CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM SISTEMA DE INFORMAÇÃO

ESTUDO DE VULNERABILIDADE DO IPSEC EM REDES IPV6

RICARDO SATO DE OLIVEIRA

Marília, 2012

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM SISTEM DE INFORMAÇÃO

ESTUDO DE VULNERABILIDADE DO IPSEC EM REDES IPV6

Monografia apresentada ao Centro Universitário Eurípides de Marília como parte dos requisitos necessários para a obtenção do grau de Bacharel em Sistema de Informação.
Orientador: Prof. Emerson Alberto Marconato.

Marília, 2012

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Ricardo Sato de Oliveira

ESTUDO DE VULNERABILIDADE DO IPSEC EM REDES IPV6

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Sistemas de Informação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Sistemas de Informação.

Nota: 7,5 (SETE E MEIO)

Orientador: Emerson Alberto Marconato

1°. Examinador: Rodolfo Barros Chiaramonte

2°. Examinador: Ricardo José Sabatine

Marília, 06 de dezembro de 2012.

Agradecimentos

Agradeço a Deus.

A minha família em especial a minha esposa Valdirene pelo amor, pela paciência e compreensão nos momentos de ausência e menor dedicação à família devido aos estudos.

A minha mãe e minhas irmãs pelo incentivo nas horas difíceis.

Agradeço meu orientador, Ms. Emersom Alberto Marconato, pela orientação e paciência.

Aos membros da banca examinadora pela disposição em analisar esse trabalho.

As grandes amizades que conquistei nesses 4 anos de graduação no UNIVEM,

Agradeço a todos aqueles que direta ou indiretamente colaboraram para a realização deste trabalho.

RESUMO

Com o crescimento da demanda por conexões, já se previa o esgotamento dos blocos IPv4 de comunicação global, principal base de comunicação da internet, com isso se tornou imprescindível a criação de um novo protocolo, o IPv6. O novo protocolo trás um novo conceito de protocolo de comunicação com novas funcionalidades juntamente com uma reformulada estrutura de segurança nativa, o IPSec. Esse trabalho tem como objetivo estudar as vulnerabilidades já detectadas anteriormente no protocolo IPv4 comparadas ao novo protocolo IPv6 com o uso da segurança IPSec, em sistemas operacionais Windows e Linux, estudando seu comportamento nas versões atuais destes sistemas operacionais.

ABSTRACT

With the growing demand for connections, already anticipated the exhaustion of IPv4 blocks of global communication, the main base of Internet communication, it has become essential to the creation of a new protocol IPv6. The new protocol brings a new concept of the communication protocol with new functionalities along with a reformed security structure, the IPSec. This work aims to study the vulnerabilities already detected previously in IPv4 protocol compared to the new IPv6 protocol with the IPSec security in Windows and Linux operating systems, smoothing his behavior in current operating systems.

SUMÁRIO

LISTA DE FIGURAS

Lista de Tabelas

LISTA DE ABREVIATURAS E SIGLAS

3G	3ª Geração
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
ARP	*Address Resolution Protocol*
RARP	*Reverse Address Resolution Protocol*
ATM	*Asynchronous Transfer Mode*
CIDR	*Classless Inter Domain Routing*
DES/3DES	*Data Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DDoS	*Distributed denial of service*
DoS	*Denial of service*
ESP	*Encapsulating Security Payload*
FDDI	*Fiber Distributed Data Interface*
HMAC	*Hash-based Message Authentication Code*
HTTP	*HyperText Transfer Protocol*
ICMPv6	*Internet Control Message Protocol version 6*
ICV	*Integrity Check Value*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IHL	*Internet Header Length*
IKE	*Internet Key Exchang*e
IP	*Internet Protocol*
IPSEC	*IP Security Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
LAN	*Local Area Network*
MAC	*Media Access Control*
MD5	*Message-Digest algorithm 5*
MitM	*Man in the Middle*
MTU	*Maximum Transmission Unit*

NA	*Neighbor Advertisement*
NAT	*Network Address Translation*
NDP/ND	*Neighbor Discovery Protocol/ Neighbor Discovery*
ND	*Neighbor Discovery*
NIC	Núcleo de Informação e Coordenação
NS	*Neighbor Solicitation*
OSI	*Open Systems Interconnection*
PING	*Packet Internet Grouper*
PPP	*Point-to-Point Protocol*
QoS	*Quality of service*
RA	*Router Advertisement*
RFC	*Request for Comments*
SA	*Security Association*
SAD	*Security Association Database*
SaaS	*Software as a Service*
SEND	*Securing Neighbor Discovery*
SHA	*Secure Hash Algorithm*
SPD	*Security Policy Database*
SPI	*Security Parameter Index*
SO	Sistema Operacional
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TCP-SYN	*Transmission Control Protocol- synchronize*
THC	*The Hackers Choice*
TLS	*Transport Layer Security*
TTL	*Time to Live*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
UDP	*User Datagram Protocol*

1. Introdução

A internet se tornou uma ferramenta indispensável nas entidades de pesquisa e empresas no mundo todo, com o conhecimento e a evolução da tecnologia a internet se tornou acessível às pessoas, tornando se também uma ferramenta de estudos, comercio e lazer. No Brasil se estima um total de 83,4 milhões de pessoas com acesso a internet (IDGNOW, 2012) e mais de 77,5 milhões de conexões entre móveis e fixas. (COMPUTERWORLD, 2012).

Com o passar dos anos e a quantidade de usuário em crescente aumento já se previa o esgotamento dos blocos de endereçamento global, principal base de comunicação da internet, que ocorreu no ano de 2011 (NIC.BR, 2011).

Segundo Florentino (2012) com as limitações estruturais do protocolo IPv4 (*Internet Protocol version 4*) que não permite o uso do IPSec em implementações de conexões seguras e a criação de apenas 4.294.967.296 endereços de IP, sobre esses números devemos considerar a expansão das conexões residenciais e móveis como o 3G (3° Geração), que foi crescente no mundo todo associado ao desperdício de endereço no inicio da internet comercial, o protocolo IPv4 vem caminhando para um colapso iminente, membros da IETF *(Internet Engineering Task Force*) iniciaram um trabalho de pesquisa de um novo protocolo de comunicação que suprisse as necessidades futuras.

Em 1994 após varias pesquisas foi sugerido um novo protocolo de comunicação o IPv6 (*Internet Protocol Version 6*), desde então o desenvolvimento do novo protocolo chamado versão 6 ou IPv6 vem sido desenvolvido com um novo conceito de comunicação, que tem a missão de expandir e otimizar a comunicação via internet corrigindo falhas estruturais do antigo protocolo, foram mais de 10 anos de pesquisas e trabalho no desenvolvimento de um novo protocolo, todo o conceito de estrutura e hierarquia conhecidos deverão ser revistos, pois grande parte da topologia de rede irá mudar com implementação do protocolo. (FLORENTINO, 2012).

1.2 Objetivo

A seguir será descrito os objetivos gerais e específicos a que se refere o trabalho. Para uma melhor compreensão do tema abordado e informações completas sobre o assunto é importante a leitura da referencias bibliográficas.

1.2.1 Objetivo Geral

O IPv6 traz uma implementação de segurança na camada 3 do modelo OSI (*Open Systems Interconnection*). O projeto visa testar métodos de ataque ao tráfego de pacotes como *Man in the Middle, Spoofing e Sniffng,* em uma rede IPv6 protegida com a segurança IPSec (*Internet Protocol Security*) em sistemas operacionais atuais que possuem suporte a transmissão de dados em IPv6, mais especifico a segurança AH (*Autentication Header*), e ESP (*Encapsulating Security Payload*) parte do mecanismos de segurança do protocolo IPsec obrigatório no protocolo IPv6.

1.2.2 Objetivos específicos

Discutir as mudanças em relação à segurança do IPv6 ao IPv4.

Mostrar os mecanismos de segurança trazido pelo IPv6.

Promover testes em sistemas operacionais Linux e Windows.

1.3 Justificativa

Com o estudo promovido nesse trabalho espera-se contribuir com informações relevantes a segurança de redes que serão implementadas sob o novo protocolo de comunicação o IPv6, que possui suporte nativo ao IPSec, evidenciando a existência ou não de falhas na segurança nos cabeçalhos AH e ESP do IPSec, que protegem a comunicação com confiabilidade e confidencialidade contra ataques de interceptação de pacotes que trafegam em uma rede segura. Foi escolhido o IPSec como tema da pesquisa por se tratar de uma segurança nativa ao protocolo IPv6.

1.4 Organizações teóricas

Faz se necessário uma descrição teórica sobre o protocolo IPv6 e suas principais características, para um melhor entendimento sobre os testes executados na pesquisa, contudo o foco terá maior relação as características do IPv6 quanto ao IPSec.

- Capítulo 2 terá como conteúdo algumas características dos Protocolos de comunicação, IPv6 e IPSec enfocando particularmente os aspectos mais relevantes para este trabalho.
- Capítulo 3 é apresentado a pesquisa desenvolvida, incluindo a metodologia e ferramentas usadas no projeto.
- Capítulo 4 será discutido os resultados da metodologia de ataque.
- Capitulo 5 são apresentadas as principais conclusões e propostas de trabalhos futuros.

2. Fundamentação teórica

A seguir serão descritas informações que serão relevantes ao entendimento do trabalho com relação a estrutura do IPv6 e suas mudanças estruturais, que permitem o uso nativo do IPSec.

2.1Vulnerabilidade e Riscos

Nos dias de hoje, as empresas dependem cada vez mais dos sistemas de informação e da Internet para fazer negócios, não podendo sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, impactando diretamente na confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores.

Através de milhões de conexões, empresas e pessoas trocam informações importantes como: transações financeiras, informações pessoais, acesso a controles empresariais, etc.; Essas informações podem ser interceptadas se alguma forma de segurança não for implementada, expondo pessoas e empresas a diversos riscos.

A segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas a usar.

A maior parte dos ataques a segurança são intencionalmente causados por pessoas que tentam obter algum benefício ou prejudicar alguém. (ZAPATER; SUZUKI, 2005).

Alguns aspectos que devemos considerar:

- Qual o valor da informação?
- Quanta confiabilidade ela requer?

- Qual o impacto em caso de vazamento?
- Qual o impacto em falta de disponibilidade?

Atualmente existem vários níveis de atacantes, cada qual com seu nível de conhecimento e principalmente quis seus principais objetivos em concluir um ataque.

Segundo NAKAMURA (2007), os atacantes são classificados como:

- ***Script Kiddies*:** esse atacante tem como característica a busca por alvos fáceis e vulnerabilidades já conhecidas por não possuir um conhecimento avançado em desenvolvimento de ataques ou ferramentas.
- ***Insiders*:** são pessoas que trabalham no local do ataque, são funcionários, ex-funcionários ou pessoas que de alguma forma conseguem se infiltrar dentro das organizações. Esse tipo de ataque envolve engenharia social, a relação do funcionário com o chefe, passando pelo suborno e a espionagem industrial.
- ***Coders*:** são os hackers que compartilham seus conhecimentos escrevendo livros ou ministrando palestras e seminários sobre suas descobertas e aventuras. Ministrar cursos também é uma das atividades desenvolvidas pelos coders que são influenciados pelo aspecto financeiro.
- ***White hat/ Hackers*:** são conhecidos também como "hackers do bem" ou "hackers éticos", e utilizam suas experiências e descobertas para colaborar com o desenvolvimento de novas técnicas de segurança e relatar as vulnerabilidades que encontram em sites ou sistemas em geral possuem elevado conhecimento sobre segurança.
- ***Black hat*/*Crackers*:** são invasores que se utilizam de seus conhecimentos avançados para invadir sistemas e roubar informações secretas das organizações. Geralmente tentam vender as informações roubadas de volta para a sua vítima, ameaçando-as de divulgação dos dados extraviados.

2.2 Protocolo

Protocolo é um acordo de comunicação em que dois pontos devem definir regras para que seja possível o envio e recebimento de uma determinada informação. (FARREL, 2005).

