UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

CRISTINA BASSO

IMPLEMENTAÇÃO DE IPSEC INTEGRADO COM O IPv6

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO
2011

CRISTINA BASSO

IMPLEMENTAÇÃO DE IPSEC INTEGRADO COM O IPv6

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas - da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Msc. Marcelo Zanetti

PATO BRANCO

2011

ATA Nº: **182**

DEFESA PÚBLICA DO TRABALHO DE DIPLOMAÇÃO DA ALUNA **CRISTINA BASSO**.

Às 08:10 hrs do dia 6 de julho de 2011, Bloco S da UTFPR, Campus Pato Branco, reuniu-se a banca avaliadora composta pelos professores Marcelo Zanetti (Orientador), Fábio Favarim (Convidado) e Fábio Rodrigues De La Rocha (Convidado), para avaliar o Trabalho de Diplomação da aluna Cristina Basso, matrícula 980358, sob o título **Implementação de IPSEC Integrado com o IPv6**; como requisito final para a conclusão da disciplina Trabalho de Diplomação do Curso Superior de Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, Coordenação de Informática. Após a apresentação a candidata foi entrevistada pela banca examinadora, e a palavra foi aberta ao público. Em seguida, a banca reuniu-se para deliberar considerando o trabalho **APROVADO**. Às 09:05 hrs foi encerrada a sessão.

Prof. Marcelo Zanetti, M.Sc.
Orientador

Prof. Fábio Favarim, Dr.
Convidado

Prof. Fábio Rodrigues De La Rocha, Dr.
Convidado

Prof. Omero Francisco Bertol, M.Sc.
Coordenador do Trabalho de Diplomação

Prof. Edilson Pontarolo, Dr.
Coordenador do Curso

AGRADECIMENTOS

Quero agradecer aos meus pais Antonio e Delci, que são meus pilares, e as pessoas mais importantes na minha vida, que me ensinaram a ser uma pessoa de caráter, com bons valores e princípios estando sempre ao meu lado, me apoiando nos momentos difíceis e sorrindo comigo nos momento alegres, me agüentando nos momentos de nervosismo.

A minha irmã Janaina e meu cunhado Ivan por sempre serem companheiros, e pelo meu lindo afilhado Arthur, por aumentar os momentos de alegria em minha vida.

Ao meu namorado Andres, que sempre esteve ao meu lado, me apoiando, sendo companheiro e me colocando para cima.

A algumas pessoas da minha família e amigos, que sempre estiveram comigo, em todos os momentos, e alguns colegas de trabalho que contribuíram para meu crescimento.

A alguns professores da universidade, em especial a Prof. Beatriz Borsoi, Prof. Soelaine Rodrigues Ascari e ao Prof. Robison Cris Brito por serem ótimas pessoas que sempre me animaram para seguir em frente, além de serem bons profissionais. Um agradecimento especial também ao Prof. Marcelo Zanetti que me auxiliou na monografia, sempre atencioso, dedicado e com paciência, me ajudando em tudo que precisei, sendo o principal idealizador desta conquista em minha vida.

“Não deixe que a saudade sufoque que a rotina acomode que o medo impeça de tentar.
Desconfie do destino e acredite em você. Gaste mais horas realizando que sonhando, fazendo que planejando, vivendo que esperando porque, embora quem quase morre esteja vivo, quem quase vive já morre”. (Luis Fernando Veríssimo)

RESUMO

BASSO, Cristina. Implementação de IPSEC Integrado com o IPv6. 2011. 66. Monografia (Tecnologia em Análise e Desenvolvimento de Sistemas). Pato Branco, 2011.

Devido ao rápido crescimento da Internet, está ocorrendo a falta de endereços *Internet Protocol version 4* (IPv4). Para atender a essa falta de endereços, deu-se a criação da nova versão do Protocolo IP, o protocolo IP versão 6 (IPv6), que irá progressivamente substituir o atual IPv4. Com a evolução da Internet além da falta de endereços surgiram problemas de segurança na comunicação de dado, a segurança é um fator muito importante que preocupa os usuários que utilizam a Internet. Este trabalho tem como finalidade demonstrar a utilização do protocolo IPv6 juntamente com o protocolo IP *Security Protocol* (IPSEC) que tem por objetivo garantir a segurança na transmissão de dados. Nesse trabalho são apresentados estudos referentes à nova versão do protocolo IP trabalhando em conjunto com o IPSEC. Posteriormente serão realizados estudos teórico-práticos sobre a implementação IPSEC em conjunto com o protocolo IPv6, a fim de documentar e realizar testes de laboratório de seu funcionamento e desempenho.

Palavras-chave: IPv6. IPSEC. Segurança de redes.

LISTA DE ABREVIATURAS E SIGLAS

3G	*3ª Geração*
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
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
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
OAKLEY	*Key Management Protocol*
PPP	*Point-to-point Protocol*
RFC	Request for Comments
RSVP	*Resource Reservation Protocol*
SA	*Security Association*
SAD	*Security Association Database*
SHA	*Secure Hash Algorithm*
SPD	*Security Policy Database*
SPI	*Security Parameter Index*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
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*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

Este capítulo apresenta as considerações inicias com uma visão geral do trabalho, os seus objetivos e a justificativa, bem como a organização do texto.

1.1 CONSIDERAÇÕES INICIAIS

> Atualmente a Internet está bastante difundida nas empresas, e tem mudado a maneira como os negócios são feitos, sendo utilizada para comunicação e troca de dados. Segundo um levantamento chamado "Estado da Internet", no dia 23/02/2011 pela Exceda, empresa de fornecimento de serviços para aceleração de aplicações e distribuição de conteúdo na web e representante da Akamai na América Latina, referente ao terceiro trimestre de 2010, mostra que o País ocupa o oitavo lugar na lista de conexões à Internet, com 13 milhões pontos de conexão*,* fornecendo acesso à Internet para 73,9 milhões de pessoas, 20% a mais que em 2009, sendo que em 2006 tinha apenas 4 milhões. (EXCEDA, 2011).

De acordo com a Fundação Getúlio Vargas (FUNDAÇÃO GETÚLIO VARGAS, 2011), o Brasil possui 60 milhões de computadores em uso, devendo chegar a 100 milhões em 2012.

Segundo a NIC.br (NIC.BR, 2009), os benefícios obtidos através das vendas pela Internet podem ser expressados pelos seguintes dados: 70% das empresas alegaram menor custo de negócio, 65% maior qualidade de serviços para o consumidor, 64% tempo de transação reduzido, 60% possibilidade de focar os consumidores individualmente, 59% equiparar-se a concorrência, 51% maior número de vendas e consumidores. Todavia a pesquisa revela que ainda 54% das empresas não adotaram nenhuma medida de apoio a segurança.

Para que essa troca de informações aconteça são necessários protocolos para estabelecer a comunicação entre uma origem e um destino, sendo o *Internet Protocol version 4* (IPv4 – (REY,1981)) o mais utilizado. Porém como a popularização da Internet aconteceu de uma forma muito rápida, ocorreu a escassez de endereços. Para suprir a necessidade de endereços IP foi projetado uma nova versão desse protocolo sendo chamada de *Internet Protocol version 6* (IPv6 – (DEERING; HINDEN, 1998)). Essa nova versão do protocolo IP além de possuir um espaço de endereçamento muito maior, também traz a possibilidade de trabalhar

com alguns mecanismos de segurança como o *IP Security Protocol* (IPSEC - (KENT; SEO, 1995)).

Muitas falhas de segurança que ocorrem nas empresas vêm do próprio ambiente interno. O IPv6, integrado com o IPSEC pode prevenir essas falhas, auxiliando a corporação a verificar quem tem ou não acesso a determinadas informações confidenciais.

Devido à influência que o protocolo de comunicação IP desempenha em relação à comunicação através da Internet, é apresentado nesse trabalho estudos referente à nova versão do protocolo IP trabalhando em conjunto com o IPSEC.

1.2 OBJETIVOS

A seguir é descrito o objetivo geral e os objetivos específicos do presente trabalho.

1.2.1 Objetivo geral

Realizar um estudo teórico-prático sobre a implementação IPSEC em conjunto com o protocolo IPv6, a fim de documentar, assim como realizar testes de laboratório de seu funcionamento e desempenho.

1.2.2 Objetivos específicos

- Estudar o IPv6;
- Estudar a implementação do IPv6 com o IPSEC;
- Estudar as formas de funcionamento do 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;
- Realizar a configuração do IPSEC em modo AH e ESP;
- Avaliar o desempenho do protocolo IPSEC em redes IPv6.

1.3 JUSTIFICATIVA

Este trabalho deve contribuir como fonte de estudo para quem necessita de alternativas mais seguras para redes de computadores, na qual a comunicação é feita utilizando o protocolo IP. Atualmente a versão mais utilizada deste protocolo é o IPv4, porém deve ser substituído em poucos anos pelo IPv6.

Praticamente todas as operações de uma empresa são feitas através da Internet, sejam elas, compras, trocas de mensagens, pagamentos, entre outros. Desta forma é necessário um maior nível de segurança na rede. Pensando em novos mecanismos de segurança o protocolo IP versão 6 foi criado para trabalhar em conjunto com o IPSEC.

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 para um grupo de funcionários, sendo que somente estes possam compartilhar seus conteúdos. 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.

Nesse trabalho será verificado o funcionamento e a aplicabilidade dos cabeçalhos *Authentication header* (AH) e *Encapsulating Security Payload* (ESP) do IPSEC quando integrado com o IPv6, para posteriormente propor algumas soluções de segurança.

Primeiramente é será feita uma pesquisa referente ao IPv6 e ao IPSEC, posteriormente serão estudadas ferramentas livres do IPSEC. Feito isso serão montados cenários de testes com os cabeçalhos AH e ESP do serviço IPSEC, que serão avaliados, para verificar o seu desempenho trabalhando em conjunto com o IPv6.

1.4 ORGANIZAÇÃO DO TEXTO

O Capítulo 2 contém o referencial teórico que fundamenta a proposta conceitual dos testes desenvolvidos. O referencial teórico está centrado No estudo do IPv6 com IPSEC.

No Capítulo 3 esta o desenvolvimento dos testes, os materiais utilizados com as tecnologias e as ferramentas utilizadas, e o método, com as principais atividades realizadas, no desenvolvimento deste trabalho.

No Capítulo 4 está a conclusão com as considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta o referencial teórico necessário para o entendimento deste trabalho. Em seguida é realizada uma descrição dos protocolos IP na versão 4 (IPv4) e 6 (IPv6), a qual é utilizada nos testes de laboratório, e também a integração da especificação 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).

São responsáveis por quais mensagens serão enviadas e recebidas, o formato de cada uma, a ordem, os caminhos que devem seguir e as ações a serem tomadas na hora de transmissão e da recepção, ou seja, os protocolos são necessários para gerenciar recursos de rede, a fim de controlar seu comportamento. Qualquer comunicação entre processos em uma rede de computadores é baseada em troca de mensagens. Quando vários processos precisam fazer a comunicação é necessário que sejam adotados protocolos, para que essas mensagens possam ser entendíveis pelo emissor e receptor.

Por exemplo, se duas pessoas estão tentando se comunicar e uma fala a língua inglesa e outra alemã, elas não irão conseguir, pois a língua que estão falando não é entendível por ambos os participantes da comunicação, o mesmo ocorre com as redes de computador, é necessário um protocolo que estabeleça as regras, para que a comunicação seja entendível pelo emissor e receptor.

Em redes de computadores existem diversos protocolos. 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).

2.1.1 Arquitetura TCP/IP (*Transmission Control Protocol*/*Internet Protocol*)

Por ser a Arquitetura mais utilizada atualmente, o TCP/IP obrigou que todos os fabricantes de sistemas operacionais de rede tenham suporte a ela.

