6**, [2014?]. Disponível em: <http://ipv6.br/cronograma/>. Acesso em: 10 abr. 2014.

ENDEREÇANENTO.**Ipv6**, [2014?]. Disponível em:
< http://ipv6.br/entenda/enderecamento/>. Acesso em: 10 abr. 2014.

SEGURANÇA.**Ipv6**, [2014?]. Disponível em:
< ipv6.br/download/ipv6-seguranca-fisl13.pdf/>. Acesso em: 10 abr. 2014.

DAVIES, J. **Introduction to IP version 6**. Microsoft Corporation: 2004. **Technet**, 2002. Disponível em
< http://technet.microsoft.com/en-us/library/cc783437%28v=ws.10%29.aspx> Acesso em: 12 abr. 2014.

DIERKS, T; ALLEN, C. The TLS Protocol. **Ietf**, 1999. Disponível em:
<http://www.ietf.org/rfc/rfc2246.txt> Acesso em: 12 abr. 2014.

ESGOTAMENTO do IPv4 em nossa região (LACNIC**). Ipv6**, [2014?]. Disponível em:
< http://ipv6.br/estatisticas/>. Acesso em: 12 abr. 2014.

FARREL, A. **A Internet e seus Protocolos: Uma análise Comparativa**. Rio de Janeiro: Elsevier, 2005.

KRAWCZYK, H; BELLARE, M; CANETTI, R. HMAC: Keyed-Hashing for Message Authentication. **Ietf**, 1997. Disponível em:
<http://www.ietf.org/rfc/rfc2104.txt> Acesso em: 15 abr. 2014.

KENT, S; SEO, K. **Security Architecture for the Internet Protocol**. RFC 4301, IETF. 2005. Disponível em: < http://www.ietf.org/rfc/rfc4301.txt> Acesso em: 16 abr. 2014.

KUROSE, J. F.; ROSS Keith. W. **Redes de Computadores e a Internet:** uma abordagem top-down. São Paulo: Person Education, 2006.