Em geral são responsáveis por quais mensagens serão enviadas e recebidas, a ordem, o formato de cada uma, os caminhos que devem seguir e as ações a serem tomadas na hora de transmissão e da recepção,. Os protocolos são necessários para gerenciar recursos de rede, para que exista um controle em seu funcionamento. 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. (TANENBAUM, 2003).

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

2.3 Arquitetura TCP/IP

Já há algum tempo, a arquitetura de comunicação de rede mais utilizada entre os dispositivos é o protocolo TCP/IP, com isso os fabricantes de sistemas operacionais seguiram

essa tendência tornando nativo em seus sistemas este protocolo de rede.

O TCP/IP forma uma pilha de protocolos de comunicação entre o computador e a 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. (SANTOS, 2010). A Figura 1 ilustra as camadas da arquitetura TCP/IP e os principais protocolos de cada camada.

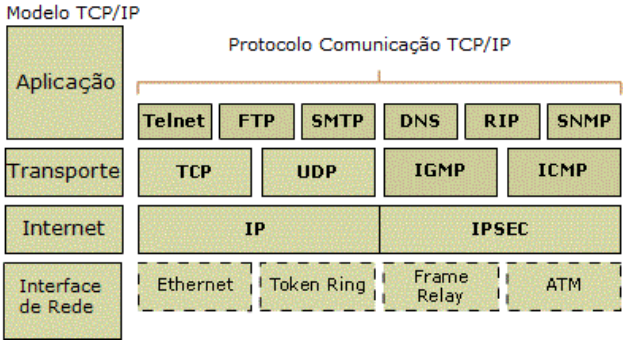

Figura 1 – Camadas TCP/IP

Fonte: Microsoft (2012).

A figura 1 ilustra a localização dos protocolos e suas respectivas camadas, o IP se localiza na camada de rede, camada responsável e estabelecer a comunicação lógica entre os dispositivos.

2.4 Protocolo IP

O Internet Protocol (IP) é o protocolo responsável pela comunicação de equipamentos em uma rede interna ou em redes externas (internet). Seu desenvolvimento teve como objetivo permitir a comunicação de dois ou mais equipamentos interligados por um meio físico através de endereços IPs, esses endereços são basicamente formados por um campo de 32 *bits*, onde são identificados o host e a rede na qual host pertence. (FARREL, 2005).

2.4.1 Protocolo IPv4

As máquinas pertencentes a uma rede TCP/IP especificamente versão 4, devem possuir um endereço IPv4, tal como 192.168.190.110, esse endereço possui 4 campos (*dotted quad)* compostos por três 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.

Quando o protocolo IP foi criado, há aproximadamente duas décadas, não foram previstas necessidades emergentes da sociedade e da sua relação com os sistemas de comunicação atuais, em particular com a Internet. (FLORENTINO, 2012). Com as pesquisas realizadas nas literatura sobre o IPv4, percebe-se que o intuito inicial desse protocolo de comunicação era inicialmente para fins específicos, onde não existiam problemas quanto à segurança, mobilidade, espaço de endereçamento e qualidade de serviço. (SANTOS, 2010).

A figura 2 ilustra a estrutura do cabeçalho do protocolo IPv4.

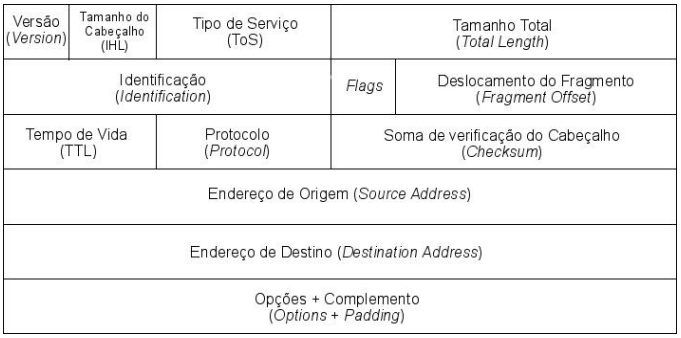

Figura 2 – Cabeçalho IPv4
Fonte: ipv6.br (2012).

O principal motivo que fez necessária a mobilização da IETF para criação de uma nova versão do cabeçalho IP foi o fim dos blocos IP disponíveis para todo o mundo. Observando o cabeçalho IPv4 na Figura 2, vemos que o tamanho de um endereço IP é de 32 *bits*, capaz de endereçar pouco mais que quatro bilhões de endereços IP (2^32).

Para o futuro a tendência é que cada casa tenha pelo menos uma máquina com acesso a Internet e, portanto, tenham um endereço IP. (FLORENTINO, 2012).

Para suprir tais necessidades foi necessária a criação de uma nova versão do protocolo IP, o IPv6. No início do desenvolvimento existiam varias divergências quanto a definição final para o modelo que substituiria a versão 4, foram desenvolvidas soluções paliativas para a falta de endereços IP, como por exemplo o NAT (*Network Address Translation).* (SOARES, 1995).

O NAT é um sistema de tradução de endereços de rede. Em uma rede interna é possível que seja criada uma infraestrutura de redes utilizando para isto endereços IPv4 privados. Entre a rede interna da organização e a rede externa (Internet), é colocada uma estação, chamada *firewall*, contendo duas interfaces de rede, uma interna, com endereço IP privado, e outra externa, com endereço IP válido. (KUROSE; ROSS, 2006)

O problema do NAT é que não se pode acessar diretamente de fora determinadas máquinas que estão atrás do *firewall*, para que isso ocorra o *firewall* deve direcionar essas conexões, pois elas utilizam endereçamento IP privado, ou seja, endereços que são reservados

e não são roteados na Internet. Essa estrutura possui limites para que as redes não sofram problemas com desempenho ou indisponibilidade. Ainda, o NAT impede que relações de confiança sejam estabelecidas entre máquinas externas com as internas, já que não há comunicação direta entre os destinos.(FLORENTINO, 2012)

Para resolver os problemas de autenticidade e confidencialidade na camada de rede foram desenvolvidos novos mecanismos para o IPSec. Esses mecanismos serão comentados nas seções seguintes de forma sucinta.

2.4.2 Protocolo Ipv6

O contexto do IPv6 é extenso, foram mais de 10 anos de pesquisas e trabalho no desenvolvimento de um novo protocolo, todo o conceito de estrutura e hierarquia conhecidos deverão ser revistos, pois grande parte dos conceitos de rede irá mudar com implementação do protocolo IPv6, podemos iniciar citando a mudança do endereçamento que mudou de 32 *bits* para 128 *bits*, possibilitando assim um método mais simples de autoconfiguração através do uso da identificação EUI-64 da maior parte das interfaces de rede gerando uma quantidade quase que infinita de endereços IPs, essa nova forma de endereçamento já diverge dos conceitos atuais não somente no endereço em si que passa de 4 grupos de 8 *bits* para 8 grupos de 16 *bits* se tornando um endereço extenso e complexo. (FLORENTINO, 2012).

Apesar de existir vários grupos hexadecimais para um endereçamento IPv6, 15% estão previamente alocados, ficando os restantes reservados para uso futuro. Devido a essa pré-alocação, serão comuns endereços com sequências de *bits* com o valor zero (SILVA; FARIA, 2001).

Existem três formas de representação de um endereço IPv6. A forma mais utilizada é x:x:x:x:x:x:x:x, onde, os “x” são números hexadecimais. Assim o endereço IPv6 é dividido em oito partes de 16 *bits*, como apresentado no seguinte exemplo:

2000:0000:0000:0000:0000:0000:0000:0000/16

Para simplificar a representação de endereços com varias sequências de zeros pode se substituir os campos pela agregação“::”. No entanto, esta apenas poderá ser efetuada uma única vez em cada endereço, evitando à ambiguidade na escrita, a seguir é representado a segunda forma no exemplo:

IP 2001:0000:0000:0000:0000:0000:000E:0123/16

IP 2001::000E:0123/16

A terceira forma de utilização na representação de endereçamento IPv6 é a abreviação de um sequência de zeros, ou o primeiro zero a esquerda de cada duo octeto de cada campo que devera respeitar a regra de ambiguidade, podendo ser compatível IPv6/IPv4, sendo útil no período de migração e coexistência de ambos os protocolos. Assim utilizamos a representação x:x:x:x:x:x:z:z:z:z, onde, os “x” indicam números hexadecimais (16 *bits*) e os “z” são valores que representam os 8 *bits* fazendo se referencia ao endereço IPv4. (FLORENTINO, 2012).

Exemplo:

IP 2001:0000:0000:0000:0192:0168:0000:0222/16

IP 2001::192:168:0:222/16

Em relação à representação do prefixo ou mascara de rede permanecem os mesmos usados no padrão Ipv4, seguindo o padrão CIDR (*Classless Inter-Domain Routing*), sendo “endereço-IPv6/tamanho do prefixo”. (RFC 4291, 2006).

No exemplo a seguir é representado um endereço que dos 128 *bits*, 64 *bits* são destinados a identificar a sub-rede. (FLORENTINO, 2012).

Exemplo:

2001:foca:dado:2::/64

As URLs (*Uniform Resource Locators*) possuem uma representação diferente em IPv6 com relação ao IPv4, quando existir a necessidade de descrição da porta de destino da

URL. Em IPv6, os endereços passam a ser inseridos entre colchetes, evitando assim ambiguidade quando a porta, que pode ser interpretado como endereço pelas regras do protocolo IPv6, mas no protocolo IPv4 é apresentada juntamente com o endereço representado após o caractere com “ : “.

IPv4 http://200.200.200.200:8080

IPv6 http://[2001:foca:dado:2::80]:8080

As definições acima são referencia ao texto Curso IPv6 Básico. (SANTOS, 2010).

2.4.3 Classificação dos endereços IPv6

Existem no IPv6 três tipos de endereços definidos:

Unicast – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface;

Anycast – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos.

Multicast – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos.

Diferente do IPv4, no IPv6 não existe endereço broadcast, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída à tipos específicos de endereços multicast. (FLORENTINO, 2012).

2.4.4 Cabeçalhos IPv4 e IPv6

Outra importante mudança é vista no cabeçalho, na versão 4 seu tamanho variava de 20 a 60 *bytes* , já na versão 6 possui um tamanho fixo de 40 *bytes.* Apesar de os endereços na versão 6 serem quatro vezes maior que os da versão 4, o seu cabeçalho base tem o dobro do tamanho da versão anterior, onde alguns campos foram removidos ou tiveram seus nomes alterados. O cabeçalho do IPv4 é composto por 12 campos fixos, podendo conter ou não opções de complemento, o novo padrão IPv6 possui 8 campos onde 3 foram herdados do antigo padrão, 4 sofreram modificações e 1 foi acrescentado, com essas mudanças o cabeçalho se tornou mais simples permitindo uma menor carga de processamento dos roteadores e incorporando a expansão da capacidade de endereçamento, encaminhamento e uma melhor aplicação do QoS (*Quality of Service*) e permitindo ainda autenticação e privacidade nos dados trafegados.(FLORENTINO, 2012).