O TCP/IP forma uma pilha de protocolos de comunicação entre computadores em rede, a origem do seu nome vem de dois protocolos, TCP e IP. Cada camada desta pilha é responsável por um grupo de tarefas. (TANENBAUM, 2003).

As camadas mais altas, iniciando pela Camada de Aplicação, lidam com dados mais abstratos, e as mais baixas, iniciadas pela Camada Física, realizam tarefas de menor nível de abstração. A Figura 1 ilustra as camadas da arquitetura TCP/IP e os principais protocolos de cada camada.

Camadas	Exemplos de Protocolos utilizados
Aplicação	HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS
Transporte	TCP, UDP, RTP, SCTP, DCCP
Rede	IP (IPv4, IPv6) , ARP, RARP, ICMP, IPsec
Enlace	Ethernet, WiFi, HDLC, Token ring, FDDI, PPP,Switch ,Frame relay
Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB

Figura 1 – Camadas TCP/IP
Fonte: Autoria própria (2011).

Como ilustrado na Figura 1 é possível ver que o protocolo IP está localizado na camada de rede, camada esta responsável por estabelecer a comunicação lógica

entre computadores. É nessa camada que é realizado o endereçamento das máquinas na rede.

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; ROSS, 2006). Estes endereços podem ser utilizados para indicar uma rede ou apenas um host individual. Para identificar a rede é necessário utilizar a máscara de rede após o IP.

Os números endereços de IPs disponíveis na versão quatro não são suficientes para atender a demanda atual da Internet. Por esse motivo estão sendo utilizados alguns mecanismos como citados abaixo para adiar o esgotamento dos endereços IPv4. 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.

No entanto, mesmo com todos esses mecanismos o esgotamento dos endereços IPv4 devem ocorrer em pouco tempo. Várias empresas já estão realizando a migração para o protocolo IPV6.

2.3 PROTOCOLO IPV6

É 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, 2011).

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 ($4x10^9$) , contra cerca de $3,4x10^{38}$ endereços da nova versão. A previsão para o esgotamento da antiga versão do protocolo está prevista para um futuro próximo (SANTOS et al., 2010).

Esta versão oferece melhorias, comparada à versão anterior, os seus cabeçalhos foram alterados para um melhor aproveitamento e desempenho. A quantidade de endereços nesta versão é muito maior, pois ela, ao contrário da antiga versão já foi criada para suportar a demanda futura de endereços IP.

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 testando a utilização do IPv6 (NETWORK WORLD, 2011). Provedores como a Global Crossing, da CTBC, e da Telefônica já fornecem trânsito IPv6 comercialmente no Brasil. Devido à importância de implantação desta nova versão do IP os governos têm começado a apoiar esta implantação. (IPv6.BR, 2011).

2.3.1 Novas Características

De acordo com a Tabela 1, pode-se visualizar algumas diferenças entre o Protocolo IP versão 4 e 6.

Tabela 1 - Diferenças entre IPv4 / IPv6

	IPv4	Ipv6
Tamanho do Endereçamento	32 bits	128 bits
Agrupamento de Bits	8 em 8	16 em 16
Forma de Representação	Decimal	Hexadecimal
Suporte ao IPSEC	Opcional	Obrigatório

Fonte: Autoria própria.

O Ipv6 possui algumas novidades em relação ao IPv4, tais como: (Ipv6.br, 2011).

- 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 o bom funcionamento do IPv6 algumas limitações do IPv4 deviam ser analisadas. Com a criação da RFC 1755 (PEREZ, 1995), que resume os requisitos

para o IPv6, foi possível que os criadores do novo protocolo considerassem todas as limitações do IPv4 ao mesmo tempo. Algumas dessas restrições segundo (FARREL, 2005, p.66) foram:

- Prover um serviço de datagrama não confiável (como IPv4);
- Prover suporte *unicast* e *multicast*;
- Assegurar que o endereçamento é adequado além de um futuro previsível;
- Ser compatível com o IPv4, para que as redes existentes não precisem reinstaladas, enquanto ainda provê um caminho simples de migração do IPv4 para o IPv6;
- Prover suporte para autenticação e criptografia;
- A simplicidade arquitetônica deverá incorporar alguns recursos "adicionais" do IPv4 que foram acrescentados com o passar dos anos;
- Não fazer suposições sobre a topologia física, mídia ou capacidades da rede;
- Não fazer nada que afete o desempenho de um roteador encaminhando datagramas;
- O novo protocolo precisa ser extensível e capaz de evoluir para atender às necessidades de serviço futuras da Internet;
- É preciso haver suporte para hosts móveis, redes e interconexões de redes;
- Permitir que os usuários criem interconexões de redes privadas em cima da infra-estrutura básica da Internet.

Quando o IPv4 foi projetado o seu objetivo era atender apenas instituições governamentais e educacionais, todavia o mesmo passou a ser utilizado com fins comercias a partir de 1993 e percebeu-se que em poucos anos estes endereços iriam se esgotar, isso só não ocorreu porque foram criadas medidas para o não esgotamento, tais como a criação de classes, o NAT, CIDR, VLSM, já citados anteriormente.

Alguns outros fatores também incentivam a implantação do IPv6, tais como:

- Os dispositivos estão cada vez mais interligados com a Internet, hoje em dia a maioria das pessoas não possuem somente um computador

que possui Internet, mais sim vários dispositivos móveis, e para que essa expansão continue ocorrendo são necessários mais endereços IPs, podendo imaginar-se a partir daí, a criação de eletrodomésticos, carros, edifícios, equipamentos inteligentes, conectados a rede. O fato da abundância de endereços IPv6 irá contribuir muito para esta evolução;

- Com a inclusão digital, a expansão das redes está cada vez mais acelerada, através de redes de terceira geração (3G), por exemplo, necessitando cada vez mais IPs;
- Que o IPv6 suporte a mobilidade, podendo conectar os dispositivos que utilizarem a Internet em qualquer rede, através de seu endereço IP de origem;
- A qualidade dos serviços irá melhorar, pois o IPv6 irá permitir o amadurecimento dos serviços que hoje ainda são iniciantes, como o VoIP, streaming de vídeo em tempo real, entre outros e fará com que novos serviços possam surgir.

Conforme a Figura 2 mais de 400 Sistemas Autônomos brasileiros já têm alocações IPv6. Segundo a RFC 1930 (HAWKINSON; BATES, 1996), um Sistema Autônomo é um grupo de redes e *gateways,* ou seja, uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos sob a gerência de uma mesma entidade administrativa.

Dentro de um mesmo sistema autônomo, os gateways estão livres para escolher os seus próprios mecanismos para obter, propagar, validar a consistência de rotas, ou seja, se a rota está apta a entregar o pacote sem problemas, ao passo que gateways pertencentes a sistemas autônomos diferentes devem negociar a forma de operação entre si.

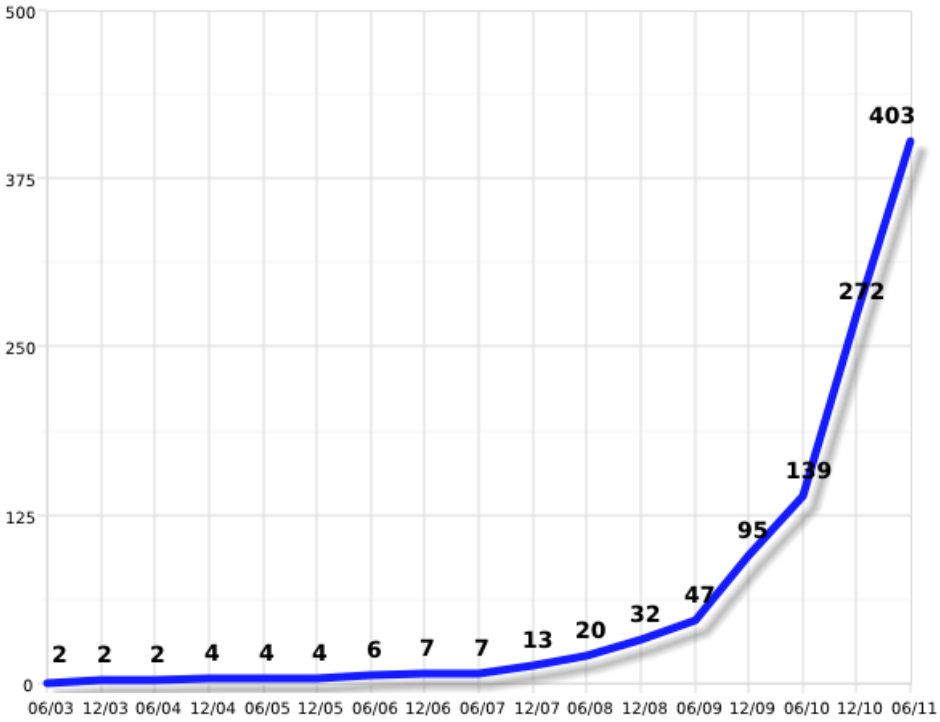

Figura 2 - Sistemas Autônomos brasileiros com alocações IPv6
Fonte: IPv6.BR (2011)

2.3.2 Endereçamento

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.

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).

Na Figura 3, podem ser visualizadas duas redes iguais, porém uma utilizando o endereços IPv6 e uma IPv4.

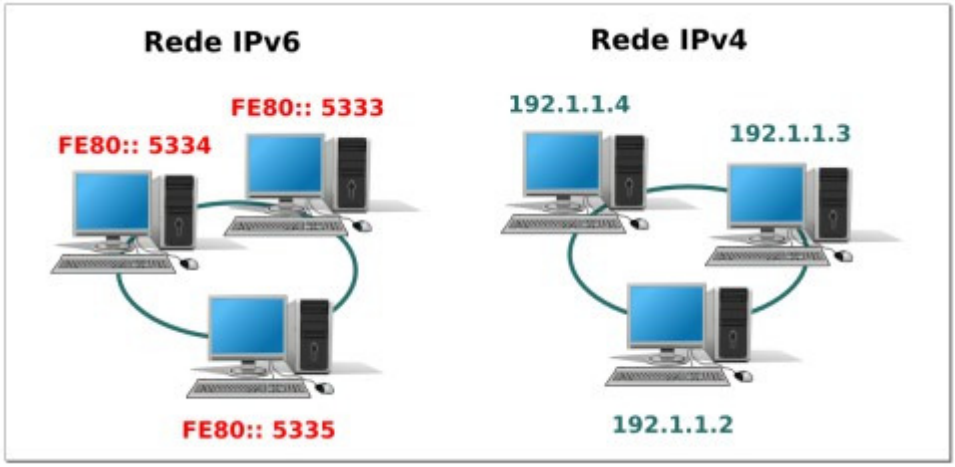

Figura 3 - Comparação de endereçamento IPv4 e IPv6
Fonte: MORIMOTO (2008)

O IPv6 faz agrupamento de 16 em 16 bits, cada caractere representa 4 bits (16 combinações), sendo representados de forma hexadecimal, com oito quartetos de caracteres em hexa, separados por ":", além dos números de 0 a 9 e os caracteres A, B, C, D, E e F, que representam os números 10, 11, 12, 13, 14 e 15, respectivamente, segundo a tabela de número hexadecimais.

A Figura 4 ilustra um endereço IPv6, explicando a sua sintaxe.

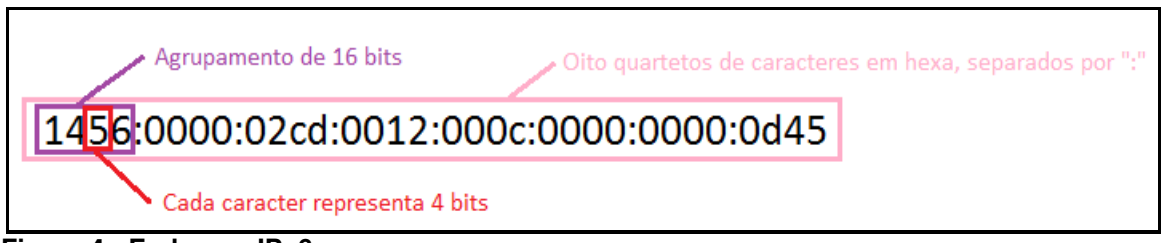

Figura 4 - Endereço IPv6
Fonte: Autoria própria (2010).

Deste modo ficou mais fácil a representação dos endereços, necessitando de menos dígitos e menos pontos para separar os campos agrupados, e para simplificar ainda mais os endereços, já que são mais extensos que a antiga versão, podem ser abreviados os espaços onde a sequência é seguida por zeros colocando apenas o separador ":", esta redução poderá ser utilizada apenas uma vez para impedir valores repetidos, também pode-se omitir os zeros à esquerda dos quartetos, em vez de escrever "0123", você pode escrever apenas "123"; em vez de "0001" apenas "1" e, em vez de "0000" apenas "0". Os endereços podem ser escritos em letra maiúscula ou minúscula. A Figura 5 mostra primeiramente um endereço IPv6 sem nenhuma abreviação, no segundo endereço são abreviados os zeros, alterando de

“0000” para apenas “0” e no terceiro endereço os zeros contínuos são alterados apenas por “::”.

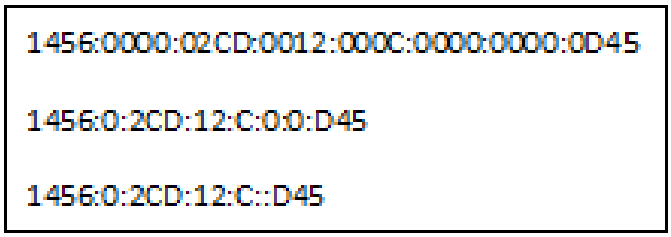

Figura 5 - Exemplo de Endereço IPv6 e suas abreviações
Fonte: Autoria própria.

2.3.2.1 Representação de Prefixos

A representação dos prefixos continua sendo apresentada da mesma maneira do IPv4, utilizando a notação CIDR. Os endereços são representados através de “endereço-IPv6/tamanho do prefixo”.

Este exemplo de prefixo de sub-rede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

Prefixo **2001:db8:3003:2::/64**
Prefixo global **2001:db8::/32**
ID da sub-rede **3003:2**

Com este tipo de representação é possível identificar a topologia de rede, segundo parâmetros, como posição geográfica, identificação da rede, como são distribuídos de forma hierárquica, o procedimento feita pela tabela de roteamento se torna mais simples, diminuindo o tempo de encaminhamento dos pacotes.

Para representar as *Uniform Resource Locators* (URLs), em IPv6, os endereços passam a ser inseridos entre colchetes, evitando assim ambiguidade quando a porta é apresentada juntamente com o endereço.

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

2.3.2.2 Tipos de Endereçamento

No Ipv6 existem três tipos de endereços:

- *Unicast*;
- *Anycast*;
- *Multicast*.

2.3.2.2.1 *Unicast*

Este tipo de endereço faz a identificação somente de uma interface, com isso os pacotes enviados a endereços unicast terão uma interface de destino única.

São utilizados para comunicação entre dois nós, por exemplo, comunicação de Voz sobre IPv6, máquinas de uma rede privada, entre outros. Sua estrutura permite agregações com prefixos de tamanho flexível. Tipos de Endereços *Unicast*:

- *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, conforme Tabela 2.

Tabela 2 - Estrutura Global Unicast

3	13	8	24	16	64 bits
FP	TLA ID	RES	NLA ID	SLA ID	InterfaceID

Fonte: (IPv6.BR, 2011)

Similar aos endereços públicos do IPv4, o Global Unicast é Globalmente roteável e acessível na Internet.

- *Link Local:* Faixa de Endereçamento FE80::/10: Deve ser utilizado apenas localmente, ou pode ser usado apenas no enlace específico onde a 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.

- *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. O ULA é inserido pelo administrador da rede e pode ser utilizado por um conjunto limitado de enlaces.

2.3.2.2.2 *Anycast*

Identifica um conjunto de interfaces, quando é enviado um pacote para um endereço anycast, é feita uma verificação através dos algoritmos de roteamento para identificar o conjunto mais próximo, e é para a interface deste conjunto que os pacotes são entregues.

Os endereços anycast são atribuídos a partir de endereços unicast e não há diferenças sintáticas entre eles. Quando um endereço unicast é atribuído a mais de uma interface, passa a ser considerado um endereço *anycast*, neste caso devem-se configurar explicitamente os nós para que saiba que lhe foi atribuído um endereço *anycast*.

Um endereço *anycast* pode descobrir serviços na rede, verificando onde está localizado o servidor mais próximo, tais como, servidores Sistema de Nomes de Domínios (DNS), Protocolo de Transferência de Hipertexto (HTTP), garantindo a redundância desses serviços. Quando vários *hosts* ou roteadores oferecem o mesmo serviço, estes endereços podem fazer o balanceamento de carga, localizando roteadores que forneçam acesso a uma determinada sub-rede ou para localizar os agentes de origem em redes com suporte a mobilidade IPv6.

2.3.2.2.3 *Multicast*

Identifica um conjunto de interfaces, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço, e não somente para a mais próxima.

No IPv6 não existem mais endereços *broadcast*, sendo que essa função de atribuição de direcionamento de um pacote para todos os nós de um mesmo domínio foi repassada para tipos específicos de endereços *multicast*. A diferenciação dos dois tipos de endereços é apenas pelo fato que no *broadcast* o pacote é enviado a todos os hosts da rede, sem exceção, enquanto no *multicast* apenas um grupo de hosts receberá o pacote. Com isso há uma redução de utilização de recursos de uma rede, pois ele transporta apenas uma cópia dedos a todos os elementos do grupo. Isso auxilia na otimização de dados aos hosts receptores. Videoconferências, vídeos, jogos on-line, atualizações de software podem utilizar as vantagens apresentadas pelo *multicast*.

No IPv4, o suporte a *multicast* é opcional, já que foi introduzido apenas como uma extensão ao protocolo, porém o suporte a *multicast* é obrigatório em todos os nós IPv6, muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço.

Os endereços *multicast* derivam do bloco FF00::/8. O prefixo FF é seguido de quatro bits utilizados como *flags* e mais quatro bits que define o escopo do grupo *multicast.* Os 112 bits restantes são utilizados para identificar o grupo multicast.

2.3.3 Cabeçalhos do IPv6

> Os cabeçalhos do IPv6 possuem 40 bytes, duas vezes maior que o do IPv4, é mais flexível e tem a possibilidade de ser estendido através de cabeçalhos adicionais. É mais eficiente que o cabeçalho da antiga versão, pois minimiza o *overhead* e reduz o custo do processamento dos pacotes (SANTOS et al., 2010).

Para tornar o cabeçalho mais simples, foram realizadas algumas mudanças no formato do cabeçalho, possui agora apenas oito campos, além de ser mais flexível, pois pode possuir cabeçalhos adicionais que não precisam ser processados por todos os roteadores intermediários. A Figura 6 exibe o cabeçalho IPv6.

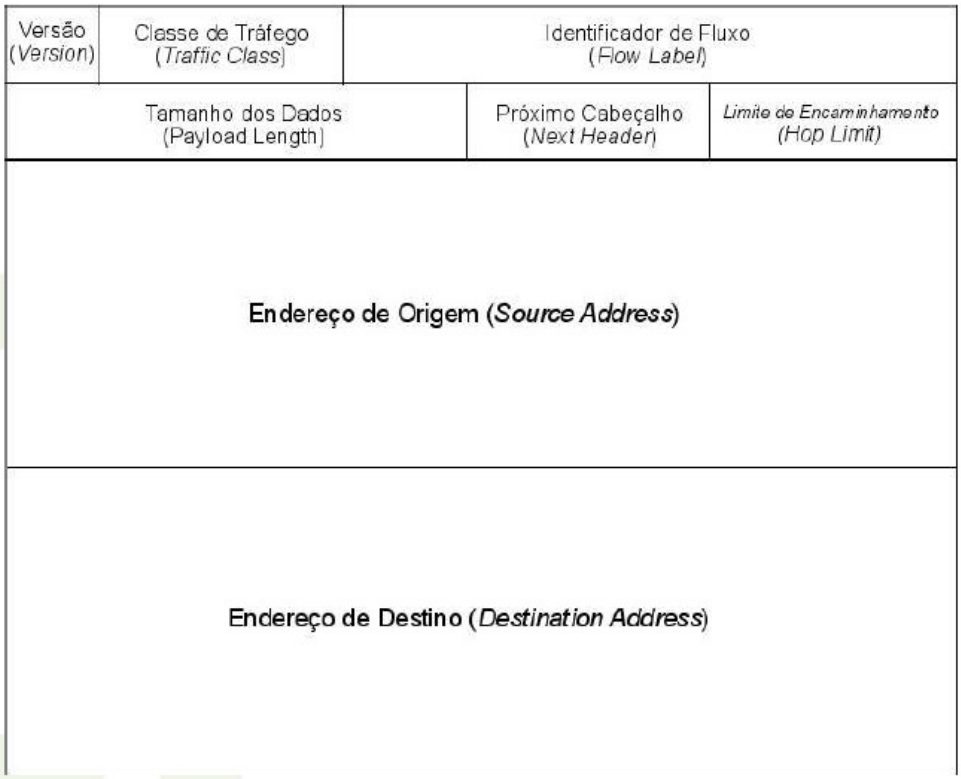

Figura 6 - Cabeçalho IPv6
Fonte: NIC.BR (2009)

Campos do Cabeçalho IPv6:

- **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.

2.3.3.1 Cabeçalhos de Extensão

O cabeçalho de extensão tem por objetivo tratar informações opcionais ou adicionais, localiza-se entre o cabeçalho base e o cabeçalho da camada de transporte, não havendo quantidade nem tamanho fixo para estes cabeçalhos, pois eles são utilizados conforme a necessidade. Caso haja múltiplos cabeçalhos de extensão no mesmo pacote, eles são adicionados em série, formando uma cadeia de cabeçalhos.

A utilização destes cabeçalhos visa aumentar a velocidade de processamento nos roteadores, pois o único cabeçalho que é processado em cada roteador é o *Hop-by-Hop,* que é utilizado para transportar informação opcional ou adicional que deve ser processada por todos os nós no caminho do pacote (IPv6.BR, 2011), e os demais pelo nó identificado no campo Endereço de Destino do cabeçalho base.

Podem-se adicionar novos cabeçalhos de extensão sem a necessidade de alterar o cabeçalho base, como mostra a Figura 7:

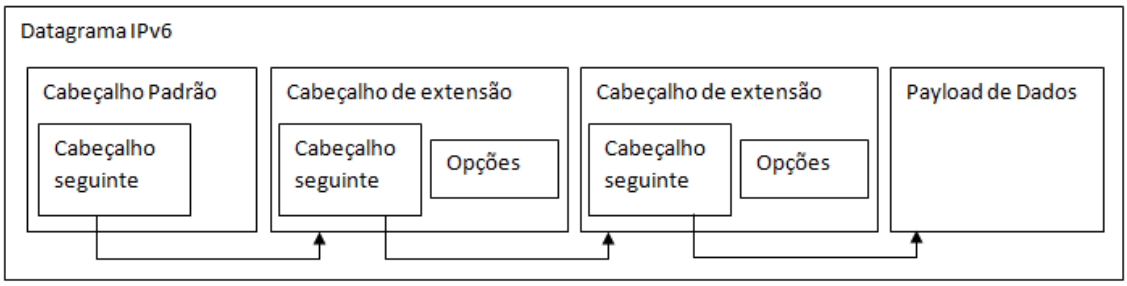

Figura 7 - Cabeçalhos de extensão
Fonte: FARREL (2005)

O IPv6 possui seis cabeçalhos de extensão:

- *Hop-by-Hop Options* (Opções de Salto-a-Salto);
- *Destination Options* (Opções de Destino);
- *Routing* (Rota de Origem);
- *Fragmentation* (Fragmentação);
- *Authentication Header* (Autenticação);
- *Encapsulating Security Payload* (Encapsulamento seguro).