Podemos comparar as mudanças ocorridas na verão 6, demonstrada na figura 3:

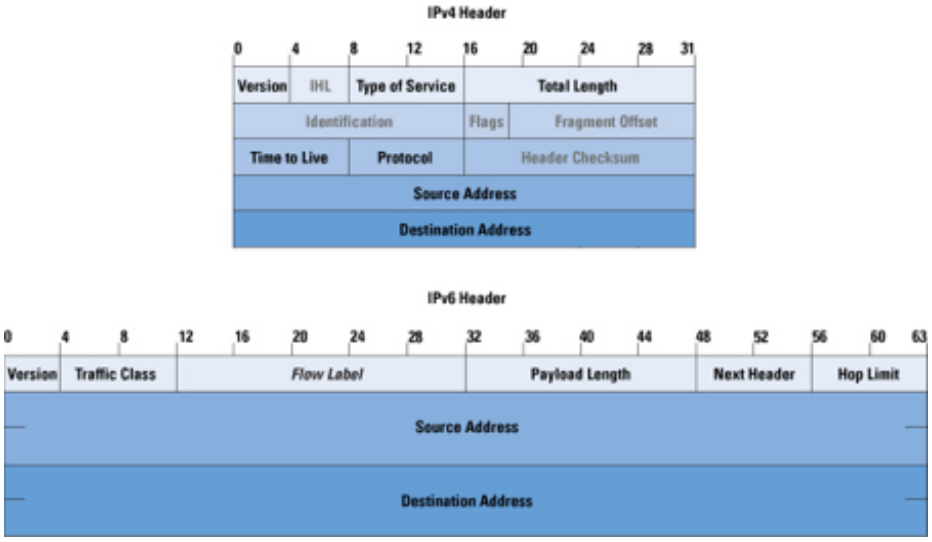

Figura 3 – Estrutura do Protocolo IPv4/IPv6

Fonte: Cisco (2011)

As mudanças do cabeçalho IPv4 para o IPv6 foram:

- ***Source Address* e *Destination Address*:** foi alterado seu tamanho de 32 *bits* para 128 *bits* no IPv6;
- **IHL *Internet Header Length***: foi eliminado do cabeçalho IPv6, pois sua função não é mais necessária devido ao tamanho fixo de 20 *bytes*;
- ***Type of Servisse**:* foi substituído pelo *Traffic Class* e *Flow Label* para as implementações de QoS (*Quality of Service*);
- ***Total Length*:** foi eliminado no IPv6 e trocado pelo campo *payload length*;
- **Identification, Fag e Offset:** foram removidos e suas funções foram passadas para o cabeçalho *Fragmentetion*;
- **TTL:** passou a ser chamar *Hop Limit* no IPv6;
- ***Protocol*:** que anunciava apenas os protocolos de camada superior, foi substituído pelo campo *Next Header*;
- ***Header Checksum*:** esse campo foi removido do novo protocolo, sua função foi delegada as camadas superiores;

Campos do cabeçalho IPv6:

- ***Version*:** Este campo possui 4 *bits* e identifica a versão do protocolo IP utilizado, seu valor de referencia deverá ser 6, se estiver na versão IPv6;
- ***Trafic Class*:** Este campo possui 8 *bits* onde os pacotes são identificados através da prioridade ou classe de serviços;
- ***Flow Label*:** 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;
- ***Payload Length:*** 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;

- ***Next Header*****:** 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;
- ***Hop Limit*****:** 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;
- ***Source Address:*** Este campo possui 128 *bits* e indica o endereço de origem do pacote;
- ***Destination Address*****:** Este campo possui 128 *bits* e indica o endereço de destino do pacote.

Informações retiradas da literatura IPv6 na Prática. (FLORENTINO, 2012).

2.4.5 Cabeçalho de extensão

Com essas mudanças o cabeçalho se tornou flexível, prevendo sua extensão por meio de cabeçalhos adicionais, o cabeçalho de extensão estão posicionados entre o cabeçalho base e o cabeçalho de camada de transporte podendo existir múltiplos cabeçalhos de extensão formando uma cadeia de cabeçalhos, como uma lista encadeada onde o campo *Next Header* aponta para o próximo cabeçalho de extensão. (FLORENTINO, 2012).

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 e os demais pelo nó identificado no campo Endereço de Destino do cabeçalho base. (FLORENTINO, 2012).

Na adição de novos cabeçalhos, o cabeçalho base fica inalterado, apenas informa

os dados do próximo cabeçalho, como mostrado na figura 4.

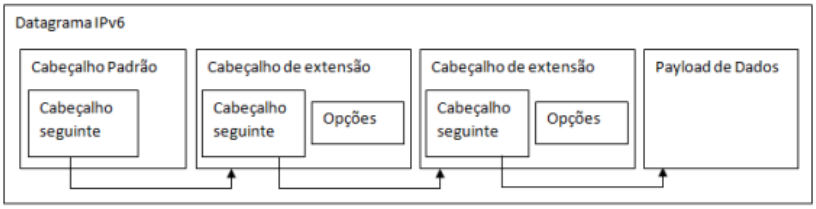

Figura 4 – Cabeçalho de extensão
Fonte: FARREL (2005)

O cabeçalhos do protocolo IPv6 possui 6 extensões:

- ***Hop-by-Hop Options*:** Opções de salto-a-salto, carrega informações que deverão ser processados por todos os nós ao longo do caminho;
- ***Destination Options:*** Opções de destino carregam informações que devem ser processadas pelo nó de destino do pacote;
- ***Routing:*** Rota de origem, utilizado como parte do mecanismo de mobilidade;
- ***Fragmentation:*** Fragmentação carrega informações sobre os fragmentos dos pacotes;
- ***Authentication Header:*** Autenticação, utilizado pelo IPSec, é identificado pelo valor 51 no campo próximo cabeçalho, atua para promover autenticidade e garantia de integridade aos pacotes;
- *Encapsulating Security Payload:* Encapsulamento seguro, Também utilizado pelo IPSec, é identificado com o valor 52 no campo próximo cabeçalho, garante a integridade e a confidencialidade dos pacotes. (FLORENTINO, 2012).

2.5 IPSec

IPSec é um conjunto de protocolos que provêm serviços de autenticidade e confidencialidade para comunicações na Internet. (KENT; ATKINSON, 1998c).

Sua função é proteger o datagrama IP inteiro no modo fim a fim, sendo que nenhuma máquina intermediária na Internet poderá ter acesso ou até mesmo modificar qualquer informação sobre a camada IP.

Sendo um método padrão para o provimento de segurança aos pacotes que trafegam em uma rede TPC/IP, o IPSec atua na camada de rede (camada 3) do modelo OSI (*Open Systems Interconnection*), diferente dos protocolos SSL (*Secure Sockets Layer*) e TLS (*Transport Layer Security*) que operam desde a camada de transporte (camada 4) até a camada de aplicação (camada 7), tornando o IPSec uma segurança mais flexível ao trafego de rede.

O framework de segurança IPSec, que já existia para o protocolo IPv4 mas não pôde ser implementado devido ao uso do NAT (*Network Address Translation*), que impede o mapeamento do IP real que originou os pacotes, no IPv6 essa implementação tornou-se possível devido a nova arquitetura de operação do IPv6, esse método padrão visa fornecer segurança as informações em comunicação entre pontos. Essa segurança de criptografia e autenticação de pacotes na camada de rede tem o objetivo de promover integridade, confidencialidade e autenticidade aos dados, impossibilitando técnicas de ataque antes utilizadas no protocolo IPv4 como *spoofing* (falsificação de endereço), ataque de negação de serviço DoS (*Denial of Service*) e analise tráfego de pacotes *sniffing*. Apesar de proteger os dados, o IPSec não pode ser implementado em algumas mensagens ICMPv6, pois para autenticá-las utilizando o cabeçalho AH (*Authentication Header*), é preciso que os nós tenham seus endereços já definidos, o que não ocorre em algumas mensagens ICMPv6 relacionadas a descoberta de vizinhança e anuncio de roteadores. Para ocorrer a negociação de chaves pelo protocolo IKE (*Internet Key Exchage*) os recursos de descoberta e anuncio não funcionariam corretamente, tornando se inviável o processo de autoconfiguração de endereços e detecção de erros pelo protocolo IPv6. (Ipv6.Br, 2012).

Dentre as vantagens e desvantagens do IPSec, podemos evidenciar:

Vantagens:

- Sistema completo que pode prover vários serviços de autenticidade e confidencialidade no tráfego de dados;
- Implementa confidencialidade dos dados de forma transparente a todas as aplicações;
- Tem um bom nível de confidencialidade;
- Redução de custos em interligação de redes institucionais;
- E um padrão, ou seja, tem que demonstrar interoperabilidade entre dispositivos.

Desvantagens:

- Complexo e não completamente maduro;
- Problemas com NAT, proxy e endereços dinâmicos (ainda em discussão na IETF);
- Possui algumas questões de interoperabilidade;
- Provoca queda de desempenho na comunicação de dados;
- E necessário criar relações de confiança entre as redes.

A arquitetura IPSec usa dois cabeçalhos para prover autenticidade e confidencialidade, o AH *Autentication Header* e ESP *Encapsulating Security Payload*.

Ainda, a plataforma IPSec utiliza o *Internet Key Exchange* (IKE), que implementa procedimentos e protocolos de troca e gerência de chaves criptográficas (HARKINS; CARREL, 1998).

A segurança implementada no IPSec, utiliza recursos independentes para realizar suas funções, foi definido pelo IETF os algoritmos de criptografia que são usados pelas funções AH e ESP.

Criptografias: DES (*Data Encryption Standard*), 3DES (*Triple Data Encryption Standard*), AES (*Advanced Encryption Standard*), HMAC (*Hash-based Message Authentication Code*), MD5 (*Message-Digest algorithm 5*), SHA1, 2 e 3 (*Secure Hash Algorithm*).

No trabalho de pesquisa foram feitos testes utilizando o modo AH com ESP em modo transporte, foram implementados como criptografia a função 3DES, e para autenticação o mecanismo HMAC com criptografia SHA1 e HMAC com MD5. A seguir descreveremos apenas os recursos utilizados como base para conhecimento.

- **3DES:** 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).

- **HMAC:** Mecanismo de autenticação de 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 da 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 :** Utiliza uma função de espalhamento unidirecional criada pela NSA, gera um valor *hash* 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).

Podemos descrever uma Associação de Segurança AS ou (Security Association SA) como um dos conceitos fundamentais do IPSec. Uma associação de segurança é uma "conexão" que viabiliza o tráfego de serviços seguros. A segurança dos serviços é garantida pela utilização dos protocolos de segurança (AH, ESP, ou ainda de ambos). Observa-se que, no caso de se usar AH e ESP em conjunto, mais de uma AS deve ser definida.

Uma associação de segurança é identificada unicamente por três parâmetros: o SPI (Security Parameter Index), o endereço IP de destino e o identificador do protocolo (AH ou ESP).

Para que dois dispositivos se conectem através de uma conexão segura, uma associação de segurança deve ser criada com um índice e os parâmetros de segurança. Essas informações estão contidas na SPI *(Security Parameter Index)* após a definição do endereço IP de destino (pertencente à entidade com que deseja estabelecer comunicação segura) essas informações são transmitidas sem criptografia.

O SPI é um campo que surge nos cabeçalhos de segurança IPv6 (AH e ESP), que não é encriptado na transmissão, já que a sua informação é essencial para decifrar a informação transmitida.

Assim, para cada sessão de comunicação autenticada entre dois nós, são necessários dois SPI - um para cada sentido, dado que cada associação de segurança é unidireccional. (SILVA; TEIXEIRA, 1999).

2.5.1 Cabeçalho AH

O cabeçalho AH tem a função de assegurar ao destinatário que o endereço IP realmente pertence ao remetente indicado no endereço de origem, com isso certifica que o conteúdo não sofreu modificações entre o remetente e o destinatário.

Para que essa segurança seja implementada, são feitas autenticações através de algoritmos de criptografia, os nativos para AH são: MD5 ou SHA1. (RFC 2402, 1998)

Formato do cabeçalho AH representado na Figura 5.