Como o foco desse trabalho é 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.

2.4 IPSEC

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)).

Desde o início da criação do IPv6 a questão da segurança foi bastante analisada, mecanismos de segurança passam a fazer parte do protocolo IPv6, sendo que qualquer par de dispositivos de uma conexão fim-a-fim possam usufruir desta segurança, com métodos que visam garantir a segurança dos dados que trafegam pela rede.

> 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 a 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 adulteradas e para ocultar informações de olhos não autorizados. (FARREL, 2005 p.484).

2.4.1 Características e Funções do IPSEC

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, conforme pode ser visualizado na Figura 8.

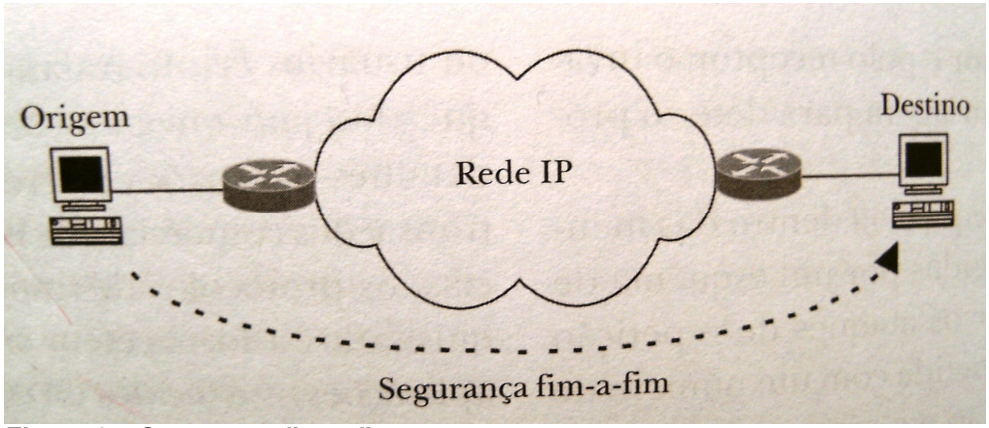

Figura 8 – Segurança fim-a-fim
Fonte: FARREL (2005 p. 488).

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

2.4.2 Arquitetura de segurança

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

2.4.2.1 Modo de transporte

No modo transporte, o emissor e receptor da comunicação segura necessitam de suporte ao IPSEC. 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 9.

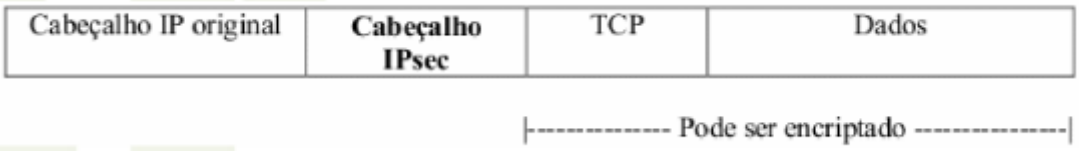

Figura 9 - Modo Transporte
Fonte: NIC.BR (2009)

2.4.2.2 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.

Na Figura 10 pode-se observar que o cabeçalho IP original, TCP e dados, foram encapsulados dentro de outro cabeçalho IP, criando um novo cabeçalho externo para comunicação com outros dispositivos do túnel.

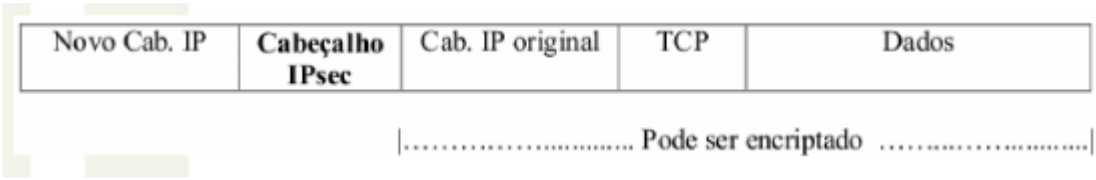

Figura 10 - Modo Túnel
Fonte: NIC.BR (2009)

2.4.3 Propriedades de Segurança

- Confidencialidade: Processo que objetiva manter dados escondidos de pessoas não autorizadas. (RICCI, 2007).
- 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).
- 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).

Quando o modo ESP do IPSEC é utilizado está se garantindo a confidencialidade na transmissão de dados. O modo AH garante a autenticidade e integridade.

2.4.4 Associação de 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:

- Estática: Os parâmetros são inseridos manualmente no ponto de origem e destino da comunicação;
- Dinâmica: Os parâmetros são gerenciados por protocolos como o IKE, não necessita da manipulação do administrador.

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

2.4.5 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).

IKE (Internet Key Exchange)

> 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).

2.4.6 Frameworks de Segurança do IPSEC (AH e ESP)

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:

- Criptografia:
    - *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).
    - 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, decriptado com a segunda chave e finalmente encriptado 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).
    - 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).

- 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).
    - 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).
    - 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).

2.4.6.1 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.

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.

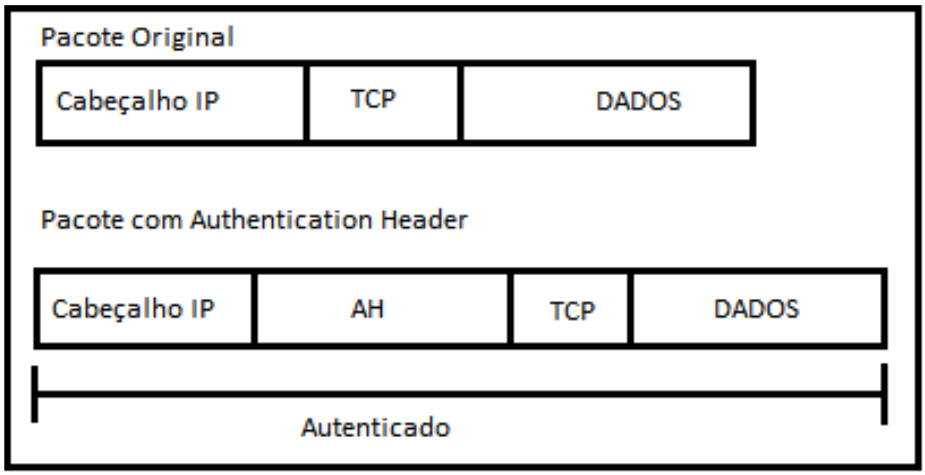

Figura 11 - AH (*Authentication Header*)
Fonte: RICCI (2007 p.176)

O Cabeçalho AH contém seis campos:

> Próximo Cabeçalho: Contém o identificador do protocolo do protocolo do próximo cabeçalho. É o mesmo valor atribuído ao campo Protocolo no cabeçalho IP original.
> Tamanho do Dado: Comprimento do cabeçalho de autenticação e não o comprimento do dado, como pode ser confundido com o nome do campo.
> Reservado: 16 bits reservados para extensão do protocolo.
> SPI (*Security Parameter Index*): Este índice, em conjunto com o protocolo AH e o endereço fonte, indica unicamente uma SA para um determinado pacote.
> Número de Sequência: Contador que identifica os pacotes pertencentes a uma determinada SA.
> 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. (SILVA, 2005 p. 79).

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.

2.4.6.1.1 AH + 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.

2.4.6.1.2 AH + Modo de operação Túnel

Com este modo de operação, os endereços IP do *gateway* e a fonte serão autenticadas, não permitindo esconder o endereço IP da rede local. Não permite a tradução de endereços NAT, conforme Figura 12.

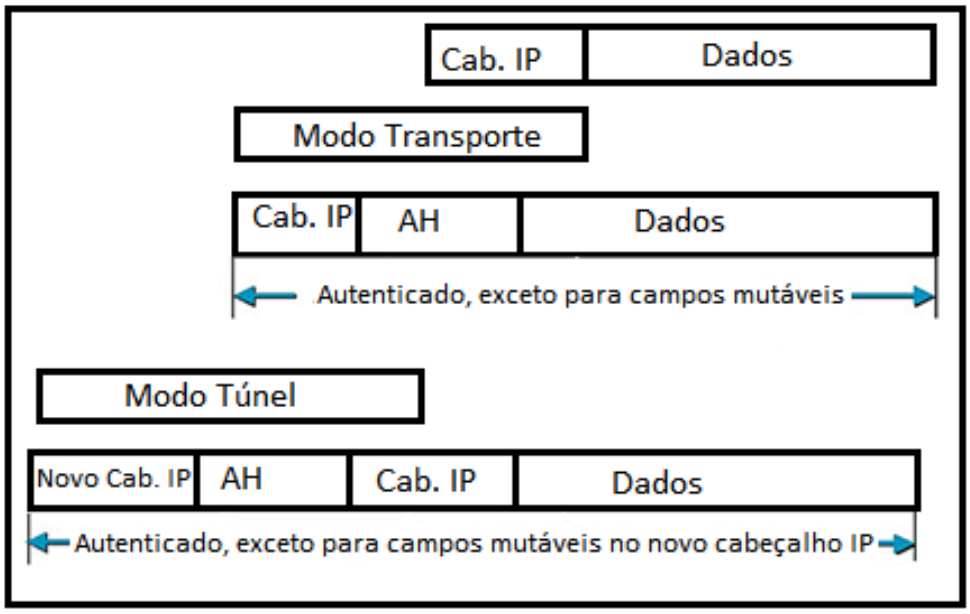

Figura 12 - Modos de operação com o AH
Fonte: Adaptado de: (MANSON, 2011.)

2.4.6.2 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,

Garante que 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 descriptografia 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.

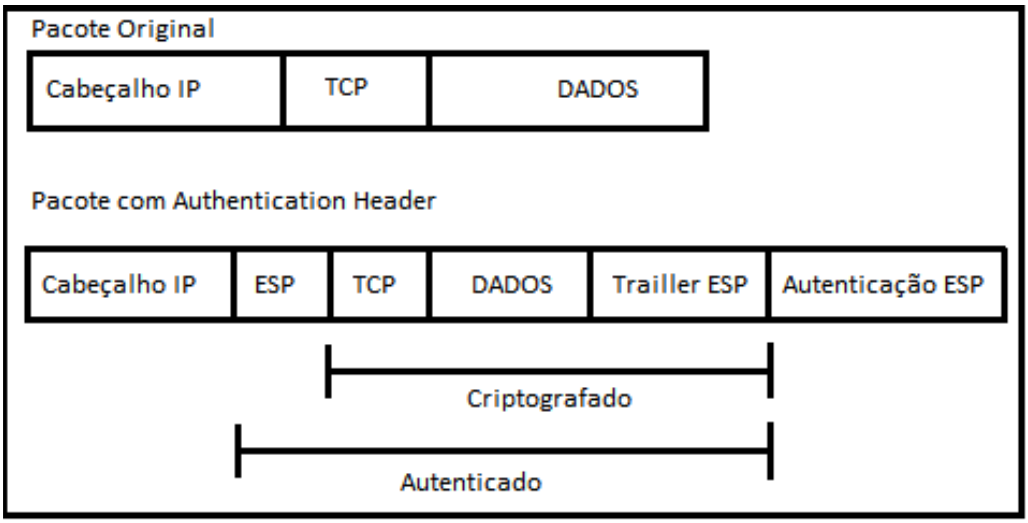

Figura 13 - ESP (*Encapsulating Security Payload*)
Fonte: RICCI (2007 p.177)

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 13.