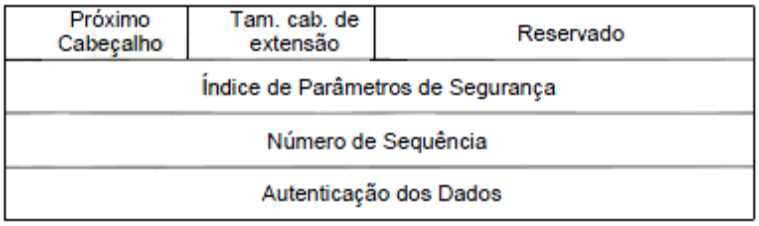

Figura 5 – Formato do Cabeçalho AH.
Fonte: Nic.BR (2011)

Os campos do cabeçalho AH são definidos como:

- **Próximo cabeçalho:** identifica o tipo de cabeçalho que vem após o AH, podendo ser outro cabeçalho IPSec (ESP) ou cabeçalhos TCP, UDP, ICMP, IP (se usar o modo de operação túnel) ou cabeçalhos de extensão;
- **Tamanho cabeçalho de extensão:** descreve quantas palavras de 32-*bits* seguem o campo SPI. Sua função é transmitir o comprimento do dado autenticado, esse campo varia em tamanho a cada transmissão do pacote. O comprimento do dado autenticado no AH pode variar dependendo do algoritmo usado;
- **Reservado**: é um campo reservado para uso futuro, preenchido com zero;
- **Índice de parâmetro de segurança (SPI):** as informações contidas nesse campo tem a função de índice na base de dados da SA *(Security Association)* do receptor do pacote, é utilizado para indicar qual algoritmo criptográfico usar;
- **Número de sequência:** sua função é informar o número de mensagens enviadas pelo transmissor para o receptor usando a SA atual. Previnem

ataques de *replay*, o transmissor deve enviar esta informação para o receptor, o que torna o receptor capaz de realizar esta prevenção;

- **Autenticação dos dados**: é o único campo de tamanho variável. Contém o *Integrity Check Value* (ICV), esse campo aloca a informação criptografada, com essa informação o receptor pode verificar a integridade a autenticidade dos dados recebidos, com o *bit* de *padding*, que podem ser inseridos caso seja necessário ajustar o tamanho deste campo aos limites exigidos pelo algoritmo. E um *checksum* seguro, criptograficamente gerado a partir da carga útil de dados, de alguns campos do IP e dos cabeçalhos de extensão, concatenado com uma chave secreta negociada entre as partes envolvidas na comunicação, durante o estabelecimento da SA e indexada pelo valor SPI. (NIC.BR, 2011a).

Segundo SILVA; FARIA, (2001) o uso do AH previne ataques do tipo:

- ***Replay*:** é realizado quando o atacante intercepta um pacote válido e autenticado pertencente a uma conexão, replica-o e o reenvia, "entrando na conversa". A utilização do campo *Sequence Number* ajuda na prevenção a este tipo de ataque, pois permite numerar os pacotes que trafegam dentro de uma determinada AS.

- ***Spoofing*:** nome dado ao atacante que assume o papel de uma máquina confiável para o destino e, com isso, ganha privilégios durante a comunicação. A autenticação AH previne este tipo de ataque;

- **MitM:** (*Man In the Middle*) homem no meio ou (*connection hijacking*) sequestro de conexão, ou seja, quando o atacante intercepta um pacote no contexto de uma conexão e passa a participar da comunicação, como se estivesse escutando uma conversa entre duas pessoas por um extensão da linha. A utilização de mecanismos de autenticação previne este tipo de ataque. (SILVA; FARIA, 2001).

Observa-se que o AH adiciona autenticação, ou seja, apenas verificou se o destinatário realmente é quem ele diz ser, porém, as informações continuam trafegando sem proteção pela rede em formato de texto, vulnerável a ser capturada através de *sniffer* e

visualizada pelo invasor. Assim, a confidencialidade é tratada por outro protocolo, que seria a encriptação da informação, tornando à ilegível ao invasor. Essa função faz parte da segurança provida pelo ESP.

2.5.2 Cabeçalho ESP (*Encapsulating Security Payload*)

O ESP permite a confidencialidade e autenticação dos dados encapsulados no pacote IP, garantindo que somente os destinatários autorizados tenham acesso ao conteúdo do pacote. O ESP pode ser usado no modo transporte ou no modo túnel, como será descrito posteriormente.

Formato do cabeçalho ESP representado na Figura 6.

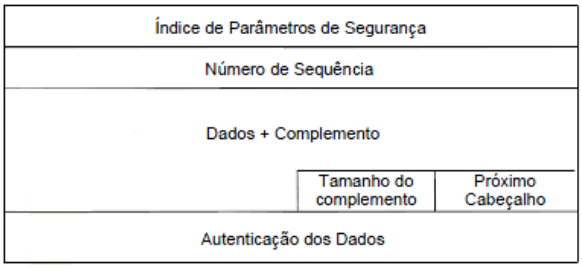

Figura 6 – Formato do Cabeçalho ESP.
Fonte: Nic.BR (2011)

Sendo os campos do cabeçalho ESP:

- **SPI:** é o índice na base de dados da SA do receptor do pacote e é utilizado para indicar qual algoritmo criptográfico usar;
- **Numero de Sequencia:** é o número de mensagens enviadas pelo transmissor para o receptor usando a SA atual. Previne ataques de *replay*

se o transmissor enviar esta informação para o receptor, o que torna o receptor capaz de realizar esta prevenção, se desejar;

- **Dados mais Complemento:** se a proteção oferecida para a mensagem for confidencialidade, este campo conterá uma versão cifrada do conteúdo da mensagem, o que substitui a mensagem inicial não cifrada. A parte cifrada também inclui os três campos do cabeçalho ESP seguindo os dados (*padding, pad length e next header*);
- **Tamanho do complemento:** número total de *bytes* do complemento contido no campo anterior;
- **Próximo Cabeçalho:** identifica o tipo de cabeçalho que segue o ESP, podendo ser cabeçalhos TCP, UDP, ICMP, IP (se usar o modo de operação túnel) ou cabeçalhos de extensão;
- **Autenticação dos Dados:** um campo opcional de tamanho variável que contém o ICV (*Integrity Check Value)*, se a mensagem receber proteção de autenticação e integridade. Porém, quando isso ocorre, a autenticação do ESP protege apenas o próprio cabeçalho. (NIC.BR, 2011)

O ESP protege o tráfego contra ataques do tipo:

- ***Replay:*** através da utilização do campo *Sequence Number*, de maneira análoga ao AH;
- **Particionamento de pacotes cifrados:** que é o que acontece quando o atacante obtém partes de pacotes cifrados e consegue montar um pacote que pode ser aceito por um dos membros da conexão. O uso de autenticação previne este tipo de ataque;
- ***Sniffer:*** ou seja, quando o atacante obtém os pacotes que trafegam na rede. A utilização da criptografia previne este tipo de ataque.

Em implementações em que se exige apenas a autenticação, ou ainda, onde a confidencialidade não deve ser usada, é recomendada a utilização do AH. No entanto, a

situação ideal é a utilização de confiabilidade e confidencialidade em conjunto, AH e ESP. (RFC 4294, 2006). Mais especificamente, é recomendado o uso do AH com a mensagem criptografada com ESP, permitindo que o destino verifique a autenticidade (AH) do pacote antes de decifrá-lo (ESP), ou ainda, verifique autenticidade e decifre o pacote em paralelo.

2.5.3 Associação de Segurança (SA)

A compreensão de uma *Security Association* (SA) é fundamental para a segurança do IPv6. Para que todo o processo funcione é necessário uma conexão SA entre os dispositivos. A segurança dos serviços é garantida pela utilização de segurança AH e ESP. Evidenciando que no caso de usar AH e ESP em conjunto, mais de uma SA deve ser definida. (RFC 2401, 1998). Uma associação de segurança é identificada por três parâmetros:

- ***Security Parameter Index* (SPI)**: que é um numero que identifica uma AS, esse parâmetro é definido durante a negociação da conexão. Todos os membros de uma AS devem conhecer o SPI correspondente e usa-lo durante a comunicação;
- **Endereço de IP de Destino**: que pode ser *unicast* ou *multicast.* No entanto, para a definição dos mecanismos de gerenciamento de SA, os mecanismos de segurança do IPv6 assumem um endereço *unicast*, estendendo as definições de *multicast*;
- **Identificador do Protocolo**: essa informação vem definida no cabeçalho nos códigos 51 para AH e o 50 para ESP.

Lembrando que o processo todo exige que a negociação para estabelecimento de uma AS envolve também a definição da chave, os algoritmos de criptografia e autenticação e os parâmetros usados por estes algoritmos.

A Associação De Segurança pode ser usada em dois modos de acordo com o que se deseja proteger. Em modo de transporte, um cabeçalho do protocolo IPSec (AH e ESP)

provê proteção para os protocolos das camadas superiores `a camada de rede, pois é inserido depois do cabeçalho IP original e antes do cabeçalho do protocolo superior. Esse modo é usado, geralmente, na topologia máquina-máquina e máquina-rede. (NIC.BR, 2011). Nas Figuras 7, 8 e 9 é mostrado onde são inseridos os cabeçalhos e quais cabeçalhos eles protegem.

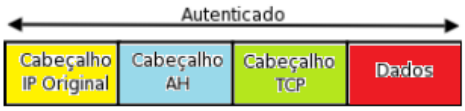

Figura 7 – AH em Modo Transporte.

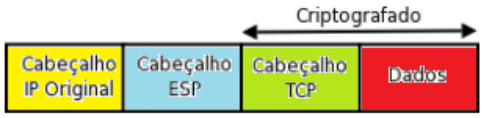

Figura 8 – ESP em Modo Transporte.

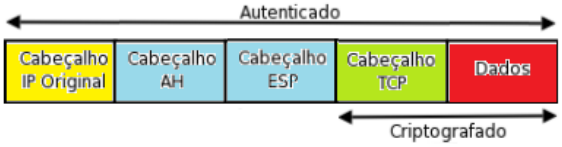

Figura 9 – AH e ESP em Modo Transporte.

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.

Não é descrito o modo túnel, pois o objetivo do trabalho testar somente o modo transporte, não se torna relevante ao trabalho considerações sobre o modo túnel.

2.6 Serviços Básicos em Redes IPv6

Com todas as mudanças descritas até o momento, o assunto mais relevante para o projeto é discutido a seguir com relação aos serviços básicos do protocolo IPv6.

O IETF *(Internet Engineering Task Force) vem ao longo dos anos* implementado e corrigido vários recursos para a comunicação em IPv6, a seguir citaremos os recursos implementados, como o recurso NDP (*Neighbor Discovery Protocol*) pertencente ao ICMPv6.

O protocolo ICMPv6 tem basicamente as mesmas funções do ICMP da versão IPv4 (RFC 1885, 1995) que são: informar características da rede, realizar diagnósticos e relatar erros no processamento de pacotes, essas informações são obtidas pela troca de mensagens ICMP (*Internet Control Message Protocol*) entre roteadores e *hosts* de uma rede, e são divididas em mensagem de erro e mensagem de informação. Em um pacote de dados, o cabeçalho ICMPv6 é precedido pelos cabeçalhos de extensão, se houver, e pelo cabeçalho base do IPv6. (NICBR, 2012). Sua estrutura geral é bem simples e igual nos dois tipos de mensagens.

O pacote ICMPv6 é identificado no cabeçalho IPv6 pelo valor 58 no campo chamado *Next Header*. Ele se localiza logo após os cabeçalho base do IPv6, se não existir cabeçalhos de extensão, conforme figura 10.

Figura 10 – Localização do Protocolo ICMPv6

Fonte: NicBr (2012).

2.6.1 Formato do Pacote ICMPv6.

O ICMPv6 possui um cabeçalho de estrutura simples, baseado em quatro campos básicos:

- O campo Type de 8 *bits*: especifica o tipo da mensagem e assim determina o formato do corpo da mensagem (campo Data). Um exemplo de seu uso é o valor 2 que representa uma mensagem "*Packet Too Big*".
- O campo Code de 8 *bits:* apresenta algumas informações adicionais sobre o motivo da mensagem. Um exemplo de seu uso seria para indicar a razão da falha de conexão entre dois dispositivos, numa mensagem "*Destination Unreachable*". Neste caso o valor 0 representaria que não há rota para o destino.
- O campo *Checksum* de 16 *bits*: é utilizado para detectar dados corrompidos no cabeçalho ICMPv6 e em parte do cabeçalho IPv6.
- O campo Data: mostra as informações relativas ao tipo da mensagem, podendo ser desde diagnósticos de rede até erros. Seu tamanho é variável de acordo com a mensagem, desde que não exceda o tamanho de MTU mínimo do IPv6 (1280 *bits*). (NICBR, 2012).