> Como pode-se 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 descriptografar as informações e remontá-lo antes de deixá-lo continuar dentro da rede destino. (SILVA, 2005 p. 82).

2.4.6.2.1 ESP + 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.

2.4.6.2.2 ESP + 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.

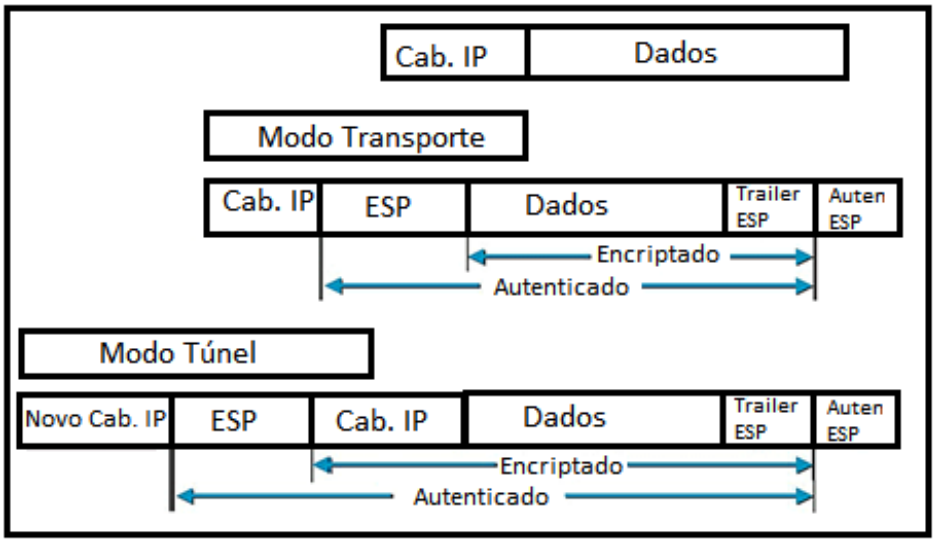

Figura 14 - Modos de operação com o ESP
Fonte: Adaptado de: (MANSON, 2011.)

O cabeçalho AH e ESP podem ser utilizados paralelamente.

3 DESENVOLVIMENTO

Este capítulo apresenta os materiais e o método utilizados na realização deste trabalho. Os materiais se referem às tecnologias e ferramentas utilizadas nos testes de laboratório, para a análise e comparação dos resultados. O método contém as etapas com os principais procedimentos utilizados para os testes.

3.1 MATERIAIS

Para o desenvolvimento dos testes de tamanho dos pacotes, foram utilizadas duas máquinas virtuais, para análise de desempenho, dois computadores interligados por um Switch, pacote ipsec-tools para configuração do IPSEC, Wireshark para análise dos pacotes.

3.1.1 Ferramenta Ipsec-tools para administração do IPSEC

O IPsec-Tools (IPSEC-TOOLS, 2011) começou como precursor dos utilitários IPsec para a plataforma Linux. O componente mais importante deste software é um avançado *Daemon Internet Key Exchange,* que pode ser usado para conexões automaticamente chave IPsec.

O Pacote ipsec-tools contém alguns utilitários para manipular conexões IPSec com o Linux-2.6.

- **libipsec:** Biblioteca com a implementação PF_KEY;
- **setkey**: Ferramenta para manipular e despejar o kernel *Security Policy Database* (SPD) e *Security Association Database* (SAD);
- **racoon:** *Internet Key Exchange Daemon* (IKE) automático para conexões com chave Ipsec**;**
- **racoonctl:** A ferramenta de controle baseado em shell para racoon,

Existem também outras ferramentas para configurar e gerenciar IPSEC, como a FreeS/WAN (LINUX FREES/WAN, 2011), QuickSec (QUICKSEC, 2011), porém o ipsec-tools é a ferramenta que possui maiores referências literárias e configuração mais acessível.

3.1.4 Wireshark

É um software para análise de pacotes que recebe contribuições de especialistas em rede de todo o mundo, é a continuação de um projeto que começou em 1998. Este programa faz a verificação dos pacotes transmitidos pela rede através de dispositivos de comunicação (ex: placa de rede) do computador. É classificado como um *sniffer*, que tem a função de verificar se há problemas na rede, conexões suspeitas ou outras atividades relacionadas à rede.

A organização dos pacotes é feita de acordo com o protocolo, semelhantes ao *tcpdump* (TCPDUMP/LIBPCAP, 2011), porém o Wireshark possui interface gráfica, conforme visualizado na Figura 15.

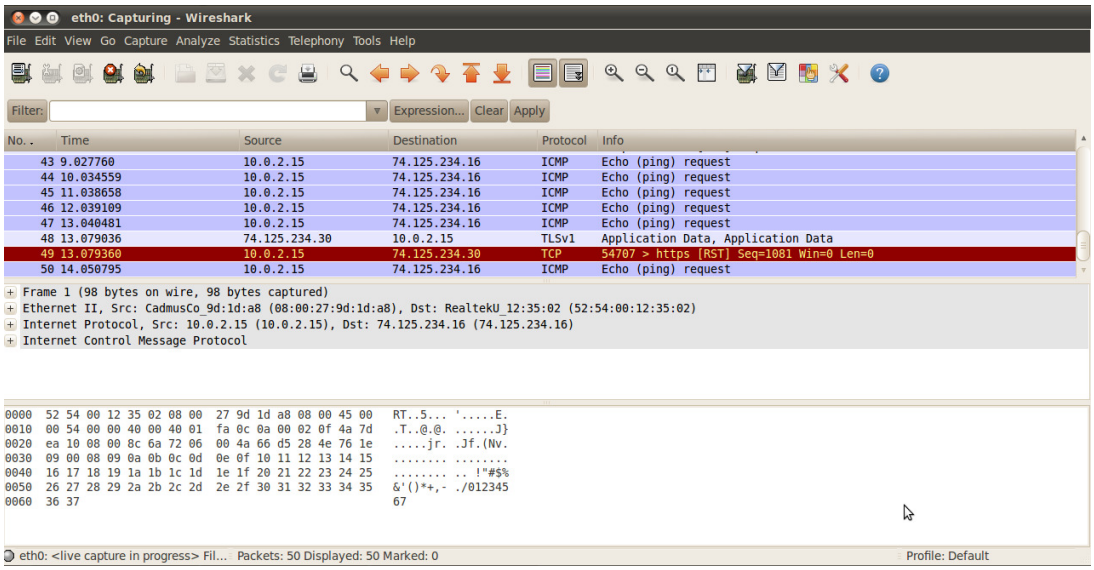

Figura 15 - Wireshark
Fonte: Autoria própria.

Com isso é possível controlar o tráfego de uma rede, podendo visualizar todos os pacotes que entram e saem, ou de qual rede um determinado pacote faz parte, através de uma lista organizada, facilitando sua posterior análise.

Também é possível controlar o tráfego de um determinado dispositivo de rede, ou de vários. Em casos de redes locais, com computadores ligados a um hub ou switch, outro usuário do Wireshark pode capturar todas as suas transmissões.

Segundo o site do Wireshark (WIRESHARK FOUNDATION, 2011), seguem alguns recursos:

- Dados podem ser capturados da *Ethernet*, FDDI, PPP, *Token-Ring*, IEEE 802.11, IP clássico sobre ATM e interface *loopback*;
- Os arquivos capturados podem ser editados e convertidos via linha de comando. 750 protocolos podem ser dissecados;
- A saída pode ser salva ou impressa em texto plano ou *PostScript*;
- A exibição de dados pode ser refinada usando um filtro;
- Filtros de exibição podem ser usados para destacar seletivamente e exibir informações coloridas no sumário;
- Todas as partes dos traços de rede capturados podem ser salvas no disco.

3.2 MÉTODO

O método utilizado para a realização deste trabalho reflete as etapas utilizadas para configurar um ambiente operacional de teste para a implementação de IPv6 integrado com o IPSEC.

Em um primeiro momento foram realizados estudos sobre ao protocolo IPv6. Nessa etapa verificou-se 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 teóricos, foram estudadas as ferramentas para realizar a configuração do IPSEC. Logo em seguida foram realizados testes de

configuração do IPv6 e do IPSEC. Depois de realizar testes de configuração foram realizados testes de desempenho do funcionamento do IPSEC e conjunto com o IPv6.

3.2.1 Configurando o IPv6

FASE 1: É utilizada a faixa de endereçamento FC00::1000/116 para o endereçamento IPv6, simulando a rede da UTFPR Pato Branco, esta faixa pode conter 4.094 números de endereços válidos (fc00::1001 até fc00::1ffe), o que seria um número maior do que o número de máquinas utilizadas na UTFPR.

Na máquina 1 adiciona-se o endereço FC00:1001/116 e na máquina 2 FC00:1002/116, de acordo com o Quadro 1, onde eth1 é a placa de rede em que o IPv6 foi adicionado.

```
ifconfig eth1 add FC00::1001/116 #Na máquina 1
ifconfig eth1 add FC00::1002/116 #Na máquina 2
```

Quadro 1: Inclusão de endereço IPv6

Depois de adicionado o endereço, este pode ser visualizado na placa de rede eth1, conforme Figura 16:

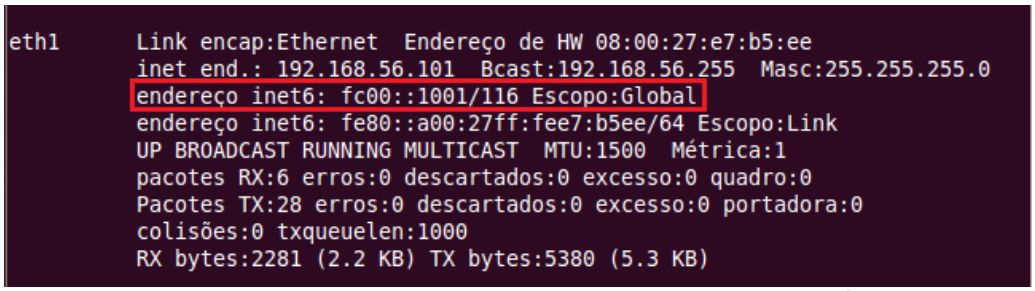

Figura 16 - Endereço IPv6 na Placa de Rede eth1 adicionado na máquina 1
Fonte: Autoria própria.

FASE 2: Verificar se há conectividade entre a máquina 1 e a máquina 2

Para isto, deve-se executar o comando ping da de uma máquina para outra.

Para isto, digita-se o comando “ping6 + endereço IPv6” , conforme

Apresentado no Quadro 2:

```
ping6 FC00::1002 #Na máquina 1
ping6 FC00::1001 #Na máquina 2
```

Quadro 2: Ping IPv6

O comando ping6 em execução pode ser visualizado através da Figura 17:

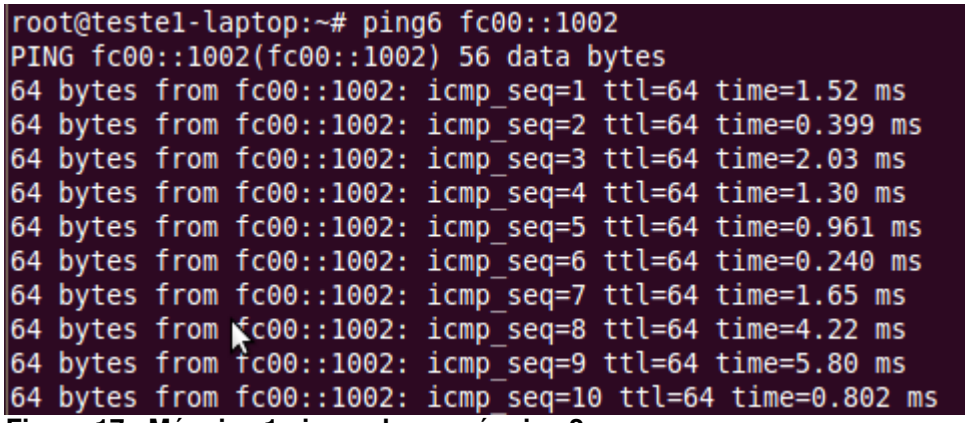

Figura 17 - Máquina 1 pingando na máquina 2
Fonte: Autoria própria.

3.2.2 Instalar o ipsec-tools nas duas máquinas virtuais

FASE 3: Realizar a instalação do Ipsec-tools, conforme quadro 3.

```
apt-get install ipsec-tools #Para a máquina 1
e 2.
```

Quadro 3: Instalação ipsec-tools

3.2.2.1 Configurar o ipsec-tools

A seguir são descritas as formas de configuração do IPSEC.

3.2.2.1.1 Modo ESP (Modo Transporte):

Todos os passos a seguir devem ser realizados nas duas máquinas (máquina 1 e máquina 2):

Passo 1: Gerar Chave ESP:

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

Quadro 4: Gerar chave ESP

Esta chave será única para cada máquina, depois de gerada deve ser incluída no arquivo *ipsec-tools.conf*, conforme apresentado no passo 2. Deve ser adicionado "0x" no início da chave, antes de ser adicionado no arquivo *Ipsec-tools.conf* o 0x indica que é uma chave expressa em hexadecimal.

Passo 2: Editar arquivo *ipsec-tools.conf*:

Este arquivo está localizado no diretório /etc e contém as configurações do IPSEC.

```
#Configuração Máquina 1 – ESP:
1 flush;
2 spdflush;
3 add FC00::1001  FC00::1002  esp 0x201 –E 3des-cbc
4 0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831; #chave da
máquina 1
5 add FC00::1002  FC00::1001   esp 0x301 –E 3des-cbc
6 0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df; #chave da
máquina 2

#Políticas de Segurança
7 spdadd FC00::1001   FC00::1002  any –P out ipsec
8  esp/transport//require;
9 spdadd FC00::1002   FC00::1001   any –P in ipsec
10   esp/transport//require;
```

Quadro 5: Configuração ipsec-tools.conf Máq. 1 ESP

Conforme o Quadro 5, é possível visualizar nas linhas 1 e 2 a diretiva responsável por limpar o banco das políticas de segurança, o comando “spdflush” removerá toda e qualquer entrada previamente criada .

Na linha 3 é adicionado 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 o Quadro 4. Nas linhas 5 e 6 é feito o mesmo procedimento mas as informações da máquina 2.

Nas linhas 7 e 9, 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 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 FC00::1001 com destino ao IP FC00::1002 e posteriormente aplica as mesmas políticas definidas para a saída dos pacotes (*out*).

Conforme apresentado no Quadro 6 é possível visualizar a configuração da máquina 2, com cabeçalho ESP.

```
      #Configuração Máquina 2 – ESP:
      flush;
      spdflush;
      add FC00::1001  FC00::1002  esp 0x201 –E 3des-cbc
        0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;     #chave     da
máquina 1
      add FC00::1002  FC00::1001   esp 0x301 –E 3des-cbc
        0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;     #chave     da
máquina 2
      #Políticas de Segurança
      spdadd FC00::1002   FC00::1001  any –P out ipsec
        esp/transport//require;
      spdadd FC00::1001   FC00::1002   any –P in ipsec
         esp/transport//require;
```

Quadro 6: Configuração ipsec-tools.conf Máq. 2 ESP

Passo 3: Inserir permissões para o arquivo *ipsec-tools.conf* (esta fase só é necessário caso o seu usuário do Ubuntu não tenha controle total)

```
chmod 750 ipsec-tools.conf
```

Quadro 7: Permissão ipsec-tools.conf

Passo 4: Iniciar serviço *setkey*

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

Quadro 8: Iniciar serviço *setkey*

3.2.2.1.2 Modo AH (Modo Transporte):

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

Passo 1: Gerar Chave AH:

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

Quadro 9: Gerar chave AH

Esta chave será única para cada máquina, possui 128 bits, depois de gerada deve ser incluída no arquivo *ipsec-tools.conf*, deve ser adicionado “0x” no início da chave.

Passo 2: Editar arquivo *ipsec-tools.conf*:

Este arquivo está localizado no diretório /etc e contém as configurações do IPSEC.

```
#Configuração Máquina 1 – AH:
1 flush;
2 spdflush;
3 add FC00::1001  FC00::1002  ah 0x200 –A hmac–md5
4  0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
5 add FC00::1002  FC00::1001   ah 0x300 –A hmac–md5
6  0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
#Políticas de Segurança
7 spdadd FC00::1001   FC00::1002  any –P out ipsec
8  ah/transport//require;
9 spdadd FC00::1002   FC00::1001   any –P in ipsec
10  ah/transport//require;
```

Quadro 10: Configuração ipsec-tools.conf Máq. 1 AH

Conforme o Quadro 10, é possível visualizar nas linhas 1 e 2 a diretiva responsável por limpar o banco das políticas de segurança, o comando “spdflush” removerá toda e qualquer entrada previamente criada .

Na linha 3 é adicionado 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 o Quadro 4. Nas linhas 5 e 6 é feito o mesmo procedimento mas as informações da máquina 2.

Nas linhas 7 e 9, 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 FC00::1001 com destino ao IP FC00::1002 e posteriormente aplica as mesmas políticas definidas para a saída dos pacotes (*out*).

Conforme apresentado no Quadro 11 é possível visualizar a configuração da máquina 2, com cabeçalho AH.

```
#Configuração Máquina 2 – AH:
flush;
spdflush;
add FC00::1001  FC00::1002  ah 0x200 –A hmac–md5
  0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
add FC00::1002  FC00::1001   ah 0x300 –A hmac–md5
  0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
#Políticas de Segurança
spdadd FC00::1002   FC00::1001  any –P out ipsec
  ah/transport//require;
spdadd FC00::1001   FC00::1002   any –P in ipsec
  ah/transport//require;
```

Quadro 11: Configuração ipsec-tools.conf Máq. 2 AH

Iniciar serviço *setkey*, conforme Quadro 8.

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.

3.2.2.1.3 Modo AH/ESP (Modo Transporte):

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

Passo 1: Gerar Chave ESP e AH

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

Quadro 12: Gerar chave ESP

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

Quadro 13: Gerar chave AH

Esta chave será única para cada máquina, depois de gerada será inclusa no arquivo *ipsec-tools.conf*, deve ser adicionado “0x” no início da chave.

Passo 2: Editar arquivo *ipsec-tools.conf*

Este arquivo está localizado no diretório /etc e contém as configurações do IPSEC.

Através do Quadro 14, pode-se visualizar a configuração do AH e conjunto com o ESP. É adicionada a configuração do AH + ESP, apresentado anteriormente através do Quadro 5 e 10.

```
      #Configuração Máquina 1 – AH/ESP:
      flush;
      spdflush;

      add FC00::1001  FC00::1002  ah 0x200 –A hmac-md5
        0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
      add FC00::1001  FC00::1002  esp 0x201 –E 3des-cbc
        0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;  #chave
da máquina 1
      add FC00::1002  FC00::1001   ah 0x300 –A hmac-md5
        0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
      add FC00::1002  FC00::1001   esp 0x301 –E 3des-cbc
        0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;  #chave
da máquina 2

      #Políticas de Segurança
      spdadd FC00::1001   FC00::1002  any –P out ipsec
        esp/transport//require
        ah/transport//require;
      spdadd FC00::1002   FC00::1001   any –P in ipsec
        esp/transport//require
        ah/transport//require;
```

Quadro 14: Configuração ipsec-tools.conf Máq. 1 AH/ESP

No Quadro 15, pode-se visualizar a configuração do AH em conjunto com o ESP da máquina 2.

```
      #Configuração Máquina 2 – AH/ESP:
      flush;
      spdflush;
      add FC00::1001  FC00::1002  ah 0x200 –A hmac-md5
        0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
```

```
      add FC00::1001  FC00::1002  esp 0x201 -E 3des-cbc
        0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;  #chave
da máquina 1
      add FC00::1002  FC00::1001   ah 0x300 -A hmac-md5
        0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
      add FC00::1002  FC00::1001   esp 0x301 -E 3des-cbc
        0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;  #chave
da máquina 2
      #Políticas de Segurança
      spdadd FC00::1002   FC00::1001  any -P out ipsec
        esp/transport//require
        ah/transport//require;
      spdadd FC00::1001   FC00::1002   any -P in ipsec
        esp/transport//require
        ah/transport//require;
```

Quadro 15: Configuração ipsec-tools.conf Máq. 2 AH/ ESP

Iniciar serviço *setkey*, conforme Quadro 8.

FASE 5: Conectando uma máquina a outra através do IPSEC

Depois de iniciar o serviço *setkey* as máquinas já irão se conectar através do IPSEC.

3.2.3 Analisando os Pacotes com o Wireshark

3.2.3.1 Sem IPSEC

Pode-se visualizar na Figura 18, pacotes sem IPSEC analisados pelo Wireshark.

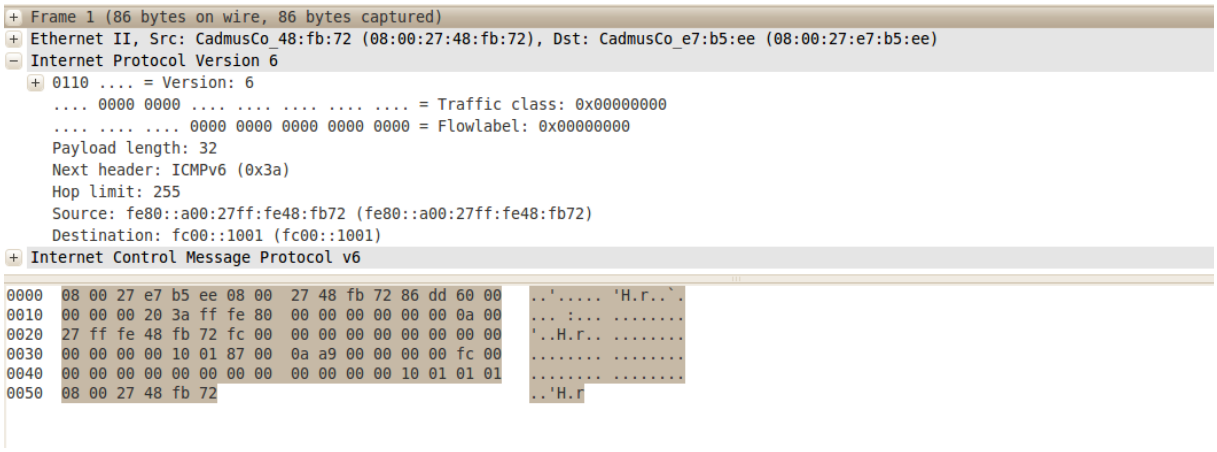

Figura 18 - Pacotes sem IPSEC analisados no Wireshark
Fonte: Autoria própria.

3.2.3.1 ESP

Pode-se visualizar na Figura 19, o cabeçalho ESP foi adicionado após o cabeçalho IP, e cabeçalho IP ficou com próximo cabeçalho o ESP.

Conforme mostrado anteriormente na Figura 9, 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.