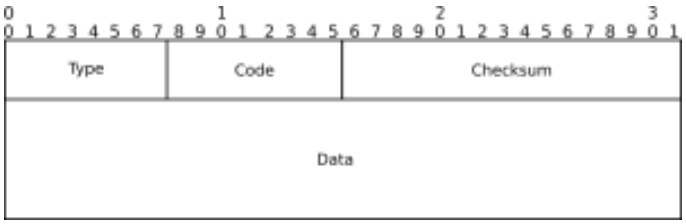

Figura 11 – Formato do Pacote ICMPv6
Fonte: NicBr (2012).

Devido o amplo conjunto de informações que podem ser transmitidas por meio dos pacotes ICMPv6, foram designadas duas classes para categorizar as mensagens: Erro e Informação. Será descrito somente a classe Informação, dentro dessa classe em especifico as mensagens: NA (*Neighbor Advertisement)* e RA (*Router Advertisement)*, devido sua

relevância na pesquisa. As demais mensagens de Informação e as de Erros poderão se consultadas na literatura disponível no final do trabalho. (NICBR, 2012).

2.6.2 NDP (*Neighbor Discovery Protocol*)

O protocolo de descoberta de vizinhança foi desenvolvido sob a finalidade de resolver os problemas de interação entre nós vizinhos em uma rede. Para isso ele atua sobre dois aspectos primordiais na comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes. (NICBR, 2012).

No caso da autoconfiguração de nós, o protocolo fornece suporte para a realização de três funcionalidades:

- *Parameter Discovery*: atua na descoberta por um nó de informações sobre o enlace (como MTU) e sobre a Internet (como *hop limit*).
- *Address Autoconfiguration:* trabalha com a autoconfiguração *stateless* de endereços nas interfaces de um nó.
- *Duplicate Address Detection:* utilizado para descobrir se o endereço que se deseja atribuir a uma interface já está sendo utilizado por um outro nó na rede.

Já no caso da transmissão de pacotes entre nós, o suporte é dado para a realização de seis funcionalidades:

- *Router Discovery:* trabalha com a descoberta de roteadores pertencentes ao enlace.
- *Prefix Discovery:* implementa a descoberta de prefixos de redes do enlace, cuja a finalidade é decidir para onde os pacotes serão direcionados numa comunicação (se é para um roteador especifico ou direto para um nó do enlace).

- *Address Resolution:* descobre o endereço físico através de um endereço lógico IPv6.
- *Neighbor Unreachability Detection:* permite que os nós descubram se um vizinho é ou se continua alcançável, uma vez que problemas podem acontecer tanto nos nós como na rede.
- *Redirect:* permite ao roteador informar ao nó uma rota melhor a ser utilizadao para enviar pacotes a determinado destino.
- *Next-Hop Determination:* algoritmo para mapear um endereço IP de destino em um endereço IP de um vizinho para onde o trafego deve ser enviado. (NICBR, 2012).

O protocolo NDP foi construído com base nas mensagens do protocolo ICMPv6 para a realização de suas tarefas. Para isso foram reservadas 5 tipos de mensagens:

- *Router Solicitation* (RS): A mensagem *Router Solicitation* é enviada por um dispositivo para requisitar aos roteadores o envio de mensagens *Router Advertisement.*
- *Router Advertisement* (RA): A mensagem *Router Advertisement* é enviada periodicamente ou em resposta à mensagem *Router Solicitation* por um roteador para anunciar sua presença no enlace.
- *Neighbor Solicitation* (NS): A mensagem *Neighbor Solicitation* é enviada por um dispositivo para requisitar a um determinado vizinho o envio de mensagens *Neighbor Advertisement*. Por causa dessa funcionalidade, ela é utilizada para suprir três necessidades básicas de comunicação em redes IPV6.
- *Neighbor Advertisement* (NA): A mensagem *Neighbor Advertisement* é enviada em resposta a uma mensagem *Neighbor Solicitation* ou espontaneamente para anunciar a mudança de alguma característica do dispositivo na rede de maneira rápida.

- *Redirect:* É enviada por roteadores para informar ao nó solicitante de uma comunicação informando o melhor caminho para seguir. (NICBR, 2012).

Essas funcionalidades foram criadas para que as rede baseadas em IPv6 exigisse uma menor complexidade possível em suas configurações, tornando se uma rede autônoma. Assim que um dispositivo se conecta a rede, o protocolo inicia um processo de integração a rede de forma automática, buscando vizinhança e anunciando sua presença na rede para outros dispositivos. (FLORENTINO, 2012). Nessa tentativa de integração, o dispositivo fica vulnerável a ataques. Algumas das mensagens ICMPv6 trocadas entre os dispositivos contem informações importantes para um invasor. Desabilitar ou bloquear essas troca de mensagens torna o gerenciamento de uma rede critico e trabalhoso.. (LINUX MAGAZINE, 2011).

3. Desenvolvimento

Este capítulo se inicia expondo uma visão das formas de obtenção de informações conhecidas para um ataque ao tráfego de dados, descrevendo materiais e o método utilizados na realização deste trabalho. Os materiais referem-se às tecnologias e ferramentas utilizadas nos testes de laboratório, para a análise das falhas. O método contém as etapas com os principais procedimentos utilizados para os testes.

O ICMPv6 apresenta uma quantidade maior de mensagem do que a versão utilizada com o IPv4. Esta característica se deve a incorporação das funções de outros protocolos como ARP/RARP (*Address Resolution Protocol - Reverse Address Resolution Protocol*) e IGMP (*Internet Group Management Protocol*). Desta forma o ICMPv6 se torna imprescindível para o funcionamento pleno do protocolo IPv6, sendo responsável pela descoberta de Vizinhança, gerenciamento de grupos *multicast* funcionamento da mobilidade IPv6, descoberta do *Path MTU (Maximum Transmission Unit)*, verificação de duplicidade de endereçamento entre outras funções.

Através dessas mensagens, facilmente um invasor conseguiria promover vários ataques como *Spoofing*, DoS (*Denial of Service*) *ou* MitM (*Man in the Middle*).

Na busca de solução para o problema a IETF criou um grupo de trabalho chamado SEND – *Securing Neighbor Discovery* que definiu um suporte para a segurança das

mensagens ICMPv6 *Neighbor Dicovery*, principal meio de ataque ao IPSec.

Foram sugeridas possíveis correção as falhas no protocolo ICMPv6 *Neighbor Discovery* como a criação de uma cadeia de certificados, a utilização de endereços gerados criptograficamente, assegurando que o transmissor de uma mensagem *Neighbor Advertisement* ou *Router Advertisement* seja o dono do endereço informado, criar uma nova opção *Neighbor Discovery*, chamada *Signature*, para proteger todas as mensagens relativas ao *Neighbor Discovery* e ao *Router Discovery*, e prevenir ataques de reenvio de mensagens por meio de duas novas opções no *Neighbor Discovery* o *Timestamp* para endereços *multicast* e *Nonce* para endereços *Unicast*. (RFC 3971, 2005).

Nonce se refere a uma informação no cabeçalho *Chechsum* para evitar o ataque por *spooff*. (RFC 4106, 2005).

Apesar dos esforços, o IPSec isoladamente não prove a segurança ao tráfego de dados, criptografar todos os dados usando todos os recurso do IPSec reduziria o desempenho da rede e aumentaria a carga de processamento nos dispositivos, sendo inviável para grandes redes implementar essa metodologia. Com o início da corrida para a ativação do IPv6, as técnicas já existentes mais o IPSec vão se tornando ferramentas importantes, dificultado o ataque aos dados. (LINUX MAGAZINE, 2011).

3.1 Materiais e Métodos

Para o desenvolvimento dos testes de segurança, foram utilizados três computadores, sendo duas estações de trabalho e uma estação atacante, os três foram interligados por um Switch não homologado para redes IPv6, simulando um ambiente de troca de dados, os testes foram feitos com sistemas operacionais Windows 7 SP1 e Ubuntu 12.04 com pacote ipsec-tools para configuração do IPSEC, IP *Security Polices* do Windows para associações seguras, THC-IPv6 Toolkit ferramenta de teste de vulnerabilidade em rede IPv6 e Wireshark para análise dos pacotes.

3.1.1 Ferramenta Ipsec-tools para administração do IPSEC

O IPsec-Tools (IPSEC-TOOLS, 2012) 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 automáticas através de um banco de dados de chave para IPsec.

O Pacote ipsec-tools contém alguns utilitários para manipular conexões IPSec:

- 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 QuickSec (QUICKSEC, 2012), porém o ipsec-tools é a ferramenta que possui maiores referências literárias e configuração mais acessível.

3.1.2 Ferramenta avançada do Windows

IP *Security Polices*, faz parte das diretivas de segurança do Windows, é uma ferramenta nativa do Windows presente na versão 2000 Server em diante, que vem sendo atualizada em cada geração de sistemas operacionais Microsoft, com a integração do IPv6 aos novos sistemas operacionais, o IP Security *Polices* se tornou uma ferramenta importante para a segurança do trafego de rede, estando integrado ao IPv6 nas versões 7 do Windows e 2008/10 Server. (MICROSOFT *LIBRARY*, 2012).

Toda a configuração é feita através de interface gráfica, como mostra a figura 12.

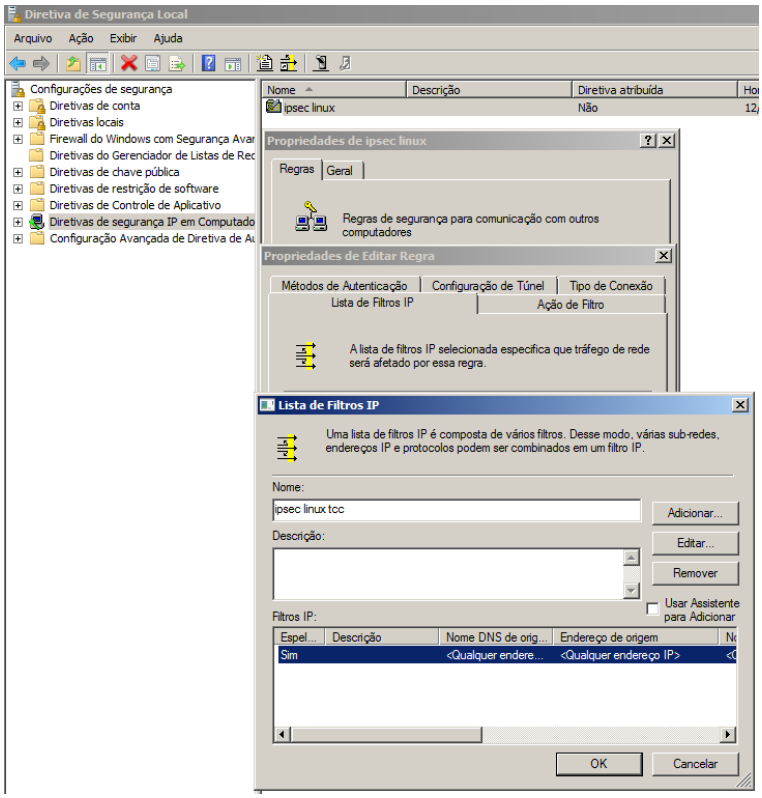

Figura 12 – Diretivas de Segurança IP

Fonte: Autoria Própria.

3.2 Método

Com o estudos sobre o protocolo IPv6 e IPSec que foram realizados no início do trabalho, pode-se entender a arquitetura dos protocolos e suas características de funcionamento para a o desenvolvimento dos cenários para os testes.

Após os cenários definidos, foram feitas as configurações no ambiente de rede utilizando o protocolo IPv6 e IPSec, para verificar se protocolo IPv6 garantirá a autenticidade da origem e dos dados por meio do AH e ESP, foram testados sistemas operacionais Windows

e Linux.

Os testes de interceptação dos dados foram feitos somente com o sistema operacional Linux, devida à limitação de compatibilidade da ferramenta THC.