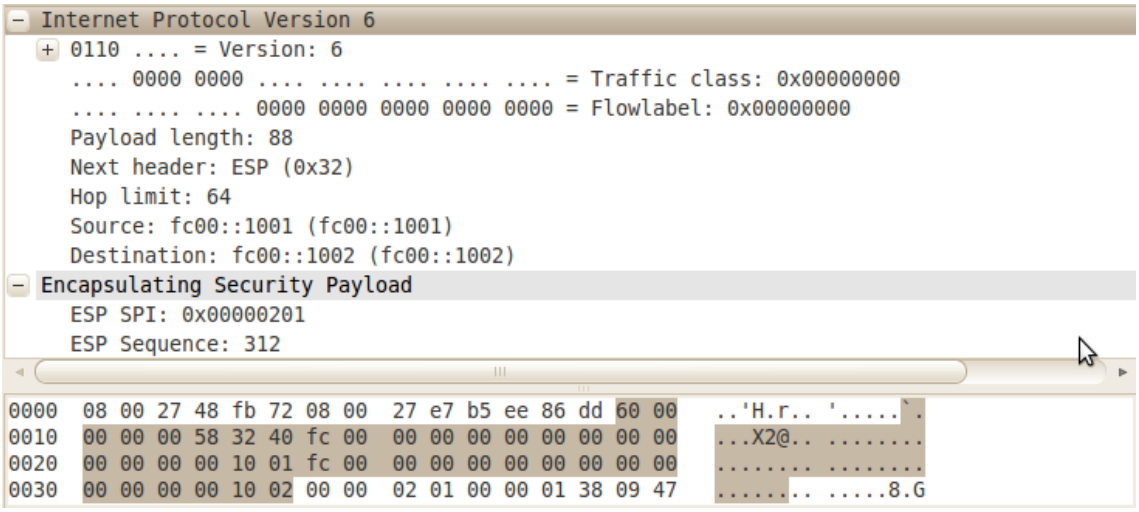

Figura 19 - Pacotes ESP analisado no Wireshark
Fonte: Autoria própria.

3.2.3.2 AH

Como se pode verificar na Figura 20, o cabeçalho AH foi adicionado dentro do cabeçalho IP.

Conforme mostrado anteriormente na Figura 9, 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.

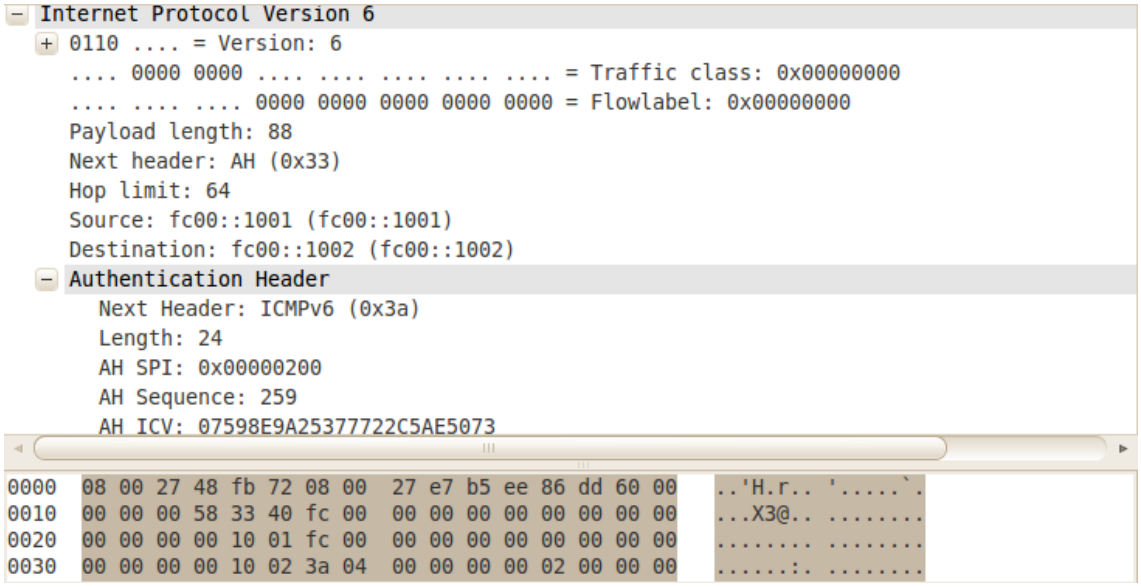

Figura 20 - Pacotes AH analisados no Wireshark
Fonte: Autoria própria.

3.2.3.3 AH/ ESP

Na Figura 21, podem-se visualizar os dois cabeçalhos em conjunto, o cabeçalho AH foi adicionado dentro do cabeçalho IP. O cabeçalho ESP foi adicionado após o cabeçalho IP, e como próximo cabeçalho o ESP.

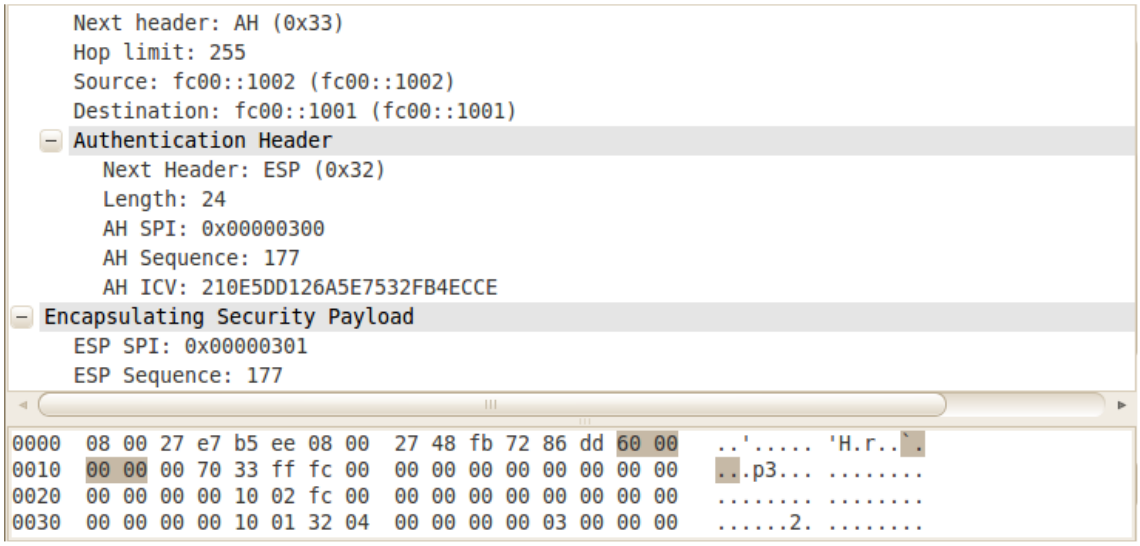

Figura 21 - Pacotes AH e ESP em conjunto analisados no Wireshark
Fonte: Autoria própria.

3.2.4 Análise do tamanho dos pacotes

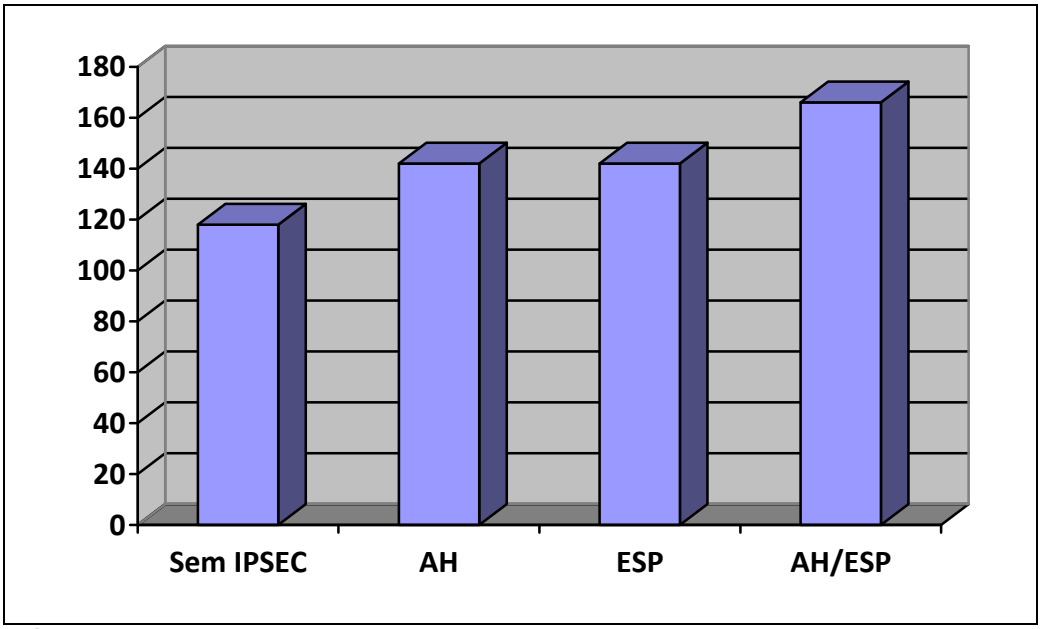

Gráfico 1 - Tamanho dos Pacotes em Bytes
Fonte: Autoria própria.

No Gráfico 1, pode-se visualizar que quando utilizado o IPSEC o tamanho do pacote aumenta, podendo tornar lenta uma rede que possui grande número de máquinas. Nos testes antes de realizar a configuração do IPSEC foi executado o comando ping entre as duas máquinas que estavam utilizando IPv6. Pode-se visualizar que o tamanho de um pacote ping utilizando IPv6 é de 188 bytes. Quando configurado com a adição do cabeçalho AH o seu tamanho é de 142 bytes e com

ESP o seu tamanho é o mesmo, 142 bytes. Em conjunto do AH e ESP o tamanho passa a ser de 166 bytes.

3.2.5 Testes de Desempenho

Para realizar os testes de desempenho foi montado um cenário com dois computadores HP Compaq 6065 Pro, Placa de rede de 100 Mbps, processador AMD Phenon(tm) II X4 B95 3.00 GHZ, memória RAM 4 GB, conectadas a um Switch Encore 100 Mbps, utilizando um cabo de par trançado de 100Mbps, conforme Figura 22.

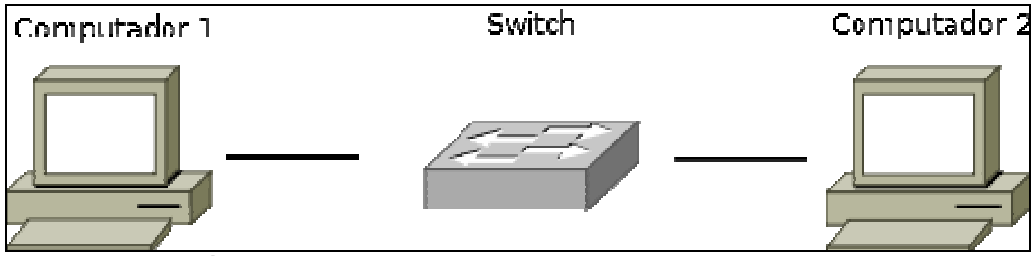

Figura 22 – Cenário de Testes de Desempenho
Fonte: Autoria Própria

Após a configuração dos endereços IPs nos computadores e a configuração do IPSEC como descrito no tópico 3.2.2.1, foi configurando um servidor de conexão remota no computador 1. Para isso foi utilizado o *Open Secure Shell* (SSH). O SSH tem o comando SCP que possibilita a cópia de arquivos de uma máquina para outra.

Foram realizados vários testes com arquivos de tamanhos distintos para medir o desempenho.

Conforme a Tabela 3, na primeira coluna, pode-se visualizar o tamanho dos pacotes que foram transferidos, após isto está descrito qual cabeçalho (sem IPSEC, AH, ESP, AH/ESP) foi adicionado e qual foi o tempo de transferência de cada arquivo. O tempo de transferência está colocado em segundos na Tabela 3.

Tabela 3 – Desempenho na Transferência dos Pacotes

Tamanho dos Pacotes	Sem IPSEC	AH	ESP	AH/ESP
50 MB	04	04	04	04
100 MB	09	09	09	09
200 MB	17	17	18	18
300 MB	26	26	26	27
400 MB	34	35	36	36
500 MB	43	44	44	46
800 MB	69	70	70	72
1,6 GB	138	141	143	145

Fonte: Autoria própria (2011).