Computadores com os sistemas operacionais Linux e Windows, transmitiram dados pela rede e esse trafego foi testado por ferramentas que praticam a técnica de *Spoofing*, buscando analisar se o AH e ESP são vulneráveis aos métodos de ataque. Os testes foram realizados com a ferramentas THC Toolkit, aplicando formas de *Spoofing* através de pacotes com informações do protocolo ICMPv6, o mesmo teste foi realizado intercalando os sistemas operacionais (ou simplesmente: SOs) sendo, primeiramente uma rede composta com computadores somente com o sistema operacional Linux, posteriormente, uma rede composta de computadores somente com o sistema operacional Windows e por ultimo um ambiente híbrido com os dois sistemas operacionais: Linux e Windows, buscando identificar se é possível aplicar a técnica de *Spoofing* quando ambos os sistemas operacionais estão presentes na mesma rede de computadores.

3.2.1 Metodologia de testes

As técnicas estudadas tiveram início no protocolo IPv4, mesmo com vários anos e muitos estudos, o IPv4 tem sido atormentado por ataques a camada de rede, conhecido como ARP *spoofing* . Para simplificar, ARP *spoofing* é um ataque do tipo ARP-*Poisoning* (ou ARP-*Spoofing*) é o meio mais eficiente de executar o ataque conhecido por *Man In The Middle*, que permite que o atacante intercepte informações confidenciais posicionando-se no meio de uma conexão entre dois ou mais dispositivos.

No ARP *Poisoning*, o dispositivo do atacante envia pacotes com respostas forjadas para requisições ARP de outros dispositivos da rede. O ARP é utilizado para descobrir os endereços MAC dos demais dispositivos da rede, já que os switches não entendem endereços IP. Esses pacotes forjados fazem com que os outros dispositivos passem a enviar seus pacotes

para o micro do atacante, que é configurado para capturar as transmissões e retransmitir os pacotes originais para os destinatários corretos. (GUIA DO HARDWARE, 2008).

Atualmente são conhecidas 3 formas de ataque utilizando as mensagens de *Router Advertisement* (RA) e protocolo *Neighbor Discovery* (ND), essas mensagens estão diretamente sujeitas da mesma maneira a 2 tipos básicos de ataques: DoS e *Address Spoofing* ou MitM (*Man in the middle*). (PACKETLIFE, 2009).

3.2.2 Definição dos testes

Podemos começar por interceptação (e modificar) mensagens enviadas entre duas máquinas em uma sub-rede, ou seja, realizar a MitM clássico (*Man in the Middle*). Realizar este tipo de ataque IPv4 é baseado na operação de requisições ARP (para o MAC correspondente um endereço IP) e em mensagens (DHCP para atribuir endereços IP dinamicamente), enviado tanto para o endereço de *broadcast* da sub-rede. Portanto, qualquer um pode responder a essas mensagens de falsificação e obter informações. Em IPv6 a técnica é a mesma, consiste no envio de mensagens ICMPv6 falsificadas em *multicast*.

3.2.3 Ferramenta de Teste

THC-IPv6 *Toolkit* (The Hackers Choice Kit de Ferramentas IPv6)

The Hackers Choice (THC) é um grupo de pesquisa, sem fins comerciais na área de segurança, que define como foco de suas pesquisas encontrar falhas de segurança, certificando que as informações estão realmente seguras. (THC, 2012).

THC-IPv6 *Toolkit*, é uma ferramenta disponível apenas para sistema operacionais

Linux, operada em modo *prompt* com a finalidade de promover testes de segurança em rede, em específico ao protocolo IPv6, explorando vulnerabilidades como: MitM (*Man-in-theMiddle*), NS *Spoofer*, NA *Spoofer*, DoS, DDoS.

O THC-ipv6 tool kit dispõem das seguintes ferramentas:

- *parasite6*: ferramenta que se aproveita das mensagens icmp *neighbor solitication/advertisement* para aplicar técnicas de *spoofer* ou *Man in the Middle*).
- *alive6*: é um *scan* de IPv6, usa a técnica de envio de mensagem de descoberta de vizinhança para obter endereços IP ativos na rede.
- dnsdict6: de DNS
- *fake_router6*: envia anúncios falsos da presença de um novo roteador na rede.
- *redir6*: redirecionador de tráfego inteligente, ideal para testes de (M*an in the Middle*) .
- *toobig6*: altera o MTU dos pacotes.
- *detect-new-ip6*: ferramenta para detectar novos endereços de IP que se integram a rede.
- *dos-new-ip6*: ferramenta que monitora e paralisa a cominação de novo IP entrantes em uma rede. (DOS).
- *trace6*: ferramenta para traçar rotas, utiliza das mensagens ICMP6 *echo request* e TCP-SYN para mapear o tráfego de dispositivos.

Na figura 13 mostra um teste utilizando a ferramenta alive6.

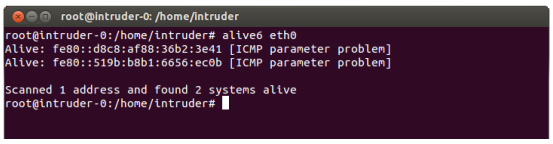

Figura 13 – Alive6

Wireshark

O Wireshark é um software de análise de pacotes, este programa faz a verificação dos pacotes transmitidos pela rede através de dispositivos de comunicação como placa de rede e USB 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 14.

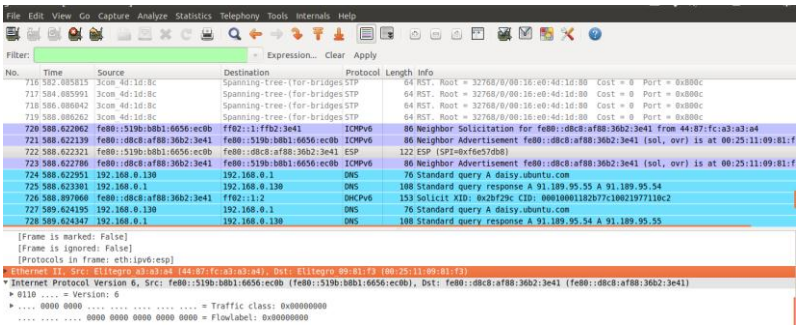

Figura 14 – Wireshark

Com wireshark é possível monitorar o tráfego de uma rede, permitindo visualizar os pacotes que trafegam na rede, descrevendo de forma organizada em uma lista de informações em tempo real, essas informações podem ser salvas e analisadas posteriormente.

Informações sobre Wireshark obtidas através do site (WIRESHARK FOUNDATION, 2012).

- 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.

3.2.4 Instalações das ferramentas de teste

Para exemplificar o processo de teste e o mesmo possa ser reproduzido, faremos uma descrição do processo de instalação das ferramentas, em geral são de fácil acesso e instalação.

Wireshark: su apt-get install wireshark

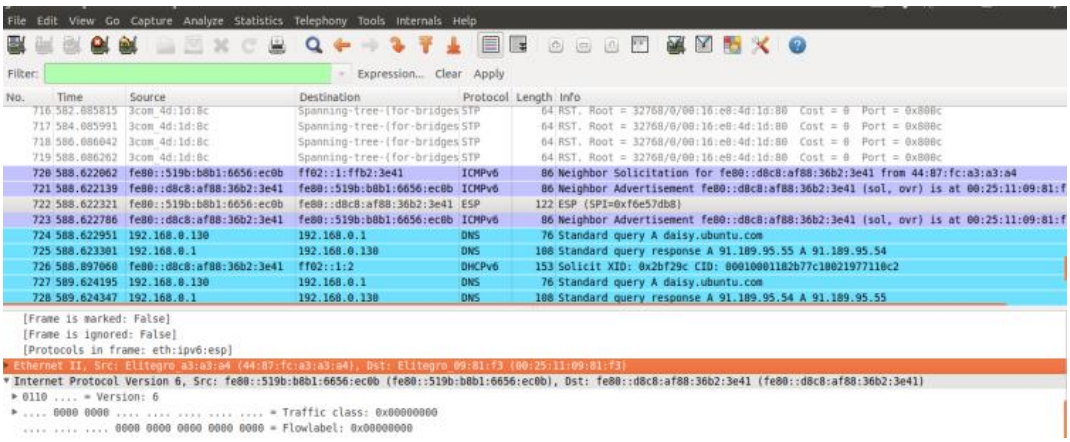

Figura 15 – Wireshark instalado

THC-IPv6 Toolkit: sudo apt-get install libpcap0.8-dev libssl-dev
cd ~/src/
wget http://www.thc.org/releases/thc-ipv6-1.8.tar.gz
tar xzvf thc-ipv6-1.8.tar.gz
cd thc-ipv6-1.8/
make
sudo make install

Comando para iniciar o ataque: Parasite6 eth0

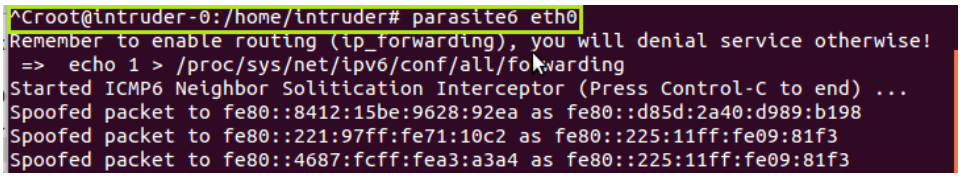

Figura 16 – THC-IPv6-Toolkit parasite6

3.2.5 Equipamentos

Para o teste descrito, foram utilizados os seguintes equipamentos: 1 switch camada 2 e três computadores, sendo:

1 Switch 3com Super Stack 3
Modelo 3C17302A

3 Computadores:
Processador AMD Athlon II X2 250
Memória RAM DDR3 1066 4Gb

Inicialmente foram feitas pesquisas de viabilidade quanto aos cenários e se identificou que não poderia ser feito os testes entre o sistema operacional Microsoft Windows 7 e o sistema operacional Ubuntu 12.04, devido as características de negociação entre os dois sistemas, quando iniciada uma conexão por uma estação Windows a combinação de AH e ESP sofre uma alteração, essa alteração não é interpretada pelo sistema Linux, que rejeita a autenticação. Existe *patch* recomendados pela Microsoft para correção, mas não foi encontrada nenhuma validação para essa correção, devido ao cronograma definido para o estudo ser curto, não permitiu realizar testes validando essa correção, para que não houvesse duvidas quanto ao resultado optamos em não testar esse cenário misto.

3.2.6 Configuração da Rede IPv6

Para todos os cenários propostos, foram feitas configurações manuais dos endereços, foram definidos endereços Locais FC00:: em IPv6 para se estabelecer uma comunicação *link local* entre os computadores.

Para os sistemas operacionais Windows foram utilizados os endereços Cliente 1 FC00::1010 e Cliente 2 FC00::1020.

Para os sistemas operacionais Ubuntu foram utilizados os endereços Cliente 1 FC00::1001, Cliente 2 FC00::1002 e Invasor FC00::1003.

Como pode ser visualizado na pagina 54 as figuras 17 a 21.

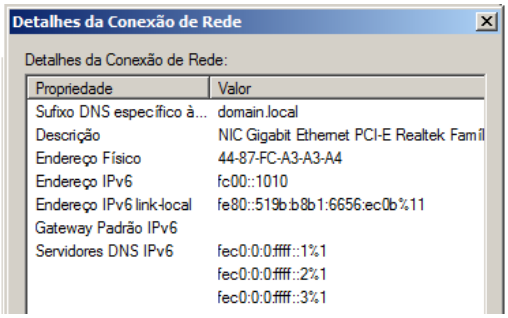

Figura 17 – Configurações rede Cliente 1

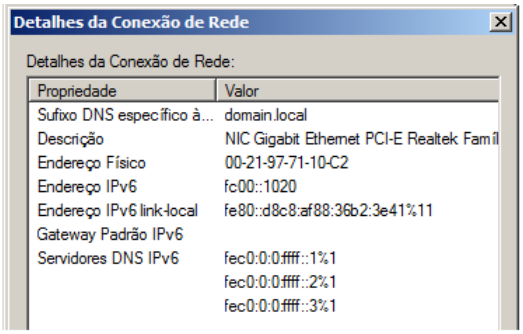

Figura 18 - Configurações rede Cliente 2

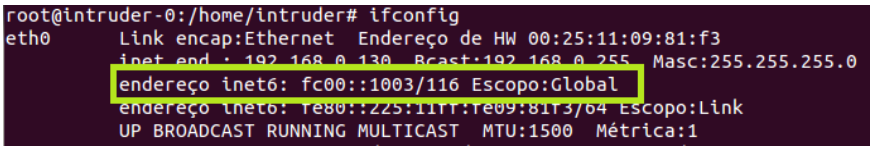

Figura 19 - Configurações rede Invasor

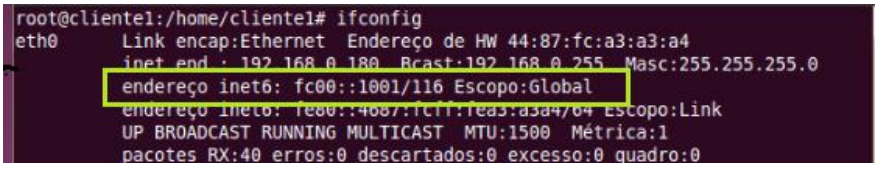

Figura 20 - Configurações rede cliente 1

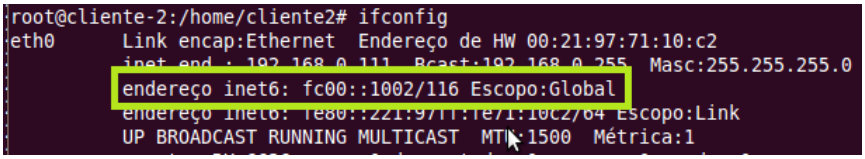

Figura 21 - Configurações rede cliente 2

3.2.7 Teste Conectividade

Para verificar a conectividade entre as estações foram realizados testes de conexão utilizando os comandos PING [IPv6 da máquina] para sistemas Microsoft e PING6 –I [interface] [IPv6 da máquina] para sistemas Linux.

Nas figuras 22 a 25 demostram o retorno positivo dos testes.

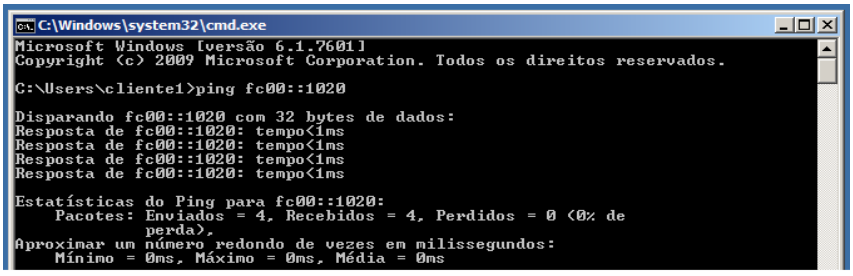

Figura 22 – Teste entre cliente 1 e 2 Windows

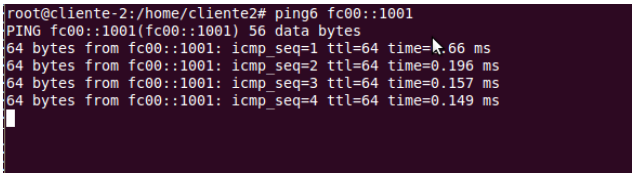

Figura 23 - Teste entre cliente 1 e 2 Linux

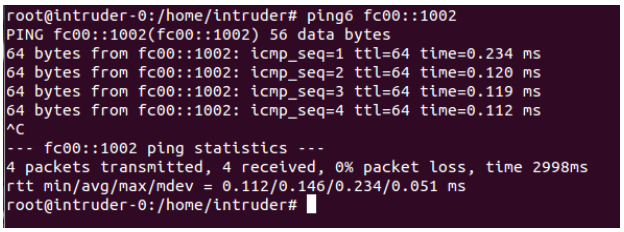

Figura 24 - Teste entre invasor e 2 Linux

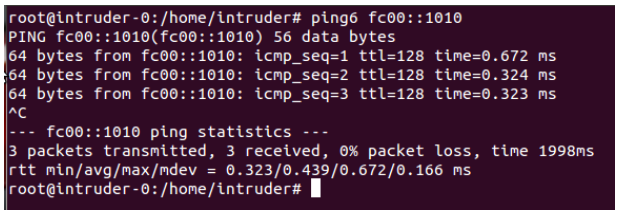

Figura 25 - Teste entre invasor e 2 Windows

3.2.8 Configuração do IPSec

Basicamente no Windows essa configuração é toda feita através de interface gráfica. Todas as configurações foram realizadas com base nas orientações da Microsoft[1]. (MICROSOFT SECPOL; 2012).

[1] Consultar ao final do trabalho nas referencias o procedimento completo (Microsoft secpol; 2012).

O procedimento realizado para Linux é padrão e foi retirado do material disponível na página do ipsec-tools KAME, os comandos ali descritos varia para cada distribuição.

Basicamente foi feita a instalação do *ipsec-tools*, após a conclusão foram acessados via *prompt* os respectivos arquivos de configuração e inseridas as regras de funcionamento. Para maiores detalhes consultar referencia (*redhat ipsec*).

Nas imagens 26 á 28 mostram as configurações realizadas:

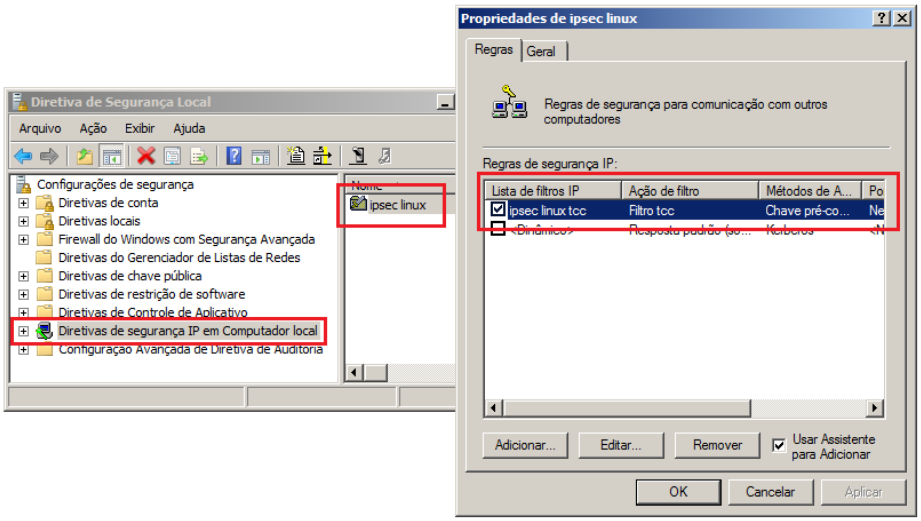

Figura 26 – Regra IPSec Windows

O processo de configuração deve ser feito em ambos os computadores.

As configurações realizadas no sistema Ubuntu podem ser vistas na Figura 27, as regras foram adicionadas no arquivo ipsec-tools.conf.

```
flush;
spdflush;

# Attention: Use this keys only for testing purposes!
# Generate your own keys!

# AH SAs using 128 bit long keys
add fc00::1010 fc00::1002 ah 0x200 -A hmac-md5
0x96358c90783bbfa3d7b196ceabe0536b;
add fc00::1002 fc00::1010 ah 0x300 -A hmac-md5
0x96358c90783bbfa3d7b196ceabe0536b;

# ESP SAs using 192 bit long keys (168 + 24 parity)
#add fc00::1001 fc00::1002 esp 0x201 -E 3des-cbc
#0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;
#add fc00::1002 fc00::1001 esp 0x301 -E 3des-cbc
#0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;

# Security policies
spdadd fc00::1010 fc00::1002 any -P in ipsec
           ah/transport//require;
#          esp /transport//require;

spdadd fc00::1002 fc00::1010 any -P out ipsec
           ah/transport//require;
#           esp/transport//require;
```

Figura 27 – Arquivo ipsec-tools.conf

```
root@cliente-2:/home/cliente2# setkey -DP
fc00::1002[any] fc00::1010[any] any
        out prio def ipsec
        ah/transport//require
        created: Nov 16 22:28:07 2012  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=105 seq=1 pid=1949
        refcnt=1
fc00::1010[any] fc00::1002[any] any
        fwd prio def ipsec
        ah/transport//require
        created: Nov 16 22:28:07 2012  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=98 seq=2 pid=1949
        refcnt=1
fc00::1010[any] fc00::1002[any] any
        in prio def ipsec
        ah/transport//require
        created: Nov 16 22:28:07 2012  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=88 seq=0 pid=1949
        refcnt=1
root@cliente-2:/home/cliente2#
```

Figura 28 – Verificação do serviço

4. Resultado das metodologias de teste

Após as configurações estudadas nos itens anteriores, foram iniciadas as transmissões de mensagens ICMPv6 NS e NA (*neighbour solicitation/advertisement spoofing*) forjados pela ferramenta parasite6 em conjunto com a ferramenta alive6 que envia mensagens de reconhecimento de vizinhança ND (*Neighbor Discovery*) na tentativa de que

alguma das duas estações venha a responder a mensagem e com isso a ferramenta pudesse interceptar o tráfego entre os dois computadores.

Entre os dois computadores foram feitas varias transmissões, entre elas: PING, acesso a diretório compartilhado e SSH, sendo que o comando PING atuou initerruptamente pelo período dos testes que duraram cerca de 60 min.

O mesmo procedimento foi aplicado para os dois cenários, chegando ao resultado de que o protocolo IPv6 sem a proteção do IPSec se torna vulnerável a ataques de mensagens NS e NA, já com a segurança implementada não foi obtido sucesso nos testes de interceptação dos pacotes e não houve respostas de vizinhança disparadas pelo *alive*6 .

Pode-se verificar nas figuras 29 e 30 a execução de teste sem a implementação do IPSec, a ferramenta *parasit*6 desvia o pacote sem que a origem e destino detectem o ataque, e a ferramenta Wireshark capturas os pacotes desviados.

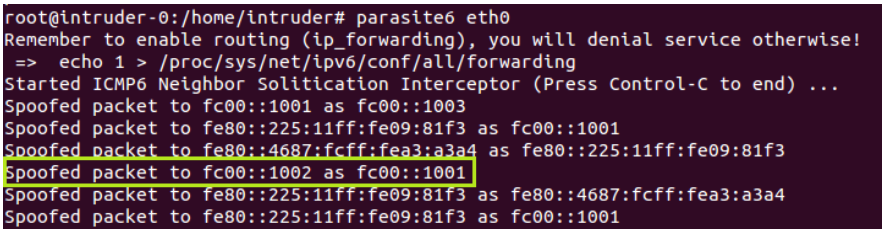

Figura 29 – *Parasite*6 invasor

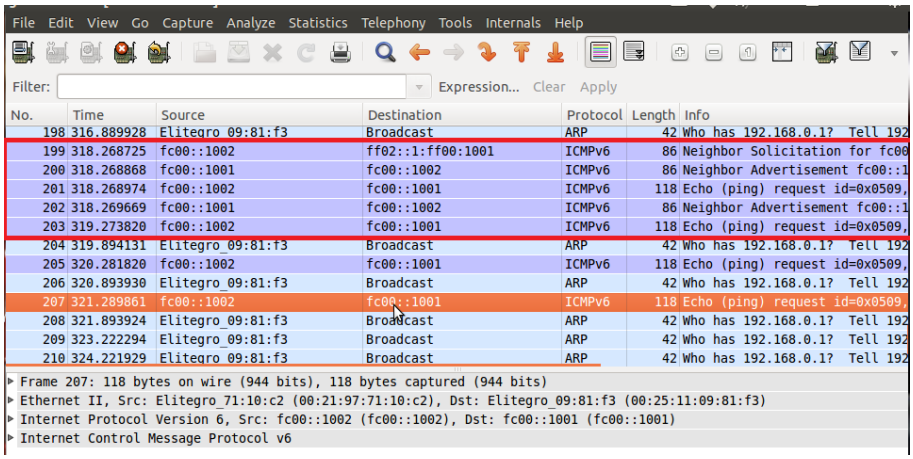

Figura 30 – Wireshark Invasor

O objetivo do teste foi demostrar que a ferramenta realmente interceptaria os pacotes, com isso foi implementada as configurações de segurança, e novamente realizamos os testes.