No primeiro teste um arquivo de 50MB foi transferido de uma máquina para outra sem configuração alguma do IPSEC. Nesse caso o tempo de transferência foi de quatro segundos, os milissegundos foram omitidos uma vez que a cada transferência gerava um valor diferente. Logo em seguida foi efetuada a configuração do IPSEC no modo AH. Nesse modo o tempo de transferência também foi de quatro segundos. No modo de configuração ESP e AH/ESP o tempo de transferência também foi de quatro segundos. Com esses testes foi possível visualizar que quando o IPSEC é configurado para transferência de arquivos pequenos não é gerando nenhum atraso adicional na transferência dos arquivos pela rede.

No segundo teste foi utilizado um arquivo de 100MB, o tempo de transferência sem configuração do IPSEC e com os modos AH, ESP e AH/ESP configurados foi o mesmo, mostrando que até mesmo para arquivos grandes o IPSESC não gera atraso adicional na transferência de arquivos.

No terceiro teste foi utilizado um arquivo de 200MB, quando a transferência foi feita sem a utilização de configuração alguma do IPSEC o tempo de transferência foi de dezessete segundos, no modo AH o tempo de transferência também foi de dezessete segundos. Quando o modo ESP foi configurado o tempo de transferência foi de dezoito segundos e no modo AH/ESP o tempo de transferência também foi de dezoito segundos. Pode-se visualizar que a configuração do modo ESP causou um segundo de atraso na transferência do arquivo.

No quarto teste foi utilizado um arquivo de 300MB, nesse teste pode-se perceber que o modo AH causou um segundo de atraso em relação ao tempo de transferência normal e o modo ESP causou dois segundos de atraso.

Foram realizados outros testes com arquivos de 400MB, 500MB, 800MB, 1.6GB para verificar se atraso seria muito maior. Após realizar os vários testes foi possível visualizar que o atraso causado pela utilização do IPSEC na transferência de arquivos pode ser considerado baixo, levando-se em consideração a segurança obtida para a transferência de arquivos.

O gráfico 2 é outra forma de visualizar os dados obtidos através dos testes.

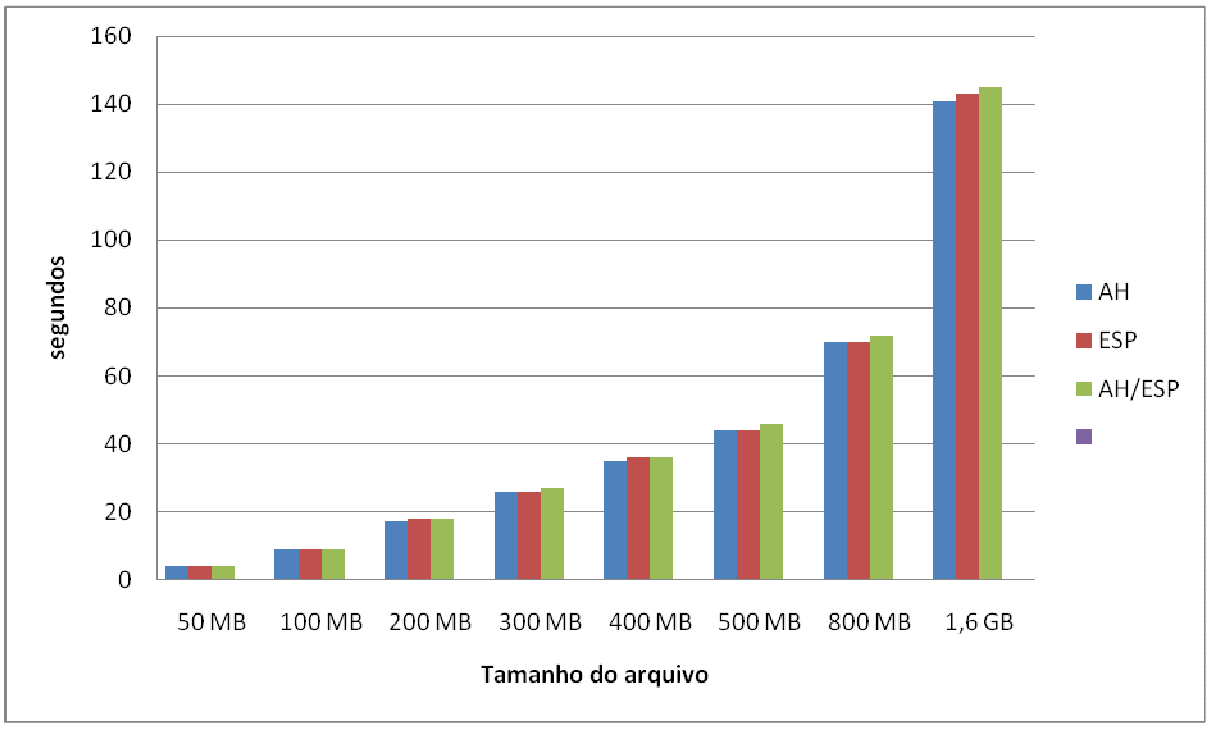

Gráfico 2 - Desempenho na Transferência dos Pacotes
Fonte: Autoria própria.

Com esse gráfico pode-se visualizar que o modo AH/ESP causa um atraso maior na transmissão de dados, o ESP gera um atraso inferior ao modo AH/ESP, mas superior ao modo AH. Através desse gráfico também pode-se visualizar que quando IPSEC é utilizado com arquivos menores que 100MB, o tempo de transferência é o mesmo que quando nenhuma configuração de IPSEC é utilizada.

4 CONCLUSÃO

A utilização do IPSEC aumenta a segurança dos dados, pois garante que estes sejam autenticados e criptografados, o que não acontece sem a utilização deste framework de segurança.

Pode-se verificar que na análise do tamanho dos pacotes, com a adição do cabeçalho de extensão AH, quando configurado ainda é possível visualizar o conteúdo do pacote, o pacote com AH aumenta 24 bytes em relação ao pacote sem IPSEC. Com ESP pode-se visualizar que o pacote foi criptografado, então não é possível que o conteúdo do pacote seja visualizado, também houve aumente de 24 bytes em relação ao pacote sem IPSEC. Utilizando os dois cabeçalhos em paralelo (AH e ESP) os pacotes são autenticados e criptografados, garantindo a total segurança dos dados transmitidos, porém houve aumento de 48 bytes, com isso nota-se que a utilização da rede aumenta o que pode ocasionar lentidão, então para fazer a utilização do IPSEC é ideal que a rede esteja preparada para isto, pois o uso de banda será maior, necessitando configurações especiais.

Nos testes de desempenho foi visualizado quando IPSEC é utilizado para a transmissão de arquivos menores quem 100MB nenhum atraso significativo é gerado. O que mostra que o IPSEC é uma solução de segurança que pode ser utilizada sem prejudicar o desempenho da rede. Porém quando o IPSEC é utilizado para a transferência de arquivos maiores de 100MB pode-se perceber quem um pequeno atraso.

Com os testes também foi possível visualizar que o modo ESP causa um maior atraso que o modo AH. Já quando o modo ESP e o modo AH são utilizados em conjunto percebeu-se que um atraso ainda maior foi gerado.

Ao realizar esta configuração houve um pouco de dificuldade por existir poucos materiais explicando o procedimento, e nada específico para o IPv6, então testes foram sendo feitos até chegar à configuração correta. A configuração do IPSEC é um pouco complexa, então é necessário que haja administradores de rede que façam corretamente esta configuração para que a rede não fique congestionada.

Mesmo com as dificuldades é válido ressaltar que o IPSEC trás muitas melhorias de segurança a rede, então se for bem configurado trará muitos benefícios a quem utilizar.

4.1 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Para melhorar o trabalho desenvolvido podem ser indicadas algumas implementações futuras para o aperfeiçoamento da pesquisa:

- Estudar o IPSEC integrado com IPv6 em Modo Túnel, onde já foi pesquisada a ferramenta Racoon (Ipsec-tools, 2011) para fazer esta configuração;
- Aperfeiçoar os gráficos de utilização da rede no modo transporte e fazer gráficos no modo túnel, realizando uma comparação entre os dois modos, medindo o desempenho de cada um, para posterior análise comparativa.

Estas implementações não foram realizadas neste trabalho devido ao curto prazo do cronograma.

.

REFERÊNCIAS

DEERING, S; HINDEN, R. **Internet Protocol, Version 6 (IPv6)**. RFC 2460, IETF. 1998. Disponível em: <http://www.ietf.org/rfc/rfc2460.txt> Acesso em: mai. 2011.

DIERKS, T; ALLEN, C. **The TLS Protocol**. RFC 2246, IETF. 1999. Disponível em: <http://www.ietf.org/rfc/rfc2246.txt> Acesso em: mai. 2011.

EXCEDA. **Brasil tem mais de 13 milhões de conexões à Internet**. 2011. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=76141>. Acesso em: mar. 2011.

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

FUNDAÇÃO GETÚLIO VARGAS. **Brasil atinge marca de 60 milhões de computadores em uso**. 2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1167875-6174,00.html>. Acesso em: mar. 2011.

HAWKINSON, J; BATES, T. **Guidelines for creation, selection, and registration of an Autonomous System (AS)**. RFC 1930, IETF. 1996. Disponível em: <http://www.ietf.org/rfc/rfc1930.txt> Acesso em: mai. 2011.

IANA. **Internet Assigned Numbers Authority**. Disponível em: <http://www.iana.org>. Acesso em: abr. 2011.

IPSEC-TOOLS. Disponível em: <ipsec-tools.sourceforge.net>. Acesso em: maio. 2011.

IPv6.BR. Disponível em: <www.ipv6.br>. Acesso em: abr. 2011.

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: mai. 2011.

KRAWCZYK, H; BELLARE, M; CANETTI, R. **HMAC: Keyed-Hashing for Message Authentication**. RFC 2104, IETF. 1997. Disponível em: <http://www.ietf.org/rfc/rfc2104.txt> Acesso em: mai. 2011.

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

LINUX FREES/WAN. Disponível em: <http://www.freeswan.org>. Acesso em: maio 2011.

MANSON, Andrew. **IPSec Overview Part Two: Modes and Transforms**. Disponível em:

<http://www.ciscopress.com/articles/article.asp?p=25477>. Acesso em: maio 2011.

MORIMOTO, Carlos. E. **Redes, Guia Prático**. Rio Grande do Sul: GDH Press e Sul Editores, 2008.

NETWORK WORLD. **Após teste, Google, Facebook e Yahoo começam a usar o IPv6 para valer**. 2011. Disponível em: http://idgnow.uol.com.br/internet/2011/06/10/apos-teste-google-facebook-e-yahoo-comecam-a-usar-o-ipv6-para-valer>. Acesso em mar. 2011.

NIC.BR. **TIC EMPRESAS 2009**, 2009. Disponível em: <http://cetic.br/empresas>. Acesso em: 08 mar. 2011.

PEREZ, M et al. **ATM Signaling Support for IP over ATM**. RFC 1755, IETF. 1995. Disponível em: < http://www.ietf.org/rfc/rfc1755.txt> Acesso em: mai. 2011.

QUICKSEC. Disponível em: <http://www.quicksec.co.uk>. Acesso em: maio 2011.

REY, Marina D. **Internet Protocol**. RFC 791, IETF. 1981. Disponível em: < http://www.ietf.org/rfc/rfc791.txt>. Acesso em: mai. 2011.

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

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

TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo, Campus, 2003.

TCPDUMP/LIBPCAP. Disponível em: <http://www.tcpdump.org>. Acesso em: maio 2011.

WIRESHARK FOUNDATION. **About Wireshark**. Disponível em: <http://www.wireshark.org/about.html>. Acesso em: maio 2011.