Como pode ser observado nas figuras 31 e 32 o teste demonstrou que após a configuração das regras de segurança do IPSec, as tentativas de se interceptar o trafego falharam, no período de 60 minutos foram realizados vários procedimentos com acesso a diretório compartilhado, PING e acesso SSH, em nenhum momento a ferramenta parasite6 efetivou uma interceptação. Foram realizados testes com a ferramenta *alive*6 aguardando uma resposta de solicitação de vizinhança, mas sem sucesso.

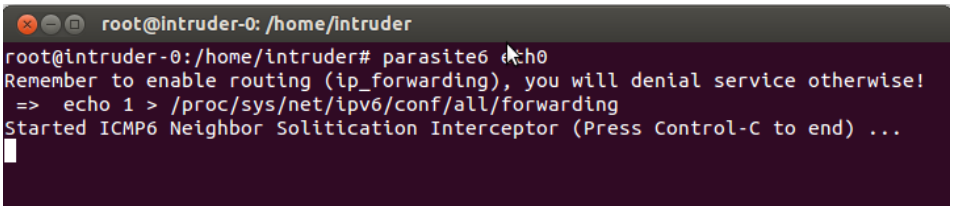

Figura 31 – parasite6 sem captura.

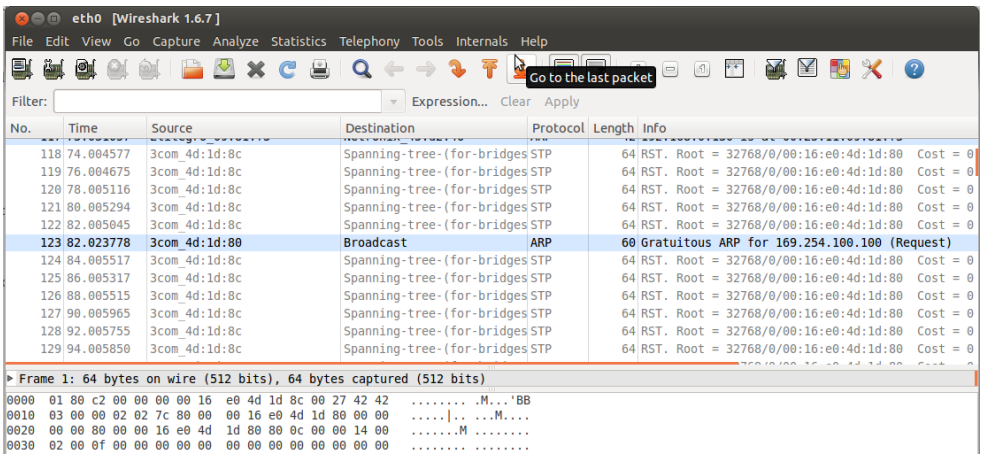

Figura 32 – Wireshark sem detecção

Os testes foram concluídos sem qualquer anomalia como fechamento do programa, mensagem de erro ou erros do sistema operacional.

Um resumo dos tipos de ataques, SOs testados e se estão vulneráveis ou não, são representados na tabela 1:

Tabela 1 – Comparativos de vulnerabilidade dos SOs

SO (Sistemas Operacional)	Sem IPSec	Com IPSec
Linux Ubuntu 12.04	Vulnerável a ataque MitM	Protegido contra MitM
Windows 7 Professional SP1	Vulnerável a ataque MitM	Protegido contra MitM
Linux Ubuntu 12.04	Vulnerável a ataque Scan	Protegido contra Scan
Windows 7 Professional SP1	Vulnerável a ataque Scan	Protegido contra Scan

5. Conclusão

No decorrer da realização do trabalho, nota-se que as principais alterações de segurança do IPv6 em relação ao IPv4 foi o uso nativo do IPSec, o uso desse recurso trouxe resultados satisfatórios. Olhando pela visão estrutural, o protocolo se tornou mais dinâmico, seu cabeçalho foi otimizado para que os padrões futuros sejam suportados, como as conexões moveis, o que torna o IPv6 um protocolo voltado as tendências futuras como o *Cloud Computing*, pois sua principal característica é a conexão ponto a ponto sem NAT com a segurança nativa do IPSec, tornando essa tendência um realidade.

Pode-se verificar nos testes que o tráfego de dados sem qualquer segurança ainda é um grande risco, a utilização do IPSec aumentou a segurança do canal de dados, impedindo que parte ou mesmo o tráfego inteiro, fosse desviado por um invasor, os testes mostraram que ao ativar o IPSec com as regras de conexão os *host* apenas respondem mensagens de outros *host* que estão na sua lista de confiança, ou seja, os *hosts* que não possuem a chave para uma

SA são automaticamente descartadas, com isso, a técnica de MitM não terá efeito, pois as mensagens são descartadas não retornando nenhuma informação ao invasor. Nas pesquisas sobre o assunto segurança da informação, o que se observa é o uso do IPSec em conjunto com outras técnicas como o controle de acesso baseado em porta com padrão 802.1x, monitorar o trafego de rede com softwares como o NDPMon, para detectar ataques aleatórios , evitando a criptografia de todo o tráfego.

A migração para a nova geração do protocolo IP, segue de forma inevitável, esse processo de transição deverá ocorrer ao logo do tempo e de forma gradual.

A implementação do IPSec nativo para IPv6 e os novos mecanismos para o novo protocolo, tornaram promissores a segurança no tráfego de dados.

5.1 Trabalhos Futuros

Como trabalho futuro existe a necessidade de se testar o desempenho da segurança IPSec em conjunto com *Cloud Computing*, visto que a evolução das ferramentas voltadas a negócio e a tendência das empresas em adotar o SaaS (*Software as a Service* ou software como serviço) segue uma tendência futura, tornaram imprescindível a elaboração de formas de proteger as informações entre as empresas e as nuvens ou seus provedores de serviço, de forma a não afetar o desempenho.

Elaborar cenários e testes mais complexos para verificar o desempenho do IPSec como um ambiente onde se trabalhe com *Active Directory*, no sentido de se testar desempenho e segurança.

Referências Bibliográficas

FLORENTINO, Adilson A. **IPv6 na Pratica.** 1º Edição, São Paulo, Linux New Media, 2012.

COMPUTERWORLD. **Banda larga no Brasil.** Disponível em: <http://computerworld.uol.com.br/telecom/2012/08/02/banda-larga-no-brasil-cresce-73-em-um-ano/ > Acessado em: set. 2012.

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

GUIA DO HARDWARE. **Segurança redes**. Disponível em: < http://www.hardware.com.br/livros/redes/arp-poisoning-mac-flooding.html> Acesso em: jun. 2012.

IETF. 2005. Disponível em: < http://www.ietf.org/rfc/rfc4301.txt> Acesso em: mai. 2012.

IGDNOW, **Internet no Brasil.** Disponível em: < http://idgnow.uol.com.br/internet/2012/09/25/brasil-ja-tem-mais-de-70-milhoes-com-acesso-direto-a-internet/ > Acesso em: set. 2012.

IMASTER. **Segurança TI.** Disponível em: < http://imasters.com.br/artigo/10117/seguranca/arp-poisoning>. Acesso em: jun. 2012.

IEEE 802.1x. **Port Based Network Access Control**. Disponivel em: < http://www.ieee802.org/1/pages/802.1x.html> Acesso em: out. 2012.

IPSEC-TOOLS. Disponível em:<ipsec-tools.sourceforge.net>. Acesso em: maio. 2012.

IPv6.BR. Disponível em: <www.ipv6.br>. Acesso em: abr. 2012.
_____. **Apostila IPv6**. Disponível em: <http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/IPv6-apostila.pdf >. Acessado em: mar. 2012.

KENT, S. A.; ATKINSON, R. **IP Authentication Header**. nov. 1998. Disponível em: <http://www.rfc-editor.org/rfc/rfc2402.txt>. Acesso em: out 2012.

_____. **IP Encapsulating Security Payload (ESP).** [S.l.], nov. 1998. 22 p. Disponível em: <http://www.rfc-editor.org/rfc/rfc2406.txt>. Acesso em: 22 out. 2012.

_____. **Security Architecture for the Internet Protocol.** [S.l.], nov. 1998. 66 p. Disponível em: <http://www.rfc-editor.org/rfc/rfc2401.txt>. Acesso em: 22 out. 2012.

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. 2012.

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

PACKETLIFE. **IPv6 neighbor spoofing. 2009.** Disponível em: < http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/ > Acesso em: set. 2012.

MICROSOFT SOLUTION. **Secpol.msc.** Disponível em: http://www.mcsesolution.com/Windows-Server-2008/configurando-o-ipsec-no-windows-server-2008.html. Acesso em: out. 2012.

MICROSOFT SUPORTE. **Conexão IPSec entre Windows e Linux.** Disponível em: < http://support.microsoft.com/kb/950826/pt>. Acessado set. 2012.

NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambientes Cooperativos**. 1. Ed. São Paulo: Novatec, 2007.

NIC.BR, **Últimos blocos IPv4.** São Paulo, 2001. Disponível em: < http://www.nic.br/imprensa/releases/2011/rl-2011-04.htm > Acesso em: abr. 2012.

_____. **Blocos IPv4**. Disponível em: < http://www.nic.br/imprensa/releases/2011/rl-2011-04.htm>. Acesso em: mar. 2012.

RFC 1885. (1995). Disponível em: <http://tools.ietf.org/html/rfc1885>. Acesso em: out. 2012.
RFC 2104. **HMAC: Keyed-Hashing for Message Authentication.** (1997). Disponível em: <http://www.ietf.org/rfc/rfc2104.txt>. Acesso em: out. 2012.

RFC 2401. (1995). **Security Architecture for the Internet Protocol.** Disponível em: <http://www.ietf.org/rfc/rfc2401.txt>. Acesso em: out. 2012.

RFC 2402. (1998). **IP Authentication Header.** Disponível em: <http://www.ietf.org/rfc/rfc2402.txt>. Acesso em: out. 2012.

RFC 3971. (1998). **SEcure Neighbor Discovery (SEND).** Disponível em: <http://www.ietf.org/rfc/rfc3971.txt>. Acesso em: out. 2012.

RFC 3971. (1998). **(GCM) and (ESP).** Disponível em: <http://www.ietf.org/rfc/rfc4106.txt>. Acesso em: out. 2012.

RFC 3971. (1998). **IPv6 Node Requirements.** Disponível em: <http://www.ietf.org/rfc/rfc4294.txt>. Acesso em: out. 2012.

RFC 4291; (2006). Disponível em < http://tools.ietf.org/html/rfc4291>. Acesso em: out. 2012.
SANTOS R. R; MOREIRA A. M; REIS E. A; ROCHA A. S. **Curso IPV6 Básico.** Disponível

em: http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/IPv6-apostila.pdf. Acesso em ago. 2012.

SILVA, A. J. S.; FARIA, M. R. **Hierarquia de Endereços** IPv6. 2001. Online. Disponível em: <http://www.rnp.br/newsgen/0103/end_ipv6.html>. Acesso em: out. 2012.

SILVA, A. J. S.; TEIXEIRA, R. C**. Arquitetura IP Security - Parte 1**. 1999. Online. Disponível em: < http://www.rnp.br/newsgen/9907/ipsec3.htm >. Acesso em: dez. 2012.

TCPDUMP/LIBPCAP. Disponível em: <http://www.tcpdump.org>. Acesso em: ago 2012

THC THE HACKER'S A CHOICE. THC-IPv6 Toolkit. Disponível em: < http://www.thc.org/>. Acessado em: ago. 2012.

THE KAME PROJECT. Disponível em: < http://www.kame.net/>. Acesso em: set. 2012.

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

WIRESHARK FOUNDATION. **About Wireshark**. Disponível em: <http://www.wireshark.org/about.html>. Acesso em: ago. 2012.

ZAPATER, M; SUZUKI, R. **Segurança da Informação**. 2005. Online. Disponível em: < http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf>. Acesso em: dez. 2012.